การออกแบบระบบเครือข่ายส่วนตัวเสมือนเพื่อตรวจสอบการทำงาน

VIRTUAL PRIVATE NETWORKING AIDED-DESIGN FOR MONITORING PERFORMANCE

วิโรจน์ จงชนะชวาวัฒน์
WIROTE JONGCHANACHAVAWAT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมไฟฟ้า
บัณฑิตวิทยาลัย
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2544

ISBN 974-648-428-1

การออกแบบระบบเครือข่ายส่วนตัวเสมือนเพื่อตรวจสอบการทำงาน

VIRTUAL PRIVATE NETWORKING AIDED-DESIGN FOR MONITORING PERFORMANCE

วิโรจน์ จงชนะชววัฒน์

WIROTE JONGCHANACHAVAWAT

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชาวิศวกรรมไฟฟ้า

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

พ.ศ. 2544

ISBN 974-648-428-1

VIRTUAL PRIVATE NETWORKING AIDED-DESIGN FOR MONITORING PERFORMANCE

WIROTE JONGCHANACHAVAWAT

A THESIS SUBMITTED IN PARTIAL FULFILLMENT

OF THE REQUIREMENT FOR THE DEGREE OF

MASTER OF ENGINEERING IN ELECTRICAL ENGINEERING

SCHOOL OF GRADUATE STUDIES

KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2001

ISBN 974-648-428-1

บัณฑิตวิทยาลัย

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การออกแบบระบบเครือข่ายส่วนตัวเสมือน เพื่อตรวจสอบการทำงาน
VIRTUAL PRIVATE NETWORKING AIDED-DESIGN FOR MONITORING PERFORMANCE

ชื่อนักศึกษา นายวิโรจน์ จงชนะชววัฒน์

รหัสประจำตัว 40061092

ปริญญา วิศวกรรมศาสตรมหาบัณฑิต

สาขาวิชา วิศวกรรมไฟฟ้า

อาจารย์ผู้ควบคุมวิทยานิพนธ์ รศ.ดร.กอบชัย เดชหาญ

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ผศ.ดร.ไกรสิน	ส่งวัฒนา	
รศ.สมยศ	จุณณะปิยะ	
รศ.ดร.สุวิพล	สิทธิชีวภาค	
รศ.ดร.ฟูศักดิ์	ชีวสุวิทย์	
รศ.ดร.กอบชัย	เดชหาญ	

วัน/เดือนปี ที่สอบ 28 กันยายน 2544 เวลา 13.30-15.30 น.

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

บัณฑิตวิทยาลัยรับรองแล้ว

(รศ.ดร.บุญวัฒน์ อัตชู)

คณบดีบัณฑิตวิทยาลัย

วันที่ 22 **เดือน** ตุลาคม **พ.ศ.** 2544

หัวข้อวิทยานิพนธ์	การออกแบบระบบเครือข่ายส่วนตัวเสมือน เพื่อตรวจสอบการทำงาน
นักศึกษา	นายวิโรจน์ จงชนะชววัฒน์
รหัสประจำตัว	40061092
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมไฟฟ้า
พ.ศ.	2544
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รศ.ดร. กอบชัย เดชหาญ

บทคัดย่อ

ความเจริญก้าวหน้าของเทคโนโลยีทางด้านเน็ตเวิร์คคอมพิวเตอร์ ในปัจจุบัน ทำให้เกิดประโยชน์ต่อการนำไปใช้งาน ในวงการธุรกิจ การศึกษา และการวิจัยมากมาย โดยเฉพาะอย่างยิ่งในวงการธุรกิจที่ต้องการให้ข้อมูลขององค์กรมีความปลอดภัย การลงทุนที่ต่ำ และสามารถรองรับการเปลี่ยนแปลงทางเทคโนโลยีได้อย่างรวดเร็ว เครือข่ายส่วนตัวเสมือน (VPN; Virtual Private Network) จึงถือว่าเป็นการออกแบบเครือข่ายด้วยความรู้ทางด้านเทคโนโลยีที่สามารถรองรับความต้องการขององค์กรต่างๆ ได้อย่างดี การวิจัยครั้งนี้ เป็นการออกแบบเครือข่ายส่วนตัวเสมือน เพื่อให้เห็นถึงสมรรถนะ และคุณสมบัติที่เด่นของการใช้ภายในองค์กร ที่ทำให้ผู้บริหารมีความมั่นใจในความปลอดภัยของข้อมูลที่เป็นความลับ และยังคงมีประสิทธิภาพทางด้านเน็ตเวิร์คที่ยอมรับได้ โดยใช้โทโปโลยีแบบไฟล์วอลล์ทูไคล์เอนท์ บนเครือข่ายแลน และแวน

Thesis Title	Virtual Private Networking Aided-Design for Monitoring Performance
Student	Mr. Wirote Jongchanachavawat
Student ID.	40061092
Degree	Master of Engineering
Programme	Electrical Engineering
Year	2001
Thesis Advisor	Assoc. Prof. Dr. Kobchai Dejhan

ABSTRACT

Advance of computer networking is beneficial to business, education and researches. Especially for businesses that require high security data, high profit margin and flexibility for supporting changes technology. Virtual private network (VPN) is the well-known for secured computerized networking of business's organizations. This thesis shows evident that VPN was good network performance and security for LAN and WAN designed with the firewall to client topology .

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้ สำเร็จลุล่วงได้อย่างดี ด้วยคำแนะนำ และคำปรึกษาเกี่ยวกับเครือข่ายส่วนตัวเสมือน จาก รศ.ดร. กอบชัย เดชหาญ ซึ่งเป็นอาจารย์ผู้ควบคุมวิทยานิพนธ์ ผู้วิจัยรู้สึกซาบซึ้งในความอนุเคราะห์จากท่าน และขอกราบขอบพระคุณเป็นอย่างสูง

ขอกราบนมัสการพระเดชพระคุณพระมงคลเทพมุนี(หลวงพ่อวัดปากน้ำ) ผู้เป็นต้นแบบในสอนสั่งให้ข้าพเจ้า รู้จักการนั่งสมาธิ และรู้วิธีแก้ปัญหาอย่างรอบคอบตามหลักของพระพุทธศาสนาขององค์สมเด็จพระสัมมาสัมพุทธเจ้า

ขอขอบพระคุณ ดร.สุนทร จริงจิตร, อ.ประพันธ์ และเพื่อนอาจารย์ สถาบันราชภัฏ สวนดุสิตที่ช่วยเหลือในการอนุเคราะห์อุปกรณ์ และให้คำแนะนำในบางจุดที่ผู้วิจัยติดปัญหาบางอย่างซึ่งมีส่วนช่วยทำให้ผู้วิจัยเข้าใจปัญหานั้น

ขอขอบพระคุณ อ.นภัทร และอ.เชื้อ ภาควิชาโทรคมนาคม สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ที่ช่วยให้คำปรึกษา แนะนำ และให้กำลังใจ กับผู้วิจัยเป็นอย่างดียิ่ง

ขอกราบขอบพระคุณด้วยความสำนึกในบุญคุณอันสูงสุดของบิดามารดาคือนายเจี๊ยบ แซ่จึง และนางเคี้ยม แซ่ลี้ แม้ท่านทั้งสองมิได้เรียนหนังสือมาก แต่ได้ให้กำเนิดข้าพเจ้า และให้การอบรมเลี้ยงดู บ่มนิสัยจนข้าพเจ้าสามารถศึกษาถึงระดับปริญญาโทนี้

ขอขอบคุณเพื่อน นักศึกษา และรุ่นน้องนักศึกษาที่ช่วยเหลือให้คำแนะนำต่างๆ พร้อมทั้งตรวจเทียบและแก้ไขทฤษฎีและอื่นๆ ที่ผิดพลาด จนสำเร็จสมบูรณ์ยิ่งขึ้นและยังให้กำลังใจต่อผู้วิจัยอย่างใกล้ชิดตลอดมา

สุดท้าย ขอขอบพระคุณผู้ที่ให้ความช่วยเหลือทุกท่านที่ไม่ได้เอ่ยนามมา ณ ที่นี้รวมถึงเจ้าหน้าที่บัณฑิตวิทยาลัยทุกท่าน คุณค่า และประโยชน์อันพึงมีจากวิทยานิพนธ์ฉบับนี้ ผู้วิจัยขอมอบแด่ผู้มีพระคุณทุกท่าน

วิโรจน์ จงชนะชววัฒน์

สารบัญ

สารบัญ

สารบัญ

สารบัญ

สารบัญตาราง

สารบัญรูป

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

สารบัญรูป(ต่อ)

บทที่ 1
บทนำ

1.1 ความเป็นมา และความสำคัญของปัญหา

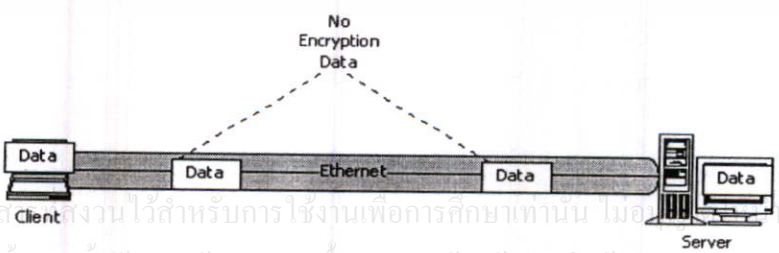
ความเจริญก้าวหน้าทางเทคโนโลยีด้านการสื่อสารข้อมูลผ่านเครือข่ายคอมพิวเตอร์ ทำให้สามารถมีการติดต่อสื่อสารผ่านกันได้ไม่ว่าผู้รับ และผู้ส่งจะอยู่กันคนละซีกโลก และสามารถที่จะรับส่งข้อมูลถึงกันได้อย่างมีประสิทธิภาพ โดยเฉพาะอย่างยิ่งในยุคนี้ ที่มีการพัฒนาเครือข่ายคอมพิวเตอร์ขนาดใหญ่ หรือเรียกว่าอินเทอร์เน็ต โดยมาจากการรวมกลุ่มของเครือข่ายย่อยๆ จำนวนมากขององค์กรต่างๆ ทั่วโลก ทำให้การติดต่อสื่อสารสามารถกระทำได้อย่างรวดเร็ว และสามารถเข้าถึงผู้รับสารได้ตลอดเวลาที่ผู้รับยังคงเชื่อมต่อกับเครือข่าย หรือไม่มีการเชื่อมต่อก็ตาม แต่ด้วยการที่มีบุคคลที่มีความรู้ แต่ขาดซึ่งคุณธรรมได้นำความรู้ทางด้านการสื่อสารข้อมูลผ่านเครือข่ายมาใช้ในการโจรกรรมข้อมูล หรือแก้ไข บิดเบือน เสริมความข้อมูล เพื่อให้ด้านรับเกิดความเสียหาย หรือนำข้อมูลที่เป็นความลับไปหาประโยชน์ใส่ตน

ดังนั้น การวิจัยครั้งจึงได้สนใจที่จะศึกษาวิทยาการการรักษาความปลอดภัย เครือข่ายคอมพิวเตอร์โดยได้นำหลักการวีพีเอ็น (VPN; Virtual Private Networking) มาทำการออกแบบศึกษาเครือข่ายส่วนตัวเสมือน หรือเครือข่ายวีพีเอ็น โดยได้ทำการตรวจสอบการทำงานคุณสมบัติทางด้านเน็ตเวิร์ค และความปลอดภัยที่จะได้รับ

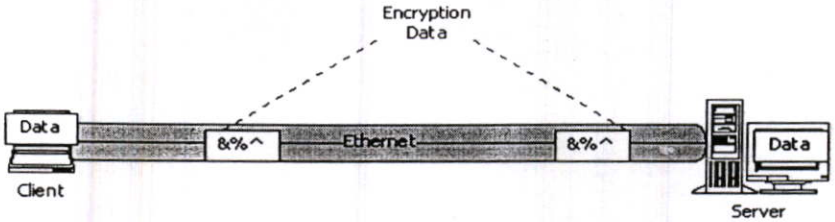
1.2 ความมุ่งหมาย และวัตถุประสงค์ของการศึกษา

ต้องการศึกษา และออกแบบเครือข่ายส่วนตัวเสมือนในวงแลน และวงแวนว่าสามารถทำให้เครือข่ายคอมพิวเตอร์มีความปลอดภัย และมีคุณสมบัติที่ยอมรับได้ในด้านเน็ตเวิร์ค

1.3 ทฤษฎี หรือแนวความคิดที่ใช้ในการวิจัย



รูปที่ 1.1 แสดงรูปการสื่อสารข้อมูลผ่านเครือข่ายรูปแบบเดิม



รูปที่ 1.2 แสดงรูปการสื่อสารข้อมูลผ่านเครือข่ายรูปแบบใหม่

หลักการเดิม ไม่มีการเอ็นคริปท์ชันข้อมูล แต่หลักการใหม่มีการเอ็นคริปท์ชันข้อมูล เพื่อให้มีความปลอดภัยมากยิ่งขึ้น ซึ่งปัจจุบันมีแฮกเกอร์เกิดขึ้นจำนวนมากซึ่งข้อมูลที่สำคัญ จะไม่ถูกนำออกจากระบบได้ และสามารถที่จะตรวจสอบผู้ที่จะนำข้อมูลนั้นๆ ไปใช้ได้

1.4 ขอบเขตการวิจัย

1.ทำการติดตั้งระบบเครือข่ายส่วนตัวเสมือนในวงแลน และแวน

2.ทำการตรวจสอบแพ็กเก็ต ขณะที่ใช้ระบบวีพีเอ็น และไม่ใช้วีพีเอ็น

3.ตรวจสอบการทำงานทางด้านเน็ตเวิร์ค โดยวัดพารามิเตอร์ที่สำคัญ คือค่าลาเทนซี (Latency) และค่าทรูพุท (Throughput) โดยเปรียบเทียบขณะที่ใช้วีพีเอ็น และไม่ใช้วีพีเอ็น

1.5 ขั้นตอนของการศึกษา

1.ทำการศึกษาทฤษฎีในการสร้างระบบเครือข่ายส่วนตัวเสมือน (VPN;Virtual Private Network)

2.ทำการออกแบบ และสร้างระบบเครือข่ายส่วนตัวเสมือน ในวงแลน และแวน

3.ทำการทดสอบคุณสมบัติในการเอ็นคริปท์ชันในการทำงานระดับแพ็กเก็ต โดยได้ทำการตรวจจับแพ็กเก็ตเพื่อตรวจสอบแพ็กเก็ต ขณะที่ใช้วีพีเอ็น และไม่ใช้วีพีเอ็น

4.ทำการตรวจสอบคุณสมบัติในด้านงานเน็ตเวิร์ค ซึ่งจะใช้พารามิเตอร์ที่สำคัญ 2 แบบ คือค่าลาเทนซี (Latency) และค่าทรูพุท โดยที่ค่าลาเทนซี ได้จากการ Ping แพ็กเก็ตที่มีขนาด Payload ที่แตกต่างกัน ส่วนในการตรวจสอบค่าทรูพุท จะใช้ FTP ไฟล์ขนาดต่างๆกัน คือ 3, 5, 7 และ 15 MB

5.สรุปผลที่ได้จากการตรวจสอบเครือข่ายส่วนตัวเสมือน

1.6 ประโยชน์ที่ได้รับ

1. ทำให้ทราบหลักการทำงานของเครือข่ายส่วนตัวเสมือน

2. ทำให้สามารถนำหลักการที่ได้มาประยุกต์ใช้ในการบริหารเครือข่ายคอมพิวเตอร์ให้เกิดประโยชน์สูงสุด โดยที่ต้องคำนึงถึงความปลอดภัยของเครือข่ายให้มากยิ่งขึ้น ตลอดจนถึงเป็นการนำแนวความคิดมาใช้ในยุคแห่งการสื่อสารที่ต้องมีการระมัดระวังในเรื่องของความปลอดภัยของข้อมูลเพื่อให้สามารถแข่งขันกับการเปิดเสรีในด้านต่างๆ โดยเฉพาะการค้าที่ต้องมีการแลกเปลี่ยนข้อมูลหรือมีการใช้การสื่อสารข้อมูลผ่านระบบออนไลน์ในการหักเงินผ่านบัญชีทางเครือข่ายอินเทอร์เน็ตได้

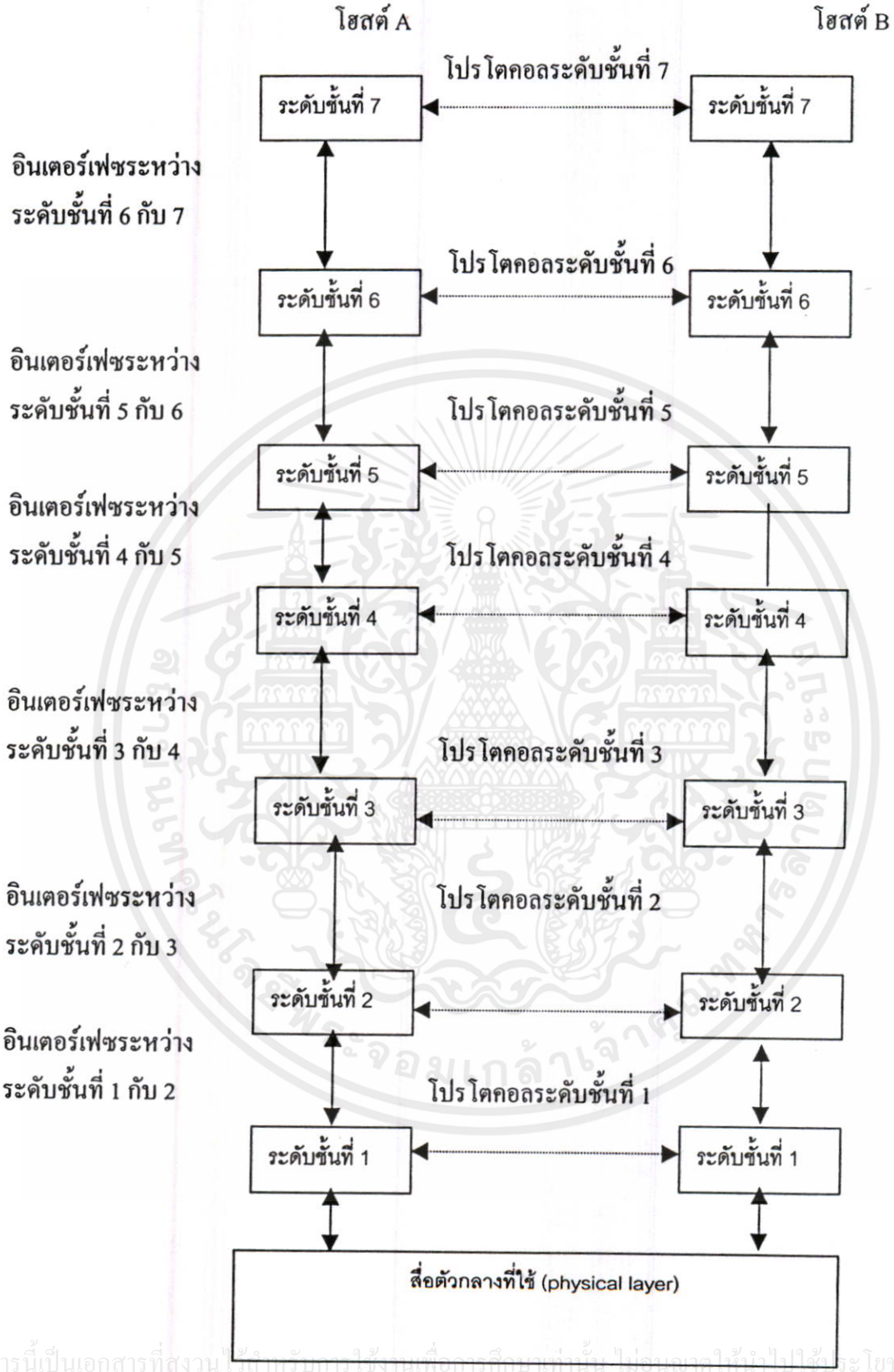
3. สามารถใช้เครือข่ายอินเทอร์เน็ต เพื่อติดต่อสื่อสารกันโดยถือว่าสามารถเป็นเครือข่ายส่วนตัวได้ จะทำให้องค์กรต่างๆ สามารถจะใช้ทรัพยากรของบริษัทได้อย่างมีประสิทธิภาพ เช่น องค์กรมีระบบศูนย์รวมข้อมูล แล้วบุคลากรในองค์กรต้องเดินทางไปยังประเทศใดๆ หรือเปิดสาขาของบริษัททั้งในและต่างประเทศ สามารถที่จะเข้าโครงข่ายอินเทอร์เน็ตเพื่อสามารถใช้ข้อมูลจากส่วนกลางของบริษัทได้ ประกอบกับไม่ต้องทำการวางระบบคอมพิวเตอร์ในสถานที่ต่างๆ หรือสาขาย่อย เป็นการประหยัดค่าใช้จ่ายในการลงทุนโครงข่าย อุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์ เช่น เครื่องขนาดใหญ่ เมนเฟรม เป็นต้น และรวมถึงค่าใช้จ่ายในการที่ต้องจ้างบุคคลากรทางด้านเทคนิคในการประจำสาขาต่างๆ ได้ด้วย

4. ทำให้ทราบแนวทางในการประยุกต์หลักการใหม่ที่กำลังจะเข้ามามีบทบาทอย่างมากขึ้นเรื่อยๆ ในประเทศไทย เพื่อจะทำให้ผู้บริหารเครือข่ายเตรียมความรู้ให้พร้อมกับการที่ผู้บริหารเครือข่ายจะต้องให้ความสนใจมากยิ่งขึ้น ในยุคการแข่งขันเสรี

บทที่ 2
สถาปัตยกรรมเครือข่ายคอมพิวเตอร์

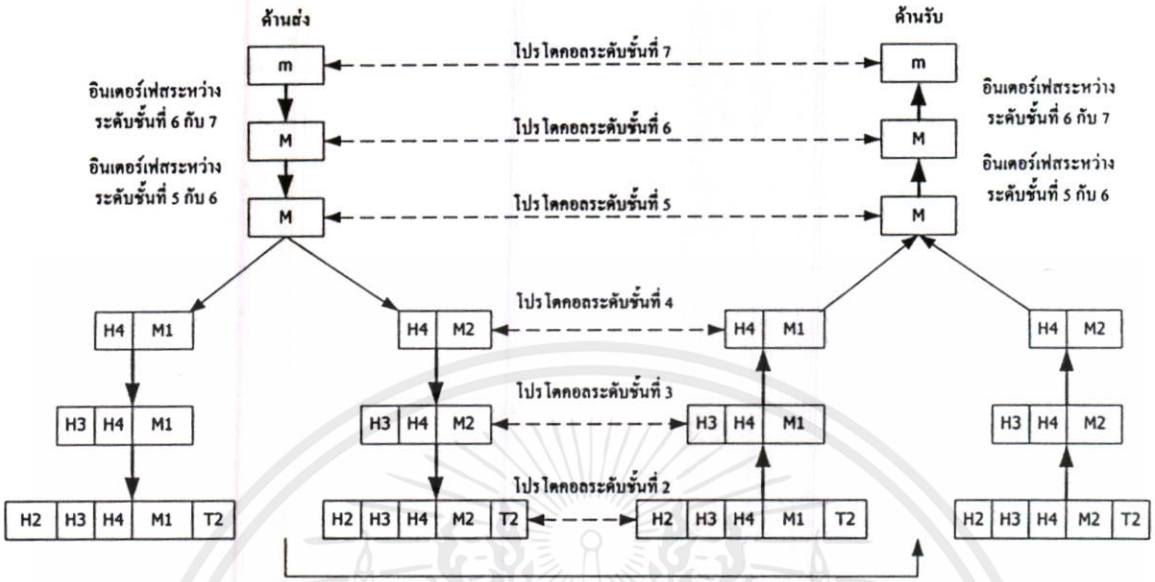
2.1 สถาปัตยกรรมเครือข่าย

หน้าที่การทำงานของการสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์มีการประยุกต์ใช้งานได้มากมาย ดังนั้นเพื่อให้การออกแบบระบบการสื่อสารข้อมูล และเครือข่ายคอมพิวเตอร์ง่ายขึ้น จึงมีการแบ่งสาระและหน้าที่ต่างๆ ของเครือข่ายคอมพิวเตอร์ออกเป็นหลายระดับชั้น (layer) ระดับล่างจะให้บริการแก่ระดับชั้นที่สูงกว่า เพื่อให้การส่งข้อมูลเป็นไปอย่างถูกต้องและมีประสิทธิภาพ โดยที่ระดับที่สูงกว่าไม่จำเป็นจะต้องรู้ว่าระดับชั้นล่างทำงานเป็นอย่างไรเพื่อให้บริการนั้นๆ ซึ่งคล้ายกันกับการเขียนโปรแกรมหลัก (main program) ใช้บริการของโปรแกรมย่อย (subprogram) โดยที่ไม่จำเป็นต้องรู้ว่าโปรแกรมย่อยมีการทำงานอย่างไร ในการทำงานของแต่ละระดับชั้นจะเป็นการให้บริการแก่ระดับบนกว่า แต่ละระดับจะมีการทำงานที่เรียกว่า เพียร์โปรเซสส์ (peer process) ซึ่งเพียร์โปรเซสส์ในระดับเดียวกันของอุปกรณ์สื่อสาร 2 เครื่องจะส่งข้อมูลติดต่อกันด้วยกฎเกณฑ์ที่แน่นอน ซึ่งกฎเกณฑ์ข้อบังคับที่ตกลงกันนี้ใช้ในการส่งข้อมูลติดต่ออย่างถูกต้อง และมีประสิทธิภาพระหว่างเพียร์โปรเซสส์ทั้งสองด้านเพื่อให้บริการแก่ระดับที่สูงกว่า สำหรับกฎเกณฑ์นี้ถูกเรียกว่า "โปรโตคอล (protocol)" ยกตัวอย่างเช่น โปรโตคอลที่ใช้ในการส่งข้อมูลติดต่อกันระหว่างเพียร์โปรเซสส์ในระดับชั้นที่ n เรียกว่าโปรโตคอลระดับที่ n (layer n protocol) การส่งข้อมูลระหว่างเพียร์โปรเซสส์ทั้งสองนี้ไม่ใช่เป็นการส่งข้อมูลกันโดยตรง แต่จะส่งข้อมูลผ่านลงมายังระดับที่ต่ำกว่าโดยใช้บริการของระดับชั้นที่ต่ำกว่า ซึ่งในท้ายสุดแล้วข้อมูลระหว่างเพียร์โปรเซสส์ทั้งสองจะถูกส่งจริงผ่านช่องสัญญาณสื่อตัวกลาง (physical layer) ที่เชื่อมระหว่างเครื่องทั้งสอง ดังนั้นจึงอาจกล่าวได้ว่าระหว่างเพียร์โปรเซสส์จะมีช่องสัญญาณทางตรรก (logical channel) เพื่อส่งข้อมูลโต้ตอบกัน แต่ข้อมูลจะถูกส่งจริงผ่านช่องสัญญาณของสื่อกลางจริง เมื่อข้อมูลถูกส่งจริงจากระดับสูงมายังระดับต่ำกว่า ทำให้มีการอินเตอร์เฟซกันระหว่างระดับชั้นที่ติดกัน ซึ่งการอินเตอร์เฟซนี้จะเป็นการกำหนดเนื้อหาและรูปแบบของการบริการที่ระดับล่างจะให้แก่ระดับที่สูงกว่า ดังนั้นในการออกแบบเครือข่ายที่ดี การอินเตอร์เฟซระหว่างระดับชั้นต้องถูกออกแบบให้รัดกุมเป็นการอินเตอร์เฟซแบบคลีน-คัท (clean-cut interface) หรือการออกแบบให้หน้าที่และการบริการต่างๆ ของแต่ละระดับชั้นชัดเจน และข้อมูลที่ส่งผ่านระหว่างอินเตอร์เฟซต้องให้มีจำนวนน้อยที่สุด การเปลี่ยนแปลงวิธีการสร้างเครือข่ายสำหรับแต่ละระดับชั้นจากเทคโนโลยีหนึ่งไปยังอีกเทคโนโลยีหนึ่งแล้วจะต้องสามารถทำได้โดยง่าย และสามารถให้บริการระดับชั้นที่สูงกว่าได้เหมือนเดิม และไม่กระทบต่อการทำงานของระดับชั้นที่สูงกว่านั้น ยกตัวอย่างเช่น การที่จะให้สื่อกลางจากสายโทรศัพท์เปลี่ยนเป็นการสื่อกลางเป็นดาวเทียม จะต้องไม่มีผลกระทบต่อโปรโตคอลที่ใช้ในแต่ละระดับชั้น



รูปที่ 2.1 แสดงการทำงานของแต่ละระดับชั้น และความสัมพันธ์ของระดับชั้น

ดังนั้น ชุดของระดับชั้นต่างๆ ตลอดจนโปรโตคอลในแต่ละชั้น ประกอบกันเป็นสถาปัตยกรรมเครือข่าย ซึ่งข้อกำหนดต่างๆ เช่น หน้าที่ สาระ และโปรโตคอลของสถาปัตยกรรมเครือข่าย ต้องมีข้อมูลที่เพียงพอกับการสร้างเครือข่ายได้ทั้ง ซอฟแวร์ หรือฮาร์ดแวร์ วิธีการสร้างเครือข่ายตลอดจนวิธีการอินเตอร์เฟซระหว่างอุปกรณ์ต่างๆ ในเครือข่ายไม่จำเป็นต้องกำหนดในสถาปัตยกรรมเครือข่าย นอกจากนั้นในเครือข่ายหนึ่งๆ รายการของโปรโตคอลทั้งหมดที่ถูกใช้ในแต่ละระดับชั้นเรียกว่า โปรโตคอลสแต็ก (protocol stack) เพื่อให้เข้าใจการทำงานของระดับชั้นต่างๆ ของเครือข่ายคอมพิวเตอร์มากขึ้น จะแสดงได้ดังรูปที่ 2.2 เป็นตัวอย่างที่ใช้ในการส่งข้อมูลของแต่ละระดับชั้น เป็นการส่งไฟล์ระหว่าง 2 เครื่อง โปรแกรมประยุกต์ของเครื่องที่ส่งจะส่งข้อมูลขนา m ให้แก่เพียร์โปรเซสส์ระดับที่ 7 ซึ่งเพียร์โปรเซสส์จะใส่เฮดเดอร์ (Header) เข้าไปพร้อมกับข้อมูล m นั้นแล้วส่งไปยังระดับที่ 6 โดยผ่านอินเตอร์เฟสระหว่างระดับ 6 และ 7 สำหรับเฮดเดอร์ที่เพิ่มเข้าไปนี้จะช่วยให้เพียร์โปรเซสส์ของระดับชั้นที่ 7 ของด้านรับสามารถทำงานได้ถูกต้องสอดคล้องกัน เช่น เฮดเดอร์อาจบ่งบอกสิทธิของผู้ส่งในการปรับปรุงไฟล์ข้อมูล เป็นต้น เมื่อระดับที่ 6 ได้รับข้อมูล ซึ่งก็คือ m + H7 ทำการบีบอัดขนาดข้อมูล และหรือ เข้ารหัสลับข้อมูลแล้วปะเฮดเดอร์เข้าไป ซึ่งจะทำให้ด้านรับสามารถแปลงข้อมูลกลับได้อย่างถูกต้อง สำหรับเพียร์โปรเซสส์ระดับที่ 5 เมื่อได้รับข้อมูล (m+H7+H6) จะปะเฮดเดอร์ของตนเองเพื่อให้บริการต่างๆ แก่ผู้ใช้ระดับสูงกว่า เช่น หากข้อมูลที่ส่งเป็นแฟ้มตำรา การกำหนดจุดแบ่งแยกของแต่ละบท ซึ่งจะช่วยให้มีการส่งข้อมูลใหม่ตั้งแต่บทที่ข้อมูลเกิดการเสียหายเท่านั้น โดยไม่ต้องส่งใหม่ตั้งแต่เริ่มต้น สำหรับระดับที่ 4 เมื่อได้รับข้อมูลจากระดับ 5 แล้วอาจจะแบ่งข้อมูลยาวๆ ออกเป็นข้อมูลที่สั้นเหมาะกับการส่งผ่านเครือข่าย แล้วปะเฮดเดอร์ซึ่งเป็นข้อมูลที่ช่วยในการควบคุมการส่ง เช่น ลำดับของข้อมูล ทำให้ด้านตรงข้ามสามารถเรียงลำดับข้อมูลได้อย่างถูกต้อง ระดับที่ 3 จะปะเฮดเดอร์เพื่อช่วยในการหาเส้นทางเดินของข้อมูลผ่านโหนดต่างๆ ของเครือข่าย แล้วส่งข้อมูลให้แก่ระดับที่ 2 ระดับนี้นอกจากจะปะเฮดเดอร์แล้วยังปะเทรเลอร์ (trailer) ซึ่งช่วยในการตรวจสอบว่าข้อมูลที่ส่งไปนั้นถูกสัญญาณรบกวนในสายรบกวนจนเสียหายหรือไม่ หลังจากนั้นจึงส่งข้อมูลให้แก่ระดับชั้นที่ 1 เพื่อส่งข้อมูลผ่านสายสื่อสารซึ่งเป็นตัวกลางส่งข้อมูลส่งข้อมูลต่อไป สำหรับด้านรับเมื่อได้รับข้อมูลแล้ว แต่ละระดับชั้น จะใช้เฮดเดอร์ในระดับเดียวกันทำงานให้สอดคล้องกับเพียร์โปรเซสส์ของด้านส่ง แล้วจึงถอดเฮดเดอร์ในระดับนั้นๆ ออก ส่งเฉพาะข้อมูลให้แก่ระดับที่สูงกว่าจากรูปที่ 2.2 จะเห็นว่าเพียร์โปรเซสส์ในระดับเดียวกันจะมีการส่งข้อมูลติดต่อกันด้วยกฎเกณฑ์ที่กำหนดไว้ในระดับชั้นนั้น เพื่อให้การส่งข้อมูลเป็นไปได้อย่างถูกต้องและมีประสิทธิภาพ การส่งข้อมูลนี้เสมือนกับมีการส่งข้อมูลถึงกันโดยตรงผ่านช่องสัญญาณทางตรรก ในความเป็นจริง การส่งข้อมูลจะถูกผ่านมายังระดับที่ต่ำกว่าและถูกส่งถึงกันจริงโดยผ่านสื่อตัวกลางเท่านั้น



รูปที่ 2.2 แสดงตัวอย่างการส่งข้อมูลระหว่างเครื่อง 2 เครื่องโดยผ่านระดับชั้นต่างๆ

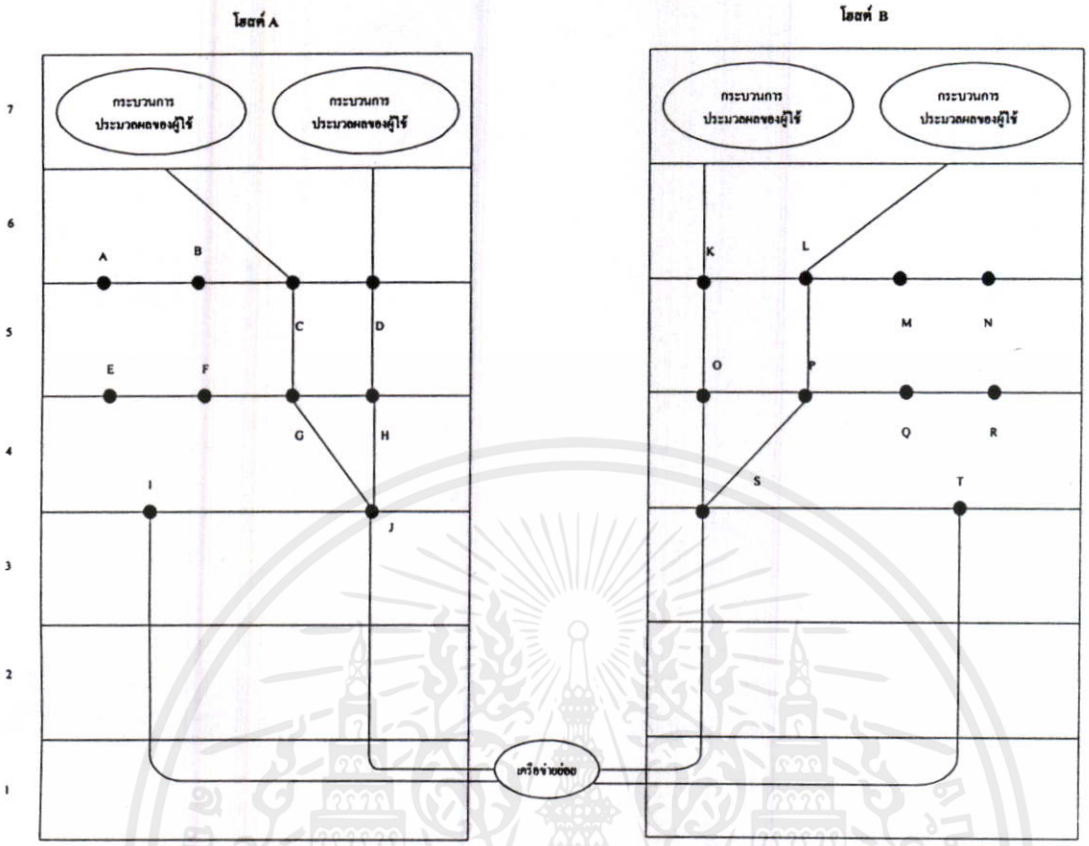
2.2 หลักการในการให้บริการของแต่ละระดับชั้น

หน้าที่หลักของแต่ละระดับชั้นคือ การให้บริการแก่ระดับชั้นที่สูงกว่า ในแต่ละระดับชั้นจะมีตัวทำงานที่เรียกว่า เอนทิตี้ (entity) ซึ่งอาจจะเป็นซอฟท์แวร์เอนทิตี้ เช่น กระบวนการประมวลผล หรืออาจจะเป็นฮาร์ดแวร์เอนทิตี้ สำหรับเอนทิตี้ในระดับเดียวกันบนเครื่องต่างกันเรียกว่า เพียร์เอนทิตี้ (peer entity) ปกติแล้วเอนทิตี้ในระดับที่ N จะทำงานเพื่อบริการให้แก่ระดับชั้นที่ N+1 ในกรณีนี้ระดับชั้น N เรียกว่า ผู้ให้บริการ (service provider) และระดับชั้นที่ N+1 เรียกว่า ผู้ใช้บริการ (service user) และการบริการอาจมีคุณภาพแตกต่างกันไป เช่น การส่งข้อมูลแบบรวดเร็วจะมีค่าใช้จ่ายสูง หรือการส่งข้อมูลช้าแต่ราคาถูก การส่งข้อมูลแบบเชื่อถือได้และรับรองความถูกต้องของการส่งข้อมูลหรือไม่รับรอง เป็นต้น การให้บริการของระดับชั้นที่ต่ำแก่ระดับชั้นที่สูงกว่า มีการกำหนดชนิดของการบริการว่าเป็นการบริการเกี่ยวกับอะไร และผู้ใช้ต้องทำอย่างไรบ้างจึงจะใช้บริการนั้นๆ ได้ และมีการกำหนดจุด (ตำแหน่ง) ที่มีการให้บริการ ซึ่งปกติแล้วการบริการจะทำได้ ณ จุดที่ให้บริการ (Service Access Point, SAP) เท่านั้น เช่น จุดที่ให้บริการของระดับชั้น N เป็นตำแหน่งที่ระดับชั้น N ให้บริการแก่ระดับชั้น N+1 ซึ่งแต่ละจุดที่ให้บริการ จะมีแอดเดรสของตัวเอง ตัวอย่างเช่น ในระบบโทรศัพท์ จุดที่ให้บริการจะเป็นเต้ารับ (socket) ของสายโทรศัพท์ที่องค์การโทรศัพท์ให้แต่ละผู้ใช้ และผู้ใช้จะเสียบสายจากเครื่องโทรศัพท์เข้ากับเต้ารับนี้ และแอดเดรสของจุดที่ให้บริการ คือเบอร์โทรศัพท์ของเต้ารับ ดังนั้นผู้ใช้จะใช้โทรศัพท์ไปหาใคร ผู้ใช้ต้องทราบแอดเดรสจุดที่ให้บริการของผู้นั้น เพื่อส่งข้อมูลให้แก่ผู้รับผ่านจุดที่ให้บริการ หรืออย่างเช่น การใช้บริการ

โปรแกรมอินเตอร์รัปท์ของดอสนั้น โปรแกรมประยุกต์ต้องทราบอินเตอร์รัปท์เวกเตอร์ (interrupt vector) เป็นแอดเดรสจุดที่ให้บริการ ดังนั้นจะเห็นได้ว่าการบริการจะเกิดขึ้น ณ ตำแหน่งของจุดที่ให้บริการ และในการส่งข้อมูลจากระดับชั้นสูงกว่าให้แก่ระดับชั้นต่ำนั้น ข้อมูลจะถูกส่งผ่านจุดที่ให้บริการจุดที่ให้บริการ ดังแสดงได้ในรูปที่ 2.3

2.2.1 การบริการแบบการเชื่อมต่อแบบต่อเนื่อง (Connection-oriented) และการเชื่อมต่อแบบไม่ต่อเนื่อง (Connectionless)

การให้บริการของระดับชั้นที่ต่ำแก่ระดับชั้นที่สูงกว่าแบ่งออกได้เป็น 2 ประเภท ประเภทแรกเรียกว่า การบริการแบบการเชื่อมต่อแบบต่อเนื่อง (Connection-oriented) ซึ่งคล้ายกับการบริการของระบบโทรศัพท์ เมื่อต้องการติดต่อกับใคร จะต้องสร้างการติดต่อ (establish connection) โดยหมุนหมายเลขโทรศัพท์ติดต่อเรียกไปยังฝ่ายรับ เมื่อฝ่ายรับๆ แล้วจะสามารถติดต่อสนทนากันได้ โดยข้อความที่ถึงผู้รับจะเรียงลำดับเช่นเดียวกับข้อความจากผู้ส่ง เมื่อสนทนาจบแล้ว จะมีการวางหู (disconnection) มีลักษณะเดียวกันกับการบริการแบบการเชื่อมต่อแบบต่อเนื่อง ผู้ใช้บริการต้องสร้างการติดต่อก่อนโดยอาศัยแอดเดรสของผู้รับ เมื่อมีการติดต่อแล้ว จะเหมือนกับมีช่องหรือท่อให้ข้อมูลผ่าน ซึ่งข้อมูลจะถูกส่งเรียงลำดับกันไปผ่านช่องหรือท่อนั้น โดยข้อมูลที่ส่งไปนั้นไม่เป็นต้องมีแอดเดรสของผู้รับอีก หลังจากส่งข้อมูลแล้วจะเลิกการติดต่อสำหรับการบริการแบบการเชื่อมต่อแบบไม่ต่อเนื่อง จะคล้ายกับการบริการของระบบไปรษณีย์ ซึ่งการส่งจดหมายแต่ละฉบับไม่ต้องมีการสร้างการติดต่อกับผู้รับก่อน จดหมายแต่ละฉบับจะต้องมีที่อยู่ของผู้รับปะไปด้วย และจดหมายฉบับต่างๆ ที่ถูกส่งจากที่หนึ่งไปยังอีกที่หนึ่งนั้นอาจถูกส่งผ่านเส้นทางไม่เหมือนกัน ทำให้จดหมายฉบับต่างๆ ของผู้ส่งที่ไปถึงผู้รับเป็นแบบไม่เรียงตามลำดับได้ ซึ่งเหมือนกับการให้บริการแบบการเชื่อมต่อแบบไม่ต่อเนื่อง ที่ไม่ต้องมีการสร้างการติดต่อของการส่ง การส่งข้อมูลแต่ละครั้งจะต้องมีการปะแอดเดรสของผู้รับ และข้อมูลแต่ละครั้งก็อาจถูกส่งไปตามเส้นทางแตกต่างกันไป ทำให้ข้อมูลที่ไปถึงผู้รับอาจมีลำดับแตกต่างจากลำดับการส่ง การบริการทั้งสองแบบนี้ยังแบ่งออกได้ตามคุณภาพของการให้บริการ กล่าวคือ กาบริการอาจเป็นแบบเชื่อถือได้ ซึ่งผู้ให้บริการรับประกันว่าจะไม่มีข้อมูลเสียหาย, สูญหายหรือข้อมูลซ้ำ การบริการแบบนี้มักจะทำโดยการให้ผู้รับตอบรับ (acknowledge) ข้อมูลที่ได้รับ ทำให้ผู้ส่งแน่ใจได้ว่าข้อมูลถึงผู้รับแล้ว การใช้บริการแบบการเชื่อมต่อแบบต่อเนื่องที่เชื่อถือได้ เช่น การส่งแฟ้มข้อมูล (file transfer) ซึ่งผู้ส่งต้องการให้ข้อมูลถูกส่งครบถ้วนถูกต้องและเรียงลำดับ นอกจากนี้การบริการแบบ การเชื่อมต่อแบบต่อเนื่อง ที่เชื่อถือได้นี้อาจแบ่งได้เป็น 2 รูปแบบคือ แมสเสจสตรีม (message stream) และไบท์สตรีม (byte stream) สำหรับแมสเสจสตรีมมีการกำหนดขอบเขตขนาดข้อมูลที่ส่งเช่น การส่งข้อมูลเป็นบล็อก บล็อกละ 1 กิโลไบท์ ซึ่งหากมีการส่ง 2 บล็อก ข้อมูลจะถึงด้านรับ 2 บล็อก บล็อกละ 1 กิโลไบท์ ส่วนแบบ



รูปที่ 2.3 แสดงการส่งข้อมูลผ่านอินเตอร์เฟส ณ ตำแหน่งจุดที่ให้บริการ

ไบท์สตรีม (byte stream) นั้นจะเป็นการส่งข้อมูลเป็นไบท์ติดต่อกันไป โดยไม่บ่งถึงขอบเขตของบล็อกข้อมูล ดังนั้น แบบนี้เมื่อผู้รับได้รับข้อมูล 2 กิโลไบท์ ผู้รับจะไม่ทราบว่าผู้ส่งส่งมา 2 ชุด ชุดละ 1 กิโลไบท์ หรือชุดเดียว 2 กิโลไบท์ สำหรับแบบ แมสเสจสตรีมนั้นเหมาะกับการประยุกต์แบบการส่งแฟ้มข้อมูล ข้อความ เอกสาร ตำรา ซึ่งข้อมูลถูกแบ่งและส่งเป็นหน้า ๆ ส่วนในการล็อกอินของเทอร์มินัลเข้าสู่โฮสต์ ซึ่งมีการทยอยส่งข้อมูลที่ละตัวอักษร โต้ตอบระหว่างเทอร์มินัลกับโฮสต์นั้นอาจเป็นแบบไบท์สตรีมได้ เนื่องจากการบริการแบบเชื่อถือได้ มักทำโดยมีการตอบรับของผู้รับและการส่งการตอบรับนี้ ทำให้เกิดโอเวอร์เฮดและทำให้ล่าช้า ซึ่งสำหรับงานประยุกต์บางอย่าง เช่น การส่งข้อมูลเสียง ผู้ใช้ต้องการได้พูดคุยส่งข้อมูลต่อเนื่องกันโดยไม่มีการล่าช้าขาดตอน ถึงแม้ว่าข้อมูลบางส่วนจะเสียหาย หรือสูญหายไปบ้าง งานประยุกต์เช่นนี้ ต้องการใช้การบริการที่รวดเร็ว ถึงแม้จะไม่รับประกันว่าข้อมูลถูกต้อง กล่าวคือ เป็นการบริการแบบการเชื่อมต่อแบบต่อเนื่อง ที่ไม่น่าเชื่อถือ (unrealiable service) ได้ สำหรับการบริการแบบการเชื่อมต่อแบบไม่ต่อเนื่อง (Connectionless) นั้นจะเหมาะสำหรับงานประยุกต์ เช่น ระบบจดหมายอิเล็กทรอนิกส์ ซึ่งไม่จำเป็นต้องสร้างการติดต่อระหว่างผู้ส่งกับผู้รับก่อน นอกจากนั้นผู้ส่งจดหมายบางรายอาจไม่ต้องการการส่งแบบน่าเชื่อถือ เพราะการส่งแบบนั้นจะต้องเสียค่าใช้จ่ายเพิ่มขึ้น ซึ่งการบริการแบบ

Connectionless ที่ไม่รับประกันความน่าเชื่อถือนี้เรียกว่าดาต้าแกรมเซอร์วิส (datagram service) ซึ่งคล้ายกับการบริการส่งโทรเลขนั่นเอง แต่ในงานบางอย่างผู้ใช้อาจต้องการบริการแบบการเชื่อมต่อแบบไม่ต่อเนื่อง ที่มีการตอบรับจากผู้รับยืนยันการรับข้อมูลด้วย ตัวอย่างของงานประเภทนี้ เช่น การส่งจดหมายลงทะเบียน เป็นต้น ซึ่งการบริการแบบนี้เรียกว่า แอคโนเลจดาต้าแกรมเซอร์วิส (acknowledged datagram service) การบริการแบบการเชื่อมต่อแบบไม่ต่อเนื่อง มีลักษณะหนึ่งคือ ด้านหนึ่งส่งข้อความเพื่อสอบถาม (request) ข้อมูลบางอย่างจากอีกด้านหนึ่ง ซึ่งด้านนั้นเมื่อได้รับข้อความสอบถามแล้วก็ค้นหาข้อมูลแล้วส่งข้อมูลตอบกลับ (reply) ไปให้ เมื่อข้อมูลตอบกลับมาถึงด้านที่สอบถามไป ด้านนั้นก็จะทราบทันทีว่าข้อความที่ส่งไปเพื่อสอบถามนั้นถึงด้านตรงข้ามแล้ว นั่นคือ การส่งข้อมูลตอบกลับมาบ่งบอกถึงการตอบรับของข้อความที่ส่งไปสอบถามด้วย การบริการในลักษณะนี้เรียกว่า การบริการร้องขอโต้ตอบ (request-reply service) รูปที่ 2.4 แสดงถึงรูปแบบต่าง ๆ ของการบริการของระดับชั้นล่างที่ให้แก่ระดับชั้นที่สูงกว่า

	การบริการ	ตัวอย่างการบริการ
Connection-oriented	message stream แบบเชื่อถือได้	การส่งเอกสารเป็นหน้าต่อๆ กันไป
	byte stream แบบเชื่อถือได้	การล็อกอินเข้าสู่โฮสต์
	แบบ Connection ที่ไม่น่าเชื่อถือ	ข้อมูลเสียง
Connectionless	datagram แบบไม่น่าเชื่อถือ	จดหมายอิเล็กทรอนิกส์
	datagram แบบเชื่อถือได้	จดหมายลงทะเบียน
	request - reply	การสอบถามฐานข้อมูล

รูปที่ 2.4 แสดงรูปแบบต่าง ๆ ของการให้บริการ

2.2.2 พริมิทีฟที่ใช้ในการบริการ (Service Primitive)

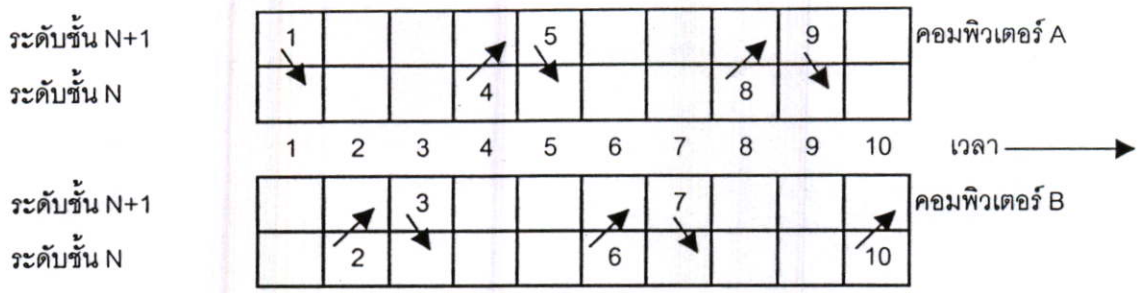
การบริการที่ระดับล่างให้แก่ระดับที่สูงกว่ามีได้หลายชนิด โดยผู้ใช้บริการจะอาศัยพริมิทีฟ (primitive) ต่าง ๆ ที่ระดับชั้นล่างได้กำหนดให้ใช้ในการรับบริการ เมื่อผู้ใช้ ๆ พริมิทีฟนี้จะทำให้เอนทิตี้ของระดับล่างทำงาน หรือรายงานข้อมูลบางอย่างให้แก่ผู้ใช้ เช่น พริมิทีฟชนิดคอนเน็คชันรีเควส (Connection Request) ซึ่งเมื่อถูกใช้ เมื่อผู้ใช้ขอใช้บริการในการติดต่อกับเพียร์เอนทิตี้ด้านตรงข้าม เมื่อผู้ใช้ใช้พริมิทีฟนั้น ระดับชั้นล่างก็จะทำงานให้มีการติดต่อได้ระหว่างเพียร์เอนทิตี้ของระดับชั้นบน หรือพริมิทีฟชนิด ดาต้ารีเควส (Data Request) ถูกใช้เพื่อขอส่งข้อมูล หรือพริมิทีฟชนิดดิสคอนเน็คชันรีเควส (Disconnection Request) ซึ่งถูกใช้ในการยกเลิกการติดต่อ หรือพริมิทีฟชนิดรีพอตท์อินดิเคชัน (Report Indication) ซึ่งถูกใช้ในการรายงานเหตุการณ์ หรือปัญหาที่เกิดในระดับชั้นล่างให้แก่ระดับชั้นบน เป็นต้นโดยทั่วไป อาจแบ่งพริมิทีฟเหล่านี้ออกเป็น 4 ชนิดคือ ร้องขอ (Request) รายงานเหตุการณ์ (Indication) ตอบสนอง (Response) และ ยืนยัน (Confirm) ดัง

แสดงในรูปที่ 5 พริมิทีฟชนิด ร้องขอ จะถูกใช้เมื่อผู้ใช้บริการต้องการจะให้ระดับชั้นล่างบริการในการทำงานบางอย่าง เช่นใช้คาต้ารีเควส (Data Request) ในการขอบริการส่งข้อมูล หรือ Abort Request ถูกใช้ในการยกเลิกการส่งข้อมูล เป็นต้น พริมิทีฟชนิดรายงานเหตุการณ์ (Indication) จะถูกส่งจากระดับชั้นล่างเพื่อให้เอนทิตี้ในระดับชั้นที่สูงทราบว่ามีเหตุการณ์ หรือการทำงานเกิดขึ้นอันเนื่องมาจากมีการร้องขอ จากผู้ใช้ด้านตรงข้าม กล่าวคือ เมื่อมีการร้องขอ ใช้บริการทำงานจากเพียร์เอนทิตี้ด้านหนึ่ง และ ร้องขอนั้นได้ถูกทำงาน หรือส่งมาแล้วจะมี Indication ซึ่งบ่งบอกถึงเหตุการณ์ หรือการทำงานของการร้องขอ นั้นส่งขึ้นมาให้เพียร์เอนทิตี้ของอีกด้าน เช่น เมื่อมีการใช้บริการคาต้ารีเควสแล้ว เมื่อข้อมูลถูกส่งมาถึงด้านรับ เพียร์เอนทิตี้ของด้านรับจะได้รับคาต้าอินดิเคชัน จากระดับชั้นที่ต่ำกว่า เป็นต้น นอกจากนั้น หากการให้บริการ หรือการทำงานของการร้องขอบางอย่างไม่สำเร็จ อาจมีอินดิเคชัน จากระดับชั้นล่างของผู้ขอใช้บริการส่งขึ้นมาให้ทราบ พร้อมทั้งชี้แจงเหตุผลของการให้บริการ หรือการทำงานไม่สำเร็จด้วย เช่นในการร้องขอ เพื่อขอใช้บริการติดต่อกับเพียร์เอนทิตี้ตรงข้าม หากผู้ให้บริการไม่สามารถทำการติดต่อให้ได้ จะมีการส่งดิสคอนเน็คอินดิเคชัน (Disconnect Indication) ให้แก่ผู้ใช้บริการนั้น พร้อมกับบ่งบอกถึงเหตุผลที่ไม่สามารถทำการติดต่อได้ด้วย สำหรับพริมิทีฟชนิด ร้องขอนั้น เอนทิตี้ของผู้ใช้บริการที่อยู่ในระดับชั้นข้างบนจะใช้ในการตอบสนองต่อเหตุการณ์ หรือ การทำงานของแต่ละการร้องขอ เช่น เมื่อมีคอนเน็คชันอินดิเคชัน(Connect Indication) ซึ่งบ่งบอกการขอติดต่อจากเพียร์เอนทิตี้ด้านตรงข้าง เอนทิตี้ด้านที่ถูกขอติดต่อมาอาจจะตอบสนองไปโดยมีโต้ตอบการร้องขอ เพื่อแสดงการยอมรับของการร้องขอนั้น สำหรับพริมิทีฟชนิดยืนยันนั้น จะถูกส่งจากผู้ให้บริการบ่งบอกให้ผู้ใช้บริการทราบว่าเอนทิตี้ด้านตรงข้ามมีการตอบสนองต่อการร้องขอนั้นอย่างใด

พริมิทีฟ	ความหมาย
Request	เอนทิตี้ต้องการให้ชั้นล่างบริการในการทำงานบางอย่าง
Indication	เอนทตี้ข้างบนได้รับรายงานเหตุการณ์หรือการทำงานที่เกิดขึ้น
Response	เอนทิตี้ต้องการตอบสนองต่อเหตุการณ์นั้น
Confirm	เอนทิตี้ได้รับการตอบสนองเกี่ยวกับสิ่งที่ขอบริการไป

รูปที่ 2.5 แสดงชนิดต่าง ๆ ของพริมิทีฟ

ลักษณะการใช้พริมิทีฟทั้ง 4 ชนิดในการขอใช้บริการ จะเปรียบเทียบได้คล้ายกับในการใช้บริการของระบบโทรศัพท์ ซึ่งมีขั้นตอนดังแสดงในตัวอย่างต่อไปนี้



1.	Connect Request	ผู้ใช้ต้นทางหมุนหมายเลขโทรศัพท์
2.	Connect Indication	เสียงโทรศัพท์ดังที่ผู้ใช้ปลายทาง
3.	Connect Response	ผู้ใช้ปลายทางยกหูโทรศัพท์
4.	Connect Confirm	ผู้ใช้ต้นทางได้ยินเสียงสัญญาณเรียกของโทรศัพท์หยุดไป
5.	Data Request	ผู้ใช้ต้นทางพูดส่งข้อความ
6.	Data Indication	ผู้ใช้ปลายทางได้ยินข้อความ
7.	Data Request	ผู้ใช้ปลายทางตอบกลับข้อความนั้น
8	Data Indication	ผู้ใช้ต้นทางได้ยินข้อความที่ตอบกลับมา
9	Disconnect Request	ผู้ใช้ต้นทางวางหูโทรศัพท์
10.	Disconnect Indication	ผู้ใช้ปลายทางได้ยินเสียงวางหูโทรศัพท์และวางหูด้วย

รูปที่ 2.6 แสดงตัวอย่างการใช้พริมิทีฟระหว่างผู้ใช้บริการและผู้ให้บริการ

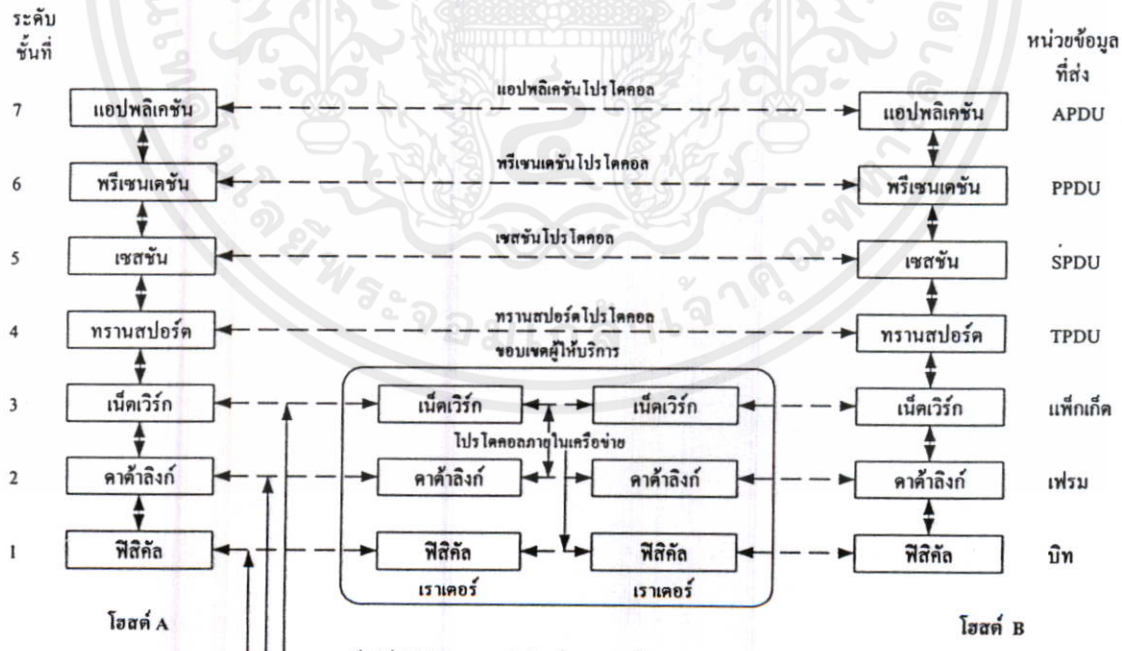
จากตัวอย่างข้างต้นจะเห็นได้ว่า การบริการบางอย่าง เช่น การขอบริการติดต่อปลายทางนั้น อาจจะต้องได้รับการยืนยันโดยมีการตอบสนองจากด้านตรงข้าม การบริการประเภทนี้เรียกว่า การบริการที่ต้องการการยืนยัน (Confirmed Service) ซึ่งจะมีการใช้พริมิทีฟทั้ง 4 ชนิด คือ ร้องขอ ,การรายงานเหตุการณ์, การโต้ตอบ และการยืนยัน เพื่อให้การบริการเสร็จสมบูรณ์ ส่วนการบริการ เช่น การขอยกเลิกการติดต่อ ไม่จำเป็นต้องได้รับการยืนยัน การบริการแบบนี้เรียกว่า การบริการที่ไม่ต้องยืนยัน (Unconfirmed Service) ซึ่งจะมีการใช้พริมิทีฟชนิดร้องขอ และ รายงานเหตุการณ์เท่านั้น ส่วนพริมิทีฟ สำหรับการบริการบางอย่าง เช่น การขอส่งข้อมูลนั้นอาจเป็นแบบต้องการยืนยัน หรือไม่ต้องยืนยันขึ้นอยู่กับว่าผู้ส่งว่าต้องการได้รับการตอบรับหรือไม่ สุดท้ายนี้ขอกล่าวถึงความสัมพันธ์ระหว่างการให้บริการกับโปรโตคอล กล่าวคือ เอนทิตี้ของระดับชั้นบนจะใช้บริการต่าง ๆ จากระดับชั้นล่างโดยการบริการจะเกิดที่จุดที่ให้บริการของอินเตอร์เฟสระหว่างระดับชั้นที่ติดกัน นอกจากนั้นระดับชั้นล่างจะมีการกำหนดพริมิทีฟ สำหรับการให้บริการแต่ละอย่าง ซึ่งเอนทิตี้ในระดับชั้นสูงกว่าจะใช้บริการโดยอาศัยพริมิทีฟเหล่านี้ สำหรับเพียร์เอนทิตี้ในระดับชั้นล่างนั้น จะใช้ โปรโตคอล ซึ่งกำหนดรูปแบบ (format) ความหมาย (meaning) และลำดับ (sequence) ของข้อมูล ใน

การส่งข้อมูลโต้ตอบกันเพื่อที่จะทำงานในการบริการแก่ระดับชั้นที่สูงกว่าตัวแบบเครือข่ายคอมพิวเตอร์แบบโอเอสไอ (OSI) [2]

2.3 ตัวแบบเครือข่ายคอมพิวเตอร์แบบโอเอสไอ (OSI)

เพื่อให้การออกแบบเครือข่ายคอมพิวเตอร์เป็นไปด้วยมาตรฐานเดียวกัน องค์การมาตรฐานสากล (International Standards Organization, ISO) ได้กำหนดตัวแบบเครือข่ายคอมพิวเตอร์ที่เรียกว่า โอเอสไอ (OSI;Open System Interconnection) ซึ่งมีเป้าหมายเพื่อให้มีการติดต่อส่งข้อมูลในลักษณะระบบเปิด (Open Systems) ได้ รูปที่ 2.7 แสดงตัวแบบเครือข่ายแบบโอเอสไอ ซึ่งแบ่งระดับชั้นออกเป็น 7 ระดับชั้น ดังนี้คือ

1. ระดับชั้นฟิสิคัล (Physical layer)
2. ระดับชั้นดาต้าลิงก์ (Data link layer)
3. ระดับชั้นเน็ตเวิร์ค (Network layer)
4. ระดับชั้นทรานสปอร์ต (Transport layer)
5. ระดับชั้นเซสชัน (Session layer)
6. ระดับชั้นพรีเซนเตชัน (Presentation layer)
7. ระดับชั้นแอปพลิเคชัน (Application layer)



APDU : Application Protocol Data Unit
TPDU : Transport Protocol Data Unit

รูปที่ 2.7 แสดงตัวแบบสถาปัตยกรรมเครือข่ายแบบโอเอสไอ

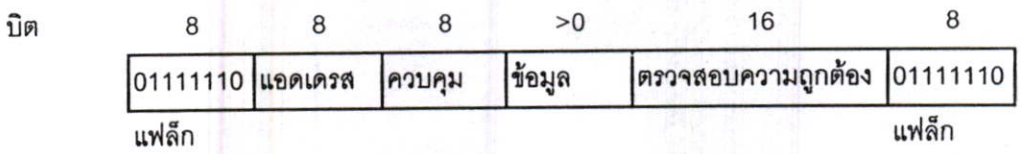
สำหรับตัวแบบโอเอสไอไม่อาจกล่าวได้ว่าเป็นสถาปัตยกรรมเครือข่าย เนื่องจากว่าในตัวแบบโอเอสไอ ไม่ได้ระบุชัดเจนถึงการบริการต่าง ๆ ที่มี ตลอดจนโปรโตคอลที่ใช้ในแต่ละระดับชั้น ตัวแบบนี้กล่าวถึงหน้าที่สาระของแต่ละระดับชั้นเท่านั้น แต่อย่างไรก็ตาม ไอเอสโอได้กำหนดมาตรฐานสำหรับโปรโตคอลที่ใช้ในแต่ละระดับชั้น ซึ่งถูกพิมพ์เป็นมาตรฐานสากลแยกออกจากตัวแบบโอเอสไอ ถัดไปเป็นการอธิบายถึงสาระโดยสังเขปของระดับชั้นต่าง ๆ

2.3.1 ระดับชั้นฟิสิคัล

สาระของระดับชั้นฟิสิคัลจะเกี่ยวกับการส่งสัญญาณบิทข้อมูลผ่านช่องสัญญาณให้ได้อย่างถูกต้องและมีประสิทธิภาพ กล่าวคือเมื่อผู้ส่งส่งบิทที่มีค่าเป็น 1 ผู้รับต้องได้รับบิทมีค่าเป็น 1 เช่นเดียวกัน และเพื่อให้การส่งบิทข้อมูลเป็นไปอย่างถูกต้อง จึงมีการกำหนดค่าแรงดันไฟฟ้าของบิท 1 และ 0 อัตราการส่งข้อมูล (สัญญาณเวลาที่ใช้ในการรับส่งข้อมูล) มาตรฐานของการส่งสัญญาณแบบแอนะล็อกและแบบดิจิตอล มาตรฐานของตัวแปลงสัญญาณ มาตรฐานของการอินเตอร์เฟซและการส่งข้อมูลโต้ตอบระหว่างอุปกรณ์ผู้ใช้ (DTE) กับอุปกรณ์สื่อสาร (DCE เช่น ตัวแปลงสัญญาณ หรือ Network Terminating Device) ในการเริ่มติดต่อข้อมูล ส่งข้อมูล และยกเลิกการติดต่อ สำหรับตัวอย่างของกฎเกณฑ์การส่งข้อมูลโต้ตอบระหว่าง DTE และ DCE เช่น ในการส่งข้อมูลด้วยโมเด็มแบบฮาล์ฟดูเพล็กซ์นั้น เมื่อ DTE ต้องการส่งข้อมูล ต้องส่งสัญญาณ RTS (Request To Send) ก่อน และเมื่อ DCE ตอบกลับมาด้วยสัญญาณ CTS (Clear To Send) แล้ว DTE จึงจะส่งข้อมูลออกไปได้ เป็นต้น นอกจากนั้นยังมีสาระของชนิด และคุณสมบัติต่าง ๆ ของสายสื่อสาร อีกทั้งช่องสัญญาณของสายสื่อสารในลักษณะของซิมเพล็กซ์ ฮาล์ฟดูเพล็กซ์ หรือฟูลดูเพล็กซ์ ตลอดจนการมัลติเพล็กซ์สัญญาณข้อมูล เป็นต้น

2.3.2 ระดับชั้นดาต้าลิงก์

หน้าที่ของระดับดาต้าลิงก์ คือ การบริการส่งข้อมูล (ซึ่งได้รับมาจากระดับชั้นเน็ตเวิร์ค) ระหว่างโหนดที่ติดกันของเครือข่าย ให้ผ่านสายส่งได้อย่างถูกต้อง และมีประสิทธิภาพ และเนื่องจากสายส่งอาจจะมีสัญญาณรบกวนทำให้ข้อมูลที่ส่งหายไป จึงจำเป็นจะต้องมีกระบวนการในการตรวจสอบความถูกต้องของการส่งข้อมูล หากผิดต้องทำการแก้ไข ซึ่งกระบวนการแก้ไขข้อมูลที่ผิดพลาดนี้สามารถทำได้อย่างมีประสิทธิภาพ โดยการนำเอาบิทข้อมูลมาทำเป็นเฟรม (บล็อกของบิทข้อมูล) และทำการตรวจสอบ และแก้ไขทั้งเฟรม ดังนั้นจึงมีการกำหนดโครงสร้าง และขอบเขตของเฟรม เพื่อเพียร์โปรเซสส์ของด้านรับจะสามารถนำเฟรมข้อมูลไปประมวลผลได้อย่างถูกต้อง รูปที่ 2.8 แสดงถึงตัวอย่างของเฟรม จะเห็นว่าการปะแฟล็ก (flag) ที่ต้นและท้ายเฟรม เพื่อให้ด้านรับสามารถรับรู้ขอบเขตของเฟรมได้ถูกต้อง



รูปที่ 2.8 แสดงตัวอย่างของเฟรมในระดับชั้นดาต้าลิงก์

นอกจากนั้นในบางครั้ง สัญญาณรบกวนในสายอาจจะทำให้เฟรมข้อมูลหายไปได้ จึงอาจต้องมีการส่งเฟรมเดิมไปใหม่หลายครั้ง ซึ่งก็อาจทำให้ด้านรับได้รับเฟรมเดิมซ้ำได้ ดังนั้นจึงเป็นหน้าที่ของระดับชั้นนี้ ในการควบคุมให้การส่งข้อมูลระหว่างโหนดที่ติดกันผ่านสายส่งเป็นไปอย่างถูกต้อง ไม่มีข้อมูลหาย หรือข้อมูลซ้ำ นอกจากนี้หน้าที่สำคัญอีกอย่างหนึ่งของระดับชั้นดาต้าลิงก์คือ ควบคุมการไหลของข้อมูล (flow control) โดยไม่ให้ด้านส่ง ๆ ข้อมูลเร็วเกินไป จนด้านรับนำข้อมูลที่รับเข้ามาส่งให้แก่ระดับเน็ตเวิร์คไม่ทัน ทำให้ข้อมูลที่เข้ามาใหม่ทับข้อมูลเดิมที่อยู่ในบัฟเฟอร์ของระดับดาต้าลิงก์ด้านรับ ซึ่งทำให้ข้อมูลเสียหายได้ และปกติแล้วกระบวนการที่ควบคุมการไหลของข้อมูลอาจจะรวมอยู่ในขั้นตอนการควบคุมความผิดพลาดได้ ระดับชั้นดาต้าลิงก์ยังมีการกำหนดวิธีการในการส่งข้อมูลระหว่างโหนดที่ติดกันทั้งในกรณีของการส่งแบบซิมเพล็กซ์ ฮาล์ฟดูเพล็กซ์ และฟูลดูเพล็กซ์ ซึ่งวิธีการส่งข้อมูลแบบฟูลดูเพล็กซ์จะยุ่งยากกว่าแบบฮาล์ฟดูเพล็กซ์ แต่ประสิทธิภาพของการส่งจะดีกว่ามาก โดยเฉพาะสำหรับการส่งข้อมูลผ่านสายส่งซึ่งมีความหน่วงในการส่งสัญญาณยาวนาน เช่น ดาวเทียม เป็นต้น

2.3.3 ระดับชั้นเน็ตเวิร์ค

หน้าที่หลักของระดับระดับชั้นเน็ตเวิร์ค คือ ควบคุมการส่งข้อมูลที่ ผู้ให้บริการส่งข้อมูลหรือเครือข่ายย่อยในส่วนของการสื่อสาร (communication subnet) รับจากผู้ใช้บริการต้นทาง เพื่อส่งข้อมูลผ่านโหนดต่าง ๆ ให้แก่ผู้ใช้บริการปลายทางได้อย่างถูกต้อง และมีประสิทธิภาพ โดยมีสาระเกี่ยวกับชนิดและรูปแบบของการบริการต่าง ๆ ที่ผู้ให้บริการส่งข้อมูลจะให้แก่ ผู้ใช้บริการส่งข้อมูล (user) นอกจากนั้นระดับชั้นเน็ตเวิร์ค ยังจัดการควบคุมการทำงานของเครือข่าย โดยกำหนดเส้นทางการส่งข้อมูลผ่านโหนดต่าง ๆ ของเครือข่ายให้ถึงปลายทางได้อย่างถูกต้องและรวดเร็ว ซึ่งวิธีการกำหนดเส้นทางเดินของข้อมูลอาจจะเป็นลักษณะที่ทุก ๆ แพ็กเกตข้อมูล (แพ็กเกตในระดับชั้นเน็ตเวิร์ค) ของข่าวสารชุดเดียวกันถูกส่งผ่านโหนดต่าง ๆ ตามเส้นทางเดียวกันเส้นทางหนึ่ง หรือเป็นลักษณะที่แต่ละแพ็กเกตถูกส่งผ่านโหนดของเส้นทางที่แตกต่างกันไป ขึ้นอยู่กับว่าเส้นทางใดที่จะสามารถส่งแพ็กเกตให้ถึงปลายทางได้เร็วที่สุด นอกจากนั้น หากในเครือข่ายมีแพ็กเกตจำนวนมากอาจทำให้เกิดการติดขัดของการส่งข้อมูล (congestion) จึงเป็นหน้าที่ของระดับชั้นเน็ตเวิร์ค ที่ต้องแก้ไขปัญหาเหล่านี้ หน้าที่อีกอย่างหนึ่งของระดับชั้นเน็ตเวิร์คก็คือ การคิดเงิน (accounting) เช่น ใช้ซอฟต์แวร์นับจำนวนแพ็กเกตหรือไบต์ข้อมูล ซึ่งส่งมาจากลูกค้าแต่ละราย เพื่อส่งบิลเก็บเงิน และ

ในกรณีที่มีการส่งข้อมูลหลาย ๆ เครือข่ายซึ่งมีอัตราการเก็บเงินแตกต่างกันไป จะทำให้การเก็บเงินยุ่งยากขึ้น ซึ่งเป็นหน้าที่ของระดับชั้นเน็ตเวิร์ค ต้องจัดการเกี่ยวกับเรื่องนี้ นอกจากนั้นการส่งข้อมูลระหว่างผู้ใช้โดยผ่านหลายเครือข่ายนั้นมีปัญหายุ่งยากหลายประการ เช่น การใช้ระบบแอดเดรสของแต่ละเครือข่ายอาจจะแตกต่างกันไป หรือ แต่ละเครือข่าย อาจจะกำหนดขนาดแพ็กเกตที่ยอมให้ผ่านเครือข่ายแตกต่างกัน ดังนั้นจึงเป็นหน้าที่ของระดับชั้นเน็ตเวิร์ค ที่ต้องกำหนดวิธีการต่าง ๆ เพื่อให้การส่งข้อมูลทำได้อย่างมีประสิทธิภาพ

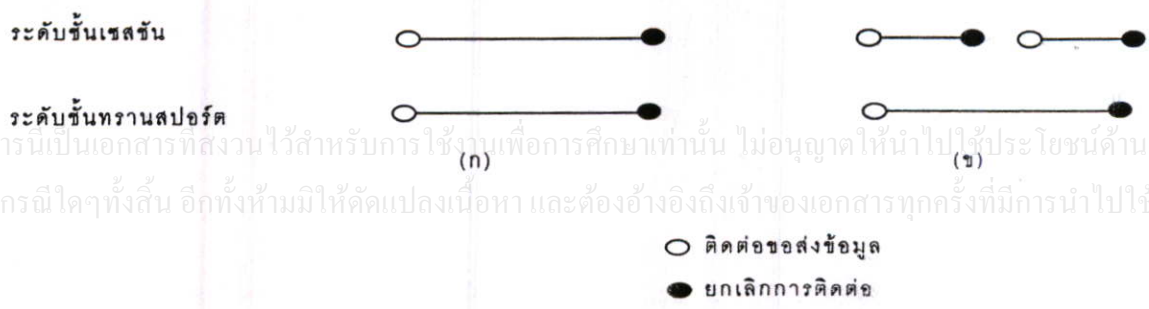
2.3.4 ระดับชั้นทรานสปอร์ต

หน้าที่หลักของระดับชั้นทรานสปอร์ตคือ การควบคุมการส่งข้อมูลของผู้ใช้ต้นทาง หรือกระบวนการประมวลผลของโฮสต้นทาง ให้ถึงผู้ใช้ปลายทาง หรือ กระบวนการประมวลผลของโฮสต์ปลายทางได้อย่างถูกต้อง และมีประสิทธิภาพ ทั้งนี้ระดับชั้นทรานสปอร์ต ทำหน้าที่เสมือนกับแผนกขนส่งของบริษัท ซึ่งรับพัสดุจากแผนกต่าง ๆ ของบริษัท และอินเตอร์เฟซกับองค์การขนส่งเพื่อใช้บริการขนส่ง และสื่อสารกับแผนกขนส่งปลายทางเพื่อควบคุมพัสดุให้ถึงปลายทางได้อย่างถูกต้องและรวดเร็ว แผนกขนส่งปลายทาง เมื่อได้รับพัสดุแล้วจะกระจายส่งให้แก่แผนกต่าง ๆ ได้อย่างถูกต้อง ซึ่งแผนกต่าง ๆ ที่ใช้บริการขนส่งพัสดุของแผนกขนส่งเปรียบเสมือนเพียร์โปรเซสส์ในระดับสูงขึ้นไป เช่น ระดับชั้นเซสชันซึ่งใช้บริการของระดับชั้นทรานสปอร์ต เพื่อส่งข้อมูลให้ถึงปลายทาง เป็นต้น นอกจากนี้ หากชนิด รูปแบบ และเทคโนโลยีของการส่งข้อมูลของเครือข่ายเปลี่ยนไปเป็นหน้าที่ของระดับชั้นทรานสปอร์ต ในการกันผู้ใช้จากการเปลี่ยนแปลงเหล่านั้น ทำให้ผู้ใช้สามารถส่งข้อมูลได้ดังเดิม โดยปกติแล้วเมื่อผู้ใช้ในระดับชั้นที่สูงต้องการจะส่งข้อมูลในแต่ละคราว ระดับชั้นทรานสปอร์ต จะใช้บริการของระดับชั้นเน็ตเวิร์ค เพื่อสร้างการติดต่อเชื่อมโยง (connection) เส้นหนึ่งหรือช่องทางหนึ่งสำหรับการส่งข้อมูล แต่ในกรณีที่ผู้ใช้มีข้อมูลจำนวนมากที่ต้องการส่งอย่างเร่งด่วน ระดับชั้นทรานสปอร์ตอาจจะใช้บริการของระดับเน็ตเวิร์คเพื่อสร้างการติดต่อหลาย ๆ การเชื่อมโยงแล้วกระจายข้อมูลส่งไปตามการเชื่อมโยง หรือช่องทางส่งข้อมูลนั้น ๆ ซึ่งทำให้ปริมาณงานของการส่งข้อมูลดีขึ้น ในทางตรงข้าม หากผู้ใช้ส่งจำนวนน้อย และการใช้บริการของระดับชั้นเน็ตเวิร์คสำหรับแต่ละการเชื่อมโยงส่งข้อมูลนั้นมีราคาแพง จะเป็นหน้าที่ของระดับชั้นทรานสปอร์ต ในการรวบรวมข้อมูลจากผู้ใช้หลาย ๆ ราย เพื่อใช้บริการส่งข้อมูลของระดับชั้นเน็ตเวิร์คเพียงการเชื่อมโยงเดียว ในกรณีที่คอมพิวเตอร์ซึ่งต้องการส่งข้อมูลทั้งสองด้านทำงานได้ในลักษณะของผู้ใช้หลาย ๆ คน (multiuser) นั้น อาจจะมีผู้ใช้ (หรือกระบวนการประมวลผล) 2 ราย เช่น A และ B ของเครื่องหนึ่งต้องการติดต่อกับผู้ใช้ 2 ราย (เช่น C และ D) ในอีกเครื่องหนึ่ง โดยที่ A อาจต้องการส่งข้อมูลให้แก่ C ส่วน B อาจต้องการส่งข้อมูลให้แก่ D ดังนั้นจึงเป็นหน้าที่ของระดับชั้นทรานสปอร์ตที่จะส่งข้อมูลทั้งหลายที่รับขึ้นมาจากระดับเน็ตเวิร์คให้แก่ผู้ใช้ C และ D ได้ถูกต้อง ซึ่งในการจัดการนี้อาจจะใช้วิธีกำหนดแอดเดรสของจุดให้บริการ (SAP) แก่ผู้ใช้แต่ละคน

ของระดับชั้นทรานสปอร์ต เพื่อจะสามารถส่งข้อมูลให้แก่ผู้ใช้ต่าง ๆ ได้อย่างถูกต้อง รูปที่ 2.7 จะเห็นได้ว่า ระดับชั้นทรานสปอร์ตเป็นการติดต่อส่งข้อมูลระหว่างเครื่องต้นทาง (Source) และเครื่องปลายทาง (Destination) กล่าวคือ ซอฟต์แวร์บนเครื่องต้นทางส่งข้อมูลติดต่อกับซอฟต์แวร์ซึ่งทำงานสอดคล้องกันบนเครื่องปลายทาง โดยใช้เฮดเดอร์ของข้อมูล ตลอดจนการส่งข้อมูลควบคุมการติดต่อ (control message) ส่วนระดับชั้นที่ซึ่งต่ำลงมาเป็นการพูดคุยติดต่อระหว่างเครื่องที่ติดกันเพื่อส่งข้อมูลไปเรื่อย ๆ ผ่านเครือข่ายจนถึงปลายทาง ซึ่งไม่ใช่เป็นการติดต่อระหว่างเครื่องต้นทางและปลายทาง เหมือนกับระดับชั้นทรานสปอร์ต ดังนั้นระดับชั้นทรานส-ปอร์ตจึงมักถูกเรียกว่า "เอนทูเอนเลเยอร์ (end to end layer)"

2.3.5 ระดับชั้นเซสชัน

ต้นแบบของโอเอสไอ ถือได้ว่าตั้งแต่ระดับชั้นทรานสปอร์ต ลงมาจะ ทำหน้าที่หลักในการสื่อสารข้อมูลส่งข้อมูลจากต้นทางถึงปลายทางให้ได้อย่างถูกต้องและมีประสิทธิภาพ ส่วนตั้งแต่ระดับชั้นเซสชัน ระดับชั้นพรีเซนเตชัน และระดับชั้นแอปพลิเคชัน ถูกจัดว่าเป็นระดับชั้นที่สูง (upper layer) ซึ่งทำหน้าที่ให้บริการความสะดวกสบายต่าง ๆ แก่ผู้ใช้ หรือแก่โปรแกรมประยุกต์โดยผู้ใช้แต่ละรายไม่จำเป็นต้องเขียนยูทิลิตี้ (utility) ของแต่ละคนขึ้นเอง สำหรับระดับชั้นเซสชันนั้นให้บริการแก่ผู้ใช้ในการสร้างเซสชัน (session) ของการติดต่อระหว่างเครื่อง ตัวอย่างของการสร้างเซสชันของการติดต่อนี้ เช่น เพื่อใช้ในการล็อกอินแต่ละเครื่องของเทอร์มินัลเข้าสู่โฮสต์ หรือในการโอนย้ายไฟล์ข้อมูลระหว่างผู้ใช้ ซึ่งปกติเมื่อมีการสร้างเซสชันของการติดต่อแล้ว ระดับชั้นเซสชันจะใช้บริการของระดับชั้นทรานสปอร์ตในการติดต่อส่งข้อมูลจากต้นทางถึงปลายทาง และเมื่อเลิกเซสชันของการติดต่อแล้ว การติดต่อส่งข้อมูลในระดับชั้นทรานสปอร์ตจะถูกยกเลิกไปด้วย ดังแสดงในรูปที่ 2.9 (ก) แต่ในบางกรณี เช่น การจองตั๋วเครื่องบินเมื่อมีการขอจองตั๋วแต่ละครั้งจะมีการสร้างเซสชันของการติดต่อระหว่างคอมพิวเตอร์ที่สำนักงานจองกับคอมพิวเตอร์สำนักงานใหญ่ (ซึ่งมีฐานข้อมูล) เมื่อจองตั๋วเสร็จแล้วเซสชันจะถูกยกเลิก แต่ไม่มีความจำเป็นในการยกเลิกการติดต่อในระดับชั้นทรานสปอร์ต เพราะว่าจะมีการติดต่อมาเพื่อใช้คอมพิวเตอร์ที่สำนักงานใหญ่อีกภายในไม่กี่นาที ซึ่งรูปแบบของการติดต่อเช่นนี้ แสดงได้ดังในรูปที่ 2.9 (ข)



รูปที่ 2.9 แสดงการติดต่อระดับชั้นเซสชันซึ่งสัมพันธ์กับการติดต่อในระดับชั้นทรานสปอร์ต

ในแต่ละเซสชันของการติดต่อกัน ระดับชั้นเซสชันจะให้บริการความสะดวกสบายต่าง ๆ นอกเหนือจากการส่งข้อมูล การบริการอย่างหนึ่งของระดับชั้นเซสชันคือ ทำให้การส่งข้อมูลเป็นไปได้ทั้งในลักษณะของฟูลดูเพล็กซ์ หรือฮาล์ฟดูเพล็กซ์ เช่น ในการประยุกต์การเข้าถึงข้อมูลจากฐานข้อมูลนั้น มักจะเป็นลักษณะที่ผู้ใช้ส่งข้อคำถาม (query) ไปยังระบบฐานข้อมูล และรอคำตอบ (reply) กลับมา จึงเป็นลักษณะของการส่งข้อมูลสลับกันไป ดังนั้นการส่งข้อมูลจะเป็นลักษณะที่ในขณะใดขณะหนึ่งนั้นผู้ใช้เป็นผู้ส่ง หรือระบบฐานข้อมูลเป็นผู้ส่ง (เป็นลักษณะฮาล์ฟดูเพล็กซ์) การควบคุมดูแลว่าฝ่ายใดจะเป็นผู้ส่งข้อมูลนั้นเรียกว่า การจัดการโต้ตอบ (dialogue management)โดยมีการใช้ดาต้าโทเคน (data token) ในการควบคุมการส่งข้อมูล ซึ่งโทเคนนี้จะถูกส่งไปมาระหว่างสองฝ่าย ฝ่ายที่ถือโทเคนจะมีสิทธิในการส่งข้อมูล เป็นต้น นอกจากนั้นในการประยุกต์ เช่น การโอนย้ายไฟล์ หากผู้ส่ง ๆ แฟ้มข้อมูลไปพิมพ์ ณ ที่ไกลออกไป และการส่งข้อมูลโดยระดับชั้นทรานสปอร์ตได้ทำหน้าที่อย่างสมบูรณ์แล้วโดยส่งข้อมูลจากด้านส่งถึงด้านรับได้อย่างถูกต้อง จึงไม่ใช่หน้าที่ของระดับชั้นทรานสปอร์ตในการแก้ปัญหาที่เกิดขึ้นนี้ ดังนั้นระดับชั้นเซสชัน จึงให้บริการการแก้ปัญหาเช่นนี้ โดยให้มีการซิงโครไนเซชันของการส่งข้อมูลระหว่างผู้ใช้ทั้งสองด้าน โดยที่ระดับชั้นเซสชันจะยอมให้ผู้ใช้แบ่งข้อความออกมาเป็นหน้า ๆ และใส่จุดซิงโครไนเซชันระหว่างแต่ละหน้า ดังแสดงในรูปที่ 2.10 ด้วยวิธีเช่นนี้เมื่อเกิดปัญหาที่หน้าใด ระบบก็สามารถปรับ (reset) สภาวะของการติดต่อส่งข้อมูลให้กลับไปยังจุดซิงโครไนเซชันก่อนหน้า และทำการส่งข้อมูลต่อจากจุดซิงโครไนเซชันนั้น

รูปที่ 2.10 แสดงตัวอย่างการใส่จุดซิงโครไนเซชัน

2.3.6 ระดับชั้นพรีเซนเตชัน

ระดับชั้นพรีเซนเตชันทำหน้าที่ต่างกับ 5 ระดับที่ได้กล่าวมาแล้วซึ่งทำหน้าที่ในการส่งย้ายบิทข้อมูลจากต้นทางไปยังปลายทาง แต่สำหรับระดับชั้นพรีเซนเตชันแล้วจะทำหน้าที่เกี่ยวกับการคงไว้ซึ่งความหมายของข้อมูลที่ส่ง กล่าวคือ เมื่อผู้ส่งได้ส่งข้อมูลที่มีความหมายอย่างไร เช่น ส่งตัวอักษร ก หรือ จำนวนตัวเลข 10 ผู้รับต้องได้รับข้อมูลซึ่งมีความหมายเดียวกันคือ ตัวอักษร ก หรือจำนวนตัวเลข 10 เป็นต้น เนื่องจากคอมพิวเตอร์ซึ่งต่างชนิดกันนั้น จะมีรูปแบบของการแทนค่าข้อมูลภายในเครื่องแตกต่างกันไป เช่น เครื่องเมนเฟรมของไอบีเอ็ม จะใช้รหัส EBCDIC แทนค่าตัว

อักษร ในขณะที่คอมพิวเตอร์อื่น ๆ ใช้รหัสแอสกี นอกจากนั้นไมโครคอมพิวเตอร์ส่วนใหญ่ใช้ 2's complement สำหรับจำนวนตัวเลข (integer) 16 บิท แต่เครื่อง CDC Cybers ใช้จำนวนบิท 60 บิท แบบ 1's complement สำหรับจำนวนตัวเลข ดังนั้นจึงเป็นหน้าที่ของระดับชั้นพรีเซนเตชันในการแปลงข้อมูลที่แทนในเครื่องด้านส่งให้อยู่ในรูปแบบที่เหมาะสมในการส่งข้อมูล แล้วแปลงข้อมูลนั้นให้อยู่ในรูปแบบที่ใช้ในเครื่องผู้รับ นอกจากนั้นระดับชั้นพรีเซนเตชัน ยังทำหน้าที่ในการบีบอัดข้อมูล (data compression) ซึ่งทำให้สามารถลดค่าใช้จ่ายในการส่งข้อมูลลงไปได้มาก และหน้าที่สำคัญอีกอย่างหนึ่งของระดับชั้นพรีเซนเตชันคือ ป้องกันข้อมูลไม่ให้ถูกอ่าน หรือแก้ไขโดยบุคคลที่ไม่ได้รับอนุญาต ตลอดจนพิสูจน์ว่าผู้ที่ส่งข้อมูลนั้นเป็นผู้ส่งจริงหรือไม่ ซึ่งใช้หลักการของการเข้ารหัสลับข้อมูล (encryption)

2.3.7 ระดับชั้นแอปพลิเคชัน

ปกติแล้วโปรแกรมประยุกต์ของผู้ใช้จะอยู่ในระดับชั้นแอปพลิเคชัน ซึ่งโปรแกรมประยุกต์เหล่านี้มีการทำงานบางอย่างคล้าย ๆ กัน เช่น การส่งแฟ้มข้อมูล หรือบางส่วนของแฟ้มข้อมูลระหว่างคอมพิวเตอร์ต่าง ๆ ดังนั้นเพื่อไม่ให้ผู้ใช้แต่ละคนพัฒนาส่วนโปรแกรมส่งแฟ้มข้อมูลแตกต่างกันไป ซึ่งจะทำให้เป็นการสิ้นเปลือง ตลอดจนอาจจะทำให้การส่งแฟ้มข้อมูลระหว่างคอมพิวเตอร์ต่าง ๆ ทำได้ลำบาก จึงมีการกำหนดมาตรฐานของการส่งแฟ้มข้อมูลในระดับชั้นแอป-พลิเคชัน เพื่อให้การบริการส่งข้อมูลให้แก่ผู้ใช้เป็นไปตามมาตรฐานเดียวกัน นอกจากนี้เนื่องจากการเก็บแฟ้มข้อมูลในคอมพิวเตอร์แต่ละระบบจะแตกต่างกัน ทั้งรูปแบบของการตั้งชื่อแฟ้มข้อมูล รูปแบบของการเก็บข้อความแต่ละบรรทัด ทำให้วิธีการเข้าถึงข้อมูลของแฟ้มข้อมูลแต่ละระบบแตกต่างกันออกไป ในการแก้ปัญหาเหล่านี้ ได้มีการใช้หลักการของหน่วยเก็บแฟ้มข้อมูลเสมือน (virtual file store) ซึ่งจะกำหนดมาตรฐานในการที่ผู้ใช้จะอินเตอร์เฟซ เพื่อใช้แฟ้มข้อมูล และมาตร-ฐานของปฏิบัติการ (opeation) ต่าง ๆ ที่ผู้ใช้จะกระทำได้กับแฟ้มข้อมูลเสมือนนี้ ดังนั้นหากระบบการเก็บภายในแฟ้มข้อมูลจริงในเครื่องคอมพิวเตอร์แตกต่างจากมาตรฐานของแฟ้มข้อมูลเสมือนแล้ว จะเป็นหน้าที่ของซอฟแวร์ในระดับชั้นแอปพลิเคชันที่จะกระทำการปรับแปลง ทำให้ผู้ใช้โปรแกรมประยุกต์สามารถเข้าถึงระบบแฟ้มข้อมูลจริงนี้ ด้วยมาตรฐานของแฟ้มข้อมูลเสมือน โดยที่ผู้ใช้ไม่จำเป็นต้องทราบรายละเอียด ภายในของระบบเก็บแฟ้มข้อมูลจริงในแต่ละเครื่อง สาระสำคัญอีกอย่างหนึ่งของระดับชั้นแอปพลิเคชัน คือ การทำให้โปรแกรมประยุกต์ที่ทำงานบนโฮสต์สามารถทำงานได้กับเทอร์มินัลชนิดต่าง ๆ ได้ ซึ่งปกติแล้วเทอร์มินัลแต่ละชนิดจะมีการใช้ตัวอักษรที่ใช้การควบคุมหน้าจอ (control characters) เช่น การเลื่อนเคอร์เซอร์ การเพิ่ม/ลบตัวอักษรหรือบรรทัด แตกต่างกันออกไป ดังนั้นโปรแกรมประยุกต์อาจต้องมีลักษณะการทำงาน (feature) ของทุกเทอร์มินัลที่ใช้โปรแกรมนั้น วิธีหนึ่งในการแก้ปัญหานี้ก็คือ การใช้หลักการของเทอร์มินัลเสมือน (virtual teminal) ซึ่งเป็นโครงสร้างข้อมูลข้อมูลแบบนามธรรม (abstract data structure) ที่

แทนหน้าจอ ซึ่งข้อมูลในโครงสร้างข้อมูลนี้จะแสดงสภาพของข้อมูลที่แสดงหน้าจอ สำหรับตัวอย่างของโครงสร้างข้อมูลนี้ เช่น อาร์เรย์ (array) 2 มิติของตัวอักษรซึ่งมีขนาดเท่ากับจอ และข้อมูลในอาร์เรย์นี้จะเหมือนกับข้อมูลที่ปรากฏบนหน้าจอของเทอร์มินัล โดยการใช้งานนั้นโครงสร้างข้อมูลจะถูกแก้ไขและอ่านได้ทั้งโปรแกรมบนเทอร์มินัล และโปรแกรมประยุกต์บนเครื่องโฮสคอมพิวเตอร์ คือเมื่อมีการกดแป้นพิมพ์ของเทอร์มินัล ตัวอักษรที่ถูกกดจะปรากฏบนจอเทอร์มินัลพร้อมกับมีการปรับปรุงเปลี่ยนแปลงตัวอักษรในโครงสร้างข้อมูลนี้ แล้วข้อมูลการปรับปรุงนี้จะถูกส่งไปให้โปรแกรมประยุกต์บนโฮสต์คอมพิวเตอร์ โดยซอฟต์แวร์ของเทอร์มินัลเสมือน (virtual terminal software) ดังนั้นโปรแกรมประยุกต์จึงสามารถทราบถึงข้อมูลที่ถูกป้อนจากเทอร์มินัล และประมวลผลข้อมูลนั้นได้ ในทางกลับกันผลลัพธ์ของการประมวลผลก็จะทำให้เกิดการปรับปรุงโครงสร้างข้อมูลเครื่องโฮสต์โดยซอฟท์แวร์เทอร์มินัลเสมือน ซึ่งข้อมูลเหล่านี้จะถูกส่งให้เทอร์มินัลเพื่อปรับปรุงโครงสร้างข้อมูลบนเทอร์มินัล และแสดงบนหน้าจอโดยซอฟต์แวร์ของเทอร์มินัลเสมือนที่ทำงานบนเทอร์มินัล ดังแสดงในรูปที่ 2.11 เช่น เมื่อโปรแกรมประยุกต์สั่งเลื่อนเคอร์เซอร์ของโครงสร้างข้อมูลไปแสดงที่มุมซ้ายของหน้าจอแล้ว ซอฟต์แวร์บนเทอร์มินัลนี้ต้องใช้ตัวอักษรควบคุมที่ถูกต้อง เพื่อเลื่อนเคอร์เซอร์ของเทอร์มินัลนั้น ๆ ไปยังมุมซ้ายของจอภาพ เป็นต้น และจากรูปที่ 2.11 การทำงานของเทอร์มินัลเสมือน มีขั้นตอนต่าง ๆ ดังต่อไปนี้

ขั้นตอนที่ 1 เมื่อกดแป้นพิมพ์ โครงสร้างข้อมูลถูกปรับปรุง

ขั้นตอนที่ 2 ข้อมูลเปลี่ยนแปลงถูกส่งไปยังโฮสต์เพื่อปรับปรุงโครงสร้างข้อมูลบนโฮสต์

ขั้นตอนที่ 3 โปรแกรมประยุกต์นำข้อมูลไปประมวลผล

ขั้นตอนที่ 4 ผลลัพธ์ที่ได้ใช้ในการปรับปรุงโครงสร้างข้อมูลหน้าจอ

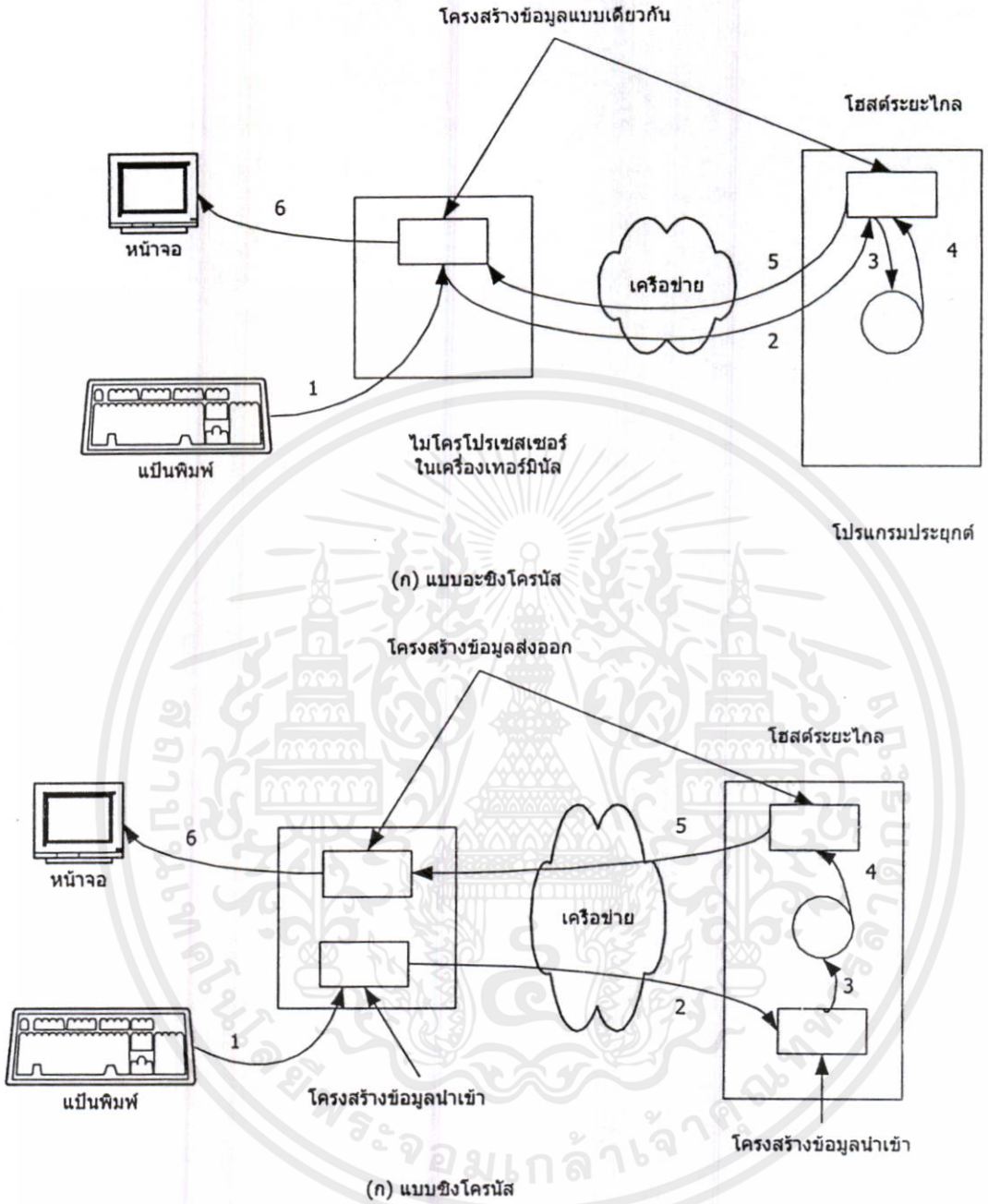
ขั้นตอนที่ 5 ข้อมูลเปลี่ยนแปลงถูกส่งไปปรับปรุงโครงสร้างข้อมูลบนเทอร์มินัล

ขั้นตอนที่ 6 หน้าจอเปลี่ยนแปลงไปตามข้อมูลตามข้อมูลในโครงสร้างข้อมูล

ระดับชั้นแอปพลิเคชัน ยังได้กำหนดมาตรฐานของการส่งจดหมายอีเล็กทรอนิกส์ (E-mail) ระหว่างผู้ใช้ของเครื่องต่าง ๆ ตลอดจนมาตรฐานของระบบสมุดโทรศัพท์ และการส่งงานประมวลผลระยะไกล (Remote Job Entry;RJE) เป็นต้น

2.3.8 การส่งข้อมูลในรูปแบบโอเอสไอ

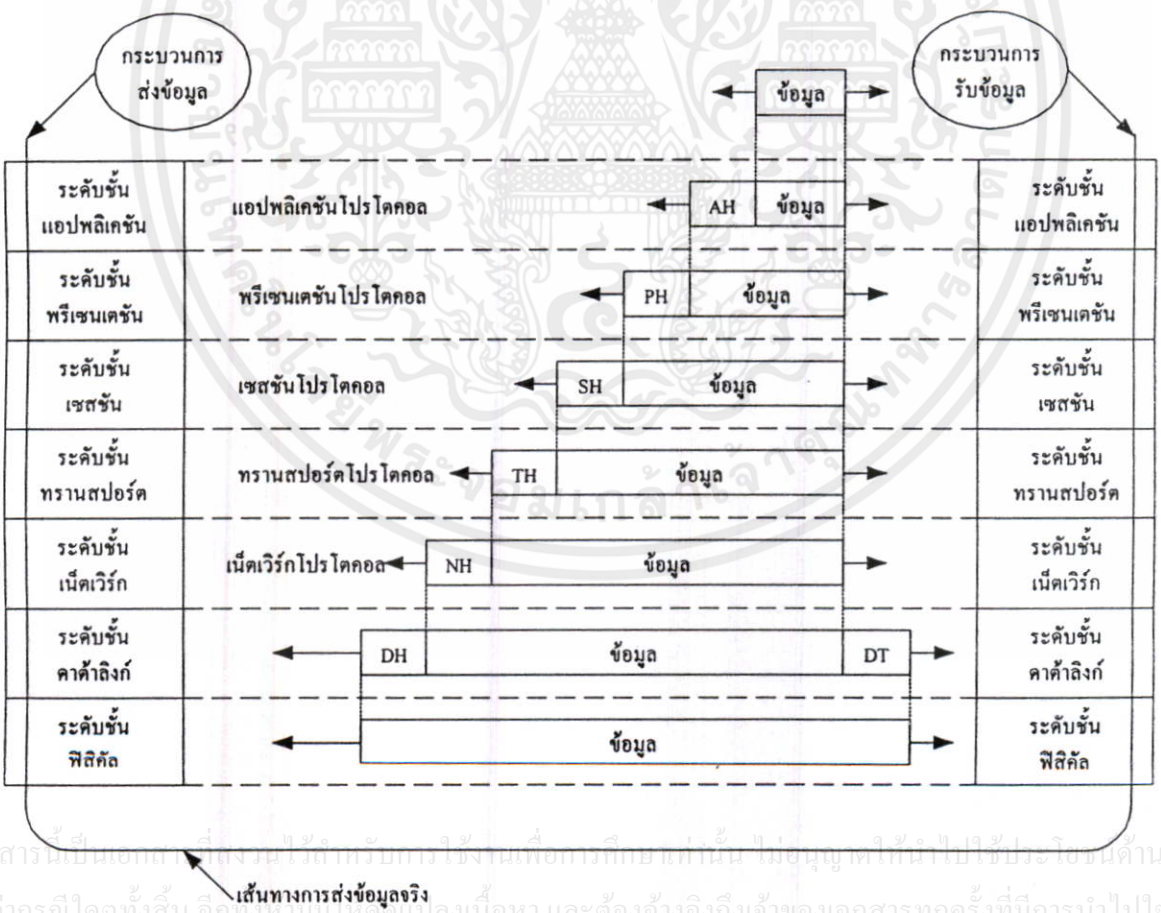
รูปที่ 2.12 แสดงถึงการส่งข้อมูลของระบบโอเอสไอ กล่าวคือ เมื่อผู้ใช้ หรือโปรแกรมประยุกต์ซึ่งอยู่ในระดับชั้นแอปพลิเคชันต้องการส่งข้อมูล ก็จะใช้บริการของระดับชั้นแอปพลิเคชัน โดยที่ระดับชั้นแอปพลิเคชันจะปะเฮดเดอร์ในระดับของตนเองเพื่อใช้ในการติดต่อด้วยกฎเกณฑ์ที่แน่นอนกับระดับชั้นแอปพลิเคชันของเครื่องด้านรับ แล้วจึงส่งข้อมูลมาให้ระดับล่าง ซึ่งต่างก็จะปะเฮดเดอร์ในระดับของตนเองเพื่อติดต่อกับเพียร์โปรเซสในระดับเดียวกัน และเฮดเดอร์เหล่านี้จะถูกมองว่าเป็นส่วนของข้อมูลสำหรับระดับชั้นล่าง เมื่อถึงระดับชั้นฟิสิกัล ข้อมูลทั้งหมดจะถูกส่งผ่าน



รูปที่ 2.11 แสดงการทำงานของเทอร์มินัลเสมือน

สายส่งไปให้แก่โหนดที่ติดกันของผู้ให้บริการส่งข้อมูล เมื่อถึงโหนดด้านรับ บิทข้อมูลนี้จะถูกรับมาจากระดับชั้นฟิสิกัลแล้วส่งไปยังระดับชั้นดาต้าลิงก์ ซึ่งจะตรวจสอบความถูกต้องของข้อมูลที่ผ่านสายส่งโดยอาศัยเทรเลอร์ที่ปะมาด้วย หากข้อมูลไม่ถูกต้องจะเป็นหน้าที่ของระดับชั้นดาต้าลิงก์ในการแก้ไข โดยอาจจะขอให้ด้านส่งทำการส่งข้อมูลมาใหม่ เมื่อได้รับข้อมูลที่ถูกต้องแล้ว ระดับชั้นดาต้าลิงก์จะถอดเฮดเดอร์ในระดับตัวเองออก และส่งข้อมูลให้ระดับชั้นเน็ตเวิร์คซึ่งจะใช้เฮดเดอร์ในระดับนี้จะพิจารณาว่าตนเองเป็นโหนดปลายทางที่ติดกับโฮสต์ผู้รับหรือไม่ หากไม่ใช่ก็จะทำการคำนวณหาโหนดที่ติดกันเพื่อจะส่งข้อมูลมายังระดับชั้นฟิสิกัล เพื่อส่งข้อมูลผ่านสายส่งไปยัง

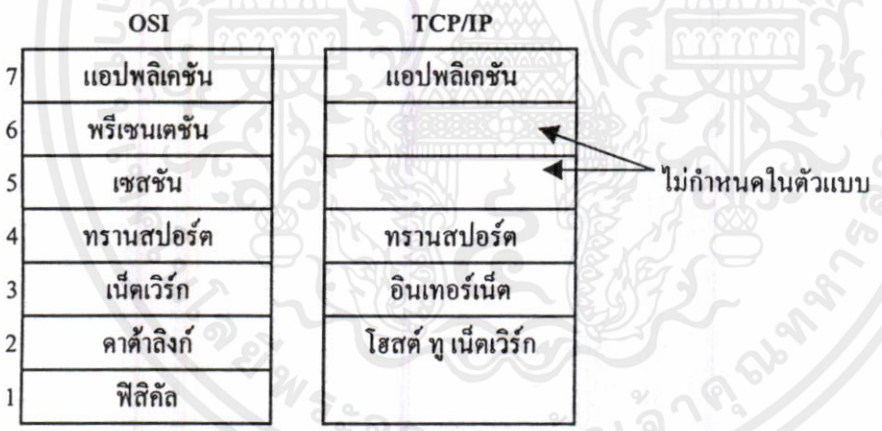
โหนดที่ได้กำหนดไว้นั้น (ดูรูปที่ 2.7 ประกอบ) ข้อมูลจะถูกส่งผ่านโหนดต่าง ๆ ของผู้ให้บริการส่งข้อมูลในลักษณะดังกล่าวข้างต้น ซึ่งในการส่งข้อมูลโต้ตอบระหว่างเพียร์โปรเซสของระดับชั้น 1-3 จะใช้โปรโตคอลของเครือข่ายย่อยภายใน (internal subnet protocol) จนกว่าจะถึงโหนดปลายทางที่ติดกับโฮสต์ผู้รับ เมื่อถึงแล้วโหนดนั้นจะส่งข้อมูลให้แก่โฮสต์ผู้รับโดยใช้โปรโตรคอลระหว่างโฮสต์และเราเตอร์ สำหรับข้อมูลที่ถึงโฮสต์แล้วจะถูกส่งต่อผ่านระดับชั้นต่าง ๆ ขึ้นไปจนถึงผู้ใช้บริการ หรือตัวประมวลผลที่อยู่ในระดับชั้นแอปพลิเคชัน ซึ่งในแต่ละระดับชั้นจะใช้เฮดเดอร์ในระดับตัวเอง และข้อมูลควบคุม เพื่อติดต่อทำงานให้สอดคล้องกับเพียร์โปรเซสส์ของผู้ส่ง โดยตั้งแต่ระดับชั้นทรานสปรอร์ตขึ้นไปเป็นโปรโตรคอลในลักษณะของต้นทางไปถึงปลายทาง (source-to-destination) หรือเอนทูเอน (end-to-end) กล่าวคือ เป็นโปรโตคอลที่ใช้ในการส่งข้อมูลโต้ตอบระหว่างโฮสต์ต้นทางกับโฮสต์ปลายทาง ส่วนทั้งสามระดับชั้นล่างเป็นโปรโตคอลในลักษณะโหนดที่ติดกัน นอกจากนั้นในการส่งข้อมูลขึ้นไปยังระดับชั้นที่สูงกว่าจะมีการถอดเฮดเดอร์ในแต่ละระดับตัวเองออก แล้วส่งเฉพาะข้อมูลให้แก่ระดับชั้นที่สูงกว่านั้น



รูปที่ 2.12 แสดงตัวอย่างของการส่งข้อมูลของตัวแบบโอเอสไอ

2.4 ตัวแบบทีซีพี/ไอพี (TCP/IP)

ตัวแบบทีซีพี/ไอพี เริ่มมาจากการศึกษาวิจัยที่ได้รับทุนสนับสนุนจากกระทรวงกลาโหมสหรัฐอเมริกา (DoD, U.S. Department of Defence) โดยช่วงแรกนั้นมีเป้าหมายในการเชื่อมโยงข้อมูลระหว่างมหาวิทยาลัยต่าง ๆ ตลอดจน หน่วยงานของรัฐ ในตอนนั้นมีการใช้สายเช่าโทรศัพท์ในการเชื่อมโยงของเครือข่าย และให้บริการส่งข้อมูลเป็นแบบมีการติดต่อกันก่อน และเรียกทั่วไปว่าอาร์พาเน็ต (ARPANET) ต่อมาเมื่อมีการเพิ่มเครือข่ายดาวเทียม และเครือข่ายวิทยุ ซึ่งมีคุณภาพของการส่งข้อมูลต่ำเข้าไปในเครือข่าย ทำให้มีความจำเป็นในการกำหนดสถาปัตยกรรมเครือข่ายใหม่ทำให้สามารถบริการส่งข้อมูลผ่านเครือข่ายที่ให้บริการทั้งแบบการเชื่อมต่อแบบต่อเนื่อง และ แบบการเชื่อมต่อแบบไม่ต่อเนื่องได้ ซึ่งสถาปัตยกรรมนี้เรียกกันทั่วไปว่า รูปแบบทีซีพี/ไอพี (TCP/IP Reference Model) ตามโปรโตคอลทีซีพี (TCP; Transmission Control Protocol) ในระดับชั้นทรานสปอร์ต และโปรโตคอลไอพี (IP; Internet Protocol) ในระดับชั้นเน็ตเวิร์ค ซึ่งเป็นโปรโตคอลสำคัญของสถาปัตยกรรมเครือข่ายนี้ สำหรับตัวแบบทีซีพี/ไอพี ที่เปรียบเทียบกับตัวแบบโอเอสไอได้แสดงดังรูปที่ 2.13 ในที่นี้จะอธิบายโดยสังเขป ถึงเนื้อหาสาระของระดับชั้นต่าง ๆ ของตัวแบบนี้



รูปที่ 2.13 แสดงตัวแบบทีซีพี/ไอพี และ ตัวแบบโอเอสไอ

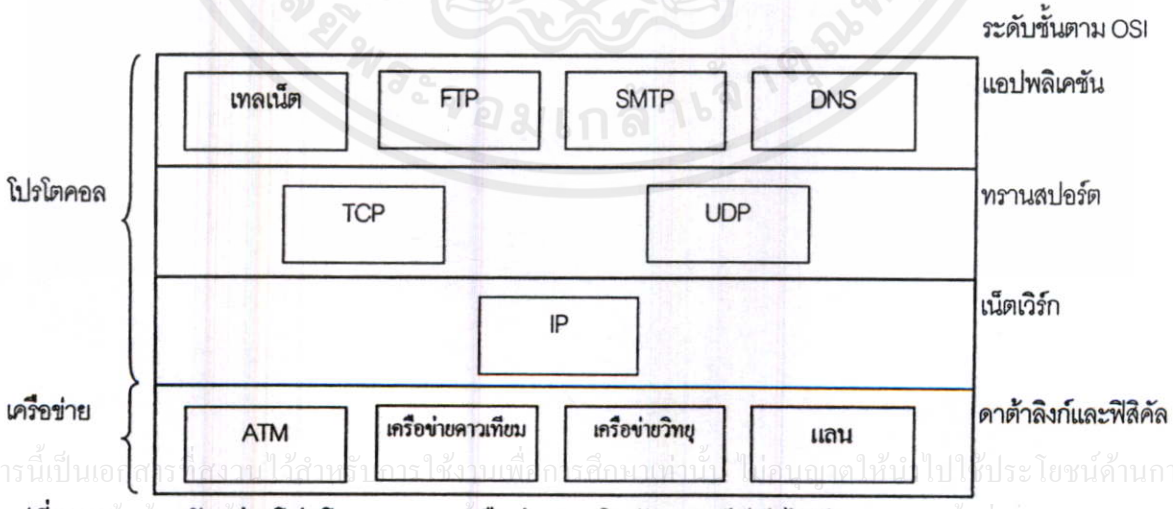
2.4.1 ระดับชั้นอินเทอร์เน็ต

เนื่องจากเป้าหมายของสถาปัตยกรรมนี้ต้องการส่งข้อมูลผ่านหลายเครือข่ายจากโฮสต์ต้นทางไปยังปลายทางได้ และเครือข่ายต่าง ๆ ที่ข้อมูลผ่านนั้น บางเครือข่ายอาจให้บริการเป็นแบบการเชื่อมต่อแบบไม่ต่อเนื่อง และไม่รับประกันความถูกต้องของข้อมูล ซึ่งเป็นปัจจัยสำคัญที่กำหนดคุณลักษณะของเครือข่ายทั้งหมด ดังนั้นโปรโตคอลในระดับชั้นนี้จึงถูกออกแบบมาให้บริการส่งข้อมูลแบบการเชื่อมต่อแบบไม่ต่อเนื่อง โดยโฮสต์ต้นทางสามารถส่งแพ็กเกตข้อมูลเข้าไปในเครือข่ายใด ๆ ได้ แล้วโปรโตคอลนี้จะส่งแพ็กเกตผ่านเครือข่ายต่าง ๆ ไปถึงปลายทางโดยแต่ละแพ็กเกตจะถูกส่งอย่างอิสระจากกันและกัน กล่าวคืออาจจะผ่านเส้นทางแตกต่างกัน และเมื่อไปถึงปลายทาง

อาจจะมีลำดับที่แตกต่างกันจากตอนส่งก็ได้ ซึ่งก็ต้องเป็นหน้าที่ของระดับชั้นทรานสปอร์ต (ซึ่งส่วนใหญ่อยู่ในเครื่องโฮสต์) ทำการควบคุมความผิดพลาดของการส่งข้อมูลเอง ดังนั้นสามารถสำคัญของระดับชั้นอินเทอร์เน็ตนี้เป็นการหาเส้นทางการส่งข้อมูล (routing) ให้ถึงปลายทางได้อย่างถูกต้อง และมีประสิทธิภาพ ซึ่งคล้ายกับสาระสำคัญของระดับชั้นเน็ตเวิร์คของโอเอสไอ

2.4.2 ระดับชั้นทรานสปอร์ต

ระดับชั้นทรานสปอร์ต ของตัวแบบทีซีพี/ไอพี ถูกออกแบบมาให้ทำหน้าที่ควบคุมการส่งข้อมูลระหว่างโฮสต์ปลายทางทั้งสอง ซึ่งก็คล้ายกับหน้าที่ของระดับชั้นทรานสปอร์ตของตัวแบบโอเอสไอ ในระดับชั้นทรานสปอร์ตของทีซีพี/ไอพี นี้มีโปรโตคอลที่ถูกใช้ 2 แบบดังแสดงในรูปที่ 2.14 โปรโตคอลแรกคือทีซีพี ซึ่งให้บริการส่งข้อมูลเป็นแบบการเชื่อมต่อแบบต่อเนื่อง คือควบคุมให้ด้านส่ง หรือด้านรับสามารถส่งข้อมูลแบบไบท์สตรีม ผ่านเครือข่ายอินเทอร์เน็ตได้อย่างถูกต้อง โดยที่ทีซีพีจะแบ่งข้อมูลที่ได้รับมาจากระดับชั้นบนออกเป็นบล็อกที่เหมาะสมกับการส่งผ่านเครือข่าย แล้วส่งข้อมูลไปยังระดับชั้นอินเทอร์เน็ต ส่วนทีซีพีปลายทางจะรวบรวมบล็อกข้อมูลที่ได้รับมาและส่งไบต์ข้อมูลที่ถูกต้องให้แก่ ระดับชั้นบน สำหรับโปรโตคอลแบบที่สองคือ ยูดีพี (User Datagram Protocol; UDP) ซึ่งให้บริการส่งข้อมูแบบการเชื่อมต่อแบบไม่ต่อเนื่อง โดยไม่เน้นความถูกต้องของลำดับของข้อมูล โปรโตคอลนี้เหมาะสำหรับงานประยุกต์ที่ต้องการความเร็วของการส่งข้อมูลมากกว่าความถูกต้องของข้อมูล เช่น การส่งข้อมูลเสียง หรือข้อมูลภาพเคลื่อนไหว นอกจากนั้นยังใช้ สำหรับงานประยุกต์แบบถามตอบข้อมูล (request-reply) และงานประยุกต์ที่ต้องการแพร่กระจายข้อมูลไปยังผู้ใช้หลายคนพร้อมกัน



รูปที่ 2.14 แสดงตัวอย่างโปรโตคอล และเครือข่ายภายในตัวแบบทีซีพี/ไอพี

2.4.3 ระดับชั้นแอปพลิเคชั่น

ตัวแบบของทีซีพี/ไอพี ไม่มีการกำหนดระดับชั้นเซสชันและระดับชั้นพรีเซนเตชัน ซึ่งถือว่าเป็นความคิดที่ถูกต้องเพราะในตัวแบบโอเอสไอนั้น ระดับชั้นเหล่านี้มีการใช้งานน้อยมาก และการที่มีระดับชั้นมากทำให้การทำงานของระบบช้าลง ในระดับแอปพลิเคชันนี้มีโปรโตคอลที่ผู้ใช้หรือโปรแกรมประยุกต์สามารถใช้บริการได้หลายชนิด เช่น เทลเน็ต (Telnet) ซึ่งเป็นโปรโตคอลสำหรับเทอร์มินัลเสมือน โดยทำให้ผู้ใช้สามารถใช้คอมพิวเตอร์ของตนเองในการที่จะเข้าไปใช้งาน (login) เครื่องคอมพิวเตอร์ที่อยู่ไกลออกไปและแสดงผลลัพธ์บนหน้าจอเครื่องตนเอง นอกจากนั้นยังมีโปรโตคอลเอฟทีพี(File Transfer Protocol;FTP) ซึ่งบริการส่งแฟ้มข้อมูลจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งอย่างมีประสิทธิภาพ รวมทั้ง โปรโตคอลเอสเอ็มทีพี (Simple Mail Transfer Protocol; SMTP) ซึ่งใช้ส่งไปรษณีย์อิเล็กทรอนิคส์ผ่านอินเทอร์เน็ต และปัจจุบันมีโปรโตคอลอีกมากที่ถูกออกแบบขึ้นเพื่อช่วยให้โปรแกรมประยุกต์สามารถทำงานภายใต้อินเทอร์เน็ตได้สะดวกขึ้น เช่น ดีเอ็นเอส (Domain Name System; DNS) ซึ่งช่วยเปลี่ยนชื่อของเครื่องโฮสต์ (เช่น cs.yale.edu) ให้เป็นไอพีแอดเดรส (IP address) ที่ใช้ในการส่งข้อมูลในอินเทอร์เน็ต และ โปรโตคอลเอชทีทีพี (HyperText Transfer Protocol; HTTP) ซึ่งใช้ในการดึงข้อมูลจากเว็บไซต์บนเวิลด์ไวด์เว็บ เป็นต้น

2.4.4 ระดับชั้นโฮสต์ ทู เน็ตเวิร์ค (Host to network)

ในส่วนที่ต่ำกว่าระดับชั้นอินเทอร์เน็ต ตัวแบบทีซีพี/ไอพี ไม่ได้กำหนดรายละเอียด เพียงแต่ระบุว่าโฮสต์จะต้องติดต่อเข้ากับเครือข่ายโดยอาศัยโปรโตคอลอย่างใดอย่างหนึ่ง เพื่อที่จะส่งแพ็กเกตผ่านเครือข่ายไปได้ ในการที่ตัวแบบทีซีพี/ไอพี ไม่กำหนดโปรโตคอลที่ใช้ในการติดต่อระหว่างโฮสต์กับเครือข่าย ทำให้ตัวแบบทีซีพี/ไอพีสามารถใช้งานได้ดีทั้งกับแลนและแวน ผู้ออกแบบโปรโตคอลเพื่อใช้ในการส่งข้อมูลจากคอมพิวเตอร์ของผู้ใช้เข้าสู่อินเทอร์เน็ต เช่น โปรโตคอล SLIP (Serial Line IP) และโปรโตคอล PPP (Point to Point Protocol) เป็นต้น

2.5 การบริการแบบการเชื่อมต่อแบบต่อเนื่อง (Connection-oriented) และการเชื่อมต่อแบบไม่ต่อเนื่อง (Connectionless) ในเครือข่าย

ปกติแล้วในการให้บริการส่งข้อมูลอาจจะแบ่งเป็นประเภทใหญ่ๆ ได้ 2 ประเภท ประเภทแรกเป็นระบบโทรศัพท์ ซึ่งก่อนใช้บริการส่งข้อมูล ผู้ใช้ต้นทางและปลายทางต้องสร้างการติดต่อกันให้ได้ก่อน (establish connection) แล้วทำการส่งข้อมูล (data transfer) หลังจากหมดข้อมูลแล้วก็ทำการยกเลิกการติดต่อ (disconection) ซึ่งไม่ว่าการทำงานในระบบโทรศัพท์จะสลับซับซ้อนเพียงไรก็ตาม แต่ผู้ใช้บริการจะเห็นว่าหลังทำการติดต่อแล้วจะมีช่องสัญญาณเชื่อมระหว่างปลายทางทั้งสอง ซึ่งข้อมูลที่ผ่านช่องสัญญานนั้นจะเรียงลำดับกันไปถึงผู้รับในลำดับเดียวกันไปถึงผู้รับใน

ลำดับเดียวกันกับที่ส่งมาจากผู้ส่ง การบริการแบบนี้เรียกกันว่า การบริการแบบการเชื่อมต่อแบบต่อเนื่อง ส่วนการบริการอีกประเภทหนึ่งเป็นการบริการของระบบไปรษณีย์ ซึ่งให้บริการโดยที่ผู้ใช้ไม่ต้องทำการติดต่อกันก่อน เมื่อใดที่ต้องการส่งข้อความก็จะเขียนแอดเดรสของผู้รับบนซองจดหมายและส่งจดหมายไป ซึ่งจดหมายแต่ละฉบับก็จะถูกส่งในเส้นทางที่อาจจะแตกต่างกัน และผู้รับปลายทางก็อาจจะได้รับจดหมายที่มีลำดับแตกต่างกันไปจากลำดับของการส่ง จึงเป็นหน้าที่ของผู้รับในการที่จะเรียงลำดับของข้อมูลเอง การบริการประเภทนี้เรียกว่า การบริการแบบการเชื่อมต่อแบบไม่ต่อเนื่อง ในทำนองเดียวกัน เครือข่ายย่อยส่วนของผู้ให้บริการก็แบ่งการบริการออกได้เป็น 2 ค่าย ค่ายหนึ่งโดยมากเป็นองค์การที่ให้บริการส่งข้อมูลอยู่แล้ว เช่น PTT ตกลงกันว่าการให้บริการนั้นควรเป็นแบบการเชื่อมต่อแบบต่อเนื่องที่เชื่อถือได้ ซึ่งเป็นการบริการที่มีลักษณะสำคัญดังต่อไปนี้

1. ก่อนทำการส่งข้อมูลเอนทิตี้ ในระดับชั้นทรานสปอร์ตของผู้ส่งต้องสร้างการติดต่อกับเอนทิตี้ในระดับชั้นทรานสปอร์ตของผู้รับ และในการติดต่อนี้หากสำเร็จจะมีการกำหนดตัวเลขบ่งบอกของการติดต่อ (identifier) ครั้งนี้ และตัวเลขบ่งบอกนี้จะถูกใช้ตลอดการส่งข้อมูลจนกว่าจะมีการยกเลิกการติดต่อ
2. ในการสร้างการติดต่อนั้น เอนทิตี้ของระดับชั้นทรานสปอร์ตตลอดจนระดับชั้นเน็ตเวิร์คจะมีการติดต่อตกลงกัน (negotiation) ถึงพารามิเตอร์ คุณภาพ ตลอดจนค่าใช้จ่ายของการให้บริการ และหากตกลงได้ก็จะทำการติดต่อ
3. หลังการติดต่อแล้ว การส่งข้อมูลเป็นแบบ 2 ทิศทาง โดยที่แพ็กเกตข้อมูลจะถูกส่งถึงผู้รับอย่างเรียงลำดับกันโดยไม่มีข้อผิดพลาด
4. การควบคุมการส่งข้อมูล (flow control) เพื่อไม่ให้ผู้ส่งส่ง ข้อมูลเร็วเกินไปจนผู้รับรับไม่ทัน ซึ่งอาจทำให้ข้อมูลที่อยู่ในบัฟเฟอร์ของผู้รับนั้นเสียหาย จะเป็นหน้าที่ของระดับชั้นเน็ตเวิร์ค

การบริการชนิดนี้ ผู้ใช้บริการอาจจะต้องเสียค่าใช้จ่ายมากขึ้นแต่ได้รับการประกันว่าข้อมูลจะเรียงลำดับกัน ไม่มีข้อมูลสูญหายหรือข้อมูลซ้ำ สำหรับอีกค่ายหนึ่ง เช่น อินเทอร์เน็ต เห็นว่าเครือข่ายย่อยของผู้ให้บริการควรมีหน้าที่ส่งบิทข้อมูลจากผู้ส่งไปยังผู้รับเท่านั้น ไม่จำเป็นต้องประกันความถูกต้องของข้อมูลหรือประกันการส่งข้อมูลแบบเรียงลำดับ เพราะในทางปฏิบัติที่ผ่านมานั้นเครือข่ายย่อยส่วนของผู้ให้บริการได้ให้บริการส่งข้อมูลซึ่งมีข้อผิดพลาดบ่อยครั้ง ดังนั้นหากโฮสต์ต้องการข้อมูลที่ถูกต้องแล้ว โฮลต์ควรทำการควบคุมความผิดพลาดของการส่งข้อมูลเองและเพื่อไม่ให้มีการควบคุมความผิดพลาดของการส่งข้อมูลซ้ำซ้อน ซึ่งจะทำให้ค่าใช้จ่ายของการส่งข้อมูลสูงขึ้น จึงเห็นว่าเครือข่ายย่อยส่วนของผู้ให้บริการควรให้บริการแบบการสื่อสารไม่ต่อเนื่อง ซึ่งไม่จำเป็นต้องมีการควบคุมความผิดพลาดหรือควบคุมการไหลของข้อมูล โดยที่ในการส่งข้อมูลต้องมีแอดเดรสปลายทางปะไปทุกๆ แพ็กเกต และแพ็กเกตข้อมูลที่ถึงผู้รับปลายทางอาจไม่เรียงลำดับกัน

จึงเป็นหน้าที่ของโฮลต์ปลายทางในการเรียงลำดับแพ็กเกตและควบคุมไม่ให้ข้อมูลหายหรือสูญหาย ตลอดจนควบคุมการไหลของข้อมูลเองการบริการทั้งสองแบบมีความแตกต่างกันหลายประการ ตารางที่ 2.1 แสดงรายละเอียดของความแตกต่างทั้งสอง จะเห็นได้ว่าการบริการสองประเภทนี้ขึ้นอยู่กับว่าความสลับซับซ้อนของการทำงานอยู่ในระดับชั้นใด สำหรับการบริการแบบการเชื่อมต่อแบบต่อเนื่อง นั้นจะอยู่ที่ระดับชั้นเน็ตเวิร์ค ส่วนแบบการเชื่อมต่อแบบไม่ต่อเนื่องนั้น ระดับทรานสปอร์ตต้องทำงานมาก ในส่วนของผู้ที่เห็นด้วยกับการบริการแบบการเชื่อมต่อแบบไม่ต่อเนื่องนี้เห็นว่าราคาของการประมวลผลของโฮลต์จะถูกลงเรื่อยๆ ดังนั้นการให้โฮสต์ทำงานสลับซับซ้อนขึ้น หรือมีการเพิ่มอุปกรณ์บางอย่างที่โฮลต์ ก็จะไม่เสียค่าใช้จ่ายมากนัก อีกทั้งหากเทคโนโลยีการส่งข้อมูลเปลี่ยนไป การปรับโฮสต์ให้เข้ากับเทคโนโลยีที่เปลี่ยนไปนั้นก็จะไม่เปลืองค่าใช้จ่ายมากนัก ส่วนเครือข่ายย่อยนั้นให้บริการส่งข้อมูลผ่านเครือข่ายมีการลงทุนที่สูง เมื่อลงทุนแล้วก็ควรจะสามารถใช้ได้นานๆ โครงสร้างการทำงานของเครือข่ายย่อยควรใช้เทคโนโลยีที่ใช้ได้นานโดยไม่ล้าสมัย เพราะการปรับเครือข่ายย่อยแต่ละครั้งโดยใช้เทคโนโลยีใหม่ๆ เพื่อเพิ่มประสิทธิภาพในการบริการข้อมูลอย่างถูกต้องและให้มีความผิดพลาดน้อยที่สุดนั้นจะใช้ค่าใช้จ่ายที่สูงมาก ในทางกลับกันผู้สนับสนุนการบริการแบบการเชื่อมต่อแบบต่อเนื่อง เช่น ผู้ให้บริการโทรศัพท์หรือการสื่อสาร กลับเห็นว่าผู้ใช้บริการส่วนใหญ่ไม่ต้องการที่จะใช้โฮสต์ทำงานสลับซับซ้อนเพื่อควบคุมการส่งข้อมูล ผู้ใช้ต้องการบริการส่งข้อมูลที่ปราศจากความผิดพลาด เพื่อจะสามารถใช้โฮสต์สำหรับงานประยุกต์อย่างเต็มที่มากกว่า ดังนั้นพิจารณาในแง่ของการประยุกต์การส่งข้อมูลโดยทั่วๆไป หากผู้ใช้บริการเห็นว่าผู้ให้บริการไม่สามารถให้บริการส่งข้อมูลได้ถูกต้องร้อยเปอร์เซ็นต์แล้วเป็นที่แน่นอนว่าผู้ใช้บริการต้องเพิ่มความสามารถบนเครื่องโฮสต์ให้ทำการตรวจสอบความผิดพลาดของการส่งข้อมูลด้วย เพื่อจะได้ข้อมูลที่ถูกต้องตามความต้องการของผู้ใช้ เช่น ในงานธนาคารซึ่งจะไม่ยอมให้เกิดความผิดพลาดเลย (แต่ในการใช้งานระบบจดหมายอิเล็กทรอนิกส์อาจยอมให้มีเกิดความผิดพลาดได้บ้าง) เมื่อเป็นเช่นนี้ผู้ใช้บริการอาจจะคิดว่าการใช้การบริการแบบการเชื่อมต่อแบบต่อเนื่อง เสียค่าใช้จ่ายในการส่งข้อมูลสูงโดยไม่จำเป็น ดังนั้นผู้ใช้อาจใช้บริการของผู้บริการที่ทำหน้าที่ส่งข้อมูลราคาถูกแทน ส่วนการควบคุมความผิดพลาดของการส่งข้อมูลสามารถทำโดยโฮสต์ของผู้ใช้เอง ปัจจุบันนี้เครือข่าย X.25 และ ATM กล่าวได้ว่าเป็นตัวแทนของเครือข่ายที่ให้บริการแบบการเชื่อมต่อแบบต่อเนื่อง ส่วนอินเทอร์เน็ตนับว่าเป็นตัวแทนของการบริการแบบ การเชื่อมต่อแบบไม่ต่อเนื่อง อย่างไรก็ตามโฮสต์ที่ใช้ทีซีพี/ไอพี จะสามารถส่งข้อมูลผ่าน ATM ได้ โดยที่ให้โฮต์ปลายทางทั้งสองสร้างการติดต่อกันโดยอินเตอร์เฟซกับ ATM แล้วให้โฮสต์ส่งไอพีแพ็กเกตผ่านเครือข่าย ATM แต่อย่างไรก็ตามการใช้งานแบบนี้ไม่มีประสิทธิภาพเท่าที่ควร เพราะมีการควบคุมความผิดพลาดของการส่งข้อมูลทั้งระดับชั้นทรานสปอร์ตด้วย ทีซีพี และระดับชั้นเน็ตเวิร์คด้วย ATM

ตารางที่ 2.1 การเปรียบเทียบระหว่างการบริการแบบการติดต่อก่อน และแบบไม่ต้องมีการติดต่อก่อน

	Connection-oriented	**Connectionless**
การสร้างการติดต่อ	**ต้องการ**	**ไม่ต้องการ**
แอดเดรสปลายทาง	ต้องการตอนสร้างการติดต่อ	ต้องการสำหรับทุกๆแพ็กเกต
ลำดับของแพ็กเกต	รับประกัน	ไม่รับประกัน
ควบคุมข้อมูลผิดพลาด	เป็นหน้าที่ของระดับชั้นเน็ตเวิร์ค	เป็นหน้าที่ของระดับชั้นทรานสปอร์ต เช่น โฮสต์
ควบคุมการไหลของข้อมูล	ระดับชั้นเน็ตเวิร์คทำให้	ระดับชั้นเน็ตเวิร์คไม่ทำให้
สามารถเจรจาตกลงระหว่างการสร้างการติดต่อได้หรือไม่	ได้	ไม่ได้
มีการใช้ตัวเลขบ่งบอกการติดต่อหรือไม่	ใช้	ไม่ใช้

2.5.1 การทำงานภายในเครือข่ายย่อยของผู้ให้บริการ

ถึงตอนนี้คงทราบกันแล้วว่าการบริการของระดับชั้นเน็ตเวิร์คให้แก่ระดับชั้นทรานสปอร์ตมี 2 ลักษณะคือ แบบการเชื่อมต่อแบบต่อเนื่อง และแบบการเชื่อมต่อแบบไม่ต่อเนื่อง ซึ่งมีลักษณะการให้บริการแตกต่างกันออกไป กล่าวถึงการทำงานภายในเครือข่ายย่อยส่วนของการสื่อสารของผู้ให้บริการเอง เช่น วิธีการหาเส้นทางและนำส่งข้อมูลผ่านเครือข่ายนั้นแบ่งออกได้เป็น 2 รูปแบบ แบบแรกต้องมีการสร้างการติดต่อก่อนส่งข้อมูล แบบนี้เรียกทั่วไปว่า เวอร์ชวลเซอร์กิต (Virtual circuit) ส่วนอีกแบบหนึ่งไม่ต้องมีการสร้างการติดต่อก่อน ซึ่งเรียกทั่วไปว่า ดาต้าแกรม (datagram) สำหรับการส่งข้อมูลแบบเวอร์ชวลเซอร์กิตนั้นจะใช้สำหรับการบริการแบบการเชื่อมต่อแบบต่อเนื่อง แบบนี้เมื่อมีการติดต่อได้แล้วจะเหมือนกับมีช่องสัญญาณแบบจุดระหว่างปลายทางทั้งสอง ดังนั้นจึงไม่ต้องหาเส้นทางของทุกๆ แพ็กเกต กล่าวคือในการสร้างการติดต่อจะมีการหาเส้นทางที่ดีที่สุดเพื่อส่งข้อมูลระหว่างปลายทางทั้งสอง หลังจากติดต่อได้แล้วแพ็กเกตก็จะถูกส่งผ่านทางที่กำหนดไว้ตลอดการส่งข้อมูล เมื่อเลิกการติดต่อเส้นทางนั้นก็ถูกยกเลิกตาม ดังนั้นจะเห็นว่าแพ็กเกตที่ส่งโดยวิธีเวอร์ชวลเซอร์กิตนี้จะเรียงลำดับกันไป สำหรับการส่งข้อมูลแบบเวอร์ชวลเซอร์กิตนี้จะคล้ายกับเซอร์กิตสวิตชิง ซึ่งในการสร้างการติดต่อจะมีการหาช่องสัญญาณทางกายภาพให้ข้อมูลผ่าน และช่องสัญญาณนั้นจะถูกใช้โดยผู้ใช้คู่หนึ่งเท่านั้น แต่ในกรณีของเวอร์ชวลเซอร์กิตนั้นเส้นทางที่กำหนดไว้อาจจะมีแพ็กเกตของผู้ใช้หลายคนถูกส่งผ่านเส้นทางนั้น สำหรับการส่งข้อมูล

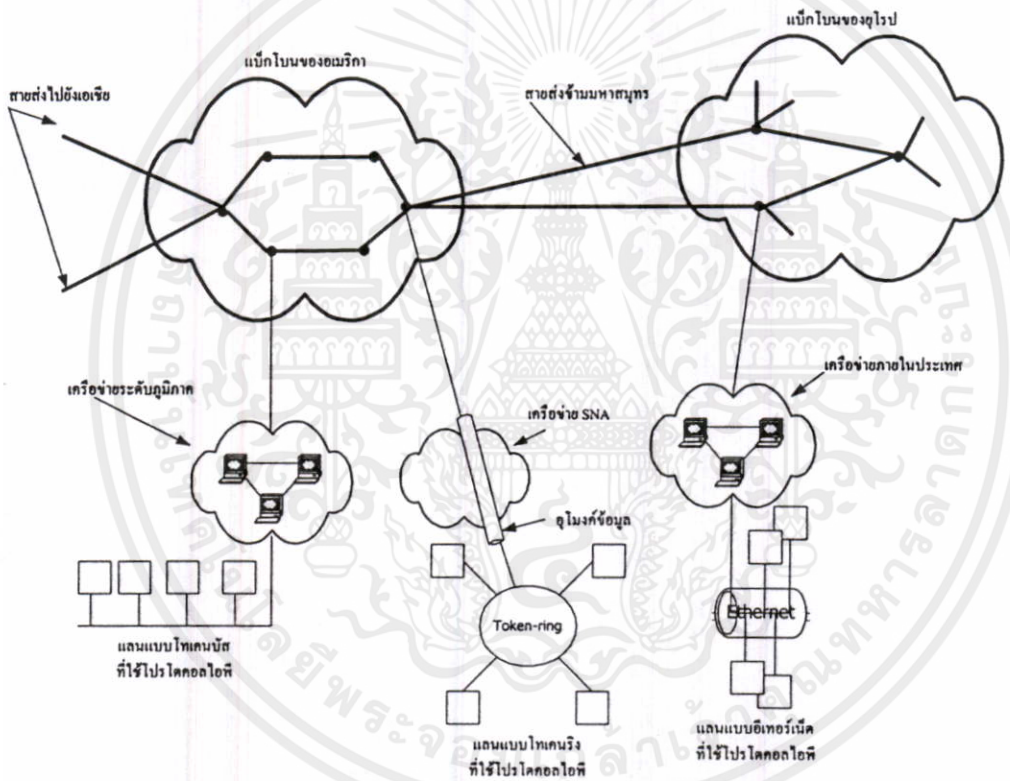
แบบดาต้าแกรมนั้น ไม่มีการหาเส้นทางล่วงหน้าเพื่อส่งข้อมูลไปตามเส้นทางที่กำหนด โดยแบบดาต้าแกรมนี้แต่ละแพ็กเกตจะถูกส่งผ่านเส้นทางที่อาจไม่เหมือนกัน กล่าวคือเมื่อแพ็กเกตเข้าสู่โหนดใด โหนดนั้นจะคำนวณว่าในบรรดาโหนดที่ติดต่อกับโหนดนั้น มีโหนดใดสามารถถึงปลายทางได้อย่างถูกต้องและรวดเร็วที่สุดแล้วจึงส่งข้อมูลไปยังโหนดนั้น ดังนั้นการส่งข้อมูลแบบนี้ข้อมูลที่ถึงโหนดปลายทาง (ที่ติดกับโฮสต์) อาจจะไม่เรียงลำดับกัน ดังนั้นการบริการเป็นแบบการเชื่อมต่อแบบต่อเนื่อง จะเป็นหน้าที่ของโหนดปลายทางในการเรียงลำดับข้อมูล และควบคุมความผิดพลาดของการส่งข้อมูลแล้วส่งให้แก่โฮสต์ แต่หากการบริการเป็นแบบการเชื่อมต่อแบบไม่ต่อเนื่อง แล้ว โหนดปลายทางจะทำงานเพียงแค่ส่งข้อมูลที่ได้รับนั้นให้แก่โฮสต์ จึงต้องเป็นหน้าที่ของโฮสต์ที่จะเรียงลำดับและควบคุมความผิดพลาดในการส่งข้อมูลเอง นอกจากนั้นจะเห็นได้ว่าสำหรับการส่งข้อมูลแบบดาต้าแกรมนั้น แต่ละโหนดของเครือข่ายต้องทำงานมาก แต่อย่างไรก็ตามแบบนี้จะมีประสิทธิภาพของการส่งสูง และเกิดปัญหาน้อยกว่าหากโหนดของเครือข่ายเกิดเสียหรือเกิดการแน่นขนัด การส่งข้อมูลภายในเครือข่ายทั้งสองแบบนี้มีข้อดีและข้อเสียแตกต่างกันหลายประการซึ่งจะได้อธิบายต่อไป แต่ก่อนอื่นจะอธิบายการส่งข้อมูลเวอร์ชวลเซอร์กิต เพื่อจะได้เข้าใจถึงความแตกต่างได้ชัดเจนยิ่งขึ้น รูปที่ 2.14 แสดงการส่งข้อมูลโดยวิธีเวอร์ชวลเซอร์กิต ซึ่งจะมีการสร้างการติดต่อและมีการกำหนดหมายเลขที่ใช้ในการติดต่อซึ่งถูกใช้เป็นหมายเลขเวอร์ชวลเซอร์กิต (virtual circuit number) สำหรับการติดต่อนั้นๆ สำหรับตัวอย่างนี้ หากโฮสต์ที่โหนด A ต้องการส่งข้อมูลติดต่อกับโฮสต์ที่โหนด D แล้ว โฮสต์ A ก็จะสร้างการติดต่อโดยการส่งแพ็กเกตร้องขอ ซึ่งจะมีแอดเดรสของปลายทางออกไป และหากโฮสต์ยังไม่เคยส่งแพ็กเกตติดต่อกับใคร ก็จะใช้หมายเลขเวอร์ชวลเซอร์กิตเป็นค่า 0 เมื่อโหนด A ได้รับแพ็กเกตร้องขอแล้ว จะหาโหนดที่ติดกันซึ่งสามารถส่งข้อมูลไปยัง D ได้เร็วที่สุด หากคำนวณได้เป็นโหนด B และในขณะนั้นโหนด A ยังไม่เคยส่งแพ็กเกตให้ B เลย โหนด A ก็จะใช้เวอร์ชวลเซอร์กิตเป็นค่า 0 ถึงตอนนี้ที่โหนด A จะสามารถสร้าง ตารางการหาเส้นทาง (routing table) ซึ่งมีข้อมูลบ่งว่าได้รับแพ็กเกตจากโฮสต์มาด้วยหมายเลขเซอร์กิต 0 และส่งออกไปยัง B ด้วยหมายเลขเซอร์กิต 0 (ดังแสดงในรูปที่ 2.14 ค) เมื่อแพ็กเกตถึง B แล้ก็จะมีการทำงานทำนองเดียวกัน ซึ่งทำให้สามารถสร้างตารางหาเส้นทางในโหนด B ที่มีข้อมูลบ่งว่าได้รับแพ็กเกตมาจาก A ด้วยหมายเลข 0 และส่งไปยัง C ด้วยหมายเลข 0 จะเห็นว่าการทำงานสำหรับแพ็กเกต Request จะเป็นเช่นนี้ในทุกโหนดตลอดเส้นทางจาก A ถึง D ทำให้เส้นทางของการส่งข้อมูลเป็น ABCD ซึ่งใช้หมายเลขเซอร์กิตของการส่งข้อมูลออกจากโฮสต์ต้นทางเป็นหมายเลข 0 และถึงโฮสต์ปลายทางเป็นหมายเลข 0 ต่อไปหากมีความต้องการส่งข้อมูลจากโฮสต์ B ไปยังโฮสต์ D บ้าง ก็จะมีการสร้างการติดต่อโดยการส่งแพ็กเกต ร้องขอออกไปยังปลายทาง ซึ่งหากโฮสต์ B ยังไม่เคยส่งแพ็กเกตให้โหนด B ก็จะใช้หมายเลขเซอร์กิตเป็นค่า 0 และโหนด B ก็จะหาเส้นทางเพื่อไปยัง D เร็วที่สุด หากได้ว่าต้องส่งแพ็กเกตไปยังโหนด C แล้ว โหนด B ก็จะใช้หมายเลขเซอร์กิตของการส่งไปยัง C เป็นหมายเลข 1 (เนื่องจาก B เคยส่งข้อมูลให้แก่ C

แล้วในเส้นทาง ABCD) ดังนั้นตารางหาเส้นทางของ B จะมีข้อมูลบ่งรับแพ็กเกตมาจากโฮสต์ด้วยหมายเลข 0 แล้วส่งไปยัง C ด้วยหมายเลข 1 กระบวนการดังกล่าวนี้ถูกทำในทุกๆ โหนดที่ผ่านไปจนถึงโฮสต์ D (ดังแสดงดังรูปที่ 2.14 ค) ถึงตอนนี้จะเห็นว่าโฮสต์ที่ D สามารถที่จะรู้ว่าแพ็กเกตที่รับมาจากโหนด D นั้นเป็นแพ็กเกตที่มาจากโฮสต์ A (ซึ่งหมายเลขเซอร์กิตของแพ็กเกตที่เข้ามาเป็นหมายเลข 0)หรือมาจากโฮสต์ B (ซึ่งหมายเลขเซอร์กิตเป็นหมายเลข 1) นอกจากนั้นจะเห็นว่าค่าหมายเลขเซอร์กิตจะถูกใช้มากขึ้นเมื่อมีการสร้างการติดต่อเพิ่มมากขึ้น แต่อย่างไรก็ตามเมื่อมีการยกเลิกการติดต่อแต่ละครั้งหมายเลขเซอร์กิตซึ่งถูกใช้สำหรับการติดต่อนั้นจะถูกปล่อยและสามารถนำไปใช้ได้สำหรับการติดต่ออื่นๆ พิจารณาว่าแพ็กเกตของข้อมูลเดียวกันที่ส่งระหว่างโฮสต์หนึ่งไปยังอีกโอสต์หนึ่งจะถูกส่งผ่านโหนดต่างๆ ของเครือข่ายถึงปลายทางได้อย่างถูกต้องอย่างไรซึ่งตัวอย่างในรูปที่ 2.14(ง) นั้น แสดงแพ็กเกตที่ถูกส่งจากโฮสต์มายังโหนด A แล้ว A ก็จะนำหมายเลขเซอร์กิตในแพ็กเกตซึ่งบ่งบอกว่าเป็นแพ็กเกตส่งมาจากโฮสต์และมีหมายเลขที่เป็นค่า 4 ไปค้นหาในตารางการหาเส้นทาง ก็จะทราบว่าต้องส่งแพ็กเกตนี้ต่อไปยังโหนด E ด้วยหมายเลขเซอร์กิตเป็นค่า 3 ดังนั้นโหนด A จึงเปลี่ยนค่าหมายเลขเซอร์กิตในแพ็กเกตเป็นค่า 3 และส่งออกไปยังโหนด E ซึ่งเมื่อแพ็กเกตถึง E ก็จะทำงานทำนองเดียวกัน คือนำค่าหมายเลขเซอร์กิตไปค้นหาในตารางการหาเส้นทาง ก็ทราบว่าต้องส่งแพ็กเกตให้ C ด้วยหมายเลขเซอร์กิตเป็น 1 จึงเปลี่ยนค่าหมายเลขเซอร์กิตในแพ็กเกตจาก 3 เป็นค่า 1 กระบวนการเช่นนี้จะถูกทำในทุกโหนดที่แพ็กเกตผ่านเส้นทาง ABCD ซึ่งบ่งแสดงด้วยเส้นทางในรูปที่ 2.14 (ค) จนกระทั่งสามารถส่งไปถึงโฮสต์ B

2.6 อินเทอร์เน็ตโปรโตคอล หรือไอพี

ในระดับชั้นเน็ตเวิร์ค อินเทอร์เน็ตถือว่าเป็นกลุ่มของเครือข่ายย่อย หรือระบบงานอิสระ (Autonomous System; AS) เชื่อมโยงกันทั่วโลก ดังแสดงในรูปที่ 2.15 สำหรับระบบงานอิสระหมายถึงเครือข่ายแต่ละเครือข่ายสามารถทำงานเป็นอิสระ ซึ่งกันและกัน จากรูปจะเห็นว่าภายในอินเทอร์เน็ตประกอบด้วยเครือข่ายกระดูกสันหลังหรือ แบ็กโบน (Backbone) ที่สร้างจากสายส่งที่มีอัตราการส่งข้อมูลสูงและเราเตอร์ที่ทำงานด้วยความเร็วสูง และจากเครือข่ายกระดูกสันหลังจะมีเครือข่ายระดับภูมิภาค (Regional network) ต่อเชื่อมโยงอยู่และจากเครือข่ายระดับภูมิภาคจะเป็นเครือข่ายแลนของมหาวิทยาลัย องค์กรต่างๆ ตลอดจนผู้จัดให้บริการอินเทอร์เน็ต (Internet Provider) ต่อเชื่อมเป็นระดับล่างของอินเทอร์เน็ต ดังจะเห็นว่าอินเทอร์เน็ตเป็นเครือข่ายขนาดใหญ่โตมากที่แต่ละเครือข่ายย่อยอาจใช้เทคโนโลยีแตกต่างกันไป ยกตัวอย่าง เช่น เครือข่ายดาวเทียม เครือข่ายเส้นใยแก้วนำแสง เครือข่ายสายทองแดง หรือเครือข่ายระบบวิทยุ แต่อย่างไรก็ตามเครือข่ายเหล่านั้นสามารถส่งข้อมูลติดต่อกันได้ เนื่องจากต่างก็ใช้อินเทอร์เน็ตโปรโตคอล (Internet Protocol) หรือไอพี เป็นมาตรฐานในการส่งข้อมูล และโปรโตคอลนี้ถูกออกแบบเพื่อให้สามารถเชื่อมโยงเครือข่ายชนิดต่างๆ จึงทำให้โฮสต์สามารถส่งแพ็กเกตให้แก่เครื่องปลายทางได้อย่างถูก

ต้อง และมีประสิทธิภาพ ไม่ว่าเครื่องปลายทางจะอยู่ในเครือข่ายเดียวกัน หรืออาจอยู่กันคนละซีกโลก สำหรับการติดต่อภายในอินเทอร์เน็ตทำได้โดยระดับชั้นทรานสปอร์ตเมื่อได้รับข้อมูล ก็จะแบ่งข้อมูลเป็นดาต้าแกรมซึ่งมีขนาดสูงสุด 64 กิโลไบต์ ในทางปฏิบัติดาต้าแกรมมีขนาดประมาณ 1,500 ไบต์ และแต่ละดาต้าแกรมเมื่อถูกส่งผ่านอินเทอร์เน็ต อาจจะถูกแตกย่อย (fragment) ลงมาอีกขึ้นอยู่กับเครือข่ายที่ผ่าน (การแตกย่อยและการรวมตัวใหม่ (reassembly) ของแต่ละเครือข่ายที่เกิดขึ้นที่เกตเวย์) เมื่อแพ็กเกตย่อยถึงปลายทาง จะถูกรวบรวมเป็นดาต้าแกรมเดิมได้โดยระดับชันเน็ตเวิร์คปลายทาง แล้วดาต้าแกรมก็จะถูกส่งให้แก่ระดับชั้นทรานสปอร์ต ซึ่งก็จะทยอยส่งข้อมูลในรูปแบบของไบต์ให้แก่ระดับชั้นที่สูงกว่า

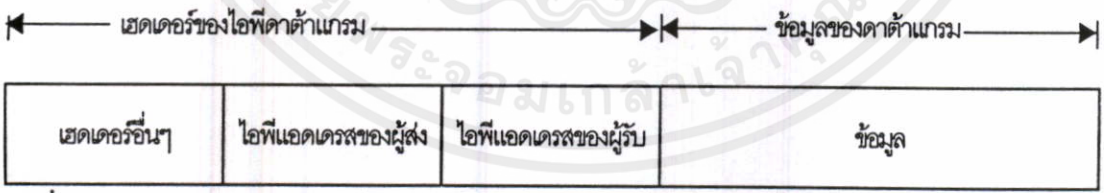


รูปที่ 2.15 ตัวอย่างของอินเทอร์เน็ตที่ประกอบด้วยหลายเครือข่ายเชื่อมโยงกัน

2.6.1 แพ็กเกตของไอพี

รูปที่ 2.16 แสดงรูปแบบของดาต้าแกรมซึ่งประกอบด้วยเฮดเดอร์และข้อมูล และรูปที่ 2.17 แสดงรูปแบบของเฮดเดอร์ซึ่งประกอบด้วยส่วนที่มีความยาวคงที่ 20 ไบต์ (5 x 32 บิทเวิร์ด) และส่วนที่มีความยาวไม่คงที่แน่นอน (option) สำหรับเวอร์ชัน บ่งบอกถึงเวอร์ชันของโปรโตคอลของดาต้าแกรม ซึ่งฟิลด์นี้จะช่วยทำให้เครื่องบางเครื่องสามารถใช้โปรโตคอลเวอร์ชันเดิมในขณะที่บางตัวเริ่มเปลี่ยนไปใช้เวอร์ชันใหม่แล้วสามารถส่งข้อมูลได้ สำหรับ IHL จะบ่งบอกความยาวของเฮดเดอร์ซึ่งรวมออปชันด้วย ความยาวนี้ใช้ 4 บิท ดังนั้นค่าต่ำสุดคือ 5 เวิร์ด และค่าสูงสุดเป็น 15 เวิร์ด

แสดงว่าสามารถมีออปชันได้ถึง 10 เวิร์ด หรือ 40 ไบต์ ส่วน ชนิดของการบริการ (Type of services) เพื่อให้โฮสต์สามารถระบุชนิดของการบริการที่ต้องการได้จากเครือข่ายสำหรับชนิดของการให้บริการ เช่น ความเชื่อถือได้ของการส่งข้อมูล ซึ่งอาจสัมพันธ์กับอัตราการส่งข้อมูลด้วย เช่นในการส่งข้อมูลเสียง อาจต้องการส่งข้อมูลด้วยอัตราส่งสูง ถึงแม้ความเชื่อถือได้ของข้อมูลจะมีน้อยลงก็ตาม แต่สำหรับการส่งแฟ้มข้อมูล ต้องการส่งข้อมูลที่ถูกต้องมากกว่าความเร็วของการส่ง สำหรับฟิลด์ Total length จะบ่งบอกความยาวทั้งหมดซึ่งรวมเฮดเดอร์และข้อมูลที่มีความยาวสูงสุดไม่เกิน 65,536 ไบต์ และไอเดนทิฟิเคชัน บ่งบอกถึงแฟร็กเมนต์ของดาต้าแกรมชุดเดียวกัน เพื่อจะรวมแฟร็กเมนต์เป็นดาต้าแกรมได้ ส่วน DF (Don't Fragment) ใช้บ่งบอกเกตเวย์ไม่ให้แยกส่วนดาต้าแกรมเป็นแฟร็กเมนต์ย่อย ซึ่งอาจเป็นเพราะปลายทางไม่สามารถจะรวมแฟร็กเมนต์เป็นดาต้าแกรมได้ ซึ่งหากดาต้าแกรมนั้นไม่สามารถผ่านเครือข่ายไปได้เนื่องจากเครือข่ายนั้นไม่ยอมให้แพ็กเกตขนาดโตผ่านแล้ว ดาต้าแกรมจะถูกทิ้งไปหรือถูกส่งไปทางเครือข่ายอื่นถึงแม้จะไม่เป็นเส้นทางที่ดีที่สุด ดังนั้นแพ็กเกตอาจจะวนในเครือข่ายต่างๆ จนกว่าจะหมดเวลาและถูกทำลาย ปกติแล้วทุกเครือข่ายต้องยอมให้แพ็กเกตที่มีขนาด 576 ไบต์ผ่านไปได้ ส่วน MF (More Fragment) จะมีค่าเป็น 1 สำหรับทุกๆ แฟร็กเมนต์ ยกเว้นแฟร็กเมนต์สุดท้ายจะมีค่าเป็น 0 ซึ่ง MF จะเป็นการตรวจเช็กซ้อนกับ Total length เพื่อตรวจให้แน่ชัดว่าไม่มีแฟร็กเมนต์ใดหลงหายไป สำหรับ Fragment offset จะบ่งบอกว่าแฟร็กเมนต์นี้เป็นออฟเซตที่เท่าไรของดาต้าแกรมนั้นซึ่งจะใช้เพื่อรวมแฟร็กเมนต์เป็นดาต้าแกรมได้ถูกต้อง ปกติแล้วแฟร็กเมนต์จะมีขนาดเล็กที่สุด 8 ไบต์ ดังนั้นใน 1 ดาต้าแกรมที่มีความยาวสูงสุด 65,536 ไบต์จะมีจำนวนแฟร็กเมนต์ได้มากที่สุด 8,192 แฟร็กเมนต์ ซึ่งจะใช้ 13 บิทสำหรับฟิลด์ Fragment offset



รูปที่ 2.16 แสดงรูปแบบของแพ็กเกตไอพี

ในการส่งข้อมูลแบบดาต้าแกรม เมื่อดาต้าแกรมเข้าไปยังโหนดใด จะมีการคำนวณหาเส้นทางเพื่อให้ไปถึงปลายทางได้อย่างถูกต้องและรวดเร็ว ซึ่งอาจเป็นไปได้ที่ทำให้ดาต้าแกรมวนอยู่ในเครือข่าย ดังนั้น จึงมีการกำหนดเวลาที่ดาต้าแกรมจะอยู่ในเครือข่ายได้โดยใช้ฟิลด์ Time to live เป็นตัวนับเวลา หากหมดเวลาดาต้าแกรมนี้จะถูกทำลาย สำหรับ Time to live หน่วยจะเป็นวินาที และเนื่องจากใช้ 8 บิทสำหรับฟิลด์นี้จึงมีค่าสูงสุดได้ 255 วินาที แต่ในทางปฏิบัติจะนับจำนวนครั้งที่ผ่านเราเตอร์ หากค่าในแพ็กเกตถูกลดไปจนเท่ากับ 0 แพ็กเกต จะถูกทิ้งและจะมีการส่งแพ็กเกตควบคุมแจ้ง

ไปให้แก่ผู้ส่งข้อมูล เมื่อดาต้าแกรมถึงปลายทางแล้ว ดาต้าแกรมจะถูกส่งให้แก่ระดับชั้นทรานสปอร์ตซึ่งในระดับชั้นทรานสปอร์ต มีโปรโตคอลหลายชนิดที่ให้บริการทั้งแบบการเชื่อมต่อแบบต่อเนื่อง เช่น ทีซีพี และแบบการเชื่อมต่อแบบไม่ต่อเนื่อง เช่น โปรโตคอลยูดีพี

รูปที่ 2.17 แสดงเฮดเดอร์ต่างๆ ของแพ็กเกตไอพี

ดังนั้นจึงมีการใช้ฟิลด์โปรโตคอลเพื่อบ่งบอกว่าดาต้าแกรมนี้เป็นของโปรโตคอลใดของระดับชั้นทรานสปอร์ต สำหรับเฮดเดอร์ตรวจสอบ (header checksum) จะใช้ตรวจสอบความถูกต้องของเฮดเดอร์ ซึ่งเฮดเดอร์ของดาต้าแกรมอาจมีการเปลี่ยนแปลงที่เกตเวย์เมื่อผ่านเข้าเครือข่ายที่แตกต่างกัน ส่วนแอดเดรสต้นทาง (source address) และแอดเดรสปลายทาง (destination address) จะเป็นแอดเดรสของทั้งหมายเลขของเครือข่ายและหมายเลขของโฮสต์ ซึ่งจะอธิบายในหัวข้อต่อไป สำหรับออปชันเพื่อเพิ่มลักษณะพิเศษที่นอกเหนือจากเวอร์ชันเริ่มแรก ตัวอย่างของออปชันที่ใช้ เช่นกำหนดความปลอดภัยของข้อมูล กำหนดเส้นทางจากต้นทางถึงปลายทาง กำหนดโหนดที่เส้นทางต้องผ่าน การบันทึกโหนดที่แพ็กเกตผ่านเป็นต้น

2.6.2 ไอพีแอดเดรส

ในอินเทอร์เน็ต ทุกโฮสต์และเราเตอร์จะต้องมีแอดเดรสเพื่อส่งข้อมูลติดต่อกัน ไอพีแอดเดรสของแต่ละโหนดนี้ จะเป็นลอจิคัลแอดเดรส ซึ่งไม่ขึ้นอยู่กับฮาร์ดแวร์หรือรูปแบบเครือข่าย (network configuration) และแอดเดรสนี้มีรูปแบบเหมือนกันไม่ว่าเป็นเครือข่ายชนิดโทเคนริง อีเทอร์เน็ต หรือชนิดอื่นๆ ปกติไอพีแอดเดรสจะประกอบด้วย 4 ไบต์ ซึ่งบ่งบอกทั้งเครือข่ายและโฮสต์ (หรือโหนดที่จะเป็นคอมพิวเตอร์หรืออุปกรณ์อื่นๆ ของเครือข่าย) ซึ่งไอพีแอดเดรส 4 ไบต์นี้จะถูกเขียนแยกแต่ละไบต์ด้วยจุดทศนิยม และแต่ละไบต์จะมีค่าซึ่งบ่งบอกด้วยเลขฐานสิบ เช่น ไอพีแอดเดรส 129.46.7.15 เป็นต้น ในการกำหนดไอพีแอดเดรสของแต่ละโหนดนั้น หากผู้ใช้ต้องการติดต่อพับอินเทอร์เน็ตจะต้องได้รับไอพีแอดเดรสจากองค์กร

DDN Network Information Center

SRI International

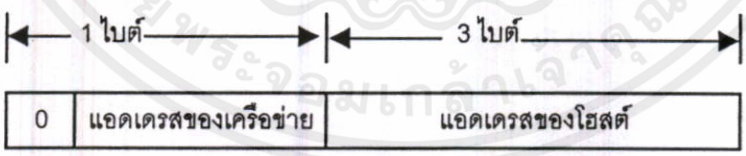
333 Ravenswood Avenue, Room EJ291

Merio Park, CA 94025

USA

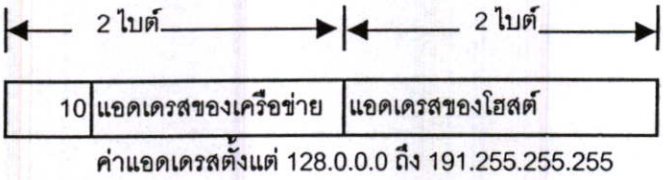
แต่หากไม่ต้องการติดต่อกับอินเทอร์เน็ต ผู้ใช้อาจจะเลือกแอดเดรสใช้เอง ซึ่งในการเลือกแอดเดรสใช้นี้ ควรกำหนดแอดเดรสของทุกโหนดภายในเครือข่ายให้สอดคล้องตามเงื่อนไขต่อไปนี้

1. ส่วนของแอดเดรสของเครือข่ายในไอพีแอดเดรสของทุกโหนดต้องมีแอดเดรสเดียวกัน เช่น ทุกโหนดบนเครือข่าย 129.47 ต้องใช้ 129.47 เป็นส่วนของแอดเดรสของเครือข่ายเป็นต้น
2. ทุกโหนดบนเครือข่ายหนึ่งจะมีไอพีแอดเดรสแตกต่างกับโหนดอื่น
   ดังได้กล่าวมาแล้วว่าไอพีแอดเดรส 4 ไบต์แบ่งออกได้เป็นส่วนของเครือข่ายและส่วนของโฮสต์ ซึ่งการกำหนดแอดเดรสของเครือข่ายและแอดเดรสของโฮสต์ยังแบ่งออกได้เป็นชนิดต่างๆ คือ คลาส (class) A, คลาส B, คลาส C, คลาส D (multicast) และคลาส E ซึ่งไม่ว่าจะเป็นคลาสใดก็ตาม ทุกๆ โหนดในเครือข่ายหนึ่งจะต้องมีส่วนของแอดเดรสเครือข่ายเหมือนกัน และจะต้องมีส่วนของแอดเดรสของโฮสต์แตกต่างกันไปสำหรับแต่ละโหนด รูปที่ 2.18 แสดงไอพีแอดเดรสคลาส A จะใช้ 1 ไบต์สำหรับส่วนของแอดเดรสเครือข่ายซึ่งบิทสูงสุดของไบต์นี้จะมีค่าเป็น 0 และใช้ 3 ไบต์สำหรับส่วนของแอดเดรสของโฮสต์ ดังนั้นจะมีเครือข่ายคลาส A ได้ 126 เครือข่าย (1-126 โดยที่หมายเลขเครือข่าย 0 และ 127 จะถูกจองไว้) และแต่ละเครือข่ายมีโฮสต์ได้ 16 ล้านโหนด



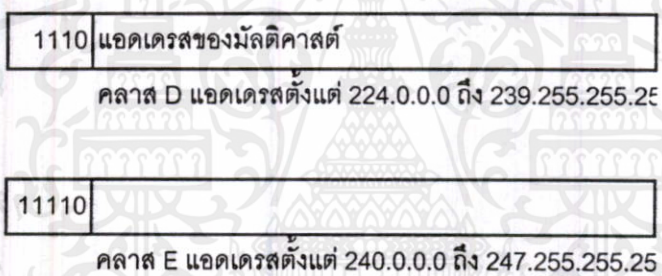
รูปที่ 2.18 แสดงแอดเดรสของคลาส A

รูปที่ 2.19 แสดงไอพีแอดเดรสคลาส B จะใช้ 2 ไบต์สำหรับส่วนของแอดเดรสเครือข่ายซึ่ง 2 บิทสูงสุดของส่วนนี้จะมีค่า 10 และใช้ 2ไบต์สำหรับส่วนของแอดเดรสของโฮสต์ ดังนั้นจะมีเครือข่ายคลาส B ได้ 16,382 เครือข่าย และแต่ละเครือข่ายมีโฮสต์ได้ 64,000 โหนด รูปที่ 2.20 แสดงไอพีแอดเดรสคลาส C จะใช้ 3 ไบต์สำหรับส่วนของแอดเดรสเครือข่ายซึ่ง 3 บิทสูงสุดของส่วนนี้มีค่าเป็น 110 ดังนั้นจะมีเครือข่ายคลาส C ได้ 2 ล้านเครือข่าย และแต่ละเครือข่ายมีโฮสต์ได้ 254 โหนด รูปที่ 2.21 แสดงแบบมัลติคลาสต์ซึ่งแพ็กเกตจะถูกส่งให้กลุ่มของโฮสต์ และคลาส E ซึ่งจองไว้ใช้ในอนาคต



รูปที่ 2.19 แสดงแอดเดรสของคลาส B

รูปที่ 2.20 แสดงแอดเดรสของคลาส C

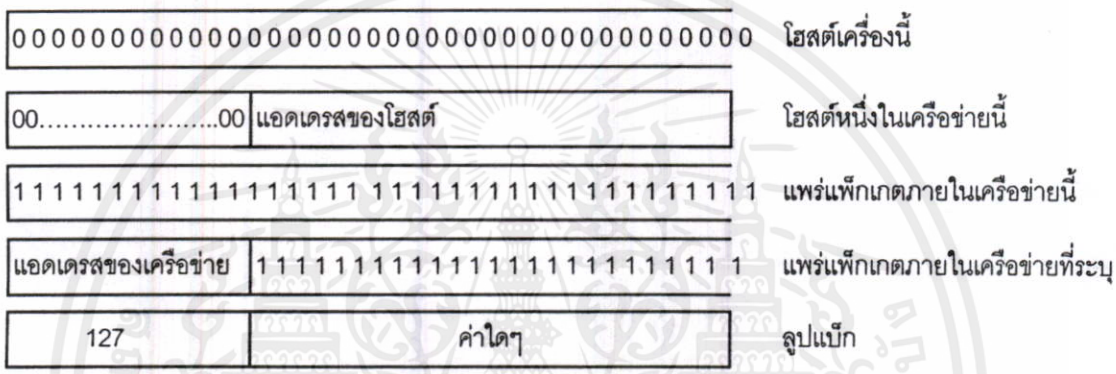


รูปที่ 2.21 แสดงแอดเดรสของคลาส D และคลาส E

นอกจากนั้นไอพีต่อไปนี้จะถูกใช้สำหรับวัตถุประสงค์เฉพาะอย่าง

- แอดเดรสของเครือข่ายสำหรับไอพีแอดเดรสที่มีส่วนของแอดเดรสของโฮสต์มีค่าเป็น 0 จะถูกใช้เป็นแอดเดรสของเครือข่าย เช่น 129.47.0.0 เป็นแอดเดรสเครือข่ายของเครือข่ายคลาส B ดังนั้นไอพีไม่ยอมให้โหนดใดมีแอดเดรสเป็น 0
- แอดเดรส 0.0.0.0 ใช้ในตอนที่โฮสต์ถูกบูต (boot) ขึ้นมา แต่หลังจากนั้นไม่ถูกใช้อีก
- ไอพีแอดเดรสที่มีส่วนของแอดเดรสของเครือข่ายเป็น 0 จะระบุถึงโฮสต์ของเครือข่ายนี้ใช้เพื่อรับส่งแพ็กเกตระหว่างโฮสต์ในเครือข่ายเดียวกัน
- บรอดคาสต์แอดเดรส (broadcast address) สำหรับไอพี ซึ่งแอดเดรสมีค่าเป็น 1 ทั้งหมดจะถูกใช้เพื่อแพร่แพ็กเกตไปยังทุกโฮสต์ของเครือข่ายนี้ และไอพีที่มีส่วนของแอดเดรสของโฮสต์มีค่าเป็น 1 ทั้งหมดจะถูกใช้สำหรับแพร่แพ็กเกตไปยังทุกโหนดในเครือข่ายนั้น เช่น 129.47.127.127 จะหมายถึงแพร่แพ็กเกตไปยังทุกโฮสต์ของเครือข่าย 129.47.0.0 ดังนั้นปกติจะไม่มีการกำหนดให้โหนดใดมีค่าแอดเดรสของโฮสต์เป็น 1 ทั้งหมด

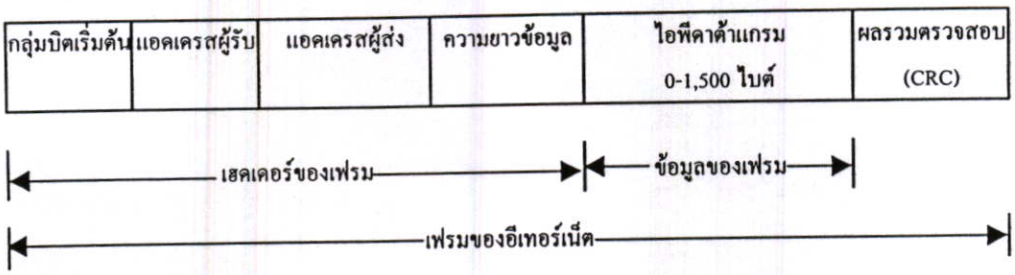
- ลูปแบ็กแอดเดรส (loopback address) 127.aa.bb.cc จะถูกสำรองสำหรับการทดสอบโดยการส่งข้อมูลกลับ แพ็กเกตที่ถูกส่งไปยังแอดเดรสนี้จะไม่ถูกส่งออกไปสู่สายส่ง แต่จะถูกมองเห็นเป็นแพ็กเกตที่เข้ามาและถูกประมวลผลที่เครื่องตนเอง ปกติแล้วการลูปแบ็กใช้เพื่อทดสอบซอฟท์-แวร์ของเครือข่ายนอกจากนั้นไอพีแอดเดรสซึ่งมีส่วนของแอดเดรสของเครือข่ายเป็น 0 ทั้งหมดหรือ 1 ทั้งหมดจะถูกสำรอง ดังนั้นจึงไม่มีการกำหนดแอดเดรสให้โฮสต์ใดมีส่วนของแอดเดรสของเครือข่ายเป็น 0 หรือ 1 ทั้งหมด เช่น แอดเดรสในคลาส B จะกำหนดให้โฮสต์มีค่าแอดเด-รสเป็น 127.127.2.1 หรือ 0.0..2.1 ไม่ได้



รูปที่ 2.22 แสดงแอดเดรสสำหรับวัตถุประสงค์เฉพาะอย่าง

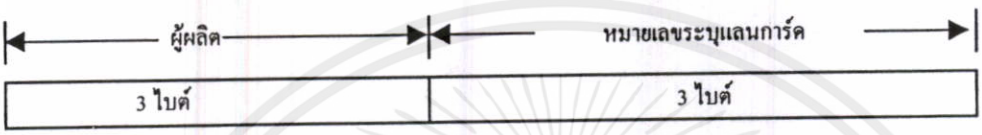
2.6.3 การแปลงไอพีแอดเดรสเป็นแอดเดรสในระดับชั้นดาต้าลิงค์

เนื่องจากไอพีแอดเดรสอยู่ในแพ็กเกตของระดับชั้นเน็ตเวิร์ค ซึ่งในการส่งข้อมูลให้ด้านตรงข้าม แพ็กเกตต้องถูกส่งให้แก่ระดับชั้นดาต้าลิงค์ ซึ่งจะนำแพ็กเกตมาทำเป็นเฟรมโดยจะมีการปะแอดเดรสในระดับชั้นดาต้าลิงค์ของด้านส่งและด้านรับไปด้วย ซึ่งแอดเดรสของเฟรมนี้อาจจะเรียกว่าเป็นฟิสิคัลแอดเดรส (physical address) และในแลน (LAN) อาจจะเรียกว่า แอดเดรส MAC (Medium Access Control) ซึ่งอีเทอร์เน็ตและโทเคนริงจะใช้ 6 ไบต์สำหรับแอดเดรส MAC สำหรับเฟรมของอีเทอร์เน็ตแลน แสดงได้ในรูปที่ 2.23 จะเห็นว่า 3 ไบต์แรกของแอดเดรสจะบ่งถึงผู้ผลิต และ 3 ไบต์ต่อไปจะเป็นหมายเลขระบุแลนการ์ด (LAN card) ที่กำหนดโดยผู้ผลิต ทำให้แอดเดรส MAC นี้มีค่าแตกต่างกันไปสำหรับแต่ละโหนดเนื่องจากระดับชั้นดาต้าลิงค์จะรู้จักเพียงแอดเดรสในระดับชั้นนี้เท่านั้น ดังนั้นด้านส่งต้องสามารถแปลงไอพีแอดเดรสของปลายทางให้เป็นฟิสิคัลแอดเดรส เพื่อที่จะส่งข้อมูลไปยังโหนดปลายทางได้ นอกจากนั้นด้านส่งจะปะไอพีแอดเดรสของตัวเองไปในแพ็กเกตด้วยซึ่งด้านรับอาจจะใช้ไอพีแอดเดรสนี้เพื่อส่งข้อมูลกลับไปยังด้านที่เริ่มส่งข้อมูลได้ ไอพีแอดเดรสไม่ขึ้นอยู่กับชนิดของเครือข่าย ดังนั้นจึงสามารถส่งแพ็กเกตข้อมูลจากเครือข่ายชนิดหนึ่งไปยังเครือข่ายอีกชนิดได้ เช่น จากโทเคนริงไปยังอีเทอร์เน็ต เป็นต้น ในการแปลงไอพีแอดเดรสเป็นฟิสิคัลแอดเดรส อาจทำได้โดยการใช้ Address Resolution Protocol (ARP) สำหรับแลน



: กลุ่มบิตเริ่มต้นเพื่อทำให้สัญญาณของด้านรับทำงานสอดคล้องกับฝั่งส่ง

(ก) รูปแบบของเฟรม



(ข) แอดเดรสของอีเทอร์เน็ต

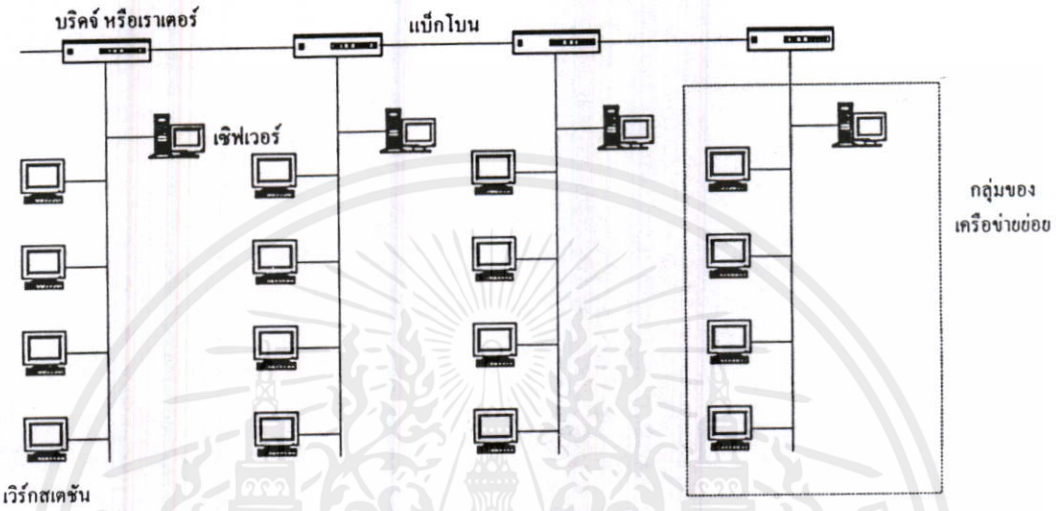
รูปที่ 2.23 แสดงเฟรมของอีเทอร์เน็ตแลน

แบบอีเทอร์เน็ต โทเคนริง และโทเคนบัส ซึ่งทำงานโดยด้านส่งเมื่อต้องการส่งข้อมูลจะแพร่แพ็กเกต ARP ซึ่งจะมีไอพีแอดเดรสของด้านรับอยู่ด้วย เมื่อแพ็กเกต ARP ได้รับโดยโหนดที่มีไอพีแอดเดรสตรงกับที่ระบุในโหนดแอดเดรสของแพ็กเกต ARP โหนดนั้นจะส่งฟิสิคัลแอดเดรสกลับมายังโหนดด้านส่ง ซึ่งจะใช้ฟิสิคัลแอดเดรสที่ได้รับเป็นแอดเดรสปลายทางของเฟรมในการส่งข้อมูลต่อไป

2.6.4 การแบ่งเครือข่ายออกเป็นเครือข่ายย่อย

เครือข่ายซึ่งมีอินเทอร์เน็ตแอดเดรส (Internet Address) หนึ่ง อาจจะถูกแบ่งเป็นเครือข่ายเล็ก ๆ หลายเครือข่าย ซึ่งเหตุผลในการแบ่งเครือข่ายอาจเป็นเพราะเพื่อที่ใช้สื่อ (media) แตกต่างกันไป เนื่องจากไม่สะดวกหรือแพงเกินไป หรือ ทำไม่ได้ที่จะต่อทุกโหนดเข้ากับสื่ออย่างหนึ่งของเครือข่ายเพราะโหนดอยู่ห่างกันมาก หรือโหนดของเครือข่ายต่อเข้ากับสื่อที่แตกต่างกันอยู่แล้ว และต้องการนำมาเชื่อมกันเพื่อใช้ทรัพยากรร่วมกันเพื่อลดการแน่นขนัด เนื่องจากการส่งข้อมูลระหว่างโหนดจะใช้ความสามารถในการส่งข้อมูลของเครือข่าย ซึ่งหากมีโหนดในเครือข่ายมากจะใช้ความสามารถในการส่งข้อมูลมาก ดังนั้นการแบ่งโหนดไปต่อกับเครือข่ายเล็ก ๆจะลดจำนวนของโหนดในแต่ละเครือข่ายลง และหากข้อมูลส่วนใหญ่ถูกส่งภายในเครือข่ายเดียวกัน ก็จะสามารถลดการแน่นขนัดของเครือข่ายได้ ดังตัวอย่างแสดงในรูปที่ 2.24 จะเห็นว่าแต่ละเครือข่ายย่อยจะมีเซิร์ฟเวอร์ของตัวเองซึ่งเวิร์กสเตชันส่วนใหญ่ก็จะใช้บริการของเซิร์ฟเวอร์ของตัวเอง ดังนั้นข้อมูลที่ส่งภายในเครือข่ายย่อยเดียวกันก็จะไม่ถูกเราเตอร์ส่งออกไปยังเครือข่ายย่อยอื่นเพื่อลดการใช้งานซีพียู ในการ

ที่มีโหนดจำนวนมากในเครือข่ายจะทำให้มีแพ็กเกตจำนวนมากถูกแพร่ส่ง เช่น แพ็กเกต ARP ซึ่งทุกโหนดภายในเครือข่ายจะต้องอ่านแพ็กเกตนี้เข้ามาตรวจสอบไอพีแอดเดรสแล้วตอบกลับหรือทิ้งแพ็กเกต ซึ่งทำให้สิ้นเปลืองเวลาซีพียูโหนดเพื่อแยกเครือข่ายหนึ่งออกจากเครือข่ายอื่น ๆ โดยการแยกเครือข่ายใหญ่ ๆ ออกเป็นเครือข่ายย่อย จะทำให้ปัญหาที่เกิดขึ้นในเครือข่าย



รูปที่ 2.24 แสดงตัวอย่างของเครือข่ายย่อย

หนึ่ง (เช่น สายอีเทอร์เน็ตหลุด) จะไม่ไปกระทบต่อเครือข่ายอื่นๆ เพื่อความปลอดภัยของข้อมูลมีมากขึ้น เพราะสำหรับเครือข่ายแบบแพร่กระจาย เช่น อีเทอร์เน็ตนั้น ทุก ๆ โหนดในเครือข่ายจะสามารถเห็นข้อมูลได้เหมือนกันหมด ดังนั้นการแยกเครือข่ายจะช่วยให้ข้อมูลในบางเครือข่ายไม่ถูกเข้าถึงได้โดยโหนดของเครือข่ายอื่นๆ สำหรับการแยกเครือข่ายออกเป็นหลายเครือข่ายย่อยนั้นอาจทำได้หลายวิธี เช่น ในกรณีที่เป็นเครือข่ายที่ใช้ในงานของผู้ใช้เท่านั้น อาจทำได้โดยการแยกเครือข่ายออกแล้วให้กำหนดแอดเดรสให้แก่เครือข่ายเหล่านั้นด้วยตนเอง แต่ในกรณีที่เครือข่ายเชื่อมโยงกับอินเทอร์เน็ต ผู้ใช้ต้องขอแอดเดรสเครือข่ายเพื่อมสำหนับเครือข่ายใหม่จาก Network Information Center แล้วต้องประกาศแอดเดรสนี้ไปทั่วโลก นอกจากนั้นเมื่อมีการย้ายเวิร์กสเตชันไปยังแสนอีกวงจะต้องเปลี่ยนไอพีแอดเดรสของเครื่องเหล่านั้น ซึ่งต้องเปลี่ยนค่าต่าง ๆ ในแฟ้ม config ของระบบปฏิบัติการ และต้องประกาศแอดเดรสใหม่ของเครื่องเหล่านั้นไปทั่วโลก สำหรับอีกรูปแบบหนึ่งของการแยกเครือข่าย ทำได้โดยการสร้างเครือข่ายย่อย (subnetwork) โดยใช้บางบิทจากส่วนของแอดเดรสของโอสต์ โดยเฉพาะในกรณีของเครือข่ายคลาส A หรือคลาส B นั้น อาจจะง่านในการแยกเป็นเครือข่ายย่อยมากกว่าการขอแอดเดรสเพิ่มเติม เพราะผู้ใช้สามารถใช้ส่วนของแอดเดรสของเครือข่ายเดิม ซึ่งจะมีค่าเหมือนกันสำหรับทุกเครือข่ายย่อยเหล่านี้ เมื่อแบ่งเครือข่ายออกเป็นเครือข่ายย่อยแล้ว แต่ละเครือข่ายย่อยจะมีคุณสมบัติดังต่อไปนี้คือ แต่ละเครื่อข่ายย่อยจะทำงานเสมือนเป็นเครือข่ายที่แตกต่างกันไป โดยที่การติดต่อระหว่างโหนดของเครือข่ายย่อยหนึ่ง

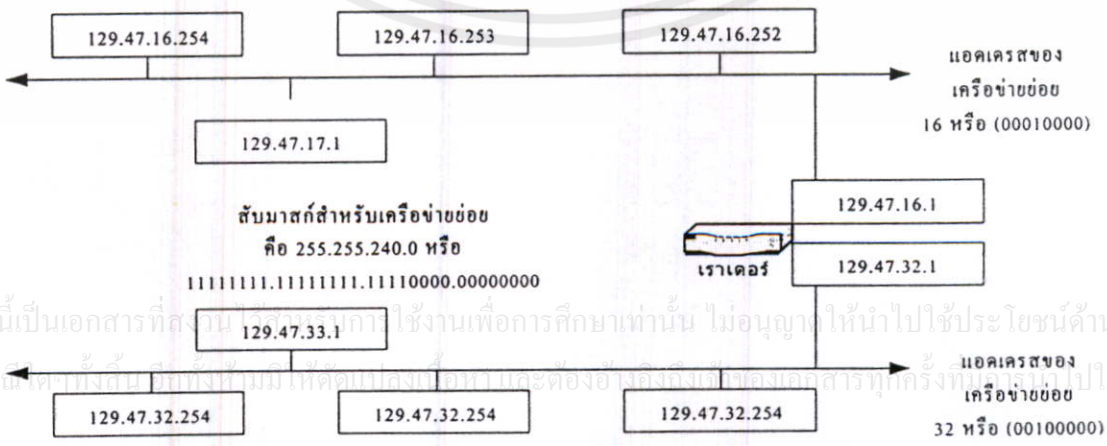
กับโหนดของเครือข่ายย่อยอื่นจะเสมือนกับการติดต่อระหว่างโหนดที่อยู่บนเครือข่ายที่แตกต่างกันไป ถึงแม้ผู้ใช้จะเห็นว่าเป็นโหนดในเครือข่ายเดียวกันเพราะมีแอดเดรสในส่วนของเครือข่ายเหมือนกันก็ตาม โปรแกรมไอพีในโหนดของผู้ส่งจะทราบว่าไอพีแอดเดรสของผู้รับเป็นโหนดที่อยู่ในอีกเครือข่ายย่อยหนึ่งและจะส่งแพ็กเกตไปให้เราเตอร์เพื่อส่งข้อมูลต่อออกไปยังโหนดผั่งรับในเครือข่ายย่อยนั้น แต่สำหนับเครือข่ายภายนอกอื่นที่มีแอดเดรสของเครือข่ายแตกต่างกันกับเครือข่ายย่อยเหล่านี้จะมองเห็นเครือข่ายย่อยเหล่านี้เป็นเครือข่ายเดียวที่มีแอดเดรสของเครือข่ายเดียวกัน สำหรับไอพีแอดเดรสของเครือข่ายย่อยมีรูปแบบต่อไปนี้

(ไอพีแอดเดรส) = (แอดเรสของเครือข่าย) (แอดเดรสของเครือข่ายย่อย)

(แอดเดรสของโฮสต์)

กล่าวคือ ส่วนของแอดเดรสของโฮสต์เดิมจะถูกแบ่งออกเป็น 2 ส่วน คือ ส่วนของแอดเดรสของคครือข่ายย่อย และส่วนของแอดเดรสของโหนด (โฮสต์) เช่น สำหรับเครือข่ายคลาส B ซึ่งไอพีแอดเดรสประกอบด้วยแอดเดรสของเครือข่าย 2 ไบต์เป็น 129.47 แล้วอีก 2 ไบต์ของไอพีแอดเดรสนี้จะถูกแบ่งออกเป็นส่วนของแอดเดรสเครือข่ายย่อยและสวนของแอดเดรสของโฮสต์ซึ่งหากใช้ 4 บิทสำหรับเครือข่ายจะสามารถมีเครือข่ายย่อยได้ 14 เครือข่าย และแต่ละเครือข่ายย่อยจะมีโฮสต์ได้ 4,094 ตัว หรือหากใช้ 8 บิทสำหรับเครือข่ายย่อยแล้ว จะสามารถมีเครือข่ายย่อยได้ 254 เครือข่าย (เครือข่ายย่อยที่มีแอดเดรสเป็น 0 หรือ 1 ทั้งหมดไม่มีการใช้) สำหรับตัวอย่างของการแบ่งเครือข่ายออกเป็นเครือข่ายย่อยแสดงในรูปที่ 2.25 ซึ่งเครือข่าย 129.47.0.0 ถูกแบ่งเป็นเครือข่ายย่อย 129.47.16.0 และ 129.47.32.0 โดยการแบ่งเป็นเครือข่ายย่อยใช้ 4 บิทสำหรับแอดเดรสของเครือข่ายย่อย ซึ่งทำให้ 4 บิทแรกของไบต์ที่ 3 ของ 129.47.0.0 มีค่าได้เป็น 0001...จนถึง1110... (14 เครือข่ายย่อย) และส่วนแอดเดรสของโฮสต์จะเหลือเพียง 12 บิท ซึ่งมีค่าแอดเดรสของโฮสต์ได้ตั้งแต่ 000000000001 ถึง 111111111110 ในตัวอย่างนี้เครือข่ายย่อยแรกมีแอดเดรสของเครือข่ายย่อยเป็น 16 (คือ 00010000) ส่วนเครือข่ายย่อยที่ 2 มีแอดเดรสของเครือข่ายย่อยเป็น 32 (คือ 00100000) นอกจากนั้นจะเห็นว่าเราเตอร์เป็นโหนดที่อยู่ในทั้งสองเครือข่ายจึงมีแอดเดรสทั้ง 2 เครือข่ายคือ 129.47.16.1 และ 129.47.32.1 และเราเตอร์นี้ยังสามารถเชื่อมเครือข่ายอื่นๆและมีไอพีแอดเดรสอื่นๆ อีกได้ เพื่อให้เข้าใจการทำงานของเครือข่ายย่อยมากขึ้น ในที่นี้จะอธิบายถึงการทำงานของเราเตอร์เมื่อได้รับแพ็กเกตเข้ามาปกติแต่ละเราเตอร์จะมีตารางที่มีค่าไอพีแอดเดรสของเครือข่ายบางวงค่าไอพีแอดเดรสนี้ในส่วนของแอดเดรสของเครือข่ายมีค่า แต่ส่วนของโฮสต์เป็นค่า 0 เช่น 129.50.0.0 เป็นต้น ค่านี้จะใช้เพื่อส่งข้อมูลไปยังทุกโฮสต์ที่อยู่ในเครือข่าย 129.50.0.0 ในตารางยังมีข้อมูลของไอพีแอดเดรสของโฮสต์ที่อยู่ในเครือข่ายเดียวกับเราเตอร์ เช่นหากเราเตอร์อยู่ในเครือข่าย 129.60.0.0 และ 129.62.0.0 ในตารางจะมีข้อมูลค่าไอพีแอดเดรสทั้งหมดที่อยู่ใน 2 เครือข่ายนี้ เช่นโฮสต์ 129.60.0.10, โฮสต์ 129.60.0.4 และโฮสต์ 129.60.0.8 เป็นต้น ข้อมูลเหล่านี้ใช้เพื่อส่งข้อ

มูลให้แก่โฮสต์ที่อยู่ในเครือข่ายเดียวกับเราเตอร์ นอกจากนั้นในตารางยังมีข้อมูลของอินเตอร์เฟสการ์ด (Interface card) หรือแลนการ์ดของเราเตอร์ที่จะใช้ในการส่งข้อมูลผ่านการ์ดไปยังปลายทางได้อย่างถูกต้อง เมื่อเราเตอร์ได้รับแพ็กเกตเข้ามา จะใช้แอดเดรสปลายทางของแพ็กเกตตรวจดูในตาราง ถ้าปลายทางอยู่ในเครือข่ายอื่นซึ่งรู้ได้โดยอาศัยข้อมูลแอดเดรสของเครือข่าย จะส่งแพ็กเกตข้อมูลผ่านอินเตอร์เฟซการ์ดไปยังเราเตอร์ตัวอื่นเพื่อส่งต่อไปยังเครือข่ายนั้น หากปลายทางเป็นโฮสต์ที่อยู่ในเครือข่ายเดียวกันกับเราเตอร์ เราเตอร์จะส่งแพ็กเกตข้อมูลให้แก่โฮสต์โดยตรง แต่ถ้าปลายทางอยู่ในเครือข่ายที่ไม่รู้จัก จะส่งแพ็กเกตนั้นไปยังดีฟอลต์เราเตอร์ (default router) ซึ่งจะมีตารางแอดเดรสที่ใหญ่กว่า ในกรณีของเครือข่ายย่อย ค่าในตารางหาเส้นทางจะเปลี่ยนแปลงบ้าง กล่าวคือจะมีไอพีแอดเดรสที่มีค่าเฉพาะในส่วนของเครือข่ายหลักและเครือข่ายย่อย แต่ส่วนโฮสต์มีค่าเป็น 0 เช่น เครือข่ายในรูปที่ 2.26 นั้น แอดเดรสในส่วนเครือข่ายคือ 129.47.0.0 และส่วนเครือข่ายย่อยไบต์ที่ 3 อาจเป็นค่า 80 (คือ 01010000) ซึ่งข้อมูลนี้ มีเพื่อจะส่งข้อมูลไปยังทุกโฮสต์ที่อยู่ในเครือข่ายย่อย 129.47.80.0 นอกจากนั้นยังมีค่าไอพีแอดเดรสของโฮสต์ที่อยู่ในเครือข่ายย่อยเดียวกันกับเราเตอร์ เช่น มีไอพีแอดเดรสของโฮสต์ 129.47.32.252 และโฮสต์ 129.47.32.253 ซึ่งอยู่ในเครือข่ายหลัก 129.47.0.0 และเครือข่ายย่อย 32 เป็นต้น ข้อมูลนี้เพื่อส่งข้อมูลให้แก่โฮสต์ที่อยู่ในเครือข่ายย่อยเดียวกันกับเราเตอร์นั่นเอง ในทางปฏิบัติ การส่งแพ็กเกตของเราเตอร์จะใช้สับเน็ตมาสก์ (Subnet mask) เช่นในรูปที่ 2.26 คือ 11111111111111111111000000000000 กับแอดเดรสปลายทางของแพ็กเกต จะทราบว่าเครือข่ายย่อยที่จะต้องส่งแพ็กเกตข้อมูลไป คือเครือข่ายใด เช่น เมื่อมีแพ็กเกตที่มีแอดเดรสหลายทางเป็น 129.47.17.1 มาถึง และนำมาแอนด์ (And) กับสับเน็ตมาสก์ จะได้ค่าเป็น 129.47.16.0 คือเป็นเครือข่ายย่อยเดียวกับที่เราเตอร์อยู่ซึ่งในตารางหาเส้นทางของมันจะมีแอดเดรสของโฮสต์ที่อยู่ในเครือข่ายย่อยนี้ด้วย จะส่งข้อมูลให้แก่โฮสต์ได้โดยตรง แต่หากปลายทางมีค่าไอพีแอดเดรสเป็น 129.47.90.7 เมื่อแอนด์กับสับเน็ตมาสก์จะได้ค่าเป็นเครือข่ายย่อย 129.47.80.0 ซึ่งเราเตอร์ต้องส่งแพ็กเกตข้อมูลออกไปให้แก่เราเตอร์อื่นต่อไป



รูปที่ 2.25 แสดงตัวอย่างการแบ่งเครือข่ายออกเป็นเครือข่ายย่อย

2.6.5 การแพร่ข้อมูลเฉพาะกลุ่มภายในอินเทอร์เน็ต

งานประยุกต์หลายอย่างที่ต้องการส่งข้อมูลให้กลุ่มของผู้ใช้พร้อมๆ กัน เช่น การส่งข้อมูลหุ้นให้แก่โบรกเกอร์ หรือการประชุมเฉพาะกลุ่ม เป็นต้น โปรโตคอลไอพีช่วยให้สามารถส่งข้อมูลติดต่อภายในกลุ่มได้โดยอาศัยแอดเดรสคลาส D ดังแสดงในรูปที่ 2.21 ซึ่งใช้ 4 บิทในการระบุคลาส และใช้ 28 บิทสำหรับระบุกลุ่มผู้ใช้ ดังนั้นจึงสามารถมีกลุ่มได้ประมาณ 250 ล้านกลุ่ม แอดเดรสแบบมัลติคาสต์นี้แบ่งได้เป็น 2 ชนิด คือ แอดเดรสชนิดถาวร และแอดเดรสชนิดชั่วคราว สำหรับแอดเดรสชนิดถาวรนั้นจะคงอยู่ตลอดโดยไม่ต้องกำหนดใหม่ทุกครั้งที่ต้องการใช้ ตัวอย่างของแอดเดรสชนิดถาวร เช่น 224.0.0.1 ซึ่งจะใช้เพื่อแพร่ข้อมูลให้แก่ทุกระบบบนแลนวงหนึ่ง หรือ 224.0.0.2 ซึ่งใช้เพื่อแพร่ข้อมูลให้แก่ทุกเราเตอร์บนแลนวงหนึ่ง เป็นต้น ส่วนแอดเดรสชนิดชั่วคราวจะต้องกำหนดก่อนที่จะใช้ทุกครั้ง โดยที่โปรเซสส์บนโฮสต์อาจจะบอกโฮสต์เข้าร่วมเป็นสมาชิกหรือออกจากการเป็นสมาชิกของกลุ่มใดกลุ่มหนึ่งได้ และแต่ละโฮสต์ จะตรวจสอบเสมอว่าขณะนี้โปรเซสส์ใดบนเครื่องตนเองเป็นสมาชิกของกลุ่มใดบ้าง การแพร่ข้อมูลแบบมัลติคาสต์นี้ทำได้โดยอาศัยเราเตอร์แบบมัลติคาสต์ (หรืออาจเป็นฟังก์ชันหนึ่งในเราเตอร์แบบมาตรฐานได้) โดยทุกๆนาทีเราเตอร์แบบมัลติคาสต์นี้จะแพร่ข้อมูลให้แก่ทุกระบบบนแลนของตนเอง โดยระบุแอดเดรสเป็น 224.0.0.1 เพื่อให้โฮสต์เหล่านั้นส่งข้อมูลที่บอกว่าโปรเซสส์บนโฮสต์เหล่านั้นอยู่ในกลุ่มใดบ้างโดยโฮสต์จะส่งแอดเดรสคลาส D ที่มันเป็นสมาชิกกลับมาให้

2.7 โปรโตคอลทีซีพี (The Internet Transport Protocols; TCP & UDP)

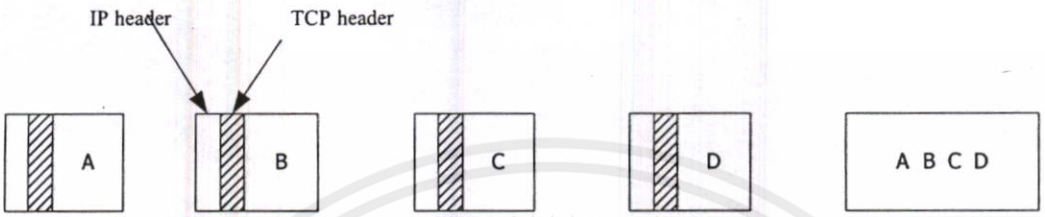
ระบบอินเทอร์เน็ตมีโปรโตคอลชั้นนำส่งข้อมูลหลักสองแบบคือ แบบทีซีพี (Transport Control Protocol) ซึ่งเป็นการเชื่อมต่อแบบต่อเนื่อง (connection-oriented) และแบบ ยูดีพี (User Datagram Protocol) ซึ่งเป็นการเชื่อมต่อแบบไม่ต่อเนื่อง (connectionless) เนื่องจาก ยูดีพี มีลักษณะคล้ายกับแพ็กเกตไอพี แต่มีการเติมข้อมูลส่วนหัวสั้นๆ เข้าไปด้วย ในที่นี้จึงจะกล่าวถึงแต่เรื่องของทีซีพี เท่านั้น โปรโตคอลทีซีพี ได้รับการออกแบบมาให้เป็นโปรโตคอลที่ไว้วางใจได้ (reliable) เพื่อใช้ในการสื่อสารผ่านระบบเครือข่ายทั่วไปที่อาจมีความผิดพลาดเกิดขึ้นในขณะนำส่งข้อมูลอยู่เสมอ ทั้งนี้การสื่อสารผ่านระบบเครือข่ายทั่วไปนั้นมีความแตกต่างกันมากมายในเรื่องรูปแบบเครือข่าย ขนาดช่องสัญญาณ ขนาดแพ็กเกต และประเภทและจำนวนพารามิเตอร์ที่ใช้ ทีซีพี จึงถูกออกแบบมาให้สามารถปรับตัวเข้ากับความแตกต่างเหล่านี้ได้เป็นอย่างดี รวมทั้งสามารถทนทานต่อความล้มเหลวในระหว่างการนำส่งข้อมูลที่อาจเกิดขึ้นเมื่อใดและในส่วนใดก็ได้ โปรโตคอลทีซีพี ถูกกำหนดเป็นมาตรฐานรุ่นแรกเรียกว่า RFC 793 ต่อมาได้รับการปรับปรุงแก้ไขเรื่อยมาจนออกมาเป็นมาตรฐาน RFC 1122 และ RFC 1323 ตามลำดับ โฮสต์ที่สนับสนุนการทำงานโปรโตคอลทีซีพี จะต้องมีเอ็นติตี้ ทีซีพี ซึ่งอาจเป็นส่วนประกอบของโปรเซสผู้ใช้หรือเป็นส่วนหนึ่งของระบบปฏิบัติการ มี

หน้าที่ในการบริหารข้อมูลของทีซีพี และติดต่อกับชั้นสื่อสารที่ควบคุมแพ็กเกตไอพีโดยตรง เอ็นติตี้ทีซีพี รับข้อมูลจากโปรเซสผู้ใช้ แบ่งข้อมูลออกเป็นส่วนย่อยที่มีขนาดไม่เกิน 64 Kbytes (โดยปกติมีขนาดประมาณ 1,500 ไบท์) แล้วจึงส่งไปยังผู้รับในรูปแบบของดาต้าแกรมไอพีแพ็กเกต เมื่อแพ็กเกตเดินทางมาถึงก็จะถูกส่งต่อให้กับเอ็นติตี้ทีซีพี ซึ่งจะสร้างข้อมูลให้กลับไปอยู่ในสภาพเดิม เนื่องจากชั้นสื่อสารที่ควบคุมการรับ-ส่งแพ็กเกตไอพี ไม่มีการรับประกันความสำเร็จในการนำส่งข้อมูล ดังนั้นเป็นหน้าที่ของเอ็นติตี้ทีซีพี ที่จะต้องกำหนดระยะเวลารอคอยให้เหมาะสมและทำการส่งแพ็กเกตซ้ำในกรณีที่จำเป็น แพ็กเกตที่เดินทางมาถึงอย่างสมบูรณ์ก็อาจอยู่ในลำดับที่ไม่ถูกต้องจึงเป็นหน้าที่ของเอ็นติตี้ทีซีพี ที่จะต้องจัดเรียงลำดับข้อมูลให้ถูกต้อง กล่าวโดยสรุปคือเอ็นติตี้ทีซีพี มีบทบาทสำคัญในการจัดการนำส่งข้อมูลให้แก่ผู้ใช้ได้อย่างถูกต้องสมบูรณ์บนพื้นฐานของการนำส่งข้อมูลแบบไอพีที่ไม่มีความสมบูรณ์ในตัวเอง

2.7.1 รูปแบบบริการของทีซีพี

บริการทีซีพี เริ่มต้นจากการที่ทั้งฝ่ายผู้รับและผู้ส่งข้อมูลสร้างส่วนควบคุมการติดต่อระหว่างกันแบบที่เรียกว่า "ซ็อคเก็ต (socket)" ซ็อคเก็ตแต่ละตัวจะมีหมายเลขที่อยู่ประกอบด้วยสองส่วนคือหมายเลขไอพีของโฮสต์และหมายเลขขนาด 16 บิทที่ใช้ภายในโฮสต์นั้นๆเรียกว่า "พอร์ต (port)" ซึ่งก็คือชื่อของเอ็นติตี้ ทีซีพี ซ็อคเก็ตแต่ละตัวสามารถนำมาใช้ควบคุมการติดต่อได้มากกว่าหนึ่งคู่การเชื่อมต่อในเวลาเดียวกันหรืออีกนัยหนึ่งการเชื่อมต่อหลายเส้นทางอาจใช้ซ็อคเก็ตเดียวกันก็ได้ การระบุการเชื่อมต่อกระทำโดยการระบุคู่ของซ็อคเก็ตที่ต้องการ เช่น (ซ็อคเก็ต1,ซ็อคเก็ต2) หมายเลขวงจรเสมือนหรือหมายเลขอื่นใดไม่มีความสำคัญสำหรับการระบุการเชื่อมต่อในระบบนี้ พอร์ตหมายเลขต่ำกว่า 256 เป็นพอร์ตที่ใช้ในงานพื้นฐานทั่วไปซึ่งถูกสำรองไว้ใช้งานเฉพาะอย่างเท่านั้น เช่น โปรเซสใดๆ ที่ต้องการสร้างการเชื่อมต่อเข้ากับโฮสต์หนึ่งเพื่อการรับ-ส่งสำเนาแฟ้มข้อมูลผ่านโปรแกรมเอฟทีพี (FTP) จะต้องระบุพอร์ตหมายเลข 21 จึงจะสามารถติดต่อกับบริการเอฟทีพีของโฮสต์ หรือการเชื่อมต่อผ่านโปรแกรมเทลเน็ต (TELNET) ก็จะต้องระบุพอร์ตหมายเลข 23 พอร์ตใช้งานพื้นฐานหมายเลขอื่นๆ อธิบายไว้ในมาตรฐาน RFC 1700 การเชื่อมต่อของเอ็นติตี้ ทีซีพีเป็นการสื่อสารสองทางแบบสมบูรณ์ (full – duplex) และเชื่อมต่อจุด-ต่อ-จุด (point-to-point) หมายความว่าการเชื่อมต่อจะมีโฮสต์อยู่เพียง 2 โฮสต์ที่ปลายสายแต่ละข้างซึ่งสามารถส่งข้อมูลสวนทางกันได้ตลอดเวลา ทีซีพี ไม่สนับสนุนการเชื่อมต่อหลายจุด (multicasting) และแบบกระจายข่าว (broadcasting) การส่งข้อมูลผ่านโปรโตคอลทีซีพีเป็นไปในลักษณะชุดหรือไบต์สตรีม (byte stream) ไม่ใช่กลุ่มของข่าวสาร (message) ขอบเขตของข่าวสารแต่ละชุดจึงไม่มีการกำหนดใช้งาน เช่น การส่งข่าวสารออกไป 4 ชุด ชุดละ 512 ไบต์ผ่าน ทีซีพี โปรโตคอล ข้อมูลทั้งหมดอาจถูกส่งไปยังผู้รับในลักษณะเป็นชุด ชุดละ 512 ไบต์ 4 ชุด ชุดละ 1,024 ไบต์ 2 ชุด ชุดละ 2,048 ไบต์ 1 ชุด หรืออย่างไรก็ได้ (ดูรูปที่ 2.26) ทางผู้รับจึงไม่สามารถทราบได้เลยว่าข้อมูลที่ส่งมานั้นประกอบด้วย

ข่าวสาร (message) กี่ชุด แฟ้มข้อมูลในระบบปฏิบัติการยูนิกส์ ใช้วิธีการเดียวกันนี้ในการเก็บข้อมูล คือผู้ใช้ไม่อาจทราบได้เลยว่าข้อมูลในแฟ้มที่กำลังอ่านอยู่นั้นถูกอ่านขึ้นมาครั้งละบล็อก ครั้งละไบต์หรือทั้งแฟ้มพร้อมกัน ทีซีพี เอ็นติตี้จึงไม่มีความสนใจในโครงสร้างของข้อมูลที่กำลังทำการรับส่งอยู่เพียงแต่ให้ความสนใจในการรับ-ส่งให้ครบจำนวนไบต์อย่างถูกต้องเท่านั้น



รูปที่ 2.26 (ก) เซ็กเมนต์ขนาด 512 ไบต์จำนวน 4 แพ็กเกต (ข) ข้อมูล 2,048 ไบต์ถูกส่งไปยังผู้รับในแพ็กเกตเดียว

เมื่อโปรเซสผู้ใช้ส่งข้อมูลมายัง ทีซีพี เอ็นติตี้ ข้อมูลนั้นอาจถูกส่งออกไปในทันที หรืออาจถูกเก็บรวบรวมไว้ก่อน (เพื่อรวบรวมส่งเป็นกลุ่มขนาดใหญ่พร้อมกัน) ในบางครั้งโปรเซสที่ส่งข้อมูลเข้ามาอาจต้องการให้ข้อมูลนั้นถูกส่งออกไปในทันที เช่น การติดต่อเข้ากับระบบโต้ตอบทันที (Interactive) เมื่อผู้ใช้พิมพ์คำสั่งเสร็จข้อมูลนั้นจะถูกส่งออกไปในทันทีที่ผู้ใช้กดแป้นพิมพ์ "Enter / Return" ในการทำงานลักษณะนี้ผู้ใช้สามารถบังคับให้ ทีซีพี เอ็นติตี้ส่งข้อมูลออกไปทันทีโดใช้คำสั่ง "Push" ข้อมูลที่ส่งไปพร้อมกับสัญญาณข้อมูลด่วนจะถูกส่งไปยังผู้รับ ทีซีพี เอ็นติตี้ไม่มีหน้าที่ในการจัดการข้อมูลนี้ จึงเป็นหน้าที่ของโปรแกรมทางผู้รับที่จะต้องแปลความหมายของข้อมูลนี้เอง กระบวนการนี้แม้ว่าจะไม่ได้อำนวยความสะดวกมากนักแต่ก็ช่วยให้โปรแกรมของผู้ใช้สามารถส่งข่าวสารด่วนพิเศษไปมาระหว่างกันได้

2.7.2 โครงสร้างโปรโตคอล ทีซีพี

โครงสร้างโดยทั่วไปของโปรโตคอล ทีซีพี ส่วนรายละเอียดของข้อมูลส่วนหัว (header) ข้อมูลในแต่ละกลุ่มที่ส่งออกไปจะมีหมายเลขลำดับขนาด 32 บิท เป็นของตนเองซึ่งจะไม่ซ้ำกันเลย ในทางทฤษฎีระบบเครือข่ายเฉพาะบริเวณทำงานที่ความเร็ว 10 เมกะบิทต่อวินาทีอาจจะทำให้หมายเลขลำดับวนกลับมาซ้ำกันได้ภายในเวลาประมาณหนึ่งชั่วโมงแต่ในความเป็นจริงนั้นจะต้องใช้เวลานานกว่านี้มาก หมายเลขลำดับถูกนำมาใช้สำหรับการส่งข้อมูลตอบรับและกระบวนการหน้าต่างสื่อสารแบบต่างๆ เอ็นติตี้ทีซีพี ของผู้ส่งและผู้รับจะแลดเปลี่ยนข้อมูลระหว่างกันครั้งละเซกเมนต์ (segment) แต่ละเซกเมนท์ประกอบด้วยข้อมูลส่วนหัวขนาดคงที่จำนวน 20 ไบต์ ตามด้วยข้อมูลส่วนตัวเลือกจำนวนหนึ่งและส่วนสุดท้ายคือข้อมูลจริง (อาจไม่มีอยู่เลยก็ได้) เอ็นติตี้ทีซีพี จะเป็นผู้

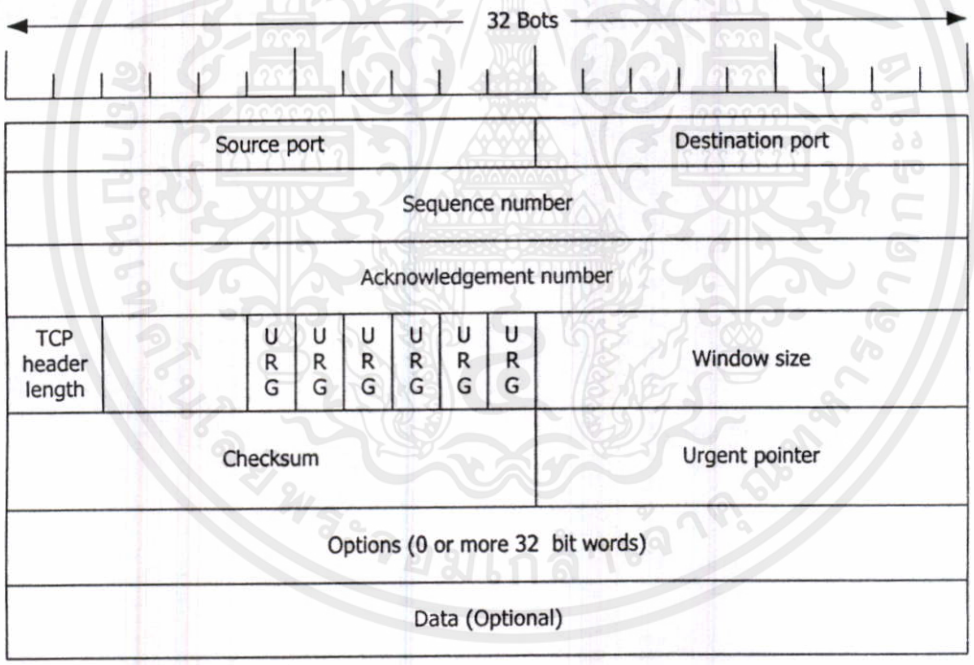
กำหนดขนาดของเซกเมนท์ที่จะใช้ ข้อมูลที่จะถูกส่งในแต่ละครั้งอาจรวบรวมมาจากหลายๆ แหล่ง หรือแบ่งข้อมูลจากแหล่งหนึ่งออกเป็นหลายๆเซกเมนท์ องค์ประกอบที่บังคับขนาดของเซ็กเมนท์มีอยู่สองส่วน ส่วนแรกเป็นขนาดจำกัดสูงสุด 64 Kbytes (หรือ 65,535 ไบต์) ขนาดของแต่ละเซก-เมนท์รวมทั้งข้อมูลส่วนหัวจะต้องไม่เกินนี้ ส่วนที่สองมาจากค่ากำหนดขนาดสูงสุดของแพ็กเกต แต่ละระบบเครือข่ายที่เรียกว่า MTU อาจมากกว่าหรือน้อยกว่า 64 Kbytes ก็ได้ แต่โดยทั่วไปแล้วจะมีขนาดน้อยกว่า ดังนั้นจึงกลายเป็นข้อจำกัดขนาดเซ็กเมนท์ไปโดยปริยาย เซ็กเมนท์ที่ถูกส่งออกมาแล้วจากโฮสต์ผู้ส่งอาจเดินทางผ่านระบบเครือข่ายต่างๆ ที่มีขนาด MTU แตกต่างกันออกไป เมื่อใดก็ตามที่ MTU จากด้านที่รับเข้ามามีขนาดใหญ่กว่า MTU ทางด้านที่จะส่งออกไป เราเตอร์ตัวที่รับข้อมูลเข้ามาจะต้องแบ่งเซ็กเมนท์นั้นออกเป็นเซ็กเมนท์ย่อยก่อนที่จะส่งออกไป เมื่อเซ็กเมนท์ถูกแบ่งออกเป็นส่วนเล็กๆ เซ็กเมนท์ใหม่แต่ละตัวจะต้องได้รับหมายเลขไอพีใหม่ที่ไม่ซ้ำกันทำให้ค่าโสหุ้ย (overhead) ในการส่งข้อมูลสูงขึ้น เพราะอย่างน้อยที่สุดทุกเซ็กเมนท์จะต้องเพิ่มข้อมูลส่วนหัวขนาดไม่ต่ำกว่า 20 ไบต์เข้าไปด้วยการควบคุมการไหลเวียนของข้อมูลแบบพื้นฐาน นิยมใช้โปรโตคอลหน้าต่างเลื่อนไหล (sliding window) เมื่อผู้ส่งส่งเซ็กเมนท์หนึ่งออกมาก็จะเริ่มจับเวลาในทันที เมื่อเซ็กเมนท์นั้นเดินทางมาถึงผู้รับแล้ว เอ็นดีดี้ ทีซีพี ของผู้รับจะส่งเซ็กเมนท์ตอบกลับมา (อาจมีข้อมูลอยู่ในนี้ด้วยหรือไม่มีเลยก็ได้) พร้อมทั้งหมายเลขลำดับของเซ็กเมนท์ตัวต่อไปที่รอคอย ถ้าหมดระยะรอคอยก่อนที่เซ็กเมนท์ตอบรับจะเดินทางมาถึง ผู้ส่งก็จะต้องส่งสำเนาเซ็กเมนท์เดินมายังผู้รับอีกครั้งหนึ่ง โปรโตคอลนี้แม้ว่าจะทำงานอย่างตรงไปตรงมาแต่ปัญหาหลายอย่าง เช่น เซ็กเมนท์นั้นเดินทางมาถึงผู้รับในลำดับที่ไม่ถูกต้อง เช่น ไบต์ที่ 1,024-2,047 เดินทางมาถึงก่อนไบต์ที่ 0-1,023 เซ็กเมนท์อาจเสียเวลาในการเดินทางนานกว่าปกติทำให้ผู้ส่งต้องส่งสำเนาเซ็กเมนท์เดินออกมา ซึ่งผู้รับอาจได้รับทั้งสองเซ็กเมนท์ ยิ่งไปกว่านั้นถ้าเซ็กเมนท์ตัวแรก (หรือตัวที่สองหรือทั้งสองตัว) ถูกแบ่งออกเป็นเซ็กเมนท์ย่อยๆ เมื่อเซ็กเมนท์ทั้งหมดเดินทางมาถึงผู้รับก็จะทำให้ผู้รับต้องทำงานหนักกว่าเดิมในการรวบรวมเซ็กเมนท์ย่อยเข้ากลุ่มให้ถูกต้องและจะต้องทราบว่าข้อมูลทั้งสองชุดนั้นคือข้อมูลเดียวกัน โปรโตคอลเอ็นดีดี้ ทีซีพี จะต้องเตรียมพร้อมในการแก้ปัญหาเหล่านี้ให้ได้อย่างมีประสิทธิภาพกรรมวิธีหลายอย่างได้ถูกพัฒนาขึ้นมาเพื่อวัตถุประสงค์นี้โดยเฉพาะดังเช่นที่จะกล่าวถึงต่อไป

2.7.3 ข้อมูลส่วนหัวของ ทีซีพี เซ็กเมนต์

รูปที่ 2.27 แสดงโครงสร้างของ ทีซีพี เซ็กเมนท์ เขตข้อมูลส่วนแรกของแต่ละเซ็กเมนท์เป็นข้อมูลส่วนหัว (header) ที่มีขนาดคงที่จำนวน 20 ไบต์ ซึ่งอาจตามด้วยข้อมูลตัวเลือกอีกจำนวนหนึ่ง ที่เหลือจะเป็นส่วนของข้อมูลที่ต้องการส่งไปยังผู้รับมีขนาดไม่เกิน 65,495 ไบต์ (เป็นข้อมูลของไอพี 20 ไบต์ และของ ทีซีพี อีก 20 ไบต์) เซ็กเมนท์ที่ไม่มีข้อมูลถูกใช้เป็นข้อมูลสำหรับการตอบรับ (acknowledgement) หรือ ข้อมูลสำหรับการควบคุม รายละเอียดของขอบเขตข้อมูลต่างๆ มี

ดังนี้ Source port และ Destination port ใช้ในการระบุหมายเลขพอร์ตที่อยู่ทางด้านปลายทั้งสองข้างของสายสื่อสาร(พอร์ตของผู้ส่งและพอร์ตของผู้รับ) โฮสต์แต่ละตัวจะเป็นผู้กำหนดหมายเลขพอร์ตที่จะใช้ซึ่งจะเป็นหมายเลขระหว่าง 256 และ 65,535 หมายเลขพอร์ต (16 บิท) เมื่อรวมเข้ากับหมายเลข IP (32 บิท) จะกลายเป็นหมายเลข TSAP หรือหมายเลขซ็อคเก็ตซึ่งจะใช้เป็นหมายเลขที่อยู่ของผู้ส่งและผู้รับข้อมูลของการเชื่อมต่อนั้น เขตข้อมูล Sequence number และ Acknowledgement number คือหมายเลขลำดับของแพ็กเกตและหมายเลขการตอบรับซึ่งจะเป็นหมายเลขแพ็กเกตในลำดับต่อไปที่ผู้รับกำลังรอคอยทั้งสองหมายเลขที่ขนาด 32 บิทและถูกควบคุมโดย ทีซีพี

เขตข้อมูล ทีซีพี header length บอกจำนวนข้อมูลควบคุมสำหรับแพ็กเกตซึ่งข้อมูลแต่ละตัวมีขนาด 32 บิทเท่ากันทั้งหมด ทั้งนี้จะใช้เป็นตัวบอกขนาดของข้อมูลตัวเลือก (option) ที่มีขนาดไม่คงที่ ตัวเลขนี้ยังใช้ในการคำนวณหาจุดเริ่มต้นของข้อมูลจริงด้วย



รูปที่ 2.27 ข้อมูลส่วนหัวของแพ็กเกตทีซีพี

ส่วนต่อไปเป็นเขตข้อมูลขนาด 6 บิท ซึ่งไม่ได้ใช้งานอะไร ตามด้วยบิทสัญญาณขนาด 1 บิท จำนวน 6 ชนิด บิท URG (Urgent) ใช้บอกความหมายว่าเป็นข้อมูลด่วน (ดังที่ได้กล่าวไปแล้ว) เมื่อถูกกำหนดค่าให้เป็น "1" เอ็นติตี้ ทีซีพี ของผู้รับจะทราบว่ามีข้อมูลพิเศษติดมาด้วย (ดู Urgent pointer ประกอบ) กระบวนการนี้เทียบเท่าได้กับการใช้อินเตอร์รัพต์ในระบบปฏิบัติการทั่วไป

บิท ACK (Acknowledgement) จะถูกกำหนดให้เป็น "1" เพื่อบอกให้ทราบว่าหมายเลขลำดับการตอบรับ (Acknowledgement number) ซึ่งเป็นหมายเลขแพ็กเกตในลำดับต่อไปที่ผู้รับกำลังรอคอยนั้นถูกต้อง แต่ถ้าเป็น "0" ก็ไม่ต้องสนใจหมายเลขนั้น

บิท PSH (Push) บอกให้เอ็นติตี้ ทีซีพี ผู้ส่งทำการส่งข้อมูลนั้นออกไปในทันที ส่วนทางด้านผู้รับก็จะบังคับให้จัดการส่งข้อมูลนั้นไปยังโปรเซสที่กำลังรออยู่ในทันทีเช่นกัน

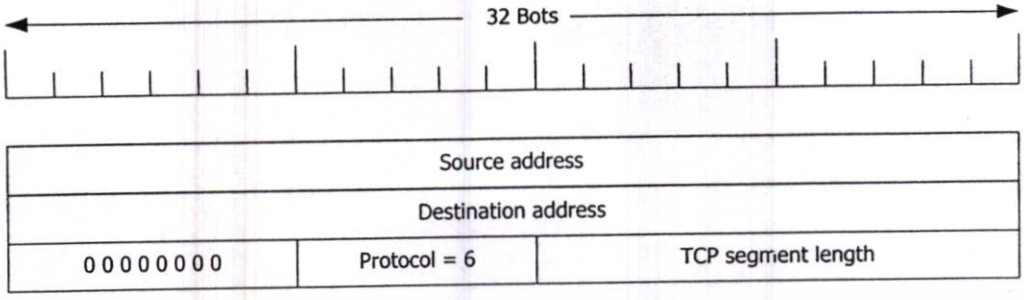
บิท RST (Reset) ใช้ในกรณีที่สื่อสารในการเชื่อมต่อนั้นเกิดความสับสนด้วยเหตุผลต่างๆ กัน เช่น โฮสต์เกิดทำงานล้มเหลว จึงต้องการให้ผู้รับยกเลิกการทำงานต่างๆ ที่ค้างอยู่แล้วเริ่มต้นกันใหม่ นอกจากนี้ยังนำไปใช้ในการปฏิเสธการเชื่อมต่อ หรือการปฏิเสธเซ็กเมนท์ที่ส่งมาซึ่งอาจจะมีข้อผิดพลาดในข้อมูลติดมาด้วย โดยทั่วไปแล้วถ้าผู้รับพบว่าบิทนี้ถูกกำหนดค่าเป็น "1" แสดงว่าได้เกิดปัญหาในการเชื่อมต่อขึ้นแล้ว

บิท SYN (Synchronous) ใช้สำหนับเริ่มต้นการเชื่อมต่อการสื่อสารซึ่งโดยปกติจะกำหนดค่าให้ SYN = 1 และ ACK = 0 ถ้าการเชื่อมต่อเรียบร้อย ผู้รับจะตอบกลับมาด้วย SYN = 1 และ ACK = 1 ซึ่งเป็นค่าที่แทนความหมาย CONNECTION REQUEST และ CONNECTION ACCEPTED นั่นเอง

บิทสุดท้ายในกลุ่มนี้คือ บิท FIN (Finish) ใช้สำหรับการยกเลิกการเชื่อมต่อเมื่อผู้ส่งไม่ต้องการส่งข้อมูลใดๆ อีกแล้ว อย่างไรก็ตาม โปรโตคอลนี้มีการทำงานแบบสมมาตร (symmetric) ดังนั้นทางฝ่ายผู้รับจะยังสามารถส่งข้อมูลกลับมายังผู้ส่งได้ต่อไปตามที่ต้องการ ทั้ง SYN และ FIN เซ็กเมนท์มีหมายเลขลำดับของตนเอง ดังนั้นจึงรับประกันได้ว่าจะทำงานตามลำดับได้อย่างถูกต้อง

การควบคุมการไหลของข้อมูลในโปรโตคอล ทีซีพี ใช้วิธีการแบบหน้าต่างเลื่อนไหล เขตข้อมูล window size บอกขนาดของข้อมูลที่อนุญาตให้ส่งได้ (มีหน่วยเป็นไบต์) ซึ่งข้อมูลจะอยู่ในลำดับที่ต่อจากเซ็กเมนท์ล่าสุดที่ส่งออกมา ค่าของ window size = 0 บอกให้ทราบว่าเซ็กเมนท์ทั้งหมดที่ส่งมานับจนถึงหมายเลขลำดับที่ "acknowledgement number – 1" นั้นผู้รับได้รับถูกต้องแต่ขอให้ผู้ส่งหยุดพักการส่งข่าวชั่วคราว เมื่อผู้รับพร้อมที่จะทำงานต่อไปก็จะส่งเซ็กเมนท์ใหม่ที่มีค่า acknowledgement number เท่าเดิมแต่กำหนดค่า window size เป็นค่ามากกว่า 0

เขตข้อมูล Checksum เป็นข้อมูลที่ช่วยในการตรวจสอบความถูกต้องของข้อมูล รูปที่ 2.27 แสดงโครงสร้างข้อมูลส่วนหัวจำลอง (pseudoheader) กระบวนการตรวจสอบเริ่มต้นด้วยการกำหนดให้ค่าของทุกบิทใน Checksum เป็น 0 ทั้งหมดและไม่นำส่วนของข้อมูลจริงมาร่วมพิจารณา ถ้าจำนวนไบต์รวมที่เหลืออยู่เป็นเลขจำนวนคี่ก็ให้เติมไบต์ 0 เข้าไป จากนั้นจึงบวกเลขทั้งหมดเข้าด้วยกัน (จำนวนละ 16 บิท) ด้วยวิธีการแบบ 1's complement ร่วมกับค่า Checksum ที่ได้รับมา ถ้าผลลัพธ์ที่เกิดขึ้นมีค่าเป็น 0 แสดงว่าข้อมูลในเซ็กเมนท์นั้นถูกต้อง ข้อมูลส่วนหัวจำลองประกอบด้วยหมายเลขไอพี ขนาด 32 บิทของผู้ส่งและผู้รับข้อมูล หมายเลขโปรโตคอล ทีซีพี ที่ใช้ (6 บิท) และขนาดของเซ็กเมนท์ (รวมทั้งข้อมูลส่วนหัวด้วย) กระบวนการนี้ แม้ว่าจะช่วยตรวจสอบความถูก



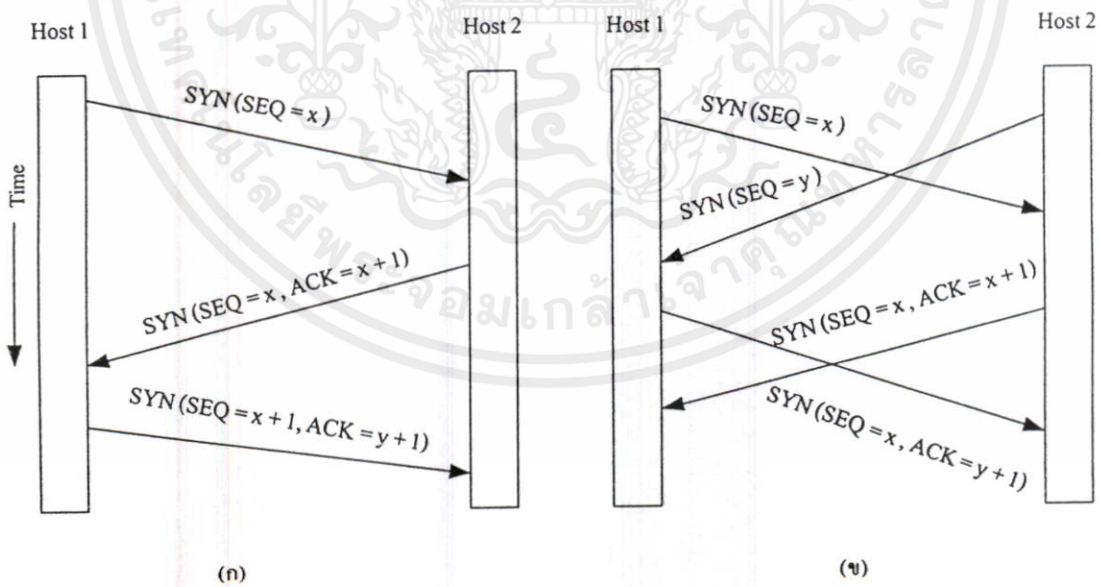
รูปที่ 2.28 ข้อมูลส่วนหัว

ต้องของข้อมูลแต่ก็ได้ละเมิดกฎความเป็นอิสระต่อกันระหว่างชั้นสื่อสาร เนื่องจากหมายเลขไอพีนั้น เป็นข้อมูลที่ใช้ในชั้นสื่อสารควบคุมไอพี (IP layer) แต่กระบวนการนี้เกิดขึ้นในชั้นสื่อสารควบคุม ทีซีพี เขตข้อมูล Option เตรียมไว้สำหรับการให้บริการพิเศษนอกเหนือไปจากที่มีอยู่ เช่น การนำไปใช้ในการบอกขนาดของข้อมูลจริงในแต่ละเซ็กเมนท์ที่ผู้รับ / ผู้ส่งต้องการ เซ็กเมนท์ขนาดใหญ่มีประสิทธิภาพการใช้งานสูงกว่าการใช้เซ็กเมนท์ขนาดเล็ก แต่โฮสต์ที่ใช้เครื่องคอมพิวเตอร์ขนาดเล็กอาจไม่สามารถจัดการข้อมูลในเซ็กเมนท์ขนาดใหญ่ได้ ดังนั้นในระหว่างการสร้างการเชื่อมต่อ ทั้งผู้ส่งและผู้รับจะประกาศขนาดของข้อมูลที่ตนเองต้องการและขนาดข้อมูลที่เล็กกว่าจะถูกนำมาใช้ ในกรณีที่ไม่มีผู้ใดแสดงขนาดที่ตนเองต้องการก็จะใช้มาตรฐาน 536 ไบต์แทน ดังนั้นโฮสต์ทุกตัวในระบบอินเทอร์เน็ตจะต้องยอมรับ ทีซีพี เซ็กเมนท์ขนาด 536+20 = 556 ไบต์ สำหรับการเชื่อมต่อผ่านสื่อสารที่มีความกว้างมาก (wide bandwidth) มีระยะเวลาการรอคอย (high delay) หรือทั้งสองอย่าง การใช้เซ็กเมนท์ขนาด 64 Kbytes ในการสื่อสารนั้นมักจะมีปัญหามาก สายสื่อสาร T3 (ความเร็ว 44.736 เมกะบิทต่อวินาที) ใช้เวลาส่งข้อมูลทั้ง 64 Kbytes ได้ใน 12 มิลลิวินาที ถ้ากำหนดให้เวลาการเดินทางข้อมูลครบหนึ่งรอบเป็น 50 มิลลิวินาที (ระยะประมาณ 4,800 กิโลเมตร บนสายใยแก้ว) แล้ว ผู้ส่งจะต้องรอ (idle) เป็นระยะเวลาประมาณ 3 ใน 4 ของเวลาสื่อสารทั้งหมดเลยทีเดียว ถ้าเป็นการสื่อสารผ่านดาวเทียมก็ยิ่งทำให้ระยะเวลาในการรอคอยนานกว่ามาก การกำหนดขนาดข้อมูลผ่าน window size ขนาด 16 ขนาด 16 บิทนี้เป็นตัวบังคับให้เซ็กเมนท์มีขนาดไม่เกิน 64 Kbytes ซึ่งถ้าสามารถกำหนดขนาดให้มากกว่านี้แล้ว ผู้ส่งก็จะสามารถส่งข้อมูลได้มากขึ้นแต่เสียเวลาการรอคอยเท่าเดิม จึงเป็นการเพิ่มประสิทธิภาพการทำงานให้สูงขึ้น มาตรฐาน RFC 1323 ได้กำหนดทางเลือก window scale ขึ้นมาใช้งานเพื่อยอมให้ผู้ส่งและผู้รับสามารถต่อรองการกำหนดขนาดเซ็กเมนท์ในระบบอัตราส่วนโดยการสลับเลื่อน window size จาก 16 บิทกลายเป็น 32 บิท นั่นคือขนาดของเซ็กเมนท์จะเพิ่มเป็น 2^{32} ไบต์ หรือเท่ากับ 4 พันล้านไบต์ โปรโตคอลทีซีพี ที่มีใช้ในปัจจุบันส่วนใหญ่จะสนับสนุนทางเลือกนี้ ทางเลือกอีกทางหนึ่งในมาตรฐาน RFC 1106 กำหนดให้ส่งข้อมูซ้ำแบบเฉพาะส่วน (ที่เสียหายในระหว่างการนำส่ง)

แทนที่จะเป็นแบบการส่งซ้ำเป็นบล็อก (go back "n" protocol) ถ้าผู้รับได้รับเซ็กเมนท์หนึ่งที่ไม่สมบูรณ์ตามด้วยเซ็กเมนท์อีกจำนวนหนึ่งที่สมบูรณ์ โปรโตคอลทีซีพี แบบเดิมจะบังคับให้ผู้ส่งจัดการส่งเซ็กเมนท์ทั้งหมดมาใหม่โดยเริ่มต้นจากเซ็กเมนท์ที่ไม่ได้รับการตอบรับ (คือเซ็กเมนท์ที่เสีย) ซึ่งรวมทั้งเซ็กเมนท์ในลำดับต่อๆ มาที่รับได้อย่างสมบูรณ์ด้วย มาตรฐาน RFC 1106 ได้เพิ่มข้อมูล NAK เพื่อเปิดโอกาสให้ผู้รับแจ้งให้ผู้ส่งจัดการส่งเฉพาะเซ็กเมนต์ที่เสียหายมาใหม่เท่านั้น

2.7.4 การบริการเชื่อมต่อโดยทีซีพีเอ็นติตี้

การสร้างการเชื่อมต่อในระบบโปรโตคอลทีซีพี ใช้กระบวนการจับมือร่วมสามขั้นตอน (three-way handshake) โดยทางผู้รับซึ่งปกติแล้วจะเป็นผู้ให้บริการ (sever) จะเรียกใช้บริการ LISTEN เพื่อรอคอยสัญญาณ CONNECT จากผู้ส่งซึ่งโดยปกติจะเป็นผู้ใช้บริการ (client) ข้อมูลหลักที่ส่งมาด้วยคือ หมายเลข IP และพอร์ตที่ใช้ ขนาดสูงสุดของเซ็กเมนท์ และอาจมีข้อมูลเกี่ยวข้องทางด้านบริหาร (ชื่อบัญชีและรหัสผ่าน) ได้ และจบลงด้วยการเรียกใช้บริการ ACCEPT เพื่อยืนยันการเชื่อมต่อกลับไป เมื่อเซ็กเมนท์ CONNECT (SYN = "1" และ ACK = "0") เดินทางมาถึงเอ็นติตี้ ทีซีพี ที่โฮสต์ปลายทางจะค้นหาโปรเซสตามหมายเลขพอร์ตที่กำหนดในเขตข้อมูล Destination port ซึ่งถ้าหาไม่พบก็จะตอบปฏิเสธด้วยเซ็กเมนท์ที่มี RST = "1" กลับไปยังผู้ส่ง



รูปที่ 2.29 (ก) การเชื่อมต่อผ่านทีซีพีในสภาวะปกติ (ข) เกิดการเรียกซ้อนกัน

เซ็กเมนท์ CONNECT ของผู้ส่งจะถูกส่งต่อไปยังโปรเซสตามพอร์ตที่ระบุ ซึ่งอาจจะตอบรับหรือปฏิเสธก็ได้ ถ้าโปรเซสนั้นต้องการสื่อสารด้วยก็จะส่งเซ็กเมนท์ตอบรับกลับไป รูปที่ 2.29 (ก) แสดงลำดับขั้นตอนการส่ง ทีซีพี เซ็กเมนท์ในการสร้างการเชื่อมต่อในสภาวะปกติระหว่างผู้ส่งและ

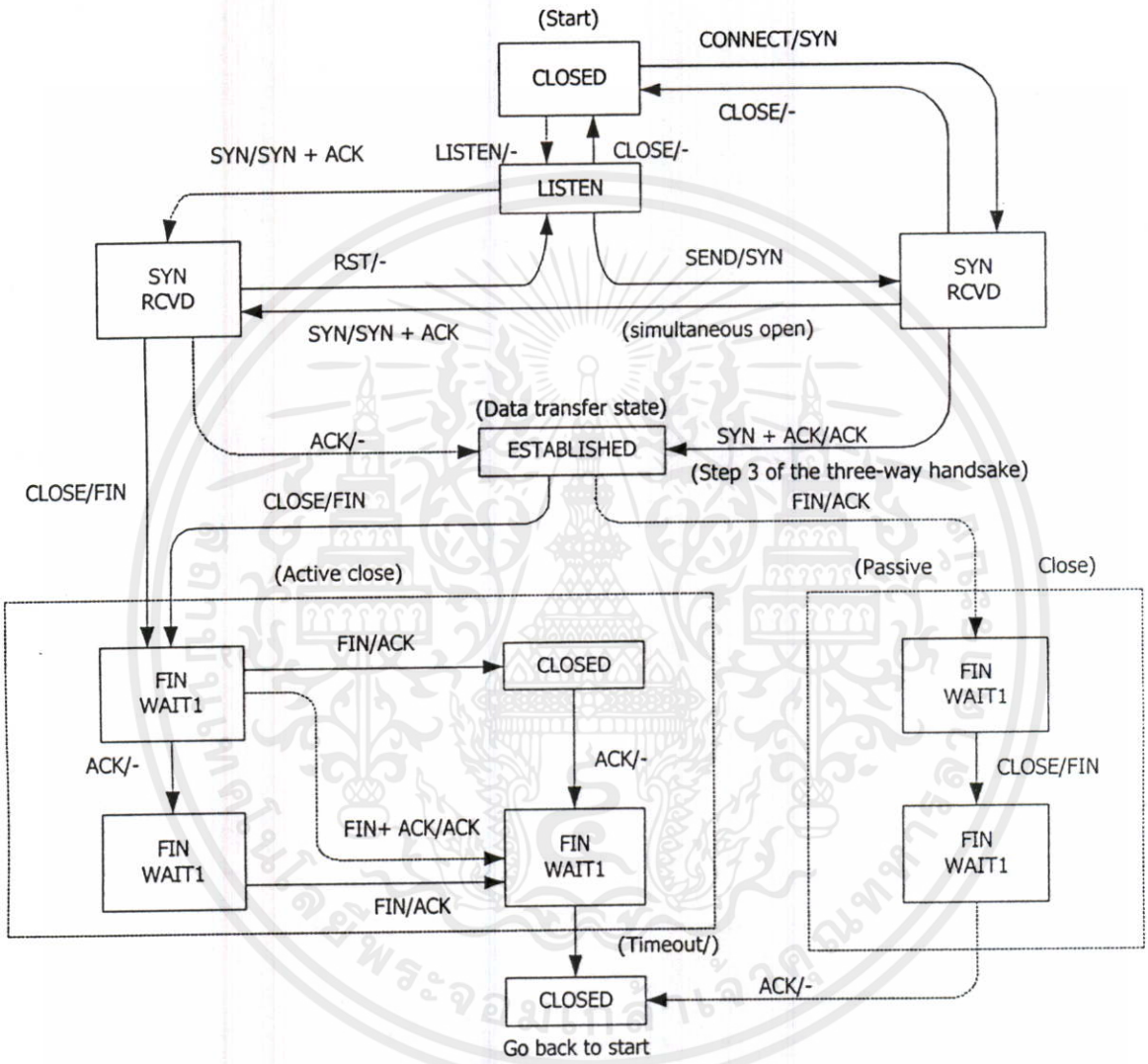
ผู้รับ ในกรณีที่โฮสต์สองแห่งพยายามสร้างการเชื่อมต่อระหว่างซ็อกเก็ตคู่เดียวกันจะเกิดเป็นลำดับขั้นตอนดังแสดงในรูปที่ 2.29 (ข) ผลสุดท้ายจะมีการเชื่อมต่อเกิดขึ้นเพียงหนึ่งช่องทางเท่านั้นเนื่องจากการเชื่อมต่อในแต่ละช่องทางจะถูกกำหนดขึ้นโดยใช้หมายเลขซ็อกเก็ตผู้ส่งและผู้รับ ถ้าการเชื่อมต่อลำดับแรกสำเร็จก็จะถูกบันทึกไว้ในตารางการสื่อสาร เช่น (x,y) ถ้าการเชื่อมต่อลำดับที่สองสำเร็จในเวลาต่อมา ข้อมูลนี้จะถูกบันทึกไว้ที่เดียวกันคือ (x,y) แม้ว่าการเชื่อมต่อในระบบ ทีซีพี จะเป็นการสื่อสารสองทางแบบสมบูรณ์ แต่การอธิบายวิธีการยกเลิกการเชื่อมต่อจะง่ายกว่าเมื่อคิดว่าเป็นการสื่อสารแบบทางเดียวจำนวนสองช่อง (ช่องขาไปและช่องขากลับ) การยกเลิกจะเกิดขึ้นในแต่ละช่องทางซึ่งจะไม่เกี่ยวข้องกันโดยตรง ผู้ที่ต้องการยกเลิก (อาจเป็นผู้รับหรือผู้ส่งก็ได้) จะส่งทีซีพีเซ็กเมนท์ที่มีค่าบิท FIN = "1" มายังอีกฝ่ายหนึ่ง เมื่อได้รับการตอบรับก็แสดงว่าการเชื่อมต่อช่องนั้นได้ถูกยกเลิกไปแล้ว ซึ่งช่องเชื่อมต่ออีกช่องหนึ่งจะยังคงใช้งานต่อไปได้นานเท่าที่ต้องการ เมื่อการเชื่อมต่อช่องที่สองถูกยกเลิกจะทำให้การเชื่อมต่อระหว่างคู่สื่อสารนั้นถูกยกเลิกไปด้วย จำนวนเซ็กเมนท์ที่ใช้ในการนี้จึงมี 4 เซ็กเมนท์ หรืออาจลดลงเหลือเพียง 3 ถ้าการขอยกเลิกของอีกช่องทางหนึ่งถูกส่งมาพร้อมกับการตอบรับการยกเลิกของช่องทางแรก ถ้าการยกเลิกเกิดขึ้นพร้อมกันทั้งสองช่องทางก็จะมีผลเหมือนกับการยกเลิกทีละช่องทาง เพื่อหลีกเลี่ยงปัญหากองกำลังสองส่วน (two-army problem) จึงกำหนดให้มีการจับเวลาในระหว่างการขอยกเลิกช่องสัญญาณ ถ้าฝ่ายหนึ่งได้ส่งเซ็กเมนท์ขอยกเลิกการใช้ช่องสัญญาณไปแล้วและไม่มีการตอบรับภายในระยะเวลาสองเท่าของอายุแพ็กเกต (packet lifetime) ก็ให้ถือว่าช่องสัญญาณนั้นถูกยกเลิกโดยอัตโนมัติ ในเวลาต่อมาอีกฝ่ายหนึ่งก็จะพบว่าไม่มีการสื่อสารเกิดขึ้นเลยก็จะยกเลิกการสื่อสารบ้าง ท้ายที่สุดช่องทางการเชื่อมต่อนั้นก็จะถูก (บังคับใช้) ยกเลิกโดยสมบูรณ์ แม้ว่ากระบวนการนี้จะไม่สมบูรณ์เท่าที่ควรแต่ยังไม่มีผู้ใดคิดกระบวนการที่สมบูรณ์ได้ จึงถือว่ายอมรับได้ ในความเป็นจริงแล้วปัญหาเกิดขึ้นน้อยมาก ขั้นตอนในการสร้างการเชื่อมต่อและการยกเลิกสามารถเขียนอธิบายด้วยไฟไนส์สเตทแมชชีนที่มีการทำงาน 11 สถานะดังแสดงในตารางที่ 2.2 ในแต่ละสถานะจะมีเหตุการณ์บางอย่างที่เป็นไปได้ซึ่งจะได้รับการตอบสนองด้วยการกระทำที่เหมาะสม ในทางตรงข้ามเหตุการณ์ที่เป็นไปไม่ได้จะกลายเป็นข้อผิดพลาดที่จะต้องรายงานให้ทราบ การเชื่อมต่อเริ่มต้นจากสถานะ CLOSED เมื่อเรียกใช้บริการ LISTEN หรือ CONNECT ก็จะเปลี่ยนสถานะไปจากเดิม ถ้าอีกฝ่ายหนึ่งเรียกใช้บริการตรงกันข้ามการเชื่อมต่อก็จะเกิดขึ้นและจะย้ายไปอยู่ในสถานะ ESTABLISHED เมื่อยกเลิกการติดต่อก็จะกลับไปอยู่ในสถานะ CLOSED อย่างเดิม รูปที่ 2.30 แสดงภาพของไฟไนท์สเตทแมชชีนในการติดต่อสื่อสาร โดยทั่วไปจะเกิดขึ้นระหว่างผู้ใช้ติดต่อกับผู้ให้บริการ ซึ่งเขียนแทนด้วยเส้นทึบหนาสำหรับผู้ใช้และเส้นไข่ปลาสำหรับผู้ให้บริการส่วนเส้นบางเป็นเหตุการณ์ไม่ปกติที่อาจเกิดขึ้น เส้นทุกชนิดจะถูกกำกับไว้ด้วย "เหตุการณ์ / การกระทำ (event / action pair)" เหตุการณ์อาจเกิดขึ้นเนื่องจากผู้ใช้เป็นผู้ทำให้เกิดขึ้น (เรียกใช้บริการ CONNECT LISTEN SEND หรือ CLOSE) เกิดจากเซ็กเมนท์เดินทางมาถึงโฮสต์ (SYN FIN

ตารางที่ 2.2 สถานะการทำงานที่เกิดขึ้นในการเชื่อมต่อผ่านทีซีพี

State	Description
CLOSED	ไม่มีการเชื่อมต่อเกิดขึ้น
LISTEN	ผู้รับพร้อม และกำลังรอคอยการเชื่อมต่อ
SYN RCVD	คำร้องขอการเชื่อมต่อมาถึงแล้ว กำลังรอการตอบรับ
SYN SENT	โปรเซสผู้ใช้ได้เริ่มดำเนินการเชื่อมต่อ
ESTABLISHED	การเชื่อมต่อสมบูรณ์
FIN WAIT 1	ผู้ส่งได้ขอยกเลิกการเชื่อมต่อ
FIN WAIT 2	ผู้รับยืนยันการยกเลิกการเชื่อมต่อ
TIME WAIT	(หลังจากเกิดข้อผิดพลาด) รอให้หมดระยะเวลารอคอย
CLOSING	ผู้รับและผู้ส่งกำลังขอยกเลิกการเชื่อมต่อ
CLOSE WAIT	อีกฝ่ายหนึ่งได้ขอยกเลิกการเชื่อมต่อ
LAST ACK	รอให้แพ็กเกตที่ส่งออกไปแล้ว ไปถึงผู้รับหรือหมดอายุ

ACK หรือ RST) หรือเกิดจากการสิ้นระยะการรอคอย ในส่วนของการกระทำจะเป็นการส่งเซ็กเมนท์สำหรับการควบคุม (SYN , FIN หรือ RST) หรือไม่มีการกระทำใดๆ (ใช้สัญลักษณ์ "-") ส่วนข้อความที่ปรากฏในวงเล็บคือคำอธิบายจากรูปดังกล่าวให้ดูกระบวนการทำงานที่เกิดขึ้นโดยเริ่มต้นจากเส้นทางของผู้ใช้บริการ (ผู้ส่ง) ซึ่งเขียนแทนเส้นทึบหนา จากนั้นจึงพิจารณาเส้นทางการทำงานของผู้ให้บริการ (ผู้รับ) ตามเส้นประ /หนา เมื่อผู้ใช้บริการส่งคำสั่ง CONNECT มาถึง เอ็นติตี้ ทีซีพี ทางด้านผู้ให้บริการ (ผู้รับ) จะสร้างระเบียนเก็บข้อมูล (connection record) สำหรับการเชื่อมต่อขึ้นมารองรับซึ่งจะมีสถานะเป็น "SYN SENT" แล้วจึงส่งเซ็กเมนท์ SYN ตอบกลับไป ในเวลาเดียวกันนี้ ทางด้านผู้ให้บริการ หรือผู้รับอาจกำลังให้บริการเชื่อมต่อหรือกำลังเริ่มการติดต่อกับโฮสต์อื่นๆ อยู่ด้วย ดังนั้นระเบียนเก็บข้อมูลการเชื่อมต่อจึงถูกสร้างขึ้นสำหรับการเชื่อมต่อแต่ละช่องทางโดยเฉพาะ เมื่อเซ็กเมนท์ SYN + ACK เดินทางมาถึงผู้รับจะทำการส่งเซ็กเมนท์ ACK กลับไปอีกครั้งหนึ่งเพื่อให้กระบวนการจับมือร่วมสามขั้นตอนเสร็จสมบูรณ์ สถานะของสื่อสารนั้นก็จะกลายเป็น "ESTABLISH" การรับ-ส่งข้อมูลจึงเกิดขึ้นได้ เมื่อโปรเซสผู้ใช้ต้องการยกเลิกการเชื่อมต่อก็จะเรียกใช้บริการ CLOSE ซึ่งจะบังคับให้เอ็นติตี้ ทีซีพี ของตนเองส่งเซ็กเมนท์ FIN มายังผู้ให้บริการและรอคอยการตอบรับ (ในรูป ใช้เส้นประล้อมเป็นกรอบสี่เหลี่ยมไว้) โดยมีสถานะเป็น "FIN WAIT 1" เมื่อการตอบรับมาถึง สถานะของผู้ใช้จะเปลี่ยนเป็น "FIN WAIT 2" ช่องทางสื่อสารจากผู้ใช้ไปยังผู้ให้บริการก็จะถูกปิดลง เมื่อผู้ให้บริการยกเลิกการเชื่อมต่อบ้างก็จะเกิดกระบวน

การแบบเดียวกัน ในขณะนี้ช่องสื่อสารระหว่างคู่นี้ได้ถูกปิดแล้วแต่เอ็นติตี้ ทีซีพี ของทั้งคู่ยังคงอยู่ในสถานะ "LAST ACK" เมื่อสิ้นสุดระยะเวลารอคอยนี้แลเวการเชื่อมต่อก็ถูกยกเลิกโดยสมบูรณ์และระเบียนเก็บข้อมูลการเชื่อมต่อของคู่นี้จะถูกลบทิ้ง

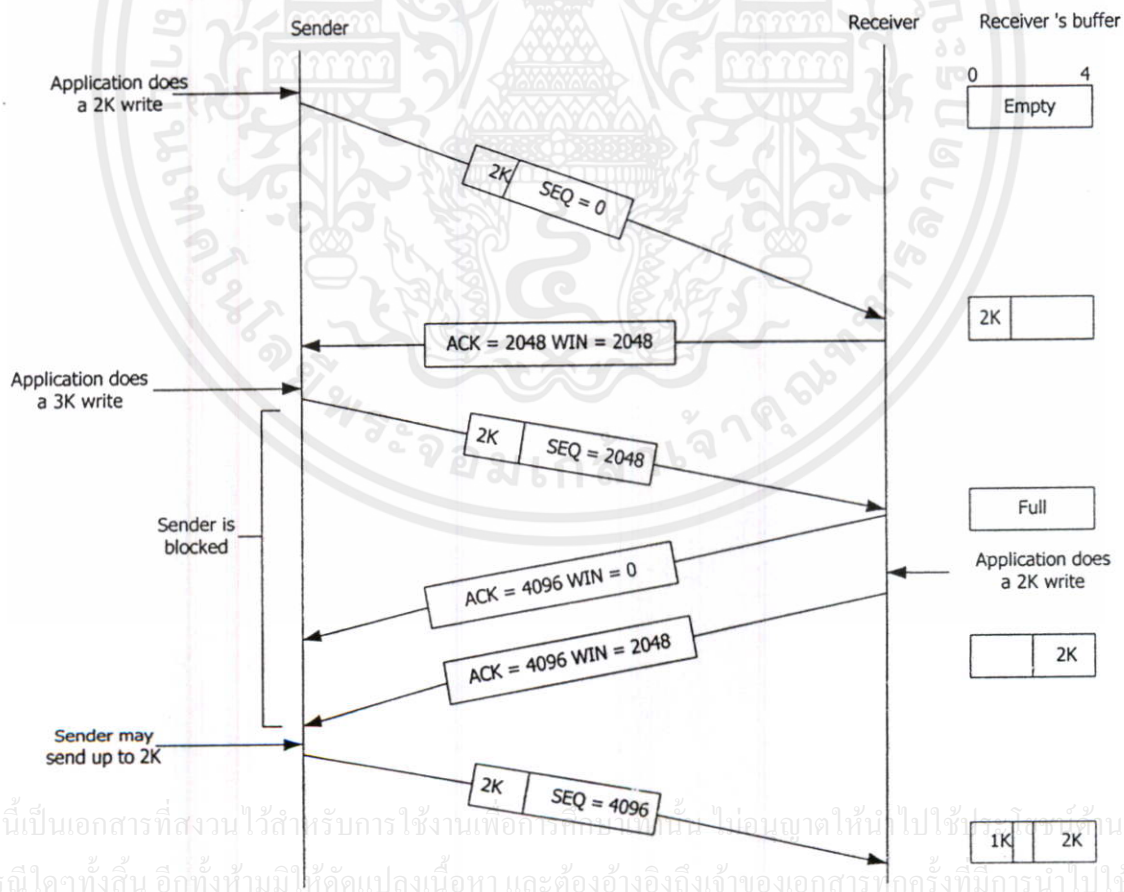


รูปที่ 2.30 ไฟไนท์สเตทแมชชีนแสดงการเชื่อมต่อในระบบ ทีซีพี

ต่อไปมาดูกระบวนการทำงานโดยเริ่มต้นจากฝ่ายผู้ให้บริการบ้าง ในสภาวะปกติผู้ให้บริการซึ่งเป็นผู้รับข้อมูลจะใช้บริการ LISTEN และหยุดการทำงานเพื่อรอคอยการเรียกจากผู้ใช้บริการ เมื่อเซ็กเมนท์ SYN มาถึง ผู้ให้บริการจะส่งแพ็กเกตตอบรับและเปลี่ยนสถานะไปเป็น "SYN RCVD" การเชื่อมต่อจะสมบูรณ์หลังจากที่ผู้ให้บริการได้รับแพ็กเกตตอบรับกลับมาอีกครั้งหนึ่งตามข้อบังคับของกระบวนกรจับมือร่วมขั้นตอนแล้วเปลี่ยนสถานะไปเป็น "ESTABLISHED"

2.7.5 วิถีทางการส่งผ่านข้อมูล

วิธีควบคุมการส่งข้อมูลในโปรโตคอลทีซีพี ไม่ได้ผูกติดอยู่กับแพ็กเกตตอบรับอย่างที่เกิดขึ้นในโปรโตคอลสื่อสารชั้นเชื่อมต่อข้อมูล (data link layer) สมมติว่าผู้รับมีบัฟเฟอร์ขนาด 4,096 ไบต์ดังแสดงในรูปที่ 2.32 ผู้ส่งจัดการส่งเซ็กเมนท์ขนาด 2,048 ไบต์มาถึงอย่างสมบูรณ์ซึ่งผู้รับก็จะส่งเซ็กเมนท์ตอบรับกลับไป อย่างไรก็ตาม ข้อมูลที่รับเข้ามานั้นทำให้ขนาดบัฟเฟอร์ลดลงไปครึ่งหนึ่ง ผู้รับจึงบอกไปยังผู้ส่งว่าขนาดของเซ็กเมนท์ในลำดับต่อไปจะมีขนาดเพียง 2,048 ไบต์เท่านั้น ต่อมาผู้ส่งจัดการส่งเซ็กเมนท์ขนาด 2,048 ไบต์มายังผู้รับซึ่งก็ได้รับการตอบรับเรียบร้อย แต่ในครั้งนี้ผู้รับแจ้งว่าขนาดเซ็กเมนท์ต่อไปเป็น 0 ไบต์ทำให้ผู้ส่งต้องหยุดส่งข้อมูลทันทีเพื่อรอให้โปรเซสทางด้านผู้รับจัดการนำข้อมูลออกไปจากบัฟเฟอร์เสียก่อน ในขณะที่ผู้รับระบุขนาดเซ็กเมนท์เป็น 0 ไบต์นั้น ผู้ส่งจะไม่สามารถส่งข้อมูลออกมาได้ นอกจากข้อยกเว้น 2 กรณี กรณีแรก ข้อมูลเร่งด่วนอาจถูกส่งออกมาได้ เช่น โปรเซสผู้ส่งอาจส่งคำสั่งมาบังคับให้โปรเซสทางผู้รับเลิกทำงานทันที หรือกรณีที่สอง ส่งเซ็กเมนท์มากระตุ้นให้ทางผู้รับส่งข้อมูลขนาดของเซ็กเมนท์ไปใหม่ (อาจจะมีเนื้อที่ว่างในบัฟเฟอร์บ้างแล้ว) ข้อยกเว้นนี้ใช้ในการป้องกันกรณีที่ข้อมูลนอกขนาดเซ็กเมนท์จากผู้รับเกิดสูญหายไปซึ่งจะทำให้ระบบเกิดสภาวะการรอคอยอย่างไม่มีที่สิ้นสุด

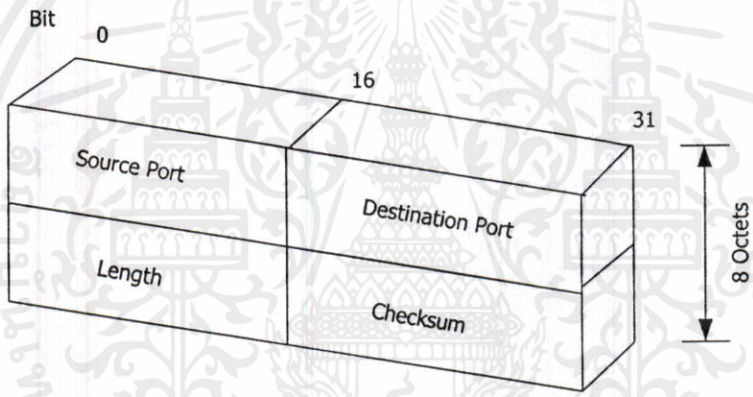


รูปที่ 2.31 การบริหารหน้าต่างสื่อสารในระบบ ทีซีพี

การทำงานโดยปกติผู้ส่งไม่ได้ถูกบังคับให้จัดการส่งข้อมูลที่โปรเซสของผู้ส่งใช้ส่งมาในทันทีในเวลาเดียวกันผู้รับก็ไม่จำเป็นจะต้องส่งเซ็กเมนท์ตอบรับในทันทีที่ได้รับเซ็กเมนท์ใหม่เข้ามา ดังเช่นในรูปที่ 2.31 เมื่อผู้รับรับข้อมูลเมื่อผู้รับนับข้อมูลขนาด 2 กิโลไบต์แรกเข้ามา (ในกรณีนี้) ผู้รับอาจเลือกที่จะไม่ส่งข้อมูลบอกขนาดเซ็กเมนท์ไปแล้วรอรับข่อมูลต่อไปจนบัฟเฟอร์เต็ม วิธีการนี้จะเปิดโอกาสให้ผู้ส่งสามารถส่งเซ็กเมนท์ขนาด 4 ไบต์มาได้ในทันทีที่ต้องการ ความคล่องตัวนี้ช่วยให้คู่สื่อสารสามารถปรับปรุงประสิทธิภาพการรับส่งข้อมูลให้เมาะสมต่อสภาพแวดล้อมของตนเองได้

2.8 โปรโตคอลยูดีพี (User datagram protocal, UPD)

โปรโตคอลยูดีพี จัดเป็นการเชื่อมต่อแบบไม่ต่อเนื่องสำหรับทำงานในระดับแอปพริเคชั่น ยูดีพี อยู่บนของไอแพ็กเก็ต



รูปที่ 2.32 แสดงยูดีพีเฮดเดอร์

ช่องเช็คซัม (checksum field) ถือว่าเป็นทางเลือก ถ้าไม่มีการตั้งค่าจะมีค่าเป็น 0 อย่างไรก็ตาม จะมีการใช้ไอพีเช็คซัมและประยุกต์ใช้งานที่ไอพีเฮดเดอร์เท่านั้น และไม่ใช้สำหรับการตรวจสอบความถูกต้องของช่องข้อมูล (data field) ซึ่งยูดีพีจะประกอบด้วย เฮดเดอร์และส่วนข้อมูลของผู้ใช้งาน (User data) ดังนั้นถ้าไม่มีการคำนวณเช็คซัมในโปรโตคอลยูดีพี จะไม่มีการตรวจสอบในข้อมูลของ ผู้ใช้งานเช่นเดียวกัน แสดงได้ดังรูปที่ 2.32

2.9 เน็ตเวิร์คซีเคียวริตี้ (Network Security)

องค์กรต่างๆ ต้องการให้ข้อมูลในองค์กรมีความปลอดภัยซึ่งความปลอดภัยของข้อมูล เป็นปัจจัยที่มีคุณค่ายิ่งสำหรับผู้บริหารและผู้ปฏิบัติการในช่วงเริ่มต้นของการใช้คอมพิวเตอร์ มีความต้องการสำหรับการปกป้องไฟล์และการจัดเก็บข้อมูล แต่ด้วยเทคโนโลยีเครือข่ายคอมพิวเตอร์ที่ก้าวหน้าทำให้ต้องทำงานร่วมกันเป็นเครือข่าย เพื่อจะได้แบ่งงานกันทำ เพื่อให้งานต่างๆ สามารถ

สำเร็จลุล่วงไปด้วยดี แต่ด้วยมีผู้มิหวังดีลักลอบข้อมูลเพื่อนำไปหาประโยชน์ใส่ตนมากกว่าองค์กร จึงทำให้ต้องมีการป้องกันเครือข่ายหรือเรียกอีกอย่างว่าเน็ตเวิร์คซีเคียวริตี้

2.9.1 องค์ประกอบหลักสำหรับความปลอดภัยของเครือข่าย

องค์ประกอบหลักที่ใช้ในพิจารณาความปลอดภัยเครือข่าย สามารถสรุปได้คือ

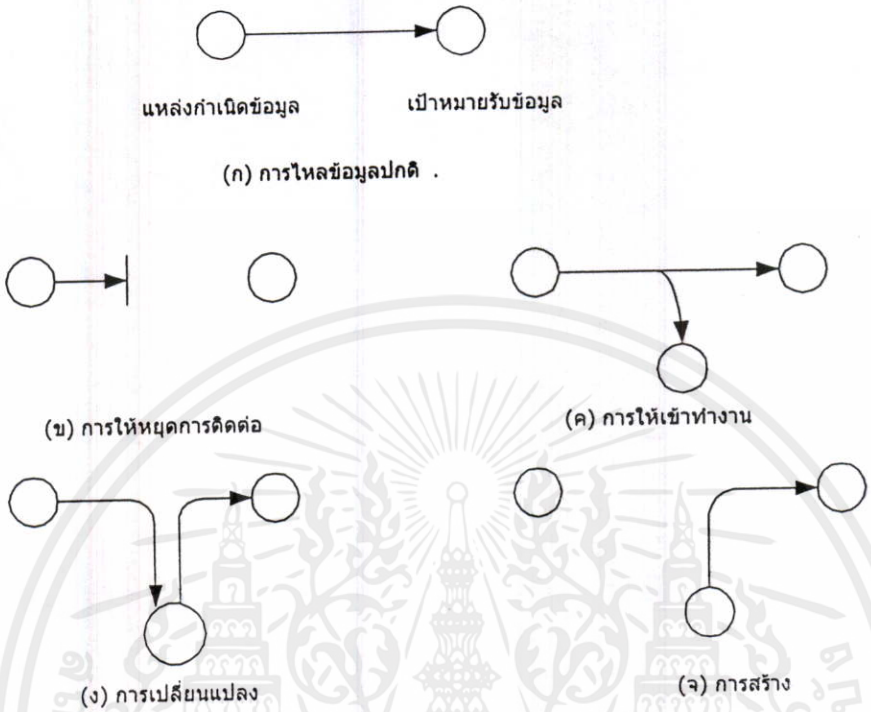
1. ความมั่นใจ (Confidentiality) ต้องการให้ข้อมูลในคอมพิวเตอร์และการจัดส่งข้อมูลสามารถเข้าไปดูได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น รวมถึงการแสดงให้เห็นบนหน้าจอ การพิมพ์รายงาน
2. การให้สิทธิ์ผู้ใช้งาน (Authentication) ต้องการให้มีการตรวจสอบสิทธิผู้ใช้งานได้อย่างถูกต้อง
3. ความมั่นใจ (Integrity) ต้องการให้ระบบคอมพิวเตอร์ และการส่งข้อมูลสามารถทำการปรับปรุงแก้ไขได้เฉพาะผู้มีสิทธิ์เท่านั้น รวมถึงการเขียน การเปลี่ยนแปลง การเปลี่ยนสถานะ การลบ การสร้างเพิ่มได้
4. การไม่ปฏิเสธ (Nonrepudiation) ต้องการให้ทั้งด้านรับและด้านส่ง ไม่สามารถปฏิเสธการรับส่งข่าวสารได้
5. การควบคุมการเข้าใช้งาน (Access Control) ต้องการในการเข้าถึงข้อมูลต่างๆ ถูกควบคุมด้วยระบบคอมพิวเตอร์
6. การใช้งานได้ง่าย (Availability) ต้องการให้ผู้มีสิทธิ์สามารถเข้าใช้งานระบบคอมพิวเตอร์ได้ตลอดเวลา

2.9.2 ประเภทของการโจมตี (Attack)

ในการลักลอบเข้าระบบเครือข่ายสามารถสรุปได้ 4 ประเภทวิธี คือ

1. การให้หยุดการติดต่อ (Interruption) คือการทำให้ระบบถูกทำลายหรือไม่สามารถใช้งานได้ ตัวอย่างเช่น การตัดสาย การสื่อสารคอมพิวเตอร์ ทำให้ไม่สามารถติดต่อกับข้อมูลได้
2. การให้เข้าทำงาน (Interception) คือผู้ไม่มีสิทธิ์สามารถเข้าระบบได้ เห็นว่าเป็นเรื่องของการขาดความมั่นใจระบบ (Confidentiality) ทำให้ผู้ไม่มีสิทธิ์เข้าทำงานกับระบบได้ โดยผู้เข้าสู่ระบบรวมถึง โปรแกรม ผู้ใช้งานและคอมพิวเตอร์
3. การเปลี่ยนแปลง (Modification) เป็นการที่ผู้ไม่มีสิทธิ์สามารถเข้าระบบ แล้วทำการแก้ไข เปลี่ยนแปลงข้อมูลได้
4. การสร้าง (Fabrication) เป็นการที่ผู้ไม่มีสิทธิ์สามารถเข้าระบบและทำการเพิ่มเติมข้อมูลได้

แสดงได้ดังรูปที่ 2.33



รูปที่ 2.33 แสดงประเภทของการโจมตี

2.9.3 วิธีการป้องกันการบุกรุกเข้าสู่เครือข่ายคอมพิวเตอร์

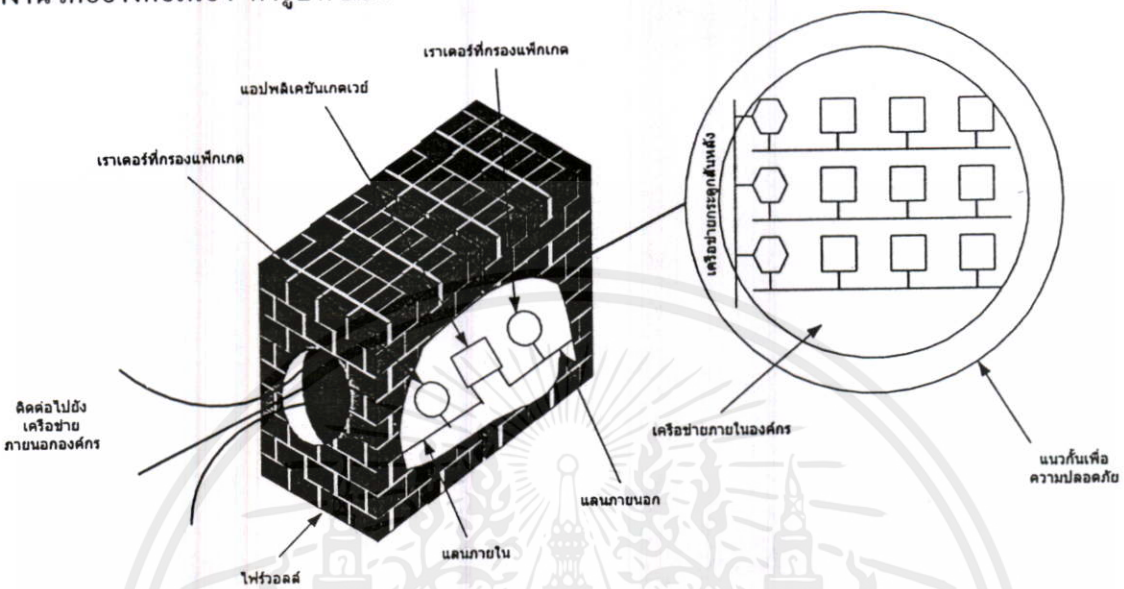
วิทยาการระบบเครือข่ายคอมพิวเตอร์ในการป้องกันเพื่อให้มีความปลอดภัยได้มีการพัฒนามาเป็นลำดับตั้งแต่เริ่มมีระบบเครือข่ายเกิดขึ้น ซึ่งปัจจุบันพบว่าเครือข่ายคอมพิวเตอร์เริ่มมีการเปิดออกสู่เครือข่ายสากล เช่น เครือข่ายอินเตอร์เน็ต จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีการป้องกันอย่างเป็นรูปธรรม ซึ่งวิธีที่นิยมสรุปได้ คือ

1. ไฟร์วอลล์ (Firewall) คือกำแพงป้องกันการเข้าสู่ระบบเครือข่าย โดยจะมีการกำหนดผู้ที่มีสิทธิเท่านั้น จึงจะเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ได้
2. วีพีเอ็น เป็นวิธีที่มีการพัฒนาไฟร์วอลล์ให้มีคุณสมบัติในการป้องกันข้อมูลให้มีความปลอดภัยมากยิ่งขึ้น ตั้งแต่ด้านส่ง ระหว่างการเดินทางของข้อมูล และด้านรับ ซึ่งจะอธิบายรายละเอียดในบทที่ 3

2.9.4 ไฟร์วอลล์ (FIREWALL)

คือ กลไกการป้องกันที่ประกอบด้วยทั้งฮาร์ดแวร์ และซอฟต์แวร์ซึ่งถูกออกแบบขึ้นเพื่อคอยป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตติดต่อเข้าสู่เน็ตเวิร์คภายในองค์กรได้ไฟร์วอลล์ หรือ "กำแพงไฟ" เป็นกำแพงที่ขวางระหว่างเน็ตเวิร์คภายในกับคอมพิวเตอร์อื่นจากภายนอก ซึ่งรวมทั้งเครื่องที่

ต่อเชื่อมกับเน็ตเวิร์คอื่น ๆ และอินเตอร์เน็ตด้วย ไฟร์วอลล์เป็นระบบรักษาความปลอดภัย มาตรฐานที่ใช้กันในองค์กรขนาดใหญ่ โดยอาศัยฮาร์ดแวร์ และซอฟแวร์หลายชุดประกอบกันเพื่อให้ทำงานได้อย่างต่อเนื่อง ดังรูปที่ 2.34



รูปที่ 2.34 แสดงการทำงานของไฟร์วอลล์

ส่วนประกอบและรายละเอียดในการติดตั้งของไฟร์วอลล์แต่ละแบบจะแตกต่างกัน แต่ไฟร์วอลล์ต่าง ๆ ก็ทำหน้าที่ในการกรองข้อมูลที่ผ่านไปมาในตำแหน่งที่เป็นประตูเชื่อมต่อเน็ตเวิร์คภายนอก และยังทำหน้าที่สำคัญในการป้องกันองค์กรเครื่องคอมพิวเตอร์ และข้อมูลสำคัญ ๆ จากผู้ที่ไม่ได้รับอนุญาตที่แอบเข้ามาในระบบ แม้ว่าการบุกรุกเข้าสู่ระบบอาจเป็นเพียงการลองวิชาของโปรแกรมเมอร์ การเล่นสนุกที่ทำไปโดยไม่มีเจตนาร้าย แต่กระทำเหล่านี้ก็ยังนับว่าเป็นการโจมตีหรือบุกรุก และก็ยังอาจก่อให้เกิดอันตรายกันระบบได้ จึงควรจะต้องมีมาตรการป้องกัน ซึ่งสำหรับไฟร์วอลล์นี้ก็คล้ายกับส่วนประกอบอื่น ๆ ของเน็ตเวิร์ค คือ มีความซับซ้อนทางด้านวิศวกรรม ที่รวมเอาแนวคิดทางเทคนิคที่แยบยลมาใช้เป็นจำนวนมาก

สรุปหน้าที่สำคัญของไฟร์วอลล์ คือ

1. ปล่อยเฉพาะข้อมูลที่ได้รับอนุญาตให้เดินทางผ่านเข้ามาถึงที่หมายได้และปฏิเสธข้อมูลที่ไม่ได้รับอนุญาต
2. ให้บริการในลักษณะของยามรักษาการณ์อิเล็กทรอนิกส์ (watchdog) ที่คอยหยุดความพยายามของแฮกเกอร์ (hacker) จากเครื่องคอมพิวเตอร์ที่ไม่รู้จัก (untrusted computer) บนอินเตอร์เน็ตภายนอก

ไฟร์วอลล์อาจเริ่มจากส่วนประกอบเพียงชิ้นเดียวไปจนถึงรุ่นที่มีหลายส่วนประกอบกัน เช่น เครื่องพิวเตอร์, เราเตอร์ และอุปกรณ์ด้านการเชื่อมต่อเน็ตเวิร์คอื่น ๆ แต่โดยรวมแล้วก็ยังคงใช้เทคโนโลยี

แบบเดียวกัน คือ packet sniffing (คอยตรวจสอบที่มาของแต่ละ packet) และ proxying (ไม่ยอมให้เข้าใช้งานเครื่องต่างๆ โดยตรงต้องทำผ่านอีกเครื่องหนึ่งในเน็ตเวิร์คที่เป็นผู้รับมอบอำนาจ) เพื่อรักษาระดับของความปลอดภัยได้มากกว่า

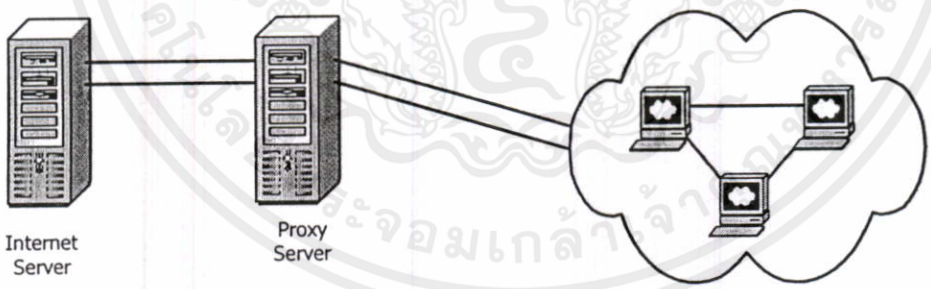
2.9.4.1 Packet Filtering

เมื่อมีการส่งข้อมูลไประหว่างภายในหรือภายนอกองค์กรข้อมูลต่าง ๆ ที่วิ่งอยู่ในเน็ตเวิร์คจะประกอบไปด้วยข้อมูลอื่น ๆ อีกมากมายที่ผู้ใช้ทั่วไปไม่เคยได้พบเห็นมาก่อน เช่น IP address ของทั้งผู้รับและผู้ส่ง หรือข้อมูลที่บอกประเภทบริการหรือโปรโตคอลที่ใช้ เช่น โปรโตคอล SMTP ที่ใช้ในการรับส่งอีเมลล์บนอินเตอร์เน็ต หรือโปรโตคอล FTP ที่ใช้ในการรับส่งไฟล์ (การใช้งานหรือบริการแต่ละประเภทจะใช้โปรโตคอลคนละแบบเสมอ และทั้งฝ่ายรับและส่งจะต้องใช้โปรโตคอลแบบเดียวกัน เพื่อให้สามารถรับส่งข้อมูลกันได้) ซึ่งข้อมูลเหล่านี้จะถูกนำมาใช้ในการ "กรอง" เพื่อเลือกแพ็กเก็ต โดยเครื่องสำหรับทำหน้าที่นี้โดยเฉพาะที่เรียกว่า Packet Filtering Router โดยจะทำหน้าที่ตรวจสอบแพ็กเก็ตใดจะสามารถผ่านเข้าไปภายใน (หรือออกจาก) เน็ตเวิร์คขององค์กรได้บ้าง (สำหรับคำว่า router ไม่จำเป็นจะต้องเป็นอุปกรณ์ทางอิเล็กทรอนิกส์โดยเฉพาะ แต่อาจเป็นเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็น router หากมีซอฟต์แวร์ และฮาร์ดแวร์ที่เหมาะสม เช่นเครื่องที่ใช้รัน Windows NT และมีเน็ตเวิร์คอะแดปเตอร์สองอัน อาจนำมาทำเป็นเราเตอร์สำหรับเชื่อมต่อระหว่างสองเน็ตเวิร์คได้) เราเตอร์จะตรวจสอบไอพีแอดเดรส (IP address) หรือประเภทของโปรโตคอลที่อยู่ในแพ็กเก็ตนั้น และยอมให้เฉพาะบางแพ็กเก็ตที่ได้รับอนุญาตเท่านั้นให้ผ่านเข้าออกเน็ตเวิร์คนั้น ๆ ได้ เนื่องจากบริการบาชนิดมักจะถูกส่งไปที่ช่องทางหรือพอร์ต (port) เดิมเสมอ (เหมือนกับสถานีโทรทัศน์แต่ละแห่งจะแพร่ภาพที่ช่องใดช่องหนึ่งเสมอ) การกรองแพ็กเก็ตจึงถูกนำมาใช้ในการเลือกบริการว่าจะไม่รับแพ็กเก็ตนั้น หรือรับมาแล้วค่อยแทนแต่ละเครื่องที่ต่ออยู่ในการเชื่อมต่อกับเน็ตเวิร์คภายนอก ในกรณีแรกพร็อกซี่เป็นมนุษย์ที่แทนบุคคลหนึ่ง แต่ในกรณีหลังนี้ พร็อกซี่เป็นเครื่องที่แทนกลุ่มคนและเน็ตเวิร์คขององค์กรทั้งหมดในการติดต่อกับโลกภายนอก ดังนั้นเมื่อผู้คนในองค์กรต้องการจะเชื่อมต่อออกไปยังไซต์ภายนอก คำขอในการติดต่อที่อยู่ในรูป ยูอาร์แอล (URL) จะถูกส่งไปยังพร็อกซี่เซิฟเวอร์ (proxy sever) ซึ่งจะทำหน้าที่ในการเชื่อมต่อจริงกับโฮสต์ภายนอกให้แล้วจึงส่งข้อมูลที่ได้รับมากลับไปยังเครื่องของผู้ที่ขอนั้นอีกทีหนึ่ง ในขณะที่ proxy server ทำงานอยู่จะสามารถให้บริการในสิ่งต่าง ๆ ได้ดังนี้

- สามารถแยกส่วนของเน็ตเวิร์คภายในและคอมพิวเตอร์ภายนอกออกจากกันได้ โดยยังควบคุมการเชื่อมต่อไปยังอินเตอร์เน็ตและไซต์อื่น ๆ ได้อย่างรวดเร็ว
- สามารถรักษาความปลอดภัยของฐานข้อมูล DNS ขององค์กร โดยการประกาศเฉพาะข้อมูล DNS เพียงอันเดียว (คือตัวมันเอง) ออกไปยังโลกภายนอก

- สามารถเก็บข้อมูลจากเว็บเพจ หรือเว็บไซต์ที่มีผู้เรียกใช้บ่อย ๆ ไว้ในหน่วยความจำหรือดิสก์ของเครื่องที่เป็น proxy หรือที่เรียกกันว่า cache ทำให้การดึงข้อมูลเร็วขึ้น (เพราะว่าผู้ดึงข้อมูลจาก Proxy server โดยตรง) และช่วยลดความจำเป็นที่จะต้องโอนถ่ายข้อมูลซ้ำๆ จากอินเตอร์เน็ต รวมทั้งลดจำนวนการเชื่อมต่อที่อาจเกิดขึ้นเป็นรายบุคคลเมื่อเชื่อมต่อไปยังไซต์เดียวกันอีกด้วย
- สามารถกลั่นกลองคำขอเชื่อมต่อจากผู้ใช้ เพื่อป้องกันการเชื่อมต่อไปยังไซต์ที่ไม่ได้รับอนุญาต หรือไซต์ที่มีข้อมูลอันไม่พึงประสงค์ต่าง ๆ (เช่นที่มีเนื้อหาขัดต่อศีลธรรม) ได้ส่งต่อไปยังเครื่องที่ทำหน้าที่ใดหน้าที่หนึ่งในองค์กร สำหรับการส่งอีเมลล์หรือโอนย้ายไฟล์ด้วย FTP ผ่านอินเตอร์เน็ตก็มักจะเป็นไปในลักษณะนี้เช่นกัน ทั้งนี้เพื่ออำนวยความสะดวกให้กับผู้ใช้ นอกจากนี้ขณะเดียวกันรักษาความปลอดภัยได้ดีกว่า เพราะไม่ต้องเปิดเน็ตเวิร์คภายในทั้งหมดเพื่อเชื่อมต่อกับเน็ตเวิร์คที่อยู่ภายนอกองค์กรโดยตรง

รูปแบบการกรองแพ็กเก็ตจะช่วยให้เน็ตเวิร์คนี้สามารถที่จะไว้ใจได้ในระดับหนึ่ง คือมีการกรองข้อมูลที่รับส่งกัน และในด้านการเชื่อมต่อออกไปยังเน็ตเวิร์คภายนอกนั้น การกรองวิธีเดียวกันนี้ก็ยังสามารถนำมาใช้เพื่อควบคุมการเข้าถึงอินเตอร์เน็ต หรือเน็ตเวิร์คอื่นได้ โดยป้องกันไม่ให้มีการรับส่งหรือเชื่อมต่อกับไซต์ที่ได้รับอนุญาต แสดงดังรูปที่ 2.35



รูปที่ 2.35 แสดงการทำงานของพร็อกซี่เซิฟเวอร์

2.9.4.2 พร็อกซี่เซิฟเวอร์ (Proxy Server)

การเชื่อมต่อเครือข่ายคอมพิวเตอร์มีการแพร่หลายมากในปัจจุบัน สำหรับองค์กรใดที่ยังไม่เป็นระบบอินทราเน็ต หรือยังคงเปิดให้ใช้การเชื่อมต่อแบบพอยท์ทูพอยท์ (point-to-point) โดยตรงเข้ากับอินเตอร์เน็ต มีโอกาสที่จะเกิดความเสียหายจากผู้ที่ลักลอบเข้ามาใช้งานในระบบอีกด้วย ดังนั้นในองค์กรใหญ่ ๆ จึงมักใช้พร็อกซี่เซิฟเวอร์ เพื่อเปิดให้เรียกใช้เว็บบนอินเตอร์เน็ตได้ และใน

ขณะเดียวกันก็ยังคงรักษาความปลอดภัยในเน็ตเวิร์คเอาไว้ได้ ความหมายที่ใช้กันทั่ว ๆ ไปของคำว่า proxy คือตัวแทนที่รับมอบอำนาจเพื่อเข้าประชุมผู้ถือหุ้นหรือในกิจกรรมอื่น ๆ (คำ proxy แปลตรงตัวว่าผู้รับมอบอำนาจ) ส่วนพร็อกซี่เซิฟเวอร์หรือบางครั้งก็เรียกว่าเป็น application gateway จะเป็นผู้ประสานงานต่าง ๆ ระหว่างโปรแกรมใช้งานที่อยู่บนเครื่องของผู้ใช้แต่ละคน (ซึ่งอาจมองเป็น client) และบนโฮสต์หรือเซิร์ฟเวอร์ สำหรับพร็อกซี่เซิฟเวอร์นี้ซึ่งจะเห็นได้ว่าพร็อกซี่เซิฟเวอร์ทำหน้าที่อยู่ในระดับสูงกว่า packet filter แบบที่เป็นฮาร์ดแวร์ และทำการกรองข้อมูลโดยอาศัยโปรโตคอลเป็นหลักเท่านั้น เมื่อนำ proxy server หรือ packet filter มาใช้งานร่วมกัน จะได้การรักษาความปลอดภัยขึ้นมาเป็นสองระดับด้วยกัน ซึ่งทั้งนี้ก็ขึ้นอยู่กับกฎเกณฑ์และข้อกำหนดที่ติดตั้งไว้ในฮาร์ดแวร์และซอฟต์แวร์ และถึงแม้ว่าจะมีระบบที่มีความสามารถในการรักษาความปลอดภัยเป็นอย่างดีแล้ว แต่ระบบดังกล่าวจะทำงานได้ดีเมื่อมีการวางแผนและดูแลอย่างเหมาะสมต่อเนื่อง

บทที่ 3
เครือข่ายส่วนตัวเสมือน

3.1 บทนำ

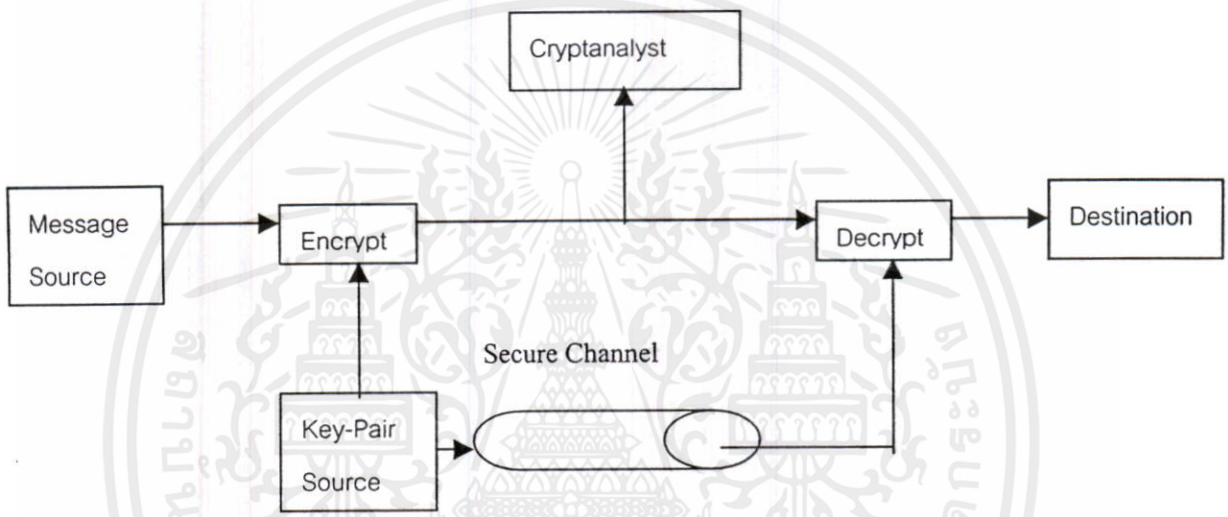
ปัจจุบันวิทยาการสมัยใหม่ ทำให้ความเจริญก้าวหน้าทางเทคโนโลยีทางด้านเน็ตเวิร์คมีการประยุกต์ใช้งานได้จำนวนมาก อาทิ เช่น สามารถจะใช้เครื่องแลปทอปที่มีวิทยุไร้สาย เชื่อมต่อเข้าสู่ระบบคอมพิวเตอร์ได้ มีความสะดวกรวดเร็ว รองรับการเปลี่ยนแปลงทางเทคโนโลยี และสามารถเชื่อมต่อเข้าอินเทอร์เน็ต ทำให้สามารถเข้าสู่เครือข่ายใดๆ ในโลกนี้ แต่ด้วยการใช้ความรู้ที่ขาดคุณธรรมจึงมีผู้ที่ใช้เทคโนโลยีทางด้านเน็ตเวิร์ค เพื่อการโจรกรรมข้อมูล และทำการปรับเปลี่ยนแก้ไขข้อมูล ทำให้ผู้รับการสื่อสารปลายทางได้รับข้อมูลที่บิดเบือน, สูญหาย, ถูกลักลอบเก็บข้อมูลด้วยวิธีการโจมตี (Attack) ในรูปแบบต่างๆ ดังนั้นจึงมีการนำหลักการในการใส่คีย์ (key) กับข้อความต้นฉบับ หรือเรียกว่า "การเอ็นคริปท์ชัน" เพื่อให้ผู้ที่มีคีย์แท้จริงเท่านั้น จึงจะสามารถถอดรหัสข้อความจริงเหล่านั้นได้ ซึ่งเป็นวิทยาการที่มีการคิดค้นตั้งแต่ในอดีตมาจนถึงปัจจุบัน และเมื่อนำมารวมใช้กับวิทยาการทางด้านเน็ตเวิร์ค ทำให้สามารถกำหนดสิทธิ ตรวจสอบสิทธิของผู้ใช้งาน และยังทำให้ข้อมูลเคลื่อนที่ไปในเครือข่ายมีความปลอดภัย เนื่องจากไม่สามารถอ่านข้อมูลเหล่านั้นได้ ถ้าปราศจากคีย์ และอัลกอริทึมเอ็นคริปท์ชันจริงที่ใช้งาน ซึ่งกลายมาเป็นเครือข่ายส่วนตัวเสมือน การบริการเครือข่ายบรอดแบนด์ แบบวีพีเอ็น กำลังมีบทบาทต่อผู้ใช้ [3] มากขึ้นเรื่อยๆ ในอนาคตของประเทศไทย และต่างประเทศ โดยเฉพาะสภาพแวดล้อมทางธุรกิจที่เปลี่ยนแปลงทำให้ระบบเครือข่ายส่วนตัวเสมือนทำให้ผู้ใช้งานมีความพึงพอใจ [5] และเน็ตเวิร์คมีความปลอดภัยมากยิ่งขึ้น และถ้านำไปประยุกต์ใช้ในการสื่อสารผ่านทางอินเทอร์เน็ต จะช่วยลดต้นทุนในการลงทุนเครือข่าย [4] เพราะสามารถใช้เครือข่ายของบริษัทแม่ โดยบริษัทสาขาที่อยู่ ณ ต่างประเทศ หรือต่างจังหวัด โดยเพียงเข้าอินเทอร์เน็ต จะสามารถทำการติดต่อเครือข่ายส่วนกลางได้

3.2 หลักการวีพีเอ็น

เครือข่ายส่วนตัวเสมือน (Virtual Private Networks; VPN) หรือวีพีเอ็น หมายถึงการทำให้เครือข่ายสาธารณะ หรือเครือข่ายภายในองค์กร สามารถเป็นเส้นทางผ่านของข้อมูลที่มีความปลอดภัย และผู้ใช้งานที่มีสิทธิเท่านั้น จึงจะสามารถเข้าใจความหมายของข้อมูลได้ ด้วยการนำหลักการของระบบคริปท์โตกราฟี ร่วมกับเทคโนโลยีทางด้านเครือข่าย จึงทำให้เครือข่ายสาธารณะ หรือภายในองค์กร มีความปลอดภัย และเสมือนว่าเป็นเครือข่ายส่วนตัว แม้เครือข่ายเหล่านั้นจะใช้ร่วมกันกับบุคคลอื่นมากมาย

3.3 ระบบคริปท์โตกราฟี (Cryptography System)

ระบบคริปท์โตกราฟี คือกระบวนการที่ทำให้ข้อมูลของผู้ส่งที่เป็นเพลนเท็ก (Plaintext. ข้อความอักษรที่อ่านออก) ให้กลายเป็นไซเฟอร์เท็ก (Ciphertext: ข้อความที่ไม่สามารถอ่านความหมายได้) หรือเรียกโปรเซสนี้ว่าการเอ็นคริปท์ชัน (Encryption) แล้วเมื่อข้อมูลถูกส่งก่อนถึงผู้รับที่มีสิทธิจะทำการแปลงข้อมูลที่ไม่สามารถอ่านความหมายให้กลายเป็นข้อมูลที่อ่านได้ โดยใช้การดีคริปท์ชัน (Decryption) ซึ่งเป็นกระบวนการในระบบคริปท์โตกราฟี จะแสดงเป็นขั้นตอนดังในรูปที่ 3.1



รูปที่ 3.1 แสดงระบบคริปท์โตกราฟี

3.3.1 กระบวนการเอ็นคริปท์โตกราฟี

กระบวนการเอ็นคริปท์โตกราฟี เป็นการทำให้แพ็กเก็ตที่อ่านออก (Plaintext) ร่วมผสมกับตัวอักษร (Key) ที่กำหนดให้สำหรับการเข้าสู่กระบวนการผสมอักษร เข้าสู่ข้อมูลจริงทำให้ไม่สามารถที่จะอ่านแพ็ตเก็ตข้อมูลเหล่านั้นได้ จนกว่าจะถึงผู้ที่มีสิทธิในการอ่านข้อมูลเหล่านั้นได้จริง จึงจะมีการนำตัวอักษรที่ร่วมในการเอ็นคริปท์มาทำการถอดตัวอักษรเหล่านั้นออก ด้วยวิธีการทางคณิตศาสตร์ที่เหมือนกัน จึงจะสามารถทำให้ผู้ที่มีสิทธิฝั่งรับสามารถที่จะอ่านข้อมูลเหล่านั้นได้ พบว่าคีย์ (key) ที่ใช้ในกระบวนการเอ็นคริปท์ หรือดีคริปท์ จะต้องเป็นตัวอักษรที่ต้องปิดเป็นความลับในการเข้าถึงข้อมูลเหล่านั้นได้ จึงทำให้ต้องมีการบริหารคีย์ ซึ่งกระบวนการในการบริหารคีย์คือการสร้างคีย์ การแจกจ่ายคีย์ และการป้องกันคีย์ที่ใช้มิให้บุคคลที่ไม่สิทธิ ทั้งภายใน และนอกสามารถรับรู้ได้

3.4 การเอ็นคริปท์ชัน

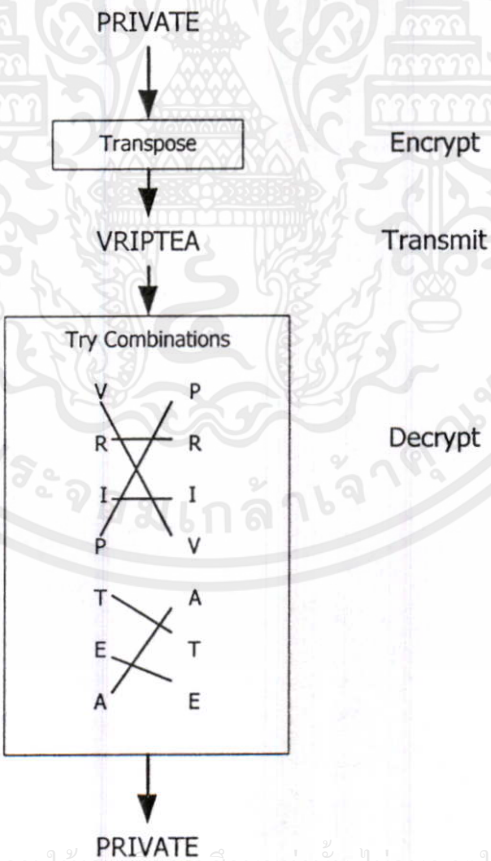
นิยามของการเอ็นคริปท์ชั่นคือกระบวนการในการเปลี่ยนแปลงข้อมูลที่อ่านแล้วเข้าใจได้ แปลงไปเป็นข้อมูลที่ไม่สามารถอ่านเข้าใจความหมายได้ ข้อมูลตอนเริ่มต้นสามารถอ่านเข้าใจความหมายได้ หรือเรียกว่า เพลนเท็ก (Plaintext) และเมื่อถูกเอ็นคริปท์ชันจะเรียกว่าไซเฟอร์เท็ก โค้ดเท็ก (ciphertext, codetext) ซึ่งไม่สามารถเข้าใจความหมายได้ มีเทคนิคในการเอ็นคริปท์ชันในหัวข้อถัดไป

3.5 เทคนิคที่ใช้ในการเอ็นคริปท์ชัน

เทคนิคที่ใช้จะเป็นหลักการพื้นฐานในการทำเอ็นคริปท์ชัน ซึ่งจะมีหลักการพื้นฐานดังนี้

3.5.1 การทรานสโพส (Transposition)

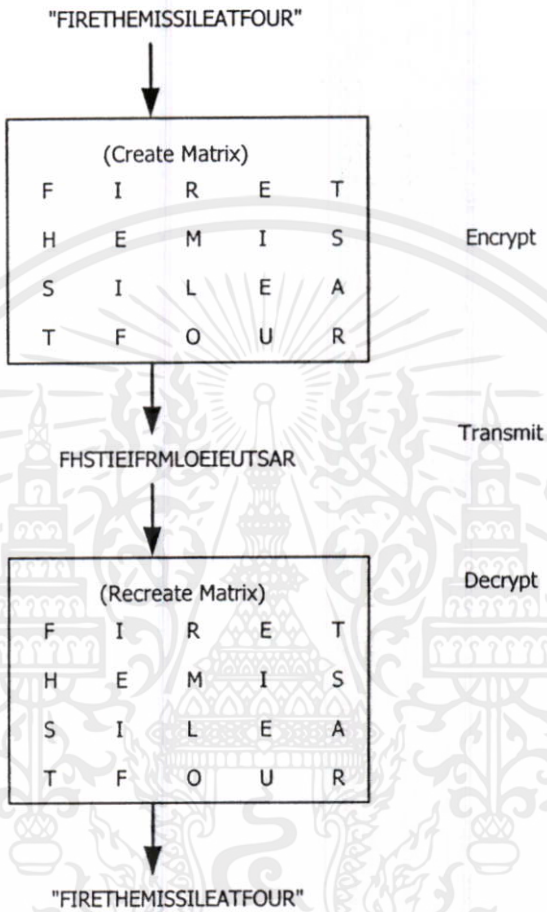
ตัวแบบข้อความอักษรสามารถถูกการทรานสโพสได้หลายวิธี ซึ่งวิธีหนึ่งแสดงได้ดังรูปที่ 3.2



รูปที่ 3.2 แสดงวิธีการทรานสโพส

จากคำว่า "PRIVATE" ถูกทรานสโพส จะกลายเป็น "VRIPTEA" ซึ่งเป็นข้อความที่ไม่สามารถอ่านเข้าใจความหมายได้ และผู้ที่ต้องการอ่านความหมายจะต้องทำการดีคริปท์ชัน เพื่อจะสามารถอ่าน

ข้อความนั้นได้ โดยการใช้วิธีการทรานสโพส มีการประยุกต์ใช้การทรานสโพสทางเมตริกซ์ มาใช้งาน การเอ็นคริปท์ชัน และดีคริปท์ชัน แสดงได้ดังรูปที่ 3.3



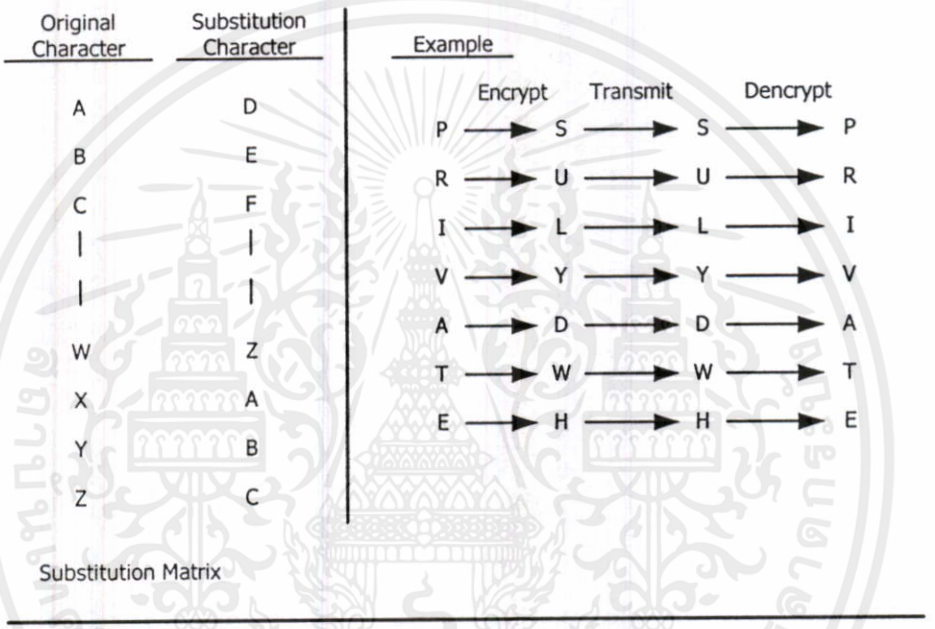
รูปที่ 3.3 แสดงการใช้ทรานสโพสเมตริกซ์

จากรูปประโยค FIRE THE MISSILE AT FOUR. เมื่อถูกการทรานสโพสจะได้เป็น FHSTIEIFRMLOEIEUTSAR ซึ่งจะกลายเป็นประโยคที่ไม่สามารถเข้าใจความหมายได้ แต่พอรู้วิธีการทรานสโพส สามารถใช้เป็นการดีคริปท์ชัน เพื่อให้สามารถแปลงกลับเป็นข้อความที่เข้าใจความหมายได้

3.5.2 การแทนที่ (Substitution)

การแทนที่ คือการใช้ตัวอักษรอื่นเปลี่ยนแทนลงในอักษรตัวเดิม (เป็นการเอ็นคริปท์ชัน) เพื่อจะกลายเป็นประโยคข้อความที่ไม่สามารถเข้าใจความหมายได้ ทำนองเดียวกัน เมื่อต้องการจะทราบความหมายที่แท้จริงของข้อความเหล่านั้น จะต้องมีการดีคริปท์ชัน โดยการแทนที่อักษรเดิมกลับเข้าสู่รูปประโยคเดิมจึงจะสามารถเข้าใจความหมายของข้อความได้แสดงตัวอย่างได้ดังรูปที่3.4

เป็นตัวอย่างของการแทนที่อักษร จากประโยคคำว่า "PRIVATE" จะถูกแปลงเป็น SULYDWH ซึ่งไม่สามารถตีความหมายได้ และทำการดีคริปท์ชันเพื่อแปลงกลับเป็นประโยคเดิม เพื่อจะสามารถเข้าใจความหมายได้ ขณะนี้มีการคิดค้นวิธีการเอ็นคริปท์ชันจากหลักการพื้นฐานที่กล่าวข้างต้นผสมผสานกับหลักการทางคณิตศาสตร์ที่นำมาใช้ในการคำนวณค่าระหว่างบิทต่อบิท หลักคณิตศาสตร์ที่ใช้คือแอนด์ ออร์ การหาร การคูณ และ การเอ็กคลูซีฟออร์ ทำให้เกิดเป็นอัลกอริทึมในการเอ็นคริปท์ชันจำนวนมากยิ่งขึ้น ซึ่งจะแสดงอัลกอริทึมที่สำคัญดังหัวข้ออื่นถัดไป



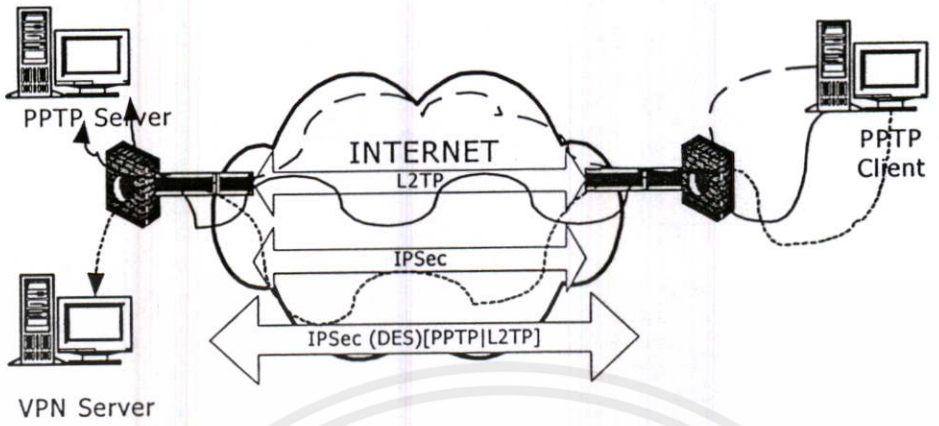
รูปที่ 3.4 แสดงวิธีการแทนที่อักษร

3.6 โปรโตคอลมาตรฐานเครือข่ายวีพีเอ็น 4 แบบ

เครือข่ายวีพีเอ็นจะมีโปรโตคอลมาตรฐานได้ 4 แบบ ที่นำมาใช้เพื่อให้การสื่อสารเครือข่ายวีพีเอ็นสามารถติดต่อสื่อสารกันได้ สามารถแสดงการทำงานเครือข่ายวีพีเอ็นโดยการใช้โปรโตคอลมาตรฐานได้ดังรูปที่ 3.5

3.6.1 โปรโตคอลพีพีทีพี (Point to Point Tunnneling Protocol; PPTP)

โปรโตคอลพีพีทีพี คิดค้นโดยบริษัทไมโครซอฟท์ ถูกออกแบบสำหรับอนุญาตให้ผู้ใช้งานสามารถหมุนโทรศัพท์ติดต่อผู้ให้บริการอินเทอร์เน็ตในพื้นที่ โดยใช้โปรโตคอลพีพีพี และใช้ทันเนลเป็นทางเดินเข้าสู่เซิฟเวอร์ และจะใช้อัลกอริทึมในการเอ็นคริปท์ชันเป็น PAP และ CHAP โปรโตคอลพีพีทีพี จะประกอบด้วยการใช้โปรโตคอลพีพีพี (PPP) และโปรโตคอลทีซีพี/ไอพี (TCP/IP) โปรโตคอลพีพีทีพีประกอบด้วยส่วนประกอบของพีพีพี เช่นการใช้มัลติโปรโตคอล, การให้สิทธิผู้ใช้งาน และในการทำให้แพ็กเก็ตบีบอัดข้อมูลส่วนตัว และ ทีซีพี/ไอพี รองรับความสามารถในการ

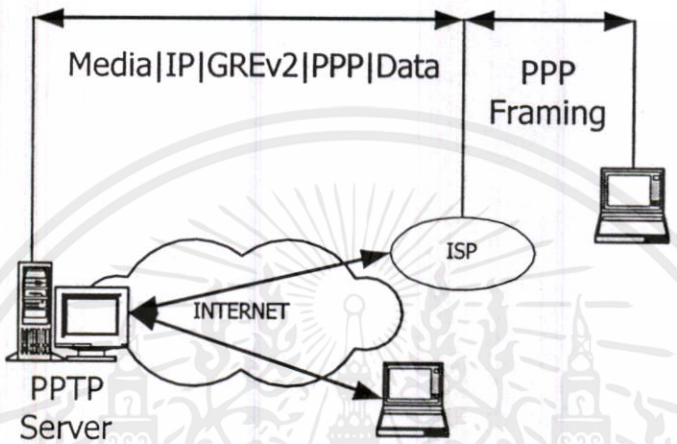


รูปที่ 3.5 แสดงการใช้โปรโตคอลมาตรฐานเครือข่ายวีพีเอ็น

หาเส้นทางของแพ็กเก็ตเหล่านั้นเพื่อผ่านไปบนอินเทอร์เน็ต โปรโตคอลพีพีทีพี อนุญาตการเอ็นแคปซูเลชันข้อมูลโดยการใช้ทันเนล โปรโตคอลพีพีทีพีเป็นเสมือนมาตรฐานอาร์เอฟซี (RFC) ดร๊าฟ มีความหมายที่สามารถเอ็นแคปซูเลตแพ็กเก็ตพีพีพี และส่งต่อให้กับปลายทางได้ โปรโตคอลพีพีทีพี สามารถใช้แพ็กเก็ตต่างๆ เช่น IP, IPX, NetBios , SNA และ wrap ให้มาอยู่ในรูปของ ไอพีแพ็กเก็ตเพื่อขนส่งข้อมูลได้ โปรโตคอลพีพีทีพี ใช้ Generic Routing Protocol (GRE) เพื่อส่งแพ็กเก็ตพีพีพีมีการใช้เอ็นคริปท์ชันสำหรับเอ็นแคปซูเลตข้อมูล และจัดแจงสำหรับการออเทนทิเคชัน โปรโตคอลพีพีทีพี ประกอบด้วยแพ็ตเก็ต 2 ประเภทในการขนส่งข้อมูล คือ
แพ็กเก็ตข้อมูล และ แพ็กเก็ตควบคุม ในส่วนของแพ็ตเก็ตควบคุมจะใช้สำหรับบอกสถานะ และการบอกสัญลักษณ์ และในแพ็กเก็ตข้อมูลจะประกอบด้วยข้อมูลของผู้ใช้งาน โดยแพ็กเก็ตข้อมูลเป็นแพ็กเก็ตที่ถูกเอ็นแคปซูเลทด้วยการใช้ Internet Generic Routing Encapsulation Protocol Version 2 (GREv2) โปรโตคอลพีพีทีพี ในการเริ่มเชื่อมต่อจะมีการตรวจสอบระหว่างจุดเชื่อมทั้ง 2 ทาง ถ้าเป็นตามข้อตรงลง และวิธีการเอ็นแคปซูเลชัน ในช่วงการสื่อสารปกติจะมีการแตกแพ็กเก็ตถ้าจำเป็นต้องทำ และ ส่วนหัวของพีพีพี จะมีการเพิ่มเลขที่เรียงลำดับ เพื่อตรวจสอบว่าแพ็กเก็ตใดสูญหายบ้าง โปรโตคอลพีพีทีพีประกอบด้วย 3 ประเภทการสื่อสาร คือ

1. การเชื่อมต่อโปรโตคอลพีพีทีพี เกิดขึ้นขณะที่ไคลเอนท์สร้งการเชื่อมต่อ พีพีพี หรือ ISDN เข้ากับผู้ให้บริการอินเทอร์เน็ต (ISP)
2. การเชื่อมต่อควบคุมโปรโตคอลพีพีทีพี การใช้อินเทอร์เน็ต ผู้ใช้งานสร้างการเชื่อมต่อโปรโตคอลพีพีทีพี ไปยัง วีพีเอ็นเซิฟเวอร์ และตั้งค่าคุณสมบัติของการใช้โปรโตคอลพีพีทีพีทันเนล (PPTP Tunnel)
3. โปรโตคอลพีพีทีพีทันเนลเครื่องไคลเอนท์และเซิฟเวอร์จะสื่อสารซึ่งกันและกัน โดยมีการเอ็นคริปท์ทันเนล

ซีเคียวริตี้ในโปรโตคอลพีพีทีพี ประกอบขึ้นใน Windows NT RAS Security การสื่อสารระหว่างผู้ใช้งานรีโมตเข้ามา และเครือข่ายส่วนตัวภายในบริษัทถูกทำโดย การใช้ RAS เอ็นคริปท์ชัน และออ-เทนทิเคชัน โปรโตคอลออเทนทิเคชันจะใช้ PAP CHAP และ MS-CHAP ดูตัวอย่างได้จากรูปที่ 3.6



รูปที่ 3.6 แสดงการทำงานโปรโตคอลพีพีทีพี

3.6.2 โปรโตคอลแอลทูเอฟ(Layer 2 Forwarding Protocol; L2F)

ในปี 1996 บริษัทซิสโก้ (Cisco) พัฒนาโปรโตคอลแอลทูเอฟ เนื่องจากความเติบโตในการให้บริการไดอัลอัพ และมีโปรโตคอลที่ใช้กันอย่างหลากหลาย วิธีหนึ่งที่ถูกสร้างขึ้นเพื่อทำให้เกิดฉากการไดอัลอัพเสมือน โดยที่โปรโตคอลที่ใช้ไม่เป็นไอพีก็สามารถใช้งานผ่านเครือข่ายอินเทอร์เน็ตได้ บริษัทซิสโก้ กำหนดแนวคิดของ ทันเนล, ความหมายของการเอ็นแคปซูเลชันบนแพ็ตเก็ตที่ไม่ใช้โปรโตคอลไอพี ผู้ใช้งานสามารถใช้โปรโตคอลพีพีพี หรือ เอสแอลไอพี (SLIP) ในการหมุนเชื่อมต่อกับผู้ให้บริการทางอินเทอร์เน็ต (ISP) และใช้โปรโตคอลแอลทูเอฟ ในการเชื่อมโยงกับคอมพิวเตอร์ส่วนกลางของบริษัท การทันเนลจะเกิดขึ้นที่จุดเชื่อมต่อกับอินเทอร์เน็ต โดยที่เราเตอร์จะใช้ซอฟแวร์ในการทันเนลทำให้เรียกว่า การเชื่อมต่อแบบทันเนล โปรโตคอลแอลทูเอฟ จะให้ประโยชน์มากมายอาทิเช่น

- โปรโตคอลอิสระ (Protocol independence) สามารถรองรับโปรโตคอลอื่นๆได้ เช่น IPX SNA
- การออเทนทิเคชัน (Authentication) รองรับโปรโตคอล เช่น PPP CHAP TACACS
- การบริหารที่อยู่ (ถูกกำหนดโดยปลายทาง)
- ทันเนลที่คล่องแคล่วและปลอดภัย
- การคิดบัญชี สามารถนำมาใช้ในการคิดคำนวณค่าใช้จ่ายที่เกิดการการใช้งานโปรโตคอลนี้ได้

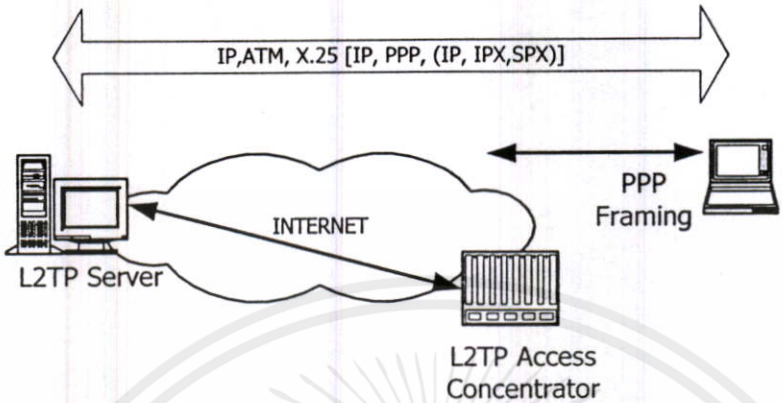
- สื่อกลางอิสระ เช่น โปรโตคอลแอลทูเอฟสามารถทำงานได้บนสื่อกลางหลายแบบเช่น ATM X.25 Frame Relay เป็นต้น

ในการติดตั้งพื้นฐาน ผู้ใช้จะการเชื่อมโยงเข้ากับผู้ให้บริการอินเทอร์เน็ตท้องถิ่น ในการร้องขอของผู้ใช้งาน ใช้ซอฟแวร์แอลทูเอฟ เป็นการเริ่มต้นทันเนล กับผู้ใช้ปลายทาง ปลายทางให้ใส่รหัสผ่านและตรวจสอบสิทธิ กำหนดที่อยู่ไอพีให้กับผู้ใช้งาน จากนั้นสภาพก็จะเสมือนกันกับการเชื่อมเข้าสู่ระบบด้วยการใช้รีโมตไดอัลอัพเข้าทำงานกับระบบโปรโตคอลแอลทูเอฟเป็นโปรโตคอลทรานสปอร์ตที่ใช้ในเครือข่ายส่วนตัวเสมือน บริษัทซิสโก้จะใช้โปรโตคอลนี้กับอุปกรณ์ฮาร์ดแวร์ของตนเอง เช่น เราเตอร์ เป็นต้น ซึ่งเมื่อนำมาใช้ในการสร้างระบบเครือข่ายวีพีเอ็น จะต้องใช้เราเตอร์ที่รองรับโปรโตคอลเดียวกัน จึงถือได้ว่ามาตรฐานโปรโตคอลนี้ใช้เฉพาะกับผลิตภัณฑ์ของซิสโก้

3.6.3 โปรโตคอลแอลทูทีพี (Layer2 Tunneling Protocol; L2TP)

โปรโตคอลแอลทูทีพีมีพื้นฐานเหมือนกันกับโปรโตคอลพีพีทีพี โดยจะใช้โปรโตคอลพีพีพีสำหรับการติดต่อสื่อสารกับผู้ให้บริการอินเทอร์เน็ต (ISP) ใช้อัลกอริทึมออเทนทิเคชันเป็น PAP และ CHAP โปรโตคอลแอลทูทีพีสามารถใช้ได้บนสื่อได้อย่างอิสระ เช่น ATM Frame หรือ IP ในปี 1996 ทั้งโปรโตคอลพีพีทีพี และแอลทูเอฟ ได้มีการเพิ่มโปรโตคอล ผู้ผลิตเช่น ไมโครซอฟท์ Ascend และ 3Com ทำงานบนโปรโตคอลพีพีทีพี ขณะที่บริษัทซิสโก้ทำงานบนแอลทูเอฟ ในปี 1998 ผู้ผลิตเหล่านี้ได้มีการใช้สัญญาไอพีทีเอฟ (IETF) ฉบับใหม่ กำหนดคุณสมบัติให้เป็นโปรโตคอลแอลทูทีพี ซึ่งอยู่ระหว่างพีพีทีพี และแอลทูเอฟ โปรโตคอลพีพีทีพีและแอลทูทีพีรองรับการบีบอัดข้อมูลด้วยซอฟแวร์ ทำให้แพ็กเก็ตผู้ใช้ลดขนาดลงได้ เทคนิคการบีบอัดข้อมูลถูกเพิ่มเข้าในการเอ็นคริปท์ชันแอลทูทีพีใช้ 2 ฟังก์ชันคือ ไคลเอนท์เหมือนเส้นทางต่อเซิฟเวอร์ อ้างได้เสมือนกับแอลเอซี (LAC:L2TP Access Concentrator) ซึ่งโปรโตคอลแอลทูทีพีมีการเข้าส่วนกลาง และเซิฟเวอร์ข้างเคียง เรียกว่า แอลเอ็นเอส (LNS) เมื่อ เครื่องคอมพิวเตอร์ส่วนบุคคลเชื่อมต่อผ่านผู้ให้บริการอินเทอร์เน็ตด้วย โปรโตคอลพีพีพีและฟังก์ชันแอลเอซีจะเริ่มการทันเนล ถัดจากนั้น แอลเอซีจะเพิ่มส่วนหัวหลากหลายบนเพย์โลดของโปรโตคอลพีพีพี แล้วแอลเอซี จะสร้างทันเนลกับอุปกรณ์แอลเอ็นเอส (LNS:L2TP Network Server) ปลายทาง อุปกรณ์นี้อาจจะเป็น เราเตอร์, เซิฟเวอร์ หรืออุปกรณ์การเข้า หลังจากการสร้างทันเนลเกิดขึ้น จะมีกลไกในการออเทนทิเคชันผู้ใช้ยกตัวอย่างเช่น TACAS (Terminal Access Controller Access Control System) หรือ RADIUS (Remote Authentication Dial In Service) token ที่สร้างสำหรับการวิเคราะห์ผู้ใช้งานโปรโตคอลแอลทูทีพี จะใช้การควบคุมข้อความเพื่อออพติไมซ์ทันเนล โปรโตคอลแอลทูทีพี คล้ายกันกับ โปรโตคอลแอลทูเอฟ ในส่วนที่เป็นขั้นตอนหลัง ซึ่งการติดตั้งแอลเอซี บนผู้ให้บริการอินเทอร์เน็ตเพิ่มเติม และเครื่องที่ผู้ใช้งานรีโมตเพื่อเชื่อมต่อกับผู้ให้บริการอินเทอร์เน็ต โปรโตคอลแอลทูทีพี จะใช้โปรโตคอลเลเยอร์ที่ 2 ที่ถูกออกแบบเพื่อเอ็นแคปซูเลต ดังนั้น โปรโตคอลไอพีเสค (IPSec) ซึ่งใช้

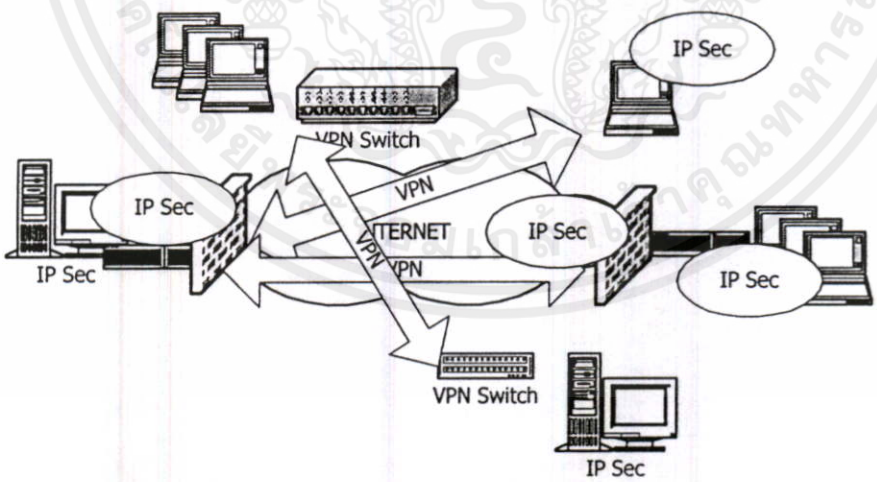
โปรโตคอลในเลเยอร์ที่ 3 จะสามารถใช้กับโปรโตคอลแอลทูทีพี สำหรับการเพิ่มความปลอดภัยเพิ่มขึ้น แสดงตัวอย่างการทำงานของโปรโตคอลแอลทูทีพีได้ดังรูปที่ 3.7



รูปที่ 3.7 แสดงการใช้โปรโตคอลแอลทูทีพีในเครือข่ายวีพีเอ็น

3.6.4 โปรโตคอลไอพีเสค(Internet Security Protocol; IPSec)

องค์กรไอพีทีเอฟ (Internet Engineering Task Force; IETF) ได้มีการทำงานเป็นกลุ่มที่เรียกว่า IP Security (IPSec) ซึ่งมีหน้าที่รับผิดชอบต่อการกำหนดมาตรฐาน และโปรโตคอลที่เกี่ยวข้องกับความปลอดภัยในอินเทอร์เน็ต เครือข่ายส่วนตัวเสมือนจะใช้มาตรฐานนี้เป็นส่วนหนึ่งในการวัดความปลอดภัย ซึ่งการประยุกต์ใช้งานโปรโตคอลไอพีเสคในเครือข่ายวีพีเอ็นแสดงได้ดังรูปที่ 3.8



รูปที่ 3.8 แสดงโปรโตคอลมาตรฐานไอพีเสคในเครือข่ายวีพีเอ็น

โปรโตคอลไอพีเสค กำหนดโครงสร้างของไอพี แพ็กเก็ต ซึ่งมีดังนี้

RFC 2401 : Security Architecture for the Internet Protocol

RFC 2402: IP Authentication Header

RFC 2403: The Use of HMAC-MD5-96 within ESP and AH

RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH

RFC 2405: The ESP DES-CBC Cipher Algorithm with Explicit IV

RFC 2406: IP Encapsulating Security Payload (ESP)

RFC 2407: The Internet IP Security Domain of Interpretation for ISAKMP

RFC 2408: Internet Security Association and Key Management Protocol (ISAKMP)

RFC 2409: The Internet Key Exchange (IKE)

RFC 2410: The Null Encryption Algorithm and Its Use with IPSec

RFC 2411: IP Security Document Roadmap

RFC 2412: The OAKLEY Key Determination Protocol

โปรโตคอลไอพีเสคสามารถจะแบ่งได้ 2 แบบของการทรานสฟอร์เมชันข้อมูลสำหรับการปกป้องแพ็ตเก็ตไอพีคือ

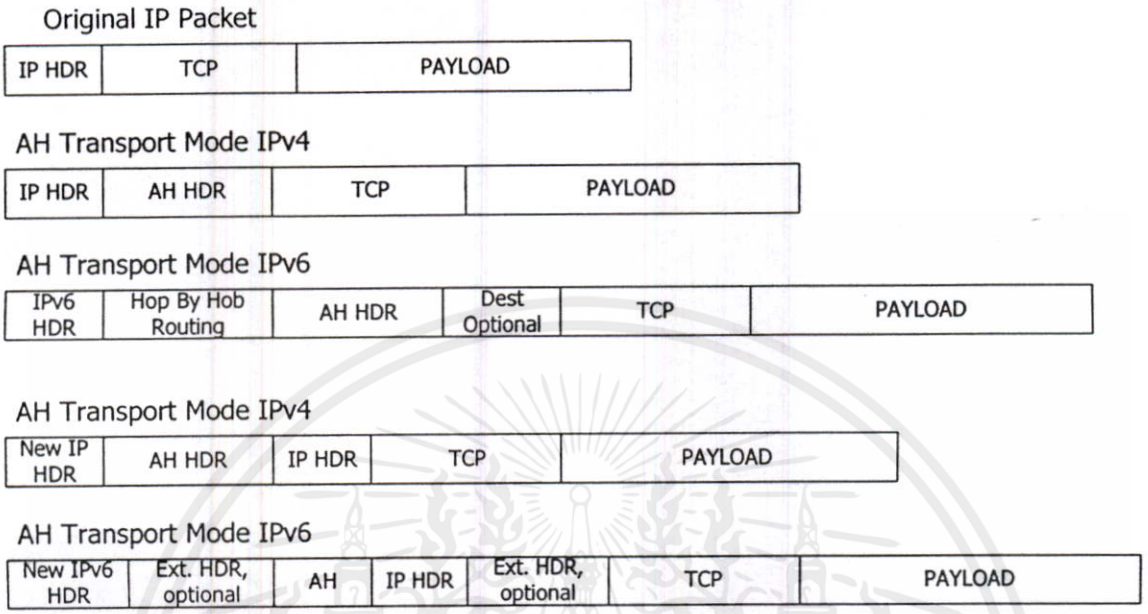
1.ออเทนทิเคชันเฮดเดอร์ (Authentication Header; AH)

RFC 2402 เป็นการอธิบายการออเทนทิเคตแพ็ตเก็ตไอพี ในบริการปกป้องส่วนการรับแพ็ตเก็ตจะทำการปฏิเสธแพ็ตเก็ตเดิม หรือทำการเลียนแบบแพ็ตเก็ตขึ้นเองเพื่อปกป้องผู้บุกรุกไอพีเสค มีการจัดการฟังก์ชันบริการ โดยใช้เลขที่สำหรับการใช้ออเทนทิเคชัน ค่าเอเอช (AH) ของผู้ส่งจะมีค่าเพิ่มขึ้นเมื่อมีการให้บริการปกป้องข้อมูล แต่ผู้รับไม่สามารถตรวจเช็คเลขนี้ได้ ค่าเอเอชจัดแจงการออเทนทิเคตให้กับไอพีแพ็ตเก็ตในระดับสูงของโปรโตคอล อย่างไรก็ตาม ค่าในส่วนหัวของไอพี อาจเปลี่ยนในการส่งโดยที่ผู้รับไม่สามารถคาดการณ์ค่าได้ ค่าเอเอช จะใช้ในทรานสปอร์และโหมดทันเนล ในทรานสปอร์ตโหมดเอเอชจะถูกแทรกหลังจากส่วนหัวเริ่มต้นไอพี และปกป้องโปรโตคอลระดับสูง ในทันเนลโหมดเอเอช จะถูกแทรกก่อนส่วนหัวเริ่มต้นของไอพี และจะมีไอพีส่วนหัวใหม่แทนที่ เอเอช ยังถูกออกแบบสำหรับไอพีวีซิก (IPV6) แสดงได้ดังรูป 3.9

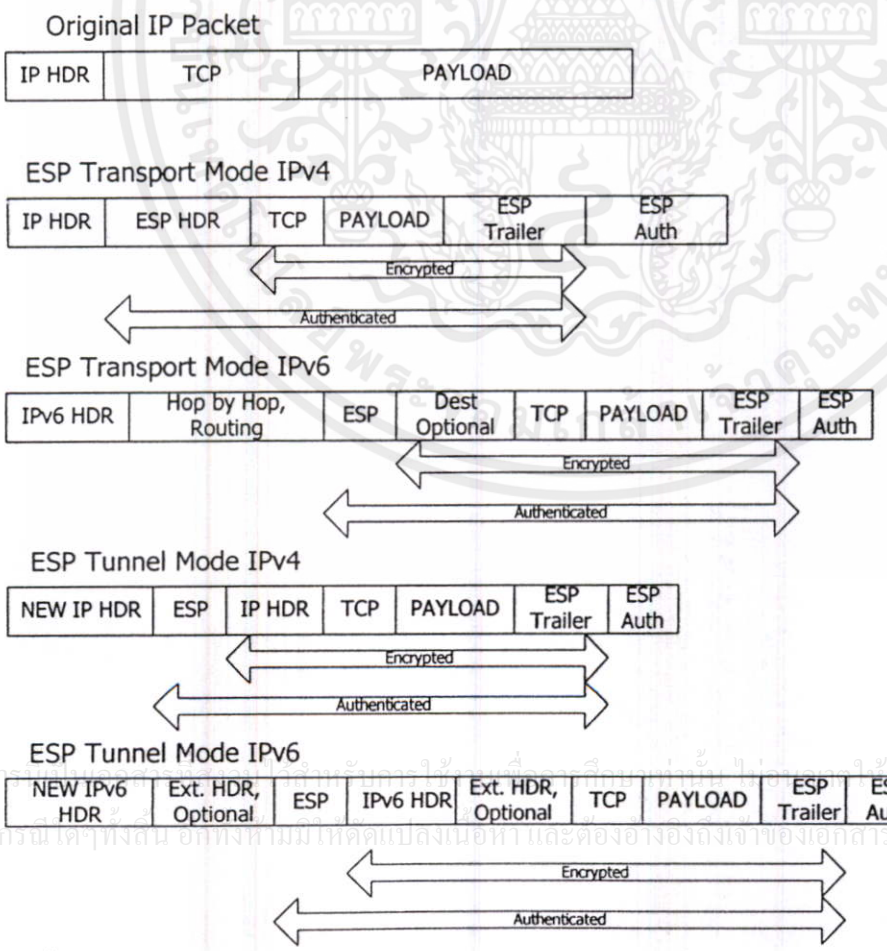
3.6.4.1 เอ็นแคปซูเลตติ้งซีเคียวริตี้เพย์โลด (Encapsulating Security Payload; ESP)

มาตรฐานเอ็นแคปซูเลตติ้งซีเคียวริตี้เพย์โลด หรืออีเอสพี (Encapsulating Security Payload; ESP) หรือ RFC-2406 มีสำหรับความปลอดภัย ออเทนทิเคต คอนเน็คชันเลสอินเทคกริตี้ (connectionless integrity) ในชุดบริการของอีเอสพี (ESP) จะถูกติดตั้งขึ้นสำหรับความปลอดภัยของดาต้าแกรมเท่านั้น เครือข่ายส่วนตัวเสมือนได้นำหลักการเอ็นแคปซูเลตติ้งมาใช้งาน [6] RFC-2406 ชี้ให้เห็นปัญหาศักยภาพในความปลอดภัยได้ ทั้ง เอเอช (AH) และอีเอสพี สามารถแบ่งได้เป็น 2 โหมด คือ ทรานสปอร์ต และทันเนลใช้ได้ทั้ง ไอพีวีโฟว์ (IPV4) และ ไอพีวีซิก (IPV6) แสดงได้ดังรูปที่ 3.10 มาตรฐานอีเอสพี จะมีอัลกอริทึมในการเอ็นคริปท์ชันและออเทนทิเคชัน มาตรฐาน

อีเอสพี สามารถเรียกใช้สำหรับ อัลกอริทึมเอ็นคริปท์ชันสมมาตร และฟังก์ชันแฮสสำหรับออเทนทิเคชัน ยกตัวอย่าง อัลกอริทึม อีเอสพี มีได้ดังนี้



รูปที่ 3.9 โหมดต่างๆ สำหรับเอเอช



รูปที่ 3.10 แสดงโหมดต่างๆ สำหรับมาตรฐานอีเอสพี

DES ใน CBC mode

HMAC กับ MD5

HMAC กับ SHA-1

NULL authentication algorithm

NULL encryption algorithm

ซึ่งในการวิจัยนี้ จะใช้โปรโตคอลไอพีเสคเป็นหลักในการทำงานของระบบเครือข่ายส่วนตัวเสมือน และอัลกอริทึมที่ใช้ในไอพีเสคจะอธิบายในหัวข้อถัดไป

3.7 อัลกอริทึมเอ็นคริปท์ชัน

อัลกอริทึมเอ็นคริปท์ชัน เป็นการใช้หลักการทางคณิตศาสตร์มาใช้ในการทำให้เพลนเท็กกลายเป็นไซเฟอร์เท็ก ซึ่งมีการพัฒนาวิธีการต่างๆ มาจากหลักทางคณิตศาสตร์ อาทิเช่น การบวก การลบ การคูณ การหาร การเพอร์มิวเตชัน และการเอ็กคลูซีฟออร์ เป็นต้น โดยที่อัลกอริทึมเอ็นคริปท์ชันแต่ละแบบจะมีชื่อเรียกที่แตกต่างกันตามวิธี และชื่อของผู้คิดค้น จะอธิบายอัลกอริทึมได้ดังนี้ คือ

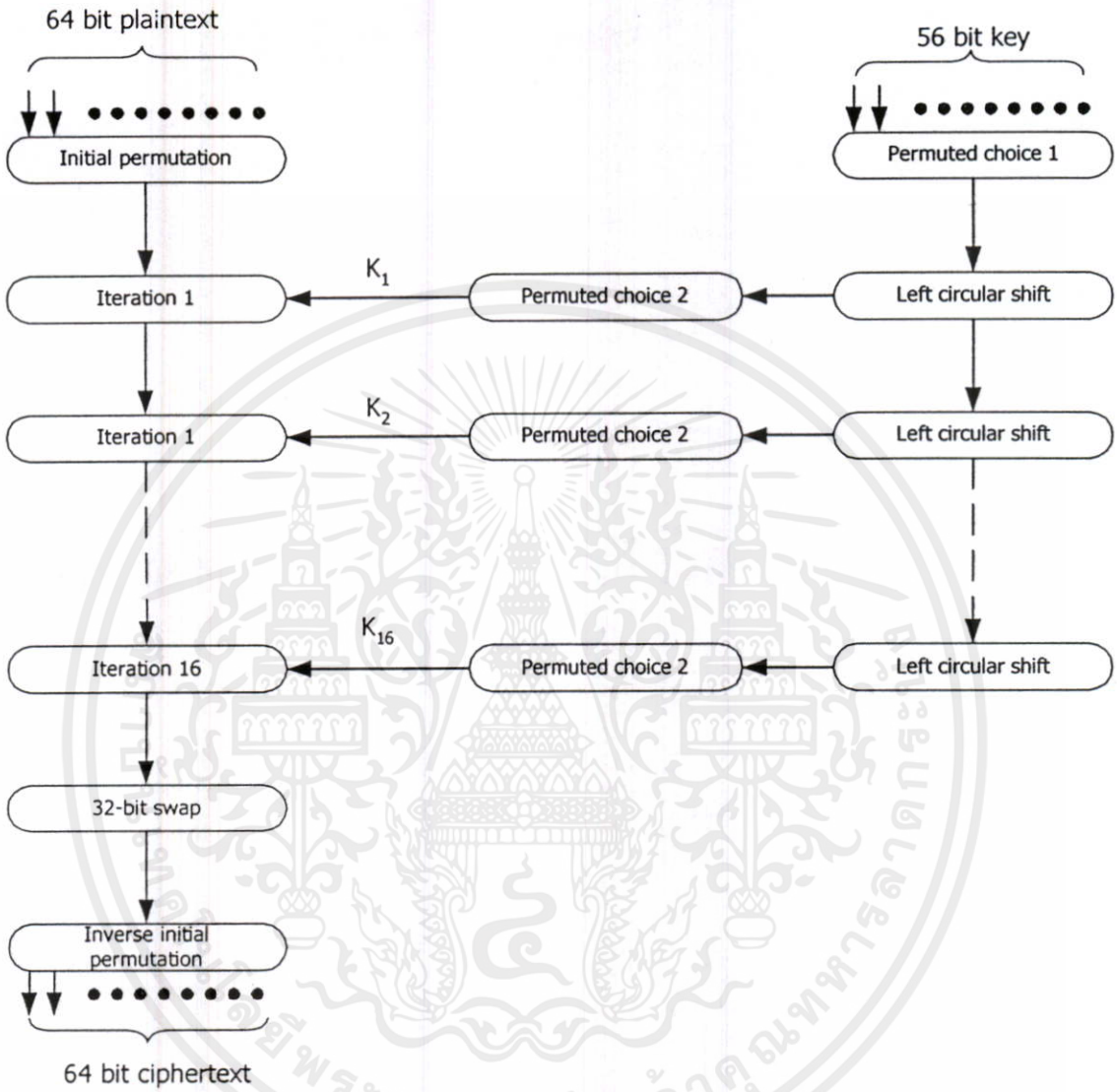
3.7.1 บล็อกไซเฟอร์

บล็อกไซเฟอร์ คือไซเฟอร์ที่เกิดจากการข้อความที่มีการแบ่งเป็นบล็อกที่มีขนาดแน่นอนมาใช้เป็นอินพุท แล้วถูกแปลงให้เป็นไซเฟอร์เท็ก เอาท์พุทที่ได้มีขนาดบล็อกเหมือนอินพุท โดยใช้หลักทางคณิตศาสตร์มาใช้ในการเอ็นคริปท์ชัน เช่น การลบ, การบวก, การทรานสโพสท์, การหาร และทรานสฟอร์เมชันลิเนียร์ นำมาใช้ทำให้เกิดอัลกอริทึมเอ็นคริปท์ชัน ซึ่งอัลกอริทึมเอ็นคริปท์ชันที่ใช้วิธีของบล็อกไซเฟอร์มีหลายอัลกอริทึม จะยกตัวอย่างคือ อัลกอริทึมเดส, อัลกอริทึมทริปเปิ้ลเดส เป็นต้น โดยจะสามารถอธิบายรายละเอียดได้ดังหัวข้อถัดไป

3.7.2 อัลกอริทึมเดส (Data Encryption Standard; DES)

เป็นอัลกอริทึมที่นิยมใช้กันอย่างกว้างขวางที่สุด จัดว่าเป็นพื้นฐานในเรื่องของมาตรฐานการเอ็นคริปท์ชัน พัฒนาโดยองค์กรเอ็นไอเอสที (The National Bureau of Standard and Technology;NIST) ในปี พ.ศ. 2520 และในปี พ.ศ. 2537 องค์กรเอ็นไอเอสที ได้มีการการันตีให้ใช้ในราชการสหรัฐเป็นเวลา 5 ปี และแนะนำให้ใช้อัลกอริทึมเดสสำหรับโปรแกรมประยุกต์ มากกว่าการปกป้องการจัดเก็บข้อมูลรูปแบบการทำงานของอัลกอริทึมเดส แสดงดังรูปที่ 3.11 มี 2 อินพุท ในฟังก์ชันเอ็นคริปท์ชัน คือ เพลนเท็ก และคีย์ที่ใช้ในการเพลนเท็กมีความยาว 64 บิท และคีย์มีความยาว 56 บิทเพลนเท็กผ่านใน 3 ระยะอันดับแรกเพลนเท็ก 64 บิท ผ่านการทำเพอร์มิวเตชันเริ่มต้น (Initial Permutation; IP) แล้วจัดบิทต่างๆ ใหม่เป็นข้อมูลอินพุทที่ถูกเพอร์มิวแล้วการทำเพอร์

มิวเตชันเบื้องต้น ในแต่ละระยะประกอบด้วยการกระทำของฟังก์ชันที่เหมือนกัน 16 ขั้นเอาท์พุท ของการกระทำของฟังก์ชันลำดับที่ 16 ประกอบด้วย 64 บิท มาจากอินพุทของอินพุทเพลนเท็ก



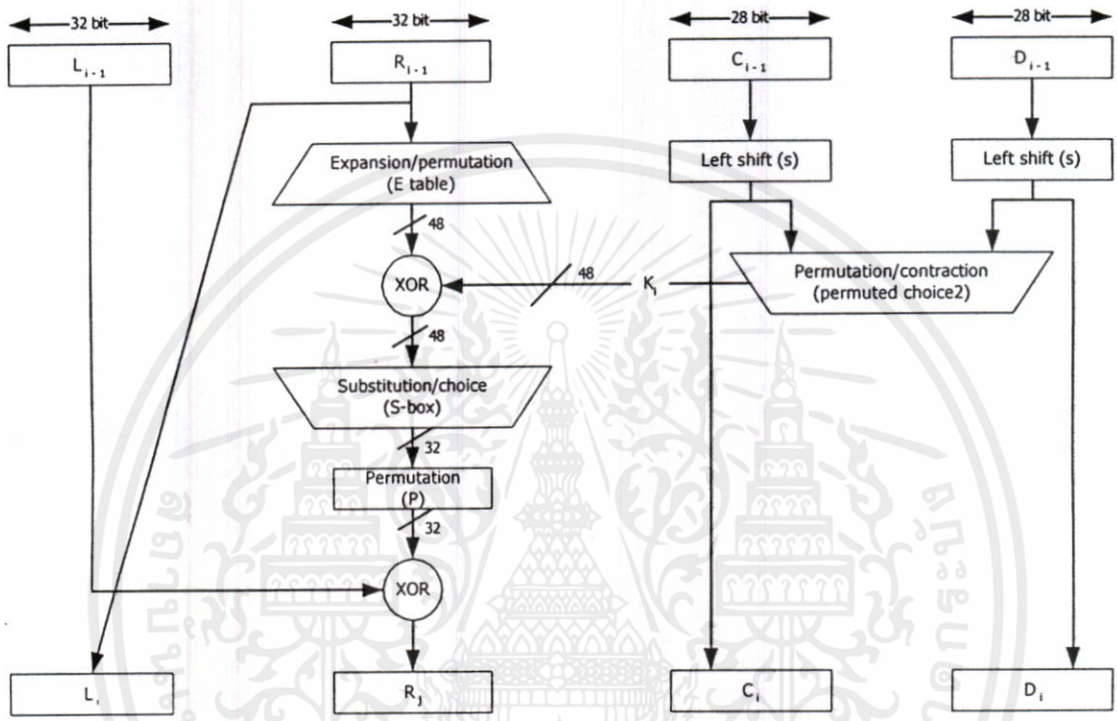
รูปที่ 3.11 อธิบายหลักของอัลกอริทึมเดส

และคีย์ เอาท์พุทครึ่งซีกซ้ายและขวา จะถูกเปลี่ยนเป็นพรีเอาท์พุท (pre-output) สุดท้ายพรีเอาท์พุทจะผ่านการเพอร์มิวเตชันอีกครั้ง (IP^{-1}) แต่เป็นการทำเพอร์มิวเตชันที่ตรงกันข้ามกับเพอร์มิวเตชันเริ่มต้น เพื่อจะได้ไซเฟอร์เท็กขนาดความยาว 64 บิท ด้านขวามือของรูปที่ 3.12 แสดงวิธีซึ่งใช้กับคีย์ 56 บิท เริ่มต้น คีย์จะถูกเพอร์มิวเตชัน ถัดจากนั้นสำหรับในแต่ละขั้นของ 16 ชั้น ซับคีย์ (Subkey; Ki) จะได้จากการรวมกันของการชิฟท์ซ้ายและการเพอร์มิวเตชันฟังก์ชันเพอร์มิวเตชันจะเหมือนกันในแต่ละขั้น แต่ซับคีย์ที่ได้จะมีค่าต่างกันเพราะว่ามีการชิฟท์ของบิทคีย์เดิมด้วย

อินพุท 64 บิท ที่ถูกเพอร์มิวเตชันจะผ่านการกระทำซ้ำ 16 รอบ แต่ละค่าของ 64 บิท จะถูกแบ่งเป็น 32 บิท เท่ากันทั้งซ้าย (L) และขวา (R) กระบวนการทั้งหมดในแต่ละขั้นจะสรุปได้สูตรสมการคือ

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, R_i)$$

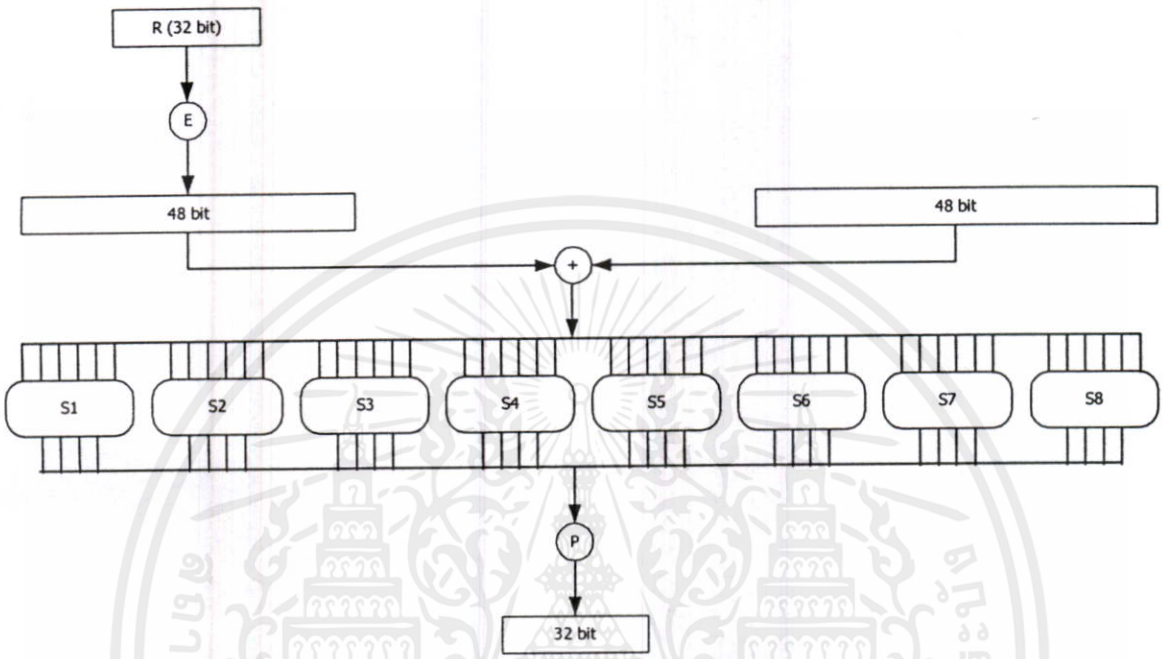


รูปที่ 3. 12 แสดงการการกระทำของอัลกอริทึมเดสเพียงขั้นเดียว

โดยที่ $\oplus$ คือ ฟังก์ชันเอ็กคลูซีฟออร์ (XOR)

ดังนั้น เอาท์พุททางซ้ายมือของการทำซ้ำ (L_i) จะเท่ากันกับอินพุทขวามือของการกระทำซ้ำ (R_{i-1}) เอาท์พุทขวามือ (R_i) คือเอ็กซ์คลูซีฟออร์ของ L_{i-1} กับการทำคอมเพล็กระหว่าง R_{i-1} และ K_i คอมเพล็กฟังก์ชันประกอบด้วยการทำทั้งเพอร์มิวเตชันและการกระทำแทนที่ การกระทำการแทนที่เรียกว่า S – boxes เป็นการทำให้ผลรวมของอินพุท 48 บิทกลายเป็น 32 บิท ย้อนกลับไปดูรูปที่ 3.11 การใช้คีย์ 56 บิท เป็นอินพุทของอัลกอริทึมขั้นแรกจะมีการเพอร์มิวเตชัน ผลที่ได้จากคีย์ 56บิท จะถูกแบ่งเป็น 28 บิท แล้วให้สัญลักษณ์ เป็น C_0 และ D_0 ในแต่ละขั้น C และ D จะมีการชิฟท์หมุนไปทางซ้ายหรือการหมุนใน 1 หรือ 2 บิท และเป็นการชิฟท์ค่าเพื่อเป็นอินพุทของรอบต่อไป ด้วยการเก็บไว้เป็นอินพุทของฟังก์ชันเพอร์มิวเตชัน ซึ่งให้เอาท์พุท 48 บิท เตรียมไว้เป็นอินพุทของฟังก์ชัน $f(R_{i-1}, K_i)$ กระบวนการดีคริปท์ชันด้วยอัลกอริทึมเดส จะคล้ายกันกับกระบวนการเอ็น-คริปท์ชัน หลักมีอยู่ว่าใช้ไซเฟอร์เท็กเป็นอินพุทของอัลกอริทึมเดส แต่ใช้คีย์ (K_i) เรียงลำดับตรงกันข้ามกับวิธีการเอ็นคริปท์ชันด้วยเหตุนี้ใช้ K_{16} เป็นการทำงานขั้นแรกตามด้วย K_{15} จนกระทั่งถึง K_1 ฟังก์ชัน

(f) แสดงได้ดังรูปที่ 3.13 อินเทอร์เรชันคีย์ (interationkey; K_I) มีค่าเท่ากับ48 บิท R อินพุทคือ 32 บิต K อินพุทจะถูกขยายเป็น 48 บิท จะถูกเอ็กคลูซีฟออร์กับค่า K_I และ48บิทที่ได้จะผ่านฟังก์ชันการแทนที่ทำให้ได้เอาท์พุท 32 บิทซึ่งจะถูกเพอร์มิวดังตารางที่ 3.1



รูปที่ 3.13 การคำนวณสำหรับ f(R,K)

การแทนที่จะรวบรวมชุดของ 8 เอสบล็อกโดยแต่ละบล็อกจะมีอินพุท 6 บิท และให้เอาท์-พุท 4 บิทการแปลงจะถูกกำหนดดังตารางที่ 3.1 ซึ่งบิทแรกและสุดท้ายของอินพุทไปถึงบล็อก S_I จากเลขฐานสอง 2 บิทจะถูกเลือกเป็นแถวดังแสดงในตารางสำหรับ S_I 4บิทกลางจะเลือกเป็นส่วนของคอลัมน์ ค่าตามเลขฐานสิบในเซลล์ที่ได้แถวและคอลัมน์ถัดจากนั้นจะถูกคอนเวิร์ทเป็น 4 บิท แสดงเป็นผลลัพธ์ของ เอาท์พุท ยกตัวอย่างใน S_Iที่มีอินพุทคือ 011011 แถว คือ 01 และคอลัมน์ คือ 1101 (คอลัมน์ 13) จะมีค่าเป็น 5 ดังนั้นจะกลายเป็นเอาท์พุทคือ 0101 รูปที่3.14 แสดงรายละเอียดสำหรับการกระทำเอสบล็อกที่ถูกแสดงเป็นแผนภาพ จะพบว่าคีย์ 56 บิท ที่ใช้เป็นอินพุทจะผ่านการเพอร์มิวเตชัน ดังตารางที่3.2 ผลที่ได้จากคีย์ 56บิท จะถูกแบ่งเป็น 2 ฝั่งคือข้างละ28 บิท เขียนสัญลักษณ์เป็น Co และ Do ในแต่ละการกระทำซ้ำ C และ D จะถูกแยกไปทำการชิฟท์ไปทางซ้ายหรือมีการหมุนเปลี่ยนบิตหรือ 2 บิทแสดงได้ดังตารางที่ 3.2 ค่าที่ได้จากการชิฟท์จะเป็นอินพุทของการผ่านกระบวนการซ้ำ

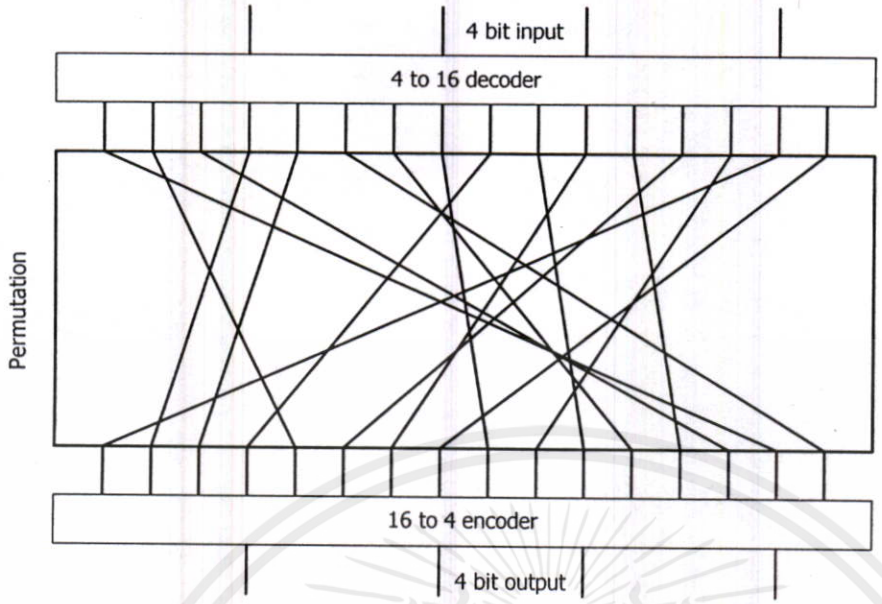
3.7.3 การดีคริปท์ชันเดส (DES Descryption)

กระบวนการดีคริปท์ชันของเดส เป็นกระบวนการที่สำคัญของดีคริปท์ชันมี กฎเกณฑ์ดังนี้

ตารางที่ 3.1 นิยามของเคสเอสบล็อก (S boxes)

Row	Column Number 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	Box
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	S_2
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S_3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	S_4
2	10	5	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	11	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	S_5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	S_6
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S_7
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	S_8
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

ใช้ไซเฟอร์เท็กเป็นอินพุท แต่จะใช้คีย์ที่มีการเรียงอินเวิร์สลำดับ จะใช้ K_{16} เป็นตัวแรกในการทำซ้ำ ตามด้วย K_{15} ตามลำดับจนครบครั้งที่ 16 สามารถดูการทำงานได้ดังรูปที่ 3.15 ซึ่งแสดงกระบวน



รูปที่ 3.14 รายละเอียดของเอสบล็อก

ตารางที่ 3.2 แสดงการใช้คีย์ DES

(a) Permuted Choice One (PC-1)

Output bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
From input bit	57	49	41	33	25	17	9	1	58	50	42	34	26	18
Output bit	15	16	17	18	19	20	21	22	23	24	25	26	27	28
From input bit	10	2	59	51	43	35	27	19	11	3	60	52	44	36
Output bit	29	30	32	32	33	34	35	36	37	38	39	40	41	42
From input bit	63	55	47	39	31	23	15	7	62	54	46	38	30	22
Output bit	43	44	45	46	47	48	49	50	51	52	53	54	55	56
From input bit	14	6	61	53	45	37	29	21	13	5	28	20	12	4

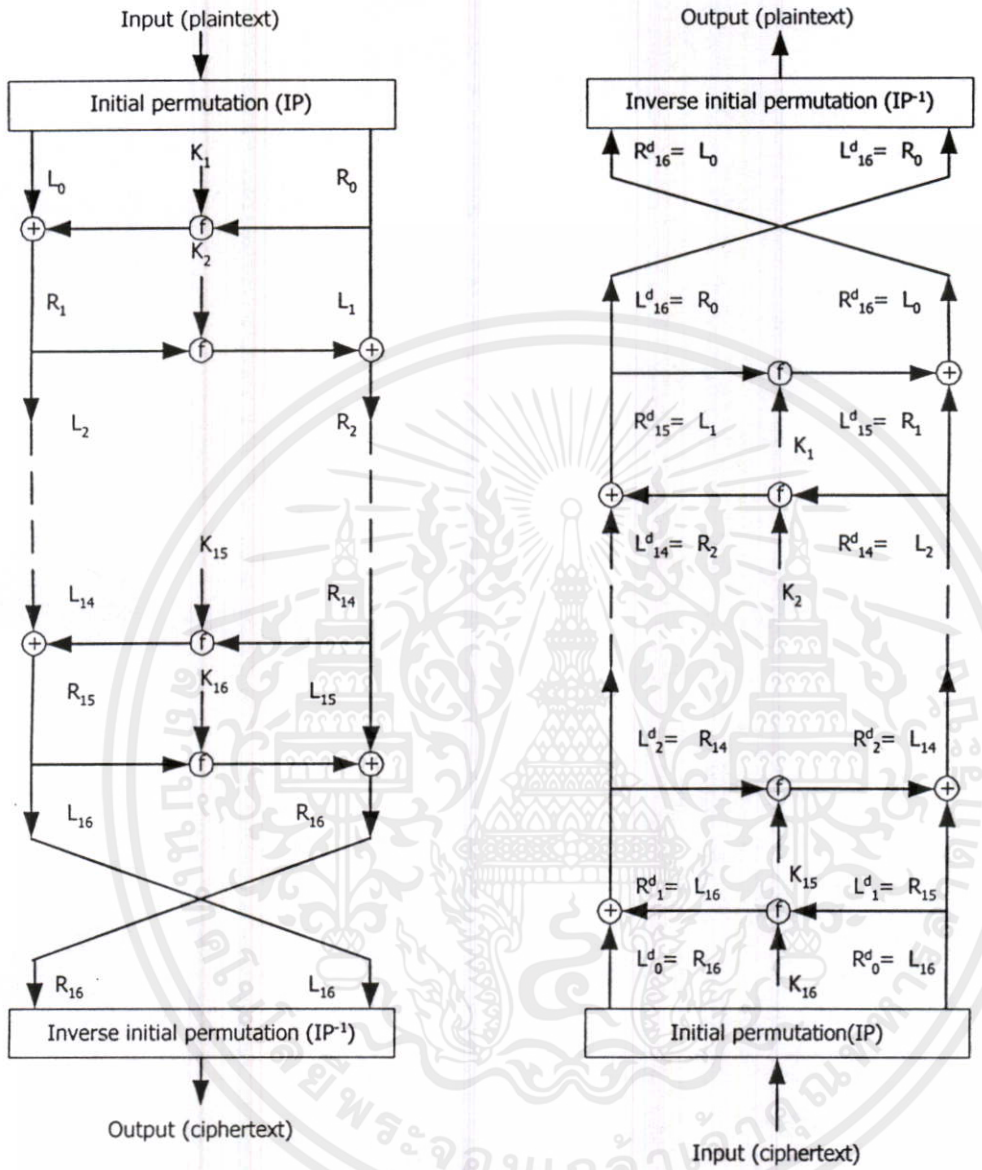
(b) Permuted Choice Two (PC-2)

Output bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
From input bit	14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
Output bit	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
From input bit	26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
Output bit	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
From input bit	51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

(c)Schedule of Left Shifts

Iteration number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

การเอ็นคริปท์ชัน รูปทางซ้ายเป็นกระบวนการเอ็นคริปท์ชันและทางขวาเป็นกระบวนการดิสคริปท์ชัน



รูปที่ 3.15 แสดงการเอ็นคริปท์ชัน และการดีคริปท์ชัน ของเดส

$$L^d_0 // R^d_0 = IP(\text{cipher text})$$

$$\text{Ciphertext} = IP^{-1}(R_{16} // L_{16})$$

จะได้ $L^d_0 // R^d_0 = IP(IP^{-1}(R_{16} // L_{16})) = R_{16} // L_{16}$

$$L_{16} = R_{15}$$

$$R_{16} = L_{15} \oplus f(R_{15}, K_{16})$$

ในฝั่งดีคริปท์ชัน

$$L^d_1 = R^d_0 = L_{16} = R_{15}$$

$$R^d_1 = L^d_0 \oplus f(R^d_0, K_{16})$$
$$= R_{16} \oplus f(R_{15}, K_{16})$$
$$= [L_{15} \oplus f(R_{15}, K_{16})] \oplus f(R_{15}, K_{16})$$

จากคุณสมบัติเอ็กซ์คลูซีฟท์ออร์

$$[A \oplus B] \oplus C = A \oplus [B \oplus C]$$
$$D \oplus D = 0$$
$$E \oplus D = E$$

จาก $L^d_1 = R_{15}$ และ $R^d_1 = L_{15}$

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

จัดรูปใหม่ได้

$$R_{i-1} = L_i$$
$$L_{i-1} = R_i \oplus f(R_{i-1}, K_i) = R_i \oplus f(L_i, K_i)$$

กระบวนการดีคริปท์ชันจะได้เป็น

$$IP^{-1}(Lo//Ro) = IP^{-1}(IP(plaintext)) = plaintext$$

3.7.4 โหมดการทำงานของอัลกอริทึมเดส (DES Modes of Operation)

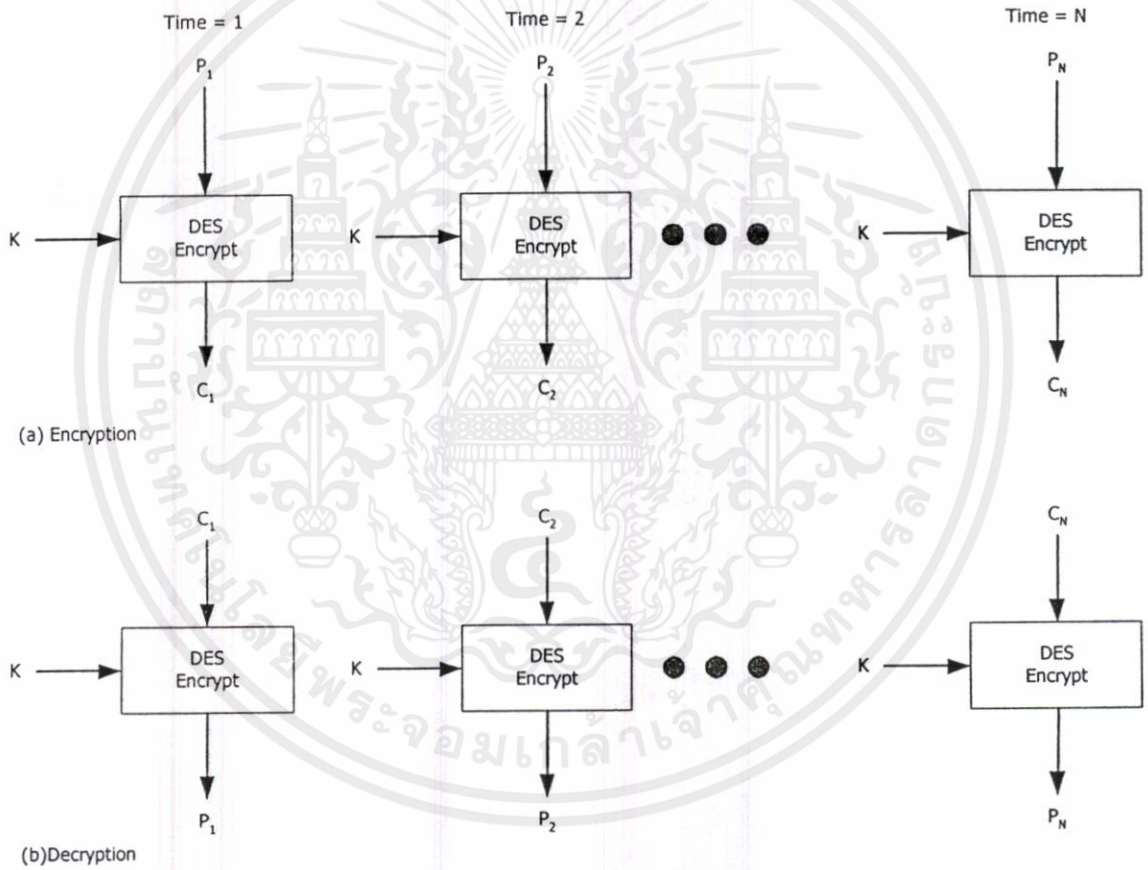
อัลกอริทึมเดสเป็นหลักพื้นฐานของการเอ็นคริปท์ชันและดีคริปท์ชันสำหรับการปกป้องข้อมูลให้มีความปลอดภัย สามารถสรุปการทำงานของอัลกอริทึมเดสได้ 4 โหมด ดังนี้

1. โหมดอีซีบี (Electronic Codebooh Modle; ECB)

เป็นโหมดพื้นฐานที่สุด ซึ่ง ข้อความธรรมดา 64 บิท แต่ละบล็อกของข้อความธรรมดาที่ถูกเอ็นคริปท์จะใช้คีย์เดียวกัน ดังรูปที่ 3.16 เทอมโค๊ดบุ๊ค จะถูกใช้เพราะว่ามีการให้ค่าคีย์ มีลักษณะเฉพาะไซเฟอร์เท็ก สำหรับทุกๆ 64 บิท บล็อกของข้อความธรรมดาสำหรับข้อความที่มีความยาวกว่า 64 บิท จะมี กระบวนการในการตัดให้ข้อความยาวแค่ 64 บิทการดีดรัปก์ชันจะถูกทำ 1 บล็อกใน 1 ครั้ง ปกติจะใช้คีย์เดียวกัน พบว่าข้อความธรรมดาประกอบด้วย บล็อก 64 บิท รวมกัน ซึ่งคือ $P_1, P_2, \ldots\ldots P_N$ตรงกันกับลำดับของบล็อกไซเฟอร์เท็ก คือ $C_1, C_2, \ldots\ldots C_N$ วิธีอีซีบีเป็นอุดมคติสำหรับปริมาณข้อมูลนั้น ๆ ยกตัวอย่างเช่น การเอ็นคริปท์ชันค่าคีย์ ดังนั้นถ้าต้องการส่งคีย์ด้วยอัลกอริทึมเดส จะทำให้มีความปลอดภัย ลักษณะที่สำคัญที่สุดของอีซีบี คือการทำให้มีข้อความธรรมดา เป็นบล็อกขนาด 64 บิท สำหรับข้อความยาวๆ โหมดอีซีบี อาจจะไม่ปลอดภัย เพราะข้อความยาวจะมีการบล็อกต่อเนื่องกัน ทำให้ คริปตานาไลท์ (Cryptanalyst) สามารถมองเห็นเป็นชุดเพลนเท็ก ไซเฟอร์เท็กมีโอกาสจะแทนที่หรือปรับเปลี่ยนได้

2. โหมดซีบีซี (Cipher Block Chaining Mode; CBC)

การแก้ข้อบกพร่องของอีซีบีจะมีการใช้เทคนิคในบล็อกเดียวข้อความเดียวกัน ถ้าซ้ำกันจะให้เป็นไซเฟอร์เท็ก บล็อกที่แตกต่างกัน วิธีนี้คือ โหมดซีบีซี (จากรูปที่ 3.17) ในแผนผังอินพุทในอัลกอริทึมเอ็นคริปท์ชัน จะทำเป็นเอ็กคลูซีฟท์ออร์ บล็อกข้อความธรรมดา ณ ปัจจุบัน กับ บล็อกไซเฟอร์เท็กก่อนหน้า ค่าคีย์ที่ใช้เดียวกันสำหรับแต่ละบล็อกผลที่ได้ ค่าอินพุทที่ผ่านฟังก์ชันเอ็น-ดริปท์ชันในแต่ละบล็อกข้อความธรรมดา จะไม่มีความสัมพันธ์กับบล็อกข้อความธรรมดาแล้วให้เห็น สำหรับการดีคริปท์ชัน แต่ละบล็อกไซเฟอร์ จะผ่านอัลกอริทึมดีคริปท์ชัน



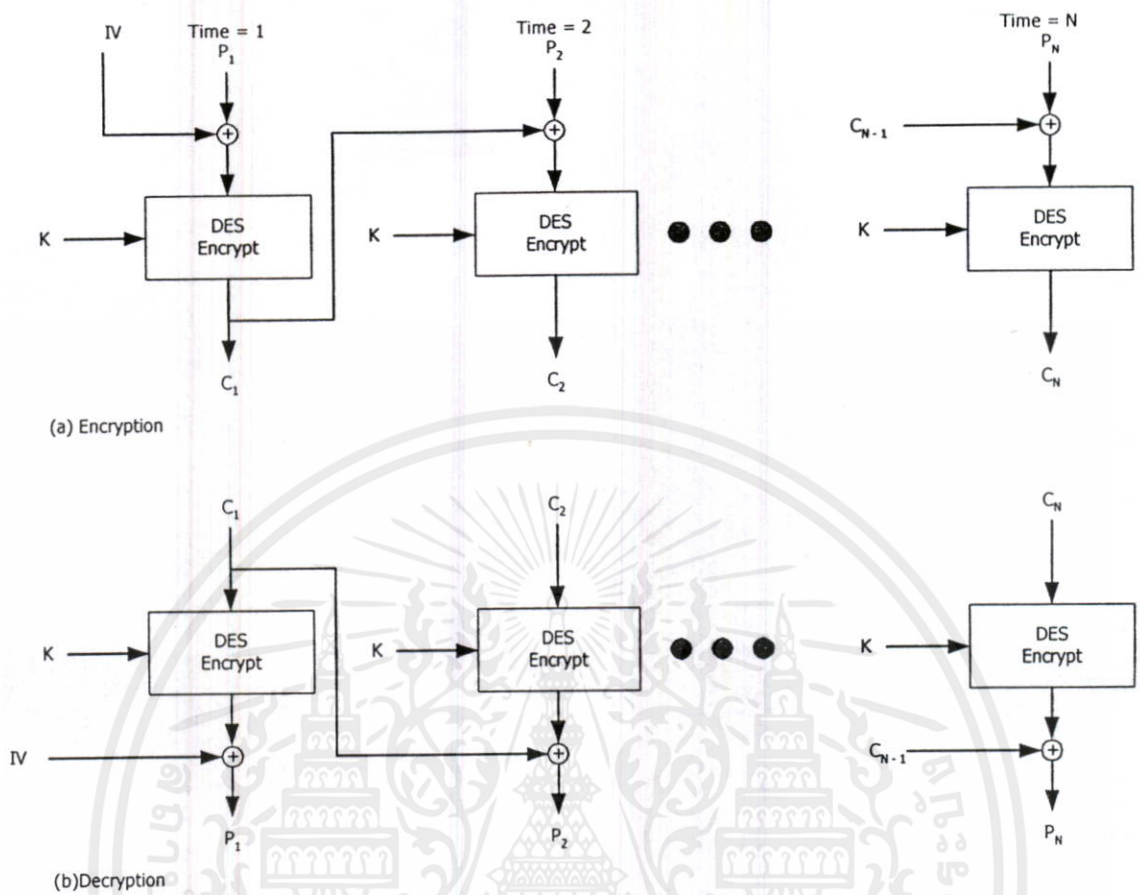
รูปที่ 3.16 แสดงโหมดอีซีบี

ผลที่ได้สามารถเขียนเป็นสมการ

$$C_n = E_k[C_{n-1} \oplus P_n]$$

แล้ว

$$D_k[C_n] = D_k[E_k(C_{n-1} \oplus P_n)]$$



รูปที่ 3.17 แสดงโหมดซีบีซี

$$D_K[C_n] = C_{n-1} \oplus P_n$$

$$C_{n-1} \oplus D_K[C_n] = C_{n-1} \oplus C_{n-1} \oplus P_n = P_n$$

ในการจะเกิดบล็อกไซเฟอร์เท็กแรกจะมีเวกเตอร์เริ่มต้น (Initialization Veotor; IV) ทำการเอ็กคลูซีฟกับบล็อกข้อความธรรมดาแรกในการดีคริปท์ชัน เวกเตอร์เริ่มต้นจะถูกเอ็กคลูซีฟออร์กับเอาท์พุทอัลกอริทึมดีคริปท์ชัน เพื่อทำให้ได้ บล็อกข้อความธรรมดาแรกกลับคืนมา เวกเตอร์เริ่มต้นต้องรู้ทั้งฝั่งรับและฝั่งส่ง สำหรับความปลอดภัยสูงสุด เวกเตอร์เริ่มต้นจะถูกปกป้องให้เสมือนเป็นการปกป้องค่าคีย์จึงต้องใช้การส่งเวกเตอร์เริ่มต้นผ่านเอ็นคริปท์ชันอีซีบี เหตุผลหนึ่งสำหรับการป้องกัน เวกเตอร์เริ่มต้น คือ ถ้าผู้ลักลอบสามารถเป็นผู้รับโดยการใช้ค่าที่แตกต่างของเวกเตอร์เริ่มต้น ผู้ลักลอบจะสามารถเลือกบิทในบล็อกแรกของข้อความธรรมดาได้

พิจารณาได้จาก

$$C_1 = E_K (IV \oplus P_1)$$

$$P_1 = IV \oplus D_K (C_1)$$

ปัจจุบันใช้การสังเกตุ X [i] แสดงบิทที่ I ของ X

$$P_I[i] = IV[i] \oplus D_K(C_I)[i]$$

ถัดไป การใช้คุณสมบัติ ของ XOR จะได้

$$P_I[i]' = IV[i]' \oplus D_K(C_I)[i]'$$

โดยที่ เครื่องหมายฝนตกจะแสดงถึงการคอมพลีเมนเตชัน หมายถึงว่าถ้าผู้ลักลอบสามารถทำนายการเปลี่ยน ค่าบิทต่าง ๆ ของเวกเตอร์เริ่มต้น ในทำนองเดียวกันบิทของค่าที่ได้รับของ P_I จะถูกเปลี่ยนแปลง สรุป การใช้ ซีบีซี เป็นโหมดที่เหมาะสมกับความที่ยาวกว่า 64 บิท

3. โหมดซีเอฟบี (Cipher Feed Book Mode; CFB)

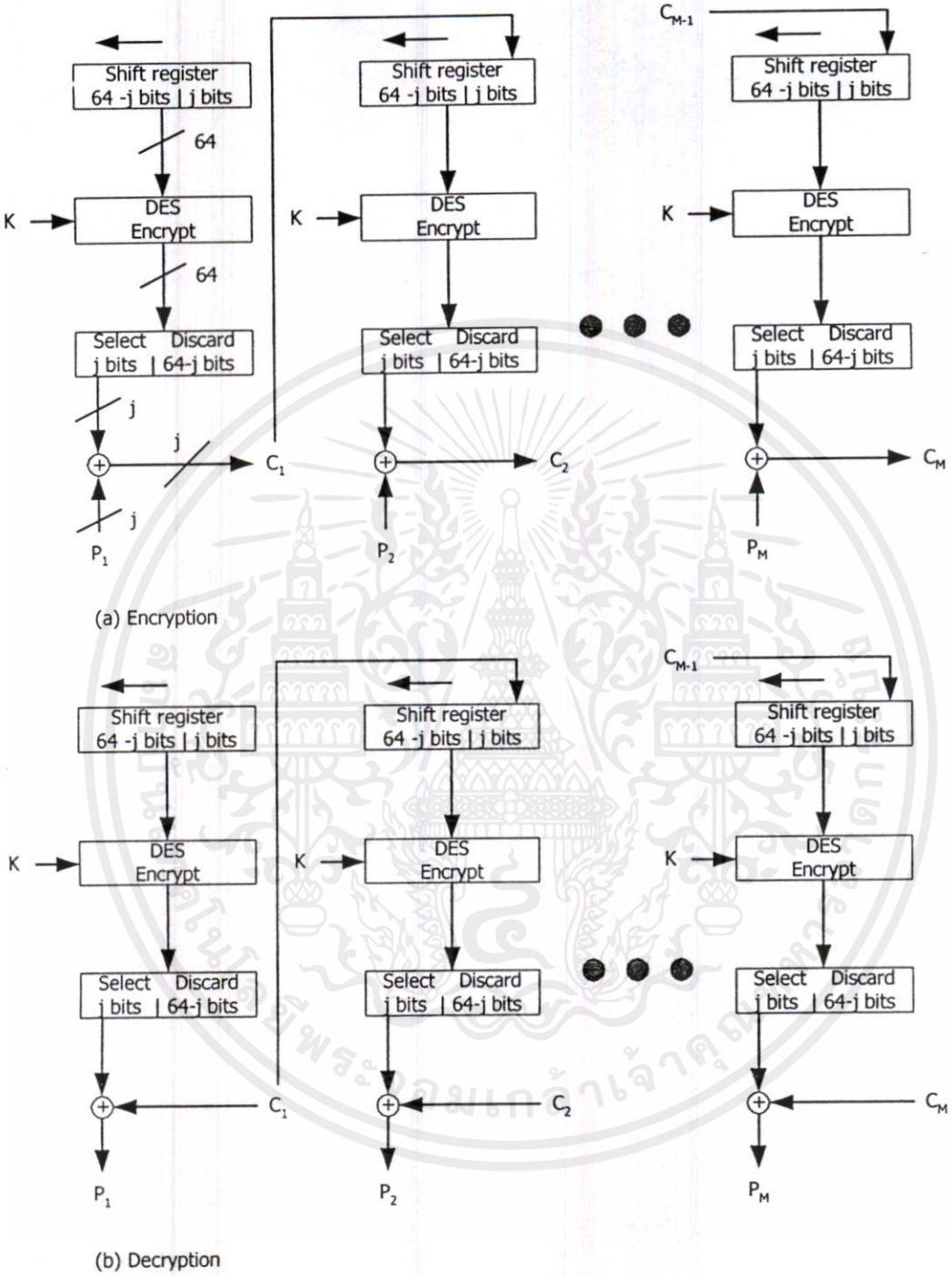
โหมดนี้จะใช้บล็อกไซเฟอร์ขนาด 64 บิท/บล็อก มีความเป็นไปได้ที่จะแปลงเดสไปเป็นสตรีมไซเฟอร์ (Stream cipher) การใช้ทั้งไซเฟอร์ฟีดแบ็ค หรือโหมดเอาท์พุทฟีดแบ็ค สตรีมไซเฟอร์ จะลดเวลาในการใส่ แพ็ดแมสเสจ (Pad message) เมื่อต้องการให้สามารถหาบล็อกต่อ ๆ กัน ได้มีการทำงานแบบเรียวไทม์ (real time) ดังนั้น ถ้ามีคาแรคเตอร์สตรีม (character stream) จะถูกส่งโดยแต่ละคาแรคเตอร์ตัวจะถูกเอ็นคริปท์อย่างต่อเนื่องกัน และส่งทันทีโดยการใช้สตรีมไซเฟอร์รูปแบบแต่ละคาแรกเตอร์เป็นคุณสมบัติหลักของสตรีมไซเฟอร์ จะเป็นไซเฟอร์ที่มีความยาวเดียวกันกับเพลนเท็ก ตัวอย่างเช่น ถ้าตัวอักษรขนาด 8 บิทจะถูกส่งตัวอักษรแต่ละตัวอักษรจะถูกเอ็นคริปท์โดยใช้ขนาด 8 บิท จากรูปที่ 3.18 แสดงผังของโหมดซีเอฟบี สมมติตัวแปรในการส่งเป็น j บิท ค่าปกติคือ j = 8 ขั้นแรก พิจารณาการเอ็นคริปท์ชัน อินพุทฟังก์ชันเอ็นคริปท์จะเป็น 64 บิท ชิฟท์รีจีสเตอร์จะเริ่มตั้งค่าเวคเตอร์เริ่มต้น (initialization Vector; IV) การดีคริปท์ชั่นจะมีผังเหมือนกัน แต่การรับไซเฟอร์จะถูกเอ็กซ์ครูซีฟออร์ กับเอาท์พุทของฟังก์ชันเมื่อจะสามารถแปลงเป็นเพลนเท็ก สามารถสรุปเป็นสมการได้คือ

$$C_I = P_I \oplus S_jE(IV)$$

ดังนั้น $$P_I = C_I \oplus S_jE(IV)$$

4. โหมดโอเอฟบี (Output Feedback Mode; OFB)

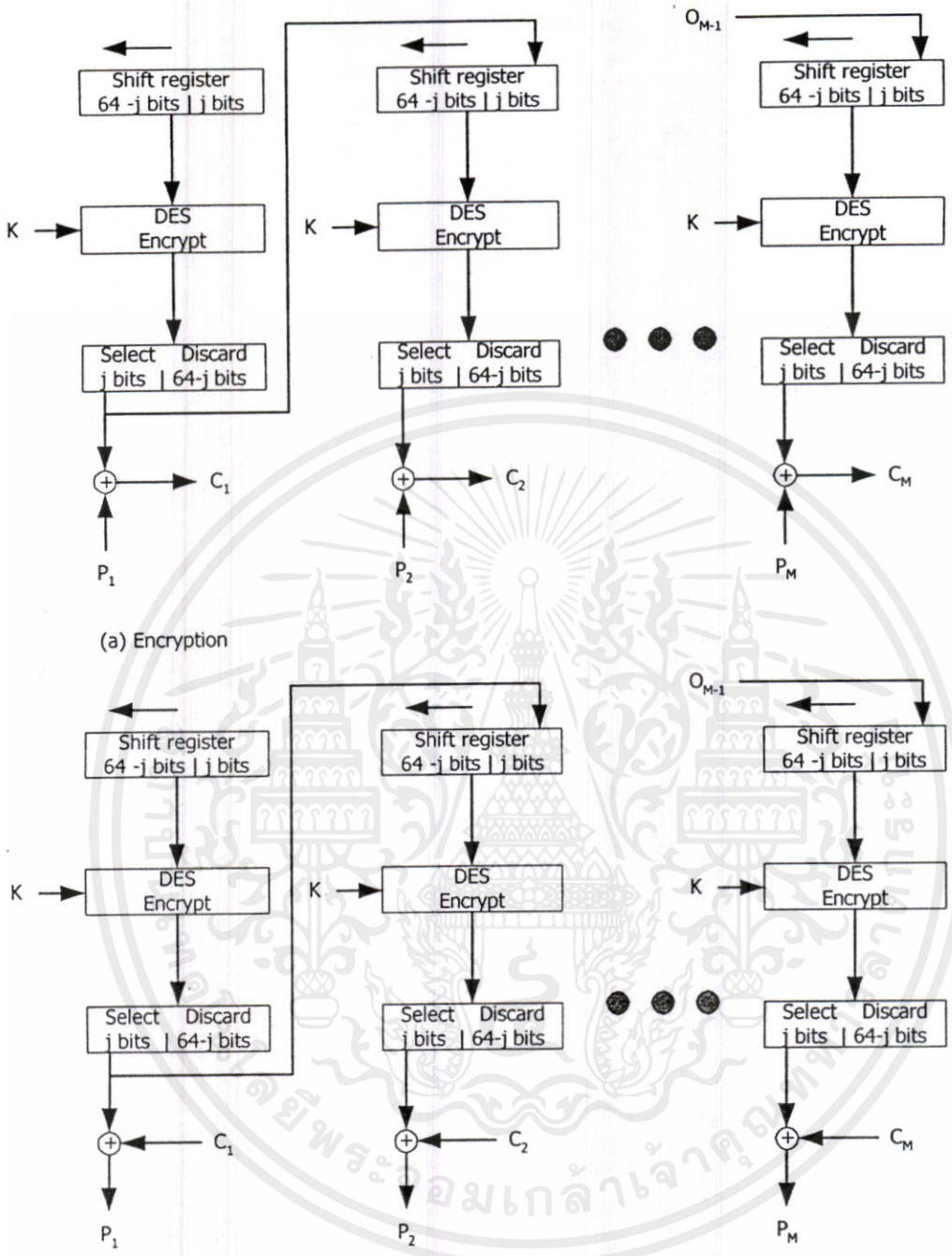
โหมดนี้คล้ายกันซีเอฟบี แสดงได้ดังรูปที่ 3.19 ค่าที่เอาท์พุทที่ได้เป็นไซเฟอร์จะถูกป้อนกลับไปที่ซีฟทรีซิสเตอร์ ข้อดีหนึ่งของ วีธีโอเอฟบี (OFB) บิทที่ผิดพลาดในการส่งข้อมูล จะไม่ส่งออกไป ยกตัวอย่างถ้าบิทผิดพลาดใน C_I จะมีผลเฉพาะค่าการแก้ที่ P_I เท่านั้น ลำดับถัดมา เพลนเท็ก จะไม่ถูกตัดด้วยซีเอฟบี, C_I จะสงวนเอาท์พุทเท่านั้นในการซีฟท์รีซิสเตอร์ และนี่คือการป้องกันการหยุดล่าข้อมูล



รูปที่ 3.18 แสดงผังโหมดซีเอฟบี

3.7.5 อัลกอริทึมทริปเปิ้ลเดส (Triple DES)

รูปแบบพื้นฐานที่สุดของการเอ็นคริปท์ชันหลายครั้งจะมีการเอ็นคริปท์ชัน 2 ครั้ง และคีย์ที่ใช้ในการเอ็นคริปท์ชันมี 2 คีย์ (ดังรูปที่ 3.20) กำหนดให้เพนเท็ก (P) คีย์เอ็นคริปท์ชัน K1 และ K2



รูปที่ 3.19 โหมดโอเอฟบี

ไซเฟอร์เท็ก (C) จะเขียนเป็นสมการ

$$C = E_{K2}[E_{K1}[P]]$$

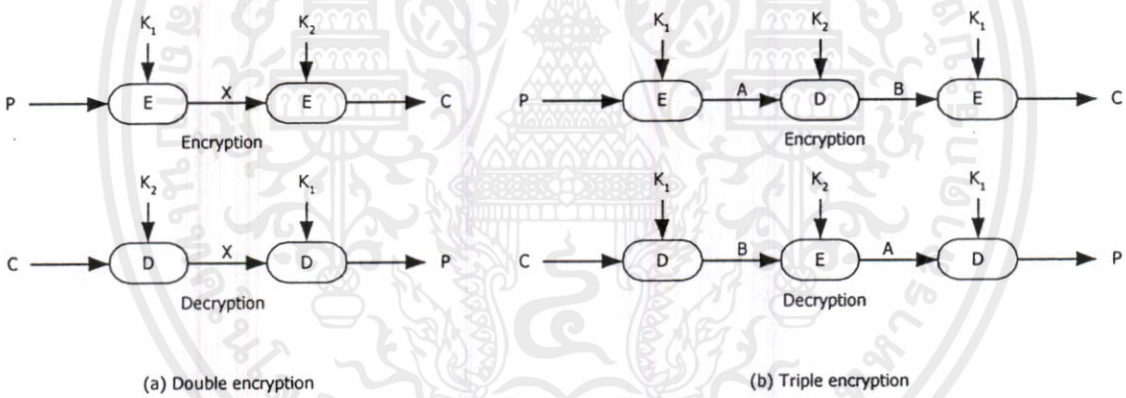
การดีคริปท์ชันจะต้องการคีย์เรียงลำดับตรงกันข้าม จะได้

$$P = D_{K1}[D_{K2}[C]]$$

จากรูปที่ได้คีย์จะมีความยาวเท่ากับ 56 x 2 = 112 บิท ผลที่ได้ทำให้เพิ่มความแข็งแกร่งให้กับคริปโตกราฟี ทริปเปิ้ลเดส เป็นอัลกอริทึมเดสที่ใช้คีย์ มากกว่า 1 ขึ้นไป ในการเอ็นคริปท์ชัน ซึ่งทำให้อัลกอริทึมเดสมีความปลอดภัยมากยิ่งขึ้น มีวิธีการทำทริปเปิ้ลเดส ได้ดังนี้

- DES-EEE3 ใช้อัลกอริทึมเดสทำงาน 3 รอบด้วยคีย์ที่ใช้ในการเอ็นคริปท์ชันแตกต่างกันทั้ง 3 รอบ
- DES-EDE3 ใช้คีย์ในการเอ็นคริปท์ชันแตกต่างกัน 3 รอบ แต่กระบวนการในการเอ็นคริปท์ชันจะใช้ เอ็นคริปท์ แล้ว ดีคริปท์ ถัดจากนั้นจะใช้เอ็นคริปท์อีกครั้ง
- DES-EEE2 การทำงานเหมือน DES-EEE3 แต่กระบวนการเอ็นคริปท์ชันจะใช้คีย์เหมือนกันทั้ง 3 รอบ
- DES-EDE2 การทำงานคล้ายกับ DES-EDE2 แต่ในรอบที่ 1 และ 3 จะใช้คีย์ที่เหมือนกัน

ในกระบวนเอ็นคริปท์ชันของทริปเปิ้ลเดส จึงมีความปลอดภัยมากกว่าอัลกอริทึมเดสมาก และยังจะเป็นอัลกอริทึมที่นิยมใช้ในอนาคตด้วย



รูปที่ 3.20 การเอ็นคริปท์ชันหลายครั้ง

ทริปเปิ้ลเดส กับการใช้ 2 คีย์

ทัชแมนเสนอวิธีการเอ็นคริปท์ชันทริปเปิ้ล โดยการใช้แค่ 2 คีย์เท่านั้น ฟังก์ชันจะมีลักษณะดังรูปที่ 3.20

$$C = E_{K1}[D_{K2}[E_{K1}[P]]]$$

3.7.6 อาร์ซี 2 (RC2)

อาร์ซี 2 เป็นไซเฟอร์บล็อกที่มีการทำงานเหมือนกันกับอัลกอริทึมเดส แต่ขนาดคีย์สามารถมีได้หลายขนาด อาร์ซี (RC) มาจาก Rivest 's Code ซึ่งเป็นชื่อผู้ค้นพบวิธีนี้ หรือ Ron Rivest of RSA Data Security ขนาดบล็อกเป็น 64 บิทและอัลกอริทึมนี้เร็วกว่าเดส ประมาณ 2-3 เท่า เมื่อ

ทดสอบโดยใช้ซอฟแวร์ ตั้งแต่ประเทศสหรัฐ เข้มงวดในการส่งออกอัลกอริทึมเอ็นคริปท์ชันว่าต้องเป็น 40 บิทเท่านั้น นักประดิษฐ์จึงได้ใช้อัลกอริทึมอื่นในการทำเป็นสินค้าส่งออกแทน ซึ่งปัจจุบันมีความสนใจในการนำอาร์ซี 5 มาใช้งาน

3.7.7 อาร์ซี 5 (RC5)

อาร์ซี 5 มีวิธีการทำงานเหมือนกันกับวิธีอัลกอริทึมเดส แต่มีความแตกต่างจากอัลกอริทึมอาร์ซีอื่น ในเรื่องของความสามารถในการใช้ขนาดบล็อก ขนาดคีย์ และจำนวนรอบที่แตกต่างกันได้หลายขนาด อาร์ซี 5 สามารถใช้

1. ขนาดบล็อกได้ 32, 64 หรือ 128 บิท
2. ขนาดคีย์อยู่ในช่วง 0 ถึง 2048 บิท
3. จำนวนรอบได้ตั้งแต่ 0 ถึง 255 รอบ

จึงถือว่าเป็นไซเฟอร์บล็อกที่เร็วชนิดหนึ่ง และเนื่องจากสามารถใช้ขนาดบล็อก 64 บิทได้จึงทำให้แทนที่อัลกอริทึมเดสได้ จากเหตุผลที่มีความคล่องตัวในการกำหนดขนาดที่แตกต่างกันได้ จึงทำให้ อาร์ซี5 เป็นอัลกอริทึมที่สำคัญมาก การกำหนดค่าซับคีย์ขึ้นอยู่กับผู้ใช้งานสามารถกำหนดได้และจำนวนซับคีย์ทั้งหมด แปรผันตามจำนวนรอบในการทำงานของอัลกอริทึมนี้ การเอ็นคริปท์ชันของ RC5 จะประกอบด้วยการกระทำทางคณิตศาสตร์ที่ซ้ำๆ กัน คือ การบวกเลข การเอ็กคลูซีฟ-ออร์ และการหมุนที่เปลี่ยนแปลง จะพบว่าการทำงานทางคณิตศาสตร์ของอาร์ซี5 นั้นง่ายในการนำไปใช้งานจริง [8] ประกอบกับสามารถตรวจสอบความถูกต้องได้

3.7.8 แฮสฟังก์ชัน (Hash Function)

แฮสฟังก์ชันเป็นการทำให้ข้อความที่มีความยาวแตกต่างกัน สามารถมีผลลัพธ์ที่มีความยาวสตริงคงที่ ปกติจะใช้ 128 บิท หรือมากกว่า แฮสฟังก์ชันเป็นวิธีหนึ่งที่ทำให้ยากในการที่จะแปลงข้อความเดิมกลับมาจากไซเฟอร์เท็ก การเปลี่ยนแแปลงรหัสการให้สิทธิข้อความที่ได้รับกำลังเป็นที่น่าสนใจขณะนี้ คือ วิธีหนึ่งของฟังก์ชันแฮสเสมือนกับว่ารหัสในการให้สิทธิผู้ใช้ดูข้อความ หรือเรียกว่า การออเทนทิเคชัน ฟังก์ชันแฮสจะรับข้อความที่มีขนาดเปลี่ยนแปลงเป็นอินพุท และให้ค่ารหัสแฮสขนาดคงที่ (H(M)) บางครั้งเรียกว่า การทำให้เป็นข้อความย่อยๆ เป็นเอาท์พุท รหัสแฮสจะเป็นฟังก์ชันของทุกบิทของข้อความและจัดเตรียมความสามารถในการตรวจจับความผิดพลาดความเปลี่ยนแปลงที่เกิดขึ้นกับบิทใดๆ จะมีผลต่อรหัสแฮส จากรูปที่ 3.21 แสดงวิธีต่างๆ ซึ่งใช้รหัสแฮสเพื่อเตรียมการให้สิทธิข้อความ ค่าจะถูกจัดอยู่ในรูปฟังก์ชันแฮส (Hash function)

$$h = H(M)$$

โดยที่ M คือ ความยาวข้อความที่เปลี่ยนแปร

H(M) คือ ค่าฟังก์ชันแฮสของความยาวที่คงที่

ค่าแฮสจะถูกเพิ่มลงในข้อความ ณ เวลา เมื่อข้อความสมมติถูกส่งถึงฝั่งรับทำการให้สิทธิข้อความนั้นโดยการคำนวณค่าแฮสอีกครั้ง เพราะว่าฟังก์ชันแฮสไม่ได้ถูกทำให้เป็นความลับ จึงต้องมีการป้องกันค่าแฮสความต้องการสำหรับฟังก์ชันแฮสที่ใช้สำหรับการให้สิทธิข้อความ จุดประสงค์ของฟังก์ชันแฮส คือ การผลิตการยืนยันสิทธิ เสมือนเป็นการตรวจสอบลายนิ้วมือของไฟล์ ข่าวสาร หรือบล็อกข้อมูล เพื่อใช้สำหรับการให้สิทธิข่าวสารของผู้ใช้งาน ฟังก์ชันแฮส ต้องมีคุณสมบัติดังนี้

1. H สามารถถูกประยุกต์ใช้กับบล็อกข้อมูลทุกๆขนาด
2. H ผลิตเอาท์พุทความยาวคงที่
3. H (x) คือ ความสัมพันธ์อย่างง่ายในการคำนวณค่าใดๆ ของ x สามารถทำได้ทั้งฮาร์ดแวร์และซอฟแวร์
4. สำหรับรหัสใดๆ ที่ให้ (m) สามารถคำนวณค่า x จากสมการ $H(x) = m$
5. สำหรับบล็อก x ใดๆ จะคำนวณเพื่อหาค่า y ที่ไม่ท่ากับ x ซึ่ง $H(y) = H(x)$
6. การคำนวณสามารถหาคู่ลำดับ (x,y) จาก $H(x) = H(y)$

ฟังก์ชันแฮสทั้งหมดทำงานโดยการใช้หลักการทั่วไป ดังนี้

อินพุท (ข้อความ ไฟล์ อื่นๆ) จะถูกแสดงเสมือนลำดับของบล็อก n บิท อินพุทจะผ่านกระบวนการบล็อกหนึ่ง ณ เวลาหนึ่ง ในช่วงการทำซ้ำหนึ่งเพื่อผลิตหนึ่งฟังก์ชันแฮส n บิทหนึ่งในฟังก์ชันแฮสง่ายที่สุด คือ การที่บิทต่อบิทเอ็กคลูซีฟออร์ของทุกๆ บล็อกสามารถสรุปได้เป็น

$$C_i = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{im}$$

โดยที่

C_i = บิทที่ I ของรหัสแฮส โดย $1 \leq I \leq N$

m = จำนวนบล็อก n บิทในอินพุท

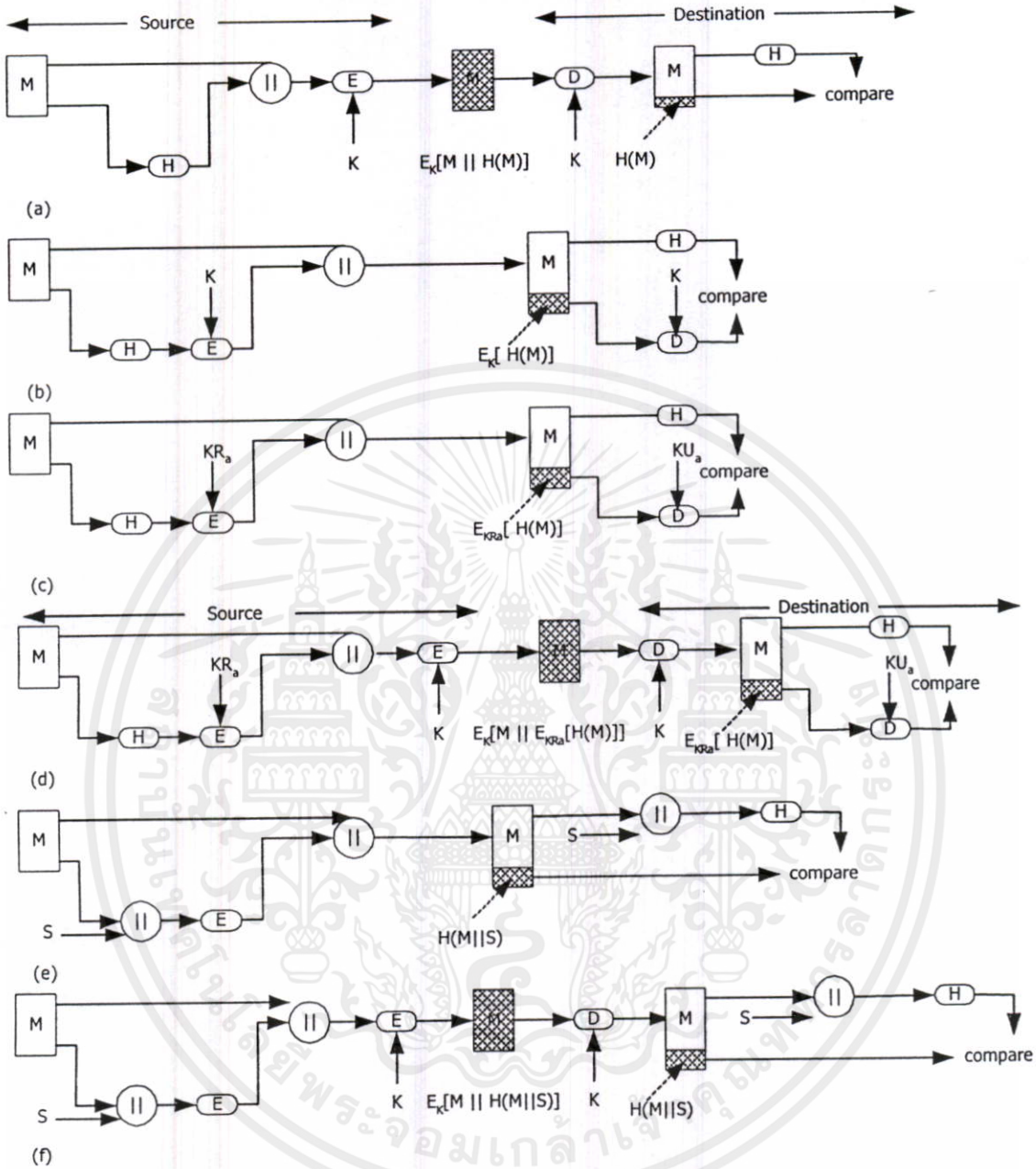
b_{ij} = บิทที่ I ในบล็อกที่ J

$\oplus$ = การทำเอ็กซ์คลูซีฟออร์

จากรูปที่ 3.22 แสดงการทำงานจะทำให้เกิดพาริตี้บิทหนึ่งสำหรับแต่ละบิทด้วยประสิทธิภาพสำหรับการสุ่มข้อมูลเสมือนการตรวจสอบควมถูกต้อง ข้อมูลแต่ละค่าแฮสของ n บิท จะมีค่าเกือบเท่ากัน ดังนั้น ความน่าจะเป็นที่ข้อมูลผิดพลาดจะเป็นผลในค่าแฮสที่ไม่เปลี่ยนแปลง คือ 2^{-n} ยกตัวอย่างถ้าใช้ค่าแฮสหนึ่ง 128 บิท จะแทนว่าความมีประสิทธิภาพของ 2^{-128}

วิธีพื้นฐานปรับปรุงการทำงานการชิฟท์หนึ่งบิทหรือการหมุนเวียนบนค่าแฮสหลังจากที่แต่ละบล็อกผ่านกระบวนการ กระบวนการสามารถเขียนสรุปได้

1. เริ่มต้นการเซ็ตค่าแฮส n บิทเป็นศูนย์
2. กระบวนการแต่ละบล็อก n บิทของข้อมูล ดังนี้
   2.1 การหมุนค่าแฮสปัจจุบันไปทางซ้าย 1 บิท

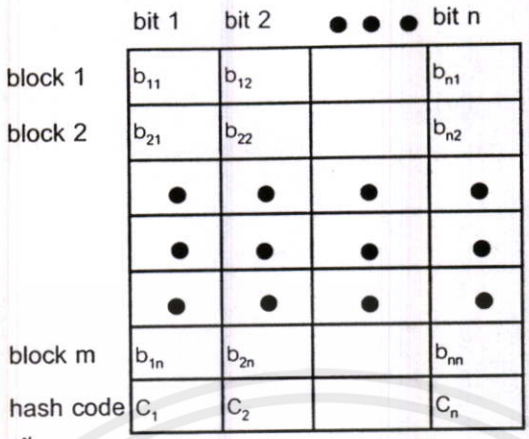


รูปที่ 3.21 พื้นฐานการใช้งานฟังก์ชันแฮส

2.2 เอ็กซ์คลูซีฟออร์บล็อกเข้าไปที่ค่าแฮส

3.7.9 เอสเอชเออัลกอริทึม (Secure Hash Algorithm; SHA และ SHA-1)

เอสเอชเออัลกอริทึม (SHA) พัฒนาโดย รัฐบาลสหรัฐ SHA-1 ถูกนำออกใช้ในปีพ.ศ. 2537 จะใช้ความยาวของอักษร และแยกย่อยข้อความขนาด 160 บิท ซึ่งทำให้ช้ากว่าแฮสฟังก์ชันอื่นๆ แต่จุดเด่นคือเรื่องความปลอดภัยที่มีขนาดความยาวบิทมากกว่า อัลกอริทึมเอสเอชเอ (Secure Hash Algorithm; SHA) ถูกพัฒนาโดย องค์กรเอ็นไอเอสที การทำงานของเอสเอชเอ อัลกอริทึมนี้จะใช้ข้อ



รูปที่ 3.22 ฟังก์ชันแฮสพื้นฐานโดยการใช้บิทเอ็กซ์คลูซีฟออร์

ความอินพุท ความยาวสูงสุดไม่เกิน 2^{64} บิท และให้เอาท์พุทข้อความย่อยๆ 160 บิทอินพุทที่ผ่านกระบวนการอยู่ในบล็อกขนาด 512 บิท แสดงดังรูปที่ 3.23 กระบวนการประกอบด้วยขั้นตอนดังนี้

ขั้นตอนที่ 1 เพิ่มบิทแพดดิ่ง

ข้อความจะถูกแพดจนกระทั่งมีความยาวเท่ากันกับ 448 modulo 512 หรือ 448 mod 512 แพดดิ่งจะถูกเพิ่มเสมอจนกว่าข้อความจะมีความยาวเท่าที่ต้องการ ดังนั้น จำนวนบิทแพดดิ่งจะอยู่ช่วง 1-512 แพดดิ่งประกอบด้วย บิท 1 บิท ตามด้วยบิท เท่าที่จำเป็น

ขั้นตอนที่ 2 เพิ่มความยาว

บล็อกขนาด 64 บิท จะถูกเพิ่มเข้าข้อความ บล็อกนี้จะถูกทำ 64 บิท ที่ยังไม่ถูกจอง และประกอบด้วยความยาวข้อความเริ่มต้น (ก่อนการแพดดิ่ง) ผลที่ได้ของครั้งแรกใน 2 ขั้นตอน จะเป็นข้อความที่เป็นจำนวนเต็ม คูณด้วย 512 บิท จะกลายเป็นความยาวข้อความในรูป แสดงการขยายข้อความเรียงตามลำดับ ขนาดบล็อก 512 บิท $Y_0, Y_1 \ldots . Y_{L-1}$ จนกระทั่งความยาวทั้งหมดคือ Lx512 บิท ในทำนองเดียวกันถ้าผลลัพธ์ที่ได้คูณ 16 เป็นเวิร์ด 32 บิท M[O....N] แสดงเวิร์ด ผลลัพธ์ของข้อความ โดย N คือ เลขจำนวนเต็ม คูณด้วย 16 จะได้สูตรเป็น

$$N = LX16$$

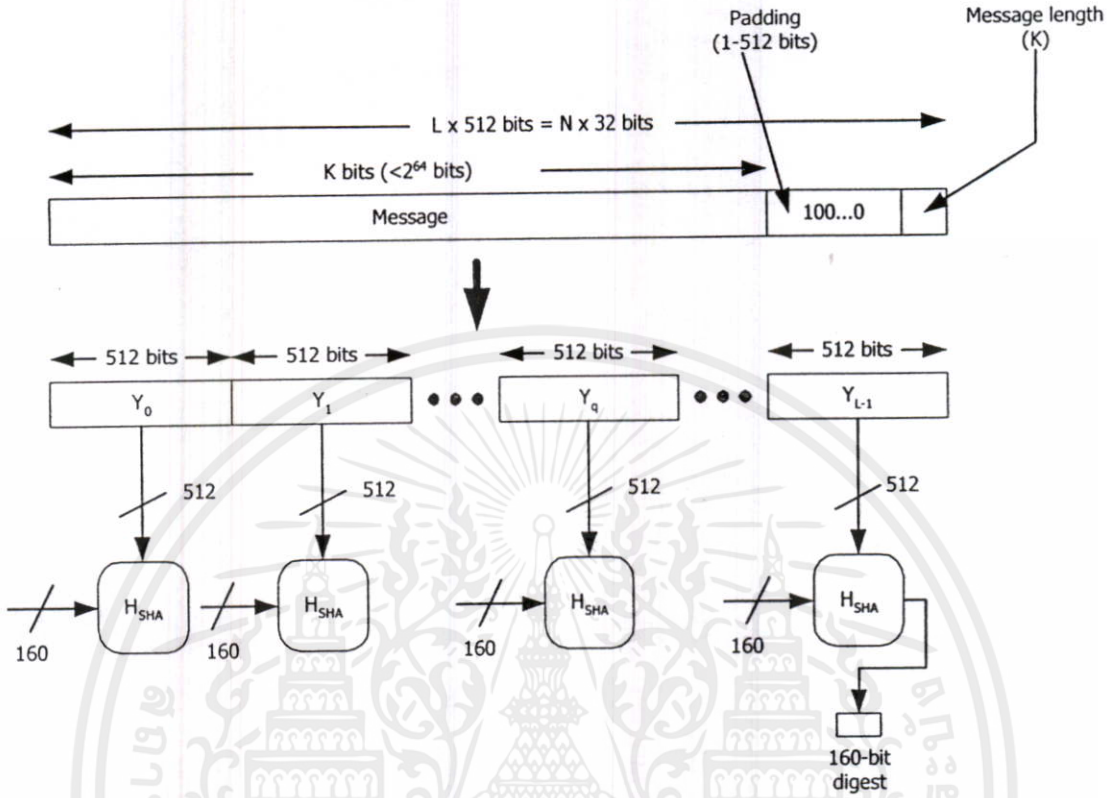
ขั้นตอนที่ 3 การเริ่มต้น บัฟเฟอร์ MD

บัฟเฟอร์หนึ่งขนาด 160 บิท จะถูกใช้ระหว่างกลางทาง และผลลัพธ์สุดท้ายของฟังก์แฮส บัฟเฟอร์จะถูกแสดง รีจีสเตอร์ 5 ตัว ขนาด 32 บิท (A,B,C,D,E) รีจีสเตอร์ เหล่านี้ จะมีค่าเป็นเลขฐานสิบหก (เรียงลำดับที่ละ 8)

A=67452301

B=EFCDAB89

C=98BADCFE



รูปที่ 3.23 การทำให้เกิดข้อความย่อยโดยใช้เอสเอชเอ

D=10325476

E=C3D2E1FO

สังเกตุได้ว่าสี่ตัวแรกมีค่าต่างๆ เหมือน MD5 แต่เรียงสลับไม่เหมือนกัน

ขั้นตอนที่ 4 กระบวนการ ข้อความในบล็อกขนาด 512 บิท (16เวิร์ด)

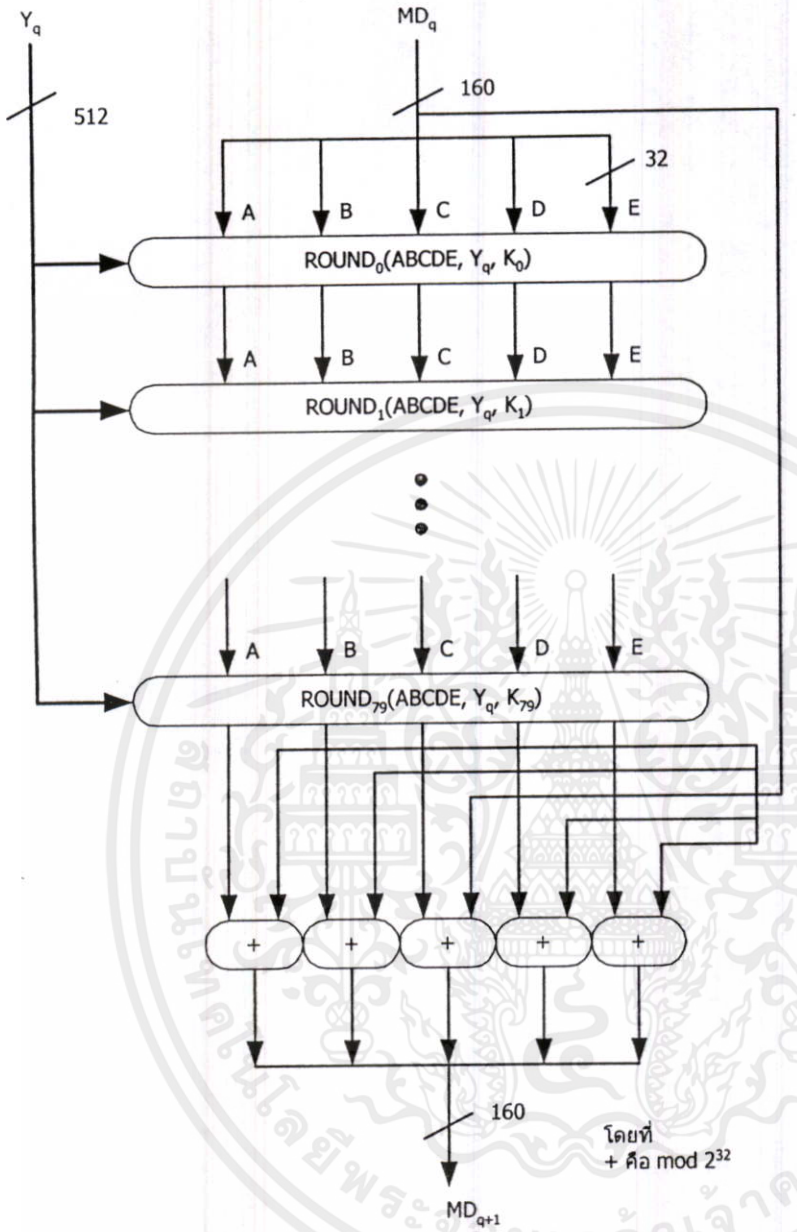
หัวใจของอัลกอริทึม คือ หนึ่งโมดูล ประกอบด้วย 80 ขั้นตอนในกระบวนการนี้ โมดูลนี้มีสัญลักษณ์ H_{SHA}ในรูปที่ 3.23 และตรรก ถูกแสดงดังรูปที่ 3.24 80 ขั้นตอนมีโครงสร้างคล้ายกัน อธิบายได้ดังนี้ สังเกตแต่ละรอบที่ทำกับอินพุทขนาดบล็อก 512 บิท ผ่านกระบวนการ (Yg) และบัฟเฟอร์ 160 บิทมีค่า ABCDE และทำการอัพเดทข้อมูลในบัฟเฟอร์ แต่ละรอบจะใช้การเพิ่มค่าคงที่ (Kt) ความเป็นจริงค่าคงที่ที่ใช้มี 4 ค่า ดังนี้

$O \leq t \leq 19$ K_t=5A827999

$20 \leq t \leq 39$ K_t=6ED9EBA1

$40 \leq t \leq 59$ K_t=8F1BBCDC

$60 \leq t \leq 79$ K_t=CA62C1D6

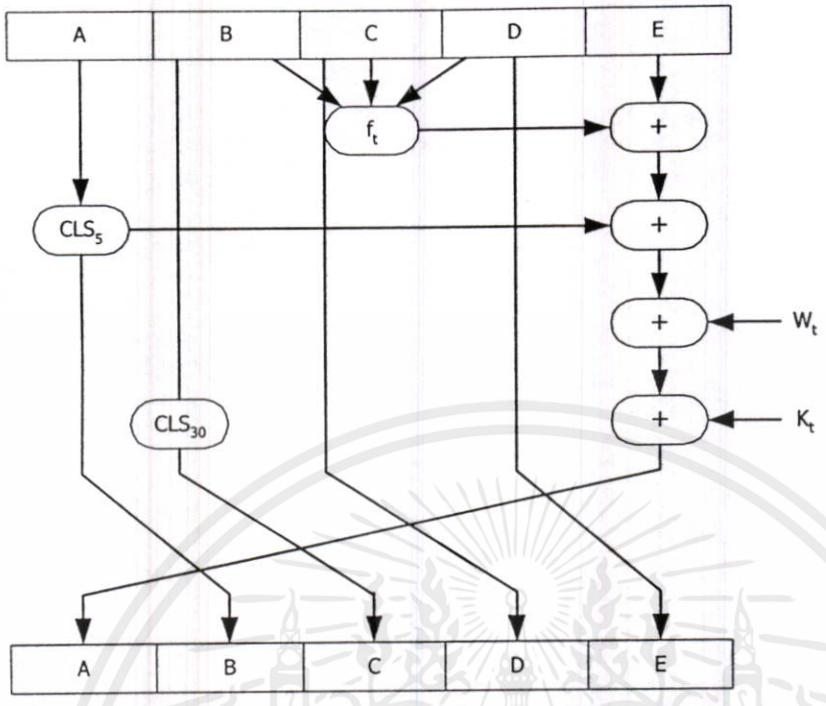


รูปที่3.24 กระบวนการเอสเอชเอของบล็อกหนึ่งขนาด 512 บิท (H_{SHA})

Y_g และ MD_g เสมือนเป็นอินพุท MD_g ถูกแทนที่ในบัฟเฟอร์ ABCDE เอาท์พุทของขั้นตอนที่ 80 จะถูกเพิ่ม MDg ไปเป็น MD_{g+1} การเพิ่มชึ้นจาก modulo 2^{32}

ขั้นตอนที่ 5 เอาท์พุท

บล็อกขนาด 512 บิท ทั้งหมดผ่านกระบวนการ จนกระทั่งถึงลำดับที่ L จะเป็นข้อความย่อยขนาด 160 บิท สามารถดูรายละเอียดเรื่องตรรกในแต่ละรอบของ 80 รอบ ของกระบวนการบล็อกหนึ่งขนาด 512 บิทแต่ละรอบจะอยู่ในรูปที่ 3.26



รูปที่ 3.25 การกระทำ SHA อย่างพื้นฐาน

$$A,B,C,D,E \leftarrow (CLS_5(A)+f_t(B,C,D)+E+W_t+K_t),A,CLS_{30}(B),C,D$$

โดยที่

A,B,C,D,E	คือ 5 คำของบัฟเฟอร์
t	คือ รอบ เป็นตัวเลขที่ $0 \leq t \leq 79$
f_t	คือ ฟังก์ชันตรรกพื้นฐาน
CLS_s	คือ การชิฟท์วนซ้าย (หมุน) ของแต่ละบิทใน 32 บิท
W_t	คือ เวิร์ด 32 บิท ได้มาจากบล็อกอินพุท 512 บิท
K_t	คือ การเพิ่มค่าคงที่ ค่าค่งที่ทั้งสี่ กำหนดดังที่กล่าวมาแล้ว
+	คือ การเพิ่ม modulo 2^{32}

แต่ละฟังก์ชันพื้นฐานทำให้ 3 เวิร์ด (32 บิท) เสมือนเป็นอินพุทและให้เอาท์พุทเวิร์ด 32 บิท แต่ละฟังก์ชันจะกระทำทางตรรกในระดับบิท แสดงดังตารางที่ 3.3

ตารางที่ 3.3 สรุปการกระทำทางตรรก

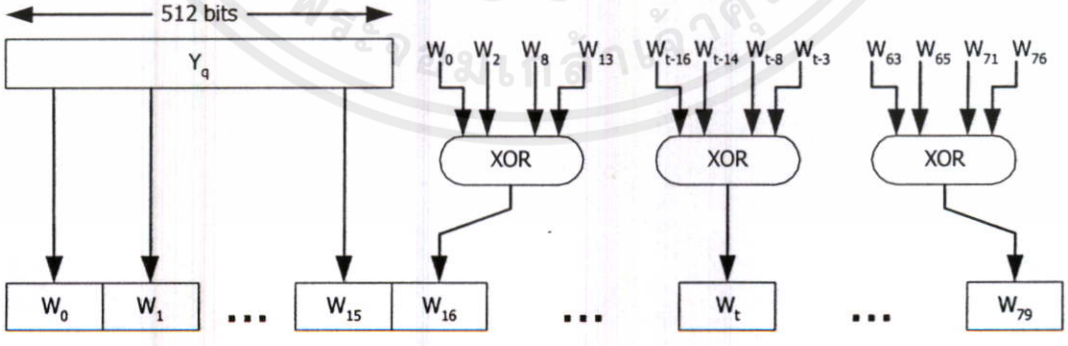
รอบ	f_t(B,C,D)
O ≤t≤19	(B.C)V(B.D)
20 ≤t≤39	B⊕C⊕D
40 ≤t≤59	(B.C)V(BD)V(C.D)
60 ≤t≤79	B⊕C⊕D

แสดงเป็น

ตารางที่ 3.4 แสดงค่าความจริงของฟังก์ชันตรรกสำหรับเอสเอชเอ

b	c	d	$f_{0..19}$	$f_{20..39}$	$f_{40..59}$	$f_{60..79}$
0	0	0	0	0	0	0
0	0	1	1	1	0	1
0	1	0	0	1	0	1
0	1	1	1	0	1	0
1	0	0	0	1	0	1
1	0	1	0	0	1	0
1	1	0	1	0	1	0
1	1	1	1	1	1	1

จากรูปที่ 3.26 แสดงแผนผัง 16 ค่าแรกของ W_t จะถูกทำโดยตรงจาก 16 เวิร์ด ของบล็อกขณะนั้น ค่าต่างๆสามารถถูกกำหนดได้ดังนี้



$$W_t = W_{t-16} \oplus W_{t-14} \oplus W_{t-8} \oplus W_{t-3}$$

รูปที่ 3.26 การสร้างอินพุท 80 เวิร์ดตามลำดับสำหรับกระบวนการเอสเอชเอของหนึ่งบล็อก

ดังนั้น สามารถสรุป การกระทำของเอสเอชเอได้เป็น

$MD_o = IV$

$MD_{g+1} = SUM_{32}(MD_g, ABCDE_g)$

$MD = MD_{L-1}$

โดยที่

IV = ค่าเริ่มต้นของบัฟเฟอร์ ABCDE กำหนดในขั้นที่ 3

$ABCDE_g$ = เอาท์พุทของรอบสุดท้ายของกระบวนการทำงานของบล็อกข้อความที่ g

L = จำนวนบล็อกในข้อความ (รวมการแพดดิ่งและความยาว)

SUM_{32} = การเพิ่ม modulo 2^{32} การกระทำแยกจากแต่ละเวิร์ดของคู่ของอินพุท

MD = ค่าข้อความย่อยสุดท้าย

3.7.10 เอ็มดี 5 (MD5; Message Digest Algorithim)

การทำงานของเอ็มดี 5 อัลกอริทึมนี้จะให้ข้อความอินพุทบล็อกขนาด 512 บิท กลายเป็นข้อความย่อย ๆ เอาท์พุท 128 บิทจากรูปที่ 3.27 แสดงกระบวนการทั้งหมดในการทำงาน มีขั้นตอนดังนี้

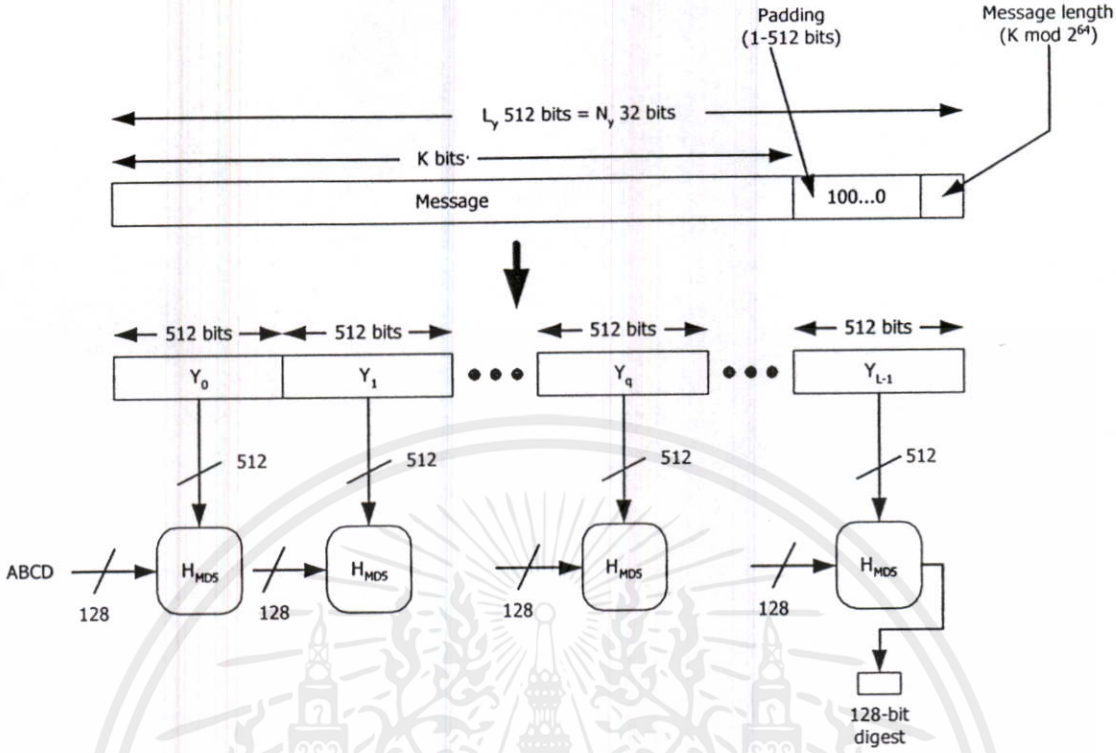
ขั้นที่ 1 การเพิ่มบิทแพดดิ่ง

ข้อความที่ถูกแพดจะมีความยาว $\equiv 448 \bmod 512$

ยกตัวอย่าง ถ้าข้อความมีความยาว 448 บิท จะถูกแพดโดย 512 บิท จะได้ความยาวเป็น 960 บิท จำนวนของแพดดิ่งบิทจะอยู่ในช่อง 1 ถึง 512 บิท จากรูปที่ 3.28 ข้อความที่ถูกขยายออกจะเป็นบล็อกขนาด 512 บิท คือ $Y_0, Y_1, \ldots, Y_{2-1}$ ดังนั้นความยาวทั้งหมดของข้อความจะเท่ากับ 2×512 บิท ทำนองเดียวกัน ผลที่ได้คูณด้วย 16 จะเป็นเวิร์ด 32 บิท

ขั้นที่ 2 การเพิ่มความยาว

64 บิทจะเป็นความยาวของข้อความเริ่มต้น (ก่อนจะแพดดิ่ง) ถ้าความยาวข้อความเริ่มต้นมากกว่า 2^{64} ถัดจากนั้น จะใช้ 2 ลำดับ ของความยาวมีความข้อความ 64 บิทที่จะใช้ ดังนั้น ความยาวข้อความเริ่มต้นจะเป็น Modulo 2^{64} ผลที่ได้จากทั้ง 2 ขั้นตอน จะเป็นเลขจำนวนเต็มที่คูณด้วย 512 บิท จากรูป ข้อความที่ถูกขยายออกจะเป็นบล็อกขนาด 512 บิท คือ $Y_0, Y_1, \ldots, Y_{l-1}$ ดังนั้นความยาวทั้งหมดของข้อความจะเท่ากับ $L \times 512$ บิท ทำนองเดียวกัน ผลที่ได้คูณด้วย เวิร์ด 32 บิท



รูปที่ 3.27 การใช้เอ็มดี 5

ขั้นที่ 3 จุดเริ่มต้นบัฟเฟอร์ MD

128 บิท บัพเฟอร์จะถูกใช้ ระหว่างนั้นและสิ้นสุดผลของฟังก์ชันแฮส (Hash Function) บัฟเฟอร์จะถูกแสดงเป็นรีอีสเตอร์ 32 บิท 4 ตัว (A B C D) รีอีสเตอร์เหล่านี้จะเป็นเลขฐาน 16

A = 01234567

B = 89ABCDEF

C = FEDCBA98

D = 76543210

ขั้นที่ 4 กระบวนการข้อความบล็อก 512 (16 เวิร์ด)

หัวใจของอัลกอริทึมจะเป็นโมดูลที่ประกอบด้วย 4 รอบของกระบวนการ โมดูลจะแสดงเป็นสัญลักษณ์ H_{MD5} ในรูปที่ 3.27 จะแสดงในเชิงตรรกดังรูปที่ 3.28 จำนวน 4 รอบ จะมีโครงสร้างคล้ายกัน แต่จะมีการใช้ฟังก์ชันตรรกที่แตกต่างกัน โดยใช้สัญลักษณ์ F G H และ I เป็นการเฉพาะในรูปฟังก์ชันทั้ง 4 เป็นสัญลักษณ์ f_F f_G f_H และ f_I ในแต่ละรอบจะใช้อินพุทบล็อกขนาด 512 บิท (Y_q) บัฟเฟอร์ A B C D ขนาด 128 บิท และอินเดทข้อมูลภายในบัฟเฟอร์แต่ละรอบจะเป็น 1 ใน 4 ของ 64 ตัวเลือก ดังตาราง T (1...64) ที่สร้างขึ้นจากฟังก์ชันไซน์ ลำดับที่ i ของ T แสดงได้เป็น T [i]มีค่าเท่ากับส่วนเลขจำนวนเต็มของ $2^{32} \times \text{abs}(\sin(i))$ โดยที่ i มีค่าเป็นเรเดียน abs(sin(i)) จะมีค่าอยู่ระหว่างเลข 0 และ 1 แต่ละตัวใน T เป็นตัวเลขจำนวนเต็มแสดงในรูป 32 บิท ตารางที่ได้จัดแจงแบบสุ่มค่าของแบบ 32 บิท แสดงได้ดังรูปตารางที่ 3.4

ขั้นที่ 5 เอาท์พุท

หลังจาก L ขนาดบล็อก 512 บิท ทั้งหมดผ่านกระบวนการ ค่าเอาท์พุทจากลำดับที่ 2 จะมีข้อความย่อยเป็น 128 บิท สามารถดูรายละเอียดได้จากตรรกในแต่ละรอบของกระบวนการ ซึ่งแสดงได้ดังรูปที่ 3.29

$$a \leftarrow b+CLS_s(a+g(b,c,d) + X[k] + T[i])$$

โดยที่

a , b , c , d คือ 4 เวิร์ดของบัฟเฟอร์

g คือ ฟังก์ชันหนึ่งของฟังก์ชัน

CLS_s คือ การชิฟท์วนขวา (การหมุน) ของ 32 บิท

X[k] คือ M[9×16+k]= ลำดับที่ k เวิร์ด 32 บิท ในลำดับที่ 9 บล็อก ขนาด 512 บิทของข้อความ

T[i] คือ ลำดับที่ i เวิร์ด 32 บิทในรูปแบบเมตริกซ์ T

t คือ ลำดับการเพิ่ม modulo 2^{32}

ฟังก์ชันสามารถสรุปได้เป็นดังตารางที่ 3.6

ตารางที่ 3.5 แสดงส่วนประกอบของ คีย์ของเอ็มดี 5

(a) ตารางค่าความจริงของฟังก์ชันตรรก

b	c	d	F	G	H	I
0	0	0	0	0	0	1
0	0	1	1	0	1	0
0	1	0	0	1	1	0
0	1	1	1	0	0	1
1	0	0	0	0	1	1
1	0	1	0	1	0	1
1	1	0	1	1	0	0
1	1	1	1	1	1	0

(b) ตาราง T ถูกสร้างจากฟังก์ชัน sine

T[1]	= D76AA478	T[17]	= F61E2562	T[33]	= FFFA3942	T[49]	= F4292244
T[2]	= E8C7B756	T[18]	= C040B340	T[34]	= 8771F681	T[50]	= 432AFF97
T[3]	= 242070DB	T[19]	= 265E5A51	T[35]	= 69D96122	T[51]	= AB9423A7
T[4]	= C1BDCEEE	T[20]	= E9B6C7AA	T[36]	= FDE5380C	T[52]	= FC93A039
T[5]	= F57C0FAF	T[21]	= D62F105D	T[37]	= A4BEEA44	T[53]	= 655B59C3
T[6]	= 4787C62A	T[22]	= 02441453	T[38]	= 4BDECFA9	T[54]	= 8F0CCC92
T[7]	= A8304613	T[23]	= D8A1E681	T[39]	= F6BB4B60	T[55]	= FFEFF47D
T[8]	= FD469501	T[24]	= E7D3FBC8	T[40]	= BEBFBC70	T[56]	= 85845DD1
T[9]	= 698098D8	T[25]	= 21E1CDE6	T[41]	= 289B7EC6	T[57]	= 6FA87E4F
T[10]	= 8B44F7AF	T[26]	= C33707D6	T[42]	= EAA127FA	T[58]	= FE2CE6E0
T[11]	= FFFF5BB1	T[27]	= F4D50D87	T[43]	= D4EF3085	T[59]	= A3014314
T[12]	= 895CD7BE	T[28]	= 455A14ED	T[44]	= 04881D05	T[60]	= 4E0811A1
T[13]	= 6B901122	T[29]	= A9E3905	T[45]	= D9D4D039	T[61]	= F7537E82
T[14]	= FD987193	T[30]	= FCEFA3F8	T[46]	= E6DB99E5	T[62]	= BD3AF235
T[15]	= A679438E	T[31]	= 676F02D9	T[47]	= 1FA27CF8	T[63]	= 2AD7D2BB
T[16]	= 49B40821	T[32]	= 8D2A4CBA	T[48]	= C4AC5665	T[64]	= EB86D391

ตารางที่ 3.6 สรุปผลของฟังก์ชัน

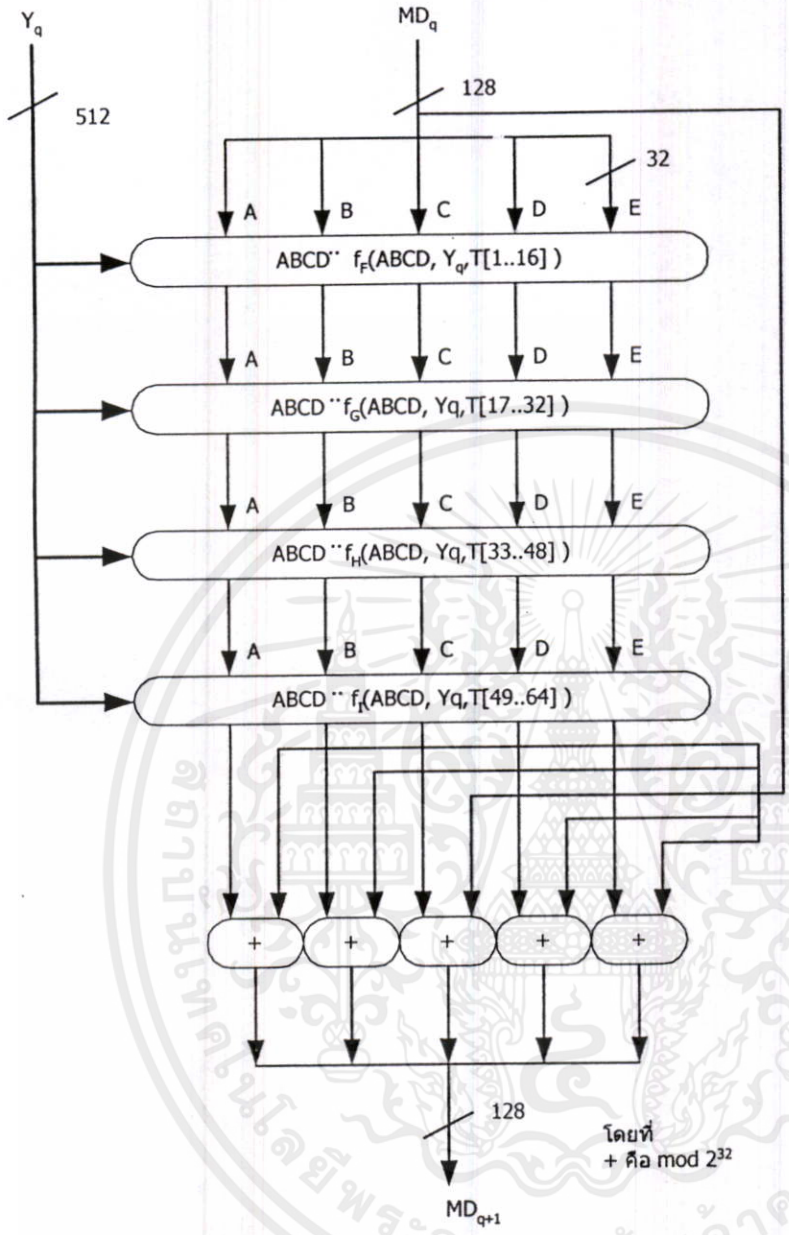
รอบ	พริมิทีฟฟังก์ชัน	g(b,c,d)
f_F	F (b,c,d)	(b.c)v(b.d)
f_G	G (b,c,d)	(b.d)v(c.d)
f_H	H (b,c,d)	b⊕c⊕d
f_I	I (b,c,d)	c⊕(b.d)

3.7.11 เอ็มดี 5 คีย์

เอ็มดี 5 คีย์ เป็นการประยุกต์ใช้เอ็มดี 5 สำหรับการออเทนทิเคชัน ซึ่งเป็นมาตรฐาน RFC 1828 ในการทำงานของเอ็มดี 5 จะทำที่แพ็กเก็ตโดยมีการเพิ่มคีย์ที่เป็นความลับของแหล่งที่ส่งในแพ็กเก็ต เมื่อถึงปลายทาง จะมีวิธีในการคำนวณเหมือนตอนเริ่มต้นที่บนแพ็กเก็ตที่ได้รับเข้ามารวมกันกับคีย์ที่เป็นความลับ และเปรียบเทียบค่าที่ได้ ด้วยวิธีดังกล่าวทำให้มีการออเทนทิเคชัน และมั่นใจข้อมูลถึงผู้มีสิทธิเท่านั้นจริง การคำนวณเอ็มดี 5 จะเป็น

key, keyfill, IP packet, key, MD5 fill

โดยที่



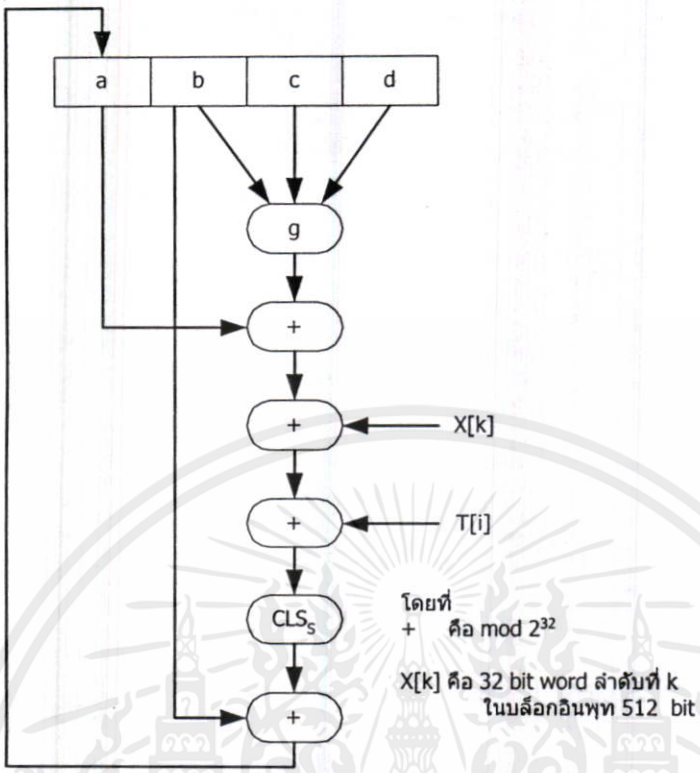
รูปที่ 3.28 แสดงกระบวนการของ MD5 สำหรับบล็อกเดียวขนาด 512 บิท

key คือ คีย์ลับสำหรับการป้องกัน

keyfill คือ การแพดดิ้ง จนกระทั่ง key รวมกับ keyfill แล้วมีความยาวเท่ากับค่าของเลขจำนวนเต็มคูณด้วย 512 บิท

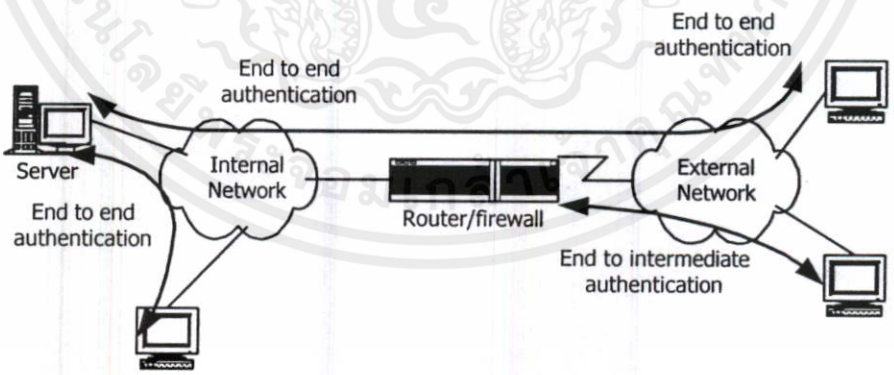
IP packet คือ ด้วยความเหมาะสมจะถูกตั้งค่าให้เป็นศูนย์

MD5 fill คือ การแพดดิ้งโดยเอ็มดี 5 จนกระทั่งความยาวทั้งหมดของบล็อกเท่ากับค่าเลขจำนวนเต็มคูณด้วย 512 บิท



รูปที่ 3.29 ส่วนประกอบของการกระทำทางคณิตศาสตร์เอ็มดี 5

ในการทำการวิจัยครั้งนี้จะใช้เอ็มดี 5 คีย์เป็นการออเทนทิเคชันไอพี เพื่อให้ข้อมูลมีความปลอดภัย ทั้งส่วนของข้อมูล และมั่นใจได้ว่าผู้ที่รับเป็นผู้ที่มีสิทธิในการรับข้อมูลได้จริง ซึ่งสามารถแสดงได้ดังรูปที่ 3.30



รูปที่ 3.30 แสดงการใช้ออเทนทิเคชันเอนทูเอน (end to end) เปรียบเทียบกับเอนทูอินเทอมีเดียท (end to intermediate)

3.8 การบริหารคีย์ (Key Management)

หลักที่ใช้ในการสร้างเครือข่ายส่วนตัวเสมือนในกระบวนการคริปโตกราฟี จะต้องมีคีย์ที่ใช้ในการเอ็นคริปท์ชัน และดีคริปท์ชัน ซึ่งคีย์มีความสำคัญต่อการทำงาน ดังนั้นต้องมีหลักในการ

บริหารคีย์ ตั้งแต่การกระจายค่าคีย์ และการบริหารคีย์ให้มีความปลอดภัยจากผู้ที่หวังลักลอบเข้าระบบ จะอธิบายหลักการได้ดังนี้

3.8.1 การกระจายค่าคีย์ (Key Distribution)

ในกระบวนการทำงาน เอ็นคริปท์ชัน ปกติทั้งฝั่งรับและส่งจะต้องมีการใช้ค่าคีย์เดียวกัน ดังนั้นการส่งค่าคีย์เป็นเทคนิคที่ต้องมีระบบคริปโตกราฟีเพราะป้องกันผู้ลักลอบเข้าอ่านคีย์
วิธีการส่งคีย์มีดังนี้

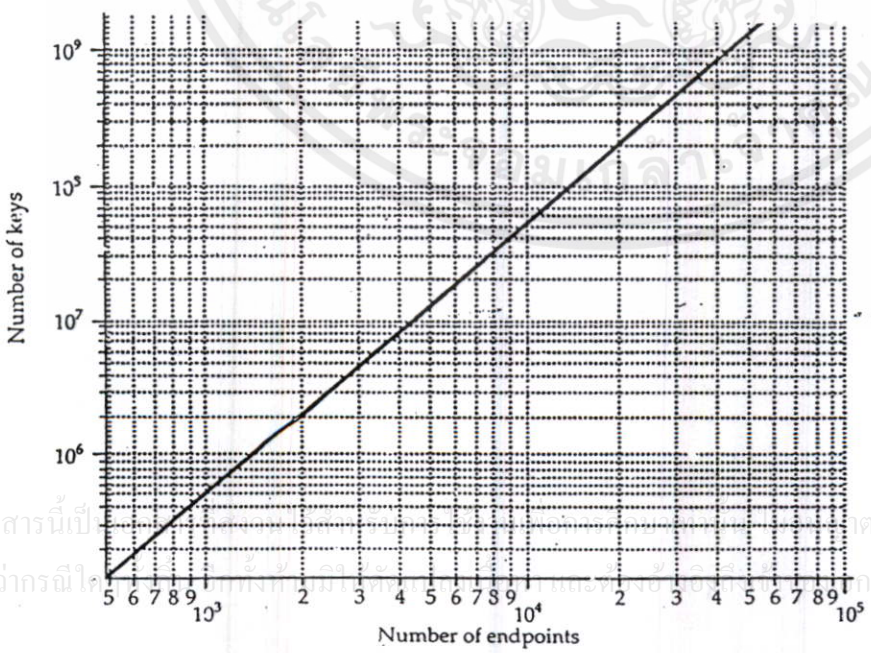
1.คีย์สามารถถูกเลือกโดย A และส่งให้ B โดยตรง

2.บุคคลที่ 3 (third party) สามารถเลือกคีย์และส่งให้ทั้ง A และ B โดยตรง

3.A และ B ใช้คีย์ปัจจุบันโดยฝั่งใดฝั่งหนึ่งสามารถคีย์ใหม่ให้โดยมีการเอ็นคริปท์ ด้วยคีย์เดิม

4.ทั้ง A และ B จะต้องเชื่อมต่อกับบุคคลที่ 3 คือ C โดย D จะส่งที่คีย์ที่ผ่านเอ็นทริปท์ให้กับ A และ B

จาก 1 และ 2 จะเป็นการรับส่งคีย์แบบธรรมดา สำหรับการเชื่อมต่อเอ็นคริปท์ชัน แล้วการใช้แบบธรรมดาไม่สะดวก ในระบบการจัดส่ง สำหรับการแลกเปลี่ยนคีย์ระหว่างโฮสท์และเทอร์มินัล ปัญหาสำคัญในการจัดส่งคีย์กับพื้นที่การให้บริการจำนวนคู่สายในการติดต่อสื่อสารที่ต้องรองรับ ถ้ามีจำนวน N โฮลท์ จำนวนความต้องการคีย์เท่ากับ [N(N-1)]/2



รูปที่ 3.31 จำนวนคีย์ที่ต้องเกิดขึ้นระหว่าง เอ็นพอยท์

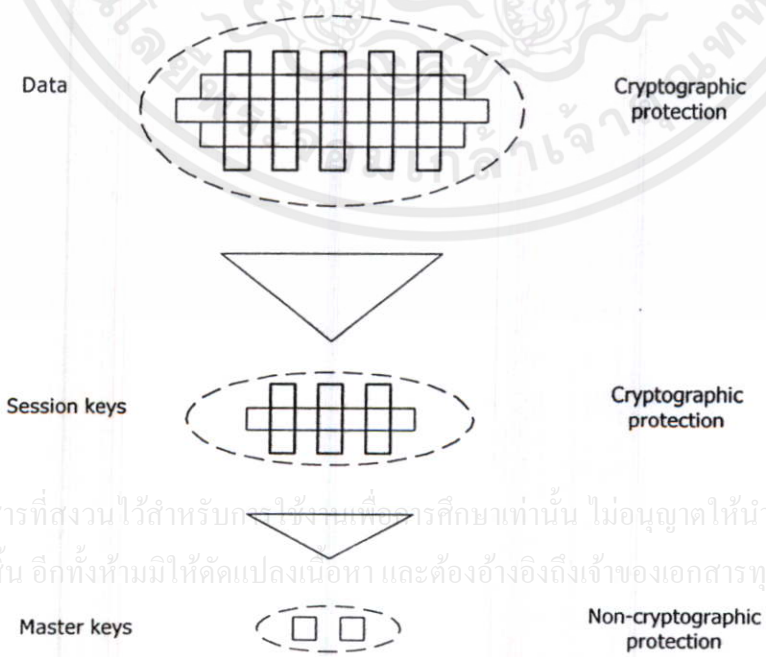
จากรูปที่ 3.31 เน็ตเวิร์คที่ใช้ในการเอ็นคริปท์ชัน 1,000 โหนด จะต้องมีการจัดส่งมากถึงประมาณ 500,000 คีย์

จากข้อ 3 มีความเป็นไปได้ทั้งการเชื่อมต่อหรือการเอ็นคริปท์ชันเอ็นทูเอ็น แต่อย่างไรก็สามารถจะถูกผู้ลักลอบเข้าดูคีย์ได้เพราะมีการส่งคีย์จำนวนมากมากดซ้ำ

จากข้อ 4 เป็นที่นิยมใช้กัน ผังที่ได้จะทำให้ ศูนย์กลางการคีย์ (Key Distribution Center) มีหน้าที่สำหรับการจัดส่งคีย์ระหว่างผู้ใช้ (โฮลท์ กระบวนการ โปรแกรมประยุกต์) ผู้ใช้งานแต่ละรายใช้คีย์เฉพาะเดียวกันกับศูนย์กลางการส่งคีย์เพื่อจะใช้ในการส่งคีย์ซึ่งกันและกัน การใช้ศูนย์กลางการส่งคีย์จะเป็นการใช้ตามลำดับคีย์ซึ่งมีทั้งหมด 2 ระดับ (แสดงดังรูปที่3.23) การติดต่อสื่องสารระหว่างระบบจะถูกเอ็นคริปท์ การใช้คีย์ชั่วคราวหรือเรียกว่า เซสชันคีย์ (sesssion key) เซสชันคีย์จะถูกใช้ระหว่างการเชื่อมต่อทางตรรก ตัวอย่างเช่น วงจรเสมือน (virtual circle) หรือการเชื่อมต่อการส่งแต่ละเซสชันคีย์ (master key) จะถูกใช้ร่วมระหว่างศูนย์กลางส่งคีย์กับปลายทางระบบหรือผู้ใช้งาน

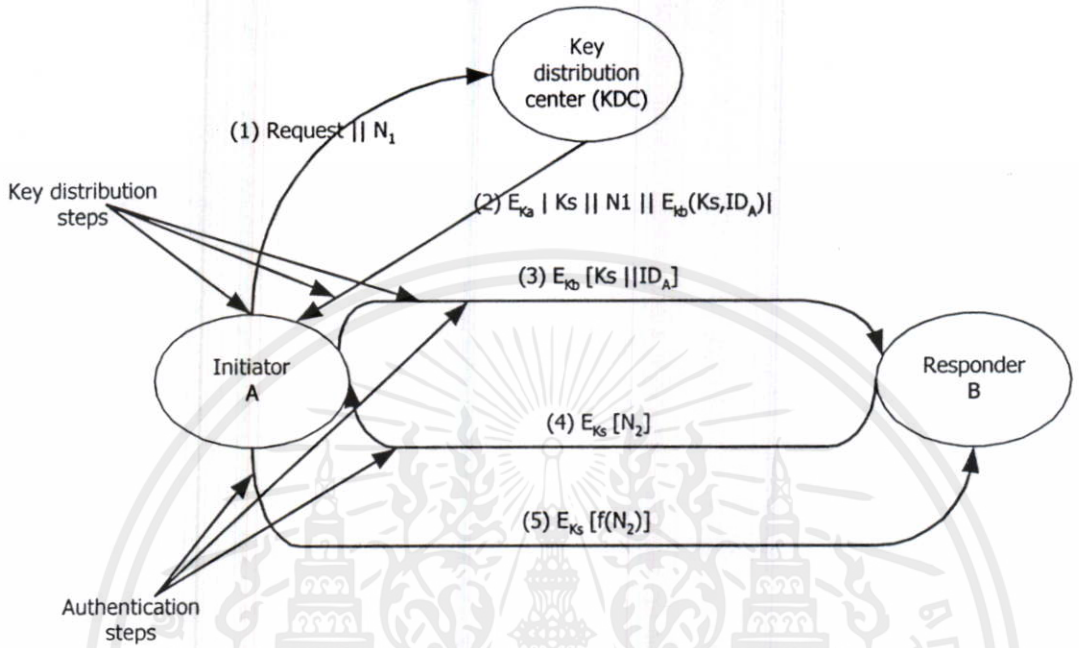
3.8.2 แผนผังการจัดส่งคีย์ (key distribution scenario)

แนวคิดในการส่งคีย์จำนวนวิธีมาก แสดงได้ด้วยรูปที่3.32 จากภาพในแต่ละผู้ใช้งานจะใช้มาสเตอร์คีย์ เฉพาะร่วมกันกับศูนย์กลางการส่งคีย์ (KDC) สมมติว่า A ต้องการเชื่อมต่อกับ B และต้องการเซสชันคีย์เพียงครั้งเดียว เพื่อส่งข้อมูลระหว่างกัน A จะมีคีย์ลับ (secret key; K_a) เป็นการรู้ระหว่าง A กับ KDC เท่านั้น ทำนองเดียวกัน B ก็ใช้มาสเตอร์คีย์เดียวกัน K_b กับ KDC จะเกิดขึ้นดังนี้



รูปที่ 3.32 การใช้คีย์ตามลำดับ (key hierarchy)

1.A เน้นความต้องการ KDC สำหรับเซสชันคีย์ เพื่อป้องกันการเชื่อมต่อถึง B จะมีการส่งข้อความ หรืออาจเรียกว่า ข้อความระยะเวลาหนึ่ง (monce) ซึ่งจะมีการกำหนดเวลา เพื่อป้องกันผู้ลักลอบรู้คีย์นั้นๆ



รูปที่ 3.33 แสดงการจัดส่งคีย์

2.KDC มีหน้าที่กับข้อความที่เอ็นคริปท์โดยการใช้ k_a ดังนั้น A จะเป็นผู้ใช้งานคนเดียวเท่านั้นที่สามารถรับข้อความนี้ได้ และ A จะรู้การเริ่มต้นของ KDC ข้อความนั้นประกอบด้วย 2 หัวข้อ สำหรับ A คือ

- เซสชันคีย์ K_s ที่ใช้สำหรับเซสชัน
- ข้อความต้องการเริ่มต้น เพื่อสามารถให้ A มีผลตอบสนองตรงตามที่ต้องการ

ถัดจากนั้น A สามารถพสูจน์ข้อความต้นแบบ ก่อนการรับโดย KDC และเพราะว่าเป็นการส่งชั่วขณะหนึ่ง ทำให้ไม่สามารถทำการส่งซ้ำได้ข้อความนี้จะรวมถึง 2 หัวข้อที่ตรงกับ B คือ

- เซสชันคีย์ K_s ที่ใช้สำหรับเซสชัน
- ลักษณะของ A (ยกตัวอย่าง เลขที่เน็ตเวิร์ค) : ID_A

ทั้งสองหัวข้อจะเอ็นคริปท์กับมาสเตอร์คีย์ที่ใช้ร่วมกันระหว่าง KDC กับ B

3. A เก็บเซสชันคีย์และส่งไปยัง B เป็นข้อมูลรายละเอียดเริ่มต้นของ KDC สำหรับ B ชื่อว่า $E_{Kb}[K_S||ID_A]$ เพราะว่าข้อมูลจะถูกเอ็นคริปท์กับ K_b เป็นการป้องกันผู้ลักลอบดู B จะรู้จักเซสชันคีย์ (K_S) รู้จัก A (จากเลขที่ ID_A) และข้อมูลเริ่มต้นที่ KDC (เพราะว่ามีการถูกเอ็นคริปท์โดยใช้ E_{kb})

ที่จุดนี้ เซสชันคีย์จะมีความปลอดภัยที่ได้รับส่งระหว่าง A กับ B และเป็นการเริ่มแลกเปลี่ยนด้วยความปลอดภัย

4.ถ้าการเอ็นคริปท์ชันไม่มีเซสชันคีย์มาด้วย B จะส่งข้อความชั่วขณะ (nonce) N_2 ไปหา A

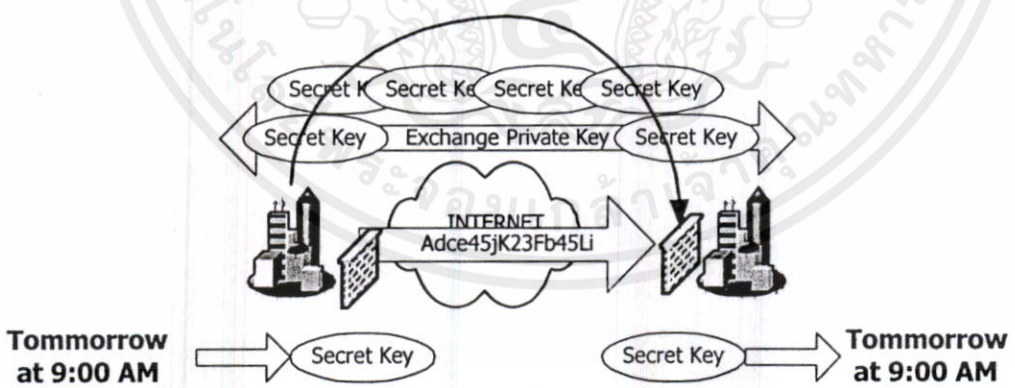
5.ด้วยการใช้ Ks A จะตอบสนอง f (N_2) โดยที่ f เป็นฟังก์ชันในการกระทำกับการแลกเปลี่ยน N_2 ยกตัวอย่างเช่น ให้มีการส่งมาใหม่

3.8.3 วงจรชีวิตเซสชันคีย์ (Session Key Lifetime)

ยิ่งมีการเปลี่ยนเซสชันคีย์บ่อยเพียงใด ยิ่งทำให้ระบบมีความปลอดภัยมากขึ้นเท่านั้น ผู้จัดการด้านความปลอดภัยเน็ตเวิร์ค จะต้องพิจารณาวงจรชีวิตเซสชันคีย์ ให้เหมาะสมสำหรับโปรโตคอลการเชื่อมต่อแบบต่อเนื่อง (connection-oriented,protocol) จะพบว่าใช้เซสชันคีย์ตลอดระยะเวลาที่มีการเชื่อมต่อเข้าสู่เน็ตเวิร์ดนั้นๆ การใช้เซสชันคีย์ตัวใหม่จะเกิดขึ้นเมื่อมีการเชื่อมต่อใหม่เท่านั้นสำหรับโปรโตคอลการเชื่อมต่อไม่ต่อเนื่อง (connectionless protocol)

3.8.4 คีย์ส่วนตัว (Private Key)

คีย์ที่เป็นส่วนตัว คือคีย์ที่ใช้ในกระบวนการเอ็นคริปท์โตกราฟี ซึ่งการบริหารคีย์สามารถบริหารได้สะดวก เพราะว่าไม่ต้องแสดงออกสู่ภายนอก จึงทำให้การบริหารงานได้ง่ายเมื่อเทียบกับคีย์สาธารณะ ระบบการเอ็นคริปท์ชันไพรเวทคีย์ (Private key Encryption System) จะใช้คีย์ที่เหมือนกันทั้งในการเอ็นคริปท์ชัน และดีคริปท์ชัน ข้อสำคัญในวิธีนี้ คือการรับส่งคีย์ที่ใช้ จะต้องมีการป้องกันเพื่อความปลอดภัย มิเช่นนั้นคีย์อาจรั่วไหลผู้ไม่มีสิทธิสามารถรับรู้ได้ ในการใช้ระบบเอ็นคริปท์ชันไพรเวทคีย์ ยกตัวอย่างเช่น อัลกอริทึมเดส ในการเอ็นคริปท์ข้อมูล

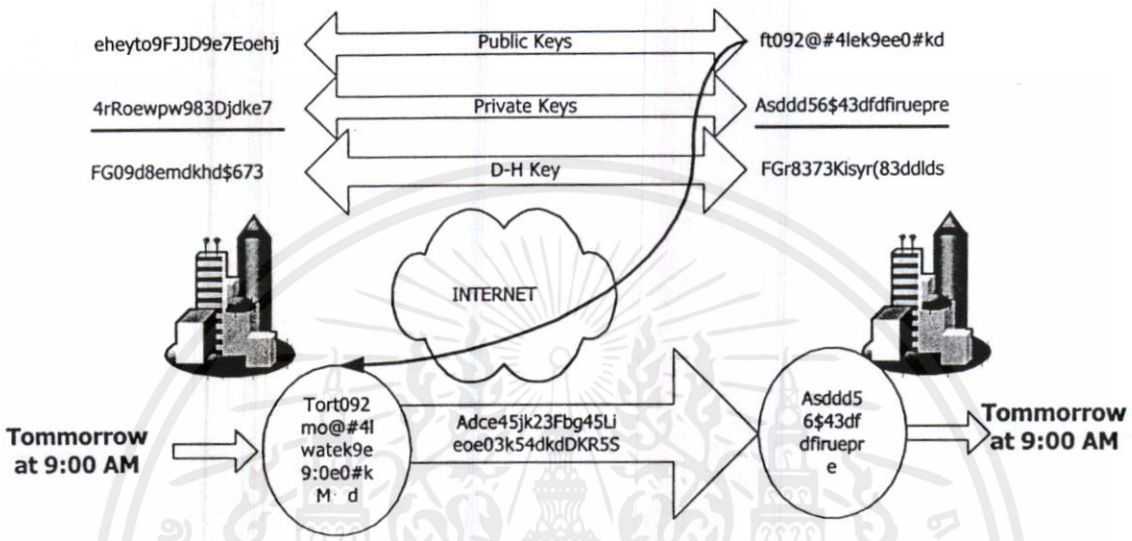


รูปที่ 3.34 แสดงกระบวนการเอ็นคริปท์ชันไพรเวทคีย์

3.8.5 คีย์สาธารณะ (Public Key)

คีย์สาธารณะ คือ คีย์ที่ใช้ในกระบวนการเอ็นคริปท์โตกราฟี ซึ่งจะมี บุคคลที่ 3 ช่วยในการบริหารคีย์ เพราะว่าต้องแสดงออกสู่บุคคลภายนอก เพื่อให้สะดวกในการใช้งาน แต่ข้อเสียคือเรื่องความเร็วในการใช้งาน คีย์สาธารณะ (Public Key) ใช้การผสมระหว่างไพรเวทคีย์ ที่เก็บเป็นความ

ลับระหว่างบุคคล และคีย์สาธารณะที่ถูกสร้างขึ้น ไพรเวทคีย์จะถูกใช้ในการดีคริปท์ข้อมูลให้มีความสัมพันธ์กันกับคีย์สาธารณะจึงจะสามารถอ่านข้อมูลเหล่านั้นได้ Rivest Shamir Adlemen (RSA) และ Diffie-Hellman (DH) เป็นระบบคีย์สาธารณะที่นิยมใช้มากในปัจจุบันในการใช้ระบบเครือข่ายวีพีเอ็น



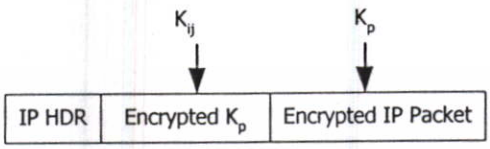
รูปที่ 3.35 แสดงอัลกอริทึมเอ็นคริปท์ชันคีย์สาธารณะ Diffie-Hellman

จากรูปทั้งฝ่ายส่งและรับ จะใช้ Diffie-Hellman คีย์ ผู้ส่งจะมีคีย์สาธารณะของผู้รับจากแหล่งกำเนิดคีย์ที่แตกต่างกัน และจะเอ็นคริปท์ข้อความได้ เป็น Tomorrow at 9: 00 a.m. พบว่าวิธีนี้จะใช้ทั้งไพรเวทคีย์ และคีย์สาธารณะดังนั้น ถ้าผู้รับมีไพรเวทคีย์ แต่ไม่มีคีย์สาธารณะจะไม่สามารถอ่านข้อมูลเหล่านั้นได้

3.8.6 SKIP (Simple Key Internet Protocol; SKIP)

ในปี 1994 Ahsar Aziz และ Whitfield Diffie ได้พัฒนา Simple Key Management Internet Protocol (SKIP) โปรโตคอลSKIP เสมือนเป็นโปรโตคอลบริหารคีย์ (Key Management Protocol) พื้นฐานแต่ละครั้งในการสื่อสาร SKIP จะสมมติให้มีคู่คีย์สาธารณะ Diffie-Hellman SKIP จะตรวจสอบการความปลอดภัยระหว่างจุดต่อจุด โดยการเอ็นคริปท์คีย์ลับที่ใช้ร่วมกัน แสดงได้ดังรูปที่ 3.37 คีย์ลับจะทำให้รู้เฉพาะส่วนที่สื่อสารกันเท่านั้น และใช้สำหรับการตรวจสอบคีย์ ในศัพท์ของ SKIP จะพบตัวแปรดังนี้ K_{ij} โดย i และ j มีความหมายในการกำหนดผู้ใช้งาน ดังนั้น Kij จึงเป็นส่วนที่มีการติดต่อระหว่างคู่สนทนา ชั้นคีย์เกิดขึ้นจะมีการอัลกอริทึมเอ็นคริปท์ชันใช้ดังตัวอย่างต่อไปนี้ คือ RC4 56 bit DES 3DES และ 128 bit SKIP จัดแจงสำหรับโปรโตคอลบริหารคีย์ และประกอบด้วยลำดับของคีย์ต่างๆที่เตรียมการเปลี่ยนแปลงตลอดเวลา คีย์ที่สร้างขึ้น จะใช้ อัลกอริทึม Diffie-Helllman ด้วยขนาดคีย์ที่อยู่ระหว่าง 5,123 ถึง 2,048 บิท คีย์ที่มีลำดับต่ำกว่าจะมีการเปลี่ยน

แปลงอย่างรวดเร็วกว่า คีย์ที่ลำดับสูงกว่า ยกตัวอย่าง K_{ij} สำหรับผู้ผลิตบางรายจะอนุญาตให้ทำการเซ็ตค่าเมื่อคีย์มีการเปลี่ยนแปลง SKIP ทำงานกับไอพีสแตกค์ การเอ็นคริปท์แพ็กเก็ตข้อมูลจะเกิดต่ำกว่าเลเยอร์ไอพี ทำให้ SKIP มองไม่เห็นด้วยอุปกรณ์ทางเน็ตเวิร์ค โปรแกรมประยุกต์ และผู้ใช้งานอื่น SKIP ใช้การคีย์เอ็นคริปท์แพ็กเก็ต



รูปที่ 3.36 แพ็กเก็ต SKIP

3.9 สถาปัตยกรรมเครือข่ายส่วนตัวเสมือน

สถาปัตยกรรมเครือข่ายส่วนตัวเสมือน คือ การออกแบบเครือข่ายส่วนตัวเสมือนให้มีคุณสมบัติตรงตามความต้องการขององค์กรในการจะใช้เป็นเครือข่ายที่ได้รับการปกป้อง จากผู้โจรกรรมข้อมูลในรูปแบบต่างๆ ที่ได้อธิบายมาแล้วในบทที่ 2

3.9.1 แนวทางในการออกแบบเครือข่ายวีพีเอ็น

ก่อนเลือกเครือข่ายวีพีเอ็นจะต้องพิจารณาว่าวีพีเอ็นให้ความปลอดภัยกับข้อมูลขององค์กรได้อย่างคุ้มค่าหรือไม่ [9] ซึ่งสามารถอธิบายเป็นสมการ

$$VPN = f(security)$$

วีพีเอ็นคือฟังก์ชันของความปลอดภัย โดยถ้ามีการเปลี่ยนแปลงของค่าความปลอดภัย จะมีผลทำให้วีพีเอ็นเปลี่ยนแปลงด้วย เช่น การใช้เอ็นคริปท์ชัน 56 บิท เวลาผ่านไปเทคนิควีพีเอ็นจะเปลี่ยนแปลงไปเป็น 128 บิท ระบบเดิมจะไม่สามารถรองรับได้ จึงควรที่จะมีการออกแบบเครือข่ายส่วนตัวเสมือนให้สามารถรองรับการขยายตัวของเทคโนโลยีในอนาคต สามารถสรุปเป็นหลักในการพิจารณาได้ดังนี้ หลักการที่ควรพิจารณาในการออกแบบเครือข่ายวีพีเอ็น

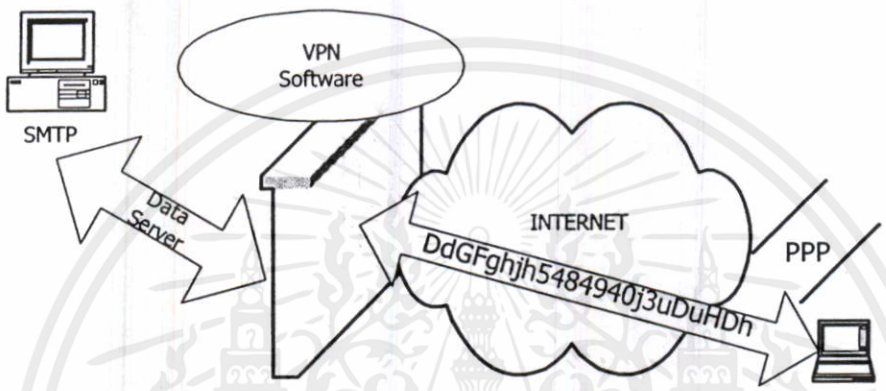
1. ควรออกแบบโปรโตคอลมาตรฐาน คือ PPTP L2TP และ IPSec ให้สามารถรองรับกับการขยายตัวของบริษัทคู่ค้า ซัพพลายเออร์ บริษัทแม่ และควรเลือกให้เป็นโปรโตคอลเดียวกัน
2. การออกแบบฮาร์ดแวร์ควรที่จะพิจารณาฮาร์ดแวร์ที่สามารถรองรับกับโครงสร้างเครือข่ายเดิมด้วย เช่น ฮาร์ดแวร์รองรับ WindowsNT ควรที่จะหาอุปกรณ์ที่สนับสนุนโดย WindowsNT แทนที่จะเลือกอุปกรณ์ทางด้าน Unix

3.9.2 โทโปโลยีวีพีเอ็น

โทโปโลยีวีพีเอ็น หมายถึง รูปแบบการออกแบบวีพีเอ็นที่ใช้ในเครือข่าย การออกแบบโครงสร้างวีพีเอ็น จะต้องพิจารณาว่าจะใช้โทโปโลยีแบบใดซึ่งสามารถที่จะอธิบายโทโปโลยีที่สำคัญได้เป็น 4 โทโปโลยีดังนี้ คือ

1. ไฟร์วอลล์ทูไคล์เอนท์โทโปโลยี

   ไฟร์วอลล์ทูไคล์เอนท์โทโปโลยี คือ การที่ใช้วีพีเอ็นเป็นไฟร์วอลล์สำหรับป้องกันผู้ลักลอบเข้าสู่เครือข่าย



รูปที่ 3.37 แสดงไฟร์วอลล์ทูไคล์เอนท์โทโปโลยี

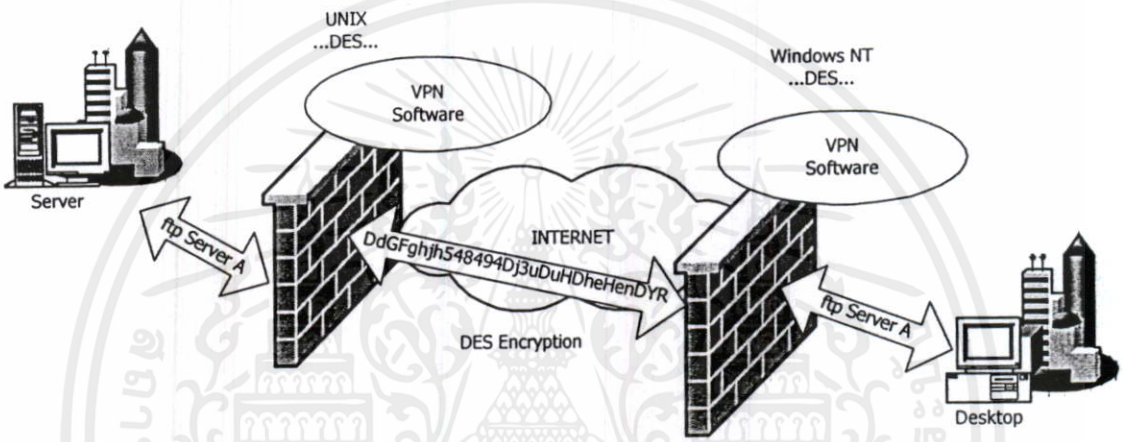
จะพบว่าโทโปโลยีนี้เป็นที่นิยมใช้กันมาก เพราะว่าสะดวก และง่ายในการติดตั้ง จากรูปที่ 3.37 เป็นตัวอย่างที่แสดงโดยการใช้แลปทอป เพื่อเข้าสู่เซิฟเวอร์ ซึ่งอยู่ข้างหลังไฟร์วอลล์ มีกระบวนการดังนี้

1. ผู้ใช้งานจากแลปทอป หมุนโทรศัพท์ ติดต่อผู้ให้บริการอินเทอร์เน็ต และเชื่อมต่อกันโดยใช้โปรโตคอลพีพีพี
2. แลปทอปต้องการคีย์จากไฟร์วอลล์ โดยอาจใช้ชื่อ และรหัสลับเอง หรือเข้าทำงานแบบไม่ต้องมีการใส่ชื่อ และรหัสลับ แต่มีการใช้แบบออโตเมติก (สามารถเข้าสู่ระบบได้อย่างสะดวกสบาย) ตรวจสอบจากเลขที่ MAC บนแลนการ์ด
3. ไฟร์วอลล์ส่งคีย์ที่ใช้ให้
4. ซอฟแวร์วีพีเอ็น ที่เครื่องแลปทอป จะรอคอยการตอบรับให้เข้าทำงานของเซิฟเวอร์ภายใน (Internal Server) โดยที่รู้ไอพีแอดเดรสปลายทาง แลปทอปจะทำการเอ็นคริปท์แพ็กเก็ตแล้วส่งให้กับไฟร์วอลล์
5. ไฟร์วอลล์จะรับไอพีแอดเดรส แล้วทำการดีคริปท์แพ็กเก็ต เพื่อส่งไปยังเซิฟเวอร์ภายในวงแลน

6. เซิฟเวอร์ภายในจะตอบกลับ และส่งข้อมูลที่ต้องการมาให้
7. ไฟร์วอลล์จะตรวจสอบเส้นทางเดิน จากตารางทันเนลวีพีเอ็นที่สร้างขึ้น เพื่อจะส่งไปที่แลปทอป
8. แลปทอปรับแพ็กเก็ตข้อมูล แล้วทำการดีคริปท์ เพื่อให้เลเยอร์ระดับชั้นแอปพลิเคชันสามารถรับรู้แพ็กเก็ต และตีความหมายได้

2. แลนทูแลนโทโปโลยี

แลนทูแลนโทโปโลยี เป็นการทำให้เป็นไฟร์วอลล์ทั้งสองฝั่ง (ฝั่งเครือข่ายที่รับ และส่ง)



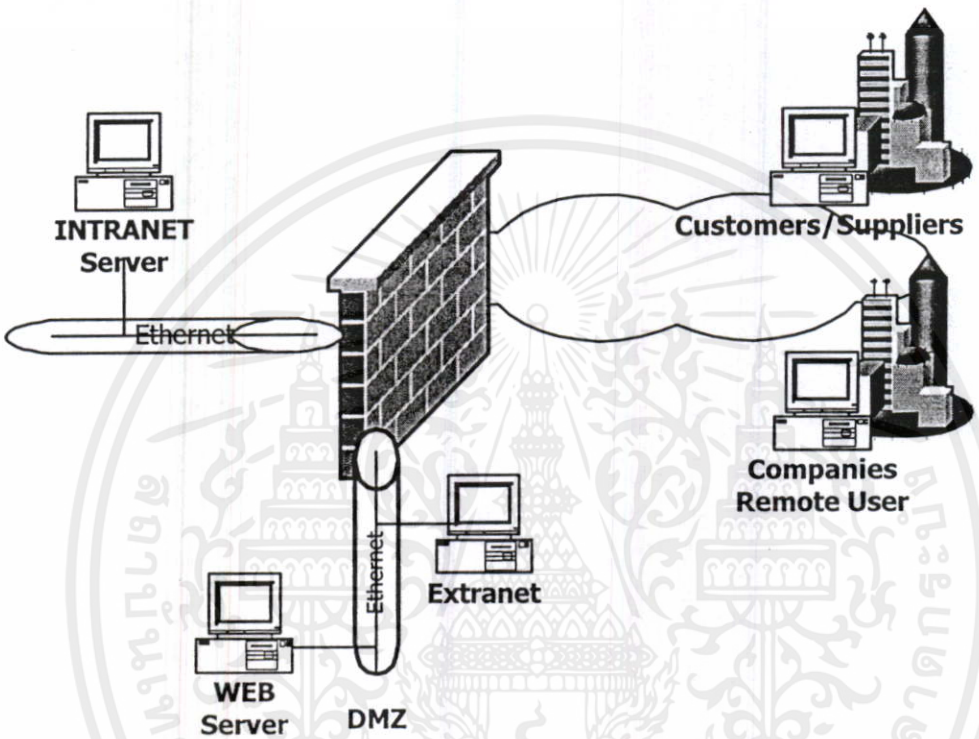
รูปที่ 3.38 แสดงตัวอย่างแลนทูแลนโทโปโลยี

จากรูปที่ 3.38 เป็นตัวอย่างแลนทูแลนโทโปโลยี ซึ่งมีขั้นตอนการทำงานดังนี้

1. ผู้ควบคุมเครือข่ายฝั่งหนึ่งจะกำหนดการเอ็นคริปท์ชัน ระหว่าง 2 เครือข่าย โดยมีการสร้างคีย์จากซอฟแวร์วีพีเอ็น
2. ผู้ใช้งานจากเครือข่ายต้องการใช้โปรแกรม FTP เพื่อเชื่อมเข้าสู่เซิฟเวอร์
3. แพ็กเก็ตจากเครื่องเดสทอปจะเป็นเพลนเท็กและผ่านเข้าไฟร์วอลล์
4. แพ็กเก็ตจะถูกเอ็นคริปท์ และส่งไอพีแอดเดรสสาธารณะ ไปยังไฟร์วอลล์อีกฝั่ง
5. ไฟร์วอลล์จะรับแพ็กเก็ต และทำการดีคริปท์ และส่งข้อมูลให้ถึงปลายทาง คือ เซิฟเวอร์
6. เซิฟเวอร์จะรับ และส่งข้อมูลกลับ
7. แพ็กเกตจะเป็นเพลนเท็ก แล้วเข้าสู่ไฟร์วอลล์
8. ไฟร์วอลล์จะทำการเอ็นคริปท์แพ็กเก็ตก่อน แล้วจึงส่งไปยังไฟร์วอลล์ฝั่งรับ
9. ไฟร์วอลล์ด้านเดสทอปที่ได้รับแพ็กเก็ต จะทำการดีคริปท์ แล้วส่งข้อมูลให้ผู้ใช้งาน

3. ไฟร์วอลล์ทูอินเทอร์เน็ต หรือเอ็กตร้าเน็ตโทโปโลยี

ไฟร์วอลล์ทูอินเทอร์เน็ตโทโปโลยี หมายถึงการทำให้อินเทอร์เน็ต หรือเอ็กตร้าเน็ต สามารถผ่านเข้าสู่ไฟร์วอลล์ได้โดยที่มีความปลอดภัย และจะใช้งานได้ ก็ต่อเมื่อผู้ใช้งานในเครื่องนั้นๆ มีสิทธิในการใช้งานเครือข่ายวีพีเอ็น

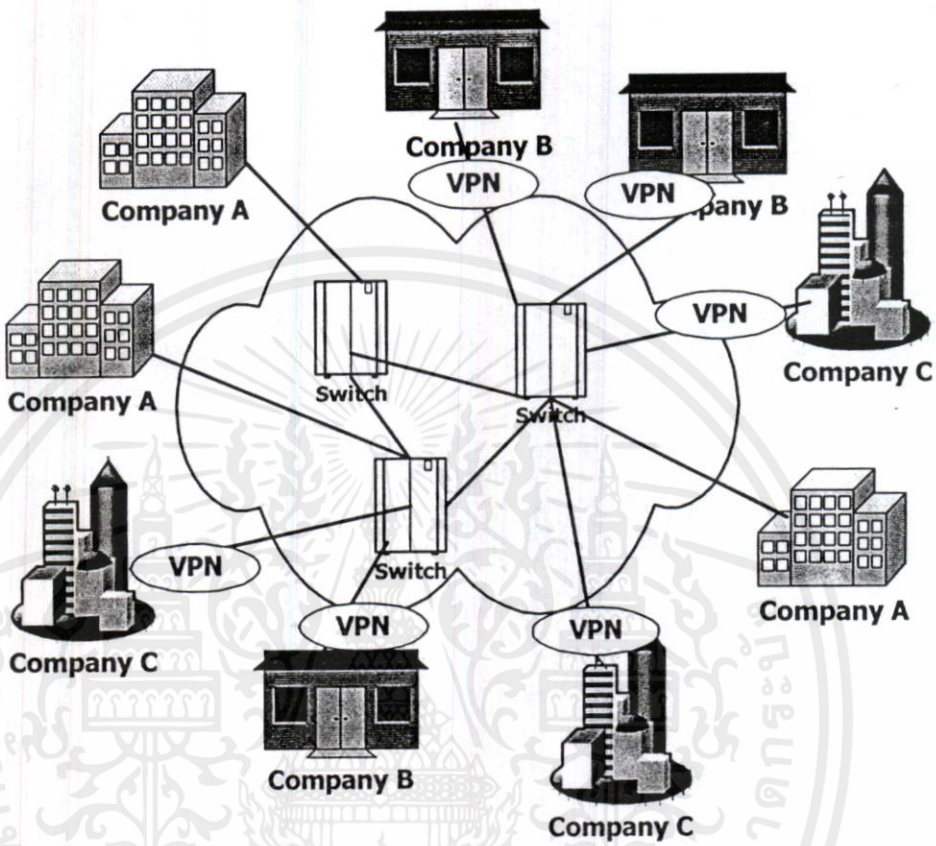


รูปที่ 3.39 แสดงไฟร์วอลล์ทูอินเทอร์เน็ตโทโปโลยี

จากรูปที่ 3.39 พบว่ามีการทำงานโดยที่ผู้ที่จะเข้าใช้งาน จะต้องได้รับสิทธิ จึงจะสามารถเข้าสู่เครือข่ายวีพีเอ็นได้ ไม่ว่าจะเป็นเครือข่ายอินเทอร์เน็ต หรือเอ็กตร้าเน็ต โดยที่ใช้หลักการในการเอ็นคริปท์ชัน และดีคริปท์ชัน เหมือนกันกับโทโปโลยีอื่น

4. เฟรม หรือ เอทีเอ็มโทโปโลยี

หมายถึง การใช้สายเช่า (Leased Line) ผ่านเข้าสู่เครือข่าย ของผู้ให้บริการวีพีเอ็น ผ่านเฟรมรีเลย์ หรือเอทีเอ็ม



รูปที่ 3.40 แสดงเฟรม หรือเอทีเอ็มโทโปโลยี

จากรูปที่ 3.40 เป็นการใช้โครงสร้างเครือข่ายที่เป็นเฟรม หรือเอทีเอ็ม โดยมีการอุปกรณ์สำหรับการทำเอ็นคริปท์ และดีคริปท์ในแต่ละเซลล์ของเครือข่าย จะเกิดการเอ็นคริปท์แพ็กเก็ตไอพี จนกว่าแพ็กเก็ตจะถึงปลายทาง เซลล์จึงจะทำการดีคริปท์ เพื่อให้ข้อมูลส่งถึงปลายทางได้ เมื่อทราบถึงโทโปโลยีวีพีเอ็น ก่อนที่จะทำการติดตั้งเครือข่ายวีพีเอ็นจะต้องมีการรู้ถึงรูปแบบที่นิยมในการติดตั้งเครือข่ายส่วนตัวเสมือนด้วย

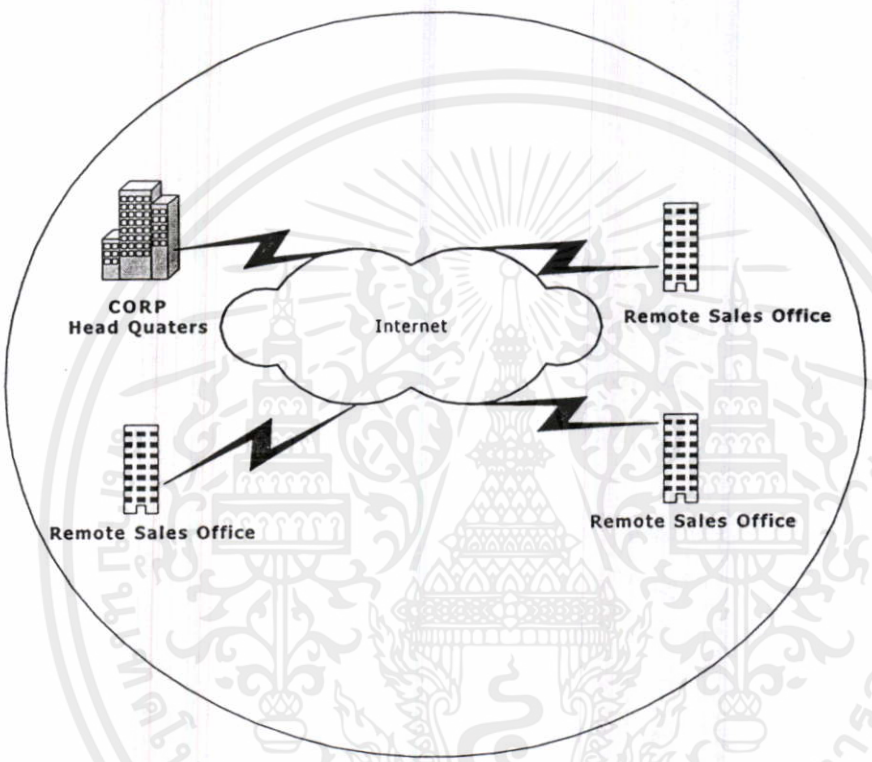
3.9.3 รูปแบบการติดตั้งเครือข่ายส่วนตัวเสมือน

จากการที่ได้ทราบถึงทฤษฎีต่างๆ ที่เกี่ยวข้องกับการออกแบบเครือข่ายส่วนตัวเสมือน ในทางปฏิบัตินั้น จะต้องมีการเข้าใจถึงรูปแบบของการติดตั้งเครือข่ายส่วนตัวเสมือนเพื่อสามารถที่ทำให้การออกแบบเครือข่ายส่วนตัวเสมือนตรงตามวัตถุประสงค์ขององค์กรที่ต้องการให้เครือข่าย

คอมพิวเตอร์มีความปลอดภัยอย่างไร ซึ่งรูปแบบหลักของการติดตั้งเครือข่ายส่วนตัวเสมือนมีทั้งหมด 4 แบบ โดยแต่ละแบบมีวัตถุประสงค์ขึ้นอยู่กับผู้ออกแบบดังนี้

1.อินทราเน็ต

อินทราเน็ตวีพีเอ็น เป็นการสร้างเครือข่ายระหว่างสำนักงานใหญ่ เชื่อมต่อกับสำนักงานย่อยต่างๆ เช่น สำนักงานใหญ่อยู่กรุงเทพฯ แล้วมีการเชื่อมต่อกันกับสำนักงานสาขาที่สมุทรปราการ เป็นต้น



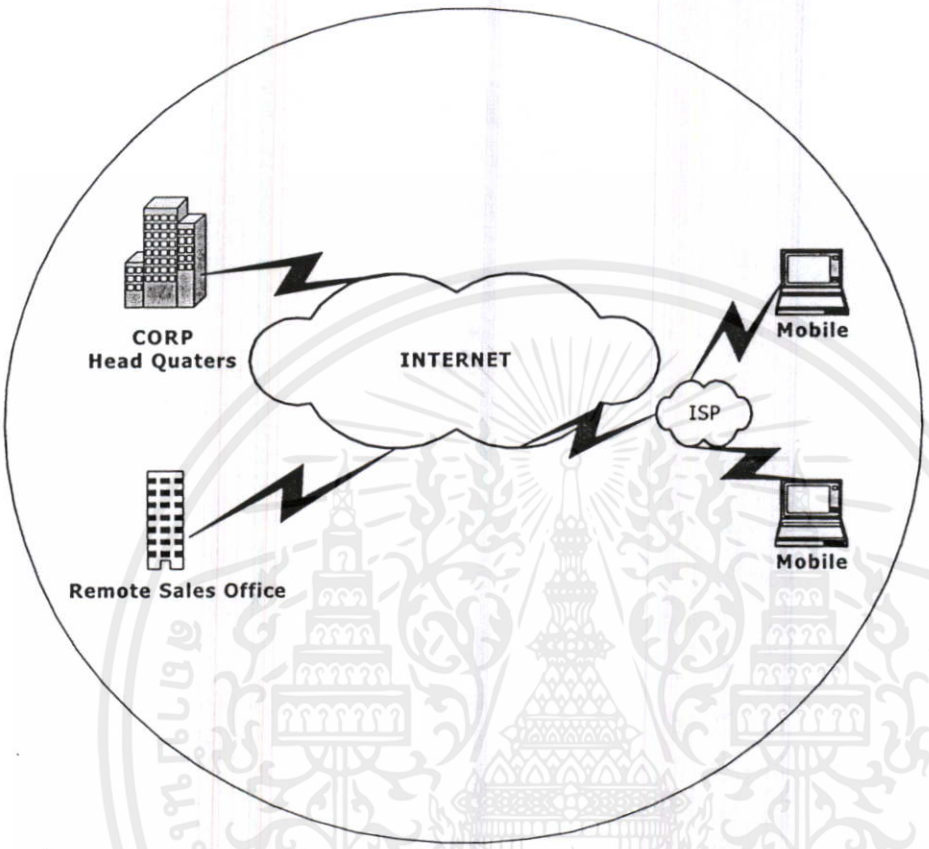
รูปที่ 3.41 แสดงอินทราเน็ตวีพีเอ็น

จากรูปที่ 3.41 เป็นการแสดงให้เห็นรูปแบบของการติดตั้งอินทราเน็ตวีพีเอ็น ตั้งแต่สำนักงานใหญ่ (Head Quarters) เชื่อมโยงผ่านเครือข่ายอินเทอร์เน็ต แล้วสำนักงานที่ทำหน้าที่เป็นหน่วยงานขายสามารถเชื่อมโยงเข้าสำนักงานใหญ่ส่วนกลางได้ โดยที่ข้อมูลมีความปลอดภัย และสามารถกำหนดให้ผู้สิทธิเท่านั้น ที่สามารถรับรู้ถึงข้อมูลได้

2. รีโมตแอสเซส

รีโมตแอสเซสวีพีเอ็น เป็นการสร้างเครือข่ายระหว่างสำนักงานใหญ่ และ ผู้ที่ใช้คอมพิวเตอร์ผ่านเครื่องวิทยุสื่อสารเพื่อสามารถเข้ามาใช้งานในเครือข่ายหลักขององค์กรได้ จากรูปที่ 3.42 จะพบว่าที่เครื่องคอมพิวเตอร์ที่รีโมตเข้ามาจะต้องมีโปรแกรมวีพีเอ็น แล้วจะทำให้สามารถที่จะสร้างอุโมงค์เอ็นคริปท์ชัน เข้าสู่สำนักงานใหญ่ได้ โดยผู้ที่เข้าใช้งานได้ จะต้องมีสิทธิเท่านั้นจึงจะสามารถเข้าสู่ระบบเครือข่ายภายในองค์กรได้ และการที่ให้ผู้ให้บริการอินเทอร์เน็ต สามารถให้บริการกับลูกค้าที่รับบริการเครือข่ายส่วนตัวเสมือนเพื่อสามารถจะหมุนโทรศัพท์เข้าสู่อินเทอร์เน็ต

ที่ใด ก็ได้ แล้วสามารถเข้าทำงานเสมือนอยู่ ณ สำนักงานใหญ่ และทำให้สะดวก รวมถึงที่ขาดมิได้ คือ สร้างความปลอดภัยในการเข้าใช้งานเครือข่ายภายในสำนักงานใหญ่ได้

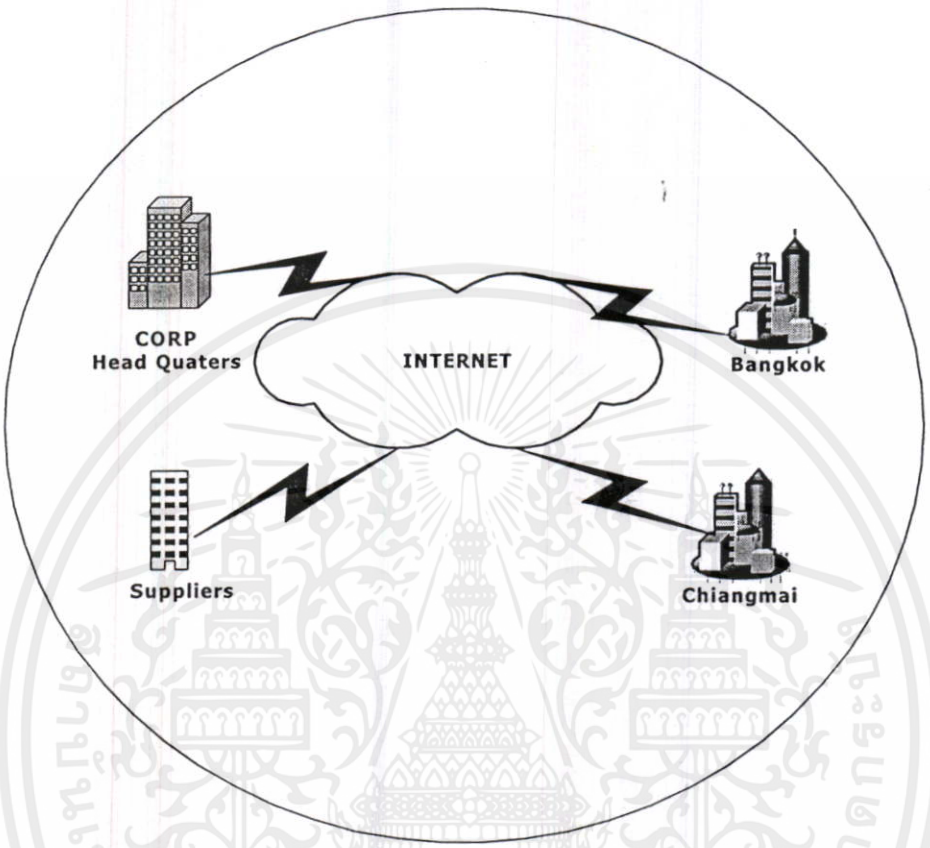


รูปที่ 3.42 แสดงรีโมตวีพีเอ็น

3. เอ็กซ์ตร้าเน็ต

เอ็กซ์ตร้าเน็ตวีพีเอ็น เป็นการสร้างเครือข่ายเชื่อมระหว่างบริษัท ลูกค้า และซัพพรายเออร์ แสดงได้ดังรูปที่ 3.43 ปัจจุบัน จะเห็นตัวอย่างเครือข่ายส่วนตัวเสมือนที่ติดตั้งแบบนี้ได้จากการที่ใช้โปรโตคอลเอชทีทีพี (HTTP) ที่ใช้เพื่อเข้าสู่เว็บ (Web) ที่ต้องการ หรือต้องการที่จะติดต่อกับหน่วยงานอื่นผ่านเว็บ ซึ่งมีส่วนสำคัญมากต่อการทำธุรกิจอีคอมเมอร์ การที่ทำให้การติดต่อสื่อสารผ่านกันง่ายขึ้น และมีความปลอดภัยโดยเฉพาะในเรื่องที่ต้องมีการโอนย้ายเงินผ่านบัญชีทางเว็บ พบว่าแม้เครือข่ายภายในองค์กรได้รับการเชื่อมต่อเข้ากับเครือข่ายทั่วไป แต่สามารถทำให้เกิดความปลอดภัยในการที่จะดำเนินธุรกรรมใดก็ตาม เพื่อให้ผู้ใช้งานที่มีสิทธิเท่านั้น จึงจะเข้าใช้งานระบบเครือข่ายภายในองค์กรได้ ยิ่งอินเทอร์เน็ตได้รับความนิยมในการที่องค์กรต่างๆ จะต้องสามารถเข้าสู่เครือข่ายอินเทอร์เน็ตให้ได้ จึงยิ่งทำให้บริษัทภายนอกองค์กรมีความสามารถในการที่จะเข้าสู่เครือข่ายภายในได้สะดวกยิ่งขึ้น ผนวกกับความปลอดภัยที่จะได้รับจากเครือข่ายส่วนตัวเสมือนทำให้

การติดตั้งแบบนี้ เหมาะสมกับองค์กรที่ต้องการติดต่อค้าขายกับองค์กรภายนอกผ่านเครือข่ายขององค์กรนั้นๆ

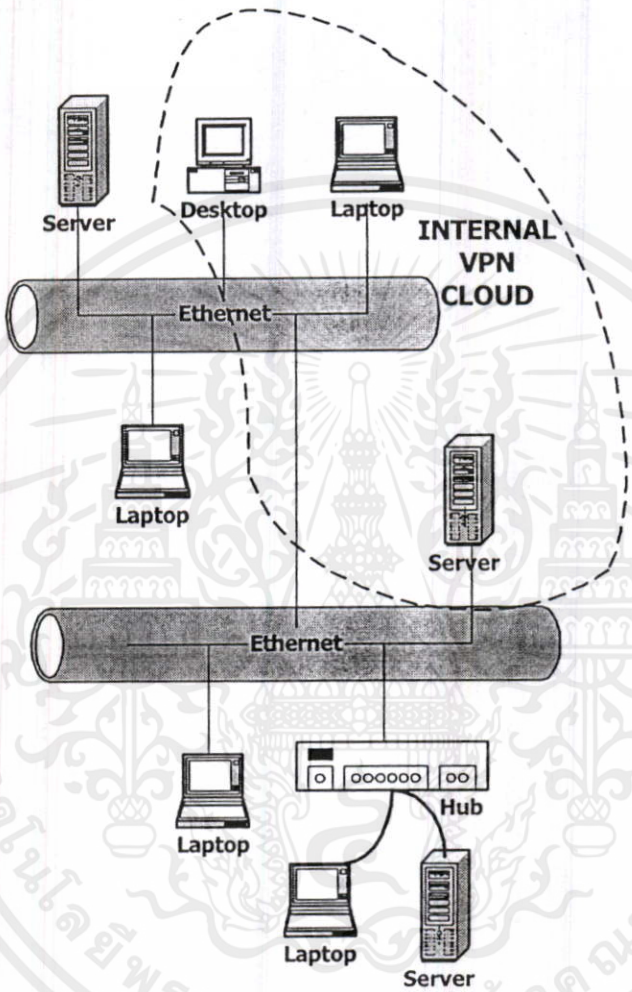


รูปที่ 3.43 แสดงเอ็กซ์ตร้าเน็ตวีพีเอ็น

4. อินทราคอมพานี

อินทราคอมพานี เป็นการสร้างเครือข่ายภายในบริษัทเอง เหตุผล เพื่อต้องการให้ข้อมูลที่มีความสำคัญสามารถที่ผ่านระบบเครือข่ายในบริษัทโดยมีความปลอดภัยมากยิ่งขึ้น เพราะว่าจากการสำรวจของเอฟบีไอ องค์กรของรัฐ สถาบันการเงิน และมหาวิทยาลัยในอเมริกาพบว่า การโจรกรรมข้อมูลนั้น มาจากบุคคลากร หรืออุปกรณ์ที่คอมพิวเตอร์ที่เชื่อมต่อภายในองค์กรนั่นเอง จากสถิติมีถึง 64 เปอร์เซ็นต์ในจำนวนคดีที่โจรกรรมข้อมูลออกสู่ภายนอก [10] จากรูปที่ 3.44 เป็นการติดตั้งเครือข่ายส่วนตัวเสมือนแบบอินทราคอมพานี โดยที่พื้นที่ที่เป็นส่วนที่แรเงา จะเป็นส่วนที่สามารถจะทำการติดต่อสื่อสารผ่านเครือข่ายภายในองค์กรได้อย่างมีความปลอดภัย เพราะว่าจากการที่สามารถกำหนดสิทธิของผู้ที่สามารถจะเข้ามารับรู้ข้อมูลที่จะใช้วิธีการโจรกรรมในรูปแบบต่างๆ ที่กล่าวมาแล้วข้างต้น ฉะนั้นการติดตั้งเครือข่ายส่วนตัวเสมือนแบบนี้ จะทำให้บริษัทมีความปลอดภัยในเรื่องของการป้องกันการถูกโจรกรรมจากบุคลากรภายในองค์กรที่ขาดคุณธรรมได้ และด้วยเหตุ

ผลนี้จึงทำให้การวิจัยครั้งนี้ ได้ทำการวิจัยโดยการออกแบบติดตั้งแบบนี้ เพื่อใช้ในการตรวจสอบการทำงานของเครือข่ายส่วนตัวเสมือน



รูปที่ 3.44 แสดงอินทราคอมพานีวีพีเอ็น

บทที่ 4
การออกแบบเครือข่ายส่วนตัวเสมือน เพื่อตรวจสอบการทำงาน

4.1 บทนำ

หลักในการออกแบบเครือข่ายส่วนตัวเสมือนจะต้องพิจารณาว่าวัตถุประสงค์หลักขององค์กรต้องการนำเครือข่ายส่วนตัวเสมือนมาใช้เพื่ออะไร ซึ่งเมื่อทราบเป้าหมายจะทำให้สามารถทำการออกแบบเครือข่ายให้ตรงตามวัตถุประสงค์ขององค์กรได้ โดยสามารถพิจารณาการออกแบบและการติดตั้งได้จากบทที่ 3 และผู้ออกแบบจะต้องมีการพิจารณาให้พร้อมสำหรับการรองรับการเปลี่ยนแปลงทางเทคโนโลยีเครือข่ายในอนาคตได้

ดังนั้น ในการวิจัยนี้ เป็นการออกแบบเครือข่ายส่วนตัวเสมือนเพื่อตรวจสอบการทำงาน จึงออกแบบเครือข่ายส่วนตัวเสมือนโดยใช้แบบไฟร์วอลล์ทูไคล์เอนท์โทโปโลยี และเลือกที่จะทำการติดตั้งในรูปแบบอินทราคอมพานี โดยได้มีการออกแบบเครือข่ายส่วนตัวเสมือนสำหรับการตรวจสอบเป็น 2 รูปแบบ คือ

1. เครือข่ายส่วนตัวเสมือนในวงแลน
2. เครือข่ายส่วนตัวเสมือนในวงแวน

4.2 การออกแบบและผลการทดสอบเครือข่ายส่วนตัวเสมือนในวงแลน

สามารถแบ่งขั้นตอนในการออกแบบและทดสอบได้ 2 ขั้น คือ

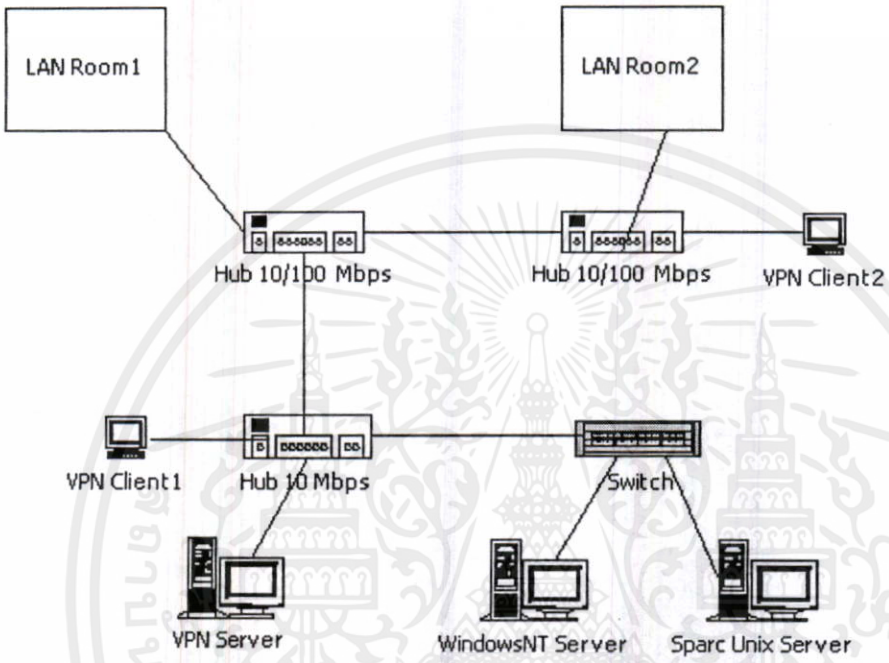
1. วิธีการทดสอบ
2. ผลการทดสอบที่ได้

ซึ่งจะมีรายละเอียดการดำเนินงานดังนี้

4.2.1 วิธีการทดสอบ

1. เลือกจุดหรือสถานที่ที่จะทำการติดตั้งเครือข่ายส่วนตัวเสมือน
2. ทำการเลือกอุปกรณ์ที่จะใช้ในการติดตั้งเครือข่าย กำหนดรายละเอียดของอุปกรณ์ฮาร์ดแวร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ไคล์เอนท์และเครื่องเซิฟเวอร์ฮับ เป็นต้น และติดตั้งดังรูปที่ 4.1
3. ทำการติดตั้งซอฟแวร์วีพีเอ็นที่เครื่องไคล์เอนท์และเครื่องเซิฟเวอร์ โดยใช้อัลกอริทึมเอ็นคริปชันแบบ RC5 และอัลกอริทึมออเท็นทิเคท แบบ MD5 Keyed และการบริหารคีย์จะใช้ SKIP Management
4. ทำการตรวจจับแพ็กเกตที่ใช้ในการรับส่งข้อมูล ระหว่างเครื่องไคล์เอนท์ และเครื่องเซิฟเวอร์ ขณะที่ใช้วีพีเอ็น และไม่ใช้วีพีเอ็น

5. ทำการทดสอบพารามิเตอร์ที่สำคัญทางด้านเน็ตเวิร์ค 2 ค่า คือ (1) ค่าลาเทนซี (Latency) โดยใช้วิธีการ Ping จำนวน 1,000 รอบ ด้วยค่า Payload ที่แตกต่างกัน ตั้งแต่ 512 1,024 2,048 และ 3,072 ไบท์ และ (2) ค่าทรูพุท (Throughput) โดยใช้วิธีตรวจสอบจาก FTP ไฟล์ ขนาดตั้งแต่ 3 5 7 และ 15 MB



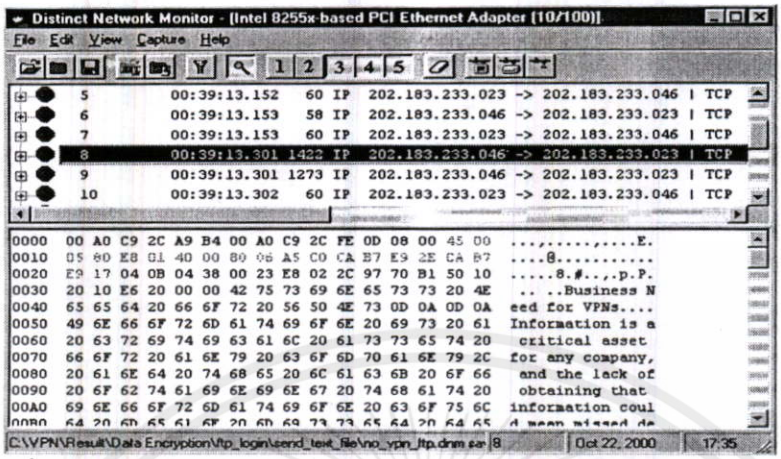
รูปที่ 4.1 เครือข่ายส่วนตัวเสมือนในวงแลน

4.2.2 ผลการทดสอบเครือข่ายส่วนตัวเสมือนในวงแลน

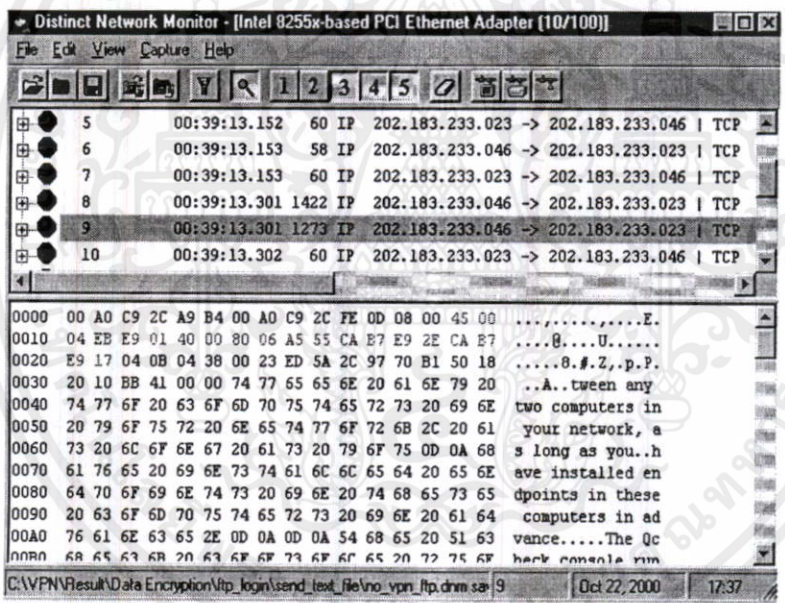
1.ผลการตรวจสอบแพ็กเกต เพื่อตรวจสอบความปลอดภัย

หลักสำคัญในการจะทำให้เกิดความปลอดภัยในเครือข่ายส่วนตัวเสมือน พบว่าจะต้องทำให้แพ็กเกตข้อมูลถูกเอ็นท์คริปท์ชันในเครือข่ายที่ส่งจากต้นทางไปสู่ปลายทาง จึงทำให้ไม่มีผู้ลักลอบสามารถนำข้อมูลที่อยู่ระหว่างการส่งไปใช้งานได้ ซึ่งสามารถดูได้จากรูปแบบการบุกรุกของผู้ลักลอบได้จากบทที่ 2 จึงทำการทดสอบแพ็กเกตขณะที่ใช้ในเครือข่ายส่วนตัวเสมือน และขณะที่ไม่ใช้เครือข่ายส่วนตัวเสมือน ทำการส่งข้อมูล แล้วใช้โปรแกรมตรวจจับแพ็กเกตตรวจสอบจะได้ผลดังรูปที่ 4.2, 4.3 และ 4.4 ซึ่งเป็นแพ็ตเก็ตที่ได้จากเครือข่ายธรรมดา สามารถอ่านข้อมูลที่ทำการส่งได้ ส่วนผลที่ได้จากรูปที่ 4.5, 4.6 และ 4.7 ซึ่งเป็นแพ็กเกตที่ได้จากเครือข่ายส่วนตัวเสมือนไม่สามารถจะอ่านข้อมูลที่ทำการส่งได้ ข้อมูลที่เห็นจะเป็นขยะหรือเรียกว่า ไซเฟอร์เท็ก

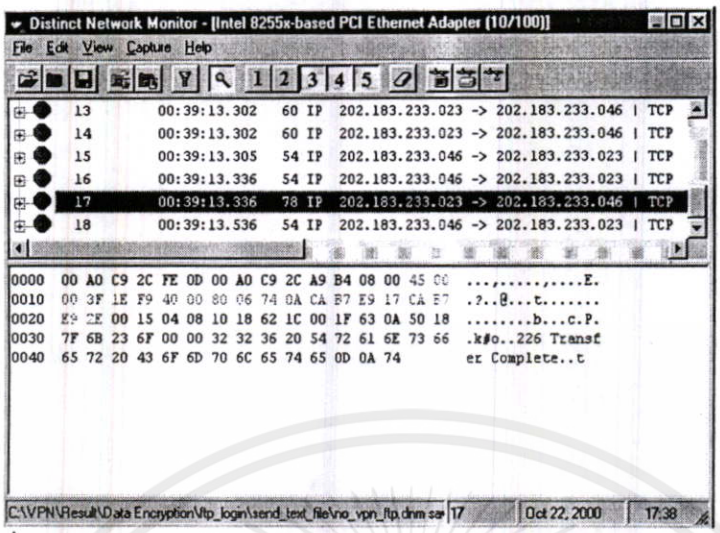
การตรวจจับแพ็กเกต ขณะไม่ใช้วีพีเอ็น



รูปที่ 4.2 ผลการตรวจสอบแพ็กเกต ขณะไม่ใช้วีพีเอ็น

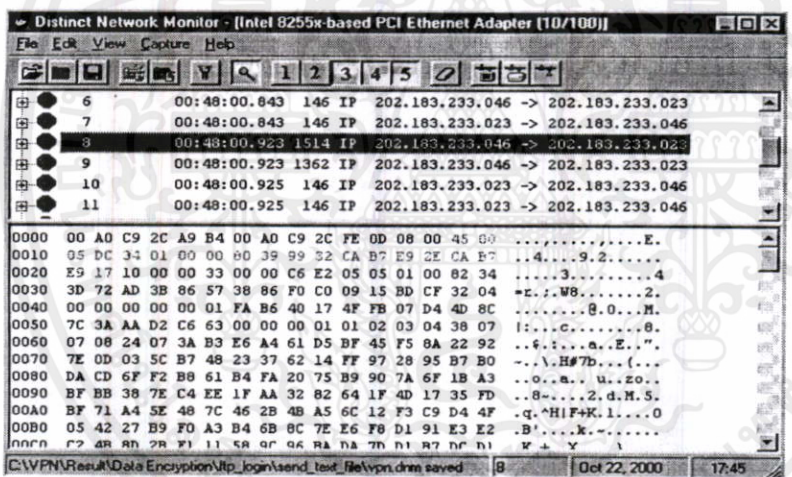


รูปที่ 4.3 ผลการตรวจสอบแพ็กเกต ขณะไม่ใช้วีพีเอ็น

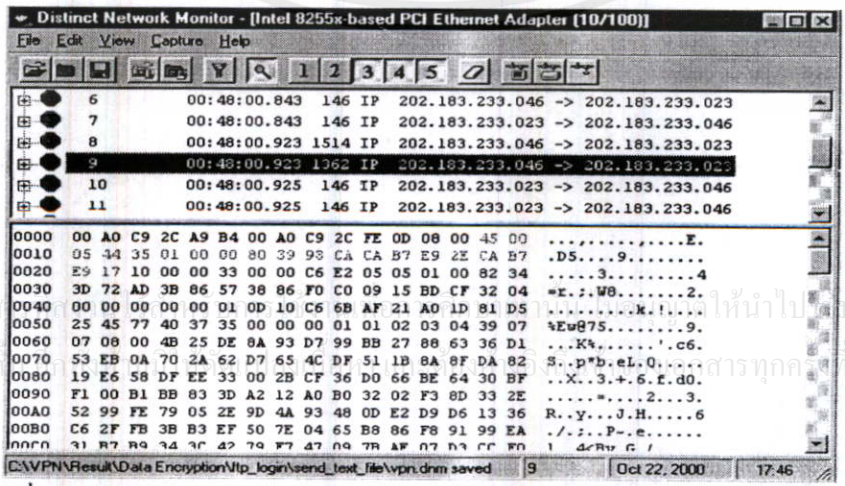


รูปที่ 4.4 ผลการตรวจสอบแพ็กเกต ขณะไม่ใช้วีพีเอ็น

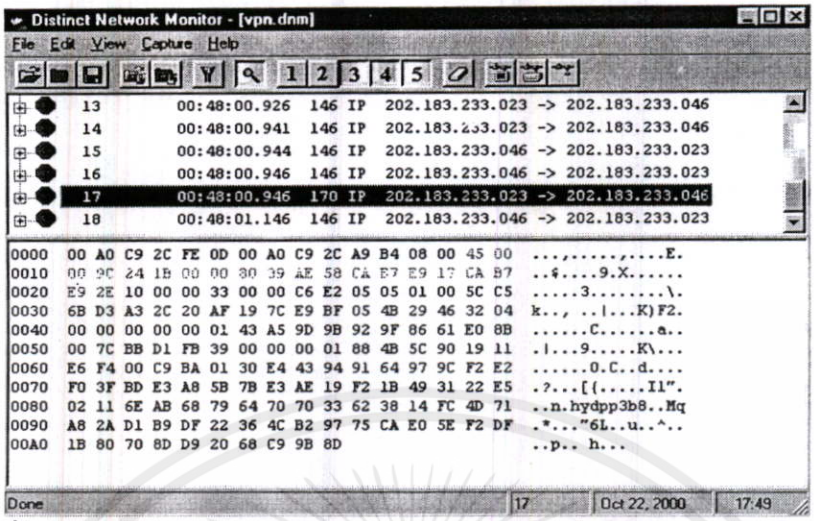
การตรวจสอบแพ็กเกต ขณะใช้วีพีเอ็น



รูปที่ 4.5 ผลการตรวจสอบแพ็กเกต ขณะใช้วีพีเอ็น



รูปที่ 4.6 ผลการตรวจสอบแพ็กเกต ขณะใช้วีพีเอ็น



รูปที่ 4.7 ผลการตรวจสอบแพ็กเกต ขณะใช้วีพีเอ็น

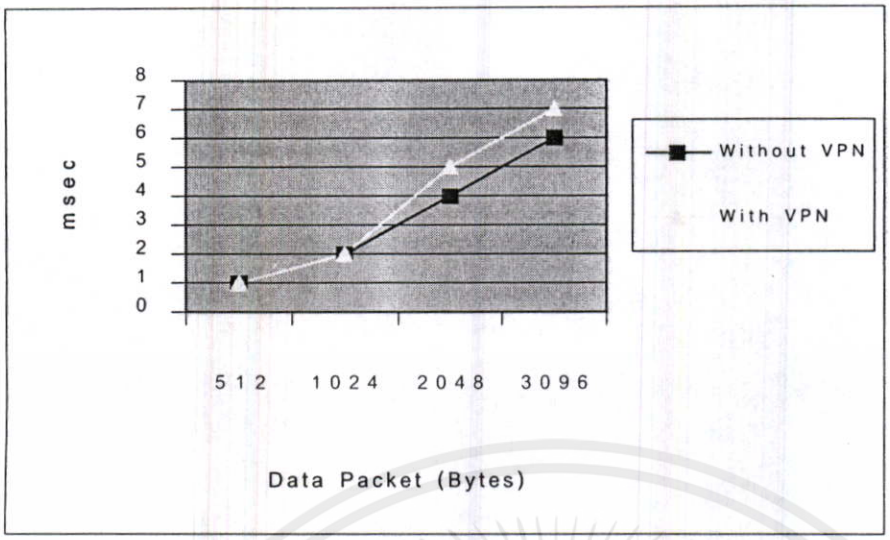
2. ผลทดสอบด้านเน็ตเวิร์ค

2.1 ค่าลาเทนซี (Latency)

ตารางที่ 4.1 แสดงค่าลาเทนซีที่วัดได้

Data Size	VPN (Min/max/avg)	No VPN (Min/max/avg)
512	2/4/1	1/3/1
1024	3/4/2	2/2/2
2048	5/9/5	4/6/4
3096	7/11/7	6/7/6

เมื่อนำข้อมูลที่ได้มาเขียนเป็นกราฟจะทำให้สามารถเปรียบเทียบข้อมูลได้ดังนี้



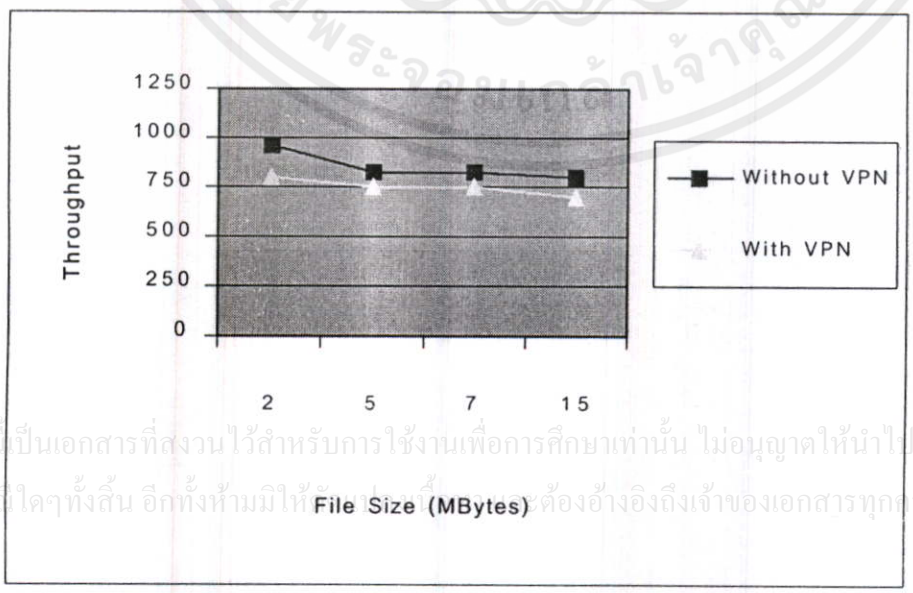
รูปที่ 4.8 กราฟแสดงผลการทดสอบค่าลาเทนซีในวงแลน

2.2 ค่าทรูพุท (Throughput)

ตารางที่ 4.2 แสดงการวัดค่าทรูพุท

File Size	Without VPN	With VPN
2	963.154	804.162
5	830.918	753.37
7	820.682	751.188
15	804.038	698.088

เมื่อนำข้อมูลที่ได้มาเขียนเป็นกราฟจะทำให้สามารถเปรียบเทียบข้อมูลได้ดังนี้



รูปที่ 4.9 กราฟแสดงผลการทดสอบค่าทรูพุทในวงแลน

4.3 การออกแบบและทดสอบเครือข่ายส่วนตัวเสมือนในวงแวน

สามารถแบ่งขั้นตอนในการออกแบบและทดสอบได้ 2 ขั้น คือ

1. วิธีการทดสอบ
2. ผลการทดสอบที่ได้

ซึ่งจะมีรายละเอียดการดำเนินงานดังนี้

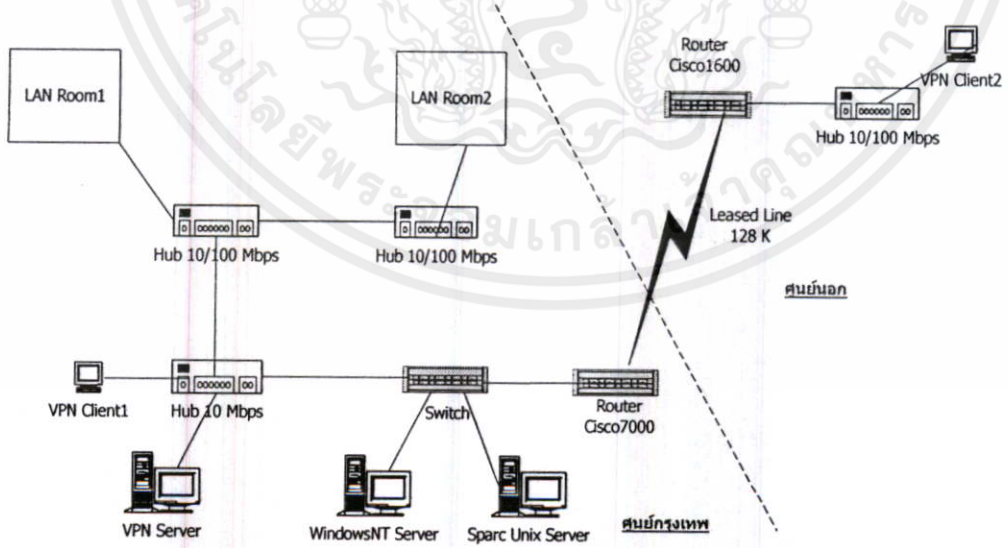
4.3.1 วิธีการทดสอบ

1.เลือกจุดหรือสถานที่ที่จะทำการติดตั้งเครือข่ายส่วนตัวเสมือน

2.ทำการเลือกอุปกรณ์ที่จะใช้ในการติดตั้งเครือข่าย กำหนดรายละเอียดของอุปกรณ์ฮาร์ดแวร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ไคล์เอนท์และเครื่องเซิฟเวอร์ ฮับ เป็นต้น และติดตั้งดังรูปที่ 4.10

3.ทำการติดตั้งซอฟแวร์วีพีเอ็นที่เครื่องไคล์เอนท์ และเครื่องเซิฟเวอร์ โดยใช้อัลกอริทึมเอ็น-คริปชันแบบ RC5 และอัลกอริทึมออเท็นทิเคทแบบ MD5 Keyed และการบริหารคีย์จะใช้ SKIP Management

4.ทำการทดสอบพารามิเตอร์ที่สำคัญทางด้านเน็ตเวิร์ค 2 ค่า คือ (1) ค่าลาเทนซี (Latency) โดยใช้วิธีการ Ping จำนวน 1,000 รอบ ด้วยค่า Payload ที่แตกต่างกัน ตั้งแต่ 512 1,024 2,048 และ 3,072 ไบท์ และ (2) ค่าทรูพุท (Throughput) โดยใช้วิธีตรวจสอบจาก FTP ไฟล์ ขนาดตั้งแต่ 3 5 7 และ 15 MB



รูปที่ 4.10 เครือข่ายส่วนตัวเสมือนในวงแวน

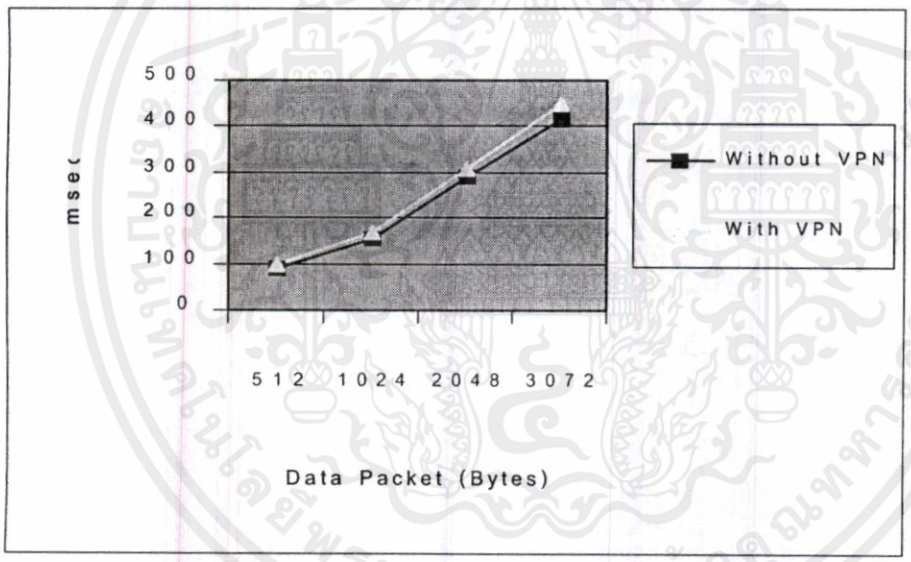
4.3.2 ผลการทดสอบเครือข่ายส่วนตัวเสมือนในวงแวน

1.ค่าลาเทนซี (Latency)

ตารางที่ 4.3 แสดงค่าลาเทนซี

Data Size	Without VPN (Min/max/avg)	With VPN (Min/max/avg)
512	83/190/89	96/112/97
1024	153/189/156	167/182/168
2048	284/289/281	309/322/310
3072	413/429/416	448/462/449

เมื่อนำข้อมูลที่ได้มาเขียนเป็นกราฟจะทำให้สามารถเปรียบเทียบข้อมูลได้ดังนี้

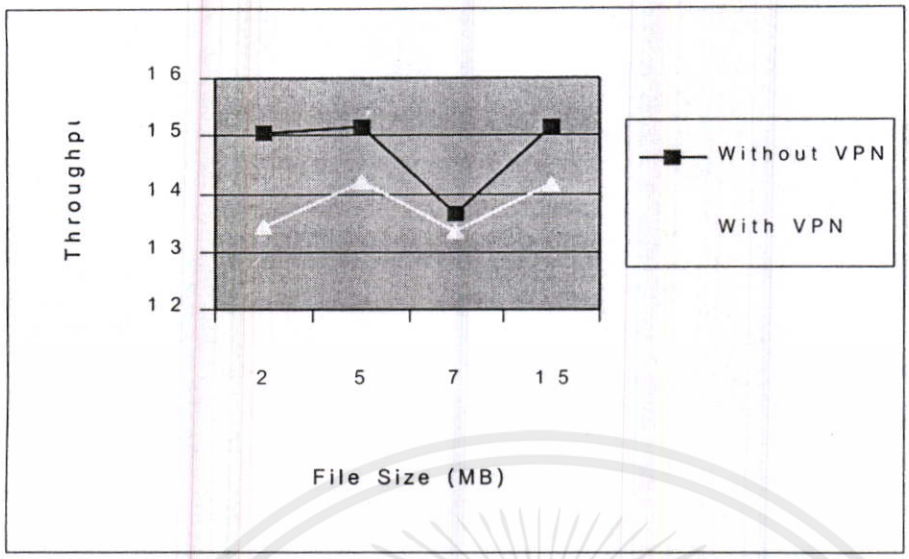


รูปที่ 4.11 กราฟแสดงผลการทดสอบค่าลาเทนซีในวงแวน

ตารางที่ 4.4 แสดงการวัดค่าทรูพุท

File Size	Without VPN	With VPN
2	15.03	13.43
5	15.17	14.22
7	13.64	13.34
15	15.16	14.15

เมื่อนำข้อมูลที่ได้มาเขียนเป็นกราฟจะทำให้สามารถเปรียบเทียบข้อมูลได้ดังนี้



รูปที่ 4.12 กราฟแสดงผลการทดสอบค่าทรูพุทในวงแวน

บทที่ 5
สรุปผล และวิจารณ์

ผลการตรวจสอบเครือข่ายคอมพิวเตอร์ที่การติดตั้งแบบอินทราคอมพานี เป็นเครือข่ายส่วนตัวเสมือนในวงแลน และวงแวน จะได้ว่าแพ็กเกตข้อมูลที่มีการรับส่งระหว่างต้นทาง และปลายทางมีความปลอดภัย เพราะว่าจากผลที่ได้จากการตรวจสอบแพ็กเก็ตของข้อมูล ขณะใช้วีพีเอ็น ไม่สามารถอ่านข้อมูลที่รับส่งกันได้ แต่ถ้าไม่ใช้วีพีเอ็นจะสามารถอ่านข้อมูลเหล่านั้นได้ ด้วยเหตุที่เครือข่ายส่วนตัวเสมือนมีการใช้หลักการของการเอ็นคริปท์ชัน ทำให้แพ็กเก็ตของข้อมูลมีความปลอดภัย และผลที่ได้จากการเปรียบเทียบประสิทธิภาพของเครือข่ายคอมพิวเตอร์ โดยพิจารณาจากพารามิเตอร์ที่สำคัญทางเน็ตเวิร์ค 2 ค่าคือ (1) ค่าลาเทนซี และ (2) ค่าทรูพุท พบว่าเครือข่ายส่วนตัวเสมือนในวงแลน และวงแวน จะมีค่าที่ต่ำกว่าเครือข่ายคอมพิวเตอร์ธรรมดาไม่มากนัก

ด้วยเหตุนี้ การที่จะนำเครือข่ายส่วนตัวเสมือนมาใช้ภายในองค์กร หรือภายนอกองค์กรโดยการติดตั้งแบบอินทราคอมพานี ถือว่ามีความปลอดภัย และเหมาะสมที่จะนำมาเป็นเครือข่ายส่วนตัวเสมือนมาใช้ในการรักษาระบบเน็ตเวิร์คให้มีความปลอดภัย และสะดวกในการประยุกต์ใช้งานในอนาคตได้เป็นอย่างดี สามารถสรุปประโยชน์เครือข่ายส่วนตัวเสมือนได้ดังนี้

1. ทำให้มั่นใจได้ว่าข้อมูลที่สำคัญ จะได้รับการส่งผ่านเครือข่ายโดยได้รับความปลอดภัย
2. สามารถตรวจสอบได้ว่าผู้ใช้งานที่ได้รับอนุญาตเท่านั้น จึงจะได้เป็นผู้ใช้ข้อมูลที่สำคัญ
3. รองรับการขยายตัวของผู้ใช้งานได้มากขึ้น และเครือข่ายในอนาคตได้อย่างคล่องตัว

การวิจารณ์

1.ผู้ที่จะนำเครือข่ายส่วนตัวเสมือนไปใช้งานควรที่จะเข้าใจการทำงานอัลกอริทึมเอ็นคริปท์ชันว่า ณ ปัจจุบันมีการพัฒนาอัลกอริทึมรุ่นใหม่ๆ ที่จะให้ความปลอดภัยกับเครือข่ายมากยิ่งขึ้นได้ เพราะว่าจะทำให้สามารถตัดสินใจในการนำระบบเครือข่ายส่วนตัวเสมือนมาใช้งานได้อย่างเหมาะสมกับเทคโนโลยีที่มีการเปลี่ยนแปลงอย่างรวดเร็ว

2.เซิฟเวอร์ที่จะใช้งานควรมีความเร็วของซีพียู ตั้งแต่รุ่นเพนเทียมทรี 300 MHz ขึ้นไป และมีหน่วยความจำ (SDRAM) 128 MB ขึ้นไป เพราะว่าจะทำให้ระบบเครือข่ายส่วนตัวเสมือนไม่รวน

เอกสารอ้างอิง

1. U. Black, "Computer Networks Protocols, Standards and Interface," 1995, New Jersey , Prentice-Hall
2. W. Stalling, "Data and Computer Communications," 5th ed., 1997, New Jersey, Prentice-Hall
3. E.C. Kim, C.S. Hong, J.G. Song, "The Multi-layer VPN Management Architecture," 1997, Telecommunication Network laboratory, Korea Telecom
4. L.G. Paul, "Who's At the Other End of your VPN?," 2000, available:http://www.EarthWeb's Crossnodes.com/Source/From_Web/VPN/EarthWeb's Crossnodes_com_Networking Resourxes for IT Professionals.html
5. J. Mizusawa, N. Shigematsu, H. Itoh, "Virtual Private Network Control System Concept," 2000, available: http://lcspub.psu.edu/entry/iel.html
6. J. Mizusawa, N. Shigematsu, H. Itoh, "Virtual Private Network Control System Concept," 2000, available: http://lcspub.psu.edu/entry/iel.html
7. G.S. Malkin, "Dial-in Virtual Private Networks Using Layer 3 Tunneling," 2000, available:http://www.lcspub.psu.edu/entry/iel.html
8. R. Baldwin, "The RC5, RC5-CBC, RC5-CBC-PAD and RC5-CTS Algorithms," 1996, MIT Laboratory for Computer Science and RSA Data Security
9. N. Anerousis, "Dynamic virtual network dimensioning in cost sensitive environments," Global Telecommunications Conference, 1999.
10. A.S. Tanenbaum, "Computer Network," Prentice-Hall, 1996

ผลงานที่ได้รับการตีพิมพ์

1. บทความชุดตรวจวัดค่าสัมประสิทธิ์ซีเบค ลงวารสารสมาคมฟิสิกส์แห่งประเทศไทย
2. บทความการออกแบบระบบเครือข่ายส่วนตัวเสมือน เพื่อตรวจสอบการทำงานลงวารสาร วิศวสาร ลาดกระบัง

ISSN 0125-1724

วิศวสาร ลาดกระบัง

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

LADKRABANG ENGINEERING JOURNAL

ปีที่ 18 ฉบับที่ 2 มิถุนายน 2544

การออกแบบระบบเครือข่ายส่วนตัวเสมือน เพื่อตรวจสอบการทำงาน

Virtual Private Networking Design-Aided Performances Monitoring

วิโรจน์ จงชนะชววัฒน์ กอบชัย เดชหาญ

คณะวิศวกรรมศาสตร์ และสำนักวิจัยการสื่อสารและเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

บทคัดย่อ

เทคโนโลยีคอมพิวเตอร์เน็ตเวิร์คได้มีการพัฒนาไปในหลายๆ รูปแบบ เพื่อให้สามารถที่จะทำการติดต่อสื่อสารกันได้สะดวกรวดเร็วยิ่งขึ้น และสามารถที่จะใช้ประโยชน์ให้ได้สูงสุดต่อการลงทุนและสามารถออกแบบโครงข่ายคอมพิวเตอร์เพื่อรองรับการขยายตัวทางธุรกิจได้อย่างคุ้มค่า บทความนี้เป็นการออกแบบเครือข่ายส่วนตัวเสมือน (Virtual Private Networking) โดยออกแบบเป็นไฟร์วอลล์ทูไคล์เอนท์ไท-ไปโลยี และปฏิบัติการตรวจสอบเพื่อแสดงให้เห็นถึงข้อมูลที่ใช้หลักการวีพีเอ็นในการเอ็นคริปท์ข้อมูล ซึ่งสามารถที่จะทำให้ข้อมูลมีความปลอดภัย และยังคงมีประสิทธิภาพที่ยอมรับได้ ในการใช้งานผ่านเครือข่ายแลน และแวน

Abstract

Computer networking technology goes faster in any ways to have the convenient communication with maximize profit from IT investment. This paper proposes a principle of the virtual private networking (VPN) in order to use the encrypted data packets for private path in data communication of computer system. The call abbreviate to VPN theory, the principle of this theory is an encription and decription of data packet for data security system. This design and implementation can prove VPN on firewall to client topology of LAN and WAN that have the security with good performances.

1. บทนำ

ปัจจุบัน ความปลอดภัยของข้อมูลในเครือข่ายคอมพิวเตอร์ ถือเป็นเรื่องที่ต้องให้ความสำคัญเป็นอันดับต้นๆ ในเวลานี้ เนื่องจากข้อมูลที่มีความสำคัญต่อองค์กรนั้น ไม่ต้องการให้บุคคลภายนอกหรือบุคคลภายในองค์กรที่ไม่ได้รับสิทธิในการรับรู้ข่าวสารข้อมูลเหล่านั้น จึงได้มีเทคโนโลยีวีพีเอ็นที่จะทำให้ปัญหาเหล่านี้ได้รับการแก้ไขและมีบทบาทอย่างมากต่อการพัฒนาระบบเครือข่ายคอมพิวเตอร์ในอนาคต เพราะการใช้วีพีเอ็น เป็นเครือข่ายส่วนตัวเสมือนในเครือข่ายหลักขององค์กรนั้น ผู้บริหารเครือข่ายจะต้องรับรู้ถึงสมรรถนะของเครือข่ายส่วนตัวเสมือนนั้น เพื่อสามารถนำมาใช้งานได้อย่างมีประสิทธิภาพ และบริหารงานเครือข่ายส่วนตัวเสมือน เพื่อให้องค์กรนั้นสามารถเก็บข้อมูลสงวนที่สำคัญขององค์กรไว้ได้

Ladkrabang Engineering Journal, Vol.18, No. 2, June 2001

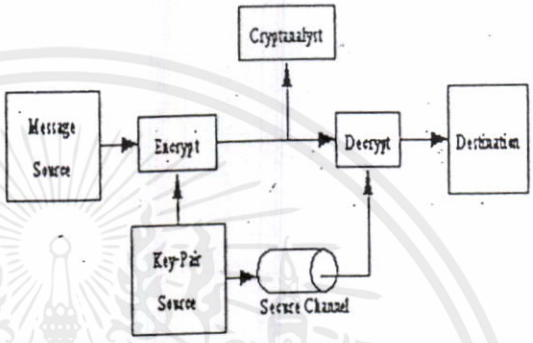
พร้อมที่จะเผชิญหน้ากับการแข่งขันในยุคข่าวสาร ถึงกับมีการกล่าวว่า องค์กรใดคุมข่าวสารได้มาก องค์กรนั้นก็จะสามารถประกอบธุรกิจได้อย่างมีประสิทธิภาพ และดำรงอยู่ภายใต้สิ่งแวดล้อมทางธุรกิจที่มีการเปลี่ยนแปลงอย่างรวดเร็วได้ จึงเป็นเหตุให้มีการวิจัยการออกแบบเครือข่ายส่วนตัวเสมือนเพื่อตรวจสอบการทำงาน

2. ทฤษฎี และหลักการ

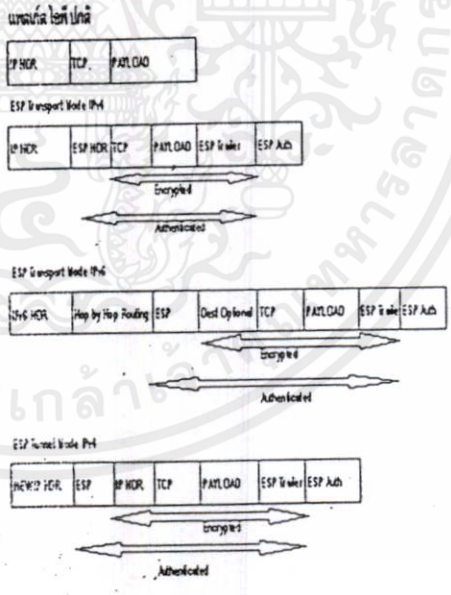
วีพีเอ็น (Virtual Private Networks; VPN) หรือ เครือข่ายส่วนตัวเสมือน มีความหมายว่าเป็นการทำให้เครือข่ายสาธารณะ หรือเครือข่ายภายในองค์กร สามารถเป็นเส้นทางผ่านของเครือข่ายที่ผู้ใช้งานที่มีสิทธิเท่านั้น จึงจะสามารถเห็นข้อมูลเหล่านั้นได้ โดยนำหลักการของการเอ็นคริปท์ชัน และดีคริปท์ชันแพ็กเก็ต เพื่อให้ข้อมูลมีความปลอดภัย และบุคคลที่มีสิทธิเท่านั้น จึงจะสามารถอ่านข้อมูลเหล่านั้นได้ โดยที่ใช้เครือข่ายสาธารณะหรือเครือข่ายภายในองค์กร เป็นสื่อกลางในการติดต่อสื่อสารผ่านเครือข่าย จึงเรียกว่า เป็นเครือข่ายส่วนตัวเสมือนประกอบด้วยหลักการดังนี้

2.1 ระบบคริปท์โตกราฟี

ระบบคริปท์โตกราฟี คือกระบวนการที่ทำให้ข้อมูลอักษรที่อ่านออก (Plaintext) ให้กลายเป็นข้อมูลที่ไม่สามารถอ่านความหมายได้ (Ciphertext) และทำนองกลับกันคือทำให้ข้อมูลที่ไม่สามารถอ่านความหมายได้ กลายเป็นข้อมูลที่อ่านได้ โดยใช้อัลกอริทึมเอ็นคริปท์ชันในการดำเนินงานซึ่งกระบวนการในระบบคริปท์โตกราฟี จะเป็นดังขั้นตอนในรูปที่ 1 ในระบบคริปท์โตกราฟีนั้น จะต้องมีอัลกอริทึมเอ็นคริปท์ ซึ่งอัลกอริทึมเอ็นคริปท์ชัน จะเป็นส่วนที่ทำให้เกิดกระเอ็นคริปท์ แพ็กเก็ตในรูปแบบต่างๆ โดยอาศัยหลักการทางคณิตศาสตร์มาประยุกต์ใช้ให้เกิดรูปแบบ ในการเอ็น คริปท์ชันแพ็กเก็ต ซึ่งอัลกอริทึมที่ใช้ คือ DES RC2 RC4 RC5 เป็นต้น และอัลกอริทึมออเท็นทิเคท (Authenticate) เป็นการให้ผู้มีสิทธิสามารถได้รับข้อมูลและอ่านข้อมูลได้นั้นจะต้องมีการใส่สิทธิลงในแพ็กเก็ตนั้นๆ เพื่อตรวจสอบว่าผู้ที่ได้สิทธินั้นสามารถได้รับและอ่านข้อมูลเหล่านั้นได้ ซึ่งอัลกอริทึมออเท็นทิเคทสำหรับเรื่องการให้มีดังนี้ คือ MD2 MD4 MD5 HMAC-SHA และ HMAC-MD5 เป็นต้น ซึ่งในแต่ละรูปแบบจะมีการใช้หลักทางคณิตศาสตร์มาเป็นรูปแบบ ในการคิดคำนวณสามารถดูการทำงานที่ระดับแพ็กเก็ตได้จากรูปที่ 2



รูปที่ 1 แสดงระบบคริปท์โตกราฟี



รูปที่ 2 แสดงการเอ็นคริปท์ชันแพ็กเก็ต

2.2 โทโปโลยีวีพีเอ็น

พิจารณาเฉพาะโทโปโลยีวีพีเอ็นที่สำคัญได้ดังนี้คือ

2.2.1 ไฟร์วอลล์ทูไคล์เอนท์โทโปโลยี

2.2.2 แลนทูแลนโทโปโลยี

2.2.3 ไฟร์วอลล์ทูอินเทอร์เน็ต หรือเอ็กซ์ตร้าเน็ตโทโปโลยี

2.2.4 เฟรม หรือเอทีเอ็มโทโปโลยี

2.3 รูปแบบการติดตั้งเครือข่ายส่วนตัวเสมือน

จากการที่ได้ทราบถึงทฤษฎีต่าง ๆ ที่เกี่ยวข้องกับการออกแบบเครือข่ายส่วนตัวเสมือน ในทางปฏิบัตินั้น จะต้องมีการเข้าใจถึงรูปแบบของการติดตั้งเครือข่ายส่วนตัวเสมือนเพื่อสามารถที่ทำให้การออกแบบเครือข่ายส่วนตัวเสมือนตรงตามวัตถุประสงค์ขององค์กรที่ต้องการให้เครือข่ายคอมพิวเตอร์มีความปลอดภัยอย่างไร ซึ่งรูปแบบหลักของการติดตั้งเครือข่ายส่วนตัวเสมือนมีทั้งหมด 4 แบบ ดังนี้

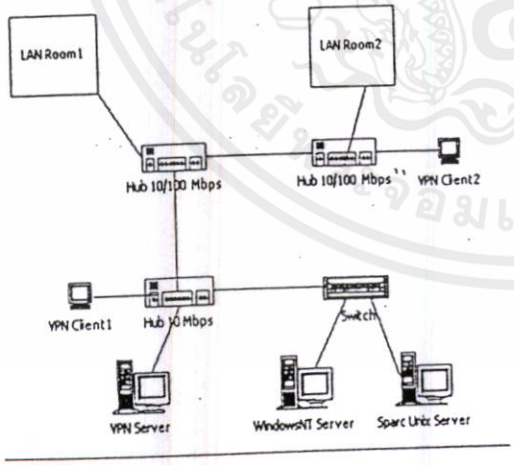
2.3.1 อินทราเน็ต

2.3.2 รีโมตแอสเซส

2.3.3 เอ็กซ์ตร้าเน็ต

2.3.4 อินทราคอมพานี

ในบทความนี้ จึงได้ใช้โทโปโลยีแบบไฟร์วอลล์ทูไคล์เอนท์ และทำการติดตั้งแบบอินทราคอมพานี มาทำการทดสอบการสร้างเครือข่ายส่วนตัวเสมือน

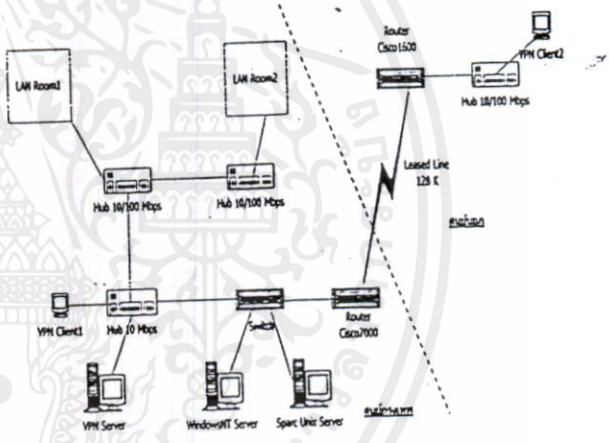


รูปที่ 3 แสดงเครือข่ายส่วนตัวเสมือนในวงแลน

3. การออกแบบเครือข่าย ส่วนตัวเสมือน

3.1 เครือข่ายส่วนตัวเสมือน ในเครือข่ายแลน และแวน มีขั้นตอนเหมือนกันในการดำเนินงานดังนี้

1. เลือกจุด หรือสถานที่ที่จะทำการติดตั้งเครือข่ายส่วนตัวเสมือน
2. ทำการเลือกอุปกรณ์ที่จะใช้ในการติดตั้งเครือข่าย กำหนดรายละเอียดของอุปกรณ์ฮาร์ดแวร์ต่างๆ เช่น เครื่องคอมพิวเตอร์ไคล์เอนท์ เครื่องคอมพิวเตอร์เซิฟเวอร์ ฮับ เป็นต้น
3. ทำการติดตั้งซอฟแวร์วีพีเอ็นที่เครื่องไคล์เอนท์ และเครื่องเซิฟเวอร์ ดังรูปที่ 3 โดยได้ใช้อัลกอริทึมเอ็นคริปท์ชันแบบ RC5 และอัลกอริทึมออเท็นทิเคท แบบ MD5 Keyed และการบริหารคีย์ ในการเอ็นคริปท์จะใช้ SKIP Management



รูปที่ 4 แสดงเครือข่ายส่วนตัวเสมือนในวงแวน

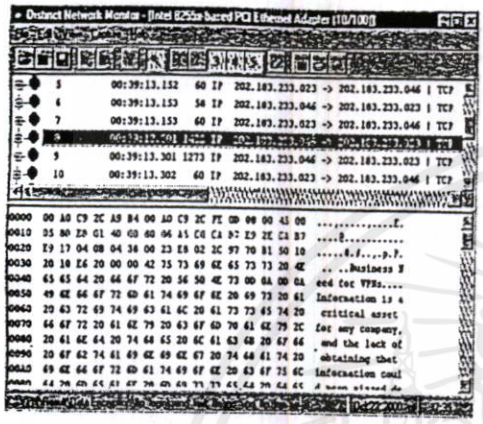
4. ผลที่ได้จากการตรวจสอบการทำงานเครือข่ายส่วนตัวเสมือน

ในการตรวจสอบการทำงานเครือข่าย จะใช้พารามิเตอร์ที่สำคัญ คือ ค่าลาเทนซี (Latency) และค่าทรูพุท (Throughput) ซึ่งเครื่องคอมพิวเตอร์เซิฟเวอร์ที่ใช้ เป็นเพนเทียมทรี 455 MHz และเครื่องไคล์เอนท์เป็นเพนเทียมทู 233 MHz ค่าลาเทนซีใช้วิธีการ Ping โดยใช้ Payload ที่แตกต่างกัน ตั้งแต่ 512, 1,024, 2,048 และ 3,072 Bytes และค่าทรูพุท ใช้วิธีตรวจสอบจาก FTP ไฟล์ขนาดตั้งแต่ 3, 5, 7 และ 15 MB

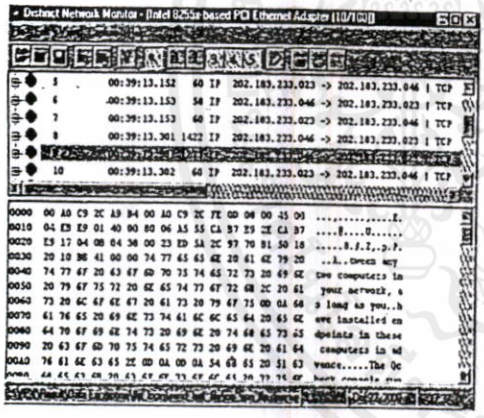
Ladkrabang Engineering Journal, Vol.18, No. 2, June 2001

4.1 ผลที่ได้จากการตรวจจับแพ็กเก็ต

แพ็กเก็ตขณะไม่ใช้วีพีเอ็น

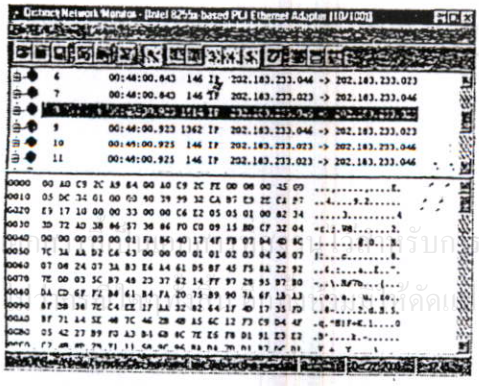


รูปที่ 5 แสดงการตรวจแพ็กเก็ตขณะไม่ใช้วีพีเอ็น

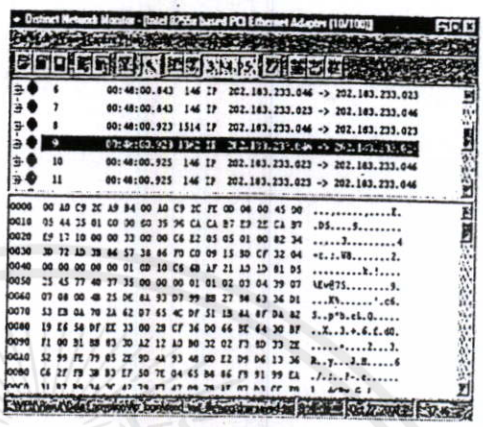


รูปที่ 6 แสดงการตรวจแพ็กเก็ตขณะไม่ใช้วีพีเอ็น

แพ็กเก็ตขณะใช้วีพีเอ็น



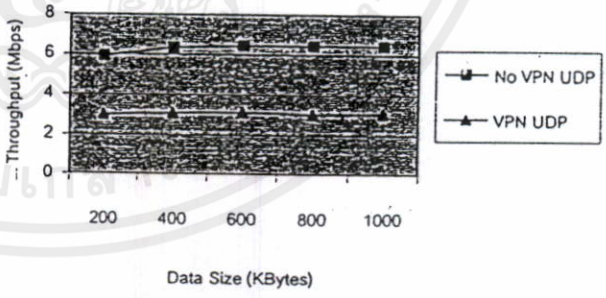
รูปที่ 7 แสดงการตรวจแพ็กเก็ตขณะใช้วีพีเอ็น



รูปที่ 8 แสดงการตรวจแพ็กเก็ตขณะใช้วีพีเอ็น

จากรูปที่ 5,6,7และ8 แพ็กเก็ตขณะที่ไม่ใช้วีพีเอ็น จะเห็นรายละเอียดต่างๆของข้อมูลในแพ็กเก็ตที่ทำการส่งในช่วงเวลานั้น ขณะที่แพ็กเก็ตที่ใช้วีพีเอ็นจะไม่สามารถอ่านรายละเอียดดังกล่าวได้

4.2 ผลที่ได้จากการตรวจสอบทรูพุท UDP

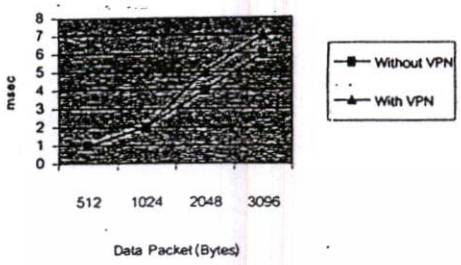


รูปที่ 9 กราฟแสดงผลการตรวจสอบทรูพุทโดยโปรโตคอล UDP

จากกราฟรูปที่ 9 ค่าทรูพุทของ UDP ขณะที่ใช้วีพีเอ็นและไม่ใช้วีพีเอ็น มีความแตกต่างกันไม่มากนัก

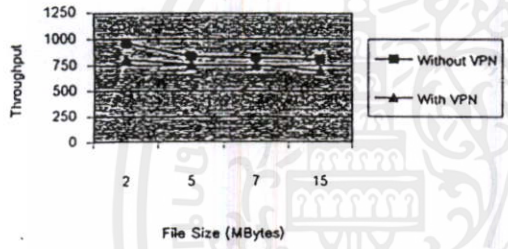
4.3 ผลการทดสอบการทำงานเครือข่ายส่วนตัวเสมือนในแลน

4.3.1 ค่าลาเทนซี (Latency)



รูปที่ 10 กราฟแสดงค่าลาเทนซี ขณะใช้วีพีเอ็น และไม่ใช้วีพีเอ็นในวงแลน

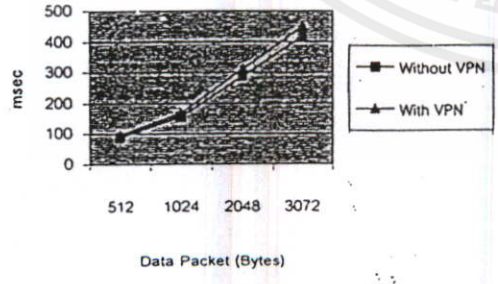
4.3.2 ค่าทรูพุท (Throughput)



รูปที่ 11 กราฟแสดงค่าทรูพุท ขณะใช้วีพีเอ็น และไม่ใช้วีพีเอ็นในวงแลน

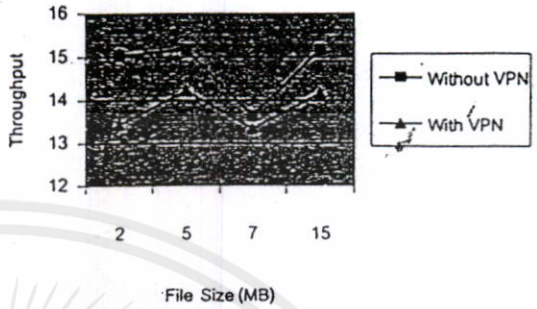
4.4 ผลการทดสอบการทำงานเครือข่ายส่วนตัวเสมือนในแวน

4.4.1 ลาเทนซี (Latency)



รูปที่ 12 กราฟแสดงค่าลาเทนซี ขณะใช้วีพีเอ็น และไม่ใช้วีพีเอ็นในวงแวน

4.4.2 ค่าทรูพุท (Throughput)



รูปที่ 13 กราฟแสดงค่าทรูพุท ขณะใช้วีพีเอ็น และไม่ใช้วีพีเอ็นในวงแลน

ผลที่ได้จากกราฟรูปที่ 10, 11, 12 และ 13 ค่าลาเทนซี และค่าทรูพุท ที่ได้ขณะใช้วีพีเอ็น และไม่ใช้วีพีเอ็นมีค่าไม่แตกต่างกันมากนัก

5.สรุปผลการทดสอบ

เครือข่ายส่วนตัวเสมือน ถือว่ามีการทำงานโดยอาศัยหลักการการเอ็นคริปท์ชัน ซึ่งใช้อัลกอริทึมในการเอ็นคริปท์จากหลักการทางคณิตศาสตร์ จึงทำให้ข้อมูลมีความปลอดภัย โดยผู้ที่ไม่ได้สิทธิในการใช้งานจริง จะไม่สามารถอ่านความหมายของข้อมูลนั้นได้ ซึ่งพิจารณาได้ผลการตรวจจับแพ็กเก็ตในเครือข่าย ถึงแม้ว่าในการทำงานของเครือข่ายจะต้องมีขั้นตอนในการตรวจสอบสิทธิ และการเอ็นคริปท์ ตลอดจนการที่ข้อมูลที่ถูกเอ็นคริปท์ จะถูกดีคริปท์ เพื่อให้สามารถอ่าน และทำงานได้นั้น จะมีรูปแบบขั้นตอนที่มากกว่าปกติก็ตาม แต่จากการตรวจสอบค่าพารามิเตอร์ที่สำคัญทางเน็ตเวิร์ค คือค่าเลเทนซี และค่าทรูพุทของเครือข่ายที่ใช้วีพีเอ็น กับเครือข่ายที่ไม่ใช้วีพีเอ็น ในเครือข่ายแลน และเครือข่ายแวน พบว่ามีค่าที่ไม่แตกต่างกันมากนัก ซึ่งถือว่าคุ้มค่าในการใช้เครือข่ายส่วนตัวเสมือนเพื่อปกป้องข้อมูลที่มีความสำคัญต่อองค์กรได้

6. เอกสารอ้างอิง

[1] N. Anerousis, "Dynamic virtual network dimensioning in cost sensitive environments," Global Telecommunications Conference, 1999.

[2] Y. Ito, O. Maeshima, M. Ishikura, "Bandwidth-guaranteed IP tunneling router With RSVP," available: http ://www.lcspub.psu.edu/entry/ iel.html

[3] G. S. Malkin, "Dial – in virtual private networks using layer 3 tunneling," available: http:// www.lcspub.psu.edu /entry/iel.html

[4] J. Mizuaawa, N. Shigematsu, H. Itoh, "Virtual private network control system concept," Japan, 1988 available: http://www.lcspub.psu.edu/entry/ iel.html

[5] S. Weber, R. Oppliger, D. Hogrefe, "An Optimization method for virtual private network design," The University of Berne, Switzerland.

[6] A. S. Tanenbaum, "Computer Networks," Prentice-Hall,1996.

[7] www.novell.com

ประวัติผู้เขียน

นายวิโรจน์ จงชนะชววัฒน์ สำเร็จการศึกษาปริญญาตรี วิทยาศาสตรบัณฑิต สาขาโซลิตสเตท-อิเล็กทรอนิกส์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง ปีพ.ศ. 2536 และสำเร็จการศึกษาปริญญาโท บริหารธุรกิจมหาบัณฑิต สาขา Operations Management สถาบันบัณฑิตพัฒน-บริหารศาสตร์ ปีพ.ศ. 2542 ทำงานระบบเครือข่ายคอมพิวเตอร์มากว่า 7 ปี ดังนี้ บริษัทบิสนิวส์ จำกัด บริษัทคริสตอลซอฟแวร์ จำกัด บริษัท ดีลอยท์ คอนซัลติ่ง จำกัด และอาจารย์สถาบันราชภัฏสวนดุสิต เป็นต้น และปัจจุบันดำรงตำแหน่งอนุกรรมาธิการงานปกครอง วุฒิสภา