หลักการระบบเครือข่ายคอมพิวเตอร์

Principles of Computer Network

นิพิฐพนธ์ ฤาชา

Nipitpon Ruecha

มหาวิทยาลัยราชภัฏกำแพงเพชร

KAMPHAENG PHET RAJABHAT UNIVERSITY

หลักการระบบเครือข่ายคอมพิวเตอร์
(Principles of Computer Network)

นิพิฐพนธ์ ฤชา

คณะเทคโนโลยีอุตสาหกรรม
มหาวิทยาลัยราชภัฏกำแพงเพชร
2569

หลักการระบบเครือข่ายคอมพิวเตอร์

พิมพ์ครั้งแรก: มิถุนายน 2569
ราคา: 250 บาท

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

นิพิฐพนธ์ ฤๅชา.

หลักการระบบเครือข่ายคอมพิวเตอร์.--ตาก : สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร แม่สอด, 2569.

309 หน้า

1. เครือข่ายคอมพิวเตอร์. 2. เครือข่ายคอมพิวเตอร์ -- การจัดการ. |.ชื่อเรื่อง.

004.6

ISBN (e-book) 978-974-388-411-5

ผู้เขียน: นิพิฐพนธ์ ฤๅขา (วท.ม. เทคโนโลยีสารสนเทศ)

จัดทำโดย:
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏกำแพงเพชร แม่สอด
เลขที่ 222 หมู่ 7 ตำบลแม่ปะ อำเภอแม่สอด
จังหวัดตาก 63110

คำนำ

หนังสือเล่มนี้ได้เรียบเรียงขึ้นมาเพื่อใช้ประกอบการเรียนการสอนรายวิชาหลักการระบบเครือข่ายคอมพิวเตอร์ (Principles of Computer Network) เหมาะสมสำหรับผู้สนใจศึกษาทางด้านเทคโนโลยีคอมพิวเตอร์และระบบเครือข่าย รวมทั้งสาขาอื่นๆ ที่เกี่ยวข้อง

ผู้เรียบเรียงได้กำหนดเนื้อหาทั้งหมด 13 บท ดังนี้ ความรู้เบื้องต้นเกี่ยวกับหลักการระบบเครือข่ายคอมพิวเตอร์ แบบจำลองเครือข่าย ข้อมูลและสัญญาณ สื่อกลางในการรับส่งข้อมูล การเชื่อมต่อเครือข่ายกับอุปกรณ์ต่างๆ การตรวจสอบข้อผิดพลาดและการควบคุมการไหลของข้อมูล ความรู้เบื้องต้นเกี่ยวกับเครือข่ายใช้สาย ความรู้เบื้องต้นเกี่ยวกับเครือข่ายไร้สาย ความรู้เบื้องต้นเกี่ยวกับอินเทอร์เน็ต แอปพลิเคชันบนระบบเครือข่าย ความรู้เบื้องต้นเกี่ยวกับโพรโทคอล การออกแบบและจัดการเครือข่าย การรักษาความปลอดภัยระบบเครือข่าย ตามลำดับ

ผู้เรียบเรียงขอกราบขอบพระคุณผู้ทรงคุณวุฒิทุกท่าน ที่ผู้เรียบเรียงได้อ้างถึงและนำความรู้จากหนังสือ ตำรา และเอกสารที่เกี่ยวข้องมารวบรวมจนทำให้หนังสือเล่มนี้สำเร็จลุล่วงไปได้ด้วยดี จึงขอขอบพระคุณผู้ที่มีส่วนร่วมทุกท่านเป็นอย่างสูงมา ณ โอกาสนี้ และหวังเป็นอย่างยิ่งว่าหนังสือเล่มนี้จะเป็นประโยชน์แก่นิสิต นักศึกษา และผู้สนใจทั่วไป ทำให้ได้รับความรู้และเกิดความเข้าใจในหลักการระบบเครือข่ายคอมพิวเตอร์ไม่มากก็น้อย สามารถนำความรู้ความเข้าใจที่ได้ไปเป็นพื้นฐานเพื่อศึกษาต่อไปได้ หากมีข้อบกพร่องประการใด ผู้เรียบเรียงขออภัยและจะปรับปรุงให้เหมาะสมในครั้งต่อไป

นิพิฐพนธ์ ฤๅชา

2569

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
ความรู้เบื้องต้นเกี่ยวกับหลักการระบบเครือข่ายคอมพิวเตอร์

เทคโนโลยีด้านระบบเครือข่ายคอมพิวเตอร์ มีบทบาทสำคัญต่อการเปลี่ยนแปลงวิถีการดำรงชีวิตของมนุษย์และการทำธุรกิจในยุคปัจจุบัน โดยเฉพาะการตัดสินใจทางธุรกิจที่จำเป็นต้องรวดเร็ว ทันการ ผู้มีอำนาจในการตัดสินใจต้องสามารถเข้าถึงข้อมูลหรือสารสนเทศได้ทันที โดยไม่จำเป็นต้องรอนานเหมือนในอดีต ประกอบกับการตัดสินในบางลักษณะงานจำเป็นต้องใช้ข้อมูลแบบทันทีทันใดเพื่อให้การตัดสินใจมีความแม่นยำมากขึ้น และภายใต้การสื่อสารที่ฉับไวนี้เอง จึงทำให้เราสามารถย่อโลกให้มีขนาดเล็กลงด้วยเทคโนโลยีระบบเครือข่ายคอมพิวเตอร์ และการสื่อสารได้ทลายข้อจำกัดเหล่านี้ ไม่ว่าจะเป็นด้านระยะทาง ภูมิประเทศและเชื้อชาติ ส่งผลให้มนุษย์เราได้กลายเป็นส่วนหนึ่งของชุมชนบนโลกใบนี้อย่างแท้จริง โดยมิได้ถูกแบ่งแยกอีกต่อไป

หลักการระบบเครือข่ายคอมพิวเตอร์ประกอบด้วยการสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์

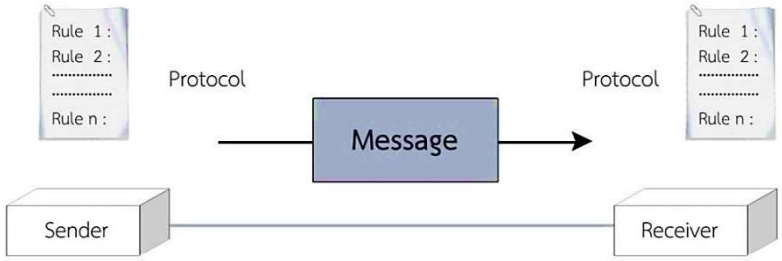
1.1 การสื่อสารข้อมูล

การติดต่อสื่อสารเป็นสิ่งที่เกิดขึ้นควบคู่กับมนุษย์ เนื่องจากมนุษย์ต้องอยู่รวมกันเป็นกลุ่ม โดยใช้ภาษาเป็นสื่อในการสื่อสารแลกเปลี่ยนข้อมูลซึ่งกันและกัน ปัจจุบันการสื่อสารข้อมูลได้มีการพัฒนาเจริญและมีความก้าวหน้ามากยิ่งขึ้น มีการส่งข้อมูลในรูปแบบอิเล็กทรอนิกส์ ซึ่งสามารถส่งผ่านข้อมูลได้ทุกประเภทไม่ว่าจะเป็นตัวอักษร ตัวเลข สัญลักษณ์ ภาพนิ่ง ภาพเคลื่อนไหวและเสียงโดยส่งผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งการเรียนรู้เกี่ยวกับการสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์นั้นนับเป็นพื้นฐานสำคัญในการทำความเข้าใจเพื่อการพัฒนา และสามารถใช้เทคโนโลยีสำหรับการติดต่อสื่อสารได้อย่างมีประสิทธิภาพ

การสื่อสารข้อมูล (Data Communications) คือ การส่งสารระหว่างผู้ส่งและผู้รับผ่านสื่อกลางต่างๆ เช่น โทรศัพท์ วิทยุ โทรทัศน์ ดาวเทียม อินเทอร์เน็ต มีหลายรูปแบบการสื่อสารและเกิดขึ้นในหลายสภาพแวดล้อม (พิสิฐ พรพงศ์เตชวาณิช และพงษ์พิสิฐ วุฒิดิษฐโชติ, 2566, หน้า 11)

1.1.1 องค์ประกอบของการสื่อสารข้อมูล

องค์ประกอบของการสื่อสารข้อมูล (Components of Data Communication System) การสื่อสารข้อมูลจะสัมฤทธิ์ผลและมีความสมบูรณ์ก็ต่อเมื่อมีองค์ประกอบครบทั้ง 5 ประการ ดังภาพที่ 1.1



ภาพที่ 1.1 ส่วนประกอบของระบบการสื่อสารข้อมูล
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 16)

การสื่อสารจะประกอบไปด้วยส่วนสำคัญ 5 ประการ ได้แก่ ข่าวสาร ผู้ส่ง ผู้รับ สื่อกลางส่งข้อมูล และโพรโทคอล (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 1-8)

1. ข่าวสาร

ข่าวสาร (Message) คือ ข้อมูลหรือสารสนเทศต่างๆ ที่อาจจะเป็นได้ทั้งข้อความ ตัวเลข รูปภาพ เสียง และวิดีโอโดยข่าวสารที่ส่งไปจะได้รับการเข้ารหัส (Encoding) เพื่อส่งผ่านสื่อกลาง เมื่อปลายทางได้รับข้อมูลจะมีการถอดรหัส (Decoding) ให้กลับมาเป็นข้อมูลดังเดิมเหมือนต้นฉบับ อย่างไรก็ตามระหว่างการลำเลียงข่าวสารผ่านสื่อกลางอาจมีสัญญาณรบกวนปะปนมากับข่าวสารก็ได้

2. ผู้ส่ง

ผู้ส่ง (Sender) คือ ผู้ทสร้างและส่งข้อมูลนั้นๆ ไปยังผู้รับโดยมีความหมายครอบคลุมตั้งแต่ผู้ใช้งานซึ่งป้อนข้อมูล ข่าวสาร คอมพิวเตอร์โฮสต์ หรือซอฟต์แวร์ที่ใช้ในการสื่อสาร

3. ผู้รับ

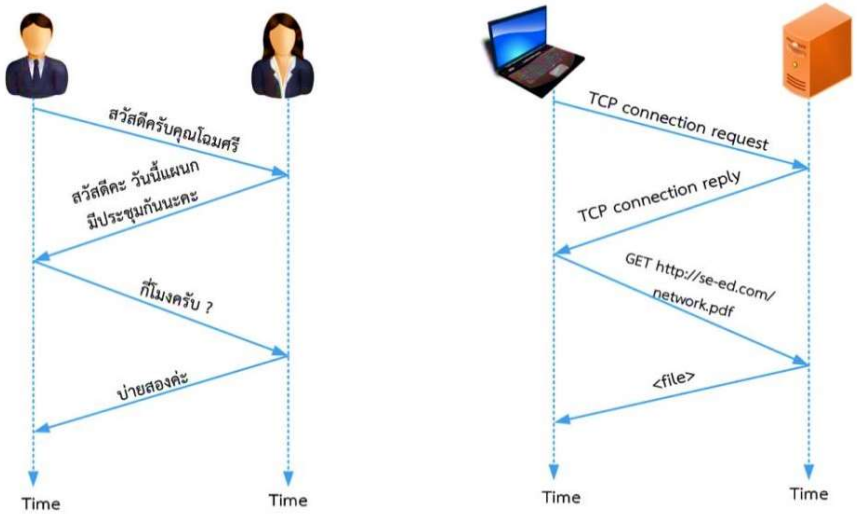
ผู้รับ (Receiver) คือ ปลายทางของการสื่อสาร โดยมีความหมายครอบคลุมตั้งแต่ผู้ใช้งานซึ่งป้อนข้อมูลข่าวสาร คอมพิวเตอร์โฮสต์ หรือซอฟต์แวร์ที่ใช้ในการสื่อสาร

4. สื่อกลางส่งข้อมูล

สื่อกลางส่งข้อมูล (Transmission Medium) ในที่นี้ คือ เส้นทางกายภาพที่ใช้ลำเลียงข้อมูลข่าวสารจากผู้ส่งไปยังผู้รับ เช่น สายโคแอ๊กเชียล สายคู่บิดเกลียว สายไฟเบอร์ออฟติก และสื่อกลางส่งข้อมูลแบบไร้สาย ได้แก่ คลื่นวิทยุ

5. โพรโทคอล

โพรโทคอล (Protocol) เป็นกฎเกณฑ์หรือข้อตกลงที่ใช้ในการสื่อสารข้อมูล เพื่อให้การสื่อสารระหว่างอุปกรณ์มีความเข้าใจในทิศทางเดียวกันสามารถสื่อสารกันได้ หากไม่มีโพรโทคอล อุปกรณ์ทั้งสองอาจจะติดต่อกันได้แต่ไม่สามารถสื่อสารให้เข้าใจกันได้ เช่น มีบุคคล 2 คน ที่ต้องการพบปะกัน และเมื่อได้พบกันแล้วแต่สนทนากันไม่รู้เรื่อง เนื่องจากคนหนึ่งพูดภาษาไทยและอีกคนหนึ่งพูดภาษาญี่ปุ่น ดังภาพที่ 1.2



ภาพที่ 1.2 เปรียบเทียบภาษาที่ใช้สื่อสารกันของมนุษย์กับโพรโทคอลที่ใช้สื่อสารในคอมพิวเตอร์
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 17)

1.1.2 คุณสมบัติพื้นฐานของระบบการสื่อสารข้อมูล

เมื่อการสื่อสารเกิดขึ้นย่อมมีการแชร์ข้อมูลข่าวสารระหว่างกัน อีกทั้งการสื่อสารยังเป็นทั้งแบบพบปะกันซึ่งหน้า (Face to Face) หรือแบบระยะไกล (Remote)

โดยเฉพาะการสื่อสารแบบระยะไกล ย่อมเกี่ยวข้องกับระยะทาง จึงจำเป็นต้องพึ่งพาเทคโนโลยีการสื่อสารโทรคมนาคม

การสื่อสารข้อมูล เป็นการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ผ่านสื่อกลางส่งข้อมูล เช่น สายเคเบิล สำหรับการสื่อสารข้อมูลจะเกิดขึ้นได้นั้น อุปกรณ์สื่อสารจะต้องเป็นส่วนหนึ่งของระบบการสื่อสารที่ถูกสร้างขึ้นจากการประสานงานเข้าด้วยกันอย่างลงตัวระหว่างอุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์ที่สำคัญระบบการสื่อสารข้อมูลจะเกิดผลได้นั้น จะขึ้นอยู่กับคุณสมบัติพื้นฐาน 4 ประการด้วยกัน ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 18)

1. การส่งมอบ

ระบบจะต้องส่งข้อมูลไปยังปลายทางได้อย่างถูกต้อง โดยข้อมูลที่ส่งไปจะต้องส่งไปยังอุปกรณ์หรือผู้ใช้ตรงตามจุดมุ่งหมายที่ต้องการ

2. ความเที่ยงตรง

ระบบจะต้องส่งข้อมูลได้อย่างเที่ยงตรง ถูกต้องและแน่นอน และในกรณีที่ข้อมูลได้รับการเปลี่ยนแปลงในระหว่างการส่ง รวมถึงข้อมูลเกิดการสูญหายหากไม่ได้รับการแก้ไขจะถือว่าข้อมูลนั้นใช้การไม่ได้

3. ระยะเวลา

ระบบจะต้องส่งข้อมูลภายใต้ระยะเวลาที่เหมาะสม เพื่อสามารถนำข้อมูลไปใช้ให้เกิดประโยชน์ เพราะถ้าระยะเวลาที่ส่งล่าช้าเกินกว่าที่จะยอมรับได้อาจไม่เกิดประโยชน์ กรณีการส่งข้อมูลวีดีโอและเสียงต้องการส่งมอบแบบทันทีทันใด โดยปราศจากความล่าช้า เราจะเรียกระบบนี้ว่า **เรียลไทม์** (Real-Time Transmission)

4. การเปลี่ยนแปลงของค่าหน่วงเวลา

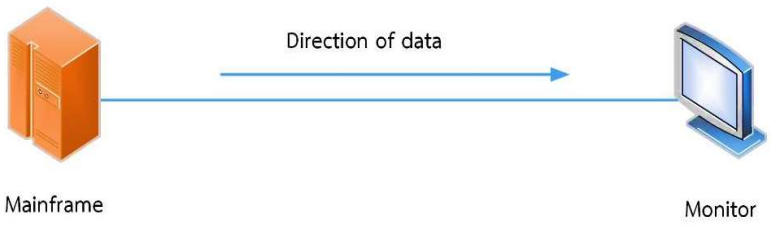
จิตเตอร์ (Jitter) เกี่ยวข้องกับค่าผิดพลาดทางเวลา ซึ่งหากมีค่าผิดพลาดมาก จะส่งผลให้สัญญาณข้อมูลเสียรูปได้ เช่น แพ็กเก็ตของชุดข้อมูลวีดีโอจะถูกส่งในทุกๆ 30 มิลลิวินาที แต่ปรากฏว่าได้มีบางแพ็กเก็ตส่งถึงล่าช้ากว่าปกติ โดยใช้เวลาถึง 40 มิลลิวินาที ย่อมส่งผลให้ภาพวีดีโอนั้นมีคุณภาพไม่สม่ำเสมอ การแสดงผลของวีดีโอดังกล่าวจะกระตุกและดูไม่ราบเรียบ เป็นต้น

1.1.3 ทิศทางการไหลของข้อมูล

การสื่อสารข้อมูลระหว่าง สองอุปกรณ์ สามารถสื่อสารได้ตามทิศทางการไหลของข้อมูล มี 3 วิธี ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 19-20)

1. การสื่อสารแบบซิมเพล็กซ์

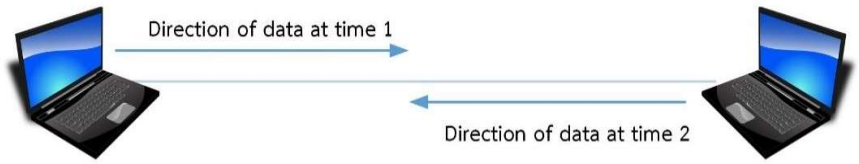
การสื่อสารแบบซิมเพล็กซ์ (Simplex Communication) เป็นการสื่อสารแบบทิศทางเดียว โดยมีอุปกรณ์ฝั่งหนึ่งทำหน้าที่เป็นฝ่ายส่ง และอีกฝั่งหนึ่งทำหน้าที่เป็นฝ่ายรับ ตัวอย่างการสื่อสารแบบซิมเพล็กซ์ เช่น คีย์บอร์ด จอภาพทั่วไปที่ใช้สำหรับการแสดงผลข้อมูล การกระจายเสียงของสถานีวิทยุ การแพร่ภาพโทรทัศน์ และการส่งข้อความผ่านทางเพจเจอร์ การสื่อสารแบบ ซิมเพล็กซ์สามารถใช้ช่องทางการสื่อสารที่มีอยู่ทั้งหมดเพื่อการส่งข้อมูลแบบทิศทางเดียวได้อย่างเต็มที่ ดังภาพที่ 1.3



ภาพที่ 1.3 การสื่อสารแบบซิมเพล็กซ์ (Simplex)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 19)

2. การสื่อสารแบบฮาล์ฟดูเพล็กซ์

การสื่อสารแบบฮาล์ฟดูเพล็กซ์ (Half-Duplex Communication) เป็นการสื่อสารที่แต่ละสถานีสามารถเป็นได้ทั้งผู้ส่งและผู้รับ แต่ไม่สามารถหน้าที่ทั้งสองอย่างได้พร้อมๆ กัน กล่าวคือ เป็นการสื่อสารแบบกึ่งทางคู่ ด้วยการผลัดกันรับ ผลัดกันส่ง ผ่านช่องสัญญาณเดียวกัน ซึ่งการเปลี่ยนสถานะจากผู้ส่งกลายเป็นผู้รับหรือการที่ผู้รับกลายเป็นผู้ส่ง จะใช้รหัสที่รับรู้กันว่ามีการส่งข้อมูลเรียบร้อยแล้ว และพร้อมที่จะรับข้อมูล เช่น การใช้รหัส “ทราบแล้วเปลี่ยน” ในวิทยุสื่อสาร ตัวอย่างสื่อสารแบบฮาล์ฟดูเพล็กซ์ เช่น การสื่อสารบนพอร์ตอนุกรม และวิทยุสื่อสาร ดังภาพที่ 1.4



ภาพที่ 1.4 การสื่อสารแบบฮาล์ฟดูเพล็กซ์ (Half-Duplex)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 19)

3. การสื่อสารแบบฟูลดูเพล็กซ์

การสื่อสารแบบฟูลดูเพล็กซ์ (Full-Duplex Communication) เป็นวิธีการสื่อสารแบบสองทิศทาง ที่ทั้งฝั่งส่งและฝั่งรับ สามารถสื่อสารพร้อมกันได้ในเวลาเดียวกัน ตัวอย่างการสื่อสารแบบฟูลดูเพล็กซ์ เช่น โทรศัพท์ ซึ่งคู่สนทนาสามารถคุยโต้ตอบกันได้ในช่วงเวลาเดียวกัน

1.2 เครือข่ายคอมพิวเตอร์

เครือข่ายคอมพิวเตอร์ (Computer Network) หมายถึง วิธีการเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันผ่านสื่อกลางต่างๆ เช่น สายสัญญาณ หรือคลื่นวิทยุ เป็นต้น สามารถสื่อสารแลกเปลี่ยนข้อมูล และใช้ทรัพยากรร่วมกันได้ โดยเนื้อหาที่เกี่ยวข้องกับการสื่อสารข้อมูลมีหลายรูปแบบ ไม่ได้จำกัดแค่เพียงเครือข่ายที่มีองค์ประกอบเป็นเครือข่ายคอมพิวเตอร์เท่านั้น

ในอดีตการแลกเปลี่ยนข้อมูลระหว่างคอมพิวเตอร์จะใช้วิธีบันทึกข้อมูลลงในแผ่นดิสก์และส่งไปยังเครื่องปลายทาง เรียกว่า สนิกเกอร์เน็ต (Sneakernet) หรือเครือข่ายคอมพิวเตอร์ที่มีคนเป็นสื่อรับส่งข้อมูล การส่งข้อมูลในลักษณะนี้ทำให้เสียเวลาและบุคลากรไปโดยเปล่าประโยชน์ และอาจทำให้ข้อมูลสูญหายและขาดความน่าเชื่อถือในระหว่างการเคลื่อนย้ายได้ ดังนั้น จึงมีการพัฒนาระบบเครือข่ายขึ้นมาเพื่อใช้ในการติดต่อสื่อสารทั้งภายในและภายนอกองค์กร (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 8-11)

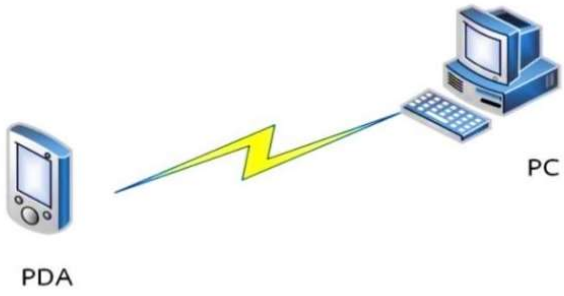
1.2.1 ประเภทของเครือข่ายคอมพิวเตอร์

เครือข่ายเป็นการเชื่อมต่อกันของคอมพิวเตอร์หรืออุปกรณ์ต่างๆ ผ่านสื่อกลางที่เป็นได้ทั้งแบบใช้สายสัญญาณและแบบไร้สายหรือคลื่นวิทยุที่เรียกว่า ไวเลท (Wireless)

นอกจากนี้ยังรวมถึงคลื่นวิทยุกระจายเสียง (Broadcast Radio) คลื่นไมโครเวฟ (Microwave) และการส่งสัญญาณผ่านดาวเทียม (Satellite) โดยขอบเขตของเครือข่ายอาจครอบคลุมการใช้งานเฉพาะบุคคลในระยะต่างๆ โดยเครือข่ายแต่ละประเภทมีรายละเอียด ดังนี้

1. เครือข่ายส่วนบุคคล

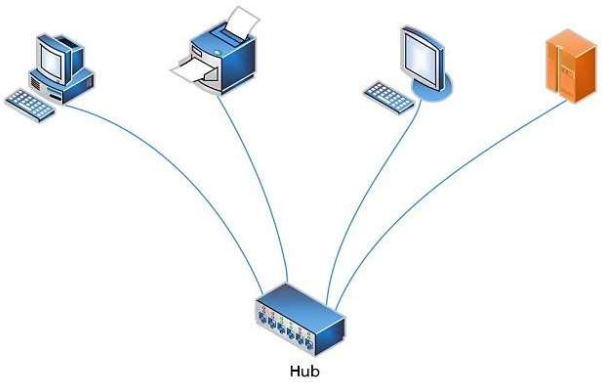
เครือข่ายส่วนบุคคลหรือเครือข่ายแพน (Personal Area Network : PAN) เป็นการเชื่อมต่ออุปกรณ์แบบพกพา เช่น โทรศัพท์มือถือ เข้าด้วยกันกับเครื่องคอมพิวเตอร์ โดยมีขอบเขตของเครือข่ายเพียงระยะทางสั้นๆ และมีลักษณะเป็นเครือข่ายไร้สาย (Wireless) สามารถเชื่อมต่ออุปกรณ์ที่อยู่ในระยะทางไม่เกิน 10 เมตร ได้แก่ บลูธูท (Bluetooth) ซึ่งเป็นการเชื่อมอุปกรณ์สองชิ้นด้วยความถี่ที่ระดับ 2.45 GHz มีอัตราการรับส่งข้อมูล 3 Mbps เป็นต้น ดังภาพที่ 1.5



ภาพที่ 1.5 แสดงการสื่อสารของเครือข่ายส่วนบุคคล (PAN)
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 9)

2. เครือข่ายเฉพาะบริเวณ

เครือข่ายเฉพาะบริเวณหรือเครือข่ายแลน (Local Area Network : LAN) เป็นเครือข่ายขนาดเล็กที่เชื่อมโยงอุปกรณ์ต่างๆ ที่อยู่ในพื้นที่ใกล้เคียงกัน มีขอบเขตครอบคลุมบริเวณห้อง อาคาร หรือสำนักงานเดียวกัน เครือข่ายแลนจะประกอบด้วยคอมพิวเตอร์หรืออุปกรณ์ต่อพ่วงตั้งแต่ 2 ชิ้นขึ้นไป หากเป็นองค์กรขนาดเล็กอาจมีแลนเพียงกลุ่มเดียว แต่ถ้าเป็นองค์กรขนาดใหญ่อาจประกอบด้วยแลนหลายกลุ่มเชื่อมโยงกัน ดังภาพที่ 1.6

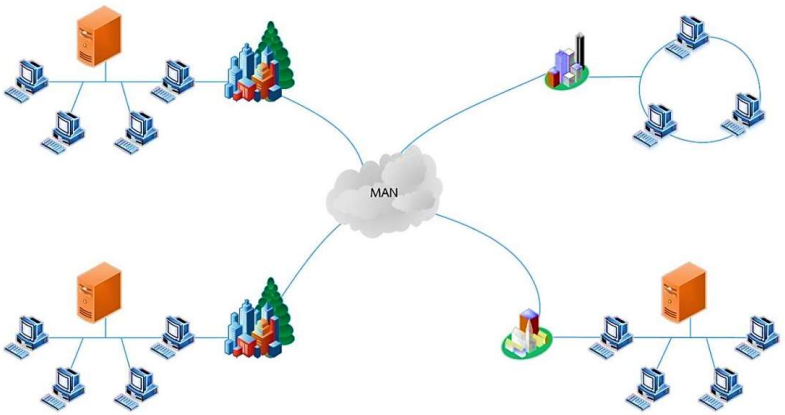


ภาพที่ 1.6 แสดงการสื่อสารของเครือข่ายเฉพาะบริเวณ (LAN)

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 9)

3. เครือข่ายระดับเมือง

เครือข่ายระดับเมืองหรือเครือข่ายแมน (Metropolitan Area Network : MAN) เป็นเครือข่ายที่มีขนาดใหญ่ครอบคลุมระดับเมือง ซึ่งอาจเป็นเครือข่ายเดียวที่มีการเชื่อมโยงภายในเมืองเดียวกันเท่านั้น เช่น การให้บริการของเคเบิลทีวีในระดับท้องถิ่น เป็นต้น หรืออาจประกอบด้วยเครือข่ายแลนหลายเครือข่ายเชื่อมโยงกันผ่านเครือข่ายสาธารณะระดับเมืองก็ได้ เช่น การเชื่อมโยงเครือข่ายแลนของบริษัทแห่งหนึ่งซึ่งมีหลายสาขาอยู่ภายในเมืองเดียวกัน เป็นต้น ดังภาพที่ 1.7

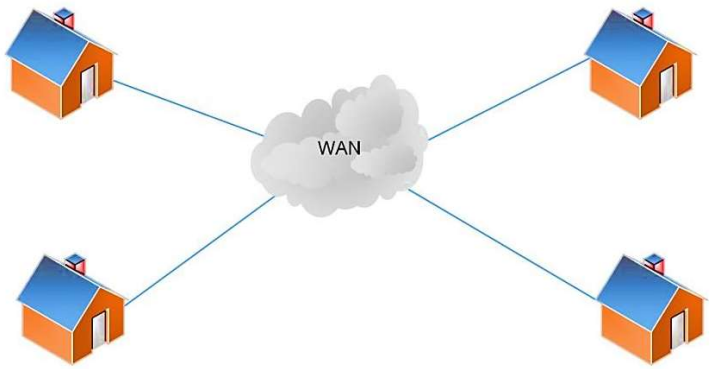


ภาพที่ 1.7 แสดงการสื่อสารของเครือข่ายระดับเมือง (MAN)

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 10)

4. เครือข่ายระยะไกล

เครือข่ายระยะไกลหรือเครือข่ายแวน (Wide Area Network : WAN) เป็นเครือข่ายที่ครอบคลุมทั่วโลก สามารถเชื่อมต่อเครือข่ายแลนที่อยู่ห่างไกลกว่าระดับเมืองได้ ผ่านเครือข่ายสาธารณะขนาดใหญ่หรือผู้ให้บริการเชื่อมโยงต่างๆ เช่น เครือข่ายอินเทอร์เน็ตที่สามารถเชื่อมโยงผู้ใช้ได้จากทั่วทุกมุมโลกผ่านผู้ให้บริการที่เรียกว่า ไอเอสพี (Internet Service Provider : ISP) ดังภาพที่ 1.8



ภาพที่ 1.8 แสดงการสื่อสารของเครือข่ายระยะไกล (WAN)

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 11)

5. เครือข่ายควบคุม

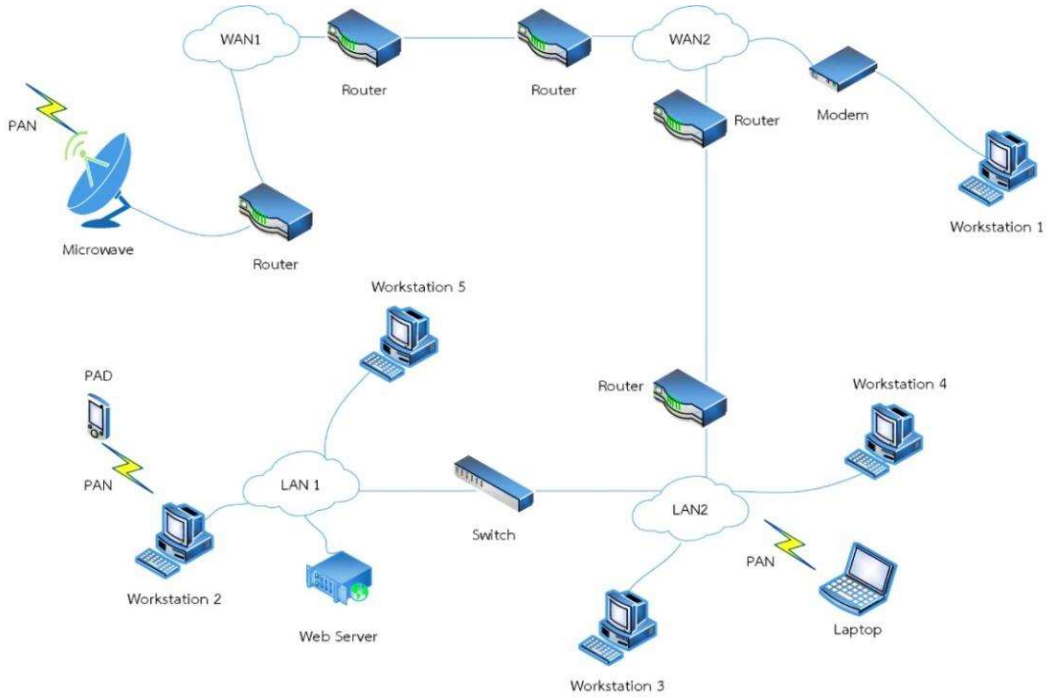
เครือข่ายควบคุมหรือแคน (Control Area Net work : CAN) มีความแตกต่างกับระบบเครือข่ายของคอมพิวเตอร์ทั่วไปเป็นอย่างมาก นิยมนำมาใช้กับโรงงานอุตสาหกรรม เพื่อเชื่อมต่อและควบคุมอุปกรณ์อิเล็กทรอนิกส์ มอเตอร์ เซ็นเซอร์ และไมโครคอนโทรลเลอร์ต่างๆ โดยเป็นระบบเครือข่ายที่มีประสิทธิภาพสูง สามารถรับส่งข้อมูลและตอบสนองการทำงานได้อย่างรวดเร็ว ตัวอย่างเช่น การนำระบบเครือข่ายแคนไปใช้งานในรถยนต์ที่ใช้เซ็นเซอร์ในการควบคุมการเปิดปิดกระจก ระบบเบรก ระบบการจ่ายน้ำมัน ระบบไฟฟ้า เป็นต้น โดยการควบคุมอุปกรณ์ดังกล่าวจำเป็นต้องอาศัยการรับส่งข้อมูลที่รวดเร็วและมีประสิทธิภาพสูง เพื่อตอบสนองต่อผู้ขับได้ทันที

1.2.2 องค์ประกอบและการทำงานของระบบเครือข่าย

เครือข่ายมีองค์ประกอบพื้นฐาน 2 ส่วน คือ องค์ประกอบด้านฮาร์ดแวร์ และด้านซอฟต์แวร์

ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์ที่ใช้งานและเชื่อมต่ออุปกรณ์ภายในเครือข่าย รวมทั้งอุปกรณ์ที่ใช้เชื่อมต่อกับภายนอกเครือข่าย

ซอฟต์แวร์ (Software) หมายถึง ระบบปฏิบัติการ โปรแกรม หรือแอปพลิเคชั่นต่างๆ ที่ใช้สนับสนุนการทำงานและให้บริการด้านต่างๆ เพื่ออำนวยความสะดวกให้แก่ผู้ใช้ให้สามารถติดต่อ สื่อสารผ่านเครือข่ายได้



ภาพที่ 1.9 แสดงการเชื่อมต่อระหว่างเครือข่ายประเภทต่างๆ

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 12)

จากภาพที่ 1.9 เป็นการนำฮาร์ดแวร์ซึ่งเป็นส่วนประกอบของเครือข่ายมาเชื่อมต่อเครือข่ายชนิดต่างๆ เข้าด้วยกัน เช่น เครือข่ายส่วนบุคคล (PAN) เครือข่ายเฉพาะบริเวณ (LAN) และเครือข่ายระยะไกล (WAN)

ระบบเครือข่ายมีฮาร์ดแวร์ที่เป็นองค์ประกอบสำคัญ ดังนี้

1. เวิร์กสเตชัน (Workstation) คือ อุปกรณ์หรือเครื่องคอมพิวเตอร์ของผู้ใช้ที่เชื่อมต่อกับระบบเครือข่าย ได้แก่ คอมพิวเตอร์ส่วนบุคคล PC

2. เซิร์ฟเวอร์ (Server) คือ คอมพิวเตอร์ที่เก็บข้อมูล แบ่งปันข้อมูล หรือคอยให้บริการในด้านต่างๆ แก่ผู้ใช้

3. ฮับ (Hub) คือ อุปกรณ์ที่ใช้เชื่อมต่ออุปกรณ์คอมพิวเตอร์ต่างๆ โดยใช้สายสัญญาณเชื่อมต่อกับพอร์ตของ Hub

4. สวิตช์ (Switch) คือ อุปกรณ์ที่ทำหน้าที่ส่งข้อมูลไปยังปลายทางเหมือนฮับ (Hub) โดย สวิตช์จะไม่ใช้วิธีกระจายข้อมูลไปยังทุกพอร์ต แต่สามารถส่งข้อมูลไปยังพอร์ตปลายทางที่ต้องการได้

5. เราท์เตอร์ (Router) คือ อุปกรณ์ที่ใช้กำหนดและเลือกเส้นทางการขนส่งข้อมูลระหว่างเครือข่าย

เครือข่ายแวน ประกอบด้วยเครือข่ายหลายชนิดเชื่อมต่อกัน โดยแต่ละเครือข่ายที่อยู่ภายในเครือข่ายแวนอาจใช้เทคโนโลยีการเชื่อมต่อที่แตกต่างกัน แต่ทุกเครือข่ายจะต้องมีส่วนประกอบสำคัญ ดังนี้

1. โหนด (Node) คือ อุปกรณ์คอมพิวเตอร์สำหรับเก็บข้อมูลที่เชื่อมต่อยู่ภายในเครือข่าย Workstation หรือ Web Server เป็นต้น

2. สายนำสัญญาณ (Transmission Line) คือ อุปกรณ์คอมพิวเตอร์สำหรับเก็บข้อมูลที่เชื่อมต่ออยู่ภายในเครือข่าย Workstation หรือ Web Server เป็นต้น

3. การเชื่อมต่อเครือข่าย (Communication Network) คือ การนำโหนด (Node) และสายนำสัญญาณ (Transmission Line) มาประกอบกันเพื่อสร้างการเชื่อมต่อระหว่างกัน

จากภาพที่ 1.10 จะเห็นว่าเครือข่ายแลนและแวนทำงานร่วมกัน หากมีผู้ใช้ต้องการใช้เครื่องเวิร์กสเตชัน 1 (Workstation 1) เพื่อเปิดเว็บเพจ (Web Page) จากเว็บเซิร์ฟเวอร์ (Web Server) ที่เชื่อมต่ออยู่ในแลน 1 เครื่องเวิร์กสเตชัน 1 จะต้องมีฮาร์ดแวร์และซอฟต์แวร์ที่จำเป็นใน การติดต่อสื่อสารกับเครือข่ายแวน 2 ก่อน ในที่นี้จะใช้การเชื่อมต่อผ่านสายโทรศัพท์ด้วยโมเด็ม หากเครือข่ายแวน 2 เป็นส่วนหนึ่งของระบบอินเทอร์เน็ตจะต้องใช้ซอฟต์แวร์ที่ใช้ติดต่อสื่อสารกันบนเครือข่ายอินเทอร์เน็ตที่เรียกว่า ทีซีพีหรือไอพี (Transmission

Control Protocol/Internet Protocol : TCP/IP) ด้วย นอกจากนี้จะเห็นว่าการเชื่อมต่อของเครือข่ายแลน 1 จะไม่มีคอมพิวเตอร์เครื่องใดที่เชื่อมต่อโดยตรงกับเครือข่ายแวนทั้งสอง ดังนั้นการเข้าถึงแวน 2 จะต้องกระทำผ่านเครือข่ายแลน 2 โดยเมื่อเครื่อง เวิร์กสเตชัน 1 ต้องการเปิดเว็บเพจจากเว็บเซิร์ฟเวอร์จะต้องอาศัยซอฟต์แวร์ที่ระบุที่อยู่ของแวน 2 เพื่อนำไปให้เราท์เตอร์ที่เชื่อมต่อระหว่างแวน 2 กับแลน 2 ค้นหาเส้นทางโดยแลน 2 จะเชื่อมอยู่กับแลน 1 ด้วยอุปกรณ์สวิตช์ เป็นต้น

1.2.3 ประโยชน์ของเครือข่ายคอมพิวเตอร์

ประโยชน์ของเครือข่าย สามารถสรุปได้ ดังนี้

1. การใช้ทรัพยากรร่วมกัน

ด้วยเทคโนโลยีเครือข่าย ทำให้เราสามารถใช้ทรัพยากรร่วมกันได้ โดยทรัพยากรในที่นี้หมายถึงอุปกรณ์ต่างๆ ที่เชื่อมต่อบนเครือข่าย ซึ่งอาจเป็นข้อมูล โปรแกรม หรือเครื่องพิมพ์ เป็นต้น (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 20)

2. ช่วยลดต้นทุน

เมื่อเครือข่ายช่วยให้เราใช้ทรัพยากรร่วมกันได้ ทำให้เราประหยัดค่าใช้จ่ายได้เช่นกัน โดยเฉพาะอุปกรณ์ที่มีราคาแพง เช่น แทนที่จะต้องซื้อเครื่องพิมพ์จำนวนหลายๆ เครื่องเพื่อเชื่อมต่อเข้ากับคอมพิวเตอร์แต่ละตัว ก็อาจซื้อเพียง 1-2 เครื่อง แล้วนำมาแบ่งปันใช้งานบนเครือข่าย

3. เพิ่มความสะดวกในด้านการสื่อสาร

ด้วยเทคโนโลยีของระบบเครือข่าย ทำให้การสื่อสารข้อมูลของพนักงานในองค์กรที่มีความสะดวกขึ้น เช่น เลขานุการแทนที่จะสำเนาเอกสารสรุปผลการประชุมเพื่อแจกจ่ายให้กับส่วนงานอื่นๆ ที่เกี่ยวข้อง ก็จะจัดพิมพ์ผ่านโปรแกรมประมวลผลคำ แล้วส่งพิมพ์ลงในไฟล์ PDF จากนั้นก็แนบไฟล์ดังกล่าวไปยังส่วนงานอื่นๆ ในรูปแบบของจดหมายอิเล็กทรอนิกส์แทน ทำให้การสื่อสารข้อมูลภายในองค์กรมีความสะดวกรวดเร็วมากขึ้น

4. ความน่าเชื่อถือและความปลอดภัยของระบบ

องค์กรต่างๆ ที่มีคอมพิวเตอร์ใช้งานเป็นจำนวนมาก การสร้างระบบเครือข่ายไว้ใช้งาน เป็นเรื่องที่สำคัญอย่างยิ่ง เนื่องจากระบบเครือข่ายจะช่วยให้ผู้ดูแลระบบสามารถจัดสรรบัญชีผู้ใช้ให้เป็นไปตามสิทธิ์ บัญชีผู้ใช้แต่ละคนจะมีรหัสผ่าน พร้อมกับระบบ

ควบคุมความปลอดภัยที่จำเป็น เช่น การกำหนดเวลาในการเข้าถึง และการกำหนดสิทธิ์ในการเข้าถึงข้อมูล เป็นต้น อีกทั้งยังช่วยให้ผู้ดูแลระบบบริหารจัดการเครือข่ายได้สะดวกมากขึ้น ผ่านการล็อกอินเข้าไปยังเซิร์ฟเวอร์เพียงแห่งเดียว ก็สามารถควบคุมระบบได้ทั้งหมด และด้วยข้อมูลต่างๆ ถูกบันทึกลงในเครื่องศูนย์กลางหรือเซิร์ฟเวอร์นี้เอง การปรับปรุงหรือเปลี่ยนข้อมูลก็จะทำอยู่ที่เดียว ครั้นเมื่อมีบุคคลใดนำข้อมูลจากศูนย์กลางไปใช้งาน ก็จะได้ข้อมูลที่ทันสมัย น่าเชื่อถือ

1.2.4 เกณฑ์วัดประสิทธิภาพของเครือข่าย

การพิจารณาถึงประสิทธิภาพของเครือข่ายว่ามีเป็นเครือข่ายที่ดีมีประสิทธิภาพนั้นใช้หลักพื้นฐานที่สำคัญในการพิจารณา ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 29-31)

1. สมรรถนะ

สมรรถนะ (Performance) ของเครือข่ายสามารถประเมินได้หลายทางด้วยกัน เช่น เวลาที่ใช้ข้อมูล (Transit Time) หมายถึง ระยะเวลาในการส่งข้อมูลจากอุปกรณ์หนึ่งไปยังอุปกรณ์อื่นๆ และเวลาตอบสนอง (Response Time) คือ ช่วงระยะเวลาทั้งหมดตั้งแต่การส่งข้อมูลจนกระทั่งมีการตอบ สนองผลลัพธ์กลับมา ดังนั้น ภาพรวมด้านสมรรถนะของเครือข่ายที่ส่งผลต่อความเร็วจึงมีอยู่หลายปัจจัยด้วยกัน ได้แก่

1.1 จำนวนผู้ใช้ หากเครือข่ายมีจำนวนผู้ใช้เชื่อมต่อใช้งานพร้อมๆ กันเป็นจำนวนมาก ย่อมส่งผลต่อเวลาตอบสนองที่ช้าลงอย่างชัดเจน โดยเฉพาะเครือข่ายที่ไม่ได้รับการออกแบบโหลดสูงสุดเพื่อรองรับความหนาแน่นของจราจรบนเครือข่าย ดังนั้น การออกแบบเครือข่ายที่ดี จึงควรประเมินค่าเฉลี่ยของจำนวนผู้ใช้ที่จะได้รับการสื่อสาร ณ เวลาหนึ่งๆ เพื่อให้เครือข่ายยังคงสามารถตอบสนองข้อมูลแก่ผู้ใช้บนเครือข่ายโดยไม่มีอาการสะดุด

1.2 ชนิดของสื่อกลาง สื่อกลางแต่ละชนิด จะมีอัตราความเร็วในการส่งข้อมูลแตกต่างกัน เช่น สายไฟเบอร์ออปติกมีความเร็วในการส่งข้อมูลสูงถึงระดับกิกะบิต และยังสามารถเชื่อมโยงระยะทางได้ไกลเป็นกิโลเมตร ในขณะที่สายคู่บิดเกลียวรองรับความเร็วที่ 100 เมกะบิต และเชื่อมโยงได้ไกลสุดเพียง 100 เมตรเท่านั้น ดังนั้น การเลือกใช้สื่อกลางการส่งข้อมูลจึงส่งผลต่อประสิทธิภาพของเครือข่าย และไม่จำเป็นต้องใช้สายไฟเบอร์ออปติกทั้งระบบเนื่องจากสิ้นเปลืองค่าใช้จ่าย ซึ่งโดยทั่วไปมักใช้สายไฟเบอร์ออปติกเป็นสายแกนหลัก (Backbone) ที่เปรียบเสมือนกระดูกสันหลังของระบบที่ทุกเครือข่ายต้องสื่อสารผ่านเส้นทางนี้ ในขณะเดียวกัน เครือข่ายย่อยที่เชื่อมโยงไปยังส่วนงานต่างๆ ก็จะใช้สายคู่บิดเกลียว

1.3 อุปกรณ์ฮาร์ดแวร์ ประสิทธิภาพของอุปกรณ์ฮาร์ดแวร์ที่เชื่อมต่อใช้งานบนเครือข่าย ย่อมส่งผลต่อความเร็วในการประมวลผลและการส่งผ่านข้อมูล เช่น เครื่องเซิร์ฟเวอร์ที่ใช้ซีพียูประสิทธิภาพสูง ย่อมช่วยให้เครือข่ายสามารถรับส่งข้อมูลได้อย่างรวดเร็วมากขึ้น

1.4 ซอฟต์แวร์ นอกจากอุปกรณ์ฮาร์ดแวร์ที่มีประสิทธิภาพแล้ว ซอฟต์แวร์ที่นำมาใช้ควบคุมระบบเครือข่ายก็ต้องมีประสิทธิภาพเช่นกัน ในระบบเครือข่ายข่าวสารที่ส่งผ่านไปยังแต่ละโหนดจะได้รับการเข้ารหัสให้อยู่ในรูปของสัญญาณ ครั้นเมื่อสัญญาณถูกส่งไปยังปลายทาง สัญญาณก็จะถูกแปลงเป็นข้อมูลเพื่อนไปใช้งานต่อไป โดยซอฟต์แวร์จะมีหน้าที่คอยบริการงานเหล่านี้ ซอฟต์แวร์ที่ดี นอกจากช่วยเพิ่มความเร็วในการประมวลผลแล้ว ยังช่วยให้การส่งข้อมูลบนเครือข่ายมีประสิทธิภาพและประสิทธิผล

2. ความน่าเชื่อถือ

ความน่าเชื่อถือ (Reliability) ของระบบเครือข่าย สามารถประเมินได้จากสิ่งต่อไปนี้

2.1 ความถี่ของความล้มเหลว เครือข่ายทุกระบบมีโอกาสล่มได้เสมอ แต่ถ้าเครือข่ายล้มเหลวเป็นประจำแสดงว่าเครือข่ายนั้นมีความน่าเชื่อถือต่ำ และด้อยคุณค่าต่อผู้ใช้งาน

2.2 ระยะเวลาในการกู้คืนหลังจากเครือข่ายล้มเหลว กรณีเครือข่ายเกิดข้อขัดข้องใดๆ ขึ้นมา หากการกู้คืนระบบเครือข่าย สามารถดำเนินการได้ด้วยระยะเวลาอันสั้น ย่อมดีกว่าการกู้คืนที่ต้องใช้ระยะเวลายาวนาน

2.3 การป้องกันภัยพิบัติ ระบบเครือข่ายที่ดีจะต้องมีระบบป้องกันภัยพิบัติต่างๆ ไม่ว่าจะเป็นภัยธรรมชาติที่เกิดขึ้นจากแผ่นดินไหว ไฟไหม้ น้ำท่วม รวมถึงการถูกโจรกรรม โดยหนึ่งในมาตรการของการป้องกันความเสียหายที่อาจเกิดขึ้นโดยฉับพลันก็คือ การใช้ซอฟต์แวร์เครือข่ายเพื่อการสำรองข้อมูล

3. ความปลอดภัย

ความปลอดภัย (Security) ของระบบเครือข่ายเป็นสิ่งสำคัญ โดยเฉพาะอย่างยิ่งระบบเครือข่ายที่เชื่อมต่อเข้ากับเครือข่ายภายนอกอย่างอินเทอร์เน็ต ซึ่งเปรียบเสมือนกับการเปิดประตูต้อนรับผู้บุกรุกเข้ามายังเครือข่ายได้ทุกเมื่อโดยความปลอดภัยของเครือข่ายจะเกี่ยวข้องกับสิ่งต่อไปนี้

3.1 การป้องกันกับบุคคลที่ไม่ได้รับการอนุญาต ข้อมูลข่าวสารที่บันทึกอยู่ในเครื่องเซิร์ฟเวอร์ ถือเป็นทรัพยากรอันมีค่ายิ่งต่อองค์กร ดังนั้น จึงจำเป็นต้องมีระบบป้องกันโดยบุคคลที่ได้รับการอนุญาตให้เข้าถึงเครือข่ายได้นั้น จะต้องมีบัญชีผู้ใช้พร้อมกรอกรหัสผ่านได้ถูกต้อง นอกจากนี้ ผู้ใช้แต่ละคนจะถูกกำหนดสิทธิ์ให้เข้าถึงข้อมูลแตกต่างกันตามแต่ละระดับและขอบเขตความรับผิดชอบ เช่น พนักงานทั่วไปไม่สามารถเข้าถึงข้อมูลเงินเดือนในแผนกบุคคลได้ นอกจากผู้จัดการ นอกจากนี้ยังสามารถใช้มาตรการป้องกันขั้นสูงขึ้นไปอีก เช่น การเข้ารหัสข้อมูล โดยหากมีผู้โจรกรรมข้อมูลไปก็ไม่สามารถเปิดอ่านได้อย่างเข้าใจ ทำให้ผู้โจรกรรมไม่สามารถนำข้อมูลดังกล่าวไปใช้ประโยชน์ใดๆ ได้จนกว่าจะรู้วิธีการถอดรหัส

3.2 ไวรัสคอมพิวเตอร์ เนื่องจากระบบเครือข่ายมีการเชื่อมต่อกับโหนดต่างๆ มากมายทั้งภายในและภายนอก ดังนั้น จึงง่ายต่อการถูกโจมตีด้วยไวรัสคอมพิวเตอร์ ไวรัสคอมพิวเตอร์จะสร้างความเสียงหายแก่ข้อมูล และอาจส่งผลกระทบต่อระบบเครือข่ายโดยรวมได้ เช่น หนอนไวรัส ดังนั้น คอมพิวเตอร์ที่ใช้งานบนเครือข่ายจำเป็นต้องติดตั้งโปรแกรมป้องกันไวรัส การป้องกันไวรัสคอมพิวเตอร์ยังถือว่าไม่เพียงพอสำหรับในยุคนี้ เนื่องจากปัจจุบันมีโปรแกรมประสงค์ร้ายมากมายที่แอบแฝงเข้ามาในรูปแบบอื่นๆ มากขึ้น เช่น สปายแวร์ โทรจัน มัลแวร์ รวมถึงแฮกเกอร์ที่ต้องการมุ่งเจาะระบบเครือข่าย ดังนั้น อุปกรณ์ไฟร์วอล (Firewall) จึงเป็นอุปกรณ์สำคัญ ที่ถูกนำมาใช้เพื่อป้องกันผู้บุกรุกเหล่านี้

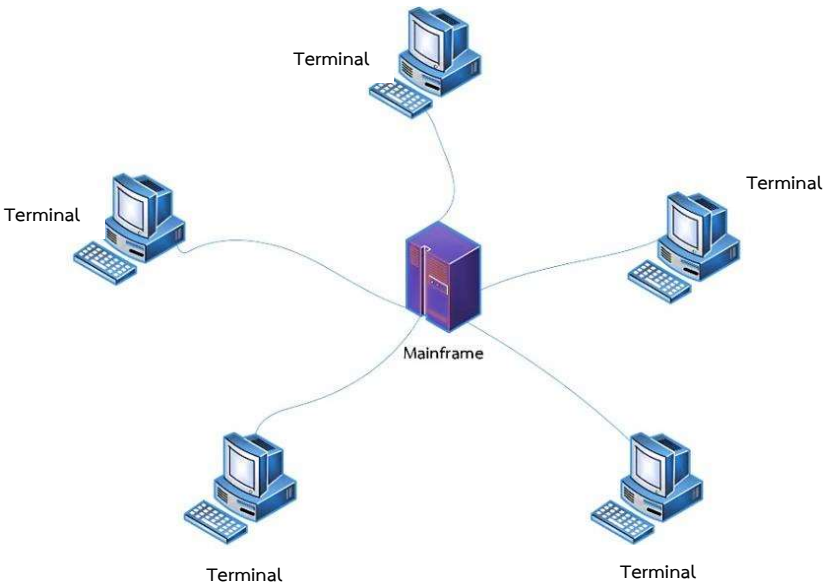
1.2.5 การเชื่อมต่อเครือข่ายขั้นพื้นฐาน

การเชื่อมต่อเครือข่ายและการสื่อสารข้อมูลในรูปแบบเรียบง่ายที่พบได้ในชีวิตประจำวัน มีรายละเอียด ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 13-19)

1. การเชื่อมต่อเทอร์มินอลกับเมนเฟรมคอมพิวเตอร์

การเชื่อมต่อเทอร์มินอลกับเมนเฟรมคอมพิวเตอร์ หรือเรียกว่า เทอร์มินอลทูเมนเฟรม คอมพิวเตอร์ (Terminal-to-Mainframe Computer) ซึ่งใช้สำหรับสอบถามข้อมูลต่างๆ ผ่านเครื่องปลายทาง (Terminal) ซึ่งเป็นอุปกรณ์ที่ประกอบด้วยคีย์บอร์ดและจอภาพ แต่ไม่มีอุปกรณ์เก็บข้อมูล โดยจะเชื่อมต่อเพื่อร้องขอบริการต่างๆ จากเมนเฟรมคอมพิวเตอร์ ดังนั้น เทอร์มินอลจะใช้เพื่อเข้าถึงข้อมูลในระบบเท่านั้น โดยเมนเฟรมคอมพิวเตอร์จะควบคุมการรับและส่งข้อมูลของแต่ละเทอร์มินอลที่เชื่อมต่ออยู่ ต่อมาได้มีการพัฒนาเครื่องคอมพิวเตอร์ส่วนบุคคลหรือพีซี (Personal Computer : PC) ขึ้นมา โดยสามารถประมวลผลและเก็บข้อมูลได้

ทำให้นิยมนำมาใช้แทนเครื่องเทอร์มินอล โดยไมโครคอมพิวเตอร์สามารถดาวน์โหลดข้อมูลจากเมนเฟรมและดำเนินการต่างๆ กับข้อมูล รวมทั้งอัพโหลดข้อมูลกลับไปยังเมนเฟรมได้ ช่วยเพิ่มความสะดวกในการทำงานมากขึ้น ทำให้องค์กรต่างๆ นำไมโครคอมพิวเตอร์และเครือข่ายแลนมาใช้งานแทนระบบเมนเฟรม



ภาพที่ 1.10 เทอร์มินอลทูเมนเฟรมคอมพิวเตอร์ (Terminal-to-Mainframe Computer)
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 14)

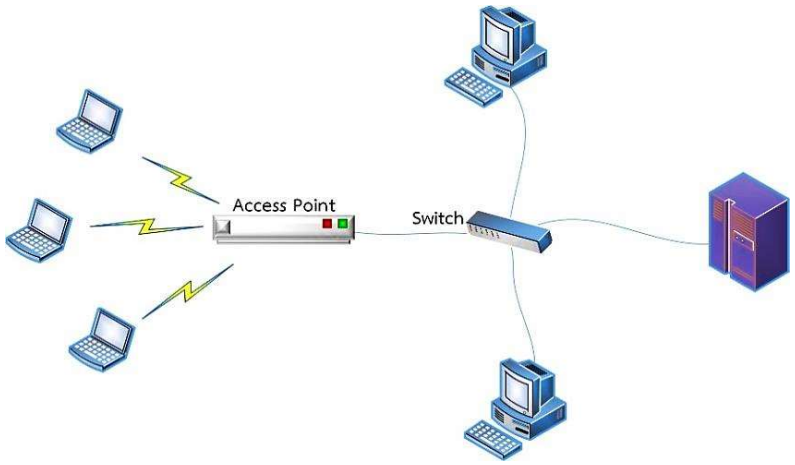
2. การเชื่อมต่อไมโครคอมพิวเตอร์กับแลน

การเชื่อมต่อเครื่องคอมพิวเตอร์ขององค์กรต่างๆ ในปัจจุบันจะใช้วิธีเชื่อมต่อเครื่อง ไมโครคอมพิวเตอร์กับแลน เรียกว่า ไมโครคอมพิวเตอร์ทูโลคอลแอเรียเน็ตเวิร์ก (Microcomputer-to-Local Area Network) ซึ่งเป็นการเชื่อมต่อที่มีค่าใช้จ่ายน้อย ดูแลรักษาง่ายและมีประสิทธิภาพสูง ระบบเครือข่ายแลนเป็นเครื่องมือที่สามารถแบ่งปันซอฟต์แวร์และอุปกรณ์ต่างๆ ได้อย่างมีประสิทธิภาพ โดยสามารถเก็บซอฟต์แวร์ต่างๆ ที่ต้องการแบ่งปันไว้ภายในเครื่องคอมพิวเตอร์ที่ทำหน้าที่เป็นศูนย์กลางที่เรียกว่า เซิร์ฟเวอร์ (Server) ได้ หากต้องการใช้งานจะใช้เครื่องคอมพิวเตอร์เชื่อมต่อกับเครือข่ายแลน จากนั้นร้องขอและดาวน์โหลดโปรแกรมที่ต้องการจากเซิร์ฟเวอร์แล้ว Execute โปรแกรมผ่านเครื่องคอมพิวเตอร์ของตน

นอกจากนี้เครือข่ายแลนยังสามารถจัดเตรียมเครื่องพิมพ์ไว้ให้บริการคอมพิวเตอร์ที่เชื่อมต่ออยู่ในเครือข่ายได้

รูปแบบการเชื่อมต่อไมโครคอมพิวเตอร์กับแลนที่นิยมใช้กันอย่างแพร่หลาย คือ ระบบ ไคลเอนต์/เซิร์ฟเวอร์ (Client/Server) ซึ่งจะใช้เครื่องคอมพิวเตอร์ผู้ใช้หรือเครื่องไคลเอนต์ (Client) เพื่อส่งคำร้องขอบริการไปยังเครื่องเซิร์ฟเวอร์ที่ต้องการเรียกใช้บริการ เช่น ต้องการดึงอีเมล (E-Mail) จะส่งคำขอไปยังเมลเซิร์ฟเวอร์ (Mail Server) โดยคำร้องขอจะถูกส่งผ่านระบบเครือข่ายไปยังเซิร์ฟเวอร์ เมื่อเซิร์ฟเวอร์ได้รับคำร้องขอจะคืนผลลัพธ์ที่ต้องการกลับมาให้เครื่องไคลเอนต์เพื่อแสดงผลลัพธ์บนจอภาพต่อไป

ปัจจุบันการเชื่อมต่อแบบไร้สาย (Wireless) กำลังได้รับความนิยมเป็นอย่างสูง และถูกนำมาใช้ร่วมกับการเชื่อมต่อเครือข่ายแบบไมโครคอมพิวเตอร์กับแลนอย่างแพร่หลาย โดยเครื่อง เวิร์กสเตชันหรือแล็ปท็อปจะใช้อุปกรณ์สื่อสารแบบไร้สายเพื่อส่งและรับข้อมูลจากจุดเชื่อมต่อ (Access Point) ซึ่งจะเชื่อมต่อกับระบบแลนอีกที โดยทำหน้าที่เป็นเหมือนสะพานระหว่างผู้ใช้ระบบไร้สายกับระบบเครือข่ายแบบใช้สายสัญญาณ ดังภาพที่ 1.11

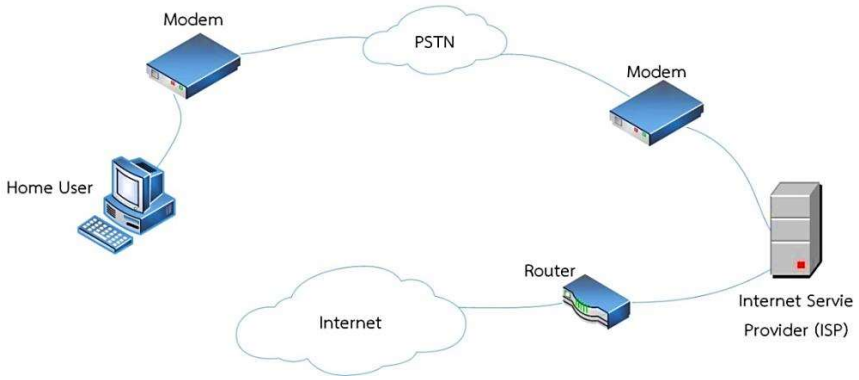


ภาพที่ 1.11 การเชื่อมต่อระหว่างเครือข่ายไร้สายกับเครือข่ายแบบใช้สายสัญญาณ
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 15)

3. การเชื่อมต่อไมโครคอมพิวเตอร์กับอินเทอร์เน็ต

ในปัจจุบันอินเทอร์เน็ตถือเป็นแหล่งข้อมูลข่าวสารที่สำคัญ หากผู้ใช้ต้องเชื่อมต่อคอมพิวเตอร์กับอินเทอร์เน็ตจากที่บ้าน ลักษณะดังกล่าวเรียกว่า Microcomputer-to-Internet โดยจะใช้โมเด็ม (Modem) และต่อสาย (Dial-Up) ไปยังผู้ให้บริการโทรศัพท์ ซึ่งจะมีความเร็วในการส่งข้อมูล 56000 บิต ต่อวินาที (56 kbps) หรือไอเอสดีเอ็น (ISDN) ซึ่งมีความเร็วมากกว่า 56 kbps

การติดต่อสื่อสารกับระบบเครือข่ายอินเทอร์เน็ตจะใช้วิธี ไดออลอัพโมเด็ม (Dial-Up Modem) โดยเชื่อมต่อไปยังคอมพิวเตอร์ที่คอยให้บริการและสามารถติดต่อกับเครือข่ายอินเทอร์เน็ตได้ เชื่อมต่อไปยังผู้ให้บริการอินเทอร์เน็ตหรือไอเอสพี (Internet Service Provider : ISP) ผ่านระบบชุมสายโทรศัพท์สาธารณะ และระบบอินเทอร์เน็ตจะใช้โพรโทคอลทีซีพีไอพี (TCP/IP) ในการรับส่งข้อมูล ดังนั้น เครื่องของผู้ใช้ต้องมีซอฟต์แวร์ที่ใช้ในการติดต่อสื่อสารกับเครือข่ายอินเทอร์เน็ตที่สนับสนุนการทำงานของโพรโทคอลดังกล่าวด้วย ดังภาพที่ 1.12



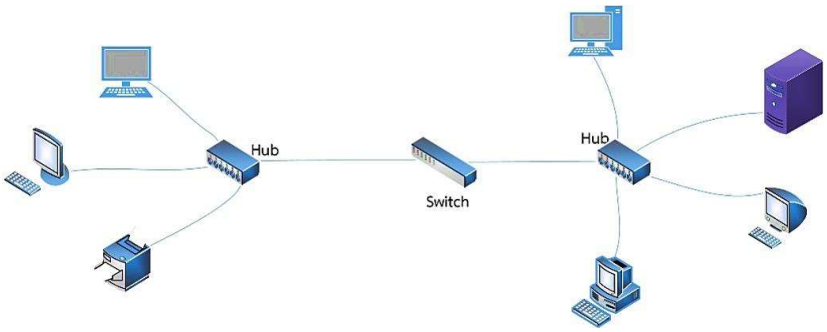
ภาพที่ 1.12 แสดงวิธีการใช้ Dial-Up Modem เพื่อเชื่อมต่ออินเทอร์เน็ต
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 16)

4. การเชื่อมต่อแลนกับแลน

ระบบเครือข่ายแลนเป็นรูปแบบที่ใช้สร้างการติดต่อสื่อสารระหว่างเครื่องคอมพิวเตอร์ภายในองค์กรที่ได้รับความนิยมเป็นอย่างสูง แต่บางองค์กรอาจต้องการใช้เครือข่ายแลนหนึ่ง เครือข่าย เพื่อแยกทรัพยากรบางอย่างหรือแผนกต่างๆ ที่อยู่ภายในองค์กรออกจากกัน แต่ก็ยังจำเป็นต้องเชื่อมต่อเครือข่ายแลนทั้งสองเข้าด้วยกัน เพื่อแบ่งปันทรัพยากรบางอย่างให้ใช้งานร่วมกันได้ เช่น ระบบแลนของแผนกจัดซื้อมีเครือข่ายเครื่องพิมพ์เชื่อมต่ออยู่ หากต้องการ

แบ่งปันให้เครือข่ายแลนของแผนกประชาสัมพันธ์ใช้งานเครื่องพิมพ์ดังกล่าวได้จะต้องเชื่อมต่อเครือข่ายแลนทั้งสองเข้าด้วยกันผ่านอุปกรณ์สำหรับเชื่อมต่อเครือข่าย เช่น สวิตช์ หรือเราท์เตอร์

การแยกข้อมูลหรือทรัพยากรบางอย่างของแต่ละแผนกออกจากกัน ถือเป็นการเพิ่มความปลอดภัยให้กับข้อมูล และลดปริมาณข้อมูลที่อยู่ในระบบเครือข่าย โดยสวิตช์เป็นอุปกรณ์ที่สามารถรองข้อมูลจากเครือข่ายที่อยู่ติดกันไม่ให้เข้ามาในเครือข่ายได้ ซึ่งจะช่วยลดปริมาณความหนาแน่นของข้อมูลในเครือข่ายได้เป็นอย่างดี ดังภาพที่ 1.13



ภาพที่ 1.13 แสดงการเชื่อมต่อเครือข่ายแลน 2 เครือข่าย ด้วยอุปกรณ์สวิตช์
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 17)

5. การเชื่อมต่อแพนกับเวิร์กสเตชัน

เครือข่ายส่วนบุคคลหรือแพน เป็นเครือข่ายรูปแบบใหม่ที่ถูกคิดค้นในปี ค.ศ.1990 โดยใช้วิธีส่งข้อมูลแบบไร้สาย (Wireless) ด้วยอุปกรณ์ชนิดต่างๆ เช่น พีดีเอ แล็ปท็อป หรืออุปกรณ์พกพาชนิดอื่นๆ รวมทั้งคอมพิวเตอร์หรือเวิร์กสเตชันที่ติดตั้งการ์ดไวเลทแลนไว้ ข้อมูลที่ส่งสามารถเป็นได้ทั้งข้อมูลเสียง เพลง หรือข้อมูลรูปแบบอื่นๆ เรียกการเชื่อมต่อลักษณะนี้ว่า การเชื่อมต่อแพนกับเวิร์กสเตชัน (Personal Area Network-to-Workstation) แสดงการเชื่อมต่อได้ดังภาพที่ 1.14

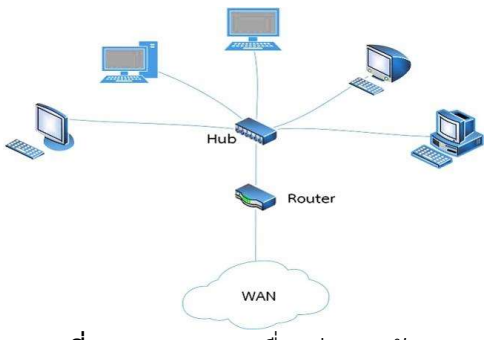
ภาพที่ 1.14 แสดงการเชื่อมต่อพีดีเอกับเวิร์กสเตชันที่อยู่ในระบบแลน
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 17)

6. การเชื่อมต่อแลนกับแมน

บริษัทขนาดใหญ่ที่มีสาขากระจายอยู่ตามสถานที่ต่างๆ ภายในเมืองเดียวกัน จะใช้วิธีการเชื่อมโยงธุรการของตนด้วยสายใยแก้วนำแสง หรือสายไฟเบอร์ออฟติก (Fiber Optic) ซึ่งสามารถส่งข้อมูลด้วยความเร็วสูงได้ เรียกระบบเครือข่ายนี้ว่า เครือข่ายระดับเมือง (Metropolitan Area Network : MAN) เป็นการเชื่อมต่อเครือข่ายด้วยความเร็วสูงจากสถานที่ต่างๆ ที่อยู่ในบริเวณที่สามารถให้บริการได้ นอกจากนี้เครือข่ายแมนอาจเชื่อมต่อกับเครือข่ายแลนเพื่อรับส่งข้อมูลระหว่างกันได้อีกด้วย จึงเรียกการเชื่อมต่อในลักษณะนี้ว่า การเชื่อมต่อแลนกับแมน (Local Area Network-to-Metropolitan Area Network)

7. การเชื่อมต่อแลนกับแวน

องค์กรประกอบที่มีเครื่องคอมพิวเตอร์จำนวนมากเชื่อมต่อกันด้วยเครือข่ายแลน หากต้องการให้คอมพิวเตอร์ที่อยู่ในเครือข่ายแลน สามารถติดต่อสื่อสารกับระบบแวนได้ จะต้องใช้อุปกรณ์เชื่อมต่อที่เรียกว่า เราท์เตอร์ (Router) เพื่อเชื่อมต่อเครือข่ายแลนและแวนเข้าด้วยกัน โดยเราท์เตอร์จะแปลงแพ็กเก็ตข้อมูลให้สามารถรับส่งข้อมูลระหว่างกันได้ เรียกการเชื่อมต่อลักษณะนี้ว่า การเชื่อมต่อแลนกับแวน (Local Area Network-to-Wide Area Network) ดังภาพที่ 1.15



ภาพที่ 1.15 แสดงการเชื่อมต่อแลนกับแวน

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 18)

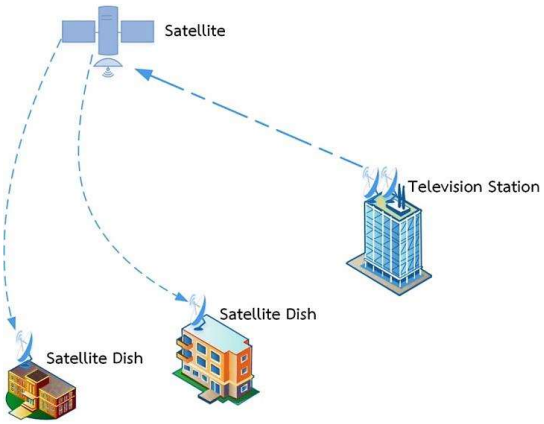
8. การเชื่อมต่อแวนกับแวน

เครือข่ายอินเทอร์เน็ตเป็นเครือข่ายขนาดใหญ่ที่ประกอบด้วยเครือข่ายย่อยๆ จำนวนมาก ดังนั้น การส่งข้อมูลไปยังปลายทางผ่านเครือข่ายอินเทอร์เน็ตจึงอาจจะต้องส่งข้อมูลผ่านเครือข่ายแวนมากกว่าหนึ่งเครือข่าย เรียกการเชื่อมต่อแบบนี้ว่า เครือข่ายระยะไกล

(Wide Area Network-to-Wide Area Network) โดยการเชื่อมต่อระหว่างเครือข่ายแวนจะต้องใช้อุปกรณ์พิเศษที่สามารถค้นหาเส้นทางได้อย่างรวดเร็ว ซึ่งก็คือเราท์เตอร์หรือสวิตช์ที่มีประสิทธิภาพสูง เมื่อแพ็กเก็ตข้อมูลถูกส่งให้กับเราท์เตอร์แล้ว แพ็กเก็ตข้อมูลจะถูกแตกออกเพื่อนำข้อมูลที่เรียกว่า ไอพีแอดเดรส (IP Address) ไปใช้ในการตัดสินใจเลือกเส้นทาง เพื่อส่งแพ็กเก็ตข้อมูลไปยังแวนที่อยู่ถัดไปจนถึงปลายทาง

9. การเชื่อมต่อด้วยไมโครเวฟกับดาวเทียม

ไมโครเวฟและดาวเทียม ถือได้ว่าเป็นเทคโนโลยีที่ได้รับการพัฒนาอย่างต่อเนื่อง ใช้ในการส่งข้อมูลระยะไกลโดยไม่ต้องใช้สายสัญญาณ จึงสามารถนำไปใช้ประโยชน์ได้หลากหลายรูปแบบ เช่น ระบบเคเบิลทีวี ระบบโทรศัพท์ อุตุนิยมวิทยา และระบบนำทาง เป็นต้น



ภาพที่ 1.16 แสดงการให้บริการของสถานีโทรทัศน์ผ่านระบบดาวเทียม
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 19)

10. การรับส่งข้อมูลผ่านเครือข่ายโทรศัพท์เคลื่อนที่

ในปัจจุบันโทรศัพท์เคลื่อนที่นับเป็นอุปกรณ์ที่มีบทบาทในชีวิตประจำวันของมนุษย์เป็นอย่างยิ่ง โดยเครือข่ายโทรศัพท์เคลื่อนที่ (Wireless Telephone Network) ได้รับการพัฒนามาอย่างต่อเนื่อง ทำให้เกิดบริการใหม่ๆ จากเทคโนโลยีดังกล่าวขึ้นมากมาย และบริการหนึ่งที่ได้รับความนิยมอย่างสูง คือ การรับส่งข้อมูลและการเชื่อมต่ออินเทอร์เน็ตผ่านเครือข่ายโทรศัพท์เคลื่อนที่ โดยจะใช้คลื่นความถี่ของโทรศัพท์ไร้สายเพื่อรับส่งข้อมูลระหว่างแล็ปท็อป ดังภาพที่ 1.17

ภาพที่ 1.17 แสดงการรับส่งข้อมูลผ่านเครือข่ายโทรศัพท์เคลื่อนที่

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 20)

1.3 สรุป

การสื่อสารข้อมูล (Data Communication) คือ การแลกเปลี่ยนข้อมูลและสารสนเทศระหว่างอุปกรณ์ผ่านทางสื่อกลางที่ใช้รับส่งข้อมูล โดยอุปกรณ์ที่ใช้ในการสื่อสารข้อมูลเป็นได้ทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ส่วนข้อมูลที่ใช้ในรับส่งกันในระบบคอมพิวเตอร์จะเป็นข้อมูลแบบดิจิทัล (Digital) ซึ่งอยู่ในรูปแบบของ 0 และ 1 โดยเรียกข้อมูลแบบนี้ว่า ไบนารี (Binary Information) การสื่อสารจะประกอบไปด้วยส่วนสำคัญ 5 ประการ ได้แก่ ข่าวสาร ผู้ส่ง ผู้รับ สื่อกลางส่งข้อมูล และโพรโทคอล

เครือข่ายคอมพิวเตอร์ (Computer Network) หมายถึง วิธีการเชื่อมต่อคอมพิวเตอร์เข้าด้วยกันผ่านสื่อกลางต่างๆ เช่น สายสัญญาณ คลื่นวิทยุ เป็นต้น เพื่อให้สามารถสื่อสาร แลกเปลี่ยนข้อมูล และใช้ทรัพยากรร่วมกันได้ โดยเนื้อหาที่เกี่ยวข้องกับการสื่อสารข้อมูลมีหลายรูปแบบ ไม่ได้จำกัดแค่เพียงเครือข่ายที่มีองค์ประกอบเป็นเครือข่ายคอมพิวเตอร์เท่านั้น เครือข่ายมี 5 ประเภท ได้แก่ เครือข่ายส่วนบุคคล เครือข่ายเฉพาะบริเวณ เครือข่ายระดับเมือง เครือข่ายระยะไกล และเครือข่ายควบคุม แต่ละเครือข่ายมีองค์ประกอบสำคัญพื้นฐาน 2 ส่วน คือ องค์ประกอบด้านฮาร์ดแวร์ และด้านซอฟต์แวร์

บทที่ 2
แบบจำลองเครือข่าย

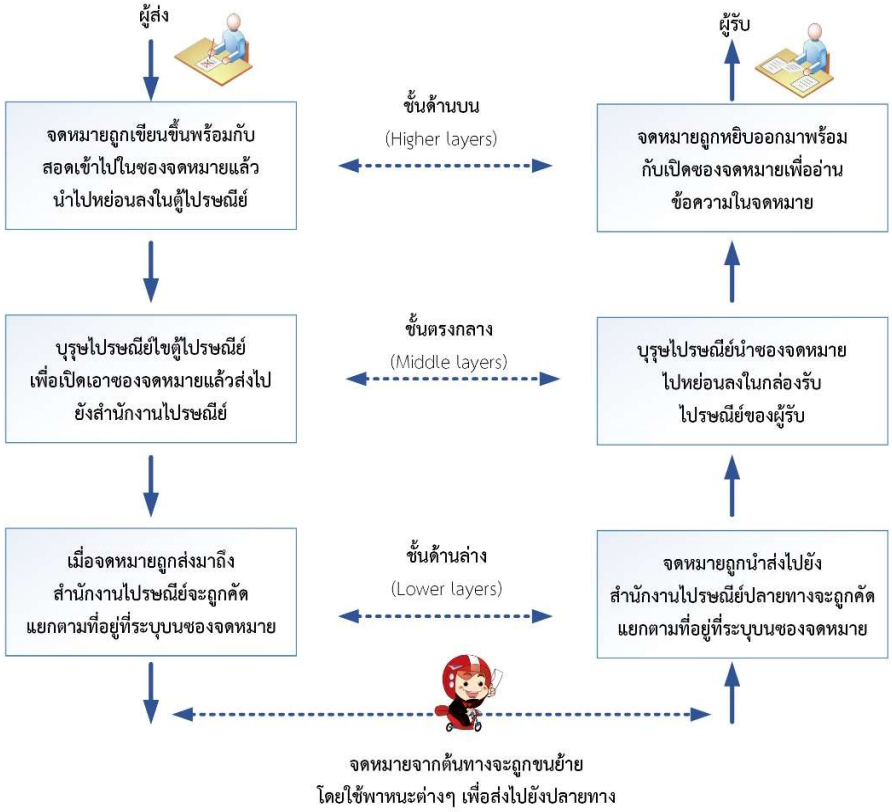
ระบบเครือข่ายหนึ่งประกอบด้วยฮาร์ดแวร์และซอฟต์แวร์ซึ่งทำหน้าที่ส่งข้อมูลจากสถานที่หนึ่งไปยังอีกสถานที่หนึ่ง ฮาร์ดแวร์ ประกอบด้วยอุปกรณ์ทางกายภาพซึ่งทำหน้าที่ประมวลผลและส่งต่อสัญญาณทางไฟฟ้าจากจุดหนึ่งของเครือข่ายไปยังอีกจุดหนึ่ง ส่วนซอฟต์แวร์ประกอบด้วยชุดคำสั่งของการให้บริการที่เป็นไปตามที่ผู้ออกแบบระบบได้กำหนดไว้ซึ่งจะทำหน้าที่ควบคุมการทำงานของฮาร์ดแวร์ และเป็นส่วนติดต่อเพื่อรับคำสั่งจากผู้ใช้งานด้วย แต่เนื่องจากระบบเครือข่ายมีกระบวนการทำงานที่ซับซ้อน ดังนั้น ในการอธิบายถึงการทำงานของระบบเครือข่ายนั้นจึงต้องแบ่งการทำงานออกเป็นระดับชั้นเพื่อให้ง่ายต่อการทำความเข้าใจ

2.1 การทำงานแบบลำดับชั้น

จากการทำงานของฮาร์ดแวร์และซอฟต์แวร์ในแต่ละเครือข่ายจะทำหน้าที่สอดประสานกันอย่างเป็นลำดับ ซึ่งแนวคิดเรื่องการทำงานแบบลำดับชั้นได้มาจากการสื่อสารในชีวิตประจำวัน เช่น การส่งจดหมายทางไปรษณีย์ การทำงานแบบลำดับชั้นจะประกอบด้วย 3 ส่วน คือ ผู้ส่ง (Sender) ผู้รับ (Receiver) และตัวกลางในการส่งข่าวสาร (Carrier) ซึ่งในที่นี้หมายถึงบุรุษไปรษณีย์นั่นเอง โดยกระบวนการส่งจดหมายจะเริ่มจาก ผู้ส่งเริ่มเขียนจดหมายเมื่อเสร็จแล้วจะต้องนำจดหมายใส่ลงไปในซองจดหมายพร้อมทั้งเขียนชื่อที่อยู่ของผู้ส่งและผู้รับ เมื่อผู้ส่งนำจดหมายไปหย่อนลงในตู้ไปรษณีย์ (Mailbox) จากนั้นบุรุษไปรษณีย์จะนำจดหมายออกจากตู้ไปยังที่ทำงานการไปรษณีย์ (Post office) เพื่อทำการคัดแยกจดหมายตามที่อยู่ของผู้รับแล้วขนส่งต่อไป สามารถทำได้หลายวิธี เช่น รถยนต์ เรือ รถไฟ หรือเครื่องบิน เมื่อจดหมายไปถึงไปรษณีย์ปลายทางจะทำการคัดแยกจดหมายแล้วส่งต่อไปตามชื่อที่อยู่ของผู้รับที่ปรากฏอยู่หน้าซองจดหมาย เมื่อผู้รับหยิบจดหมายจากตู้ไปรษณีย์ของตนเอง ก็จะเปิดซองและเริ่มต้นอ่านจดหมาย จึงเสร็จสิ้นการทำงาน (นรรัตน์ วัฒนมงคล, 2561, หน้า 21)

เมื่อพิจารณาแล้วจะเห็นได้ว่าในแต่ละชั้นของการทำงานนั้นจะมีหน้าที่แตกต่างออกไป ที่ต้นทางจะต้องทำงานจากระดับชั้นบนสุด (การเริ่มเขียนจดหมาย) ไปยังระดับชั้นที่อยู่ล่างสุด (การหย่อนจดหมายลงไปในตู้ไปรษณีย์) จากนั้นเจ้าหน้าที่ไปรษณีย์ทั้งหมดจะทำหน้าที่เป็นตัวกลางขนส่งข่าวสารซึ่งอาจจะเป็นจดหมาย เอกสาร หรือพัสดุ โดยใช้ยานพาหนะชนิดต่างๆ ส่วนที่ปลายทางจะทำงานจากระดับชั้นล่างสุด (ที่ทำการไปรษณีย์ปลายทางรับจดหมาย) ไป

จนถึงระดับบนสุด (ผู้รับอ่านจดหมาย) โดยที่แต่ละระดับชั้นจะต้องดำเนินการให้แล้วเสร็จก่อนจึงจะสามารถส่งไปต่อยังชั้นที่อยู่ติดกันได้ ดังภาพที่ 2.1



ภาพที่ 2.1 แสดงลำดับการทำงานของการส่งจดหมายทางไปรษณีย์
ที่มา : (นรรัตน์ วัฒนมงคล, 2561, หน้า 22)

แบบจำลองการสื่อสารข้อมูลและเครือข่ายที่ได้รับความนิยมมากที่สุดตั้งแต่ก่อน ค.ศ. 1990 คือ แบบจำลองโอเอสไอ (Open Systems Interconnection : OSI) คนส่วนใหญ่เชื่อว่าแบบจำลอง โอเอสไอจะกลายมาเป็นมาตรฐานสำหรับการสื่อสารที่ดีที่สุด ซึ่งในเวลาต่อมากลับไม่เป็นเช่นนั้น เนื่องจากโพรโทคอลทีซีพีไอพี (Transmission Control Protocol/Internet Protocol : TCP/IP) เป็นแบบจำลองที่มีโครงสร้างทางสถาปัตยกรรมโดดเด่นในเชิงพาณิชย์ เพราะถูกนำมาใช้และผ่านการทดสอบอย่างเข้มข้นในเครือข่ายอินเทอร์เน็ต ในขณะที่แบบจำลองโอเอสไอไม่เคยถูกนำมาใช้อย่างเต็มรูปแบบ ในบทนี้จะขอกล่าวถึงแบบจำลองโอเอสไอและโพรโทคอลทีซีพีไอพี โดยมีรายละเอียดดังต่อไปนี้

2.2 แบบจำลองโอเอสไอ

ไอเอสโอ (ISO) เป็นองค์กรที่ได้รับการยอมรับทั่วโลกทำหน้าที่กำหนดมาตรฐานสากล ช่วงปี ค.ศ.1970 ได้จัดตั้งคณะกรรมการขึ้นมา เพื่อสร้างแบบจำลองสถาปัตยกรรมเครือข่าย เพื่อใช้เป็นแบบมาตรฐานในการสื่อสารระหว่างคอมพิวเตอร์ภายใต้ชื่อว่าแบบจำลองโอเอสไอ (Open System Interconnection : OSI) และในปี ค.ศ.1984 จึงได้ประกาศใช้แบบจำลองโอเอสไออย่างเป็นทางการเพื่อใช้เป็นแบบอ้างอิงเครือข่ายมาตรฐานสากล

มาตรฐานระบบเปิด (Open System) จะอนุญาตให้ระบบสามารถสื่อสารกันได้แม้ว่าอุปกรณ์จะมีสถาปัตยกรรมระบบที่แตกต่างกันก็ตาม กล่าวคือ แบบจำลองโอเอสไอมีจุดประสงค์เพื่อให้ระบบที่มีความแตกต่างกันสามารถสื่อสารร่วมกันได้ผ่านมาตรฐานสื่อสารที่เป็นสากล โดยไม่จำเป็นต้องเข้าไปเปลี่ยนแปลงประการใดๆ บนอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ อย่างไรก็ตามแบบจำลองโอเอสไอมิใช่โพรโทคอล แต่เป็นเพียงแบบจำลองแนวความคิดซึ่งเป็นเพียงทฤษฎีช่วยสร้างความเข้าใจในหลักการทำงานของแต่ละชั้นสื่อสาร เพื่ออำนวยความสะดวกต่อผู้ออกแบบระบบสื่อสาร (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 66)

แบบจำลองโอเอสไอ เตรียมการรายละเอียดต่างๆ ของฟังก์ชันและบริการที่สามารถเกิดขึ้นได้ในแต่ละเลเยอร์ รวมถึงการทำงานร่วมกันของแต่ละเลเยอร์โดยตรงทั้งข้างบนและข้างล่าง (พิสิฐ พรพงศ์เตชวาณิช และพงษ์พิสิฐ วุฒิดิษฐโชติ, 2566, หน้า 71)

กรอบการทำงานบนแบบจำลองโอเอสไอจะแบ่งชั้นสื่อสารเรียกว่า **เลเยอร์** (Layer) ซึ่งมีทั้งสิ้น 7 ชั้นสื่อสาร ดังนี้ (นรรัตน์ วัฒนมงคล, 2561, หน้า 22)

ชั้นที่ 1 ชั้นสื่อสารกายภาพ (Physical Layer)
ชั้นที่ 2 ชั้นเชื่อมโยงข้อมูล (Data link Layer)
ชั้นที่ 3 ชั้นติดต่อระดับเครือข่าย (Network Layer)
ชั้นที่ 4 ชั้นขนส่งข้อมูล (Transport Layer)
ชั้นที่ 5 ชั้นควบคุมเซสชัน (Session Layer)
ชั้นที่ 6 ชั้นนำเสนอข้อมูล (Presentation Layer)
ชั้นที่ 7 ชั้นติดต่อแอปพลิเคชัน (Application Layer)

อย่างไรก็ตาม เทคโนโลยีเครือข่ายการสื่อสารทั้งหลายไม่จำเป็นที่จะต้องอ้างอิงชั้นสื่อสารบนแบบจำลองโอเอสไอครบทั้งเจ็ดชั้น เนื่องจากบางเทคโนโลยีอาจรวมชั้นสื่อสารบางชั้น

มาเป็นชั้นเดียวกัน หรืออาจข้ามการทำงานบางชั้นโดยเฉพาะกรณีชั้นนั้นๆ ไม่จำเป็นต่อการทำงาน (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 67)

2.2.1 แนวคิดในการแบ่งชั้นสื่อสาร

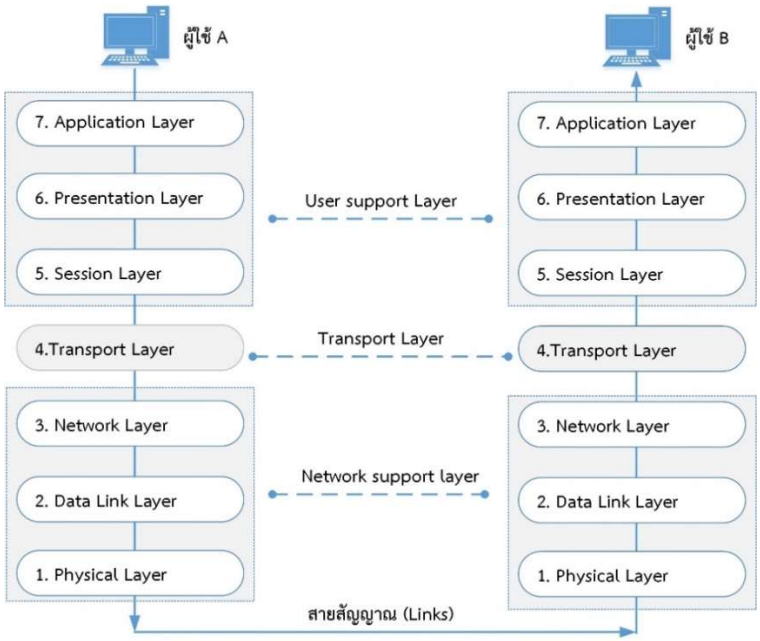
แนวคิดในการแบ่งชั้นสื่อสารบนแบบจำลองโอเอสไอ สามารถสรุปเป็นข้อๆ ได้ดังนี้ (นรรัตน์ วัฒนมงคล, 2561, หน้า 22)

1. เพื่อลดความซับซ้อน ทำให้ง่ายต่อการเรียนรู้และการทำความเข้าใจ
2. เพื่อให้แต่ละชั้นสื่อสาร มีบทบาทหน้าที่อย่างชัดเจน และแตกต่างกัน
3. เพื่อให้แต่ละชั้นสื่อสารสามารถปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมาย และสอดคล้องกับมาตรฐานสากล
4. จากขอบเขตความรับผิดชอบในแต่ละชั้นสื่อสาร ทำให้การสื่อสารเกิดความคล่องตัว และยังป้องกันกรณีการเปลี่ยนแปลงบนชั้นสื่อสารหนึ่งๆ ที่อาจส่งผลกระทบต่อชั้นสื่อสารอื่นๆ
5. จำนวนชั้นสื่อสารจะต้องมีเพียงพอต่อการกำหนดหน้าที่ให้กับแต่ละชั้นสื่อสารได้อย่างเหมาะสมและครบถ้วน แต่ก็ไม่ควรมีมากเกินไปจนแลดูเทอะทะหรือเกินความจำเป็น

2.2.2 สถาปัตยกรรมการแบ่งชั้น (Layer Architecture)

แบบจำลองโอเอสไออธิบายถึงสิ่งที่เกิดขึ้นเมื่ออุปกรณ์ที่เชื่อมโยงกันสนทนากัน ลำดับชั้นทั้งหมดจะสนับสนุนในส่วนฮาร์ดแวร์และซอฟต์แวร์ รวมทั้งการติดต่อถึงกันของทั้งสองข้างที่ต้องการสื่อสารเข้าด้วยกันคือด้านส่งและด้านรับ ระบบเครือข่ายคอมพิวเตอร์สมัยใหม่จะออกแบบให้มีโครงสร้างที่แน่นอน และเพื่อเป็นการลดความซับซ้อน ระบบเครือข่ายส่วนมากจึงแยกการทำงานออกเป็นชั้นๆ โดยกำหนดหน้าที่ในแต่ละชั้นไว้อย่างชัดเจน แบบจำลองโอเอสไอประกอบด้วย 7 ชั้น คือชั้นกายภาพ ชั้นเชื่อมโยงข้อมูล ชั้นเครือข่าย ชั้นเคลื่อนย้ายข้อมูล ชั้นแบ่งแยกข้อมูล ชั้นนำเสนอข้อมูล และชั้นประยุกต์ใช้งาน ตามลำดับ จากภาพที่ 2.2 จะแสดงการทำงานที่เกี่ยวข้องกันในแต่ละชั้นเมื่อต้องการส่งข่าวสารจากผู้ใช้ A ไปยังผู้ใช้ B เริ่มต้นในขณะที่ข่าวสารถูกส่งจาก A ไป B ผ่านอุปกรณ์เครือข่ายชนิดต่างๆ จำนวนมากกว่าที่ข่าวสารจะเดินทางไปถึงผู้ใช้ปลายทาง โดยอุปกรณ์เครือข่ายที่ข่าวสารเคลื่อนที่ผ่านส่วนใหญ่จะทำงานภายใน 3 ชั้นแรกของแบบจำลองเท่านั้น

การพัฒนาแบบจำลองในแต่ละชั้นมีหน้าที่การทำงานที่แตกต่างกัน แต่ละชั้นทำหน้าที่ในการให้บริการกับชั้นที่อยู่สูงขึ้นถัดไป เช่น ชั้นที่ 3 จะได้รับบริการจากชั้นที่ 2 และเป็นผู้ให้บริการกับชั้นที่ 4 ส่วนการติดต่อระหว่างคอมพิวเตอร์สองเครื่องนั้น ถึงแม้ว่าจะมีการส่งข้อมูลขึ้นหรือลงไปตามชั้นต่างๆ แต่ความจริงจะเป็นการติดต่อระหว่างชั้นเดียวกันเท่านั้น เช่น ชั้นที่ x ของเครื่องหนึ่งจะติดต่อกับชั้นที่ x ของอีกเครื่องหนึ่ง เนื่องจากภายในชั้นเดียวกันจะมีโพรโทคอลเหมือนกันจึงทำให้สามารถสื่อสารกันได้เข้าใจ ในขณะที่ชั้นอื่นๆ มีโพรโทคอลที่แตกต่างกันออกไป การสื่อสารเช่นนี้จะเป็นไปตามกฎเกณฑ์ข้อตกลงของที่ประชุมซึ่งจะถูกเรียกว่าโพรโทคอล และกระบวนการของอุปกรณ์สื่อสารแต่ละตัวในชั้นที่กำหนดจะถูกเรียกว่า กระบวนการเพียร์ทูเพียร์ (Peer-to-Peer Processes : PPP) ดังนั้น การสื่อสารระหว่างอุปกรณ์เครือข่ายคือกระบวนการเพียร์ทูเพียร์ ที่ใช้โพรโทคอลได้อย่างเหมาะสมกับแต่ละชั้นของแบบจำลอง ดังภาพที่ 2.2 (นรรัตน์ วัฒนมงคล, 2561, หน้า 22-26)



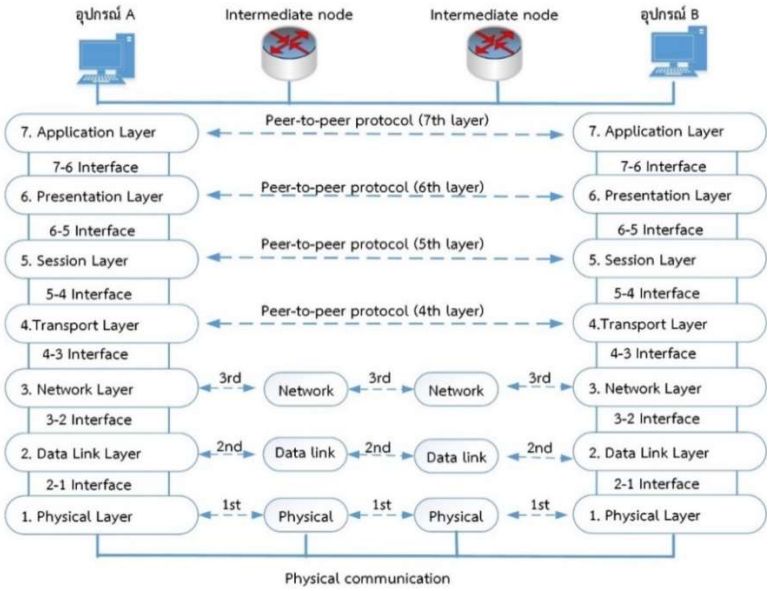
ภาพที่ 2.2 การแบ่งชั้นการทำงานตามแบบจำลองโอเอสไอ

ที่มา : (นรรัตน์ วัฒนมงคล, 2561, หน้า 25)

2.2.3 กระบวนการเพียร์ทูเพียร์ (Peer-to-Peer Processes)

ที่ชั้นกายภาพการสื่อสารจะเกิดขึ้นได้โดยตรง จากรูปที่ 2.2 อุปกรณ์ A ต้องการส่งบิตข้อมูลไปยังอุปกรณ์ B ผ่านอุปกรณ์เครือข่ายจำนวนมาก โดยชั้นที่อยู่สูงจะต้องทำการสื่อสารกับชั้นที่อยู่ต่ำกว่าของอุปกรณ์ A ไปยังอุปกรณ์ B และมีการสำรองข้อมูลที่ผ่านการประมวลผลแล้วในแต่ละชั้นก่อนที่จะส่งข้อมูลผ่านต่อไปยังชั้นถัดไป เนื่องจากแต่ละชั้นมีการทำงานแตกต่างกัน ดังนั้นหากมีข้อผิดพลาดเกิดขึ้นในระหว่างการสื่อสารจะสามารถตรวจจอบข้อมูลย้อนกลับไปยังชั้นที่เกิดปัญหาขึ้นเพื่อแก้ไขใหม่ในชั้นที่ 1 ข้อมูลทั้งหมดจะถูกแปลงให้อยู่ในรูปที่สามารถถูกส่งผ่านไปยังอุปกรณ์ภาครับได้ ที่อุปกรณ์ภาครับในชั้นที่ 2 และชั้นที่สูงขึ้นไป ข่าวสารจะถูกเปิดเผยออกโดยการประมวลผลที่เกิดขึ้นในแต่ละชั้นเพื่อแปลความหมายออกมา

ในการส่งข้อมูลระหว่างชั้นนั้นจะต้องอาศัยอุปกรณ์อินเตอร์เฟซ (Interface) เป็นตัวกลางในการติดต่อระหว่างชั้น ถึงแม้ว่าแต่ละชั้นจะมีการเปลี่ยนแปลงวิธีการทำงานไป แต่หากอินเตอร์เฟซไม่เปลี่ยน การเปลี่ยนแปลงนั้นจะไม่ส่งผลกระทบต่อการทำงานระหว่างกันในแต่ละชั้น หมายความว่า ผู้ออกแบบระบบสามารถเปลี่ยนแปลงหรือเพิ่มเติมการทำงานในแต่ละชั้นใดๆ ได้โดยไม่ต้องไปแก้ไขการทำงานของชั้นอื่นๆ ตามไปด้วย หรือกล่าวได้อีกทางหนึ่งว่าแต่ละชั้นจะมีการทำงานที่เป็นอิสระจากกัน ดังภาพที่ 2.3



ภาพที่ 2.3 กระบวนการทำงานเพียร์ทูเพียร์ตามแบบจำลองโอเอสไอ

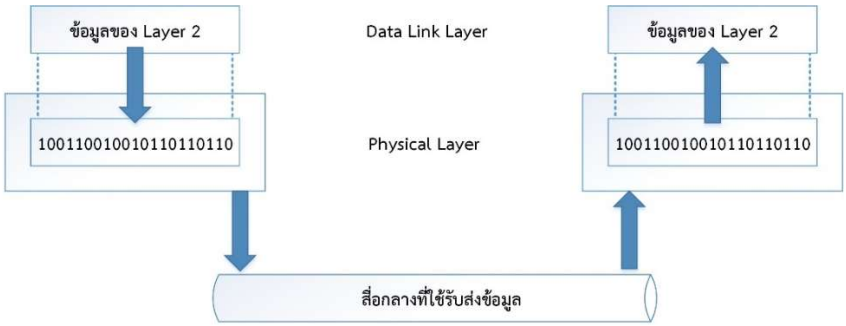
ที่มา : (นรรัตน์ วัฒนมงคล, 2561, หน้า 26)

2.2.4 การจัดชั้นสื่อสารในแบบจำลองโอเอสไอ

แบบจำลองโอเอสไอ (OSI Model) ได้แบ่งรายละเอียดและหน้าที่ของแต่ละชั้นสื่อสารไว้แตกต่างกัน โดยมีวัตถุประสงค์เพื่อคอยให้บริการแก่ชั้นสื่อสารที่อยู่สูงกว่า โดยชั้นที่อยู่สูงกว่าไม่จำเป็นต้องทราบรายละเอียดการทำงานของชั้นที่อยู่ต่ำกว่า แบบจำลองของโอเอสไอประกอบด้วย 7 ชั้นสื่อสาร ซึ่งมีรายละเอียดดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 22-32)

ชั้นที่ 1 ชั้นสื่อสารกายภาพ

ชั้นสื่อสารกายภาพ (Physical Layer : Layer 1) เป็นชั้นที่อยู่ล่างสุดของแบบจำลองโอเอสไอซึ่งมีหน้าที่จัดการกับการติดต่อสื่อสารในระดับกายภาพ กล่าวคือ เป็นชั้นที่ทำการติดต่อกับอุปกรณ์และสื่อกลางโดยตรง โดยข้อมูลที่อยู่ในชั้นนี้จะเป็นข้อมูลระดับบิต (Bit) มีลักษณะข้อมูลแบบไบนารี (Binary) หรือเลขฐานสอง (มี 1 และ 0 เท่านั้น) ข้อมูลเหล่านี้จะถูกส่งผ่านสื่อกลางมาในรูปแบบของสัญญาณต่างๆ เช่นสัญญาณไฟฟ้า และสัญญาณแสง เป็นต้น ดังภาพที่ 2.4



ภาพที่ 2.4 แสดงตัวอย่างการส่งข้อมูลชั้นสื่อสารกายภาพ

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 22)

จากภาพที่ 2.4 ต้นทางข้อมูลจากชั้นที่ 2 จะถูกส่งมาที่ชั้นติดต่อระดับกายภาพ โดยจะจัดการกับข้อมูลระดับบิตให้อยู่ในรูปแบบของสัญญาณก่อนที่จะส่งผ่านสื่อกลางต่างๆ ที่ใช้ในการรับส่งข้อมูล เมื่อสัญญาณดังกล่าวส่งถึงยังปลายทางชั้นติดต่อระดับกายภาพก็จะแปลงกลับจากสัญญาณเป็นข้อมูลระดับบิตและส่งข้อมูลดังกล่าวไปยังชั้นที่ 2 ต่อไป

หน้าที่ที่เกี่ยวข้องกับชั้นติดต่อระดับกายภาพ

1. สามารถเข้าใจถึงลักษณะการเชื่อมต่อระหว่างอุปกรณ์และสื่อกลาง ทราบถึงชนิดของสื่อกลาง ทำให้เข้าใจถึงรูปแบบของสัญญาณต่างๆ ที่ส่งมาได้

2. ทำหน้าที่จัดการกับข้อมูลระดับบิต โดยสามารถเข้ารหัสข้อมูลระดับบิตให้อยู่ในรูปแบบสัญญาณเพื่อทำการส่งผ่านสื่อกลางที่เชื่อมต่ออยู่ กล่าวคือ ทำการเปลี่ยน 1 และ 0 ให้เป็นสัญญาณรูปแบบต่างๆ

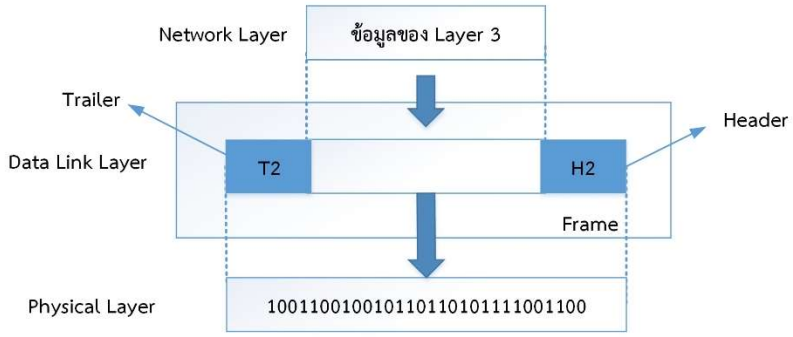
3. คำนวณหาอัตราการส่งข้อมูลจากจำนวนบิตที่ส่งในหนึ่งวินาที เพื่อให้ทราบถึงระยะเวลาในการส่งข้อมูล สามารถหาได้ในชั้นติดต่อระดับกายภาพ

4. ชั้นติดต่อระดับกายภาพจะเข้าใจถึงลักษณะของการเชื่อมโยงและรูปแบบการส่งข้อมูลแบบต่างๆ ทำให้ทราบถึงทิศทางในการส่งข้อมูลและสถานะในการติดต่อสื่อสารกับโหนดอื่นๆ เช่น การเชื่อมต่อในลักษณะจุดต่อจุด (Point-to-Point) ที่มีการส่งข้อมูลแบบฮาฟดูเพล็กซ์ (Half-Duplex) แต่ละเครื่องจะทราบว่าเส้นทางเชื่อมโยงมีหนึ่งเส้นทางโดยใช้ร่วมกันเพียงแค่ 2 เครื่องเท่านั้นและทั้ง 2 เครื่องสามารถสลับสถานะเป็นผู้รับหรือผู้ส่งข้อมูลได้ เป็นต้น

5. สามารถเข้าใจถึงโครงสร้างเครือข่ายแบบต่างๆ ได้ เนื่องจากในการเชื่อมต่อระหว่างอุปกรณ์บนเครือข่ายแต่ละแบบจะมีโครงสร้างการเชื่อมต่อที่แตกต่างกัน เช่น โครงสร้างเครือข่ายแบบรูปดาว การเชื่อมต่อระหว่างอุปกรณ์จะถูกรวมไว้ที่ศูนย์กลาง แต่โครงสร้างเครือข่ายแบบเมช จะนำทุกอุปกรณ์บนเครือข่ายมาเชื่อมต่อกันเป็นต้น

ชั้นที่ 2 ชั้นเชื่อมโยงข้อมูล (Data Link Layer : Layer 2)

ในชั้นเชื่อมโยงข้อมูล (Data Link Layer : Layer 2) นี้จะรับผิดชอบการเชื่อมโยงของข้อมูล ตรวจสอบความถูกต้องของการติดต่อจากโหนดหนึ่งไปยังอีกโหนดหนึ่ง (Node-to-Node) และความสมบูรณ์ของการรับส่งข้อมูล ซึ่งกระบวนการส่งข้อมูลจะถูกต้องและสมบูรณ์ได้นั้น ผู้รับจะต้องได้ข้อมูลที่ถูกต้องพร้อมทั้งตรวจสอบความผิดพลาดก่อนที่จะส่งข้อความตอบกลับไปยังผู้ส่ง และผู้ส่งจะต้องได้รับข้อความตอบกลับดังกล่าวด้วย สำหรับในชั้นเชื่อมโยงข้อมูลนี้จะทำการแบ่งข้อมูลระดับบิตที่ได้จากชั้นติดต่อระดับกายภาพให้เป็นชุดข้อมูลที่เรียกว่า **เฟรม** (Frame) ก่อนจะส่งไปยังชั้นถัดไป ดังภาพที่ 2.5



ภาพที่ 2.5 แสดงตัวอย่างการส่งข้อมูลชั้นเชื่อมโยงข้อมูล

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 23)

ข้อมูลในชั้นเชื่อมโยงข้อมูลที่ได้รับจากชั้นที่ 3 จะนำมาจัดการเพิ่มเติมข้อมูลในส่วนหัว (Header) และส่วนหาง (Trailer) ก่อนจะทำการส่งไปยังชั้นที่ 1 เพื่อแปลงเป็นสัญญาณและส่งไปยังปลายทาง ดังภาพที่ 2.5 เมื่อปลายทางได้รับข้อมูลที่ผ่านการจัดการในชั้นที่ 1 เรียบร้อยแล้วจะดำเนินการแปลงข้อมูลระดับบิตกลับไปเป็นข้อมูลในรูปแบบของเฟรมและถอดข้อมูลที่เพิ่มเติมในส่วนหัวและส่วนทางออก ก็จะได้ชุดข้อมูลที่พร้อมจะส่งไปยังชั้นที่ 3 ต่อไป

หน้าที่ที่เกี่ยวข้องกับชั้นเชื่อมโยงข้อมูล

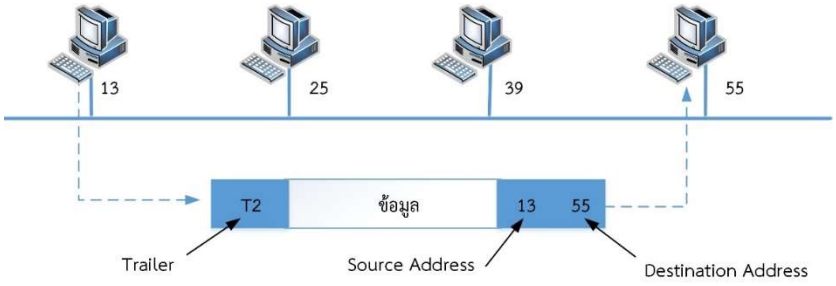
1. ทำการแบ่งข้อมูลระดับบิตที่ได้รับจากชั้นติดต่อระดับกายภาพให้เป็นชุดข้อมูลที่สามารถนำไปใช้ในชั้นถัดไปได้ เรียกชุดข้อมูลดังกล่าวว่า เฟรม (Frame)

2. มีการปรับปรุงข้อมูลส่วนหัว (Header) ซึ่งเป็นข้อมูลบ่งบอกถึงที่อยู่ระดับกายภาพ (Physical Address) ลงในส่วนแรกสุดของเฟรม โดยที่อยู่ระดับกายภาพของผู้ส่งเรียกว่า Source Address และของผู้รับเรียกว่า Destination Address

3. สามารถควบคุมการไหลของข้อมูล เมื่ออัตราการส่งข้อมูลจากต้นทางมีปริมาณมากกว่าอัตราการรับข้อมูลที่ปลายทางจะทำการขัดขวางและควบคุมการไหลของข้อมูลเพื่อไม่ให้เกิดการล้นของข้อมูลขึ้น ซึ่งอาจส่งผลให้เครือข่ายหยุดการทำงาน

4. ตรวจสอบและควบคุมความผิดพลาดของข้อมูล เพื่อป้องกันเฟรมที่เสียหายและทราบถึงเฟรมที่อาจสูญหายในระหว่างการส่ง โดยจะทำการเพิ่มข้อมูลส่วนหาง (Trailer) ลงในส่วนท้ายของเฟรม

5. ควบคุมการเชื่อมต่อ เมื่อมีการเชื่อมต่อระหว่างอุปกรณ์มากกว่า 2 ชิ้นขึ้นไป ภายในเส้นทางที่เชื่อมโยงเดียวกัน ซึ่งจำเป็นต้องใช้โพรโทคอลในชั้นเชื่อมโยงข้อมูลเป็นตัวดูแลและควบคุมการเชื่อมต่อดังกล่าว ดังภาพที่ 2.6

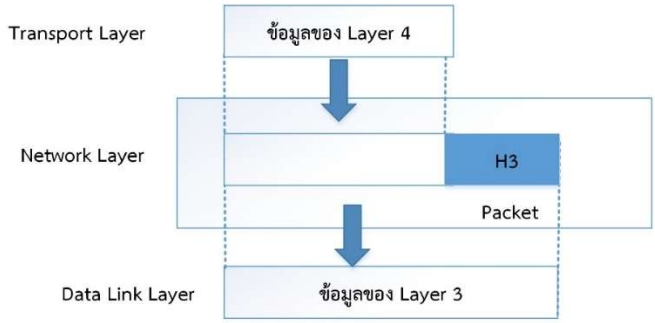


ภาพที่ 2.6 แสดงตัวอย่างการส่งข้อมูลในชั้นเชื่อมโยงข้อมูล
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 24)

จากภาพที่ 2.6 เป็นการรับส่งข้อมูลภายในเครือข่ายที่ถูกจัดการโดยใช้เชื่อมโยงข้อมูล หากต้นทางและปลายทางมีที่อยู่ในระดับกายภาพ คือ 13 และ 55 ตามลำดับ ข้อมูลดังกล่าวจะถูกเพิ่มลงในส่วนหัว (Header) ของเฟรมข้อมูลซึ่งจะมีข้อมูลที่เกี่ยวข้องกับที่อยู่ระดับกายภาพ (Physical Address) บรรจุไว้ด้วย ทำให้ข้อมูลถูกส่งไปยังเครื่องปลายทางที่อยู่ภายในเครือข่ายเดียวกันได้อย่างถูกต้อง

ชั้นที่ 3 ชั้นติดต่อระดับเครือข่าย

ชั้นติดต่อระดับเครือข่าย (Network Layer : Layer 3) เป็นชั้นที่ดูแลเกี่ยวกับเส้นทางในการรับส่งข้อมูลจากต้นทางไปยังปลายทาง ซึ่งจะทำการค้นหาเส้นทางในการขนส่งข้อมูลและจัดการที่อยู่ของปลายทาง โดยชั้นการติดต่อระดับเครือข่ายจะรับผิดชอบเฉพาะการติดต่อสื่อสารระหว่างต้นทางและปลายทางที่อยู่เครือข่ายเดียวกัน ส่วนการติดต่อที่อยู่ภายในเครือข่ายหรือใช้เส้นทางการเชื่อมโยงเดียวกันจะเป็นหน้าที่ของชั้นเชื่อมโยงข้อมูล สำหรับข้อมูลที่ถูกจัดการในชั้นนี้จะเป็นกลุ่มข้อมูลที่เรียกว่า **แพ็กเก็ต** (Packet) ดังภาพที่ 2.7



ภาพที่ 2.7 แสดงตัวอย่างการส่งข้อมูลชั้นติดต่อระดับเครือข่าย
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 25)

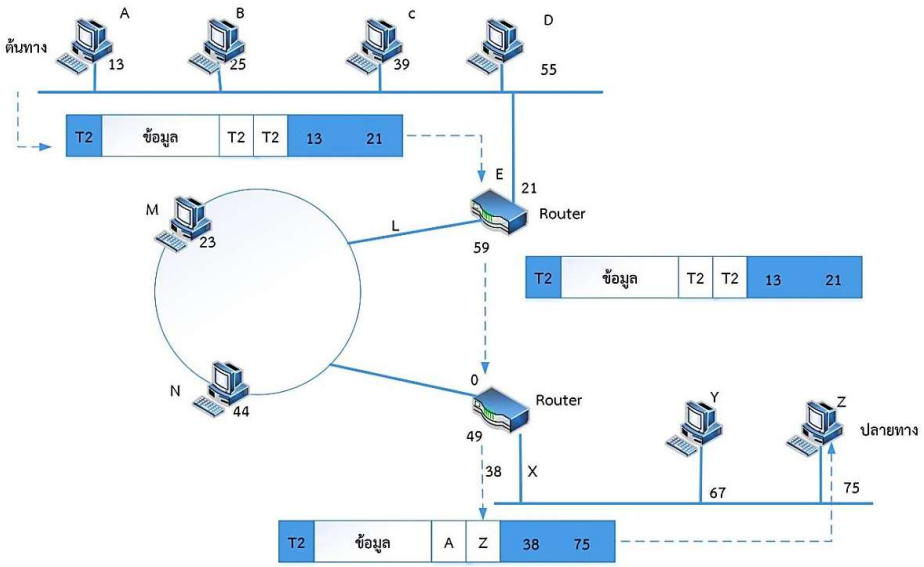
เมื่อได้รับข้อมูลจากชั้นที่ 4 ในชั้นติดต่อระดับเครือข่ายจะเพิ่มเติมข้อมูลในส่วนหัวเข้าไป ซึ่งข้อมูลดังกล่าวจะเป็นที่อยู่ระดับโลจิคอล (Logical) ที่จำเป็นต่อการส่งข้อมูลระหว่างเครือข่าย จากนั้นจึงส่งแพ็กเก็ตข้อมูลที่ถูกจัดการเรียบร้อยแล้วไปยังชั้น 2 สำหรับปลายทางในชั้นติดต่อเครือข่ายเมื่อได้รับแพ็กเก็ตข้อมูลก็จะทำการถอดข้อมูลส่วนหัวออกและข้อมูลส่วนที่เหลือก็จะส่งไปอย่างชั้นที่ 4 ต่อไป

หน้าที่การทำงานของชั้นติดต่อระดับเครือข่าย

1. ค้นหาเส้นทางในการขนส่งข้อมูลจากต้นทางไปยังปลายทาง เมื่อเครือข่ายต่างๆ มีการเชื่อมต่อกันจนกลายเป็นเครือข่ายขนาดใหญ่หรือที่เรียกว่า อินเทอร์เน็ตเวิร์ก (Internetwork) ทำให้เกิดการเชื่อมต่อกันระหว่างอุปกรณ์ของต่างเครือข่าย จึงจำเป็นต้องมีการค้นหาเส้นทางที่จะส่งกลุ่มข้อมูลหรือแพ็กเก็ตไปยังปลายทางที่ถูกต้อง

2. การระบุที่อยู่จะมีการบ่งบอกถึงที่อยู่ระดับเครือข่าย (Network Address) และที่อยู่ของเครื่องปลายทาง ซึ่งที่อยู่ระดับเครือข่ายนั้นจะช่วยให้แพ็กเก็ตถูกส่งไปยังเครือข่ายที่ถูกต้อง โดยที่อยู่ดังกล่าวจะเป็นของอุปกรณ์ที่เป็นตัวเชื่อมโยงเข้ากับเครือข่ายอื่นหรือเครือข่ายของต้นทาง

3. ที่อยู่ระดับตรรกะ (Logical Address) จะถูกบรรจุลงในข้อมูลส่วนหัว (Header) ซึ่งแตกต่างจากที่อยู่ระดับกายภาพ (Physical Address) เนื่องจากการส่งแพ็คเกจไปยังเครือข่ายอื่นไม่สามารถใช้ที่อยู่ระดับกายภาพได้ แต่จะต้องใช้ที่อยู่ระดับตรรกะแทน ทำให้มีการบรรจุที่อยู่ระดับตรรกะของผู้รับและผู้ส่งไปด้วย ดังภาพที่ 2.8



ภาพที่ 2.8 แสดงตัวอย่างการส่งข้อมูลชั้นติดต่อระดับเครือข่าย

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 26)

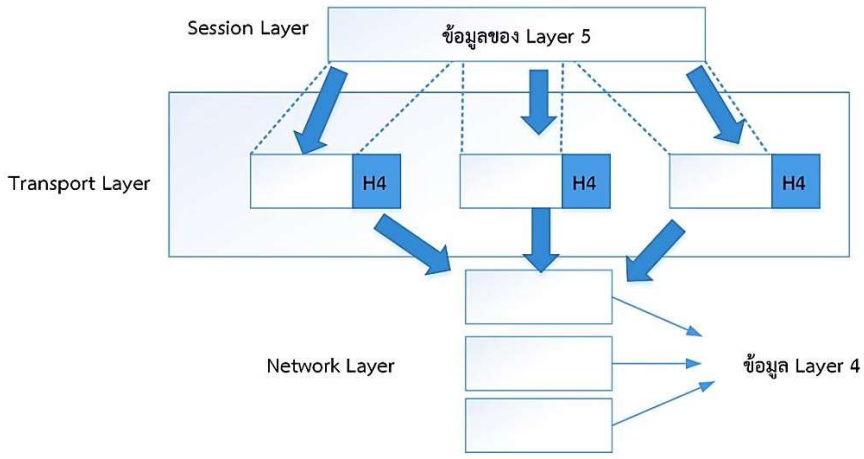
จากภาพที่ 2.8 เป็นการส่งข้อมูลจากเครื่องต้นทางซึ่งมีที่อยู่ระดับเครือข่ายและระดับกายภาพคือ A (Network Address) และ 13 (Physical Address) โดยต้องการส่งข้อมูลไปยังเครื่องปลายทางที่อยู่ในเครือข่ายแลนอีกเครือข่ายหนึ่ง ซึ่งมีที่อยู่ระดับเครือข่ายและที่อยู่ระดับกายภาพคือ Z (Network Address) และ 75 (Physical Address) เนื่องจากเครื่องทั้งสองนั้นอยู่ต่างเครือข่ายกัน จึงไม่สามารถใช้เพียงที่อยู่ในระดับกายภาพได้ ในการรับส่งดังกล่าวจำเป็นต้องใช้ที่อยู่ระดับเครือข่ายและที่อยู่ระดับกายภาพควบคู่กัน โดยที่อยู่ระดับเครือข่ายนั้นจะสามารถระบุที่อยู่ของเครื่องปลายทาง ซึ่งอยู่นอกเครือข่ายแลนของตนได้ สำหรับที่อยู่ระดับเครือข่ายนี้จะบรรจุอยู่ในแพ็กเก็ตข้อมูลที่ถูกกำหนดขึ้นจากการทำงานของชั้นติดต่อระดับเครือข่ายซึ่งที่อยู่ระดับเครือข่ายนั้นจะไม่มีการเปลี่ยนแปลงใดๆ เกิดขึ้นเมื่อเดินทางระหว่างเครือข่าย แต่สำหรับที่อยู่ระดับกายภาพนั้นจะเปลี่ยนแปลงเสมอเมื่อเดินทางเข้าสู่เครือข่ายใหม่ เมื่อผ่านอุปกรณ์เชื่อมต่อของเครือข่ายนั้นที่อยู่ระดับกายภาพจะถูกกำหนดขึ้นใหม่ตามรูปแบบของแต่ละเครือข่าย

ในการส่งข้อมูลไปยังเครื่องไปทางนั้นชั้นติดต่อระดับเครือข่ายจะส่งแพ็กเก็ตข้อมูลให้กับชั้นเชื่อมโยงซึ่งจะหาตำแหน่งของเครื่องด้วยที่อยู่ระดับกายภาพ แต่เมื่อต้องการส่ง

ข้อมูลข้ามไปยังเครือข่ายอื่นแล้ว ที่อยู่ระดับกายภาพเดิมจะถูกเปลี่ยนแปลงให้เข้ากับเครือข่ายนั้นด้วย โดยอุปกรณ์เชื่อมต่อระหว่างเครือข่าย เช่น เราท์เตอร์ จะมีหน้าที่ในการค้นหาเครื่องของผู้รับที่ถูกต้อง โดยจะทำการจัดเก็บตารางเส้นทางไว้เพื่อใช้ค้นหาว่ามีเครื่องปลายทางเชื่อมต่ออยู่ภายในเครือข่ายของตนหรือไม่ หากไม่มีก็จะดูเส้นทางอื่นและส่งต่อไปยังอุปกรณ์เชื่อมต่อระหว่างเครือข่ายต่อไป

ชั้นที่ 4 ชั้นขนส่งข้อมูล

ชั้นขนส่งข้อมูล (Transport Layer : Layer 4) เป็นชั้นที่เกี่ยวข้องกับการขนส่งข้อมูลจากต้นทางไปยังปลายทาง (End-to-End) และตรวจสอบความถูกต้องของแพ็กเก็ต โดยจะทำการตรวจสอบแพ็กเก็ตที่ส่งมาว่าครบถ้วนและสมบูรณ์หรือไม่ ถ้าข้อมูลที่ส่งมามีขนาด 12 MB เมื่อ แพ็กเก็ตเดินทางไปยังปลายทางข้อมูลที่ได้รับก็จะต้องมีขนาด 12 MB เท่าเดิมไม่เกิดการสูญหายหรือเสียหายระหว่างทาง หากตรวจพบว่ามีแพ็กเก็ตไม่ครบก็จะต้องทำการส่งใหม่อีกครั้ง หลังจากได้รับแพ็กเก็ตทั้งหมดแล้วจึงทำการจัดเรียงแพ็กเก็ตให้ได้ตามลำดับอย่างถูกต้องก่อนทำการส่งต่อไปยังชั้นถัดไป ในชั้นขนส่งข้อมูลนั้นจะมีการควบคุมความผิดพลาดและควบคุมการไหลของข้อมูลเหมือนกับในชั้นเชื่อมโยงข้อมูล สำหรับการเชื่อมต่อเส้นทางในการขนส่งนั้นจะเริ่มต้นด้วยการสร้างเส้นทาง จากนั้นจึงทำการขนส่งข้อมูลเมื่อเสร็จเรียบร้อยแล้วจึงยกเลิกเส้นทางเชื่อมต่อ ดังภาพที่ 2.9



ภาพที่ 2.9 แสดงตัวอย่างการส่งข้อมูลชั้นขนส่งข้อมูล

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 28)

ข้อมูลจากชั้นที่ 5 จะถูกแบ่งย่อยและเพิ่มเติมข้อมูลส่วนหัวในชั้นขนส่งข้อมูลซึ่งข้อมูลส่วนหัวจะบรรจุที่อยู่ของพอร์ต (Port Address) ไว้ หลังจากนั้นส่วนย่อยที่ถูกแบ่งจะถูกลำเลียงสู่ชั้นที่ 3 ตามลำดับการแบ่งอย่างถูกต้อง เพื่อเตรียมส่งข้อมูลต่อไป ดังภาพที่ 2.9 เมื่อข้อมูลถูกส่งไปยังปลายทางแล้ว ข้อมูลจากชั้นที่ 3 จะถูกลำเลียงมาถอดข้อมูลส่วนหัวออกและประกอบข้อมูลที่ถูกแบ่งย่อยมาจากต้นทางกลับคืนสภาพเดิมตามลำดับข้อมูลที่ถูกต้อง จากนั้นจึงส่งไปยังชั้นที่ 5 ต่อไป

หน้าที่การทำงานของชั้นขนส่งข้อมูล

1. มีการเพิ่มข้อมูลลงในส่วนหัวของแพ็กเก็ต ซึ่งจะเป็นข้อมูลบ่งบอกที่อยู่อีกรูปแบบหนึ่งเรียกว่า ที่อยู่ของพอร์ต (Port Address) เนื่องจากในการขนส่งข้อมูลนั้น หมายถึงการขนส่งระหว่างเครื่องสองเครื่อง คือ ต้นทางและปลายทาง เมื่อข้อมูลไปถึงปลายทางในขณะนั้นเครื่องปลายทางอาจมีการดำเนินงานในกระบวนใดๆ เช่น มีการใช้งานแอปพลิเคชัน เป็นต้น จึงจำเป็นต้องระบุที่อยู่ของพอร์ตเพื่อให้ข้อมูลเดินทางเข้าสู่เครื่องปลายทางโดยไม่ส่งผลกระทบต่อการทำงานดังกล่าว

2. ข้อมูลในชั้นนี้จะถูกแบ่งย่อย (Segment) โดยในแต่ละส่วนย่อยจะมีการระบุลำดับของข้อมูลไว้ ซึ่งลำดับดังกล่าวจะถูกเรียงอีกครั้งโดยชั้นขนส่งข้อมูลของเครื่องปลายทาง หากมีลำดับใดขาดหายไปก็จะทราบทันทีว่าการขนส่งข้อมูลไม่สมบูรณ์

3. ควบคุมการเชื่อมต่อโดยเชื่อมต่อเส้นทางในการส่งข้อมูล 2 ลักษณะ คือ

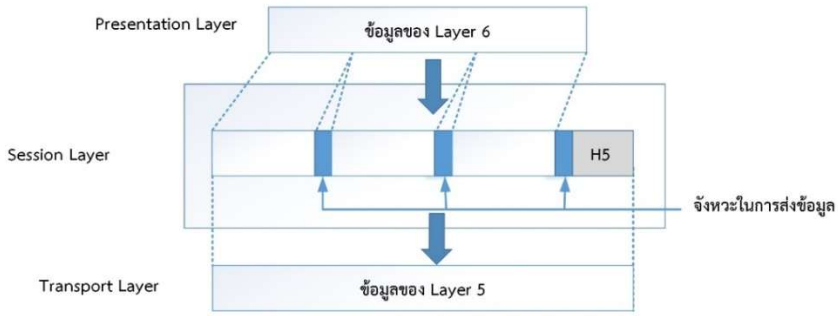
3.1 Connectionless เป็นการส่งข้อมูลไปยังปลายทางโดยไม่มีการสร้างเส้นทางเชื่อมต่อสำหรับส่งข้อมูลก่อน โดยจะไม่ทราบว่าแพ็กเก็ตจะส่งถึงปลายทางหรือไม่และมีเส้นทางการขนส่งเป็นอย่างไร

3.2 Connection-Oriented เป็นการส่งข้อมูลที่มีการสร้างเส้นทางระหว่างต้นทางและปลายทางก่อนทำการส่ง ทำให้ทราบว่าแพ็กเก็ตเดินทางอย่างไรและถึงปลายทางหรือไม่ สำหรับเส้นทางดังกล่าวนั้น เมื่อส่งข้อมูลเรียบร้อยก็จะถูกยกเลิกไป หากมีการขนส่งข้อมูลอีกครั้งก็จะสร้างเส้นทางเชื่อมต่อใหม่

4. ควบคุมความผิดพลาดและการไหลของข้อมูล คล้ายกับในชั้นเชื่อมโยงข้อมูล แต่ในชั้นนี้จะเป็นการควบคุมและตรวจสอบความผิดพลาดและการไหลของข้อมูลในจุดเชื่อมต่อระหว่างต้นทางและปลายทาง (End-to-End) ไม่ใช่แค่การเชื่อมต่อเพียงจุดเดียวเท่านั้น

ชั้นที่ 5 ชั้นควบคุมเซสชัน

ชั้นควบคุมเซสชัน (Session Layer : Layer 5) เป็นชั้นที่ควบคุมการติดต่อสื่อสารผ่านเครือข่ายระหว่างต้นทางและปลายทาง โดยมีหน้าที่ในการดูแลและควบคุมกระบวนการสื่อสารในขณะนั้น ซึ่งกระบวนการที่เกิดขึ้นในช่วงใดช่วงหนึ่งเรียกว่า เซสชัน (Session) ทำให้แต่ละเซสชันทราบว่าจะเริ่มหรือหยุดเมื่อใดและรอคอยคำสั่งในการดำเนินงานต่อไป สำหรับชั้นควบคุมเซสชันนี้อาจหมายถึงชั้นควบคุมลำดับสั่งของเครือข่าย (Network Dialog Controller) ดังภาพที่ 2.10



ภาพที่ 2.10 แสดงตัวอย่างการทำงานชั้นควบคุมเซสชั่น

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 30)

ในชั้นควบคุมเซสชันจะรับข้อมูลจากการชั้นที่ 6 มาจัดการเพิ่มเติมข้อมูลส่วนหัวและแทรกจังหวะในการส่งข้อมูลเข้าไปยังแต่ละส่วนของข้อมูลอย่างเท่าๆ กัน ก่อนที่ข้อมูลทั้งหมดจะนำไปแบ่งส่วนย่อยในชั้นที่ 4 ต่อไป ดังภาพที่ 2.10 ซึ่งจังหวะในการส่งข้อมูลที่แทรกเข้าไปนั้นจะช่วยให้อัตราการส่งข้อมูลเป็นไปอย่างสม่ำเสมอหรืออยู่ในจังหวะที่เหมาะสมกับปริมาณของข้อมูลเพื่อป้องกันการล้นของข้อมูล ในทางกลับกันเมื่อมีข้อมูลมาถึงชั้นควบคุมเซสชันที่ปลายทางก็จะทำการถอดข้อมูลส่วนหัวและจังหวะในการส่งข้อมูลออกไป จากนั้นจึงส่งไปยังชั้นที่ 6 ต่อไป

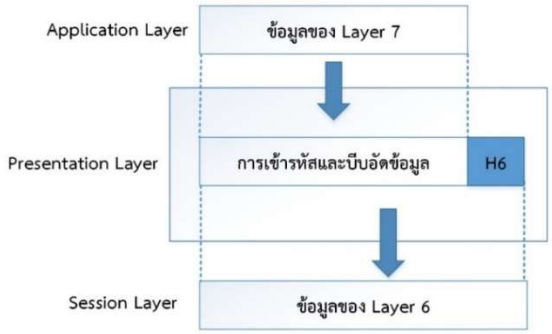
หน้าที่การทำงานของชั้นควบคุมเซสชัน

1. ควบคุมรูปแบบการติดต่อสื่อสารที่เกิดขึ้นในระหว่างกระบวนการติดต่อสื่อสารของทั้งต้นทางและปลายทางโดยกำหนดรูปแบบการส่งข้อมูลได้ 2 ลักษณะ คือ แบบผลักดัน (Half-Duplex) และแบบส่งไปพร้อมกัน (Full-Duplex)

2. ควบคุมจังหวะในการรับส่งข้อมูล (Synchronization) โดยในระหว่างกระบวนการติดต่อสื่อสารจะมีการกำหนดจุดตรวจสอบขึ้น เพื่อเป็นการตรวจการรับข้อมูลและป้องกันการสูญหายของข้อมูลบางส่วนที่อาจเกิดขึ้นในระหว่างการติดต่อสื่อสาร เช่น ข้อมูลทั้งหมดมีปริมาณ 500 หน่วยข้อมูล และทำการกำหนดจุดตรวจสอบทุกๆ 100 หน่วยข้อมูล หากเกิดข้อผิดพลาดในระหว่างการส่งข้อมูลหน่วยที่ 405 ก็จะเริ่มส่งข้อมูลใหม่ตั้งแต่หน่วยที่ 401 ในทางกลับกันหากไม่มีการกำหนดจุดตรวจสอบก็จะต้องเริ่มส่งข้อมูลใหม่ตั้งแต่หน่วยที่ 1 เป็นต้น

ชั้นที่ 6 ชั้นนำเสนอข้อมูล

ชั้นนำเสนอข้อมูล (Presentation Layer : Layer 6) เป็นชั้นที่ทำหน้าที่ในการตรวจสอบโครงสร้างของข้อมูล (Syntax) และความหมายของข้อมูล (Semantics) เพื่อให้อยู่ในรูปแบบที่เข้าใจได้อย่างถูกต้องตามความต้องการของต้นทางและปลายทาง ในชั้นนี้อาจมีการเข้ารหัสด้วยวิธีการต่างๆ เช่น รหัส ASCII เป็นต้น ซึ่งในปลายทางก็จะต้องทำการถอดรหัสที่กำหนดจากต้นทางในชั้นนี้เช่นกัน กล่าวคือ ข้อมูลในชั้นนี้จะถูกแปลงให้อยู่ในรูปแบบมาตรฐานก่อนทำการส่งและทำการแปลงกลับเป็นรูปแบบที่เครื่องปลายทางสามารถเข้าใจได้ ดังภาพที่ 2.11



ภาพที่ 2.11 แสดงตัวอย่างการส่งข้อมูลชั้นนำเสนอข้อมูล

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 31)

ในขั้นนำเสนอข้อมูลนั้นจะนำข้อมูลที่ได้รับจากชั้นที่ 7 มาเข้ารหัสและบีบอัดข้อมูล หลังจากนั้นจึงเพิ่มเติมข้อมูลส่วนหัวก่อนทำการส่งไปยังชั้นที่ 5 ต่อไป ดังภาพที่ 2.11 สำหรับชั้นนำเสนอข้อมูลที่ปลายทางนั้นจะถอดข้อมูลส่วนหัวออกก่อนแล้วจึงทำการถอดรหัสและคลายข้อมูลที่ถูกจัดการมาจากต้นทาง ทำให้ได้ข้อมูลที่สามารถนำไปใช้งานในชั้นที่ 7

หน้าที่การทำงานของชั้นนำเสนอข้อมูล

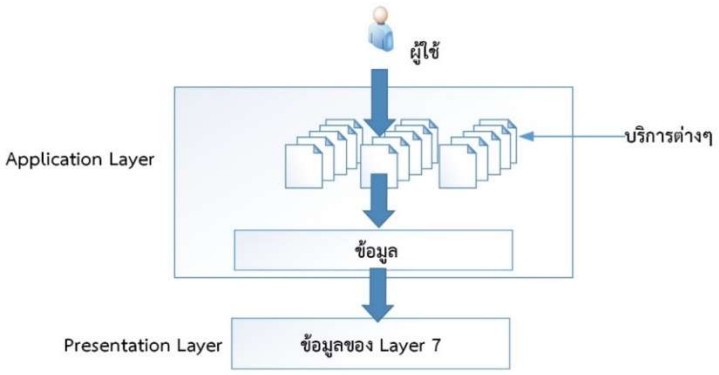
1. ทำการแปลงข้อมูลที่ใช้ในการติดต่อสื่อสารระหว่างต้นทางและปลายทาง ซึ่งเป็นข้อมูลระดับบิตให้กลับเป็นข้อมูลในรูปแบบต่างๆ เช่น ตัวอักษร ตัวเลข และสัญลักษณ์ เป็นต้น การแปลงข้อมูลจำเป็นต่อการติดต่อสื่อสารเป็นอย่างยิ่ง เนื่องจากระบบของแต่ละเครื่องมีความแตกต่างกัน อาจทำให้ข้อมูลที่ได้รับผิดพลาดได้

2. มีการเข้ารหัสและถอดรหัสข้อมูล ข้อมูลที่ต้นทางจำเป็นต้องมีการเข้ารหัสก่อนการส่งเพื่อป้องกันข้อมูลที่อาจเกิดการเปลี่ยนแปลงไประหว่างการส่ง และเมื่อถึงปลายทางก็ต้องถอดรหัสเพื่อให้ข้อมูลที่เข้ารหัสนั้นกลับเป็นข้อมูลเดิมตามต้นฉบับ

3. บีบอัดขนาดของข้อมูลเพื่อช่วยลดจำนวนบิตของข้อมูลที่จะทำการส่ง เช่น ข้อความที่มีความยาวมาก ข้อมูลเสียง ข้อมูลที่เป็นวีดีโอ เป็นต้น ซึ่งการบีบอัดจะช่วยให้การขนส่งข้อมูลทำได้ง่ายและรวดเร็วขึ้น

ชั้นที่ 7 ชั้นติดต่อแอปพลิเคชัน

ชั้นติดต่อแอปพลิเคชัน (Application Layer : Layer 7) เป็นชั้นบนสุดของแบบจำลอง OSI ซึ่งถือได้ว่าเป็นชั้นแรกที่มีการติดต่อผู้ใช้ก่อนที่จะทำการติดต่อกับเครือข่ายโดยจะมีการจัดการรูปแบบและโครงสร้างของภาษาที่แอปพลิเคชันใช้ติดต่อสื่อสารระหว่างกัน ซึ่งมีการสร้างอินเตอร์เฟซต่างๆ เพื่อรองรับบริการที่ต้องใช้งานผ่านเครือข่าย เช่น การติดต่อสื่อสารผ่านจดหมายอิเล็กทรอนิกส์ (E-mail) บริการเคลื่อนย้ายข้อมูล การจัดการฐานข้อมูล การให้บริการข้อมูลข่าวสารต่างๆ เป็นต้น สำหรับในชั้นนี้จะไม่มีการเพิ่มส่วนหัวและส่วนหางลงในข้อมูล ดังภาพที่ 2.12



ภาพที่ 2.12 แสดงตัวอย่างการส่งข้อมูลชั้นติดต่อแอปพลิเคชัน

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 32)

สำหรับชั้นติดต่อระดับแอปพลิเคชันจะเป็นการติดต่อระหว่างผู้ใช้กับแอปพลิเคชัน เมื่อผู้ใช้ทำการป้อนข้อมูลที่ต้องการส่งผ่านแอปพลิเคชันแล้ว ข้อมูลดังกล่าวจะถูกส่งออกไปยังชั้นที่ 6 เพื่อเตรียมการเข้ารหัสและบีบอัดข้อมูลต่อไป ดังภาพที่ 2.12 และในชั้นติดต่อระดับแอปพลิเคชันของปลายทาง ข้อมูลที่ผ่านการถอดรหัสและคลายข้อมูลจากชั้นที่ 6 แล้วจะถูกนำมาประมวลผลโดยแอปพลิเคชันหรือบริการต่างๆ ที่เหมือนกับต้นทาง ทำให้ข้อมูลที่ส่งมาตอบสนองต่อผู้ใช้เครื่องปลายทางหรือผู้รับ กล่าวคือ แอปพลิเคชันหรือบริการจะเป็นตัวตอบสนองและนำเสนอข้อมูลจากผู้ส่งต่อผู้รับนั่นเอง

หน้าที่การทำงานของชั้นนำเสนอข้อมูล

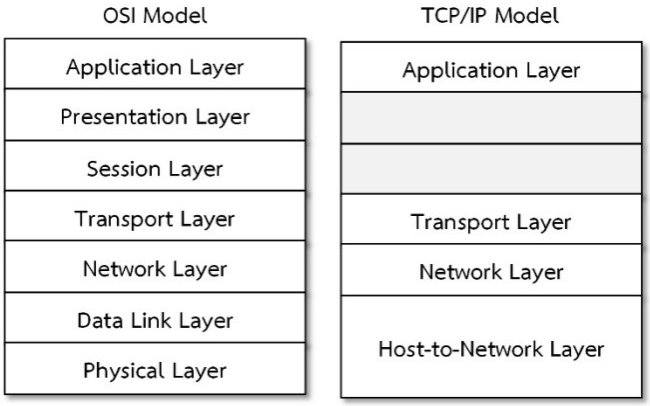
1. มีบริการติดต่อสื่อสารและจัดการเกี่ยวกับเครือข่าย การรับส่งจดหมายอิเล็กทรอนิกส์การติดต่อกับฐานข้อมูล การถ่ายโอนข้อมูลต่างๆ และการติดต่อเข้าใช้เครื่องอื่นในระยะไกล (Remote Access)

การทำงานและความสำคัญของแต่ละชั้นในแบบจำลองโอเอสไอ จะมีการเพิ่มเติมข้อมูลต่างๆ ที่จำเป็นต่อการรับส่งข้อมูล หรือติดต่อสื่อสารจากเครื่องต้นทาง ไปยังเครื่องปลายทาง ซึ่งแบบจำลองโอเอสไอนั้น เป็นต้นแบบทำให้การพัฒนาโพรโทคอลเป็นไปในทิศทางเดียวกัน และมีรูปแบบที่เป็นมาตรฐาน

2.3 แบบจำลองทีซีพี/ไอพี

แบบจำลองทีซีพี/ไอพี (Transmission Control Protocol/Internet Protocol : TCP/ IP) เป็นชุดโพรโทคอลที่ได้รับการพัฒนามาจากระบบเครือข่ายที่ชื่อว่า อาร์พาเน็ต (ARPANET) ซึ่งได้รับการสนับสนุนทุนจากกระทรวงกลาโหมสหรัฐอเมริกา โดยในช่วงแรกอาร์พาเน็ตมีวัตถุประสงค์เพื่อเชื่อมโยงการติดต่อสื่อสารระหว่างคอมพิวเตอร์ในมหาวิทยาลัยและหน่วยงานของรัฐ โดยการใช้สายเช่าโทรศัพท์ (Leased Line) เพื่อเชื่อมโยงเครือข่าย ต่อมาได้มีการนำระบบสื่อสารด้วยคลื่นวิทยุและดาวเทียมมาใช้งานในระบบ ทำให้ระเบียบแบบแผนในการติดต่อสื่อสารที่มีอยู่เดิมไม่สามารถนำมาใช้งานได้ จึงจำเป็นต้องมีการปรับเปลี่ยนข้อตกลงและสถาปัตยกรรมเครือข่าย โดยมีวัตถุประสงค์หลัก คือ เชื่อมต่อระบบที่มีความแตกต่างกันให้สามารถติดต่อสื่อสารกันได้ จนปี ค.ศ.1974 ได้เกิดโพรโทคอลที่ชื่อว่า ทีซีพี/ไอพี ขึ้นมา และได้พัฒนาการทำงานในด้านต่างๆ ของทีซีพี/ไอพีจนสำเร็จสมบูรณ์ในปี ค.ศ.1988 เรียกแบบจำลองดังกล่าวว่า แบบจำลองทีซีพี/ไอพี (TCP/IP Model) หรือแบบจำลองอ้างอิงเครือข่ายอินเทอร์เน็ต

(Internet Reference Model) สามารถเปรียบเทียบแบบจำลองโอเอสไอกับแบบจำลองทีซีพี/ไอพี ดังภาพที่ 2.13 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 34)



ภาพที่ 2.13 แสดงการเปรียบเทียบแบบจำลองโอเอสไอกับแบบจำลองทีซีพี/ไอพี
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 34)

แบบจำลองทีซีพี/ไอพีจะไม่กำหนดชั้นสื่อสารที่อยู่ในระดับเดียวกับชั้นนำเสนอข้อมูล (Presentation Layer) และชั้นควบคุมเซสชัน (Session Layer) ของแบบจำลองโอเอสไอ เนื่องจากแบบจำลองโอเอสไอมีการใช้งานชั้นสื่อสารทั้งสองน้อยมากแต่แบบจำลองทีซีพี/ไอพีจะกำหนดชั้นสื่อสารไว้ 4 ชั้น ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 34-35)

1. ชั้นควบคุมการติดต่อระดับเครือข่าย (Host-to-Network Layer) เป็นชั้นที่ไม่ได้กำหนดรายละเอียดอย่างเป็นทางการไว้ หน้าที่หลักของชั้นสื่อสารนี้ คือ รับข้อมูลจากชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ต (Internet Layer) แล้วส่งไปยังโหนดปลายทางตามเส้นทางที่กำหนดไว้ เมื่อผู้รับได้รับข้อมูลแล้ว ชั้นควบคุมการติดต่อระดับเครือข่ายจะส่งข้อมูลให้กับชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ตต่อไป

2. ชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ต (Internet Layer) ในชั้นนี้จะใช้วิธีการส่งข้อมูลที่เรียกว่า ระบบเครือข่ายแบบสลับช่องสื่อสารระดับแพ็กเก็ต (Packet-Switching Network) ซึ่งเป็นการติดต่อสื่อสารแบบไม่ต่อเนื่อง และไม่มีการประกันความถูกต้องของข้อมูล โดยเครื่องต้นทางจะส่งข้อมูลขนาดเล็กที่เรียกว่า แพ็กเก็ต ไปยังเครือข่ายใดๆ ในระบบอย่างอิสระจนกว่าข้อมูลจะถึงปลายทาง หากมีการส่งกลุ่มของแพ็คเก็ตต่อเนื่องที่เป็นชุดเดียวกัน การเดินทางของแต่ละแพ็คเก็ตก็ยังเป็นการทำงานอย่างอิสระต่อกัน ดังนั้น แอปพลิเคชันของฝั่งผู้รับ

จำเป็นต้องตรวจสอบและจัดเรียงแพ็คเก็ตให้ถูกต้องก่อนนำข้อมูลไปใช้งาน โดยชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ตจะกำหนดกฎเกณฑ์การติดต่อสื่อสารด้วยโพรโทคอลทีซีพี/ไอพี

3. ชั้นขนส่งข้อมูล (Transport Layer) เป็นชั้นที่ทำหน้าที่ควบคุมการขนส่งข้อมูลจากต้นทางไปยังปลายทาง และตรวจสอบความถูกต้องของแพ็กเก็ตข้อมูลเหมือนกับชั้นขนส่งข้อมูลของ แบบจำลองโอเอสไอโดยมีโพรโทคอลที่สามารถใช้งานได้ 2 ชนิด คือ ทีซีพี ซึ่งใช้วิธีส่งข้อมูลแบบ Connection-Oriented ที่มีการควบคุมความถูกต้องและการไหลของข้อมูลให้มีความเหมาะสม ส่วนโพรโทคอลอีกชนิดคือยูดีพี ซึ่งใช้วิธีส่งข้อมูลแบบ Connectionless ที่ไม่มีการตรวจสอบความถูกต้องของข้อมูล

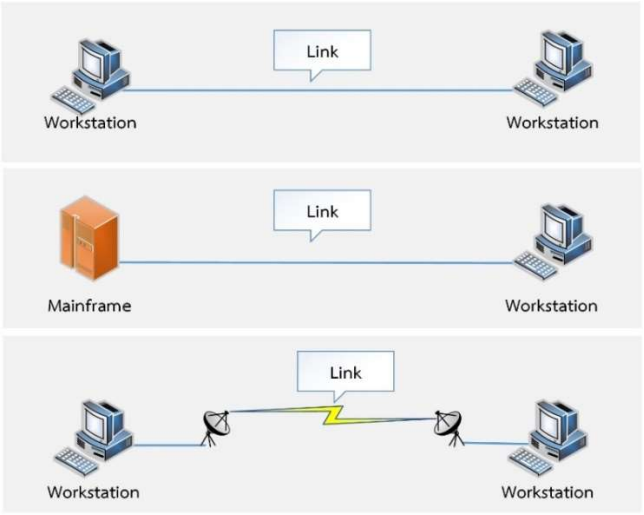
4. ชั้นติดต่อระดับแอปพลิเคชัน (Application Layer) เป็นชั้นที่เกี่ยวข้องกับการติดต่อ ระหว่างผู้ใช้กับแอพพลิเคชัน และคอยควบคุมข้อมูลที่จะส่งผ่านไปยังชั้นอื่นๆ นอกจากนี้ยังรวบรวมการทำงานที่ไม่จำเป็นของชั้นสื่อสารที่ไม่ได้ถูกใช้งาน คือชั้นนำเสนอข้อมูล (Presentation Layer) และชั้นควบคุมเซสชัน (Session Layer) ของแบบจำลองโอเอสไอไว้ด้วย

2.4 การเชื่อมต่อเครือข่าย

การเชื่อมต่อเครือข่าย (Line Configuration) หมายถึง ความสัมพันธ์ของอุปกรณ์สื่อสารที่ส่งผ่านลิงก์ซึ่งในเชิงกายภาพแล้ว ลิงก์ก็คือเส้นทางสื่อสารเพื่อโอนข้อมูลจากอุปกรณ์หนึ่งไปยังอุปกรณ์หนึ่ง โดยสามารถเชื่อมต่อได้ 2 รูปแบบด้วยกัน ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 102-103)

2.4.1 การเชื่อมต่อแบบจุดต่อจุด

การเชื่อมต่อแบบจุดต่อจุด (Point-to-Point) เป็นการเชื่อมต่อระหว่างอุปกรณ์สองตัว ช่องทางการสื่อสารจะถูกจับจองเพื่อสื่อสารระหว่างอุปกรณ์ทั้งสองเท่านั้น และโดยปกติการเชื่อมต่อแบบจุดต่อจุดมักใช้สายเคเบิลในการเชื่อมโยงระหว่างต้นทางกับปลายทาง และยังรวมถึงการเชื่อมโยงแบบไร้สาย เช่น คลื่นไมโครเวฟดังภาพที่ 2.14

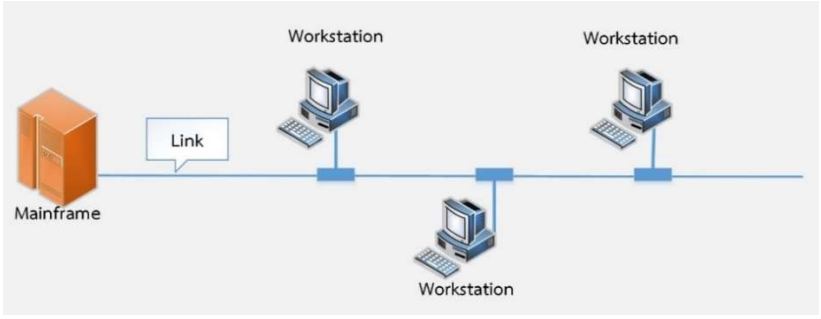


รูปที่ 2.14 การเชื่อมต่อแบบจุดต่อจุด (Point-to-Point)

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 102)

2.4.2 การเชื่อมต่อแบบหลายจุด

การเชื่อมต่อแบบหลายจุด (Multi-Point/Multi-Drop) เป็นการเชื่อมต่อที่แตกต่างจากแบบแรก โดยจะมีอุปกรณ์มากกว่าหนึ่งชิ้นเชื่อมต่อเข้ากับลิงก์เดียวกัน เพื่อใช้เป็นเส้นทางในการสื่อสารร่วมกัน แม้ว่าวิธีนี้ช่วยประหยัดสายสื่อสารได้เป็นอย่างดี แต่ก็มีข้อเสียคือข้อมูลที่สื่อสารภายในช่องในสายส่งอาจชนกันได้ ดังนั้น จึงต้องมีกลไกควบคุมการรับข้อมูลภายในสายส่ง เพื่อไม่ให้เกิดการชนกัน อย่างไรก็ตาม เครือข่ายที่ใช้งานในยุคปัจจุบันส่วนใหญ่จะใช้วิธีการเชื่อมต่อแบบหลายจุด ดังภาพที่ 2.15



ภาพที่ 2.15 การเชื่อมต่อแบบหลายจุด (Multi-Point)

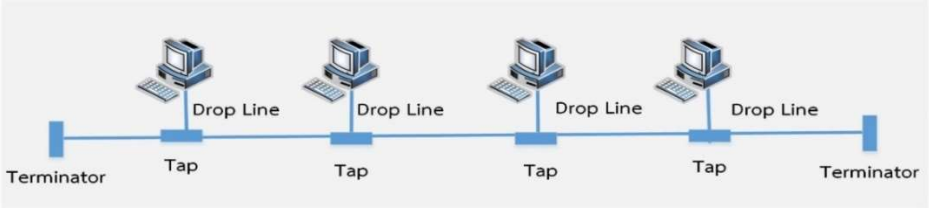
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 103)

2.5 รูปแบบการเชื่อมต่อเครือข่าย

การเชื่อมต่อเครือข่ายหรือโทโพโลยี (Topologies) เป็นการเชื่อมต่อเครือข่ายระหว่างโหนดในมุมมองเชิงกายภาพ วิธีเชื่อมต่อแบ่งออกเป็น 4 รูปแบบ ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2565, หน้า 103-110)

2.5.1 โทโพโลยีแบบบัส (Bus Topology)

โทโพโลยีแบบบัส (Bus Topology) จะมีสายเคเบิลเส้นหนึ่งทำหน้าที่เป็นสายแกนหลักที่ทุกๆ โหนดบนเครือข่ายจะต้องเชื่อมต่อเข้ากับสายเส้นนี้ จึงมีลักษณะคล้ายกับราวแขวนเสื้อผ้า ดังภาพที่ 2.16



ภาพที่ 2.16 โทโพโลยีแบบบัส (Bus topology)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 104)

โทโพโลยีแบบบัส แต่ละโหนดจะเชื่อมต่อเข้ากับการสายเคเบิลเส้นหนึ่ง ซึ่งสายเส้นนี้จะทำหน้าที่เป็นสายแกนหลัก โดยมี Drop Lines เชื่อมต่อเข้ากับสายเคเบิล และ Tap คือคอนเน็กเตอร์ที่นำมาใช้เป็นอุปกรณ์เชื่อมต่อ ส่วนปลายสายทั้งสองฝั่งของสายเคเบิลจะมีอุปกรณ์ปิดท้ายที่เรียกว่า **เทอร์มิเนเตอร์** (Terminator) เพื่อดูดซับสัญญาณและป้องกันการสะท้อนกลับของสัญญาณเมื่อวิ่งมายังสุดปลายสาย

ข้อดีและข้อเสียของโทโพโลยีแบบบัส

ข้อดี

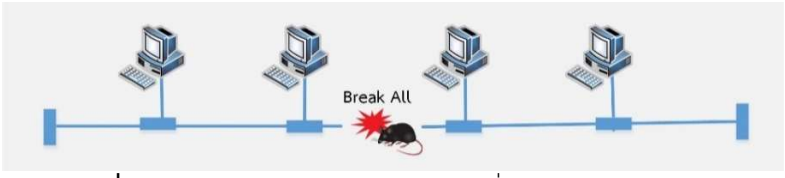
1. รูปแบบโครงสร้างไม่ซับซ้อน ติดตั้งง่าย
2. ง่ายต่อการเพิ่มจำนวนโหนด เนื่องจากสามารถเชื่อมต่อเข้ากับสายแกนหลักได้ทันที
3. ประหยัดสายสื่อสาร เพราะใช้สายแกนหลักเพียงเส้นเดียว

ข้อเสีย

1. หากสายแกนหลักเกิดชำรุดหรือขาด เครือข่ายจะหยุดชะงักทันที

2. กรณีเกิดข้อผิดพลาดบนเครือข่าย จะค้นหาจุดผิดพลาดยาก เนื่องจากทุกอุปกรณ์ต่างก็เชื่อมต่อเข้ากับสายแกนหลักทั้งหมด

3. แต่ละโหนดที่เชื่อมต่อบนสายแกนหลัก จะต้องมีระยะห่างตามข้อกำหนด

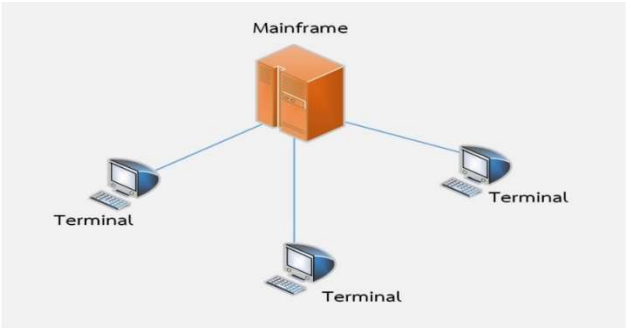


ภาพที่ 2.17 สายเคเบิลขาด ณ จุดใดจุดหนึ่งของโทโพโลยีแบบบัส

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 104)

2.5.2 โทโพโลยีแบบดาว

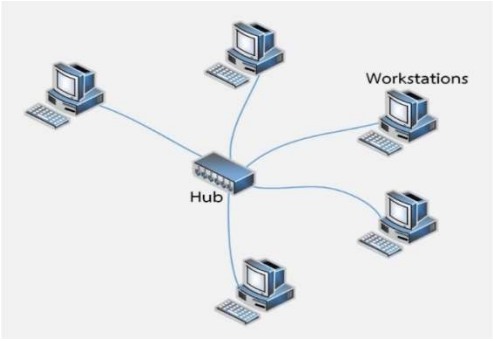
โทโพโลยีแบบดาว (Star Topology) มีจุดเริ่มต้นมาจากการเชื่อมต่อเทอร์มินัลเข้ากับเครื่องเมนเฟรมที่นิยมใช้กันในอดีต โดยเมนเฟรมคอมพิวเตอร์จะทำหน้าที่เป็นศูนย์กลางในการเชื่อมต่อ และเทอร์มินัลทุกเครื่องจะถูกเชื่อมต่อเข้ากับศูนย์กลางแห่งนี้ ดังภาพที่ 2.18



ภาพที่ 2.18 โทโพโลยีแบบดาวที่มีเมนเฟรมคอมพิวเตอร์เป็นศูนย์กลาง

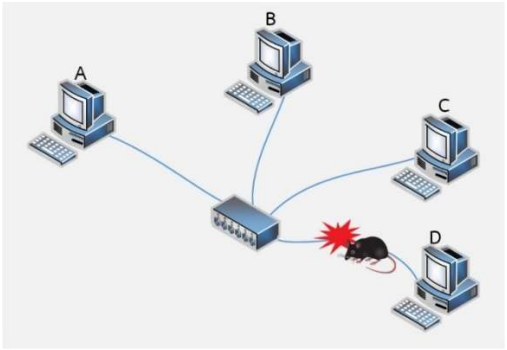
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 105)

การเชื่อมต่อตามโทโพโลยีแบบดาวในยุคปัจจุบัน อุปกรณ์ที่นิยมนำมาใช้เป็นศูนย์กลางควบคุมสายสื่อสารทั้งหมดก็ คือ **ฮับ** (Hub) กล่าวคือ ทุกๆ โหนดบนเครือข่ายจะต้องเชื่อมโยงสายสื่อสารกับอุปกรณ์ฮับ โดยฮับจะทำหน้าที่รับข้อมูลจากผู้ส่ง เพื่อส่งไปยังโหนดปลายทาง ดังภาพที่ 2.19

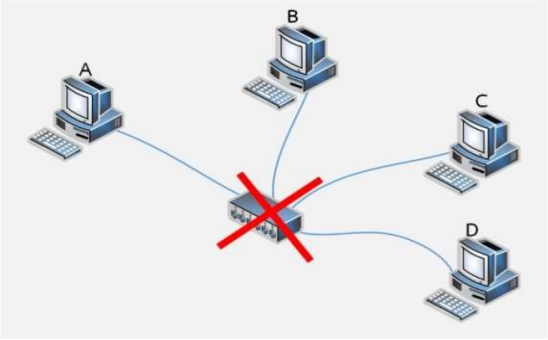


ภาพที่ 2.19 การใช้อุปกรณ์ฮับเป็นศูนย์กลางการรับส่งข้อมูลโทโพโลยีแบบดาว
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 105)

แม้ว่ารูปแบบทางกายภาพของการเชื่อมต่อแบบดาว จะดูเหมือนกับการเชื่อมต่อแบบจุดต่อจุดก็ตาม แต่การเชื่อมต่อดังกล่าวเพียงต้องการให้ระบบมีความคงทนยิ่งขึ้น เมื่อเทียบกับการเชื่อมต่อแบบบัส ทั้งนี้ การรับส่งข้อมูลภายในฮับยังคงกระจายไปทั่วทุกๆ พอร์ต เช่นเดียวกับระบบบัส อันเนื่องมาจากทุกพอร์ตบนฮับได้เชื่อมต่อเข้ากับบัสเส้นเดียวกันนั่นเอง ดังนั้น การนำอุปกรณ์ฮับมาใช้เป็นศูนย์กลางการรับส่งข้อมูล ก็เพื่อให้เครือข่ายมีความคงทนยิ่งขึ้น กล่าวคือ หากสายสื่อสารบนโหนดใดโหนดหนึ่งเกิดชำรุดหรือขาด จะส่งผลเฉพาะเพียงโหนดนั้นๆ ไม่ได้ส่งผลกระทบต่อระบบโดยรวม ซึ่งแตกต่างจากโทโพโลยีแบบบัส ที่จะส่งผลต่อระบบโดยรวมทันที พิจารณาจากภาพที่ 2.20 พบว่า เมื่อสายเคเบิลของโหนด D เกิดความเสียหายขึ้นมาก็จะส่งผลต่อโหนด D เท่านั้น โหนดอื่นๆ ที่เหลือยังคงใช้งานได้ตามปกติ แต่ถ้าอุปกรณ์ฮับเสียเครือข่ายบนเซกเมนต์นั้นก็จะใช้การไม่ได้ทั้งหมดเช่นกัน ดังภาพที่ 2.21



ภาพที่ 2.20 สายเคเบิลที่เชื่อมต่อเข้ากับฮับถูกทำลายของโทโพโลยีแบบดาว
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 106)



ภาพที่ 2.21 อุปกรณ์ฮับเสียหายส่งผลกระทบต่อเครือข่ายของโทโพโลยีแบบดาว
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 106)

ข้อดีและข้อเสียของโทโพโลยีแบบดาว

ข้อดี

1. มีความคงทนสูง กล่าวคือ หากสายเคเบิลบางโหนดเกิดชำรุดหรือขาด จะส่งผลต่อโหนดนั้นๆ เท่านั้น โหนดอื่นๆ ยังคงใช้งานได้ตามปกติ

2. เนื่องจากมีจุดศูนย์กลางควบคุมอยู่ที่ฮับ การจัดการจึงง่ายและสะดวก

ข้อเสีย

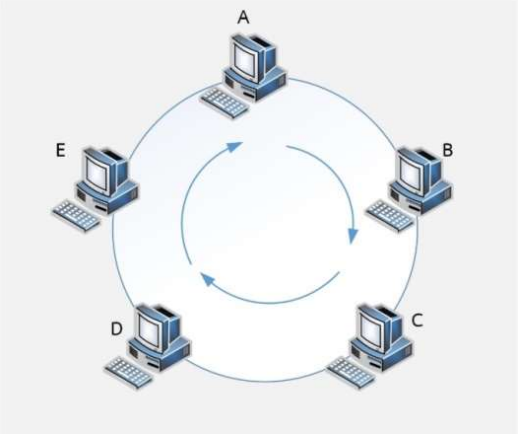
1. ใช้สายเคเบิลมาก เพราะต้องใช้จำนวนสายเท่ากับจำนวนเครื่องที่เชื่อมต่อ

2. หากต้องการเพิ่มโหนด ฮับจะต้องมีพอร์ดว่างให้เชื่อมต่อ

3. เนื่องจากมีจุดศูนย์กลางอยู่ที่ฮับ หากอุปกรณ์ฮับเสีย เครือข่ายที่เชื่อมต่อเข้ากับเซกเมนต์นั้นๆ จะใช้งานการไม่ได้

2.5.3 โทโพโลยีแบบวงแหวน

การเชื่อมต่อเครือข่ายแบบวงแหวน (Ring Topology) โดยทุกๆ โหนดจะมีการเชื่อมต่อไปยังโหนดต่อไป จนกระทั่งโหนดแรกกับโหนดสุดท้ายเชื่อมโยงกัน จึงเกิดเป็นวงกลมหรือวงแหวนขึ้นมา ดังภาพที่ 2.22



ภาพที่ 2.22 โทโพโลยีแบบวงแหวน (Ring Topology)

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 107)

เมื่อพิจารณาจากภาพที่ 2.22 แล้ว จะพบว่าแต่ละโหนดบนเครือข่ายจะมีการเชื่อมต่อกันแบบจุดต่อจุด การนำส่งสัญญาณจะส่งทอดจากโหนดหนึ่งไปยังอีกโหนดหนึ่งไปเรื่อยๆ ในทิศทางเดียวกัน จึงทำให้แต่ละโหนดในวงแหวนทำหน้าที่คล้ายกับเครื่องทวนสัญญาณไปในตัว

ข้อดีและข้อเสียของโทโพโลยีแบบวงแหวน

ข้อดี

1. แต่ละโหนดในวงแหวนมีโอกาสส่งข้อมูลได้เท่าเทียมกัน
2. ประหยัดสายสัญญาณ
3. ง่ายต่อการติดตั้ง รวมถึงการเพิ่ม/ลด จำนวนโหนด

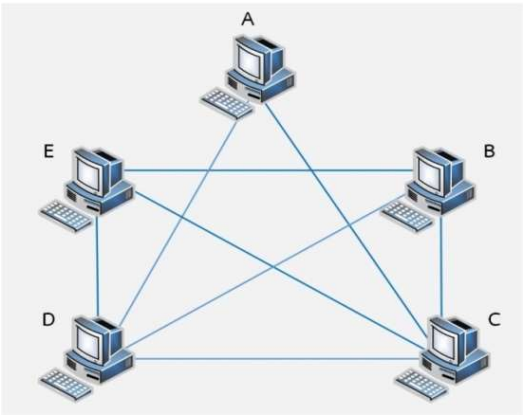
ข้อเสีย

1. หากวงแหวนชำรุดหรือขาด จะส่งผลต่อระบบทั้งหมด
2. ยากต่อการตรวจสอบ กรณีมีโหนดใดโหนดหนึ่งเกิดข้อขัดข้อง เนื่องจากต้องตรวจสอบทีละจุดจนกว่าจะพบจุดที่มีปัญหา

2.5.4 โทโพโลยีแบบเมช

โทโพโลยีแบบเมช (Mesh Topology) จัดเป็นการเชื่อมต่อเครือข่ายแบบจุดต่อจุดอย่างแท้จริง เนื่องจากแต่ละโหนดจะมีลิงก์สื่อสารเป็นของตนเอง สำหรับการส่งผ่านข้อมูลถึงกัน นอกจากจะใช้ลิงก์เชื่อมโยงสื่อสารกันโดยตรงแล้ว ยังสามารถใช้ลิงก์หรือเส้นทางอื่นๆ เพื่อ

เชื่อมโยงไปยังโหนดปลายทางได้อีกด้วย เครือข่ายเมชจึงเป็นโทโพโลยีที่มีความเสถียรสูง กล่าวคือ แม้ว่าจะมีบางลิงก์เสียหายหรือลิงก์นั้นมีจราจรคับคั่ง ก็ยังสามารถสื่อสารได้ด้วยการเลี่ยงไปใช้เส้นทางอื่นๆ แทน ดังภาพที่ 2.23



ภาพที่ 2.23 โทโพโลยีแบบเมช (Mesh Topology)

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 108)

ข้อดีและข้อเสียของโทโพโลยีแบบเมช

ข้อดี

1. เนื่องจากเป็นการเชื่อมต่อกันโดยตรงระหว่างโหนด ดังนั้น แบนด์วิดธ์บนสายสื่อสารจึงถูกนำมาใช้ได้อย่างเต็มที่ โดยไม่มีโหนดใดเข้ามาแชร์ใช้งาน

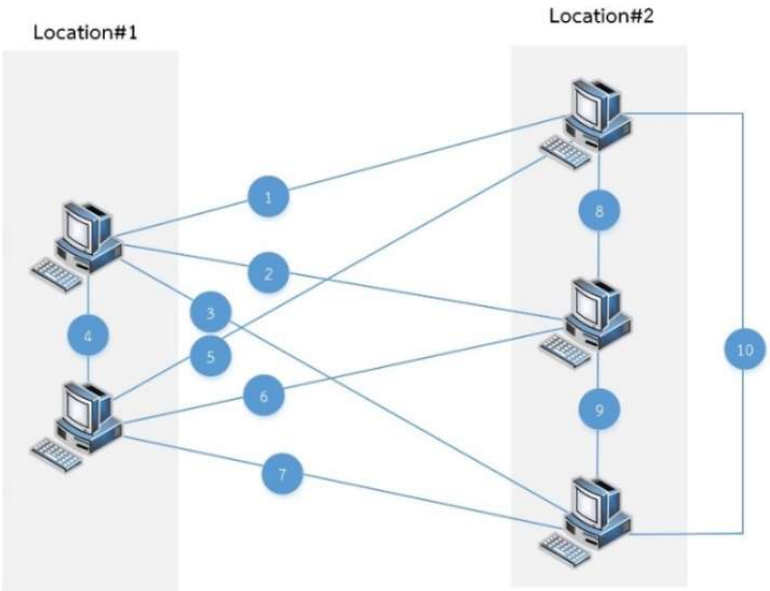
2. มีความปลอดภัย และความเป็นส่วนตัวในข้อมูลที่สื่อสารกันระหว่างโหนด

3. ระบบมีความทนทานต่อความผิดพลาด (Fault-Tolerant) สูง เนื่องจากหากมีลิงก์ใดชำรุดหรือเสียหาย ก็สามารถเลี่ยงไปใช้เส้นทางอื่นแทนได้

ข้อเสีย

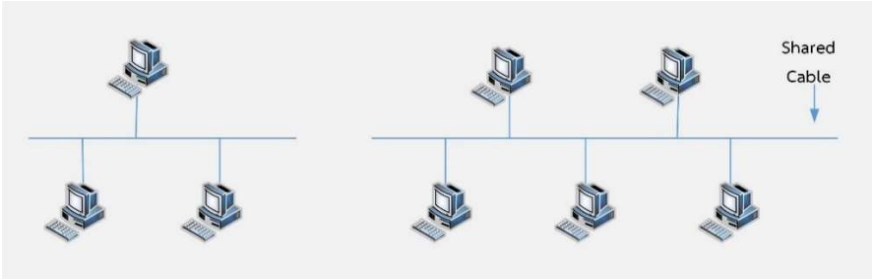
1. เป็นรูปแบบการเชื่อมต่อเครือข่ายที่สิ้นเปลืองสายสื่อสารมากที่สุด เนื่องจากโทโพโลยีแบบเมช ใช้สายสื่อสารสิ้นเปลือง ประกอบกับหากมีการเชื่อมต่อโหนดเพิ่มขึ้น จะส่งผลต่อจำนวนสายสื่อสารที่ต้องใช้ในระบบ ดังนั้น จึงมีสูตรเพื่อคำนวณหาจำนวนจุดเชื่อมต่อ คือ นำจำนวนเครื่องทั้งหมดยกกำลังสอง แล้วลบด้วยจำนวนเครื่องทั้งหมด จากนั้นนำไปหารด้วย 2 ก็จะได้จำนวนสายทั้งหมดที่ใช้ในการเชื่อมต่อ

ตัวอย่าง มีคอมพิวเตอร์จำนวน 5 เครื่อง โดย 2 เครื่องอยู่ที่ Location#1 และอีก 3 เครื่องตั้งอยู่ Location#2 เมื่อแทนค่าลงในสูตรก็จะได้ 10 นั่นหมายความว่า จะต้องใช้สายสื่อสาร จำนวน 10 เส้น เพื่อเชื่อมต่อจุดต่อจุดเข้ากับอุปกรณ์ทั้ง 5 ดังภาพที่ 2.24



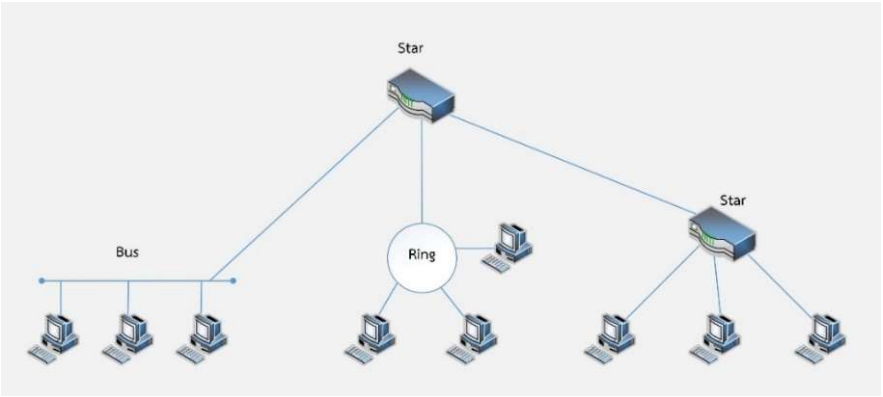
ภาพที่ 2.24 ตัวอย่างการต่อสายสื่อสารเพื่อเชื่อมต่อแบบจุดต่อจุดกับอุปกรณ์
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 109)

อย่างก็ตาม หากต้องการเพิ่มคอมพิวเตอร์อีกโหนดหนึ่งเข้าไปยัง Location#1 เมื่อแทนค่าลงในสูตรแล้ว จะต้องเพิ่มสายสื่อสายจากเดิม 10 เส้น มาเป็น 15 เส้น (มิใช่เพิ่มสายเพียงหนึ่งเส้นตามจำนวนโหนดที่เพิ่ม) แต่ถ้าเป็นการเชื่อมต่อเครือข่ายด้วยโทโพโลยีแบบบัส จะสามารถเพิ่มโหลดด้วยการเชื่อมต่อเข้ากับสายแกนหลักได้ทันที ดังภาพที่ 2.25 และจากเครือข่ายตามรูปแบบการเชื่อมต่อที่แตกต่างกันนี้เอง หากนำมาเชื่อมต่อเข้าด้วยกันก็จะเรียกว่าไฮบริดโทโพโลยี (Hibrid Topology) ดังภาพที่ 2.26



ภาพที่ 2.25 การเพิ่มโหนดบนโทโพโลยีแบบบัส

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 110)



ภาพที่ 2.26 ไฮบริดโทโพโลยี

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 110)

2.6 สรุป

การสื่อสารข้อมูลและระบบเครือข่ายเข้ามามีบทบาทในชีวิตประจำวันของมนุษย์มากขึ้น และถูกนำไปใช้ในการแลกเปลี่ยนข้อมูลข่าวสารในรูปแบบต่างๆ โดยเฉพาะการนำไปใช้ในด้านธุรกิจเพื่อรองรับการเติบโตและการขยายตัวขององค์กรต่างๆ ที่เป็นไปอย่างรวดเร็ว ดังนั้น การดำเนินธุรกิจจึงจำเป็นต้องนำเทคโนโลยีใหม่ๆ มาประยุกต์ใช้ภายในองค์กร เพื่อเพิ่มประสิทธิภาพในการติดต่อ สื่อสารหรือบริการต่างๆ ประโยชน์ที่ได้รับจากการนำเทคโนโลยีต่างๆ มาใช้งาน คือ ลดเวลาการทำงาน ประหยัดค่าใช้จ่ายในการส่งข้อมูลข่าวสาร สามารถรับข้อมูลและสารสนเทศจากแหล่งกำเนิดข้อมูลโดยตรง ช่วยปรับปรุงการบริหารงานขององค์กรทำให้การ

ส่งและกระจายข้อมูลทำได้อย่างรวดเร็วและสามารถขยายการดำเนินงานขององค์กรได้อย่างมีประสิทธิภาพ

สถาปัตยกรรมเครือข่ายเป็นแบบจำลองในการติดต่อสื่อสารระหว่างส่วนประกอบต่างๆ ของเครือข่าย โดยแบ่งหน้าที่หรือบริการต่างๆ ของระบบเครือข่ายออกเป็นหลายระดับชั้น (Layer) หรือเรียกว่าชั้นสื่อสาร แต่ละชั้นสื่อสารจะกำหนดบริการของฮาร์ดแวร์ ซอฟต์แวร์ หรือทั้งสองอย่างไว้ในปัจจุบันมาตรฐานของสถาปัตยกรรมเครือข่ายที่ได้รับการยอมรับในระดับสากล คือแบบจำลองโอเอสไอ (OSI Model) และแบบจำลองทีซีพี/ไอพี (TCP/IP Model) ซึ่งใช้ในระบบอินเทอร์เน็ต

การเชื่อมต่อเครือข่าย คือ ความสัมพันธ์ของอุปกรณ์สื่อสารที่ส่งผ่านลิงก์ ซึ่งในเชิงกายภาพแล้ว ลิงก์ คือ เส้นทางสื่อสารเพื่อโอนข้อมูลจากอุปกรณ์หนึ่งไปยังอุปกรณ์หนึ่ง โดยสามารถเชื่อมต่อ 2 รูปแบบ ได้แก่ การเชื่อมต่อแบบจุดต่อจุด (Point-to-Point) และการเชื่อมต่อแบบหลายจุด (Multi-Point/Multi-Drop)

การเชื่อมต่อเครือข่ายหรือโทโพโลยี เป็นการเชื่อมต่อเครือข่ายระหว่างโหนดในมุมมองเชิงกายภาพ แบ่งออกเป็น 4 รูปแบบด้วยกัน คือ โทโพโลยีแบบบัส โทโพโลยีแบบดาว โทโพโลยีแบบวงแหวน และโทโพโลยีแบบเมช

บทที่ 3
ข้อมูลและสัญญาณ

ในโลกปัจจุบันมนุษย์จำเป็นต้องสื่อสารกับมนุษย์ หุ่นยนต์ เครื่องจักร การสื่อสารดังกล่าวหมายถึงการสื่อใจความและความหมายที่ฝ่ายหนึ่งอยากจะบอกกับอีกฝ่ายหนึ่ง ใจความและความหมายดังกล่าวไม่มีรูปแบบที่จับต้องได้ จำเป็นต้องแปลงให้อยู่ในรูปของข้อมูล เช่น ข้อมูลในรูปของเลขฐานสอง เป็นต้น ข้อมูลดังกล่าวนี้เป็นตัวแทนที่มีรูปแบบต่างๆ กันเพื่อแสดงสารสนเทศ แต่ในการส่งข้อมูลดังกล่าว จำเป็นต้องแปลงข้อมูลให้อยู่ในรูปของสัญญาณและปรับให้สามารถส่งผ่านช่องสื่อสารได้ เนื่องจากข้อมูลเป็นเสมือนสัญลักษณ์ที่แสดงสารสนเทศและไม่มีพลังงานเพียงพอในการส่งไปในที่ไกลได้ มนุษย์จำเป็นต้องแปลงสารสนเทศที่ต้องการสื่อให้เป็นข้อมูลและสัญญาณเพื่อส่งผ่านสื่อไปยังมนุษย์ หุ่นยนต์ และเครื่องจักร ในทำนองเดียวกัน เครื่องจักรและหุ่นยนต์ที่ต้องการสื่อสารกับเครื่องจักรหรือหุ่นยนต์หรือมนุษย์ ก็ต้องแปลงสารสนเทศที่ต้องการสื่อให้เป็นสัญญาณเช่นเดียวกัน แล้วทำการส่งไปยังมนุษย์ หุ่นยนต์ หรือเครื่องจักรตามที่ต้องการ

ในกระบวนการสื่อสารระหว่างนั้นจำเป็นต้องเปลี่ยนสารสนเทศให้อยู่ในรูปของข้อมูลและสัญญาณ หากการสื่อสารดังกล่าวอยู่ในที่ไกลจำเป็นต้องมีเครื่องมือสื่อสารช่วย เครื่องมือสื่อสารดังกล่าวต้องอาศัยหลักการและทฤษฎีการประมวลผลสัญญาณและหลักการสื่อสารทางไกล รวมทั้งหลักการอื่นๆ ถึงแม้ผู้ส่งสารจะไม่ได้เป็นผู้ออกแบบและสร้างระบบดังกล่าวแต่ก็คงหลีกเลี่ยงการรู้จักสัญญาณเพื่อเลือกใช้เครื่องมือที่เหมาะสมไม่ได้ นอกจากนี้ มนุษย์ยังมีความจำเป็นที่จะต้องจัดเก็บสารสนเทศจำนวนมาก เช่น เสียง ภาพ ตัวอักษร เป็นต้น ซึ่งมักถูกจัดเก็บในรูปของข้อมูลบ้างสัญญาณบ้าง และมีหลายกรณีที่ต้องมีการประมวลผลสัญญาณและข้อมูลเพื่อทำการบีบอัดให้มีขนาดเล็กให้เหมาะสมกับพื้นที่จัดเก็บต่อไป (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 2-7)

3.1 ความหมายของข้อมูลและสัญญาณ

สารสนเทศที่จัดเก็บอยู่ในระบบคอมพิวเตอร์ และถูกนำมาถ่ายโอนผ่านเครือข่ายคอมพิวเตอร์ สามารถแบ่งออกเป็น 2 ประเภทด้วยกัน คือ ข้อมูลและสัญญาณ โดยมีความหมายดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 159)

ข้อมูล (Data) คือ เป็นสิ่งที่มีอยู่จริง สิ่งที่มีความหมายในตัว ข้อมูลอาจอยู่ในรูปตัวเลข ตัวอักษร ภาพนิ่ง รวมถึงภาพเคลื่อนไหว ในขณะเดียวกันข้อมูลที่บรรจุอยู่ในระบบคอมพิวเตอร์ อาจเป็นชื่อไฟล์คอมพิวเตอร์กับแอดเดรสที่ใช้จัดเก็บข้อมูลเหล่านั้นบนฮาร์ดดิสก์ ภาพยนตร์ที่บันทึกอยู่บนแผ่นซีดี เพลงที่บันทึกอยู่บนแผ่นซีดี ภาพถ่ายจากกล้องดิจิทัลที่บันทึกอยู่ในการ์ดหน่วยความจำ เป็นต้น

สัญญาณ (Signal) คือ ปริมาณใดๆ ที่สามารถเปลี่ยนแปลงและสัมพันธ์ไปกับเวลา สัญญาณที่ใช้ในการสื่อสาร คือ กระแสไฟฟ้าและคลื่นแม่เหล็กไฟฟ้า ตัวอย่างสัญญาณ ได้แก่ การสนทนาผ่านระบบโทรศัพท์ การสัมภาษณ์รายการสดจากต่างประเทศผ่านระบบสื่อสารดาวเทียม การใช้คอมพิวเตอร์ส่งงานไปพิมพ์ที่เครื่องพิมพ์ผ่านสายเคเบิลที่เชื่อมต่อระหว่างกัน การดาวน์โหลดข้อมูลจากอินเทอร์เน็ตผ่านสายโทรศัพท์แล้วนำมาบันทึกไว้ในเครื่องของเรา เป็นต้น

ในการส่งผ่านข้อมูล ไม่ว่าจะผ่านสายสื่อสารหรือส่งผ่านอากาศก็ตาม ข้อมูลที่ส่งไปจะต้องถูกแปลงเป็นสัญญาณก่อน ซึ่งตามปกติ ฝั่งส่งจะมีอุปกรณ์ฮาร์ดแวร์ไว้คอยทำหน้าที่แปลงข้อมูลมาเป็นสัญญาณเพื่อพร้อมส่งผ่านไปยังเครือข่าย ในขณะที่ปลายทางหรือฝั่งรับก็จะแปลงสัญญาณกลับมาเป็นข้อมูลเพื่อนำไปใช้งานต่อไป

3.2 แอนะล็อกและดิจิทัล

แอนะล็อกและดิจิทัล (Analog and Digital) แม้ว่าข้อมูลและสัญญาณจะมีความแตกต่างกันบ้างเล็กน้อย แต่ทั้งข้อมูลและสัญญาณสามารถทำได้เหมือนกันคือ สามารถแสดงให้อยู่ในรูปของแอนะล็อกและดิจิทัลได้ ดังนี้ (นรรัตน์ วัฒนมงคล, 2561, หน้า 47-49)

3.2.1 ข้อมูลแอนะล็อกและดิจิทัล

ข้อมูลสามารถอยู่ในรูปของแอนะล็อกและดิจิทัล โดยข้อมูลแอนะล็อกจะกล่าวถึงข้อมูลข่าวสารที่มีความต่อเนื่อง ส่วนข้อมูลดิจิทัลจะกล่าวถึงข้อมูลข่าวสารที่มีความไม่ต่อเนื่อง เช่น นาฬิกาแบบแอนะล็อกจะมีเข็มในหลักชั่วโมง นาที และวินาทีที่ใช้บอกเวลา ซึ่งการเคลื่อนที่ของเข็มนาฬิกาแต่ละอันมีความต่อเนื่อง ในทางตรงกันข้ามนาฬิกาแบบดิจิทัล การบอกเวลาในหลักชั่วโมงและนาที จะมีการเปลี่ยนแปลงอย่างทันทีทันใด เช่น จากเวลา 10.04 เปลี่ยนเป็น 10.05

ข้อมูลแอนะล็อก (Analog Data) เป็นข้อมูลรูปแบบหนึ่งที่มีลำดับต่อเนื่องกัน (Continuous Form) เช่น เสียงของมนุษย์ เสียงดนตรี เสียงเครื่องจักรที่กำลังทำงาน หรือเสียง

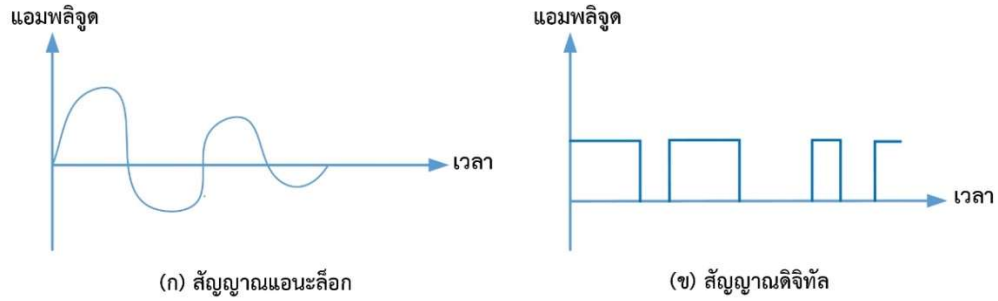
อื่นๆ ที่ได้ยินจากธรรมชาติจะเป็นรูปคลื่นแบบที่มีลักษณะต่อเนื่อง ขณะที่เสียงพูดถูกส่งผ่านอากาศ หากนำไมโครโฟนมารับคลื่นเสียงนี้จะสามารถทำการแปลงคลื่นนี้ให้กลายเป็นสัญญาณแอนะล็อกหรือสัญญาณดิจิทัลได้

ข้อมูลดิจิทัล (Digital Data) เป็นข้อมูลรูปแบบหนึ่ง ซึ่งมีลักษณะไม่ต่อเนื่องกันหรือแยกจากกัน (Discrete Form) โดยอยู่ในรูปไบนารี (Binary) ของบิต คือมีเฉพาะ 0 และ 1 เท่านั้น เช่น ข้อมูลที่ถูกจัดเก็บไว้ในหน่วยความจำของคอมพิวเตอร์ซึ่งข้อมูลนี้จะอยู่ในรูปของบิต 0 และ 1 มีค่าไม่ต่อเนื่อง เมื่อต้องการส่งข้อมูลระหว่างอุปกรณ์ภายในคอมพิวเตอร์เครื่องนั้น จะต้องทำการแปลงข้อมูลดิจิทัลให้กลายเป็นสัญญาณดิจิทัลเสียก่อนจึงจะสามารถส่งไปได้ แต่หากต้องการส่งข้อมูลออกไปภายนอกเครื่องคอมพิวเตอร์ จะต้องทำการแปลงข้อมูลดิจิทัลให้กลายเป็นสัญญาณแอนะล็อกก่อนที่จะส่งสัญญาณผ่านสื่อชนิดต่างๆ

3.2.2 สัญญาณแอนะล็อกและดิจิทัล

สัญญาณแอนะล็อก (Analog Signal) มักถูกแสดงแทนด้วยสัญญาณรูปคลื่นไซน์ (Sine Wave) มีลักษณะเป็นสัญญาณแบบต่อเนื่อง ข้อเสียของสัญญาณแอนะล็อก คือ สามารถถูกรบกวนได้ง่ายจากสัญญาณรบกวน (Noise) ส่งผลให้การกำจัดสัญญาณรบกวนออกจากข้อมูลต้นฉบับอาจทำได้ยาก เมื่อสัญญาณเดินทางไปถึงผู้รับจะทำให้ผู้รับได้รับข้อผิดพลาด เมื่อต้องการส่งข้อมูลออกไปในระยะทางไกลๆ ระดับของสัญญาณจะถูกลดทอนลง ดังนั้น จึงต้องใช้อุปกรณ์ที่ช่วยเพิ่มกำลังหรือความเข้มให้สัญญาณที่เรียกว่า **อุปกรณ์ขยายสัญญาณ** (Amplifier) จึงทำให้สามารถส่งสัญญาณในระยะไกลได้ อย่างไรก็ตามการเพิ่มของสัญญาณจะส่งผลให้สัญญาณรบกวนถูกขยายเพิ่มขึ้นด้วย

สัญญาณดิจิทัล (Digital Signal) มีลักษณะเป็นรูปคลื่นสี่เหลี่ยม (Square Wave) เป็นสัญญาณแบบไม่ต่อเนื่อง คือ สัญญาณสามารถเปลี่ยนแปลงจาก 0 ไป 1 หรือจาก 1 ไป 0 ได้ทุกเมื่อ ข้อดีของสัญญาณดิจิทัลคือ สามารถสร้างสัญญาณขึ้นได้ด้วยต้นทุนที่ต่ำกว่าสัญญาณแอนะล็อกและมีความทนทานต่อสัญญาณรบกวนได้ดีกว่า อีกทั้งยังสามารถจำแนกระหว่างข้อมูลกับสัญญาณรบกวนได้ง่ายกว่าแบบแอนะล็อก กรณีที่มีสัญญาณรบกวนปะปนมาไม่มากก็ยังคงรูปสัญญาณเดิมได้ โดยอุปกรณ์ที่ทำหน้าที่ทวนสัญญาณเดิมให้คงรูปเดิมเหมือนต้นฉบับในการส่งข้อมูลแบบดิจิทัลจะเรียกว่า **เครื่องทวนสัญญาณ** (Repeater)

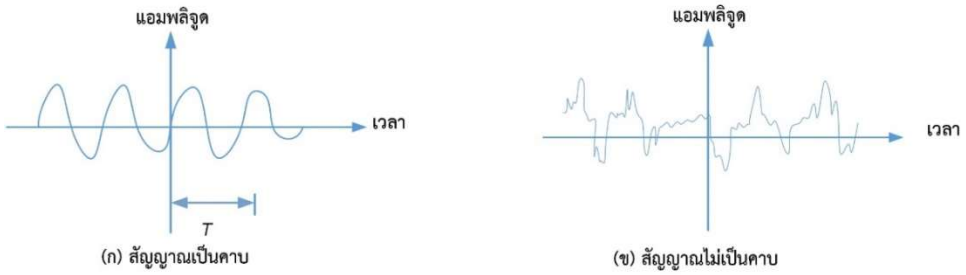


ภาพที่ 3.1 ตัวอย่างสัญญาณแอนะล็อกและสัญญาณดิจิทัล

ที่มา : (นรรัตน์ วัฒนมงคล, 2561, หน้า 49)

3.2.3 สัญญาณเป็นคาบและสัญญาณไม่เป็นคาบ

เมื่อพิจารณาว่าสัญญาณจะมีลักษณะเหมือนกันหรือซ้ำกันทุกช่วงเวลาหรือไม่ สามารถแบ่งลักษณะของสัญญาณได้เป็น 2 ประเภท คือ สัญญาณเป็นคาบ หมายถึง สัญญาณที่มีลักษณะรูปแบบของสัญญาณซ้ำรูปแบบเดิมทุกคาบเวลา และสัญญาณไม่เป็นคาบ หมายถึง สัญญาณที่มีการเปลี่ยนแปลงระดับของแอมพลิจูดได้โดยไม่ต้องมีรูปแบบหรือไม่จำเป็นต้องมีรูปคลื่นที่แน่นอน เมื่อคาบเวลา (Period) หมายถึง เวลาที่คลื่นเกิดการเปลี่ยนแปลงจากจุดเริ่มต้นจนถึงจุดสิ้นสุดก่อนที่จะเริ่มต้นเปลี่ยนแปลงสัญญาณซ้ำลักษณะเช่นเดิมอีกครั้ง หรือเป็นเวลาของการเปลี่ยนแปลงสัญญาณใน 1 ไซเคิล (Cycle) สามารถพิจารณาได้จากภาพที่ 3.2



ภาพที่ 3.2 ตัวอย่างของสัญญาณเป็นคาบและสัญญาณไม่เป็นคาบ

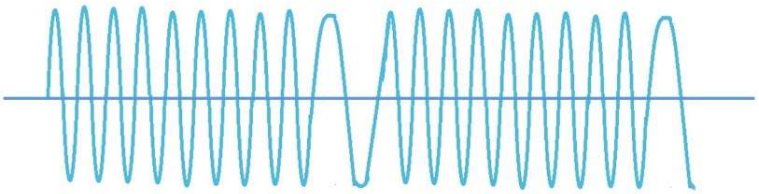
ที่มา : (นรรัตน์ วัฒนมงคล, 2561, หน้า 49-50)

ทั้งสัญญาณแอนะล็อกและสัญญาณดิจิทัลสามารถมีรูปแบบที่เป็นไปได้ทั้งสัญญาณเป็นคาบและสัญญาณไม่เป็นคาบ อย่างไรก็ตาม โดยทั่วไปเมื่อกล่าวถึงการสื่อสารข้อมูล

นั้น สัญญาณแอนะล็อกมักจะหมายถึงสัญญาณเป็นคาบ และสัญญาณดิจิทัลจะหมายถึงสัญญาณไม่เป็นคาบ

3.3 สัญญาณแอนะล็อก

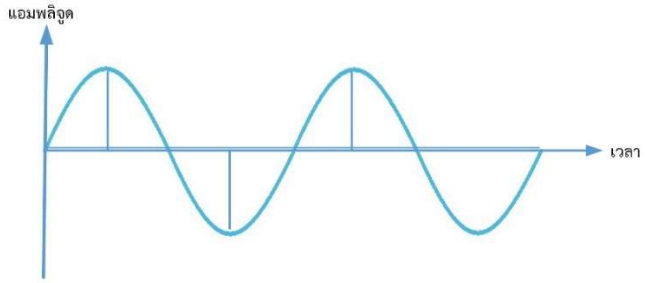
สัญญาณแอนะล็อก (Analog Signal) เป็นสัญญาณในรูปแบบของคลื่นต่อเนื่องที่ได้จากการแปลงข้อมูลแอนะล็อก เช่น เสียง แสงสว่าง ความร้อน ความดัน เป็นต้น องค์ประกอบสำคัญของสัญญาณแอนะล็อกแบบง่าย (Simple Analog Signal) คือ ซายน์เวฟ (Sine Wave) ดังภาพที่ 3.3 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 47-48)



ภาพที่ 3.3 แสดงตัวอย่างสัญญาณข้อมูลแบบแอนะล็อก
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 47)

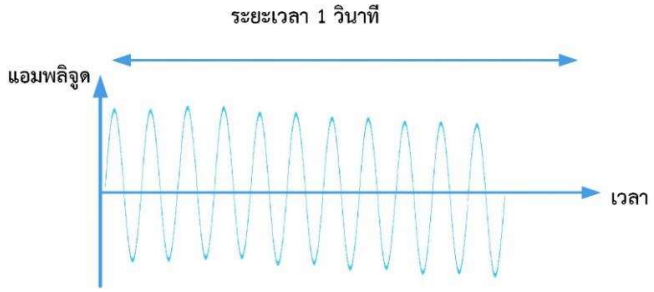
สัญญาณแอนะล็อกเกิดจากการประกอบของซายน์เวฟ โดยมีลักษณะสำคัญ 3 ประการ ดังนี้

1. แอมพลิจูด (Amplitude) คือ ค่าการกระจัด (ระยะจากแนวสมดุลถึงจุดบนคลื่น) ของจุดใดจุดหนึ่งบนลูกคลื่นซึ่งค่าการกระจัดสูงสุดและต่ำสุดบนซายน์เวฟจะอยู่บนจุดยอดของคลื่น สำหรับหน่วยที่ใช้วัดค่าของแอมพลิจูดมีได้หลายแบบ เช่น โวลต์ (Volt) หรือ วัตต์ (Watt) เป็นต้น ขึ้นอยู่กับชนิดของสัญญาณ ดังภาพที่ 3.4



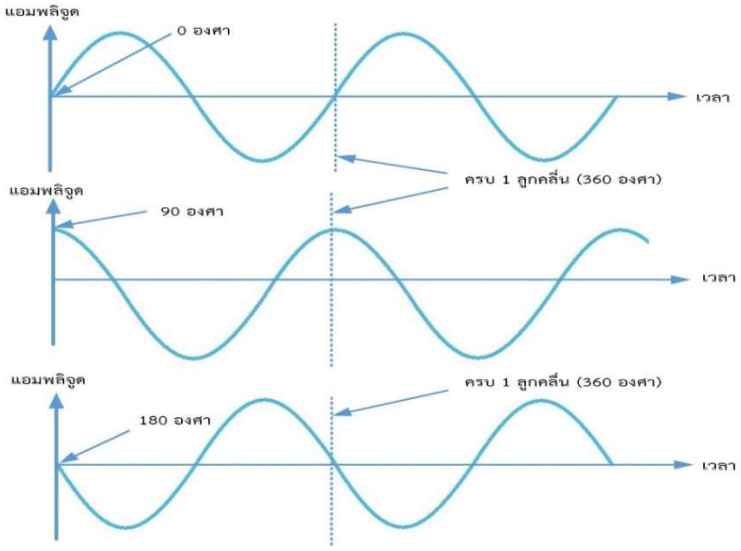
ภาพที่ 3.4 แสดงแอมพลิจูดของสัญญาณแอนะล็อก
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 47)

2. ความถี่ (Frequency) คือ จำนวนของลูกคลื่นใน 1 วินาที ซึ่งค่าความถี่จะมีมากหรือน้อยขึ้นอยู่กับการเปลี่ยนแปลงของจำนวนลูกคลื่นในหนึ่งหน่วยเวลา หากคลื่นไม่เกิดการเปลี่ยนแปลงใดๆ แสดงว่ามีความถี่เป็นศูนย์และถ้ามีการเปลี่ยนอย่างรวดเร็วในหน่วยเวลาที่ไม่สามารถวัดได้ หรือหน่วยเวลาเท่ากับศูนย์ แสดงว่ามีความถี่อย่างไม่จำกัด (Infinity) ดังภาพที่ 3.5



ภาพที่ 3.5 แสดงความถี่ในเวลา 1 วินาทีของสัญญาณแอนะล็อก
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 48)

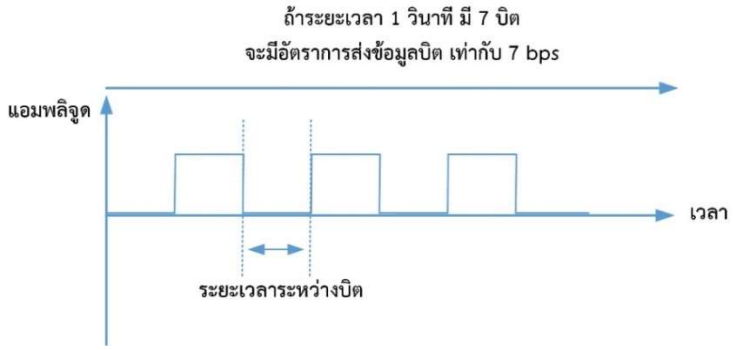
3. เฟส (Phase) คือ ตำแหน่งของคลื่น ณ เวลาเท่ากับศูนย์ ซึ่งเฟสก็เป็นตำแหน่งที่คลื่นเริ่มต้นที่เวลาศูนย์นั่นเอง โดยตำแหน่งดังกล่าวจะถูกเรียกเป็นองศาตามรูปแบบของซายน์เวฟ โดยหนึ่งลูกคลื่นจะมี 360 องศา หรือ 1 วงกลม ดังภาพที่ 3.6



ภาพที่ 3.6 แสดงความแตกต่างของเฟสในสัญญาณแอนะล็อก
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 48)

3.4 สัญญาณดิจิทัล

สัญญาณดิจิทัล (Digtal Signal) เป็นสัญญาณไฟฟ้าแบบไม่ต่อเนื่องที่ได้จากการแปลงข้อมูลดิจิทัล ซึ่งเป็นรหัสแบบไบนารี (Binary Code) มีค่าของข้อมูลเป็น 0 และ 1 เท่านั้น เช่น สัญญาณโทรศัพท์หรือวิทยุแบบดิจิทัล เป็นต้น โดยทั่วไปแทนข้อมูล 0 ด้วยค่าแรงดันไฟฟ้า (Voltage) ศูนย์โวลต์ และข้อมูล 1 แทนด้วยค่าแรงดันไฟฟ้าบวก ดังภาพที่ 3.7 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 49-52)



ภาพที่ 3.7 แสดงสัญญาณดิจิทัล

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 49)

คุณลักษณะที่สำคัญในสัญญาณดิจิทัล มี 2 ประการ ดังนี้

1. ระยะเวลาระหว่างบิต (Bit Interval) คือ หน่วยเวลาที่ใช้ในระหว่างการส่งข้อมูลเพียง 1 บิต

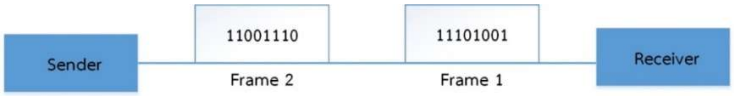
2. อัตราการส่งข้อมูลบิต (Bit Rate) คือ จำนวนบิตที่สามารถส่งได้ในเวลา 1 วินาที กล่าวคือ เป็นอัตราในการส่งข้อมูลบิตทั้งหมดในเวลา 1 วินาที มีหน่วยเป็น บิตต่อวินาที (bps)

วิธีการส่งข้อมูลแบบดิจิทัล

วิธีการขนส่งข้อมูลแบบดิจิทัล เป็นการส่งข้อมูลในระดับบิต แบ่งได้ 2 ลักษณะ ดังนี้

1. Serial Transmission

เป็นการขนส่งในลักษณะเป็นลำดับโดยจะใช้การขนส่งแบบเดี่ยว กล่าวคือ จะใช้ช่องทางการส่งข้อมูลเพียงหนึ่งช่องทางโดยส่งไปทีละหนึ่งบิตต่อหนึ่งหน่วยเวลา โดยข้อมูลนั้นจะถูกแบ่งออกเป็นเฟรมและจะถูกประกอบกลับเมื่อไปถึงยังปลายทาง การขนส่งข้อมูลด้วยวิธีการนี้นิยมใช้กันทั่วไป เช่น การขนส่งข้อมูลที่เชื่อมต่อผ่าน Serial Cable หรือ Serial Port เป็นต้น ดังภาพที่ 3.8



ภาพที่ 3.8 แสดงการขนส่งแบบ Serial Transmission

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 50)

2. Parallel Transmission

เป็นการขนส่งในลักษณะคู่ขนาน กล่าวคือ จะใช้ช่องทางมากกว่าหนึ่งช่องทาง และส่งแบบขนานกันโดยส่งข้อมูลหนึ่งบิตต่อหนึ่งช่องทางในหนึ่งหน่วยเวลาเดียวกัน การส่งข้อมูลในลักษณะนี้จะสามารถส่งข้อมูลได้รวดเร็วกว่าแบบ Serial แต่นิยมใช้กับการขนส่งข้อมูลในระยะใกล้ โดยจะใช้จำนวนช่องทางการขนส่งตามจำนวนบิตข้อมูลที่เข้ารหัสไว้ ทำให้สิ้นเปลืองสายส่งกว่าแบบ Serial ที่ใช้สายส่งเพียงเส้นเดียว เช่น การส่งข้อมูลระหว่างอุปกรณ์ 2 ชิ้น ผ่านทาง Parallel Port ซึ่งชุดข้อมูลหนึ่งชุดมีทั้งหมด 8 บิต ดังนั้นการขนส่งข้อมูลดังกล่าวจะมีช่องทางในการขนส่ง 8 ช่องทาง โดยมีการขนส่งแบบขนานพร้อมกัน 8 บิต เป็นต้น ดังภาพที่ 3.9

ภาพที่ 3.9 แสดงการขนส่งแบบ Serial Transmission

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 50)

ข้อดีและข้อเสียของการขนส่งข้อมูลแบบ Serial Transmission และ Parallel Transmission สามารถสรุปได้ดังตารางที่ 3.1

ตารางที่ 3.1 แสดงข้อดีและข้อเสียของการขนส่งข้อมูลแบบ Serial Transmission และ Parallel Transmission

รูปแบบการส่งข้อมูล	ข้อดี	ข้อเสีย
Serial Transmission	ประหยัดค่าใช้จ่ายและส่งได้ระยะไกล	ส่งข้อมูลได้ช้ากว่าแบบ Parallel Transmission
Parallel Transmission	ส่งข้อมูลได้เร็วกว่าแบบ Serial Transmission	ค่าใช้จ่ายสูง และใช้ได้ระยะใกล้

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 50)

จังหวะในการส่งข้อมูลแบบดิจิทัล (Synchronization)

ในการขนส่งข้อมูลนั้นจำเป็นต้องมีปัจจัยสำคัญหลายประการเพื่อให้ข้อมูลสามารถเดินทางไปถึงปลายทางอย่างสมบูรณ์ และได้ข้อมูลที่ถูกต้อง ปัจจัยที่สำคัญ คือ จังหวะในการส่งข้อมูล (Synchronization) เนื่องจากข้อมูลแบบดิจิทัลนั้นจะถูกส่งมาเหมือนกับกระแสของข้อมูลหรือ Stream ซึ่งมีการเรียงลำดับและมีข้อมูลจำนวนมาก เมื่อถึงปลายทางแล้วจะถูกนำมาประกอบกลับคืนเป็นข้อมูลเดิมตามลำดับที่ได้รับ จังหวะในการส่งข้อมูลแบบดิจิทัล สามารถแบ่งออกได้เป็น 2 แบบ ดังนี้

1. Asynchronous

เป็นการขนส่งที่อาศัยบิตพิเศษเพื่อบอกถึงจุดเริ่มต้นและจุดสิ้นสุดของข้อมูล เรียกว่า Start และ Stop Bit ซึ่งบรรจุไว้ที่ส่วนหัวและส่วนท้ายของชุดข้อมูลตามลำดับ โดยบิตพิเศษดังกล่าวจะเป็นตัวบ่งบอกถึงการขนส่งข้อมูลว่าสิ้นสุดหรือไม่ ซึ่งไม่ใช่การส่งแบบอาศัยจังหวะหรือ Synchronous การขนส่งข้อมูลแบบนี้ในแต่ละชุดข้อมูลจะต้องเว้นระยะเวลาหนึ่งเพื่อที่จะส่งชุดข้อมูลลำดับต่อไปโดยไม่สามารถส่งไปพร้อมกันได้และจะต้องใช้จำนวนบิตเพิ่มขึ้นอีก 2 บิต ต่อหนึ่งชุดข้อมูล ซึ่งอาจส่งผลให้ข้อมูลที่มีจำนวนชุดข้อมูลมากๆ มีปริมาณของบิตเพิ่มขึ้น ทำให้ขนส่งช้าและอาจส่งผลให้เกิดความหนาแน่นของข้อมูลขึ้นในระบบเครือข่ายได้อีกด้วย โดยข้อมูลที่สูงจะมีขนาด 8 บิต ดังภาพที่ 3.10

ภาพที่ 3.10 แสดงชุดข้อมูลในการส่งแบบ Asynchronous

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 51)

2. Synchronous

เป็นการส่งข้อมูลโดยอาศัยการเข้าจังหวะ ภายในชุดข้อมูลทั้งหมดนั้นจะมีการใส่ข้อมูลพิเศษที่เรียกว่า SYN Characters เพื่อเป็นตัวบ่งบอกถึงลำดับของการส่งทำให้ผู้รับและผู้ส่งมั่นใจได้ว่าข้อมูลทั้งหมดถูกต้องและสมบูรณ์ การเพิ่ม SYN ลงในชุดข้อมูลนั้นจะทำให้การส่งทำได้รวดเร็วและมีประสิทธิภาพมากกว่าแบบ Asynchronous โดยเฉพาะการส่งข้อมูลจำนวนมาก เนื่องจาก SYN นั้นใช้พื้นที่ในการบรรจุเข้าไปในชุดข้อมูลที่น้อยกว่าอีกทั้งข้อมูลทั้งหมดยังถูกรวมเข้าด้วยกันเป็นบล็อกของข้อมูล (Block of Data) ทำให้ไม่จำเป็นต้องใช้ SYN ในปริมาณมากเท่ากับการใช้ Start และ Stop Bit การขนส่งข้อมูลโดยอาศัย Synchronous จึงมีประสิทธิภาพมากกว่าอย่างเห็นได้ชัดเมื่อข้อมูลมีขนาดใหญ่ ดังภาพที่ 3.11

ภาพที่ 3.11 แสดงบล็อกข้อมูลในการส่งแบบ Synchronous

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 51)

ข้อดีและข้อเสียของการขนส่งข้อมูลแบบ Asynchronous และ Synchronous สรุปได้ดังตารางที่ 3.2

ตารางที่ 3.2 แสดงข้อดีและข้อเสียของการขนส่งข้อมูลแบบ Asynchronous และแบบ Synchronous

รูปแบบการส่งข้อมูล	ข้อดี	ข้อเสีย
Asynchronous	มีรูปแบบเรียบง่าย และมีค่าใช้จ่ายต่ำ	ข้อมูลยิ่งมากยิ่งส่งได้ช้า และความถูกต้องของข้อมูลน้อยกว่าแบบ Synchronous
Synchronous	ส่งข้อมูลได้เร็ว และความถูกต้องของข้อมูลสูงกว่าแบบ Asynchronous	ค่าใช้จ่ายสูง

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 52)

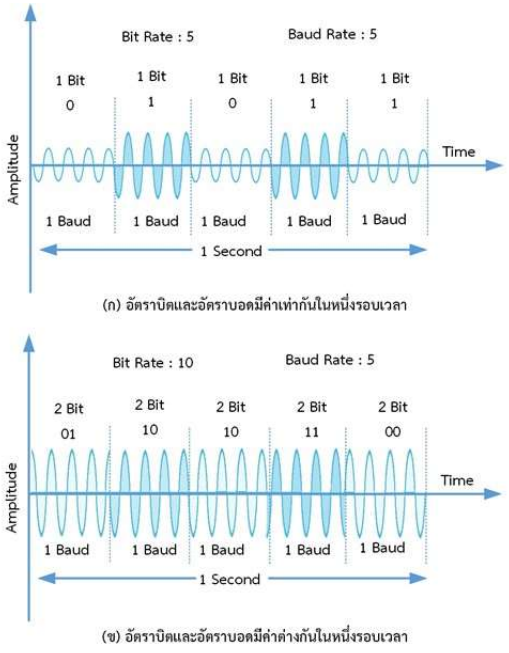
หน่วยวัดความเร็วในการส่งข้อมูลแบบดิจิตอล

หน่วยวัดความเร็วในระบบสื่อสารที่จะกล่าวถึงต่อไปนี้ คือ อัตราบิต (Bit Rate/Data Rate) และอัตราบอด (Baud Rate) ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 168-169)

1. อัตราบิต คือ จำนวนบิตที่สามารถส่งได้ภายในหนึ่งหน่วยเวลา มีหน่วยวัดความเร็วเป็นบิตต่อวินาที (bit per second : bps)

2. อัตราบอด คือ จำนวนของสัญญาณที่สามารถส่งได้ต่อการเปลี่ยนสัญญาณในหนึ่งหน่วยเวลา (baud per second)

ตัวอย่างในระบบขนส่ง กำหนดให้อัตราบอดคือรถโดยสาร และอัตราบิตคือผู้โดยสาร ถ้ารถสามารถบรรทุกผู้โดยสารได้ครั้งละหนึ่งคน และมีรถโดยสารจำนวน 1,000 คัน ก็จะขนถ่ายผู้โดยสารจากจุดหนึ่งไปยังอีกจุดหนึ่งได้เพียง 1,000 คน แต่ถ้ารถโดยสารแต่ละคันสามารถบรรทุกผู้โดยสารได้คันละ 4 คน การขนถ่ายผู้โดยสารจากจุดหนึ่งไปยังอีกจุดหนึ่งก็จะเพิ่มขึ้นเป็น 4,000 คน แสดงว่าอัตราบิตจะต้องมีมากกว่าหรือเท่ากับอัตราบอดเสมอ ดังนั้นเป้าหมายของระบบการสื่อสารก็คือ ควรเพิ่มจำนวนผู้โดยสารให้มากขึ้นและใช้ยานพาหนะให้ลดน้อยลง ดังนั้น อัตราบอดจึงถูกใช้เป็นตัวกำหนดแบนด์วิดธ์ที่จำเป็นในการส่งสัญญาณข้อมูล ดังภาพที่ 3.12



ภาพที่ 3.12 แสดงความสัมพันธ์ระหว่างอัตราบิตกับอัตราบอด

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 169)

3.5 การแปลงข้อมูลให้เป็นสัญญาณ

ข้อมูลและสัญญาณ สามารถเป็นได้ทั้งแอนะล็อกหรือดิจิทัล ซึ่งโดยส่วนใหญ่แล้วสัญญาณแอนะล็อกจะใช้ลำเลียงข้อมูลแอนะล็อก และสัญญาณดิจิทัลก็จะลำเลียงข้อมูลดิจิทัล การตัดสินใจว่าจะใช้สัญญาณแอนะล็อกหรือดิจิทัลนั้น ขึ้นอยู่กับอุปกรณ์ส่งและสภาพแวดล้อมที่สัญญาณจะต้องเดินผ่าน เนื่องจากอุปกรณ์บางชนิดจะสนับสนุนสัญญาณแอนะล็อกหรือดิจิทัลเพียงอย่างเดียวเท่านั้น เช่น ระบบโทรศัพท์ที่ถูกสร้างเพื่อส่งเสียงพูดของมนุษย์ ซึ่งเป็นข้อมูลแอนะล็อก ดังนั้น ระบบโทรศัพท์แบบดั้งเดิมจึงถูกสร้างขึ้นเพื่อส่งสัญญาณแอนะล็อกเป็นหลัก ดังนั้น ในการส่งข้อมูลดิจิทัลจากคอมพิวเตอร์ผ่านสายโทรศัพท์จึงต้องใช้สัญญาณแอนะล็อก ในขณะเดียวกันการส่งผ่านข้อมูลแอนะล็อกด้วยสัญญาณดิจิทัลก็ถือเป็นเรื่องปกติ จึงสรุปได้ว่า ไม่ว่าข้อมูลที่ต้องการสื่อสารจะอยู่ในรูปแบบแอนะล็อกหรือดิจิทัล ก็สามารถส่งผ่านไปยังระบบสื่อสารได้ทั้งสิ้น เพียงแต่ต้องมีการแปลงรูปหรือเข้ารหัสข้อมูลเหล่านั้นให้อยู่ในรูปแบบของสัญญาณที่เหมาะสมกับสื่อกลางประเภทนั้นๆ ปัจจุบันมีการนำระบบดิจิทัลมาใช้งานแพร่หลายมากขึ้น เช่น สถานีโทรทัศน์ที่ใช้สัญญาณดิจิทัลเพราะให้คุณภาพสัญญาณที่ดีกว่าและมีช่องรายการเพิ่มมากขึ้น การแปลงข้อมูลเป็นสัญญาณต่างๆ แบ่งออกเป็น 4 รูปแบบ ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 169-175)

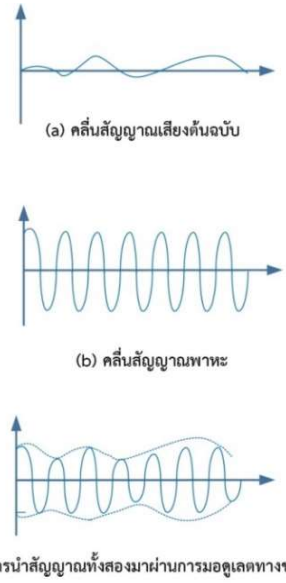
3.5.1 การแปลงข้อมูลแอนะล็อกเป็นสัญญาณแอนะล็อก

การแปลงข้อมูลแอนะล็อกเป็นสัญญาณแอนะล็อก (Analog Data to Analog Signal) จัดเป็นรูปแบบการแปลงที่ง่ายและใช้ต้นทุนต่ำ ด้วยการใช้อุปกรณ์ช่วยในการแปลงสัญญาณ เช่น กรณีเปิดวิทยุคลื่น FM ที่ความถี่ 101.5 เมกะเฮิรตซ์ ซึ่งคลื่นสถานีดังกล่าวจะส่งออกไปยังผ่านความถี่นี้ แต่ด้วยเสียงพูดของมนุษย์อยู่บนย่านความถี่ต่ำคือ ช่วง 300-3,400 เฮิรตซ์ ส่วนเสียงดนตรีจะอยู่บนย่านความถี่ที่ 30-20,000 เฮิรตซ์ และเพื่อให้เสียงพูดและเสียงดนตรีสามารถส่งออกไปยังย่านความถี่ 101.5 เมกะเฮิรตซ์ได้ จึงต้องมีเทคนิคการส่ง ดังนั้นเราจึงควรทำความเข้าใจเกี่ยวกับสัญญาณพาหนะและการมอดูเลตกัน ดังภาพที่ 3.13

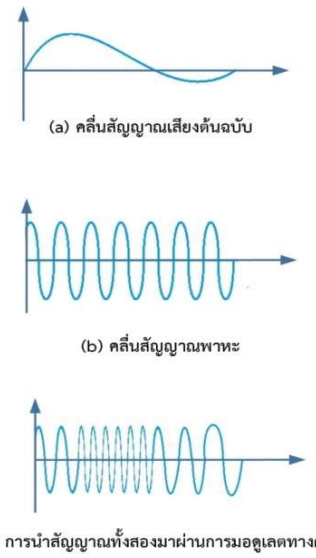
ภาพที่ 3.13 การแปลงเสียงพูดให้เป็นสัญญาณแอนะล็อกผ่านโทรศัพท์แบบพื้นฐาน
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 170)

สัญญาณพาหนะ (Carrier Signal) เป็นคลื่นความถี่สูงและเป็นคลื่นสัญญาณไฟฟ้าที่สามารถส่งออกผ่านสื่อกลางได้บนระยะทางไกลๆ เมื่อมีการนำสัญญาณพาหนะมารวมเข้ากับสัญญาณเสียง เรียกเทคนิคนี้ว่า **การมอดูเลต (Modulate)** ก็จะได้คลื่นสัญญาณใหม่ที่พร้อมส่งออกผ่านไปยังสื่อกลาง เช่น อากาศ ครั้นสถานีได้ส่งสัญญาณที่ผ่านการมอดูเลตแล้ว สถานีฝั่งรับก็จะมีกรรมวิธีในการแยกสัญญาณพาหนะออกจากสัญญาณเสียง ซึ่งเราเรียกเทคนิคนี้ว่า **การดีมอดูเลต (Demodulate)**

พิจารณาจากภาพที่ 3.14 เป็นการมอดูเลตสัญญาณแอนะล็อกกับคลื่นพาหนะ โดยภาพที่ 3.14 (a) คือสัญญาณแอนะล็อกซึ่งเป็นสัญญาณต้นฉบับ ส่วนภาพที่ 3.14 (b) เป็นสัญญาณพาหนะ และภาพที่ 3.14 (c) เป็นการนำคลื่นทั้งสองมาผ่านเทคนิคการมอดูเลตทางขนาด (Amplitude Modulation : AM) ที่ใช้กับคลื่นวิทยุ AM จะพบว่าขนาดของคลื่นพาหนะจะมีค่าเปลี่ยนแปลงไปตามรูปแบบของสัญญาณที่ส่ง ในขณะที่ภาพ 3.15 เป็นการมอดูเลตทางความถี่ (Frequency Modulation : FM) ที่ใช้กับคลื่นวิทยุ FM โดยความถี่ของคลื่นพาหนะจะมีค่าเปลี่ยนแปลงไปตามสัญญาณที่มอดูเลต ซึ่งจะเห็นได้จากขนาดของรูปคลื่น ไม่ได้ถูกเปลี่ยนแปลงไปตามการลดของระดับสัญญาณ ดังภาพที่ 3.14 และ 3.15



ภาพที่ 3.14 การมอดูเลตทางขนาด (AM)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 171)



ภาพที่ 3.15 การมอดูเลตทางความถี่ (FM)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 171)

3.5.2 การแปลงข้อมูลดิจิทัลเป็นสัญญาณดิจิทัล

สัญญาณดิจิทัล ค่าที่เป็นไปได้คือค่าไบนารี 0 และ 1 เท่านั้น เราสามารถแทนไบนารี 1 เป็นระดับแรงดันสูงหรือต่ำก็ได้ เช่น หากใช้ค่าไปนารี แทนระดับแรงดันสูง ก็จะต้องใช้ค่าไบนารี 0 แทนระดับแรงดันต่ำหรือกรณีใช้ค่าไบนารี 1 แทนระดับแรงดันต่ำ ก็ต้องใช้ค่าไบนารี 0 แทนระดับแรงดันสูง เป็นต้น ดังภาพที่ 3.16 และ 3.17

ภาพที่ 3.16 การแปลงข้อมูลดิจิทัลเป็นสัญญาณดิจิทัลด้วยอุปกรณ์ Digital Transceiver
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 172)

การเข้ารหัส

การแปลงข้อมูลดิจิทัลเป็นสัญญาณดิจิทัล จะมีเทคนิคการเข้ารหัสสัญญาณหลายวิธีด้วยกัน ดังนี้

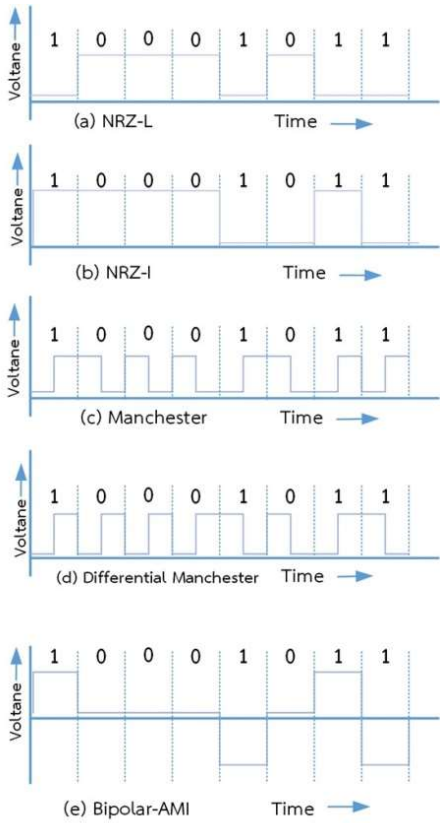
1. การเข้ารหัสแบบ NRZ-L (NonReturn-to-Zero-Level) จัดเป็นวิธีที่ง่ายที่สุด โดยระดับสัญญาณจะขึ้นอยู่กับสถานะของบิต พิจารณาจากภาพที่ 3.17 (a) จะพบว่าหากบิตข้อมูลที่มีค่าเป็น 1 ก็แทนระดับแรงดันต่ำ หรือบิตข้อมูลมีค่าเป็น 0 ก็แทนระดับแรงดันสูง การเข้ารหัสด้วยวิธีนี้จัดเป็นวิธีแบบตรงไปตรงมา แต่ก็มีข้อเสียคือ ยากต่อการตัดสินใจว่าจุดใดเป็นจุดเริ่มต้นหรือจุดสิ้นสุดของช่วงสัญญาณที่ใช้แทนค่าบิตบิตหนึ่ง และกรณีบิตข้อมูลเกิดมีค่าเดียวกันแบบต่อเนื่อง จะทำให้ยากต่อการควบคุมจังหวะ (Synchronized)

2. การเข้ารหัสแบบ NRZ-I (NonReturn-to-Zero-Invert) เป็นเทคนิคการเข้ารหัสที่คล้ายคลึงกับวิธี NRZ-L แต่มีความแม่นยำกว่า โดยการเปลี่ยนแปลงสัญญาณจะเกิดขึ้น ณ จุดเริ่มต้นของบิต และการเปลี่ยนแปลงสัญญาณจะเกิดขึ้นต่อเมื่อพบบิตข้อมูลที่มีค่าเป็น 1 และหากพบบิตข้อมูลที่มีค่าเป็น 0 ก็จะไม่มีการเปลี่ยนแปลงค่าใดๆ ซึ่งเป็นไปดังภาพที่ 3.17 (b)

3. การเข้ารหัสแบบแมนเชสเตอร์ (Manchester Encoding) เป็นเทคนิคการเข้ารหัสที่นิยมใช้บนเครือข่ายอีเทอร์เน็ต (10Base-T) การเข้ารหัสด้วยวิธีนี้ จะมีการเปลี่ยนแปลงสัญญาณ ณ จุดกึ่งกลางของบิตเพื่อนำไปใช้แทนบิตข้อมูลและการกำหนดจังหวะ โดยการเปลี่ยนแปลงจากต่ำไปสูง (⌐) จะแทนค่า 1 ในขณะที่การเปลี่ยนแปลงจากสูงไปต่ำ (¬) จะใช้แทนค่า 0 ซึ่งเป็นไปดังภาพที่ 3.17 (c)

4. การเข้ารหัสแบบดิฟเฟอร์เรนเชียลแมนเชสเตอร์ (Differential Manchester Encoding) การเข้ารหัสด้วยวิธีนี้ จะเปลี่ยนแปลงสัญญาณ ณ จุดกึ่งกลางของบิต เช่นเดียวกับวิธีการเข้ารหัสแบบแมนเชสเตอร์ แต่จะนำใช้เพื่อการกำหนดจังหวะเท่านั้น โดยการเปลี่ยนสัญญาณจะเกิด ณ จุดเริ่มต้นของบิตข้อมูลที่มีค่าเป็น 0 เท่านั้น ดังภาพที่ 3.17 (d)

5. การเข้ารหัสแบบไบโพลาร์ (Bipolar-AMI) เป็นการเข้ารหัสที่ใช้ระดับแรงดันไฟฟ้าแบบสามระดับ (แรงดันบวก, ศูนย์ และลบ) โดยเมื่ออุปกรณ์ส่งค่าไบนารี 0 ค่าแรงดัน 0 ก็จะถูกส่งไป แต่ถ้าอุปกรณ์ส่งค่าไบนารี 1 ระดับแรงดันที่ส่งไปสามารถเป็นไปได้ทั้งค่าบวกและค่าลบ ซึ่งขึ้นอยู่กับค่าไบนารี 1 ค่าสุดท้ายที่ถูกส่งไป เช่น ถ้าค่าสุดท้ายของค่าไบนารี 1 ถูกส่งไปเป็นแรงดันบวกแล้ว ค่าไบนารี 1 ตัวถัดไปจะส่งเป็นแรงดันลบ และในทำนองเดียวกัน ถ้าค่าสุดท้ายของค่าไบนารี 1 ถูกส่งไปเป็นแรงดันลบ ค่าไบนารี 1 ตัวถัดไปก็จะส่งเป็นแรงดันบวก ซึ่งเป็นไปดังภาพที่ 3.17 (e)



ภาพที่ 3.17 ตัวอย่างการเข้ารหัสดิจิทัลทั้ง 5 รูปแบบ

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 172)

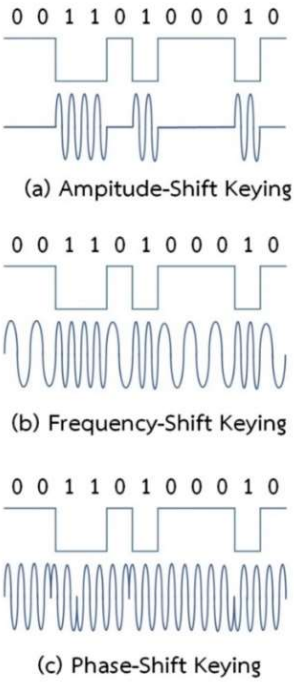
3.5.3 การแปลงข้อมูลดิจิทัลเป็นสัญญาณแอนะล็อก

อุปกรณ์แปลงข้อมูลดิจิทัลมาเป็นสัญญาณแอนะล็อก และแปลงสัญญาณแอนะล็อกกลับมาเป็นข้อมูลดิจิทัลนั้นเรียกว่า **โมเด็ม** ตัวอย่างเช่น การเข้าถึงเครือข่ายอินเทอร์เน็ตแบบ Dial-Up ซึ่งโมเด็มต้นทางจะแปลงข้อมูลคอมพิวเตอร์ (ดิจิทัล) มาเป็นสัญญาณแอนะล็อกเพื่อส่งข้อมูลผ่านสายสื่อสารบนระบบโทรศัพท์ ครั้นเมื่อสัญญาณส่งถึงปลายทางโมเด็มอีกฝั่งหนึ่งก็จะแปลงสัญญาณแอนะล็อกให้กลับมาเป็นข้อมูลดิจิทัลเพื่อส่งให้กับคอมพิวเตอร์ใช้งานต่อไปดังภาพที่ 3.18

ภาพที่ 3.18 การแปลงข้อมูลดิจิทัลเป็นสัญญาณแอนะล็อกด้วยอุปกรณ์โมเด็ม
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 174)

ปกติสัญญาณโทรศัพท์จะถูกนำไปใช้เป็นช่องสัญญาณเสียง ครั้นเมื่อต้องการนำส่งด้วยสัญญาณดิจิทัล จึงต้องแปลงสัญญาณให้อยู่ในรูปแบบที่เหมาะสมกับระบบสื่อสาร หรือที่เรียกกันว่า**การมอดูเลต** โดยจะใช้สัญญาณพาหนะส่งผ่านเข้าไปในช่องสัญญาณ และด้วยเทคนิคการมอดูเลตยังทำให้เราสามารถส่งข้อมูลได้ในอัตราเร็วที่สูงขึ้นภายใต้แบนด์วิดธ์ที่เท่าเดิม เช่น สัญญาณโทรศัพท์ที่มีแบนด์วิดธ์เพียง 4 KHz ก็จะส่งข้อมูลด้วยความเร็วสูงขึ้นเป็น 56 Kbps เป็นต้น

เทคนิคการมอดูเลตสัญญาณดิจิทัลจะคล้ายคลึงกับการส่งสัญญาณแอนะล็อก แต่จะมีความแตกต่างกันคือ สัญญาณที่ต้องการมอดูเลตจะต้องเป็นสัญญาณดิจิทัลที่มีระดับแรงดันค่อนข้างแน่นอน ดังนั้น สัญญาณพาหนะก็จะถูกเปลี่ยนไปตามแอมพลิจูด ความถี่ หรือเฟส ที่มีระดับแน่นอนเช่นกัน โดยการมอดูเลตจะประกอบไปด้วยวิธี ASK (Amplitude-Shift Keying), FSK (Frequency-Shift Keying) และ PSK (Phase-Shift Keying) ดังภาพที่ 3.19



ภาพที่ 3.19 การมอดูเลตสัญญาณดิจิทัลด้วยเทคนิค ASK, FSK, และ PSK
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 174)

3.5.4 การแปลงข้อมูลแอนะล็อกเป็นสัญญาณดิจิทัล

โคเดค (Code/Decoder) เป็นอุปกรณ์สำคัญที่นำมาใช้แปลงข้อมูลแอนะล็อกมาเป็นสัญญาณดิจิทัลด้วยเทคนิคการแปลงเสียงสนทนาเป็นสัญญาณดิจิทัล (Voice Digitization) ในขณะเดียวกันก็ยังสามารถแปลงกลับมาเป็นสัญญาณแอนะล็อกได้ ตัวอย่างอุปกรณ์โคเดค เช่น ซาวด์การ์ด สแกนเนอร์ วอยซ์เมล และวีดีโอคอนเฟอเร็นซ์ ดังภาพที่ 3.20

ภาพที่ 3.20 การแปลงข้อมูลแอนะล็อกให้เป็นสัญญาณดิจิทัลด้วยอุปกรณ์โคเดค
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 175)

ในการสื่อสารผ่านช่องสัญญาณ สัญญาณอาจถูกรบกวนจากแหล่งกำเนิดสัญญาณอื่นๆ หรืออาจถูกลดทอนจากช่องสัญญาณ สิ่งเหล่านี้ส่งผลให้สัญญาณที่ส่งมีความผิดเพี้ยนไป เป็นเหตุให้ฝั่งรับตีความข้อมูลข่าวสารผิดพลาด ในกรณีของสัญญาณดิจิทัลที่มีเซตของค่าสัญญาณเป็นเซตจำกัด จะส่งผลดีให้ฝั่งรับสามารถคาดเดาหรือตีความข่าวสารที่มาถึงได้ดีกว่าสัญญาณแอนะล็อกที่มีค่าสัญญาณเป็นเซตอนันต์ การสื่อสารดิจิทัลจึงมีคุณภาพของข่าวสารดีกว่าการสื่อสารแอนะล็อกอย่างชัดเจน และนิยมใช้กันอย่างแพร่หลาย (พงศธร เศรษฐีขจร, 2558, หน้า 2)

3.6 สรุป

การขนส่งข้อมูลมีทั้งข้อมูลที่เป็นแอนะล็อกและดิจิทัลจึงจำเป็นต้องเข้าใจถึงรูปแบบของสัญญาณที่ใช้ในการขนส่งข้อมูลดังกล่าว สัญญาณแอนะล็อกเป็นสัญญาณในรูปแบบของซายน์เวฟซึ่งมีลักษณะ คือ แอมพลิจูด ความถี่ และเฟส สำหรับสัญญาณดิจิทัลเป็นสัญญาณที่อยู่ในรูปแบบของข้อมูลบิตซึ่งมีค่าเป็นศูนย์และหนึ่งเท่านั้น สัญญาณแต่ละรูปแบบจะเหมาะสมกับการขนส่งข้อมูลแตกต่างกันไปซึ่งอาจขึ้นอยู่กับความต้องการของระบบอุปกรณ์ที่รองรับและความเหมาะสมในการติดต่อสื่อสารระหว่างต้นทางและปลายทาง

การขนส่งข้อมูลในรูปแบบของสัญญาณจำเป็นต้องปรับเปลี่ยนลักษณะรูปแบบของสัญญาณเป็นไปตามรูปแบบต่างๆ เช่น จากดิจิทัลเป็นแอนะล็อก ได้แก่ การแปลงข้อมูลจากคอมพิวเตอร์เป็นสัญญาณไฟฟ้า หรือแปลงจากแอนะล็อกเป็นแอนะล็อก ได้แก่ สัญญาณที่มีความถี่สูงปรับเป็นสัญญาณที่มีความถี่เหมาะสมกับอุปกรณ์ของผู้รับ การเปลี่ยนแปลงสัญญาณให้อยู่ในรูปแบบที่เหมาะสมดังกล่าวจะใช้การมอดูเลตซึ่งมีอยู่หลายวิธีตามความเหมาะสมและความต้องการของการติดต่อสื่อสาร

บทที่ 4
สื่อกลางในการรับส่งข้อมูล

การสื่อสารข้อมูลในระบบเครือข่ายคอมพิวเตอร์ต้องอาศัยสื่อกลางที่ใช้ในการส่งข้อมูล โดยสื่อกลางในการรับส่งข้อมูล (Transmission Media) สามารถแบ่งได้เป็น 2 ประเภท คือ สื่อกลางแบบใช้สาย ได้แก่ สายคู่บิดเกลียว สายโคแอ๊กเชียล และสายใยแก้วนำแสง ส่วนสื่อกลางแบบไร้สาย เช่น ระบบโทรศัพท์เคลื่อนที่ หรือระบบการส่งสัญญาณผ่านดาวเทียม เป็นต้น

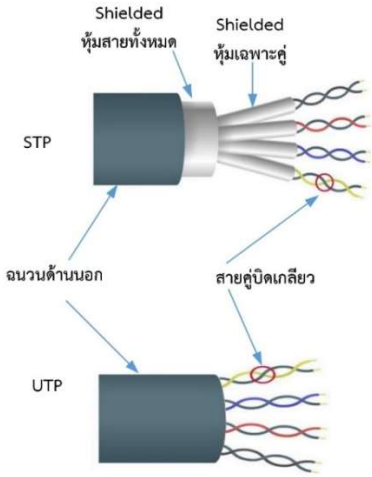
4.1 สื่อกลางแบบใช้สาย

สื่อกลางแบบใช้สายสัญญาณ (Guided Media) เป็นสื่อกลางที่ใช้เชื่อมต่อระหว่างอุปกรณ์ เพื่อขนส่งข้อมูลในระดับกายภาพไปตามสายสัญญาณประเภทต่างๆ โดยสื่อกลางประเภทนี้สามารถกำหนดเส้นทางของข้อมูลได้ (Guided Media) แบ่งออกเป็น 3 ชนิด ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 72-80 และพิสิฐ พรพงศ์เตชวาณิช และพงษ์พิสิฐ วุฒิดิษฐโชติ, 2566, หน้า 125-130)

4.1.1 สายคู่บิดเกลียว

สายคู่บิดเกลียวหรือสายคู่ตีเกลียว (Twisted-Pair Cable) เป็นสายสัญญาณที่นิยมใช้ในระบบโทรศัพท์และระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วยเส้นลวดทองแดงที่มีฉนวนหุ้มจำนวน 2 เส้น นำมาบิดเป็นเกลียวเข้าด้วยกัน โดยทั่วไปสายคู่บิดเกลียวหลายๆ คู่ จะถูกรวมเข้าด้วยกันโดยการพันเป็นสายเคเบิลเพียงเส้นเดียว การบิดเกลียวของเส้นลวดทองแดงที่มีฉนวนหุ้มแต่ละคู่เป็นการลดการแทรกสอดของคลื่นแม่เหล็กไฟฟ้าระหว่างสายแต่ละคู่ เส้นลวดทองแดงที่ใช้มีความหนาตั้งแต่ 0.016-0.036 นิ้ว (วาทิต เบญจพล, 2555, หน้า 52)

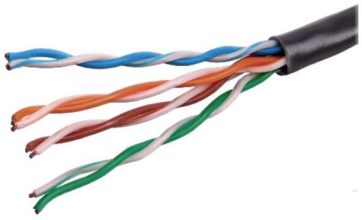
การนำสายคู่บิดเกลียวมาใช้กับระบบโทรศัพท์ เพื่อเชื่อมต่อระหว่างเครื่องโทรศัพท์ที่อยู่บ้านกับผู้ให้บริการระบบโทรศัพท์ สามารถทำได้ในระยะทางหลายกิโลเมตร โดยไม่ต้องใช้อุปกรณ์ทวนสัญญาณ สายคู่บิดเกลียวที่นิยมนำมาใช้ในระบบเครือข่ายคอมพิวเตอร์จะเป็นสายทองแดงหุ้มฉนวนบิดเกลียวพันกันเป็นคู่ ในสายเคเบิล 1 เส้น จะบรรจุสายคู่บิดเกลียวไว้ทั้งหมด 4 คู่ โดยแบ่งสายคู่บิดเกลียวออกเป็น 2 ชนิด คือ สายคู่บิดเกลียวแบบไม่หุ้มชิลด์ (UTP) และสายคู่บิดเกลียวแบบหุ้มชิลด์ (STP) ดังภาพที่ 4.1



ภาพที่ 4.1 แสดงส่วนประกอบของสายคู่บิดเกลียวแบบหุ้มชิลด์ (STP) และแบบไม่หุ้มชิลด์ (UTP)

1. สายคู่บิดเกลียวแบบไม่หุ้มชิลด์ (UTP : Unshielded Twisted Pair)

สายคู่บิดเกลียวหรือ ยูทีพี (UTP) เป็นสายคู่บิดเกลียวที่มีวัสดุฉนวนหรือพลาสติกห่อหุ้มด้านนอกเท่านั้น สามารถส่งได้ทั้งสัญญาณแบบแอนะล็อกและดิจิทัล เป็นสายที่มีราคาถูก มีความยืดหยุ่นในการใช้งาน และติดตั้งง่าย แต่มีประสิทธิภาพสูง นิยมนำมาใช้ในระบบเครือข่ายแลน อีเทอร์เน็ต และโทเค็นริง ดังภาพที่ 4.2



ภาพที่ 4.2 แสดงตัวอย่างสายคู่บิดเกลียวแบบ UTP

2. สายคู่บิดเกลียวแบบหุ้มชิลด์ (STP : Shielded Twisted Pair)

สายคู่บิดเกลียวแบบหุ้มชิลด์หรือ เอสทีพี (SPT) เป็นสายคู่บิดเกลียวที่ภายในจะมีแผ่นโลหะบางๆ ทำหน้าที่เป็นชิลด์ (Shield) ห่อหุ้มอีกชั้นหนึ่ง เพื่อป้องกันสัญญาณรบกวนจากคลื่นแม่เหล็กไฟฟ้า สายเอสทีพีจะมีราคาสูงกว่าสายยูทีพี และสามารถป้องกันสัญญาณรบกวนได้ดีกว่า นิยมใช้ในโรงงานอุตสาหกรรมที่มีสัญญาณรบกวนจากเครื่องจักรต่างๆ

สายคู่บิดเกลียวจะใช้หัวเชื่อมต่อแบบ RJ-45 ที่คล้ายกับหัวเชื่อมต่อกับสายโทรศัพท์ทั่วไป แต่มีขนาดใหญ่กว่า และสามารถเชื่อมสายคู่บิดเกลียวได้ 4 คู่ ซึ่งมีจำนวนมากกว่าสายโทรศัพท์ ดังภาพที่ 4.3

ภาพที่ 4.3 แสดงตัวอย่างสายคู่บิดเกลียวและหัวเชื่อมต่อ RJ-45

มาตรฐานของสายคู่บิดเกลียวถูกจำแนกประเภท เรียกว่า Category หรือ Cat ตามด้วยหมายเลขที่ระบุประเภทของสาย เช่น Category 1 หรือ Cat 1 Category 5 หรือ Cat 5 เป็นต้น มาตรฐานของสายคู่บิดเกลียว แสดงได้ดังตารางที่ 4.1

ตารางที่ 4.1 แสดงมาตรฐานของสายคู่บิดเกลียว

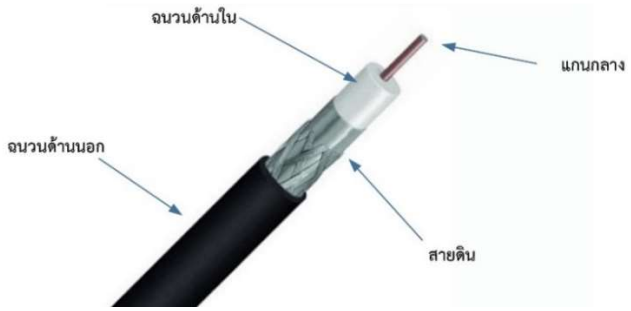
ประเภท	คุณสมบัติ
Category 1/Class A	ใช้ในระบบโทรศัพท์มีอัตราการส่งข้อมูลที่ต่ำมาก และไม่สามารถส่งข้อมูลแบบดิจิทัลได้
Category 2/Class B	สามารถส่งข้อมูลแบบดิจิตอลได้แล้ว แต่ก็มีอัตราการส่งข้อมูลที่ค่อนข้างต่ำ คือ 4 Mbps โดยภายในประกอบด้วยสายคู่บิดเกลียวจำนวน 4 คู่
Category 3/Class C	มีอัตราการส่งข้อมูล 16 Mbps และมีสายคู่บิดเกลียวจำนวน 4 คู่
Category 4	มีอัตราการส่งข้อมูล 20 Mbps และมีสายคู่บิดเกลียวจำนวน 4 คู่
Category 5/Class D	มีอัตราการส่งข้อมูลสูงกว่า 100 Mbps โดยใช้เพียงแค่ 2 คู่สายเท่านั้น อัตราการส่งข้อมูลสูงสุด 1000 Mbps
Category 5e	มีคุณภาพสายที่ดีกว่า Cat 5 ปกติ และรองรับการส่งข้อมูลแบบส่งได้พร้อมกัน (Full-Duplex)
Category 6/Class E	มีอัตราการส่งข้อมูลที่สูงขึ้น รองรับ Bandwidth ได้ ถึง 250 MHz

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 75)

ปัจจุบันมาตรฐานของสายคู่บิดเกลียวที่นิยมนำมาใช้ในระบบเครือข่าย คือ มาตรฐาน Category 5 ซึ่งสายแต่ละคู่จะถูกพันกันถี่ขึ้นเพื่อลดสัญญาณรบกวน และสายทองแดงจะถูกหุ้มด้วยฉนวนที่ทำจากเทฟลอน ซึ่งเป็นวัสดุที่ช่วยลดสัญญาณรบกวนจากสายคู่อื่นๆ ที่อยู่ใกล้เคียงได้เป็นอย่างดี ทำให้ได้คุณภาพของสัญญาณที่ดี และส่งข้อมูลได้สูงถึง 100 Mbps ปัจจุบัน ได้มีการพัฒนาสายสัญญาณมาตรฐานใหม่ที่เรียกว่าว่า Category 7/Class F ซึ่งรองรับแบบมัลติมีเดียได้อย่างเต็มรูปแบบมากขึ้น

4.1.2 สายโคแอ๊กเชียล (Coaxial Cable)

สายโคแอ๊กเชียลหรือเรียกสั้นๆ ว่า สายโคแอ๊ก (Coax) เป็นสายที่มีรูปแบบเรียบง่าย ใช้กับระบบเครือข่ายในยุคแรกๆ โดยโครงสร้างชั้นนอกสุดจะห่อหุ้มด้วยวัสดุที่เป็นฉนวนหรือพลาสติก ซึ่งภายในประกอบด้วยสายทองแดงเป็นแกนกลาง หุ้มด้วยวัสดุที่เป็นฉนวนและมีตัวนำไฟฟ้าที่ทำด้วยใยโลหะบางๆ ถักเป็นตาข่ายหุ้มอยู่ในชั้นถัดไป แกนกลางที่เป็นสายทองแดงจะทำหน้าที่เป็นตัวนำสัญญาณ ส่วนประกอบอื่นๆ จะใช้สำหรับป้องกันสัญญาณรบกวนจากภายนอกและใช้เป็นสายดิน ดังภาพที่ 4.4



ภาพที่ 4.4 แสดงส่วนประกอบของสายโคแอ๊กเชียล

สายโคแอ๊กเชียลเป็นสายสื่อสารที่มีฉนวนห่อหุ้มดีกว่าสายคู่บิดเกลียว ทำให้ส่งข้อมูลได้เร็วและไกลกว่า มาตรฐานของสายโคแอ๊กเชียลจะแตกต่างกันไปตามการใช้งานหรือคุณสมบัติ เมื่อนำไปใช้ในเครือข่ายอีเทอร์เน็ต จะใช้มาตรฐาน RG-58 เป็นต้น มาตรฐานของสายโคแอ๊กเชียลจะใช้คำนำหน้าว่า RG ซึ่งย่อมาจาก Radio Government โดยสามารถแบ่งประเภทของสายโคแอ๊กเชียลได้ แสดงได้ดังตารางที่ 4.2

ตารางที่ 4.2 แสดงประเภทของสายโคแอ๊กเชียล

ประเภท	ลักษณะการใช้งาน
RG-6/U	สูญเสียสัญญาณน้อยเมื่อใช้กับคลื่นความถี่สูง ใช้เป็นสายเคเบิลทีวีและสายเคเบิลโมเด็ม
RG-8/U	ใช้ใน Thick Ethernet (10Base5) และคลื่นวิทยุสมัครเล่น
RG-11/U	ใช้ใน Thick Ethernet
RG-58/U	ใช้ในวิทยุสื่อสาร วิทยุสมัครเล่น และ Thin Ethernet (10Basee2)
RG/62	ใช้ในเครือข่าย ArcNet

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 77)

ส่วนประกอบที่สำคัญของการใช้งานสายโคแอ๊กเชียล คือ หัวเชื่อมต่อ (Connector) โดยหัวเชื่อมต่อที่นิยมนำมาใช้ คือ หัวเชื่อมต่อแบบ BNC ซึ่งมีหลายลักษณะ ดังนี้

1. หัวเชื่อมต่อสาย BNC ใช้สำหรับเชื่อมต่อเข้ากับสาย ดังภาพที่ 4.5

ภาพที่ 4.5 แสดงหัวเชื่อมสาย BNC

2. หัวเชื่อมต่อสาย BNC แบบ Barrel ใช้สำหรับเชื่อมต่อระหว่างสายให้มีความยาวมากขึ้น ดังภาพที่ 4.6

ภาพที่ 4.6 แสดงหัวเชื่อมสาย BNC แบบ Barrel

3. หัวเชื่อมต่อสาย BNC แบบตัว T ใช้สำหรับเชื่อมต่อระหว่างสายกับ Network Card ดังภาพที่ 4.7

ภาพที่ 4.7 แสดงหัวเชื่อมสาย BNC แบบตัว T

4. หัวเชื่อมสายจุดสิ้นสุดสัญญาณ (Terminator) ใช้สำหรับเชื่อมต่อที่ปลายสายเพื่อเป็นตัวดูดซับสัญญาณไม่ให้เกิดการสะท้อนกลับไปยังต้นทาง ซึ่งจำเป็นในโครงสร้างเครือข่ายแบบบัส เนื่องจากจะช่วยป้องกันสัญญาณรบกวนในเส้นทางการเชื่อมโยงหลัก (Backbone) ดังภาพที่ 4.8

ภาพที่ 4.8 แสดงหัวเชื่อมสายจุดสิ้นสุดสัญญาณ

สายโคแอ็กเชียลที่นิยมใช้กันมีอยู่ 2 ชนิด โดยแบ่งตามเทคโนโลยีของสัญญาณที่ใช้ขนส่ง คือ Baseband Coaxial และ Broadband Coaxial

1. Baseband Coaxial หรือสายโคแอ็กเชียลแบบช่วงสัญญาณแคบ มีความต้านทาน 50 โอห์ม ใช้สำหรับส่งข้อมูลแบบดิจิทัล โดยทั่วไปนำไปใช้เชื่อมต่อระหว่างฮับที่อยู่ในเครือข่ายแลน

2. Broadband Coaxial หรือสายโคแอ็กเชียลแบบช่วงสัญญาณกว้าง มีความต้านทาน 75 โอห์ม ใช้สำหรับส่งข้อมูลแบบแอนะล็อก นิยมใช้เป็นสายเคเบิลในระบบเคเบิล

ทีวี โดยสามารถครอบคลุมพื้นที่ได้มากกว่าการใช้สายโคแอ็กเชียลแบบช่วงสัญญาณแคบ แต่จำเป็นต้องใช้อุปกรณ์ขยายสัญญาณ

นอกจากนี้สายโคแอ็กเชียลยังสามารถแบ่งประเภทได้ตามลักษณะทางกายภาพของสาย โดยแบ่งออกเป็น 2 ประเภท ดังนี้

1. สายโคแอ็กเชียลแบบบาง (Thin Coaxial Cable)

เป็นสายที่มีขนาดเล็ก มีความต้านทาน 50 โอห์ม ขนาดเส้นผ่าศูนย์กลางไม่เกิน 0.64 มิลลิเมตร นำไปใช้งานกับเครือข่ายได้เกือบทุกประเภท เนื่องจากมีขนาดเล็กและมีความยืดหยุ่นสูง ส่งข้อมูลได้ระยะสูงสุดไม่เกิน 185 เมตร สายประเภทนี้มีแกนกลางอยู่ 2 ประเภท คือ แกนกลางแบบสายทองแดงเส้นเดียว กับแกนกลางแบบเส้นใยโลหะหลายเส้น

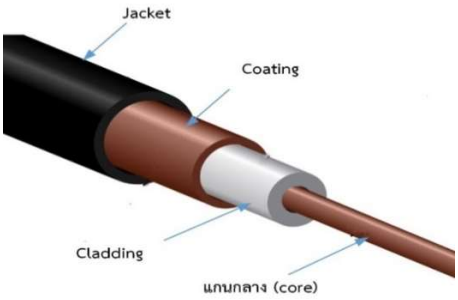
2. สายโคแอ็กเชียลแบบหนา (Thick Coaxial Cable)

เป็นสายที่มีขนาดหนากว่าแบบแรก ค่อนข้างแข็ง มีขนาดเส้นผ่าศูนย์กลางประมาณ 1.27 เซนติเมตร จึงส่งข้อมูลได้ไกลกว่าสายโคแอ็กเชียลแบบบาง โดยมีระยะทางสูงสุดไม่เกิน 500 เมตร ในระบบเครือข่ายคอมพิวเตอร์ยุคแรกๆ จะใช้สายประเภทนี้เพื่อเชื่อมต่อเส้นทางข้อมูลหลักหรือ Backbone แต่ในปัจจุบันไม่มีการนำสายประเภทนี้มาใช้งานแล้ว นิยมใช้สายใยแก้วนำแสงแทน

4.1.3 สายใยแก้วนำแสง (Fiber-Optic Cable)

สายใยแก้วนำแสง (Fiber-Optic Cable) เป็นสายสัญญาณที่ขนส่งข้อมูลด้วยสัญญาณแสง โดยอาศัยคุณสมบัติด้านการหักเหและการสะท้อนของแสง กล่าวคือ เมื่อแสงเกิดการหักเหด้วยมุมหรือองศาที่เหมาะสมจะทำให้ควบคุมและแบ่งช่องสัญญาณได้ตามองศาที่เกิดการหักเห การสะท้อนก็เป็นตัวช่วยให้แสงเดินทางไปบนสายใยแก้วนำแสงได้ โดยอาศัยหลักการสะท้อน คือ มุมตกระทบเท่ากับมุมสะท้อน การส่งข้อมูลของสายใยแก้วนำแสงจะเป็นแบบทิศทางเดียว (One-Way) หากต้องการส่งข้อมูลแบบไปกลับหรือสองทิศทาง (Two-Way) จะต้องใช้สายใยแก้วนำแสงจำนวน 2 เส้น

สายใยแก้วนำแสงประกอบด้วนส่วนแกนกลาง (Core) ซึ่งอยู่ด้านในสุดทำหน้าที่นำสัญญาณแสง ชั้นแรกถูกหุ้มด้วย Cladding และชั้นที่สองหุ้มด้วย Coating ซึ่งวัสดุแต่ละส่วนจะมีค่าการหักเหของแสงที่แตกต่างกัน วัสดุทั้งสองส่วนที่ห่อหุ้มแกนกลางไว้จะทำหน้าที่เป็นตัวหักเหของแสงเงาทำให้เกิดการสะท้อนกลับหมด ดังนั้น แสงจะเดินทางอยู่ภายในส่วนแกนกลางเท่านั้น นอกจากนี้ด้านนอกสุดยังถูกห่อหุ้มด้วย Jacket ซึ่งเป็นวัสดุป้องกันใยแก้วนำแสงที่อยู่ด้านในอีกด้วย ดังภาพที่ 4.9



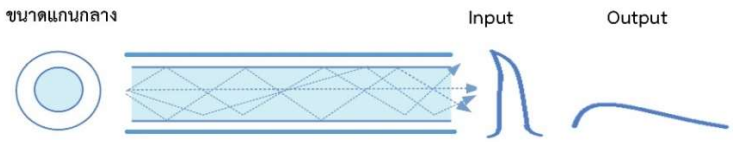
ภาพที่ 4.9 แสดงส่วนประกอบของสายใยแก้วนำแสง
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 77)

สายใยแก้วนำแสง แบ่งตามความสามารถในการนำแสง ออกเป็น 2 ชนิด คือ สายใยแก้วนำแสงชนิดหลายโหมด (Multimode Fiber) และชนิดโหมดเดียว (Singlemode Fiber) ดังนี้

1. สายใยแก้วนำแสงชนิดหลายโหมด (Multimode Fiber)

เป็นการใช้ลำแสงมากกว่าหนึ่งลำแสง โดยนำมาหักเหและสะท้อนด้วยมุมองศาที่แตกต่างกัน ซึ่งลำแสงแต่ละเส้นจะเกิดการสะท้อนและเดินทางด้วยรูปแบบที่แตกต่างกันโดยสิ้นเชิง ลักษณะการเดินทางของลำแสงนี้แบ่งได้ 2 แบบ คือ

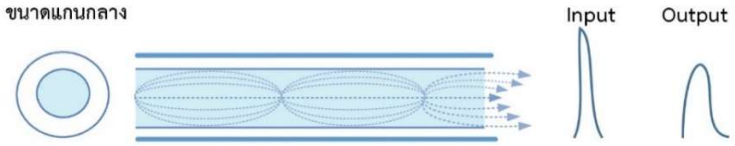
1.1 Multimode Step-Index Fiber เป็นการใช้แต่ละลำแสงเดินทางด้วยมุมหักเหแตกต่างกันอย่างไม่เป็นระเบียบ โดยลำแสงจะมีมุมหักเหที่แตกต่างกันโดยสิ้นเชิง ทำให้การรับส่งข้อมูลมีความคลาดเคลื่อนสูง ดังภาพที่ 4.10



ภาพที่ 4.10 แสดงสายใยแก้วนำแสง Multimode แบบ Step-Index
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 78)

1.2 Multimode Graded-Index Fiber เป็นการกำหนดมุมหักเหของแต่ละลำแสงเรียงตามลำดับอย่างเป็นระเบียบ โดยลำแสงจะมีการเปลี่ยนแปลงของมุมอย่างชัดเจน ทำให้ต้องใช้แกนกลางที่มีขนาดใหญ่ เพื่อให้การกำหนดค่าการหักเหทำได้ใกล้เคียงกัน

มากที่สุด และง่ายต่อการรวบรวมข้อมูลที่ปลายทาง ซึ่งวิธีการนี้จะมีประสิทธิภาพมากกว่าแบบ Multimode Step-Index Fiber ดังภาพที่ 4.11



ภาพที่ 4.11 แสดงสายใยแก้วนำแสง Multimode แบบ Graded-Index
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 79)

2. สายใยแก้วนำแสงชนิดโหมดเดียว (Singlemode Fiber)

เป็นการใช้ลำแสงเพียงลำแสงเดียวเพื่อขนส่งข้อมูลไปยังปลายทาง แต่จะต้องมีแหล่งกำเนิดแสงที่มีความเข้มสูงอยู่ในมุมขนานกับส่วนแกนกลางให้มากที่สุด กล่าวคือจะให้ลำแสงเดินทางภายในใยแก้วนำแสงเป็นเส้นตรง ลักษณะดังกล่าวทำให้แกนกลางของสายประเภทนี้มีขนาดเล็กกว่าสายประเภทอื่น โดยจะให้ลำแสงเดินทางกายในสายใยแก้วนำแสงได้เพียง 1 ลำแสง ทำให้การรับและรวบรวมข้อมูลทำได้ง่ายขึ้น เนื่องจากลำแสงจะไม่กระจัดกระจาย และการรับส่งข้อมูลมีความรวดเร็วกว่าแบบ Multimode Fiber ดังภาพที่ 4.12

ภาพที่ 4.12 แสดงสายใยแก้วนำแสง Singlemode
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 79)

หัวเชื่อมต่อกับสายใยแก้วนำแสงก็เป็นสิ่งสำคัญเพราะหัวเชื่อมต่อแต่ละประเภทจะมีความเหมาะสมกับชนิดของสายใยแก้วนำแสงแตกต่างกัน หัวเชื่อมต่อบางแบบนิยมใช้กับสายใยแก้วนำแสงแบบ Multimode หรือบางแบบอาจเหมาะกับ Singlemode นอกจากหัวเชื่อมต่อแล้วแหล่งกำเนิดแสงก็เป็นสิ่งที่ขาดไม่ได้ในการใช้สายใยแก้วนำแสง เช่น แอลอีดี (Light-Emitting Diode : LED) เป็นต้น แอลอีดีเป็นแหล่งกำเนิดแสงที่มีราคาถูก ลำแสงที่ได้ก็จะมีประสิทธิภาพไม่สูงมากนัก ข้อจำกัดของแอลอีดีคือการควบคุมมุมหักเหทำได้ยากและลำแสง

แตกกระจายได้ง่ายหากใช้ในระยะทางไกล ทำให้การใช้แอลอีดีสามารถส่งข้อมูลได้ในระยะสั้น ดังภาพที่ 4.13

ภาพที่ 4.13 แสดงตัวอย่างหัวเชื่อมต่อของสายใยแก้วนำแสง

ข้อดีของสายใยแก้วนำแสง มีดังนี้

1. ปลอดภัยจากสัญญาณรบกวน เนื่องจากคลื่นแม่เหล็กไฟฟ้าไม่มีผลกระทบต่อสัญญาณแสง

2. สัญญาณแสงเดินทางได้ในระยะทางที่ไกลกว่าสายสัญญาณประกอบอื่นและสัญญาณอ่อนกำลังยาก จึงไม่จำเป็นต้องอาศัยอุปกรณ์ขยายสัญญาณ

3. รองรับปริมาณการขนส่งข้อมูลได้มากกว่าสายประเภทอื่น

ข้อเสียของสายใยแก้วนำแสง มีดังนี้

1. เป็นสายสัญญาณที่มีราคาสูง นอกจากนี้แหล่งกำเนิดสัญญาณแสงยังมีราคาสูงกว่าแหล่งกำเนิดสัญญาณไฟฟ้าหลายเท่าตัว

2. การติดตั้งค่อนข้างยากและซับซ้อน ต้องใช้บุคลากรที่เชี่ยวชาญ

3. เกิดความเสียหายได้ง่ายกว่าสายประเภทอื่น ทำให้ต้องดูแลและบำรุงรักษาเป็นอย่างดี

4.2 สื่อกลางแบบไร้สาย

สื่อกลางแบบไร้สาย (Unguided Media) ใช้สำหรับขนส่งข้อมูลทางกายภาพด้วยคลื่นหรือสัญญาณที่เดินทางในอากาศ โดยไม่ใช้สายสัญญาณเป็นตัวข้อมูล และสื่อกลางประเภทนี้ไม่สามารถกำหนดเส้นทางของข้อมูลได้ (Unguided Media) ตัวอย่างของระบบที่ใช้สื่อกลางแบบไร้สาย ได้แก่ การสื่อสารด้วยคลื่นวิทยุ การสื่อสารผ่านระบบดาวเทียม ระบบโทรศัพท์ไร้สาย ระบบอินฟราเรด และบลูทูธ เป็นต้น การส่งข้อมูลผ่านสื่อกลางแบบไร้สายเริ่มต้นจากระบบ AM

Radio, FM Radio และการส่งสัญญาณโทรทัศน์ในปี ค.ศ.1950 ต่อมาได้มีการพัฒนาระบบดาวเทียมขึ้นในปี ค.ศ.1962 และการส่งข้อมูลผ่านสื่อกลางแบบไร้สายยังได้รับการพัฒนามาจนถึงปัจจุบัน

การส่งข้อมูลแบบไร้สายจะใช้การเปลี่ยนแปลงของคลื่นแม่เหล็กไฟฟ้า (Electromagnetic Wave) ที่เกิดจากการเคลื่อนที่ของอิเล็กตรอนในการส่งสัญญาณ ซึ่งคลื่นแม่เหล็กไฟฟ้าสามารถเดินทางไปยังสถานที่ต่างๆ ได้อย่างอิสระ และสามารถส่งสัญญาณได้ไกลจนถึงอวกาศ โดยคลื่นแม่เหล็กไฟฟ้าจะมีจำนวนคลื่นที่เกิดขึ้นในเวลา 1 วินาที หรือความถี่คลื่น (Frequency) แตกต่างกัน เมื่อคลื่นแม่เหล็กไฟฟ้าเดินทางผ่านตัวกลางที่เป็นสายทองแดงหรือสายใยแก้วนำแสง จะมีความเร็วลดลงและแต่ละความถี่จะมีความเร็วไม่เท่ากันด้วย ตัวอย่างช่วงคลื่นความถี่ที่นำมาใช้ในการส่งสัญญาณต่างๆ ดังภาพที่ 4.14 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 80-88)

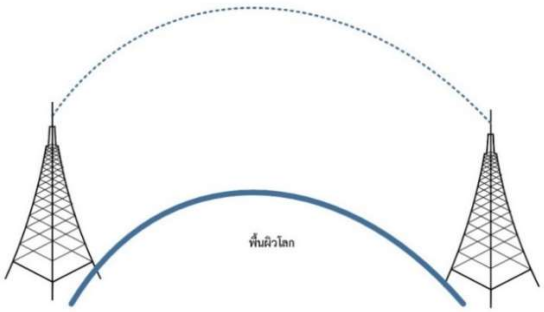
ภาพที่ 4.14 แสดงความถี่ของคลื่นแม่เหล็กไฟฟ้าที่ถูกนำมาใช้งาน
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 81)

4.2.1 การสื่อสารด้วยคลื่นวิทยุ (Radio Wave)

การสร้างคลื่นวิทยุเพื่อใช้ส่งสัญญาณสามารถทำได้ง่าย และครอบคลุมระยะทางไกล นอกจากนี้คลื่นวิทยุยังเดินทางออกจากแหล่งกำเนิดคลื่นแบบกระจายไปทุกทิศทาง และสามารถทะลุวัตถุทึบแสงได้ดี ทำให้คลื่นวิทยุได้รับความนิยมในการนำมาใช้เพื่อส่งสัญญาณกันอย่างแพร่หลาย แต่คลื่นวิทยุก็มีข้อเสีย คือ หากใช้คลื่นความถี่ต่ำกำลังของสัญญาณจะลดลงอย่างรวดเร็ว แต่สามารถทะลุวัตถุทึบแสงได้เป็นอย่างดี หากใช้ความถี่สูงจะส่งสัญญาณได้ไกลแต่เมื่อพบวัตถุทึบแสง สัญญาณจะถูกสะท้อนกลับ และอาจถูกรบกวนด้วยคลื่นแม่เหล็กไฟฟ้าหรือคลื่นรบกวนต่างๆ ได้ง่าย เช่น ฝนตก ฟ้าผ่า หรือคลื่นรบกวนจากเครื่องใช้ไฟฟ้า เป็นต้น

การสื่อสารด้วยคลื่นวิทยุสามารถทำได้ 3 ลักษณะ ดังนี้

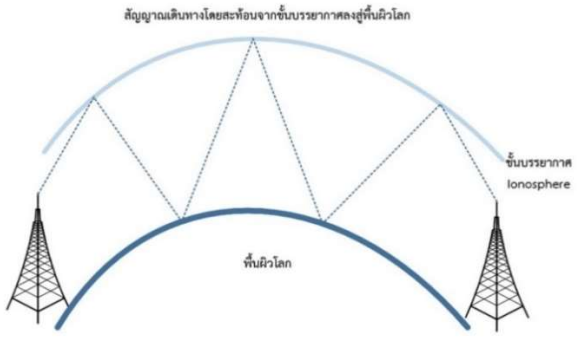
1. คลื่นดิน (Ground Wave) เป็นการส่งคลื่นวิทยุที่อยู่ในช่วงความถี่ไม่เกิน 2 MHz ซึ่งคลื่นวิทยุจะเดินทางขนานตามแนวโค้งของพื้นโลกอยู่ในชั้นบรรยากาศโทรโพสเฟียร์ (Troposphere) การส่งคลื่นวิทยุแบบนี้จะได้รับผลกระทบจากปรากฏการณ์ทางธรรมชาติโดยตรง เช่น ฟ้าผ่า และอุณหภูมิ เป็นต้น ซึ่งทำให้เกิดสัญญาณรบกวนต่างๆ ขึ้น การส่งคลื่นวิทยุลักษณะดังกล่าวที่รู้จักกันดี คือ คลื่นวิทยุ FM ดังภาพที่ 4.15



ภาพที่ 4.15 แสดงการสื่อสารคลื่นวิทยุแบบ Ground Wave

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 82)

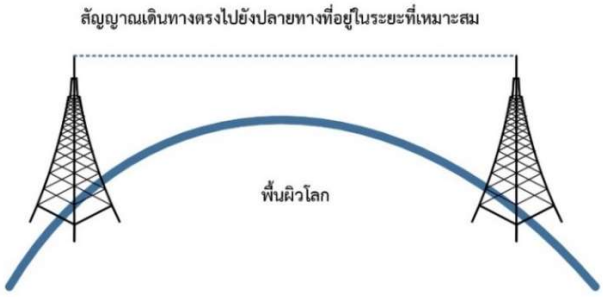
2. คลื่นฟ้า (Sky Wave) เป็นการส่งคลื่นวิทยุที่อยู่ในช่วงความถี่ระหว่าง 2-3 MHz ซึ่งคลื่นวิทยุจะเดินทางไปถึงชั้นบรรยากาศไอโอโนสเฟียร์ (Ionosphere) โดยจะสะท้อนกลับมายังพื้นโลก และสะท้อนกลับขึ้นไประหว่างชั้นบรรยากาศกับพื้นโลกจนถึงปลายทาง การส่งคลื่นวิทยุแบบนี้สามารถส่งได้ถึง 1,000 กิโลเมตร ดังภาพที่ 4.16



ภาพที่ 4.16 แสดงการสื่อสารคลื่นวิทยุแบบ Sky Wave

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 83)

3. คลื่นอวกาศ (Space Wave) เป็นการส่งคลื่นวิทยุที่อยู่ในช่วงความถี่มากกว่า 30 MHz ขึ้นไป ซึ่งคลื่นวิทยุจะเดินทางเป็นเส้นตรงจากจุดหนึ่งไปยังอีกจุดหนึ่งที่ไม่เกินกว่าแนวโค้งของผิวโลก คือ ต้นทางกับปลายทางต้องอยู่บนพื้นผิวโลกระดับเดียวกัน หรืออยู่ในระดับสายตานั่นเอง การส่งคลื่นวิทยุแบบนี้จะมีความถี่สูง ทำให้ไม่ถูกสะท้อนกลับมาจากชั้นบรรยากาศไอโอโนสเฟียร์ (Ionosphere) จึงใช้ส่งสัญญาณจากพื้นโลกไปยังดาวเทียมได้ ดังภาพที่ 4.17



ภาพที่ 4.17 แสดงการสื่อสารคลื่นวิทยุแบบ Line-of-Sight
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 83)

ช่วงความถี่ของคลื่นวิทยุที่ใช้ในการติดต่อสื่อสารจะอยู่ระหว่าง 3 KHz ถึง 300 GHz โดยแบ่งออกเป็น 8 ช่วง ดังนี้

1. VLF (Very Low Frequency) อยู่ในช่วงความถี่ต่ำระหว่าง 3-30 KHz ซึ่งการส่งคลื่นในช่วงนี้จะทำได้ในอากาศระดับพื้นผิวโลก การส่งข้อมูลด้วยความถี่ VLF จะได้รับผลกระทบโดยตรงจากสัญญาณรบกวนที่เกิดจากธรรมชาติ เช่น ความร้อน และคลื่นไฟฟ้าที่เกิดจากฟ้าผ่า เป็นต้น VLF จะใช้สำหรับการติดต่อสื่อสารวิทยุทางไกลที่ใช้ในทางทหาร

2. LF (Low Frequency) อยู่ในช่วงความถี่ต่ำระหว่าง 30-300 KHz มีความสามารถเหมือนกับ VLF และถูกรบกวนจากสัญญาณรบกวนทางธรรมชาติได้ง่ายเช่นกัน นิยมนำมาใช้ในการติดต่อสื่อสารวิทยุทางไกลที่ใช้ในทางทหาร

3. MF (Middle Frequency) อยู่ในช่วงความถี่ระหว่าง 300 KHz ถึง 3 MHz เป็นความถี่ที่เดินทางถึงชั้นบรรยากาศโทรโพสเฟียร์ (Troposphere) ซึ่งเป็นชั้นบรรยากาศที่อยู่ล่างสุด MF มีระยะทางในการส่งที่จำกัด เนื่องจากหากส่งในระยะทางไกล คลื่นต้องเดินทางเข้าสู่ชั้นบรรยากาศไอโอโนสเฟียร์ (Ionosphere) จะทำให้สัญญาณถูกดูดซับไปในชั้นบรรยากาศจนหมด ความถี่ระดับกลางนี้นิยมใช้กับสัญญาณวิทยุคลื่น AM

4. HF (High Frequency) อยู่ในช่วงความถี่ระดับสูงระหว่าง 3-30 MHz เป็นความถี่ที่เดินทางไปถึงชั้นบรรยากาศไอโอโนสเฟียร์ (Ionosphere) เมื่อคลื่นเดินทางถึงระดับชั้นบรรยากาศนี้ คลื่นจะสะท้อนกลับมายังพื้นโลก HF เป็นช่วงความถี่ที่ใช้ในด้านต่างๆ เช่น วิทยุสมัครเล่น วิทยุชุมชน (Citizen's Band หรือ CB) การสื่อสารระยะไกลทางทหาร โทรเลข และโทรศัพท์ เป็นต้น

5. VHF (Very High Frequency) อยู่ในช่วงความถี่ระดับสูงระหว่าง 30-300 MHz ใช้วิธีการส่งข้อมูลในลักษณะของคลื่นอวกาศ หรือ Line-of-Sight เช่น คลื่นวิทยุ FM และสัญญาณทีวีย่านความถี่ VHF เป็นต้น

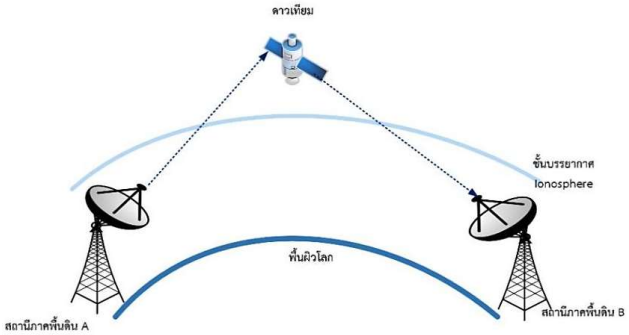
6. UHF (Ultrahigh Frequency) อยู่ในช่วงความถี่ระดับ 300 MHz ถึง 3 GHz ใช้ในการส่งลักษณะ Line-of-Sight เช่น สัญญาณทีวีย่าน UHF โทรศัพท์ไร้สาย และคลื่นไมโครเวฟ เป็นต้น

7. SHF (Super High Frequency) อยู่ในช่วงความถี่ระดับสูงระหว่าง 3-30 GHz ใช้ในการส่งสัญญาณลักษณะ Line-of-Sight บางครั้งก็ใช้ในการส่งสัญญาณทะลุชั้นบรรยากาศเพื่อใช้ในการสื่อสารผ่านดาวเทียมทางการทหาร นอกจากนี้ยังใช้เพื่อส่งสัญญาณผ่านดาวเทียม และการติดต่อสื่อสารด้วยเรดาร์ (Radar) เป็นต้น

8. EHF (Extremely High Frequency) อยู่ในช่วงความถี่ระดับสูงระหว่าง 30-300 GHz ใช้ในการส่งสัญญาณทะลุชั้นบรรยากาศ เช่น การติดต่อสื่อสารด้วยเรดาร์ (Radar) สื่อสารผ่านดาวเทียม และใช้ในการค้นคว้าวิจัยทางด้านวิทยาศาสตร์ เป็นต้น

4.2.2 การสื่อสารผ่านดาวเทียม (Satellite Communication)

การสื่อสารผ่านดาวเทียมจะใช้คลื่นไมโครเวฟ (Microwave) ที่มีความถี่คลื่นอยู่ในช่อง EHF ซึ่งเป็นความถี่ระดับสูงระหว่าง 30-300 GHz คลื่นนี้สามารถเดินทางผ่านชั้นบรรยากาศไอโอโนสเฟียร์ โดยทำการส่งสัญญาณทะลุออกไปยังนอกชั้นของบรรยากาศ มีปลายทางอยู่ที่ดาวเทียมที่โคจรอยู่รอบโลก ซึ่งเป็นตัวกลางในการรับสัญญาณจากผู้ส่งและทำการส่งต่อไปยังปลายทาง อุปกรณ์ที่ใช้ในการรับส่งสัญญาณที่พื้นผิวโลก คือ จานรับสัญญาณ (Antennas) สำหรับการติดต่อสื่อสารผ่านดาวเทียมจำเป็นต้องอาศัยดาวเทียมที่โคจรรอบโลกเป็นตัวกลางในการรับและส่งต่อสัญญาณ ดังภาพที่ 4.18



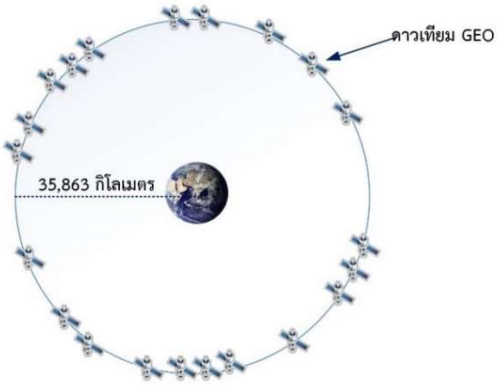
ภาพที่ 4.18 แสดงการสื่อสารผ่านดาวเทียม

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 84)

ดาวเทียมที่ใช้ในการติดต่อสื่อสาร สามารถแบ่งตามระดับความสูงของพื้นโลก ได้ดังนี้

1. Geostationary Satellites (GEO)

เป็นดาวเทียมที่มีโคจรรอบโลกสูงจากพื้นโลก 35,863 กิโลเมตร เรียกสั้นๆ ว่า GEO Satellites ซึ่งโคจรอยู่รอบโลกโดยนำโดยทำมุมที่องศาเดิมกับโลกเสมอและเคลื่อนที่ไปพร้อมกับการหมุนของโลก ทำให้ตำแหน่งดาวเทียม GEO จะอยู่จุดเดิมเสมอ สถานีภาคพื้นดิน (Earth Station) สามารถค้นหาดาวเทียม GEO เพื่อส่งสัญญาณได้ง่ายและไม่จำเป็นต้องเปลี่ยนคลื่นความถี่ให้ยุ่งยาก เนื่องจากดาวเทียม GEO ไม่เคลื่อนออกจากตำแหน่งเดิม แต่ด้วยระดับความสูงที่ค่อนข้างมากอาจทำให้เกิดปัญหาสัญญาณอ่อนระหว่างส่ง ดังภาพที่ 4.19



ภาพที่ 4.19 แสดงดาวเทียม GEO

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 85)

2. Low-Earth-Orbiting Satellites (LEO)

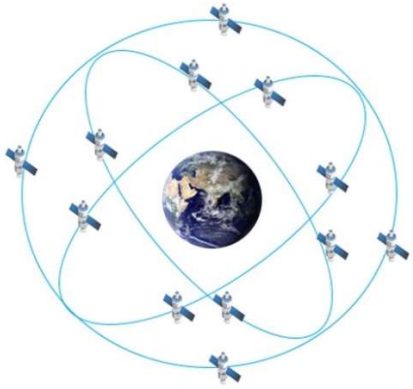
ดาวเทียม LEO Satellites เป็นดาวเทียมที่โคจรอยู่ในระดับความสูงจากพื้นโลก 500-1,500 กิโลเมตร ซึ่งเป็นดาวเทียมที่โคจรอยู่ในระดับต่ำ การเคลื่อนที่ของดาวเทียมจึงค่อนข้างเร็วทำให้ต้องมีการเปลี่ยนแปลงความถี่ของคลื่นสัญญาณทุกครั้ง ในการส่งข้อมูลระหว่างสถานีภาคพื้นดินอาจมีการใช้ดาวเทียม LEO มากกว่า 2 ดวง เนื่องจากดาวเทียม LEO จะเคลื่อนที่เปลี่ยนตำแหน่งไปรอบโลกด้วยความเร็ว ดังนั้น จึงต้องมีการเปลี่ยนดาวเทียมที่เป็นตัวกลางในการรับส่งข้อมูลเสมอ ด้วยระดับความเร็วสูงที่ไม่มากของดาวเทียม LEO ทำให้การส่งสัญญาณทำได้รวดเร็วและมีความเข้มของสัญญาณมากแต่ก็จำเป็นต้องเปลี่ยนความถี่ในการส่งอยู่ตลอดเวลา ดังภาพที่ 4.20

ภาพที่ 4.20 แสดงดาวเทียม LEO

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 86)

3. Middle-Earth-Orbiting Satellites (MEO)

ดาวเทียม MEO Satellites เป็นดาวเทียมที่มีวงโคจรอยู่ในระดับกลางมีความสูงจากพื้นโลก 5,000-18,000 กิโลเมตร มีการเคลื่อนที่ด้วยความเร็วไม่มากนักจึงไม่ต้องเปลี่ยนคลื่นความถี่บ่อยครั้งเท่ากับดาวเทียม LEO แต่ต้องใช้กำลังในการส่งสัญญาณมากกว่าดาวเทียม LEO ดังภาพที่ 4.21



ภาพที่ 4.21 แสดงดาวเทียม MEO

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 86)

4.2.4 ระบบโทรศัพท์ไร้สาย (Cellular Phone)

ระบบโทรศัพท์ไร้สายจะใช้การรับส่งสัญญาณจากเสาสัญญาณที่เชื่อมโยงกันเป็นเครือข่ายโทรศัพท์ไร้สาย โดยแต่ละหน่วยของเครือข่ายของโทรศัพท์ไร้สาย เรียกว่า **เซลล์** (Cell) โดยเซลล์จะถูกควบคุมโดย MTSO (Mobile Telephone Switching Office) ซึ่งเป็นสถานีย่อยในการติดต่อระหว่างเซลล์กับศูนย์กลางเครือข่ายโทรศัพท์มือถือ หากการติดต่อสื่อสารระหว่างเซลล์มีการเปลี่ยนแปลงตำแหน่งของผู้รับหรือผู้ส่ง เคลื่อนที่จากเซลล์หนึ่งไปยังอีกเซลล์หนึ่ง ทำให้สัญญาณจากเซลล์เดิมอ่อนลง MTSO จะทำการสร้างเซลล์ใหม่ที่กำลังเคลื่อนที่เข้าใกล้เพื่อให้สัญญาณในการติดต่อชัดเจนมากขึ้น โดยไม่ทำให้การติดต่อสื่อสารในระหว่างนั้นขาดหาย การเปลี่ยนแปลงดังกล่าว เรียกว่า Handoff

4.2.5 อินฟราเรด (Infrared)

อินฟราเรดเป็นการติดต่อแบบไร้สายโดยอาศัยคลื่นแม่เหล็กไฟฟ้ารูปแบบหนึ่งที่เรียกว่า แสงอินฟราเรด (Infrared) มีความยาวคลื่นมากกว่าแสงที่มองเห็นได้ (Visible Light) แต่น้อยกว่าคลื่นวิทยุ ทำให้ไม่สามารถมองเห็นได้ด้วยตาเปล่า นอกจากนี้ยังไม่สามารถเดินทางผ่านวัตถุทึบแสงได้ และใช้ในการติดต่อสื่อสารระยะไกล เช่น รีโมทควบคุมอุปกรณ์ต่างๆ จุดเด่นของแสงอินฟราเรด คือ ราคาถูก ง่ายต่อการผลิตและเดินทางเป็นเส้นตรง อินฟราเรดนิยมนำมาใช้กับการติดต่อสื่อสารในเครือข่ายส่วนบุคคลหรือเชื่อมต่อระหว่างอุปกรณ์ 2 ชิ้น

แสงอินฟราเรดยังสามารถนำมาใช้ในงานด้านอื่นได้ทั้งด้านการทหาร และการแพทย์ เช่น ใช้เพื่อตรวจมะเร็งเต้านม หรือ กล้องจับความร้อนด้วยคลื่นอินฟราเรด เป็นต้น

4.2.6 บลูทูธ (Bluetooth)

บูลทูธเป็นการติดต่อสื่อสารแบบไร้สายที่ถูกพัฒนาขึ้นเพื่อใช้ในการเชื่อมต่อระหว่างอุปกรณ์อิเล็กทรอนิกส์โดยเฉพาะอุปกรณ์ขนาดเล็กที่พกพาได้ บลูทูธปัจจุบัน รุ่น 5.3 มีความเร็วสูงสุด 2 Mbps ส่งข้อมูลได้ในระยะ 240 เมตร บลูทูธ 5.3 มีการปรับปรุงการทำงานของ Bluetooth Basic Rate / Enhanced Data Rate (BR/EDR) ตัวคอนโทรลเลอร์ที่ทำหน้าที่จัดการกับขนาดของ Encryption Key ในขั้นตอนการจับคู่การเชื่อมต่อด้วยการกำหนดขนาดขั้นต่ำของ Key ที่รองรับได้ ช่วยให้ขั้นตอนการเข้ารหัสมีความยืดหยุ่นมากขึ้น ช่วยให้เครื่องโฮสต์สามารถเลือกใช้งานระดับความปลอดภัยที่เหมาะสมกับประเภทของข้อมูลที่มีการแลกเปลี่ยน โดยอ้างอิงกับมาตรฐานความปลอดภัย บลูทูธ 5.3 สามารถสื่อสารกับอุปกรณ์ที่เป็นโฮสต์ ด้วยความถี่จริงของอุปกรณ์เสริมเพื่อหลีกเลี่ยงการถูกรบกวนสัญญาณ และเพื่อเสถียรภาพในการเชื่อมต่อ และมีคุณสมบัติ Periodic Advertising Enhancements ที่ช่วยลดความซับซ้อนในการแลกเปลี่ยนข้อมูลระหว่างตัวอุปกรณ์ เพราะตามปกติแล้ว อุปกรณ์ Bluetooth จะมีการส่งข้อมูลเดิมซ้ำ ๆ เพื่อตรวจเช็คความน่าเชื่อถือ แต่ใน Bluetooth 5.3 ใช้เทคนิคใหม่ที่จะตรวจสอบเพียงครั้งเดียว ตัดขั้นตอนการตรวจสอบซ้ำที่ไม่จำเป็นทิ้งไป ช่วยให้ประหยัดพลังงาน และยืดอายุการทำงานของแบตเตอรี่ (https://tips.thaiware.com/2467.html) อุปกรณ์ที่นิยมใช้บลูทูธ เช่น โทรศัพท์มือถือ เครื่องคอมพิวเตอร์ โน๊ตบุ๊ค และ PDA ดังภาพที่ 4.22

ภาพที่ 4.22 แสดงตัวอย่างอุปกรณ์ที่ใช้การขนส่งข้อมูลแบบบลูทูธ 5.3
ที่มา : (https://www.lazada.co.th/)

4.3 ปัจจัยที่ส่งผลกระทบต่อการเลือกใช้สื่อกลาง

สิ่งสำคัญในการออกแบบและปรับปรุงระบบเครือข่ายคอมพิวเตอร์ให้มีประสิทธิภาพ คือ การเลือกชนิดของสื่อกลางสำหรับส่งข้อมูล โดยมีปัจจัยต่างๆ ที่ต้องพิจารณา ดังนี้ (สุธี พงศา-สกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 88-89)

1. ค่าใช้จ่าย (Cost) ชนิดของสื่อกลางที่นำมาใช้จะมีผลโดยตรงต่อค่าใช้จ่ายในการนำระบบเครือข่ายมาใช้งาน เช่น สายคู่บิดเกลียวจะมีราคาถูกกว่าสายใยแก้วนำแสง และสายโคแอ๊กเชียล ดังนั้น การเลือกสื่อกลางที่เหมาะสมจะช่วยให้ค่าใช้จ่ายในการติดตั้งระบบลดลง แต่ควรพิจารณาด้วยว่าอุปกรณ์ต่างๆ ที่มีอยู่สามารถรองรับสื่อกลางประเภทใดได้บ้าง และอุปกรณ์ประเภทใดที่ต้องใช้อัตราการรับส่งข้อมูลสูง แล้วนำปัจจัยเหล่านี้มาพิจารณาประกอบเพื่อเลือกใช้สื่อกลางที่เหมาะสมที่สุด โดยใช้วิธีเปรียบเทียบระหว่างราคากับประสิทธิภาพที่ได้ รวมทั้งปริมาณและความต้องการในการรับส่งข้อมูลขององค์กร

2. ความเร็ว (Speed) ประสิทธิภาพในการขนส่งข้อมูลของสื่อกลางจะพิจารณาจากความเร็ว 2 ชนิด คือ ความเร็วในการส่งข้อมูล (Data Transmissions Speed) และความเร็วในการถ่ายทอดสัญญาณ (Propagation Speed) โดยความเร็วในการส่งข้อมูล คือ จำนวนบิตที่สามารถส่งได้ใน 1 วินาที โดยจำนวนบิตสูงสุดต่อวินาทีที่แต่ละสื่อกลางสามารถส่งได้ขึ้นอยู่กับ Bandwidth ของสื่อกลาง ระยะเวลาในการส่งข้อมูล สัญญาณรบกวน และสภาพแวดล้อมต่างๆ ส่วนความเร็วในการถ่ายทอดสัญญาณ คือ ความเร็วในการเคลื่อนที่ของสัญญาณผ่านสื่อกลาง ดังนั้น ในระบบที่ต้องใช้การรับข้อมูลด้วยความเร็วสูง เช่น ระบบการส่งสัญญาณผ่านดาวเทียมจึงจำเป็นต้องเลือกสื่อกลางที่มีความเร็วในการถ่ายทอดสัญญาณสูง เป็นต้น

3. ระยะทาง (Distance) และการขยายเครือข่าย (Expandability) ระบบเครือข่ายที่มีสายคู่บิดเกลียวเป็นสื่อกลางจะสามารถขยายต่อระบบได้ง่ายที่สุด ส่วนสายโคแอ๊กเชียลจะขยายต่อระบบได้ง่ายกว่าสายใยแก้วนำแสง สาเหตุที่สายคู่บิดเกลียวสามารถขยายต่อระบบได้ง่ายกว่าสายโคแอ๊กเชียลและสายใยแก้วนำแสง เพราะสายคู่บิดเกลียวสามารถเชื่อมต่อสายได้ง่ายและสะดวกรวดเร็ว แต่สายคู่บิดเกลียวมีข้อจำกัดของเรื่องระยะทางในการส่งข้อมูลที่สามารถส่งได้ในระยะ 100 เมตร แต่สายโคแอ๊กเชียลบางชนิดสามารถส่งข้อมูลได้ไกลถึง 1 กิโลเมตร ส่วนสายใยแก้วนำแสงสามารถส่งข้อมูลได้หลายกิโลเมตรโดยไม่จำเป็นต้องใช้อุปกรณ์ทวนสัญญาณ

4. สภาพแวดล้อม (Environment) อาจส่งผลกระทบต่อประสิทธิภาพในการส่งข้อมูลได้ เช่น ในโรงงานอุตสาหกรรมที่ประกอบด้วยเครื่องจักรและอุปกรณ์ต่างๆ ซึ่งอาจแผ่รังสีคลื่นแม่เหล็กไฟฟ้าแทรกเข้าไปยังสายเคเบิลที่ใช้ส่งข้อมูล หากจำเป็นต้องเดินสายเคเบิลผ่าน

อุปกรณ์เหล่านี้ ควรห่อหุ้มด้วยชิลด์เพื่อป้องกันไม่ให้เกิดสัญญาณรบกวนแทรกเข้ามาภายในสายเคเบิลได้ หรือเปลี่ยนมาใช้สายใยแก้วนำแสงแทน เนื่องจากแสงจะไม่ได้รับผลกระทบจากคลื่นแม่เหล็กไฟฟ้าที่เครื่องจักรปล่อยออกมานั่นเอง

5. ความปลอดภัย (Security) ในกรณีที่ต้องการความปลอดภัยของข้อมูลสูง ควรเลือกใช้สื่อกลางที่เชื่อมต่อสายได้ยาก เนื่องจากอาจมีผู้ลักลอบต่อสัญญาณเพื่อขโมยข้อมูล โดยสื่อกลางแบบสายสัญญาณทุกชนิดสามารถลักลอบต่อสายสัญญาณเพื่อดักฟังข้อมูลที่เป็นสัญญาณแม่เหล็กไฟฟ้าได้ไม่ยาก ยกเว้นสื่อกลางที่เป็นสายใยแก้วนำแสง เนื่องจากสัญญาณจะอยู่ในรูปของแสงที่ทำให้การดักฟังทำได้ยาก ส่วนการติดต่อสื่อสารแบบไร้สายนอกจากจะถูกคลื่นรบกวนได้ง่ายแล้ว ยังถูกลักลอบดักฟังข้อมูลได้ง่ายอีกด้วย วิธีการเพิ่มความปลอดภัยให้กับการสื่อสารข้อมูลทั้งแบบใช้สายสัญญาณและแบบไร้สาย คือ เพิ่มระบบการตรวจสอบและพิสูจน์ข้อมูล โดยในระบบที่ใช้สื่อกลางแบบสายสัญญาณจะใช้ซอฟต์แวร์สำหรับเข้ารหัสและถอดรหัสข้อมูล ส่วนระบบที่ใช้สื่อกลางแบบไร้สายจะใช้ Spread Spectrum Technology เพื่อจำกัดสิทธิ์การเข้าใช้งานระบบเครือข่ายไร้สายแทน

4.4 ปัจจัยที่ส่งผลกระทบต่อการขนส่งข้อมูล

ในการขนส่งข้อมูลผ่านสื่อกลางต่างๆ ย่อมมีอุปสรรคและปัจจัยทั้งภายในและภายนอกระบบที่ทำให้เกิดอุปสรรคในการขนส่งข้อมูลและอาจเกิดความผิดพลาดขึ้น ปัจจัยพื้นฐานที่ส่งผลกระทบต่อการขนส่งข้อมูลมีหลายประการ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 89-91)

1. ความแรงของสัญญาณ ในการขนส่งสัญญาณหากความแรงของสัญญาณมีไม่มากพอ จะส่งผลให้สัญญาณอ่อนลง (Attenuation) เนื่องจากการสูญเสียพลังงานในระหว่างเดินทางบนสื่อกลาง ซึ่งอาจเกิดจากแรงต้านจากวัสดุที่นำมาผลิตสื่อกลางที่มีความแตกต่างกัน และอาจมีคุณสมบัติดูดซับสัญญาณมากเกินไป หรืออาจเกิดจากสภาพแวดล้อม อุณหภูมิที่ส่งผลกระทบให้พลังงานของการส่งสัญญาณลดน้อยลง เมื่อพลังงานสูญเสียไปมากความแรงของสัญญาณย่อมลดลง จึงมีการเพิ่มอุปกรณ์ขยายสัญญาณ (Amplifier) เพื่อช่วยให้ความแรงของสัญญาณเพิ่มสูงขึ้นเหมือนเดิมและสามารถเดินทางไปยังปลายทางได้อย่างสมบูรณ์ หรือมีการตั้งเสารับสัญญาณหรือสถานีย่อยเพื่อเป็นตัวทวนสัญญาณให้กับต้นทางในระหว่างการส่ง ซึ่งจะช่วยแก้ไขปัญหาความอ่อนของสัญญาณได้

2. สัญญาณรบกวน (Noise) เป็นอีกปัจจัยหนึ่งที่ส่งผลให้ข้อมูลผิดพลาดไปจากเดิม เนื่องจากมีข้อมูลหรือสัญญาณบางชนิดแทรกเข้าไปในสัญญาณข้อมูล ทำให้สัญญาณที่ปลายทางได้รับไม่ถูกต้องหรือไม่ชัดเจน สัญญาณรบกวนนั้นเกิดได้หลายลักษณะ เช่น สัญญาณรบกวนจากความร้อน สัญญาณรบกวนจากสิ่งแวดล้อม และสัญญาณรบกวนภายในสื่อกลาง เป็นต้น สัญญาณรบกวนที่เกิดขึ้นกับการขนส่งข้อมูลผ่านสายสัญญาณเสมอ คือ สัญญาณแทรกข้าม (Crosstalk) ซึ่งเกิดจากสัญญาณบนสายเส้นหนึ่งไปรบกวนสัญญาณที่อยู่ใกล้เคียง เนื่องจากการขนส่งข้อมูลของแต่ละสายนั้นอาจทำให้เกิดคลื่นสัญญาณที่ขัดแย้งกันและส่งผลให้ไปรบกวนสัญญาณข้อมูลซึ่งกันและกัน สำหรับวิธีแก้ไขปัญหาของ Crosstalk นั้นทำได้โดยการใช้สายสัญญาณชนิดสายคู่บิดเกลียว (Twisted-pair) ซึ่งการบิดเกลียวของสายจะทำให้สัญญาณที่จะไปรบกวนการนั้นถูกหักล้างออกไป โดยจำนวนเกลียวยิ่งมากการเกิด Crosstalk ก็ยิ่งลดลงด้วย

3. ช่วงความถี่ หรือ แบนด์วิชท์ (Bandwidth) เป็นอีกหนึ่งปัจจัยที่ส่งผลกระทบต่อการขนส่งข้อมูล เนื่องจากเป็นตัวกำหนดขนาดและปริมาณช่วงความถี่ของช่องสัญญาณที่สามารถนำมาใช้ในการขนส่งข้อมูลได้ ซึ่งในการส่งสัญญาณช่วงความถี่จะบ่งบอกถึงจำนวนของสัญญาณที่ถูกกำหนดขึ้นด้วยความถี่ระดับต่างๆ ยิ่งช่วงความถี่กว้างการแบ่งช่องสัญญาณก็สามารถทำได้อย่างมีประสิทธิภาพ ทำให้มีจำนวนช่องสัญญาณมากขึ้น การเพิ่มประสิทธิภาพในการขนส่งข้อมูลสามารถใช้เทคโนโลยีการรวมสัญญาณ (Multiplexing) จะทำให้มีช่องสัญญาณในการขนส่งข้อมูลเพิ่มขึ้นและยังช่วยในการจัดการขนส่งข้อมูลให้เหมาะสมกับความต้องการอีกด้วย

4. การผิดรูปของสัญญาณ หรือที่เรียกว่า Distortion เป็นการเปลี่ยนแปลงของรูปสัญญาณที่ผิดเพี้ยนไปจากเดิม โดยสัญญาณที่ส่งออกไปถึงปลายทางจะผิดรูปไปจากสัญญาณเดิม ทำให้ได้สัญญาณที่ไม่ถูกต้อง ซึ่งในแต่ละสัญญาณจะมีความถี่แตกต่างกัน การเดินทางไปยังปลายทางก็ย่อมใช้เวลาที่แตกต่างกัน ทำให้เกิดการผิดรูปของสัญญาณซึ่งอาจทำให้สัญญาณเปลี่ยนแปลงไปได้ทั้งแอมพลิจูด ความถี่ และเฟสของสัญญาณ โดยการผิดรูปของสัญญาณเกิดจากการเปลี่ยนแปลงของคลื่นไฟฟ้าที่เกิดขึ้นภายในตัวอุปกรณ์หรือเกิดจากกระบวนการต่างๆ ที่ต้นทางหรือปลายทางก็ได้ เช่น เกิดการผิดรูปในระหว่างการ Modulation เป็นต้น

4.5 สรุป

สื่อกลางในการติดต่อสื่อสารเพื่อขนส่งข้อมูลจากต้นทางไปยังปลายทาง มีหลายประเภท การเลือกใช้สื่อกลางขึ้นอยู่กับระยะทาง ระยะเวลา อัตราการส่งข้อมูล ปริมาณผู้ใช้ที่สามารถรองรับได้ในเวลาเดียวกัน งบประมาณ และความต้องการด้านประสิทธิภาพ โดยสื่อกลางในการขนส่งข้อมูลมีทั้งแบบใช้สายสัญญาณและแบบไร้สาย แบบใช้สายสัญญาณจะเป็นการติดต่อในระยะใกล้ภายในเครือข่าย ภายในอาคาร จากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ซึ่งมีสายสัญญาณให้เลือกใช้หลายชนิดคือสายโคแอ๊กเชียล สายคู่บิดเกลียว ทั้งแบบ UTP และ STP และสายใยแก้วนำแสง ซึ่งแต่ละชนิดก็มีคุณสมบัติและข้อจำกัดในการเลือกใช้ที่แตกต่างกัน ดังนั้นควรเลือกใช้ให้เหมาะสมกับความต้องการที่กล่าวไว้แล้วข้างต้น สำหรับสื่อกลางแบบไร้สายนั้นจะเป็นการติดต่อด้วยการใช้คลื่นวิทยุหรือคลื่นแสงซึ่งขึ้นอยู่กับความเหมาะสมของลักษณะการใช้งาน คลื่นวิทยุในแต่ละช่วงความถี่ก็มีความเหมาะสมและมีลักษณะการใช้งานที่แตกต่างกันออกไป เช่น ใช้สำหรับวิทยุสื่อสาร โทรศัพท์ไร้สาย และการสื่อสารผ่านดาวเทียม เป็นต้น นอกจากการติดต่อสื่อสารในระยะไกลแล้วสื่อแบบไร้สายยังติดต่อในระยะใกล้โดยไม่ต้องใช้สายสัญญาณได้ เช่น อินฟราเรด และบลูทูธ ดังนั้น สื่อกลางในแต่ละประเภทจะมีความเหมาะสมและมีประสิทธิภาพที่บ่งบอกถึงข้อจำกัดของการนำไปใช้งาน จึงควรพิจารณาเลือกชนิดของสื่อกลางที่เหมาะสมและมีประโยชน์สูงสุดต่อระบบ เพื่อไม่ให้สิ้นเปลืองงบประมาณและเทคโนโลยีในการขนส่งข้อมูลไปโดยเปล่าประโยชน์

บทที่ 5
การเชื่อมต่อเครือข่ายกับอุปกรณ์ต่างๆ

การเชื่อมต่ออุปกรณ์คอมพิวเตอร์กับอุปกรณ์ต่างๆ เช่น จอภาพ แป้นพิมพ์ เมาส์ เป็นการเชื่อมต่ออุปกรณ์ที่เป็นส่วนประกอบของคอมพิวเตอร์ ซึ่งปัจจุบันมีการนำคอมพิวเตอร์มาทำงานร่วมกับอุปกรณ์อื่นๆ เช่น เครื่องพิมพ์ หรือโมเด็ม เพื่อเชื่อมต่อไปยังระบบอินเทอร์เน็ต ซึ่งจะช่วยเพิ่มความสะดวกสบายและประสิทธิภาพให้กับการทำงานภายองค์กรมากยิ่งขึ้น โดยปัจจุบันองค์กรต่างๆ นิยมเชื่อมต่อคอมพิวเตอร์ภายในด้วยระบบแลน และจัดเตรียมเซิร์ฟเวอร์ไว้คอยให้บริการต่างๆ เช่น การจัดเก็บและสำรองข้อมูล ระบบอีเมล์ อินเทอร์เน็ต และโปรแกรมประเภทต่างๆ เป็นต้น

การเชื่อมต่อระหว่างคอมพิวเตอร์กับอุปกรณ์ต่างๆ เป็นแนวคิดของอินเตอร์เฟซเกิดขึ้นในชั้นกายภาพ (Physical Layer) โดยอุปกรณ์แต่ละชนิดมีการทำงานและวิธีการเชื่อมต่อระหว่างอุปกรณ์ที่แตกต่างกัน ดังนั้น จึงมีการกำหนดมาตรฐานของอินเตอร์เฟซแบบต่างๆ ขึ้นมา การเชื่อมต่อระหว่างคอมพิวเตอร์ที่พบได้บ่อยครั้ง คือ การเชื่อมต่อระหว่างคอมพิวเตอร์กับโมเด็มด้วยวิธี Dial-Up Modem ผ่านสายโทรศัพท์ ทำให้เครื่องคอมพิวเตอร์สามารถเชื่อมต่อไปยังระบบอินเทอร์เน็ตได้ แม้ว่าในปัจจุบันจะมีเทคโนโลยีใหม่ๆ ที่ช่วยเพิ่มความเร็วในการส่งข้อมูลให้กับโมเด็ม แต่หลักการทำงานของโมเด็มก็ยังไม่มีการเปลี่ยนแปลง

5.1 โมเด็ม

โมเด็ม (Modem) เป็นอุปกรณ์สำหรับเชื่อมต่อสื่อสารระยะไกล เช่น การสื่อสารระยะไกลระหว่างสาขา และอินเทอร์เน็ต โมเด็มเป็นเสมือนโทรศัพท์สำหรับคอมพิวเตอร์ที่จะช่วยให้ระบบคอมพิวเตอร์สามารถสื่อสารกับคอมพิวเตอร์อื่นๆ ได้ทั่วโลก (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 95-100)

5.1.1 การทำงานขั้นพื้นฐานของโมเด็ม

ในอดีตสายสัญญาณที่ใช้ในระบบโทรศัพท์จะรองรับเฉพาะสัญญาณแอนะล็อก จึงต้องมีการแปลงข้อมูลของคอมพิวเตอร์ที่อยู่ในรูปแบบดิจิทัลให้กลายเป็นสัญญาณแอนะล็อกก่อน จึงส่งสัญญาณไปบนสายโทรศัพท์ได้ เทคนิคที่ใช้ในการแปลงข้อมูล เรียกว่า การมอดูเลต โดยโมเด็มจะแปลงข้อมูลดิจิทัลไปเป็นสัญญาณแอนะล็อก รวมทั้งแปลงสัญญาณแอนะล็อกไป

เป็นข้อมูลดิจิทัล เทคนิคที่นำมาใช้ในการมอดูเลตเพื่อแปลงข้อมูลดิจิทัลให้เป็นสัญญาณแอนะล็อก คือ ASK, FSK และ PSK จากนั้นปลายทางจะดีมอดูเลตเพื่อแยกสัญญาณพาหะ (Carries Signal) ออกจากข้อมูลดิจิทัล โมเด็มรุ่นแรกๆ จะใช้เทคนิคการมอดูเลตหลายแบบในการแปลงข้อมูล โดยจะส่งข้อมูลที่ความเร็ว 33,600 บิตต่อวินาที (33 Kbps)

การแบ่งชนิดของโมเด็ม นิยมแบ่งตามความเร็วสูงสุดในการขนส่งข้อมูลคอมพิวเตอร์ที่เชื่อมต่อกับโมเด็มที่มีความเร็วสูง 56 Kbps เรียกว่า โมเด็ม 56k เป็นต้น โดยโมเด็ม 56k ถูกออกแบบมาให้รองรับอัตราการส่งข้อมูลที่หลากหลายได้ เนื่องจากอาจมีความจำเป็นต้องเชื่อมต่อกับโมเด็มรุ่นเก่าที่มีอัตราการส่งข้อมูลต่ำ หรือมีปัจจัยที่อาจทำให้การรับส่งข้อมูลระหว่างโมเด็มมีความเร็วลดลง

5.1.2 มาตรฐานการทำงานของโทรศัพท์

โมเด็มรุ่นใหม่จะจัดเตรียมกลุ่มของมาตรฐานการทำงานของโทรศัพท์ (Standard Telephone Function) โดยฟังก์ชันเหล่านี้จะประกอบด้วย (โอภาส เอี่ยมสิริวงศ์, 2561, หน้า 218-219)

1. การตอบรับอัตโนมัติ (Auto Answer) โมเด็มจะรับสายที่โทรเข้ามาแบบอัตโนมัติเมื่อมีสัญญาณบนสาย

2. การหมุนโทรศัพท์อัตโนมัติ (Auto Dial) โมเด็มสามารถหมุนโทรศัพท์เพื่อโทรออกได้โดยอัตโนมัติ รวมถึงการสนับสนุนรหัสพิเศษเพื่อใช้ในการโทรออก เป็นต้น

3. การยกเลิกการติดต่ออัตโนมัติ (Auto Disconnect) โมเด็มสามารถยกเลิกการติดต่อ เมื่อตรวจพบว่าสัญญาณที่สื่อสารกันนั้นได้หลุดออกจากกันแล้ว อีกทั้งยังสามารถรีเซตตัวเองให้กลับมาอยู่ในสถานะพร้อมใช้งานได้ตามปกติ

4. การโทรซ้ำอัตโนมัติ (Auto Redial) เมื่อโมเด็มไม่สามารถติดต่อเลขหมายปลายทางได้ จะมีกระบวนการโทรซ้ำอัตโนมัติ และหากระบบมีการกำหนดเลขปลายทางสำรองเอาไว้ โมเด็มก็จะหมุนเพื่อโทรเข้าเลขปลายทางสำรองทันที เมื่อไม่สามารถติดต่อเลขหมายแรกได้

5.1.3 การเจรจาต่อรองเพื่อการเชื่อมต่อ

การเจรจาต่อรองเพื่อการเชื่อมต่อ (Connection Negotiation) คือ การกำหนดอัตราความเร็วในการส่งข้อมูลระหว่างโมเด็ม มีอยู่ 2 ประเภท คือ การถอยหลัง (Fallback) และการเดินหน้า (Fall Forward) เมื่อโมเด็ม 2 ตัว สร้างการเชื่อมต่อกัน จะมีการสร้างข้อตกลงเกี่ยวกับความเร็วในการขนส่งข้อมูลที่จะใช้ โดยจะกำหนดบนพื้นฐานของความเร็วสูงสุดที่โมเด็มสามารถรองรับได้ และสัญญาณรบกวนที่เกิดขึ้นจากการเชื่อมต่อ หากโมเด็มทั้งสองไม่สามารถใช้ความเร็วในการส่งข้อมูลสูงสุดได้ จะลดความเร็วลงมา เรียกว่า การถอยหลัง โดยจะลดจนกระทั่งโมเด็มทั้งสองฝั่งยอมรับความเร็วดังกล่าว แต่ถ้าโมเด็มทั้งสองไม่สามารถกำหนดความเร็วในการส่งข้อมูลร่วมกันได้ ความเร็วจะถูกลดลงมาจนถึง 0 Kbps และการเชื่อมต่อจะถูกยกเลิก (Disconnect) ในกรณีที่สัญญาณรบกวนในสายโทรศัพท์ลดลง โมเด็มทั้งสองจะกำหนดให้ให้มีความเร็วในการส่งข้อมูลเพิ่มขึ้น เรียกว่า การเดินหน้า (โอภาส เอี่ยมสิริวงศ์, 2561, หน้า 219)

5.1.4 การแก้ไขข้อผิดพลาด

โมเด็มจะมีเครื่องมือที่เรียกว่า การแก้ไขข้อผิดพลาด (Error Correction) ถูกคิดค้นในปี ค.ศ. 1980 โดยบริษัท Microcom Corporation ซึ่งได้สร้างชุดของโมเด็มที่มีฟังก์ชันการแก้ไขข้อผิดพลาดแบบอัตโนมัติไว้ โดยการติดต่อสื่อสารกันระหว่างโมเด็มของเครื่องคอมพิวเตอร์ จะมีการตรวจสอบความถูกต้องของข้อมูล หากข้อมูลที่ส่งมายังโมเด็มปลายทางมีข้อผิดพลาดจะมีการส่งข้อความเตือนไปยังโมเด็มที่ส่งข้อมูล (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 98)

5.1.5 การส่งสำเนาเอกสาร

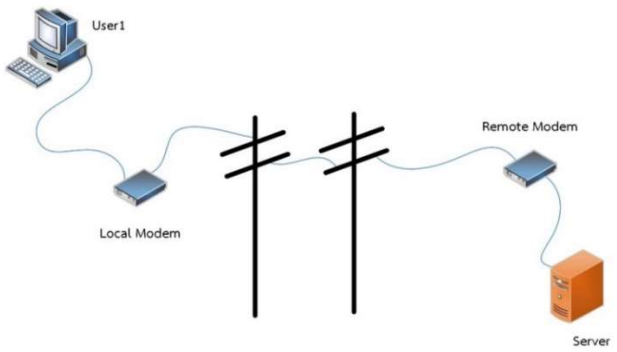
โมเด็มส่วนใหญ่จะมีความสามารถในการส่งสำเนาเอกสาร หรือแฟกซ์ (Fax) ซึ่งมีรูปแบบที่แตกต่างกัน จึงต้องมีการกำหนดมาตรฐานในการส่งข้อมูลด้วยโพรโทคอลที่ต่างกัน ตัวอย่างมาตรฐานของการส่งแฟกซ์ผ่านโมเด็ม ได้แก่ V17 V27ter และ V.29 เป็นต้น โดยมาตรฐาน V ถูกกำหนด โดยองค์กร International Telecommunication Union (ITU) และโมเด็มส่วนใหญ่ในปัจจุบันสามารถรองรับการส่งสำเนาเอกสารได้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 98)

5.1.6 ความปลอดภัย

โมเด็มจะมีฟังก์ชันความปลอดภัย(Security) เพื่อจำกัดการเข้าถึงเครือข่ายคอมพิวเตอร์หรือระบบไว้ มาตรฐานความปลอดภัยดังกล่าว คือ Blacklisting, Callback Security และ Backdoor Entry โดย Blacklisting คือ การใช้ความสามารถของโมเด็มเพื่อบล็อกผู้ใช้บางคนที่พยายาม Remote เข้าสู่ระบบ, Callback Security คือ การป้องกันผู้ไม่หวังดีหมุนโมเด็มเข้ามา และ Backdoor Entry คือการใช้งานร่วมกับการใส่รหัสผ่านเพื่อให้ผู้ต้องการใช้งานระบบด้วย Remote Modem ใส่รหัสผ่านก่อนเข้าใช้งาน (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 98)

5.1.7 การทดสอบการเชื่อมต่อ

โมเด็มจะจัดเตรียมวิธีการทดสอบการเชื่อมต่อที่เรียกว่า Loop Back ไว้ 2 แบบ คือ Local Loop Back และ Remote Loop Back โดยเครื่องมือทั้งสองนี้จะใช้สำหรับตรวจสอบการเชื่อมต่อระหว่างคอมพิวเตอร์กับโมเด็มว่ามีการเชื่อมต่อกันอยู่หรือไม่ รวมทั้งตรวจสอบว่า Local Modem และ Remote Modem สามารถเชื่อมต่อกันได้หรือไม่ ให้พิจารณาการเชื่อมต่อระหว่างโมเด็มทั้ง 2 รูปแบบ ดังภาพที่ 5.1



ภาพที่ 5.1 แสดงการเชื่อมต่อระหว่าง Local Modem กับ Remote Modem
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 99)

จากภาพที่ 5.1 การทดสอบด้วย Local Loop Back จะใช้คอมพิวเตอร์ของ User1 ส่งข้อมูลไปยัง Local Modem ของตน จากนั้น Local Modem จะส่งข้อกลับไปยังคอมพิวเตอร์ของ User1 ทันที การทดสอบดังกล่าวเป็นการตรวจสอบว่าคอมพิวเตอร์ของ User1 มีการเชื่อมต่อกับ Local Modem อยู่หรือไม่ ส่วนการทดสอบด้วย Remote Loop

Back จะให้คอมพิวเตอร์ของ User1 ส่งข้อมูลไปยัง Local Modem จากนั้น Local Modem จะส่งสัญญาณไปยัง Remote Modem เมื่อ Remote Modem ได้รับข้อมูลก็จะส่งสัญญาณตอบกลับมาให้กับ Local Modem ทันที การทดสอบดังกล่าวใช้สำหรับตรวจสอบว่า Local Modem และ Remote Modem สามารถเชื่อมต่อกันได้หรือไม่ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 98-99)

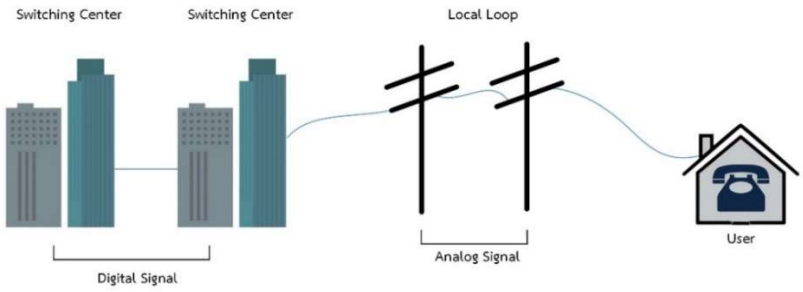
5.1.8 โมเด็มแบบติดตั้งภายในและโมเด็มแบบติดตั้งภายนอก

โมเด็มที่นำมาติดตั้งใช้งานร่วมกับเครื่องคอมพิวเตอร์หรือพีซี สามารถแบ่งได้เป็น 2 ชนิด คือโมเด็มแบบติดตั้งภายใน (Internal Modem) กับโมเด็มแบบติดตั้งภายนอก (External Modem) โดยโมเด็มแบบติดตั้งภายใน คือ โมเด็มที่ใช้ติดตั้งกับช่องต่อ (Slot) ที่อยู่ภายในคอมพิวเตอร์โดยไม่ต้องใช้พาวเวอร์ซัพพลายจากภายนอกหรือสายเคเบิลในการเชื่อมต่อ โดยทั่วไปเครื่องคอมพิวเตอร์จะติดตั้งโมเด็มประเภทนี้มาให้แล้ว ข้อเสียของโมเด็มแบบติดตั้งภายใน คือ หากช่องต่อที่ใช้ติดตั้งการ์ดเต็มจะไม่สามารถติดตั้งโมเด็มได้ และอาจเกิดการชนกันระหว่าง Interrupt Request (IRQ) ของโมเด็มกับ IRQ ของอุปกรณ์อื่นๆ โดย IRQ ทำหน้าที่กำหนดช่องทางในการร้องขอการขัดจังหวะของอุปกรณ์เพื่อติดต่อกับไมโครโปรเซสเซอร์ ส่วนโมเด็มแบบติดตั้งภายนอก คือ โมเด็มที่ติดตั้งภายนอกและใช้พาวเวอร์ซัพพลายแยกจากเครื่องคอมพิวเตอร์ และใช้สายเคเบิลในการเชื่อมต่อผ่านพอร์ตต่างๆ เช่น Serial Port, USB Port หรือ FireWire Port เป็นต้น

5.2 โมเด็ม 56 K

โมเด็ม 33 Kbps ได้รับการพัฒนาและถูกนำมาใช้กันอย่างแพร่หลาย โดยใช้วิธีการเชื่อมต่อแบบแอนะล็อกผ่านสายโทรศัพท์ ต่อมาได้มีการพัฒนาโมเด็ม 33 Kbps ให้มีความเร็วเพิ่มขึ้นเป็น 56 Kbps เรียกว่า โมเด็ม 56K ซึ่งออกแบบมาให้มีการทำงานแบบ Hybrid คือ สามารถทำงานได้ทั้งกับสัญญาณแอนะล็อกและดิจิทัล เมื่อต้องการส่งข้อมูลจากโมเด็มไปยัง Remote Computer หรือ Upstream จะยังคงใช้สัญญาณแอนะล็อกด้วยการมอดูเลต ซึ่งมีข้อจำกัด คือ สามารถส่งข้อมูลได้เร็วถึง 33 Kbps แต่ถ้าต้องการรับข้อมูลจาก Remote Computer หรือ Downstream ด้วยโมเด็ม 56K จะใช้สัญญาณดิจิทัลแทนสัญญาณแอนะล็อก และส่งข้อมูลขนาด 8 บิต ได้ถึง 8000 ครั้งต่อวินาที หรือ 64 Kbps การรับส่งข้อมูลระหว่างผู้ให้บริการโทรศัพท์กับผู้ใช้ตามบ้านก็ไม่สามารถใช้ความเร็วได้ถึง 64 Kbps เนื่องจากเมื่อผู้ให้บริการ

โทรศัพท์ส่งสัญญาณโทรศัพท์แบบดิจิทัลขนาด 64 Kbps มา สัญญาณดังกล่าวจะถูกส่งจาก Switching Center หนึ่งไปยัง Switching Center อื่นๆ และเมื่อสัญญาณโทรศัพท์ถูกส่งไปตามบ้านจะต้องเดินทางผ่าน Local Loop ซึ่งเป็นส่วนของสายที่ใช้เชื่อมต่อระหว่างบ้านและผู้ให้บริการโทรศัพท์ แต่ Local Loop จะรองรับเฉพาะสัญญาณแอนะล็อกเท่านั้น จึงทำให้ความเร็วในการส่งข้อมูลลดลง ดังภาพที่ 5.2 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 100-101)



ภาพที่ 5.2 แสดงการส่งสัญญาณผ่าน Local Loop

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 100)

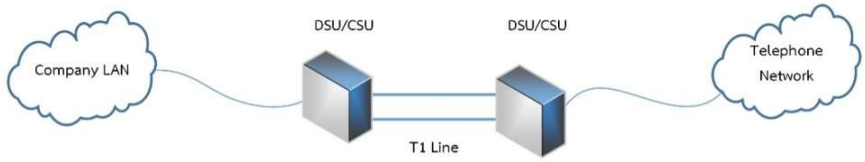
ก่อนที่สัญญาณโทรศัพท์จะถูกส่งไปยัง Local Loop ผู้ให้บริการโทรศัพท์จะต้องแปลงสัญญาณดิจิทัลเป็นสัญญาณแอนะล็อกก่อน เมื่อสัญญาณแอนะล็อกถูกส่งไปบน Local Loop จนถึงบ้านของผู้ใช้แล้ว สัญญาณแอนะล็อกจะถูกแปลงกลับเป็นสัญญาณดิจิทัลโดยโมเด็ม 56K เนื่องจากข้อมูลที่ใช้รับส่งภายในเครื่องคอมพิวเตอร์จะอยู่ในรูปแบบของดิจิทัล โดยข้อมูลขนาด 64 Kbps ที่ผ่าน Local Loop จะเหลือความเร็วประมาณ 56 Kbps เท่านั้น

เมื่อมีการนำโมเด็ม 56K มาใช้ในระยะแรก มีการสร้างรูปแบบการเชื่อมต่อ 2 มาตรฐานคือ X2 และ K56flex ซึ่งทั้งสองมาตรฐานถูกพัฒนาโดย 2 บริษัทที่เป็นคู่แข่งกัน จึงไม่สามารถนำมาใช้งานร่วมกันได้ ต่อมาองค์กร ITU ได้กำหนดมาตรฐานใหม่ขึ้นมาชื่อ V.90 ซึ่งได้รับการยอมรับกันอย่างกว้างขวาง และได้พัฒนามาตรฐาน มาเป็น V.92 โดยเพิ่มคุณสมบัติสำคัญ 2 ประการ คือ การเพิ่มความเร็วในการเชื่อมต่อแบบ Upstream ระหว่างผู้ใช้กับผู้ให้บริการเป็น 48 Kbps ซึ่งมาตรฐาน V.90 จะมีความเร็วที่ 33 Kbps และโมเด็มมาตรฐาน V.92 สามารถใช้งานโทรศัพท์ได้ในขณะที่เชื่อมต่อข้อมูลอยู่ โดยการเชื่อมต่อจะถูกหยุดไว้ชั่วขณะ

5.3 การเชื่อมต่อเครือข่ายระยะไกลด้วยโมเด็มแบบอื่นๆ

หลักการทำงานของโมเด็มจะมอดูเลตข้อมูลดิจิทัลของคอมพิวเตอร์ให้เป็นสัญญาณที่เหมาะสมสำหรับส่งไปบนสายโทรศัพท์ และจะดีมอดูเลตสัญญาณไปเป็นข้อมูลดิจิทัลอีกครั้ง นอกจากการส่งข้อมูลผ่านสายโทรศัพท์แบบดั้งเดิมแล้ว ยังมีเทคนิคในการส่งข้อมูลอีก 4 แบบ ซึ่งสามารถใช้เชื่อมต่อคอมพิวเตอร์กับระบบเครือข่ายระยะไกลได้ คือ T1 Digital Telephone Line, Cable Television Network, Integrated Service Digital Network (ISDN) และ Digital Subscriber Line (DSL) โดยเทคโนโลยีการส่งข้อมูลแต่ละรูปแบบจะต้องใช้อุปกรณ์เฉพาะของตนเองเพื่อแปลงข้อมูลดิจิทัลให้อยู่ในรูปแบบที่สามารถจัดส่งออกไปได้ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 101-103)

1. Channel Service Unit/Data Service Unit (CSU/DSU) เป็นอุปกรณ์ที่ใช้สำหรับแปลงข้อมูลดิจิทัลให้อยู่ในรูปแบบที่เหมาะสมต่อการจัดส่ง โดยอัตราการส่งข้อมูลจะขึ้นอยู่กับเทคโนโลยีที่นำมาใช้ในการขนส่งข้อมูล หากนำมาใช้กับเทคโนโลยี T1 Digital Telephone Line บนสายคู่เช่าแบบ T1 (T1 Line) อัตราการส่งข้อมูลจะสูงกว่า 1.544 Mbps แต่ถ้านำไปใช้กับเทคโนโลยีสายคู่เช่า (Leased Line) จะมีอัตราการส่งข้อมูลอยู่ระหว่าง 56-64 Kbps โดยฝั่งผู้ใช้ บริการจะต้องใช้อุปกรณ์ DSU/CSU เพื่อเชื่อมต่อระบบของตนเข้าสู่สายเชื่อมต่อ ดังภาพที่ 5.3



ภาพที่ 5.3 แสดงการใช้ CSU/DSU เพื่อเชื่อมต่อเครือข่ายแลนกับสายคู่เช่าแบบ T1
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 101)

อุปกรณ์ CSU จะส่งสัญญาณไปบนสายคู่เช่า T1 เมื่อตัวรับสัญญาณของผู้ให้บริการได้รับสัญญาณ จะทำการแยกสัญญาณรบกวนออกไป โดย CSU จะทำหน้าที่เก็บข้อมูลการใช้งานต่างๆ และยังสามารถส่งสัญญาณ Loop Black เพื่อทดสอบการเชื่อมต่อได้อีกด้วย ส่วน DSU ใช้สำหรับจัดการการเชื่อมต่อกับ T1 ในแต่ละจุด โดยจะควบคุมการแปลงสัญญาณให้อยู่ในรูปแบบที่กำหนด

2. Cable Modem เป็นอุปกรณ์ที่ใช้แยกข้อมูลของคอมพิวเตอร์ออกเป็นสัญญาณทีวีที่ส่งมาตามสายเคเบิลทีวี เป็นบริการสำหรับการสื่อสารข้อมูลระบบแวนด้วยความเร็วสูง ตัวอย่างของระบบ Cable Modem ได้แก่ การเชื่อมต่อกับอินเทอร์เน็ตผ่านเคเบิลทีวี

Cable Modem เป็นอุปกรณ์ที่ใช้เชื่อมต่อกับ PC ผ่านทางการ์ดแลน (Ethernet Network Interface Card) โดยสามารถส่งข้อมูลได้ที่ความเร็ว 300 Kbps ถึง 2.5 Mbps แต่การส่งระหว่าง Upstream กับ Downstream จะมีความเร็วไม่เท่ากัน โดยข้อมูลที่เป็น Downstream ซึ่งถูกส่งจากผู้ให้บริการไปยังผู้ใช้บริการจะมีความเร็วมากกว่าข้อมูล Upstream ที่ผู้ใช้ส่งให้กับผู้ให้บริการ แต่โดยทั่วไปการส่งสัญญาณกับเครือข่ายแวนหรือระบบอินเทอร์เน็ต ผู้ใช้งานจะใช้การส่งข้อมูลแบบ Downstream เพื่อดาวน์โหลดเว็บเพจ หรือข้อมูลต่างๆ มากกว่าแบบ Upstream ดังนั้น Cable Modem จึงไม่เหมาะกับองค์กรหรือผู้ใช้ที่ต้องการ Upstream ข้อมูลบ่อยครั้ง

โครงสร้างพื้นฐานของระบบ Cable Modem ประกอบด้วย 6 ส่วน ดังนี้

2.1 Cable Modem Termination System (CMTS) ทำหน้าที่หาเส้นทางและแปลงข้อมูลให้เป็นคลื่นความถี่วิทยุ

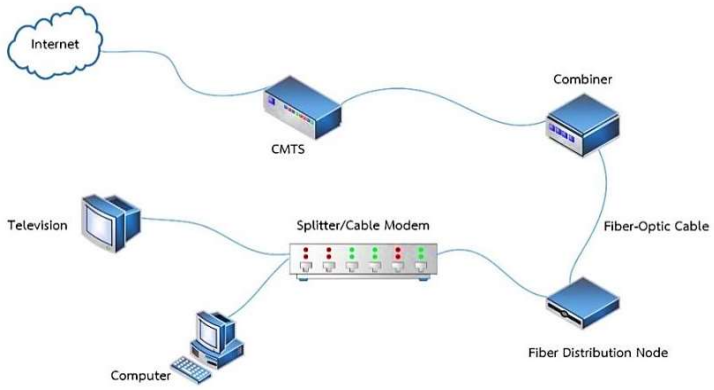
2.2 Combiner ทำหน้าที่รวมความถี่ของแพ็กเกจข้อมูลกับความถี่ของช่องสัญญาณเคเบิลทีวี

2.3 สายใยแก้วนำแสง (Fiber-Optic) ทำหน้าที่เป็นสื่อกลางเพื่อรับส่งข้อมูล โดยจะคอยรับสัญญาณที่ส่งมาจากอุปกรณ์ Combiner

2.4 Fiber Distribution Node ทำหน้าที่กระจายสัญญาณที่ได้รับมาจากสายใยแก้ว-นำแสงไปยังกลุ่มผู้ใช้ตามบ้านที่เชื่อมต่อด้วยสายโคแอ็กเชียล

2.5 Splitter จะรับสัญญาณและนำมาแยกข้อมูลคอมพิวเตอร์ (เช่น เว็บเพจ) กับข้อมูลที่เป็นความถี่ของสัญญาณโทรทัศน์ออกจากกัน แล้วส่งสัญญาณโทรทัศน์ไปยังเครื่องรับโทรทัศน์ ส่วนข้อมูลคอมพิวเตอร์จะถูกส่งไปยัง Cable Modem

2.6 Cable Modem จะรับสัญญาณข้อมูลคอมพิวเตอร์จาก Splitter มาแปลงกลับเป็นข้อมูลดิจิทัลเพื่อส่งให้กับคอมพิวเตอร์นำไปใช้งานต่อไป



ภาพที่ 5.4 แสดงโครงสร้างพื้นฐานของระบบ Cable Modem
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 103)

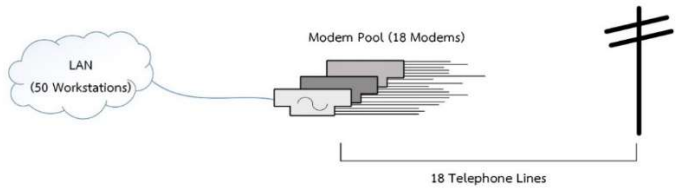
3. ISDN Modem หรือ Integrated Services Digital Network (ISDN) เป็นเครือข่ายที่ให้บริการในระบบดิจิทัลทั้งต้นทางและปลายทางเต็มรูปแบบ สามารถส่งข้อมูลในรูปของมัลติมีเดียได้หลายรูปแบบ เช่น เสียง ภาพนิ่ง และวิดีโอ โดยมีความเร็วในการส่งข้อมูลได้ถึง 128 Kbps ไม่ต้องแปลงสัญญาณด้วยการมอดูเลตเพื่อส่งข้อมูลบนสายโทรศัพท์ ข้อมูลจึงมีความถูกต้องและน่าเชื่อถือมากขึ้น โดย ISDN จะอาศัย ISDN Modem เพื่อแปลงสัญญาณดิจิทัลของคอมพิวเตอร์ให้อยู่ในรูปแบบที่สามารถส่งไปยังปลายทางได้

4. DSL Modem หรือ Digital Subscriber Line (DSL) เป็นการสื่อสารข้อมูลแบบดิจิทัลด้วยความเร็วสูงสุดผ่านสายโทรศัพท์ที่มีอยู่เดิม โดยผู้ใช้จะเชื่อมต่อกับบริการของ DSL ผ่าน DSL Modem และในทางทฤษฎีสามารถส่งข้อมูลด้วยอัตราเร็วสูงถึง 6.1 Mbps ทำให้สามารถรองรับการส่งข้อมูลทั้ง ภาพ เสียง และวิดีโอได้อย่างต่อเนื่อง DSL เป็นเทคโนโลยีที่ทันสมัยและได้รับความนิยมเป็นอย่างสูง

5.4 โมเด็มพูล

โมเด็มพูล (Modem Pool) เป็นเทคนิคในการทำให้ Workstation หลายๆ ตัว สามารถเข้าถึงโมเด็มร่วมกันได้โดยไม่ต้องติดตั้งโมเด็มไว้ที่ Workstation ทุกตัว เช่น มี Workstation จำนวน 10 เครื่อง ที่เชื่อมต่ออยู่ในระบบแลนสามารถทำให้ Workstation ทุกเครื่องเข้าใช้งานโมเด็มร่วมกันได้ด้วยเทคนิค Modem Pool นั่นเอง แม้ว่าราคาของโมเด็มจะไม่

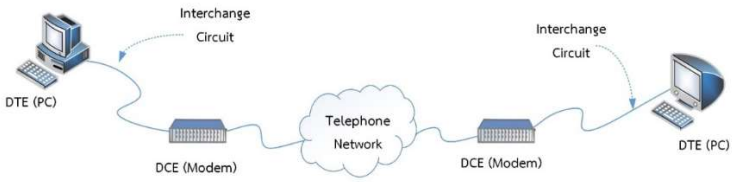
สูงมาก แต่ถ้าภายในองค์กรมีความต้องการใช้งานโมเด็มจำนวนมาก จะทำให้ค่าใช้จ่ายในการซื้ออุปกรณ์โมเด็มและจำนวนสายโทรศัพท์เพิ่มสูงขึ้นด้วย โมเด็มพูลจึงจัดเตรียมเครื่องมือที่ช่วยควบคุมการเชื่อมต่อโมเด็มกับสายโทรศัพท์ไว้ ไม่ให้ Workstation ที่ไม่ได้ใช้งานโมเด็มเชื่อมต่อกับคู่สายไว้ตลอดเวลา วิธีการดังกล่าวช่วยลดความต้องการใช้คู่สายโทรศัพท์ได้ โดยอาจจะขอคู่สายจากผู้ให้บริการเพียง 1 ใน 3 ของจำนวนพนักงานที่ต้องการใช้งานเท่านั้น ดังภาพที่ 5.5 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 101)



ภาพที่ 5.5 แสดงภาพของ Modem Pool ที่มีโมเด็มจำนวน 18 ตัว
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 104)

5.5 อินเตอร์เฟซที่ใช้เชื่อมต่อคอมพิวเตอร์กับอุปกรณ์ต่างๆ

อินเตอร์เฟซ (Interface) คือ วิธีการหรือลักษณะในการเชื่อมต่อระหว่างคอมพิวเตอร์กับอุปกรณ์ต่างๆ เช่น โมเด็ม จอภาพหรือเครื่องพิมพ์ เรียกว่า Interfacing ซึ่งการเชื่อมต่อจะพิจารณาในระดับชั้นกายภาพเป็นหลัก อุปกรณ์บนเครือข่ายคอมพิวเตอร์แบ่งได้ 2 แบบ คือ DTE และ DCE โดยที่ DTE เป็นอุปกรณ์ที่ถือเป็นแหล่งกำเนิดสัญญาณหรือรับส่งสัญญาณ เป็นอุปกรณ์ต้นทาง ส่วนปลายทางคือเครื่องคอมพิวเตอร์ ส่วน DCE เป็นอุปกรณ์ที่ทำหน้าที่ส่งต่อหรือแปลงสัญญาณ ซึ่งเชื่อมต่ออยู่กับ DTE ได้แก่ โมเด็ม โดยการเชื่อมต่อระหว่าง DTE และ DCE เรียกว่าวงจรแลกเปลี่ยน (Interchange Circuit) ซึ่งเป็นกลุ่มของสัญญาณที่ใช้รับส่งกันภายในสายส่ง ดังภาพที่ 5.6 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 105-111)



ภาพที่ 5.6 แสดงภาพการเชื่อมต่อวงจรแลกเปลี่ยนระหว่าง DTE และ DCE
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 105)

5.5.1 มาตรฐานของอินเตอร์เฟซ

ปัจจุบันมีผู้ผลิตคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ ขึ้นมาเป็นจำนวนมาก ดังนั้น จึงจำเป็นต้องมีการกำหนดมาตรฐานในการเชื่อมต่อระหว่างอุปกรณ์ต่างๆ (Interface Standard) ซึ่งมีอยู่หลายมาตรฐาน แต่ทุกมาตรฐานจะมีคุณลักษณะ 2 ข้อ ดังนี้

1. ต้องได้รับการพัฒนาและเห็นชอบจากองค์กรชั้นนำที่กำหนดมาตรฐานต่างๆ โดยองค์กรกำหนดมาตรฐานที่ได้รับการยอมรับ ได้แก่

1.1 Institute for Electrical and Electronics Engineers (IEEE)

1.2 American National Standard Institute (ANSI)

1.3 International Telecommunication Union (ITU)

1.4 International Organization for Standardization (ISO)

1.5 Electronic Industries Association (EIA)

องค์กรเหล่านี้จะทำหน้าที่กำหนดมาตรฐานของอินเตอร์เฟซให้กับอุปกรณ์ต่างๆ เพื่อทำให้ผลิตภัณฑ์จากผู้ผลิตสามารถทำงานร่วมกันได้ นอกจากนี้มาตรฐานต่างๆ ที่กำหนดขึ้นยังทำให้เทคโนโลยีใหม่ๆ สามารถทำงานร่วมกับเทคโนโลยีเดิมที่มีอยู่ได้

2. ประกอบด้วย 4 Component ดังนี้

2.1 Electrical Component คือ การควบคุมและจัดการกับแรงดันไฟฟ้าและส่วนประกอบอื่นๆ ที่เกี่ยวข้องกับไฟฟ้า

2.2 Mechanical Component คือ การจัดการกับส่วนที่ใช้เป็นตัวเชื่อมต่อ (Connector) หรือลักษณะของปลั๊กต่อ (Plug) โดยจะกำหนดทั้งรูปร่างและขนาดของตัวเชื่อมต่อ รวมทั้งจำนวนและการจัดเรียงพิน (Pin)

2.3 Functional Component จะอธิบายหน้าที่ของแต่ละพินในตัวเชื่อมต่อรวมทั้งหน้าที่ของวงจรต่างๆ

2.4 Procedural Component จะอธิบายวิธีการทำงานของแต่ละวงจร

5.5.2 ตัวอย่างอินเตอร์เฟซที่สำคัญ

อินเตอร์เฟซสำคัญที่ใช้ในการเชื่อมต่ออุปกรณ์ต่างๆ กับคอมพิวเตอร์ มีดังนี้

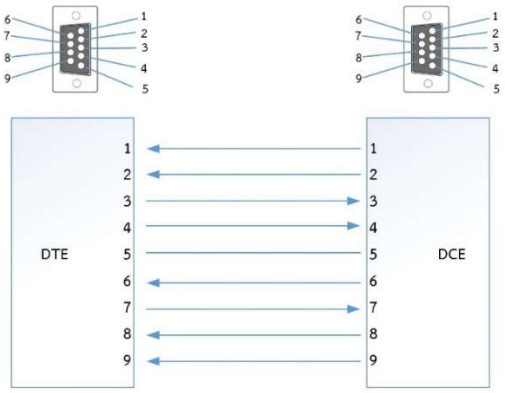
1. EIA RS-232 เป็นอินเตอร์เฟซที่ใช้ในการเชื่อมต่อระหว่าง DTE กับโมเด็ม ซึ่งทำหน้าที่ เป็น DCE เพื่อใช้แปลงข้อมูลให้เป็นสัญญาณแอนะล็อกสำหรับส่งไปยังระบบโทรศัพท์ ในปัจจุบันจะเป็นมาตรฐาน RS-232F ซึ่งมีความแตกต่างกับ RS-232 เล็กน้อย โดย

มาตรฐาน RS-232 จะส่งข้อมูลได้ไม่เกิน 20 Kbps คุณลักษณะของ Electrical Component ของมาตรฐาน RS-232 จะกำหนดคุณสมบัติทางไฟฟ้าของสัญญาณและการส่งเหมือนกับมาตรฐาน ITU V.28 ซึ่งจะใช้ระดับแรงดันไฟฟ้าที่แตกต่างกัน 2 ช่วง สำหรับแทนข้อมูล โดยแรงดันที่มากกว่า +3 Volt จะมีค่าเป็น 1 ส่วนแรงดันที่มีค่าน้อยกว่าหรือเท่ากับ -3 Volt จะมีค่าเป็น 0

คุณลักษณะทางด้าน Mechanical Component ของ RS-232 จะกำหนดคุณสมบัติทางกายภาพของปลั๊กตามมาตรฐาน ISO 2110 ซึ่งมาตรฐานทั่วไปของตัวเชื่อมต่อที่ใช้คือ DB-25 ซึ่งมี 25 พิน นอกจากนี้ยังมีตัวเชื่อมต่ออีกแบบซึ่งมีขนาดเล็กกว่า คือ DB-9 ซึ่งมี 9 พิน โดยเรียกพอร์ตดังกล่าวได้อีกอย่างว่า พอร์ต ซีเรียล (Serial Port) ดังภาพที่ 5.7

ภาพที่ 5.7 แสดงภาพของ Connector แบบ DB-25 (ซ้าย) และ DB-9 (ขวา)

จากภาพที่ 5.7 สามารถนำมาแสดงการรับส่งข้อมูลระหว่าง DTE กับ DCE ด้วยอินเตอร์เฟซ แบบ DB-9 ได้ ดังภาพที่ 5.8



ภาพที่ 5.8 แสดงการรับส่งข้อมูลระหว่าง DTE กับ DCE ผ่านอินเตอร์เฟซแบบ DB-9
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 108)

ขั้นตอนของการติดต่อสื่อสารด้วยโมเด็ม ซึ่งมีการเชื่อมต่อด้วยตัวเชื่อมต่อแบบ DB-9 สามารถสรุปได้ดังนี้

1. Local DTE จะใช้งาน Data Terminal Ready ผ่านพินหมายเลข 4 เพื่อบอก DCE (ในที่นี้คือโมเด็ม) ว่าต้องการหมุนโมเด็ม

2. Local Modem ส่งสัญญาณ DCE Ready ด้วยพินหมายเลข 6 ให้กับ DTE

3. Local DTE ส่งหมายเลขโทรศัพท์ที่ต้องการหมุนให้กับโมเด็มผ่าน Transmitted Data ด้วยพินหมายเลข 3

4. Remote DTE (หรือ Remote Modem) จะแจ้งเตือนไปยัง Remote DTE ว่าจะมีการร้องขอการเชื่อมต่อจาก Local DTE ผ่าน Ring Indicator ด้วยพินหมายเลข 9 เข้ามา

5. Remote DTE จะใช้ Data Terminal Ready ผ่านพินหมายเลข 4 เพื่อแจ้งว่าพร้อมรับการเชื่อมต่อสัญญาณ

6. Remote Modem ส่ง Carrier Signal กลับไปยัง Local Modem

7. Remote Modem ส่ง DCE Ready ด้วยพินหมายเลข 6 ไปยัง Remote DTE

8. Local Modem ได้รับ Carrier Signal ที่ส่งมาจาก Remote Modem และแจ้งไปยัง DTE ด้วย Received Line Signal ผ่านพินหมายเลข 1

9. Local Modem ส่ง Carrier Signal ไปยัง Remote Modem

10. Remote Modem ได้รับ Carrier Signal และแจ้งไปยัง DTE ผ่าน Received Ling Signal Detector ด้วยพินหมายเลข 1

11. หาก Local DTE ต้องการส่งข้อมูลจะใช้ Request To Send ผ่านพินหมายเลข 7

12. Local Modem ตอบสนองด้วยการส่ง Clear To Send ผ่านพินหมายเลข 8

13. Local DTE ส่งข้อมูลดิจิทัลผ่าน Transmitted Data ด้วยพินหมายเลข 3 ไปยัง Local Modem ซึ่งจะแปลงข้อมูลดิจิทัลให้กลายเป็นสัญญาณแอนะล็อกเพื่อส่งไปยัง Remote Modem

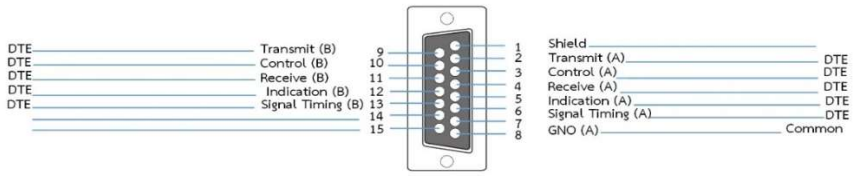
14. เมื่อสัญญาณมาถึง Remote Modem จะแปลงสัญญาณแอนะล็อกให้เป็นข้อมูลดิจิทัลแล้วส่งให้กับ DTE ผ่าน Received Data ด้วยพินหมายเลข 2

2. EIA RS-449 อินเตอร์เฟซที่มีอัตราเร็วในการส่งข้อมูลแบบมาตรฐาน RS-232 นั้นทำได้ค่อนข้างช้า ดังนั้น EIA จึงได้พัฒนาอินเตอร์เฟซมาตรฐานใหม่ขึ้นมา คือ RS-449 เพื่อนำมาใช้แทน RS-232 และได้มีการปรับปรุงการทำงานในส่วนต่างๆ ให้ดีขึ้น เพิ่มวงจรใหม่ 10 ฟังก์ชัน แต่ก็ไม่ได้รับความนิยมมากนัก โดยมาตรฐาน RS-449 สามารถส่งข้อมูลได้ถึง 2 Mbps และเปลี่ยนมาใช้ตัวเชื่อมต่อแบบ 37 พิน ดังภาพที่ 5.9

ภาพที่ 5.9 แสดงภาพ Connector แบบ RS-449

3. X.21 เป็นอินเตอร์เฟซที่ได้รับการออกแบบสำหรับนำมาใช้แทนมาตรฐาน RS-232 นิยมนำมาใช้สำหรับส่งข้อมูลแบบดิจิทัลระหว่างคอมพิวเตอร์กับระบบ ISDN โดยมาตรฐานของ X Series ถูกพัฒนามาเพื่อใช้งานกับ Switching, Routing และส่งสัญญาณแบบไบนารี ส่วน V Series ถูกออกแบบมาเพื่อส่งสัญญาณแบบแอนะล็อกจึงเหมาะกับการส่งสัญญาณเสียงมากกว่า

มาตรฐาน X.21 จะใช้ตัวเชื่อมต่อแบบ 15 พิน และมีเพียง 4 วงจรเท่านั้น โดย แต่ละวงจรสามารถบรรจุสัญญาณที่แตกต่างกันได้ พิจารณาตัวเชื่อมต่อแบบ X.21 ดังภาพที่ 5.10



ภาพที่ 5.10 แสดงภาพตัวเชื่อมต่อแบบ X.21

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 108)

4. RAID (Redundant Array of Independent Disk) เป็นเทคโนโลยีอินเตอร์เฟซที่ใช้เชื่อมต่อฮาร์ดดิสก์หลายๆ ตัวไว้ภายในคอมพิวเตอร์เครื่องเดียวกัน เรียกว่า Disk Array โดยจะมองเหมือนเป็นฮาร์ดดิสก์ตัวเดียวกันและเก็บข้อมูลบางส่วนที่เหมือนกันไว้ในฮาร์ดดิสก์แต่ละตัว (ยกเว้น RAID 0 ที่ไม่มีการเก็บข้อมูลซ้ำกัน) ลักษณะดังกล่าวเป็นการเพิ่มประสิทธิภาพในการเก็บรักษาข้อมูลไม่ให้มีการสูญหายได้ดียิ่งขึ้น โดย RAID มีรูปแบบต่างๆ ที่สำคัญ ดังนี้

4.1 RAID 0 เพื่อเพิ่มความเร็วในการอ่านและเขียนข้อมูลในฮาร์ดดิสก์ โดยนำฮาร์ดดิสก์มากกว่า 1 ตัว มาต่อกันในลักษณะแบบ Non-Redundant เรียกเทคนิคนี้ว่า Striping ดังนั้น ถ้าฮาร์ดดิสก์ตัวใดเสียหายข้อมูลต่างๆ ที่อยู่ในฮาร์ดดิสก์ตัวนั้นก็จะสูญหายตามไปด้วย

4.2 RAID 1 หรือเรียกว่า Disk Mirroring เพื่อสร้างความปลอดภัยให้กับข้อมูลประกอบด้วยฮาร์ดดิสก์ 2 ตัว ซึ่งเก็บข้อมูลเหมือนกันทุกประการ ดังนั้น หากฮาร์ดดิสก์ตัวใดตัวหนึ่งได้รับความเสียหาย ข้อมูลก็จะถูกเก็บไว้ในฮาร์ดดิสก์อีกตัวหนึ่ง และถูกเรียกใช้งานได้ตามปกติ

4.3 RAID 2 มีจุดเด่นในเรื่องของการป้องกันข้อมูล โดยจะแบ่งข้อมูลในระดับบิต เพื่อเก็บลงในฮาร์ดดิสก์แต่ละตัว และมีฮาร์ดดิสก์กลุ่มหนึ่งเก็บข้อมูลที่ใช้ในการตรวจสอบและแก้ไขข้อผิดพลาด (ECC หรือ Error Checking and Correcting) ทำให้ข้อมูลมีความปลอดภัยมากยิ่งขึ้น หากข้อมูลมีการสูญหายสามารถเรียกคืนได้ผ่านฮาร์ดดิสก์ที่เก็บข้อมูลของ ECC ไว้ จุดด้อยของ RAID 2 คือ ต้องใช้ฮาร์ดดิสก์จำนวนมากในการเก็บรักษาข้อมูล ทำให้ฮาร์ดดิสก์ทั้งระบบต้องทำงานหนักขึ้น RAID 2 จึงไม่เป็นที่นิยมมากนัก

4.4 RAID 3 มีลักษณะคล้ายกับ RAID 2 แต่มีการปรับปรุงให้สามารถอ่านและเขียนข้อมูลได้เร็วยิ่งขึ้น เพราะใช้วิธีการต่อพ่วงฮาร์ดดิสก์แต่ละตัวแบบ Stripe และมีการตัดแบ่งข้อมูลแนวระดับ Byte นอกจากนี้ยังใช้ Parity ในการตรวจสอบและแก้ไขข้อผิดพลาดของข้อมูลแทน ECC และใช้ฮาร์ดดิสก์เก็บ Parity เพียงแค่ตัวเดียวเท่านั้น แต่ปัญหาของการใช้ RAID 3 คือ ปัญหาคอขวด เนื่องจากมีการกระจายข้อมูลไปอย่างทุกฮาร์ดดิสก์ ทำให้ฮาร์ดดิสก์ที่เก็บ Parity ทำงานได้ช้า

4.5 RAID 4 มีลักษณะทำงานคล้ายกับ RAID 3 แต่จะตัดแบ่งข้อมูลในระดับ Block ทำให้การอ่านข้อมูลแบบ Random ทำได้อย่างรวดเร็ว

4.6 RAID 5 จะใช้วิธีการกระจายการเก็บ Parity ไว้ในฮาร์ดดิสก์แต่ละตัว โดยถูกรวม อยู่กับข้อมูลทั่วไป ช่วยลดปัญหาคอขวดที่เกิดขึ้นใน RAID 3 และ RAID 4 นอกจากนี้ยังสามารถเปลี่ยนฮาร์ดดิสก์ที่มีปัญหาได้ในขณะที่ระบบยังทำงานอยู่ เรียกว่า Hot Swap นั่นเอง

5.6 มาตรฐานของอินเตอร์เฟซที่ใช้รับส่งข้อมูลด้วยความเร็วสูง

มาตรฐานของอินเตอร์เฟซได้มีการพัฒนารูปแบบใหม่ๆ ขึ้นมา เพื่อใช้เชื่อมต่อระหว่างอุปกรณ์ต่างๆ โดยมีอินเตอร์เฟซที่น่าสนใจ 6 รูปแบบ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 111-113)

5.6.1 FireWire

FireWire เป็น IEEE 1394 เป็นมาตรฐานในการเชื่อมต่ออุปกรณ์ต่างๆ โดยสามารถพ่วงต่ออุปกรณ์ได้มากกว่า 60 ชิ้น และสามารถรับส่งข้อมูลได้ถึง 400 Mbps นิยมนำมาใช้กับอุปกรณ์ประเภทมัลติมีเดียที่ต้องใช้อัตราการส่งข้อมูลสูง และเนื่องจาก FireWire ถูกนำมาใช้เป็น Digital Interface ของข้อมูลแบบดิจิทัล ทำให้ไม่ต้องมีการแปลงสัญญาณดิจิทัลของเครื่องคอมพิวเตอร์ให้เป็นสัญญาณแอนะล็อก และสนับสนุนการทำงานแบบ Hot Plug คือ เชื่อมต่อและใช้งานได้ทันที

FireWire รองรับการเชื่อมต่อ 2 รูปแบบ คือ Asynchronous Connection และ Isochronous Connection โดย Asynchronous Connection จะสนับสนุนอุปกรณ์แบบเก่า เช่น Modem และ Printer ส่วน Isochronous Connection จะรองรับการส่งข้อมูลด้วยความเร็วสูง ซึ่งเป็นสิ่งสำคัญสำหรับการขนส่งข้อมูลแบบมัลติมีเดีย ดังนั้น FireWire จึงเหมาะสำหรับการขนส่งข้อมูลในรูปแบบดิจิทัล เสียง และวิดีโอต่างๆ

5.6.2 Universal Serial Bus (USB)

USB เป็นมาตรฐานเชื่อมต่อแบบใหม่ที่ได้รับการพัฒนาร่วมกันระหว่าง Compaq, IBM, Intel, DEC, Northern Telecom, NEC และ Microsoft เพื่อเพิ่มประสิทธิภาพในการเชื่อมต่อให้กับอุปกรณ์ต่างๆ และช่วยลดปัญหาการใช้มาตรฐานการเชื่อมต่อที่แตกต่างกันของอุปกรณ์ USB นั้นเป็น Digital Interface ที่ทำให้อุปกรณ์ที่ใช้การเชื่อมต่อแบบ Parallel และ Serial สามารถใช้ตัวเชื่อมต่อแบบเดียวกันได้ USB มีการเชื่อมต่อแบบ USB คือ

Plug & Play ซึ่งเป็นคุณสมบัติที่ทำให้คอมพิวเตอร์รู้จักกับอุปกรณ์ที่เชื่อมต่อกันได้แบบอัตโนมัติ นอกจากนี้ยังสนับสนุน Hot Swap ทำให้สามารถถอดอุปกรณ์ได้โดยไม่ต้องปิดคอมพิวเตอร์

การใช้งาน USB ในช่วงแรกจะมีความเร็วประมาณ 1.5 Mbps ซึ่งค่อนข้างช้า จึงได้มีการพัฒนาให้มีความเร็วเพิ่มขึ้นปัจจุบัน USB ได้มีการพัฒนามาตรฐานเป็น USB 3.0, USB 3.1, USB 3.2, USB 4.0, USB Type A, USB Type C

5.6.3 SCSI

Small Computer System Interface (SCSI) หรือ สกัสซี่ เป็นมาตรฐานการเชื่อมต่อระหว่างอุปกรณ์ฮาร์ดแวร์กับระบบบัสด้วยความเร็วสูง แต่ต้องติดตั้ง SCSI Adapter หรือ SCSI Control สำหรับการควบคุมการเชื่อมต่อ สามารถเชื่อมต่ออุปกรณ์ได้ถึง 7-15 ชิ้น ต่อ SCSI 1 พอร์ต โดยทั่วไปอุปกรณ์ที่นำมาเชื่อมต่อจะเป็นสื่อสำหรับเก็บข้อมูลที่มีความจุสูง เช่น CD-ROM, DVD-ROM, Printer, Scanner และ ZIP Drive ปัจจุบัน SCSI ได้รับความนิยมน้อยลง เนื่องจากมีอินเตอร์เฟซชนิดอื่น คือ USB และ FireWire ซึ่งได้รับความนิยมเพิ่มขึ้น จุดเด่นของ SCSI คือ การนำ ไปใช้เชื่อมต่อกับฮาร์ดดิสก์มากกว่า 1 ตัว ข้อมูลมีความปลอดภัยมากขึ้น สามารถถอดเปลี่ยนฮาร์ดดิสก์ตัวใหม่เข้าไปได้ในขณะที่ระบบกำลังทำงานอยู่การเชื่อมต่อแบบ SCSI นิยมไปใช้กับ Database Server และ File Server

5.6.4 PATA และ SATA

ปัจจุบันการเชื่อมต่ออุปกรณ์ภายในต่างๆ ของคอมพิวเตอร์ เช่น ฮาร์ดดิสก์และไดร์ฟซีดีรอมต่างๆ นิยมใช้การเชื่อมต่อผ่านมาตรฐาน SATA (Serial Advanced Technology Architecture) ซึ่งเป็นสถาปัตยกรรมใหม่ที่ใช้ในการเชื่อมต่ออุปกรณ์ภายในต่างๆ แทนมาตรฐานการเชื่อมต่อแบบ PATA หรือ Parallel ATA ซึ่งมีข้อจำกัด คือ มีอัตราความเร็วในการส่งข้อมูลเพียง 133 Mbyte/sec เท่านั้น การเชื่อมต่อ SATA สามารถเชื่อมต่อและติดตั้งง่าย สายที่ใช้เชื่อมต่อมีความยาวได้ถึง 2 เมตร และมีความเร็วในการส่งข้อมูลสูงกว่า USB 2.0 และ FireWire ถึง 6 เท่า

5.6.5 eSATA หรือ External SATA

eSATA เป็นอินเตอร์เฟซแบบใหม่สามารถนำฮาร์ดดิสก์หรืออุปกรณ์อื่นๆ มาเชื่อมต่อกับคอมพิวเตอร์แบบ SATA ได้ทันทีโดยไม่ต้องปิดเครื่องเหมือนกับการเชื่อมต่อผ่านพอร์ต USB และ FireWire แต่ eSATA สามารถส่งข้อมูลได้เร็วกว่าหลายเท่าตัว

5.7 สรุป

การเชื่อมต่อกับอินเทอร์เน็ตผ่านโมเด็ม โดยโมเด็มจะแปลงข้อมูลของคอมพิวเตอร์ที่มีอยู่ในรูปแบบดิจิทัลให้เป็นสัญญาณแอนะล็อกก่อนจึงจะสามารถส่งสัญญาณไปบนสายโทรศัพท์ได้ โดยเทคนิคที่ใช้ในการแปลงจากข้อมูลดิจิทัลเป็นสัญญาณแอนะล็อก คือ การ Modulation โมเด็มที่มีคุณสมบัติต่างๆ มากมายรองรับอัตราการส่งข้อมูลที่มีหลายรูปแบบ มีระบบรักษาความปลอดภัย หรือระบบการตรวจสอบและแก้ไขข้อผิดพลาด เป็นต้น โดยโมเด็มที่ใช้งานในยุคแรกจะมีความเร็วเพียง 33 Kbps ต่อมาได้มีการพัฒนาให้มีความเร็วเพิ่มขึ้นเป็น 56 Kbps เรียกว่าโมเด็ม 56K

เทคโนโลยีในการ Dial-Up Modem เพื่อส่งข้อมูลมีอยู่หลายรูปแบบ นอกจากการส่งข้อมูลผ่านสายโทรศัพท์แบบดั้งเดิมแล้ว ยังมีเทคนิคในการส่งข้อมูลอีก 4 แบบ ซึ่งสามารถนำมาใช้เชื่อมต่อคอมพิวเตอร์กับระบบเครือข่ายระยะไกลได้ คือ T1 Digital Telephone Line, Cable Television Network, Integrated Service Digital Network (ISDN) และ Digital Subscriber Line (DSL) โดยเทคโนโลยีการส่งข้อมูลแต่ละรูปแบบจะต้องมีอุปกรณ์เฉพาะของตนเพื่อแปลงข้อมูลดิจิทัลให้อยู่ในรูปแบบที่สามารถจัดส่งออกไปได้ โดยเทคโนโลยีที่กำลังได้รับความนิยมอย่างสูง คือ DSL

การเชื่อมต่อทางกายภาพของคอมพิวเตอร์กับอุปกรณ์ต่างๆ เช่น โมเด็ม ต้องอาศัยมาตรฐานการเชื่อมต่อ หรือ อินเตอร์เฟซ ซึ่งมีอยู่หลายมาตรฐาน แต่ทุกมาตรฐานการเชื่อมต่อจะมีคุณลักษณะสำคัญ 2 ข้อ คือ ต้องได้รับการพัฒนาและเห็นชอบจากองค์กรชั้นนำและต้องมี 4 Component

มาตรฐานการเชื่อมต่อแบบเดิม เช่น RS-232 และ EIS RS-499 นั้น มีอัตราการรับส่งข้อมูลที่ค่อนข้างช้า ดังนั้น จึงมีการพัฒนามาตรฐานการเชื่อมต่อแบบใหม่ๆ ขึ้นมา ทำให้การรับส่งข้อมูลมีความเร็วขึ้น เช่น USB และ FireWire เป็นต้น ซึ่งสามารถส่งข้อมูลได้หลายร้อยล้านบิตต่อวินาที (Mbps) โดยเรียกมาตรฐานการเชื่อมต่อประเภทนี้ว่า มาตรฐานการเชื่อมต่อความเร็วสูง

บทที่ 6
การตรวจสอบข้อผิดพลาดและการควบคุมการไหลของข้อมูล

กระบวนการส่งข้อมูลไปบนสื่อกลางประเภทต่างๆ อาจมีความผิดพลาดเกิดขึ้นระหว่างการขนส่งได้ โดยรูปแบบของข้อมูลที่ส่งมาจากต้นทางอาจถูกสัญญาณรบกวน (Noise) ระหว่างกระบวนการขนส่งจนข้อมูลมีรูปแบบที่เปลี่ยนแปลงไป ทำให้ผู้รับปฏิเสธการรับข้อมูลดังกล่าว เนื่องจากข้อมูลที่ส่งมาไม่อยู่ในรูปแบบที่ถูกต้อง อย่างไรก็ตามการส่งข้อมูลไม่สามารถหลีกเลี่ยงสัญญาณรบกวนได้ ดังนั้น วิธีแก้ไขปัญหาดังกล่าว คือ การตรวจสอบความผิดพลาดของข้อมูล

6.1 สัญญาณรบกวนและข้อผิดพลาด

สัญญาณรบกวน (Noise) เป็นสัญญาณที่ไม่พึงประสงค์ทำให้สัญญาณข้อมูลเกิดความผิดพลาดได้ สัญญาณรบกวนเกิดมาจากหลายสาเหตุด้วยกัน เช่น สภาพแวดล้อมที่ส่งผลให้เกิดสัญญาณรบกวนทางไฟฟ้าหรืออุณหภูมิ การป้องกันสัญญาณรบกวนสามารถทำได้หลายวิธีขึ้นอยู่กับชนิดของสัญญาณรบกวน ดังนั้น การทำความเข้าใจเกี่ยวกับความแตกต่างและสาเหตุของการเกิดสัญญาณรบกวนแต่ละรูปแบบจะช่วยให้การนำเทคนิคและการนำสัญญาณรบกวน (Noise Reduction) มาใช้เพื่อจำกัดปริมาณของสัญญาณรบกวนที่จะส่งไปยังผู้รับทำได้สะดวกขึ้น

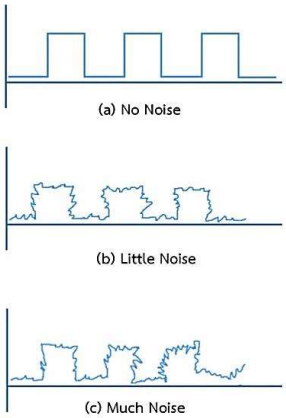
ข้อผิดพลาด (Error) ที่เกิดขึ้นระหว่างการส่งข้อมูล เกิดขึ้นได้หลายสาเหตุ เช่น การส่งสัญญาณไฟฟ้าที่ไม่ต่อเนื่อง ซึ่งอาจเกิดข้อผิดพลาดจากไฟฟ้าดับหรือการใช้สายทองแดงแบบเก่าที่ถูกรบกวนโดยสัญญาณต่างๆ ระบบไมโครเวฟและวิทยุ ก็สามารถถูกรบกวนโดยสัญญาณต่างๆ ได้ แม้แต่การส่งข้อมูลผ่านสายใยแก้วนำแสง (Fiber-Optic) ก็สามารถถูกรบกวนโดยสัญญาณรบกวนในรูปแบบต่างๆ ได้เช่นกัน (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 181)

6.1.1 ประเภทของสัญญาณรบกวน

สัญญาณรบกวนส่งผลต่อความสูญเสียของสัญญาณ สัญญาณรบกวนมีหลายชนิด ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 181-185 และ (พิสิฐ พรพงศ์เตชวาณิช และ พงษ์พิสิฐ วุฒิดิษฐโชติ, 2566, หน้า 123)

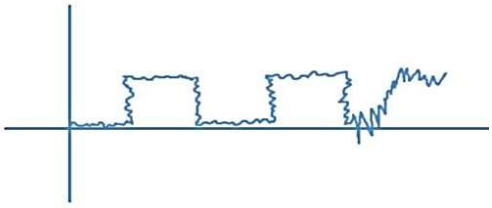
1. ไวท์นอยส์ (White Noise) หรือ เทอร์มัลนอยส์ (Thermal Noise) จัดเป็นสัญญาณรบกวนที่เกิดจากอุณหภูมิความร้อน ซึ่งไม่สามารถหลีกเลี่ยงได้เพราะเป็นผลพวงมาจาก

การเคลื่อนที่ของอิเล็กตรอนบนลวดตัวนำ ดังนั้น ถ้าอุณหภูมิสูงขึ้นระดับของสัญญาณรบกวนก็สูงขึ้นตาม สัญญาณรบกวนชนิดนี้ไม่มีรูปแบบที่แน่นอน สามารถกระจายไปทั่วบนย่านความถี่ต่างๆ การป้องกันสามารถทำได้ด้วยการใช้อุปกรณ์ปรับสัญญาณกรณีเป็นสัญญาณดิจิทัล ดังภาพที่ 6.1



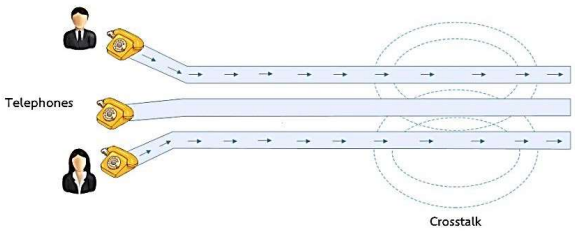
ภาพที่ 6.1 ลักษณะของสัญญาณที่ถูกรบกวนด้วยไวท์นอยส์ (White Noise) ขนาดต่างๆ
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 182)

2. อิมพัลส์นอยส์ (Impulse Noise) หรือ Noise Spike เป็นสัญญาณรบกวนแบบไม่ต่อเนื่อง (Noncontiguous Noise) ที่เกิดขึ้นในระยะเวลาสั้นๆ ซึ่งยากต่อการตรวจสอบ เนื่องจากสัญญาณรบกวนในลักษณะนี้จะเกิดแบบสุ่ม และอาจอยู่ในช่วงใดของสัญญาณก็ได้ สัญญาณรบกวนแบบ Impulse Noise เกิดจากแรงดันของกระแสไฟฟ้าแรงสูงจากภายนอก ได้แก่ ฟ้าผ่า ส่งผลให้กระแสไฟฟ้าภายในสายทองแดงเปลี่ยนไปจากเดิม หรืออาจเกิดจากอุปกรณ์ที่สร้างหรือใช้กระแสไฟฟ้าแรงดันสูง เช่น เครื่องกำเนิดไฟฟ้าหรือมอเตอร์ไฟฟ้าขนาดใหญ่ ดังภาพที่ 6.2 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 126)



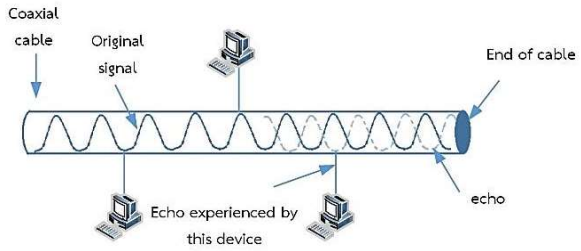
ภาพที่ 6.2 ลักษณะของสัญญาณที่ถูกรบกวนด้วย Impulse Noise
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 126)

3. ครอสทอล์ก (Crosstalk) คือ สัญญาณรบกวนที่เกิดจากการวางสายสื่อสารหลายๆ เส้นไว้ด้วยกันทำให้สัญญาณรบกวนจากสายต่างๆ รบกวนซึ่งกันและกัน นอกจากนี้การใช้สายสื่อสารที่มีขนาดเล็กเกินไปหรือการใช้สายสื่อสารที่มีระดับความแรงมากไปก็ทำให้เกิดปัญหานี้ได้ ในระบบโทรศัพท์แบบเก่าที่ใช้สายหุ้มฉนวนก็ได้รับผลกระทบจากสัญญาณ Crosstalk ทำให้ผู้ใช้ได้ยินเสียงรบกวนในสายโทรศัพท์ขณะทำการสนทนา สาเหตุสำคัญอีกประการที่ทำให้เกิด Crosstalk คือความชื้นสัมพัทธ์และอากาศที่เปียกขึ้นจึงทำให้มี Crosstalk ในสายสัญญาณของระบบโทรศัพท์เพิ่มมากขึ้น ดังภาพที่ 6.3



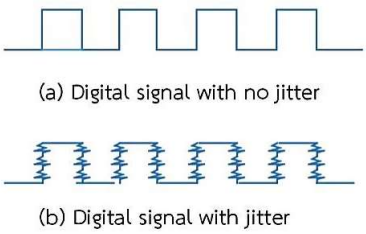
ภาพที่ 6.3 ลักษณะของสัญญาณที่ถูกรบกวนด้วย Crosstalk
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 183)

4. เอกโค (Echo) เป็นสัญญาณสะท้อนกลับ (Reflection) ซึ่งคล้ายกับการตะโกนเสียงใสในห้องว่างๆ แล้วเสียงนั้นก้องกลับมาให้เราได้ยิน เอกโคเกิดขึ้นได้ในกรณีใช้สายโคแอ็กเชียลเป็นสื่อกลาง เมื่อสัญญาณได้เดินทางไปยังสุดปลายสายจะเกิดการสะท้อนกลับ ทำให้โหนดใกล้เคียงได้ยินและคิดว่าสายส่งสัญญาณในขณะนั้นไม่ว่าง จึงรอส่งข้อมูลแทนที่จะส่งข้อมูลได้ทันที การป้องกันทำได้โดยใช้อุปกรณ์ที่เรียกว่า **เทอร์มิเนเตอร์** (Terminator) เช่น ในระบบเครือข่ายท้องถิ่นที่เชื่อมต่อแบบบัส ปลายสายทั้งสองฝั่งของสายโคแอ็กเชียลจะต้องถูกปิดด้วยเทอร์มิเนเตอร์ เพื่อดูดซับสัญญาณเหล่านี้ มิให้เกิดการสะท้อนกลับมา ดังภาพที่ 6.4



ภาพที่ 6.4 ลักษณะของสัญญาณที่ถูกรบกวนด้วยสัญญาณสะท้อนกลับ (Echo/Reflection)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 183)

5. จิตเตอร์ (Jitter) เป็นเหตุการณ์ที่เกิดจากความถี่ของสัญญาณถูกเปลี่ยนแปลงไปอย่างต่อเนื่อง ทำให้มีการเลื่อนเฟสไปเป็นค่าอื่นๆ อย่างต่อเนื่องด้วย ในการป้องกันทำได้ด้วยการเลือกใช้วงจรอิเล็กทรอนิกส์ที่มีคุณภาพ หรือการนำอุปกรณ์รีพีตเตอร์มาใช้ ดังภาพที่ 6.5



ภาพที่ 6.5 ลักษณะของสัญญาณที่ถูกรบกวนด้วย Jitter
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 184)

6. Delay Distortion เป็นการผิดเพี้ยนของสัญญาณที่เกิดจากการเคลื่อนที่ของสัญญาณข้อมูลที่มีความถี่ต่างกันด้วยความเร็วที่ต่างกัน ทำให้สัญญาณที่ส่งมาทีหลังซ้อนทับสัญญาณก่อนหน้าจนเกิดการผสมรวมกันทำให้ข้อมูลผิดพลาด ส่วนวิธีการแก้ไขทำได้โดยติดตั้งอุปกรณ์ Equalizer เพื่อปรับความเร็วในการเคลื่อนที่ของแต่ละความถี่ให้เท่ากัน

7. Attenuation เกิดจากสัญญาณที่ส่งอ่อนกำลังลงทำให้ถูกรบกวนได้ง่าย วิธีแก้ปัญหาดังกล่าวทำได้โดยใช้อุปกรณ์ Amplifier หรือ Repeater เพื่อเพิ่มกำลังให้สัญญาณแอนะล็อกหรือสัญญาณดิจิทัลตามลำดับ

6.2 การป้องกันข้อผิดพลาด

การป้องกันข้อผิดพลาด (Error Prevention) จากสัญญาณรบกวนและข้อผิดพลาดที่เกิดขึ้นระหว่างการส่งข้อมูลนั้นมีหลายรูปแบบโดยผลกระทบที่ได้รับจากสัญญาณรบกวนระหว่างการส่งข้อมูล คือ สถานีที่ส่งสัญญาณมีอัตราการส่งข้อมูลลดลงทำให้อัตราเร็วในการรับข้อมูลของฝั่งผู้รับสูงกว่า การป้องกันข้อผิดพลาดก่อนที่จะเกิดปัญหารบกวน สามารถทำได้หลายวิธี ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 128)

1. การติดตั้งสัญญาณที่มีฉนวนหุ้มเพื่อลดสัญญาณรบกวนที่เกิดจากสนามแม่เหล็กไฟฟ้าหรือ Crosstalk

2. ใช้สายโทรศัพท์ที่มีการกรองสัญญาณรบกวนซึ่งถูกจัดเตรียมโดยผู้ให้บริการโทรศัพท์ เช่น สายคู่เช่า (Leased Line) ซึ่งมีการกรองสัญญาณมีระดับคงที่และมีอัตราการเกิดข้อผิดพลาดต่ำ

3. เปลี่ยนมาใช้อุปกรณ์ที่มีเทคโนโลยีใหม่ๆ แม้ว่าอุปกรณ์เหล่านี้จะมีราคาแพงก็ตาม แต่ก็สามารถลดข้อผิดพลาดต่างๆ ได้เป็นอย่างดี

4. การติดตั้งอุปกรณ์ทวนสัญญาณ เช่น Repeater สำหรับเพิ่มกำลังสัญญาณดิจิทัล หรือติดตั้ง Amplifier เพื่อเพิ่มกำลังสัญญาณแอนะล็อก เป็นต้น

5. ตรวจสอบคุณสมบัติของสื่อกลางที่จะนำมาใช้ เช่น สาย CAT5e สามารถส่งข้อมูลได้ในระยะไม่เกิน 100 เมตร หากนำสาย CAT5e มาใช้ส่งสัญญาณที่มีระยะทางมากกว่า 100 เมตร อาจทำให้สัญญาณขาดหาย ดังนั้น จะต้องติดตั้ง Repeater เพื่อทวนสัญญาณด้วย ปัจจุบันได้พัฒนาสาย CAT5e เป็น CAT6e

สรุปวิธีการป้องกันสัญญาณรบกวนในรูปแบบต่างๆ ดังแสดงในตารางที่ 6.1

ตารางที่ 6.1 แสดงวิธีการป้องกันสัญญาณรบกวนในรูปแบบต่างๆ

ชนิดของ Noise	**เทคนิคที่ใช้ป้องกัน**
White Noise	ใช้ Filter กับสัญญาณแอนะล็อก และใช้ Signal Generator กับสัญญาณดิจิทัล
Impulse Noise	ใช้ Filter พิเศษเพื่อปรับปรุงสัญญาณแอนะล็อก
Crosstalk	หุ้มฉนวนให้กับสายเคเบิล
Echo	ติดตั้งอุปกรณ์ป้องกันสัญญาณย้อนกลับที่ต้นและปลายสายโคแอ๊กเชียล
Jitter	เพิ่มอุปกรณ์อิเล็กทรอนิกส์ที่มีประสิทธิภาพมากขึ้น
Delay Distortion	เพิ่มอุปกรณ์ Equalize เพื่อปรับระดับความเร็วในการส่งข้อมูลของความถี่แตกต่างกัน
Attenuation	ใช้อุปกรณ์ Amplifier กับสัญญาณแอนะล็อก ส่วนสัญญาณดิจิทัลให้ใช้ Regenerator

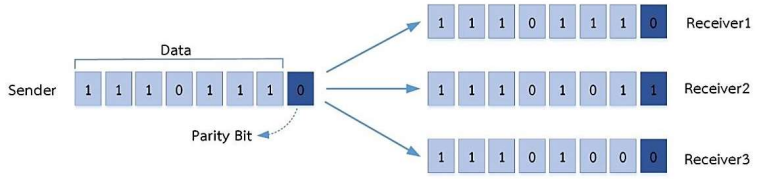
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 128)

6.3 การตรวจสอบข้อผิดพลาด

แม้ว่าจะมีการใช้เทคนิคต่างๆ เพื่อป้องกันข้อผิดพลาดที่เกิดขึ้น แต่ในบางครั้งข้อมูลก็อาจเกิดข้อผิดพลาดขึ้นได้ ดังนั้น จึงจำเป็นต้องมีการตรวจสอบข้อผิดพลาดที่อาจเกิดขึ้นกับข้อมูลที่รับมา เพื่อให้มั่นใจได้ว่าข้อมูลดังกล่าวมีความถูกต้องและไม่มีข้อผิดพลาดใดๆ เกิดขึ้นระหว่างการส่งข้อมูล หากตรวจสอบพบข้อผิดพลาดจะต้องใช้เทคนิคต่างๆ เพื่อนำมาแก้ไขปัญหาที่เกิดขึ้นได้อย่างถูกต้อง โดยสามารถเพิ่มกระบวนการตรวจสอบข้อผิดพลาดไว้ในแบบจำลองของการสื่อสารได้หลายส่วนแต่โดยทั่วไปนิยมเพิ่มไว้ใน Data Link Layer เมื่อมีการสร้างเฟรมข้อมูลในระดับชั้น Data Link จะมีการเพิ่มข้อมูลบางอย่างสำหรับการตรวจสอบข้อผิดพลาด (Error-Detection) เมื่อเฟรมข้อมูลถูกส่ง ไปยังปลายทางแล้ว อุปกรณ์ปลายทางจะรับข้อมูลตามลำดับและนำข้อมูลในส่วนของ Error Detection เพื่อตรวจสอบความถูกต้องต่อไป โดยวิธีการตรวจสอบข้อผิดพลาดสามารถทำได้หลายวิธี ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 128-131)

1. Parity Check เป็นการตรวจสอบข้อผิดพลาดแบบง่ายๆ ใช้กับ Asynchronous Connection โดย Parity Check มี 2 ประเภท คือ Simple Parity และ Longitudinal Parity

1.1 Simple Parity หรือ Vertical Redundancy Check เป็นวิธีการตรวจสอบข้อ ผิดพลาดที่มีวิธีการแบบเรียบง่าย โดยสามารถทำได้ 2 วิธี คือ Even Parity โดยการเติมบิต 0 ต่อท้ายบิตข้อมูล หากจำนวนบิต 1 ภายในข้อมูลมีค่าเป็นเลขคู่ เพื่อให้จำนวนบิต 1 เป็นเลขคู่เหมือนเดิม และ Odd Parity ซึ่งจะเติมบิต 1 ในบิตข้อมูล หากจำนวนบิต 1 ภายในข้อมูลเป็นเลขคี่ เพื่อให้จำนวนบิต 1 เป็นเลขคู่ ถ้านำวิธีการดังกล่าวมาใช้ในการตรวจสอบข้อมูล ตัวอักษรที่เข้ารหัสด้วย ASCII ซึ่งมีขนาด 7 บิต Parity Bit จะถูกเพิ่มต่อท้ายข้อมูลเป็นบิตที่ 8 เช่น ตัวอักษร W ซึ่งเขียนในรูปแบบของไบนารี คือ 1110111 หากใช้วิธีของ Parity Bit จะต้องนับจำนวนบิตที่มีค่าเป็น 1 ในที่นี้ได้เป็นเลขคู่ (Even) ดังนั้น จึงเติมบิต 0 ต่อท้ายทำให้ได้ข้อมูลเป็น 11101110 เป็นต้น แต่ข้อจำกัดที่สำคัญของ Simple Parity คือ สามารถตรวจสอบข้อผิดพลาดได้เพียงบิตเดียวเท่านั้น ไม่สามารถตรวจสอบข้อผิดพลาดที่เกิดขึ้นตั้งแต่ 2 บิตขึ้นไป หรือ Burst Error ได้ เช่น หากได้รับข้อมูลของตัวอักษร W เป็น 10001110 ซึ่งมีบิตข้อมูลที่ผิดพลาดจำนวน 2 บิต การใช้ Simple Parity จะไม่สามารถตรวจสอบได้ ดังนั้นวิธี Simple Parity จึงไม่มีประสิทธิภาพเท่าที่ควร นอกจากนี้ยังต้องมีการเพิ่มจำนวนบิตให้กับทุกตัวอักษร หากมีการส่งข้อมูลจำนวนมากจะทำให้ข้อมูลมีขนาดใหญ่ขึ้นด้วย ตัวอย่างการตรวจสอบความถูกต้องของตัวอักษร W ซึ่งมีข้อมูลเป็น 1110111 ด้วยวิธี Simple Parity ดังภาพที่ 6.6



ภาพที่ 6.6 แสดงการตรวจสอบข้อมูลด้วยวิธี Simple Parity

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 129)

จากภาพข้างต้นเมื่อ Sender ส่งข้อมูลไปยังปลายทาง 3 แห่ง คือ Receiver1, Receiver2 และ Receiver3 โดย Receiver1 ได้รับข้อมูลที่ถูกต้องส่วน Receiver2 ได้รับข้อมูลที่ข้อมูลผิดพลาดจำนวน 1 บิต ทำให้ Parity Bit ถูกเปลี่ยนจาก 0 ไปเป็น 1 เมื่อใช้วิธีการตรวจสอบด้วย Simple Parity จะสามารถตรวจจับได้เนื่องจาก Parity Bit ของ sender มีค่าเป็น 0 แต่ Parity Bit ของ Receiver 2 มีค่าเป็น 1 นั่นเอง แต่ในกรณีของ Receiver3 ซึ่งมีข้อผิดพลาดจำนวน 2 บิต จะไม่สามารถตรวจสอบข้อผิดพลาดได้เนื่องจาก Parity Bit ของ Sender และ Receiver3 มีค่าเหมือนกัน

1.2 Longitudinal Parity หรือ Horizontal Parity เป็นวิธีที่นำมาใช้เพื่อแก้ไขปัญหาที่เกิดขึ้นกับ Simple Parity โดยจัดเตรียมบิตเพิ่มเติม เรียกว่า Parity Check ไว้สำหรับตรวจสอบข้อผิดพลาดที่จำเป็น โดยวิธีการนี้สามารถตรวจจับ Burst Error ได้แต่ไม่สามารถตรวจสอบข้อมูลที่มีบิตข้อผิดพลาดเป็นจำนวนคู่ในตำแหน่งเดียวกันได้เนื่องจากจะมีค่า Parity Check และ Parity Bit ค่าเดิม ดังแสดงในตารางที่ 6.2 และ 6.3

ตารางที่ 6.2 แสดงตารางของข้อมูลต้นฉบับ

ข้อมูล	ไบนารี							Parity Bit
Data 1	1	1	0	1	0	1	1	1
Data 2	1	1	1	1	1	1	1	1
Data 3	0	1	0	1	0	1	0	1
Data 4	0	0	1	1	0	0	1	1
Parity Check	0	1	0	0	1	1	1	0

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 130)

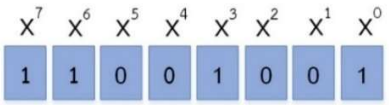
ตารางที่ 6.3 แสดงข้อผิดพลาดใน Data1 และ Data2 ที่ Longitudinal Parity ไม่สามารถตรวจสอบพบได้

ข้อมูล	ไบนารี							Parity Bit
Data 1	1	0	1	1	0	1	1	1
Data 2	1	0	0	1	1	1	1	1
Data 3	0	1	0	1	0	1	0	1
Data 4	0	0	1	1	0	0	1	1
Parity Check	0	1	0	0	1	1	1	0

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 130)

2. Cyclic Redundancy Checksum (CRC) การตรวจสอบข้อผิดพลาดของข้อมูลด้วยวิธี Simple Parity และ Longitudinal Parity เป็นวิธีที่มีอัตราความผิดพลาดสูงจึงมีการคิดวิธี Cyclic Redundancy Checksum (CRC) หรือเรียกสั้นๆ ว่า Cyclic Checksum ขึ้นมา โดยใช้วิธีเพิ่มบิตที่ใช้ตรวจสอบข้อมูลตั้งแต่ 8-32 ลงไปในตอนท้ายของแพ็กเก็ตโดยฝั่งที่รับข้อมูลจะวิเคราะห์ข้อมูลแบบ Polynomial แล้วเปรียบเทียบกับผลลัพธ์ของทั้งฝั่งผู้รับและผู้ส่ง หากข้อมูลมีข้อผิดพลาดเกิดขึ้น ผู้รับจะแจ้งกลับไปยังผู้ส่งเพื่อให้ส่งข้อมูลมาใหม่

วิธีการตรวจสอบข้อผิดพลาดของ CRC นั้นจะกำหนดให้บิตข้อมูลทางด้านขวาสุดมีค่าเป็น X^0 ส่วนข้อมูลในตำแหน่งถัดไปจะมีค่าเป็น X^1 เรียงกันไปตามลำดับ หากต้องการเขียน Polynomial ของข้อมูล 11001001 สามารถทำได้ดังภาพที่ 6.7



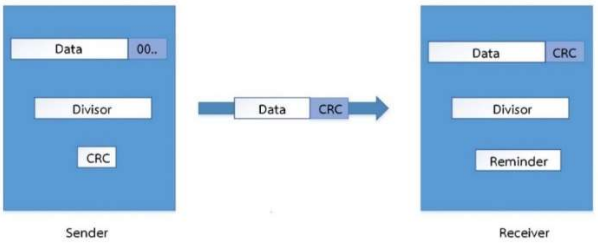
ภาพที่ 6.7 แสดงการเขียน Polynomial ของข้อมูล 11001001

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 131)

จากภาพข้างต้นสามารถแทนข้อมูล 1100101 ด้วย Polynomial ได้เป็น $X^7+X^6+X^3+1$ จะเห็นว่าการแทนค่า Polynomial ของข้อมูลที่มีจำนวน a บิต จะแทนด้วย Polynomial ที่มีความยาว a เทอม ซึ่งมีค่าตั้งแต่ X^{k-1} (ค่าแรก) ถึง X^0 (ค่าสุดท้าย)

การใช้ CRC เพื่อตรวจสอบข้อมูลจะใช้หลักการหารเลขฐาน 2 โดยจะเพิ่มกลุ่มของบิตต่อท้ายข้อมูล เพื่อทำให้สามารถหารด้วยจำนวนที่กำหนดไว้ล่วงหน้าที่เรียกว่า ตัวหาร

(Divisor) หรือกุญแจรหัสได้ เมื่อส่งข้อมูลออกไปและผู้รับได้รับข้อมูลแล้ว จะทำการตรวจสอบโดยการหารข้อมูลที่ได้รับด้วยกุญแจรหัส ถ้าผลการหารลงตัวแสดงว่าข้อมูลถูกต้อง ดังภาพที่ 6.8



ภาพที่ 6.8 แสดงการส่งข้อมูลของ CRC Check

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 131)

เทคนิค CRC จะใช้ Generating Polynomial เพื่อหาค่าของ Divisor โดยทั่วไปสมการของ Polynomial ที่นิยมใช้การมีดังนี้

CRC-12 = $X^{12} + X^{11} + X^3 + X^2 + X^1 + 1$

CRC-16 = $X^{16} + X^{15} + X^2 + 1$

CRC-CCITT = $X^{16} + X^{12} + X^5 + 1$

CRC-32 = $X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^8 + X^7 + X^5 + X^4 + X^2 + X + 1$

Asynchronous Transfer Mode CRC = $X^8 + X^2 + X + 1$

6.4 การควบคุมการไหลของข้อมูล

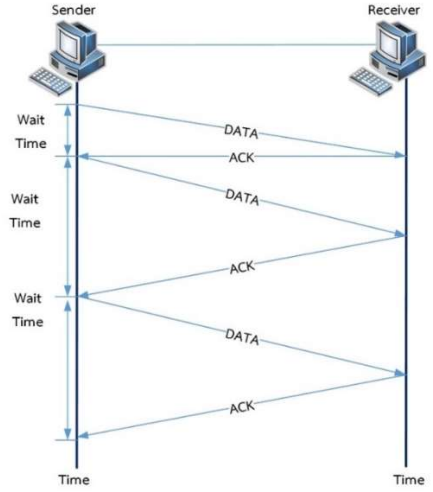
การควบคุมการไหลของข้อมูล (Flow Control) ประกอบด้วย กลุ่มวิธีการที่ทั้งสองฝั่งจะมีการโต้ตอบกันว่า จะให้ส่งข้อมูลจำนวนเท่าใด เพื่อควบคุมมิให้ฝั่งรับรับข้อมูลมากเกินไป เพื่อมิให้เกิดปัญหาด้านการสื่อสารดังกล่าว ระบบเครือข่ายที่ดีจึงต้องมีกระบวนการโต้ตอบซึ่งกันและกัน เพื่อจะได้รับทราบและยืนยันในสิ่งที่ต้องการแล้วนำไปสู่การสื่อสารที่สมบูรณ์ ดังนั้น อุปกรณ์ฝั่งรับจะต้องแจ้งไปยังอุปกรณ์ฝั่งส่งให้รับทราบก่อนที่การรับจะถึงขีดจำกัด ด้วยการร้องขอให้ฝั่งส่งทยอยส่งข้อมูลมาในปริมาณน้อย หรืออาจหยุดส่งเฟรมข้อมูลชั่วคราว นอกจากนี้ข้อมูลที่หลั่งไหลเข้ามาฝั่งรับจะต้องตรวจสอบข้อมูลก่อนนำไปประมวลผลทุกครั้ง ซึ่งปกติจะมีความเร็วช้ากว่าการส่งผ่านข้อมูล ดังนั้น อุปกรณ์ฝั่งรับจึงต้องมีการบล็อกจำนวนความจำที่เรียกว่า **บัฟเฟอร์** (Buffer) เพื่อจับจองไว้สำหรับจัดเก็บข้อมูลที่เข้ามาจนกระทั่งประมวลผลเสร็จ

เมื่อหน่วยความจำบัฟเฟอร์เต็ม ฝั่งรับก็จะแจ้งให้ฝั่งส่งว่าให้หยุดส่ง (Halt) จนกว่าจะประมวลผลเสร็จสิ้นแล้วจึงรับข้อมูลในลำดับถัดไปได้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 301-304)

การควบคุมการไหลของข้อมูล แบ่งออกเป็น 2 วิธี ดังนี้

1. วิธีหยุดและรอ (Stop-and-Wait Flow Control)

วิธีนี้ฝั่งส่งจะส่งเฟรมข้อมูลให้หนึ่งเฟรมและรอการตอบ Acknowledge (ACK) จากฝั่งรับ ครั้นเมื่อฝั่งส่งได้รับสัญญาณ ACK จากฝั่งรับแล้ว จะถือเป็นสัญญาณตอบรับ “OK” ว่าได้รับข้อมูลเป็นที่เรียบร้อยแล้ว ฝั่งส่งก็จะส่งเฟรมในลำดับถัดไป ข้อดีของการควบคุมการไหลของข้อมูลด้วยวิธีนี้ก็คือเป็นวิธีพื้นฐานอย่างง่าย โดยแต่ละเฟรมที่ส่งไปจะต้องขอรับสัญญาณ ACK เสมอเพื่อให้ฝั่งส่งรับทราบและส่งเฟรมในลำดับถัดไป สำหรับในกรณีที่ฝั่งรับต้องหยุดการรับข้อมูลชั่วคราวก็จะใช้วิธีง่ายๆ นั่นคือการไม่ส่งสัญญาณ ACK กลับไปนั่นเอง ข้อเสียของวิธีนี้ก็คือความล่าช้า เนื่องจากทุกๆเฟรมที่ส่งไปจะต้องได้รับการตอบรับก่อนเสมอ



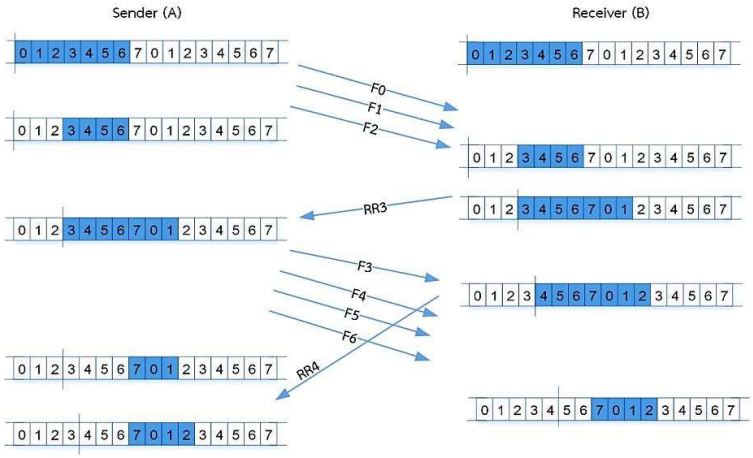
ภาพที่ 6.9 การควบคุมการไหลของข้อมูลด้วยวิธีหยุดและรอ (Stop-and-Wait Flow Control)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 302)

2. วิธีเลื่อนหน้าต่าง (Sliding-Window Flow Control)

วิธีนี้ฝั่งส่งสามารถส่งเฟรมข้อมูลหลายๆ เฟรม ก่อนที่จะได้รับการตอบรับ กล่าวคือฝั่งรับจะมีการตอบรับกลับไปเพียงบางเฟรมเท่านั้น การตอบรับสัญญาณ ACK ในหนึ่งครั้ง จึงหมายถึงการได้รับเฟรมมาแล้วหลายเฟรมนั่นเอง ซึ่งเป็นวิธีที่มีประสิทธิภาพสูงกว่าแบบแรก

พิจารณาจากภาพที่ 6.10 สมมุติว่ากำหนดให้เลขแสดงลำดับมีขนาด 3 บิต จึงทำให้ขนาดของหน้าต่างสามารถบรรจุเฟรมได้สูงสุดถึง 7 เฟรม ในช่วงเริ่มต้นทั้งสถานี A และ B จะ

ถูกกำหนดให้ส่งเฟรมทั้ง 7 โดยเริ่มต้นจาก 0 (F0) ภายหลังจากที่สถานี A ส่งเฟรม F0, F1 และ F2 ไปโดยไม่ได้รับการตอบรับสัญญาณ ACK สถานี A ก็จะหดหน้าต่างลงให้เหลือเพียง 4 เฟรม และคัดลอกเฟรมที่ส่งไปทั้งสามเก็บไว้ในบัฟเฟอร์ ส่วนหน้าต่างที่หดลงเหลือเพียง 4 เฟรมนี้สถานี A สามารถส่งเฟรมทั้งสี่ได้ด้วยการเริ่มต้นจากเฟรม F3 แต่ขณะนั้นสถานี B ได้ตอบรับรหัส RR (Receive Ready) หมายเลข 3 กลับมาซึ่งหมายความว่า “ฉันได้รับเฟรมทั้งหมดที่ส่งมาแล้วถึง F2 และพร้อมที่จะรับตั้งแต่ F3 ถัดไปอีก 7 เฟรม” เมื่อ สถานี A ได้รับการตอบรับดังกล่าวจึงทำการเลื่อนหน้าต่างโดยเริ่มที่เฟรมหมายเลข 3 ถัดไปจนครบ 7 เฟรม (F3, F4, F5, F6, F7, F0, F1) พร้อมกับเคลียร์บัฟเฟอร์ทิ้งไปอย่างรวดเร็ว เนื่องจากไม่มีความจำเป็นต้องเก็บเฟรม F0, F1 และ F2 อีกต่อไปจากนี้สถานี A ก็จะส่งเฟรม F3, F4, F5 และ F6 ไปอย่างรวดเร็วซึ่งในขณะนั้นเป็นช่วงเวลาที่สถานี B ได้รับเฟรม F3 และมีการตอบรับ RR4 กลับมาเพื่อบอกว่า “ฉันพร้อมที่จะรับเฟรมหมายเลข 4 และถัดไปอีก 7 เฟรม (F4, F5, F6, F7, F0, F1, F2)” ซึ่งช่วงเวลาที่มีการตอบรับ RR4 กลับมานั้น สถานี A ได้ส่งเฟรม F4, F5 และ F6 ไปก่อนแล้ว ดังนั้นสถานี A ก็เพียงเปิดหน้าต่างเพื่อส่ง 4 เฟรมถัดไปโดยเริ่มต้นจากเฟรม F7 ดังภาพที่ 6.10



ภาพที่ 6.10 การควบคุมการไหลของข้อมูลด้วยวิธีเลื่อนหน้าต่าง (Sliding-Window Protocol)
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 303)

จากตัวอย่างข้างต้นใช้หมายเลขลำดับขนาดเพียง 3 บิตจึงทำให้สามารถระบุเฟรมสูงสุดได้ 7 เฟรม แต่ในสภาพความเป็นจริงแล้วอาจกำหนดขนาดหน้าต่างที่มีขนาดใหญ่กว่านี้ เช่น ลิงก์ของระบบดาวเทียม หากหน้าต่างบรรจุเฟรมสูงสุดได้กี่เพียง 7 เฟรม การสื่อสารระหว่างฝั่งส่งกับฝั่งรับก็จะเกิดค่าหน่วงเวลาที่สูงมาก ดังนั้น จึงปรับหมายเลขลำดับให้มีขนาด 7 บิต ส่งผลให้ขนาดหน้าต่างหนึ่งๆ สามารถบรรจุข้อมูลได้มากถึง 127 เฟรม

6.5 การควบคุมข้อผิดพลาด

การควบคุมข้อผิดพลาด (Error Control) เมื่อรับข้อมูลจากต้นทางแล้วนำมาตรวจสอบข้อผิดพลาด ผู้รับสามารถดำเนินการด้วยวิธีการต่างๆ เพื่อควบคุมข้อผิดพลาดที่เกิดขึ้นได้ตามความเหมาะสมโดยทั่วไปจะตอบสนองต่อข้อผิดพลาดได้ 3 วิธีคือ ดังนี้ (สุธี พงศาสกุลชัยและณรงค์ ล่ำดี, 2557, หน้า 132-138)

1. วิธีไม่ตอบสนองต่อข้อมูลที่ผิดพลาด การควบคุมข้อผิดพลาดด้วยวิธีนี้ไม่เป็นที่นิยมใช้กันแต่ก็ถูกนำไปใช้ในการส่งข้อมูลของบางระบบ WAN เช่น Frame Relay ซึ่งรองรับวิธีการควบคุมข้อผิดพลาดแบบ Do Nothing เมื่อเฟรมข้อมูลถูกส่งไปถึง Frame Relay Switch ข้อมูลจะตรวจสอบด้วยวิธี CRC Check หากพบข้อผิดพลาด เฟรมข้อมูลจะถูกทิ้งไป เหตุผลที่ต้องใช้การควบคุมข้อผิดพลาดด้วยวิธีการดังกล่าวคือเครือข่ายแบบ Frame Relay จะใช้สายใยแก้วนำแสงที่มีอัตราความผิดพลาดของข้อมูลต่ำมาก ดังนั้น จึงไม่จำเป็นต้องนำเทคนิคการควบคุมข้อผิดพลาดที่ซับซ้อนมาใช้งาน เนื่องจากผู้รับจะมีการเก็บข้อมูลของเฟรมที่ขาดหายไปและจะส่งคำร้องของเฟรมข้อมูลที่เกิดข้อผิดพลาดไปยังผู้ส่งอีกครั้ง

2. วิธีส่งข้อความเตือนกลับไป การควบคุมข้อผิดพลาดด้วยวิธีการนี้จะส่ง Message กลับไปยังผู้ส่งข้อมูลแบบอัตโนมัติเป็นวิธีการที่ได้รับความนิยมเป็นอย่างสูงและใช้เกณฑ์ที่เรียกว่า ARQ ซึ่งย่อมาจาก Automatic Repeat request เป็นเทคนิคที่ใช้ในการควบคุมข้อผิดพลาดแบ่งได้ 3 ชนิด ดังนี้

2.1 Stop-and-Wait ARQ เป็นเทคนิคการควบคุมข้อผิดพลาดที่ใช้กฎเกณฑ์ที่เรียกว่า Stop-and-Wait ARQ มีรูปแบบที่เรียบง่าย จึงเป็นวิธีที่มีข้อจำกัดและขอบเขตในการใช้งานอยู่บ้าง เช่น User1 ซึ่งเป็นผู้ส่งทำการส่งแพ็คเก็ตข้อมูลให้กับเครื่องคอมพิวเตอร์ของ User2 เมื่อ User1 ส่งแพ็คเก็ตข้อมูลออกไปแล้วจะหยุดรอการตอบกลับจาก User2 ซึ่งผลลัพธ์จากส่งข้อมูล สามารถแบ่งได้ 4 รูปแบบ ดังนี้

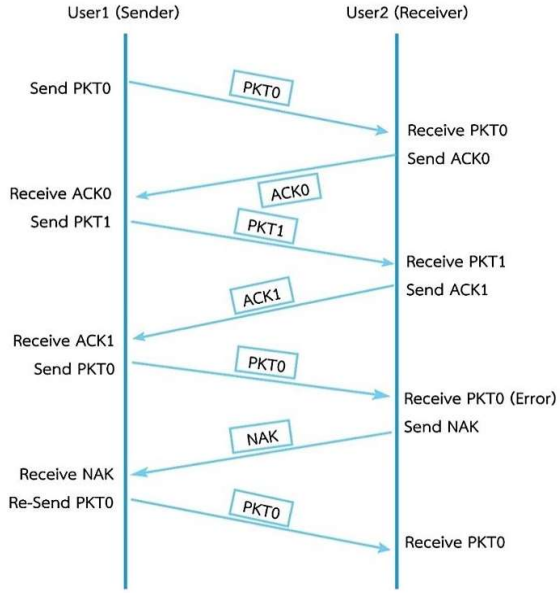
2.1.1 แพ็คเก็ตข้อมูลถูกส่งกลับไปยังปลายทางโดยไม่เกิดข้อผิดพลาดใดๆ User2 จะตอบสนองโดยส่งสัญญาณ Acknowledgment หรือ ACK กลับมา เมื่อ User1 ได้รับสัญญาณ ACK ก็จะแพ็คเก็ตข้อมูลในลำดับถัดไปให้กับ User2

2.1.2 แพ็คเก็ตข้อมูลที่ถูกส่งไปยังปลายทางเกิดข้อผิดพลาดขึ้น User2 จะตอบสนองโดยส่งสัญญาณ Nonacknowledgment หรือ NAK กลับมา เมื่อ User1 ได้รับสัญญาณ NAK ก็จะส่งแพ็คเก็ตข้อมูลเดิมให้กับ User2 อีกครั้ง

2.1.3 แพ็คเก็ตข้อมูลถูกส่งไปถึง User2 โดยไม่เกิดข้อผิดพลาดใดๆ และ User2 ส่งสัญญาณ ACK กลับมา แต่สัญญาณ ACK เกิดสูญหายระหว่างการส่ง กรณีดังกล่าว User1 จะรอสัญญาณตอบกลับโดยไม่ส่งแพ็คเก็ตข้อมูลใหม่ไปให้ เมื่อรอสัญญาณ ACK จนถึงระยะเวลาที่กำหนดไว้ หรือ Timeout จะส่งแพ็คเก็ตข้อมูลเดิมให้กับ User2 อีกครั้ง เมื่อ User2 ได้รับข้อมูลจะไม่ทราบว่าเคยได้รับแพ็คเก็ตดังกล่าวมาแล้ว จนอาจทำให้เกิดความผิดพลาดขึ้นได้ ดังนั้น จึงมีการกำหนดหมายเลขให้กับแพ็คเก็ตข้อมูลโดยมีค่าเป็น 0 และ 1 สลับกันไป หาก User1 ส่งแพ็คเก็ตที่มีหมายเลขเป็น 0 ให้กับ User2 แล้วสัญญาณ ACK สูญหายไป User1 จะทำการส่งแพ็คเก็ตหมายเลข 0 ใหม่อีกครั้ง เมื่อ User2 ได้รับแพ็คเก็ตหมายเลข 0 ติดต่อกัน 2 แพ็คเก็ตก็ทราบว่าสัญญาณ ACK ของแพ็คเก็ตข้อมูลที่ส่งไปได้สูญหายไประหว่างการส่ง

2.1.4 User1 ส่งแพ็คเก็ตข้อมูลให้กับ User2 แต่แพ็คเก็ตสูญหายระหว่างทางทำให้ User2 ไม่ได้ส่งสัญญาณ ACK กลับมา เมื่อถึงเวลาที่กำหนดไว้ User1 จะส่งแพ็คเก็ตข้อมูลเดิมให้กับ User2 อีกครั้ง

เทคนิคการควบคุมข้อผิดพลาด Stop-and-Wait ARQ สามารถแสดงตัวอย่างการส่งข้อมูลตามขั้นตอนดังกล่าว ดังภาพที่ 6.11

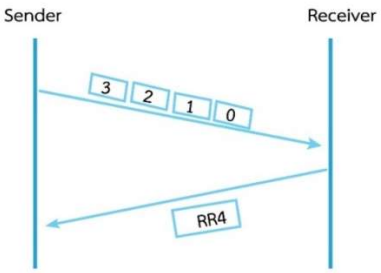


ภาพที่ 6.11 แสดงภาพการรับส่งข้อมูลแบบ Stop-and-Wait ARQ

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 134)

2.2 Sliding Window Protocol เป็นเทคนิคที่ยอมให้มีการส่งหลายแพ็คเก็ตข้อมูลได้ในเวลาเดียวกัน ผู้รับข้อมูลจะส่งสัญญาณตอบรับที่เรียกว่า Receive Ready หรือ RR กลับมา โดยสามารถตอบกลับแพ็คเก็ตข้อมูลได้กว่า 1 แพ็กเก็ต โดย Sliding Window Protocol ถูกสร้างขึ้นเมื่อปี ค.ศ.1970 ซึ่งในขณะนั้นระบบเครือข่ายคอมพิวเตอร์มีข้อจำกัดสำคัญ 2 ประการ คือ ความเร็วในการส่งข้อมูลของสื่อกลาง และการประมวลผลข้อมูลทำได้ช้ากว่าในปัจจุบันค่อนข้างมาก ทำให้ไม่สามารถส่งข้อมูลกลับไปยังปลายทางด้วยความเร็วสูงได้ นอกจากนี้ Buffer ที่ใช้ในอุปกรณ์เครือข่ายยังมีข้อจำกัด เนื่องจากหน่วยความจำมีราคาสูง ทำให้การเก็บแพ็คเก็ตข้อมูลที่เข้าและออกทำได้อย่างจำกัด ดังนั้น การใช้งาน Sliding Window Protocol ในขณะนั้นจึงกำหนดให้ ณ เวลาหนึ่งสามารถส่งแพ็คเก็ตได้เพียงครั้งละ 7 แพ็กเก็ต แล้วหยุดรอสัญญาณ Acknowledgement แต่การส่งข้อมูลได้เพียงครั้งละ 7 แพ็คเก็ต นั้นมีขนาดน้อยไป จึงได้มีการขยายความสามารถให้ Sliding Window Protocol สามารถรองรับแพ็คเก็ตได้ถึง 127 แพ็กเก็ต นอกจากนี้โพรโทคอลใหม่ๆ ยังสามารถปรับขนาดของแพ็คเก็ตให้เหมาะสมกับปริมาณของข้อมูลที่อยู่ในเครือข่ายได้อีกด้วย แต่ในที่นี้จะกล่าวถึง Sliding Window Protocol ที่ส่งข้อมูลได้ครั้งละ 7 แพ็กเก็ต เท่านั้น

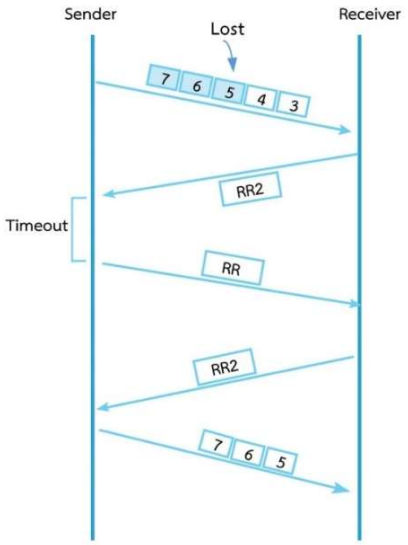
ลำดับของแพ็คเก็ตในข้อมูล Sliding Window Protocol จะถูกจัดเรียงตามหมายเลข 0-7 จะเห็นได้ว่ามีลำดับหมายเลขของแพ็คเก็ตทั้งหมด 8 ลำดับ แต่ Sliding Window Protocol นั้นสามารถส่งข้อมูลได้เพียงครั้งละ 7 แพ็กเก็ต การส่งข้อมูลแต่ละครั้งแพ็คเก็ตข้อมูลจะไม่สามารถมีหมายเลขเดียวกันได้ เมื่อผู้รับได้รับข้อมูลจะส่งสัญญาณ Acknowledgement กลับมายังผู้ส่งซึ่งจะมีหมายเลขระบุจำนวนแพ็คเก็ตที่ได้รับส่งกลับมายังผู้ส่ง เช่น หากต้นทางต้องการส่งข้อมูลครั้งละ 4 แพ็กเก็ต ให้กับผู้รับ เมื่อได้รับแล้วผู้รับจะส่ง Acknowledgement (RR) ที่ระบุจำนวนแพ็คเก็ตที่ได้รับกลับมาให้กับผู้ส่งในที่นี้คือ RR4 นั่นเอง



ภาพที่ 6.12 แสดงภาพการรับส่งข้อมูลแบบ Sliding Window Protocol จำนวน 4 แพ็คเก็ต
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 135)

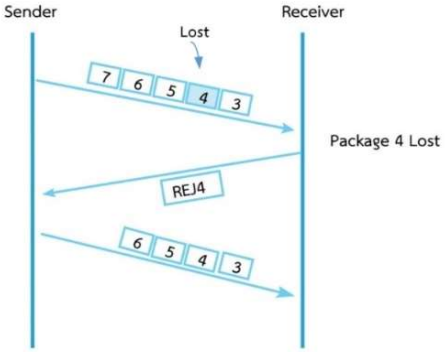
2.3 Go-back-N ARQ เป็นเทคนิคเพิ่มเติมสำหรับควบคุมข้อผิดพลาดของ Sliding Window Protocol โดยใช้วิธีให้ผู้รับแจ้งไปยังโหนดที่ส่งข้อมูลว่าให้ส่งแพ็คเก็ตได้จำนวนเท่าใด โดยผู้ส่งต้องหยุดรอสัญญาณ ACK แต่จำนวนแพ็คเก็ตที่ส่งไปต้องไม่เกินจำนวนสูงสุดที่ผู้รับสามารถรับได้

ในกรณีที่แพ็คเก็ตสูญหายระหว่างการส่ง เช่น เมื่อส่งครั้งละ 5 แพ็กเก็ตให้กับผู้รับคือแพ็คเก็ตลำดับที่ 3 ถึง 7 แล้วสามแพ็คเก็ตสุดท้าย คือ แพ็คเก็ตที่ 5 ถึง 7 เกิดสูญหาย ทำให้ผู้ส่งได้รับเฉพาะสัญญาณ Acknowledge ของ 2 แพ็คเก็ต แรก เมื่อผู้ส่งหยุดรอจนถึงเวลาTimeout แล้ว จะส่งคำสั่ง RR ไปยังผู้รับเพื่อตอบเพื่อสอบถามถึงแพ็คเก็ตที่เหลืออยู่ เมื่อผู้รับได้รับสัญญาณ RR ก็จะตอบสนองโดยส่ง RR2 กลับไปยังผู้ส่ง เพื่อแจ้งให้ทราบว่าได้รับเฉพาะ 2 แพ็คเก็ตแรก ผู้ส่งจึงส่งทั้ง 3 แพ็กเก็ต ที่สูญหายมาใหม่อีกครั้ง ดังภาพที่ 6.13



ภาพที่ 6.13 แสดงภาพการตรวจสอบข้อผิดพลาดด้วย Go-back-N ARQ
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 136)

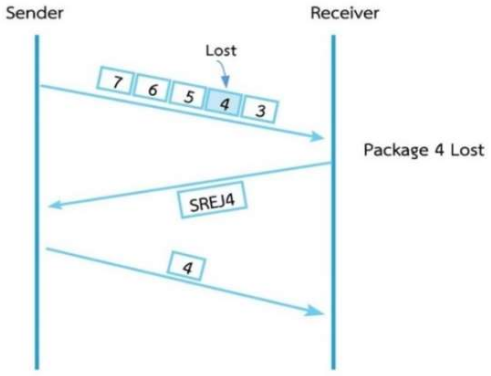
เมื่อแพ็คเก็ตลำดับที่ 4 ซึ่งอยู่ระหว่างแพ็คเก็ตอื่นเกิดข้อผิดพลาดหรือสูญหายระหว่างการส่งผู้รับจะแจ้งกลับโดยส่ง Message ที่เรียกว่า REJ4 (ตัวเลข 4 คือ แจ้งให้ทราบว่าแพ็คเก็ตหมายเลข 4สูญหาย) กลับไปยังต้นทางเพื่อแจ้งให้ทราบว่าแพ็คเก็ตลำดับที่ 4 สูญหายไปต้นทางจะส่ง แพ็คเก็ตข้อมูลตั้งแต่ลำดับที่ 4 ถึง 7 ให้กับผู้รับอีกครั้งหนึ่ง แม้ว่าแพ็คเก็ตลำดับที่ 5 ถึง 7 จะไม่เกิดข้อผิดพลาดก็ตามทำให้ต้องเสียเวลาในการส่งข้อมูลอีกครั้ง ดังภาพที่ 6.14



ภาพที่ 6.14 แสดงภาพการใช้ Go-back-N ARQ เพื่อตรวจสอบข้อมูลที่ผิดพลาด

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 136)

2.4 Selective-Reject ARQ เป็นวิธีที่มีประสิทธิภาพมากกว่า Go-back-N ARQ นำโดย Go-back-N ARQ มาปรับปรุงในเรื่องของการส่งข้อมูลที่ไม่ให้เกิดข้อผิดพลาดให้กับผู้รับใหม่อีกครั้ง ด้วยการส่งเฉพาะแพ็คเก็ตที่สูญหายหรือเกิดข้อผิดพลาดให้กับผู้รับเท่านั้น หากผู้รับได้รับแพ็คเก็ตที่ส่งมาจากต้นทางแล้วตรวจสอบว่าแพ็คเก็ตลำดับที่ n เกิดข้อผิดพลาดหรือสูญหายระหว่างการส่ง ผู้รับจะจัดสรรพื้นที่ว่างในหน่วยความจำไว้สำหรับเก็บแพ็คเก็ตดังกล่าวที่จะถูกส่งมาจากต้นทางอีกครั้ง เช่น เมื่อส่งแพ็คเก็ตครั้งละ 5 แพ็กเก็ต ให้กับผู้รับ คือ แพ็คเก็ตลำดับที่ 3 ถึง 7 หากแพ็คเก็ตลำดับที่ 4 ซึ่งอยู่ระหว่างแพ็คเก็ตอื่นเกิดข้อผิดพลาดหรือสูญหายระหว่างการส่ง ผู้รับจะแจ้งกลับโดยส่ง Message ที่เรียกว่า SREJ4 (ตัวเลข 4 คือ บอกให้ส่งแพ็คเก็ตหมายเลข 4 มาใหม่) กลับไปยังต้นทางเพื่อแจ้งให้ทราบว่าแพ็คเก็ตลำดับที่ 4 สูญหายไป จากนั้นต้นทางจะส่งเฉพาะแพ็คเก็ตลำดับที่ 4 มาใหม่อีกครั้งหนึ่ง ดังภาพที่ 6.15



ภาพที่ 6.15 แสดงภาพการตรวจสอบข้อผิดพลาดด้วย Selective-Reject ARQ

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 137)

3. วิธีแก้ไขข้อผิดพลาดให้ถูกต้อง การควบคุมข้อผิดพลาดด้วยวิธีแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้องแล้วดำเนินการตามขั้นตอนต่อไปถือเป็นวิธีการที่เหมาะสมที่สุด แต่การแก้ไขปัญหาด้วยวิธีการดังกล่าวทำได้ค่อนข้างยาก โดยผู้รับสามารถแก้ไขข้อผิดพลาดได้หลายวิธี เช่น วิธีที่เรียกว่า Forward Error Correction (FEC) ซึ่งเป็นการแก้ไขข้อผิดพลาดในการรับส่งข้อมูล โดยฝั่งผู้ส่งจะเพิ่มข้อมูลซ้ำกัน (Redundant Information) ในระดับบิตเข้าไปในข้อมูลที่ต้องการส่ง เมื่อฝั่งผู้รับได้รับข้อมูลจะทำการตรวจสอบและแก้ไขข้อผิดพลาดของข้อมูลในระดับบิตได้โดยไม่ต้องให้ต้นทางส่งข้อมูลเดิมมาใหม่ เช่น หากต้องการส่งข้อมูลเป็น 1100101 ต้นทางจะทำการส่งข้อมูลที่ซ้ำกันจำนวน 2 ตัวให้กับแต่ละบิต โดยจะได้ข้อมูลเป็น 111 111 000 000 111 000 111 เมื่อส่งข้อมูลดังกล่าวไปยังปลายทางแล้วเกิดข้อผิดพลาดขึ้น เช่น ได้รับข้อมูลเป็น 111 111 **001** 000 111 000 111 จะเห็นได้ว่าข้อมูลชุดที่ 3 มีบิตข้อมูลที่ผิดพลาดเกิดขึ้น ผู้รับจะตรวจสอบและเปรียบเทียบกับบิตข้อมูลที่ซ้ำกันในชุดเดียวกัน ในที่นี้จะกำหนดให้ชุดข้อมูลที่ 3 มีค่าเป็น 0 เนื่องจากมีบิตที่เป็น 0 จำนวน 2 ตัว มากกว่าบิตที่เป็น 1 ซึ่งมีเพียง 1 ตัว นั่นเอง ดังตารางที่ 6.4

ตารางที่ 6.4 แสดงการแก้ไขข้อผิดพลาดด้วยวิธี Forward Error Correction

ข้อมูลต้นฉบับ	1	1	0	0	1	0	1
ข้อมูลที่ผ่าน FEC	111	111	000	000	111	000	111
ข้อมูลที่ผู้รับได้รับ	111	111	**001**	000	111	000	111
แปลงข้อมูลกลับ	1	1	0	0	1	0	1

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 138)

6.6 สรุป

ระหว่างการส่งข้อมูลไปบนสื่อกลางประเภทต่างๆ อาจเกิดข้อผิดพลาดขึ้นได้ อาจมีสาเหตุจากสัญญาณรบกวน (Noise) ซึ่งมีหลายรูปแบบ ดังนั้น การทำความเข้าใจเกี่ยวกับความแตกต่างและสาเหตุของการเกิดสัญญาณรบกวนแต่ละรูปแบบจะช่วยให้การนำเทคนิคและวิธีการวิธีการลดสัญญาณรบกวน (Noise-Reduction) มาใช้เพื่อจำกัดปริมาณของสัญญาณรบกวนที่จะส่งไปยังผู้รับทำได้สะดวกยิ่งขึ้น โดยรูปแบบของสัญญาณรบกวนที่พบได้บ่อยครั้ง ได้แก่ White Noise, Impulse Noise, Crosstalk, Echo, Jitter, Delay Distortion และ Attenuation โดยการป้องกันข้อผิดพลาดที่เกิดจากสัญญาณรบกวนทำได้หลายวิธีเช่นติดตั้งสัญญาณที่มีฉนวนหุ้มใช้

อุปกรณ์ที่มีเทคโนโลยีใหม่ๆ ติดตั้งอุปกรณ์ทวนสัญญาณหรือใช้สายที่มีการกรองสัญญาณรบกวน เป็นต้น

การตรวจสอบข้อผิดพลาดที่เกิดขึ้นกับข้อมูลที่ราบเป็นสิ่งสำคัญเนื่องจากทำให้มั่นใจว่าข้อมูลดังกล่าวมีความถูกต้องและไม่มีข้อผิดพลาดใดๆ เกิดขึ้นเพื่อไม่ให้ผู้รับนำข้อผิดพลาดไปใช้งานจนอาจเกิดความเสียหายแก่ระบบหรือธุรกิจได้โดยมีวิธีการตรวจสอบข้อผิดพลาดดังนี้ หลายวิธี เช่น Parity Check (Simple Parity และ Longitudinal Parity) และ Cyclic Redundancy Checksum (CRC) เป็นต้น

ผู้รับดำเนินการด้วยวิธีต่างๆ เพื่อควบคุมข้อผิดพลาดที่เกิดขึ้นกับข้อมูลที่รับสัญญาณได้ตามความเหมาะสมโดยทั่วไปจะตอบสนองต่อข้อผิดพลาดได้ 3 วิธี คือ ไม่ตอบสนองหรือกระทำการใดๆ ต่อข้อมูลที่ผิดพลาด (Do nothing) ส่งข้อความเตือนกับปลายแบบอัตโนมัติ (Return Message) และแก้ไขข้อผิดพลาดให้ถูกต้อง (Correct Error) โดยวิธีการส่งข้อความแบบอัตโนมัติเป็นวิธีที่ได้รับความนิยมเป็นอย่างสูง สามารถแบ่งรูปแบบการส่งข้อความได้ 3 ชนิด คือ Stop-and-Wait ARQ, Go-back-N ARQ และ Selective-Reject ARQ

บทที่ 7
ความรู้พื้นฐานเกี่ยวกับระบบเครือข่ายแบบใช้สาย

ระบบเครือข่ายใช้สายเป็นระบบเครือข่ายที่เชื่อมต่ออุปกรณ์สื่อสารด้วยสายนำสัญญาณประเภทสายทองแดงและสายใยแก้วนำแสง การเชื่อมต่อในระบบเครือข่ายต้องการให้มีอัตราความเร็วของการรับส่งข้อมูลที่สูง ระบบเครือข่ายที่เชื่อมต่อด้วยสายใยแก้วจะมีอัตราความเร็วข้อมูลที่สูงและค่าใช้จ่ายในการติดตั้งระบบที่สูงกว่าระบบเครือข่ายที่เชื่อมต่อด้วยสายทองแดง ระบบเครือข่ายที่ใช้สายทองแดงเชื่อมต่อเป็นระบบที่มีการใช้งานอย่างกว้างขวาง ทำให้ได้รับการพัฒนาด้านความเร็วเพื่อให้การรับส่งข้อมูลสูงขึ้นอย่างต่อเนื่อง

การพัฒนาการเชื่อมต่อคอมพิวเตอร์เข้ากับระบบเครือข่ายแบบใช้สายได้มีการพัฒนาเป็นเครือข่ายอินเทอร์เน็ตในยุคปัจจุบัน มีวัตถุประสงค์เพื่อสร้างเครือข่ายการสื่อสารที่มีความพร้อมในการใช้งาน มีความยืดหยุ่น สามารถใช้งานได้ด้วยความเร็วสูง เนื่องจากระบบเครือข่ายคอมพิวเตอร์ช่วยทำให้ผู้ใช้งานสามารถแลกเปลี่ยนข้อมูลข่าวสารและความรู้ได้อย่างไร้พรหมแดน เทคโนโลยีที่เกี่ยวข้องกับระบบเครือข่ายแบบใช้สาย ได้แก่ อีเทอร์เน็ต โคเทนริง โคเทนบัส เอฟดีดีไอ ไอเอสดีเอ็น เฟรมรีเลย์ และเอทีเอม

7.1 ประเภทของระบบเครือข่ายแบบใช้สาย

การเชื่อมต่ออินเทอร์เน็ตแบบใช้สาย (Wire Internet) คือ การเชื่อมต่อโดยที่มีตัวกลาง ได้แก่ สายแลน เข้ามาเป็นเสมือนเส้นทางที่ทำให้อินเทอร์เน็ตและคอมพิวเตอร์สามารถเชื่อมต่อเข้าหากันได้เป็นอย่างดี การเชื่อมต่อแบ่งออกเป็น 2 ประเภท ดังนี้

7.1.1 การเชื่อมต่ออินเทอร์เน็ตรายบุคคล (Individual Connection) เป็นลักษณะของการเชื่อมต่ออินเทอร์เน็ตของประชาชนทั่วไป เนื่องจากในอดีตยังจำเป็นต้องใช้ระบบสายโทรศัพท์เพื่อทำการเข้าสู่อินเทอร์เน็ต ผู้ใช้งานจะต้องสมัครเป็นสมาชิกกับผู้ที่ให้บริการทางอินเทอร์เน็ต เมื่อสมัครแล้วจะได้เบอร์โทรศัพท์ รหัสผู้ใช้งานและรหัสผ่าน วิธีการใช้งาน คือ การนำโมเด็มมาเชื่อมต่อกับระบบคอมพิวเตอร์เพื่อให้เกิดการหมุนไปยังเบอร์โทรศัพท์ที่ได้มาแล้วก็จะสามารถใช้บริการอินเทอร์เน็ตได้ ในปัจจุบันวิธีการอีกแบบสำหรับการเชื่อมต่ออินเทอร์เน็ตรายบุคคล คือ การใช้เครือข่ายใยแก้วนำแสง (Fiber Optic) ซึ่งก็จะใกล้เคียงกันกับระบบที่กล่าว

มาแต่คุณภาพจะดีกว่า องค์ประกอบโดยรวมของการเชื่อมต่ออินเทอร์เน็ตรายบุคคลก็จะประกอบไปด้วย โทรศัพท์บ้าน คอมพิวเตอร์ และผู้ให้บริการอินเทอร์เน็ต

7.1.2 การเชื่อมต่ออินเทอร์เน็ตแบบองค์กร (Corporate Connection) เป็นการเชื่อมต่ออินเทอร์เน็ตแบบใช้สายสำหรับองค์กรต่างๆ บริษัทเอกชน โรงเรียน โรงพยาบาล หน่วยงานราชการ ซึ่งหน่วยงานเหล่านี้จะมีเครือข่ายในระบบท้องถิ่นที่เรียกว่าเครือข่ายแลนเป็นของตัวเอง โดยจะทำการเชื่อมต่อกับอินเทอร์เน็ตไว้อยู่ตลอดเวลาผ่านสายเช่า (Leased Line) สามารถใช้งานอินเทอร์เน็ตได้ตลอดเวลา ซึ่งการใช้อินเทอร์เน็ตผ่านระบบแลนจะไม่มีการเชื่อมต่อเหมือนกับผู้ใช้แบบรายบุคคลที่จำเป็นต้องใช้คู่สายโทรศัพท์เพื่อที่จะเข้าสู่ระบบอินเทอร์เน็ตได้

7.2 อีเทอร์เน็ต

อีเทอร์เน็ต (Ethernet) เป็นระบบการขนส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ของเครือข่ายแลนในยุคแรกๆ ถูกคิดค้นขึ้นในปี ค.ศ.1973 โดยมีวัตถุประสงค์เพื่อใช้ในการแลกเปลี่ยนข้อมูลและแบ่งปันข้อมูลกันภายในเครือข่ายเท่านั้น ต่อมาได้มีการพัฒนาอีเทอร์เน็ตให้มีประสิทธิภาพมากขึ้นเนื่องจากมีการนำไปใช้อย่างแพร่หลาย (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 158)

7.2.1 การทำงานของอีเทอร์เน็ต

การ์ดเครือข่าย (Network Card) แต่ละแผ่นนั้นมี Physical Address ของตัวเอง เมื่อสถานีส่งเฟรมไปยังบัสทุกสถานีที่เชื่อมต่อกัน เครือข่ายจะคัดเฟรม ซึ่งสถานีแต่ละแห่งจะตรวจสอบ Address ของเฟรม และถ้าตรงกับ NIC Address ของสถานีนั้นๆ จะรับเฟรมนั้นไว้ ถ้าไม่ตรงก็จะละทิ้งเฟรมนั้นไป (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 73)

เครือข่ายอีเทอร์เน็ต สถานีแต่ละแห่งจะใช้โพรโทคอล CSMA/CD ในการเข้าถึงเครือข่ายเพื่อทำการส่งข้อมูล โดย CSMA/CD มีกระบวนการทำงาน ดังนี้

1. ในกรณีที่สถานีต้องการจะส่งข้อมูล สถานีนั้นจะรับรู้ถึงช่องสัญญาณ ถ้าไม่มีการส่งข้อมูลสถานีนั้นก็จะส่งข้อมูลและตรวจสอบข้อผิดพลาด แต่ถ้าช่องสัญญาณนั้นมีการใช้งานอยู่ สถานีนั้นจะรอจนกว่าจะว่าง เมื่อว่างแล้วจะส่งข้อมูลอีกครั้ง

2. ในกรณีที่สถานี 2 แห่ง ส่งข้อมูลในเวลาเดียวกันบนบัส จะทำให้เฟรมนั้นเกิดการชนกัน สถานีที่ตรวจสอบความผิดพลาดก่อนจะส่ง Jamming Code ไปยังบัส โดยจะแจ้ง

สถานีอื่นๆ ว่ามีการชนกันของข้อมูลเกิดขึ้น

3. สถานีที่เกิดการชนกันของข้อมูลจะรอ Back-Off Algorithm จากนั้นจะส่งข้อมูลใหม่

7.2.2 อีเทอร์เน็ต หรือ IEEE 802.3

เพื่อให้การพัฒนาระบบเครือข่ายอีเทอร์เน็ต (Ethernet network) มีมาตรฐานในทิศทางเดียวกัน สถาบันวิชาชีพวิศวกรไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers : IEEE) หรือ IEEE ได้กำหนดตั้งชื่อโครงการพัฒนาคือ IEEE Project 802 โดยมองถึงการพัฒนาในระดับชั้นกายภาพ (physical layer) และระดับชั้นเชื่อมโยงข้อมูล (data link layer) ของแบบจำลองโอเอสไอหรือของแบบจำลองทีซีพี/ไอพี ดังภาพที่ 7.1 (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-8)

ภาพที่ 7.1 มาตรฐาน IEEE สำหรับระบบเครือข่ายอีเทอร์เน็ต

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-9)

จากภาพที่ 7.1 แสดงการเปรียบเทียบระดับชั้นการทำงานในแบบจำลองมาตรฐาน IEEE กับมาตรฐานแบบจำลองโอเอสไอ โดยแบบจำลองมาตรฐาน IEEE ได้แบ่งย่อยระดับชั้นการทำงานของ Data Link Layer ในแบบจำลองโอเอสไอออกเป็น 2 ระดับชั้นย่อย ได้แก่ ระดับชั้นย่อยแอลแอลซี (Logical Link Control : LLC) ทำหน้าที่ควบคุมการไหลของข้อมูล (Flow Control) ความผิดพลาดของข้อมูล (Error Control) และการจัดเก็บเฟรมข้อมูล (Framing) และระดับชั้นย่อยแมค (Media Access Control : MAC) ที่ทำหน้าที่บริหารจัดการเฟรมข้อมูล ระดับชั้นย่อย LLC ของแบบจำลองมาตรฐาน IEEE สามารถใช้โพรโทคอลชนิดเดียวกันรายการทำงานกับเครือข่ายแบบที่แตกต่างกันได้ โดยโพรโทคอลในระดับชั้นย่อย LLC จะติดต่อสื่อสารกับแต่ละชนิดโพรโทคอลระดับชั้นย่อยแมคของแต่ละชนิดเครือข่ายแลน เช่น โพรโทคอล CSMA/CD สำหรับเครือข่ายอินเทอร์เน็ต และโพรโทคอล Token-Passing สำหรับ

เครือข่ายแลนแบบวงแหวนและแบบบัส และสำหรับระดับชั้นกายภาพในแบบจำลองมาตรฐาน IEEE ได้ทำการแบ่งส่วนการพัฒนาในระดับชั้นกายภาพของแบบจำลองโอเอสไอให้ชัดเจนและสอดคล้องกับระดับชั้นย่อยแมค ได้แก่ ระดับชั้นกายภาพอีเทอร์เน็ต ระดับกายภาพโทเค็นริง และระดับชั้นกายภาพโทเค็นบัส

7.2.3 การเชื่อมต่อใช้งานอีเทอร์เน็ต

เครือข่ายอีเทอร์เน็ตนั้นใช้สื่อกลางในการเชื่อมต่อได้ 4 ชนิด คือ 10BaseT 10Base2 และ 10Base5 และ 10Base-F ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 336-345)

1. 10Base5

รูปแบบการเชื่อมต่อเครือข่ายแบบ 10Base5 จัดเป็นต้นแบบของเครือข่ายอีเทอร์เน็ตในช่วงเริ่มต้น ใช้การเข้าถึงแบบ CSMA/CD ที่ทำงานอยู่บนสายโคแอ๊กเชียล RG-8 แบบหนา หรือ Thicknet เพราะเป็นสายที่มีซีลด์ที่หนามากป้องกันสัญญาณรบกวนได้ดี คุณสมบัติและการใช้งานของ 10Base5 สรุปได้ดังนี้

1.1 ระยะสูงสุดในแต่ละส่วนคือ 500 เมตร (ไม่ต้องใช้ Repeater)

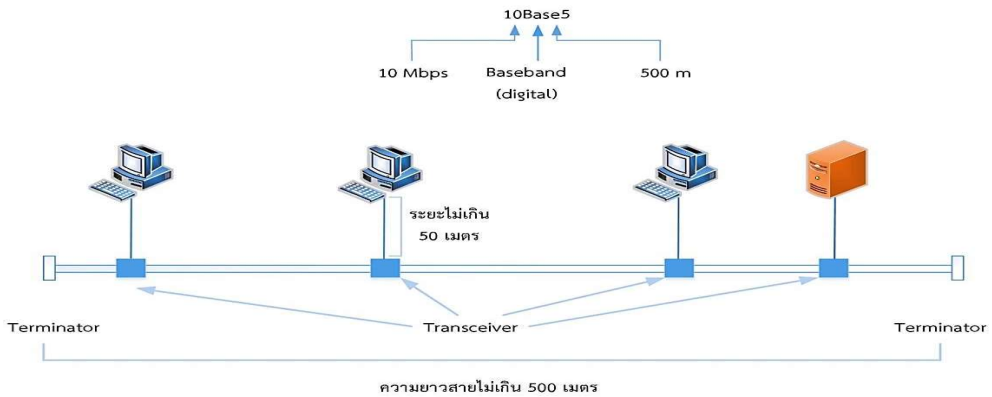
1.2 อุปกรณ์จะเชื่อมต่อกับ Backbone ผ่าน Transceiver

1.3 ระยะสูงสุดของสาย Attachment Unit Interface (AUI) คือ 50 เมตร

1.4 ระยะที่ใกล้ที่สุดระหว่าง Transceiver คือ 2.5 เมตร

1.5 ในแต่ละส่วนของเครือข่ายมี Transceiver ได้สูงสุด 100 ตัว

1.6 จุดปลายของเครือข่ายเชื่อมต่อกับตัวต้านทานขนาด 50 โอห์ม



ภาพที่ 7.2 โทโพโลยีของ 10Base5

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-13)

2. 10Base2

การเชื่อมต่อเครือข่ายแบบ 10Base2 ได้รับการพัฒนามาจาก 10Base5 หรือ Thinnet โดยใช้สายเคเบิลแบบบางคือ RG-58 ที่สำคัญคือ 10Base2 มีต้นทุนการติดตั้งถูกกว่าแบบ 10Base5 และยังติดตั้งได้ง่ายกว่า คุณสมบัติและการใช้งานของ 10Base2 สรุปได้ดังนี้

2.1 10 Base2 จะใช้ Thin Coaxial ด้วยหัวต่อ BNC

2.2 ระยะทางสูงสุดของแต่ละส่วนคือ 185 เมตร

2.3 ระยะทางสูงสุดของเครือข่ายคือ 925 เมตร ซึ่งจะต้องใช้ Repeater 4 ตัว

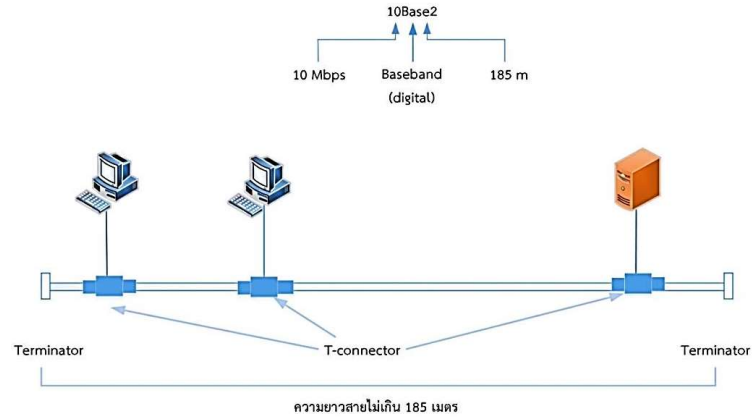
2.4 Transceiver จะอยู่ใน NIC เลย

2.5 ระยะทางที่ใกล้ที่สุดระหว่างหัวต่อแบบ T คือ 0.5 เมตร

2.6 แต่ละส่วนจะสามารถมีหัวต่อได้สูงสุด 30 หัวต่อ

2.7 อุปกรณ์แรกและอุปกรณ์สุดท้ายในแต่ละส่วนจะต้องต่อด้วยตัวต้านทาน 50 โอห์ม เรียกว่า BNC Terminator ซึ่งจะช่วยป้องกันการสะท้อนของสัญญาณ

2.8 หัวต่อแบบ T จะต่อเข้ากับอุปกรณ์อีเทอร์เน็ตโดยตรง



ภาพที่ 7.3 โทโพโลยีของ 10Base2

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-14)

3. 10BaseT

การเชื่อมต่อเครือข่ายแบบ 10BaseT จะใช้การเชื่อมต่อแบบบัส ด้วยการนำสายสัญญาณมาเชื่อมต่อกับอุปกรณ์ฮับ จะช่วยให้ระบบมีความคงทนมากยิ่งขึ้น โดยเฉพาะหากสายเคเบิลบนโหนดใดเกิดขาดหรือเสียหาย โหนดอื่นๆ ก็ยังคงใช้งานได้ตามปกติ ซึ่งแตกต่างจากการเชื่อมต่อแบบ 10Base5 และ 10Base2 เมื่อสายเคเบิลเกิดความเสียหายจะทำให้เครือข่าย

หยุดการทำงานทันที เนื่องจากจุดที่เสียหายถือเป็นส่วนหนึ่งของสายแกนหลักนั่นเอง ข้อจำกัดของ 10BaseT มีดังนี้

3.1 ระยะทางสูงสุดของแต่ละส่วนคือ 100 เมตร

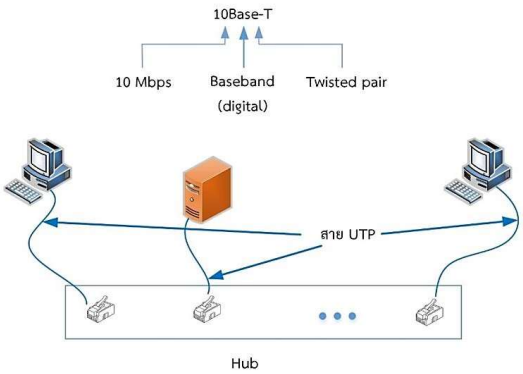
3.2 Transceiver จะอยู่ใน NIC

3.3 สายที่จะใช้สายคือ 22-266 AWG UTP Cat-4 หรือ Cat-5

3.4 อุปกรณ์ที่เชื่อมต่อ เป็นโครงสร้างรูปดาว (Star Topology)

3.5 อุปกรณ์ที่ใช้หัวต่อมาตรฐาน AUI สามารถเชื่อมต่อกับ Hub โดยใช้ 10BaseT Transceiver

3.6 10BaseT Topology อนุญาตให้มีตัวทวน (Repeater) ที่เชื่อมต่อเข้าด้วยกันมากที่สุด 4 ตัว และมีขนาดสูงสุด 500 เมตร



ภาพที่ 7.4 โทโพโลยีของ 10Base-T

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-14)

4. 10Base-F

การเชื่อมต่อเครือข่ายแบบ 10Base-F ถูกพัฒนาขึ้นโดยนำสายไฟเบอร์ออฟติกหรือสายใยแก้วนำแสงมาใช้แทนสายโคแอ็กเชียล คุณสมบัติของ 10Base-F สรุปได้ดังนี้

4.1 อัตราความเร็วในการส่งข้อมูลที่ 10 Mbps

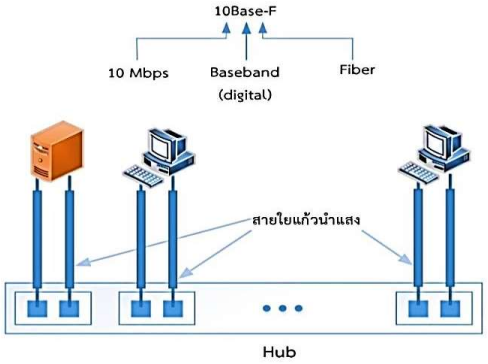
4.2 ใช้วิธีส่งสัญญาณแบบเบสแบนด์

4.3 ระยะทางระหว่างโหนดกับฮับ เชื่อมโยงได้ไกลสูงสุด 2 กิโลเมตร

4.4 เป็นเครือข่ายรูปแบบ Star Bus

4.5 ภายในหนึ่งเซกเมนต์ สามารถเชื่อมต่อโหนดได้ไม่เกิน 1024 เครื่อง

4.6 ใช้สายไฟเบอร์ออฟติกแบบมัลติโหมด คอนเน็กเตอร์แบบ ST หรือ SC และใช้การ์ดเครือข่ายแบบไฟเบอร์ออปติกแบบคอนเน็กเตอร์คู่



ภาพที่ 7.5 โทโพโลยีของ 10Base-F

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-15)

7.3 อีเทอร์เน็ตยุคใหม่ (Modern Ethernet)

มาตรฐานเครือข่ายอีเทอร์เน็ต 10BaseT 10Base2 10Base5 และ 10Base-F ล้วนเป็นอีเทอร์เน็ตแบบดั้งเดิมที่รองรับความเร็วเพียง 10 Mbps ต่อมาอีเทอร์เน็ตได้มีการพัฒนาอย่างต่อเนื่อง เพื่อปรับปรุงด้านประสิทธิภาพและความเร็ว จึงเกิดอีเทอร์เน็ตยุคใหม่ขึ้นมา ดังนี้ (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 355-358)

7.3.1 ฟาสต์อีเทอร์เน็ต (Fast Ethernet)

ฟาสต์อีเทอร์เน็ต หรืออีเทอร์เน็ตความเร็วสูงมีอัตราความเร็วการรับส่งข้อมูล 100 Mbps โดยได้ทำการพัฒนาต่อจากเครือข่าย Standard Ethernet ที่มีอัตราความเร็วการรับส่งข้อมูล 10 Mbps และเครือข่ายฟาสต์อีเทอร์เน็ตยังได้เพิ่มลักษณะการทำงานที่ให้อุปกรณ์สื่อสารที่มีอัตราความเร็วการรับส่งข้อมูล 10 Mbps สามารถทำการสื่อสารกับอุปกรณ์สื่อสารภายในเครือข่ายฟาสต์อีเทอร์เน็ตได้โดยอัตโนมัติ เรียกลักษณะการทำงานนี้ว่า Auto Negotiation อย่างไรก็ตามตัวอุปกรณ์สื่อสารที่สามารถทำงานได้ในลักษณะดังกล่าวต้องมีการระบุโหมดการทำงานไว้ เช่น 10/100 Mbps เป็นต้น

รูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต

รูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต ได้ทำการจัดการพัฒนาด้านโทโพโลยีของเครือข่ายเป็นแบบดาว โดยมีอุปกรณ์ฮับหรือสวิตซ์ทำหน้าที่เชื่อมต่ออุปกรณ์สื่อสารต่างๆ ให้ติดต่อสื่อสารกันได้ในเครือข่ายและด้านการเข้ารหัสสัญญาณของข้อมูลบนสายนำสัญญาณที่เหมาะสมและรองรับได้ เพื่อให้มีอัตราความเร็วการรับส่งข้อมูลที่สูงขึ้น มาตรฐานเครือข่ายฟาสต์อีเทอร์เน็ตที่ได้ทำการพัฒนาแสดงได้ดังตารางที่ 7.1

ตารางที่ 7.1 แสดงรูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต

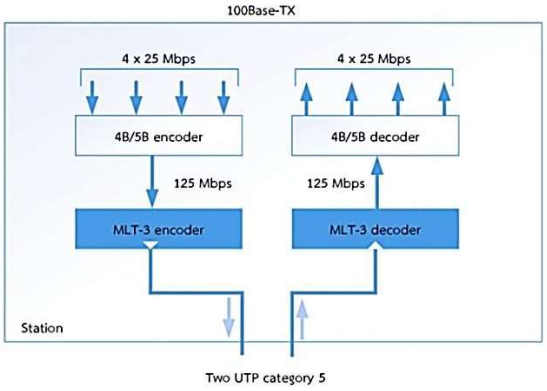
รูปแบบฟาสต์อีเทอร์เน็ต	ชนิดสายนำสัญญาณ	ความยาวสาย	การเข้ารหัสข้อมูล
100Base-TX	UTP หรือ STP	100 เมตร	4B5B + MLT-3
100Base-FX	Fiber	185 เมตร	4B5B + NRZ-I
100Base-T4	UTP	100 เมตร	Two 8B/6T

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 355)

ในตารางที่ 7.1 แต่ละรูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต จะขึ้นอยู่กับชนิดและความยาวของสายนำสัญญาณที่ใช้และรูปแบบวิธีการของการเข้ารหัสสัญญาณเพื่อทำให้ระบบเครือข่ายมีอัตราความเร็วการรับส่งข้อมูล 100 Mbps รูปแบบฟาสต์อีเทอร์เน็ตมีรายละเอียดดังนี้

1. 100Base-TX

รูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต แบบ 100Base-TX เป็นเครือข่ายแลนที่ใช้สายสัญญาณแบบสายคู่บิดเกลียวรับส่งข้อมูล จำนวน 2 คู่แบบ CAT5-UTP หรือ STP โดยกระบวนการจัดการรับส่งข้อมูลที่สถานี (station) จะทำการนำสัญญาณข้อมูลจำนวน 4 ช่องสัญญาณที่มีอัตราความเร็ว 25 Mbps มาเข้ารหัสข้อมูลแบบบล็อก (Block) แบบ 4B/5B ผลจากการเข้ารหัสได้อัตราบิตข้อมูลรวมใหม่เท่ากับ 125 Mbps ก่อนนำไปเข้ารหัสข้อมูลอีกครั้งด้วยวิธีการเข้ารหัส Line Encoder แบบ MLT-3 เพื่อให้การรับส่งมีการตอบสนองในด้านแบนด์วิดท์ที่ดี ดังภาพที่ 7.6

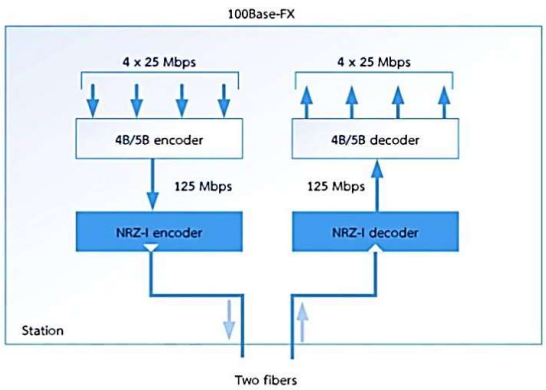


ภาพที่ 7.6 วิธีรับส่งข้อมูลแบบ 100Base-TX

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-18)

2. 100Base-FX

รูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต แบบ 100Base-FX เป็นเครือข่ายแลนที่ใช้สายสัญญาณรับส่งข้อมูล จำนวน 2 คู่ แบบสายใยแก้วนำแสง กระบวนการจัดการรับส่งข้อมูลที่สถานีใช้สัญญาณข้อมูลจำนวน 4 ช่องสัญญาณที่มีอัตราความเร็ว 25 Mbps นำมาเข้ารหัสแบบบล็อกแบบ 4B/5B ทำให้มีอัตราบิตข้อมูลรวมเท่ากับ 125 Mbps และถูกเข้ารหัสอีกครั้งด้วยวิธีการเข้ารหัสแบบ NRZ-I ซึ่งเป็นวิธีการเข้ารหัสที่ไม่ซับซ้อน เนื่องจากสายใยแก้วนำแสงตอบสนองด้านแบนด์วิดท์ได้ดีอยู่แล้ว ลักษณะการเข้ารหัสของเครือข่ายแสดงได้ดังภาพที่ 7.7

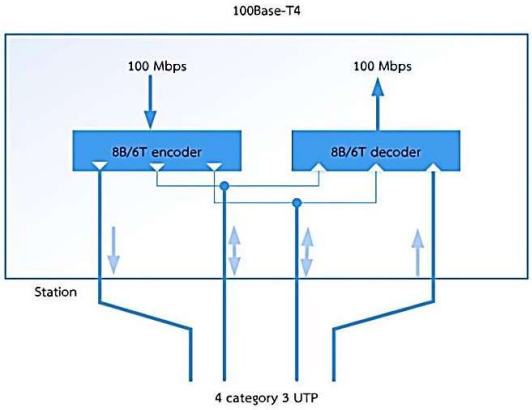


ภาพที่ 7.7 วิธีรับส่งข้อมูลแบบ 100Base-FX

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-18)

3. 100Base-T4

รูปแบบเครือข่ายฟาสต์อีเทอร์เน็ต แบบ 100Base-T4 เป็นเครือข่ายแลนที่ใช้สายนำสัญญาณรับส่งข้อมูลจำนวน 4 คู่ สำหรับสายทองแดงชนิด CAT3-UTP หรือสูงกว่า เพื่อทำการส่งสัญญาณข้อมูล 1 ช่องสัญญาณรวมกันด้วยอัตราบิต 100 Mbps แล้วทำการเข้ารหัสเป็น Block อีกครั้งแบบ 8B/6T โดยในขณะเดียวกันอินพุตและเอาท์พุตบางส่วนของการเข้ารหัส 8B/6T จะทำการจับคู่เชื่อมโยงเพื่อทำการรับและส่งข้อมูลร่วมกัน ดังแสดงในภาพที่ 7.8



ภาพที่ 7.8 วิธีรับส่งข้อมูลแบบ 100Base-T4

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-19)

7.3.2 กิกะบิตอีเทอร์เน็ต

เป็นเครือข่ายอีเทอร์เน็ตที่มีอัตราความเร็วในการรับส่งข้อมูลขนาด 1000 Mbps หรือ 1 Gbps และทาง IEEE ได้กำหนดมาตรฐานการเรียกชื่อเป็น IEEE 802.3z ระบบเครือข่ายกิกะบิตอีเทอร์เน็ตได้ถูกออกแบบให้ทำงานร่วมกับเครือข่าย Standard Ethernet และฟาสต์อีเทอร์เน็ต โดยสนับสนุนการทำงานของอุปกรณ์บนเครือข่ายในโหมด Auto Negotiation เนื่องจากระบบเครือข่าย กิกะบิตอีเทอร์เน็ตต้องการอัตราความเร็วการรับส่งข้อมูลที่สูงถึง 1 Gbps ทำให้การเข้าถึงสื่อกลางผ่านสายนำสัญญาณจะเป็นแบบฟูลดูเพล็กซ์ (Full-Duplex) ทำให้การรับส่งข้อมูลผ่านสายนำสัญญาณเป็นแบบสองทางในเวลาพร้อมกันได้โดยไม่มีปัญหาเรื่องของการชนกันของข้อมูลที่รับส่งทำให้เครือข่ายแบบนี้ไม่ต้องจำเป็นใช้โพรโทคอลแบบ CSMA/CD สำหรับการควบคุมการเข้าถึงสื่อกลางแบบฮาฟดูเพล็กซ์ (Half-Duplex) อย่างไรก็ตามแม้วิธีการรับข้อมูลแบบ Full-Duplex จะไม่เกิดปัญหาของการชนกันของสัญญาณข้อมูล แต่สัญญาณข้อมูลจะถูกลดทอนกำลังลงตามความยาวของสายนำสัญญาณที่ใช้เชื่อมต่อสื่อสาร ทำให้

สัญญาณข้อมูลมีความผิดพลาดในการรับส่งและมีอัตราความเร็วการรับส่งข้อมูลต่ำลง และสำหรับการเชื่อมต่อกับอุปกรณ์เครือข่ายที่มีวิธีการรับส่งข้อมูลแบบ Half-Duplex การจัดการติดต่อสื่อสารสามารถทำได้โดยผ่านอุปกรณ์ฮับ

รูปแบบเครือข่ายกิกะบิตอีเทอร์เน็ต

การพัฒนาของระบบเครือข่ายกิกะบิตอีเทอร์เน็ตจะมีการปรับเปลี่ยนข้อมูลในชั้นกายภาพที่มีความซับซ้อนกว่าเครือข่าย Standard Ethernet และ Fast Ethernet ได้แก่ 1) ลักษณะของโทโพโลยีที่เป็นแบบดาว 2) การใช้จำนวนสายนำสัญญาณแบบ 2 คู่สายหรือ 4 เส้น และแบบ 4 คู่สายหรือ 8 เส้น 3) รูปแบบวิธีการเข้ารหัสสัญญาณข้อมูลบนแต่ละสายนำสัญญาณที่ใช้ มาตรฐานเครือข่ายกิกะบิตอีเทอร์เน็ตที่ได้รับการพัฒนาจากการปรับเปลี่ยนดังกล่าวแสดงได้ดังตารางที่ 7.2

ตารางที่ 7.2 แสดงรูปแบบเครือข่ายกิกะบิตอีเทอร์เน็ต

รูปแบบกิกะบิตอีเทอร์เน็ต	ชนิดสายนำสัญญาณ	ความยาวสาย	การเข้ารหัสข้อมูล
100Base-SX	Fiber S-W	550 เมตร	8B/10B + NRZ
100Base-LX	Fiber L-W	5000 เมตร	8B/10B + NRZ
100Base-CX	STP	25 เมตร	8B/10B + NRZ
100Base-T4	UTP	100 เมตร	4D-PAM5

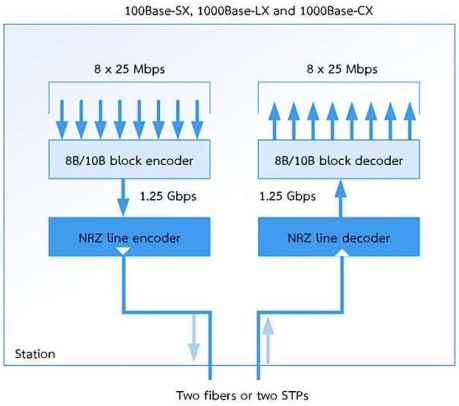
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 357)

จากตารางที่ 7.2 แต่ละรูปแบบกิกะบิตอีเทอร์เน็ตขึ้นอยู่กับชนิดและความยาวของสายนำสัญญาณที่ใช้และรูปแบบวิธีการเข้ารหัสสัญญาณ จากตารางชนิดสายนำสัญญาณแบบสายใยแก้วจะมีความยาวสำหรับการเชื่อมต่อในเครือข่ายมากกว่าความยาวของสายนำสัญญาณแบบสายทองแดง

1. 1000Base-SX และ 1000Base-LX

รูปแบบเครือข่ายกิกะบิตอีเทอร์เน็ตแบบ 1000Base-SX และแบบ 1000Base-LX เป็นเครือข่ายแลนที่ใช้สายนำสัญญาณ 2 คู่แบบสายใยแก้วนำแสง โดยเครือข่าย 1000Base-SX ใช้สายใยแก้วนำแสงชนิดความยาวคลื่นสั้น และเครือข่าย 1000Base-LX ใช้สายใยแก้วนำแสงชนิดความยาวคลื่นยาว และเครือข่ายกิกะบิตอีเทอร์เน็ตแบบ 1000Base-CX จะใช้สายนำสัญญาณ 2 คู่ แบบสายคู่บิดเกลียว STP โดยเครือข่ายเหล่านี้ใช้เทคนิคการเข้ารหัสสัญญาณข้อมูลที่อัตราความเร็วรับส่งข้อมูล 125 Mbps จำนวน 8 ช่องสัญญาณ เข้ารหัสแบบ

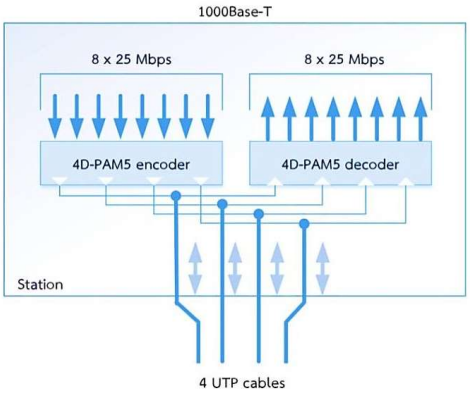
8B/10B เพื่อให้ได้อัตราความเร็วรับส่งข้อมูลรวมเท่ากับ 1.25 Gbps และส่งไปเข้ารหัสข้อมูลอีกครั้งด้วยเทคนิคการเข้ารหัสแบบ NRZ ดังภาพที่ 7.9



ภาพที่ 7.9 วิธีรับส่งข้อมูลของ 1000Base-SX, 1000Base-LX และ แบบ 1000Base-CX
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-21)

2. 1000Base-T4

รูปแบบเครือข่ายกิกะบิตอีเทอร์เน็ตแบบ 1000Base-T4 เป็นเครือข่ายแลนที่ใช้สายนำสัญญาณ 4 คู่ แบบสายคู่บิดเกลียว UTP เครือข่ายนี้ทำการเข้ารหัสสัญญาณข้อมูลที่มีอัตราความเร็วการรับส่ง 125 Mbps จำนวน 8 ช่องสัญญาณด้วยเทคนิคการเข้ารหัสแบบ 4D-PAM5 และทำการจับคู่เชื่อมโยงแต่ละอินพุตและเอาท์พุตของการเข้ารหัสแบบ 4D-PAM5 ให้เข้าคู่กันสำหรับการรับและส่งข้อมูลเพื่อให้สัญญาณที่ถูกเข้ารหัสตอบสนองต่อแบนด์วิดท์ข้อมูลได้อย่างเหมาะสม ดังภาพที่ 7.10



ภาพที่ 7.10 วิธีรับส่งข้อมูลแบบ 1000Base-T4
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 8-21)

7.3.3 เท็นกิกะบิตอีเทอร์เน็ต (10 Gigabit Ethernet)

เท็นกิกะบิตอีเทอร์เน็ต เป็นเทคโนโลยีเครือข่ายใหม่สำหรับเครือข่ายอีเทอร์เน็ตที่มีอัตราความเร็วการรับส่งข้อมูลที่สูงขนาด 10 Gbps สนับสนุนโครงสร้างเครือข่ายทั้งแบบแลนและแบบแมน และอาจรวมถึงเครือข่ายแบบแวน เทคโนโลยีเครือข่ายนี้ทางคณะกรรมการ IEEE เรียกมาตรฐานนี้ว่า IEEE 802.3ae โครงสร้างเครือข่ายชนิดนี้จะใช้สายใยแก้วนำแสง 2 สาย สำหรับการติดต่อสื่อสารแบบ Full-Duplex และแบ่งรูปแบบเครือข่ายได้เป็น 4 รูปแบบดังแสดงในตารางที่ 7.3

ตารางที่ 7.3 รูปแบบเครือข่ายเท็นกิกะบิตอีเทอร์เน็ต

รูปแบบเท็นกิกะบิตอีเทอร์เน็ต	ชนิดสายนำสัญญาณ	ความยาวสาย	การเข้ารหัสข้อมูล
100Base-SR	Fiber 850 nm	300 เมตร	64B66B
100Base-LR	Fiber 1310 nm	10 กิโลเมตร	64B66B
100Base-EW	Fiber 1350 nm	40 กิโลเมตร	SONET
100Base-X4	Fiber 1310 nm	300 เมตร ถึง 10 กิโลเมตร	8B10B

ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 358)

จากตาราง 7.3 รูปแบบเครือข่ายเครือข่ายเท็นกิกะบิตอีเทอร์เน็ตจะใช้สายใยแก้วนำแสงที่เหมาะสมกับแต่ละความยาวคลื่นแสงและทำให้ระยะทางการติดต่อสื่อสารมีความแตกต่างกัน ในขณะเดียวกันแต่ละเทคนิควิธีการเข้ารหัสสัญญาณข้อมูลบนแต่สายที่เหมาะสมก็จะมีผลต่ออัตราความเร็วการรับส่งข้อมูลด้วย

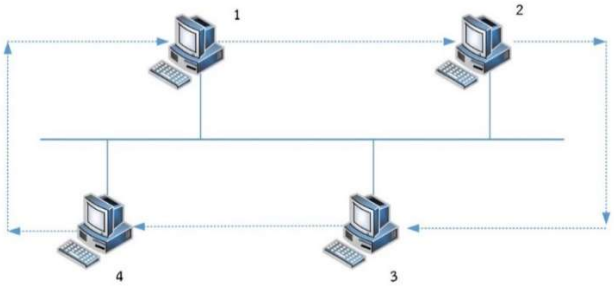
7.4 โทเค็นบัส และโทเค็นริง

โทเค็นบัส และโทเค็นริง (Token Bus and Token Ring) เป็นเครือข่ายท้องถิ่นที่มีการกล่าวถึงน้อยในปัจจุบัน สามารถสรุปเนื้อหาได้ดังนี้ (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 56-60)

7.4.1 โทเค็นบัส

โทเค็นบัส (Token Bus) เป็นเครือข่ายที่รวมข้อดีของอีเทอร์เน็ตและโทเค็นริงเข้าด้วยกัน รูปแบบการติดตั้งในเชิงกายภาพจะเหมือนกับอีเทอร์เน็ต แต่ใช้วิธีเข้าถึงสื่อกลางแบบ

Token Passing จึงไม่เกิดการชนกันของกลุ่มข้อมูลภายในสายส่ง โทเค็นบัสมีรูปแบบทางกายภาพแบบบัสแต่การทำงานภายในเป็นแบบวงแหวน ปัจจุบันเครือข่ายโทเค็นบัสไม่มีการใช้งานแล้ว ดังภาพที่ 7.11



ภาพที่ 7.11 เครือข่ายโทเค็นบัส

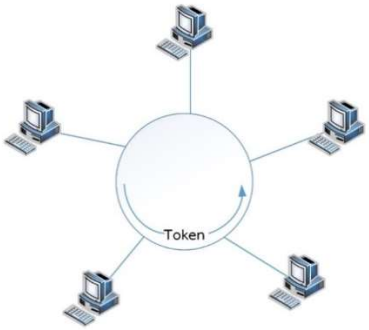
ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 56)

7.4.2 โทเค็นริง

เทคโนโลยีโทเค็นริง (Token Ring) เป็นโครงสร้างของแลนที่มีประสิทธิภาพสูง ซึ่งออกแบบเพื่อรองรับการใช้งานที่มีจำนวนมาก เครือข่ายโทเค็นริงประกอบด้วยวงแหวนสถานี (Ring Station) และสื่อที่ใช้ดังภาพที่ 7.12 ซึ่งเป็นการทำงานแบบร่วมอนุญาตให้อุปกรณ์เชื่อมต่อกันโดยผ่านวงแหวน เครือข่ายโทเค็นริงใช้อุปกรณ์ Wiring Concentrator หรือเรียกว่า Multistation Access Unit (MAU) เครือข่ายโทเค็นริงสามารถปรับค่าด้วยวงแหวนหนึ่งวง หรือมากกว่าหนึ่งวงก็ได้ และใช้กับเซิร์ฟเวอร์มากถึง 3 เครื่อง ที่สามารถเชื่อมต่อในแต่ละวงได้

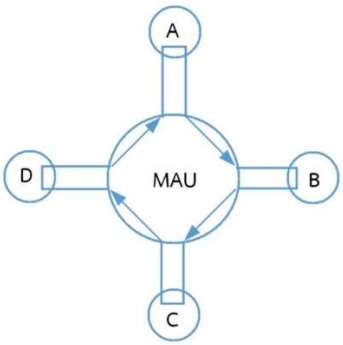
การทำงานของโทเค็นริง

การไหลของข้อมูลในเครือข่ายโทเค็นริงจะผ่านไปตามสถานีแต่ละแห่งที่อยู่บนวงแหวน และแต่ละสถานีจะส่งข้อมูลไปยังสถานีอื่นๆ ต่อไปบนวงแหวน ในทางกายภาพโทเค็นริงมีลักษณะโครงสร้างเป็นแบบดาวและทางไฟฟ้าคือโครงสร้างแบบวงแหวน โดยที่โทเค็นเป็นเฟรมขนาด 3 ไบต์ เคลื่อนที่เป็นรูปวงรอบๆ เครือข่าย เครือข่ายโทเค็นริงจะใช้รหัสโทเค็นเป็นตัวประสานการทำงานบนวงแหวน โดยโทเค็นว่างจะเกิดขึ้นทุกๆ หน่วยเวลา เมื่อสถานีใดต้องการส่งข้อมูลก็จะรอครอบครองโทเค็น เมื่อครอบครองได้แล้วก็จะแนบข้อมูลไปพร้อมกับโทเค็น แต่ถ้าไม่มีสถานีใดส่งข้อมูล โทเค็นก็จะหมุนเวียนในวงแหวนไปเรื่อยๆ ดังภาพที่ 7.12 และ 7.13



ภาพที่ 7.12 โครงสร้างระบบ Token Ring

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 48)



ภาพที่ 7.13 แสดงทิศทางของข้อมูลในเครือข่าย Token Ring

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 48)

การเชื่อมต่อเครือข่ายโทเค็นริง

สถานีวงแหวน (Ring Station) หรือที่เรียกว่า Multistation Access Unit (MAU) หรือ Multiple Access Unit (MAU) โดยคอมพิวเตอร์แต่ละตัวเชื่อมต่อกับ MAU และแต่ละ MAU นั้น สามารถเชื่อมต่อสถานีได้สูงสุด 8 สถานี โดยที่สายคู่บิดเกลียวหุ้มฉนวน (STP) และสายคู่บิดเกลียวไม่หุ้มฉนวน (UTP) นั้นจะใช้สำหรับเครือข่ายโทเค็นริงที่มีความเร็ว 16 และ 4 Mbps ตามลำดับ ในขณะที่สถานีเชื่อมต่อกับวงแหวนนั้นมีการทำงานดังนี้

1. สถานีรับข้อมูลจากวงแหวนและส่งต่อไปยังสถานีต่อไป
2. สถานีนำข้อมูลของตัวเองออกจากวงแหวน
3. แต่ละสถานีส่งต่อข้อมูลบนวงแหวนและเมื่อข้อมูลกลับสู่สถานีที่ส่งออกไป สถานีจะตรวจสอบข้อผิดพลาดของข้อมูลนั้น

การขยายวงแหวน สถานีที่เชื่อมต่อวงแหวนในเครือข่ายโทเค็นริงนั้นจะเชื่อมต่อกับ MAU ได้สูงสุด 8 สถานี ซึ่งในกรณีที่ต้องการจะเชื่อมต่อสถานี 16 แห่งเข้ากับวงแหวนนั้น จะต้องใช้ MAU 2 หน่วย โดยที่แต่ละ MAU จะมีพอร์ต Ring-Out และ Ring-In ซึ่งต้องเชื่อมต่อพอร์ต Ring-Out ของ MAU1 เข้ากับ Ring-In ของ MAU2 และเชื่อมต่อพอร์ต Ring-In ของ MAU1 กับ Ring-Out ของ MAU2 ทำให้วงแหวนมีขนาดใหญ่ขึ้นและสามารถเชื่อมต่อสถานีได้ถึง 16 สถานี

การจัดการวงแหวน

โทเค็นริงและโพรโทคอลนั้นถูกออกแบบเพื่อสร้างเครือข่ายโทเค็นริงให้มีการจัดการได้ด้วยตนเอง เครือข่ายโทเค็นริงนั้นจะถูกจัดการด้วย Token Ring Network Card ทั้งหมด Token Ring NIC (Network Interface Card) นั้นจะมีฟังก์ชันการจัดการเครือข่าย เช่น การเชื่อมต่อสถานีใหม่เข้ากับเครือข่ายโดยที่ไม่มีการหยุดชะงัก

การตรวจจับความผิดพลาดและแก้ไข บนวงแหวนจะมีสถานีหนึ่งซึ่งทำหน้าที่คล้ายกับมอนิเตอร์ใช้งาน ส่วนสถานีอื่นจะทำหน้าที่มอนิเตอร์สำรอง มอนิเตอร์ใช้งานมีหลักการทำงาน ดังนี้

1. สร้าง 24 บิต Token
2. กระจายเฟรม MAC ของมอนิเตอร์ใช้งานทุกๆ 7 วินาที ไปยังทุกๆ สถานีในวงแหวน ซึ่งจะแจ้งให้ทราบว่ามีมอนิเตอร์ใช้งานอยู่บนวงแหวน
3. กำหนด Address ของ Upstream ทุกแห่งใช้งานของรอบข้าง
4. ตรวจสอบความเสียหายของโทเค็นและเฟรม
5. บำรุงรักษาวงแหวนหลัก (Ring Master) และตรวจสอบสำหรับเวลาควบคุม (Control Timing)
6. ในการกำจัดวงแหวนนั้น มอนิเตอร์ใช้งานจะส่งเฟรมเตือน เพื่อแจ้งให้ทุกสถานีทราบว่ามีปัญหาเกิดขึ้นบนเครือข่ายและการส่งต่อโทเค็นจะหยุดลง
7. เมื่อมอนิเตอร์ใช้งานล้มเหลว จะมีมอนิเตอร์สำรองทำหน้าที่เป็นมอนิเตอร์ใช้งานแทนทันที

การเพิ่มสถานีเข้าไปในวงแหวน การเพิ่มสถานีเข้ากับเครือข่ายจะมีลำดับการทำงานดังนี้

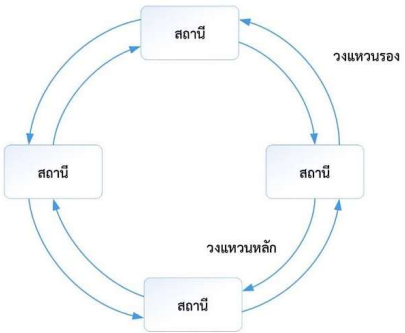
1. เชื่อมต่อสถานีเข้ากับวงแหวนทางกายภาพ
2. สถานีจะส่ง เฟรม MAC ให้กับ MAU เพื่อทดสอบการเชื่อมต่อของสาย

3. สถานีนั้นจะต้องยืนยัน Address ของตัวเองอีกครั้งโดยส่งเฟรม MAC กับต้นทางเดิมและปลายทาง และตรวจสอบสถานีของส่วนของเฟรมนั้นในกรณีที่สถานีใดสถานีหนึ่งคัดลอกเฟรมนั้นด้วย

7.5 เอฟดีดีไอ

เอฟดีดีไอ (FDDI) เป็นแลนความเร็วสูงที่ใช้โครงสร้างแบบวงแหวนด้วยอัตราของข้อมูลเท่ากับ 100 Mbps ซึ่งจะใช้วงแหวน 2 วง ที่เรียกว่าโครงสร้างวงแหวนคู่ เอฟดีดีไอมีลักษณะคล้ายกับโทเค็นริง คือจะใช้สายใยแก้วนำแสงเป็นตัวกลางในการส่งผ่านข้อมูล ข้อได้เปรียบหลักจากการใช้สายใยแก้วนำแสง ได้แก่ ระบบรักษาความปลอดภัย เนื่องจากไม่มีสัญญาณไฟฟ้าระหว่างสายนำสัญญาณกับหัวต่อ

เอฟดีดีไอจะใช้วงแหวน 2 วง โดยให้วงหนึ่งเป็นวงหลักและอีกวงหนึ่งเป็นวงรองตามลำดับ โดยข้อมูลจะเคลื่อนที่ไปตามทิศทางตรงข้ามกัน วงแหวนหลักจะใช้สำหรับส่งข้อมูลและวงแหวนรองจะใช้สำหรับสำรองข้อมูลในกรณีที่เกิดปัญหากับวงแหวนหลัก เอฟดีดีไอจะอนุญาตให้จำนวนสถานีมากกว่า 1000 สถานี เชื่อมต่อกับวงแหวนได้ มีขนาดเส้นรอบวงยาวสูงสุดประมาณ 200 กิโลเมตร ดังภาพที่ 7.14 (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 107)



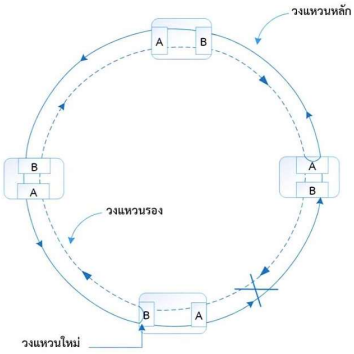
ภาพที่ 7.14 แสดงการถ่ายเทข้อมูลของ FDDI

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 108)

7.5.1 การทำงานของเอฟดีดีไอ

เอฟดีดีไอใช้วงแหวน 2 วง ในทิศทางตรงกันข้าม ถ้าวงใดหยุดชะงัก อีกวงจะรองรับข้อมูลทั้งหมดแทน ในกรณีที่หยุดชะงักในตำแหน่งเดียวกันทั้ง 2 วง วงแหวนนั้นจะสามารถเชื่อมต่อเข้าด้วยกันเพื่อจะสร้างเป็นวงแหวนเดียวได้

สถานีทุกสถานีต้องการที่จะส่งข้อมูล FDDI Access Method จะกำหนดว่าจะต้องรอนานเพียงใดจึงจะส่งข้อมูลได้ โดยการรวมกันระหว่างข้อมูลขนาดใหญ่กับการส่งความเร็วสูง เอฟดีดีไอจึงสามารถถ่ายโอนข้อมูลได้อย่างมีประสิทธิภาพจากจุดหนึ่งไปที่ต่างๆ เหมาะสำหรับเครือข่ายแกนหลัก (backbone network) ดังภาพที่ 7.15

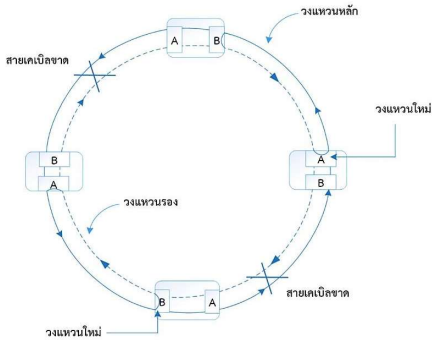


ภาพที่ 7.15 FDDI Wrapping

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 111)

7.5.2 การตรวจสอบข้อผิดพลาดในเอฟดีดีไอ

ระบบสามารถตอบสนองฮาร์ดแวร์และซอฟต์แวร์ที่ขัดข้องหรือผิดพลาดได้ และทำให้ระบบสามารถทำงานได้ต่อได้ในขณะที่ยังมีการขัดข้องอยู่ เนื่องจาก FDDI ใช้ระบบใยแก้วนำแสง 2 วง คือ วงแหวนหลักและวงแหวนรอง ซึ่งการเดินทางของข้อมูลจะกลับทิศกัน ทำให้ระบบนี้รองรับการเกิดข้อผิดพลาดได้ ถ้าวงแหวนหลักเกิดการผิดพลาด FDDI จะใช้วงแหวนรองที่ใช้การสำรองข้อมูล หากกรณีเกิดความเสียหายทั้ง 2 วง ระบบนี้เชื่อมต่อวงแหวนทั้ง 2 วงเข้าด้วยกัน (wraps) อย่างอัตโนมัติ และเปลี่ยนระบบไปสู่วงแหวนเดี่ยว ดังภาพที่ 7.16



ภาพที่ 7.16 การเกิดความเสียหายต่อสาย 2 จุด และ FDDI จะเชื่อมวงทั้ง 2 วงเข้าด้วยกัน

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 112)

7.6 ไอเอสดีเอ็น

ไอเอสดีเอ็น (Integrated Services Digital Network : ISDN) เป็นเครือข่ายโทรคมนาคมสาธารณะที่ได้พัฒนาการให้บริการด้านการสื่อสารจากระบบเครือข่ายพีเอสทีเอ็นให้มีประสิทธิภาพมากขึ้น ให้บริการด้านการสื่อสารข้อมูลแบบต่างๆ เช่น ข้อความ เสียง และภาพในรูปแบบสัญญาณทั้งแอนะล็อกและดิจิทัล ในระบบเครือข่ายสวิตชิงแบบดิจิทัลการเชื่อมต่อกับระบบเครือข่ายไอเอสดีเอ็นจะใช้อุปกรณ์เชื่อมต่อเฉพาะแบบดิจิทัล จึงเป็นเครือข่ายที่เน้นการให้บริการการสื่อสารข้อมูลและอุปกรณ์สำหรับการเชื่อมต่อแบบดิจิทัลเป็นส่วนใหญ่

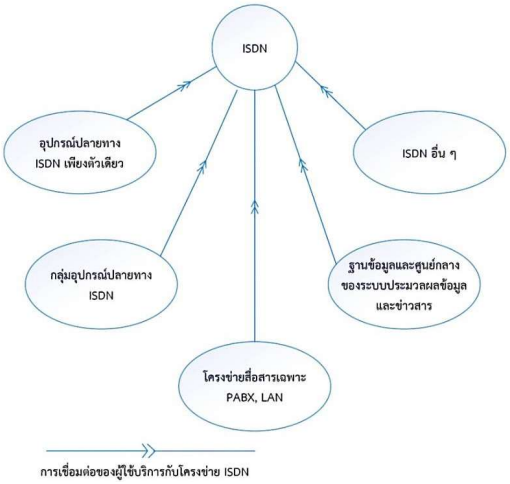
การเข้าไปใช้บริการในเครือข่ายไอเอสดีเอ็น ทำได้โดยต่อผ่านอุปกรณ์สื่อสารข้อมูลกับเครือข่ายไอเอสดีเอ็นที่จุดเชื่อมต่อระหว่างเครือข่ายกับผู้ใช้บริการ เพื่อให้ผู้ใช้บริการได้รับบริการต่างๆ ที่มีอยู่ภายในเครือข่ายไอเอสดีเอ็นมากที่สุด และเพื่อให้โครงสร้างของสัญญาณเป็นแบบเดียวกันทั้งหมด (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 143-148)

7.6.1 ลักษณะการเชื่อมต่อเครือข่ายไอเอสดีเอ็น

การเข้าไปใช้บริการภายในเครือข่ายไอเอสดีเอ็นจำเป็นต้องผ่านอุปกรณ์เชื่อมต่อมาตรฐานที่ได้กำหนดเอาไว้ สำหรับการเชื่อมต่ออุปกรณ์สื่อสารข้อมูลชนิดนั้นๆ การเชื่อมต่ออุปกรณ์สื่อสารข้อมูลในเครือข่ายไอเอสดีเอ็น มีหลายรูปแบบ ดังนี้

1. การต่อเข้ากับอุปกรณ์ปลายทางสำหรับเครือข่ายไอเอสดีเอ็นตัวเดียว
2. การต่อเข้ากับอุปกรณ์ปลายทางสำหรับเครือข่ายไอเอสดีเอ็นหลายตัว
3. การต่อเข้ากับเครือข่ายสื่อสารเฉพาะ เช่น เครือข่ายท้องถิ่น (LAN) ตู้สาขาโทรศัพท์ (PABX)
4. การต่อเข้ากับฐานข้อมูล ศูนย์กลางของระบบการประมวลผลข้อมูลและข่าวสาร
5. การต่อเข้ากับอุปกรณ์ปลายทางที่ไม่ได้ออกแบบสำหรับเครือข่ายไอเอสดีเอ็น
6. การต่อเข้ากับเครือข่ายอื่นๆ

การเชื่อมต่ออุปกรณ์สื่อสารข้อมูลในเครือข่ายไอเอสดีเอ็นมีหลายแบบ ดังแสดงในภาพที่ 7.17

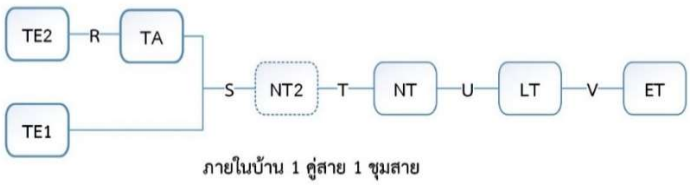


ภาพที่ 7.17 การเชื่อมต่อของผู้ใช้บริการกับเครือข่าย ISDN

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 146)

7.6.2 การเชื่อมต่อระหว่างเครือข่ายไอเอสดีเอ็นกับผู้ใช้บริการ

การเชื่อมต่อระหว่างเครือข่ายไอเอสดีเอ็นกับผู้ให้บริการประกอบด้วยอุปกรณ์ที่ทำหน้าที่ต่างๆ เช่น TE1, TE2, NT และ TA ที่ต่ออยู่กับจุดเชื่อมต่อมาตรฐาน โดยกำหนดไว้ 5 จุด คือ จุดเชื่อมต่อมาตรฐาน R, S, T, U และ V ดังภาพที่ 7.18



ภาพที่ 7.18 จุดเชื่อมต่อมาตรฐานและอุปกรณ์ต่างๆ ในเครือข่ายไอเอสดีเอ็น

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 146)

อุปกรณ์เชื่อมต่อกับจุดมาตรฐาน แบ่งออกเป็น 3 กลุ่มใหญ่ ดังนี้

1. อุปกรณ์ปลายทาง (Terminal Equipment) ซึ่งอยู่ภายในบ้านผู้ใช้บริการทำหน้าที่เป็นตัวกลางในการติดต่อสื่อสารระหว่างผู้ใช้บริการกับเครือข่ายไอเอสดีเอ็น ที่จุดเชื่อมต่อจะมีอุปกรณ์ปลายทางได้สูงสุด 8 เครื่องสำหรับ Basis Access Interface (BAI) อุปกรณ์ปลายทาง (Terminal Equipment หรือ TE) มีอยู่ด้วยกัน 2 แบบ ดังนี้

1.1 อุปกรณ์ปลายทางประเภทที่ 1 หรือ TE1 (Terminal Equipment Type 1) เป็นอุปกรณ์ปลายทางที่ออกแบบสำหรับไอเอสดีเอ็น และสามารถต่อเข้ากับชุดเชื่อมต่อมาตรฐาน S ได้โดยตรง ไม่จำเป็นต้องมีอุปกรณ์อื่นมาช่วยในการเปลี่ยนสัญญาณกับเครือข่าย

1.2 อุปกรณ์ปลายทางประเภทที่ 2 หรือ TE2 (Terminal Equipment Type 2) เป็นอุปกรณ์ปลายทางที่มีใช้ในปัจจุบัน ซึ่งจำเป็นต้องมี Terminal Adapter หรือ TA เพื่อต่อกับจุดเชื่อมต่อมาตรฐาน S โดย TA ทำหน้าที่แปลงลักษณะบางอย่างของอุปกรณ์ TE2 เช่น เปลี่ยนแปลงโพรโทคอล ของไอเอสดีเอ็นที่จุดเชื่อมต่อมาตรฐาน S เป็นต้น

2. อุปกรณ์เชื่อมต่อเครือข่าย (Network Termination หรือ NT) แบ่งออกเป็น 2 แบบ ดังนี้

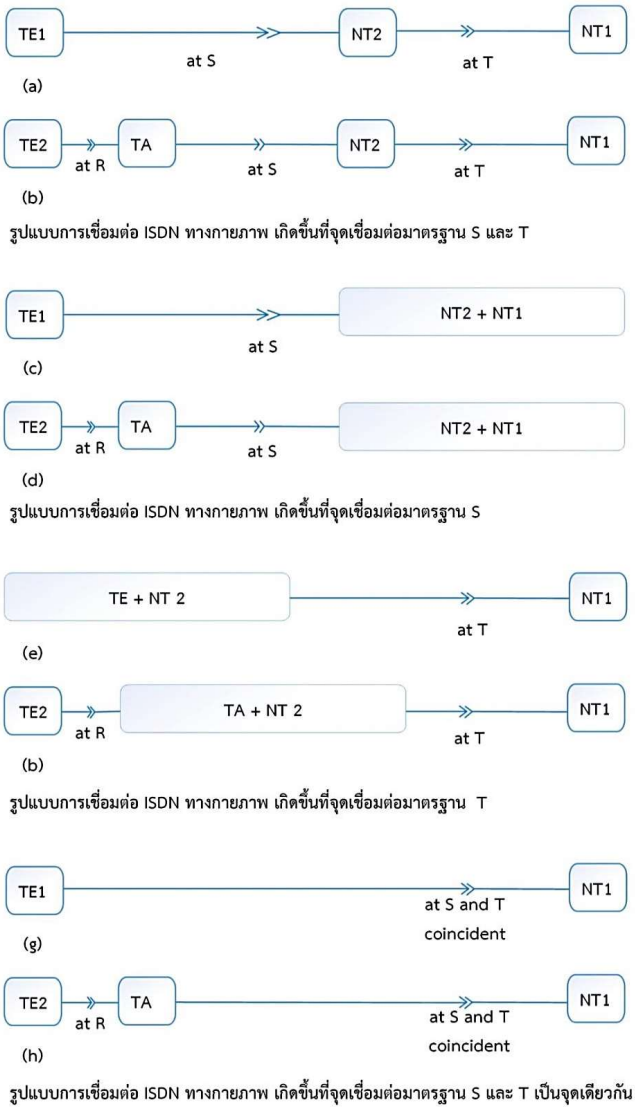
2.1 อุปกรณ์เชื่อมต่อเครือข่ายประเภทที่ 1 หรือ NT1 (Network Termination 1) ต่อกับจุดเชื่อมต่อมาตรฐาน S หรือ T มีหน้าที่แปลงสัญญาณจากคู่สายเข้าสู่โครงสร้างของช่องสัญญาณ ลักษณะของคู่สายจะเป็นสายโทรศัพท์ธรรมดา (Copper Wire) 1 คู่สาย อุปกรณ์ NT1 นี้ จะเป็นตัวแบ่งแยกระหว่างอุปกรณ์ของผู้ใช้บริการกับอุปกรณ์ของเครือข่ายไอเอสดีเอ็น ให้บริการครอบคลุมโพรโทคอลชั้นที่ 1 ของแบบจำลองโอเอสไอ และทำการเทอร์มิเนต (Termination) คู่สายด้วย

2.2 อุปกรณ์เชื่อมต่อเครือข่ายประเภทที่ 2 หรือ NT2 (Network Termination 2) เป็นอุปกรณ์ที่จะมีหรือไม่ก็ได้ หากไม่มีแสดงว่าจุดเชื่อมต่อมาตรฐาน S หรือ T เป็นจุดเดียวกัน หากมีอุปกรณ์ NT2 เชื่อมต่ออยู่จะให้บริการครอบคลุมโพรโทคอลชั้นที่ 1, 2 และ 3 ของแบบจำลองโอเอสไอ มีการสวิตช์และมัลติเพล็กซ์ ทำให้ต่ออุปกรณ์ปลายทางเข้ากับเครือข่ายไอเอสดีเอ็นได้มากขึ้น ตัวอย่างของอุปกรณ์ NT2 ได้แก่ Intercom PABX และ LAN

3. อุปกรณ์เชื่อมต่อสายและเชื่อมต่อชุมสายหรือ LT (Line Terminal และ Exchange Terminal) อุปกรณ์เชื่อมต่อสาย (Line Terminal) เป็นอุปกรณ์ที่ติดตั้งอยู่ในชุมสายไอเอสดีเอ็นสำหรับใช้ต่อสายของผู้ให้บริการกับชุมสาย ส่วนอุปกรณ์เชื่อมต่อชุมสายหรืออีที (Exchange Terminal : ET) เป็นอุปกรณ์ที่ติดตั้งอยู่ในชุมสายไอเอสดีเอ็นทำหน้าที่ส่งสัญญาณเพื่อการเริ่มต้นและติดต่อระหว่างชุมสายไอเอสดีเอ็น

7.6.3 รูปแบบการเชื่อมต่อ (Interface Configuration)

รูปแบบการเชื่อมต่อของอุปกรณ์ปลายทางกับอุปกรณ์เชื่อมต่อเครือข่ายสามารถกระทำได้หลายรูปแบบขึ้นอยู่กับผู้ใช้บริการ ดังแสดงในภาพที่ 7.19



ภาพที่ 7.19 รูปแบบการเชื่อมไอเอสดีเอ็นต่อกับอุปกรณ์ต่างๆ

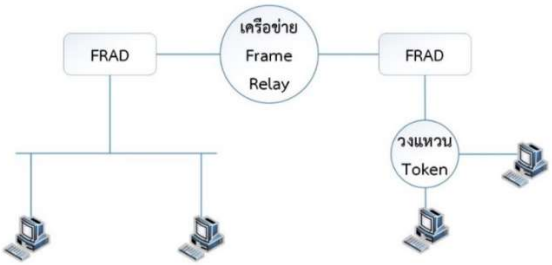
ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 148)

จากภาพที่ 7.19 ที่จุดเชื่อมต่อมาตรฐาน S อุปกรณ์ปลายทาง TE1 สามารถต่อผ่านอุปกรณ์ TA ที่จุดเชื่อมต่อมาตรฐาน R ก่อน แล้วจึงทำการเชื่อมต่อที่จุดเชื่อมต่อมาตรฐาน S เหมือนกับ TE1

7.7 เทคโนโลยีเฟรมรีเลย์

เฟรมรีเลย์ (Frame Relay) ถูกออกแบบครั้งแรกสำหรับเครือข่ายไอเอสดีเอ็นซึ่งจะใช้สำหรับ ITU-T ในปี 1984 ITU-T อนุมัติให้ข้อเสนอและมาตรฐานนี้เข้าสู่ข้อกำหนดหน้าที่ของรีเลย์และเราท์เตอร์ในชั้นเชื่อมโยงข้อมูลของแบบจำลองโอเอสไอ จึงทำให้องค์กรขนาดใหญ่ที่มีสถานที่ตั้งหลายๆ ที่สามารถเชื่อมต่อเข้าด้วยกันเป็นเครือข่ายได้ เช่น องค์กรมีสำนักงานกว่า 100 แห่ง ในแต่ละแห่งต้องใช้สายเท่ากับจำนวนสำนักงานที่จะเชื่อมต่อเครือข่าย ด้วยเหตุที่วิธีการเช่าสายจากหน่วยงานที่ให้บริการโทรศัพท์จะไม่ค่อยคุ้มค่า เฟรมรีเลย์จึงเป็นทางเลือกอีกทางหนึ่งซึ่งมีค่าใช้จ่ายน้อยกว่าการเช่าสาย ทำให้สามารถใช้แลนสำหรับเชื่อมต่อระหว่างกันโดยไม่คำนึงถึงความหลากหลายของโพรโทคอลที่ใช้

เฟรมรีเลย์ เป็นโพรโทคอลสวิตช์แพ็กเกจ ถูกเสนอจากบริษัทผู้ให้บริการโทรศัพท์ที่จะเปลี่ยนจากโพรโทคอล X.25 ไปเป็นลักษณะ Wide Area Network (WAN) สถาปัตยกรรมของเฟรมรีเลย์ ประกอบด้วยเครือข่าย Frame Relay, Frame Relay Assembler/ Disassembler (FRAD) และผู้ใช้แลน การทำงานของ FRAD มีไว้สำหรับการแปลงรูปแบบของเฟรมจากสถานีนั้นเป็นรูปแบบของเครือข่ายเฟรมรีเลย์และในทางกลับกันด้วย โดยที่แบบอ้างอิงของเฟรมรีเลย์ จะทำงานในชั้นเชื่อมโยงข้อมูลและชั้นสื่อสารกายภาพของแบบจำลองโอเอสไอ ดังภาพที่ 7.20 (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 123-126)



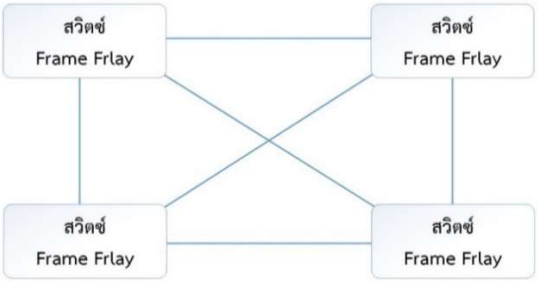
ภาพที่ 7.20 โครงสร้างของเฟรมรีเลย์

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 124)

7.7.1 เครือข่ายเฟรมรีเลย์

เครือข่ายเฟรมรีเลย์ ประกอบด้วยสวิตช์เฟรมรีเลย์ ซึ่งจะเชื่อมต่อระหว่างแต่ละตัวโดยผ่าน T-1, T-3 หรือสายใยแก้วนำแสง โดยสวิตช์อยู่ในสำนักงานกลางของสถานีแต่ละแห่ง และเครือข่ายเฟรมรีเลย์ จะถูกควบคุมโดยบริษัทผู้ให้บริการโทรศัพท์

เฟรมรีเลย์ เป็นการบริการโดยใช้วงจรเช่าเพื่อเชื่อมต่อองค์กรแต่ละแห่งเข้าด้วยกันแม้จะอยู่ต่างที่กันก็ตาม เครือข่ายที่ต้องการเชื่อมต่อผ่านเฟรมรีเลย์จะต้องมีอุปกรณ์ Frame Relay Access เช่น ระบบแลน เราท์เตอร์ สวิตช์เฟรมรีเลย์ การบริการเฟรมรีเลย์ ดังภาพที่ 7.21



ภาพที่ 7.21 เครือข่ายเฟรมรีเลย์

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 124)

การทำงานของสวิตช์เฟรมรีเลย์ จะติดตั้งอยู่ที่สำนักงานของบริษัทผู้ให้บริการโทรศัพท์มีการทำงาน ดังนี้

1. ตรวจสอบข้อผิดพลาดของข้อมูลที่ได้รับจากผู้ใช้หรือสวิตช์ก่อนหน้านั้น หากมีข้อผิดพลาดจะทำการละทิ้งข้อมูลส่วนนั้นออก และในทางตรงกันข้ามจะส่งต่อไปยังสวิตช์ตัวถัดไปหรือปลายทาง

2. จะใช้การมัลติเพล็กซ์แบบแพ็กเก็ตเชิงสถิติ (Statistical Packet Multiplexing) สำหรับการมัลติเพล็กซ์และการหาเส้นทาง

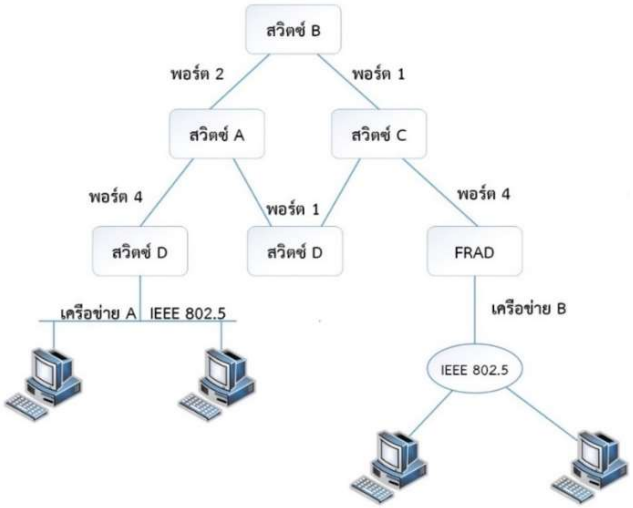
3. จัดการเรื่องความสมบูรณ์ของข้อมูล โดยจะมีการตรวจสอบข้อผิดพลาดและทำการส่งข้อมูลซ้ำอีกรอบ

4. เมื่อข้อมูลถูกส่งระหว่างสวิตช์จะไม่มีการรับรู้ระหว่างสวิตช์

7.7.2 การทำงานของเฟรมรีเลย์

การทำงานของเทคโนโลยีเฟรมรีเลย์ เมื่อเครือข่าย A เชื่อมต่อกับสวิตช์ A ผ่าน FRAD และเครือข่าย B เชื่อมต่อผ่าน FRAD ไปยังสวิตช์ C การเชื่อมต่อแต่ละส่วนนั้นมี DLCI เป็นของตัวเองซึ่งกำหนดจากผู้ให้บริการใน PVC แต่ละวงจร เส้นทางระหว่าง 2 สถานีนี้เรียกว่า Virtual Circuit ซึ่งเฟรมรีเลย์รองรับทั้ง Permanent Virtual Circuit (PVC) และ

Switched Virtual Circuit (SVC) โดยจะรองรับ PVC หลายๆ วงจรในเวลาเดียวกัน ทำให้สามารถเชื่อมต่อได้หลายสถานีด้วยการเชื่อมต่อทางเดียว ดังภาพที่ 7.22

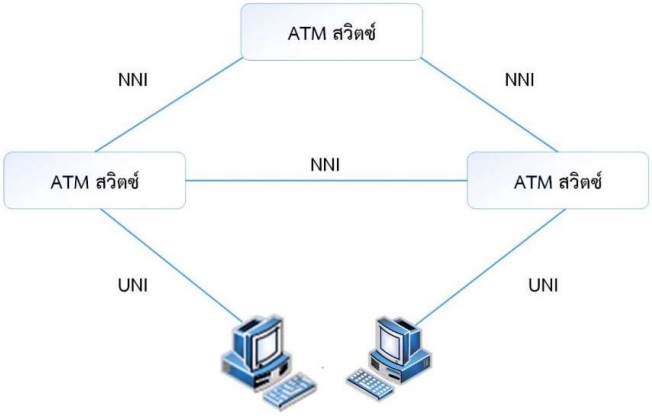


ภาพที่ 7.22 การทำงานของเฟรมรีเลย์

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 126)

7.8 เครือข่ายเอทีเอ็ม

เครือข่ายเอทีเอ็ม (Asynchronous Transfer Mode : ATM) เป็นเทคโนโลยีของเครือข่ายซึ่งสามารถใช้ทางด่วนข้อมูล (Information Superhighway) ส่งข้อมูลได้มากกว่า เช่น ข้อมูล เสียง รูป การสแกนภาพ วิดีโอคอนเฟอร์เรนซ์ ทั้งเครือข่ายภายในและภายนอก สามารถรองรับข้อมูลทั้งหมดผ่านวงจรปกติได้ เอทีเอ็มจะใช้แบนด์วิดท์ตามความต้องการของผู้ใช้งาน โดยไม่ขึ้นกับโปรแกรมที่ใช้ และมีการทำงานอยู่ระหว่าง 1.5 Mbps -2 Gbps ในเครือข่ายทุกประเภท นอกจากนั้นเอทีเอ็มยังใช้ในการเครือข่าย B-ISDN ได้อีกด้วย เครือข่ายของเอทีเอ็มประกอบด้วย สวิตช์และผู้ใช้งาน การเชื่อมต่อของเอทีเอ็มสามารถแบ่งออกได้เป็น 2 ประเภท ได้แก่ Switch-to-Switch Interface (หรือ Network-to-Network Interface เรียกว่า NNI) และ Switch-to User Interface (เรียกว่า UNI) ดังภาพที่ 7.23 (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 127-130)



ภาพที่ 7.23 การเชื่อมต่อของเครือข่ายเอทีเอ็ม

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 128)

7.8.1 ประเภทของการเชื่อมต่อเครือข่ายเอทีเอ็ม

เครือข่ายเอทีเอ็ม จะใช้วิธีการเชื่อมต่อ 2 ประเภท คือ

1. พีวีซี (Permanent Virtual Connection : PVC) จะติดตั้งโดยผู้จัดการเครือข่าย กลุ่มของสวิตช์เครือข่ายระหว่างแหล่งกำเนิดและเป้าหมายของเอทีเอ็ม จะถูกโปรแกรมด้วยค่าสำหรับ VCI/VPI การส่งข้อมูลจะมีความน่าเชื่อถือมากสำหรับการเชื่อมต่อแบบนี้

2. เอสวีซี (Switched Virtual Circuit : SVC) สำหรับการเชื่อมต่อแบบนี้ จะตั้งค่าอัตโนมัติโดย Signaling Protocol ซึ่ง SVC จะใช้กันอย่างกว้างขวางเนื่องจากไม่ต้องติดตั้งด้วยตนเอง แต่จะมีความน่าเชื่อถือน้อยลงเมื่อเทียบกับ PVC

Connection Identifier มีการเชื่อมต่อในเอทีเอ็ม Cell Header อยู่ 2 ประเภท คือ Virtual Path Identifier (VPI) และ Virtual Channel Identifier (VCI) ซึ่งเป็นการหาเส้นทางและการแสดง Cell การเชื่อมต่อแบบ VPI และ VCI จะไม่แสดงจุดหมายปลายทางและที่อยู่ปลายทาง แต่จะแสดงถึงการเชื่อมต่อซึ่งจะนำไปสู่ปลายทาง โดยที่ 1 VPI อาจประกอบด้วยหลายๆ VCI

ถ้าให้ VPI เป็นจำนวนทางรถไฟ และ VCI เป็นจำนวนรถบรรทุก แต่ละรางสามารถขนส่งได้รถบรรทุกได้หลายคัน รถบรรทุกแต่ละคันจะมีเลขเป็นเอกลักษณ์และไว้แสดง VCI ของตัวมันเอง ในขณะที่ Cell เข้าสู่สวิตช์ สวิตช์จะทำหน้าที่ให้ตัวเลข VCI ใหม่ให้กับ Cell

7.8.2 สวิตช์เอทีเอ็ม

สวิตช์เอทีเอ็ม สามารถดำเนินการกับ Cell ที่ความเร็วสูง และมีการทำงานตามลำดับ ดังนี้

1. Cell จะรับข้อมูลทางพอร์ตขาเข้า ซึ่ง VPI/VCI header จะตรวจสอบเพื่อหาพอร์ตขาออกซึ่งส่งข้อมูลออก

2. ส่วน VPI/VCI จะถูกดัดแปลงไปยังค่าใหม่สำหรับพอร์ตขาออก

3. Header Error Control (HEC) จะใช้สำหรับการตรวจสอบข้อผิดพลาดและแก้ไขในส่วนของ Heard Field ของแต่ละ Cell ถ้า HEC ไม่สามารถแก้ไขข้อผิดพลาดได้ สวิตช์เอทีเอ็มจะละทิ้ง Cell นั้น

4. สวิตช์มีส่วนควบคุมซึ่งสามารถปรับค่าในตารางกำหนดเส้นทางได้

5. สวิตช์รองรับการสวิตช์ Cell ได้ในอัตราอย่างน้อย 1,000,000 Cell ต่อวินาที

สวิตช์เอทีเอ็ม มีลักษณะพิเศษ ดังนี้

1. ความจุของบัฟเฟอร์มีมากพอที่จะเก็บ Cell ที่เข้ามาและตารางกำหนดเส้นทาง

2. มีความเร็วพอที่จะถ่ายโอนข้อมูล Cell ที่เข้ามาไปยังพอร์ตขาออก

3. มี 16-32 พอร์ตขาเข้าและออก

4. รองรับ AAL ทั้งหมดทุกประเภท

5. รองรับการเชื่อมต่อทั้งแบบ PVC และ SVC

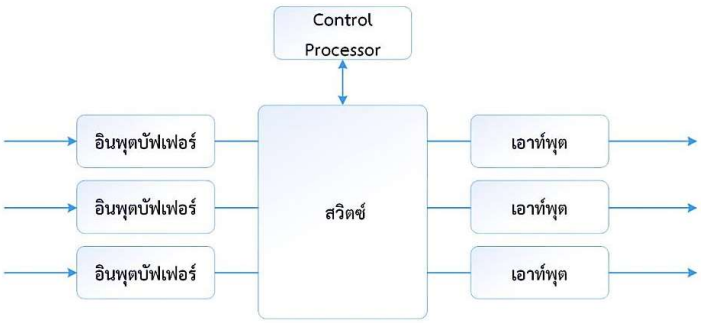
6. รองรับการเชื่อมต่อแบบจุดต่อหลายจุด

7. สามารถควบคุมความคับคั่งของข้อมูลได้

7.8.3 สถาปัตยกรรมของสวิตช์เอทีเอ็ม

ส่วนประกอบที่สำคัญของเครือข่ายเอทีเอ็มคือ สวิตช์มีความสามารถในการประมวลผลกว่าล้าน Cell ต่อวินาที สถาปัตยกรรมของสวิตช์เอทีเอ็มใช้การมัลติเพล็กซ์แบบแพ็กเก็ตสถิต (Statistical Packet Multiplexing หรือ SMP) ซึ่ง SPM จะสามารถจัดสรรแบนด์วิดท์สำหรับช่องขาเข้าซึ่งทำงานอยู่ตลอดเวลา หน้าที่ส่วนควบคุมการประมวลผลจะควบคุมบัฟเฟอร์อินพุต/เอาต์พุต และปรับปรุงตารางกำหนดเส้นทางของสวิตช์ ซึ่งมีสถาปัตยกรรมที่แตกต่าง 2-3 ประเภท ที่ใช้สำหรับสวิตช์เอทีเอ็ม เช่น Delta Switch Matrix และ Banyan Switch Matrix

ATM Switch Blocking สวิตช์เอทีเอ็มเกี่ยวข้องกับ Blocking และ Traffic Congestion ซึ่งจะมี Fabric Blocking และ Head of the line blocking โดยที่ Fabric Blocking จะเกิดขึ้นเมื่อความจุของ Fabric ของสวิตช์น้อยกว่าผลรวมของอัตราของข้อมูลที่เข้า ซึ่งในกรณีนี้จะทำให้สวิตช์ ละทิ้งบาง Cell จะมีข้อจำกัดอยู่ประมาณ 16 หรือ 32 OC-3 พอร์ตขาเข้า ส่วน Head of the line blocking เกิดขึ้นเมื่อพอร์ตขาออกมีความคับครั้งและมี Cell กำลังรอที่เข้าทางพอร์ตขาเข้า สวิตช์จะต้องละทิ้ง Cell บางตัวที่พอร์ตขาออก ซึ่งสวิตช์บางตัวจะสุ่ม Cell ที่จะละทิ้ง และทุกๆ สถานีจะต้องส่งข้อมูลใหม่อีกครั้ง ยิ่งไปกว่านั้น สวิตช์ที่มี Intelligent Switch จะละทิ้ง Cell ที่มาจากแหล่งกำเนิดเพียงแหล่งเดียวออกไป ดังภาพที่ 7.24

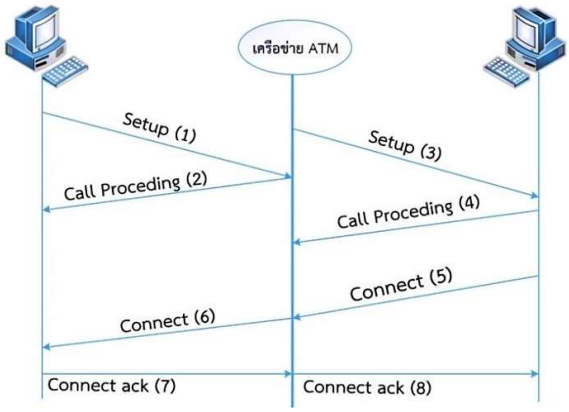


ภาพที่ 7.24 สถาปัตยกรรมของสวิตช์ ATM

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า132)

7.8.4 การเชื่อมต่อระบบผ่านสัญญาณเอทีเอ็ม

ผู้ใช้ที่ต้องการเชื่อมต่อผ่านเครือข่ายเอทีเอ็มไปยังปลายทาง ซึ่งข้อมูลส่งผ่านเครือข่ายจากสวิตช์ไปยังสวิตช์ ด้วยค่า VPI = 0 และ VCI = 5 และการเชื่อมต่อจะแสดงตัวสำหรับต่อสวิตช์จนกระทั่งถึงปลายทาง ดังภาพที่ 7.25 แสดงผู้ใช้ ATM เพื่อสร้างการเชื่อมต่อระหว่างสวิตช์เอทีเอ็มและเครือข่าย และเครือข่ายจะสร้างการเชื่อมต่อไปยังผู้ใช้ปลายทาง ดังภาพที่ 7.25



ภาพที่ 7.25 สัญญาณเอทีเอ็มในการตั้งค่าการเชื่อมต่อ

ที่มา : (ประสิทธิ์ ทีฆพุฒิ, 2559 หน้า 132)

7.8.5 ชั้นการทำงานของเครือข่ายเอทีเอ็ม

เครือข่ายเอทีเอ็มมีทั้งหมด 4 ชั้นด้วยกัน ใช้กับการจราจรที่แตกต่างกันออกไป มีรายละเอียด ดังนี้

1. Adaptation Layer Type 1 (AAL1) ออกแบบสำหรับ Class A Traffic ด้วย CBR เช่น Circuit Emulation และใช้สำหรับวีดีโอแบบไม่มีการบีบอัดและโทรศัพท์ ซึ่งเป็นสิ่งสำคัญที่ Cell จะต้องมีการเรียงลำดับที่ถูกต้องสำหรับการติดต่อสื่อสารด้วยเสียง ดังนั้น จึงต้องเพิ่มลำดับเข้าใน SAR Sublayer

2. Adaptation Layer Type 2 (AAL2) ใช้สำหรับ VBR เช่น Compressed Voiceและ Audio รูปแบบของ AAL2 Cell มีข้อมูลของ Application Layer ถูกส่งต่อไปยัง SAR Sublayer โดย SAR Sublayer จะแบ่งข้อมูลออกเป็นส่วนย่อยๆ เป็น Payload ขนาด 45 ไบต์ และเพิ่ม Header 1 ไบต์ และ 2 ไบต์ สำหรับ Trailer ในแต่ละ Payload จากนั้น SAR จะส่งข้อมูลต่อยัง ATM Layer

3. Adaptation Layer Type 3/4 (AAL3/4) เมื่อ AAL3 และ AAL4 มีการตั้งข้อกำหนดของทั้งสอง AAL ร่วมกันจึงได้เป็น AAL3/4 ที่ถูกออกแบบเพื่อจะใช้งานกับเฟรมที่มีขนาด 64 kB และแบ่งข้อมูลเป็นแต่ละ Cell AAL3/4 เหมาะสำหรับข้อมูลที่ไม่ต้องการให้เกิดความสูญเสียแต่อาจเกิดการดีเลย์ได้ โดยที่ AAL3/4 ใช้สำหรับการส่งข้อมูลแบบ Connection-Oriented รูปแบบของ AAL3/4 ซึ่ง Convergence Sublayer จะรับข้อมูลจากชั้นที่สูงกว่าและเพิ่ม CS header/ trailer ขนาด 4 ไบต์เข้าไป เรียกว่า CS-PDU ซึ่ง CS จะส่ง CS-PDU ไปยัง

SAR Sublayer และทำหน้าที่แบ่งข้อมูลออกเป็นส่วนย่อย ๆ โดยมี Payload และ SAR Header/Trailer ขนาด 44 และ 2 ไบต์ ตามลำดับ

4. Adaptation Layer Type 5 (AAL5) เป็นทางเลือกที่ดีที่สุดสำหรับการถ่ายโอนข้อมูลในเอทีเอ็มเพราะส่วนควบคุมทั้งหมดจะอยู่ใน Cell สุดทาง ซึ่งรูปแบบ AAL5 สามารถใช้กับ LAN Emulation และสามารถรองรับรูปแบบเฟรมของอีเทอร์เน็ตและโทเค็นริงขนาดใหญ่ได้ AAL5 ใช้สำหรับความยาวข้อมูลที่เปลี่ยนแปลงได้มากถึง 65 kb ซึ่ง 65 kb นี้จะแบ่งเป็น Cell ย่อยๆ แต่ละ Cell จะมี Header เหมือนกัน โดยที่ Cell สุดท้ายจะนำเอาข้อมูลควบคุมที่ต้องการทั้งหมด AAL5 Cell มีลักษณะคล้ายๆ AAL3/4 แต่จะใช้ส่วนควบคุมน้อยกว่า

ข้อมูลจากชั้นบนจะถูกส่งไปยัง CS ซึ่งจะทำการเพิ่ม Trailer ให้กับข้อมูลเพื่อสร้าง CS-PDU โดย CS จะส่ง CS-PDU ไปยัง SAR เพื่อแบ่งเป็น Cell ย่อยๆ Cell ละ 48 ไบต์ แต่ละ Cell จะถูกส่งไปยัง ATM Layer ซึ่งถูกเพิ่ม Header ขนาด 5 ไบต์ ให้กับแต่ละ Cell และส่งต่อไปยัง Physical Layer สำหรับส่งต่อไป

7.8.6 ข้อดีและข้อจำกัดของเครือข่ายเอทีเอ็ม

เครือข่ายเอทีเอ็ม มีข้อดี ดังนี้

1. มีความเร็วในการรับส่งข้อมูลสูง

2. รองรับข้อมูลสำหรับการรับส่งได้หลายรูปแบบทั้งอัตราความเร็วข้อมูลคงที่และไม่คงที่และรวมถึงปริมาณของข้อมูลที่มากได้

เครือข่ายเอทีเอ็ม มีข้อจำกัด ดังนี้

1. การยอมรับใช้งานในปัจจุบันยังมีน้อยเมื่อเทียบกับเครือข่ายอีเทอร์เน็ต ที่ได้รับการพัฒนาด้านความเร็วของการรับส่งข้อมูลที่สูงขึ้นอย่างต่อเนื่อง โดยไม่ได้เปลี่ยนแปลงโครงสร้างพื้นฐานสื่อสารเดิมมากหรือการเปลี่ยนแปลงมีความซับซ้อนน้อยกว่าเครือข่ายเอทีเอ็ม

2. การเปลี่ยนไปใช้งานระบบเครือข่ายเอทีเอ็มมีค่าใช้จ่ายค่อนข้างสูง

7.9 สรุป

ระบบเครือข่ายใช้สายเป็นระบบเครือข่ายที่เชื่อมต่ออุปกรณ์สื่อสารด้วยสายนำสัญญาณประเภทสายทองแดงและสายใยแก้วนำแสง โดยการเชื่อมต่อของแต่ละประเภทสายนำสัญญาณในระบบเครือข่ายต้องการให้มีอัตราความเร็วของการรับส่งข้อมูลที่สูง การเชื่อมต่ออินเทอร์เน็ตแบบใช้สาย (Wire Internet) มีการเชื่อมต่อด้วยกันอยู่ 2 ประเภท คือ การเชื่อมต่ออินเทอร์เน็ตรายบุคคล และการเชื่อมต่ออินเทอร์เน็ตแบบองค์กร

อีเทอร์เน็ต (Ethernet) เป็นระบบการขนส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ของเครือข่ายแลนในยุคแรกๆ มีวัตถุประสงค์เพื่อใช้ในการแลกเปลี่ยนข้อมูลและแบ่งปันข้อมูลกันภายในเครือข่ายเท่านั้น แต่ต่อมาได้มีการพัฒนาอีเทอร์เน็ตให้มีประสิทธิภาพมากขึ้นเนื่องจากมีการนำไปใช้อย่างแพร่หลาย ได้แก่ อีเทอร์เน็ตยุคใหม่ (Modern Ethernet) ประกอบด้วย ฟาสต์อีเทอร์เน็ต (Fast Ethernet) กิกะบิตอีเทอร์เน็ต และเท็นกิกะบิตอีเทอร์เน็ต (10 Gigabit Ethernet)

เทคโนโลยีที่เกี่ยวข้องกับเครือข่ายใช้สายมีหลายเทคโนโลยี ได้แก่ โทเค็นบัส เป็นเครือข่ายที่รวมข้อดีของอีเทอร์เน็ตและโทเค็นริงเข้าด้วยกัน รูปแบบการติดตั้งในเชิงกายภาพจะเหมือนกับอีเทอร์เน็ต แต่ใช้วิธีเข้าถึงสื่อกลางแบบ Token Passing จึงไม่เกิดการชนกันของกลุ่มข้อมูลภายในสายส่ง โทเค็นริง (Token Ring) ออกแบบเพื่อรองรับการใช้งานที่มีจำนวนมาก ประกอบด้วยวงแหวนสถานี (Ring Station) และสื่อที่ใช้ สามารถที่จะปรับค่าด้วยวงแหวนหนึ่งวง หรือมากกว่าหนึ่งวงและใช้ได้กับเซิร์ฟเวอร์มากถึงจำนวน 3 เครื่องที่สามารถเชื่อมต่อในแต่ละวงได้ เทคโนโลยีเอฟดีดีไอ (FDDI) เป็นแลนความเร็วสูงที่ใช้โครงสร้างแบบวงแหวนด้วยอัตราของข้อมูลเท่ากับ 100 Mbps ซึ่งจะใช้วงแหวน 2 วง ที่เรียกว่าโครงสร้างวงแหวนคู่ เอฟดีดีไอมีลักษณะคล้ายกับโทเค็นริง คือจะใช้ใยแก้วนำแสงเป็นตัวกลางในการส่งผ่านข้อมูล ข้อได้เปรียบหลักจากการใช้สายใยแก้วนำแสง ได้แก่ ระบบรักษาความปลอดภัย เนื่องจากไม่มีสัญญาณไฟฟ้าระหว่างสายนำสัญญาณกับหัวต่อ เทคโนโลยีไอเอสดีเอ็น (ISDN) เป็นเครือข่ายโทรคมนาคมสาธารณะที่ได้พัฒนาการให้บริการด้านการสื่อสารจากระบบเครือข่ายพีเอสทีเอ็นให้มีประสิทธิภาพมากขึ้น เครือข่ายไอเอสดีเอ็น ให้บริการด้านการสื่อสารข้อมูลแบบต่างๆ เช่น ข้อความ เสียง และภาพ ในรูปแบบสัญญาณทั้งแอนะล็อกและดิจิทัล เทคโนโลยีเฟรมรีเลย์ (Frame Relay) ถูกออกแบบครั้งแรกสำหรับไอเอสดีเอ็นทำให้องค์กรขนาดใหญ่ที่มีสถานที่ตั้งหลายๆ ที่สามารถเชื่อมต่อเข้าด้วยกันเป็นเครือข่ายได้ และเทคโนโลยีเครือข่ายเอทีเอ็ม (Asynchronous Transfer Mode : ATM) เป็นเทคโนโลยีของเครือข่ายซึ่งสามารถใช้ทางด่วน

ข้อมูล (Information Superhighway) ที่สามารถส่งข้อมูลได้มากกว่า เช่น ข้อมูล เสียง รูป สแกน วิดีโอคอนเฟอร์เรนซ์ ทั้งเครือข่ายภายในและภายนอกสามารถรองรับข้อมูลทั้งหมดผ่านวงจรปกติได้

บทที่ 8
ความรู้เบื้องต้นเกี่ยวกับระบบเครือข่ายแบบไร้สาย

ปัจจุบันเทคโนโลยีระบบเครือข่ายคอมพิวเตอร์ได้พัฒนาขึ้นอย่างรวดเร็วและนำไปใช้ร่วมกับการทำงานหลากหลายรูปแบบอย่างแพร่หลาย สำหรับการสื่อสารผ่านระบบเครือข่ายก็มีการนำเทคโนโลยีดังกล่าวมาใช้ในการแลกเปลี่ยนข้อมูล ส่วนใหญ่มักนำมาใช้กับอุปกรณ์สื่อสารหรืออุปกรณ์อิเล็กทรอนิกส์ขนาดเล็ก พกพาสะดวก ทำให้การสื่อสารมีขอบเขตกว้างไกลมากยิ่งขึ้น อีกทั้งสามารถเชื่อมต่อกับเครือข่ายที่ต้องการได้ตลอดเวลา ระบบการเชื่อมต่ออินเทอร์เน็ตสามารถทำได้ 2 รูปแบบ คือ การเชื่อมต่ออินเทอร์เน็ตแบบใช้สาย (Wire Internet) กับการเชื่อมต่ออินเทอร์เน็ตแบบไร้สาย (Wireless Internet)

เครือข่ายแบบไร้สาย (Wireless Network) คือ ระบบเครือข่ายใดๆ ที่เชื่อมต่อหรือแลกเปลี่ยนข้อมูลระหว่างกันโดยไม่ใช้สื่อกลางที่เป็นสายสัญญาณ แต่จะใช้สื่อกลางแบบไร้สายในรูปแบบต่างๆ เช่น คลื่นวิทยุ หรือคลื่นไมโครเวฟ อินฟราเรด และบลูทูธ เป็นต้น วิวัฒนาการของเทคโนโลยีไร้สายเริ่มขึ้นในปี ค.ศ.1896 โดยนำมาใช้ในการสื่อสารครั้งแรกเพื่อการโทรเลข ต่อมาได้มีการพัฒนารูปแบบต่างๆ เช่น การสื่อสารด้วยคลื่นความถี่วิทยุ การติดต่อสื่อสารผ่านดาวเทียม โทรศัพท์ไร้สาย และการแลกเปลี่ยนข้อมูลด้วยบลูทูธ เป็นต้น

8.1 ประเภทของเครือข่ายแบบไร้สาย

เทคโนโลยีของเครือข่ายแบบไร้สายสามารถนำไปใช้ได้ทั้งเครือข่ายขนาดใหญ่และขนาดเล็ก จึงมีการแบ่งประเภทของเครือข่ายแบบไร้สาย ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 274-275)

8.1.1 เครือข่ายแบบไร้สายส่วนบุคคล

เครือข่ายแบบไร้สายส่วนบุคคล (Wireless Personal Area Network : Wireless PAN) เป็นเครือข่ายแบบไร้สายขนาดเล็กแบบส่วนตัว ครอบคลุมพื้นที่ขนาดเล็ก รับส่งข้อมูลจะใช้สื่อไร้สายจำพวกคลื่น เช่น คลื่นวิทยุ และแสงอินฟราเรด มักใช้ในการติดต่อระหว่างอุปกรณ์คอมพิวเตอร์ด้วยกันเอง เช่น เมาส์ จอคอมพิวเตอร์ คีย์บอร์ด แป้นพิมพ์ และเครื่องพิมพ์ เป็นต้น เครือข่ายแบบไร้สายระยะใกล้ที่นิยมใช้ในปัจจุบัน ได้แก่ เทคโนโลยีบูลทูธ (Bluetooth) ซึ่งใช้คลื่นวิทยุรัศมีสั้น (Shot-Range Radio) และ IrDA (Infrared Data Association) ที่ใช้แสง

อินฟราเรดส่งข้อมูล โดยเทคโนโลยีทั้งสองสามารถนำไปใช้ร่วมกับอุปกรณ์อิเล็กทรอนิกส์ต่างๆ เช่น โทรศัพท์มือถือ โน้ตบุ๊ค กล้องดิจิทัล สแกนเนอร์ และหูฟัง เป็นต้น

8.1.2 เครือข่ายแบบไร้สายเฉพาะบริเวณ

เครือข่ายแบบไร้สายเฉพาะบริเวณ (Wireless Local Area Network : Wireless LAN) เป็นเครือข่ายแบบไร้สายที่มีรัศมีในการรับส่งข้อมูลพื้นที่ในขอบเขตที่ไม่กว้างนัก แต่ก็ไม่ใหญ่มากกว่า WPAN นำไปใช้ภายในอาคาร สำนักงาน และบ้านพักอาศัย นอกจากนี้ยังเชื่อมต่อและแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์ได้มากขึ้น Wireless LAN เป็นเครือข่ายแลนที่นำเทคโนโลยีไร้สายมาใช้ในการเชื่อมต่อระหว่างอุปกรณ์ในเครือข่าย โดยใช้การรับส่งข้อมูลด้วยคลื่นวิทยุ อินฟราเรด หรือบูลทูธ

8.1.3 เครือข่ายแบบไร้สายขนาดกลาง

เครือข่ายแบบไร้สายขนาดกลาง (Wireless Metropolitan Area Network : Wireless MAN) เป็นเครือข่ายแบบไร้สายที่มีขนาดใหญ่กว่า Wireless LAN และมีบริเวณการเชื่อมต่อระหว่างเครือข่ายที่กว้างขึ้น ภายในเครือข่ายประกอบด้วยเครือข่ายขนาดเล็กจำนวนมากที่เชื่อมต่อระหว่างกันในระยะไกลด้วยจานรับสัญญาณ ซึ่งอาจใช้สื่อกลางในการส่งข้อมูลด้วยคลื่นวิทยุหรือคลื่นไมโครเวฟ Wireless MAN เป็นมาตรฐานจาก IEEE 802.16 ปัจจุบันรู้จักกันในชื่อ WiMAX (Worldwide Interoperability of Microwave Access) ซึ่งเป็นวิวัฒนาการของเทคโนโลยีไร้สายในยุค 4G และ 5G การพัฒนาของเทคโนโลยีไร้สายนี้ทำให้การสื่อสารและติดต่อทางธุรกิจมีความคล่องตัวและรวดเร็วยิ่งขึ้น

8.1.4 เครือข่ายแบบไร้สายขนาดใหญ่

เครือข่ายแบบไร้สายขนาดใหญ่ (Wireless Wide Area Network : Wireless WAN) เป็นเครือข่ายแบบไร้สายที่มีรัศมีในการรับส่งข้อมูลครอบคลุมพื้นที่ขนาดใหญ่มาก มีบริเวณกว้างเป็นระยะทางหลายกิโลเมตร โดยทั่วไปเครือข่ายประเภทนี้จะเป็นเครือข่ายสาธารณะที่มีทั้งภาครัฐและเอกชนทำหน้าที่เป็นผู้ให้บริการ เช่น เครือข่ายของโทรศัพท์เคลื่อนที่ เครือข่ายวิทยุ เครือข่ายโทรทัศน์ เครือข่ายการส่งข้อมูลผ่านดาวเทียม และ Broadband Wireless เป็นต้น

8.2 ข้อดีและข้อเสียของเครือข่ายแบบไร้สาย

เครือข่ายแบบไร้สายสามารถนำไปใช้งานและอำนวยความสะดวกด้านการติดต่อสื่อสารได้ดี แต่การนำไปใช้งานจำเป็นต้องคำนึงถึงข้อดีและข้อเสียของระบบด้วย เพื่อให้สามารถใช้งานได้อย่างเต็มประสิทธิภาพและตอบสนองต่อความต้องการขององค์กรอย่างสมบูรณ์ ข้อดีหรือข้อเสียของเครือข่ายแบบไร้สาย มีดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 275-277)

ข้อดี

1. เป็นเครือข่ายที่อำนวยความสะดวกต่อผู้ใช้ เครือข่ายแบบไร้สายสามารถช่วยอำนวยความสะดวกแก่ผู้ใช้ได้เป็นอย่างมาก สามารถนำไปใช้งานในสภาพแวดล้อมหรือสถานที่ที่แตกต่างกันได้ดี กล่าวคือ ผู้ใช้สามารถใช้งานได้ทั้งในองค์กรหรือบริษัท และภายในบ้านโดยไม่จำเป็นต้องคำนึงถึงโครงสร้างของเครือข่ายมากเหมือนกับระบบเครือข่ายแบบใช้สายสัญญาณ ทำให้สามารถติดต่อและแลกเปลี่ยนข้อมูลโดยไม่ต้องกังวลในเรื่องของสถานที่และเวลาที่ใช้ในการติดตั้ง

2. เพิ่มความคล่องตัวในการทำงาน เครือข่ายแบบไร้สายผู้ใช้ไม่จำเป็นต้องเชื่อมต่ออุปกรณ์ต่างๆ โดยตรงหรือผ่านสื่อกลางประเภทสายสัญญาณ ทำให้การย้ายอุปกรณ์ไม่ก่อให้เกิดปัญหาในการสื่อสาร ผู้ใช้สามารถแลกเปลี่ยนข้อมูลภายในเครือข่ายได้ทุกบริเวณที่มีสัญญาณครอบคลุมอยู่ ผู้ใช้สามารถเคลื่อนที่ไปพร้อมกับทำงานหรือติดต่อสื่อสารได้ โดยที่สัญญาณและข้อมูลไม่สูญหายไประหว่างการขนส่ง

3. การติดตั้งง่ายและรวดเร็ว เนื่องจากเป็นเครือข่ายที่ไม่ต้องอาศัยสื่อกลางประเภทสายสัญญาณ ทำให้การเชื่อมโยงระหว่างอุปกรณ์ของผู้ใช้กับอุปกรณ์การเชื่อมต่อต่างๆ ภายในเครือข่ายทำได้ง่ายและรวดเร็ว

4. การขยายเครือข่ายทำได้ง่าย การขยายเครือข่ายแบบใช้สายจำเป็นต้องเพิ่มจุดเชื่อมต่อสายสัญญาณ ถ้าหากระบบเครือข่ายดังกล่าวไม่ได้ถูกออกแบบเพื่อรองรับการขยายไว้ล่วงหน้า อาจจะต้องเสียเวลาและค่าใช้จ่ายเพิ่ม แต่เครือข่ายนี้สามารถติดตั้งอุปกรณ์ต่างๆ ได้ง่าย เพราะมีความยืดหยุ่นและคล่องตัวในการใช้งานสูง

5. ลดค่าใช้จ่ายโดยรวมในระยะยาว การติดตั้งเครือข่ายแบบไร้สายใช้งบประมาณค่อนข้างสูงทำให้ไม่เหมาะกับองค์กรขนาดเล็ก แต่มีความคุ้มทุนในระยะยาวดีกว่าเครือข่ายแบบสายสัญญาณ เนื่องจากมีข้อได้เปรียบในเรื่องของความยืดหยุ่นของเครือข่ายที่มีมากกว่า หากในอนาคตมีการเปลี่ยนแปลงเกิดขึ้น

ข้อเสีย

1. ความปลอดภัยของข้อมูล เนื่องจากการติดต่อสื่อสารระหว่างอุปกรณ์ภายในเครือข่ายแบบไร้สายสามารถทำได้ทุกๆ บริเวณที่มีสัญญาณครอบคลุมอยู่ ทำให้ผู้ไม่หวังดีสามารถเข้ามาในระบบ เพื่อดักจับข้อมูล และขโมยข้อมูลได้ง่าย โดยไม่สามารถตรวจสอบตำแหน่งของผู้บุกรุกได้อย่างชัดเจน

2. ความน่าเชื่อถือ เนื่องจากเครือข่ายแบบไร้สายเป็นระบบที่มีการรักษาความปลอดภัยได้ยาก ทำให้ข้อมูลที่รับส่งภายในเครือข่ายแบบไร้สายมีความน่าเชื่อถือน้อยกว่าเครือข่ายแบบใช้สาย และการรับส่งข้อมูลต้องอาศัยคลื่นวิทยุ จึงต้องระมัดระวังสัญญาณคลื่นวิทยุอื่นๆ ที่อาจเข้ามารบกวนเครือข่าย ส่งผลให้ปลายทางได้รับข้อมูลที่ไม่ถูกต้อง

3. ระยะทางในการติดต่อสื่อสาร เนื่องจากระบบเครือข่ายแบบไร้สายเป็นการส่งข้อมูลด้วยสัญญาณคลื่นวิทยุ จึงมีข้อจำกัดในเรื่องของบริเวณและระยะเวลาในการส่งข้อมูล ผู้ใช้ที่อยู่ห่างจากจุดกำเนิดสัญญาณอาจย่อมได้รับสัญญาณที่ไม่สม่ำเสมอ หากต้องการให้เครือข่ายแบบไร้สายมีระยะทางในการติดต่อระหว่างผู้ใช้เพิ่มขึ้น จำเป็นต้องเพิ่มอุปกรณ์ทวนสัญญาณหรือเพิ่มจุดในการติดตั้งเชื่อมต่อกับเครือข่ายแบบไร้สายให้มีจำนวนมากขึ้น

4. ความเร็วในการส่งข้อมูล เครือข่ายแบบไร้สายสามารถส่งข้อมูลด้วยความเร็วในช่วง 1-54 Mbps ส่วนเครือข่ายแบบใช้สายมีความเร็วในการส่งข้อมูลอยู่ในในช่วงตั้งแต่ 100 Mbps จนถึงระดับ Gbps ทำให้ความเร็วในการแสดงข้อมูลแตกต่างกันมาก หากเป็นการใช้งานในองค์กรขนาดใหญ่ที่ต้องการความเร็วในการส่งข้อมูลสูงควรเลือกใช้เครือข่ายแบบไร้สาย

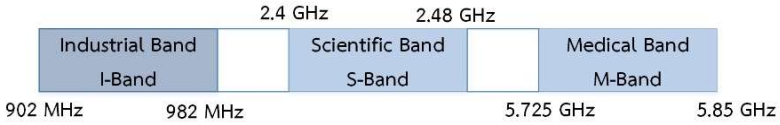
5. ค่าใช้จ่ายในการติดตั้ง ปัจจุบันอุปกรณ์ของเครือข่ายแบบไร้สายไม่ว่าจะเป็น Access Point และ Wireless Interface Card มีราคาค่อนข้างสูง ดังนั้น ค่าใช้จ่ายสำหรับการติดตั้งระบบเครือข่ายแบบไร้สายครั้งแรกจะมีราคาสูง แต่ในอนาคตของอุปกรณ์เหล่านี้มีแนวโน้มลดลง เนื่องจากการแข่งขันของบริษัทผู้ผลิตอุปกรณ์

8.3 การส่งข้อมูลของระบบเครือข่ายแบบไร้สาย

การส่งข้อมูลของระบบเครือข่ายแบบไร้สาย (Wireless Network Transmission) สามารถแบ่งได้ 2 วิธี คือ การส่งข้อมูลด้วยคลื่นวิทยุและการส่งข้อมูลด้วยอินฟราเรด โดยมีรายละเอียด ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 278-279)

8.3.1 การส่งข้อมูลด้วยคลื่นวิทยุ (Radio Frequency Transmission)

คลื่นวิทยุมีความถี่ตั้งแต่ 1-20 GHz ต่อมา องค์กร FCC ของประเทศสหรัฐอเมริกาได้กำหนด ISM Bands ขึ้นมาเพื่อกำหนดช่วงความถี่สาธารณะของคลื่นวิทยุให้ใช้งานด้านอุตสาหกรรม วิทยาศาสตร์ และการแพทย์ โดยมีช่วงความถี่ระหว่าง 902 MHz ถึง 5.8 GHz ดังภาพที่ 8.1



ภาพที่ 8.1 ความถี่ของการคลื่นวิทยุ ISM Bands

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 278)

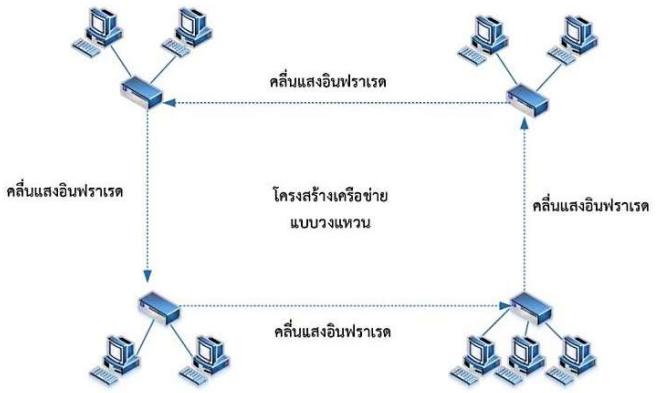
ประเทศต่างๆ จะมีการกำหนดขึ้นความถี่สาธารณะแตกต่างกันไป สำหรับคลื่นความถี่ 2.4 GHz เป็นคลื่นสาธารณะที่อนุญาตให้ใช้ได้ทั่วโลก

8.3.2 การส่งข้อมูลด้วยอินฟราเรด (Infrared)

อินฟราเรดเป็นคลื่นแสงชนิดหนึ่งที่มองไม่เห็น เนื่องจากมีความยาวคลื่นต่ำกว่าคลื่นแสงปกติที่มนุษย์สามารถมองเห็นได้ สามารถนำมาใช้งานในด้านระบบเครือข่ายได้ เช่น ใช้รับส่งข้อมูลในระยะใกล้ มีการรับส่งข้อมูลภายในห้องเดียวเท่านั้นในระยะทางไม่เกิน 2 เมตร และมีความเร็วประมาณ 4 Mbps การทำงานของอินฟราเรดที่ใช้ในอุปกรณ์ทั่วไปส่วนใหญ่จะเป็นการทำงานระหว่าง 2 อุปกรณ์ มากกว่าการใช้งานเป็นระบบเครือข่าย สามารถแบ่งการทำงานของอินฟราเรดได้ 2 ลักษณะ ดังนี้

1. Point-to-Point

เป็นการเชื่อมต่อระหว่างอุปกรณ์ที่สื่อสารกันด้วยอินฟราเรดแบบ Point-to-Point เชื่อมโยงกันเป็นเครือข่ายแบบวงแหวน การทำงานของอินฟราเรดในลักษณะนี้นิยมใช้ตั้งเป็นระบบเครือข่าย Token Ring แบบไร้สาย โดยอุปกรณ์ที่รับส่งคลื่นอินฟราเรดจะต้องอยู่ภายใต้รัศมีความกว้างของคลื่นอินฟราเรด หรือที่เรียกว่า Line of Sight ดังภาพที่ 8.2

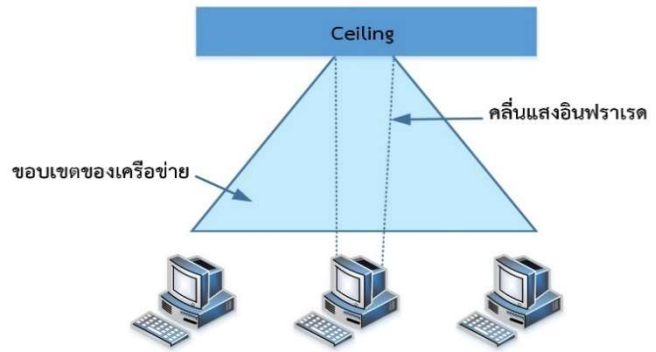


ภาพที่ 8.2 เครือข่าย Token Ring แบบไร้สายโดยใช้คลื่นแสงอินฟราเรด

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 280)

2. Diffused LAN

เป็นการเชื่อมต่อโดยใช้เครือข่ายสะท้อนของคลื่นอินฟราเรดกับวัตถุ วัตถุที่ทำหน้าที่ในการสะท้อนคลื่นอินฟราเรดเรียกว่า Ceiling โดยเครือข่ายลักษณะนี้เครื่องที่อยู่ภายในระยะหรือความกว้างของคลื่นอินฟราเรดจะได้รับสัญญาณทุกเครื่อง เมื่อเครื่องส่งสัญญาณไปกระทบที่ Ceiling แล้ว คลื่นสัญญาณดังกล่าวก็จะถูกส่งไปยังเครื่องอื่นๆ ที่อยู่ภายในเครือข่ายที่จัดตั้ง ดังภาพที่ 8.3



ภาพที่ 8.3 เครือข่าย Diffused LAN

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 281)

8.4 เทคโนโลยีเครือข่ายแบบไร้สาย

8.4.1 บลูทูธ (Bluetooth)

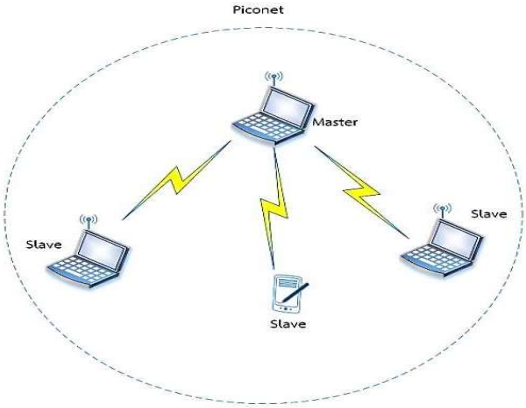
บลูทูธ (Bluetooth) เป็นเทคโนโลยีไร้สายอีกรูปแบบหนึ่งที่เป็นต้นแบบของมาตรฐาน IEEE 802 2.15 (Wireless Personal Area Network) ซึ่งเป็นเครือข่ายไร้สายระยะใกล้ที่ใช้คลื่นวิทยุความถี่ 2.4 GHz ในการรับส่งข้อมูลและใช้เทคนิค FHSS เข้ามาช่วยในการส่งข้อมูล โดยมีอัตราเร็วในการส่งข้อมูล ตั้งแต่ 720 Mbps แต่ไม่เกิน 1 Kbps ภายในระยะทางไม่เกิน 10 เมตร เทคโนโลยีนี้ได้ถูกพัฒนาและนำไปประยุกต์ใช้กับอุปกรณ์สื่อสารขนาดเล็กหรืออุปกรณ์อิเล็กทรอนิกส์เพื่อความสะดวกในการใช้งาน ปัจจุบันมีอุปกรณ์หลายชนิดที่รองรับเทคโนโลยีบลูทูธ เช่น Pocket PC, โทรศัพท์มือถือ หูฟัง คอมพิวเตอร์โน้ตบุ๊ค เครื่องพิมพ์ และเมาส์ ดังภาพที่ 8.4 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 281-284)

ภาพที่ 8.4 ตัวอย่างอุปกรณ์ที่ใช้บลูทูธในการรับส่งข้อมูล

ลักษณะเครือข่ายบลูทูธ (Bluetooth)

บลูทูธ มีสถาปัตยกรรมเป็น Master-Slave Architecture ซึ่งสามารถแบ่งเครือข่ายตามลักษณะการทำงานได้ 2 ชนิดคือ

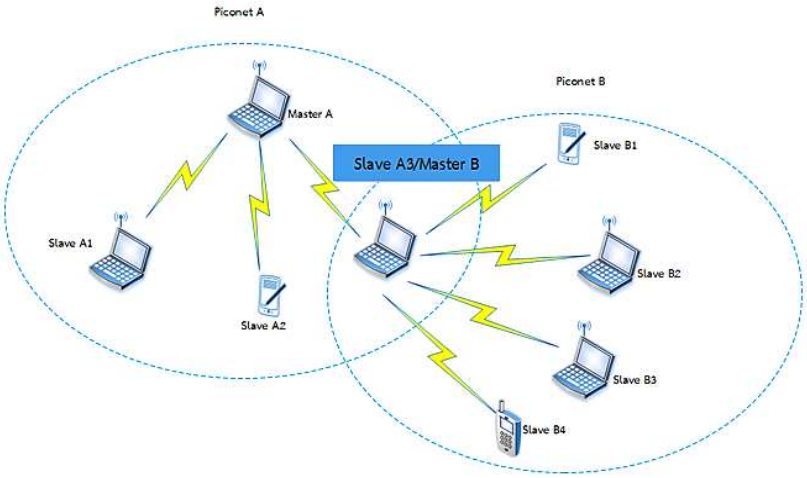
1. Piconet เป็นเครือข่ายบลูทูธที่มีขนาดเล็ก มีเครื่องภายในเครือข่ายได้ทั้งหมดไม่เกิน 8 เครื่อง โดย 1 เครื่องในเครือข่ายจะทำหน้าที่เป็นเครื่องแม่ข่าย (Master) ส่วนที่เหลือเป็นเครื่องลูกข่าย (Slave) การเชื่อมต่อระหว่าง Master กับ Slave สามารถทำได้ทั้งแบบหนึ่งเครื่องต่อหนึ่งเครื่อง (one-to-one) หรือแบบหนึ่งเครื่องต่อหลายเครื่อง (one-to-many) ดังภาพที่ 8.5



ภาพที่ 8.5 เครือข่าย Piconet

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 283)

2. Scatternet เป็นเครือข่ายบลูทูธที่เกิดจากการขยายเครือข่ายของ Piconet ระบบเครือข่ายของ Scatternet จะใช้เครื่องหนึ่งที่ทำหน้าที่เป็น Slave ของ Piconet ในขณะเดียวกันก็ทำหน้าที่เป็นเครื่อง Master ของอีก Piconet ด้วย ทำให้เครื่องดังกล่าวสามารถรับข้อมูลจากเครื่อง Master ของเครือข่ายตนและส่งข้อมูลดังกล่าวต่อไปยังเครื่อง Slave ในอีก Piconet ที่เครื่องนั้นทำหน้าที่เป็น Master นั่นเอง ดังภาพที่ 8.6



ภาพที่ 8.6 เครือข่าย Scatternet

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 283)

ประเภทของบลูทูธ

บลูทูธแบ่งออกเป็น 2 กลุ่มหลัก คือ (ชัชชัย คุณบัว, 2562, หน้า 91-99)

1. บลูทูธคลาสสิก ได้แก่ กลุ่มของบลูทูธตั้งแต่เวอร์ชัน 1 ถึง เวอร์ชัน 3 เน้นเพื่อการเชื่อมต่อระหว่างอุปกรณ์รอบข้าง และการส่งข้อมูลที่อัตราเร็วที่สูงขึ้น เช่น ในเวอร์ชัน 2 ได้มีการเพิ่มการสื่อสารข้อมูลที่เรียกว่า Enhanced DataRate (EDR) เพื่อให้สามารถส่งข้อมูลที่ความเร็ว 3 Mbps จากนั้นในเวอร์ชัน 3 ได้ปรับปรุงให้สามารถส่งข้อมูลสูงถึง 24 Mbps โดยทำงานร่วมกับการสื่อสารบนการเชื่อมต่อกับมาตรฐาน IEEE 802.1145

2. บลูทูธพลังงานต่ำ (Bluetooth Low Energy: BLE) ได้แก่ กลุ่มของบลูทูธตั้งแต่เวอร์ชัน 4.0 เพื่อให้สามารถทำงานด้วยแบตเตอรี่ขนาดเล็ก ด้วยเทคโนโลยี IoT ทำให้บลูทูธมีการปรับปรุงเป็นเวอร์ชัน 4.1 จนกระทั่งปัจจุบันอยู่ระหว่างการพัฒนาการสื่อสารในรูปแบบเมช (Mesh) ในเวอร์ชัน 5 มีรายละเอียด ดังนี้

2.1 Bluetooth 4.0 เป็นเวอร์ชันแรกของบลูทูธพลังงานต่ำกำหนดขึ้นโดยองค์กร BluetoothSpecial Interest Group (SIG) เพื่อรองรับอุปกรณ์พกพาต่างๆ เช่น นาฬิกาอัจฉริยะ (Smart Watch) บลูทูธ 4.0 มีคุณสมบัติ ดังนี้

2.2.1 การมีชั้นของโปรโตคอล (Protocol Stack) ที่ไม่ซับซ้อน Lightweight)

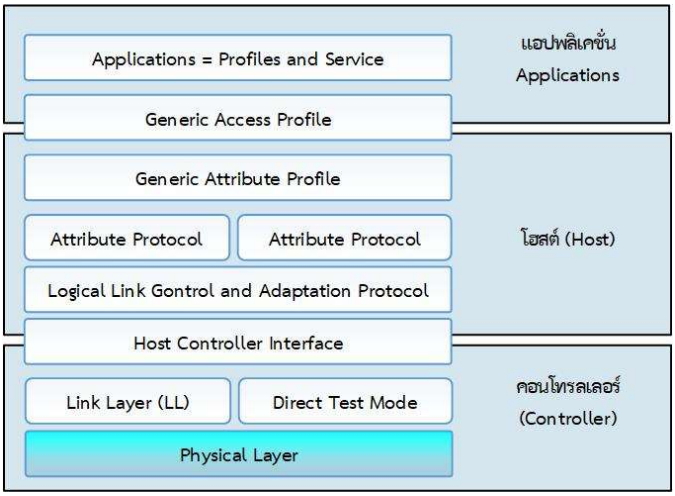
2.2.2 สามารถทำงานร่วมกับบลูทูธตั้งแต่เวอร์ชัน 4.0 ขึ้นไป

2.2.3 สามารถส่งข้อมูลได้ที่ความเร็ว 1 Mbps

2.2.4 ระยะทางการส่งประมาณ 10 เมตร

2.2.5 รองรับการรบกวนจากอุปกรณ์สื่อสารที่ใช้ช่อง 2.4 GHz

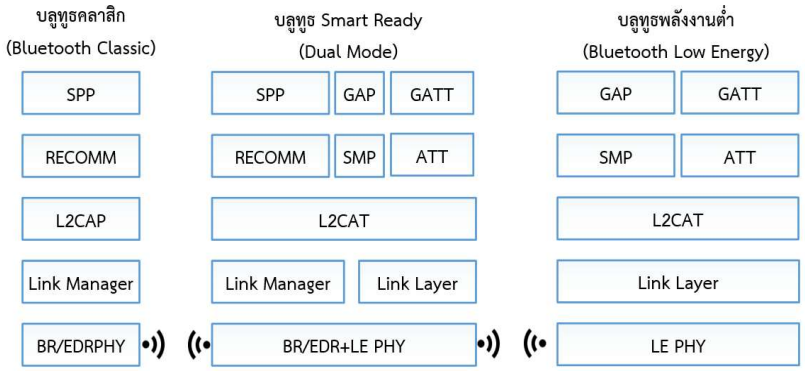
เพื่อให้ชั้นของโพรโทคอลบลูทูธ 4.0 ไม่ซับซ้อนมาก จึงมีการแบ่งชั้นโพรโทคอลออกเป็น 2 ส่วนหลัก โดยส่วนแรกเป็นส่วนของคอนโทรลเลอร์ (Controller) เพื่อรองรับการทำงานเกี่ยวกับการใช้งานช่องสัญญาณ การกำหนดรูปแบบของแพ็กเก็ต และส่วนที่สองเป็นส่วนของโฮสต์ (Host) เพื่อรองรับการทำงานด้านต่างๆ ที่เกี่ยวข้องกับการจัดการการเชื่อมต่อและแอปพลิเคชัน การแบ่งข้อมูลออกเป็นส่วนๆ (Fragmentation) การรวมข้อมูล (De-fragmentation) และการทำมัลติเพล็กซิ่ง รวมไปถึงด้านความปลอดภัย (Security) ดังภาพที่ 8.7



ภาพที่ 8.7 เลเยอร์ของโพรโทคอลของบลูทูธพลังงานต่ำ

ที่มา : (ชัชชัย คุณบัว, 2562, หน้า 96)

เพื่อให้บลูทูธ 4.0 สามารถทำงานร่วมกับบลูทูธเวอร์ชันก่อนหน้าได้ จึงมีการพัฒนา Chip) ขึ้นเพื่อรองรับบลูทูธ 4.0 เป็น 2 รูปแบบ คือ บลูทูธที่มีเลเยอร์ของโพรโทคอลที่ 5.4 เป็นการทำงานแบบ Single Mode และ บลูทูธที่แก้ไขชั้นของโพรโทคอลพร้อมทั้งเพิ่มส่วนของ Basic Rate (BR)/Enhanced Data Rate (EDR) ที่มีในเวอร์ชันก่อนทำให้บลูทูธในแบบที่สองนี้ สามารถรองรับการทำงานร่วมกับบลูทูธคลาสสิก เป็นการแบบดูอัลโหมด (Dual Mode) ดังภาพที่ 8.8



ภาพที่ 8.8 การเปรียบเทียบเลเยอร์ของโปรโตคอลของบลูทูธทั้ง 3 ประเภท

ที่มา : (ชัชชัย คุณบัว, 2562, หน้า 97)

2.2 Bluetooth 4.1

เพื่อให้รองรับการทำงานกับ IoT ทำให้บลูทูธ 4.1 สามารถทำงานเป็นอุปกรณ์ต่อพ่วง (Peripheral) และฮับ (Hub) ได้ในเวลาเดียวกัน เช่น อุปกรณ์นาฬิกาอัจฉริยะ (SmartFlatch) สามารถทำหน้าที่เสมือนฮับเพื่อรองรับข้อมูลจากอุปกรณ์วัดการเต้นของหัวใจ พร้อมซึ่งเป็นอุปกรณ์ต่อพ่วง (Peripheral) กับมือถือเพื่อแสดงข้อความต่างๆ จากอุปกรณ์ชนิดอื่นนอกจากนี้บลูทูธ 4.1 ยังสามารถกำหนดการใช้ช่องสัญญาณได้ ทำให้สามารถทำงานร่วมกับโปรโตคอล IPv6

2.3 Bluetooth 4.2

บลูทูธ 4.2 ได้เพิ่มระดับความปลอดภัยให้สูงขึ้น โดยใช้การเข้ารหัสแบบเส้นโค้งซึ่งวงรี (Elliptic Curve Cryptography) และใช้ Advanced Encryption Standard-Counter with CBC-MAC (AES-CCM) เพื่อเข้ารหัสข้อความที่ส่ง ทำให้สามารถป้องกันการดักฟัง (Eavesdropping) และป้องกันการโจมตีแบบ Man in The Middle (MITM) ระหว่างอุปกรณ์บนลิงก์เลเยอร์ให้มีความปลอดภัยมากขึ้น

2.4 Bluetooth 5 เพิ่มระยะและแบนด์วิดท์

บลูทูธ 5 เป็นเวอร์ชั่นล่าสุด ซึ่งได้เพิ่มส่วนสำคัญสองส่วน คือ การเพิ่มระยะการสื่อสารและแบนด์วิดท์เป็น 2 เมกะบิตต่อวินาที การเพิ่มแบนด์วิดท์ที่สูงขึ้นทำให้อุปกรณ์ IoT สามารถอัปเดตแบบ Over-The-Air (OTA) ได้อย่างรวดเร็วมากขึ้น ซึ่งโดยทั่วไปแล้วอุปกรณ์ IoT จะประกอบไปด้วยเซ็นเซอร์ต่างๆ และบ่อยครั้งจำเป็นต้องมีการเพิ่มจำนวนเซ็นเซอร์ให้มากขึ้น ทำให้ต้องมีการปรับเปลี่ยนฟังก์ชันและความปลอดภัยที่สูงขึ้นการทำ OTA ทำให้เกิดความรวดเร็วในการ อัปเดต นอกเหนือจากนี้การเพิ่มความเร็วเป็น 2 เมกะบิตต่อวินาที ทำให้การสื่อสารใช้เวลาน้อยลงในการส่งข้อมูลขนาดเท่ากัน ซึ่งจะส่งผลให้อุปกรณ์สามารถเข้าสู่โหมดสลีป (Sleep Mode) ได้มากขึ้น และลดการใช้พลังงานลง

นอกจากนั้นบลูทูธ 5 ยังมีการเพิ่มระยะทางการสื่อสารเป็น 4 เท่าจากบลูทูธ 4.2 ทำให้การสื่อสารของบ้านอัจฉริยะ (Smart Home) สามารถสื่อสารแบบสตาร์ (Star) ผ่านไปยังฮับได้โดยตรง ทำให้ไม่จำเป็นต้องใช้การสื่อสารแบบเมช (Mesh) และมีการใช้ Forward Error Correction (FEC) เพื่อให้ภาครับสามารถตรวจสอบและแก้ไขความผิดพลาดที่อาจเกิดขึ้นโดยไม่จำเป็นต้องมีการส่งใหม่ และบลูทูธ 5 ยังได้ขยายส่วนบรรจุข้อมูลของแอดเวอร์ไทซิ่ง (Advertising) จากเดิม 27 ไบต์เป็น 251 ไบต์เพื่อให้การส่งข้อมูลในเบคอน (Beacon) ได้มากขึ้น

จากที่กล่าวมาข้างต้น ทำให้สามารถสรุปความแตกต่างของบลูทูธเวอร์ชันต่างๆ ได้ในตารางที่ 8.1

ตารางที่ 8.1 เปรียบเทียบความแตกต่างของบลูทูธ

Feature	บลูทูธคลาสสิก	บลูทูธ 4.x	บลูทูธ 5
ระยะการสื่อสาร	ประมาณ 100	ประมาณ 100	ประมาณ 200
การใช้งานช่องสัญญาณ	ฟรีเควนซีฮอปปิ้ง	ฟรีเควนซีฮอปปิ้ง	ฟรีเควนซีฮอปปิ้ง
อัตราการส่งข้อมูล (Mbps)	1-3	1	2
ความหน่วง (ms)	< 100	<6	<3
เน็ตเวิร์กโทโพโลยี	Piconet, scatternet	Star-bus, Mesh	Star-bus, Mesh
การสื่อสารมากกว่า 1 ฮอป	Scatternet	Yes	Yes
โปรไฟล์	Yes	Yes	Yes
จำนวนโหนดหรือสลาฟ	7	Unlimited	Unlimited
ขนาดของเมสเสจ (ไบต์)	Up to 358	31	255

ที่มา : (ชัชชัย คุณบัว, 2562, หน้า 99)

8.4.2 Wireless LAN

Wireless LAN เป็นเครือข่ายแบบไร้สายเฉพาะบริเวณ ซึ่งเป็นแลนประเภทหนึ่งที่ใช้คลื่นวิทยุหรืออินฟราเรดเป็นสื่อกลางในการรับส่งข้อมูล มาตรฐานของ Wireless LAN เรียกว่า IEEE 802.11 ในช่วงเริ่มต้นมีอัตราเร็วในการส่งข้อมูลเพียง 2 Mbps แต่ในปัจจุบันตามมาตรฐาน IEEE 802.11g ในย่านความถี่ 2.4 GHz และ IEEE 802.11a ในย่านความถี่ 5 GHz มีอัตราเร็วในการส่งข้อมูลถึง 54 Mbps ต่อมาได้มีการพัฒนาอัตราความเร็วให้เพิ่มขึ้น โดยทางสถาบัน IEEE ได้พัฒนามาตรฐานใหม่ คือ 802.11ax มาตรฐาน Wi-Fi ที่หลายฝ่ายคาดว่าจะเป็นมาตรฐานถัดจาก 802.11ac คือ 802.11ax ที่จะให้บริการความเร็วสูงกว่า 2 Gbps ในการรับส่งข้อมูล (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 284)

องค์ประกอบของ Wireless LAN

องค์ประกอบที่สำคัญของ Wireless LAN มี 2 ส่วน ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 284-293)

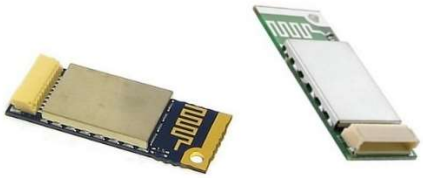
1. Access Point

เป็นอุปกรณ์ที่ใช้เป็นตัวกลางในการรับและส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ที่ติดตั้งการ์ดเครือข่ายแบบไร้สายให้สามารถติดต่อสื่อสารกันได้ ลักษณะการทำงานจะทำหน้าที่เหมือนฮับที่ใช้กับระบบเครือข่ายทั่วไป โดยเป็นตัวเชื่อมโยงระหว่างเครื่องคอมพิวเตอร์กับเครือข่ายแบบไร้สาย เพื่อให้อุปกรณ์สามารถสื่อสารแลกเปลี่ยนข้อมูลกันได้ ลักษณะของอุปกรณ์ชนิดนี้จะมีทั้งแบบที่มีเสาอากาศและแบบที่ซ่อนเสาอากาศไว้ โดยเสาอากาศสามารถปรับเปลี่ยนหรือขยายกำลังของคลื่นให้ครอบคลุมพื้นที่ให้มากขึ้นได้ด้วย สามารถรองรับอุปกรณ์ที่เข้ามาเชื่อมต่อภายในเครือข่ายแบบไร้สายได้ ตั้งแต่ 16-128 เครื่อง Access Point จะมีพอร์ต RJ-45 สำหรับใช้เชื่อมโยงเข้ากับเครื่องใช้สายแบบเดิมที่มีอยู่ได้ ตัวอย่างของ Access Point แสดงดังภาพที่ 8.9

ภาพที่ 8.9 ตัวอย่าง Access Point

2. Wireless Network Interface Card (Wireless NIC)

เป็น NIC ที่ใช้สำหรับเครือข่ายแบบไร้สายโดยเฉพาะ มีหน้าที่เหมือนกับ NIC ที่ใช้ในเครือข่ายแลน คือ ควบคุมการรับส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์ แต่จะใช้วิธีการส่งข้อมูลแบบไร้สาย โดยจะแปลงข้อมูลดิจิทัลจากเครื่องผู้ใช้ไปเป็นคลื่นวิทยุเพื่อส่งไปยังปลายทางโดยใช้อากาศเป็นสื่อกลางในการส่งข้อมูลในลักษณะกระจาย เมื่อได้รับคลื่นวิทยุจะทำหน้าที่แปลงกลับให้เป็นข้อมูลดิจิทัล ลักษณะ Wireless NIC มีหลายรูปแบบ เช่น PCI, PCMCIA และ USB เป็นต้น โดย Wireless NIC แต่ละแบบจะมีความสะดวกในการใช้งานแตกต่างกันขึ้นอยู่กับความต้องการของผู้ใช้ ตัวอย่างการ์ดไร้สาย ดังภาพที่ 8.10



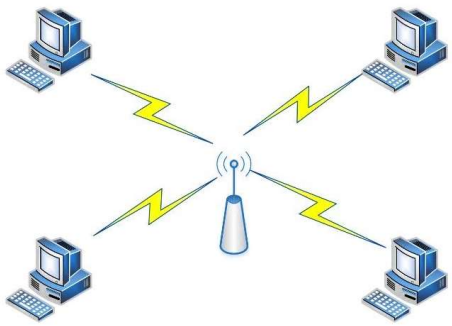
ภาพที่ 8.10 ตัวอย่าง Wireless Network Interface Card

ลักษณะการทำงานของ Wireless LAN

ลักษณะการทำงานของ Wireless LAN มี 2 รูปแบบ ดังนี้

1. แบบติดต่อผ่าน Access Point

Access Point เปรียบเสมือนฮับหรือสวิตซ์ที่ทำหน้าที่กระจายสัญญาณไปยังอุปกรณ์รับส่งสัญญาณในเครือข่าย โดยมีโครงสร้างการเชื่อมต่อระหว่างอุปกรณ์เป็นแบบ Client/Server และมี Access Point เป็นสื่อกลางในการรับส่งสัญญาณระหว่าง Server และ Client โดย Access Point มีการเชื่อมโยงกับ Access Point ตัวอื่นหรือเชื่อมโยงกับเครือข่ายแลนก็ได้ นอกจากนี้ยัง Access Point ยังสามารถเป็นศูนย์กลางในการควบคุมอุปกรณ์ของเครือข่าย Wireless LAN ได้อีกด้วย ดังภาพที่ 8.11

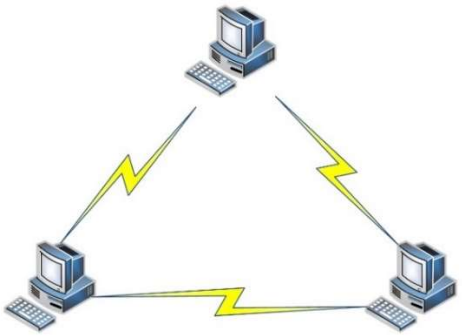


ภาพที่ 8.11 ลักษณะการทำงานของ Wireless LAN แบบติดต่อผ่าน Access Point
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 286)

2. แบบ Ad-hoc Networking

คอมพิวเตอร์สามารถส่งข้อมูลมาหากันได้โดยตรงไม่ต้องอาศัย Access Point และมีโครงสร้างการเชื่อมต่อแบบ Peer-to-Peer ซึ่งเป็นการติดต่อสื่อสารระหว่างเครือข่ายคอมพิวเตอร์ที่ไม่ต้องมีศูนย์กลางทำหน้าที่ควบคุมและจัดการกับการติดต่อสื่อสาร

ลักษณะของการทำงานของ Ad-hoc นั้น เครื่องคอมพิวเตอร์จะเชื่อมต่อระหว่างการเป็นเครือข่ายขนาดเล็ก และใช้วิธีการแพร่กระจายสัญญาณข้อมูลผ่านทางอากาศโดยไม่ต้องทราบว่าปลายทางอยู่ในตำแหน่งใด เพียงแต่เครื่องปลายทางจะต้องอยู่ภายในขอบเขตรัศมีที่สามารถทำการติดต่อสื่อสารกันได้ ดังภาพที่ 8.12



ภาพที่ 8.12 ลักษณะการทำงานของ Wireless LAN แบบ Ad-hoc Networking
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 286)

การควบคุมการส่งข้อมูลของ Wireless LAN

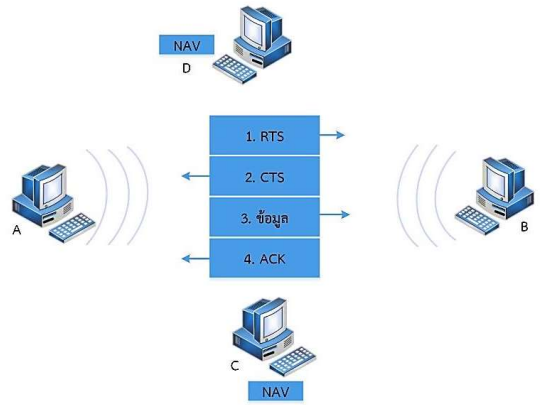
การควบคุมการส่งข้อมูลผ่าน Wireless LAN มี 2 ลักษณะ ดังนี้

1. Distributed Coordination Function (DCF)

การควบคุมการส่งข้อมูลผ่าน Wireless LAN แบบ DCF ใช้หลักการ CSMA/CA ในการควบคุมข้อมูล ซึ่งมี 2 วิธี ดังนี้

1.1 การใช้ Physical Carrier Sense เมื่อสถานีใดต้องการส่งข้อมูล จะตรวจสอบว่าคลื่นว่างหรือไม่ ถ้าว่างก็จะส่งข้อมูล ถ้าไม่ว่างจะต้องรอ ในกรณีที่มีข้อมูลชนกันสถานีที่ส่งข้อมูลไปทีหลังจะต้องรอแล้วค่อยส่งข้อมูลใหม่

1.2 การใช้ MACAW (Multiple Access with Collision Avoidance for Wireless) ร่วมกับ Virtual Carrier Sense ปัญหาที่สำคัญของ Physical Carrier Sense คือ คอมพิวเตอร์อาจตรวจสอบไม่ได้ว่ามีการส่งข้อมูลอยู่ เนื่องจากรัศมีของคลื่นที่ส่งข้อมูลไม่ครอบคลุมคอมพิวเตอร์ทุกเครื่อง ดังนั้น ข้อมูลอาจเกิดการชนกันได้ เรียกปัญหานี้ว่า Hidden Node Problem ซึ่งสามารถแก้ไขได้ด้วยการใช้ MACAW ร่วมกับ Virtual Carrier Sense โดยมีหลักการทำงาน ดังภาพที่ 8.13



ภาพที่ 8.13 การควบคุมการส่งข้อมูลแบบ DCF โดยใช้หลักการ MACAW และ Virtual Carrie Sense
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 287)

จากภาพที่ 8.13 จะเห็นว่า A ต้องการส่งข้อมูลให้ B โดยมีขั้นตอน ดังนี้

ขั้นที่ 1 A ส่ง RTS (Request To Send) ประกอบด้วยที่อยู่ของ B และความยาวของข้อมูลที่ต้องการส่งไปยัง B โดยทุกสถานีอยู่ในรัศมีของ A จะได้รับ RTS ที่ถูกกระจายสัญญาณมาจาก A และกำหนดให้หยุดส่งข้อมูลตามระยะเวลาที่ระบุใน CTS (Clear To Send)

ขั้นที่ 2 B ตรวจสอบว่ามีการส่งข้อมูลหรือไม่ ถ้าสัญญาณว่าง ก็จะส่ง CTS (Clear To Send) ซึ่งประกอบด้วยความยาวของข้อมูลที่ A ต้องการส่ง (คัดลอกจาก RTS) ให้กับ A โดยทุกสถานีที่อยู่ในรัศมีของ B จะได้รับ CTS ที่ถูกกระจายสัญญาณมาจาก B และจะกำหนดให้หยุดส่งข้อมูลตามระยะเวลาที่ระบุใน CTS ซึ่งค่าระยะเวลาที่กำหนดนั้นเรียกว่า NAV (Network Allocation Vector) โดยเครื่องอื่นๆ จะส่งข้อมูลได้ก็ต่อเมื่อระยะเวลาตามค่า NAV สิ้นสุดลง

ขั้นที่ 3 A จะส่งข้อมูลให้ B

ขั้นที่ 4 เมื่อ B ได้รับข้อมูลเรียบร้อยแล้วจะส่ง ACK (Acknowledge) กลับไปยัง A เพื่อแจ้งว่าได้รับข้อมูลเรียบร้อยแล้ว

2. Point Coordination Function (PCF)

เป็นเทคนิคที่ใช้วิธีการ Polling กล่าวคือ จะใช้ Access Point เป็นศูนย์กลางในการควบคุมการส่งข้อมูล โดย Access Point จะมีหน้าที่ในการสอบถามสถานีต่างๆ

ที่อยู่ภายในรัศมีว่าต้องการข้อมูลหรือไม่ วิธีนี้จะช่วยหลีกเลี่ยงไม่ให้ข้อมูลชนกัน เนื่องจาก Access Point เป็นผู้ดูแลการส่งข้อมูลทั้งหมดนั่นเอง

มาตรฐาน Wireless LAN

มาตรฐาน Wireless LAN คือ IEEE 802.11 ซึ่งมีหลายรุ่น ในที่นี้จะกล่าวถึงมาตรฐานต่างๆ ที่สำคัญของ Wireless LAN ดังนี้

1. IEEE 802.11a เป็นมาตรฐานที่เริ่มนำมาใช้ในปี ค.ศ. 1999 ซึ่งใช้เทคนิคในการส่งข้อมูลแบบ OFDM (Orthogonal Frequency Division Multiplexing) ที่สามารถรับส่งข้อมูลได้ด้วยความเร็วสูงสุด 50 Mbps โดยใช้คลื่นวิทยุที่ความถี่ 5 GHz ซึ่งเป็นความถี่สาธารณะสำหรับใช้งานในประเทศสหรัฐอเมริกา แต่เป็นความถี่ที่ไม่ได้รับอนุญาตให้ใช้งานได้อย่างอิสระในประเทศไทยเนื่องจากเป็นความถี่สำหรับกิจการทางดาวเทียม ข้อเสียของ IEEE 802 .11a คือ อุปกรณ์มีราคาแพง และรัศมีการใช้งานมีระยะแคบ คือ ประมาณ 50 เมตรเท่านั้น ดังนั้นจึงไม่ค่อยได้รับความนิยมมากนัก

2. IEEE 802.11b เป็นมาตรฐานที่เริ่มนำเข้ามาใช้ในปี ค.ศ. 1999 ซึ่งเป็นที่รู้จักกันดีและได้รับความนิยมอย่างแพร่หลาย โดยใช้เทคนิคการส่งข้อมูลแบบ DSSS (Direct Sequence Spread Spectrum) ที่สามารถรับส่งข้อมูลได้ด้วยอัตราความเร็วสูงสุด 11 Mbps และใช้คลื่นวิทยุความถี่ 2.4 GHz ซึ่งเป็นความถี่ที่มีการใช้งานในหลายเทคโนโลยี เช่น Bluetooth โทรศัพท์ไร้สาย และเตาไมโครเวฟ ทำให้การใช้งานมักพบปัญหาในเรื่องของสัญญาณรบกวนค่อนข้างมาก ส่วนข้อดีของมาตรฐาน IEEE 802.11b ก็คือ มีรัศมีในการส่งข้อมูลประมาณ 100 เมตร ซึ่งครอบคลุมในบริเวณที่กว้างกว่ามาตรฐาน IEEE 802.11a

3. IEEE 802.11g เป็นมาตรฐานที่เริ่มนำมาใช้ในปี ค.ศ. 2003 ซึ่งเข้ามาทดแทนมาตรฐาน IEEE 802.11b โดยใช้เทคนิคการส่งข้อมูลแบบ DSSS (Direct Sequence Spread Spectrum) บนคลื่นวิทยุความถี่ 2.4 GHz และสามารถยังรับส่งข้อมูลได้ด้วยอัตราความเร็วสูงสุด 54 Mbps ซึ่งเป็นอัตราเร็วในการส่งข้อมูลที่สูงกว่ามาตรฐาน IEEE 802.11 b โดยมีรัศมีในการขนส่งข้อมูลครอบคลุมพื้นที่ประมาณ 100 เมตร ซึ่งกว้างกว่ามาตรฐาน IEEE 802.11a จึงได้รับความนิยมมากในปัจจุบัน

4. IEEE 802.11n เป็นมาตรฐานใหม่ที่เริ่มพัฒนาในปี ค.ศ. 2004 ซึ่งพัฒนาเพิ่มเติมจากมาตรฐานรุ่นก่อนๆ โดยใช้คลื่นวิทยุที่ความถี่ 2.4 GHz และ 5 GHz ซึ่งมีความเร็วสูงสุดที่ 248 mbps การพัฒนา IEEE 802.11n ขึ้นมาก็เพื่อต้องการให้มีรัศมีในการขนส่งข้อมูลครอบคลุมบริเวณที่กว้างขึ้น และอัตราความเร็วในการรับส่งข้อมูลสูงกว่ามาตรฐานแบบเดิมๆ

5. IEEE 802.11-2012 ในปี ค.ศ. 2007 กลุ่มงาน TGmb ได้รับการอนุมัติให้รวบรวมการแก้ไขทั้งหมดให้เป็นเวอร์ชันที่เรียกว่า REVmb หรือ 802.11mb ที่ประกอบด้วย 802.11k, r, y, n, w, p, z, v, u, s

6. IEEE 802.11ac เป็นมาตรฐานที่ 5 GHz ให้ทรูพุทกับแลนไร้สายแบบหลายสถานีสูงกว่าที่อย่างน้อย 1 Gbps และสำหรับลิงก์เดี่ยวที่อย่างน้อย 500 Mbps โดยการใช้ RF แบนด์วิดธ์ที่กว้างกว่า (80 หรือ 160 MHz) สตรีมมากกว่า (สูงถึง 8 สตรีม) และมอดูเลตที่ความจุสูงกว่า (สูงถึง 256 QAM)

7. IEEE 802.11ad หรือ WiGig เกิดจากการผลักดันจากผู้ผลิตฮาร์ดแวร์ ในปี ค.ศ. 2012 Marvell และ Wilocity ได้ประกาศการเป็นคู่ค้าใหม่เพื่อนำ Wi-Fi Solution แบบ Tri-Band ใหม่ออกสู่ตลาด โดยการใช้ความถี่ที่ 60 GHz ทรูพุททางทฤษฎีสูงสุดถึง 7 Gbps มาตรฐานนี้จะออกสู่ตลาดเมื่อปี ค.ศ. 2014

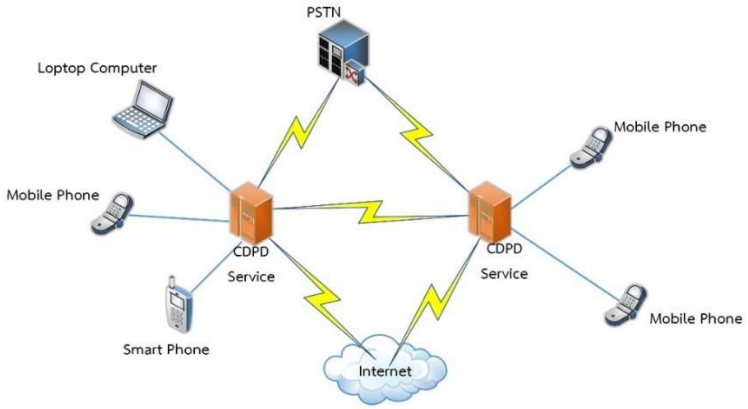
8. IEEE 802.11ax หรือ Wi-Fi เป็นมาตรฐานที่พัฒนาต่อยอดจาก 802.11ac ที่รองรับการรับส่งข้อมูลแบบ MIMO สูงสุดที่ 4 Spatial Streams โดยเพิ่มประสิทธิภาพในการรับส่งข้อมูลต่อ Stream ให้มากกว่าเดิมอีกหลายเท่า ซึ่งมาตรฐาน 802.11ax ยังคงใช้ช่วงคลื่นความถี่ 5 GHz เช่นเดียวกับ 802.11ac เนื่องจากมีช่องสัญญาณที่กว้าง (80 และ 160 MHz) และเลือกใช้ได้เป็นจำนวนมาก

มาตรฐานและโพรโทคอลของระบบเครือข่ายแบบไร้สาย

ระบบเครือข่ายแบบไร้สายเป็นการส่งข้อมูลรูปแบบใหม่ที่มีพัฒนาการอย่างต่อเนื่อง ทำให้เกิดมาตรฐานและโพรโทคอลที่ใช้ในการส่งข้อมูลใหม่ๆ ขึ้นมาโดยมาตรฐานและโพรโทคอลของระบบเครือข่ายแบบไร้สายที่ควรรู้จักมีดังนี้

1. Cellular Digital Packet Data (CDPD)

CDPD หรือ Wireless IP หรือ โพรโทคอล IP ไร้สาย ซึ่งเป็นมาตรฐานการสื่อสารไร้สายแบบสองทางที่ใช้ในการส่งแพ็กเก็ตข้อมูลผ่านช่องสัญญาณในระบบโทรศัพท์มือถือ โดยการเชื่อมต่อกับอุปกรณ์ไร้สายเข้ากับอินเทอร์เน็ตจะมีความเร็ว 19.2 Kbps และการส่งข้อมูลจะใช้ช่วงความถี่ของคลื่นวิทยุ โดยข้อมูลที่ส่งมานั้นสามารถเดินทางพร้อมกับการติดต่อสื่อสารพื้นฐานของโทรศัพท์มือถือได้ กล่าวคือ ในขณะที่ข้อมูลเดินทางมาการสื่อสารด้วยเสียงก็ยังสามารถใช้งานได้ แสดงการเชื่อมต่อของเครือข่าย CDPD ได้ดังภาพที่ 8.14



ภาพที่ 8.14 ลักษณะการ CDPD Network

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 291)

CDPD เป็นการติดต่อด้วยโมเด็มไร้สาย ซึ่งมีอยู่ภายในเครื่องโทรศัพท์มือถือหรืออุปกรณ์อื่นๆ ที่ติดตั้งโมเด็มไร้สายไว้ หากต้องการใช้งานจะต้องเชื่อมต่อผ่านผู้ให้บริการ CDPD นอกจากนี้ การส่งข้อมูลไปยังเครือข่ายอื่นสามารถเชื่อมต่อได้ทั้งเครือข่ายของโทรศัพท์มือถือ เครือข่ายโทรศัพท์สาธารณะ (PSTN) และเครือข่ายอินเทอร์เน็ต การให้บริการ CDPD นิยมใช้อย่างแพร่หลายในประเทศสหรัฐอเมริกา ซึ่งมีผู้ให้บริการอยู่จำนวนมาก รวมถึงอีกหลายประเทศ เช่น แคนาดา เม็กซิโก นิวซีแลนด์ และจีน เป็นต้น

2. Wireless Application Protocol (WAP)

WAP ถูกพัฒนาขึ้นในปี ค.ศ. 1997 โดยบริษัทชั้นนำทางเทคโนโลยีโทรศัพท์มือถือในสมัยนั้น คือ Motorola Nokia Ericsson และ Phone.com เพื่อช่วยให้อุปกรณ์เคลื่อนที่ไร้สายสามารถเชื่อมต่อกับอุปกรณ์เครือข่ายอินเทอร์เน็ตได้ ซึ่งใช้พื้นฐานการเชื่อมต่อและการแสดงผลเหมือนกับ Browser บนเครื่องคอมพิวเตอร์ เพียงแต่การใช้งานอุปกรณ์เหล่านี้จะมีข้อจำกัดที่ขนาดและปริมาณของข้อมูล โพรโทคอล WAP จะทำงานในลักษณะ Client/Server โดยภายในอุปกรณ์ไร้สายจะต้องติดตั้งซอฟต์แวร์ที่ทำหน้าที่ในฝั่งของ Client และส่วนฝั่งของ Server จะทำหน้าที่ของผู้ให้บริการ อุปกรณ์เคลื่อนที่ไร้สายที่ใช้งาน WAP ส่วนใหญ่จะเป็นโทรศัพท์มือถือบางรุ่นที่สามารถรองรับการใช้งานได้ นอกจากนี้ WAP ยังช่วยให้การติดต่อสื่อสารกับระบบเครือข่ายอินเทอร์เน็ตมีความกว้างไกลมากขึ้น เนื่องจากโทรศัพท์มือถือสามารถเชื่อมต่อได้เกือบทุกที่ที่อยู่ในขอบเขตสัญญาณของผู้ให้บริการและสามารถเชื่อมต่อระหว่างผู้ใช้กับเครือข่ายที่หลากหลายได้

3. Infrared Data Association (IrDA)

IrDA เป็นมาตรฐานการสื่อสารการค้นหาด้วยระบบไร้สายที่รู้จักกันกว้างขวางตั้งแต่อดีตจนถึงปัจจุบัน โดยนิยมใช้อุปกรณ์เคลื่อนที่ไร้สายจำพวก PDA และโทรศัพท์มือถือบางรุ่น หรือในอุปกรณ์อำนวยความสะดวกต่างๆ เช่น คีย์บอร์ดไร้สาย รีโมท และของเล่นบางชนิด การเชื่อมต่อของ IrDA จะเป็นแบบ Point-to- Point เพื่อให้อุปกรณ์ทั้ง 2 ชนิดสามารถติดต่อสื่อสารกันได้ แต่ทั้งนี้การทำงานของ IrDA จะใช้ได้ในระยะที่จำกัดและอุปกรณ์ทั้งสองจะเชื่อมต่อกันในแนวระดับเดียวกัน หรือ Line of Sight

4. Third Generation (3G) for Mobile Communication

3G เป็นชื่อเรียกของยุคที่มีการพัฒนาระบบเครือข่ายแบบไร้สายที่มีเทคโนโลยีก้าวหน้ามากขึ้น ทำให้ผู้ผลิตและผู้ให้บริการต่างๆ จำเป็นต้องสร้างมาตรฐานเพื่อให้มีทิศทางการพัฒนาเป็นไปในรูปแบบเดียวกัน จึงมีการรวมตัวและตั้งกลุ่มที่เรียกขึ้นว่า 3G.IP ขึ้น โดยมีจุดประสงค์เพื่อสร้างมาตรฐานของเทคโนโลยีไร้สายที่พัฒนาขึ้น ในยุค 3G สมาชิกของ 3G.IP ประกอบด้วยบริษัทชั้นนำด้านอุปกรณ์ไร้สายรวมถึงผู้ให้บริการเครือข่าย เช่น AT&T, Ericsson, Nokia และ Nortel Network เป็นต้น เทคโนโลยีที่ถูกพัฒนาขึ้นจะใช้สำหรับการสื่อสารด้วยเสียงและข้อมูลความเร็วสูง เพื่อรองรับการติดต่อสื่อสารอย่างสมบูรณ์แบบในอนาคต เช่น การสื่อสารด้วยเสียงและภาพ และการถ่ายทอดวีดีโอผ่านอุปกรณ์ไร้สาย เป็นต้น โดยการสื่อสารในรูปแบบดังกล่าวจะดำเนินการอยู่บนเครือข่ายที่ใช้งานด้วย IP หรือเครือข่ายอินเทอร์เน็ตนั่นเอง

5. Enhanced Data Rates for Global Evolution (EDGE)

EDGE ถูกพัฒนาและนำมาใช้งานเมื่อปี ค.ศ.2002 เพื่อใช้ในเครือข่าย GSM ที่มีความเร็วในการส่งข้อมูลสูง เนื่องจาก EDGE สามารถรับส่งข้อมูลได้ด้วยอัตราความเร็วสูงสุดที่ 384 Kbps ซึ่งเป็นการส่งข้อมูลด้วยระบบโทรศัพท์เคลื่อนที่ที่เร็วกว่ารูปแบบอื่น โดย EDGE เกิดขึ้นเมื่อมีการพัฒนาเข้าสู่ยุค 3G ซึ่งการติดต่อสื่อสารในยุคนี้จำเป็นต้องใช้วิธีการส่งข้อมูลที่รวดเร็วและรองรับปริมาณข้อมูลได้มากขึ้น ปัจจุบัน EDGE จึงถูกนำมาให้บริการผ่านเครือข่ายโทรศัพท์มือถือต่างๆ อย่างแพร่หลายทั่วโลก

6. Fourth Generation (4G)

เทคโนโลยี 4G เป็นเครือข่ายไร้สายความเร็วสูงชนิดพิเศษ หรือเป็นเส้นทางด่วนสำหรับข้อมูลที่ไม่ต้องอาศัยการใช้สาย โดยระบบเครือข่ายใหม่นี้ จะสามารถใช้งานได้แบบไร้สาย รวมถึงคุณสมบัติการเชื่อมต่อเสมือนจริงในรูปแบบ 3 มิติ (Three-Dimensional) ระหว่าง

ผู้ใช้โทรศัพท์ด้วยกันเอง นอกจากนั้น สถานีฐาน ซึ่งทำหน้าที่ในการส่งผ่านสัญญาณโทรศัพท์เคลื่อนที่จากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง เทคโนโลยี 4G จะสามารถส่งผ่านข้อมูลแบบไร้สายด้วยระดับความเร็วสูงที่เพิ่มขึ้นถึง 100 Mbps ซึ่งห่างจากความเร็วของชุดอุปกรณ์ที่ใช้กันอยู่ในปัจจุบัน ที่ระดับ 10 Kbps เทคโนโลยี 4G มีการปรับปรุงมากกว่า 3G อย่างมีนัยสำคัญ นอกจากเรื่องคลื่นความถี่ ความครอบคลุม และความสามารถ และยังมีประโยชน์อื่นๆ อีกมาก เช่น คุณภาพของการบริการ QoS (Quality of Service) รูปแบบการใช้งานระบบเคลื่อนที่ที่มากขึ้น และการสนับสนุนด้านความปลอดภัย

7. เทคโนโลยี 5G

เทคโนโลยี 5G เป็นเทคโนโลยีเซลลูลาร์ไร้สายยุคที่ 5 ที่รองรับการขยายช่องสัญญาณเพื่อรองรับการสื่อสารจำนวนมาก เช่น การสื่อสารของวิดีโอแบบ 360 องศา สนองต่อการทำงานของแอปพลิเคชันความจริงเสมือน การสื่อสารของเทคโนโลยี 5G เป็นการสื่อสารที่มีความเสถียรและเวลาหน่วงที่ต่ำรองรับการสื่อสารแบบเรียลไทม์ และการสื่อสารภาวะวิกฤติ เช่น ระบบการแพทย์ทางไกล การแจ้งเตือนอุบัติเหตุระบบจราจรที่มีประสิทธิภาพ การใช้งานรถยนต์แบบไร้คนขับ เป็นต้น นอกจากนี้เทคโนโลยี 5G ยังรองรับการเจริญเติบโตของการใช้อุปกรณ์ IoT และยังรองรับการสื่อสารแบบ Device-to- Device (D2D) ที่เป็นการสื่อสารของระบบเซลลูลาร์ในรูปแบบใหม่ทำให้อุปกรณ์สามารถสื่อสารกันเองโดยไม่ต้องผ่านสถานีฐาน (Base Station) ลดภาระการทำงานของระบบลง ทำให้การใช้งานช่องสัญญาณมีประสิทธิภาพดีขึ้น รวมถึงลดการใช้พลังงานในการส่งข้อมูลที่เกิดขึ้น (ชัชชัย คุณบัว, 2562, หน้า 253-255)

ประโยชน์และปัญหาของ Wireless LAN

การใช้เทคโนโลยี Wireless LAN ทำให้เกิดความสะดวก และได้รับประโยชน์อย่างมาก ดังนี้

1. การติดตั้งเครือข่ายทำได้ง่าย และสะดวกต่อการเคลื่อนย้ายอุปกรณ์คอมพิวเตอร์ต่าง ๆ เนื่องจากไม่จำเป็นต้องเดินสายสัญญาณ

2. ประหยัด เนื่องจากไม่มีค่าใช้จ่ายในการติดตั้งสายสัญญาณ

ถึงแม้การนำ Wireless LAN มาใช้จะช่วยให้เกิดความสะดวกสบายมากก็ตาม แต่เทคโนโลยีดังกล่าวก็ยังคงมีข้อด้อยและปัญหาหลายประการดังนี้

1. การออกแบบมีการกระจายตัว (Propagation) ของคลื่นให้ครอบคลุมทำได้ยาก เนื่องจากการเกิดจุดอับคลื่นและถูกรบกวนได้ง่าย

2. หากใช้วิธีส่งข้อมูลด้วยอินฟราเรดจะทำให้การขยายเครือข่ายทำได้ยาก เนื่องจากอินฟราเรดไม่สามารถผ่านวัตถุทึบแสงหรือทะลุผนังห้องได้ ทำให้เครือข่ายถูกจำกัดอยู่ในรัศมีที่แคบ ดังนั้นหากต้องการติดตั้งเครือข่าย Wireless LAN นอกอาคารจึงทำได้ยาก

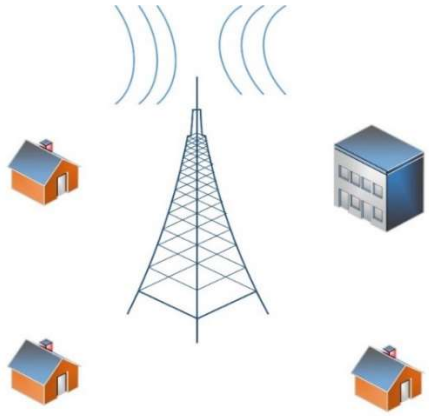
3. Wireless LAN นิยมใช้คลื่นวิทยุในการรับส่งข้อมูล จึงมักถูกรบกวนด้วยคลื่นแม่เหล็ก ไฟฟ้าและคลื่นรบกวนอื่นๆ ได้ง่าย

8.5 บรอดแบนด์ไร้สาย

บรอดแบนด์ไร้สาย (Broadband Wireless) จะใช้เสาอากาศที่ทำหน้าที่ส่งสัญญาณและเครื่องรับสัญญาณสำหรับติดตั้งตามบ้านเรือน อาศัยคลื่นวิทยุความถี่ 10-66 GHz เป็นสื่อกลางสำหรับรับส่งข้อมูล ซึ่งมีระยะทางการรับส่งในรัศมีหลายกิโลเมตร จึงเรียกเครือข่ายดังกล่าวว่า Wireless Area Network (Wireless MAN) ซึ่งเป็นเครือข่ายแบบไร้สายบริเวณกว้าง

ลักษณะของบรอดแบนด์ไร้สาย

การส่งข้อมูลมีลักษณะเป็น Full-Duplex คือ สามารถรับส่งข้อมูลได้พร้อมกัน โดยใช้คลื่นวิทยุส่งข้อมูลด้วยความถี่สูงมาก และเดินทางเป็นเส้นตรง มักจะถูกน้ำดูดกลืน (Absorb) ง่าย ซึ่งเป็นปัญหาสำคัญของคลื่นความถี่สูง เนื่องจากในสภาวะอากาศที่มีฝนหรือหิมะตกจะเป็นอุปสรรคสำคัญในการรับส่งข้อมูล จึงต้องมีการควบคุมความผิดพลาดของข้อมูลอย่างรอบคอบและระมัดระวังเป็นพิเศษ สำหรับองค์ประกอบของลักษณะ Broadband Wireless แสดงได้ดังภาพที่ 8.15



ภาพที่ 8.15 ลักษณะของ Broadband Wireless

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 942)

จากภาพที่ 8.15 องค์ประกอบของ Broadband Wireless ที่สำคัญมี 2 ส่วน ส่วนแรก คือ กลุ่มของ Base Station ซึ่งเป็นเสาอากาศที่มีจานรับสัญญาณหลายตัว โดยแต่ละตัวจะดูแลเฉพาะจานรับสัญญาณของตนเท่านั้น ส่วนที่สอง คือ เสาอากาศที่มีจานรับส่งสัญญาณตามบ้านเรือน ซึ่งข้อมูลที่ส่งจะต้องทำการโมดูเลชันด้วยวิธี QAM-64 QAM-16 และ QPSK ก่อน สำหรับเทคโนโลยีที่ช่วยในการส่งข้อมูลมี 2 วิธี คือ FDD (Frequency Division Duplexing) และ TDD (Time Division Duplexing) โดยเรียกการส่งข้อมูลจาก Base Station ไปยังบ้านเรือนว่า Downstream ซึ่งใช้ Base Station ในการควบคุมการรับส่งข้อมูล ส่วนการส่งข้อมูลจากบ้านเรือนไปยัง Base Station เรียกว่า Upstream ซึ่งการควบคุมการรับส่งข้อมูลเป็น Connection-Oriented ดังนั้น การติดต่อแต่ละครั้งจะต้องสร้างการเชื่อมต่อก่อนการส่งข้อมูล และต้องกำหนดหรือระบุบริการที่จะใช้ในการส่งแต่ละครั้ง โดยมีบริการ 4 รูปแบบดังนี้

1. Constant Bit Rate Service เป็นการส่งข้อมูลที่กำหนดค่าได้ โดย Bandwidth ที่ขอมีจำนวนแน่นอนและส่วนใหญ่เป็นบริการสำหรับส่งข้อมูลเสียง

2. Real-Time Variable Bit Rate Service เป็นการส่งข้อมูลที่ไม่ได้กำหนดค่า Bandwidth โดย Base Station จะมีระยะเวลาเป็นช่วงๆ สำหรับการสอบถามค่า Bandwidth ที่ผู้ใช้ต้องการในแต่ละครั้ง ซึ่ง Bandwidth ที่ขอในแต่ละครั้งจะมีจำนวนไม่เท่ากัน ส่วนใหญ่เป็นบริการที่ใช้สำหรับส่งข้อมูลจำพวกสื่อประสม (Multimedia) และภาพเคลื่อนไหวต่างๆ

3. Non-Real-Time Variable Bit Rate Service เป็นการส่งข้อมูลที่กำหนดค่าไม่ได้ ซึ่งต่างจากบริการแบบที่ 2 เนื่องจาก Base Station จะสอบถามค่า Bandwidth ที่ผู้ใช้ต้องการเมื่อใดก็ได้ และ Bandwidth ที่ขอในแต่ละครั้งจะมีจำนวนไม่เท่ากัน โดยส่วนใหญ่ใช้สำหรับส่งข้อมูลจำนวนมาก และไฟล์ข้อมูลมีขนาดใหญ่

4. Best-Efforts Service บริการลักษณะนี้จะไม่มีการสอบถามการขอ Bandwidth จาก Base Station แต่ผู้ใช้ต้องร้องขอเพื่อแบ่ง Bandwidth กันเอง ส่วนใหญ่ใช้สำหรับการส่งข้อมูลประเภทอื่นที่นอกเหนือจากขอบเขตของบริการทั้ง 3 แบบข้างต้น

8.6 ไวแมกซ์

ไวแมกซ์ (WiMAX) เป็นมาตรฐานของเทคโนโลยีสำหรับการติดต่อสื่อสารระยะไกลของ IEEE 802.16 ที่เกี่ยวข้องกับเครือข่ายแบบไร้สายแบบ Broadband Wireless มาตรฐานไวแมกซ์นี้มีความคล้ายกับมาตรฐานเครือข่ายแบบไร้สายแบบ ไวไฟ (Wi-Fi) แตกต่างกันในเรื่องของระยะทางที่สามารถเชื่อมต่อเครือข่ายได้ ไวแมกซ์เป็นเทคโนโลยีที่เชื่อมต่อ Last Mile คือ

การเชื่อมต่อระหว่างผู้ใช้กับผู้ให้บริการในระยะสุดท้าย เช่น องค์การโทรศัพท์ บริษัทเคเบิลทีวี และ ISP เป็นต้น โดย Last Mile เป็นพื้นฐานการเชื่อมต่อในหลายๆ เทคโนโลยี เช่น DSL และ Cable Modem เป็นต้น (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 295-296)

การเชื่อมต่อของไวแมกซ์นั้นจะคล้ายกับเทคโนโลยี DSL ที่ความเร็วและขนาดของช่วงสัญญาณจะแปรผันตามระยะทาง โดยมาตรฐานแล้วไวแมกซ์จะรองรับได้ถึง 70 Mbps ในระยะทางที่ไกลถึง 112 กิโลเมตร แต่อาจมีปัจจัยหลายอย่างที่รบกวนสัญญาณ เช่น ตึกสูง สภาพอากาศ คลื่นสัญญาณอื่นๆ ซึ่งปัจจัยเหล่านี้จะส่งผลกระทบต่อช่วงความเร็วในระยะทาง 2 กิโลเมตร ไวแมกซ์จะรองรับการขนส่งข้อมูลที่ความเร็ว 10 Mbps จำนวนผู้ใช้ก็เป็นอีกตัวแปรหนึ่งที่ส่งผลให้ความเร็วลดลงได้ ยิ่งมีผู้ใช้จำนวนมากความเร็วในการขนส่งข้อมูลก็จะลดลง

ความแตกต่างระหว่างไวแมกซ์และ Wi-Fi มีดังนี้

1. ไวแมกซ์เป็นเครือข่ายแบบไร้สายที่ใช้งานในระยะไกลหลายกิโลเมตรแต่ Wi-Fi เป็นเครือข่ายแบบไร้สายที่ใช้งานระยะใกล้เท่านั้น

2. คลื่นความถี่ที่ใช้ใน Wi-Fi จะเป็นคลื่นความถี่ที่ใช้โดยไม่ต้องขออนุญาต แต่คลื่นความถี่ที่ใช้ใน WiMAX จำเป็นที่จะต้องขออนุญาตเปิดให้บริการก่อน

3. QoS (Quality of Service) ของไวแมกซ์มีความน่าเชื่อถือมากกว่า เนื่องจากไวแมกซ์มีการเชื่อมต่อระหว่างผู้ใช้กับสถานีย่อย (Base Station) ซึ่งมีระบบที่รับประกันการไหลของข้อมูลได้แน่นอนกว่า Qos ของ Wi-Fi

4. ไวแมกซ์มีการเชื่อมต่อที่ยืดหยุ่นมากกว่า Wi-Fi เนื่องจากมีการจัดการด้านสัญญาณที่ค่อนข้างมีประสิทธิภาพสูง และมีการสนับสนุนในด้านการเปลี่ยนสิทธิ์ถือครองสัญญาณ เช่น Hondoff ทำให้การติดต่อสื่อสารมีการต่อเนื่อง

5. Wi-Fi เป็นเทคโนโลยีที่มีราคาต่ำกว่าไวแมกซ์และเป็นเทคโนโลยีในระยะใกล้ การใช้งานกับเครือข่ายขนาดเล็กที่มีพื้นที่ครอบคลุมในหนึ่งห้องทำงานหรือภายในบ้าน Wi-Fi จึงค่อนข้างเหมาะสมกว่าไวแมกซ์

8.7 การระบุตัวตนการเข้าใช้งานในเครือข่ายแบบไร้สาย

เครือข่ายแบบไร้สายถึงแม้จะมีข้อดีอยู่มากมาย แต่ด้วยความยืดหยุ่นในการเชื่อมต่อเข้าสู่ระบบทำได้ในทุกบริเวณที่รับสัญญาณ อาจทำให้เกิดช่องทางที่ผู้ไม่ประสงค์ดีเข้าโจมตีเครือข่ายได้ ซึ่งในจุดนี้อาจทำให้ผู้ใช้ไม่มั่นใจในความปลอดภัยและความมั่นคงของเครือข่ายแบบไร้สาย ดังนั้น การกำหนดให้ผู้ใช้ทุกคนต้องระบุตัวตนก่อนเข้าใช้งานในระบบเครือข่ายแบบไร้สาย

จึงเป็นสิ่งสำคัญ เพื่อเป็นการสร้างมาตรการความปลอดภัยให้กับเครือข่ายแบบไร้สายได้ในขั้นต้น การระบุตัวตนเป็นการพิสูจน์แก่ผู้ให้บริการเครือข่ายแบบไร้สายว่าตนเองคือผู้ใช้ที่ได้รับการยืนยันและอนุญาตให้เข้าใช้ในระบบนี้ได้

เมื่อเครื่อง Client ต้องการรับส่งข้อมูลผ่านเครือข่ายแบบไร้สายก็จะดำเนินการร้องขอและรอการตอบกลับยืนยันสถานะการพิสูจน์ตัวตนว่าถูกต้องหรือไม่ แสดงขั้นตอนการพิสูจน์ตัวตนได้ดังภาพที่ 8.16

ภาพที่ 8.16 การพิสูจน์ตนเองกับเครือข่ายแบบไร้สาย

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 296)

จากภาพที่ 8.16 อธิบายขั้นตอนได้ ดังนี้

1. เมื่อเครื่อง Client ต้องการที่จะเชื่อมต่อกับเครือข่าย ก็ส่งคำร้องขอในรูปแบบการกระจายข้อมูล (Broadcast) ไปยังจุดกำเนิดสัญญาณหรือผู้ให้บริการ

2. ผู้ให้บริการหรือ Access Point ได้รับสัญญาณการร้องขอที่กระจายมาก็จะตอบกลับไปยังเครื่อง Client เพื่อให้ดำเนินการส่งข้อมูลพิสูจน์ตัวตนต่อไป

3. เมื่อเครื่อง Client ได้รับสัญญาณการตอบกลับมาแล้ว จึงดำเนินการส่งข้อมูลเพื่อพิสูจน์ตัวตน โดยจะพิจารณาระหว่างการเชื่อมต่อกับ Access Point หรือผู้ให้บริการตำแหน่งใด

4. หลังจากที่พิจารณาแล้วว่า Access Point หรือผู้ให้บริการใดเหมาะสมที่สุด ซึ่งอาจพิจารณาจากความเข้มของสัญญาณที่ดีที่สุด จึงเริ่มดำเนินการส่งข้อมูลไปพิสูจน์ตัวตนและขออนุญาตเข้าใช้เครือข่าย

5. เมื่อ Access Point หรือผู้ให้บริการได้รับข้อมูลพิสูจน์ตัวตนจากเครื่อง Client แล้วก็จะดำเนินการพิจารณาผลการตรวจสอบ และส่งผลลัพธ์ดังกล่าวไปยังเครื่อง Client เพื่อให้รับทราบว่าอนุญาตให้เข้าใช้งานหรือไม่

6. เมื่อพิสูจน์ตัวตนสำเร็จ เครื่อง Client สามารถระบุตัวตนได้และมีความน่าเชื่อถือพอที่จะเข้าใช้งานเครือข่าย เครื่อง Client จะส่งข้อมูลส่วนที่เหลือกลับไปเพื่อยืนยันอีกครั้ง

7. จากนั้น Access Point หรือผู้ให้บริการก็จะตอบกลับ หลังจากที่ได้รับข้อมูลส่วนที่เหลือของ Client แล้วเพื่อเปิดสถานะการเข้าใช้งานให้เครื่อง Client ทราบ พร้อมกับข้อมูลที่จำเป็นในการระบุตัวตนภายในเครือข่ายได้อย่างถูกต้อง

จากที่กล่าวมาเป็นเพียงการส่งคำร้องขอและการยืนยันสถานการณ์ใช้งานในเครือข่ายนั้น ซึ่งกระบวนการพิสูจน์หรือระบุตัวตนมีหลายรูปแบบ ขึ้นอยู่กับวิธีการที่ระบบเครือข่ายเป็นผู้กำหนด สำหรับวิธีการระบุตัวตนมี ดังนี้

1. การระบุตัวตนแบบง่าย

เป็นการระบุตัวตนในเครือข่ายแบบไร้สายพื้นฐานที่ไม่มีขั้นตอนซับซ้อนมากนัก เป็นการระบุตัวตนตามมาตรฐาน 802.11 โดยให้ความสำคัญกับอุปกรณ์ขนาดเล็กที่ต้องการเชื่อมต่อกับเครือข่ายแบบไร้สาย เช่น โทรศัพท์มือถือ และ PDA เป็นต้น เพราะอุปกรณ์เหล่านี้ไม่เหมาะกับกระบวนการระบุตัวตนที่ซับซ้อน

2. การระบุตัวตนแบบใช้ Key

การระบุตัวตนของเครื่อง Client ด้วย Key โดยการใช้ WEP (Wired Equivalency Privacy) เพื่อสร้างความปลอดภัยในการเข้าใช้งาน ซึ่งอาศัยกลไกวิธีการเข้ารหัสและถอดรหัสที่จำเป็นต้องใช้ Key ในการระบุตัวตน วิธีนี้จะกำหนด Key ให้กับเครื่อง Client ทุกเครื่องแบบตายตัว โดยในอุปกรณ์ Access Point นั้นจะส่งฟังก์ชันที่ใช้สำหรับการเข้ารหัสข้อมูลที่จะทำการกระจายส่งไปยัง Client ทั่วเครือข่าย ทำให้เครื่อง Client ที่มี Key ที่ถูกต้องเท่านั้นจึงจะสามารถถอดข้อมูลแท้จริงออกมาได้ หากมีผู้ไม่ประสงค์ดีเข้ามาเชื่อมต่อกับเครือข่ายแบบไร้สายนี้ ไม่สามารถระบุตัวตนด้วย Key ที่ถูกต้องตามที่ผู้ให้บริการได้กำหนดไว้ ก็จะไม่สามรถใช้งานเครือข่ายนี้ได้

3. การระบุตัวตนด้วยวิธีการกลั่นกรอง MAC

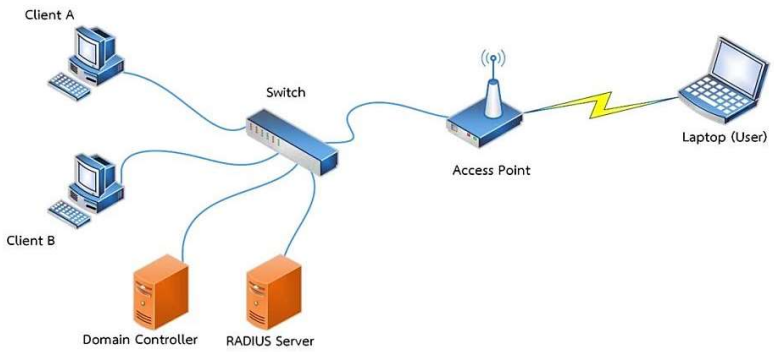
วิธีการระบุตัวตน ด้วยการตรวจสอบหมายเลข MAC หรือ MCC Address ซึ่งจะเป็นหมายเลขที่อ้างอิงอยู่ในระดับชั้นกายภาพของการ์ดไร้สายที่ใช้เชื่อมต่อกับเครือข่าย โดยอุปกรณ์ชนิดนี้จะถูกผลิตให้มีหมายเลข MAC ที่ไม่ซ้ำกัน ทำให้สามารถระบุตัวตนของอุปกรณ์นี้ได้โดยจริง วิธีการตรวจสอบ MAC Address นี้เรียกได้อีกอย่างว่า MAC Address Filtering ซึ่งจะกลั่นกรองหมายเลข MAC ของเครื่อง Client ที่ร้องขอมาทั้งหมด และตรวจสอบตัวตนหาความถูกต้องก่อนจะเปิดอนุญาตให้เข้าใช้งานในเครือข่าย

การกลั่นกรอง MAC Address นั้นจะเป็นหน้าที่ของ Access Point โดยพิจารณา MAC Address ที่ได้บันทึกไว้ในฐานข้อมูลรายชื่อของผู้ใช้ที่ได้รับอนุญาต หากพบว่ามี MAC

Address ตรงกับฐานข้อมูลก็จะเปิดให้เครื่อง Client เข้าใช้งานภายในเครือข่ายได้ตามปกติ แต่ถ้า MAC Address ดังกล่าวไม่ตรงกับที่บันทึกไว้ Access Point ก็จะยกเลิกการติดต่อสื่อสารกับเครื่อง Client นี้ทันที สำหรับวิธีการระบุตัวตนด้วย MAC Address นี้จะสามารถพิสูจน์ความถูกต้องของผู้ใช้ได้เป็นอย่างดี แต่จะเหมาะกับเครือข่ายขนาดเล็ก เนื่องจากในการกลั่นกรอง MAC Address นั้นจำเป็นต้องบันทึกหมายเลขลงฐานข้อมูล ถ้าเครือข่ายมีขนาดใหญ่ หรือมีจำนวนเครื่อง Client มากเกินไป ส่งผลให้ฐานข้อมูลมีขนาดใหญ่ในขณะที่ความสามารถของ Access Point นั้นรองรับจำนวน MAC Address ได้อย่างจำกัด

4. การระบุตัวตนและสิทธิ์การเข้าใช้งานด้วย RADIUS Server

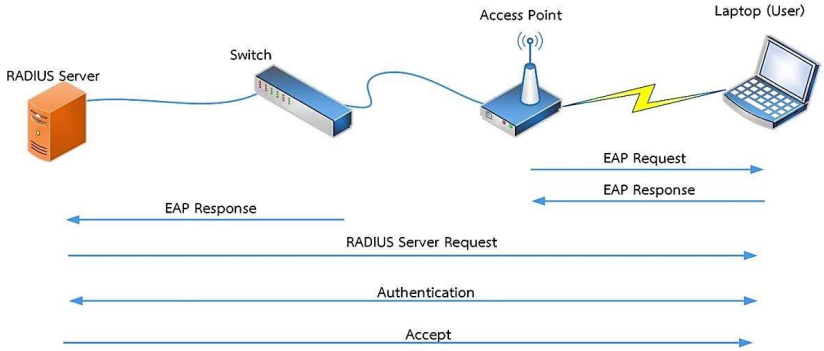
เป็นวิธีการระบุตัวตนและพิสูจน์สิทธิ์ในการเข้าใช้งานเครือข่ายโดยอาศัย Server ที่มีหน้าที่เฉพาะในการเก็บข้อมูลที่สำคัญของผู้ใช้ เรียกว่า RADIUS Server (RADIUS : Remote Authentication Dial-In User Service) ที่เป็น Server สำหรับตรวจสอบและอนุญาตการเข้าใช้งานของผู้ใช้โดย RADIUS Server จะมีฐานข้อมูลผู้ใช้ ซึ่งจัดเก็บข้อมูลที่จำเป็นต่อการพิสูจน์ตัวตนและสิทธิ์ในการเข้าใช้งาน เช่น รหัสผ่าน การทำงานของ RADIUS Server จะประสานงานร่วมกับ Domain Controller เนื่องจากข้อมูลจะไม่ถูกจัดเก็บไว้บน RADIUS Server ทั้งหมด แต่จะดึงข้อมูลที่ใช้ในการพิสูจน์ตัวตนจาก Domain Controller แทน โดยชื่อผู้ใช้ที่มีสิทธิ์จะถูกบันทึกไว้ในบัญชีรายชื่อที่อยู่ในฐานข้อมูลของ RADIUS Server เมื่อมีการร้องขอเข้าใช้บริการ RADIUS Server จะดำเนินการตรวจสอบข้อมูลต่างๆ ทั้งสิทธิ์ในการเข้าใช้ ชื่อผู้ใช้และรหัสผ่าน โดยจะดึงข้อมูลที่จำเป็นจาก Domain Controller มาใช้ในการตรวจสอบลักษณะการเชื่อมต่อของระบบการระบุตัวตนด้วย RADIUS Server แสดงการเชื่อมต่อได้ดังภาพที่ 8.17



ภาพที่ 8.17 ลักษณะการเชื่อมต่อกับเครือข่ายที่ RADUIS Server

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 299)

การระบุตัวตนด้วยการพิสูจน์สิทธิ์นั้นจะใช้โพรโทคอล EAP (Extensible Authentication Protocol) เป็นตัวกลางในการติดต่อสื่อสารระหว่าง RADIUS Server กับ Access Point ซึ่งมีหน้าที่ในการรับส่งข้อมูลที่จะใช้ในการระบุตัวตนของผู้ใช้และขนส่งข้อมูลที่จำเป็นในกระบวนการดังกล่าว ขั้นตอนการทำงานแสดงได้ดังภาพที่ 8.18



ภาพที่ 8.18 แสดงขั้นตอนการพิสูจน์ตัวตนผ่าน RADIUS Server
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 300)

จากภาพที่ 8.18 การติดต่อสื่อสารในกระบวนการนี้จะใช้โพรโทคอล EAP เป็นตัวกลางในการติดต่อทั้งหมด เมื่อเครื่อง Client เชื่อมโยงเข้าสู่ระบบเครือข่ายแล้ว Access Point จะดำเนินการติดต่อกับเครื่อง Client เพื่อร้องขอให้ส่งข้อมูลสำหรับใช้ในการระบุตัวตนเครือข่ายนี้ โดยเครื่อง Client จะต้องตอบกลับไปยัง Access Point ได้รับข้อมูลจากเครื่องและสิทธิ์การเข้าใช้งาน และรอการติดต่อกลับมาจาก RADIUS Server หลังจากที่ Access Point ได้รับข้อมูลจากเครื่อง Client แล้วจะส่งต่อไปยัง RADIUS Server เพื่อให้เริ่มกระบวนการพิสูจน์ตัวตนกับเครื่อง Client โดย RADIUS Server ก็จะเริ่มดำเนินการตรวจสอบ หากถูกต้องก็จะส่งข้อความแจ้งให้เครื่อง Client ทราบ เพื่อเตรียมตัวเข้าใช้งานในเครือข่าย หลังจากนั้น RADIUS Server ก็จะอนุญาตให้เครื่อง Client ที่ผ่านการพิสูจน์ตัวตนแล้วเข้าใช้งานเครือข่ายได้ ซึ่งกระบวนการทำงานต่างๆ จะผ่านทาง Access Point

นอกจากวิธีการระบุตัวตนที่กล่าวมาแล้ว การประยุกต์ใช้วิธีต่างๆ เข้าด้วยกันก็ช่วยให้การพิสูจน์ตัวตนในระบบเครือข่ายมีประสิทธิภาพมากขึ้นได้ เช่น กรณีที่ต้องการเพิ่มความปลอดภัยให้กับข้อมูลที่ใช้สำหรับพิสูจน์ตัวตนผ่านทาง RADIUS Sever ก็อาจนำวิธีการเข้ารหัสด้วย WEP เพื่อป้องกันการดักจับข้อมูลจากผู้อื่น ซึ่งการใช้ Key สำหรับเข้ารหัสข้อมูลไว้จะช่วย

ให้ผู้ที่ดักจับข้อมูลนี้ไปไม่สามารถดึงข้อมูลสำคัญอย่างรหัสผ่านออกไปได้ การระบุตัวตนในเครือข่ายก็จะมีความถูกต้องและสมบูรณ์มากยิ่งขึ้น

8.8 สรุป

เครือข่ายแบบไร้สายเข้ามามีอิทธิพลต่อการทำงาน และการดำเนินชีวิตของมนุษย์ในยุคปัจจุบันเป็นอย่างมาก เครือข่ายแบบไร้สายประเภทต่างๆ แบ่งได้ 3 กลุ่มใหญ่ คือ เครือข่ายแบบไร้สายระยะใกล้ เครือข่ายแบบไร้สายเฉพาะบริเวณ และเครือข่ายแบบไร้สายบริเวณกว้าง

บลูทูธ (Bluetooth) เป็นเครือข่ายแบบไร้สายระยะใกล้ ซึ่งใช้คลื่นวิทยุความถี่ 2.4 GHz และส่งข้อมูลด้วยเทคนิค FHSS มีอัตราเร็วในการส่งข้อมูล 722 Kbps ด้วยระยะทางประมาณ 10 เมตร นิยมนำไปใช้ในการรับส่งข้อมูลระหว่างอุปกรณ์ต่างๆ แทนการใช้สายเชื่อมต่อ เช่น Pocket Pc, โทรศัพท์มือถือ, หูฟัง, คอมพิวเตอร์โน้ตบุ๊ก, เครื่องพิมพ์ และเมาส์

Wireless LAN เป็นเครือข่ายแบบไร้สายเฉพาะบริเวณ โดยถือเป็น LAN ประเภทหนึ่งที่ใช้คลื่นวิทยุ (Radio) หรืออินฟราเรด (Infrared) เป็นสื่อกลางในการรับส่งข้อมูล มาตรฐานของ Wireless LAN เรียกว่า IEEE 802.11 ซึ่งในช่วงแรกมีอัตราความเร็วในการส่งข้อมูลเพียง 2 Mbps แต่ปัจจุบันมีความเร็วเพิ่มมากขึ้น โดยมาตรฐาน IEEE 802.11g ย่านความถี่ 2.4 GHz และ IEEE 802.11ax ย่านความถี่ 5 GHz มีอัตราความเร็วในการส่งข้อมูลถึง 10 Gbps องค์ประกอบที่สำคัญของ Wireless Lan คือ แบบติดต่อผ่าน Access Point และแบบ Ad-hoc Networking นอกจากนี้ยังแบ่งวิธีการควบคุมการส่งข้อมูลออกเป็น 2 แบบ คือ Distributed Coordination Function (DCF) และ Point Coordination Function (PCF) โดยทั่วไปจะใช้แบบ DCF เป็นหลัก สำหรับ PCF เป็นเพียงอีกทางเลือกหนึ่งเท่านั้น

บรอดแบนด์ไร้สาย (Broadband Wireless) เป็นเครือข่ายแบบไร้สายบริเวณกว้าง โดยมีมาตรฐาน คือ IEEE 802.16 และมีองค์ประกอบที่สำคัญ 2 ส่วน คือ Base Station ซึ่งทำหน้าที่ส่งสัญญาณ และเครื่องรับสัญญาณที่ติดตั้งตามบ้านเรือน โดยใช้คลื่นวิทยุความถี่ 10-66 GHz เป็นสื่อกลางสำหรับรับส่งข้อมูลที่มีระยะทางการรับส่งข้อมูลในรัศมีหลายกิโลเมตร Broadband Wireless นำมาใช้เพื่อแก้ปัญหาค่าใช้จ่ายในการติดตั้งสายสัญญาณ Fiber Optic ที่มีราคาสูง

ไวแมกซ์ (WiMAX) เป็นเครือข่ายแบบไร้สายอีกรูปแบบหนึ่งที่ได้รับการกำหนดให้เป็นมาตรฐาน IEEE 802.16 โดยเป็นเครือข่ายในระยะไกล เพื่อขยายประสิทธิภาพให้กับเครือข่ายแบบไร้สายที่มีอยู่ให้ดียิ่งขึ้น Wi-Fi จะมีขอบเขตครอบคลุมพื้นที่ในระยะสั้นเท่านั้น WiMAX เป็น

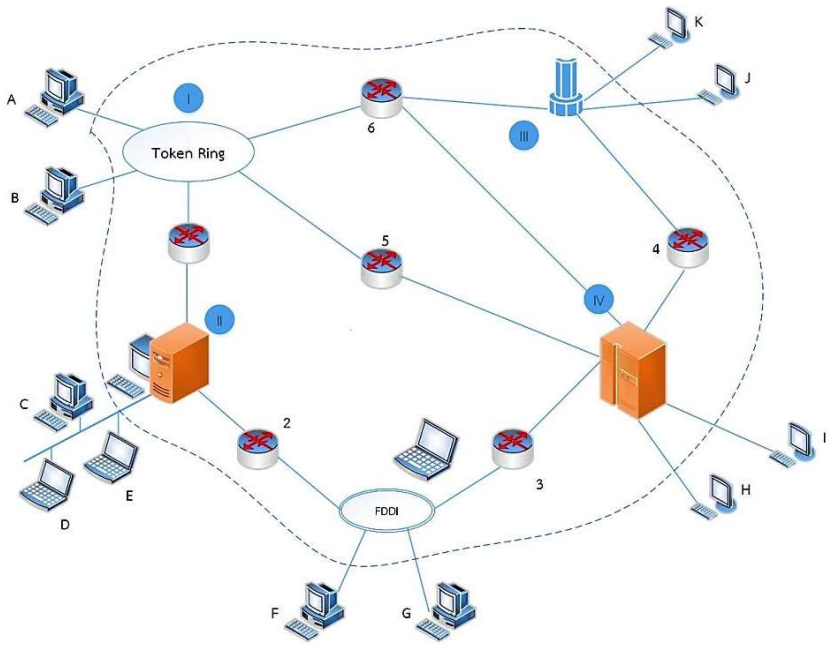
เทคโนโลยีที่คล้ายคลึงกับ DSL เมื่อระยะทางไกลมากขึ้นช่วงของสัญญาณและความเร็วจะลดลง ในระยะ 2 กิโลเมตร WiMAX จะรองรับการขนส่งข้อมูลที่ความเร็ว 10 Mbps ซึ่งความเร็วเฉลี่ยต่อผู้ใช้หนึ่งคนจะมีค่าเท่าๆ กัน เนื่องจาก การใช้งาน WiMAX จะต้องแบ่งปันสัญญาณร่วมกัน จำนวนผู้ใช้มากความเร็วก็จะลดลง

ในการเข้าใช้งานเครือข่ายแบบไร้สายจำเป็นต้องมีการระบุตัวตน เนื่องจากผู้ใช้ทุกคนสามารถเข้าใช้งานในเครือข่ายแบบไร้สายได้จากทุกที่ที่มีสัญญาณครอบคลุม โดยการระบุตัวตนจะเป็นการแสดงสิทธิ์ของผู้ใช้ที่สามารถเข้าใช้งานในเครือข่ายแบบไร้สายนี้ได้ ทำให้เครือข่ายมีความปลอดภัยมากยิ่งขึ้น การระบุตัวตนสามารถทำได้หลากหลายวิธี ได้แก่ การระบุตัวตนแบบง่าย การระบุตัวตนแบบใช้ Key การระบุตัวตนด้วยวิธีการกลั่นกรอง MAC และการระบุตัวตนและสิทธิ์การเข้าใช้งานด้วย RADIUS Server ซึ่งแต่ละวิธีนั้นจะมีจุดประสงค์และรูปแบบการใช้งานที่แตกต่างกัน โดยสามารถนำมาประยุกต์ใช้งานร่วมกันเพื่อให้มีความปลอดภัยมากขึ้น

บทที่ 9
ความรู้เบื้องต้นเกี่ยวกับอินเทอร์เน็ต

อินเทอร์เน็ต (Internet) ย่อมาจากคำว่า International Network หมายถึง เครือข่าย คอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าไว้ด้วยกัน เพื่อให้เกิดการสื่อสารและการแลกเปลี่ยนข้อมูลร่วมกันโดยอาศัยตัวเชื่อมเครือข่ายภายใต้มาตรฐานการเชื่อมโยงเดียวกัน คือ โพรโทคอลทีซีพี/ไอพี โพรโทคอลนี้จะช่วยให้คอมพิวเตอร์ที่มีฮาร์ดแวร์ที่แตกต่างกันสามารถติดต่อถึงกันได้ เครือข่ายอินเทอร์เน็ตนับเป็นเครือข่ายที่ยิ่งใหญ่มาก มีเครื่องคอมพิวเตอร์หลายล้านเครื่องทั่วโลกเชื่อมต่อกับระบบ ทำให้คนในโลกทุกชาติทุกภาษาสามารถติดต่อสื่อสารกันได้ โดยไม่ต้องเดินทาง (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 407)

โพรโทคอลทีซีพี/ไอพี เป็นเครือข่ายที่เชื่อมโยงคอมพิวเตอร์ประเภทต่างๆ เข้าด้วยกัน และมีหลายพันเครือข่าย ซึ่งอาจทำซึ่งอาจเป็นได้ทั้งอีเทอร์เน็ต โทเค็นริง หรือ เอฟดีดีไอ ดังภาพที่ 9.1



ภาพที่ 9.1 เครือข่ายอินเทอร์เน็ตที่ประกอบไปด้วยเครือข่ายหลายประเภทเชื่อมโยงกัน
ที่มา : (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 407)

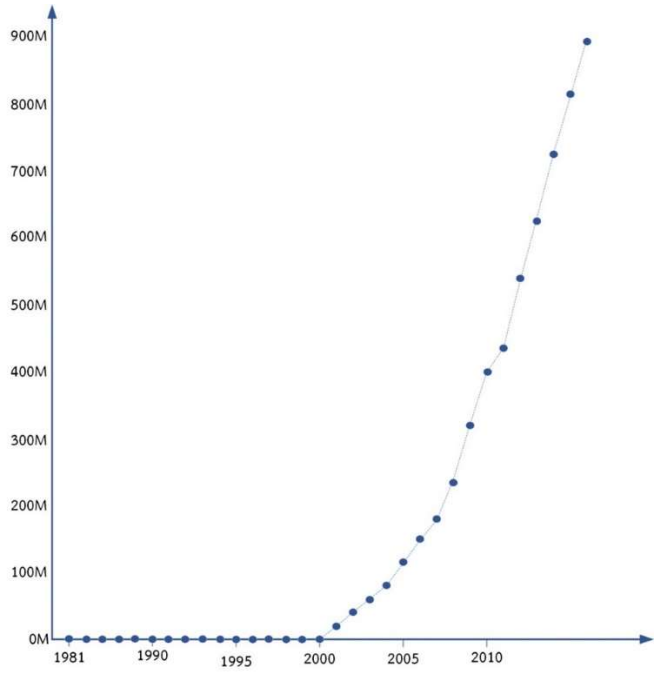
9.1 ประวัติอินเทอร์เน็ต

อินเทอร์เน็ตได้ริเริ่มขึ้นมาจากโครงการอาร์พาเน็ต (Advanced Research Project Agency) ภายใต้กระทรวงกลาโหมของประเทศสหรัฐอเมริกา โดยอาร์พาเน็ตเป็นเครือข่ายแพ็กเก็ตสวิตช์ชิง ที่มีคอมพิวเตอร์ลิงก์เชื่อมโยงถึงกันแบบจุดต่อจุดบนสายสื่อสารความเร็วสูง อาร์พาเน็ตเป็นเครือข่ายที่ถูกใช้เป็นตัวแทนด้านความมั่นคงในการป้องกันประเทศ โดยมีวัตถุประสงค์ เพื่อให้นักวิทยาศาสตร์ที่ทำการวิจัยด้านเทคโนโลยีซึ่งมักพักอาศัยกระจายอยู่ตามพื้นที่ต่างๆ ห่างไกลกัน สามารถแลกเปลี่ยนข้อมูลระหว่างกันได้ภายใต้โครงการวิจัยของทางการทหาร และเพื่อให้เครือข่ายยังคงสามารถสื่อสารใช้งานได้ แม้ว่าจะถูกโจมตีหรือถูกทำลายด้วยอาวุธนิวเคลียร์ก็ตาม (โอภาส เอี่ยมสิริวงศ์, 2559, หน้า 408)

อาร์พาเน็ต คือเครือข่ายระดับประเทศหรือแวน ที่ถูกทดลองใช้งานเมื่อปี ค.ศ. 1969 ประกอบด้วยคอมพิวเตอร์ที่ใช้เป็นศูนย์กลาง 4 เครื่อง แต่ละเครื่องจะตั้งอยู่ที่มหาวิทยาลัยแคลิฟอร์เนียแห่งนครลอสแอนเจลิส มหาวิทยาลัยแคลิฟอร์เนียแห่งนครซานตาบาร์บารา มหาวิทยาลัยยูทาห์ และสถาบันวิจัยสแตนฟอร์ด ซึ่งคอมพิวเตอร์ส่วนกลางทั้งสี่จะทำหน้าที่เป็นโฮสต์ ส่วนคอมพิวเตอร์ลูกข่ายต่างๆ สามารถเข้าถึงข้อมูลระหว่างกันบนสายเครือข่ายความเร็วสูง (Leased Line) จึงทำให้นักวิจัยในโครงการสามารถติดต่อสื่อสารผ่านจดหมายอิเล็กทรอนิกส์ รวมถึงการแลกเปลี่ยนข้อมูลงานวิจัยระหว่างกันได้

ต่อมาหน่วยงานต่างๆ ได้เล็งเห็นประโยชน์จากเครือข่ายดังกล่าวโดยเฉพาะนักวิจัยได้พัฒนาเครือข่ายเพื่อใช้งานในหน่วยของตนและมีการเชื่อมโยงเครือข่ายด้วยโพรโทคอล TCP/IP เป็นครั้งแรกและต่อมาก็ได้เปลี่ยนจากเครือข่ายเฉพาะกลุ่มแม่เป็นเครือข่ายแบบสาธารณะที่ประชาชนทั่วไปสามารถเข้าถึงเพื่อใช้งานได้ เรียกว่า **อินเทอร์เน็ต**

ปัจจุบันอินเทอร์เน็ตได้กลายเป็นเครื่องมือสื่อสารยุคใหม่ ที่มีขอบเขตครอบคลุมทั่วทุกมุมโลก และมีเครื่องคอมพิวเตอร์จำนวนมากที่ผู้ใช้งานได้เชื่อมต่อเข้ากับอินเทอร์เน็ต ดังภาพที่ 9.2 สำหรับประเทศไทยได้ริเริ่มใช้งานอินเทอร์เน็ตเมื่อปี พ.ศ. 2530 และใช้งานได้อย่างสมบูรณ์ด้วยการเชื่อมต่อระหว่างสถาบันอุดมศึกษาในประเทศไทยกับสหรัฐอเมริกาเมื่อปี พ.ศ. 2535 และหลังจากนั้นเป็นต้นมาเครือข่ายอินเทอร์เน็ตได้ขยายการใช้งานในวงกว้างมากขึ้น มีการขยับขยายให้ประชาชนทั่วไปสามารถเข้าถึงเพื่อใช้งานได้โดยมิได้ถูกจำกัดอีกต่อไป ต่อมามีการก่อตั้งบริษัทผู้ให้บริการอินเทอร์เน็ต เช่น อินเทอร์เน็ตแห่งประเทศไทย กสท. โทรคมนาคม TOT และ KFC เป็นต้น ซึ่งบริษัท ISP เหล่านี้จะทำหน้าที่เชื่อมต่อเครือข่ายหรือคอมพิวเตอร์ของเราให้สามารถเชื่อมโยงกับเครือข่ายอินเทอร์เน็ตได้



ภาพที่ 9.2 การเจริญเติบโตของจำนวนคอมพิวเตอร์ที่มีการเชื่อมต่ออินเทอร์เน็ต
ที่มา : (Douglas E. Comer, 2015, P 53)

9.2 การเชื่อมต่ออินเทอร์เน็ต

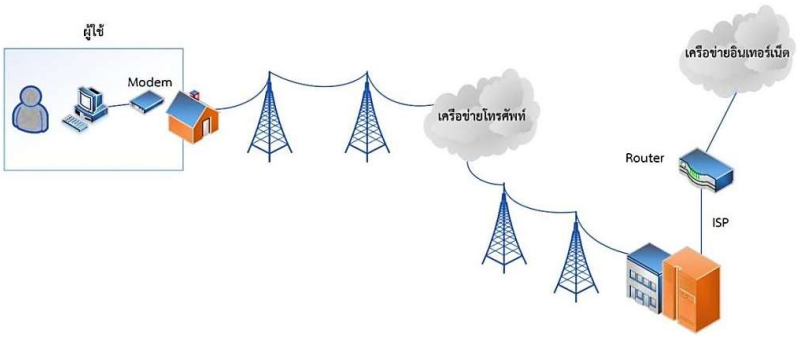
การใช้งานอินเทอร์เน็ตได้รับความนิยมอย่างแพร่หลายในด้านการค้า การทำธุรกิจ การติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และด้านความบันเทิง ทำให้อินเทอร์เน็ตเป็นสิ่งจำเป็นมากขึ้น ปัจจุบันการเชื่อมต่ออินเทอร์เน็ตทำได้หลายรูปแบบ การเชื่อมต่ออินเทอร์เน็ตที่ควรรู้จักมีดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 268-269)

การเชื่อมต่ออินเทอร์เน็ต

ปัจจุบันการเชื่อมต่ออินเทอร์เน็ตทำได้เพียงแค่มีอุปกรณ์ที่เหมาะสมโดยเชื่อมต่อผ่านสายโทรศัพท์ไปยังผู้ให้บริการอินเทอร์เน็ตหรือ ISP ก่อนที่จะเข้าสู่เครือข่ายอินเทอร์เน็ตเพื่อใช้บริการที่ต้องการต่อไป การเชื่อมต่ออินเทอร์เน็ตของผู้ใช้ 2 กลุ่มคือ กลุ่มผู้ใช้อินเทอร์เน็ตจากบ้านและกลุ่มผู้ใช้อินเทอร์เน็ตเครือข่ายในองค์กร ซึ่งจะอธิบายถึงความแตกต่างของการเชื่อมต่อแต่ละรูปแบบ ดังนี้

1. การเชื่อมต่ออินเทอร์เน็ตจากที่บ้าน (Home-to-Internet)

การเชื่อมต่ออินเทอร์เน็ตของผู้ใช้กลุ่มนี้จะมีจุดประสงค์การใช้งานที่หลากหลาย เช่น ความบันเทิง และการศึกษา เป็นต้น หากผู้ใช้ต้องการเชื่อมต่ออินเทอร์เน็ตเพื่อความบันเทิง ควรใช้เทคโนโลยีที่ตอบสนองขนาดของข้อมูลที่ใหญ่กว่าผู้ใช้ทั่วไป ดังนั้น จึงต้องใช้เทคโนโลยีที่มีความเร็วสูง เช่น ADSL เป็นต้น การเชื่อมต่ออินเทอร์เน็ตแบบทั่วไปโดยใช้เครื่องคอมพิวเตอร์ส่วนบุคคลและโมเด็มเชื่อมต่ออินเทอร์เน็ต ดังภาพที่ 9.3



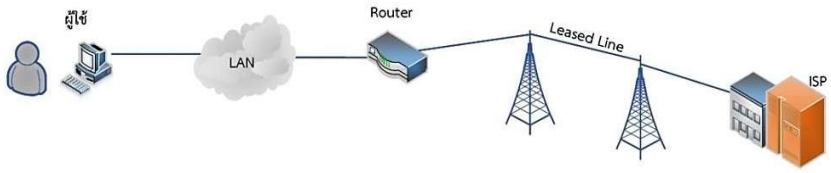
ภาพที่ 9.3 แสดงการเชื่อมต่ออินเทอร์เน็ตจากที่บ้าน

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 268)

จากภาพที่ 9.3 ผู้ใช้จะเชื่อมต่ออินเทอร์เน็ตด้วยโมเด็มผ่านเครือข่ายโทรศัพท์ซึ่งเป็นระบบการขนส่งข้อมูลแบบ Circuit Switching และเชื่อมต่อกับผู้ให้บริการ ISP ก่อนที่จะดำเนินการเชื่อมโยงผู้ใช้เข้ากับเครือข่ายอินเทอร์เน็ตตามที่ร้องขอ เมื่อผู้ใช้ร้องขอบริการผ่านแอปพลิเคชันหรือ Web Browser โดยมีโพรโทคอล HTTP คอยดูแลการเชื่อมโยงระหว่างผู้ใช้กับ Server หลังจากที่ผ่านกระบวนการร้องขอข้อมูลต่างๆ แล้วหน้าจอของ Web Browser ก็จะแสดงข้อมูลของเว็บไซต์หรือบริการที่ผู้ใช้ต้องการ

2. การเชื่อมต่ออินเทอร์เน็ตจากที่ทำงาน (Work-to-Internet)

การเชื่อมต่อของผู้ใช้กลุ่มนี้ส่วนใหญ่จะมีจุดประสงค์ในการติดต่อสื่อสารหรือแลกเปลี่ยนข้อมูล หรือใช้ในการค้นคว้าข้อมูลที่เกี่ยวข้องกับงานที่ตนรับผิดชอบ ทำให้การเชื่อมต่ออินเทอร์เน็ตแตกต่างกันออกไปตามรูปแบบของเครือข่ายภายในองค์กร และนโยบายในการติดต่อสื่อสารผ่านเครือข่าย เช่น องค์กรที่ให้ความสำคัญในการติดต่อสื่อสารกับหน่วยงานในปกครองของตนมากกว่าการติดต่อสื่อสารกับภายนอก เป็นต้น การเชื่อมต่ออินเทอร์เน็ตจากที่ทำงานแสดงได้ดังภาพที่ 9.4



ภาพที่ 9.4 แสดงการเชื่อมต่ออินเทอร์เน็ตจากที่ทำงาน

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 268)

ผู้ใช้จะเข้าใช้บริการเครือข่ายอินเทอร์เน็ตด้วยโดยอาศัยระบบเครือข่ายแลนภายในองค์กรและเชื่อมโยงกับผู้ให้บริการ ISP ด้วย เราท์เตอร์ ซึ่งเป็นองค์ประกอบสำคัญในการเชื่อมโยงเครือข่ายขององค์กรเข้ากับเครือข่ายอินเทอร์เน็ต สื่อกลางในการติดต่อสื่อสารนั้นอาจแตกต่างกัน เช่น สายเช่า และเฟรมรีเลย์ เป็นต้น เมื่อผู้ใช้ต้องการเก็บข้อมูลก็จะร้องขอไปยัง Server ซึ่งมีกระบวนการเหมือนกับการเชื่อมต่ออินเทอร์เน็ตจากบ้าน แต่การใช้บริการบางอย่างจะมีประสิทธิภาพมากกว่า เนื่องจากภายในองค์กรมี Server ที่คอยให้บริการในด้านต่างๆ จึงอำนวยความสะดวกในการใช้งานได้เป็นอย่างดี อีกทั้งยังมีระบบรักษาความปลอดภัยด้วย

9.3 ดีเอ็นเอส

ดีเอ็นเอส (Domain Name System : DNS) เป็นการติดต่อสื่อสารบนเครือข่ายอินเทอร์เน็ตโดยใช้ TCP/IP เพื่อส่งข้อมูลจำเป็นต้องระบุตำแหน่งต้นทางและปลายทางโดยใช้ระบบการตั้งชื่อโดเมนขึ้นมา เพื่อกำหนดชื่อให้กับที่อยู่ดังกล่าว ทำให้การอ้างอิงทำได้สะดวกยิ่งขึ้น

9.3.1 การตั้งชื่อด้วยระบบ DNS

การตั้งชื่อด้วยระบบ DNS จะช่วยให้การจัดการกับเครือข่ายหรือเครื่องคอมพิวเตอร์ที่มีจำนวนมากในเครือข่ายอินเทอร์เน็ตมีความเป็นระเบียบมากยิ่งขึ้น การกำหนดชื่อโดเมนของเว็บไซต์ควรกำหนดให้สื่อความหมายและสอดคล้องกับเนื้อหาภายในเว็บของตน การตั้งชื่อด้วยระบบ DNS แบ่งออกเป็น 3 ส่วน ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 248-252)

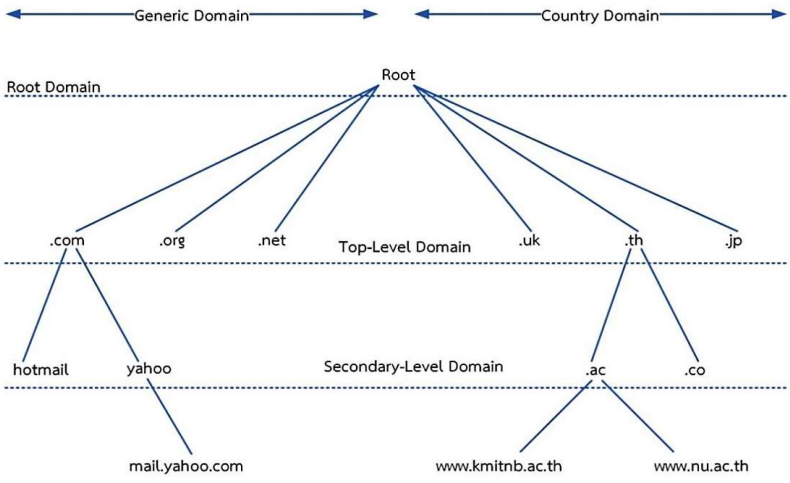
1. Name Resolver เป็นส่วนที่ทำหน้าที่แปลงจากชื่อให้กลายเป็นหมายเลข IP ซึ่งอาจมีซอฟต์แวร์ที่ถูกสร้างขึ้นมากับแอปพลิเคชันที่ใช้งานหรืออาจมีการติดตั้งภายในเครื่อง

Client อยู่แล้วโดยส่วนนี้จะสนับสนุนให้เครื่อง Client ที่ต้องการติดต่อสื่อสารสามารถเชื่อมโยงไปยังเครื่องปลายทางที่มี Domain Name ตามที่ระบุไว้

2. Domain Name Space เป็นส่วนแยกระหว่าง Domain Name หลักและย่อย ซึ่งแต่ละโดเมนจะมีชื่อและมีโดเมนย่อยแยกออกมาได้อีก การเรียกชื่อ Domain Name ทั้งหมดจะใช้เครื่องหมาย “.” คั่นระหว่างแต่ละโดเมน Domain Name Space จะถูกแยกตามระดับของโดเมนตั้งแต่โดเมนหลักที่อยู่บนสุดและโดเมนย่อยที่อยู่ระดับล่างลงมา

3. Name Server เป็นส่วนหนึ่งของเครื่องคอมพิวเตอร์ที่ทำหน้าที่ในการจัดการข้อมูลบางส่วนในระบบ DNS โดย Name Server จะทำหน้าที่ค้นหาโดเมนภายในฐานข้อมูลของตน เมื่อมีการร้องขอมาหรืออาจจะส่งคำร้องขอไปยัง Name Server อื่นที่มีการบันทึกโดเมนที่ตนเองไม่ได้มีการบันทึกไว้ การที่ Name Server มีส่วนของโดเมนตรงกับของตนเองหมายถึง Name Server ดังกล่าวเป็นเจ้าของโดเมนนั้น

การติดต่อสื่อสารกันโดยอาศัย Domain Name นั้นคล้ายกับการระบุที่อยู่ในการส่งจดหมายผ่านทางไปรษณีย์ จำเป็นต้องระบุรายละเอียดที่ชัดเจนและครบถ้วนเช่นกัน โดยจะมีการแบ่งเป็นโดเมนหลักและย่อยซึ่งแต่ละ Domain Name Space นั้นก็สามารถระบุตัวตนหรือที่อยู่ของปลายทางได้มากขึ้นและอาจมีโดเมนย่อยแยกออกมาได้อีกจนกว่าจะได้ที่อยู่ที่ถูกต้อง โครงสร้างของระบบ DNS แสดงดังภาพที่ 9.5



ภาพที่ 9.5 แสดงโครงสร้างของระบบ DNS และตัวอย่าง Domain Name

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 249)

โครงสร้างของระบบ DNS จะแสดงโครงสร้างรูปต้นไม้ ซึ่งมีการแบ่งระดับการแยกโดเมนหลักและรองลดลงตามลำดับ โดยมีองค์ประกอบ ดังนี้

1. Root Domain คือ ระดับสูงสุดของระบบโดเมนที่เป็นความสำคัญในการแยกตัวเป็นหลัก โดยทุกโดเมนจะอยู่ภายใต้ระดับของ Root Domain ทั้งหมด

2. Top-Level Domain คือ ระดับโดเมนรองจาก Root Domain ซึ่งเป็นระดับแรกสุดในการกำหนด Domain Name โดยในระดับนี้จะเป็นโดเมนหลักในการแยกย่อยของโดเมนอื่น

3. Second-Level Domain คือ โดเมนระดับถัดลงมาจากระดับ Top-Level ซึ่งจะเป็นโดเมนที่มีไว้สำหรับบุคคลหรือองค์กรที่ต้องการใช้ Domain name

9.3.2 ประเภทของ DNS

DNS เป็นระบบที่แปลง IP Address ให้อยู่ในรูปแบบข้อความหรือคำที่มีความหมายแทนการใช้ชุดตัวเลข และจำแนกกลุ่มของข้อมูลบนเครือข่ายอินเทอร์เน็ตออกจากกัน เพื่อให้ผู้ใช้สามารถจำและทราบถึงรายละเอียดข้อมูลหรือบริการต่างๆ ที่ผู้ให้บริการนำเสนอต่อผู้ใช้ โดย DNS สามารถแบ่งชื่อโดเมนออกเป็น 3 กลุ่ม คือ ดังนี้

1. โดเมนทั่วไป (Generic Domain)

เป็นโดเมนระดับบนสุดซึ่งเกี่ยวข้องกับองค์กรต่างๆ เช่น หน่วยงานราชการ สถาบันการศึกษา และองค์กรทางธุรกิจ เป็นต้น ชื่อของโดเมนทั่วไปบางชื่อนิยมใช้กันเป็นมาตรฐานโลก แต่บางชื่ออาจมีการใช้ในบางประเทศเท่านั้น ดังตารางที่ 9.1

ตารางที่ 9.1 แสดงรายละเอียดโดเมนทั่วไป

โดเมน	กลุ่ม
.com	องค์กรธุรกิจการค้า (Commercial Organization)
.edu	สถาบันการศึกษา (Educational Organization)
.net	หน่วยงานเครือข่าย (Networking Organization)
.org	องค์กรจัดตั้ง (Organization)
.gov	หน่วยงานรัฐบาลของสหรัฐ (Government Organization)

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 251)

2. โดเมนรหัสประเทศ (Country Domain)

เป็นโดเมนที่ใช้รหัสของประเทศในการจำแนกกลุ่ม ซึ่งใช้ตัวอักษรย่อตามมาตรฐานของ ISO ตามชื่อของแต่ละประเทศ เช่น .th ประเทศไทย และ .jp ประเทศญี่ปุ่น เป็นต้น ส่วนในระดับรองลงมาเป็นการย่อตัวย่อขององค์กรหรือหน่วยงานหรืออาจจะเป็นรหัสแต่ละประเทศ แสดงตัวอย่างโดเมนรหัสประเทศ ดังตารางที่ 9.2

ตารางที่ 9.2 แสดงรายละเอียดโดเมนรหัสประเทศ

โดเมน	ประเทศ
.au	ออสเตรเลีย
.de	เยอรมัน
.fr	ฝรั่งเศส
.jp	ญี่ปุ่น
.kr	เกาหลี
.uk	สหราชอาณาจักร
.th	ไทย

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 251)

3. อินเวอร์สโดเมน (Inverse Domain)

บางครั้งเรียกว่า อาร์พาโดเมน (APPA Domain) เป็นโดเมนที่เรียงลำดับความสำคัญกลับกัน หรือตรงกันข้ามกับโดเมนแบบอื่นๆ โดยจะกำกับด้านท้ายของชื่อโดเมนว่า arpa ซึ่งเป็นชื่อของหน่วยงานที่เริ่มต้นพัฒนา TCP/IP คือ ARPA

9.3.3 DNS Server

ระบบ DNS จำเป็นต้องมีฐานข้อมูลที่คอยเก็บรายชื่อโดเมนไว้ เพื่อใช้ในการจัดการและค้นหาเมื่อมีการร้องขอจาก Client ซึ่งการจัดการดังกล่าวนั้นจะต้องมี Server ค่อยทำหน้าที่นี้โดยเฉพาะ เนื่องจากในบางองค์กรมีหมายเลข IP จำนวนมาก เครื่อง Server ดังกล่าวนี้เรียกว่า Domain Name System Server (DNS Server) หรือเรียกสั้นๆ ว่า Domain Name Server โดยการทำงานของ DNS Server นั้นจะประกอบด้วยฐานข้อมูลและซอฟต์แวร์ที่ช่วยในการตรวจสอบว่า Domain Name นี้ตรงกับหมายเลข IP ใดๆ ซึ่งทุกๆ โดเมนจะต้องมี DNS Server ดูแล

9.3.4 กระบวนการทำงานของ DNS Server

DNS Server การทำงานคล้ายกับการติดต่อสื่อสารด้วยระบบโทรศัพท์ DNS Server มีหน้าที่ในการรอฟังคำสั่งและตอบกลับไปยังผู้ใช้ โดยคำร้องที่ส่งมาเกี่ยวกับการสอบถามที่อยู่ปลายทางที่ผู้ใช้ต้องการติดต่อ Domain Name และ IP Address แต่การตอบกลับไปยัง DNS Server จะมีข้อจำกัดเนื่องจากข้อมูลที่ผู้ใช้ต้องการอาจไม่มีฐานข้อมูลของ DNS Server ก็ได้ จึงต้องส่งคำร้องขอดังกล่าวไปยัง DNS Server ตัวอื่น ซึ่ง DNS Server จะมีการทำงานตอบสนองต่อการร้องขอ ดังนี้

1. DNS Server จะยอมรับการร้องขอจากแอปพลิเคชันที่ต้องการค้นหาจากหมายเลข IP ของ Domain Name

2. DNS Server จะยอมรับคำร้องขอจาก DNS Server อื่นที่ต้องการทราบหมายเลข IP ของ Domain Name

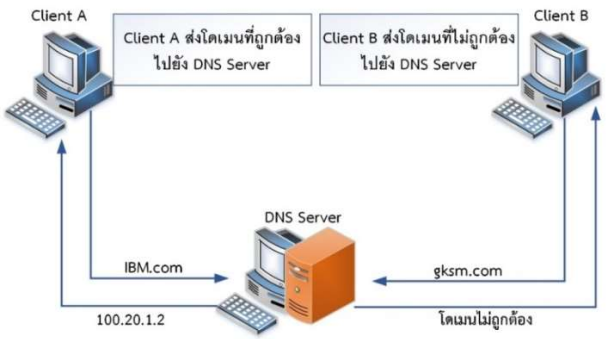
3. เมื่อ DNS Server ได้รับคำร้องขอ จะตอบสนอง ดังนี้

3.1 DNS Server จะตอบสนองต่อคำร้องขอได้เมื่อหมายเลข IP ของโดเมนดังกล่าวเป็นหมายเลขที่ DNS Server รู้จัก

3.2 DNS Server สามารถติดต่อ DNS Server อื่นเพื่อระบุหมายเลข IP ที่ผู้ใช้ร้องขอได้

3.3 หากหมายเลข IP ที่ผู้ร้องขอมา DNS Server ไม่มีข้อมูลเก็บไว้ DNS Server ก็จะส่งหมายเลข IP ของ DNS Server อื่นที่อาจมีหมายเลข IP ดังกล่าวแทน

3.4 DNS Server จะตอบกลับข้อความแสดงข้อความผิดพลาด หากผู้ใช้ส่งคำร้องที่มีข้อมูลไม่ถูกต้อง หรืออาจเป็นข้อมูลที่ไม่ปรากฏอยู่ในฐานข้อมูลเลย กระบวนการทำงานแบบง่ายๆ ของ DNS Server แสดงดังภาพที่ 9.6



ภาพที่ 9.6 แสดงกระบวนการทำงานของ DNS Server

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 252)

จากภาพที่ 9.6 เมื่อเครื่อง Client A และ B ต้องการทราบข้อมูลที่ DNS Server จะส่งคำร้องไปยัง DNS Server โดย Client A ต้องการทราบหมายเลข IP ของ IBM.com ก็จะส่งคำร้องไปสอบถาม DNS Server และหาก DNS Server ทราบตำแหน่งก็จะตอบกลับด้วยหมายเลข IP ของโดเมน DNS Server จะตอบกลับมาด้วยหมายเลข IP ของ IBM.com คือ 100.20.1.2 ในกรณี Client B ต้องการทราบหมายเลข IP ของ gksm.com ก็จะทำการส่งคำร้องไปเช่นกัน แต่โดเมนดังกล่าวไม่ปรากฏอยู่ในฐานข้อมูลของ DNS Server ดังนั้น DNS Server จึงตอบกลับมาให้ Client B ทราบว่าไม่มีโดเมนดังกล่าว ในบางกรณี DNS Server ติดต่อกันเองทำให้ทราบโดเมนของ DNS Server อื่นที่เกี่ยวข้องกับหมายเลข IP ของโดเมน gksm.com ส่งผลให้ DNS Server อาจส่งโดเมนนั้นกลับไปยังผู้ใช้ด้วย

แอปพลิเคชันในเครื่อง Client เมื่อทำการร้องขอมายัง DNS Server จะมีกระบวนการทำงาน ดังนี้

1. แอปพลิเคชันที่ต้องการทราบหมายเลข IP จะทำการค้นหาจากข้อมูลที่บันทึกไว้ภายในเครื่อง Client ก่อน หากไม่พบก็จะทำการส่ง Domain Name ที่ต้องการทราบไปยัง DNS Server

2. เครื่อง Client จะทำการเก็บข้อมูล UDP ไปยัง DNS Server ที่อยู่ใกล้ที่สุด

3. DNS Server ที่ได้รับคำร้องขอจาก Client นั้นจะค้นหาหมายเลข IP ของโดเมนนั้นและส่งกลับไป

4. เมื่อเครื่อง Client ได้รับหมายเลข IP ดังกล่าวก็จะส่งไปยังแอปพลิเคชันที่ร้องขอมาเพื่อให้ดำเนินการอื่นๆ ต่อไป

9.4 ทีซีพี/ไอพี

ทีซีพี/ไอพี (Transmission Control Protocol/Inter Protocol : TCP/IP) เป็นโพรโทคอลสำคัญที่ใช้ในการเชื่อมโยงและติดต่อสื่อสารในเครือข่ายอินเทอร์เน็ต โดยทำหน้าที่เป็นตัวกลางในการติดต่อสื่อสารทั้งภายในและภายนอกองค์กร TCP/IP ได้รับความนิยมอย่างสูง เนื่องจากเป็นโพรโทคอลที่เป็นกลาง ทำให้ระบบที่แตกต่างกันสามารถติดต่อสื่อสารกันได้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 253-257)

9.4.1 การแบ่งชั้นของทีซีพี/ไอพี

TCP/IP มีทั้งหมด 4 ชั้น คือ ชั้นติดต่อสื่อสารระหว่างแอปพลิเคชัน (Application Layer) ชั้นติดต่อระหว่างโฮสต์ (Host-to-Host Layer) ชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ต (Internet Layer) และชั้นควบคุมการติดต่อระดับเครือข่าย (Network Access Layer) ซึ่งมีรายละเอียด ดังนี้

ชั้นที่ 4 ชั้นติดต่อระหว่างแอปพลิเคชัน (Application Layer)

ชั้นนี้จะมีโพรโทคอลที่ดูแลและจัดการเกี่ยวกับการติดต่อไปยังแอปพลิเคชัน ซึ่งเป็นส่วนที่ติดต่อกับผู้ใช้ โพรโทคอลที่สำคัญ มีดังนี้

1. SMTP (Simple Mail Transfer Protocol) เป็นโพรโทคอลที่คอยสนับสนุนการส่งจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ตหรือ E-mail โดย STMP จะช่วยให้ผู้ใช้ทั้งสองฝ่ายสามารถเปลี่ยนแปลงข้อมูลผ่านทาง E-mail ได้ แม้ว่าผู้ใช้ทั้งสองจะอยู่ต่างระบบกันก็ตาม STMP สามารถสนับสนุนการส่งข้อมูลไปยังผู้รับตั้งแต่หนึ่งคนขึ้นไปได้ สามารถบรรจุข้อมูลได้หลายรูปแบบ เช่น ข้อความ เสียง ภาพ และวีดีโอ เป็นต้น

2. FTP (File Transfer Protocol) เป็นโพรโทคอลมาตรฐานที่สนับสนุนการถ่ายโอนข้อมูลหรือไฟล์ระหว่างคอมพิวเตอร์ 2 เครื่อง ซึ่งการถ่ายโอนข้อมูลนั้นต้องมีการระบุตัวตนเพื่อให้สามารถเชื่อมต่อและสร้างช่องทางในการถ่ายโอนข้อมูล เช่น ชื่อที่ใช้ในการเข้าระบบและรหัสผ่าน เป็นต้น เมื่อมีการเชื่อมต่อเกิดขึ้นคอมพิวเตอร์อีกเครื่องก็จะทำการตรวจสอบและระบุตัวตนของเครื่องที่ต้องการเข้าระบบ หากการยืนยันตัวตนถูกต้อง ก็สามารถดำเนินการถ่ายโอนข้อมูลได้ สำหรับโพรโทคอล TCP จะทำหน้าที่ในการสร้างเส้นทางการเชื่อมต่อระหว่างเครื่องทั้งสองและเส้นทางในการถ่ายโอนข้อมูล

3. HTTP (Hypertext Transfer Protocol) เป็นโพรโทคอลที่ใช้ในการติดต่อข้อมูลบนอินเทอร์เน็ตที่จะถูกใช้งานโดย WWW (World Wide Web) โดย HTTP จะเป็นตัวรับส่งข้อมูลหรือไฟล์ภาษา HTML ที่ใช้ในการแสดงหน้าเว็บเพจ HTTP จะทำการร้องขอโดยการส่งข้อมูลทั้งหมดหรือบางส่วนไปยังเครื่อง Server หลังจากนั้นเครื่อง Server จะทำการประมวลผลแล้วตอบสนองตามข้อมูลที่ได้รับมา ในอดีตข้อมูลที่ใช้แสดงผลหน้าเว็บเพจอาจต้องประมวลผลจากฝั่งของ Server เท่านั้น ทำให้การแสดงผลช้า แต่ในปัจจุบันเครื่องฝั่งผู้ใช้สามารถเก็บข้อมูลที่จำเป็นในการแสดงผลหน้าเว็บเพจไว้เกือบทั้งหมด และสามารถประมวลผลเองได้ ทำให้ Server แบกภาระน้อยลง ส่งผลให้การแสดงผลมีความรวดเร็วมากขึ้น การติดต่อระหว่างผู้ใช้กับ Server จะใช้ผ่านโปรแกรมที่เรียกว่า Web Browser

ชั้นที่ 3 ชั้นติดต่อระหว่างโฮสต์ (Host-to-Host Layer)

ชั้นติดต่อระหว่างโฮสต์ (Host-to-Host Layer) จะคอยดูแลเกี่ยวกับการส่งข้อมูล ซึ่งที่มีโพรโทคอลที่สำคัญ ดังนี้

1. UDP (User Datagram Protocol) เป็นโพรโทคอลที่คอยดูแลและให้บริการในการส่งข้อมูลโดยเรียกข้อมูลดังกล่าวว่า ดาต้าแกรม (Datagram) การส่งข้อมูล UDP เป็นการส่งแบบ Connectionless คือ จะไม่สร้างเส้นทางขนส่งข้อมูลก่อนทำให้ไม่สามารถทราบสถานะการเดินทางของข้อมูลได้ ทำให้ขาดความน่าเชื่อถือ แต่ก็มีข้อดี คือ จะมีประสิทธิภาพสูง หากข้อมูลมีขนาดเล็ก เนื่องจากสามารถส่งข้อมูลได้ทันทีโดยไม่ต้องเสียเวลาเพื่อสร้างการเชื่อมต่อ ดังนั้น UDP จึงนิยมใช้กับการแพร่กระจายข้อมูล (Broadcast) โดยที่ข้อมูล UDP สร้างขึ้น เป็นแพ็กเก็ตข้อมูลที่เรียกว่า User Datagram

2. TCP (Transmission control Protocol) เป็นโพรโทคอลที่ดูแลและให้บริการในการส่งข้อมูลเหมือนกับ UDP แต่ TCP จะใช้การส่งข้อมูลแบบ Connection-Oriented ซึ่งต้องสร้างเส้นทางในการขนส่งข้อมูลก่อน จึงมีความน่าเชื่อถือมากกว่า UDP โดย TCP สามารถรับรองได้ว่าข้อมูลที่ส่งไปนั้นถึงปลายทางอย่างแน่นอน TCP จะแบ่งข้อมูลที่ทำการส่งทั้งหมดออกเป็นแพ็กเก็ตย่อยๆ สำหรับการเชื่อมต่อ และแจ้งให้ปลายทางทราบว่าต้องการส่งข้อมูล ปลายทางก็จะตอบกลับพร้อมส่งข้อมูลหรือรหัสที่จำเป็นในการส่งข้อมูล เมื่อต้นทางได้รับการตอบกลับดังกล่าวก็จะส่งข้อมูลกลับมายังปลายทาง เพื่อยืนยังการเชื่อมต่อหลังจากติดต่อเพื่อขอสร้างเส้นทางเสร็จสมบูรณ์ ต้นทางก็จะเริ่มทำการขนส่งข้อมูลผ่านเส้นทางดังกล่าว เมื่อการขนส่งสิ้นสุดลงก็จะยกเลิกเส้นทางนั้น ดังนั้น การส่งข้อมูลในครั้งต่อไปจึงจำเป็นต้องสร้างเส้นทางขึ้นใหม่

ชั้นที่ 2 ชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ต (Internet Layer)

ชั้นนี้มีโพรโทคอลที่เกี่ยวข้องคือ IP, RARP, ARP, ICMP และ IGMP ซึ่งมีรายละเอียด ดังนี้

1. IP (Internet Protocol) เป็นโพรโทคอลสำคัญที่คอยรับข้อมูลหรือคำสั่งจากโพรโทคอลที่อยู่ระดับชั้นสูงกว่า และทำงานร่วมกับโพรโทคอล TCP โดย IP จะมีหน้าที่รับผิดชอบในการหาเส้นทางให้กับแพ็กเก็ตข้อมูลที่ส่งมาจากชั้นที่อยู่สูงกว่า การขนส่งของ IP นั้นจะเป็นแบบ Connectionless ซึ่งไม่จำเป็นต้องมีการติดต่อเพื่อสร้างเส้นทางก่อนการส่ง ทำให้มีความน่าเชื่อถือน้อยและไม่มีการรับประกันว่าข้อมูลจะถึงปลายทาง สำหรับข้อมูล IP มีหน้าที่รับผิดชอบนั้นเป็นแพ็กเก็ตข้อมูลที่เรียกว่า Datagram ซึ่งภายในประกอบด้วยส่วนของข้อมูลและ

ส่วนหัว โดยส่วนหัวมีขนาดตั้งแต่ 20-60 bytes มีข้อมูลที่จำเป็นบรรจุภายใน เช่น เวอร์ชันของโพรโทคอล ข้อมูลบอกความยาวของส่วนหัว (Header Length) ข้อมูลบอกความยาวของแพ็กเก็ต (Total Length), IP Address ต้นทาง (Source IP Address) และ IP Address ปลายทาง (Destination IP Address) เป็นต้น

2. ARP (Address Resolution Protocol) เป็นโพรโทคอลที่มีหน้าที่รับผิดชอบการติดต่อสื่อสารภายในเครือข่ายเดียวกันหรือภายในแลน โดยใช้หมายเลข Network Card หรือ NIC (Network Interface Card) ซึ่งเป็นที่อยู่ของแต่ละเครื่องในระดับกายภาพ โดย ARP จะทำการค้นหาหมายเลขเครื่องด้วยการกระจายข้อมูล (Broadcast) ไปยังทุกเครื่องที่อยู่ในเครือข่ายเดียวกันเมื่อพบเครื่องที่หมายเลขตรงกับข้อมูลที่ส่งมาก็จะตอบกลับไปยังเครื่องที่ร้องขอ หลังจากนั้นทั้งสองเครื่องก็จะสามารถสื่อสารกันได้โดยตรง ARP จะมี IP Address ของเครื่องที่ต้องการจึงจะสามารถค้นหาเครื่องดังกล่าวได้โดยจะได้รับหมายเลข MAC Address ตอบกลับมาเพื่อใช้ในการติดต่อกัน

3. RARP (Reverse Address Resolution Protocol) เป็นโพรโทคอลที่มีหน้าที่เหมือนกับ ARP แต่ RARP จะใช้วิธีติดต่อกับคอมพิวเตอร์ปลายทางด้วย MAC Address สำหรับกระบวนการทำงานก็คล้ายกับ ARP แตกต่างเพียงข้อมูลที่ใช้ในการติดต่อเท่านั้น

4. ICMP (Internet Control Message Protocol) เป็นโพรโทคอลที่ทำหน้าที่เกี่ยวกับการควบคุมข้อความที่เกิดขึ้นในระหว่างการติดต่อสื่อสารในเครือข่าย ซึ่งจะรายงานปัญหาที่เกิดขึ้นกลับมายังผู้ส่ง แต่การส่งข้อมูลของ ICMP เป็นแบบ Connectionless ซึ่งข้อความที่ส่งมานั้นไม่มีการรับประกันว่าจะมาถึงปลายทางได้อย่างแน่นอน ข้อความดังกล่าวอาจสูญหายระหว่างทางก็เป็นไปได้ โดย ICMP จะรายงานเหตุการณ์ที่เกิดขึ้นในระหว่างการส่งข้อมูล เช่น รายงานความหนาแน่นของข้อมูล เพื่อให้ผู้ใช้ทราบถึงความหนาแน่นของข้อมูลที่มีมากเกินไปหรือไม่ รายงานระยะเวลาการใช้แพ็กเก็ต หากแพ็กเก็ตใช้เวลาในการเดินทางไปยังปลายทางเกินกว่าเวลาที่กำหนดแล้วแพ็กเก็ตนั้นจะต้องถูกปล่อยทิ้งไปซึ่งทำซึ่งจำเป็นต้องแจ้งให้ผู้ใช้ทราบด้วย เป็นต้น

5. IGMP (Internet Group Management Protocol) เป็นโพรโทคอลที่ทำหน้าที่ในการแจ้งและรายงานข้อมูลให้กับกลุ่ม IP Address เป็นสมาชิกของกลุ่ม Multicast ซึ่งเป็นการส่งข้อมูลแบบต่อแบบหนึ่งต่อหลายเครื่อง (One-to-Many) โดยจะแจ้งข้อมูลดังกล่าวแก่เราท์เตอร์ที่อยู่ภายในเครือข่าย เพื่อให้เครือข่ายสามารถรองรับการติดต่อรูปแบบดังกล่าวได้

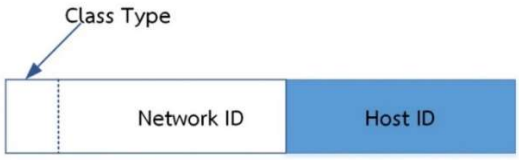
IGMP ถูกออกแบบมาให้สนับสนุนการทำงานของเราท์เตอร์เพื่อระบุเครื่องต่างๆ ที่อยู่ภายในกลุ่มของการติดต่อแบบ Multicast

ชั้นที่ 1 ชั้นควบคุมการติดต่อระดับเครือข่าย (Network Access Layer)

เป็นชั้นที่คอยดูแลการติดต่อสื่อสารในระดับเครือข่ายของอุปกรณ์ต่างๆ ที่จำเป็นในการเชื่อมต่อและสัญญาณที่ใช้ในอุปกรณ์นั้น

9.5 ไอพีแอดเดรส

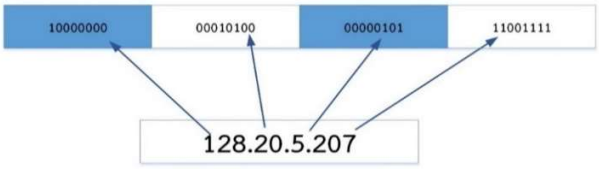
ในเครือข่ายอินเทอร์เน็ตจำเป็นต้องมีการระบุที่อยู่โดยการใช้โพรโทคอล IP การระบุที่อยู่เฉพาะของอุปกรณ์หรือโหนดต่างๆ ภายในเครือข่ายสามารถทำได้โดยการใช้หมายเลข IP Address ซึ่งมีหมายเลขที่อยู่ในชั้นติดต่อระดับเครือข่ายหากอยู่ภายในเครือข่ายเดียวกันจะต้องมีหมายเลขไม่ซ้ำกันและหมายเลข IP นี้ ยังช่วยในการแบ่งกลุ่มของอุปกรณ์หรือหน่วยต่างๆ ภายในเครือข่ายได้ปัจจุบันใช้ IPv4 หรือ IPv6 และมีโครงสร้างดังภาพที่ 9.7 (สุธี พงศา-สกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 257-259)



ภาพที่ 9.7 แสดงโครงสร้างของ IP Address

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 257)

การระบุชั้นที่อยู่นั้นจะแบ่งกลุ่มของหมายเลขดังกล่าวด้วยวิธีการที่เรียกว่า Dotted Decimal Natation ซึ่งเป็นการเปลี่ยนแปลง IP Address ของ IPv4 ที่มีทั้งหมด 32 บิต ให้สามารถอ่านและทำความเข้าใจได้ง่ายขึ้นวิธีการดังกล่าวจะแบ่งการอ่านเลขทั้ง 32 บิต เป็น 4 ชุด ชุดละ 8 บิต ซึ่งหมายเลขที่แปลงมาจาก IP Address ของแต่ละชุดนั้นจะใช้คั่นด้วยเครื่องหมายจุด โดยแปลงเลขฐานสองจำนวน 8 บิต ให้เป็นเลขฐานสิบ จะได้ IP Address ที่สามารถอ่านและจดจำได้ง่ายขึ้นดังภาพที่ 9.8



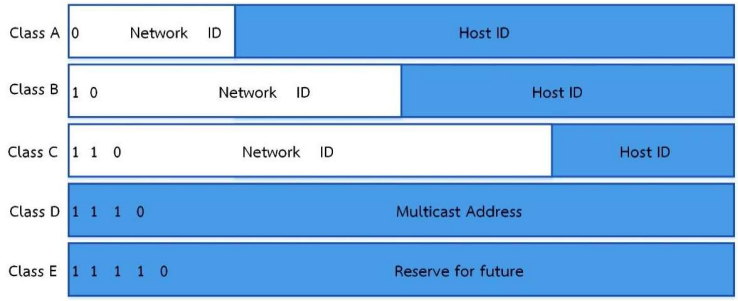
ภาพที่ 9.8 แสดงวิธีการ Dotted Decimal Natation

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 258)

นอกจากนี้ IP Address ยังมีการแบ่งออกเป็นหลายระดับซึ่งในแต่ละระดับจะมีรูปแบบการนำไปใช้งานและรูปแบบโครงสร้างของ IP Address ที่แตกต่างกันด้วย

9.5.1 การจำแนกระดับของ IP Address

รูปแบบโครงสร้างของ IPv4 แบ่งได้เป็น 5 ระดับ แต่ละระดับจะมีความยาวของจำนวนบิตที่แตกต่างกัน โดยแต่ละระดับถูกนำไปใช้ในองค์กรที่มีขนาดหรือความจำเป็นต้องการจำนวนอุปกรณ์ในเครือข่ายที่แตกต่างกันดังภาพที่ 9.9



ภาพที่ 9.9 แสดงรูปแบบโครงสร้างของ IP Address แต่ละระดับ

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 258)

รายละเอียดในแต่ละระดับมีดังนี้

1. Class A มีรูปแบบ คือ บิตแรกเป็นเลข 0 เท่านั้น โดย 8 บิตแรกจะทำหน้าที่เป็นหมายเลขเครือข่าย (Network ID) ซึ่งหมายความว่า Class A จะมีเครือข่ายได้ 128 เครือข่าย คือเครือข่ายที่มี Network ID เท่ากับ 0-127 ไม่นับหมายเลขเครือข่าย 0 และ 127 (ถูกจองไว้) จึงมีทั้งหมด 126 เครือข่าย สำหรับ 24 บิตที่เหลือจะเป็นหมายเลขของเครื่อง Host (Host ID) ซึ่งจะใช้ได้ตั้งแต่ 1.0.0.0 ถึง 126.255.255.255 เมื่อสังเกต พบว่า จำนวนเครื่อง Host จะมีค่อนข้างมากแต่จำนวนเครือข่ายจะมีน้อย ดังนั้น IP Address ใน Class A จึงไม่

เหมาะสมกับเครือข่ายที่มีขนาดใหญ่ที่ประกอบด้วยเครือข่ายเชื่อมต่อกัน เช่น เครือข่ายอินเทอร์เน็ต เป็นต้น

2. Class B สองบิตแรกจะนำไปใช้ 1 และ 0 โดย 16 บิตแรกใช้ระบุหมายเลขเครือข่ายและอีก 16 บิตที่เหลือเป็นหมายเลขของเครื่อง Host ซึ่งจะได้ IP Address ตั้งแต่ 128.0.0.0 ถึง 191.255.255.255 โดยหมายเลขเครือข่ายจะมีได้ทั้งหมด 16,382 เครือข่าย และในแต่ละเครือข่ายของหมายเลขเครื่อง Host จะมีจำนวน 65,534 เครื่อง

3. Class C ใช้ 3 บิตแรก เป็น 110 และใช้ 24 บิตแรก เป็นหมายเลขของเครือข่าย บิตที่เหลืออีก 8 บิต เป็นหมายเลขของเครื่อง Host ซึ่งจะได้ IP Address ตั้งแต่ 192.0.0.0 ถึง 223.255.255.255 ทำให้มีการทำให้มีจำนวนเครือข่ายมากแต่มีจำนวนเครื่อง Host น้อยคือ 254 เครื่องเท่านั้น

4. Class D ใช้ 4 บิตแรกเป็น 1110 ซึ่งเป็น IP Address ที่ใช้สำหรับการ Multicast โดยใช้ในการขนส่งข้อมูลไปยังปลายทางหลายเครื่อง ซึ่งแต่ละเครื่องจะอยู่คนละเครือข่ายกัน ส่วน 28 บิตที่เหลือ จะเป็นหมายเลขของ Multicast (Multicast Address) จึงมี IP Address ตั้งแต่ 224.0.0.0 ถึง 239.255.255.255

5. Class E ใช้ 5 บิตแรกเป็น 11110 เป็น IP Address ที่สำรองไว้ในอนาคต ปัจจุบันยังไม่มีการนำมาใช้งานจริง Class E มี IP Address ตั้งแต่ 240.0.0.0 ถึง 247.255.255.255

จากที่กล่าวมาทั้งหมด IP Address มีการสงวนบางหมายเลขไว้ใช้ในกรณีพิเศษ เช่น 255.255.255.255 จะสงวนไว้ใช้กับการกระจายของข้อมูล (Broadcast) เป็นต้น เช่น IP Address 190.9.255.255 จะมีหน้าที่ในการส่งข้อมูลแบบกระจายไปยังเครื่อง Host ทั้งหมดที่อยู่ในเครือข่ายเป็น 190.9.X.X เท่านั้น เป็นต้น

9.5.2 IPv6

เนื่องจากการขยายตัวและความนิยมในการใช้งานเครือข่ายอินเทอร์เน็ตมีเพิ่มมากขึ้นทำให้มีการคิดค้นและพัฒนา IP ในเวอร์ชันใหม่ขึ้นมาแทนที่ IPv4 ซึ่งมีข้อเสียคือหมายเลขต้องไม่ซ้ำกัน ทำให้การคาดการณ์ว่า IP Address ของ IPv4 อาจไม่พอต่อความต้องการที่เพิ่มขึ้นอย่างรวดเร็ว จึงได้มีการพัฒนา IPv6 ขึ้นเพื่อนำมาใช้งานในอนาคต และสามารถทำงานร่วมกับ IPv4 ข้อดีของ IPv6 มีดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 259-260)

1. มีขนาดในการเก็บ IP Address เพิ่มมากขึ้น จากเดิมที่ IPv4 ใช้เป็น 32 บิต แต่ IPv6 จะใช้ทั้งหมด 128 บิต ทำให้สามารถรองรับปริมาณของ IP Address ที่มากขึ้นได้

2. IPv6 ปรับเปลี่ยนรูปแบบข้อมูลส่วนหัว (Header) ขึ้นใหม่ โดยสามารถสนับสนุนการหาเส้นทางของเราท์เตอร์ได้ดีมากขึ้น

3. มีการเพิ่ม Flow Label เพื่อช่วยในการทำงานและสนับสนุนข้อมูลที่มีลักษณะต่อเนื่อง (Streaming) เช่น ข้อมูลเสียงและข้อมูลวีดีโอแบบ Real-time

4. สามารถสนับสนุนการรักษาความปลอดภัยของข้อมูล เนื่องจากมีการเพิ่มฟังก์ชันในการเข้ารหัสและระบุตัวตนของข้อมูลให้มีประสิทธิภาพและปลอดภัยขึ้น

5. รองรับเทคโนโลยีใหม่ๆ ในอนาคตหากมีเทคโนโลยีใหม่หรือแอปพลิเคชันที่ต้องการเพิ่มเติมส่วนต่างๆ ของโพรโทคอลก็สามารถทำได้

IPv6 แบ่งการใช้งาน IP Address ได้ 3 ประเภท คือ

1. Unicast Address เป็นการระบุเครื่องคอมพิวเตอร์ที่มีหมายเลข IP Address ตามที่กำหนดเท่านั้น

2. Anycast Address เป็น IP Address ที่กำหนดให้กับกลุ่มของเครื่องคอมพิวเตอร์ โดยจะแบ่งกลุ่มออกเป็นเซตที่เรียกว่า Anycast Address ซึ่งเป็นการส่งผู้ส่งรายเดียวกับผู้รับหลายราย โดยจะเป็นผู้รับที่อยู่ใกล้ที่สุด เมื่อข้อมูลถูกส่งไปยังเครื่องใดเครื่องหนึ่งในเซตนั้น เครื่องที่อยู่ภายในเซตเดียวก็จะได้รับข้อมูลดังกล่าวทุกเครื่อง โดย Anycast Address เปรียบเสมือนคำนำ หน้าชื่อ (Prefix Address) หากมีคำนำหน้าชื่อเหมือนกันแสดงว่าอยู่ในเซตเดียวกัน

3. Multicast Address เป็น IP Address ที่ถูกกำหนดให้กับกลุ่มเหมือนกับ Anycast Address ซึ่งจะมีลักษณะการส่งข้อมูลคล้ายกับการ Broadcast แต่ Multicast จะส่งไปยังเครื่องทุกเครื่องที่อยู่ในกลุ่มเท่านั้น กล่าวคือ Broadcast จะส่งแบบผู้ส่งรายเดียวได้ทั้งหมด (one-to-all) แต่ Multicast จะส่งแบบผู้ส่งรายเดียวผู้รับหลายราย (one-to-many) โดยข้อมูลจะถูกส่งไปยังเครื่องปลายทางที่อยู่ภายในกลุ่มเดียวกันเท่านั้น

จากที่กล่าวมาจะเห็นได้ว่า IPv6 มีการพัฒนารูปแบบและการระบุที่อยู่ของเครื่องคอมพิวเตอร์ที่ใช้งานผ่านเครือข่ายอินเทอร์เน็ตได้อย่างมีประสิทธิภาพมากขึ้น สามารถรองรับการพัฒนาและขยายตัวของเครือข่ายอินเทอร์เน็ตได้เป็นอย่างดี ปัจจุบัน IPv6 ถูกนำมาใช้แทนที่ IPv4 อย่างสมบูรณ์

9.6 สรุป

อินเทอร์เน็ตเป็นเครือข่ายที่มีขนาดใหญ่ประกอบไปด้วยผู้ให้บริการหลายระดับ โดยเรียกผู้ให้บริการทางด้านอินเทอร์เน็ตว่า ไอเอสพี (ISP) แบ่งออกเป็น 3 ระดับ คือ ระดับประเทศ ระดับภูมิภาคและระดับท้องถิ่น การเชื่อมต่ออินเทอร์เน็ตมีการพัฒนามาตั้งแต่อดีตจนถึงปัจจุบัน ทั้งการเชื่อมต่ออินเทอร์เน็ตแบบพื้นฐานที่ได้รับความนิยมในอดีต ก็คือการเชื่อมต่อผ่านโมเด็ม ซึ่งมีความเร็วสูงสุดเพียง 56 K ทำให้มีการพัฒนาเทคโนโลยีต่างๆ เพื่อให้การเชื่อมต่อทำได้รวดเร็วยิ่งขึ้น เกิดการเชื่อมต่อแบบ DSL ซึ่งเทคโนโลยีประเภทนี้มีความเร็วในการขนส่งข้อมูลที่สูงกว่าโมเด็มจึงได้รับความนิยมอย่างสูง นอกจากนี้ ADSL ก็เป็นอีกหนึ่งเทคโนโลยีที่ได้รับความนิยมโดยเฉพาะกับผู้ใช้ทั่วไป เนื่องจากมีอัตราการรับข้อมูลค่อนข้างสูง ในขณะที่อัตราการส่งข้อมูลต่ำกว่า

ระบบ DNS ช่วยให้การเข้าถึงข้อมูลต่างๆ บนเครือข่ายอินเทอร์เน็ตทำได้ง่ายกว่าการใช้ IP Address เนื่องจากในเครือข่ายอินเทอร์เน็ตมีผู้ให้บริการข้อมูลอยู่เป็นจำนวนมาก การตั้งชื่อโดเมนจะช่วยให้ผู้ใช้สามารถจดจำและเชื่อมโยงไปยังผู้ให้บริการดังกล่าวได้ง่ายกว่า การจำแนกกลุ่มของโดเมนออกเป็น 3 ประเภท คือ โดเมนทั่วไป โดเมนรหัสประเทศ และอินเวอร์สโดเมน

TCP/IP โพรโทคอลพื้นฐานที่ใช้ในการติดต่อสื่อสารระหว่างกันผ่านเครือข่ายอินเทอร์เน็ต ประกอบด้วยชุดโพรโทคอลที่ทำหน้าที่ดูแลในระดับชั้นต่างๆ หลายตัวด้วยกัน โดยในชั้นติดต่อระดับแอปพลิเคชันจะมีโพรโทคอลที่สำคัญ คือ SMTP FTP และ HTTP ส่วนชั้นติดต่อระหว่างโฮสต์จะมีโพรโทคอลที่สำคัญคือ UDP และ TCP และชั้นติดต่อระดับเครือข่ายอินเทอร์เน็ตนั้นจะมีโพรโทคอลที่สำคัญ เช่น IP ARP RARP ICMP และ IGMP เป็นต้น โพรโทคอลแต่ละตัวก็จะมีหน้าที่รับผิดชอบแตกต่างกันไปโดยจะสอดคล้องกับการทำงานของแต่ละระดับชั้นซึ่งคอยอำนวยความสะดวกและสนับสนุนการทำงานของ TCP/IP ให้เป็นไปอย่างราบรื่น

ในการติดต่อสื่อสารผ่านเครือข่ายอินเทอร์เน็ตจำเป็นต้องใช้การระบุที่อยู่ของเครือข่ายเพื่อยืนยันตัวตนให้เครือข่ายอินเทอร์เน็ตทราบและอนุญาตให้เข้าใช้บริการได้ด้วย IP Address ซึ่งแต่ละเครื่องที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตนั้นจะต้องมี IP Address ที่ไม่ซ้ำกันดังนั้น IP Address จึงมีความสำคัญต่อการเข้าใช้บริการผ่านเครือข่ายอินเทอร์เน็ต ซึ่งในปัจจุบันการขยายตัวและปริมาณผู้ใช้งานเครือข่ายอินเทอร์เน็ตเพิ่มขึ้นอย่างรวดเร็วทำให้ IP Address ที่ใช้อยู่คือ IPv4 อาจไม่เพียงพอต่อการขยายตัวดังกล่าว จึงต้องมีการพัฒนา IPv6 ขึ้นมาทดแทนโดยเพิ่มขนาดของไอพีแอดเดรสจาก 32 บิตเป็น 128 บิต เพื่อให้เพียงพอต่อความต้องการ

บทที่ 10
ความรู้เบื้องต้นเกี่ยวกับโพรโทคอลทีซีพี/ไอพี

โพรโทคอล เป็นข้อตกลงที่ใช้ควบคุมการสื่อสารข้อมูลภายในเครือข่าย โพรโทคอลมีลักษณะเช่นกับภาษาที่ใช้ในการสื่อสารของมนุษย์ที่ต้องใช้ภาษาเดียวกันจึงจะสามารถสื่อสารกันได้ โดยทั่วไปเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่ใช้โพรโทคอลชนิดเดียวกันเท่านั้นจึงจะสามารถติดต่อและส่งข้อมูลระว่างอุปกรณ์ได้ โพรโทคอลที่ถูกพัฒนาเพื่อใช้ในการแลกเปลี่ยนข้อมูลบนเครือข่ายอินเทอร์เน็ต คือ โพรโทคอลทีซีพี/ไอพี (Transmission Control Protocol/ Internet Protocol : TCP/IP) เป็นโพรโทคอลที่ทำให้คอมพิวเตอร์ภายในระบบเครือข่ายอินเทอร์เน็ตสามารถเชื่อมโยงเข้าหากันและติดต่อสื่อสารแลกเปลี่ยนข้อมูลกันได้ โดยใช้การแบ่งระดับชั้นของระบบจำลองทีซีพี/ไอพี (TCP/IP Model) (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-5 - 10-12)

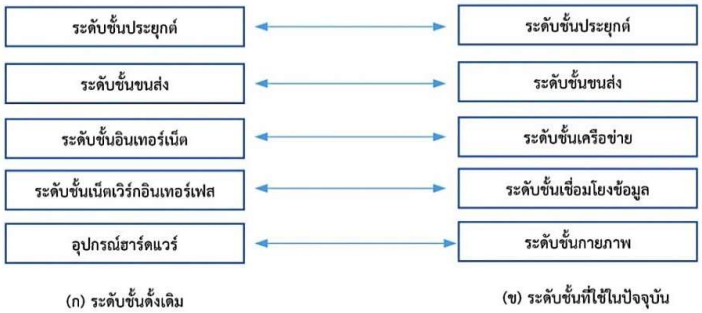
10.1 ความหมายของโพรโทคอลทีซีพี/ไอพี

โพรโทคอลทีซีพี/ไอพี (TCP/IP Protocol) เป็นชุดโพรโทคอลที่พัฒนาขึ้นมาเพื่อใช้สำหรับการแลกเปลี่ยนข้อมูลบนเครือข่ายอินเทอร์เน็ต ประกอบด้วยโมดูลต่างๆ ที่เกี่ยวข้องกัน โดยในแต่ละระดับชั้นของแบบจำลอง TCP/IP จะโพรโทคอลอิสระต่างๆ อยู่รวมกัน ซึ่งจะนำไปใช้ประโยชน์ได้ตามความต้องการ โดยที่ระดับชั้นต่างๆ เหล่านี้ไม่จำเป็นต้องเป็นอิสระต่อกัน

โพรโทคอลทีซีพี/ไอพี ประกอบด้วย โพรโทคอลทีซีพี (Transmission Control Protocol : TCP) และโพรโทคอลไอพี (Internet Protocol: IP) ทำงานในระดับชั้นที่แตกต่างกัน โดยโพรโทคอลทีซีพีทำงานอยู่ในระดับบน ทำหน้าที่จัดการแบ่งข้อความหรือไฟล์ที่ผู้ส่งต้องการส่งออกไปเป็นส่วนเล็กๆ เรียกว่า แพ็คเก็ต (Packet) แล้วส่งออกไปบนระบบเครือข่ายอินเตอร์เน็ตผ่านโพรโทคอลทีซีพีในเครื่องคอมพิวเตอร์ของผู้รับ แล้วจะนำข้อความหรือไฟล์แต่ละแพ็คเก็ตที่ได้รับมาประกอบกลับเป็นข้อความหรือไฟล์ตามเดิม ส่วนโพรโทคอลไอพีทำงานอยู่ในระดับล่าง ทำหน้าที่จัดการเกี่ยวกับที่อยู่เครื่องคอมพิวเตอร์ปลายทาง หรือแอดเดรส (Address) ที่ต้องการจะส่งข้อความเป็นแพ็กเก็ตแต่ละแพ็คเก็ตออกไป โดยที่เกตเวย์ (Gateway) แต่ละแห่งที่เชื่อมอยู่ในระบบเครือข่ายจะทำหน้าที่ตรวจสอบที่อยู่ก่อนที่จะส่งข้อความไปให้

ระดับชั้นในการจำลองทีซีพี/ไอพี ดั้งเดิมแบ่งออกเป็น 4 ระดับชั้น และเมื่อเปรียบเทียบกับระดับชั้นที่ใช้ในระดับของแบบจำลองโอเอสไอ (Open Systems Interconnection : OSI)

แบบจำลองทีซีพี/ไอพีได้พัฒนาขึ้นมาก่อนแบบจำลองโอเอสไอ ดังนั้น ระดับชั้นในแบบจำลองทีซีพี/ไอพี จึงไม่สอดคล้องกับแบบจำลองโอเอสไอ ดังภาพที่ 10.1



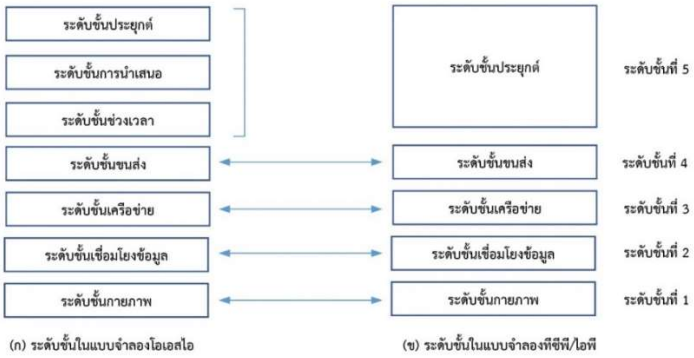
ภาพที่ 10.1 แสดงระดับชั้นในแบบจำลอง TCP/IP ดั้งเดิมเปรียบเทียบกับระดับชั้นที่ใช้ในปัจจุบัน
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-6)

โพรโทคอลทีซีพี/ไอพี ใช้รูปแบบการติดต่อสื่อสารตามแบบจำลองไคลเอนท์/เซิร์ฟเวอร์ (Client/Server) โดยเครื่องคอมพิวเตอร์ของผู้ใช้จัดเป็นเครื่องผู้ใช้บริการ (Client) จะได้รับบริการต่างๆ จากเครื่องผู้ให้บริการ (Server) ที่ได้เชื่อมต่อกับระบบเครือข่ายอินเทอร์เน็ต โดยทำการเชื่อมต่อแบบจุดต่อจุด คือ การสื่อสารในแต่ละครั้งของโพรโทคอลทีซีพี/ไอพี จะเป็นการสื่อสารจากจุดที่เป็นเครื่องมือผู้ให้บริการหรือโฮสต์ โดยโฮสต์นั้นจะมีการเชื่อมต่อระบบเครือข่ายอินเทอร์เน็ต ไปยังอีกจุดหนึ่งหรืออีกเครื่องหนึ่ง

10.1.1 การแบ่งระดับชั้นของแบบจำลองทีซีพี/ไอพี

การแบ่งระดับชั้นของแบบจำลองทีซีพี/ไอพี แบ่งออกเป็น 5 ระดับชั้น ดังนี้

1. ระดับชั้นที่ 1 ระดับกายภาพ (Physical Layer)
2. ระดับชั้นที่ 2 ระดับชั้นเชื่อมโยงข้อมูล หรือดาต้าลิงก์ (Data Link Layer)
3. ระดับชั้นที่ 3 ระดับชั้นเครือข่าย หรือเน็ตเวิร์ก (Network Layer)
4. ระดับชั้นที่ 4 ระดับชั้นขนส่ง หรือ ทรานสปอร์ต (Transport Layer)
5. ระดับชั้นที่ 5 ระดับชั้นประยุกต์ หรือแอปพลิเคชัน (Application Layer)



ภาพที่ 10.2 แสดงระดับชั้นในแบบจำลองโอเอสไอกับแบบจำลองทีซีพี/ไอพีที่ใช้ในปัจจุบัน
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-6)

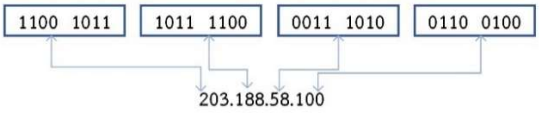
10.1.2 การกำหนดแอดเดรสของโพรโทคอลทีซีพี/ไอพี

อินเทอร์เน็ตแอดเดรส (Internet Address) หรือ ไอพีแอดเดรส (Internet Protocol address : IP address) เป็นที่อยู่หรือแอดเดรสของการเชื่อมต่อระหว่างโฮสต์ หรือเราท์เตอร์ และเครือข่าย สังเกตว่าถ้าอุปกรณ์มีการเคลื่อนย้ายไปยังเครือข่ายอื่นแล้ว ไอพีแอดเดรสจะต้องเปลี่ยนไปตามการเชื่อมต่อกับเครือข่ายนั้น

ในปัจจุบันมีการใช้งานไอพีแอดเดรสมี 2 รุ่น ได้แก่ ไอพีแอดเดรส รุ่นที่ 4 (IPv4) และ ไอพีแอดเดรส รุ่นที่ 6 (IPv6)

1. ไอพีแอดเดรส รุ่น 4

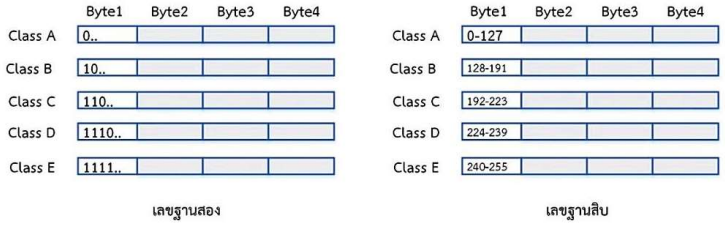
ไอดีแอดเดรส รุ่นที่ 4 (IP address version 4: IPv4) จะมีขนาด 4 ไบต์ หรือ 32 บิต แต่ละไบต์มีจุดเป็นตัวแบ่งเพื่อให้ง่ายต่อการอ่านและการจดจำ รูปแบบของไบต์และจุดแบ่ง ดังแสดงในภาพที่ 10.3



ภาพที่ 10.3 แสดงรูปแบบไอพีแอดเดรส รุ่นที่ 4
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-8)

จากภาพที่ 10.3 ไอพีแอดเดรส รุ่นที่ 4 ขนาด 4 ไบต์ แต่ละไบต์ เป็นกลุ่มของเลขฐานสองเมื่อนำมาแปลงเป็นเลขฐานสิบจะมีค่าตัวเลขอยู่ระหว่าง 0 ถึง 255

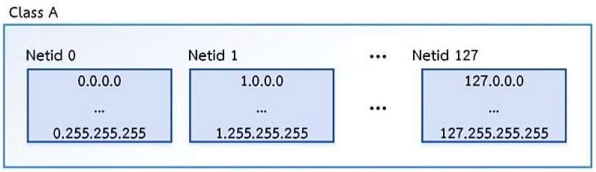
ไอพีแอดเดรส รุ่นที่ 4 ประกอบด้วย 1) หมายเลขเครือข่าย หรือเน็ตไอดี (Netid) และ 2) หมายเลขโฮสต์ หรือโฮสต์ไอดี (Hostid) โดยแบ่งออกเป็น 5 คลาส ดังภาพที่ 10.4



ภาพที่ 10.4 แสดงคลาสทั้งหมดของไอพีแอดเดรส รุ่นที่ 4

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-8)

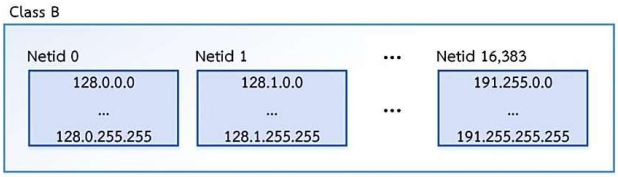
1.1 คลาสเอ (Class A) มีไบต์แรกเป็นหมายเลขเครือข่าย โดยบิตแรกกำหนดให้เป็น 0 ทำให้หมายเลขเครือข่ายมีขนาด 7 บิต ดังนั้น สามารถมีจำนวนหมายเลขเครือข่ายในคลาสเอได้ 2^7 = 128 จำนวน แต่ละหมายเลขเครือข่ายมีหมายเลขโฮสต์ขนาด 24 บิต จึงทำให้สามารถมีจำนวนโฮสต์ในแต่ละหมายเลขเครือข่ายของคลาสเอได้สูงสุดถึง 2^{24} = 16 ล้านโฮสต์ ดังแสดงในภาพที่ 10.5



ภาพที่ 10.5 แสดงหมายเลข IP address ในคลาสเอ

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-9)

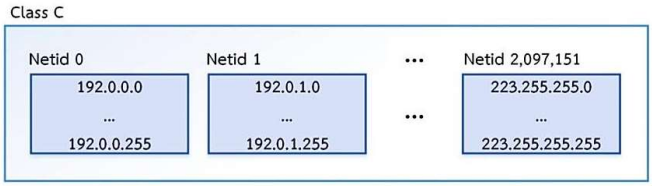
1.2 คลาสบี (Class B) มีไบต์แรกและไบต์ที่สองเป็นหมายเลขเครือข่าย โดยบิตแรกกำหนดให้เป็น 10 ทำให้หมายเลขเครือข่ายมีขนาดยาว 14 บิต ดังนั้น สามารถมีจำนวนหมายเลขเครือข่ายในคลาสบีได้ 2^{14} = 16,384 จำนวน แต่ละหมายเลขเครือข่ายจะมีหมายเลขโฮสต์ขนาด 16 บิต จึงทำให้สามารถมีจำนวนโฮสต์ในแต่ละเครือข่ายของคลาสบีได้สูงสุด 2^{16} = 65,536 โฮสต์ ดังแสดงในภาพที่ 10.6



ภาพที่ 10.6 แสดงหมายเลข IP address ในคลาสบี

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-9)

1.3 คลาสซี (Class C) มีไบต์ที่ 1 ถึง 3 เป็นหมายเลขเครือข่าย โดยบิตแรกกำหนดให้เป็น 110 ทำให้หมายเลขเครือข่ายมีขนาดยาว 21 บิต ดังนั้น สามารถมีจำนวนหมายเลขเครือข่ายในคลาสซี ได้ 2^{21} = 2,097,152 จำนวน แต่ละหมายเลขเครือข่ายมีหมายเลขโฮสต์ขนาด 8 บิต จึงทำให้สามารถมีจำนวนโฮสต์ในแต่ละหมายเลขเครือข่ายของคลาสซีได้สูงสุด 2^{8} = 254 โฮสต์ ดังแสดงในภาพที่ 10.7



ภาพที่ 10.7 แสดงหมายเลข IP address ในคลาสซี

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-10)

1.4 คลาสดี (Class D) กำหนดให้บิตแรกเป็น 1110 ซึ่งใช้สำหรับกระจายข้อมูลข่าวสารแบบหลายจุด (Multicast) และมีเพียงหมายเลขเครือข่ายเดียว ดังแสดงในภาพที่ 10.8

ภาพที่ 10.8 แสดงหมายเลข IP address ในคลาสดี

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-10)

1.5 คลาสอี (Class E) กำหนดให้บิตแรกเป็น 1111 ซึ่งใช้เป็นบิตสำรองสำหรับอนาคต มีเพียงหมายเลขเครือข่ายเดียว ดังแสดงในภาพที่ 10.9

ภาพที่ 10.9 แสดงหมายเลข IP address ในคลาสอี

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-10)

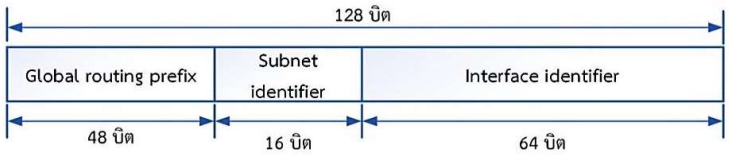
สรุปได้ว่า ไอพีแอดเดรส รุ่นที่ 4 เป็นแอดเดรสของการเชื่อมต่อระหว่างโฮสต์และเครือข่าย ขนาด 4 ไบต์ หรือ 32 บิต โดยตำแหน่งไบต์แรกของไอพีแอดเดรส ช่วยทำให้ทราบได้ว่าไอพีแอดเดรสดังกล่าวอยู่ในคลาสใด

2. ไอพีแอดเดรส รุ่นที่ 6

ไอพีแอดเดรส รุ่นที่ 6 (IP address version 6: IPv6) เป็นส่วนขยายแอดเดรสของไอพีแอดเดรส รุ่นที่ 4 และมีความยาวขนาด 16 ไบต์ หรือ 128 บิต IPv6 มีความยาวของแอดเดรสเป็น 4 เท่าของ IPv4

แบบเลขฐานสอง เป็นการใช้งานเมื่อมีการเก็บค่าไว้ในเครื่องคอมพิวเตอร์ ส่วนแบบจุดคู่ของทศนิยมเลขฐานสิบหก จะเป็นการแบ่งแอดเดรสออกเป็น 8 ส่วน โดยแต่ละส่วนประกอบด้วยเลขฐานสิบหก 4 หลัก ซึ่งแต่ละส่วนจะแยกกันด้วยเครื่องหมายจุดคู่

2.1 การจัดสรรพื้นที่แอดเดรส (Address Space Allocation) ของ IPv6 จะแบ่งเป็นบล็อกๆ หลายขนาด โดยบล็อกส่วนใหญ่ยังไม่ได้มีการกำหนดการใช้งานเพียงแต่มีไว้เพื่อรองรับการใช้งานที่เพิ่มขึ้นในอนาคต บล็อกต่างๆ ในพื้นที่แอดเดรส (Space Address) จะมีการใช้งานสำหรับการติดต่อสื่อสารแบบแบบหนึ่งต่อหนึ่ง (One-to-One Communication) ระหว่างสองโฮสต์ในระบบอินเทอร์เน็ตที่เรียกว่า บล็อกแอดเดรสแบบโกลบอลยูนิแคส (Global Unicast Address Block) มีการกำหนดให้สามบิตแรกทางซ้ายมือมีค่า 001 เหมือนกัน ดังนั้นบล็อกนี้จะมีขนาด 2^{125} บิต ซึ่งเพียงพอกับการใช้งานอินเทอร์เน็ตในอนาคต โดยแอดเดรสในบล็อกนี้ จะแบ่งออกเป็น 3 ส่วนดังแสดงในภาพที่ 10.10



ภาพที่ 10.10 แสดงแอดเดรสแบบโกลบอลยูนิแคส

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-12)

2.2 การตั้งค่าอัตโนมัติ (Autoconfiguration) ของโฮสต์จะยังคงใช้โพรโทคอล DHCP สามารถจัดสรรแอดเดรสของ IPv6 ไปให้โฮสต์ได้โดยที่โฮสต์สามารถตั้งค่าตัวเองได้ โดยมีกระบวนการ ดังนี้

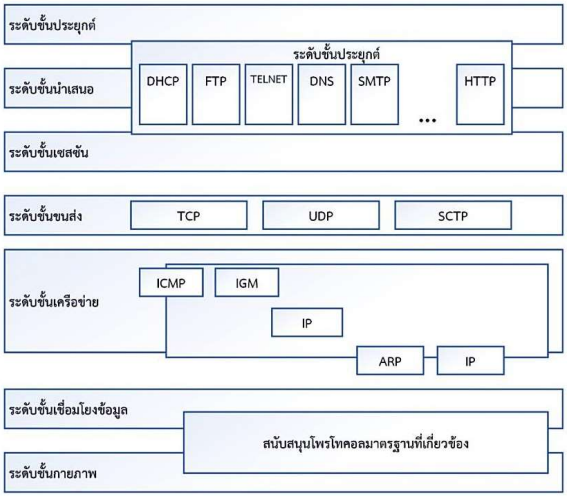
2.2.1 โฮสต์จะทำการสร้างแอดเดรสท้องถิ่น (Link Local Address) ของตัวเอง โดยการสร้าง 10 บิต 1111 1110 10 แล้วเพิ่มบิตศูนย์จำนวน 54 บิต จะได้เป็น FE80 : 0 : 0 : 0 : 0 ซึ่งสามารถเขียนเป็นตัวย่อโดยใช้เทคนิคการบีบอัดเลขศูนย์ (zero compression) เมื่อเจอบิตศูนย์ต่อกันสามารถใช้เครื่องหมาย “: : ” จุดคู่ซ้ำ (Double Colon) แทนได้ ดังนั้น FE80 : 0 : 0 : 0 : 0 จะเป็น FE80 : : ต่อมาเพิ่มการระบุอินเตอร์เฟซ 64 บิตเข้าไป ผลที่ได้จะเป็นแอดเดรสลิงก์ท้องถิ่น

2.2.2 ถ้าโฮสต์ทำการทดสอบแล้วพบว่า แอดเดรสลิงก์ท้องถิ่นมีความเป็นหนึ่งเดียว (Unique) และไม่มีการใช้โดยโฮสต์อื่นๆ โฮสต์จะส่งข้อความออกไปและรอจนได้ข้อความตอบรับ ถ้ากระบวนการนี้ล้มเหลวโฮสต์ไม่สามารถตั้งค่าตัวเองได้ จะมีการนำโพรโทคอล DHCP มาใช้แทน

2.2.3 ถ้าขั้นตอนการทดสอบโฮสต์พบว่า มีความเป็นหนึ่งเดียวสำเร็จแล้ว โฮสต์จะส่งข้อความเกี่ยวกับเราท์เตอร์ออกไปให้เราท์เตอร์ท้องถิ่น ถ้ามีเราท์เตอร์ท้องถิ่นกำลังทำงานอยู่ในเครือข่าย โฮสต์จะได้รับข้อความตอบกลับ ซึ่งประกอบด้วยส่วนเติมด้านหน้าของเส้นทางโกลบอล และส่วนระบุเครือข่ายย่อย โดยโฮสต์จะนำทั้งสองส่วนแล้วเพิ่มส่วนระบุอินเตอร์เฟซเข้าไปเพื่อสร้างแอดเดรสแบบโกลบอลยูนิแคส

10.2 ระดับชั้นแบบจำลองทีซีพี/ไอพี

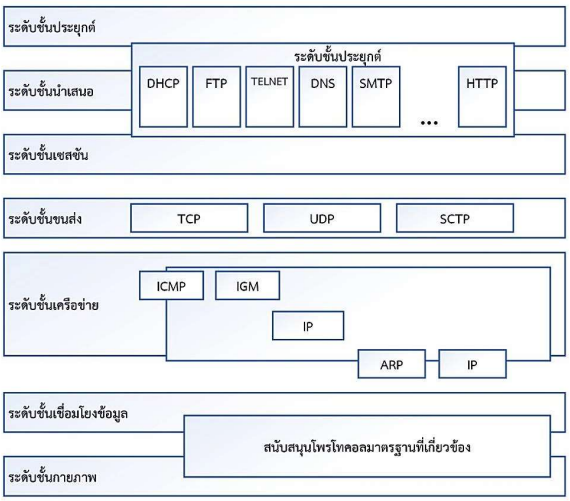
แบบจำลองทีซีพี/ไอพี ประกอบด้วยชั้นทั้งหมด 5 ระดับชั้น ได้แก่ ระดับชั้นกายภาพ ระดับชั้นเชื่อมโยงข้อมูล ระดับชั้นเครือข่าย ระดับชั้นขนส่งและระดับชั้นประยุกต์ โดยจะมีตัวอย่างโพรโทคอล ย่อยทำงานอยู่ในแต่ละระดับชั้น ดังแสดงในภาพที่ 10.11 มีรายละเอียด ดังภาพที่ 10.11 (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-17 – 10-48)



ภาพที่ 10.11 แสดงการเปรียบเทียบโพรโทคอลย่อยของแบบจำลอง TCP/IP และแบบจำลอง OSI
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-18)

แบบจำลองทีซีพี/ไอพี แบ่งระดับชั้นออกเป็น 5 ระดับชั้น ดังนี้

1. ระดับชั้นกายภาพและระดับชั้นเชื่อมโยงข้อมูล ระดับชั้นกายภาพ และระดับชั้นเชื่อมโยงข้อมูล ของแบบจำลองทีซีพี/ไอพี จะไม่มีการกำหนดโพรโทคอลย่อยพิเศษใดๆ ในระดับชั้นเหล่านี้ แต่จะทำหน้าที่สนับสนุนการทำงานของโพรโทคอลมาตรฐานที่เกี่ยวข้องและทำหน้าที่เหมือนกับระดับกายภาพและระดับเชื่อมโยงของแบบจำลองโอเอสไอ ดังภาพที่ 10.12



ภาพที่ 10.12 แสดงโพรโทคอลย่อยของแบบจำลอง TCP/IP กับระดับชั้นการทำงานในแบบจำลอง OSI
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-18)

2. ระดับชั้นเครือข่าย (Network Layer) ของโพรโทคอล TCP/IP ทำหน้าที่สนับสนุนการทำงานของโพรโทคอลไอพี (Internetwork Protocol: IP) โดยจะแบ่งการสื่อสารในระดับชั้นนี้ ออกเป็น 2 ชนิด ได้แก่

2.1 การสื่อสารแบบหนึ่งต่อหนึ่ง หรือยูนิคแคส (Unicast) เป็นการติดต่อสื่อสารระหว่างผู้ส่งหนึ่งคนกับผู้รับหนึ่งคน การสื่อสารชนิดนี้เป็นการสื่อสารระหว่างโหนดแบบง่ายๆ จึงไม่สามารถรองรับการส่งข้อมูลระหว่างโหนดได้ในกรณีที่โหนดในการรับส่งมีจำนวนเพิ่มมากขึ้น

2.2 การสื่อสารแบบหนึ่งต่อหลายหรือมัลติแคส (Multicast) เป็นการติดต่อสื่อสารระหว่างผู้ส่งหนึ่งคนกับผู้รับหลายคน การสื่อสารชนิดนี้เป็นการส่งข้อมูลจากโหนดต้นทางหนึ่งโหนดไปยังกลุ่มโหนดปลายทางเฉพาะกลุ่มที่ต้องการรับข้อมูลเท่านั้น

ในปัจจุบันโพรโทคอลที่ใช้ในระดับชั้นเครือข่าย ประกอบด้วย โพรโทคอล รุ่นที่ 4 และโพรโทคอล รุ่นที่ 6

รูปแบบของโพรโทคอลไอพี รุ่นที่ 4

สำหรับระดับชั้นเครือข่าย (Network layer) ในรุ่นที่ 4 (Version 4) ประกอบด้วย 4 โพรโทคอล ได้แก่

1. โพรโทคอลหลัก (Main Protocol) 1 โพรโทคอล ได้แก่ โพรโทคอลไอพี รุ่นที่ 4 (IPv4)

2. โพรโทคอลเสริม (Auxiliary Protocol) 4 โพรโทคอล ได้แก่ โพรโทคอลไอซีเอ็มพี รุ่น 4 (ICMPv4) โพรโทคอลไอจีเอ็มพี (IGMP) โพรโทคอลเออาร์พี (ARP) และโพรโทคอลอาร์เออาร์พี (RARP)

โพรโทคอล IPv4 เป็นโพรโทคอลที่มีกลไกในการส่งผ่านข้อมูลด้วยโพรโทคอล TCP/IP ซึ่งเป็นโพรโทคอลที่ไม่มีการสร้างการเชื่อมต่อก่อนทำการส่งข้อมูล (Connectionless) หรือเกิดจากการเชื่อมต่อเส้นทางทุกๆ ครั้งที่มีการส่งข้อมูล 1 ดาต้าแกรม (Datagram) โดยไม่จำเป็นต้องทราบถึงข้อมูลดาต้าแกรมที่ส่งก่อนหน้านี้หรือข้อมูลที่ส่งตามมา แต่ในการส่งข้อมูล 1 ดาต้าแกรม อาจเกิดการส่งได้หลายครั้งในกรณีที่มีการแบ่งข้อมูลออกเป็นส่วนย่อยๆ (Fragmentation) แล้วจึงนำข้อมูลย่อยๆ มารวมกันเมื่อถึงปลายทางและการส่งข้อมูลแบบไม่มีการสร้างการเชื่อมต่อจะมีความน่าเชื่อถือในการส่งข้อมูลค่อนข้างน้อย (Unrealiable)

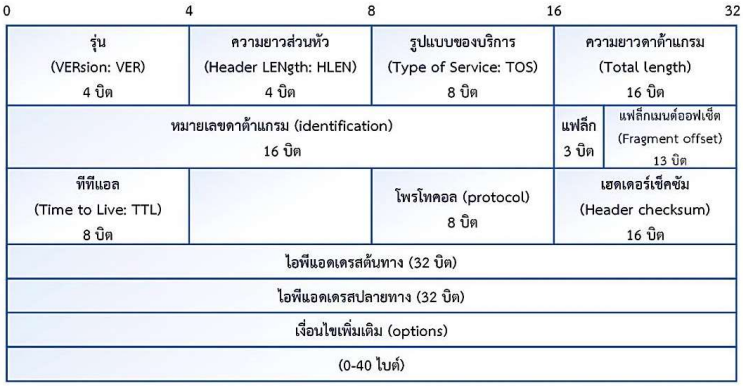
โพรโทคอล IPv4 จะส่งข้อมูลในรูปของแพ็กเก็ต เรียกว่า ดาต้าแกรม (Datagram) หรือ ไอพีดาต้าแกรม (IP Datagram) ดังแสดงในภาพที่ 10.13 ประกอบด้วยส่วนหัว (Header) และส่วนข้อมูล (Data)

ภาพที่ 10.13 แสดงไอพีดาต้าแกรมของโพรโทคอล IPv4

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-20)

องค์ประกอบของไอพีดาต้าแกรม แต่ละดาต้าแกรมจะมีการส่งผ่านอย่างอิสระต่อกัน ทำให้ดาต้าแกรมเหล่านี้ไปถึงปลายทางได้ด้วยเส้นทางที่แตกต่างกันและไม่จำเป็นต้องเรียงลำดับ หรืออาจจะมีการส่งข้อมูลซ้ำได้ จากลักษณะการทำงานดังกล่าวแสดงให้เห็นว่า การทำงานของโพรโทคอล IPv4 ไม่มีความสลับซับซ้อนแต่มีความน่าเชื่อถือต่ำ แต่หากต้องการให้การส่งข้อมูลมีความน่าเชื่อถือมากขึ้นใน IPV4 จะทำงานควบคู่กับโพรโทคอล TCP ที่มีเครื่องมือในการติดตามเส้นทางการเดินทางและการเรียงลำดับข้อมูลในการจัดส่งก่อนถึงปลายทาง

รูปแบบของไอพีดาต้าแกรม ประกอบด้วย ส่วนหัว (header) มีขนาด 20-60 ไบต์ และส่วนของข้อมูล (data) มีขนาด 20-65,536 ไบต์ ดังภาพที่ 10.14



ภาพที่ 10.14 แสดงส่วนหัวไอพีดาต้าแกรมของโพรโทคอล IPv4

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-20)

ส่วนหัวของไอพีดาต้าแกรม ประกอบด้วยฟิลด์ต่างๆ ดังนี้

1. รุ่น หรือเวอร์ชัน (VERsion: VER) เป็นฟิลด์แรกที่ใช้กำหนดหมายเลขรุ่นของโพรโทคอล IP ปัจจุบันมีการใช้ทั้ง ไอพี เวอร์ชัน 4 (IPv4) และไอพี เวอร์ชัน 6 (IPv6)

2. ความยาวของส่วนหัว (Header LENgth: HLEN) เป็นฟิลด์ที่ใช้ระบุความยาวของส่วนหัวของดาต้าแกรม มีขนาด 20-60 ไบต์ โดย 1 ไบต์ มีค่าเท่ากับ 8 บิต

3. รูปแบบการบริการ (Type of Service: TOS) เป็นฟิลด์ที่มีขนาด 8 บิตที่ใช้กำหนดค่าต่างๆ ที่เกี่ยวข้องกับรูปแบบการบริการที่มีให้สำหรับฝ่ายผู้ส่ง เช่น ระดับความน่าเชื่อถือ ระดับค่าหน่วงเวลา เป็นต้น

4. ความยาวดาต้าแกรม (Total length) เป็นฟิลด์ที่ใช้ระบุความยาวดาต้าแกรมที่ใช้ในโพรโทรคอล IP มีขนาด 16 บิต หรือ 2 ไบต์ โดยสามารถระบุความยาวได้สูงสุดถึง 65,536 ไบต์

5. หมายเลขดาต้าแกรม (Identification) เป็นฟิลด์ที่ใช้ในการบอกหมายเลขของดาต้าแกรมในกรณีที่มีการแยกดาต้าแกรมเป็นส่วนย่อย หรือแฟล็กเมนต์ (Fragment) เมื่อข้อมูลส่งถึงปลายทางแล้ว ข้อมูลที่มีหมายเลขดาต้าแกรมเดียวกัน จะนำมารวมตัวกัน หรือถ้ามีการส่งผ่านดาต้าแกรมไปยังเครือข่ายที่ต่างกัน อาจมีการแบ่งเป็นแฟล็กเมนต์ เพื่อให้สอดคล้องกับขนาดของเฟรม (Frame) ของเครือข่ายนั้นๆ และในฟิลด์นี้จะมีการระบุหมายเลขของแฟล็กเมนต์ด้วย

6. แฟล็ก (Flag) เป็นฟิลด์ที่ใช้ระบุว่า ดาต้าแกรมสามารถที่จะทำแฟล็กเมนต์ได้หรือไม่รวมถึงระบุลำดับของแฟล็กเมนต์ว่าเป็นแฟล็กเมนต์แรก แฟล็กเมนต์กลางหรือแฟล็กเมนต์สุดท้าย

7. ออฟเซ็ตของส่วนย่อย หรือแฟล็กเมนต์ออฟเซ็ต (Fragment Offset) เป็นฟิลด์ที่ระบุหมายเลขที่ใช้ในการกำหนดตำแหน่งข้อมูลในดาต้าแกรมที่มีการแยกส่วน เพื่อให้สามารถนำกลับมาเรียงต่อกันได้อย่างถูกต้อง

8. ทีทีแอล (Time to Live: TTL) เป็นฟิลด์ที่ใช้ระบุจำนวนครั้งที่มากที่สุดของการส่งดาต้าแกรมจากอุปกรณ์หนึ่งไปยังอีกอุปกรณ์หนึ่งเพื่อป้องกันการส่งข้อมูลวนซ้ำอยู่ในเครือข่ายไม่รู้จบ โดยเริ่มต้นจากการกำหนดฟิลด์นี้จากโฮสต์ต้นทาง ในขณะที่มีการส่งดาต้าแกรมผ่านเครือข่ายอินเทอร์เน็ตจากเราท์เตอร์หนึ่งไปยังอีกตัวหนึ่ง 1 ครั้ง ค่านี้จะลดลงทีละหนึ่งจนกระทั่งเป็นศูนย์ ถ้าดาต้าแกรมยังส่งไม่ถึงปลายทาง ดาต้าแกรมจะถูกยกเลิกซึ่งหมายความว่า หมดเวลา (Time Out) ในระหว่างการส่งข้อมูล

9. โพรโทคอล (Protocol) เป็นฟิลด์ที่ใช้ระบุว่า มีการใช้โพรโทคอลชนิดใดที่ใช้ในการส่งดาต้าแกรม เช่น โพรโทคอล TCP โพรโทคอล UDP โพรโทคอล ICMP เป็นต้น

10. การตรวจสอบผลรวมของส่วนหัว หรือเฮดเดอร์เช็คซัม (Header Checksum) เป็นฟิลด์ที่ใช้ตรวจสอบความถูกต้องของข้อมูลส่วนหัวของดาต้าแกรม ฟิลด์นี้มีขนาด 16 บิต

11. ที่อยู่ของไอพีต้นทาง หรือไอพีแอดเดรสต้นทาง (Source IP Address) เป็นฟิลด์ที่ใช้ระบุ แอดเดรสต้นทางของผู้ส่งดาต้าแกรม

12. ที่อยู่ของไอพีปลายทาง หรือไอพีแอดเดรสปลายทาง (Destination IP Address) เป็นฟิลด์ที่ใช้ระบุแอดเดรสปลายทางที่ส่งดาต้าแกรมออกไป

13. เงื่อนไขเพิ่มเติม (Options) เป็นฟิลด์ที่ใช้กำหนดฟังก์ชันการทำงานเพิ่มเติม ซึ่งอาจใช้ได้หรือไม่ได้ก็ได้ โดยฟิลด์นี้มีหน้าที่เกี่ยวข้องกับการกำหนดควบคุมเส้นทางและเวลาที่ใช้ในการส่งข้อมูล

โพรโทคอลเสริมสำหรับโพรโทคอลไอพี รุ่น 4

โพรโทคอล IPv4 ประกอบด้วย 4 โพรโทคอลเสริมที่ทำงานร่วมกัน ได้แก่ โพรโทคอลเออาร์พี โพรโทคอลอาร์เออาร์พี โพรโทคอลไอซีเอ็มพี รุ่น 4 และโพรโทคอลไอจีเอ็มพี มีรายละเอียด ดังนี้

1. โพรโทคอลเออาร์พี (Address Resolution Protocol: ARP) ทำหน้าที่เปลี่ยนไอพีแอดเดรสให้เป็นหมายเลขแม็คแอดเดรส (MAC Address) วิธีการนี้จะใช้งานเมื่อโฮสต์หรือเราท์เตอร์ต้องการค้นหาที่อยู่ทางกายภาพ (Physical Address) บนระบบเครือข่าย

2. โพรโทคอลอาร์เออาร์พี (Reverse Address Resolution Protocol: RARP) ทำหน้าที่ตรงกันข้ามกับโพรโทคอล ARP โดยจะทำการแปลงแมคแอดเดรสให้เป็นไอพีแอดเดรส

3. โพรโทคอลไอซีเอ็มพี รุ่น 4 (Internet Control Message Protocol Version 4: ICMPv4) เป็นโพรโทคอลที่ใช้โดยโฮสต์ (Host) และเกตเวย์ (Gateway) สำหรับรายงานความผิดพลาดที่เกิดขึ้นจากการส่งข้อมูลกลับไปยังโฮสต์ของฝ่ายผู้ส่ง เช่น เมื่อส่งข้อมูลไปแล้วไม่พบโฮตส์ปลายทาง เครือข่ายหรือลิงก์สำหรับเชื่อมโยงเสียหาย เป็นต้น

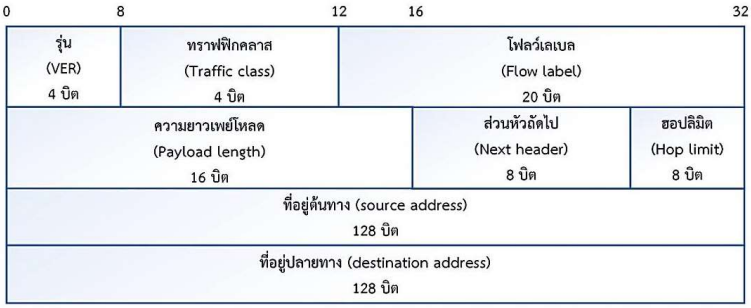
โพรโทคอล ICMPv4 จะเก็บเฉพาะข้อมูลที่อยู่หรือแอดเดรส (Address) ของโฮสต์ต้นทางกับโฮสต์ปลายทาง โดยไม่เก็บข้อมูลที่อยู่เราท์เตอร์ต่างๆ ที่ได้ส่งผ่านข้อมูลไป เมื่อเกิดปัญหาในการส่งข้อมูลโพรโทคอล ICMPv4 จะทำการส่งรายงานความผิดพลาดกลับไปที่โฮสต์ของฝ่ายผู้ส่งเท่านั้น

4. โพรโทคอลไอจีเอ็มพี (Internet Group Message Protocol: IGMP) เป็นโพรโทคอล ที่มีการติดต่อสื่อสารแบบมัลติคาส โดยโฮสต์ต้นทางจะส่งข้อมูลเพียงชุดเดียวไปยังกลุ่มสมาชิกที่อยู่ปลายทาง

รูปแบบของโพรโทคอลไอพี รุ่นที่ 6

โพรโทคอลไอพี รุ่นที่ 6 (IPv6) ถูกออกแบบมาใช้งานแทน โพรโทคอล IPv4 เพื่อรองรับการทำงานสำหรับส่วนเพิ่มเติมของโพรโทคอล (Extension of Protocol) ในส่วนของเทคโนโลยีและโปรแกรมประยุกต์ใหม่ๆ เช่น สนับสนุนในส่วนข้อมูลภาพและเสียง ณ เวลาจริง (Real Time Audio and Video) และสนับสนุนในส่วนของความปลอดภัยของข้อมูลในด้านการเข้ารหัส (Encryption) และการยืนยันตัวตน (Authentication) โพรโทคอล IPv6 มีลักษณะ ดังนี้

1. รูปแบบแพ็คเก็ตของโพรโทคอล IPv6 แต่ละแพ็คเก็ตประกอบด้วยส่วนหัวฐาน หรือเบสเฮดเดอร์ (Base Header) ขนาด 40 ไบต์ และเพย์โหลด (Payload) ที่มีขนาดสูงสุด 65,535 ไบต์ มีรายละเอียดของแต่ละฟิลด์ ดังภาพที่ 10.15



ภาพที่ 10.15 แสดงรูปแบบของส่วนหัวฐานหรือเบสเฮดเดอร์ของโพรโทคอล IPv6
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-24)

รูปแบบของส่วนหัวฐานหรือเบสเฮดเดอร์ของโพรโทคอล IPv6 มีรายละเอียดดังนี้

1.1 รุ่น (Version) เป็นฟิลด์ที่ใช้ระบุรุ่นของโพรโทคอลไอพี มีขนาด 4 บิต

1.2 ทราฟฟิกคลาส (Traffic Class) เป็นฟิลด์ที่ใช้จำแนกความแตกต่างของเพย์โหลดที่ต้องการวิธีการส่งข้อมูลที่แตกต่างกัน มีขนาด 8 บิต โดยฟิลด์ใช้แทนฟิลด์รูปแบบการบริหาร (TOS) ในโพรโทคอล IPv4

1.3 โฟลว์เลเบล (Flow Label) เป็นฟิลด์ที่ใช้สนับสนุนการส่งผ่านข้อมูลภาพและเสียงในเวลาจริงในรูปแบบดิจิทัล มีขนาด 20 บิต

1.4 ความยาวเพย์โหลด (Payload Length) เป็นฟิลด์ที่ใช้ระบุความยาวของไอพีดาต้าแกรมรวมกับส่วนเบสเฮดเดอร์ มีขนาด 2 ไบต์ หรือ 16 บิต

1.5 ส่วนหัวถัดไป (Next Header) เป็นฟิลด์ที่ใช้ระบุรายละเอียดของส่วนเบสเฮดเดอร์ในดาต้าแกรม มีขนาด 8 บิต โดยเป็นได้ทั้งส่วนเพิ่มเติมของส่วนหัว (Optional Extension Header) ในโพรโทคอล IP และส่วนหัวของแพ็กเก็ตที่ถูกห่อหุ้มในโพรโทคอล UDP หรือโพรโทคอล TCP

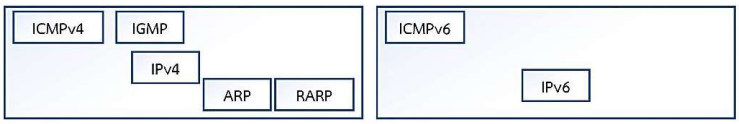
1.6 ฮอปลิมิต (Hop Limit) เป็นฟิลด์ที่ใช้ระบุจำนวนครั้งที่มากที่สุดของการส่งดาต้าแกรมจากอุปกรณ์หนึ่งไปอีกอุปกรณ์หนึ่ง มีขนาด 8 บิต ทำหน้าที่เหมือนกับฟิลด์ทีทีแอลใน IPv4

1.7 ที่อยู่ต้นทาง (Source Address) เป็นฟิลด์ที่บอกถึงต้นทางของดาต้าแกรม มีขนาด 16 ไบต์

1.8 ที่อยู่ปลายทาง (Destination Address) เป็นฟิลด์ที่บอกถึงปลายทางของดาต้าแกรม มีขนาด 16 ไบต์

2. รูปแบบแพ็กเก็ตของโพรโทคอลไอซีเอ็มพี รุ่นที่ 6 โพรโทคอล ICMP เป็นโพรโทคอลที่ได้รับการพัฒนาเป็นโพรโทคอล ICMP รุ่น 6 (Internet Control Message Protocol version 6: ICMPv6) ซึ่งมีวัตถุประสงค์เพื่อรองรับปริมาณการใช้งานที่เพิ่มขึ้น โดยโพรโทคอล ICMPv6 จะมีความซับซ้อนมากกว่าโพรโทคอล ICMPv4

โพรโทคอล ICMPv6 เป็นการรวมกันของโพรโทคอล ICMPv4 โพรโทคอล IGMP โพรโทคอล ARP และโพรโทคอล RARP ดังภาพที่ 10.16



(ก) ระดับชั้นเครือข่ายของรุ่นที่ 4 (ข) ระดับชั้นเครือข่ายของรุ่นที่ 6

ภาพที่ 10.16 แสดงการเปรียบเทียบโพรโทคอลย่อยๆ ที่ทำงานในระดับชั้นเครือข่ายของรุ่นที่ 4 และ 6
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-26)

3. ระดับชั้นขนส่งและระดับชั้นประยุกต์

ระดับชั้นขนส่งในแบบจำลอง TCP/IP อยู่ระหว่างระดับชั้นประยุกต์และระดับชั้นเครือข่าย โดยจะมีหน้าที่ให้บริการต่างๆ กับระดับชั้นประยุกต์และรับบริการต่างๆ จากระดับชั้นเครือข่าย ระดับชั้นขนส่งจะทำหน้าที่ประสานงานระหว่างโปรแกรมประยุกต์ของเครื่องผู้ใช้บริการและโปรแกรมประยุกต์เครื่องผู้ให้บริการ การเชื่อมต่อแบบกระบวนการถึงกระบวนการ (Process-to-Process Connection)

3.1 ระดับชั้นขนส่ง

เนื่องจากการส่งข้อมูลของโพรโทคอลไอพีในระดับชั้นเครือข่าย จะส่งจากเครื่องคอมพิวเตอร์ที่เป็นโฮสต์ต้นทางไปยังเครื่องปลายทาง ภายในแต่ละโฮสต์ประกอบด้วย การทำงานแบบกระบวนการหลายกระบวนการ ดังนั้น การส่งข้อมูลของโพรโทคอล TCP/IP ในระดับชั้นขนส่ง ซึ่งทำงานบนโพรโทคอล IP จึงส่งข้อมูลจากกระบวนการหนึ่งไปยังอีกกระบวนการหนึ่ง (Process-to-Process) ผ่านหมายเลขพอร์ต (Port Numbers) จากต้นทางไปยังปลายทาง

หมายเลขพอร์ตแต่ละพอร์ตกำหนดไว้ตั้งแต่ 0 ถึง 65,535 โดยหมายเลขพอร์ตตั้งแต่ 0 ถึง 1,023 จะสงวนไว้เพิ่มการบริการมาตรฐานของโฮสต์ที่เป็นเครื่องให้บริการหรือเซิร์ฟเวอร์ (Server) ตัวอย่างดังตารางที่ 10.1

ตารางที่ 10.1 ตัวอย่างหมายเลขพอร์ตที่สงวนไว้เพื่อการบริการมาตรฐาน

หมายเลขพอร์ต	บริการ
21	โพรโทคอลเอฟทีพี (File Transfer Protocol: FTP)
23	โพรโทคอลเทลเน็ต (Terminal Network: TELNET)
25	โพรโทคอลเอสเอ็มทีพี (Simple Mail Transfer Protocol: SMTP)
53	โพรโทคอลดีเอ็นเอส (Domain Name Server: DNS)
67	โพรโทคอลบู๊ท (Bootstrap Protocol: BOOTP)
80	โพรโทคอลเอชทีทีพี (Hypertext Transfer Protocol: HTTP)
110	โพรโทคอลพ็อป 3 (Post Office Protocol-version3: POP3)

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-26)

โพรโทคอล TCP/IP ในระดับชั้นขนส่ง จะประกอบไปด้วย 3 โพรโทคอล ที่ทำงานร่วมกัน ได้แก่ โพรโทคอลยูดีพี (UDP) โพรโทคอลทีซีพี (TCP) และโพรโทคอลเอสซีทีพี (SCTP) ดังนี้

1. โพรโทคอลยูดีพี (User Datagram Protocol: UDP) เป็นโพรโทคอลพื้นฐานของระดับชั้นขนส่งในโพรโทคอล TCP/IP โดยแพ็กเก็ตข้อมูลที่ประกอบจากโพรโทคอล UDP เรียกว่า ดาต้าแกรม ผู้ใช้หรือยูสเซอร์ดาต้าแกรม (user datagram) โดยส่วนหัวของดาต้าแกรมผู้ใช้ประกอบ
ด้วยฟิลด์ต่างๆ ดังนี้

1.1 ที่อยู่พอร์ตต้นทาง (Source Port Address) มีขนาด 16 บิต สามารถสร้างที่อยู่พอร์ตหรือพอร์ตแอดเดรส ได้ตั้งแต่ 0 ถึง 65,535

1.2 ที่อยู่พอร์ตปลายทาง (Destination Port Address) มีขนาด 16 บิต สามารถสร้างที่อยู่พอร์ตหรือพอร์ตแอดเดรส ได้ตั้งแต่ 0 ถึง 65,535

1.3 ความยาวของยูสเซอร์ดาต้าแกรม (Total Length) เป็นความยาวรวมของทั้งส่วนหัวและส่วนที่เป็นข้อมูลของยูสเซอร์ดาต้าแกรม มีขนาด 16 บิต

1.4 การตรวจสอบผลรวมหรือเช็คซัม (Checksum) เป็นฟิลด์ขนาด 16 บิต ใช้สำหรับตรวจสอบข้อผิดพลาดที่เกิดขึ้น

รูปแบบของยูสเซอร์ดาต้าแกรมของโพรโทคอล UDP ดังแสดงในภาพที่ 10.17

ภาพที่ 10.17 แสดงรูปแบบของยูสเซอร์ดาต้าแกรม
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-29)

โพรโทคอล UDP เป็นโพรโทคอลชนิดไม่สร้างการเชื่อมต่อก่อนทำการส่งข้อมูล (Connectionless) มีความน่าเชื่อถือน้อย แต่เหตุผลที่โพรโทคอล UDP ยังคงได้รับความนิยมในการใช้งาน เนื่องจากเป็นโพรโทคอลที่มีโครงสร้างไม่ซับซ้อน มีค่าโอเวอร์เฮด (Overhead)

ต่ำ โดยถ้ากระบวนการใดต้องส่งข้อความสั้นๆ และไม่คำนึงถึงความน่าเชื่อถือมากนัก ก็สามารถใช้โพรโทคอล UDP ได้

โพรโทคอล UDP จะทำการจัดหาเฉพาะฟังก์ชันพื้นฐานที่จำเป็นสำหรับการส่งข้อมูล ไม่จัดหาฟังก์ชันสำหรับการเรียงค่าลำดับข้อมูล เมื่อเกิดความเสียหายจะไม่สามารถระบุได้ว่า แพ็กเก็ตข้อมูลส่วนใดเสียหาย ถ้าต้องการทราบว่าแพ็กเก็ตข้อมูลส่วนใดเสียหายให้ใช้โพรโทคอล ICMP เป็นตัวช่วยเหลือ

2. โพรโทคอลทีซีพี (Transmission Control Protocol : TCP) เป็นโพรโทคอลที่มีความน่าเชื่อถือ เพราะมีการสร้างเส้นทางการส่งข้อมูลก่อนทำการส่งข้อมูล (Connection Oriented) โดยโพรโทคอล TCP จะทำการสร้างวงจรเสมือน (Virtual Circuit) ระหว่างฝ่ายผู้ส่งและฝ่ายผู้รับ เพื่อให้เกิดความคล่องตัวในระหว่างการส่งและรับข้อมูล โพรโทคอล TCP จะจัดหาฟังก์ชันสำหรับการเรียงระดับข้อมูลผู้รับให้เหมือนข้อมูลต้นฉบับ หากข้อมูลเกิดความเสียหายจากการขนส่ง จะสามารถตรวจสอบได้ว่า แพ็กเก็ตข้อมูลหรือเซกเมนต์ (Segment) ใดเกิดเสียหาย จากนั้นจะทำการขนส่งซ้ำใหม่

ข้อแตกต่างระหว่างโพรโทคอล TCP และ UDP คือ โพรโทคอล TCP มีความน่าเชื่อถือในการส่งข้อมูลมากกว่าโพรโทคอล UDP ในขณะที่โพรโทคอล UDP มีความรวดเร็วในการส่ง แต่โพรโทคอล TCP จะเสียเวลาในการสร้างเส้นทางการส่งข้อมูลก่อนทำการส่งข้อมูล

สำหรับการส่งข้อมูล โพรโทคอล TCP จะแบ่งขนาดข้อมูลเป็นหน่วยย่อยและบรรจุข้อมูลแต่ละหน่วยย่อยลงในเฟรมเฟรมหนึ่ง เรียกว่า เซกเมนต์ (Segment) โดยหมายเลขลำดับของเซกเมนต์ใช้ในการเรียงลำดับกลับเมื่อข้อมูลส่งถึงปลายทาง ดังภาพที่ 10.18

ภาพที่ 10.18 แสดงรูปแบบส่วนหัวของเซกเมนต์ของโพรโทคอลทีซีพี

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-30)

2.1 รูปแบบส่วนหัวของโพรโทคอลทีซีพี ประกอบด้วยฟิลด์ต่างๆ ดังนี้

2.1.1 ที่อยู่พอร์ตต้นทาง (Source Port Address) มีขนาด 16 บิต สามารถสร้างที่อยู่พอร์ตหรือพอร์ตแอดเดรส ได้ตั้งแต่ 0 ถึง 65,535

2.1.2 ที่อยู่พอร์ตปลายทาง (Destination Port Address) มีขนาด 16 บิต สร้างที่อยู่ของพอร์ตหรือพอร์ตแอดเดรส ได้ตั้งแต่ 0 ถึง 65,535

2.1.3 หมายเลขลำดับของเซกเมนต์ (Sequence Number) โดยฟิลด์นี้จะแสดงตำแหน่งของข้อมูลเริ่มต้นก่อนถูกแบ่งออกเป็นเซกเมนต์ โดยข้อมูลจะถูกแบ่งออกเป็น 2 เซกเมนต์หรือมากกว่า

2.1.4 หมายเลขแจ้งการรับรู้ (Acknowledgment Number) ฟิลด์นี้มีขนาด 32 บิต ใช้ตอบกลับไปยังฝ่ายผู้ส่งเพื่อยืนยันว่า ได้รับข้อมูลเรียบร้อยแล้ว โดยปกติผู้รับจะส่งหมายเลขเซกเมนต์ลำดับถัดไปของข้อมูลที่ต้องการให้ฝ่ายผู้ส่งตอบกลับมา

2.1.5 ความยาวส่วนหัว (Header LENgth: HLEN) เป็นฟิลด์ที่ระบุความยาวส่วนหัวมีขนาดเป็นจำนวนเท่าของ 4 บิต และใน 4 บิต สามารถแทนตัวเลขระหว่าง 0 ถึง 15 ดังนั้น ความกว้างของส่วนหัวที่มีค่าสูงสุดได้ 60 ไบต์ และขนาดเล็กที่สุดของส่วนหัวมีขนาด 20 ไบต์ โดยส่วนที่เหลืออีก 40 ไบต์ ใช้ในส่วนเพิ่มเติม (option)

2.1.6 ฟิลด์สำรอง (Reserverd Field) เป็นฟิลด์ขนาด 6 บิต ซึ่งสำรองไว้เผื่ออนาคต

2.1.7 ฟิลด์ควบคุม (Control Field) เป็นฟิลด์ขนาด 6 บิต อยู่ติดกับฟิลด์สำรองประกอบด้วย 6 บิต ได้แก่ บิต URG ACK PSH RST SYN และ FIN แต่ละบิตทำหน้าที่เป็นอิสระจากกัน ดังนี้

1) URG (URGent Point Field Significant) เป็นบิตที่ใช้กำหนดว่าข้อมูลในเซกเมนต์นี้ต้องการการดำเนินการโดยด่วน

2) ACK (ACKnowledgment Field SSignificant) เป็นบิตที่แสดงสถานการณ์ตอบรับ ถ้าบิตเป็น 1 แสดงว่า หมายเลขลำดับเซกเมนต์ของการตอบรับในลำดับถัดไปนั้น ผู้รับกำลังรอคอยอยู่ และถ้าบิตเป็น 0 แสดงว่า ผู้รับไม่ต้องสนใจ

3) PSH (PuSH Function) เป็นบิตที่บอกให้ผู้รับปลายทางส่งข้อมูลที่เก็บไว้ในบัฟเฟอร์ให้กับระดับชั้นประยุกต์ได้ทันที

4) RST (ReSeT The Connection) เป็นบิตที่ใช้สำหรับการตั้งค่าใหม่ หรือเพื่อเปิดการเชื่อมต่อรอบใหม่

5) SYN (SYHchronize The Sequence Numbers) เป็นบิตที่แสดงความต้องการให้มีการดำเนินการประสานเวลา หรือการซิงโครไนซ์ระหว่างผู้ส่งและผู้รับ

6) FIN (FINish) เป็นบิตที่ใช้สำหรับการหยุดการเชื่อมต่อ

2.1.8 ขนาดหน้าต่าง (Window Size) เป็นฟิลด์ขนาด 16 บิต ที่ใช้ระบุขนาดของหน้าต่างซึ่งใช้สำหรับการเลื่อนหน้าต่าง (Sliding-Window)

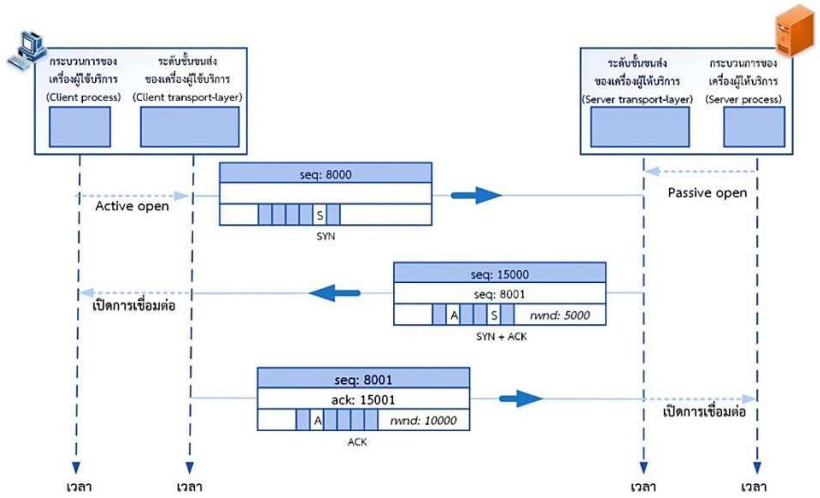
2.1.9 การตรวจสอบผลรวม (Checksum) เป็นฟิลด์ขนาด 16 บิต ใช้ตรวจสอบข้อผิดพลาดของข้อมูล

2.1.10 ตัวชี้เร่งด่วน (Urgent Pointer) เป็นฟิลด์ที่ใช้ระบุตำแหน่งสุดท้ายของข้อมูลที่ฝ่ายผู้ส่งต้องการจะส่งอย่างเร่งด่วนไปยังฝ่ายผู้รับ ฟิลด์นี้จะใช้งานควบคู่กับ URG เมื่อบิต URG มีการกำหนดค่า แสดงว่าข้อมูลในเซกเมนต์นี้ต้องการการดำเนินการโดยด่วน

2.1.11 ทางเลือกและการกำหนดรายละเอียดเพิ่มเติม (Options and Padding) เป็นฟิลด์ที่สามารถเลือกได้ว่าจะใช้หรือไม่ใช้ก็ได้ในกรณีที่ต้องการส่งข้อมูลเพิ่มเติมให้กำหนดค่าไว้ที่นี้

2.2 การเชื่อมต่อของโพรโทคอลทีซีพี ประกอบด้วย 3 สถานะ มีรายละเอียดดังนี้

2.2.1 การสร้างการเชื่อมต่อ (Connection Establishment) ในโพรโทคอล TCP เรียกว่าการทำแฮนด์เชค 3 ขั้นตอน (Three-way Handshaking) ดังภาพที่ 10.19



ภาพที่ 10.19 แสดงการสร้างการเชื่อมแบบการทำแฮนด์เชค 3 ขั้นตอน

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-32)

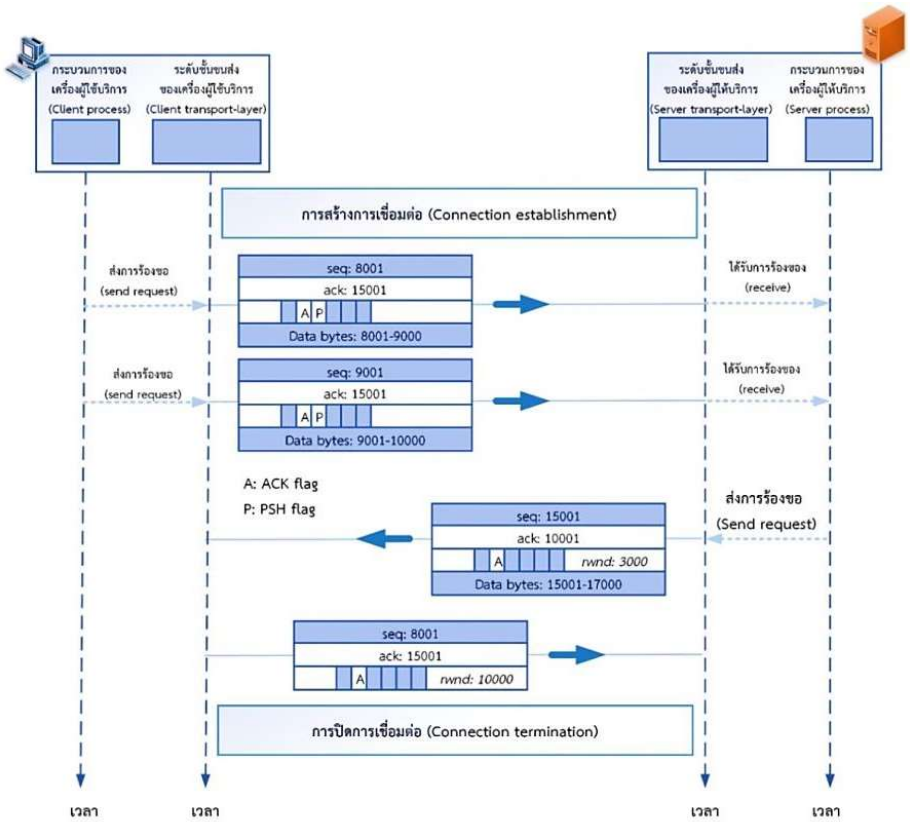
จากภาพที่ 10.19 การสร้างการเชื่อมต่อแบบการทำแฮนด์เชค 3 ขั้นตอน เมื่อเครื่องผู้ใช้บริการ ต้องการเชื่อมต่อกับเครื่องผู้ให้บริการ โดยใช้โพรโทคอล TCP ในระดับชั้นขนส่ง โดยเครื่องผู้ให้บริการจะบอกโพรโทคอล TCP ว่าเตรียมพร้อมกับการเชื่อมต่อแล้ว (เรียกว่า Passive Open) ต่อมามีเครื่องผู้ใช้บริการได้ส่งการร้องขอเพื่อเชื่อมต่อ (เรียกว่า Active Open) โพรโทคอล TCP จะเริ่มขั้นตอนการทำแฮนด์เชค 3 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 เครื่องผู้ใช้บริการจะส่งเซกเมนต์ SYN โดยทำการเซ็คบิต SYN ในฟิลด์ควบคุมและส่งเลขลำดับเซกเมนต์ (seq: 8000) ไปให้เครื่องผู้ให้บริการ ซึ่งเซกเมนต์นี้จะเป็นหมายเลขลำดับของการทำซิงโครไนซ์ (Synchronization)

ขั้นตอนที่ 2 เมื่อเครื่องผู้ให้บริการได้รับ SYN จากเครื่องผู้ใช้บริการแล้ว จะส่งเซกเมนต์ SYN + ACK โดยทำการเซ็ตบิต SYN และ ACK ในฟิลด์ควบคุม หมายถึงเครื่องผู้ให้บริการแสดงการตอบรับการเชื่อมต่อกับเครื่องผู้ใช้บริการ พร้อมส่งรายละเอียดหมายเลขลำดับเซกเมนต์ มีค่าเป็น seq: 15000 และหมายเลขแจ้งการรับรู้ (ack: 8001) รวมทั้งขนาดหน้าต่างของผู้รับ มีค่าเป็น rwnd: 5000

ขั้นที่ 3 เมื่อเครื่องผู้ใช้บริการได้รับ SYN+ACK แล้วเครื่องผู้ใช้บริการจะส่งเซกเมนต์ ACK โดยการเซ็ตบิต ACK ในฟิลด์ควบคุม หมายความว่า เครื่องผู้ใช้บริการแสดงการรับทราบการเชื่อมต่อกับเครื่องผู้ให้บริการ พร้อมส่งรายละเอียดหมายเลขลำดับเซกเมนต์ (sep: 8001) และหมายเลขแจ้งการรับรู้ (ack: 15001) รวมทั้งขนาดหน้าต่าง (rwnd: 10000)

2.2.2 การส่งผ่านข้อมูล (Data Transfer) หลังจากทำการสร้างการเชื่อมต่อแล้ว การส่งผ่านข้อมูลในโพรโทคอล TCP แบบสองทิศทาง (Bidirection) จะเริ่มจากทั้งเครื่องผู้ใช้บริการและเครื่องผู้ให้บริการทำการส่งข้อมูลและแจ้งการรับรู้ (Acknowledgment) ดังภาพที่ 10.20



ภาพที่ 10.20 แสดงการส่งผ่านข้อมูล

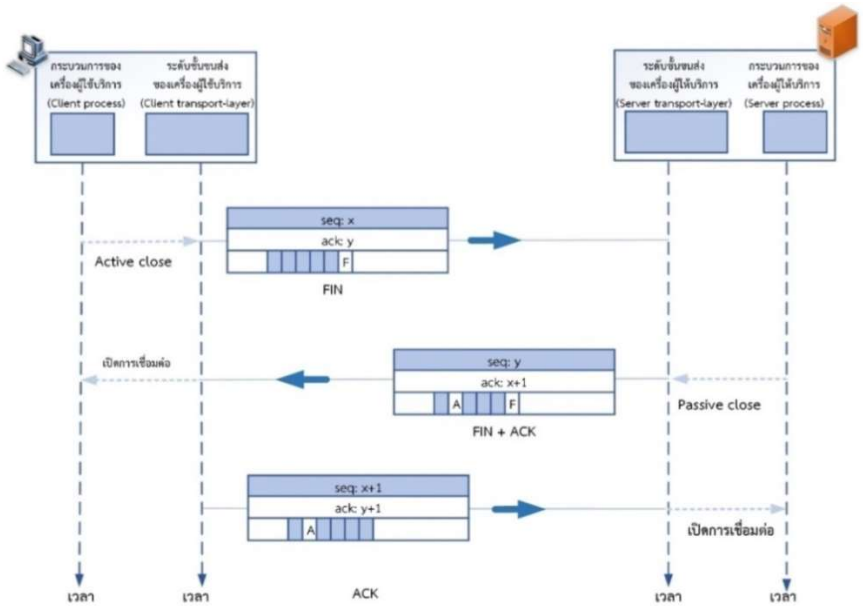
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-34)

จากภาพที่ 10.20 ซึ่งเป็นตัวอย่างหลังจากที่มีการสร้างการเชื่อมต่อเรียบร้อย เครื่องใช้บริการทำการส่งการร้องขอ (Send Request) ข้อมูลจำนวน 2 เซกเมนต์ๆ ละ 1,000 ไบต์ รวมทั้งเซ็ตบิต ACK และ PSH ในฟิลด์ควบคุม (การเซ็ตบิต PSH เพื่อให้เครื่องผู้ให้บริการ TCP ทราบว่าให้ทำการส่งข้อมูลทันที) เมื่อเครื่องผู้ให้บริการได้รับการร้องขอแล้ว จะเริ่มส่งข้อมูลให้เครื่องผู้ใช้บริการตามที่ร้องขอ หลังจากที่เครื่องผู้ใช้บริการได้รับข้อมูลตามที่ร้องขอแล้ว จะส่งเซกเมนต์ที่เซ็ตบิต ACK เพื่อเป็นการแจ้งการรับรู้และจะไม่มีการส่งข้อมูลอีก เป็นการสิ้นสุดการส่งผ่านข้อมูล

2.2.3 การปิดการเชื่อมต่อ (Connection Termination) มี 2 ตัวเลือก ได้แก่ การทำแฮนด์เชค 3 ขั้นตอน และการทำแฮนด์เชค 4 ขั้นตอน แบบการเลือกปิดแบบครึ่งทาง ดังนี้

1) การทำแฮนด์เชค 3 ขั้นตอน สำหรับปิดการเชื่อมต่อ

การทำแฮนด์เชค 3 ขั้นตอน สำหรับการปิดการเชื่อมต่อ เริ่มต้นจากเครื่องผู้ใช้บริการ TCP ได้รับกระบวนการคำสั่งปิดการเชื่อมต่อจากเครื่องผู้ใช้บริการ (Active Code) จึงส่งเซกเมนต์ FIN ไปให้เครื่องผู้ให้บริการ เมื่อเครื่องผู้ให้บริการ TCP ได้รับเซกเมนต์ FIN แล้ว จึงส่งเซกเมนต์ FIN และ ACK ไปให้เครื่องผู้ใช้บริการ TCP เพื่อยืนยันว่าได้รับเซกเมนต์ FIN และจะทำการปิดการเชื่อมต่อ หลังจากนั้นเครื่องผู้ใช้บริการ TCP จะทำการส่งเซกเมนต์ ACK เพื่อยืนยันการได้รับการแจ้งปิดการเชื่อมต่อจากเครื่องผู้ให้บริการ TCP ดังภาพที่ 10.21



ข้อสังเกต: x และ y เป็นหมายเลขลำดับใดๆ เพียง 1 หมายเลข

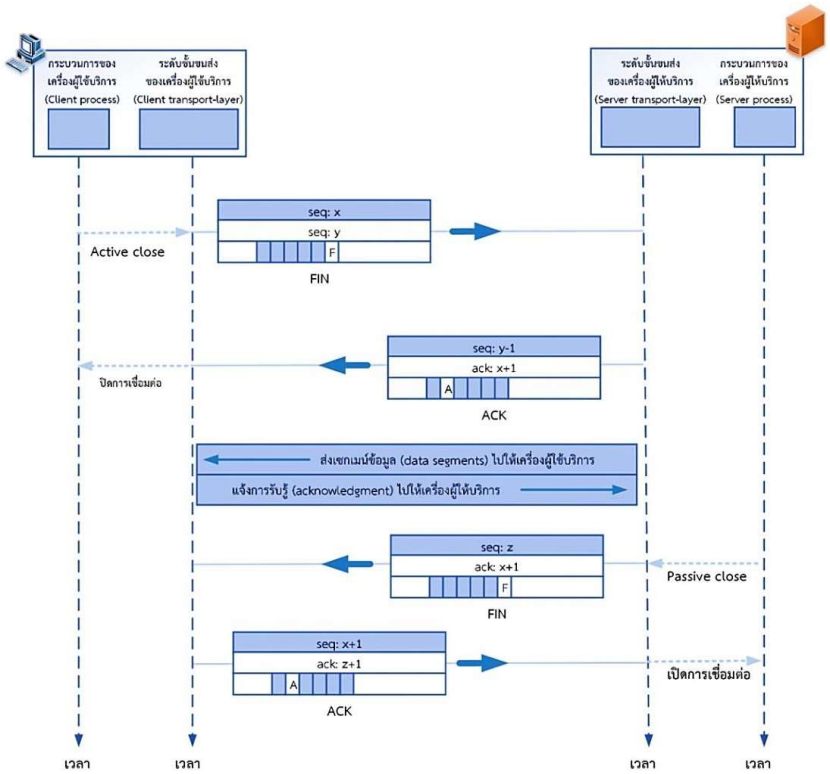
ภาพที่ 10.21 แสดงการทำแฮนด์เชค 3 ขั้นตอนสำหรับปิดการเชื่อมต่อ

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-35)

2) การทำแฮนด์เชค 4 ขั้นตอน

การทำแฮนด์เชค 4 ขั้นตอน ด้วยการเลือกปิดแบบครึ่งทาง (Four-way hand-shaking with half-close option) จะมีการนำไปใช้เกี่ยวกับการจัดเรียงข้อมูล (Sorting) เช่น

เครื่องผู้ใช้บริการส่งข้อมูลไปให้เครื่องผู้ให้บริการ โดยเครื่องผู้ให้บริการจะต้องรับข้อมูลทั้งหมดมาก่อน จากนั้นเครื่องผู้ใช้บริการส่งข้อมูลหมดแล้วสามารถปิดการเชื่อมต่อได้ เมื่อเครื่องผู้ให้บริการได้รับข้อมูลทั้งหมดแล้ว จะยังคงเปิดการเชื่อมต่อเพื่อทำการจัดเรียงข้อมูล ดังภาพที่ 10.22



ข้อสังเกต: x, y และ z เป็นหมายเลขลำดับใดๆ เพียง 1 หมายเลข

ภาพที่ 10.22 แสดงการทำแฮนด์เชค 4 ขั้นตอนด้วยการเลือกปิดแบบครึ่งทาง
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-36)

จากภาพที่ 10.22 เมื่อการส่งผ่านข้อมูลจากเครื่องผู้ใช้บริการไปยังเครื่องผู้ให้บริการสิ้นสุดแล้ว เครื่องผู้ใช้บริการจะทำการเชื่อมต่อโดยการเลือกปิดแบบครึ่งทางด้วยการส่งเซกเมนต์ FIN เมื่อเครื่องผู้ให้บริการได้ยอมรับการเชื่อมต่อแบบครึ่งทางด้วยการส่งเซกเมนต์ ACK กลับไปให้เครื่องผู้ใช้บริการ โดยเครื่องผู้ให้บริการจะยังคงส่งข้อมูลจนกระทั่งส่งข้อมูลเรียบร้อยแล้ว จึงทำการส่งเซกเมนต์ FIN กลับไปให้เครื่องผู้ใช้บริการ เมื่อเครื่องผู้ให้บริการรับทราบแล้วจึงส่งเซกเมนต์ ACK ตอบกลับไปให้เครื่องผู้ให้บริการ

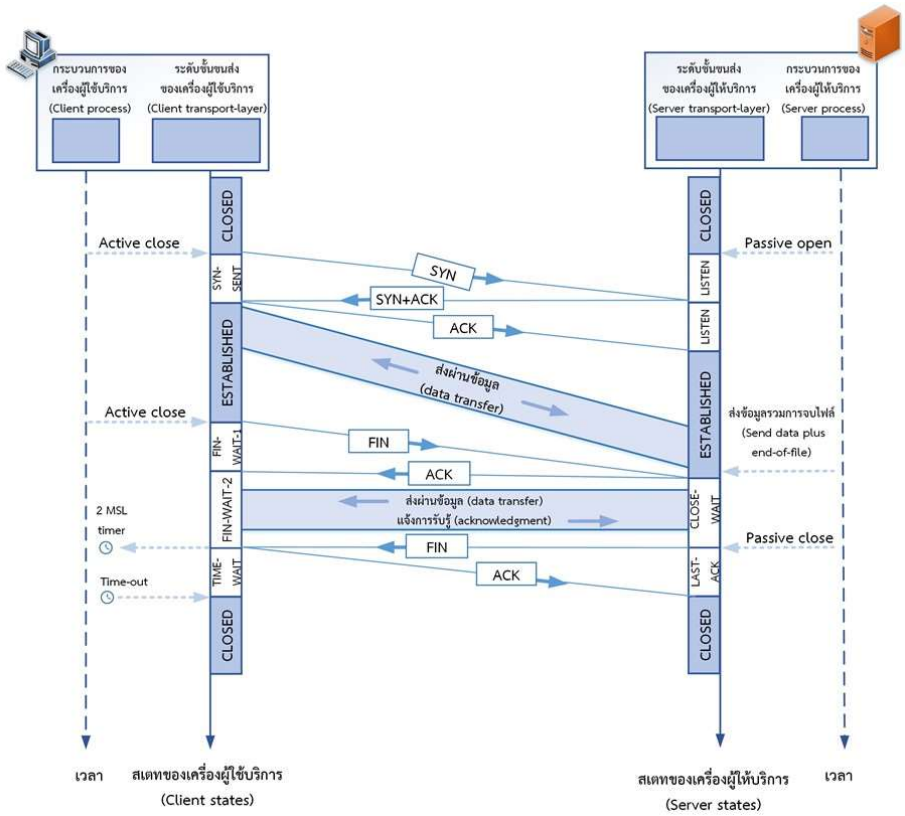
หลังจากทำการเชื่อมต่อแบบครึ่งทาง เครื่องผู้ให้บริการสามารถส่งข้อมูลไปให้เครื่องผู้ใช้บริการ และเครื่องผู้ใช้บริการจะสามารถแจ้งการรับรู้ไปให้เครื่องผู้ให้บริการได้ แต่เครื่องผู้ใช้ บริการไม่สามารถส่งข้อมูลใดๆ ไปให้เครื่องผู้ให้บริการได้

2.3 ไดอะแกรมการเปลี่ยนสเตท (State Transition Diagram) ในโพรโทคอล TCP เป็นเหตุการณ์ใดๆ ที่เกิดขึ้นในระหว่างที่มีการเชื่อมต่อ โดยเริ่มจากการสร้างการเชื่อมต่อ การส่งผ่านข้อมูลรวมทั้งการปิดการเชื่อมต่อ โดยโพรโทคอล TCP ได้กำหนดสถานะหรือสเตท (State) ว่า ไฟไนต์สเตทแมชชีน (Finite State Machine: FSM) มีรายการสเตทของโพรโทคอล TCP ดังแสดงในตารางที่ 10.2 และภาพที่ 10.23

ตารางที่ 10.2 รายการสเตทของโพรโทคอล TCP

สเตท (state)	รายละเอียด
CLOSED	ไม่มีการเชื่อมต่อ (no connection exists)
LISTEN	ได้รับคำสั่งจากเครื่องผู้ใช้บริการให้สร้างการเชื่อมต่อ; รอคำสั่ง SYN (Passive open received; waiting for SYN)
SYN-SENT	ส่งคำสั่ง SYN; รอคำสั่ง ACK (SYN sent; waiting for ACK)
SYN-RCVD	สั่งคำสั่ง SYN + ACK; รอคำสั่ง ACK (SYN + ACK sent; waiting for ACK)
ESTABLISHED	สร้างการเชื่อมต่อ; กำลังดำเนินการส่งผ่านข้อมูล (connection establishments; data transfer in progress)
FIN-WAIT-1	ส่งคำสั่ง FIN ครั้งที่ 1; รอคำสั่ง ACK (first FIN sent; waiting for ACK)
FIN-WAIT-2	ได้รับ ACK จากการส่งคำสั่ง FIN ครั้งที่ 1; รอคำสั่ง FIN ครั้งที่ 2 (ACK to first FIN received; waiting for second FIN)
CLOSE-WAIT	ได้รับคำสั่ง FIN ครั้งที่ 1, ได้ส่งคำสั่ง ACK แล้ว; รอปิดการเชื่อมต่อ (first FIN received, ACK sent; waiting for application to close)
TIME-WAIT	ได้รับคำสั่ง FIN ครั้งที่ 2, ได้ส่งคำสั่ง ACK แล้ว; รอให้หมดระยะเวลาสองรอบของการส่งเซกเมนต์ของโพรโทคอล TCP (second FIN received, ACK sent; waiting for 2 MSL[1] time-out)
LAST-ACK	ส่งคำสั่ง FIN ครั้งที่ 2; รอคำสั่ง ACK (Second FIN sent; waiting for ACK)
CLOSING	ปิดการเชื่อมต่อทั้งเครื่องผู้ใช้บริการและเครื่องผู้ให้บริการทันที (both sides decide to close simultaneously)

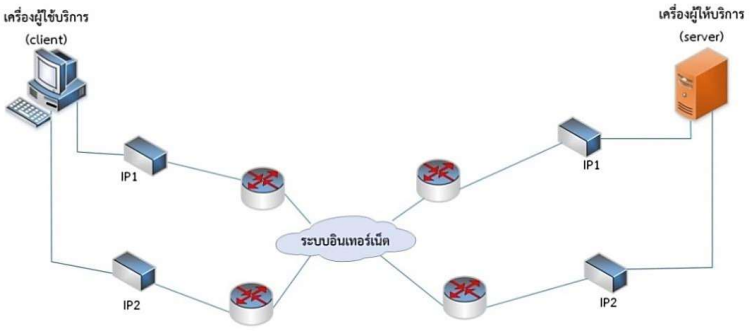
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-6)



ภาพที่ 10.23 แสดงไดอะแกรมของการเปลี่ยนสเตทตามแกนเวลาสำหรับสถานการณ์ทั่วไป
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-37)

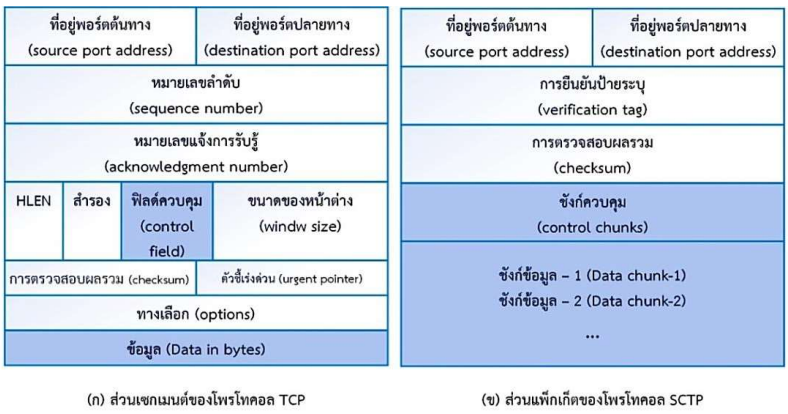
3. โพรโทคอลเอสซีทีพี (Stream Control Transmission Protocol: SCTP) เป็นโพรโทคอลที่สนับสนุนระบบงานประยุกต์ใหม่ๆ โดยรวมเอาคุณลักษณะที่ดีของโพรโทคอล UDP และโพรโทคอล TCP เข้าไว้ด้วยกัน สำหรับการเชื่อมต่อแบบมัลติมีเดีย (Multimedia Communication) โดยการติดต่อสื่อสารของโพรโทคอล SCTP เป็นแบบกระบวนการถึงกระบวนการ (Process-to-Process)

3.1 มัลติโฮมมิง (Multihoming) การเชื่อมต่อของโพรโทคอล SCTP เป็นการเชื่อมต่อได้หลายไอพีแอดเดรส เรียกว่า การให้บริการแบบมัลติโฮมมิง เมื่อเครื่องผู้ใช้บริการได้ทำการเชื่อมต่อกับเครือข่ายท้องถิ่นจำนวน 2 แห่ง โดยใช้ 2 ไอพีแอดเดรส (IP1 และ IP2) ฝั่งเครื่องผู้ให้บริการมีการเชื่อมต่อกับสองเครือข่ายท้องถิ่น (LAN) ผ่านโพรโทคอล SCTP ดังภาพที่ 10.24



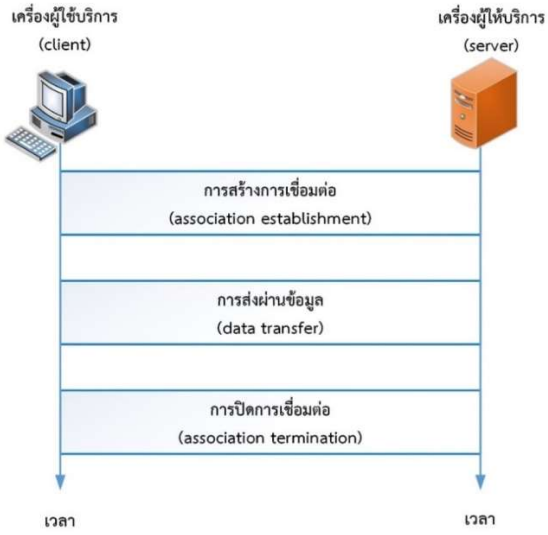
ภาพที่ 10.24 แสดงแนวคิดของมัลติโฮมมิง
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-40)

3.2 รูปแบบแพ็กเก็ตของโพรโทคอลเอสซีทีพี แพ็กเก็ตของโพรโทคอล SCTP ประกอบด้วยส่วนของชังก์ข้อมูล (Data Chunk) และส่วนของชังก์ควบคุม (Control Chunk) โดยส่วนแพ็กเก็ตของโพรโทคอล SCTP จะมีบทบาทหน้าที่เหมือนกับส่วนเซกเมนต์ของโพรโทคอล TCP ดังแสดงการเปรียบเทียบของส่วนเซกเมนต์ของโพรโทคอล TCP และส่วนแพ็กเก็ตของโพรโทคอล SCTP โดยส่วนควบคุมในโพรโทคอล SCTP จะประกอบด้วยส่วนควบคุมที่แบ่งออกเป็นหลายๆ ส่วนที่เรียกว่า ชังก์ (Chunk) แต่ละชังก์มีขนาด 4 ไบต์ ในขณะที่ส่วนควบคุมของโพรโทคอล TCP เป็นฟิลด์ควบคุมประกอบด้วย 6 บิต และในส่วนของชังก์ข้อมูลของโพรโทคอล SCTP จะมีหลายชังก์ซึ่งแต่ละชังก์มีขนาด 4 ไบต์ ดังภาพที่ 10.25



ภาพที่ 10.25 แสดงการเปรียบเทียบระหว่างเซกเมนต์ของ TCP และแพ็กเก็ตของ SCTP
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-41)

3.3 การเชื่อมต่อของโพรโทเอสซีทีพี การเชื่อมต่อของโพรโทรคอลมี 3 สถานะ ได้แก่ การสร้างการเชื่อมต่อ (Association Establishment) การส่งผ่านข้อมูล (Data Transfer) และการปิดการเชื่อมต่อ (Association Termination) ดังภาพที่ 10.26



ภาพที่ 10.26 แสดงการเชื่อมต่อของโพรโทคอล SCTP

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-41)

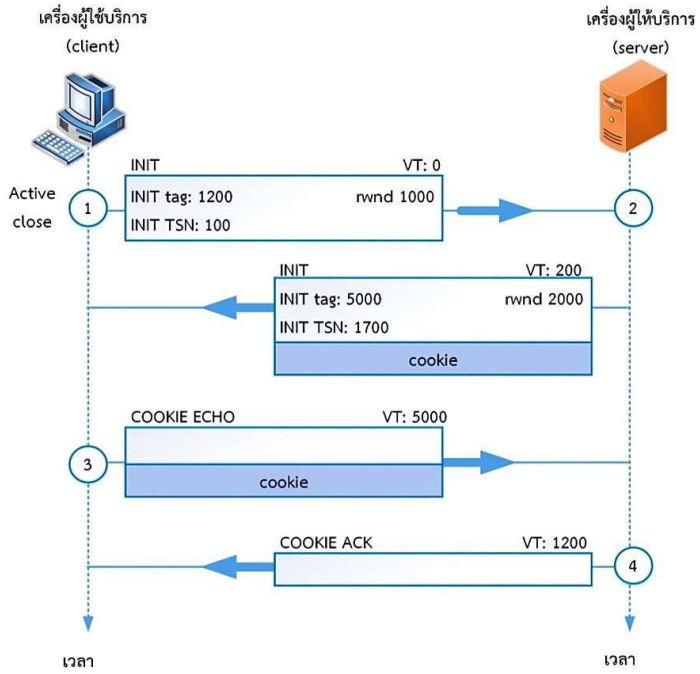
การสร้างการเชื่อมต่อของโพรโทคอลซีทีพี มีดังนี้

3.3.1 การสร้างการเชื่อมต่อของโพรโทคอล SCTP (Association Establishment) จำเป็นต้องใช้การทำแฮนด์เชค 4 ขั้นตอน โดยกระบวนการทำงานเริ่มต้นเมื่อเครื่องผู้ใช้บริการต้องการสร้างการเชื่อมต่อกับเครื่องผู้ให้บริการผ่านโพรโทคอล SCTP ในระดับชั้นขนส่ง โดยมี 4 ขั้นตอน ซึ่งมีการส่งแพ็กเก็ตที่ประกอบด้วยชนิดของชังก์ ตามตารางที่ 10.3 ดังแสดงในขั้นตอนในภาพที่ 10.27

ตารางที่ 10.3 ชนิดของชังก์ (Type of Chunks)

ชนิด (type)	คำสั่งของชังก์ (chunk)	รายละเอียด (description)
0	DATA	ข้อมูลผู้ใช้งาน (User Data)
1	INIT	การเริ่มติดตั้งการเชื่อมต่อ (Set up an association)
2	INIT ACK	แจ้งการรับรู้ชังก์ของ INIT (Acknowledges INIT Chunk)
3	SACK	เลือกการแจ้งการรับรู้ (Selective Acknowledgment)
4	HEARTBEAT	ตรวจสอบการใช้งานในระดับเดียวกัน (Probes the peer for liveliness)
5	HEARTBEAT ACK	แจ้งการรับรู้ชังก์ของ HEARTBEAT (Acknowledges HEARTBEAT Chunk)
6	ABORT	ยกเลิกการเชื่อมต่อ (Aborts an Association)
7	SHUTDOWN	ปิดการเชื่อมต่อ (Terminates an Association)
8	SHUNDOWN ACK	แจ้งการรับรู้ชังก์ของ SHUTDOWN (Acknowledge SHUTDOWN Chunk)
9	ERROR	รายงานข้อผิดพลาดโดยปราศจากการปิดการเชื่อมต่อ (Reports errors without shutting down)
10	COOKIE ECHO	แพ็กเก็ตที่ 3 ในการสร้างการเชื่อมต่อ (Third packet in Association Establishment)
11	COOKIE ACK	แจ้งการรับรู้ของ COOKIE (Acknowledge COOKIE Chunk)
14	SHUTDOWN COMPLETE	แพ็กเก็ตที่ 3 ในการปิดการเชื่อมต่อ (Third packet in association termination)
192	FORWARD TSN	การปรับค่าหมายเลขลำดับการขนส่ง (Transmission Sequence Number: TSN) (for adjusting cumulating TSN)

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-42)



ภาพที่ 10.27 แสดงการสร้างการเชื่อมต่อด้วยการทำแฮนด์เชค 4 ขั้นตอนของโพรโทคอล SCTP
ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-43)

จากภาพ 10.27 แสดงการสร้างการเชื่อมต่อด้วยการทำแฮนด์เชค 4 ขั้นตอนของโพรโทคอล SCTP มีขั้นตอนดังนี้

ขั้นตอนที่ 1 เครื่องผู้ใช้บริการส่งแพ็กเก็ตแรกบรรจุชังก์ของ INIT โดยมีหมายเลขการยืนยันป้ายระบุ (Verification tag: VT) เป็น 0 เพราะว่ายังไม่มีการยืนยันป้ายระบุสำหรับการส่งจากเครื่องผู้ใช้บริการมายังเครื่องผู้ให้บริการในขั้นตอนนี้ โดยส่วนชังก์ของ INIT ประกอบด้วย Init tag: 1200 เป็นป้ายระบุสำหรับแพ็กเก็ตที่ส่งจากเรื่องผู้ให้บริการมายังเครื่องผู้ใช้บริการ โดยกำหนด Init TSN: 100 และ rwnd: 1000 สังเกตว่า ในขั้นตอนนี้ยังไม่มีการส่งชังก์ข้อมูล

ขั้นตอนที่ 2 เครื่องผู้ให้บริการส่งแพ็กเก็ตที่ 2 ซึ่งบรรจุชังก์ของ INIT ACK โดยมีหมายเลขการยืนยันป้ายระบุ เป็น 1,200 (ตามที่กำหนด Init tag: 1200 จากแพ็กเก็ตแรกในขั้นตอนที่ 1) โดยส่วนชังก์ของ INIT ACK ประกอบไปด้วย Init tag: 5000 เป็นป้ายระบุจำนวนแพ็กเก็ตที่ส่งมาจากเครื่องผู้ใช้บริการมายังเครื่องผู้ให้บริการ โดยกำหนด Init TSN: 1700 สำหรับการส่งข้อมูล (Data Flow) จากเครื่องผู้ให้บริการมายังเครื่องผู้ใช้บริการ และกำหนด

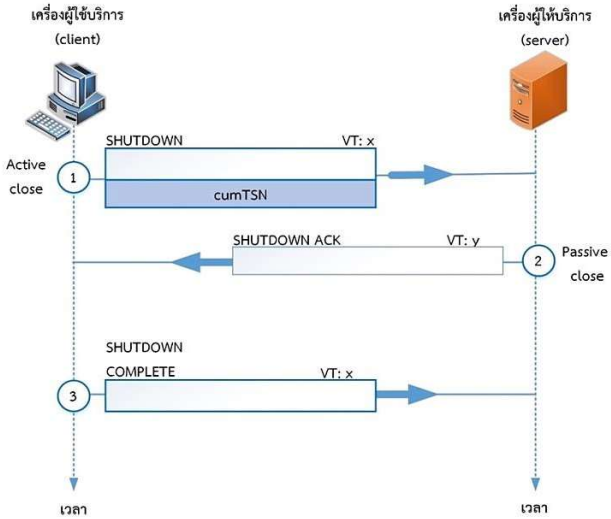
rwnd: 2000 เพื่อเป็นการอนุญาตให้เครื่องผู้ใช้บริการส่งชังก์ข้อมูลมากับแพ็กเก็ตที่ 3 ได้ และจะส่ง COOKIE ไปให้เครื่องผู้ใช้บริการ

ขั้นตอนที่ 3 เครื่องผู้ใช้บริการส่งกับแพ็กเก็ตที่ 3 บรรจุชังก์ของ COOKIE ECHO ที่มี VT: 5000 โดยเป็นการตอบกลับสถานะของ COOKIE ตามที่เครื่องผู้ให้บริการส่งมา โดยโพรโทคอล SCTP อนุญาตให้มีการรวมชังก์ของข้อมูลในแพ็กเก็ตนี้ได้

ขั้นตอนที่ 4 เครื่องผู้ให้บริการส่งแพ็กเก็ตที่ 4 บรรจุชังก์ของ COOKIE ACK เพื่อเป็นการแจ้งการยืนยันชังก์ของ COOKIE ECHO โดยโพรโทคอล SCTP อนุญาตให้มีการรวมชังก์ของข้อมูลในแพ็กเก็ตนี้ได้

3.3.2 การส่งผ่านข้อมูลของโพรโทคอล SCTP หลังจากทำการสร้างการเชื่อมต่อแล้ว การส่งผ่านข้อมูลเป็นแบบสองทิศทาง โดยมีการส่งข้อมูลทั้งเครื่องผู้ใช้บริการและเครื่องผู้ให้บริการ โดยการส่งข้อมูลของโพรโทคอล SCTP จะมีการส่งข้อมูลแบบมัลติโฮมมิง คือ การอนุญาตให้มีการติดต่อสื่อสารได้หลายๆ ไอพีแอดเดรส โดยจะมี 1 ไอพีแอดเดรสที่มีการกำหนดให้เป็นไอพีแอดเดรสหลัก โดยกำหนดระหว่างระยะการสร้างการเชื่อมต่อของโพรโทคอล SCTP โดยไอพีแอดเดรสที่เหลือจะเป็นไอพีแอดเดรสทางเลือก สังเกตว่าแอดเดรสต้นทางจะเป็นไอพีแอดเดรสหลักของแอดเดรสปลายทาง

3.3.3 การปิดการเชื่อมต่อของโพรโทคอล SCTP จะใช้การส่ง 3 แพ็คเก็ตเป็นการปิดการเชื่อมต่อ ดังภาพที่ 10.28



ภาพที่ 10.28 แสดงการปิดการเชื่อมต่อของโพรโทคอล SCTP

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-44)

จากภาพที่ 10.28 แสดงการปิดการเชื่อมต่อของโพรโทคอล SCTP จะใช้การส่ง 3 แพ็คเก็ต เป็นการปิดการเชื่อมต่อมีขั้นตอน ดังนี้

ขั้นตอนที่ 1 เมื่อเครื่องผู้ใช้บริการต้องการปิดการเชื่อมต่อเรียกว่า active open จัดส่งชังก์ของ SHUTDOWN ที่มีหมายเลขยืนยันป้ายระบุเป็น xโดยไม่ระบุหมายเลขชังก์ของ cumTSN (เป็นเครื่องหมายลำดับไบต์สุดท้ายที่ได้รับ) ไปให้เครื่องผู้ให้บริการ

ขั้นตอนที่ 2 เครื่องผู้ให้บริการต้องการปิดการเชื่อมต่อ เรียกว่า passive close จะส่งชังก์ของ SHUTDOWN ACK ที่มีหมายเลขยืนยันป้ายระบุเป็น y กลับไปให้เครื่องผู้ใช้บริการ

ขั้นตอนที่ 3 เครื่องผู้ใช้บริการส่งชังก์ของ SHUTDOWN COMPLETE ที่มีหมายเลขยืนยันป้ายระบุเป็น x ไปให้เครื่องผู้ให้บริการเพื่อยืนยันการปิดการเชื่อมต่อ

4. ระดับประยุกต์ หรือระดับชั้นแอปพลิเคชัน ระดับชั้นประยุกต์ เป็นระดับชั้นที่เกี่ยวข้องกับระบบงานประยุกต์ ซึ่งมีการจัดเตรียมโพรโทคอลต่างๆ เพื่อสนับสนุนการบริการให้กับผู้ใช้งาน โดยโพรโทคอลสำคัญๆ จะกล่าวโดยสังเขป ดังนี้

4.1 โพรโทคอลดีเอชซีพี (Dynamic Host Configuration Protocol:DHCP) เป็นโพรโทคอลที่ใช้กำหนดหรือจัดสรรหมายเลขไอพีแอดเดรสจากเครื่องหนึ่งไปยังอีกเครือข่ายหนึ่ง หรือมีการเชื่อมต่อหรือตัดออกจากเครือข่าย ซึ่งไม่สามารถใช้แอดเดรสกายภาพ (Physical Address) ไอพีแอดเดรสชุดเก่าของโฮสต์นั้นๆ ได้

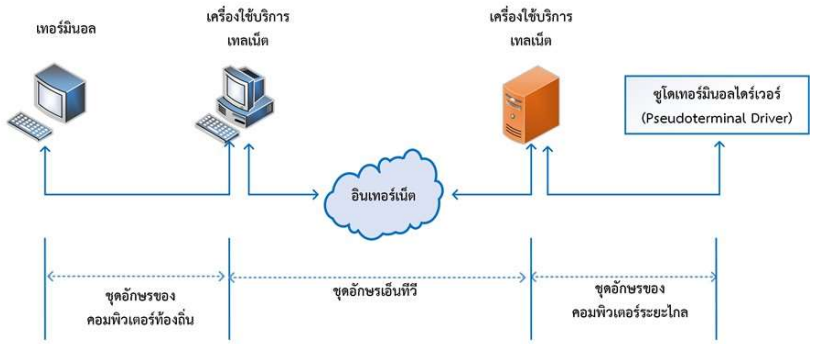
4.2 โพรโทคอลดีเอ็นเอส (Domain Name System: DNS) เป็นโพรโทคอลที่ใช้ชื่อโดเมนแทนการระบุด้วยไอพีแอดเดรส เมื่อโพรโทคอล DNS ทำงานร่วมกับโพรโทคอล TCP/IP โดยโพรโทคอล DNS ทำหน้าที่เชื่อมต่อระหว่างชื่อโดเมนกับไอพีแอดเดรสนั้นๆ การใช้ชื่อโดเมนแทนไอพีแอดเดรสเพราะสะดวกในการจดจำมากกว่า

4.3 โพรโทคอลเทลเน็ต (TELecommunication NET: TELNET) เป็นโพรโทคอลที่ช่วยทำให้เทอร์มินอล (Terminal) ใดๆ สามารถเชื่อมต่อระบบเครือข่ายจากระยะไกลได้ โดยการทำตัวเสมือนเป็นเทอร์นิมอลหนึ่งของเครือข่ายแบบระยะไกลด้วยวิธีการทำรีโมทล็อกอิน (Remote Login)

เมื่อผู้ใช้งานต้องการเข้าถึงโปรแกรมบนเครือข่ายจากระยะไกล จะทำการรีโมทล็อกอินโดยการกรอกข้อมูลใดๆ ลงไปบนระบบปฏิบัติการของเครื่องผู้ใช้งานเพื่อเข้าใช้งานระบบเครือข่ายจากระยะไกล เครื่องผู้ใช้งานจะรับตัวอักษรที่เป็นข้อมูลดังกล่าวโดยไม่ทำการตีความ จากนั้นจะทำการส่งตัวอักษรนั้นไปยังโปรแกรมเทลเน็ตของฝ่ายผู้ใช้งาน ซึ่งโปรแกรมจะทำการ

แปลงตัวอักษรดังกล่าวให้อยู่ในรูปของชุดอักษรเอ็นวีที (Network Virtual Terminal characters: NVT characters) และส่งต่อไปยังโพรโทคอล TCP/IP ของผู้ใช้งาน ข้อความดังกล่าวจะส่งผ่านระบบอินเทอร์เน็ตมายังโพรโทคอล TCP/IP ที่ฝ่ายเครือข่ายทางไกล และเมื่อได้รับตัวอักษรแล้วระบบ ปฏิบัติการจะทำการส่งผ่านไปยังบริการเทลเน็ต (telnet services) ซึ่งเป็นบริการที่รับผิดชอบการแปลงตัวอักษรให้อยู่ในรูปแบบที่ระบบเครือข่ายทางไกลสามารถเข้าใจได้

อย่างไรก็ ตามตัวอักษรไม่สามารถผ่านโดยตรงไปยังระบบปฏิบัติการได้ เพราะว่าระบบปฏิบัติการไม่ได้ออกแบบมาให้รับตัวอักษรจากบริการเทลเน็ต วิธีแก้ปัญหา คือ การติดตั้งซอฟต์แวร์เพิ่มเติม เรียกว่า ซูโดเทอร์มินอลไดร์เวอร์ (Pseudotermianl Driver) เพื่อทำให้เสมือนว่าตัวอักษรมาจากเทอร์มินอล แล้วระบบปฏิบัติการจะทำการส่งผ่านตัวอักษรนั้นไปยังโปรแกรมอื่นๆ ต่อไป ดังภาพที่ 10.29



ภาพที่ 10.29 แสดงแนวคิดของชุดอักษร NVT

ที่มา : (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 10-46)

4.4 โพรโทคอลเอฟทีพี (File Transfer Protocol: FTP) เป็นโพรโทคอลที่บริการด้านการทำสำเนาแฟ้มข้อมูลระหว่างโฮสต์กับโฮสต์ แม้ว่าแต่ละโฮสต์จะมีโครงสร้างข้อมูลและวิธีการแสดงข้อมูลที่แตกต่างกันก็ตาม

4.5 โพรโทคอลเอสเอ็มทีพี (Simple Mail Transfer Protocol: SMTP) เป็นโพรโทคอลที่ใช้กำหนดเครื่องผู้ใช้บริการและเครื่องผู้ให้บริการที่รับส่งข้อมูลบนระบบอินเทอร์เน็ต โดยโพรโทคอล SMTP จะทำงานร่วมกับโพรโทคอลพ็อป (Post Office Protocol: POP) ซึ่งเป็นโพรโทคอลแบบเครื่องผู้ใช้บริการ/เครื่องผู้ให้บริการ เพื่อให้บริการไปรษณีย์อิเล็กทรอนิกส์บนระบบอินเทอร์เน็ต

4.6 โพรโทคอลเอชทีทีพี (hypertext Transfer Protocol: HTTP) ใช้สำหรับเข้าถึงข้อมูลบนเวิลด์ไวด์เว็บ จัดเป็นตัวกลางในการรับส่งข้อมูลระหว่างโปรแกรมเบราเซอร์ และเครื่องผู้ให้บริการเว็บ โดยหน้าที่ของโพรโทคอล HTTP จะคล้ายกับการรวมกันของโพรโทคอล FTP และโพรโทคอล SMTP

4.6.1 เวิลด์ไวด์เว็บ เป็นข้อมูลที่มีการเชื่อมต่อเข้าด้วยกันจากทุกจุดบนโลกผ่านระบบเครือข่ายอินเทอร์เน็ต มีลักษณะให้บริการชนิดเครื่องผู้ใช้บริการ/เครื่องผู้ให้บริการแบบกระจาย โดยเครื่องผู้ใช้บริการจะใช้โปรแกรมเบราเซอร์ เพื่อเข้าถึงบริการต่างๆ ซึ่งกระจายอยู่ในหลายๆ ที่เรียกว่า ไซต์ (Sites) แต่ละไซต์ประกอบด้วยเอกสารหลายๆ หน้า โดยเอกสารแต่ละหน้าเรียกว่า หน้าเว็บเพจ (Webpage) เช่น เมื่อผู้ใช้บริการต้องการข้อมูลจากไซต์ ก. จะทำการร้องขอผ่านเบราเซอร์ของไซต์ที่ระบุที่อยู่ของไซต์ที่เรียกว่า โพรโทคอลยูอาร์แอล (URL) จากนั้นเครื่องผู้ให้บริการ ก. จะหาข้อมูลและส่งกลับไปยังเครื่องผู้ใช้บริการ

4.6.2 โพรโทคอลยูอาร์แอล (Uniform Resource Locator: URL) เป็นมาตรฐานสำหรับระบุข้อมูลบนอินเทอร์เน็ต โดยโพรโทคอล URL ประกอบด้วยข้อมูล 4 ส่วน ได้แก่ โพรโทคอล คอมพิวเตอร์โฮสต์ พอร์ต และทางเดิน โดยมีรูปแบบ ดังนี้

protocol://host:port/path

1) protocol เป็นชื่อโพรโทคอล เช่น HTTP เป็นต้น

2) host เป็นคอมพิวเตอร์ที่มีข้อมูลที่ต้องการ

3) port เป็นองค์ประกอบทางเลือกอาจระบุหรือไม่ก็ได้ ถ้าพอร์ตอยู่รวมอยู่ด้วยกันจะเขียนแทรกอยู่ระหว่าง host และ path โดยที่ port จะแยกกับ host ด้วยเครื่องหมายทวิภาค หรือจุดคู่ “:”

4) path เป็นตำแหน่งของแฟ้มข้อมูลซึ่งมีข้อมูลที่ต้องการอยู่ โดยมีเครื่องหมายทับ “/” ก่อนหน้า path

10.4 สรุป

โพรโทคอลทีซีพี/ไอพี ประกอบด้วยโพรโทคอล 2 โพรโทคอล ที่ทำงานในระดับชั้นที่แตกต่างกัน โดยมีโพรโทคอลทีซีพี (Transmission Control Protocol : TCP) ทำงานอยู่ในระดับบน คือทำหน้าที่จัดการแบ่งข้อความหรือไฟล์ที่ผู้ส่งต้องการส่งออกไปเป็นส่วนเล็กๆ ที่เรียกว่า แพ็คเก็ต (Packet) แล้วส่งออกไปบนระบบเครือข่ายอินเทอร์เน็ตผ่านโพรโทคอลทีซีพีในเครื่องคอมพิวเตอร์ของผู้รับ แล้วจะนำข้อความหรือไฟล์แต่ละแพ็คเก็ตที่ได้รับมาประกอบกลับเป็นข้อความหรือไฟล์ตามเดิมและโพรโทคอลไอพี (Internet Protocol: IP) ทำงานอยู่ในระดับล่าง ทำหน้าที่ในการจัดการเกี่ยวกับที่อยู่เครื่องคอมพิวเตอร์ปลายทาง หรือแอดเดรส (Address) ที่ต้องการจะส่งข้อความเป็นแพ็กเก็ตแต่ละแพ็คเก็ตออกไป โดยที่เกตเวย์ (Gateway) แต่ละแห่งที่เชื่อมอยู่ในระบบเครือข่ายจะทำหน้าที่ตรวจสอบที่อยู่ก่อนที่จะส่งข้อความไปให้ ปัจจุบันมีการใช้งานไอพีแอดเดรส 2 รุ่น ได้แก่ ไอพีแอดเดรส รุ่นที่ 4 และ ไอพีแอดเดรส รุ่นที่ 6

แบบจำลองทีซีพี/ไอพี ประกอบด้วยชั้นทั้งหมด 5 ระดับชั้น ได้แก่ ระดับชั้นกายภาพ ระดับชั้นเชื่อมโยงข้อมูล ระดับชั้นเครือข่าย ระดับชั้นขนส่งและระดับชั้นประยุกต์ แต่ละชั้นจะประกอบด้วยโพรโทคอลอิสระต่างๆ หลายชนิด

บทที่ 11
แอปพลิเคชันบนระบบเครือข่าย

ในปัจจุบันเทคโนโลยีได้มีการพัฒนาอย่างต่อเนื่องและรวดเร็ว หนึ่งในเทคโนโลยีที่เกิดขึ้นมา นั้นคือ สมาร์ทโฟนและแท็บเล็ต และด้วยความสามารถต่างๆ ที่มีมากมายและรอบด้านนี้เอง จึงมีผู้นิยมใช้เป็นจำนวนมาก ซึ่งเรียกได้ว่าแทบจะทุกคนต้องมีสมาร์ทโฟน และแท็บเล็ตเพื่อใช้ทำงานหรือเพื่อความบันเทิง ภายในอุปกรณ์สื่อสารนี้จะมีแอปพลิเคชัน (Application) ที่ทำหน้าที่ควบคุมการทำงานของเครือข่ายเรียกว่า Network Application ดังนั้น การทำงานของแอปพลิเคชันบางฟังก์ชันก็สามารถใช้งานบนเครื่องได้ทันที แต่บางฟังก์ชันก็ต้องมีการเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ตจึงจะใช้งานได้

11.1 ความรู้พื้นฐานเกี่ยวกับแอปพลิเคชัน

แอปพลิเคชัน (Application) หมายถึง โปรแกรมต่างๆ ที่สามารถนำมาใช้งานได้โดยการติดตั้งที่เครื่องคอมพิวเตอร์ ซึ่งในอดีตมักจะนำไปติดตั้งและใช้งานโดยการประมวลผลที่เครื่องคอมพิวเตอร์เพียงเครื่องเดียว แต่หลังจากที่มีการนำระบบเครือข่ายเข้ามาใช้งานกันอย่างแพร่หลาย การประมวลผลโปรแกรมต่างๆ ไม่ได้จำกัดอยู่ที่คอมพิวเตอร์เพียงเครื่องเดียวอีกต่อไป เนื่องจากสามารถประมวลผลด้วยคอมพิวเตอร์หลายเครื่องผ่านเครือข่ายได้ โดยโปรแกรมต่างๆ ที่ใช้งานผ่านเครือข่าย และทำงานใน Application Layer จะเรียกว่า Network Application (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 310)

ประเภทของแอปพลิเคชัน

แอปพลิเคชันที่เรานิยมใช้กันบนอุปกรณ์เคลื่อนที่ (Mobile Device) แบ่งรูปแบบของการพัฒนาได้ 3 รูปแบบ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 310-311)

1. Native Application คือ แอปพลิเคชันที่ถูกพัฒนาโดยอาศัย Library หรือ SDK ของแพลตฟอร์ม (Platform) นั้นๆ และจะต้องพัฒนาด้วยภาษาของแต่ละแพลตฟอร์ม เช่น แอนดรอยด์ (Android) ใช้ภาษาจาวา (Java) วินโดวส์โฟน (Windows Phone) ใช้ภาษาซีชาร์ป (C#) และไอโอเอส (iOS) ใช้ภาษาอ็อปเจ็คซี (Object-C) เป็นต้น ทั้งนี้ข้อดีของการพัฒนาแอปพลิเคชันแบบ Native คือ สามารถดึงทรัพยากรของระบบมาใช้งานได้เต็มที่และมีประสิทธิภาพสูงสุด แต่ก็ยังมีข้อเสียก็คือเมื่อต้องการพัฒนาแอปพลิเคชันให้สามารถใช้งานกับ

แพลตฟอร์มอื่นได้ จะต้องเริ่มพัฒนาแอปพลิเคชันใหม่ ซึ่งทำให้ต้นทุนในการพัฒนาสูงและใช้เวลานาน

2. Hybrid Application หรือ Cross-platform Application คือ แอปพลิเคชันที่พัฒนาโดยอาศัยเฟรมเวิร์ค (Framework) ซึ่งจะใช้ภาษาใดภาษาหนึ่งเป็นตัวกลางสำหรับการพัฒนา เฟรมเวิร์คจะทำการแปลงภาษานั้นๆ ให้แอปพลิเคชันสามารถใช้งานได้ทุกแพลตฟอร์ม ข้อดีของการพัฒนาแอปพลิเคชันแบบนี้ คือ สามารถลดระยะเวลาในการพัฒนาให้สั้นลงและแอปพลิเคชันยังสามารถใช้งานทรัพยากรได้ดีอีกด้วย

3. Web Application คือ แอปพลิเคชันที่แสดงหน้าเว็บผ่านตัว Application แทนการเข้าเบราว์เซอร์ (Browser) ซึ่งการใช้งานแอปพลิเคชันจะต้องเชื่อมต่ออินเทอร์เน็ตตลอดเวลาและอาจจะไม่สามารถใช้ทรัพยากรบางอย่างของระบบได้ ทั้งนี้ข้อดีของการพัฒนาแอปพลิเคชันแบบนี้ก็คือใช้เวลาในการพัฒนาได้รวดเร็ว

เนื่องจากปัจจุบันมีการพัฒนาแอปพลิเคชันที่ใช้ในระบบเครือข่ายมากมาย การทำความเข้าใจต่อกระบวนการของแอปพลิเคชันต่างๆ ช่วยให้สามารถดำเนินการผ่านระบบเครือข่ายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น แอปพลิเคชันที่ผู้ใช้ทั่วไปรู้จักกันเป็นอย่างดี เช่น อีเมล หรือจดหมายอิเล็กทรอนิกส์ และแอปพลิเคชันที่ใช้ในการดำเนินธุรกิจ เรียกว่า การพาณิชย์อิเล็กทรอนิกส์ หรืออีคอมเมิร์ซ (Electronic Commerce) เป็นต้น

11.2 เวิลด์ไวด์เว็บ

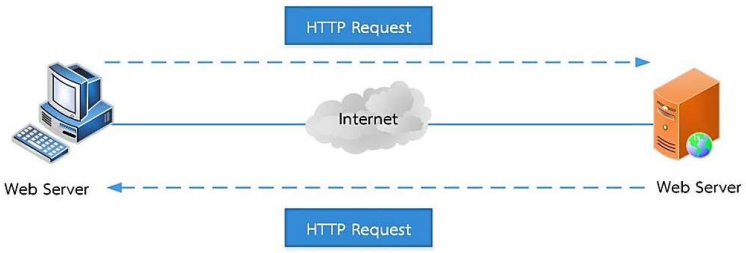
เวิลด์ไวด์เว็บ (World Wide Web: WWW) ได้ถูกคิดค้นโดย Tim Berners-Lee และทีมงาน European Particle Physics Laboratory (CERN) ซึ่งเริ่มจากการพัฒนาลักษณะการเชื่อมโยงข้อมูลแบบใหม่ที่เรียกว่า Hypertext โดยข้อมูลของแต่ละหน้าจะเชื่อมต่อกันได้ ต่อมา CERN จึงได้คิดค้น Web Browser ขึ้นในปี ค.ศ.1990 ทำให้ World Wide Web ถูกนำมาใช้และเป็นที่รู้จักกันในปี ค.ศ. 1991 หลังจากนั้น World Wide Web จึงถูกนำมาใช้กันอย่างกว้างขวางจนถึงปัจจุบัน เนื่องจากมีแอปพลิเคชันที่เชื่อมโยงให้ผู้คนทั่วโลกติดต่อสื่อสารกันได้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 314)

เวิลด์ไวด์เว็บ (World Wide Web) ใช้โพรโทคอล HTTP ในการติดต่อข้อมูลข่าวสาร โดยใช้การรับส่งไฟล์ HTML (HyperText Markup Language) ผ่านเครือข่ายอินเทอร์เน็ตและนำเสนอข้อมูลในรูปแบบของหน้าเว็บเพจ (Web Page) ซึ่งแสดงข้อมูลได้หลายอย่าง เช่น ข้อความ รูปภาพ ภาพเคลื่อนไหว เสียง และวิดีโอ เป็นต้น โดยแหล่งที่ใช้เก็บรวบรวมเพจเหล่านี้

เรียกว่า เว็บไซต์ (Web Site) เมื่อเข้าไปยังเว็บไซต์จะพบกับหน้าเพจที่เรียกว่า โฮมเพจ (Home Page) ซึ่งเป็นหน้าแรกของเว็บไซต์นั้นๆ นอกจากนี้ยังเป็นเว็บไซต์ยังเป็นแหล่งรวบรวมรายการเชื่อมโยงไปยังเว็บเพจหน้าอื่นอีกด้วย (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 314)

11.2.1 ลักษณะการทำงานของเวิลด์ไวด์เว็บ

เวิลด์ไวด์เว็บ (World Wide Web) มีสถาปัตยกรรม Client Server โดยมีคอมพิวเตอร์ฝั่งที่ให้บริการ คือ Web Server สำหรับให้บริการเว็บเพจอยู่ในรูปแบบของ Hypertext Markup Language (HTML) ส่วนผู้ใช้บริการหรือฝั่ง Client จะมีโปรแกรม Web Browser เช่น Netscape Navigator, Internet Explorer, Mozilla Firefox หรือ Opera ไว้สำหรับส่งคำร้องเพื่อเข้าใช้บริการ การสื่อสารระหว่าง Web Browser กับ Web Server ใช้มาตรฐานที่เรียกว่า HyperText Transfer Protocol (HTTP) แสดงการทำงานระหว่าง Client และ Server ได้ดังภาพที่ 11.1 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 314-318)



ภาพที่ 11.1 แสดงลักษณะการทำงานของ World Wide Web
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 315)

จากภาพที่ 11.1 Client จะส่งคำขอ เรียกว่า HTTP Request ประกอบด้วย URL (Uniform Resource Locator) เช่น www.google.com และข้อมูลอื่นๆ ที่จำเป็นสำหรับการร้องขอเว็บเพจที่ต้องการ เมื่อ Web Server ได้รับคำร้องขอแล้วจะทำการประมวลผลและส่ง HTTP Response ซึ่งเป็นหน้าเว็บเพจที่ถูกร้องขอกลับไปยัง Client รายละเอียดของ HTTP Request และ HTTP Response มีดังนี้

1. HTTP Request มีส่วนประกอบที่สำคัญ 3 ส่วน ดังนี้

1.1 Request Line ประกอบด้วยข้อมูล 3 ส่วน ได้แก่ Method, URL, และ HTTP Version โดยมีรายละเอียด ดังนี้

1.1.1 Method เป็นคำสั่งต่างๆ ที่ Client ร้องขอให้ Server จัดการ ซึ่งมีหลายคำสั่ง ดังนี้

1) GET เป็นคำสั่งที่กำหนดให้ Server ทำการส่งข้อมูลของหน้าของเว็บเพจมาให้ฝั่งผู้ใช้ที่ทำการร้องขอ เช่น GET http://www.ktpbook.com/main/Default.asp HTTP/1.1

2) HEAD เป็นคำสั่งที่ใช้ Server ส่งเฉพาะส่วนหัวของหน้าเว็บเพจ เช่น ต้องการตรวจสอบว่า URL นั้นมีจริงหรือไม่

3) PUT เป็นคำสั่งตรงข้ามกับ GET โดยจะส่งหน้าเว็บเพจให้ Server

4) DELETE เป็นคำสั่งที่เป็นคำสั่งลบหน้าเว็บเพจที่ระบุ

1.1.2 URL (Uniform Resource Locator) เป็นการระบุหน้าเว็บเพจที่ต้องการ เช่น www.google.com

1.1.3 HTTP Version เป็นเวอร์ชันของโพรโทคอล HTTP ที่ Client ใช้ โดยมีรุ่นต่างๆ ของ HTTP ได้แก่ HTTP/1.0, HTTP/1.1 และ HTTP/1.2

1.2 Request Header เป็นส่วนของการให้ข้อมูลและร้องขอข้อมูลต่างๆ โดย Client จะกำหนดสิ่งที่ต้องการไว้ใน Request Header ตัวอย่างของ Request Header มีดังนี้

1.2.1 User-Agent เป็นรายละเอียดที่เกี่ยวข้องกับ Web Browser ของ Client

1.2.2 Accept-Charset หมายถึง ประเภทตัวอักษรของเว็บเพจที่ Client ต้องการ

1.2.3 Data บอกวันและเวลาที่ส่งข้อมูล

1.3 Request Body เป็นส่วนของข้อมูลที่ Client ต้องการส่งให้ Server เช่น ข้อมูลที่กรอกลงในแบบฟอร์ม

2. HTTP Response มีส่วนประกอบที่สำคัญ 3 ส่วน ดังนี้

2.1 Request Status ประกอบด้วย 3 ส่วน ได้แก่ HTTP Version, Code Status และ Description โดยมีรายละเอียด ดังนี้

2.1.1 HTTP Version เป็นเวอร์ชันของโพรโทคอล HTTP ของ Server

2.1.2 Status Code เป็นตัวเลข 3 หลัก ซึ่งแบ่งได้ 5 กลุ่ม

2.1.3 Description เป็นข้อความที่ต่อจาก Status Code เช่น HTTP/1.1 200 OK,

HTTP/1.1 301 Moved Permanently และ HTTP/1.1 403 Forbidden

2.2 Response Header เป็นส่วนที่บรรจุข้อมูลเกี่ยวข้องกับผลลัพธ์ที่ส่งคืน ตัวอย่างของ Response Header มีดังนี้

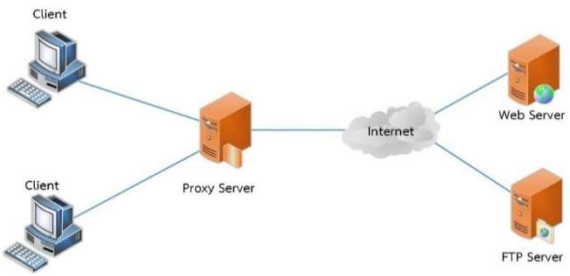
2.2.1 Server เป็นข้อมูลที่เกี่ยวข้องกับรายละเอียดต่างๆ ของ Server

2.2.2 Content-Length หมายถึง ความยาวของหน้าเว็บเพจที่มีหน่วยเป็นไบต์

2.2.3 Date บอกวัน และเวลาที่ส่งข้อมูล

2.3 Response Body เป็นหน้าเพจที่ Server ส่งให้ Client ตามคำร้องขอ ซึ่งมีหลายรูปแบบ เช่น HTML, Microsoft Word และ Adobe PDF

3. Proxy Server คือ เครื่อง Server ที่ทำหน้าที่แทนเครื่อง Client ในการติดต่อสื่อสารกับ Web Server โดยทำหน้าที่เป็นสื่อกลางคล้ายกับ Gateway เพื่อให้ Web Browser ติดต่อไปยัง Web Server ผ่านทาง Proxy Server เนื่องจากการติดต่อระหว่าง Web Browser กับ Web Server นั้นส่วนใหญ่จะใช้ HTTP ซึ่งบางครั้งอาจเกิดความยุ่งยากเพราะ Web Browser ที่ใช้งานอยู่อาจใช้งานได้เพียงบางโพรโทคอล เช่น Web Server รุ่นเก่านั้นอาจไม่ได้ใช้ HTTP ในการติดต่อสื่อสาร ซึ่งทำให้ Web Browser ไม่สามารถสื่อสารกับ Web Server ดังกล่าวได้ หรืออาจใช้โพรโทคอลที่อยู่นอกเหนือการทำงานของ Web Browser นั้น ดังนั้น การใช้ Proxy Server จึงเป็นอีกหนทางหนึ่งที่ช่วยให้ Web Browser สามารถสื่อสารกับ Web Server อื่นได้ ดังภาพที่ 11.2



ภาพที่ 11.2 แสดงการเชื่อมต่อของ Proxy Server

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 317)

การใช้ Proxy Server จะช่วยลดภาระของ Web Browser ลง เนื่องจาก Web Browser ไม่จำเป็นต้องรู้จักโพรโทคอลอื่นๆ มากจนเกินความจำเป็น เพราะมี Proxy Server ทำหน้าที่เป็นตัวกลางในการติดต่อสื่อสารอยู่แล้ว นอกจากนี้ Proxy Server ยังช่วยลด

ปริมาณความหนาแน่นของผู้ใช้ที่ต้องการติดต่อกับ Web Server ได้ในระดับหนึ่งด้วย เนื่องจาก Proxy Server จะบันทึกและจัดเก็บหน้าเว็บเพจที่ผู้ใช้ได้เข้าใช้งานล่าสุดไว้ เมื่อผู้ใช้ต้องการร้องขอข้อมูลของหน้าเว็บเพจดังกล่าวอีกครั้ง Proxy Server ก็จะทำหน้าที่เป็นผู้ตอบกลับและผู้ส่งข้อมูลที่มีอยู่ไปให้ Web Browser ทันทีสามารถตอบสนองความต้องการได้อย่างรวดเร็ว และลดจำนวนผู้ใช้ที่ต้องเชื่อมต่อกับ Web Server โดยไม่จำเป็นได้ในระดับหนึ่ง

11.2.2 Web Browser และ Web Server

Web Browser เป็นแอปพลิเคชันที่จำเป็นในการติดต่อสื่อสารในเครือข่ายอินเทอร์เน็ต โดยเฉพาะการเข้าใช้งานเว็บไซต์ต่างๆ ที่จำต้องมีการรับส่งข้อมูลกับ Web Server โดย Web Browser จะคอยติดต่อกับ Web Server เพื่อรับข้อมูลและแสดงผลตามที่ผู้ใช้ต้องการ โดยนำโพรโทคอลต่างๆ มาใช้จัดการกับการรับส่งข้อมูล ผู้ใช้งาน คือ ฝั่งผู้ใช้ (Client) คือ Web Browser และฝั่งผู้ให้บริการ (Server) คือ Web Server ซึ่งมีรายละเอียดการทำงานดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 318-321)

1. การทำงานของ Web Server

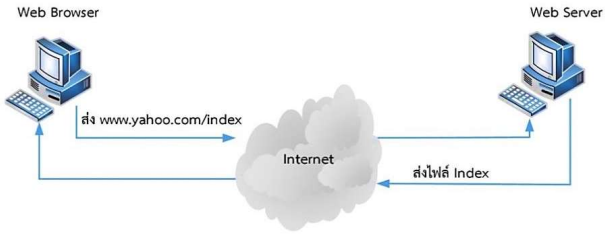
ภายในเครื่อง Server มีแอปพลิเคชันหรือซอฟต์แวร์ซึ่งมีหน้าที่ในการจัดการข้อมูลเกี่ยวกับเว็บไซต์เหล่านั้น จะเรียก Server ดังกล่าวว่า Web Server โดยมีหน้าที่ในการเก็บข้อมูลของเว็บเพจแต่ละหน้าไว้ เว็บเพจจะถูกเขียนขึ้นมาด้วยภาษา HTML (Hypertext Markup Language) เพื่อใช้ในการแสดงผล ซึ่งแต่ละเว็บเพจนั้นสามารถบรรจุข้อมูลต่างๆ ได้หลากหลาย เช่น ข้อความ ตัวอักษร ภาพ เสียง และวิดีโอ เป็นต้น

Web Server จะอยู่ในสถานะพร้อมสำหรับการติดต่อจาก Web Browser เสมอ เพื่อรอรับการร้องขอข้อมูลหน้าเว็บเพจจาก Web Browser ของผู้ใช้ เมื่อมีการร้องขอเกิดขึ้น Web Server จะดำเนินการตอบกลับพร้อมกับส่งข้อมูลที่ผู้ใช้ต้องการไปยัง Web Browser นั้น และให้ Web Browser แสดงผลแก่ผู้ใช้ต่อไป การทำงานของ Web Server จึงมีส่วนสำคัญที่ต้องทำการเก็บข้อมูลต่างๆ ไว้รวมทั้งอาจต้องมีการประมวลผลในบางกรณี หน้าที่ของ Web Server ในปัจจุบันอาจไม่ซับซ้อนมากเนื่องจากเครื่อง Client มีประสิทธิภาพสูงจึงสามารถประมวลผลบางส่วนได้ด้วยตนเอง

2. การทำงานของ Web Browser

Web Browser เป็นแอปพลิเคชันที่ส่วนใหญ่ในการแสดงผลของเว็บเพจ เนื่องจากเป็นตัวส่งคำร้องขอไปยัง Web Server เพื่อให้ส่งข้อมูลของเว็บเพจนั้นมายังเครื่อง Client โดยจะทำหน้าที่แปลงข้อมูลของเว็บเพจที่ถูกส่งมาจาก Web Server ซึ่งอยู่ในรูปแบบของ

HTML ให้สามารถแสดงผลลัพธ์เป็นหน้าเว็บเพจที่สมบูรณ์แก่ผู้ใช้ได้ การทำงานระหว่าง Web Browser กับ Web Server แสดงได้ดังภาพที่ 11.3



ภาพที่ 11.3 แสดงการทำงานระหว่าง Web Browser กับ Web Server

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 320)

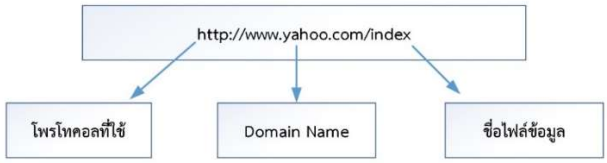
จากภาพที่ 11.3 มีกระบวนการทำงาน ดังนี้

1. ผู้ใช้กรอกที่อยู่ของเว็บไซต์ที่เรียกว่า URL เพื่อให้ Web Browser ค้นหาที่อยู่ของ Web Server นั้น โดยอาศัย Domain Name ที่ระบุอยู่ใน URL ซึ่งกระบวนการนี้เป็นการส่งคำร้องขอเปิดหน้าเว็บเพจของเว็บไซต์ดังกล่าว ในที่นี้ คือ www.yahoo.com/index

2. เมื่อ Web Server ปลายทาง ซึ่งก็คือ www.yahoo.com ได้รับคำร้องดังกล่าวแล้ว ก็จะเริ่มดำเนินการค้นหาไฟล์ข้อมูลต่างๆ ที่จำเป็นและส่งกลับไปยังเครื่อง Client นั้น โดยไฟล์ข้อมูลทั้งหมดจะอยู่ในคำร้องของผู้ใช้ ในที่นี้ก็คือไฟล์ index

3. ไฟล์ index จะส่งมายังเครื่อง Client โดยจะถูก Web Browser นำมาแปลงจากข้อมูลภาษา HTML ให้กลายเป็นรายละเอียดต่างๆ ของหน้าเว็บเพจนั้น และแสดงแก่ผู้ใช้บนหน้าจอ

URL เปรียบเสมือนที่อยู่ของ Web Server ที่จะส่งข้อความกลับมาในเว็บเพจ URL เป็นชื่อเฉพาะของเว็บไซต์ต่างๆ โดยจะมี URL ซ้ำกันไม่ได้ การใช้ URL เพื่อระบุที่อยู่ของเว็บไซต์ที่ผู้ใช้ต้องการติดต่อด้วยนั่น ช่วยให้ผู้ใช้จดจำได้ง่ายมากกว่าการใช้ IP Address โดยโครงสร้างของ URL แสดงดังภาพที่ 11.4



ภาพที่ 11.4 แสดงโครงสร้างของ URL

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 320)

11.3 อีเมล

ในอดีตการส่งเอกสารต่างๆ จะใช้วิธีการส่งทางไปรษณีย์ และโทรสาร ซึ่งอาจเสียเวลาและค่าใช้จ่ายในการจัดส่งค่อนข้างมาก โดยเฉพาะการติดต่อสื่อสารกันข้ามประเทศ เมื่อเทคโนโลยีอินเทอร์เน็ตถูกพัฒนาขึ้น จึงมีการประยุกต์ใช้งานการส่งจดหมายผ่านระบบเครือข่าย ซึ่งเรียกว่า Electronic Mail หรือ อีเมล (E-mail) วิธีการนี้ช่วยลดค่าใช้จ่ายและประหยัดเวลาได้อย่างมาก เนื่องจากผู้ใช้สามารถส่งข้อความ หรือข้อมูลผ่าน E-mail จากที่ห่างไกลมาถึงผู้รับโดยทางเครือข่ายอินเทอร์เน็ต การติดต่อสื่อสารด้วยอีเมลจึงเป็นวิธีที่สะดวกและรวดเร็ว (สุธี พงศา-สกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 321-327)

11.3.1 ข้อดีของอีเมล

ข้อดีของอีเมล มีดังนี้

1. ส่งข้อมูลได้หลายลักษณะ เช่น ข้อความ รูปภาพ ภาพเคลื่อนไหว เสียง และวิดีโอ
2. ส่งได้อย่างรวดเร็วและครอบคลุมทั่วโลก แม้ว่าผู้รับจะอยู่ต่างประเทศ หรืออยู่ในสถานที่ห่างไกลก็ตาม
3. ส่งให้ผู้รับได้หลายคนพร้อมกัน
4. เสียค่าใช้จ่ายในการส่งน้อยกว่า เมื่อเปรียบเทียบกับการส่งจดหมายธรรมดา
5. มีพื้นที่ในการจัดเก็บจดหมายเก่า และสามารถจัดเก็บกับพื้นที่ได้ด้วยตนเอง

นอกจากนี้ข้อดีที่ได้กล่าวมาแล้ว ฟังก์ชันต่างๆ ของ E-mail ยังสามารถช่วยสนับสนุนความต้องการในการติดต่อสื่อสารได้อย่างดี ฟังก์ชันของ E-mail มีดังนี้

1. Composition เป็นฟังก์ชันที่ช่วยให้ผู้ใช้สามารถกำหนดรูปแบบของข้อความ โดยผ่าน Text Editor ที่มีความสามารถหลากหลายรูปแบบ ช่วยให้ผู้ใช้สามารถสร้างจดหมายที่มีความน่าสนใจมากกว่าการอ่านแค่เพียงข้อความที่เป็นตัวอักษรเพียงอย่างเดียว ฟังก์ชันนี้จึงช่วยให้ผู้ใช้สามารถจัดวางองค์ประกอบแนะนำรูปแบบที่น่าสนใจแทรกลงในเนื้อหาของจดหมายได้ง่าย

2. Transfer E-mail ถูกส่งโดยโพรโทคอล TCP/IP ซึ่งเป็นโพรโทคอลที่มีความน่าเชื่อถือในการรับส่งข้อมูลผ่านเครือข่ายอินเทอร์เน็ต การส่ง E-mail จึงมีความแน่นอนว่าจะเดินทางไปยังผู้รับได้ อีกทั้งยังทราบได้ว่า E-mail ดังกล่าวถูกส่งมาจากใคร เพราะการรับส่ง E-mail จำเป็นต้องมีการเชื่อมต่อระหว่างผู้รับและผู้ส่ง

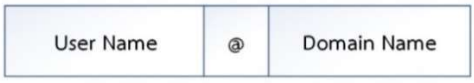
3. Reporting การส่ง E-mail ทุกครั้งมีการรายงานสถานะของผู้ใช้ให้ทราบว่า E-mail นั้นเดินทางไปถึงผู้รับแล้วหรือยัง หากเกิดข้อผิดพลาดขึ้นก็จะมีข้อความแจ้งให้ผู้ใช้ทราบว่า E-mail ดังกล่าวไม่สามารถส่งกลับไปยังปลายทางได้ ในบางกรณี E-mail นั้นอาจถูกตีกลับมา โดยผู้ให้บริการเอง เพื่อแจ้งรายละเอียดให้ทราบว่าเหตุใดจึงไม่สามารถส่ง E-mail นั่นได้ ซึ่งเป็นฟังก์ชันที่มีประโยชน์อย่างมากต่อผู้ใช้

4. Displaying เป็นฟังก์ชันการใช้งานที่ช่วยแสดงผล E-mail มีหน้าต่างการแจ้งเตือนบนหน้าจอให้ผู้ใช้ทราบว่าขณะนี้มี E-mail ส่งมา และผู้ใช้ก็สามารถเข้าไปอ่านได้โดยตรง ผู้ใช้สามารถทราบสถานะของตู้จดหมาย (Mailbox) ของตนได้จากหน้าจอคอมพิวเตอร์โดยที่ไม่ต้องเข้าไปดูถึงหน้าตู้จดหมายก็ได้

5. Disposition ผู้ใช้จะสามารถจัดการกับจดหมายในตู้ของตนเองได้ โดยผ่านทางหน้าจอคอมพิวเตอร์ซึ่งสามารถลบหรือจัดเก็บจดหมายได้ รวมถึงการส่งต่อ (Forward) จดหมายได้รับมา ฟังก์ชันนี้จึงช่วยให้ผู้ใช้สามารถควบคุมตู้จดหมายทำให้การใช้งาน E-mail มีความคล่องตัวและสะดวกมากยิ่งขึ้น

11.3.2 สถาปัตยกรรมของอีเมล

การติดต่อสื่อสารด้วย E-mail นั้นจะมีรูปแบบแตกต่างจากการส่งจดหมายแบบธรรมดา เนื่องจากการส่งจดหมายจะต้องมีชื่อและที่อยู่ แต่ E-mail จะใช้ชื่อที่อยู่ที่เรียกว่า E-mail Address ของผู้รับหรือ ผู้ส่งเป็นสำคัญ รูปแบบของ E-mail Address แสดงได้ดังภาพที่ 11.5

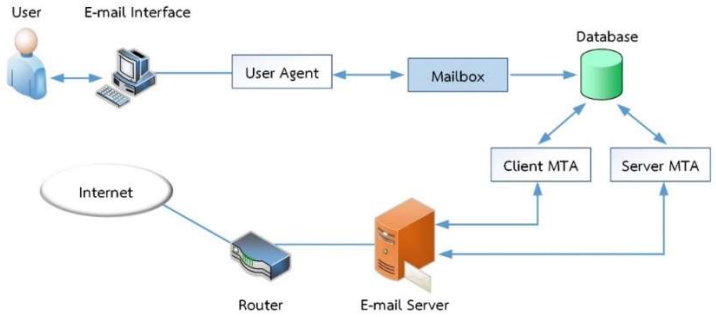


ภาพที่ 11.5 แสดงรูปแบบของ E-mail Address
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 322)

จากภาพที่ 11.5 ส่วนแรกเป็น User Name คือชื่อของเจ้าของ E-mail Address สามารถกำหนดได้ว่าจะใช้ชื่ออะไร มีความหมายหรือไม่มีก็ได้ ส่วนหลัง คือ Domain Name ที่เจ้าของได้ใช้บริการ E-mail นั้นอยู่ และถูกคั่นด้วยเครื่องหมาย “@” ซึ่งถือได้ว่าเป็นเอกลักษณ์เฉพาะของรูปแบบ E-mail Address เช่น Suwit@gmail.com เป็นต้น

นอกจากนี้ การระบุตัวผู้รับสามารถทำได้มากกว่าหนึ่งคน การส่ง E-mail ถึงผู้รับคนอื่นๆ อาจระบุในช่องที่ผู้รับเรียกว่า CC (Carbon Copy) และ BCC (Blind Carbon Copy) โดย CC จะแสดงชื่อผู้รับให้เห็นทั้งหมด แต่ BCC จะซ่อนที่อยู่ของผู้รับคนอื่นๆ ทั้งหมด

การส่ง E-Mail ผู้ใช้จะใช้งานผ่านเครื่องคอมพิวเตอร์ และทำการติดต่อกับ Server ที่ทำหน้าที่ในการจัดการกับ E-mail ซึ่งเรียกว่า E-mail Server มีหน้าที่ในการจัดเก็บและจัดการขั้นตอนต่างๆ ที่ผู้ใช้สั่งการผ่านแอปพลิเคชันในเครื่องคอมพิวเตอร์ กระบวนการใช้งานของผู้ใช้นั้นสามารถแสดงได้ดังภาพที่ 11.6



ภาพที่ 11.6 แสดงสถาปัตยกรรมของ E-mail

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 323)

จากภาพที่ 11.6 ผู้ใช้จะดำเนินการเชื่อมต่อกับแอปพลิเคชันของ E-mail จากเครื่องคอมพิวเตอร์ โดยใช้ User Agent เป็นสื่อกลางในการติดต่อกับกล่องจดหมาย (Mailbox) และบริการต่างๆ ของ E-mail โดยข้อมูลทั้งหมดจะถูกจัดเก็บไว้ในฐานข้อมูล เมื่อมีการรับส่งหรือเข้าใช้ระบบ E-mail จะต้องใช้ Mail Transfer Agent (MTA) เป็นตัวกลางในการติดต่อกับ E-mail Server หลังจากนั้นข้อมูลจึงถูกส่งไปยังปลายทางผ่านทางเครือข่ายอินเทอร์เน็ต

11.3.3 องค์ประกอบของอีเมล

จะเห็นได้ว่า E-mail มีส่วนประกอบที่สำคัญหลายอย่าง ทั้งในส่วนของผู้ใช้และ E-mail Server ได้แก่ Mailbox, Database, E-mail Interface, User Agent และ Mail Transfer Agent (MTA) มีรายละเอียดที่สำคัญ ดังนี้

1. กล่องจดหมาย (Mailbox)

กล่องจดหมาย (Mailbox) โดยทั่วไปจะหมายถึงกล่องรับจดหมายที่ส่งมาเพื่อรอให้ผู้รับมาเปิดและนำจดหมายไปอ่าน แต่ในระบบ E-mail นั้น กล่องจดหมายเปรียบเสมือนฐานข้อมูลในการจัดเก็บ E-mail ทั้งหมดที่ผู้ใช้มี ถึงแม้ว่าผู้ใช้จะเปิดอ่าน E-mail

นั้นไปแล้วก็ตาม E-mail ดังกล่าวก็ยังถูกจัดเก็บไว้ในกล่องจดหมาย ผู้ใช้สามารถใช้งานกล่องจดหมายได้หลายรูปแบบ เช่น เขียนจดหมายผ่านทาง Text Editor ลบ E-mail ที่ไม่ต้องการและส่ง E-mail โดยข้อมูลต่างๆ เหล่านี้จะถูกจัดเก็บไว้ในกล่องจดหมายจนกว่าผู้ใช้จะลบออกไป แอปพลิเคชัน E-mail บางตัวก็จะเก็บ E-mail ที่ลบไปแล้วไว้สักระยะหนึ่งจึงค่อยลบทิ้ง นอกจากนี้ยังมีบริการจัดเก็บ E-mail ที่ผู้ใช้ส่งไปโดยการคัดลอกสำเนาของ E-mail นั้นไว้และบันทึกลงในฐานข้อมูล เรียกว่า Spool จากที่กล่าวมาทั้งหมดจะเห็นได้ว่ากล่องจดหมาย E-mail นั้นมีความสำคัญมาก เนื่องจากทำให้ผู้ใช้สามารถจัดการ และควบคุมการรับส่ง E-mail ได้ ดังนั้นจึงมีการรักษาความปลอดภัยให้กับกล่องจดหมายเป็นอย่างดี เพื่อไม่ให้ข้อมูลที่เก็บไว้ถูกขโมยไป

2. User Agent

User Agent เป็นโปรแกรมที่มีไว้สำหรับให้ผู้ใช้สามารถอ่าน สร้าง แก้ไข และเลือกวิธีการส่งอีเมล โดยผู้ใช้สามารถอ่านอีเมลได้จาก Mail Box ที่เปรียบเสมือนกับกล่องจดหมาย ซึ่งทำหน้าที่เก็บไฟล์อีเมลต่างๆ ไว้ โดยทั่วไปโปรแกรม User Agent จะแสดงข้อมูลของจดหมายต่างๆ ใน Mail Box เพื่อให้ผู้ใช้เลือกอ่านจดหมายได้ ตัวอย่างของ User Agent ได้แก่ Microsoft Outlook และ Eudora สำหรับมาตรฐานของ Message ที่สำคัญมี 2 ชนิด ดังนี้

2.1 RFC 822 เป็นมาตรฐานของ Message ที่อยู่ในรูปแบบ Plain Text ไม่มีลูกเล่นหรือกราฟิกอื่นๆ โดย Message ของ RFC 822 จะประกอบไปด้วย Header ต่างๆ ดังตารางที่ 11.1

ตารางที่ 11.1 แสดง Header ของ RFC 822

Header	รายละเอียด
To:	E-mail Address หรือที่อยู่ของผู้รับ โดยสามารถส่งให้ผู้รับได้หลายคน
Cc:	E-mail Address หรือที่อยู่ของผู้รับที่ต้องการส่งสำเนาข้อมูลของผู้รับในช่อง To:
Bcc:	E-mail Address หรือที่อยู่ของผู้รับ โดยผู้รับจะไม่ทราบว่าอีเมลที่ส่งมาให้ถูกส่งไปให้กับผู้อื่นด้วย
From:	ผู้ที่ทำหน้าที่สร้าง Message
Sender:	ผู้ที่ทำหน้าที่ส่งอีเมล
Received:	Message Transfer Agent จะบันทึกรายละเอียดเกี่ยวกับรหัส วัน และเวลาของอีเมลที่ได้รับ
Return-Path:	เส้นทางที่สามารถส่งข้อมูลกลับไปยังผู้ส่งอีเมลนั้นมาให้

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 324)

2.2 MIME (Multipurpose Internet Mail Extensions) เป็นมาตรฐานที่ถูกสร้างขึ้นมาเพื่อใช้สำหรับการส่งไฟล์แนบไปกับอีเมล เช่น รูปภาพ ภาพเคลื่อนไหว และวิดีโอ เป็นต้น โดยการเพิ่ม Header ต่างๆ ใน RFC 882 เพื่อระบุชนิดของข้อมูลที่ต้องการแนบ ดังตารางที่ 11.2

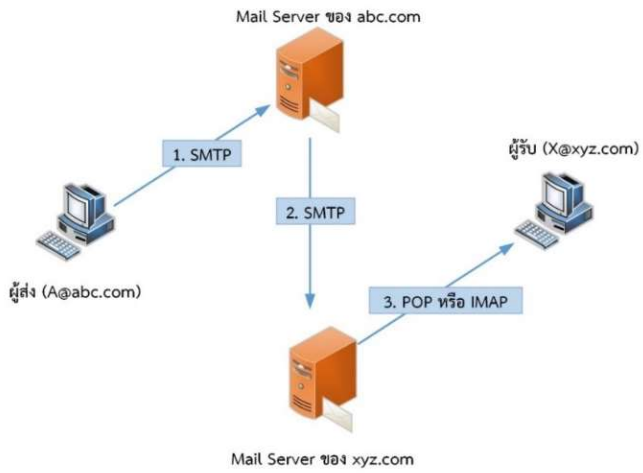
ตารางที่ 11.2 แสดง Header ของ MIME

Header	รายละเอียด
MIME-Version:	ระบุเวอร์ชันของ MIME เช่น เวอร์ชัน 1.0
Content-Description:	บอกรายละเอียดของ Message ที่ส่งมา
Content-Id:	รหัสเฉพาะของอีเมล
Content-Transfer-Encoding:	บอกวิธีที่ใช้ในการเข้ารหัสข้อมูล เช่น Base64
Content-Type:	ระบุชนิดและรูปแบบของข้อมูล เช่น Video/Mpeg และ Image/Jpeg

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 325)

3. Message Transfer Agent

Message Transfer Agent เป็นส่วนที่ทำหน้าที่ส่งอีเมลที่สร้างจาก User Agent ไปยังจุดหมายปลายทาง ตัวอย่างของการส่งอีเมล แสดงได้ดังภาพที่ 11.7



ภาพที่ 11.7 แสดงตัวอย่างการส่ง E-mail

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 325)

จากภาพที่ 11.7 ผู้ส่ง A@abc.com ต้องการส่งอีเมลให้กับผู้รับ X@xyz.com โดยมีขั้นตอนในการส่งและอ่านอีเมล ดังนี้

ขั้นที่ 1 อีเมลของผู้ส่ง A จะส่งไปยัง Mail Server ของผู้ส่งในที่นี้ คือ abc.com โดยใช้ STMP เป็นมาตรฐานในการส่งข้อมูล

ขั้นที่ 2 Mail Server ของผู้ส่ง (abc.com) จะทำหน้าที่ส่งเมลไปยัง Mail Server ของผู้รับในที่นี้ คือ xyz.com โดยใช้ SMTP เป็นมาตรฐานในการส่งข้อมูล และอีเมลนั้นถูกจัดเก็บไว้ใน Mail Box

ขั้นที่ 3 เมื่อผู้รับ X ต้องการเปิดอีเมลจะต้องใช้ POP (Post Office Protocol) หรือ IMAP (Internet Message Access Protocol) เพื่อดาวน์โหลดข้อมูลจาก Mail Box ในเครื่องของผู้รับ

ลักษณะการทำงานแบ่งออกเป็น 2 ส่วนที่สำคัญ คือ ส่วนของการส่งอีเมล และส่วนของการอ่านอีเมล โดยมีรายละเอียด ดังนี้

1. การส่งอีเมล มาตรฐานที่เกี่ยวข้องกับการส่งอีเมลที่ใช้ในปัจจุบัน คือ SMTP (Simple Mail Transfer Protocol) ซึ่งจะทำหน้าที่ตรวจสอบข้อมูลที่เข้ามาที่พอร์ต 25 หากได้รับการติดต่อเพื่อส่งอีเมลก็จะส่ง Message เพื่อเจรจาเกี่ยวกับการส่งข้อมูล ถ้าเจรจาสำเร็จก็จะรับอีเมลนั้นมา และจัดเก็บไว้ใน Mail Box ของ Mail Server กรณีที่มีความผิดพลาดเกิดขึ้นขณะเจรจา หรือขณะรับส่งข้อมูล ก็จะรายงานความผิดพลาดกลับไปยังผู้ส่ง

2. การอ่านอีเมล มาตรฐานที่สำคัญเกี่ยวกับการอ่านอีเมลที่ใช้ในปัจจุบันมี 2 มาตรฐาน ได้แก่ POP (Post Office Protocol) และ IMAP (Internet Message Access Protocol)

2.1 Post Office Protocol (POP) เป็นมาตรฐานสำหรับการอ่านอีเมลเวอร์ชันที่ใช้ในปัจจุบัน คือ POP3 โดยทำงานในลักษณะ Offline เนื่องจากมีการดึงข้อมูลจาก Mail Server มาเก็บไว้ที่เครื่องของผู้ใช้เมื่อ Client ต้องการเปิดอ่านอีเมล จะต้องสร้างการติดต่อไปยังพอร์ต 110 ของ Mail Server ที่เก็บอีเมล โดยมีกระบวนการ 3 ขั้นตอน คือ

2.1.1 ขั้นการตรวจสอบสิทธิ์ในการใช้งาน (Authorization) ซึ่งผู้ใช้สามารถยืนยันสิทธิ์ในการใช้งานด้วยการใส่ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

2.1.2 ขั้นดำเนินการ (Transaction) หลังจากได้รับการตรวจสอบสิทธิ์ และสามารถผ่านเข้าไปใช้งานได้แล้ว อีเมลจาก Mail Box ของ Mail Server จะถูกดาวน์

โหลดมาเก็บไว้ที่เครื่องของผู้ใช้ โดยผู้ใช้จัดการกับอีเมลเหล่านี้โดยโปรแกรม User Agent เช่น การเปิดอ่านและลบอีเมลทิ้ง

2.1.3 ขั้นการปรับปรุงข้อมูล (Update) เป็นขั้นตอนสุดท้ายเพื่อยุติการติดต่อระหว่างผู้ใช้กับ Mail Server โดยการปรับปรุงข้อมูลใน Mail Box เช่น การลบอีเมลจาก Mail Box ของ Mail Server ที่ถูกดาวน์โหลดไปเก็บยังเครื่องของผู้ใช้เรียบร้อยแล้ว

2.2 IMAP (Internet Message Access Protocol) เป็นมาตรฐานสำหรับการอ่านอีเมลอีกรูปแบบหนึ่งที่มีความแตกต่างจาก POP คือ มาตรฐาน IMAP ช่วยให้ผู้ใช้บริการสามารถเลือกดาวน์โหลดเฉพาะอีเมลที่ต้องการได้ ในขณะที่มาตรฐาน POP ต้องดาวน์โหลดอีเมลทั้งหมดที่อยู่ใน Mail Box นอกจากนี้ IMAP ยังสามารถรองรับการทำงานได้ทั้งแบบ Online และ Offline ส่วนมาตรฐาน POP รองรับได้เฉพาะการทำงานแบบ Offline เท่านั้น โดยการทำงานของ IMAP แบบ Offline ถึงแม้ว่าจะดึงอีเมลมาอ่านที่เครื่องของผู้ใช้แล้วก็ตาม แต่อีเมลดังกล่าวก็ยังคงจัดเก็บไว้ใน Server เช่นเดิม หาก Client ต้องการเปิดอ่านอีเมล จะต้องสร้างการติดต่อไปยังพอร์ต 143 ของ Mail Server ที่เก็บอีเมล และจะเห็นได้ว่าการที่ข้อมูลอีเมลยังคงอยู่ที่ Mail Server ทำให้ผู้ใช้ IMAP สามารถจัดการกับอีเมลจากคอมพิวเตอร์เครื่องใดก็ได้ รวมทั้งเข้าใช้งานอีเมลจากที่ใดๆ ก็ได้

11.3.3 Webmail

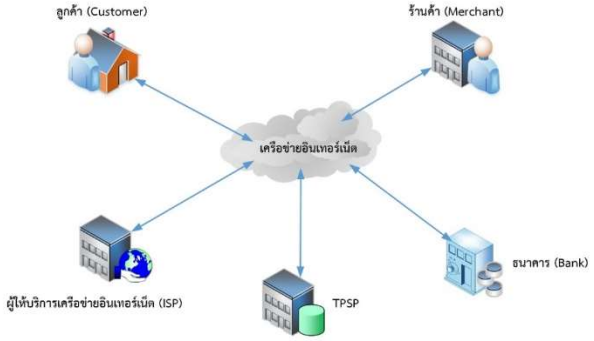
Webmail เป็นบริการอีเมลโดยใช้โปรแกรม Web Browser ในการรับ ส่ง สร้าง แก้ไข และการจัดการอื่นๆ ที่เกี่ยวกับอีเมล โดยใช้มาตรฐาน HTTP ในการติดต่อสื่อสารและแสดงผลในรูปแบบของเว็บเพจ ปัจจุบันเว็บไซต์ต่างๆ มีบริการอีเมลให้ใช้ได้โดยไม่เสียค่าใช้จ่าย เช่น Hotmail, Yahoo และ Gmail เป็นต้น แต่จะจำกัดขนาดของ Mail Box ในระดับหนึ่ง ดังนั้น Webmail จึงเหมาะสำหรับผู้ใช้งานทั่วไป เนื่องจากไม่จำเป็นต้องติดตั้งโปรแกรมใดๆ ใช้เพียง Web Browser ก็สามารถเข้าสู่บริการได้

11.4 อีคอมเมิร์ซ

อีคอมเมิร์ซ (E-Commerce) หรือ การพาณิชย์อิเล็กทรอนิกส์ หมายถึง การทำการค้าผ่านระบบสื่อสารอิเล็กทรอนิกส์ เช่น เครือข่ายอินเตอร์เน็ต เป็นต้น โดยพัฒนาแอปพลิเคชันที่ใช้ในด้านธุรกิจ การค้าขาย การขนส่งสินค้า และการชำระเงิน เพื่ออำนวยความสะดวกในการติดต่อระหว่างลูกค้ากับเจ้าของสินค้าหรือบริการผ่านทางเครือข่ายอินเทอร์เน็ต ทำให้ไม่ต้องเดินทาง

ติดต่อซื้อขายกันโดยตรง และไม่ต้องลงทุนสูง เนื่องจากการดำเนินการทุกอย่างทำด้วยแอปพลิเคชัน เช่น การเลือกซื้อสินค้า ดูรายละเอียดสินค้า สั่งซื้อสินค้า และชำระเงิน เป็นต้น ดังนั้น การพาณิชย์อิเล็กทรอนิกส์จึงได้รับความนิยมอย่างแพร่หลายในปัจจุบัน

อีคอมเมิร์ซเป็นการรวมและเชื่อมต่อความสัมพันธ์ขององค์กรทางด้านธุรกิจต่างๆ ไว้ด้วยกันทั้งในส่วนของลูกค้า ร้านค้า และธนาคาร ทำให้องค์กรทางธุรกิจสามารถติดต่อกันโดยมีศูนย์กลางเป็นระบบเครือข่ายอินเทอร์เน็ต ซึ่งครอบคลุมไปทั่วโลก ความสัมพันธ์ของการค้าอิเล็กทรอนิกส์ แสดงได้ดังภาพที่ 11.8 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 327)



ภาพที่ 11.8 แสดงความสัมพันธ์ของส่วนประกอบต่างๆ ในการพาณิชย์อิเล็กทรอนิกส์
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 328)

จากภาพที่ 11.8 แสดงถึงความสัมพันธ์ขององค์กรหรือบุคคลที่เกี่ยวข้องกับอีคอมเมิร์ซ โดยมีรายละเอียด ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 328-329)

1. ลูกค้า (Customer) ลูกค้าหรือผู้บริโภคที่ต้องการซื้อสินค้าและใช้บริการอีคอมเมิร์ซ โดยส่วนใหญ่จะเป็นกลุ่มลูกค้าที่ต้องการความสะดวกในการเลือกซื้อสินค้า หรือเป็นผู้ค้ารายย่อยที่ต้องการสั่งซื้อสินค้าจากบริษัทหรือองค์กรร้านค้าขนาดใหญ่

2. ร้านค้า (Merchant) คือ กลุ่มองค์กร บริษัท หรือบุคคลที่ต้องการขายสินค้าและบริการต่างๆ ผ่านทางอีคอมเมิร์ซ โดยมีความต้องการที่แตกต่างกัน เช่น ขยายการตลาดให้ครอบคลุมลูกค้าทุกประเภท เพิ่มทางเลือกในการซื้อสินค้าให้กับลูกค้า อำนวยความสะดวกแก่ลูกค้าประจำ หรือต้องการทำธุรกิจด้วยเงินลงทุนที่ไม่สูงเกินไป เป็นต้น

3. ธนาคาร (Bank) คือ องค์กรด้านการเงิน ดูแลการชำระเงินในอีคอมเมิร์ซ อำนวยความสะดวกให้กับร้านค้าที่เป็นสมาชิก โดยทำหน้าที่ตรวจสอบการชำระเงินผ่านช่องทางต่างๆ เช่น บัตรเครดิต หรือการโอนเงินผ่านทางระบบเครือข่ายอินเทอร์เน็ต เป็นต้น

4. ผู้ให้บริการด้านอินเทอร์เน็ต (ISP: Internet Service Provider) คือ องค์กรที่ดูแลระบบเครือข่ายอินเทอร์เน็ต และจัดการเกี่ยวกับการจดทะเบียนเว็บไซต์ การตั้งชื่อเว็บไซต์ และตรวจสอบความเหมาะสมของสินค้าหรือบริการที่นำมาวางขายในระบบเครือข่ายอินเทอร์เน็ต

5. TPSP (Transaction Processing Service Provider) คือ องค์กรที่ดูแลระบบการประมวลผลการชำระเงิน เพื่อเพิ่มความน่าเชื่อถือให้กับอีคอมเมิร์ซ และความปลอดภัยในระหว่างการชำระเงิน โดยองค์กรนี้จะทำหน้าที่เชื่อมต่อระบบการชำระเงินของร้านค้ากับธนาคาร ทำให้การดำเนินการด้านการเงินสะดวกและปลอดภัยยิ่งขึ้น องค์กรประเภทนี้จะจัดตั้งขึ้นเพื่อทำหน้าที่นี้โดยเฉพาะ หรืออาจจะเป็นหน่วยงานที่อยู่ภายใต้การดูแลขององค์กรด้านการเงินก็ได้

11.4.1 ประเภทของอีคอมเมิร์ซ

จากความสัมพันธ์ระหว่างองค์กรและกลุ่มบุคคลต่างๆ ทำให้อีคอมเมิร์ซหรือการพาณิชย์อิเล็กทรอนิกส์สามารถแบ่งได้ 4 ประเภท ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 329-331)

1. C2B (Customer to Business) เป็นการทำการค้าระหว่างลูกค้ากับเจ้าของสินค้าหรือบริการ เช่น การสั่งซื้อหนังสือผ่านเว็บไซต์ของร้านหนังสือ เป็นต้น

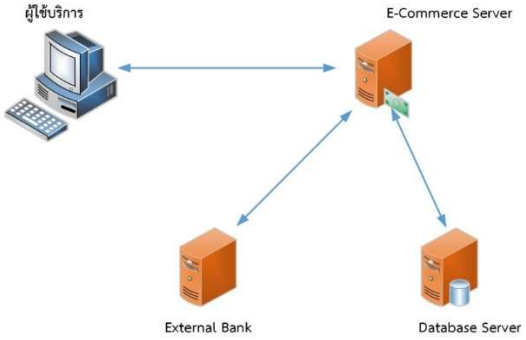
2. B2B (Business to Business) เป็นการทำการค้าระหว่างผู้ให้บริการด้วยกันเอง แต่อาจจะเป็นผู้ให้บริการหรือเจ้าของสินค้าที่แตกต่างกัน โดยทำการแลกเปลี่ยนสินค้าหรือบริการระหว่างกัน เช่น ร้านค้าสั่งซื้อหนังสือจากตัวแทนจำหน่ายหรือโรงพิมพ์โดยตรง เป็นต้น

3. B2C (Business to Customer) เป็นการทำการค้าระหว่างผู้ให้บริการหรือเจ้าของสินค้ากับผู้บริโภค เนื่องจากผู้ให้บริการมีความต้องการสินค้าหรือบริการอย่างที่ผู้บริโภคสามารถจัดหาให้ได้ เช่น ตัวแทนจำหน่ายหรือโรงพิมพ์ซื้อต้นฉบับมาจากผู้เขียน หรือร้านค้าซื้อหนังสือมือสองจากลูกค้าเพื่อนำมาจำหน่ายต่อ เป็นต้น

4. C2C (Customer to Customer) เป็นการทำการค้าระหว่างผู้บริโภคด้วยกัน ซึ่งอาจเป็นการแลกเปลี่ยนสินค้าหรือบริการระหว่างกันตามความพึงพอใจทั้งสองฝ่าย เช่น ผู้บริโภคซื้อหนังสือมือสองจากผู้บริโภคอีกคนหนึ่งที่ประกาศขายผ่านทางเว็บไซต์ เป็นต้น

สรุปได้ว่า อีคอมเมิร์ซหรือการพาณิชย์อิเล็กทรอนิกส์เป็นการเชื่อมโยงระหว่างผู้ใช้หลายกลุ่มที่มีความต้องการในการทำธุรกิจหรือการแลกเปลี่ยนข้อมูล โดยจะติดต่อสื่อสารผ่านทางเครือข่ายอินเทอร์เน็ตซึ่งจำเป็นต้องมีเครื่อง Server ทำหน้าที่รองรับบริการที่แตกต่างกัน เช่น Server ที่ควบคุมเว็บแอปพลิเคชัน หรือ Server ที่จัดการประมวลผลทางด้าน

การเงินซึ่งอาจอยู่ในส่วนธนาคารหรือสถาบันการเงิน เป็นต้น การทำงานร่วมกันของ Server และเครื่องผู้ใช้ในอีคอมเมิร์ซแสดงได้ดังภาพที่ 11.9



ภาพที่ 11.9 แสดงองค์ประกอบของ E-Commerce

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 330)

11.4.2 องค์ประกอบของบริการอีคอมเมิร์ซ

การซื้อขายสินค้าและบริการผ่านอิเล็กทรอนิกส์ มีองค์ประกอบที่สำคัญ 3 ส่วน ดังนี้

1. การขายสินค้า เป็นส่วนของหน้าร้านสำหรับแสดงสินค้า ประกอบด้วย รายการสินค้า การเลือกสินค้าที่ต้องการ โดยสามารถเลือกได้หลายชนิดลงในตะกร้าสั่งซื้อ (Shopping Cart)

2. การชำระเงิน ลูกค้าสามารถเลือกวิธีการชำระได้หลายวิธี เช่น การชำระโดยใช้บัตรเครดิต และการชำระโดยการหักเงินจากบัญชีธนาคาร ดังนั้น E-Commerce จึงต้องมีการเชื่อมต่อกับธนาคารต่างๆ เพื่อทำธุรกรรมเกี่ยวกับการชำระเงินของลูกค้า

3. ฐานข้อมูลของสินค้า เป็นฐานข้อมูลเกี่ยวกับสินค้า เช่น รายชื่อสินค้า ราคา และจำนวนสินค้าคงเหลือ

อีคอมเมิร์ซหรือการพาณิชย์อิเล็กทรอนิกส์จำเป็นต้องมีความปลอดภัยและมีความน่าเชื่อถือสูง เนื่องจากเป็นการทำงานที่เกี่ยวข้องกับการค้าขาย และการเงิน หากเกิดข้อผิดพลาดย่อมส่งผลต่อทุกองค์กรที่เกี่ยวข้องอย่างแน่นอน ดังนั้น จึงต้องคำนึงถึงส่วนประกอบต่างๆ อย่างรอบคอบเพื่อให้อีคอมเมิร์ซสามารถตอบสนองต่องานด้านธุรกิจอย่างมีประสิทธิภาพ สรุปข้อดีและข้อเสียของการพาณิชย์อิเล็กทรอนิกส์ได้ดังนี้

ข้อดีของอีคอมเมิร์ซ

1. การทำธุรกิจสามารถดำเนินได้ตลอด 24 ชั่วโมง
2. ขอบเขตการติดต่อสื่อสารในการดำเนินธุรกิจครอบคลุมทั่วโลก
3. ประหยัดเวลาในการเดินทางเพื่อติดต่อสื่อสารด้านธุรกิจโดยตรง
4. ใช้งบประมาณในการลงทุนต่ำ
5. การเพิ่มความสะดวกให้แก่ลูกค้าประจำและขยายฐานลูกค้าใหม่ได้อย่างมีประสิทธิภาพ
6. การประชาสัมพันธ์สินค้าหรือบริการทำได้ง่าย

ข้อเสียของอีคอมเมิร์ซ

1. ระบบต้องการมีการรักษาความปลอดภัยในระดับสูง ทำให้เกิดความยุ่งยากในการพัฒนาแอปพลิเคชัน
2. บางประเทศยังไม่มีกฎหมายที่คุ้มครองการซื้อขายผ่านอีคอมเมิร์ซ
3. ลูกค้าหรือผู้ที่ต้องการซื้อขายผ่านอีคอมเมิร์ซจะต้องมีความรู้ในการใช้งานเครือข่ายอินเทอร์เน็ตพอสมควร
4. ระบบต้องการอาศัยเครือข่ายอินเทอร์เน็ตเพื่อใช้เป็นสื่อกลางในการดำเนินการตลอดเวลา
5. ต้องมีบุคลากรที่มีความรู้ในการพัฒนาและดูแลแอปพลิเคชันให้ทำงานได้อย่างมีประสิทธิภาพเสมอ

11.5 การวิเคราะห์โพรโทคอล

นอกจากแอปพลิเคชันที่ใช้ในการติดต่อสื่อสารและจัดการกับทรัพยากร รวมทั้งการทำงานของเครือข่ายแล้ว ยังมีแอปพลิเคชันอีกรูปแบบหนึ่งที่ใช้สำหรับการตรวจสอบการขนส่งข้อมูล และการเดินทางของแพ็กเก็ตข้อมูล โดยทำการวิเคราะห์เพื่อให้ผู้ดูแลระบบเครือข่ายทราบถึงสถานะต่างๆ ที่จำเป็น เพื่อป้องกันความผิดพลาดของระบบหรือผู้บุกรุก ช่วยให้ระบบสามารถตอบสนองความต้องการของผู้ใช้ได้อย่างสม่ำเสมอ นอกจากนี้ยังใช้ในการวิเคราะห์ระบบเครือข่าย โดยการจำลองสถานการณ์เพื่อให้ทราบถึงปัญหาที่จะเกิดขึ้นและหาวิธีการแก้ไข ก่อนที่จะสร้างหรือติดตั้งระบบเครือข่ายและนำไปใช้งานจริงต่อไป เรียกว่า การวิเคราะห์โพรโทคอล (Protocol Analyzer) โดยแอปพลิเคชันเหล่านี้มีหลายรูปแบบและใช้ชื่อเรียกแตกต่างกันไป เช่น Network Analyzer, Protocol Analyzer และ Packet Sniffer ซึ่งแต่ละแอปพลิเคชันมี

รูปแบบในการนำไปใช้ที่แตกต่างกัน เช่น Ethernet Sniffer นำไปใช้ในระบบเครือข่ายอีเทอร์เน็ต Wireless Sniffer นำไปใช้ในระบบเครือข่ายไร้สาย เป็นต้น (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 331)

11.5.1 ลักษณะการทำงานของแอปพลิเคชัน

แอปพลิเคชันต่างๆ ที่กล่าวมามีลักษณะการทำงานคล้ายๆ กันโดยจะจับแพ็กเก็ตมาแล้วดำเนินการถอดแพ็กเก็ตเพื่อนำข้อมูลมาวิเคราะห์ต่อไป สามารถแบ่งได้ 3 ลักษณะ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 331-332)

1. Capture เป็นขั้นตอนแรกที่จะดำเนินการ คือ การจับ (Capture) แพ็กเก็ตที่ต้องการซึ่งเดินทางอยู่ในระบบเครือข่าย โดยนำ Frame ข้อมูลในแพ็กเก็ตมาเป็นตัวอย่างในการวิเคราะห์

2. Decode เป็นขั้นตอนการถอดรหัส (Decode) โดยถอดข้อมูลออกจากแพ็กเก็ต หรือ Frame ข้อมูล ซึ่งภายในอาจมีข้อมูลที่แสดงถึงตัวหนังสือหรือข้อความที่ไม่สามารถอ่านเข้าใจได้ แต่จะเป็นข้อความที่คอมพิวเตอร์ หรือโพรโทคอลเข้าใจ ซึ่งอาจเป็นการเข้ารหัสตามเลขฐาน เช่น MAC Address ของเครื่องต้นทางและเครื่องปลายทาง เป็นต้น

3. Reporting เป็นขั้นตอนการสรุปข้อมูลที่ได้จากการวิเคราะห์ ซึ่งเป็นข้อมูลที่จำเป็นต่อผู้ดูแลและจัดการเครือข่าย

นอกจากข้อมูลที่ได้จากการถอดแพ็กเก็ตโดยตรงแล้ว แอปพลิเคชันยังสามารถแสดงข้อมูลที่จำเป็นต่างๆ ให้ผู้ใช้ทราบ เช่น ข้อความแจ้งข้อผิดพลาด อัตราการติดต่อสื่อสารของข้อมูล ขนาดของแพ็กเก็ต และข้อความแจ้งเตือนจากการโจมตีจากผู้บุกรุก ซึ่งข้อมูลดังกล่าวมีความจำเป็นและมีประโยชน์ต่อผู้ดูแลระบบหรือเครือข่ายเป็นอย่างมาก ปัจจุบันได้มีการออกแบบและพัฒนาแอปพลิเคชันเหล่านี้ให้สามารถใช้งานได้ง่ายขึ้น โดยการนำเสนอข้อมูลด้วยรูปภาพ และนำ Dashboard มาประยุกต์ใช้งานด้วย เช่น จำนวนหรือเปอร์เซ็นต์ของประสิทธิภาพในการทำงาน หรือความผิดพลาดที่เกิดขึ้น เป็นต้น

ในปัจจุบันแอปพลิเคชันที่ใช้วิเคราะห์ข้อมูลในระบบเครือข่ายได้มีการประยุกต์ประสิทธิภาพทั้งทางด้านวิธีการใช้งานและการแสดงผล โดยแอปพลิเคชันต่างๆ ที่ทำงานเกี่ยวข้องกันมารวมในรูปแบบของ Network Application เพื่อตอบสนองการบริหารและการจัดการประสิทธิภาพของเครือข่าย ทำให้ทราบถึงข้อมูลต่างๆ ในระบบเครือข่าย เช่น สาเหตุของการเกิดข้อผิดพลาด ความหนาแน่นของข้อมูลเกิดตรงส่วนใดในเครือข่าย เวลาที่เกิดข้อผิดพลาดและส่งผลกระทบต่อส่วนใดในระบบเครือข่าย เป็นต้น

11.6 แอปพลิเคชันที่ทำงานบนระบบเครือข่าย

แอปพลิเคชันที่ทำงานบนระบบเครือข่าย (Network Application) แต่ละชนิดเหมาะสำหรับการใช้งานที่แตกต่างกันไป นอกเหนือจาก WWW และอีเมลแล้ว Network Application อื่นๆ ที่นิยมใช้ในปัจจุบัน ได้แก่ Tenet, File Transfer Protocol (FTP), Video Conference, Instant Messaging และ Web Services โดยมีรายละเอียด ดังนี้ (สุธี พงศา-สกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 334-337)

1. Telnet

เทลเน็ต (Telnet) เป็นแอปลิเคชันสำหรับเข้าใช้งานคอมพิวเตอร์ที่ต้องการจากเครื่องคอมพิวเตอร์อีกเครื่องหนึ่งผ่านระบบเครือข่ายอินเทอร์เน็ต โดยผู้ใช้จะต้องป้อนคำสั่งผ่านคอมพิวเตอร์ของตัวเองไปยังคอมพิวเตอร์ปลายทาง ซึ่งจะส่งผลลัพธ์กลับมาที่เครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้สามารถใช้ทรัพยากรต่างๆ ของคอมพิวเตอร์ปลายทางเหมือนกับการเข้าใช้งานจากคอมพิวเตอร์โดยตรง แต่ผู้ใช้บริการจะต้องติดตั้งโปรแกรม Telnet Client และคอมพิวเตอร์ปลายทางจะต้องติดตั้งโปรแกรม Telnet Server เพื่อใช้ในการรับส่งคำสั่ง ข้อควรระวังในการใช้ Telnet คือ การถูกคุกคามจากบุคคลที่ไม่ปรารถนาดี สำหรับการป้องกันอาจทำได้โดยกำหนดบัญชีชื่อผู้ใช้ และรหัสผ่านไว้ที่เครื่อง Server และทำการกำหนดหมายเลข IP ที่อนุญาตให้ใช้บริการTelnet ได้

2. File Transfer Protocol (FTP)

File Transfer Protocol (FTP) เป็นแอปลิเคชันสำหรับการรับส่งไฟล์ผ่านเครือข่ายอินเทอร์เน็ต โดยผู้ใช้บริการสามารถดึงไฟล์ข้อมูลของเครื่อง Server มาเก็บที่เครื่องของตนได้ เรียกว่า การดาวน์โหลดข้อมูล ส่วนการส่งไฟล์ข้อมูลไปเก็บบนเครื่อง Server เรียกว่า การอัพโหลดข้อมูล

คอมพิวเตอร์ที่ใช้บริการ FTP เรียกว่า FTP Server และคอมพิวเตอร์ของผู้ใช้บริการ เรียกว่า FTP Client เมื่อต้องการรับส่งไฟล์ข้อมูล ผู้ใช้บริการจะต้องเชื่อมต่อไปยัง FTP Server โดยการส่งการร้องขอ FTP Request ไปยัง FTP Server โดยทั่วไปไฟล์ข้อมูลที่อยู่บน FTP Server จะถูกบีบอัดให้มีขนาดเล็ก เพื่อเป็นการประหยัดเนื้อที่ในการจัดเก็บ และเพิ่มความเร็วในการรับส่งข้อมูล ปัจจุบันสามารถแบ่ง Server ที่ใช้ที่ให้บริการ FTP ได้เป็น 2 ประเภท ดังนี้

2.1 Closed Site เป็น Server ที่ผู้ใช้บริการต้องสมัครสมาชิกก่อนจึงจะสามารถเชื่อมต่อได้ โดยผู้ใช้จะต้องป้อนชื่อผู้ใช้และรหัสผ่านได้รับจากการสมัครสมาชิก เมื่อเข้าสู่ FTP Server แล้วจะปรากฏรายชื่อของไฟล์และไดเร็คทอรี่ที่ผู้ใช้สามารถใช้งานได้

2.2 Anonymous Site เป็น Server สาธารณะที่ผู้ใช้สามารถเชื่อมต่อได้โดยไม่ต้องสมัครสมาชิก โดยการป้อนคำว่า Anonymous เป็นชื่อผู้ใช้ และใช้เบอร์อีเมลของผู้ใช้เป็นรหัสผ่าน ซึ่งบาง Server อาจไม่ต้องใช้รหัสผ่านก็ได้ เมื่อเข้าสู่ FTP Server แล้ว จะปรากฏรายชื่อของไฟล์ และไดเร็คทอรี่ที่ผู้ใช้สามารถดาวน์โหลดได้ ดังนั้น ผู้ใช้ทราบเพียงชื่อของ Server ที่ให้บริการก็สามารถเชื่อมต่อเพื่อดาวน์โหลดไฟล์ที่ต้องการได้ทันที การใช้งาน Anonymous Sits อาจจะมีการจำกัดสิทธิ์การเข้าถึงข้อมูลไว้ เช่น ผู้ใช้จะเห็นเฉพาะบางไฟล์หรือบางไดเร็คทอรี่เท่านั้น หรืออาจจะไม่สามารถส่งไฟล์ไปเก็บที่เครื่อง Server ได้ เป็นต้น

3. Video Conference

Video Conference เป็น Real-Time Application ที่สามารถแลกเปลี่ยนข้อมูลเสียงและวิดีโอได้ เหมาะสำหรับใช้ในการประชุม ซึ่งผู้เข้าร่วมประชุมไม่จำเป็นต้องอยู่ในสถานที่เดียวกันแต่สามารถพูดคุยและมองเห็นหน้ากันได้ ประโยชน์ของ Video Conference คือ ประหยัดเวลาและค่าใช้จ่ายในการเดินทางเข้าร่วมประชุม

อุปกรณ์ที่จำเป็นสำหรับ Video Conference ได้แก่ เครื่องคอมพิวเตอร์ที่ติดตั้งการ์ดเสียง กล้องถ่ายวิดีโอ ไมโครโฟน ลำโพง และโปรแกรมที่ใช้ควบคุมการรับส่งข้อความ ภาพ เสียง และไฟล์ต่างๆ ให้มีประสิทธิภาพ เพื่อให้การประชุมเป็นไปอย่างราบรื่น

4. Instant Messaging (IM)

Instant Messaging (IM) เป็น Real-Time Application ที่สามารถส่งข้อความสั้นๆ โต้ตอบกันได้แบบ Real-Time กล่าวคือ ผู้รับจะได้รับข้อความทันทีที่มีการส่งข้อความ ซึ่งกำลังเป็นที่นิยมในปัจจุบัน ปัจจุบันมีการพัฒนาให้สามารถส่งไฟล์ ข้อมูล รูปภาพ เสียง ภาพเคลื่อนไหว และวิดีโอ ตัวอย่างโปรแกรม Instant Message ที่ใช้ในปัจจุบัน ได้แก่ ICQ, AOL, MAN Messenger และ Yahoo Messenger เป็นต้น

5. Web Server

Web Server เป็น Web Application ที่ติดตั้งบนฝั่ง Server ทำหน้าที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต โดย Application อื่นๆ สามารถเรียกใช้งานและติดต่อสื่อสารกันผ่านภาษา XML (eXtensible Markup Language) และด้วยคุณสมบัติของภาษา XML จึงทำให้ Application ที่อยู่ภายใต้ระบบปฏิบัติการต่างกัน สามารถทำงานร่วมกันได้บนโพรโทคอล HTTP

เช่น Application ที่ทำงานอยู่บนระบบปฏิบัติการ Windows สามารถเรียกใช้งาน Application ที่ทำงานอยู่บนระบบ ปฏิบัติการ Unix ได้ เป็นต้น

11.7 สรุป

แอปพลิเคชัน (Application) คือโปรแกรมต่างๆ ที่สามารถนำมาใช้งานได้โดยการติดตั้งที่เครื่องคอมพิวเตอร์

World Wide Web เป็นแอปพลิเคชันที่ทำให้เครือข่ายอินเทอร์เน็ตเป็นที่รู้จักกันอย่างแพร่หลาย ซึ่งใช้โพรโทคอล HTTP ในการติดต่อข้อมูลข่าวสาร ผ่านเครือข่ายอินเทอร์เน็ตและนำเสนอข้อมูลในรูปแบบของหน้าเว็บเพจ (Web Page) ซึ่งแสดงข้อมูลได้หลายอย่าง

อีเมล (E-mail) การส่งจดหมายผ่านระบบเครือข่าย วิธีการนี้ช่วยลดค่าใช้จ่ายและประหยัดเวลาได้อย่างมาก เนื่องจากผู้ใช้สามารถส่งข้อความ หรือข้อมูลผ่านE-mail จากที่ห่างไกลมาถึงผู้รับโดยทางเครือข่ายอินเทอร์เน็ต การติดต่อสื่อสารด้วย E-mail จะใช้ชื่อที่อยู่ที่เรียกว่า E-mail Address ของผู้รับหรือผู้ส่งเป็นสำคัญ

อีคอมเมิร์ซ (E-Commerce) หรือ การพาณิชย์อิเล็กทรอนิกส์ หมายถึง การทำการค้าผ่านระบบสื่อสารอิเล็กทรอนิกส์ เช่น เครือข่ายอินเทอร์เน็ต เพื่ออำนวยความสะดวกในการติดต่อระหว่างลูกค้ากับเจ้าของสินค้าหรือบริการผ่านทางเครือข่ายอินเทอร์เน็ต ทำให้ไม่ต้องเดินทางติดต่อซื้อขายกันโดยตรง และไม่ต้องลงทุนสูง เนื่องจากการดำเนินการทุกอย่างทำได้ด้วยแอปพลิเคชัน

Protocol Analyzer เป็นอีกวิธีหนึ่งที่ใช้ในการวิเคราะห์แพ็กเก็ตข้อมูลที่เกิดจากกระบวนการขนส่งข้อมูลของโพรโทคอลชนิดต่างๆ เพื่อให้ทราบถึงการทำงานของข้อมูลที่อยู่ภายในแพ็กเก็ต การวิเคราะห์ดังกล่าวอาจทำให้ทราบถึงสาเหตุต่างๆ เช่น ความหนาแน่นของข้อมูลที่อาจเกิดจากปริมาณหรือขนาดของแพ็กเก็ตข้อมูล เป็นต้น โดยแอปพลิเคชันเหล่านี้มีหลายรูปแบบและใช้ชื่อเรียกแตกต่างกันไป เช่น Network Analyzer, Protocol Analyzer และ Packet Sniffer เป็นต้น

Network Application แต่ละชนิดเหมาะสำหรับการใช้งานที่แตกต่างกันไป นอกเหนือจาก WWW และอีเมลแล้ว Network Application อื่นๆ ที่นิยมใช้ในปัจจุบัน ได้แก่ Tenet, File Transfer Protocol (FTP), Video Conference, Instant Messaging และ Web Services

บทที่ 12
การออกแบบและจัดการเครือข่าย

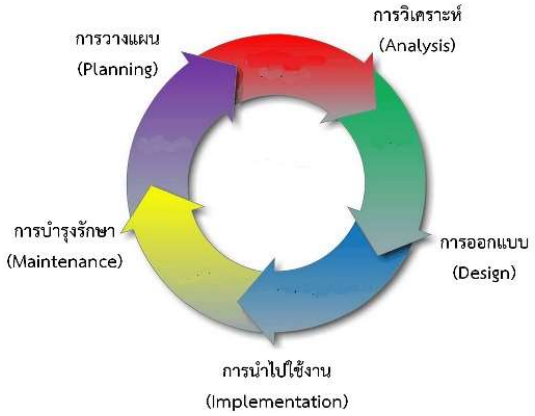
สิ่งสำคัญอีกประการหนึ่งที่เกี่ยวข้องกับการใช้งานเครือข่ายคอมพิวเตอร์ คือ การจัดการเครือข่ายในด้านต่างๆ เครือข่ายที่สามารถตอบสนองความต้องการและรองรับผู้ใช้ได้อย่างทั่วถึง จำเป็นต้องมีการจัดการเครือข่ายที่มีประสิทธิภาพ ทั้งในด้านการทำงาน การออกแบบการควบคุมข้อผิดพลาด การจัดการกลุ่มผู้ใช้ และการจัดการด้านความปลอดภัย โดยในบทนี้จะกล่าวถึงเครื่องมือและมาตรฐานในการจัดการเครือข่ายที่สำคัญ หลักการทำงานของโพรโทคอล รวมทั้งแนวทางในการจัดการค่าใช้จ่ายของระบบเครือข่าย

12.1 การออกแบบเครือข่าย

การออกแบบเครือข่าย (Network Design) เป็นการเพิ่มประสิทธิภาพให้กับเครือข่ายคอมพิวเตอร์ที่มีการใช้งานอยู่เดิม มีการปรับปรุงโครงสร้างเพิ่มเติมหรือลดขนาดของเครือข่ายคอมพิวเตอร์ มีการนำระบบงานประยุกต์ เทคโนโลยี หรือโพรโทคอลมาใช้เป็นในการพัฒนาเพิ่มขีดความสามารถให้แก่เครือข่ายคอมพิวเตอร์ (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2560, หน้า 13-30)

การออกแบบและพัฒนาระบบเครือข่ายมีวัตถุประสงค์สำคัญที่แตกต่างกัน เช่น เพื่อขยายจำนวนและฐานของผู้ใช้ เพื่อสร้างความพึงพอใจให้แก่ผู้ใช้ สร้างมาตรฐานบริการให้กับลูกค้าอย่างครบถ้วน เพิ่มผลกำไรและการเติบโตขององค์กร และเพิ่มประสิทธิภาพในการดำเนินงาน เป็นต้น โดยแต่ละวัตถุประสงค์ย่อมมีทิศทางในการพัฒนาและความต้องการที่แตกต่างกัน ดังนั้น การวิเคราะห์และการออกแบบจะใช้วงจรการพัฒนาระบบมาช่วย โดยวงจรการพัฒนาระบบจะวางแผนที่ได้รับความนิยมและนำมาใช้กันอย่างแพร่หลาย คือ System Development Life Cycle (SDLC)

System Development Life Cycle (SDLC) เป็นรูปแบบโครงสร้างของวงจรการพัฒนาระบบ ประกอบด้วยขั้นตอนต่างๆ ได้แก่ การวางแผน การวิเคราะห์ การออกแบบ การนำไปใช้งาน และการบำรุงรักษา โดยมีรายละเอียดของลำดับแสดงดังภาพที่ 12.1 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 392)



ภาพที่ 12.1 แสดงกระบวนการของ Systems Development Life Cycle
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 392)

12.1.1 การพัฒนาระบบด้วยกระบวนการ SDLC

ขั้นตอนการพัฒนาระบบด้วยกระบวนการ SDLC มีดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 393-394)

1. การวางแผน (Planning) เป็นขั้นตอนในการจำแนกปัญหา โดยระบุปัญหาที่เกิดขึ้นและกำหนดวัตถุประสงค์ในการพัฒนาระบบ เพื่อให้ทราบแนวทางในการดำเนินการได้อย่างคร่าวๆ และต้องคำนึงถึงเป้าหมายในการแก้ไขปัญหาต่างๆ เป็นหลัก

2. การวิเคราะห์ (Analysis) เป็นขั้นตอนที่นำข้อมูลต่างๆ มาวิเคราะห์และตัดสินใจ เพื่อให้ทราบถึงวิธีการที่จะนำมาใช้ในการแก้ไขปัญหา โดยต้องมีการพิจารณาความต้องการของระบบเพื่อให้ทราบแนวทางในการพัฒนาของแต่ละส่วนว่าจำเป็นต้องใช้ทรัพยากรหรือระยะเวลามากน้อยเพียงใด

3. การออกแบบ (Design) เป็นขั้นตอนการออกแบบและสร้างแนวทางในการพัฒนาตามข้อมูลที่ผ่านการวิเคราะห์ซึ่งจะแสดงถึงรูปแบบของระบบได้ชัดเจนมากขึ้น มีการจัดทำเอกสารการออกแบบหรือโครงสร้างต่างๆ ที่สามารถนำเสนอต่อผู้ใช้ทราบรายละเอียดงาน

4. การนำไปใช้งาน (Implementation) เป็นขั้นตอนที่จะเริ่มดำเนินการติดตั้งระบบ และเตรียมพร้อมที่จะใช้งานจริงโดยอาจแทนที่ระบบดังกล่าวทันทีหรือค่อยๆ เปลี่ยนแปลงในบางส่วนเพื่อสร้างความคุ้นเคยแก่ผู้ใช้เสียก่อน ซึ่งในขั้นตอนนี้จำเป็นต้องมีการอบรมวิธีการใช้งานแก่ผู้ใช้ทั้งหมดด้วย

5. การบำรุงรักษา (Maintenance) เป็นขั้นตอนหลังจากการนำระบบที่พัฒนามาใช้งานแล้ว โดยจะต้องรวบรวมข้อมูลการใช้งาน และเตรียมการแก้ไขข้อผิดพลาดต่างๆ ที่อาจเกิดขึ้นซึ่งอาจเกิดขึ้น เพื่อให้การทำงานของระบบมีประสิทธิภาพมากขึ้น ขั้นตอนนี้ควรทำอย่างต่อเนื่องจนแน่ใจว่าผู้ใช้สามารถใช้งานได้อย่างคล่องตัว และสามารถแก้ปัญหาได้ในระดับหนึ่ง

การพัฒนาระบบแบบ SDLC เป็นรูปแบบวงกลม แสดงให้เห็นถึงการพัฒนาในแต่ละขั้นตอนไม่จำเป็นต้องดำเนินการตามลำดับ ขึ้นอยู่กับขนาดของงานหรือรูปแบบการดำเนินงาน โดยตั้งอยู่บนพื้นฐานของวัตถุประสงค์ที่องค์กรคาดหวังไว้ การดำเนินงานแบบ SDLC อาจดำเนินการหลายขั้นตอนควบคู่กันไป โดยแต่ละขั้นตอนจำเป็นต้องมีการวางแผนและวิเคราะห์โดยนักวิเคราะห์ระบบ เพื่อให้สามารถดำเนินงานในแต่ละขั้นตอนได้อย่างมีประสิทธิภาพ

12.1.2 ปัจจัยสำคัญในการออกแบบระบบเครือข่าย

ปัจจัยสำคัญที่ต้องคำนึงในการออกแบบระบบเครือข่าย มีดังนี้ (สุธี พงศา-สกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 394-396)

1. การรวบรวมและวิเคราะห์ความต้องการ

การออกแบบระบบเครือข่าย ควรทราบความต้องการของผู้ใช้งานหรือวัตถุประสงค์ในการใช้งานระบบเครือข่าย รวมทั้งนโยบายของแต่ละองค์กรก่อน เพื่อให้ทราบถึงแนวทางในการออกแบบ การเลือกใช้อุปกรณ์และเทคโนโลยีที่เหมาะสมกับความต้องการ โดยรวบรวมความต้องการของผู้ใช้หรือบุคลากรในองค์กรแล้วนำมาวิเคราะห์ความต้องการที่แท้จริงเพื่อเป็นแนวทางในการออกแบบระบบเครือข่าย

2. รูปแบบที่เหมาะสมสำหรับเครือข่าย

เมื่อทราบถึงความต้องการและวัตถุประสงค์ขององค์กรแล้ว แต่ละองค์กรอาจจะเลือกใช้ประเภทของเครือข่ายที่แตกต่างกัน ซึ่งรวมถึงรูปแบบโครงสร้างของเครือข่ายและการเชื่อมโยงระหว่างอุปกรณ์กับกลุ่มผู้ใช้ภายในระบบเครือข่ายด้วย โดยขึ้นอยู่กับลักษณะทางกายภาพขององค์กร เนื่องจากสถานที่หรือที่ตั้งของแต่ละองค์กรอาจแตกต่างกัน

3. เทคโนโลยีและอุปกรณ์

ความต้องการของเทคโนโลยีและอุปกรณ์ที่ใช้ก็เป็นอีกหนึ่งปัจจัยที่ส่งผลต่อการออกแบบระบบเครือข่าย เนื่องจากเทคโนโลยีและอุปกรณ์แต่ละชนิดมีข้อจำกัดและขีด

ความสามารถต่างกัน ดังนั้น จึงควรเลือกเทคโนโลยีและอุปกรณ์ที่สามารถเพิ่มประสิทธิภาพและความคุ้มค่าในการนำไปใช้กับระบบเครือข่าย

4. งบประมาณ

งบประมาณเป็นอีกปัจจัยที่อาจส่งผลกระทบต่อปัจจัยอื่นๆ ได้ เนื่องจากการเลือกใช้เทคโนโลยีหรืออุปกรณ์ที่ทันสมัยและมีประสิทธิภาพอาจต้องใช้งบประมาณค่อนข้างสูง สำหรับองค์กรขนาดเล็กงบประมาณเป็นปัจจัยที่อาจส่งผลกระทบต่อการทำงานทั้งองค์กรได้ ดังนั้น ควรนำงบประมาณมาใช้อย่างเหมาะสมภายใต้ขอบเขตความต้องและวัตถุประสงค์ในการใช้งานระบบเครือข่าย

5. การให้บริการ

ระบบเครือข่ายต้องสนับสนุนและช่วยเหลือการทำงานของผู้ใช้ด้วยการให้บริการต่างๆ ที่สอดคล้องกับความต้องการและวัตถุประสงค์ของแต่ละองค์กร ดังนั้น การออกแบบระบบเครือข่ายจึงต้องพิจารณาถึงรูปแบบของบริการที่จำเป็นและสิ่งอำนวยความสะดวกในการดำเนินงานต่างๆ ภายในองค์กร โดยองค์กรอาจแยกหน้าที่ให้บริการออกเป็นกลุ่ม ซึ่งมีเครื่อง Server เป็นตัวจัดการและให้บริการต่างๆ เช่น การจัดเก็บข้อมูลโดย File Server การรับส่ง E-mail โดย Mail Server และการแสดงผลของแอปพลิเคชันโดย Application Server เป็นต้น

12.2.3 การทดสอบและประเมินประสิทธิภาพของระบบเครือข่าย

ขั้นตอนสุดท้ายก่อนที่จะสรุปเพื่อเสนอต่อผู้ใช้หรือลูกค้า คือ การทดสอบประสิทธิภาพรวมทั้งข้อผิดพลาดที่เกิดขึ้นจากระบบเครือข่ายที่ได้ออกแบบไว้ และเป็นการประเมินให้ผู้ใช้เห็นถึงประสิทธิภาพที่ได้จากเทคโนโลยีและอุปกรณ์ที่เลือกใช้ มีรายละเอียด ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 403)

1. การทดสอบระบบเครือข่ายที่ออกแบบ

การทดสอบระบบเครือข่ายนั้นจะเกี่ยวข้องกับการหาข้อผิดพลาดที่อาจเกิดขึ้นกับระบบ ซึ่งเป็นการป้องกันและเป็นตัววัดความสามารถของระบบเครือข่ายที่ได้ออกแบบ การทดสอบจะใช้วิธีการต่างๆ โดยผู้เชี่ยวชาญและผู้ใช้ภายในองค์กร การทดสอบควรพิจารณาถึงปัจจัยที่สำคัญ ดังนี้

1.1 ตรวจสอบว่าระบบเครือข่ายตอบสนองต่อผู้ใช้ได้ตรงความต้องการและวัตถุประสงค์หรือไม่

1.2 ตรวจสอบบริการของระบบเครือข่ายว่าครอบคลุมกับรูปแบบการทำงานของผู้ใช้หรือไม่

1.3 ค้นหาปัญหาและข้อผิดพลาดที่อาจเกิดขึ้นทั้งในเครือข่ายย่อยและเส้นทางการเชื่อมโยงหลักของระบบเครือข่าย

1.4 ทดสอบเส้นทางการเชื่อมโยงและระบบเครือข่ายสำรองว่าพร้อมใช้งานหรือไม่

1.5 วิเคราะห์ผลกระทบที่เกิดขึ้นเมื่อเกิดข้อผิดพลาดต่างๆ

1.6 ระบุถึงความเสี่ยงที่อาจเกิดขึ้นกับระบบเครือข่ายเพื่อวางแผนสำรองไว้ล่วงหน้า

1.7 สร้างความเชื่อมั่นให้กับผู้ใช้ซึ่งการแก้ไขปัญหาที่เกิดขึ้นในการทดสอบระบบเครือข่าย

2. การประเมินประสิทธิภาพของระบบเครือข่ายที่ออกแบบ

การประเมินประสิทธิภาพของระบบเครือข่ายนั้นจะต้องทำหลังจากขั้นตอนการทดสอบระบบในรูปแบบต่างๆ เพื่อหาความพึงพอใจหรือความสามารถของระบบว่าตรงกับที่องค์กรและผู้ใช้ต้องการหรือไม่ การประเมินประสิทธิภาพอาจทำได้ทั้งด้านเทคนิคและด้านความพึงพอใจ โดยทางเทคนิคจะประเมินจากการแสดงผล ความสามารถในการตอบสนองต่อผู้ใช้จำนวนข้อผิดพลาดที่เกิดขึ้นและความเร็วในการขนส่งข้อมูล สำหรับการประเมินด้านความพึงพอใจนั้น จะวัดจากความพึงพอใจของผู้ใช้ว่าตรงกับความต้องการมากน้อยเพียงใด

นอกจากที่กล่าวมาแล้ว การทำเอกสารยังเป็นอีกขั้นตอนที่จำเป็นต้องคำนึงด้วย เนื่องจากเอกสารเป็นส่วนที่ผู้ใช้สามารถพิจารณาดูได้โดยตรง ซึ่งรายละเอียดในเอกสารนั้นจะแตกต่างกันขึ้นอยู่กับความต้องการของแต่ละองค์กรว่าควรนำมาพิจารณาเพื่อช่วยในการตัดสินใจ

12.2 การจัดการเครือข่าย

การจัดการเครือข่าย (Network Management) คือ กระบวนการตรวจสอบ แก้ไข และควบคุมระบบเครือข่าย เพื่อให้มีความน่าเชื่อถือ สามารถตอบสนองความต้องการของผู้ใช้และทำงานได้อย่างมีประสิทธิภาพ โดย ISO ได้กำหนดมาตรฐานสำหรับจัดการระบบเครือข่ายครอบคลุม 5 ด้าน มีรายละเอียดดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 370-375)

12.2.1 การจัดการด้านการกำหนดค่าของระบบเครือข่าย (Configuration Management)

การจัดการด้านการกำหนดค่าของระบบเครือข่าย เป็นการกำหนดค่าที่จำเป็นต่อการใช้งานในระบบเครือข่าย โดยจะกำหนดไว้ตั้งแต่เริ่มติดตั้งระบบเครือข่าย หรือเมื่อต้องการเปลี่ยนแปลงการทำงานบางอย่างกับระบบเครือข่าย เช่น การลดหรือเพิ่มจำนวนของเครือข่าย การติดตั้งคอมพิวเตอร์เพิ่มเติม และการเพิ่มรายชื่อผู้ใช้งาน เป็นต้น สามารถแบ่งได้ 2 ระบบ ดังนี้

1. การตั้งค่า หรือการกำหนดค่าใหม่ (Reconfiguration) เป็นการเปลี่ยนแปลงที่เกิดขึ้นในระบบเครือข่ายที่ส่งผลให้ผู้ดูแลระบบเครือข่ายต้องตั้งค่า หรือกำหนดค่าต่างๆ ใหม่จากการเปลี่ยนแปลงใน 3 ด้าน ดังนี้

1.1 การกำหนดค่าใหม่ให้แก่ฮาร์ดแวร์ (Hardware Reconfiguration) การเปลี่ยนแปลงด้านฮาร์ดแวร์ในระบบเครือข่ายจะส่งผลให้ต้องกำหนดค่าต่างๆ ใหม่ เพื่อให้ผู้ใช้สามารถเข้าใช้ทรัพยากรต่างๆ ในเครือข่ายได้ เช่น การนำคอมพิวเตอร์เครื่องใหม่มาติดตั้งเพิ่มในระบบ ต้องกำหนดหมายเลข IP ให้แก่คอมพิวเตอร์ดังกล่าว เพื่อให้สามารถเข้าใช้งานอินเทอร์เน็ตได้ เป็นต้น

1.2 การกำหนดค่าใหม่ให้แก่ซอฟต์แวร์ (Software Reconfiguration) เป็นการจัดการที่เกี่ยวข้องกับการเปลี่ยนแปลงต่างๆ ที่เกิดขึ้นกับซอฟต์แวร์ เช่น การติดตั้งโปรแกรมใหม่ การอัพเดตโปรแกรม และการอัพเดตระบบปฏิบัติการ เป็นต้น องค์กรขนาดใหญ่ที่มีคอมพิวเตอร์จำนวนมากสามารถนำระบบเครือข่ายมาใช้ให้เป็นประโยชน์ โดยให้ผู้ใช้ที่ต้องการอัพเดต และติดตั้งโปรแกรมใหม่ดาวน์โหลดจาก Server ที่จัดเก็บซอฟต์แวร์เหล่านั้นไว้

1.3 การกำหนดค่าใหม่ให้แก่ผู้ใช้งานในระบบเครือข่าย (User-Account Reconfiguration) เป็นการจัดการผู้ใช้งานในระบบเครือข่าย เช่น การเพิ่มหรือลดบัญชีรายชื่อผู้ใช้ การกำหนดสิทธิ์ในการใช้งานทรัพยากรของเครือข่าย เป็นต้น

2. การจัดทำเอกสาร (Documentation) เป็นการบันทึกรายละเอียดของการตั้งค่า หรือกำหนดค่า (Configuration) ต่างๆ เมื่อมีการเปลี่ยนแปลงในระบบเครือข่าย โดยจัดทำให้อยู่ในรูปของเอกสาร และเก็บไว้เป็นข้อมูลขององค์กร เพื่อใช้ประโยชน์ในอนาคต สามารถแบ่งได้ 3 ประเภท ดังนี้

2.1 เอกสารฮาร์ดแวร์ (Hardware Documentation) เป็นเอกสารสำหรับบันทึกการเปลี่ยนแปลงที่เกิดขึ้นกับฮาร์ดแวร์ในระบบเครือข่าย แบ่งออกได้ 2 ประเภท ดังนี้

2.1.1 เอกสารแสดงที่ตั้งของฮาร์ดแวร์ เป็นเอกสารแสดงสถานที่ตั้งของฮาร์ดแวร์ และแสดงการเชื่อมต่อของฮาร์ดแวร์ในระบบเครือข่าย

2.1.2 เอกสารแสดงรายละเอียดฮาร์ดแวร์ เป็นเอกสารที่ระบุรายละเอียดของฮาร์ดแวร์แต่ละชนิดที่อยู่ในระบบเครือข่าย เช่น ประเภทหมายเลข Serial วันเวลาที่ซื้อ ใบประกันสินค้า และรายชื่อ ที่อยู่ หรือเบอร์ติดต่อของผู้จำหน่ายฮาร์ดแวร์ เป็นต้น

2.2 เอกสารซอฟต์แวร์ (Software Documentation) เป็นเอกสารที่จัดทำขึ้นเพื่อบันทึกรายละเอียดของซอฟต์แวร์ที่นำมาใช้ในระบบเครือข่าย เช่น ประเภท เวอร์ชัน และวันเวลาที่ติดตั้งซอฟต์แวร์

2.3 เอกสารรายชื่อผู้ใช้งาน (User-Account Documentation) เป็นเอกสารที่จัดทำขึ้นเพื่อบันทึกรายละเอียดของผู้ใช้งานในระบบเครือข่าย เช่น ข้อมูลเกี่ยวกับรายชื่อผู้ใช้งาน กลุ่มของผู้ใช้งาน และสิทธิ์ในการใช้งาน เป็นต้น เอกสารควรได้รับการแก้ไขข้อมูลให้ทันสมัยอยู่เสมอ เพราะการเปลี่ยนแปลงผู้ใช้งานในระบบอาจเกิดขึ้นได้ตลอดเวลา

12.2.2 การจัดการด้านความผิดพลาด (Fault Management)

การจัดการด้านความผิดพลาด เป็นการจัดการปัญหาและความผิดพลาดต่างๆ ที่เกิดขึ้นในระบบ แบ่งได้เป็น 4 ขั้นตอน ดังนี้

1. การตรวจสอบ (Detecting) เป็นขั้นตอนในการระบุปัญหา และความผิดพลาดต่างๆ ที่เกิดขึ้นพร้อมทั้งระบุบริเวณเครือข่ายที่ได้รับความเสียหาย เพื่อนำข้อมูลที่ได้มาตรวจสอบสาเหตุของปัญหาและความผิดพลาดของระบบเครือข่ายที่เป็นไปได้

2. การแยกประเภทของปัญหา และความผิดพลาด (Isolating) การแยกประเภทของปัญหา และความผิดพลาดที่เกิดขึ้นจะทำให้ระบุกลุ่มของผู้ใช้ที่ได้รับผลกระทบจากความผิดพลาดที่เกิดขึ้นได้ นอกจากนี้ยังสามารถกำหนดระยะเวลาในการดำเนินการแก้ไขปัญหาและความผิดพลาดของแต่ละประเภทได้อีกด้วย

3. การแก้ปัญหา (Correcting) เป็นขั้นตอนการดำเนินงานแก้ปัญหา โดยต้องคำนึงถึงความเร่งด่วนในการใช้งาน และระยะเวลาที่ใช้ในการแก้ปัญหาแต่ละประเภท

4. การบันทึก (Recording) เป็นการบันทึกรายละเอียดที่เกี่ยวกับการจัดการปัญหา และข้อผิดพลาดที่เกิดขึ้น โดยบันทึกเกี่ยวกับลักษณะของปัญหาที่เกิดขึ้นในระบบ บริเวณที่เกิดปัญหา สาเหตุที่อาจเป็นไปได้ การดำเนินการเพื่อแก้ปัญหา ค่าใช้จ่าย และระยะเวลาที่ใช้ในแต่ละขั้นตอน การบันทึกมีความสำคัญ ดังนี้

4.1 ข้อมูลที่บันทึกไว้สามารถนำไปจัดการกับปัญหาแบบเดียวกันที่อาจเกิดขึ้นในอนาคต โดยไม่ต้องเสียเวลาและค่าใช้จ่ายในการค้นหาสาเหตุ หรือวิธีแก้ไขปัญหา

4.2 ทราบปัญหาที่เกิดขึ้นซ้ำๆ ในบริเวณเดิม ซึ่งอาจนำไปสู่ปัญหาใหญ่ของระบบโดยรวมได้ ดังนั้น หากปัญหาเหล่านี้ได้รับการบันทึกไว้ ผู้ดูแลระบบจะสามารถสังเกตเห็นและแก้ปัญหาได้ทันท่วงที

4.3 ข้อมูลที่ได้รับการบันทึกไว้สามารถนำมาจัดเก็บเป็นสถิติของปัญหาที่เกิดขึ้นกับระบบเครือข่าย และอาจนำข้อมูลทางสถิติดังกล่าวมาวิเคราะห์ เพื่อหาวิธีป้องกันไม่ให้เกิดปัญหาเดิมอีก

12.2.3 การจัดการด้านประสิทธิภาพ (Performance Management)

การจัดการด้านประสิทธิภาพ เป็นการจัดการระบบเครือข่าย เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพสูงสุด ซึ่งปัจจัยที่บ่งบอกถึงประสิทธิภาพของระบบเครือข่าย ได้แก่ ปริมาณข้อมูล การจราจร อัตราส่งผ่านข้อมูล และระยะเวลาตอบกลับ โดยผู้ดูแลระบบต้องคอยตรวจสอบและจัดการให้ปัจจัยเหล่านี้อยู่ในระดับที่ยอมรับได้ รายละเอียดของปัจจัยทั้ง 4 ด้าน มีดังนี้

1. ปริมาณข้อมูล (Capacity) โดยทั่วไปแต่ละเครือข่ายจะถูกออกแบบให้สามารถรองรับในปริมาณที่แตกต่างกัน เช่น ระบบเครือข่ายแลนถูกออกแบบมาเพื่อรองรับคอมพิวเตอร์จำนวน 50 เครื่อง จะมีอัตราการส่งข้อมูลอยู่ในระดับหนึ่ง ถ้ามีการเพิ่มจำนวนคอมพิวเตอร์ในระบบเครือข่ายเกิน 50 เครื่อง อาจทำให้ปริมาณข้อมูลในเครือข่ายสูงขึ้น ซึ่งจะส่งผลให้อัตราการส่งข้อมูลลดลง และอาจทำให้เครือข่ายล่มได้ ดังนั้น เครือข่ายที่ต้องการให้ระบบทำงานได้อย่างมีประสิทธิภาพจึงไม่ควรนำคอมพิวเตอร์มาติดตั้งไว้มากกว่าที่ได้ออกแบบ

2. การจราจร (Traffic) ในระบบเครือข่ายแบ่งการจราจรออกเป็น 2 ส่วน คือ การจราจรภายในระบบเครือข่ายโดยวัดระดับการจราจรด้วยวิธีการนับแพ็กเก็ตภายในระบบเครือข่าย และการจราจรภายนอกระบบเครือข่าย โดยวัดระดับการจราจรด้วยวิธีการนับจำนวนแพ็กเก็ตที่แลกเปลี่ยนกันระหว่างเครือข่าย

3. อัตราการส่งผ่านข้อมูล (Throughput) เป็นความสามารถในการถ่ายโอนข้อมูลของอุปกรณ์เครือข่าย เช่น ฮับ สวิตช์ และเราท์เตอร์ โดยวัดจากความสามารถของอัตราเร็วในการส่งข้อมูล ซึ่งมีหน่วยเป็น Kbps, Mbps และ Gbps

4. ระยะเวลาตอบกลับ (Response Time) เป็นระยะเวลาทั้งหมดที่ใช้เพื่อแสดงผลลัพธ์ โดยเริ่มนับตั้งแต่ผู้ใช้บริการส่งคำร้องเพื่อขอใช้บริการจนกระทั่งได้ผลลัพธ์

กลับมา โดยผู้ดูแลระบบสามารถพิจารณาประสิทธิภาพของระบบเครือข่ายจากระยะเวลาตอบกลับ มี 2 ค่า คือ ระยะ เวลาตอบกลับเฉลี่ย (Average Response Time) และระยะเวลาตอบกลับในช่วงที่มีการใช้งานเครือข่ายสูงสุด (Peak-Hour Response Time) หากระยะเวลาตอบกลับมีค่าสูงขึ้นจะแสดงถึงปัญหาร้ายแรงของระบบเครือข่าย และจำเป็นต้องได้รับการแก้ไขโดยทันที

12.2.4 การจัดการด้านบัญชีผู้ใช้งาน (Accounting Management)

โดยทั่วไปทรัพยากรของระบบเครือข่ายสามารถรองรับผู้ใช้งานได้เพียงจำนวนหนึ่งเท่านั้น ดังนั้น หากต้องการให้ระบบเครือข่ายมีประสิทธิภาพมากขึ้น จำเป็นต้องควบคุม และจำกัดการใช้งานทรัพยากรในระบบเครือข่ายของผู้ใช้ ซึ่งเรียกว่าการจัดการด้านบัญชีผู้ใช้งาน (Accounting Management) โดยวิเคราะห์จากการใช้งานทรัพยากรเครือข่ายของผู้ใช้ในปัจจุบัน จากนั้นนำผลการวิเคราะห์ที่ได้มากำหนด หรือแบ่งปันการเข้าใช้ทรัพยากรให้เหมาะสม โดยอาจกำหนดในรูปของผู้ใช้เป็นกลุ่ม หรือเป็นรายบุคคลก็ได้

บัญชีผู้ใช้งานในระบบเครือข่ายแบ่งได้ 2 ประเภท คือ บัญชีผู้ใช้ (User Account) และบัญชีกลุ่มผู้ใช้ (Group Account) มีรายละเอียด ดังนี้

1. บัญชีผู้ใช้ (User Account)

การกำหนดชื่อผู้ใช้ของแต่ละคนมีผลต่อการจัดการระบบบัญชีรายชื่ออย่างมากการให้ผู้ใช้สามารถกำหนดชื่อได้อย่างอิสระเพื่อที่จะจดจำได้ง่าย แต่สร้างความยุ่งยากในด้านการบริหารและจัดการบัญชีรายชื่อ เนื่องจากชื่อของผู้ใช้อาจเป็นคำที่ไม่มีความหมายหรือเป็นคำที่ใช้กันซ้ำๆ ทำให้ไม่สามารถระบุรายละเอียดในด้านอื่นๆ ของผู้ใช้ได้เลย แต่ถ้ามีการตั้งชื่อโดยอาศัยโครงสร้างข้อมูลของผู้ใช้ เช่น ชื่อจริง ตำแหน่ง และแผนก เมื่อนำมาใช้ร่วมกันก็อาจทำให้ได้ชื่อเข้าใช้งานที่จดจำง่าย และช่วยให้บริหารบัญชีรายชื่อได้สะดวกมากขึ้น

สำหรับรหัสผ่านควรให้ผู้ใช้ตั้งโดยอิสระเพื่อให้ผู้ใช้แต่ละคนสามารถจดจำรหัสผ่านของตนเองได้ง่ายขึ้น โดยองค์กรอาจมีนโยบายให้รหัสผ่านต้องมีจำนวนตัวเลขหรืออักษรทั้งหมดอย่างน้อยกี่ตัว ขึ้นอยู่กับว่าระบบต้องการความปลอดภัยมากเพียงใด ในกรณีผู้ใช้กรอกรหัสผ่านไม่ครบถ้วนตามจำนวนครั้งที่กำหนด ให้ปิดบัญชีรายชื่อดังกล่าวชั่วคราวเพื่อป้องกันการลักลอบเข้าระบบ

2. บัญชีกลุ่มผู้ใช้ (Group Account)

บัญชีกลุ่มผู้ใช้ ใช้สำหรับกำหนดสิทธิ์ให้ผู้ใช้ที่มีหน้าที่หรือความรับผิดชอบที่คล้ายกัน เพราะผู้ใช้ในกลุ่มเดียวกันย่อมมีความต้องการด้านทรัพยากรเหมือนกัน การกำหนด

กลุ่มผู้ใช้จะช่วยให้สามารถจัดการและดูแลทรัพยากรต่างๆ ได้อย่างดี เนื่องจากการจัดการทรัพยากรเพียงครั้งเดียวจะส่งผลต่อกลุ่มผู้ใช้ทั้งหมด โดยไม่ต้องจัดการหรือควบคุมเป็นรายบุคคล ภายในแต่ละกลุ่มผู้ใช้จะต้องมีสิทธิ์ในการเข้าถึงข้อมูลและทรัพยากรที่เท่าเทียมกัน ไม่ควรให้เกิดความเหลื่อมล้ำหรือให้สิทธิพิเศษแก่บุคคลใดบุคคลหนึ่ง กลุ่มผู้ใช้ที่มีลำดับความสำคัญมากก็จะเข้าถึงทรัพยากรต่างๆ ได้ทั่วถึงและครอบคลุมมากกว่าผู้ใช้ที่มีลำดับความสำคัญน้อย

12.2.5 การจัดการด้านความปลอดภัย (Security Management)

การจัดการด้านความปลอดภัย (Security Management) เป็นการควบคุมการเข้าใช้ทรัพยากรเครือข่ายให้เป็นไปตามนโยบายด้านความปลอดภัยของระบบเครือข่าย เพื่อป้องกันอันตรายจากผู้ไม่หวังดีที่อยู่ทั้งภายในและภายนอกองค์กร สร้างความมั่นใจแก่ผู้ใช้ และเป็นการเพิ่มความน่าเชื่อถือแก่องค์กรอื่นที่จำเป็นต้องทำงานร่วมกัน การจัดการด้านความปลอดภัยสามารถทำได้หลายด้าน เช่น การพัฒนาการทำงานของอุปกรณ์เชื่อมต่อเครือข่าย และการเพิ่มทักษะและความรู้ให้แก่บุคลากรภายในองค์กร เป็นต้น เพื่อป้องกันความผิดพลาดที่อาจจะเกิดและส่งผลต่อความปลอดภัยของระบบเครือข่าย

จากที่กล่าวมาการจัดการด้านความปลอดภัยในระบบเครือข่ายเป็นเพียงแค่หนทางป้องกันการบุกรุกจากบุคคลที่ไม่หวังดีเท่านั้น หากบุคลากรทั้งหมดภายในองค์กรขาดความรอบคอบ และขาดจิตสำนึกในการดูแลรักษาความปลอดภัยของข้อมูลและทรัพยากร ถึงแม้จะมีระบบรักษาความปลอดภัยที่ดีมากเพียงใดก็ไม่อาจสร้างความมั่นคงและความเชื่อมั่นให้กับองค์กรได้

12.3 วัตถุประสงค์ในการออกแบบและจัดการเครือข่าย

การบริหารและการจัดการกับเครือข่ายของแต่ละอุปกรณ์อาจมีความแตกต่างกันออกไป แต่ไม่ว่าจะเป็นองค์กรขนาดใดก็ตาม จำเป็นต้องมีนโยบายในการดำเนินงานที่ชัดเจน เพื่อบ่งบอกทิศทางการพัฒนาและการเจริญเติบโตขององค์กรได้เป็นอย่างดี โดยระบบเครือข่ายที่จะนำมาใช้ในองค์กรนั้นจำเป็นต้องสอดคล้องกับนโยบาย เพื่อช่วยในการพัฒนาและขยายตัวของธุรกิจ ดังนั้น ในการบริหารและการจัดการกับระบบเครือข่ายในเชิงธุรกิจจึงต้องมีเป้าหมายและวัตถุประสงค์ที่ชัดเจน เพื่อช่วยสร้างความมั่นใจให้กับผู้ใช้ โดยมุ่งเน้นในเรื่องความพึงพอใจของลูกค้า งบประมาณ และผลกำไรซึ่ง วัตถุประสงค์ในการบริหารและจัดการเครือข่ายสามารถแบ่งได้ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 375-379)

12.3.1 ความพึงพอใจของผู้ใช้ (User Satisfaction)

การสร้างความพึงพอใจให้แก่ผู้ใช้ทั้งหมดมีส่วนเกี่ยวข้องกับระบบเครือข่ายเป็นวัตถุประสงค์อีกข้อหนึ่งที่ควรให้ความสำคัญ โดยเฉพาะในองค์กรที่เกี่ยวข้องกับธุรกิจต่างๆ ผู้ใช้ในที่นี้อาจรวมถึงลูกค้า ซึ่งเป็นกลุ่มที่สำคัญมากกว่าองค์กร เพราะเป็นผู้ที่สร้างรายได้และผลกำไรให้กับองค์กร การจัดการเครือข่ายเพื่อให้ผู้ใช้ทุกคนพอใจนั้นควรคำนึงถึงองค์กรองค์ประกอบ ดังนี้

1. ประสิทธิภาพในการแสดงผล (Performance) การวัดประสิทธิภาพในการแสดงผลจะวัดจากเวลาในการตอบสนอง (Response Time) โดยจำนวนของเวลาในการตอบสนองนั้นจะวัดจากระยะเวลาตั้งแต่ผู้ใช้ดำเนินการเปิดข้อมูลหรือร้องขอข้อมูลไปจนถึงการแสดงผลข้อมูลดังกล่าวบนหน้าจอจนครบถ้วนสมบูรณ์ การตอบสนองที่รวดเร็วจะช่วยให้ผู้ใช้สามารถดำเนินงานต่างๆ ได้อย่างคล่องตัว เนื่องจากไม่ต้องเสียเวลาในการรอผลลัพธ์นานเกินไป

2. เรียกใช้งานได้ง่ายและต่อเนื่อง (Availability) ระบบเครือข่ายที่สามารถตอบสนองความต้องการของผู้ใช้ได้ตลอดเวลาจะช่วยสร้างความพึงพอใจแก่ผู้ใช้ได้มาก เนื่องจากสามารถเรียกใช้งานเมื่อใดก็ได้ตามความต้องการ มีขั้นตอนที่ไม่ยุ่งยากหรือซับซ้อนมากเกินไป โดยเฉพาะในองค์กรที่เกี่ยวข้องกับการทำธุรกรรมผ่านระบบเครือข่าย ซึ่งจำเป็นต้องเปิดให้บริการลูกค้าตลอดเวลา และเมื่อใดที่ลูกค้าต้องการงานบนระบบเครือข่ายแล้วไม่ได้รับการตอบสนองที่ดีหรือเกิดความยุ่งยาก ย่อมสร้างความไม่พอใจแก่ลูกค้า

3. ความเชื่อถือ (Reliability) ความน่าเชื่อถือในการทำงานของระบบเครือข่ายจะเกี่ยวข้องกับอัตราความผิดพลาดของเครือข่ายทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์ หากอัตราการเกิดข้อผิดพลาดน้อย จะส่งผลให้มีความน่าเชื่อถือมากขึ้น ดังนั้น ระบบเครือข่ายจึงจำเป็นต้องมีมาตรฐานสำหรับการรองรับปัญหาหรือข้อผิดพลาดที่อาจเกิดขึ้นได้เสมอ และจะต้องไม่ส่งผลกระทบที่รุนแรงต่อผู้ใช้ เช่น การใช้เครื่อง ATM หากผู้ใช้โอนเงินไปยังบัญชีปลายทาง การดำเนินการควรใช้เวลาไม่นานเกินไป เพื่อให้ผู้ใช้มั่นใจว่าระบบสามารถทำงานได้เป็นปกติ และถ้าเกิดข้อผิดพลาดขึ้น ระบบควรแจ้งให้ผู้ใช้ทราบและไม่ควรให้เกิดผลกระทบต่อจำนวนเงินที่ทำการโอนด้วย เป็นต้น

4. การจัดเก็บและสำรองข้อมูล (Backup) การจัดเก็บและการสำรองข้อมูลนับเป็นองค์ประกอบหนึ่งที่สำคัญ เนื่องจากจะช่วยสร้างความน่าเชื่อถือให้กับระบบเครือข่ายและช่วยให้ผู้ใช้เกิดความมั่นใจได้อีกทางหนึ่ง การสำรองข้อมูลมีทั้งในส่วนของซอฟต์แวร์และ

ฮาร์ดแวร์ การสำรองในส่วนของซอฟต์แวร์ คือการจัดเก็บสำรองข้อมูลที่ใช้ในกระบวนการต่างๆ ไว้ในแหล่งอื่นที่มีซอฟต์แวร์คอยควบคุมดูแลการสำรองข้อมูล ส่วนการสำรองในส่วนของฮาร์ดแวร์ คือการเชื่อมต่ออุปกรณ์ต่างๆ นั้นควรมีเส้นทางสำรองในการเชื่อมโยงแลกเปลี่ยนข้อมูล หรือมีการจัดเก็บข้อมูลในระหว่างการขนส่งข้อมูลไว้เป็นช่วงๆ เพื่อป้องกันการสูญหายของข้อมูล

12.3.2 งบประมาณผลกำไร (Cost Effectiveness)

งบประมาณและผลกำไรเป็นวัตถุประสงค์ที่ควรให้ความสำคัญ เนื่องจากการพัฒนาระบบเครือข่ายเพื่อใช้งานนั้นต้องใช้องค์ประกอบต่างๆ จำนวนมาก และมีเรื่องค่าใช้จ่ายมาเกี่ยวข้อง ในองค์กรขนาดเล็กอาจไม่ได้รับผลกระทบมากนัก แต่องค์กรขนาดใหญ่ เมื่อมีการนำระบบเครือข่ายมาใช้งานอาจต้องเสียงบประมาณจำนวนมาก ดังนั้นจึงจำเป็นต้องพิจารณาและคำนึงถึงองค์ประกอบต่อไปนี้

1. การวางแผน (Planning) การวางแผนที่ดีจะช่วยให้การพัฒนาระบบเครือข่ายไม่สิ้นเปลืองงบประมาณมากเกินความจำเป็น การวางแผนจะเริ่มต้นจากการวิเคราะห์ความต้องการโดยรวมขององค์กร เพื่อให้ระบบเครือข่ายอยู่ภายในขอบเขตความต้องการ เมื่อมีการวางแผนที่ดีการดำเนินการต่างๆ ก็จะทำได้ง่ายและรวดเร็ว ทำให้เวลาที่ใช้ในการดำเนินงานต่างๆ ลดลง

2. การขยายและการเพิ่ม (Expansion) เป็นส่วนที่เกิดจากการวางแผนเพื่อรองรับการเปลี่ยนแปลงในอนาคต ส่งผลให้การขยายขนาดขององค์กรหรือการเพิ่มเติมของอุปกรณ์เข้ามาในเครือข่ายทำได้ง่ายและเสียงบประมาณไม่มาก การลงทุนเพื่อออกแบบและพัฒนาระบบขึ้นมาใหม่อาจเป็นวิธีที่สิ้นเปลืองงบประมาณมากกว่าการอาศัยพื้นฐานของระบบเครือข่ายเดิมมาปรับปรุง เพิ่มเทคโนโลยีให้ทันสมัย ช่วยให้ได้ระบบเครือข่ายที่สามารถตอบสนองต่อความต้องการใหม่ที่เกิดขึ้น โดยเฉพาะการเพิ่มจำนวนของผู้ใช้ในระบบเครือข่ายที่มีการขยายตัวค่อนข้างเร็วกว่าความต้องการในรูปแบบอื่น

3. การนำกลับมาใช้ใหม่ (Reuse) เป็นวิธีการที่ช่วยให้ประหยัดงบประมาณได้มากและเห็นผลที่สุด เนื่องจากเป็นการนำทรัพยากรที่มีอยู่แล้วนำกลับมาใช้ใหม่โดยเฉพาะอุปกรณ์พื้นฐาน เช่น เครื่องคอมพิวเตอร์ที่สามารถอัพเกรดให้มีความสามารถและประสิทธิภาพมากขึ้น หรือการอัพเดทแอปพลิเคชันให้มีความทันสมัยและเหมาะกับเทคโนโลยีนั้นๆ แต่ประสิทธิภาพการทำงานควรอยู่ในระดับที่น่าพอใจ เพราะการนำทรัพยากรเดิมกลับมาใช้ใหม่อาจส่งผลต่อการทำงานทั้งระบบ และอาจไม่สอดคล้องกับเทคโนโลยีใหม่ ทำให้ต้องเสีย

งบประมาณมากกว่าเดิม อย่างไรก็ตามการนำกลับมาใช้ใหม่ควรมีการวางแผนและวิเคราะห์ความต้องการของระบบเครือข่ายและผู้ใช้อย่างถี่ถ้วน

12.4 เครื่องมือออกแบบและจัดการเครือข่าย

ปัจจุบันซอฟต์แวร์ที่นำมาใช้เป็นเครื่องมือในการจัดการระบบเครือข่ายนั้นมีมากมายหลายค่าย เช่น IBM's NetView, HP's OpenView, Sun's SunNet Manager และ Novell's NMS เป็นต้น สำหรับเครื่องมือการจัดการระบบเครือข่าย (Network Management Tools) แบ่งออกเป็น 3 ประเภท ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 379-382)

12.4.1 เครื่องมือสำหรับการวิจัย (Diagnostic Tools)

เครื่องมือสำหรับการวิจัย เป็นเครื่องมือสำหรับการตรวจจับปัญหา และระบุบริเวณที่เกิดความผิดพลาด ช่วยให้ผู้ใช้ระบบทราบถึงความผิดปกติที่เกิดขึ้นในระบบเครือข่ายและสามารถหาแนวทางแก้ไขปัญหาได้ ตัวอย่างของเครื่องมือประเภทนี้ ได้แก่

1. Analog Line Monitors เป็นเครื่องมือสำหรับตรวจจับคลื่นรบกวน (Noise) ที่เกิดขึ้นกับระบบเครือข่าย โดยตรวจสอบจากสัญญาณแอนาล็อกของโมเด็ม

2. Cable Testers เป็นเครื่องมือสำหรับการตรวจจับความผิดพลาดที่เกิดในสาย สัญญาณ โดยตรวจสอบจากสัญญาณที่อยู่ภายในสายสัญญาณ

3. LAN Analyzers เป็นเครื่องมือสำหรับตรวจจับความผิดพลาดต่างๆ ในระบบเครือข่ายแลนโดยตรวจสอบจากค่าต่างๆ เช่น ตรวจสอบการจราจร (Network Traffic) ตรวจสอบปริมาณข้อมูล ตรวจสอบปริมาณการส่งข้อมูลระหว่างเครือข่าย และการตรวจสอบสัญญาณเพื่อหาข้อผิดพลาด นอกจากนี้ ยังมีข้อมูลช่วยเหลือในการจัดการและการกำหนดค่าต่างๆ ในระบบเครือข่ายด้วย ดังภาพที่ 12.2

ภาพที่ 12.2 แสดงตัวอย่าง Diagnostic Tools สำหรับอุปกรณ์ไร้สาย

12.4.2 เครื่องมือสำหรับการตรวจสอบ (Monitoring Tools)

เครื่องมือสำหรับการตรวจสอบ เป็นเครื่องมือสำหรับการตรวจสอบค่าต่างๆ ในระบบเครือข่าย เพื่อหาทางป้องกันปัญหาที่อาจเกิดขึ้นในระบบเครือข่าย มีดังนี้

1. Performance Monitors เป็นเครื่องมือที่ใช้รวบรวมข้อมูลต่างๆ ที่มีผลต่อประสิทธิภาพของระบบเครือข่าย เช่น ชนิดและจำนวนของบริการที่ใช้ ระยะเวลาการตอบกลับต่อการใช้บริการ จำนวน Buffer ที่ใช้และระยะเวลาของการประมวลผลข้อมูล ซึ่งข้อมูลเหล่านี้สามารถนำมาวิเคราะห์เพื่อหาประสิทธิภาพโดยรวมของระบบเครือข่ายได้ นอกจากนี้ยังสามารถมองเห็นถึงแนวโน้มการใช้งานเครือข่ายในอนาคต ช่วยให้วางแผนเพื่อป้องกันปัญหาที่อาจเกิดขึ้นได้

2. Network Configuration Tools เป็นเครื่องมือเพื่อใช้สำหรับการวางแผนในการกำหนดค่าต่างๆ ของระบบเครือข่ายเพื่อให้ระบบเครือข่ายทำงานได้อย่างมีประสิทธิภาพ

3. Log Files เป็นแหล่งเก็บบันทึกกิจกรรมการใช้งานในเครือข่าย ผู้ดูแลระบบสามารถนำ Log Files มาตรวจสอบเพื่อหาทางป้องกันปัญหาที่อาจเกิดขึ้นในระบบเครือข่ายได้ นอกจากนี้ในกรณีที่เกิดปัญหาในระบบเครือข่ายก็สามารถตรวจสอบได้จาก Log Files เช่นเดียวกันดังภาพที่ 12.3

ภาพที่ 12.3 แสดงตัวอย่าง Bandwidth Monitoring Tools

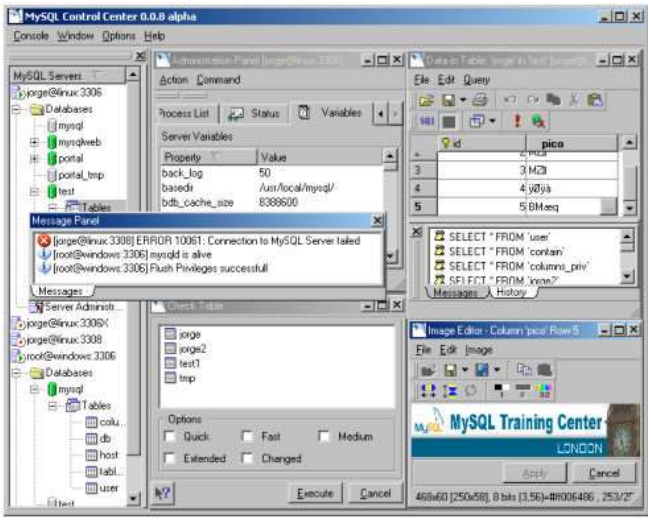
12.4.3 เครื่องมือสำหรับการจัดการ (Management Tools)

เครื่องมือสำหรับการจัดการ เป็นเครื่องมือสำหรับการจัดการระบบเครือข่ายในด้านต่างๆ ดังนี้

1. Project Planning Tools เป็นเครื่องมือที่ช่วยในการกำหนด วางแผน ตรวจสอบ ติดตาม และแก้ไข กิจกรรมต่างๆ ของโครงการ กำหนดทรัพยากรที่ต้องใช้ในโครงการ และวางแผนด้านระยะเวลาของโครงการ ซึ่งสามารถนำมาช่วยในการจัดการระบบเครือข่ายในด้านต่าง ๆ เช่น การแบ่งหน้าที่ของทีมงานในการดูแลระบบเครือข่าย การวางแผนงานด้านต่างๆ เพื่อดูแลระบบเครือข่าย และการวางแผนงาน เพื่อกำหนดระยะเวลาในการติดตั้งอุปกรณ์ซอฟต์แวร์ใหม่ๆ เป็นต้น

2. Database Management Systems and Report Generators เป็นเครื่องมือที่ใช้ในการดึงข้อมูลเกี่ยวกับสถิติ และการทำงานของระบบเครือข่าย ซึ่งถูกจัดเก็บในระบบฐานข้อมูล สามารถนำข้อมูลดังกล่าวมาสร้างเป็นรายงานได้

3. Inventory Software เป็นซอฟต์แวร์ที่ช่วยในการจัดเก็บข้อมูลต่างๆ ของอุปกรณ์เครือข่าย เช่น ชนิดของซีพียู ระบบปฏิบัติการที่ใช้ ลักษณะของฮาร์ดดิสก์ที่ใช้ และข้อมูลเกี่ยวกับการตั้งค่า ทั้งนี้ข้อมูลของการกำหนดค่าอุปกรณ์เหล่านี้จะช่วยให้ผู้ดูแลระบบทราบถึงรายละเอียดที่เกี่ยวข้องกับอุปกรณ์เครือข่ายทั้งหมดและช่วยให้จัดการ และกำหนดค่าต่างๆ ภายในเครือข่ายทำได้ง่ายขึ้น ดังภาพที่ 12.4



ภาพที่ 12.4 แสดงตัวอย่าง Database Management Tools

12.5 การจัดการค่าใช้จ่ายของระบบเครือข่าย

การจัดการค่าใช้จ่าย (Cost Management) จะมีผลกระทบต่อรายรับรายจ่ายขององค์กร ดังนั้น หากสามารถออกแบบและจัดการระบบเครือข่ายได้ดีและมีประสิทธิภาพ จะช่วยลดค่าใช้จ่ายขององค์กรได้เป็นอย่างมาก แนวทางในการจัดการ มีดังนี้

12.5.1 การรวบรวมแหล่งที่มาของค่าใช้จ่ายที่เกี่ยวข้องกับระดับระบบเครือข่ายทั้งหมดพร้อมจัดทำสถิติ

เป็นการรวบรวมข้อมูลเกี่ยวกับแหล่งที่มาของค่าใช้จ่ายที่เกี่ยวข้องกับระบบเครือข่ายทั้งหมด เช่น ค่าใช้จ่ายในการซ่อมแซมระบบเครือข่าย การจ้างบุคลากรในการดูแลระบบ ค่าใช้จ่ายด้านฮาร์ดแวร์และซอฟต์แวร์ และค่าใช้จ่ายในด้านการอบรมการใช้งานระบบเครือข่าย เป็นต้น จากนั้นนำข้อมูลที่ได้มาจัดทำเป็นสถิติของค่าใช้จ่ายแต่ละด้านเป็นประจำทุกปี ซึ่งสถิติที่ได้สามารถนำมาใช้ประโยชน์ในการเปรียบเทียบ วางแผน และหาแนวทางจัดการสำหรับอนาคตได้

12.5.2 การพัฒนามาตรฐานในการกำหนดค่าต่างๆ ของระบบเครือข่าย (Network Configuration)

การพัฒนามาตรฐานในการกำหนดค่าต่างๆ ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ในระบบเครือข่าย (Hardware and Software Configuration) ให้แก่อุปกรณ์คอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ Server และ Client จะช่วยให้ค้นหา ตรวจสอบ และแก้ไขปัญหาต่างๆ เป็นไปในแนวทางเดียวกัน ทำให้สะดวก รวดเร็ว และง่ายขึ้น

12.5.3 การลดระยะเวลาในการติดตั้งฮาร์ดแวร์และซอฟต์แวร์ใหม่

การติดตั้งฮาร์ดแวร์ และซอฟต์แวร์ในแต่ละครั้งจะต้องเสียค่าใช้จ่ายให้กับช่างและผู้เชี่ยวชาญในการติดตั้ง หากการติดตั้งใช้ระยะเวลานานยอมเสียค่าใช้จ่ายเพิ่มขึ้น ดังนั้น ควรวางแผนในการติดตั้งให้ดีเพื่อลดระยะเวลาในการติดตั้งให้น้อยที่สุด

12.5.4 การใช้ระบบอัตโนมัติ

ซอฟต์แวร์บางชนิดสามารถนำมาใช้งานเพื่อสร้างระบบอัตโนมัติขึ้นในระบบเครือข่าย เช่น การนำ Electronic Software Distribution (ESD) มาช่วยอัพเกรดซอฟต์แวร์แบบอัตโนมัติ และการใช้บริการจัดสรรหรือแจกจ่าย IP Address โดยอัตโนมัติ (Dynamic Host Configuration Protocol : DHCP) ซึ่งจะช่วยประหยัดทั้งเวลา และค่าใช้จ่ายในการจัดการกับระบบเครือข่าย

12.5.5 การจัดตั้งศูนย์กลางระบบให้ช่วยให้ความช่วยเหลือด้านเครือข่าย

ในอดีตเมื่อมีผู้ใช้มีปัญหาเกี่ยวกับระบบเครือข่าย สามารถขอความช่วยเหลือจากเจ้าหน้าที่ด้านระบบเครือข่ายที่มีประจำอยู่ในละแผนกขององค์กรได้ ซึ่งต้องเสียค่าใช้จ่ายในการจ้างพนักงาน อีกทั้งเจ้าหน้าที่แต่ละคนก็อาจมีความเชี่ยวชาญที่แตกต่างกัน ทำให้ไม่สามารถแก้ไขปัญหาที่เกิดขึ้นได้ทั้งหมด ดังนั้น เพื่อให้เกิดการลดค่าใช้จ่ายในส่วนนี้ องค์กรควรจัดตั้งศูนย์กลางระบบให้ความช่วยเหลือด้านเครือข่ายขึ้น โดยศูนย์กลางดังกล่าวจะช่วยรวบรวมปัญหาด้านเครือข่าย และผู้เชี่ยวชาญเฉพาะด้านให้ความช่วยเหลือ และแก้ไขปัญหาให้แก่ผู้ใช้ได้

12.5.6 การศึกษาและเรียนรู้เทคโนโลยีใหม่ๆ ในการจัดการระบบเครือข่าย

การศึกษา และเรียนรู้เทคโนโลยีใหม่ๆ เพื่อใช้ในการจัดการระบบเครือข่าย อาจจำเป็นต้องจัดซื้อเทคโนโลยีที่ทันสมัย ทำให้ต้องเสียค่าใช้จ่ายจำนวนมาก แต่ก็จะช่วยให้ระบบทำงานต่างๆ สะดวกสบาย และคล่องตัวขึ้น นอกจากนี้ การเพิ่มความรู้และทักษะให้กับบุคคลขององค์กร เพื่อให้เกิดความชำนาญในเทคโนโลยีใหม่ๆ ก็จำเป็นยิ่ง เนื่องจากเป็นการลงทุนที่คุ้มค่าในระยะยาว เพราะองค์กรไม่ต้องเสียค่าใช้จ่ายในการจ้างผู้เชี่ยวชาญ หรือบุคลากรจากภายนอกมาดูแลระบบของตนเอง

12.6 สรุป

การออกแบบเครือข่าย (Network Design) มีความสำคัญต่อการทำงานขององค์กรและหน่วยงานต่างๆ โดยเฉพาะองค์กรขนาดใหญ่ ซึ่งจำเป็นต้องมีการจัดการและบริหารทรัพยากรให้มีประสิทธิภาพ ระบบเครือข่ายภายในย่อมมีความซับซ้อนมากกว่าองค์กรขนาดเล็ก ปัจจัยที่สำคัญต้องต้องพิจารณาในการออกแบบระบบเครือข่าย ได้แก่ การรวบรวมและวิเคราะห์ความต้องการ รูปแบบที่เหมาะสมสำหรับเครือข่าย เทคโนโลยีและอุปกรณ์ งบประมาณ การให้บริการ

การจัดการเครือข่าย (Network Management) คือ กระบวนการเกี่ยวข้องกับการตรวจสอบ แก้ไข และควบคุมระบบเครือข่าย เพื่อให้มีความน่าเชื่อถือ สามารถตอบสนองความต้องการของผู้ใช้ และทำงานได้อย่างมีประสิทธิภาพ โดย ISO ได้กำหนดมาตรฐานสำหรับจัดการระบบเครือข่ายครอบคลุม 5 ด้าน ได้แก่ ด้านการกำหนดค่าของระบบเครือข่าย (Configuration Management) ด้านความผิดพลาด (Fault Management) ด้านประสิทธิภาพ (Performance Management) ด้านบัญชีผู้ใช้งาน (Accounting Management) และด้านความปลอดภัย (Security Management)

การบริหารและการจัดการกับเครือข่ายของแต่ละอุปกรณ์อาจมีความแตกต่างกันออกไป แต่ไม่ว่าจะเป็นองค์กรขนาดใดก็ตาม จำเป็นต้องมีนโยบายในการดำเนินงานที่ชัดเจน เพื่อเป็นตัวบ่งบอกทิศทางการพัฒนาและการเจริญเติบโตขององค์กรได้เป็นอย่างดี ดังนั้น ในการบริหารและการจัดการกับระบบเครือข่ายในเชิงธุรกิจจึงต้องมีเป้าหมายและวัตถุประสงค์ที่ค่อนข้างชัดเจน โดยมุ่งเน้นในเรื่องความพึงพอใจของลูกค้า งบประมาณ และผลกำไร

การจัดการเครือข่ายจำเป็นต้องมีเครื่องมือหรือระบบเพื่ออำนวยความสะดวกในการตรวจสอบ ดูแลควบคุม และปรับปรุงแก้ไขข้อผิดพลาดที่อาจเกิดขึ้นในระดับหนึ่ง ซึ่งปัจจัยสำคัญอีกอย่างหนึ่งที่ช่วยให้ผู้บริหารเครือข่ายสามารถดูแลระบบขององค์กรได้สะดวกยิ่งขึ้น คือ การนำระบบจัดการเครือข่ายมาใช้ เนื่องจากภายในแต่ละองค์กรอาจมีโครงสร้างของระบบเครือข่ายที่ซับซ้อนมากหรือน้อยแตกต่างกันไปตามสถานที่ สภาพแวดล้อม และนโยบาย หากขาดระบบจัดการเครือข่ายที่ดีอาจทำให้การดูแลแต่ละส่วนของเครือข่ายทำได้ไม่ทั่วถึง ระบบเครือข่ายจะรวมถึงอุปกรณ์ต่างๆ ภายในเครือข่ายด้วย ทำให้ผู้บริหารสามารถจัดการกับอุปกรณ์ผ่านระบบบริหารเครือข่ายได้โดยตรง จึงช่วยประหยัดเวลาในการจัดการทรัพยากรและช่วยให้ตัดสินใจได้รวดเร็วขึ้นด้วย

การจัดการกับระบบเครือข่ายที่สำคัญอีกด้าน คือ การจัดการค่าใช้จ่าย ซึ่งจะมีผลกระทบต่อรายรับรายจ่ายขององค์กร ดังนั้น หากสามารถออกแบบและจัดการระบบเครือข่ายได้ดีและมีประสิทธิภาพ จะช่วยลดค่าใช้จ่ายขององค์กรได้เป็นอย่างมาก

บทที่ 13
การรักษาความปลอดภัยระบบเครือข่าย

อินเทอร์เน็ตเป็นเครือข่ายแบบสาธารณะที่อนุญาตให้บุคคลใดก็ได้สามารถเข้าถึง เพื่อเชื่อมต่อใช้งาน ดังนั้น ทุกๆ คนบนโลกใบนี้ไม่ว่าจะอยู่แห่งใดหากระบบการสื่อสารครอบคลุมไปถึงก็สามารถเข้าถึงแหล่งค้นคว้าหาความรู้ได้ทั่วโลก รวมไปถึงการสื่อสารผ่านอีเมล การแชท การประชุม การซื้อสินค้าออนไลน์ และการทำการค้าผ่านระบบอีคอมเมิร์ซ แต่ในด้านมืดของอินเทอร์เน็ตก็มีอยู่ไม่น้อย เพราะได้กลายเป็นแหล่งซ่องสุมของกลุ่มผู้ใช้บางคนที่มีจุดประสงค์หรือเป้าหมายที่แตกต่างไป เช่น ต้องการขัดขวางหรือจ้องทำลายระบบไม่ให้สามารถใช้งานได้ การก่อการร้าย การลักลอบขโมยข้อมูลสำคัญของคู่แข่งทางธุรกิจ และการล้วงความลับทางราชการ เป็นต้น ซึ่งถือว่าเป็นภัยคุกคามในอีกรูปแบบหนึ่งที่องค์กรทั่วไปต้องหาทางป้องกัน

13.1 การรักษาความปลอดภัยระบบเครือข่าย

ระบบเครือข่ายที่ใช้สำหรับเชื่อมต่อผู้ใช้จำนวนมากให้สามารถติดต่อสื่อสารกันได้ทั้งภายในและภายนอกองค์กร รวมทั้งการเชื่อมต่อกับระบบเครือข่ายสาธารณะซึ่งอาจมีผู้ไม่ประสงค์ดีแอบแฝงเข้ามา เพื่อขโมยหรือทำให้ข้อมูลที่สำคัญเกิดความเสียหายได้ ดังนั้น การวางมาตรการหรือนโยบายในการรักษาความปลอดภัยสำหรับข้อมูลของผู้ใช้จึงเป็นสิ่งจำเป็น โดยระบบความปลอดภัยดังกล่าวจะต้องได้รับการพัฒนาและเปลี่ยนแปลงไปตามยุคสมัย เนื่องจากความก้าวหน้าของเทคโนโลยีทำให้ผู้ไม่ประสงค์ดีมีรูปแบบและวิธีการเข้ามาก่อกวนระบบได้ง่ายและมีหลายวิธี ซึ่งผู้ดูแลระบบหรือผู้ให้บริการจะต้องคำนึงถึงการรักษาความปลอดภัยทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์ ทั้งนี้ บุคคลที่เข้าถึงระบบเครือข่ายส่วนตัวโดยไม่ได้รับอนุญาตเรียกว่า **แฮกเกอร์** (Hacker) (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 342)

13.1.1 การรักษาความปลอดภัยในระบบเครือข่าย

หลักเกณฑ์ในการรักษาความปลอดภัยของระบบเครือข่าย มีลักษณะดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 342-343)

1. การการรักษาความลับ (Privacy) เป็นการรักษาความลับระหว่างผู้ส่งและผู้รับ เพื่อเพิ่มความมั่นใจในการรับส่งข้อมูลว่าข้อมูลที่ส่งไปยังปลายทางมีความถูกต้องเหมือนต้นฉบับ การรักษาความปลอดภัยในการสื่อสารระบบเครือข่ายสามารถป้องกันด้วยการใช้ Key

เพื่อเข้ารหัสและถอดรหัส เช่น วิธี Secret Key ซึ่ง Key ในการเข้ารหัสและถอดรหัสจะใช้เพียงหนึ่งดอกเท่านั้น โดยผู้ส่งและผู้รับจะใช้ Key นี้ร่วมกัน เป็นต้น

2. การระบุตัวตน (Authentication) การที่ผู้รับสามารถระบุตัวตนหรือที่มาของข้อมูลได้ว่าผู้ใดเป็นผู้ส่ง ทำให้ตัดสินใจได้ว่าข้อมูลที่ได้รับมามีความปลอดภัยและน่าเชื่อถือ การระบุตัวตนดังกล่าวไม่เกี่ยวข้องกับการส่งข้อมูลโดยตรงแต่จะเกี่ยวข้องกับการเข้าถึงข้อมูลต่างๆ วิธีการที่นิยมใช้ระบุตัวตน คือ การให้ผู้ใช้กรอกชื่อและรหัสผ่านก่อนเข้าสู่ระบบ

3. ความสมบูรณ์ของข้อมูล (Integrity) ข้อมูลที่ส่งนั้นต้องมีความสมบูรณ์ ไม่ถูกเปลี่ยนแปลงหรือแก้ไขในระหว่างการส่ง ทำให้ผู้รับเกิดความไว้วางใจในระบบเครือข่ายที่ใช้ขนส่งข้อมูล ดังนั้น ระบบรักษาความปลอดภัยควรคำนึงถึงความสมบูรณ์ของข้อมูล เพราะนอกจากจะเป็นเรื่องของการสร้างความมั่นใจต่อผู้ใช้แล้ว ยังแสดงถึงประสิทธิภาพของระบบรักษาความปลอดภัยอีกด้วย

4. พิสูจน์ข้อเท็จจริงได้ (Non-Repudiation) ผู้รับต้องสามารถพิสูจน์ได้ว่าผู้ใดเป็นผู้ส่งที่แท้จริง และผู้ส่งก็สามารถระบุได้เช่นเดียวกันว่าข้อมูลดังกล่าวถึงปลายทางและผู้รับยืนยันเพื่อรับข้อมูลนั้นไว้เรียบร้อยแล้ว ในระบบรักษาความปลอดภัยจำเป็นต้องระบุการรับส่งข้อมูลไว้อย่างชัดเจน เพื่อไม่ให้เกิดความขัดแย้งเมื่อฝ่ายใดฝ่ายหนึ่งปฏิเสธผลลัพธ์ที่เกิดขึ้น

13.1.2 ลักษณะของผู้โจมตี (Hacker)

โดยทั่วไปลักษณะของผู้โจมตี (Hacker) สามารถแบ่งได้ 5 ประเภท ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 344)

1. แฮกเกอร์มืออาชีพ เป็นผู้ที่มีความรู้ ทักษะ ความชำนาญ ความเชี่ยวชาญด้านระบบเครือข่าย และการใช้คอมพิวเตอร์ได้เป็นอย่างดี สามารถเจาะระบบเข้าไปอ่านหรือขโมยข้อมูลที่สำคัญ และโจมตีระบบคอมพิวเตอร์ขององค์กรต่างๆ ได้

2. แฮกเกอร์มือสมัครเล่น เป็นแฮกเกอร์ที่ใช้โปรแกรมสำเร็จรูป เพื่อเจาะหรือโจมตีระบบ แฮกเกอร์มือสมัครเล่นถือได้ว่ามีจำนวนมากที่สุดในบรรดาแฮกเกอร์ทั้งหลาย เนื่องจากไม่จำเป็นต้องมีความรู้ ทักษะ และความเชี่ยวชาญทางด้านระบบเครือข่ายคอมพิวเตอร์ที่ลึกซึ้ง ก็สามารถเจาะหรือโจมตีระบบได้ นอกจากนี้ แฮกเกอร์เหล่านี้ยังสามารถพัฒนาตนเองให้กลายเป็นแฮกเกอร์มืออาชีพในอนาคตได้อีกด้วย

3. อาชญากรทางคอมพิวเตอร์ ซึ่งอาจทำคนเดียวหรือทำเป็นขบวนการก็ได้ การก่ออาชญากรรมมีหลายลักษณะ เช่น การขโมยหมายเลขบัตรเครดิตเพื่อนำไปใช้ในการซื้อสินค้าทางอินเทอร์เน็ต การขโมยข้อมูลที่เป็นความลับทางด้านการค้าเพื่อนำไปขายให้แก่คู่แข่ง

และการขโมยข้อมูลสำคัญที่เป็นความลับขององค์กรต่างๆ จากนั้นนำข้อมูลที่ขโมยได้มาต่อรองหรือข่มขู่องค์กรเหล่านั้น เพื่อแลกกับผลประโยชน์บางอย่างที่ต้องการ เป็นต้น

4. ผู้ก่อการร้ายทางคอมพิวเตอร์ การก่อการร้ายในปัจจุบันอาจไม่จำเป็นต้องใช้อาวุธทางทหาร เพื่อทำให้ฝ่ายตรงข้ามเกิดความเสียหายอีกต่อไป แต่สามารถใช้ประโยชน์จากเครือข่ายคอมพิวเตอร์เป็นอาวุธหรือเครื่องมือในการก่ออาชญากรรมในการก่อการร้าย เช่น การเจาะระบบเครือข่ายเพื่อเปลี่ยนแปลง แก้ไขข้อมูลต่างๆ ที่สำคัญของรัฐบาล การขโมยข้อมูลที่เป็นความลับทางการทหาร และการขโมยข้อมูลที่เกี่ยวข้องกับความมั่นคงของประเทศ เป็นต้น

5. พนักงานหรือลูกจ้างในองค์กร การโจมตีจากผู้มีสิทธิ์เข้าระบบได้อย่างถูกต้องนั้นจะก่อให้เกิดความเสียหายที่ร้ายแรงกว่าผู้ที่เจาะหรือผู้โจมตีระบบจากภายนอกองค์กร ซึ่งอาจเกิดจากพนักงานที่ไม่ซื่อสัตย์ หรือพนักงานที่เกิดความไม่พอใจองค์กรที่มีความรู้ความสามารถในเรื่องระบบเครือข่าย

13.1.3 รูปแบบของการโจมตีระบบเครือข่าย

การโจมตีระบบเครือข่ายนั้นมีหลากหลายรูปแบบ แต่ที่พบได้ทั่วไปมีดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 345-348)

1. การโจมตี Server เนื่องจาก Server เปรียบเสมือนคลังเก็บข้อมูลที่สำคัญจำนวนมาก และเป็นแหล่งที่ให้บริการแก่ผู้ใช้ที่หลากหลาย ดังนั้น ข้อมูลและบริการต่างๆ บน Server อาจตกเป็นเป้าหมายของแฮกเกอร์ทั้งหลายได้

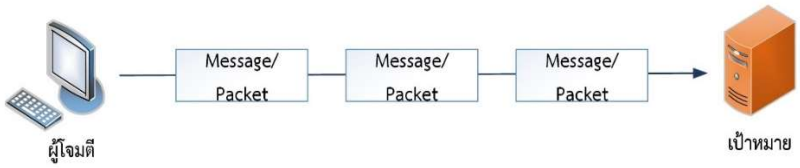
2. การโจมตี Client ข้อมูลที่เก็บไว้ในเครื่องคอมพิวเตอร์ของ Client ที่แฮกเกอร์ต้องการมีมากมาย เช่น Password หมายเลขบัตรเครดิต และข้อมูลสำคัญที่เป็นความลับต่างๆ เป็นต้น โดยแฮกเกอร์จะนำข้อมูลที่ขโมยได้ไปใช้ประโยชน์ต่างๆ เช่น นำ Password ที่ขโมยได้เข้าไปใช้บริการจาก Server เพื่อเปลี่ยนแปลงหรือแก้ไขข้อมูลบางอย่าง การนำหมายเลขบัตรเครดิตทำธุรกรรมออนไลน์และการนำข้อมูลสำคัญที่ขโมยได้ไปขาย เป็นต้น

3. การดักจับแพ็กเก็ต เป็นวิธีการโจมตีและบุกรุกเข้าเครือข่ายที่ใช้การดักจับข้อมูลที่ถูกแบ่งเป็นส่วนย่อยๆ เช่น แพ็กเก็ตข้อมูล เรียกวิธีการนี้ว่า Packet Sniffer โดยผู้บุกรุกจะคอยเฝ้าดักจับแพ็กเก็ตข้อมูลที่ขนส่งผ่านมาและเปิดดูข้อมูลที่อยู่ภายใน แพ็กเก็ตข้อมูลบางประเภทไม่มีการเข้ารหัสไว้ และเป็นข้อมูลแบบ Clear Text ทำให้สามารถอ่านข้อมูลเข้าใจง่าย โดยข้อมูลดังกล่าวอาจเป็นข้อมูลที่ผู้บุกรุกต้องการหรือนำไปใช้ในการโจมตีรูปแบบอื่นได้อีก เช่น ชื่อและรหัสของผู้ใช้ เป็นต้น

4. การโจมตีแบบ Man-in-the-Middle เป็นการโจมตีที่คอยดักจับเอาแพ็กเก็ตข้อมูลที่ส่งระหว่างต้นทางกับปลายทางก่อนดำเนินการโจมตี โดยลักษณะการโจมตีแบบนี้ผู้โจมตีจะแอบแฝงอยู่ในเส้นทางที่ข้อมูลเดินทางผ่าน และผู้โจมตีจะดำเนินการคัดลอกหรือดัดแปลงข้อมูลเหล่านั้น โดยไม่มีผู้ใดทราบว่ามีบุคคลที่สามคั่นระหว่างการขนส่งข้อมูล เนื่องจากการส่งข้อมูลยังดำเนินไปตามปกติ โดยข้อมูลดังกล่าวจะถูกนำไปใช้สำหรับการโจมตีครั้งต่อไป

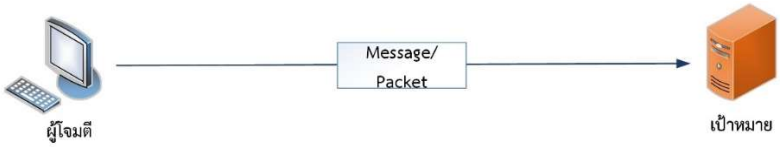
5. การโจมตีแบบ Denial-of-Service Attacks : DoS จุดประสงค์หลักของการโจมตีรูปแบบนี้ คือ การพยายามทำให้เป้าหมาย หรือระบบเครือข่ายที่ถูกโจมตีล่ม และไม่สามารถให้บริการแก่ Client อื่นๆ ได้ ลักษณะการโจมตีแบบ DoS มี 3 รูปแบบ ดังนี้

5.1 การโจมตีโดยการส่ง Message หรือ Packet จำนวนมากไปยังเป้าหมาย เพื่อให้ Server หรือ Router ต้องจัดการกับ Message จำนวนมากจนไม่สามารถให้บริการแก่ Client อื่นได้ แสดงดังภาพที่ 13.1



ภาพที่ 13.1 แสดงการส่ง Message หรือ Packet จำนวนมากเพื่อโจมตีเป้าหมาย
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 346)

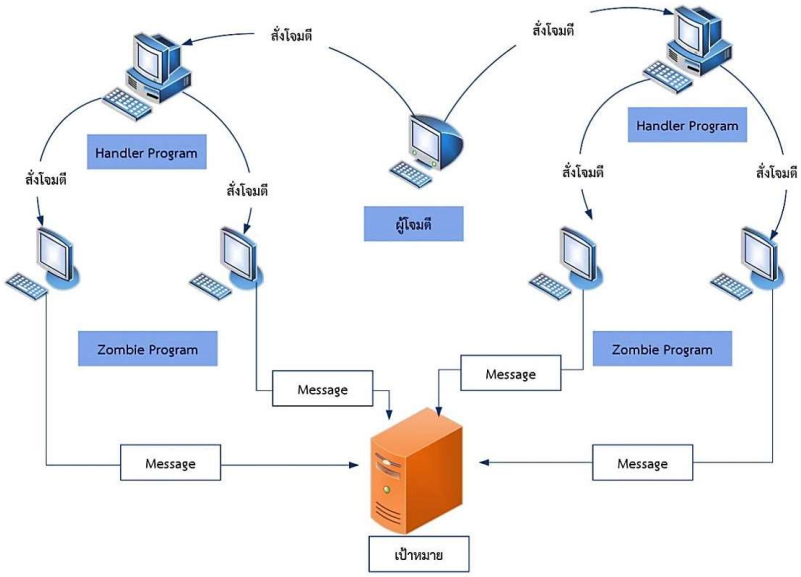
5.2 การโจมตีโดยการส่ง Message หรือ Packet เดียว โดยใช้ Message ดังกล่าวทำลายระบบการทำงานของ Server หรือ Router ซึ่ง Message หรือ Package นี้จะมีประสิทธิภาพเพียงพอที่จะทำให้ระบบล่มได้ แสดงดังภาพที่ 13.2



ภาพที่ 13.2 แสดงการส่ง Message หรือ Packet เดียวเพื่อโจมตีเป้าหมาย
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 346)

5.3 การโจมตีแบบ Distributed Denial-of-Service (DDoS) เป็นการโจมตีที่รุนแรงกว่า 2 วิธีที่กล่าวมาในข้างต้น เนื่องจากใช้คอมพิวเตอร์มากกว่าหนึ่งเครื่องโจมตี

พร้อมกัน ซึ่งการส่ง Message หรือ Package จากหลายเครื่องพร้อมกันนั้นทำให้ระบบเครือข่ายล่มอย่างรวดเร็ว ลักษณะของการโจมตีจะเป็นไปดังภาพที่ 13.3



ภาพที่ 13.3 แสดงการโจมตีแบบ Distributed Denial-of-Service (DDoS)

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 346)

จากภาพที่ 13.3 แสดงลักษณะของการโจมตี สามารถอธิบายได้ดังนี้

1. ผู้โจมตีจะส่งหรือแพร่กระจาย Handler Program และ Zombie Program ให้กระจายไปยังเครื่องคอมพิวเตอร์ต่างๆ ให้มากที่สุดเพื่อรอการโจมตี

2. เมื่อต้องการโจมตีก็จะสั่งให้ Handler Program ที่ฝังตัวในเครื่องคอมพิวเตอร์ต่างๆ ทำงานพร้อมกัน

3. Handler Program ทำงานโดยสั่งคำสั่งไปที่ Zombie Program เพื่อให้เริ่มทำงาน

4. Zombie Program เริ่มทำงานตามคำสั่ง โดยการส่ง Message หรือ Package ไปยังเครื่องเป้าหมาย

การโจมตีแบบนี้จะแกะรอยเพื่อหาผู้โจมตีได้ยาก เนื่องจากการโจมตีเกิดจากคอมพิวเตอร์หลายเครื่องและผู้โจมตีจะทำลาย Zombie Program หลังจากที่ทำการโจมตีเรียบร้อยแล้ว

6. การโจมตีจาก Virus, Worm, Trojan Horse และ Spam

6.1 Virus เป็นโปรแกรมชนิดหนึ่งที่สามารถทำลายระบบคอมพิวเตอร์ได้ ลักษณะของการทำลายมีหลายรูปแบบ เช่น การลบไฟล์ในฮาร์ดดิสก์ การเปลี่ยนแปลงและแก้ไขไฟล์ต่างๆ เป็นต้น Virus สามารถแพร่กระจายไปยังโปรแกรมต่างๆ ภายในเครื่องคอมพิวเตอร์และทำสำเนาตัวเองเพิ่มขึ้น รวมทั้งแพร่กระจายไปยังเครื่องอื่นๆ โดยอาศัยตัวกลาง เช่น โปรแกรมและไฟล์ข้อมูล เป็นต้น หากคอมพิวเตอร์เครื่องใดเปิดไฟล์ข้อมูลที่ติด Virus ก็จะทำให้เครื่องติด Virus ชนิดดังกล่าวด้วย

6.2 Worm เป็นโปรแกรมชนิดหนึ่งที่สามารถแพร่กระจายภายในระบบเครือข่ายโดยการทำสำเนาตัวเอง ซึ่งจะแตกต่างกับ Virus คือ Worm จะแพร่กระจายโดยอาศัยเพียงระบบเครือข่ายคอมพิวเตอร์เท่านั้น และไม่จำเป็นต้องเกาะติดไปกับโปรแกรมหรือไฟล์ข้อมูลใดๆ ในขณะที่ Virus จะต้องอาศัยตัวกลางสำหรับการแพร่กระจาย

6.3 Trojan Horse เป็นโปรแกรมที่ซ่อนหรือแฝงตัวอยู่กับโปรแกรมอื่นๆ โดยเฉพาะโปรแกรมที่ดาวน์โหลดมาจากอินเทอร์เน็ตซึ่งมีจุดประสงค์ที่แตกต่างกัน เช่น การทำลายระบบคอมพิวเตอร์ และการขโมยข้อมูลต่างๆ เป็นต้น

6.4 Spam เป็นรูปแบบของการส่งอีเมลลักษณะหนึ่งที่มีจุดประสงค์ เพื่อการโฆษณาหรือประชาสัมพันธ์สินค้าผ่านทางเครือข่ายอินเทอร์เน็ต โดยใช้อีเมลเป็นสื่อกลาง แต่ก็มีการแอบแฝง Virus หรือ Worm ติดมากับอีเมลเหล่านั้นด้วย ดังนั้น ผู้คนส่วนใหญ่จึงไม่กล้าเปิดอ่านอีเมลเหล่านี้ หากไม่ทราบที่มาของผู้ส่งอย่างชัดเจน นอกจากนี้ Spam ยังสร้างความรำคาญแก่ผู้ใช้อีกด้วย

7. Scanning Attacks

เป็นเทคนิคใช้สำหรับการค้นหา IP Address และบริการต่างๆ ของเป้าหมายที่ต้องการโจมตี โดยการส่ง Scanning Message เพื่อสอบถามข้อมูลที่ต้องการจากเป้าหมาย

13.1.4 รูปแบบการรักษาความปลอดภัย

การโจมตีระบบเครือข่ายนั้นมีหลากหลายรูปแบบ ทั้งการแอบแฝงเข้ามาในเครือข่าย หรือการโจมตีการทำงานของเครือข่ายโดยตรง การโจมตีแต่ละรูปแบบมีวัตถุประสงค์ที่แตกต่างกัน เช่น ลอบเข้ามาในระบบเครือข่ายเพื่อล้วงความลับ โจมตีเพื่อก่อกวนให้เครือข่ายทำงานได้ไม่เต็มที่ หรือสร้างความเสียหายแก่อุปกรณ์ต่างๆ เพื่อให้เครือข่ายไม่สามารถใช้งานได้ ดังนั้น การป้องกันการโจมตีจากผู้บุกรุกจึงจำเป็นต้องปรับเปลี่ยนไปตามรูปแบบดังกล่าว การ

รักษาความปลอดภัยในระบบแบ่งออกเป็น 2 ระดับ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 348-351)

1. การรักษาความปลอดภัยในระดับกายภาพ (Physical Security)

ในอดีตวิธีการที่ใช้โจมตีระบบเครือข่ายยังไม่ก้าวหน้า จึงนิยมป้องกันผู้บุกรุกด้วยวิธีพื้นฐาน คือ การป้องกันห้องควบคุมหรือห้องที่จัดเก็บเครื่องคอมพิวเตอร์ต่างๆ โดยกำหนดให้เข้าออกได้เฉพาะคนที่ได้รับสิทธิ์ และปิดห้องไว้อย่างแน่นหนา ซึ่งวิธีดังกล่าวก็ยังคงใช้อยู่ในปัจจุบันเพียงแต่มีการใช้อุปกรณ์ที่ทันสมัยมากขึ้น เช่น การใช้เครื่องสแกนลายนิ้วมือ การใช้บัตรประจำตัวและรหัสในการเข้าออกสถานที่ และการใช้กล้องรักษาความปลอดภัยบันทึกภาพของผู้เข้าออกสถานที่ไว้ เป็นต้น การป้องกันในลักษณะนี้อาจช่วยได้เพียงระบุตัวตนของผู้บุกรุกเท่านั้น แต่ไม่สามารถป้องกันความเสียหายที่เกิดขึ้นได้

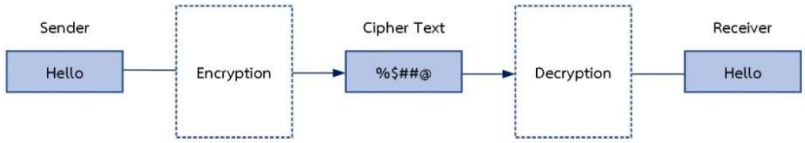
นอกจากนี้การรักษาความปลอดภัยในระดับกายภาพยังรวมถึงการติดตั้งอุปกรณ์ป้องกันผู้บุกรุกโดยตรง ได้แก่ การติดตั้งอุปกรณ์ Firewall การป้องกันในลักษณะนี้จะช่วยให้สร้างความมั่นใจให้กับการรับส่งข้อมูลได้อีกทางหนึ่ง อย่างไรก็ตามการรักษาความปลอดภัยของระบบเครือข่ายระดับกายภาพก็จำเป็นต้องใช้งานควบคู่กับวิธีการอื่นๆ เพื่อให้รักษาความปลอดภัยมีประสิทธิภาพมากขึ้น

2. การรักษาความปลอดภัยในระดับแอปพลิเคชัน (Software Security)

การรักษาความปลอดภัยในระดับของซอฟต์แวร์หรือแอปพลิเคชัน เพื่อป้องกันการบุกรุกที่โจมตีระบบเครือข่ายโดยอาศัยช่องโหว่ของแอปพลิเคชันในระบบเครือข่าย เนื่องจากเป็นรูปแบบที่ผู้บุกรุกสามารถโจมตีระบบได้จากระยะไกล และไม่จำเป็นต้องเข้าถึงอุปกรณ์หรือสถานที่ ซึ่งการรักษาความปลอดภัยในระดับแอปพลิเคชันสามารถทำได้หลายลักษณะ ดังนี้

2.1 การระบุตัวตนด้วยชื่อผู้เข้าใช้และรหัสผ่าน (ID and Password) ซึ่งเป็นวิธีรักษาความปลอดภัยขั้นพื้นฐานและนิยมใช้กันอย่างแพร่หลาย เนื่องจากเป็นวิธีที่ง่ายและสะดวกในการใช้งาน ทุกคนต้องเข้าสู่ระบบผ่านการระบุตัวตนด้วยชื่อผู้เข้าใช้และรหัสที่กำหนดขึ้นเอง หรือระบบเป็นผู้กำหนดให้ โดยที่รหัสจะต้องถูกเก็บในความลับ ระบบเป็นผู้เก็บข้อมูลและรหัสของผู้ใช้ไว้ เพื่อใช้ตรวจสอบเมื่อผู้ใช้เข้าสู่ระบบ ผู้บุกรุกบางกลุ่มอาจติดตั้งโปรแกรมที่สามารถตรวจจับรหัสสำหรับเข้าสู่ระบบได้ จึงต้องนำเทคโนโลยีอื่นๆ มาประยุกต์ใช้ด้วย เช่น การเข้ารหัสข้อมูล เป็นต้น วิธีการระบุตัวตนดังกล่าวจึงนำมาใช้สำหรับรักษาความปลอดภัยในระดับเบื้องต้นเท่านั้น

2.2 การเข้ารหัสข้อมูล (Encryption) เป็นการรักษาความปลอดภัยให้กับข้อมูล โดยนำข้อมูลที่ต้องการส่งมาเข้ารหัสหรือที่เรียกว่า Encryption เพื่อไม่ให้ข้อความถูกอ่านได้โดยง่าย กระบวนการเข้ารหัสนั้นจะมีวิธีการใช้ Key สำหรับเข้ารหัสหลายวิธี โดยผู้รับจำเป็นจะต้องมี Key ที่ใช้ในการถอดรหัสกลับเป็นเหมือนข้อความต้นฉบับ โดยจะเรียกข้อมูลดังกล่าวนี้ว่า Cipher Text ดังภาพที่ 13.4



ภาพที่ 13.4 แสดงกระบวนการรักษาความปลอดภัยข้อมูลด้วยการเข้ารหัส
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 350)

2.3 การใช้ลายเซ็นดิจิทัล (Digital Signature) ในระบบการเข้ารหัสบางประเทศอาจจำเป็นต้องอาศัยลายเซ็นดิจิทัล เพื่อระบุตัวตนของผู้รับและผู้ส่ง ลายเซ็นดิจิทัลจึงเป็นตัวช่วยระบุตัวตนของผู้รับและผู้ส่งได้ในระดับหนึ่ง คล้ายกับบัตรประจำตัวประชาชนแต่จะปลอดภัยกว่า เนื่องจากไม่มีใครทราบข้อมูลของผู้ใช้ลายเซ็นดังกล่าวนอกจากผู้รับและผู้ส่งเท่านั้น

2.4 Secure Sockets Layer (SSL) เป็นวิธีการรักษาความปลอดภัยให้กับข้อมูลที่นิยมใช้ในการทำธุรกิจผ่านระบบเครือข่าย เช่น หมายเลขบัตรเครดิต การใช้ SSL จะเริ่มจากการติดตั้ง SSL ซอฟต์แวร์ไว้ในเครื่องทั้งฝั่งผู้ใช้ และฝั่ง Server ก็จะตอบกลับเพื่อยืนยันตัวตนโดยการเข้ารหัสเมื่อตรวจสอบและระบุตัวตนเรียบร้อยแล้ว Server ก็จะตอบกลับเพื่อยืนยันว่าการรับส่งข้อมูลดังกล่าวเสร็จสิ้น ซึ่งกระบวนการทำงานของ SSL จะเป็นขั้นตอนหนึ่งในการดูแลข้อมูลสำคัญ และช่วยให้ลูกค้ามั่นใจในการทำธุรกิจกับองค์กรหรือหน่วยงานว่าเงินที่ใช้ในการซื้อสินค้านั้นส่งไปยังผู้จำหน่ายสินค้าที่ถูกต้อง

SSL เป็นโพรโทคอลชนิดหนึ่งที่ถูกพัฒนาขึ้นเพื่อทำหน้าที่ในการเข้ารหัสข้อมูลและการระบุตัวตนระหว่างเครื่อง Server กับ Client โดยทำงานอยู่ในชั้น Transport Layer ทำให้สามารถนำ SSL ไปประยุกต์ใช้งานอื่นๆ นอกเหนือจากการใช้ผ่านเว็บแอปพลิเคชัน

13.2 ระบบรักษาความปลอดภัย

ระบบรักษาความปลอดภัย แบ่งได้ 2 ระบบ ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 351-358)

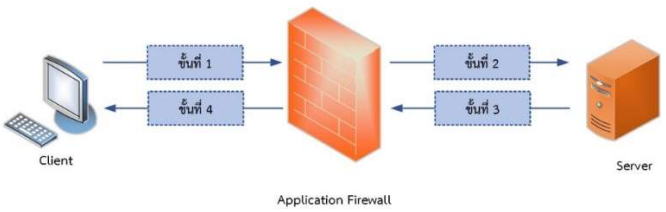
13.2.1 ระบบป้องกันการโจมตี (Attack prevention Systems)

ระบบป้องกันการโจมตีที่นิยมใช้มี 4 ระบบ ได้แก่

1. Firewall จะถูกนำมาติดตั้งเพื่อกั้นระหว่างระบบเครือข่ายภายในองค์กรและอินเทอร์เน็ต มีหน้าที่ตรวจสอบและกลั่นกรอง Message ต่างๆ ที่เข้าออกจากระบบเครือข่ายภายในองค์กร เพื่อป้องกันอันตรายและการโจมตีในรูปแบบต่างๆ Firewall แบ่งออกเป็น 2 ประเภท ดังนี้

1.1 Packet Filter Firewall ใช้ตรวจสอบและกลั่นกรอง IP Packet โดยพิจารณาจาก Header ของ IP Packet ซึ่งประกอบด้วยหมายเลข IP ต้นทางและปลายทาง หมายเลขพอร์ตต้นทางและปลายทาง และประเภทของโพรโทคอล ควบคุมการเข้าออกของ Message ต่างๆ เรียกว่า Access Control Lists (ACL) ซึ่งประกอบด้วยรายการของกฎเกณฑ์ต่างๆ โดยกำหนดลักษณะของ Packet ที่สามารถผ่านเข้าออกระบบเครือข่ายได้ หาก Packet มีลักษณะที่ไม่เป็นไปตามกฎเกณฑ์แสดงว่า Packet ดังกล่าวอาจเป็นอันตรายต่อระบบเครือข่าย Firewall จะไม่อนุญาตให้ Packet นั้นเข้ามาภายในระบบเครือข่าย

1.2 Application (Proxy) Firewall เป็น Firewall ที่ทำหน้าที่ตรวจสอบและกลั่นกรอง Message ในระดับ Application Layer สำหรับ Application Message ที่เข้ามาจะมีรูปแบบที่หลากหลาย เช่น อีเมล, SMTP, FTP, HTTP และ Telnet เป็นต้น ทำให้ลักษณะของ Application Message แต่ละชนิดมีความแตกต่างกัน ดังนั้น วิธีการตรวจสอบและกลั่นกรอง Application Message จะต้องแยกตรวจสอบโดยใช้ Application Proxy Program ของแต่ละ Application เช่น FTP Proxy, SMTP Proxy และ HTTP Proxy ดังภาพที่ 13.5



ภาพที่ 13.5 แสดงขั้นตอนการทำงานของ Application Firewall

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 352)

จากภาพที่ 13.5 ลักษณะการทำงานของ Application Firewall เป็นดังนี้

ขั้นที่ 1 Client จะส่ง Request Message เพื่อเข้ามาขอใช้บริการต่างๆ จาก Server โดยผ่านการตรวจสอบจาก Application Firewall

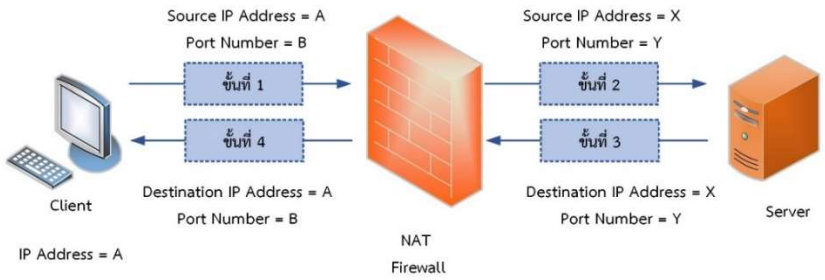
ขั้นที่ 2 Request Message ที่ผ่านการตรวจสอบแล้วจะส่งต่อเข้าไปเพื่อขอบริการที่ Server

ขั้นที่ 3 หลังจากทราบจำนวนคนแล้ว Server จะส่งคำตอบหรือ Response Message กลับไปยัง Client โดยต้องผ่านการตรวจสอบจาก Application Firewall

ขั้นที่ 4 Response Message ที่ผ่านการตรวจสอบจะถูกส่งกลับไปให้ Client

2. Network Access Translation (NAT)

แฮกเกอร์ที่ต้องการเจาะหรือโจมตีระบบเครือข่ายจำเป็นต้องรู้ IP Address และบริการต่างๆ ของเป้าหมาย วิธีการที่นิยมใช้เพื่อป้องกัน IP Address จากเหล่าแฮกเกอร์ ได้แก่ Network address Translator (NAT) ซึ่งใช้ซ่อน IP Address ที่แท้จริงของเครื่องคอมพิวเตอร์ สำหรับ Firewall ส่วนใหญ่นิยมใช้เทคนิคนี้ช่วยป้องกันระบบเครือข่ายภายในองค์กร ซึ่งเรียกว่า NAT Firewall โดยมีหลักการทำงาน ดังภาพที่ 13.6



ภาพที่ 13.6 แสดงหลักการทำงานของ Application Firewall

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 353)

จากภาพที่ 13.6 สามารถอธิบายหลักการทำงานได้ดังนี้

ขั้นที่ 1 เมื่อ Client ที่อยู่ภายในองค์กรส่ง Packet ออกมา NAT Firewall จะเปลี่ยนหมายเลข IP ต้นทาง จาก A เป็น X และหมายเลขพอร์ต จาก B เป็น Y

ขั้นที่ 2 บันทึกการเปลี่ยนแปลงที่เกิดขึ้นไว้ในตาราง Translation Table พร้อมส่ง Packet ที่เปลี่ยนแปลงแล้วไปยังเป้าหมายที่ต้องการ

ขั้นที่ 3 เมื่อ Server ตอบกลับมา NAT Firewall จะทำการตรวจสอบหมายเลข IP และ หมายเลขพอร์ตของ Packet ที่เข้ามากับตาราง Translation Table หากมีค่าตรงกัน ก็จะแปลงหมายเลข IP และหมายเลขพอร์ตให้ Packet นั้น ในที่นี้จะเปลี่ยนหมายเลข IP จาก X เป็น A และหมายเลขพอร์ตจาก Y เป็น B

ขั้นที่ 4 หลังจากที่ NAT Firewall เปลี่ยนหมายเลข IP และหมายเลขพอร์ตแล้ว Packet จะถูกส่งกลับไปยัง Client เดิมได้อย่างถูกต้อง

3. Intrusion Detection System

ปัจจุบันการใช้ Firewall เพื่อป้องกันระบบเครือข่ายภายในองค์กรเพียงอย่างเดียว อาจไม่เพียงพอสำหรับป้องกันการโจมตีจากแฮกเกอร์ แนวทางหนึ่งที่นำมาใช้ คือ Interaction Detection System คือ การวิเคราะห์ Massage ที่เข้ามาในระบบเพื่อหาแหล่งที่มา ความถี่ในการส่ง ลักษณะ และรูปแบบของ Massage หากพบว่า Message ใดมีลักษณะที่ไม่น่าไว้ใจจะบันทึกข้อมูลไว้ และเมื่อ Message ลักษณะดังกล่าวถูกส่งเข้ามาในระบบอีกครั้งจะได้แจ้งเตือนไปยังผู้ดูแลระบบ เพื่อให้ผู้ดูแลทราบว่ามีผู้บุกรุกหรือโจมตีระบบเครือข่าย ซึ่งจะช่วยให้ผู้ดูแลระบบสามารถจัดการปัญหาได้ทันท่วงที

4. ระบบป้องกันเครื่อง Server และเครื่องคอมพิวเตอร์ภายในองค์กร

แม้ว่าองค์กรจะมีทั้ง Firewall และ Intersection Detection System ที่ดี แต่อาจไม่สามารถป้องกันระบบเครือข่ายจากการบุกรุกของแฮกเกอร์บางคนได้ เพื่อเพิ่มความปลอดภัยให้กับระบบมากยิ่งขึ้นๆ ควรเพิ่มวิธีการป้องกันคอมพิวเตอร์ภายในองค์กร ดังนี้

4.1 การ Update Software เนื่องจากระบบปฏิบัติการที่นำมาติดตั้งในเครื่องคอมพิวเตอร์นั้นอาจมีจุดอ่อนหรือช่องโหว่ เพื่อหาแนวทางในการป้องกันและรักษาความปลอดภัยด้วยการอัพเดตซอฟแวร์ให้มีความทันสมัยอยู่เสมอ

4.2 การติดตั้ง Firewall ให้กับคอมพิวเตอร์ทุกเครื่องภายในองค์กร หากแฮกเกอร์สามารถเจาะระบบเครือข่ายภายในองค์กรเข้ามาได้ Firewall ที่ถูกติดตั้งให้กับคอมพิวเตอร์แต่ละเครื่องในองค์กรจะเป็นกำแพงอีกชั้นหนึ่งที่สามารถป้องปกป้องคอมพิวเตอร์ให้ปลอดภัยจากแฮกเกอร์ได้

4.3 การพิสูจน์ตัวตนในการเข้าใช้ Server (Server Authentication) เป็นเทคนิคที่ใช้ในการพิสูจน์ตัวตนของบุคคลที่มีสิทธิ์ในการเข้าใช้บริการจาก Server รูปแบบหนึ่งโดยแบ่งได้ 3 ประเภท ดังนี้

4.3.1 การพิสูจน์ตัวตนด้วยรหัสผ่าน (Password Authentication) เป็นการพิสูจน์ตัวตนในการเข้าใช้บริการจาก Server แนวทางในการกำหนดรหัสผ่านที่ดีมีลักษณะดังนี้

1) มีความยาวอย่างน้อย 8 อักษร

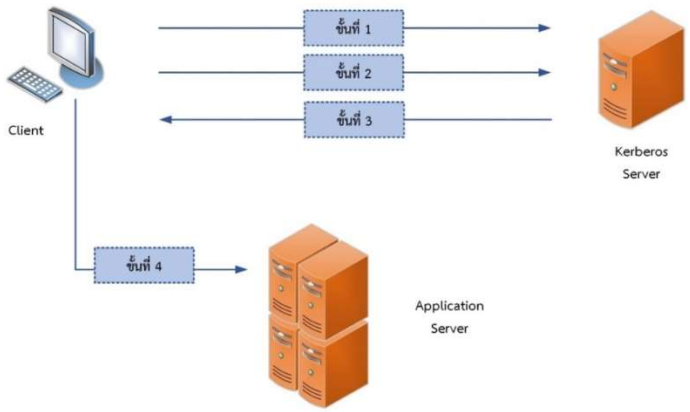
2) มีตัวเลขอยู่ด้วยอย่างน้อยหนึ่งตัว

3) มีตัวอักษรพิเศษหรือสัญลักษณ์ต่างๆ เช่น $, # และ _ อย่างน้อยหนึ่งตัวอักษรรวมอยู่ด้วยแต่ไม่ควรกำหนดไว้ท้ายรหัสผ่าน

4) กำหนดให้มีตัวอักษรพิมพ์เล็กและพิมพ์ใหญ่ปะปนกันไป

5) กำหนดให้มีตัวอักษรภาษาอื่นๆ อยู่ร่วมกัน

4.3.2 การพิสูจน์ตัวตนด้วย Kerberos คือ โพรโทคอลที่ใช้พิสูจน์ตัวตนบนระบบเครือข่าย ซึ่งเป็นเทคนิคหรือวิธีการที่คิดค้นขึ้นมาเพื่อแก้ปัญหาความไม่ปลอดภัยของการพิสูจน์ตัวตนแบบเดิมที่มีการส่งรหัสผ่านบนเครือข่ายโดยที่ไม่มีการเข้ารหัสข้อมูล ซึ่งทำให้รหัสผ่านอาจถูกดักจับได้สำหรับเทคนิคนี้จะใช้ข้อมูลที่ได้รับการเข้ารหัสก่อนส่งในทุกขั้นตอน และข้อมูลเหล่านี้สามารถเปิดอ่านได้โดยใช้รหัสผ่านร่วมกันเท่านั้น ดังภาพที่ 13.7



ภาพที่ 13.7 แสดงหลักการทำงานของ Kerberos Authentication

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 355)

จากภาพที่ 13.7 มีขั้นตอนการทำงาน ดังนี้

ขั้นที่ 1 ผู้ใช้จะทำการพิสูจน์ตัวตนเพื่อให้ Kerberos Server เชื่อว่าผู้ใช้มีสิทธิ์ในการเข้ามาใช้งานจริง Kerberos Server จะเก็บฐานข้อมูลบัญชีรายชื่อผู้ใช้ และรหัสผ่านผู้ใช้แต่ละรายไว้

ขั้นที่ 2 ผู้ใช้ทำการร้องขอบัตรผ่านของ Application Server ที่ต้องการเข้ามาใช้บริการ

ขั้นที่ 3 Kerberos Server จะส่งบัตรผ่านของ Application Server ที่ผู้ใช้ต้องการกลับมา

ขั้นที่ 4 ผู้ใช้สามารถเข้าไปใช้บริการจาก Application Server โดยใช้บัตรผ่านที่ได้มา

4.3.3 การพิสูจน์ชีวลักษณะ (Biometric Authentication) เป็นการพิสูจน์ตัวตนจากอวัยวะต่างๆ ของร่างกายรวมถึงการเคลื่อนไหวของผู้ใช้ ดังนี้

1) การพิสูจน์ตัวตนจากลายนิ้วมือ เนื่องจากลายนิ้วมือของแต่ละบุคคลมีความแตกต่างกัน วิธีนี้เป็นที่นิยมมากที่สุดเนื่องจากต้นทุนไม่สูง

2) การพิสูจน์ตัวตนจากม่านตา เป็นวิธีการระบุตัวตนผู้ใช้โดยการตรวจจากแบบแผนของม่านตา (Iris Pattern) ม่านตาจะสามารถระบุหรือบ่งบอกตัวตนของแต่ละคนได้ดีกว่าการตรวจจากลายนิ้วมือ โดยทั่วไปการพิสูจน์ลักษณะนี้จะใช้กับองค์กรขนาดใหญ่ที่ต้องการความปลอดภัยสูงเพื่อป้องกันข้อมูลที่เป็นความลับรั่วไหล

3) การพิสูจน์ตัวตนโดยการจดจำใบหน้า เนื่องจากรูปหน้าของบางคนอาจมีลักษณะใกล้เคียงกัน ดังนั้นการพิสูจน์แบบนี้จะนำไปใช้ตรวจสอบขั้นต้นเท่านั้น เช่น สายการบินบางแห่งอาจนำมาใช้ตรวจสอบเบื้องต้นเพื่อป้องกันผู้ก่อการร้าย

4) การพิสูจน์โดยวิธีการอื่นๆ เช่น เสียง ลายมือชื่อ และการจดจำลักษณะของเส้นเลือด (Vein Recognition) เป็นต้น

4.4 การจำกัดสิทธิ์การใช้ Server (Limiting Permissions on Servers) พนักงานในองค์กรแต่ละคนย่อมมีสิทธิ์ในการเข้าใช้บริการจาก Server แตกต่างกันขึ้นอยู่กับลักษณะของงานที่ปฏิบัติ เช่น พนักงานทั่วไปจะรับสิทธิ์ในการอ่านข้อมูลจากฐานข้อมูลส่วนกลางขององค์กรเท่านั้น แต่สำหรับพนักงานที่ทำหน้าที่เป็นผู้ดูแลฐานข้อมูลจะสามารถ อ่าน เขียน ลบ และแก้ไขข้อมูลต่างๆ ในฐานข้อมูลได้ เป็นต้น

13.2.2 ระบบรักษาความปลอดภัยของการสื่อสาร (Secure Communication Systems)

ระบบรักษาความปลอดภัยของการสื่อสาร (Secure Communication Systems) เป็นระบบที่ช่วยป้องกันอันตรายจากแฮกเกอร์ที่พยายามอ่านข้อมูลที่ใช้ในการติดต่อสื่อสาร การทำงานระบบนี้มี 4 ขั้นตอน ได้แก่

ขั้นตอนที่ 1 การเจรจาตกลง (Negotiation of Security Parameters) เป็นขั้นตอนการเจรจาเพื่อเลือกวิธีรักษาความปลอดภัยของทั้งสองฝ่าย

ขั้นตอนที่ 2 การพิสูจน์ตัวตนของแต่ละฝ่าย (Mutual Authentication) เพื่อยืนยันหรือทำให้แน่ใจว่าเป็นบุคคลที่ได้กล่าวอ้างจริง

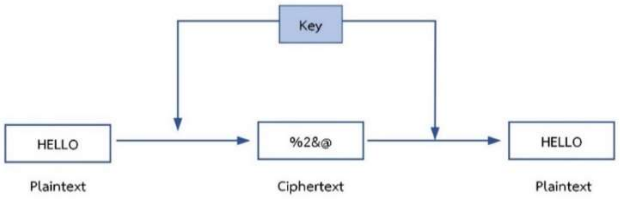
ขั้นตอนที่ 3 การแลกเปลี่ยน Key เพื่อใช้สำหรับการเข้ารหัสและถอดรหัส Message เนื่องจากการส่ง Message ถึงกันนั้นจำเป็นต้องคำนึงถึงความปลอดภัยของ Message ดังนั้น จึงต้องเข้ารหัส Message ที่ส่งหากัน สำหรับ Key ในที่นี้หมายถึงสายอักขระของบิต (Bit String) เช่น 1000010001 และ 1010111011 ที่ใช้สำหรับการเข้าและถอดรหัสข้อความ

ขั้นตอนที่ 4 ส่ง Message เพื่อติดต่อสื่อสารกัน โดยแต่ละไฟล์จะสามารถเปิดอ่านMessage ของอีกฝ่ายได้โดยการถอดรหัส Message ด้วย Key ที่ได้แลกเปลี่ยนการจากขั้นตอนที่ 3

13.3 การเข้ารหัสข้อมูล

การรักษาความลับของข้อมูลเป็นประเด็นหนึ่งที่สำคัญของการรักษาความปลอดภัยในการติดต่อสื่อสาร เพื่อป้องกันการดักจับจากแฮกเกอร์ วิธีที่นิยมนำมาใช้ คือ การเข้ารหัสข้อมูล (Encryption) มี 2 วิธี ดังนี้ (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 358-361)

13.3.1 การเข้ารหัส Symmetric Key Encryption การเข้ารหัสรูปแบบนี้ จะใช้ Key เพียงตัวเดียวในการเข้าและถอดรหัสข้อมูล ดังภาพที่ 13.8

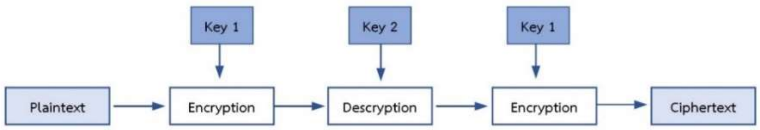


ภาพที่ 13.8 แสดงหลักการทำงานของ Symmetric Key Encryption
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 358)

การเข้ารหัส Symmetric Key Encryption มีหลายอัลกอริธึมที่ใช้ในการเข้ารหัสข้อมูลในรูปแบบนี้ ได้แก่

1. Data Encryption Standard (DES) ความยาวของ Key คือ 56 บิต เป็นความยาวที่ค่อนข้างน้อย แฮกเกอร์จึงสามารถเดา Key ได้ง่าย

2. Triple Data Encryption Standard (3DES) พัฒนามาจากการเข้ารหัสแบบ DES โดยวิธีการนี้คิดขึ้นมาเพื่อแก้ปัญหาของ DES ที่มีความยาวของ Key สั้นเกินไป แสดงวิธีการเข้าและถอดรหัส ดังภาพที่ 13.9 และภาพที่ 13.10



ภาพที่ 13.9 แสดงการเข้ารหัสแบบ Triple Data Encryption Standard (3DES)

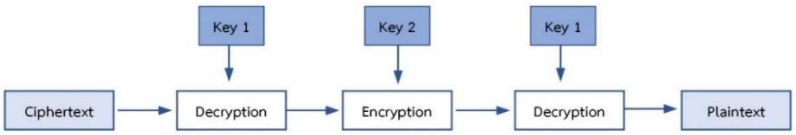
จากภาพที่ 13.9 การเข้ารหัสและแบ่งเป็นจะแบ่งเป็น 3 ขั้นตอน ดังนี้

ขั้นที่ 1 ทำการเข้ารหัส (Encrypt) Plaintext ใช้ Key 1

ขั้นที่ 2 ทำการถอดรหัส (Decrypt) Message จากขั้นที่ 1 โดยใช้ Key 2

ขั้นที่ 3 ทำการเข้ารหัส (Encrypt) Message จากขั้นที่ 2 โดยใช้ Key 1

ผลลัพธ์ที่ได้ คือ Ciphertext



ภาพที่ 13.10 แสดงการถอดรหัสแบบ Triple Data Encryption Standard (3DES)

ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 359)

จากภาพที่ 13.10 การถอดรหัสจะแบ่งเป็น 3 ขั้นดังนี้

ขั้นที่ 1 การถอดรหัส (Decrypt) Ciphertext ใช้ Key 1

ขั้นที่ 2 ทำการเข้ารหัส (Encrypt) Message จากขั้นที่ 1 ใช้ Key 2

ขั้นที่ 3 ทำการถอดรหัส (Decrypt) Message จากขั้นที่ 2 โดย Key 1

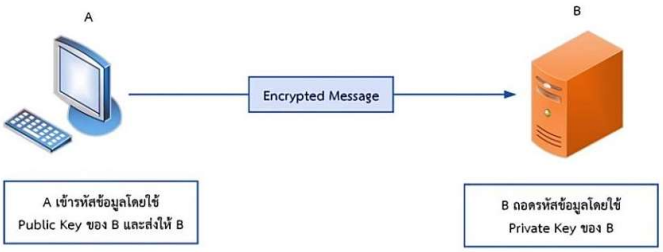
ผลลัพธ์ที่ได้ คือ Plaintext

3. Advanced Encryption Standard (AES) เป็นมาตรฐานที่กำหนดให้ความยาวของ Key มีขนาด 128, 192 และ 256 บิต โดยความยาวของข้อมูลที่จะนำมาเข้ารหัสมีขนาด 128 บิต สำหรับอัลกอริธึมที่นิยมใช้ ได้แก่ Rijndael Algorithm ซึ่งเป็นมาตรฐานที่มี

ประสิทธิภาพและมีความปลอดภัยสูง และสามารถนำไปใช้กับอุปกรณ์คอมพิวเตอร์ขนาดเล็ก เช่น มือถือ ปาล์ม และ Pocket PC เป็นต้น

13.3.2 การเข้ารหัส Public Key Encryption

ข้อเสียอย่างหนึ่งของ Symmetric Key Encryption คือ การส่ง Key ไปให้กับผู้รับเพื่อใช้ในการถอดรหัส ซึ่งจำเป็นต้องหาวิธีการส่งที่ปลอดภัย จึงได้มีการคิดค้นวิธีการใหม่เพื่อการลดความเสี่ยงและระยะเวลาในการส่ง Key เรียกว่า Public Key Encryption โดยมี Key ที่เกี่ยวข้องจำนวน 2 Key ได้แก่ Public Key เป็น Key สาธารณะที่ต้องประกาศให้ทุกคนได้ทราบ และ Private Key เป็น Key ที่ต้องเก็บเป็นความลับ และทราบได้เฉพาะผู้ที่เป็นเจ้าของเท่านั้น เพื่อนำไปถอดรหัสข้อความที่มีการเข้ารหัสโดยใช้ Public Key แสดงลักษณะการทำงาน ดังภาพที่ 13.11



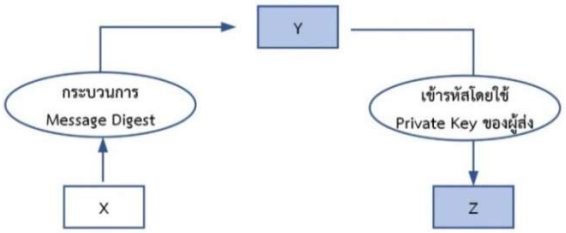
ภาพที่ 13.11 แสดงการส่งข้อมูลโดยใช้ Public Key Encryption
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 361)

จากภาพที่ 13.11 สามารถอธิบายได้ว่า ผู้ส่ง A ส่งข้อมูลไปยัง B โดยเข้ารหัสข้อมูลด้วย Public Key ของ B (Public Key ของผู้รับ) ผู้รับ B สามารถถอดรหัสข้อมูลโดยใช้ Private Key ของ B

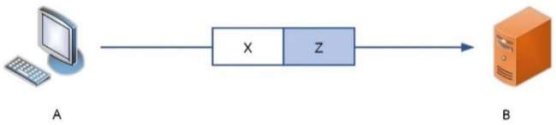
13.4 ลายเซ็นอิเล็กทรอนิกส์

ลายเซ็นอิเล็กทรอนิกส์ (Digital Signatures) คือ การลงนามเพื่อรับรองเอกสารในโลกของคอมพิวเตอร์ก็สามารถนำหลักการดังกล่าวมาใช้ได้เช่นเดียวกัน ซึ่งเป็นเทคนิคที่ใช้ Private Key และ Public Key มาช่วยในการเข้าและถอดรหัสข้อมูลนั้นจะใช้ระยะเวลานาน เนื่องจากข้อความบางอย่างมีความยาวค่อนข้างมาก จึงต้องใช้เทคนิคที่เรียกว่า Message Digests เพื่อช่วยให้ข้อความเหล่านั้นสั้นลงและมีความยาวคงที่ โดยการใช้ Hash Function

ตัวอย่างของ Message เช่น MD5 และ SHS-1 เป็นต้น พิจารณาการใช้ Message Digest ดังภาพที่ 13.12 และภาพที่ 13.13 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 361-363)



ภาพที่ 13.12 แสดงเทคนิคลายเซ็นอิเล็กทรอนิกส์โดยใช้กระบวนการ Message Digest
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 361)



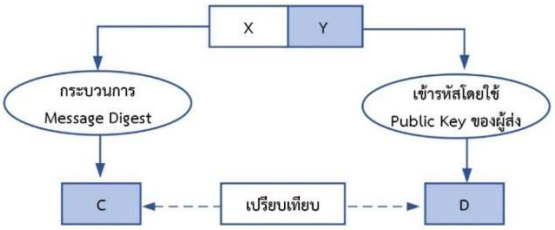
ภาพที่ 13.13 แสดงการส่งข้อมูลของ Digital Signature Message
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 362)

จากภาพที่ 13.12 และภาพที่ 13.13 สามารถอธิบายได้ ดังนี้

1. นำข้อความต้นฉบับที่ต้องการส่ง ได้แก่ Message X มาผ่านกระบวนการ Message Digest จะกลายเป็น Message Y

2. นำข้อความที่ผ่านการ Digest ได้แก่ Message Y มาเข้ารหัสโดยใช้ Private Key ของผู้ส่งข้อความจะกลายเป็น Message Z

3. ผู้ส่งจะต้องส่งทั้ง Message X ซึ่งเป็นข้อความต้นฉบับ และ Message Z ซึ่งเป็นข้อความที่ผ่านการเข้ารหัสไปด้วยกัน ดังภาพที่ 13.14



ภาพที่ 13.14 แสดงกระบวนการที่เกิดขึ้นในฝั่งผู้รับ
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 362)

จากภาพที่ 13.14 แสดงให้เห็นถึงกระบวนการทำงานฝั่งผู้รับ ดังนี้

1. นำข้อความต้นฉบับ ได้แก่ Message X มาผ่านกระบวนการ Message Digest โดยสมมติผลลัพธ์ที่ได้คือ Message C

2. นำ Message Z มาถอดรหัส โดยใช้ Public Key ของผู้ส่ง (ในที่นี้คือ A) โดยสมมติผลลัพธ์ที่ได้ คือ Message D

3. ทำการเปรียบเทียบ Message C และ D หากเป็นค่าเดียวกันแสดงว่า Message ถูกส่งมาจาก A จริง

ประเด็นสำคัญในเรื่องการรักษาความปลอดภัยในการติดต่อสื่อสารที่เกี่ยวข้องกับลายเซ็นอิเล็กทรอนิกส์ ได้แก่

1. การพิสูจน์ตัวตน (Authentication) การใช้เทคนิคลายเซ็นอิเล็กทรอนิกส์นั้นสามารถบ่งบอกหรือระบุถึงที่มาของ Message ได้เนื่องจากการใช้ Private Key ของผู้ส่งเพื่อเข้ารหัสข้อมูล ซึ่งจะมีเพียง Public Key ของผู้ส่งเท่านั้นจึงจะนำมาถอดรหัส Message ดังกล่าวได้ ดังนั้น จึงไม่มีผู้ใดสามารถเปลี่ยนแปลงได้เนื่องจาก Private Key จะถูกเก็บเป็นความลับนั่นเอง

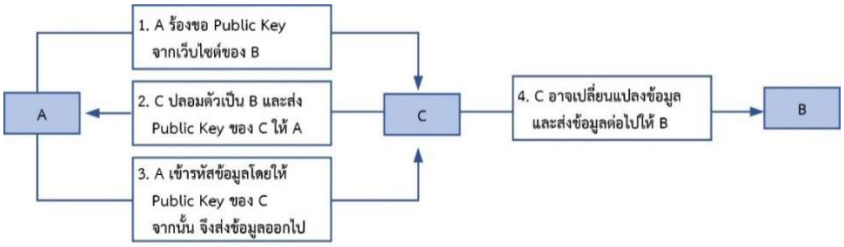
2. การทำให้ผู้ส่งปฏิเสธความรับผิดชอบต่อข้อมูลที่ส่งไม่ได้ (Nonrepudiation) เนื่องจากข้อมูลจากการส่งแบบลายเซ็นอิเล็กทรอนิกส์นั้นมี 2 ส่วน คือ ข้อความต้นฉบับ และข้อความที่ได้รับการเข้ารหัส ถ้าต้องการพิสูจน์ว่าข้อความนั้นถูกส่งมาจากบุคคลใด ทำได้ด้วยการนำข้อความต้นฉบับมาเข้ารหัส โดยใช้ Private Key ของผู้ส่ง จากนั้นนำมาเปรียบเทียบกับข้อความที่ได้รับการเข้ารหัส ถ้าตรงกันจะทำให้ผู้ส่งไม่สามารถปฏิเสธความรับผิดชอบได้

3. ความถูกต้องของข้อมูล (Integrity) การใช้เทคนิคลายเซ็นอิเล็กทรอนิกส์ช่วยรักษาข้อมูลให้มีความถูกต้องเสมอ ซึ่งข้อมูลที่ถูกปลอมแปลงผู้รับไม่สามารถถอดรหัสข้อมูลได้ ดังนั้น ผู้รับจะไม่สามารถนำข้อมูลที่ผิดเพี้ยนไปใช้อย่างได้ และไม่ส่งผลกระทบต่อการทำงานทั้งหมด

นอกจากนี้ยังมีวิธีการที่เรียกว่า Public Key ซึ่งใช้หลักการ Public Key Encryption โดยนำข้อความที่ผ่านการเข้ารหัสด้วยลายเซ็นอิเล็กทรอนิกส์แล้วมาเข้ารหัสด้วย Public Key ของผู้รับ วิธีนี้จะช่วยเพิ่มความสามารถของการรักษาความปลอดภัยในเรื่องการรักษาความลับได้อีกด้วย

13.5 ใบรับรองอิเล็กทรอนิกส์

ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) คือ ข้อมูลอิเล็กทรอนิกส์ ซึ่งออกโดยผู้ให้บริการออกใบรับรอง (Certification Authority : CA) เพื่อใช้บ่งบอกถึงตัวตนในโลกอิเล็กทรอนิกส์ โดยทำการตรวจสอบข้อมูลของเจ้าของใบรับรอง และจะทำการรับรองกุญแจสาธารณะ (Public Key) ใบรับรองบันทึกข้อมูลอิเล็กทรอนิกส์ประกอบด้วย ข้อมูลของผู้เป็นเจ้าของใบรับรอง เช่น ชื่อ-สกุล ตำแหน่ง กุญแจสาธารณะ ของผู้เป็นเจ้าของใบรับรอง และลายมือชื่อดิจิทัลของผู้ให้บริการออกใบรับรอง ซึ่งข้อมูลในใบรับรองจะทำการยืนยันความเชื่อมโยงระหว่างเจ้าของลายมือชื่อกับข้อมูล สำหรับใช้สร้างลายมือชื่อดิจิทัล โดยใบรับรองเป็นส่วนประกอบสำคัญสำหรับการตรวจสอบลายมือชื่อดิจิทัล ปัญหาของการใช้ Public Key Encryption มีลักษณะดังภาพที่ 13.15 (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 363)



ภาพที่ 13.15 แสดงปัญหาที่เกิดขึ้นจากการใช้ Public Key
ที่มา : (สุธี พงศาสกุลชัย และณรงค์ ล่ำดี, 2557, หน้า 363)

จากภาพที่ 13.15 จะเห็นได้ว่า A ต้องการส่งข้อมูลให้กับ B โดยใช้วิธี Public Key Encryption แต่เกิดปัญหา คือ C สามารถปลอมตัวเป็น B ได้ และส่ง Public Key ของ C ไปให้ A นำไปเข้ารหัส โดยที่ A ไม่ทราบว่า Public Key นั้น เป็นของ C จึงทำให้ C สามารถเปิดอ่านข้อความดังกล่าวได้โดยใช้ Private Key ของ C จากที่กล่าวมา ผู้ส่งจะไม่สามารถแน่ใจได้ว่า Public Key เป็นของบุคคลที่ต้องการส่งให้อย่างแท้จริง เนื่องจากสามารถปรับแต่งได้ ดังนั้น การแก้ปัญหาดังกล่าวจึงทำได้โดยการใช้ใบรับรองอิเล็กทรอนิกส์ (Digital Certificate) ซึ่งมีส่วนประกอบ 3 ส่วน ดังนี้

ส่วนที่ 1 Public Key ของบุคคลที่ต้องการขอใบรับรองอิเล็กทรอนิกส์

ส่วนที่ 2 ส่วนระบุตัวตนของผู้ที่เป็นเจ้าของ Public Key เช่น ชื่อ สกุล ที่อยู่ และ E-mail Address เป็นต้น

ส่วนที่ 3 ส่วนที่นำข้อมูลของส่วนที่ 1 และส่วนที่ 2 มาผ่านกระบวนการ Message Digest โดยวิธี SHA-1 และนำข้อมูลที่ได้มาเข้ารหัส โดยใช้ Private Key ที่ออกโดยองค์กร Certificate Authority (CA)

การตรวจสอบใบรับรองอิเล็กทรอนิกส์ สามารถทำได้ดังนี้

ขั้นตอนที่ 1 นำส่วนที่ 3 ของใบรับรองอิเล็กทรอนิกส์มาถอดรหัสโดยใช้ Public Key ของ Certificate Authority

ขั้นตอนที่ 2 นำส่วนที่ 1 และส่วนที่ 2 มาเปรียบเทียบ ผ่านกระบวนการ SHA-1

ขั้นตอนที่ 3 นำข้อมูลที่ได้จากขั้นที่ 1 และ 2 มาเปรียบเทียบ หากตรงกันแสดงว่าเป็นใบรับรองอิเล็กทรอนิกส์ของบุคคลนั้นจริง

13.6 สรุป

การเชื่อมต่อกับระบบเครือข่ายสาธารณะซึ่งอาจมีผู้ไม่ประสงค์ดีแอบแฝงเข้ามาเพื่อขโมยหรือทำให้ข้อมูลที่สำคัญเกิดความเสียหายได้ เรียกว่า แฮกเกอร์ (Hacker)

การโจมตีระบบเครือข่ายนั้นมีหลากหลายรูปแบบ ทั้งการแอบแฝงเข้ามาในเครือข่ายหรือการโจมตีการทำงานของเครือข่ายโดยตรง เช่น การโจมตี Server หรือ Client การดักจับแพ็กเก็ต การโจมตีแบบ Man-in-the-Middle การโจมตีแบบ Denial-of-Service Attacks : DoS การโจมตีจาก Virus, Worm, Trojan Horse และ Spam เป็นต้น

การรักษาความลับของข้อมูลวิธีที่นิยมนำมาใช้ คือ การเข้ารหัสข้อมูล (Encryption) ลายเซ็นอิเล็กทรอนิกส์ (Digital Signatures) และใบรับรองอิเล็กทรอนิกส์ (Digital Certificate)

บรรณานุกรม

กิตติ ภักดีวัฒนะกุล และสุธี พงศาสกุลชัย. (2554). เครือข่ายคอมพิวเตอร์. กรุงเทพฯ : เคทีพี คอมพ์ แอนด์ คอนซัลท์.

ชัชชัย คุณบัว. (2562). **IoT สถาปัตยกรรมการสื่อสาร Internet of Things**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

ธวัชชัย ชมศิริ. (2553). **Computer & network security : ความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

นรรัตน์ วัฒนมงคล. (2561). **การสื่อสารข้อมูลและเครือข่าย.** กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

ไนน์ ดิสทริบิวชั่น. (2013). **802.11b/g/n 1T2R Wireless LAN PCI card**. [ออนไลน์]. เข้าถึงได้จาก : http : www.ninedistribution.com/product/Allied/AIRNet/Standalone-Series/ATWNP300N.html. [สืบค้นเมื่อวันที่ 1 มีนาคม 2565].

ประกาย นาดี. (ม.ป.ป). **การสื่อสารข้อมูล.** [ออนไลน์]. เข้าถึงได้จาก : http://www.rmuti.ac.th/user/prakai/datacommunication_and_network/slide_01.ppt. [สืบค้นเมื่อวันที่ 28 สิงหาคม 2565].

ประสิทธิ์ ทีฆพุฒิ. (2559). **เครือข่ายระบบโทรคมนาคม.** กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

พงศธร เศรษฐีธร. (2558). **การสื่อสารดิจิทัล.** กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

พิสิฐ พรพงศ์เตชวาณิช และพงษ์พิสิฐ วุฒิดิษฐโชติ. (2566). **เครือข่ายคอมพิวเตอร์และการสื่อสาร.** กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

ภัทรสินี ภัทรโกศล. (2555). **เครือข่ายคอมพิวเตอร์.** กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

มหาวิทยาลัยเทคโนโลยีพระนคร. (ม.ป.ป). **IEEE 802.11.** [ออนไลน์]. เข้าถึงได้จาก : http://www.noc.mut.ac.th/km/km-2562-1/. [สืบค้นเมื่อวันที่ 28 สิงหาคม 2565].

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2560). **เอกสารการสอนชุดวิชา การสื่อสารข้อมูลและระบบเครือข่ายคอมพิวเตอร์ หน่วยที่ 1-5 ฉบับปรับปรุงครั้งที่ 1**. กรุงเทพฯ : มหาวิทยาลัยสุโขทัยธรรมาธิราช.

_____. (2560). **เอกสารการสอนชุดวิชา การสื่อสารข้อมูลและระบบเครือข่ายคอมพิวเตอร์ หน่วยที่ 6-10 ฉบับปรับปรุงครั้งที่ 1**. กรุงเทพฯ : มหาวิทยาลัยสุโขทัยธรรมาธิราช.

มหาวิทยาลัยสุโขทัยธรรมาธิราช. (2560). **เอกสารการสอนชุดวิชา การสื่อสารข้อมูลและระบบเครือข่ายคอมพิวเตอร์ หน่วยที่ 11-15 ฉบับปรับปรุงครั้งที่ 1**. กรุงเทพฯ : มหาวิทยาลัยสุโขทัยธรรมาธิราช.

มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง. (2558). **โลกใหม่ใครกำกับ? กรณีศึกษาเกี่ยวกับอินเทอร์เน็ต 2559.** (พิมพ์ครั้งที่ 1). กรุงเทพฯ : มูลนิธิเพื่ออินเทอร์เน็ตและวัฒนธรรมพลเมือง.

วาทิต เบญจพลกุล. (2555). **การสื่อสารข้อมูลและโครงข่าย.** กรุงเทพฯ : จุฬาลงกรณ์มหาวิทยาลัย.

สุธี พงศาสกุลชัย และณรงค์ ล่ำดี. (2557). **การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์.** พิมพ์ครั้งที่ 3. กรุงเทพฯ : เคทีพี.

อาณัติ รัตนถิรกุล. (2558). **ก้าวสู่อาชีพผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ในองค์กร**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

โอภาส เอี่ยมสิริวงศ์. (2559). **เครือข่ายคอมพิวเตอร์และการสื่อสาร (ฉบับปรับปรุงเพิ่มเติม)**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

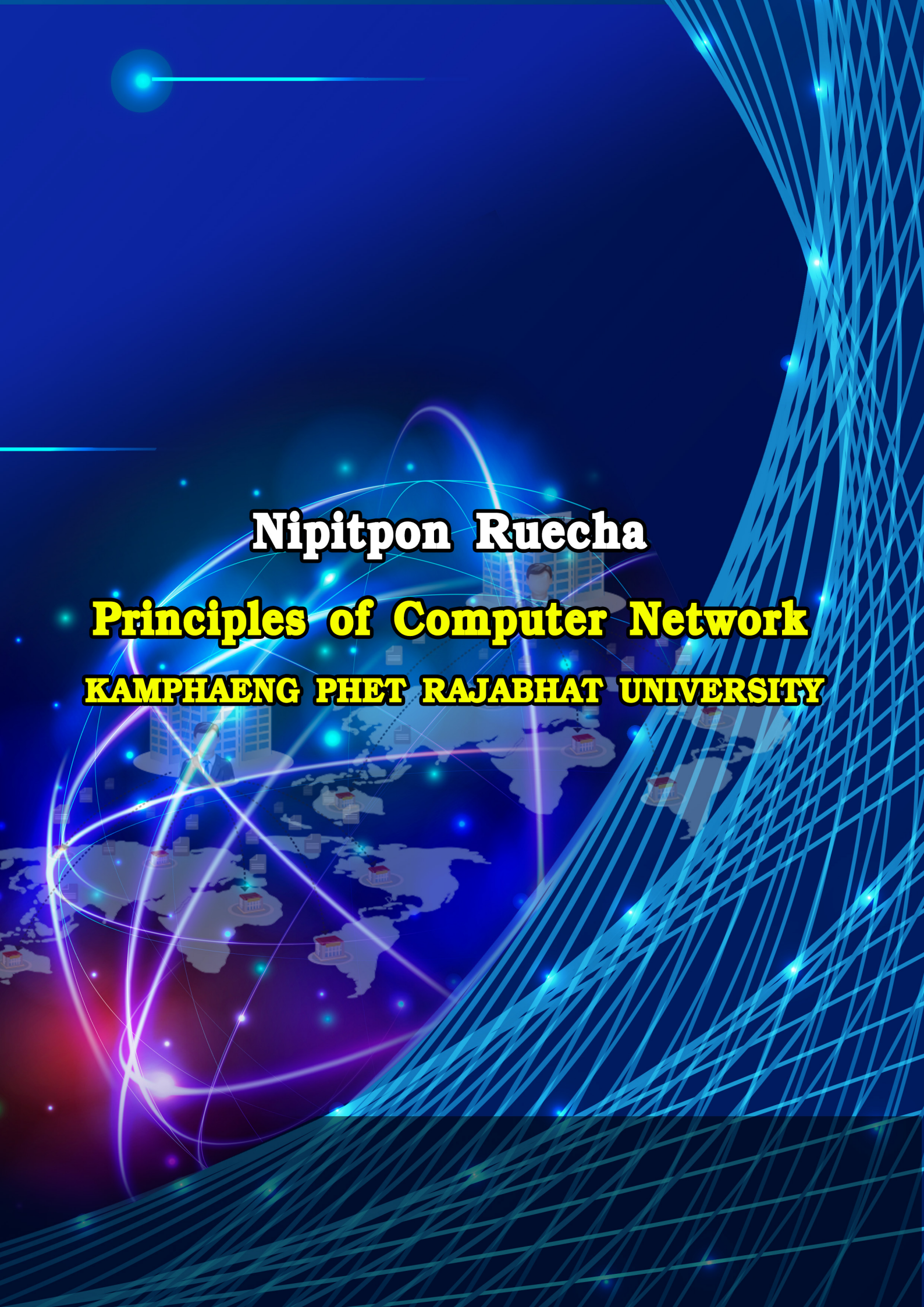
_____. (2558). **พื้นฐานเครือข่ายคอมพิวเตอร์**. กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

Behrouz A. Forozan. (2013). **Data Communications and Networking.** (5th ed). New York: McGraw-Hill.

Douglas E. Comer. (2015). **Computer Networks and Internet.** (6th ed). Boston : Pearson.

J. Cowley. (2014). **Communication and Networking an Introduction**. (2th ed). ISBN-10: 1-84628-488-0,Spinger-Verlag London.

ดัชนี



Nipitpon Ruecha

Principles of Computer Network

KAMPHAENG PHET RAJABHAT UNIVERSITY