บทที่ 3
โครงสร้างสถาปัตยกรรมของระบบเครือข่าย
(Network Architecture)

การทำงานของระบบเครือข่ายต้องอาศัยองค์ประกอบมากมาย ซึ่งองค์ประกอบทั้งหมดจะต้องเข้ากันได้พอดี เหมือนเป็นชิ้นส่วนหนึ่งของตัวต่อภาพปริศนา ไม่เพียงแต่ชิ้นส่วนเหล่านี้จะต้องทำงานด้วยกันได้อย่างราบเรียบ แต่ยังต้องสามารถอาศัยส่วนอื่นสำหรับการให้บริการที่แตกต่างกัน ตัวอย่างเช่นโปรแกรมประยุกต์จะต้องเชื่อถือในสายเคเบิลพื้นฐานของระบบเครือข่าย การสื่อสาร ฮาร์ดแวร์ (**Hardware**) และซอฟต์แวร์ (**software**) ระบบเครือข่ายว่าจะสามารถรับและส่งข้อมูลระหว่างเครื่องลูกข่ายด้วยกันเอง หรือระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่าย หรือระหว่างเครื่องแม่ข่ายกับเครื่องลูกข่าย หรือระหว่างเครื่องแม่ข่ายด้วยกันเองได้อย่างเที่ยงตรง และในทำนองเดียวกันโครงสร้างพื้นฐานด้านฮาร์ดแวร์ของระบบเครือข่ายจะต้องเชื่อในซอฟต์แวร์ การสื่อสารของระบบเครือข่าย และการให้บริการที่แตกข้อมูลลงเป็นแพ็กเก็ตข้อมูลขนาดเล็กที่ได้รับการกำหนดแอดเดรส (**addressing**) และมีขนาดที่เหมาะสำหรับการส่งไปบนระบบเครือข่าย เพื่อรับรองว่าส่วนต่างๆ และชิ้นส่วนเหล่านี้สามารถทำงานร่วมกันได้ ผู้ผลิตฮาร์ดแวร์และซอฟต์แวร์ระบบเครือข่ายจะต้องทำตามชุดของคำแนะนำในการออกแบบและสร้างผลิตภัณฑ์ แนวทางคำแนะนำที่รู้จักกันดีและถูกนำมาใช้อย่างกว้างขวาง คือชุดของคุณลักษณะเฉพาะที่ได้รับการพัฒนาในปี ค.ศ. **1978** โดยองค์กรมาตรฐานสากล (**International Organization for Standardization – ISO**) คุณลักษณะเฉพาะเหล่านี้ได้ถูกนำมาทบทวนและนำออกมาใช้ในปี ค.ศ. **1984** ซึ่งเรียกว่า **Open Systems Interconnection Reference Model** หรือเรียกอย่างง่ายๆ ว่า **OSI Reference Model** หรือเรียกสั้นๆ ว่า **OSI model**

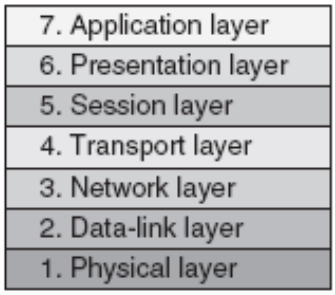
3.1 สถาปัตยกรรมโครงสร้าง OSI Reference Model

เมื่อมองอย่างผิวเผินในครั้งแรก การต่อเติมบางสิ่งเข้าไปในคุณสมบัติพื้นฐานของระบบเครือข่ายด้วยชื่อที่มีความสำคัญว่า **Open System Interconnection Reference Model** อาจจะดูเหมือนว่ามีบางสิ่งบางอย่างที่เยิ่นเย้อและเป็นเทคนิคมากจนเกินไป ซึ่งที่จริงแล้วไม่ใช่อย่างที่คิด **ISO** ออกแบบชุดของคุณลักษณะเฉพาะที่เป็นโครงร่างสำหรับการเข้าชุดที่อธิบายสถาปัตยกรรมของระบบเครือข่าย ผู้ผลิตส่วนประกอบฮาร์ดแวร์และซอฟต์แวร์ใดๆ สามารถที่จะใช้โครงร่างนี้ในการสร้างผลิตภัณฑ์ที่ทำ 2 อย่างนี้

- สื่อสารกับอุปกรณ์อื่น
- มีสถาปัตยกรรมแบบเป็นลำดับชั้น (**layered architecture**) อย่างเป็นระเบียบ ซึ่งส่วนประกอบในเลเยอร์ระดับหนึ่งต้องอาศัยการให้บริการที่จัดให้มีโดยเลเยอร์ระดับอื่น โดยที่ไม่ต้องคำนึงถึงวิธีการจัดตั้งการให้บริการเหล่านั้น

หรือกล่าวอีกอย่างหนึ่งได้ว่า **OSI Reference Model** อธิบายรูปแบบ โครงสร้าง สำหรับการสร้างอุปกรณ์ที่สามารถทำงานร่วมกันได้ในการเชื่อมต่อการสื่อสารของระบบเครือข่ายอย่างเป็นสากลในระบบเปิด (**Open System**) ซึ่งเป็นโครงสร้างอ้างอิงเพราะถึงแม้ว่าจะอธิบายว่าส่วนต่างๆ ของระบบเครือข่ายมีการทำงานอย่างไร

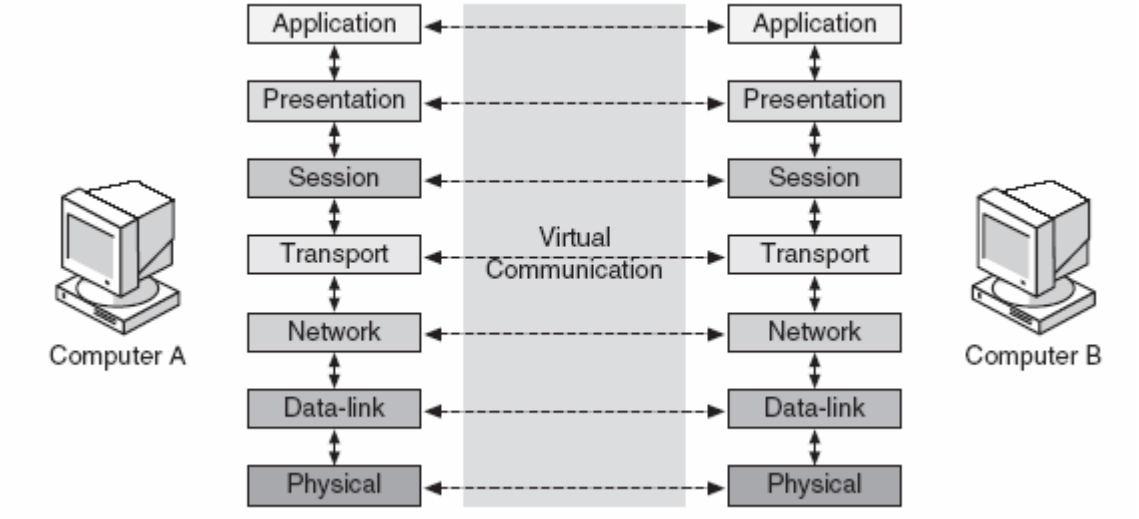
โครงสร้าง **OSI** ถูกสร้างขึ้นมาจากชุดของโพรโตคอลต่าง **7** ระดับชั้น หรือเลเยอร์ **(layers)** แต่ละเลเยอร์มีหน้าที่รับผิดชอบสำหรับการปฏิบัติบางอย่าง หรือการให้บริการที่ช่วยในการเตรียมข้อมูลให้พร้อมที่จะทำการส่งไปบนระบบเครือข่าย โดยแต่ละเลเยอร์จะโต้ตอบกับเลเยอร์ระดับที่อยู่ข้างเคียงเท่านั้น และแต่ละเลเยอร์ก็จะอาศัยการเชื่อมต่อ **(interface)** ที่ตกลงใจว่าจะเสนอให้มีบริการอย่างไรกับเลเยอร์ระดับที่อยู่เหนือขึ้นไป และจะเข้าไปใช้บริการในเลเยอร์ระดับที่อยู่ต่ำลงมาได้อย่างไร รูปที่ **3 – 1** เป็นโครงร่างของ **OSI Model** ทั้ง **7** เลเยอร์ โดยกำหนดเลเยอร์เป็นลำดับชั้นตั้งแต่ฮาร์ดแวร์ เริ่มตั้งแต่การขนส่งข้อมูลทางกายภาพ **(Physical)** ที่ส่วนล่างสุดและไปสิ้นสุดที่โปรแกรมประยุกต์ที่ส่วนบนสุด ซึ่งเป็นโปรแกรมประยุกต์ **(Application)** และยังกำหนดหมายเลขให้กับเลเยอร์ต่างๆ ตั้งแต่เลข **1** ถึง **7** โดยเริ่มนับจากเลเยอร์ระดับล่างสุด คือ **Physical Layer** เป็นเลเยอร์ที่ **1**



รูปที่ **3 – 1 OSI Reference Model**

3.2 การทำงานของ OSI Reference Model

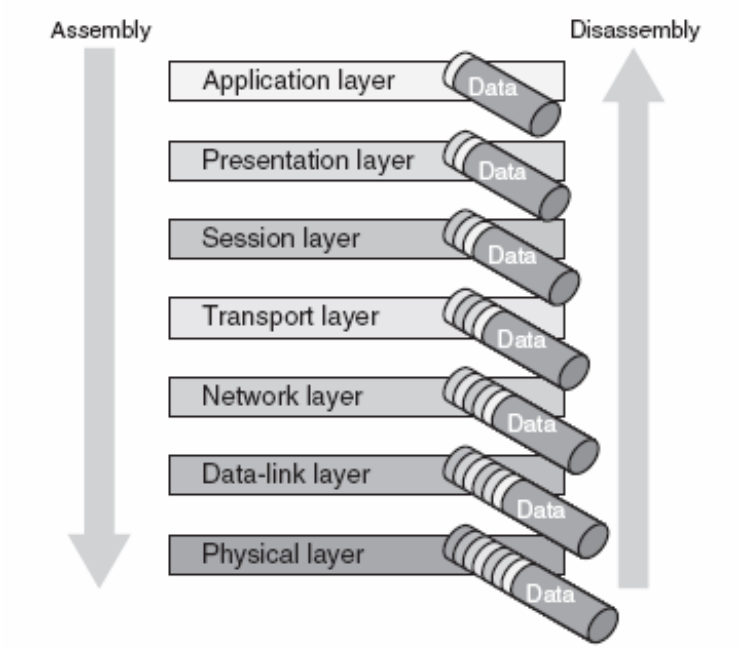
การอธิบายระบบเครือข่ายในความหมายของ **OSI layers** ทั้ง **7** เลเยอร์เป็นวิธีที่ดี แต่จะมีคำถามว่าแพ็กเก็ตข้อมูลจะเดินทางจากเครื่องคอมพิวเตอร์ **A** ไปยังเครื่องคอมพิวเตอร์ **B** ได้อย่างไร? แผนผังในรูปที่ **3 – 2** แสดงให้เห็นภาพของกระบวนการในการสื่อสารข้อมูล



รูปที่ **3 – 2** การจัดโครงสร้างการสื่อสารของ **OSI Reference Model** ทั้ง **7** เลเยอร์

1. สิ่งแรกที่เห็นคือทั้งเครื่องคอมพิวเตอร์ **A** และเครื่องคอมพิวเตอร์ **B** มีโครงสร้างเป็น **OSI Model 7** เลเยอร์

2. เมื่อเครื่องคอมพิวเตอร์ **A** พร้อมที่จะส่งสัญญาณข้อมูลไปยังเครื่องคอมพิวเตอร์ **B** แต่ละเลเยอร์ในเครื่องคอมพิวเตอร์ **A** จะถือว่ามีการสื่อสารกับเลเยอร์ในระดับเดียวกันในเครื่องคอมพิวเตอร์ **B** ถึงแม้ว่าจะไม่มีการสื่อสารระหว่างเลเยอร์เหล่านี้เกิดขึ้นจริง เลเยอร์ระดับต่างๆ บนเครื่องคอมพิวเตอร์ทั้งคู่จะถือว่ามีการสื่อสารกันด้วยภาษาเดียวกัน และทำตามกฎเกณฑ์อย่างเดียวกัน เพื่อให้มั่นใจว่าแต่ละเลเยอร์บนเครื่องคอมพิวเตอร์ฝ่ายผู้รับจะได้รับแพ็กเก็ตข้อมูลแบบเดียวกับที่รวบรวมโดยแต่ละเลเยอร์บนเครื่องคอมพิวเตอร์ฝ่ายผู้ส่ง
3. แพ็กเก็ตข้อมูลที่แท้จริงจะเริ่มถูกสร้างขึ้นที่ระดับสูงที่สุดคือ **application layer** บนเครื่องคอมพิวเตอร์ **A** และเคลื่อนลงมาทีละระดับชั้นจนมาถึงชั้นล่างสุด คือ **physical layer** เมื่อแพ็กเก็ตเคลื่อนผ่านจากระดับหนึ่งไปยังระดับถัดไป ก็จะมีการเพิ่มข่าวสารการส่งสัญญาณข้อมูลเข้ามา (การกำหนดที่อยู่ การจัดรูปแบบและอื่นๆ) สำหรับเรื่องที่แต่ละ เลเยอร์รับผิดชอบ ดังนั้นกระบวนการนำออกและประกอบขึ้นมาใหม่ซึ่งแต่ละเลเยอร์เพิ่มเข้ามาเพื่อให้ได้ผลผลิตที่เป็นแพ็กเก็ตข้อมูลที่สามารถขนส่งไปทางสายสื่อสารทางกายภาพได้ ดังแสดงตามรูปที่ **3 – 3**



รูปที่ **3 – 3** การประกอบและถอดแพ็กเก็ตข้อมูลในเลเยอร์ระดับต่างๆ

4. เมื่อแพ็กเก็ตเคลื่อนตัวลงมาถึง **physical layer** (ซึ่งรวมการ์ดเชื่อมต่อระบบเครือข่าย) ก็จะแปลงให้เป็นกระแสข้อมูลแบบอนุกรม และส่งออกไปผ่านสื่อกลางการส่งสัญญาณ (เช่น สายเคเบิล) ซึ่งเป็นเลเยอร์เดียวที่เครื่องคอมพิวเตอร์ **A** มีการสื่อสารกับคอมพิวเตอร์ **B** จริง ถึงแม้ว่าที่นี่เครื่องคอมพิวเตอร์ **A** และ **B** จะไม่ได้สื่อสารกันโดยตรงเนื่องจากเครื่องทั้งสองมีการเชื่อมต่อกันโดยสื่อตัวกลางการขนส่งข้อมูลเดียวกัน
5. เมื่อการส่งสัญญาณข้อมูลมาถึงเครื่องคอมพิวเตอร์ **B** กระบวนการนี้จะเริ่มทำในทางตรงกันข้าม ซึ่งจะทำการแยกแพ็กเก็ตออกโดยผ่าน **OSI layer** ทั้ง **7** เลเยอร์
6. ที่ **physical layer** บนเครื่องคอมพิวเตอร์ **B** จะแปลงกระแสข้อมูลแบบอนุกรมให้เป็นรูปแบบของแพ็กเก็ตและส่งไปยังเลเยอร์ระดับถัดไป คือ **data link layer**

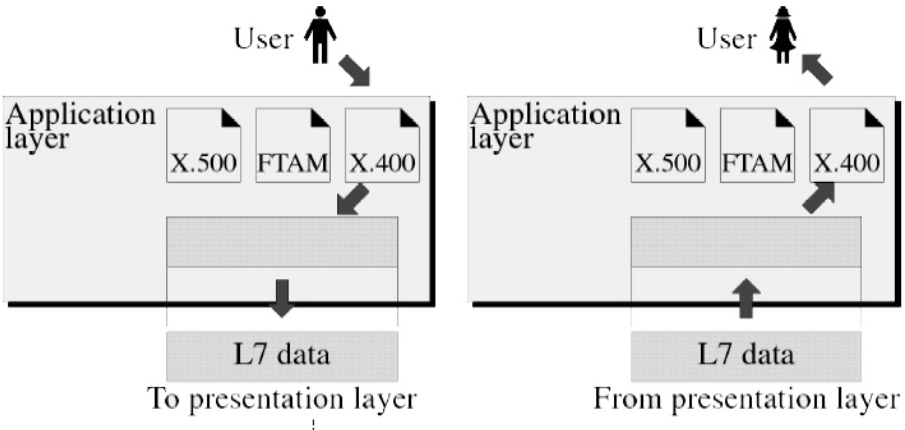
7. เมื่อแพ็กเก็ตเดินทางผ่านเลเยอร์ระดับต่างๆ ขึ้นมา ในแต่ละเลเยอร์ก็จะแยกข่าวสารเกี่ยวกับการกำหนดที่อยู่และการจัดรูปแบบของแพ็กเก็ตที่เพิ่มเขามาโดยเครื่องคอมพิวเตอร์ **A** ออก จนกระทั่งเมื่อถึงเลเยอร์ระดับสูงที่สุด คือ **application layer** ก็จะเหลือเฉพาะข้อมูลที่เหมือนกับที่ส่งมาจาก **application layer** ของเครื่องคอมพิวเตอร์ **A**

3.3 การทำงานของแต่ละเลเยอร์

ในหัวข้อนี้จะมาดูว่าเลเยอร์ระดับต่างๆ เหล่านี้ เป็นตัวแทนสำหรับอะไร และแต่ละเลเยอร์ทำอะไรบ้าง เนื่องจากจะเป็นการง่ายในการเห็นกระบวนการการโยกย้ายข้อมูลอย่างสมบูรณ์โดยเริ่มการส่งและการรับข้อมูลของโปรแกรมประยุกต์

3.3.1 Application Layer (Layer 7)

Application layer ของ **OSI Model** เป็นส่วนที่เกี่ยวข้องกับการจัดการให้ระบบเครือข่าย **access** เข้าไปยังโปรแกรมประยุกต์ และเป็นระดับที่ถูกครอบครองโดยโปรแกรมประยุกต์หลายอย่าง เช่นโปรแกรมการรับ/ส่งอีเมลล์ โปรแกรมการโยกย้ายไฟล์ โปรแกรมการเข้าถึงฐานข้อมูล และแม้แต่โปรแกรมการจัดการระบบเครือข่าย นอกจากนั้น **application layer** ยังเป็นอะไรที่ทำให้ระบบเครือข่ายมีฟังก์ชันในการ **access** ไฟล์และเครื่องพิมพ์ แบ่งปันการใช้ทรัพยากร และการใช้บริการไดเร็กทอรี่ นั่นคือการใช้ฐานข้อมูล (ไดเร็กทอรี่) ที่กำหนดผู้ใช้และทรัพยากรทั้งหมดบนระบบเครือข่าย

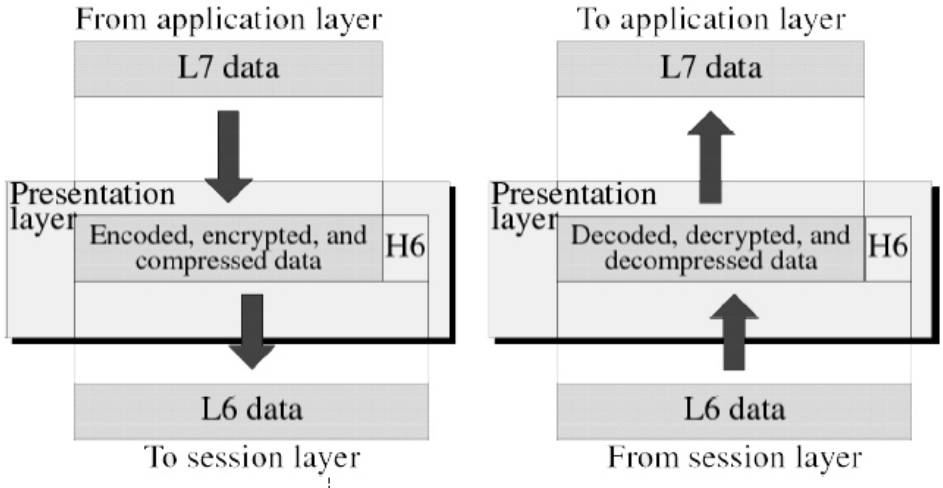


รูปที่ **3 – 4 Application Layer**

เนื่องจากมีโปรแกรมประยุกต์ที่เกี่ยวข้องกับระบบเครือข่ายเป็นจำนวนมาก ในระดับ **application** จึงเป็นเหมือนสิ่งที่งดงามที่สะท้อนถึงวิธีการที่แตกต่างกันหลายวิธีที่ทำให้โปรแกรม **access** และใช้ระบบเครือข่ายได้ ตัวอย่างเช่นทั้งโปรแกรมการโยกย้ายไฟล์และโปรแกรมการรับ/ส่งอีเมลล์ได้รับสิทธิในการ **access** ในระดับนี้ แต่โปรแกรมการโยกย้ายไฟล์จะเกี่ยวข้องกับการโยกย้ายไฟล์จากที่แห่งหนึ่งไปยังที่อีกแห่งหนึ่งเป็นหลัก ส่วนโปรแกรมการรับ/ส่งอีเมลล์ ต้องการการให้บริการที่เกี่ยวข้องกับการจัดการ การจัดเก็บ และการจัดส่งข่าวสาร ซึ่งทั้งสองกรณีนี้โปรแกรมจะต้องอาศัยโปรโตคอลในระดับ **application-level** ซึ่งโปรโตคอลที่กำหนดคุณลักษณะเฉพาะของการรับ/ส่งอีเมลล์ เรียกว่า **X.400** โปรโตคอลที่กำหนดคุณลักษณะเฉพาะของการให้บริการไดเร็กทอรี่เรียกว่า **X.500** และโปรโตคอลที่กำหนดคุณลักษณะเฉพาะของการโยกย้ายไฟล์เรียกว่า **FTP (File Transfer Protocol)** ซึ่งจะอธิบายเรื่องเหล่านี้ในรายละเอียดในเรื่องของโปรโตคอลต่อไปภายหลัง

3.3.2 Presentation layer (Layer 6)

Presentation layer มีหน้าที่หลักในการทำให้มั่นใจว่าข้อมูลที่ทำการส่งระหว่างเครื่องคอมพิวเตอร์ 2 เครื่องได้รับการเข้ารหัสด้วยอักษรแบบเดียวกัน คุณอาจจะทราบแล้วว่า เครื่องคอมพิวเตอร์มักจะไม่ค่อยใช้รหัสแบบเดียวกันสำหรับข้อความและอักขระแบบอื่น ตัวอย่างเช่นเครื่องคอมพิวเตอร์ส่วนใหญ่จะใช้รหัส **ASCII (American Standard Code for Information Interchange)** แต่ในบางครั้งเครื่องคอมพิวเตอร์ที่ใช้ **ASCII code** อาจจะต้องการที่จะสื่อสารกับเครื่องคอมพิวเตอร์ **IBM Mainframe** ซึ่งใช้รหัสที่เรียกว่า **EBCDIC (Extended Binary Coded Decimal Interchange Code)** ถึงแม้ว่า **ASCII** จะใช้เลขฐานสอง 7 หรือ 8 บิต ในการแทนอักขระจำนวน 256 ตัว และ **EBCDIC** ใช้เลขฐานสอง 8 บิต ในการแทนอักขระจำนวน 256 ตัวเช่นเดียวกัน แต่ค่าของเลขฐานสองที่กำหนดให้อักขระตัวเดียวกันของทั้ง 2 วิธีก็ไม่จำเป็นต้องมีค่าเท่ากัน ตัวอย่างเช่นตัวอักษร **a** ใน **ASCII** มีค่าเท่ากับ 97 ส่วนในรหัส **EBCDIC** จะมีค่าเท่ากับ 129



รูปที่ 3 – 5 Presentation Layer

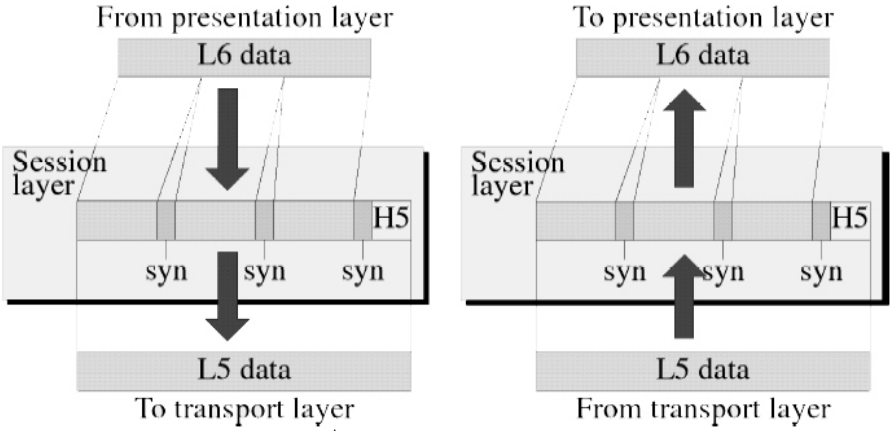
สิ่งต่างๆ เหล่านี้เป็นหน้าที่รับผิดชอบของ **Presentation layer** ในการทำให้มั่นใจว่าเครื่องคอมพิวเตอร์ทั้งคู่ใช้การแทนค่าแบบเดียวกันสำหรับข้อมูล นอกจากนั้น **presentation layer** ยังรองรับการเข้ารหัสข้อมูลหรือการบีบอัดข้อมูลตามความต้องการ

3.3.3 Session layer (Level 5)

จนถึงขณะนี้คุณได้เห็นแล้วว่าใน **OSI model** นั้น งานของ **application layer** คือจัดเตรียมให้มีการ **access** เข้าไปยังระบบเครือข่ายและส่งต่อข้อมูลไปยัง **presentation layer** ซึ่งทำให้มั่นใจว่าข้อมูลนั้นถูกแสดงแทนในรูปแบบที่เครื่องคอมพิวเตอร์ทั้งฝ่ายผู้ส่งและฝ่ายผู้รับสามารถเข้าใจได้ แล้วมีอะไรต่อไป? ในขณะนี้ข้อมูลเคลื่อนย้ายลงไปยัง **Session layer** ที่มีหน้าที่รับผิดชอบสำหรับทำให้โปรแกรมประยุกต์บนเครื่องคอมพิวเตอร์ ฝ่ายผู้ส่งและฝ่ายผู้รับสามารถจัดตั้งการเชื่อมต่อที่เรียกว่า **session** ซึ่งเปรียบเทียบได้กับการสนทนากันทางโทรศัพท์

ประการแรก ให้จำไว้ว่าหน้าที่รับผิดชอบของ **session** คือการจัดตั้งการสื่อสารระหว่าง 2 ฝ่ายที่เรียกว่า **application entities** หรือ **AE** คุณอาจจะคิดเกี่ยวกับ **AE** โดยเปรียบเทียบกับ บุคคล 2 คนที่ต้องการ

สนทนากันโดยใช้โทรศัพท์ เมื่อเริ่มกระบวนการ **session layer** บนเครื่องคอมพิวเตอร์ที่สื่อสารกันจะจัดตั้งการเชื่อมต่อ ถ้าต้องการ นอกจากนั้น **session layer** ยังดูแลเรื่องการวัดความปลอดภัย เช่นอายุการใช้งานของรหัสผ่าน ส่วนนี้ของกระบวนการคล้ายกับการหมุนโทรศัพท์ที่ปลายด้านหนึ่งและมีการตอบรับที่ปลายทางอีกด้านหนึ่ง และถามว่าใช่คนที่คุณต้องการพูดด้วยหรือไม่ ในทันทีที่การเชื่อมต่อได้รับการจัดตั้ง **session layer** จะทำให้การสนทนาเป็นไปอย่างราบเรียบ ซึ่งทำได้โดยการเฝ้าตรวจสอบและควบคุมการไหลของข้อมูลให้เป็นจังหวะ ควบคุมว่าใครเป็นผู้ส่งเมื่อใด และนานเท่าใด ส่วนนี้เปรียบได้กับการมีกรรมการกลางในการสนทนาทางโทรศัพท์ เพื่อที่ให้คู่สนทนาผลัดกันควบคุมการใช้สายและไม่พูดพร้อมกันในเวลาเดียวกัน



รูปที่ 3 – 6 Session Layer

เมื่อการส่งข้อมูลเสร็จสิ้น **Session layer** จะมีหน้าที่รับผิดชอบในการทำให้มั่นใจว่าการสนทนาสิ้นสุดลงด้วยความเรียบร้อย (คู่สนทนาวางสาย)

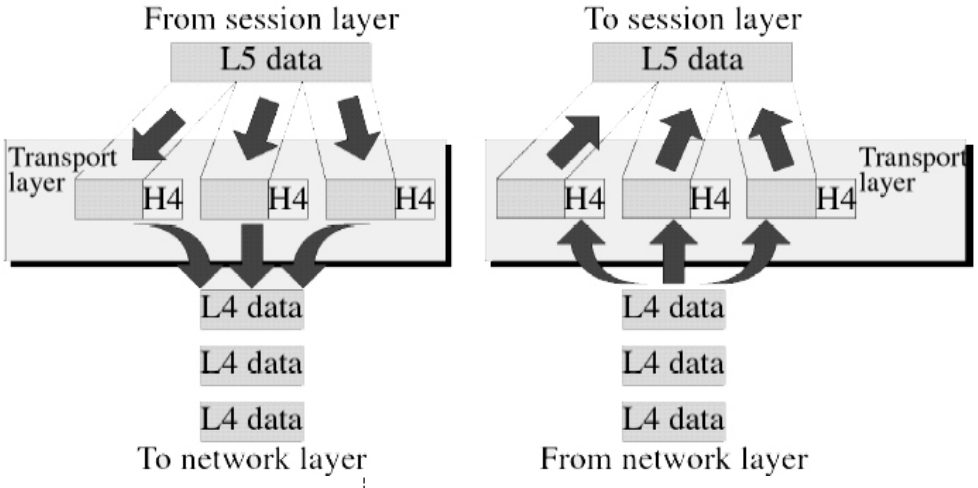
Session layer ประกอบด้วยโปรโตคอลที่สนับสนุนการให้บริการต่างๆ ที่มีในระดับนี้เช่นเดียวกับเลเยอร์อื่นๆ ใน **OSI Reference Model** ซึ่งโปรโตคอลตัวหนึ่งที่พบคือ **NetBEUI (NetBIOS Extended User Interface)** ที่จัดให้มีในระบบเครือข่ายของ **Microsoft** อย่างไรก็ตาม **NetBIOS** คือโปรแกรมประยุกต์สำหรับการเชื่อมต่อ **(application programming interface)** หรือ **API** ที่ทำให้โปรแกรมประยุกต์สามารถร้องขอการให้บริการในระดับ **session-level**

3.3.4 Transport layer (Layer 4)

Transport layer เป็นเหมือนบริษัทขนส่งของ **OSI Reference Model** ที่จริงแล้วไม่ใช่ทำการเคลื่อนย้ายระวาง แต่มีหน้าที่รับผิดชอบในการทำให้มั่นใจว่าทำการจัดส่งข้อมูลโดยปราศจากความผิดพลาด หรืออะไรที่กล่าวถึงคุณภาพในการให้บริการ **(quality of service)** หรือ **QoS** โดยเฉพาะอย่างยิ่ง **transport layer** จะทำให้มั่นใจว่าข้อมูลจะไม่สูญหายหรือเกิดการทำซ้ำ ซึ่งเป็นส่วนหนึ่งของความรับผิดชอบของ **transport layer**

- ที่ **transport layer** บนคอมพิวเตอร์เครื่องผู้ส่งจะแตกก้อนข้อมูล (ซึ่งถูกส่งผ่านไปยังเลเยอร์ที่มีขนาดเท่ากับขนาดแรกเริ่ม) ให้เป็นแพ็กเก็ตซึ่งมีขนาดตามที่ **network layer** ที่อยู่ต่ำลงไปต้องการ บนเครื่องคอมพิวเตอร์ฝ่ายผู้รับ **transport layer** จะทำการประกอบแพ็กเก็ตที่ได้รับให้เป็นก้อนข้อมูลซึ่งมีขนาดเท่าเดิม

- ถ้าใช้การสื่อสารที่ไม่จัดตั้งการเชื่อมต่อ (**connectionless communications**) แพ็กเก็ตข้อมูลอาจจะถูกส่งไปตามเส้นทางต่างๆ และไปถึงปลายทางไม่เป็นลำดับ **transport layer** บนคอมพิวเตอร์เครื่องผู้ส่งจะกำหนดลำดับหมายเลขให้กับแพ็กเก็ตแล้วทำการส่งออกไปอย่างสมบูรณ์เพื่อรับรองว่าแพ็กเก็ตเหล่านั้นจะถูกจัดส่งและประกอบขึ้นมาใหม่อย่างถูกต้อง



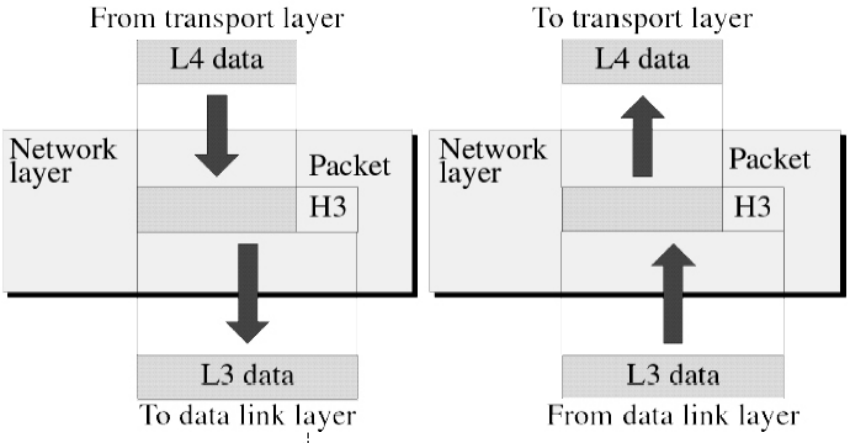
รูปที่ 3 – 7 **Transport Layer**

- **Transport layer** จัดเตรียมสำหรับ การจัดส่งแบบ **end-to-end** ซึ่งรวมถึงสัญญาณการตอบรับจากเครื่องคอมพิวเตอร์ฝ่ายผู้รับว่าได้รับข้อมูลโดยปราศจากความผิดพลาด
- ถ้า **frame buffer** ซึ่งเป็นแหล่งเก็บข้อมูลชั่วคราวบนเครื่องคอมพิวเตอร์ฝ่ายผู้รับ มีข้อมูลอยู่เต็ม **transport layer** จะสั่งให้เครื่องคอมพิวเตอร์ฝ่ายผู้ส่งหยุดรอก่อนที่จะส่งข้อมูลมาอีก
- **Transport layer** อาจจะมีหน้าที่รับผิดชอบสำหรับการ **multiplex** ข้อมูล หรือสนทนาและติดตามว่าอะไรเป็นอะไร

จุดสำคัญคือ **Transport layer** จะอยู่ระหว่างเลเยอร์ที่เกี่ยวข้องกับโปรแกรมประยุกต์ที่อยู่เหนือขึ้นไปกับ **subnet** ซึ่งเป็นเลเยอร์ที่เกี่ยวข้องกับระบบเครือข่ายและฮาร์ดแวร์ที่อยู่ต่ำลงมา การที่เป็นตัวกลางระหว่างเลเยอร์ทั้งสองกลุ่ม **transport layer** จึงเป็นผู้รับประกันความน่าเชื่อถือให้กับเลเยอร์ที่เกี่ยวข้องกับโปรแกรมประยุกต์ที่อยู่เหนือขึ้นไป ไม่ว่าใน **subnet** หรือเลเยอร์ที่อยู่ต่ำลงมาจะมีความน่าเชื่อถือเพียงใด

3.3.5 Network layer (Layer 3)

Network layer เป็นเลเยอร์ที่อยู่สูงที่สุดในบรรดา **subnet** ของ **OSI Reference Model** ซึ่งความจริงแล้วก็คือผู้ควบคุม **subnet** ที่มีหน้าที่รับผิดชอบในการกำหนดเส้นทางการส่งข้อมูล และกำหนดแอดเดรสให้กับข้อมูลทั้งภายในระบบเครือข่ายและระหว่างระบบเครือข่าย เช่นเดียวกับการที่ **transport layer** รับรองความน่าเชื่อถือให้กับเลเยอร์ที่อยู่สูงขึ้นไป **network layer** จะช่วยเหลือทุกเลเยอร์ที่อยู่เหนือขึ้นไป รวมทั้ง **transport layer** ที่ต้องการทราบทุกสิ่งเกี่ยวกับการส่งสัญญาณข้อมูลจริงและเทคโนโลยีการกำหนดเส้นทางที่ **subnet** ใช้



รูปที่ 3 – 8 Network Layer

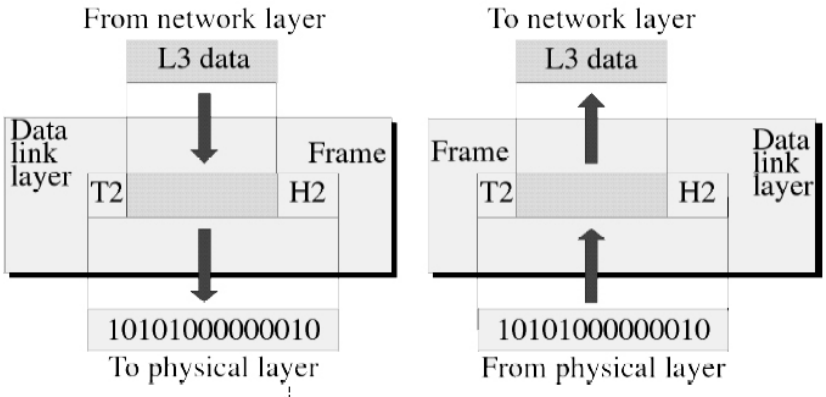
สำหรับหน้าที่ในการกำหนดเส้นทางการส่งข้อมูลนั้น ใน **network layer** บนเครื่องคอมพิวเตอร์ฝ่ายผู้ส่งจะพิจารณาว่าจะใช้เส้นทางใดในการส่งข้อมูล ตามพื้นฐานตัวเลือกตามจำนวนของตัวแปร ซึ่งประกอบด้วยสถานะของระบบเครือข่าย ภาระในการขนส่งข้อมูล การส่งสัญญาณข้อมูลในระบบเครือข่ายหรือระหว่างระบบเครือข่ายบนสื่อตัวกลางหลายแบบ สำหรับทิศทางในการกำหนดเส้นทางการส่งสัญญาณข้อมูลนั้น ถ้าจำเป็น **network layer** จะโยกย้ายแพ็กเก็ต (ในทางเทคนิคจะเรียกว่าเฟรมข้อมูลในเลเยอร์ที่อยู่ต่ำกว่า **network layer**) ไปยังเราท์เตอร์ซึ่งเป็นอุปกรณ์ระบบเครือข่ายที่ทำหน้าที่เป็นจุดเปลี่ยนเส้นทางระหว่างระบบเครือข่ายที่ใช้พื้นฐานสถาปัตยกรรมที่แตกต่างกัน เนื่องจากขนาดของเฟรมข้อมูลที่เรียกว่า **maximum transmission unit** หรือ **MTU** จะมีขนาดเปลี่ยนแปลงไปตามประเภทของระบบเครือข่ายที่แตกต่างกัน ดังนั้น **network layer** บนเครื่องคอมพิวเตอร์ฝ่ายผู้ส่งยังต้องมีหน้าที่รับผิดชอบในการอนุญาตให้เราท์เตอร์สามารถแตกเฟรมข้อมูลให้มีขนาดเล็กลง ถ้าเฟรมนั้นๆ มีขนาดใหญ่เกินกว่าที่เราท์เตอร์จะรองรับได้ ในทางกลับกัน **network layer** บนเครื่องคอมพิวเตอร์ฝ่ายผู้รับจะมีหน้าที่รับผิดชอบในการประกอบเฟรมข้อมูลที่ถูกแตกออกเป็นชิ้นเล็กๆ เหล่านั้นเข้าด้วยกัน

ในเรื่องของการกำหนดแอดเดรสนั้น **Network layer** บนเครื่องคอมพิวเตอร์ฝ่ายผู้ส่งจะมีหน้าที่ในการแจกจ่ายแอดเดรสระบบเครือข่าย (**network address**) ทางตรรกะและทางกายภาพ นั่นคือจะต้องแปลงแอดเดรสระบบเครือข่ายของโหนดต่างๆ (แอดเดรสทางตรรกะ) ให้เป็นแอดเดรสทางกายภาพซึ่งเป็นที่อยู่อย่างแท้จริงได้อย่างเที่ยงตรง สำหรับโปรโตคอลที่ทำงานบน **network layer** คือ **IP (Internet Protocol)** และ **X.25** ที่ใช้ในระบบเครือข่ายแบบแพ็กเก็ตสวิตชิ่ง (**packet-switching**) ซึ่งจะอธิบายรายละเอียดภายหลัง

3.3.6 Data link layer (Layer 2)

Data link layer อยู่ระหว่างและสื่อสารกับ **physical layer** ที่อยู่ด้านล่าง กับ **network layer** ที่อยู่เหนือขึ้นไป ถึงแม้ว่า **data link** จะไม่ใช่คำที่มีความหมายในตัวเองเช่นเดียวกับ **physical** หรือ **application** แต่ฟังก์ชันการทำงานของ **data link layer** ก็เป็นไปอย่างมีเหตุมีผลที่ทำให้เข้าใจได้ง่าย คือมีส่วนเกี่ยวข้องกับข้อมูล (**data**) และการเชื่อมต่อ (**link**) ระหว่างเครื่องคอมพิวเตอร์ ดังนั้นงานของ **data link layer** จะมีพื้นฐานอยู่บนการปฏิบัติ 2 อย่าง คือ

- จัดรูปแบบของแพ็กเก็ต หรือเฟรมข้อมูล ให้เป็นรูปแบบตามความต้องการตามประเภทของสถาปัตยกรรมระบบเครือข่าย (นั่นคือส่วนที่เกี่ยวกับข้อมูล)
- สร้างการเชื่อมต่อทางตรรกะและทำให้สิ้นสุดการเชื่อมต่อระหว่างโหนดต่างๆ บนระบบเครือข่าย และส่งแพ็กเก็ตเหล่านั้นไปบน **physical layer**

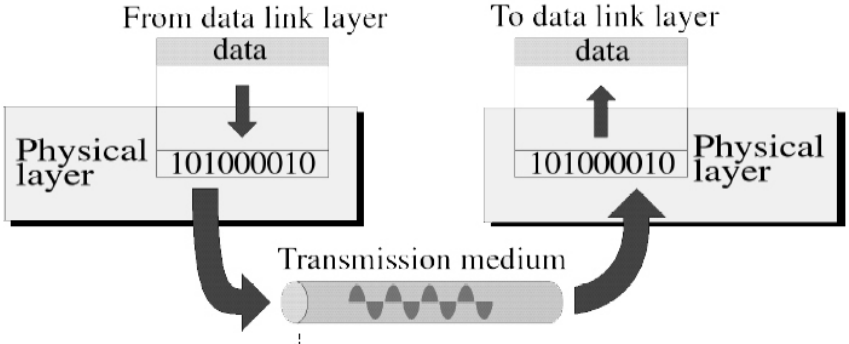


รูปที่ **3 – 9 Data link Layer**

ในการทำงานของ **Data link layer** ไม่เพียงแต่จัดขนาดของแพ็กเก็ตข้อมูลและสร้างการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ เพื่อให้เกิดความมั่นใจ เช่นเดียวกับเลเยอร์อื่นๆ ว่าจะสามารถส่งสัญญาณข้อมูลได้โดยปราศจากความผิดพลาด **data link layer** ยังมีหน้าที่รับผิดชอบในการควบคุมการไหลของเฟรมข้อมูล สำหรับการตอบรับการส่งสัญญาณข้อมูล และเมื่อจำเป็นถ้าข้อมูลถูกทำลายในระหว่างการเดินทางก็จะทำการส่งสัญญาณข้อมูลออกไปใหม่

3.3.7 Physical layer (Layer 1)

สุดท้ายก็มาถึง **physical layer** ซึ่งเป็นเลเยอร์การเชื่อมต่อทางกายภาพ ที่นี่กระแสข้อมูลซึ่งมีค่าเป็น **1s** และ **0s** จะถูกผลักดันผ่านระบบเครือข่ายจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง **physical layer** จะเกี่ยวข้องกับสื่อกลางของระบบเครือข่าย คือสายเคเบิล หัวเชื่อมต่อ การ์ดเชื่อมต่อ และสัญญาณทางไฟฟ้า มีคุณลักษณะเฉพาะเป็นจำนวนมากที่กำหนดสำหรับส่วนต่างๆ เหล่านี้ ตัวอย่างเช่น มีคุณลักษณะเฉพาะสำหรับกำหนดจำนวนและฟังก์ชันการทำงานของแต่ละ **pins** ของหัวเชื่อมต่อ มีคุณลักษณะเฉพาะสำหรับสายเคเบิลประเภทต่างๆ และคุณลักษณะเฉพาะที่กำหนดว่าจะต่อสายเคเบิลเหล่านั้นเข้ากับการ์ดเชื่อมต่อระบบเครือข่ายได้อย่างไร



รูปที่ **3 – 10 Physical Layer**

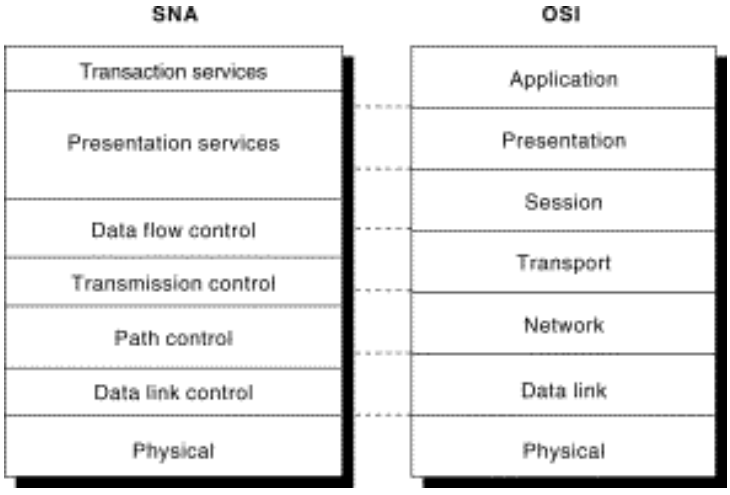
นอกเหนือจากส่วนประกอบทางกายภาพที่สามารถแตะต้องได้เหล่านี้แล้ว **Physical layer** ยังเตรียมบางสิ่งที่แทบจะมองไม่เห็นแต่มีความสำคัญเท่ากับสัญญาณข้อมูล นั่นคือการเข้ารหัสและถอดรหัสบิตข้อมูล โดยการกำหนดช่วงเวลาและทำให้เกิดขึ้นในเวลาเดียวกันตามวิธีที่ต้องการเพื่อให้มั่นใจว่าข้อมูลจะถูกส่งออกไปอย่างเที่ยงตรง โดยทำให้แต่ละบิตถูกส่งออกไปและไปถึงในสภาวะเดียวกัน

OSI Reference Model เป็นโครงสร้างแบบหนึ่งที่มักจะถูกอ้างถึงในการอธิบายการทำงานของระบบเครือข่ายเป็นระดับชั้น ซึ่งเป็นการระบุโปรโตคอลที่ใช้ในแต่ละเลเยอร์ของระบบเครือข่าย (**protocol XX** ทำงานใน **YY layer**) อย่างไรก็ตาม **OSI** ก็ไม่ใช่โครงสร้างของระบบเครือข่ายที่มีเพียงอย่างเดียว ยังคงมีโครงสร้างระบบเครือข่ายแบบอื่นอีก 2 แบบที่มีการจัดแบ่งเป็นเลเยอร์ระดับชั้นต่างๆ เช่นเดียวกันและบรรยายเกี่ยวกับสถาปัตยกรรมของระบบเครือข่าย แบบแรกคือสถาปัตยกรรมโครงสร้างของ **IBM** ที่เรียกว่า **SNA** และอีกแบบหนึ่งคือโครงสร้างที่เกี่ยวกับเครือข่ายอินเตอร์เน็ต ที่เรียกว่า **TCP/IP Reference Model** หรือ **Internet Reference Model**

3.4 SNA 5 – 7 layers (The five To seven layers of SNA)

SNA ซึ่งเป็นชื่อเรียกโดยย่อของ **System Network Architecture** ได้รับการออกแบบโดยบริษัท **IBM** ในปี **1970s** ให้เป็นวิธีสำหรับการทำให้ผลิตภัณฑ์ของบริษัท **IBM** (เครื่องคอมพิวเตอร์เมนเฟรม เครื่องเทอร์มินอล และเครื่องพิมพ์) สามารถสื่อสารและแลกเปลี่ยนข้อมูลระหว่างกันได้ เดิมทีได้มีการออกแบบ **SNA** ตามความสัมพันธ์ระหว่างเครื่องคอมพิวเตอร์เมนเฟรม กับเครื่องเทอร์มินอล แต่ในภายหลังได้มีการปรับปรุงให้เป็นคุณลักษณะเฉพาะที่เรียกว่า **APPC (Advanced Program to Program Communication)** เพื่อให้ครอบคลุมรวมถึงเครื่องมินิคอมพิวเตอร์และเครื่องไมโครคอมพิวเตอร์

โครงสร้าง **SNA** ซึ่งเกิดขึ้นก่อน **ISO/OSI Reference Model** แต่สามารถเปรียบเทียบกับ **ISO** ได้ โครงสร้างพื้นฐานของ **SNA** ประกอบด้วย 5 เลเยอร์ และปรับปรุงโดยการเพิ่มอีก 2 เลเยอร์ เพื่อให้สมบูรณ์เหมือนกับ **ISO/OSI model** โครงสร้างพื้นฐานและส่วนขยายของ **SNA layer** แสดงตามรูปที่ **3 – 11**



รูปที่ **3 - 11** โครงสร้างพื้นฐานและส่วนขยาย ของสถาปัตยกรรมระบบเครือข่าย **SNA**

3.4.1 Transaction services Layer

เลเยอร์ซึ่งอยู่สูงที่สุดของโครงสร้าง **SNA** คือ **Transaction services layer** ประกอบด้วยโปรโตคอลซึ่งมีหน้าที่รับผิดชอบในการสื่อสารระหว่างโปรแกรมประยุกต์กับโปรแกรมประยุกต์ ซึ่งเทียบได้กับ **application layer** ใน **ISO/OSI Reference Model**

3.4.2 Presentation services Layer

เลเยอร์ที่อยู่ถัดลงมา คือ **Presentation services** (หรือการจัดการฟังก์ชัน) รองรับการจัดรูปแบบการบีบอัด และแปลงข้อมูลระหว่าง **ASCII** กับ **EBCDIC** เมื่อคุณนึกย้อนไปงานเหล่านี้จะเทียบได้โดยตรงกับหน้าที่รับผิดชอบของ **Presentation layer** ใน **ISO/OSI Reference Model**

3.4.3 Data flow control layer

เมื่อเคลื่อนต่ำลงมาอีกในโครงสร้าง **SNA** จะพบกับ **Data flow control layer** ซึ่งเลเยอร์นี้จะอธิบายกฎที่จะต้องทำตามในระหว่างการสื่อสาร เช่นการกู้คืนจากความผิดพลาด และไม่ว่าข้อมูลจะมีการเคลื่อนย้ายทั้ง 2 ทิศทางในเวลาเดียวกัน (**full duplex**) หรือต่างเวลากัน (**half duplex**) บางส่วนของเลเยอร์นี้สามารถเทียบได้กับ **Session layer** ใน **ISO/OSI Reference Model**

3.4.4 Transmission control layer

เลเยอร์ที่อยู่ถัดลงมา คือ **Transmission control** รองรับการสนทนาระหว่าง **nodes** ที่สื่อสารกันโดยจะควบคุมการเริ่ม การสิ้นสุด และรักษาการสนทนา กำหนดเส้นทางให้ข้อมูลเดินทางไปบนระบบเครือข่าย และทำให้มั่นใจว่าข้อมูลไปถึงปลายทางอย่างถูกต้อง บางส่วนของเลเยอร์นี้สามารถเทียบได้กับ **Session layer** ใน **ISO/OSI Reference Model** อย่างไรก็ตามในเรื่องของการกำหนดเส้นทางให้กับข้อมูลและการทำให้มั่นใจในการจัดส่งข้อมูลได้อย่างถูกต้อง ของ **transmission control** ยังเทียบได้กับ **transport layer** และ **network layer** ใน **ISO/OSI Reference Model**

3.4.5 Path control layer

Path control layer ในโครงสร้าง **SNA** มีหน้าที่ทำการเชื่อมต่อระหว่างโหนด จัดการการเชื่อมต่อและกำหนดเส้นทางให้กับข้อมูล ในเรื่องของการทำงานแล้วเลเยอร์นี้จะสามารถเปรียบเทียบได้กับ **Transport layer** และ **Network layer** ใน **ISO/OSI Reference Model**

3.4.6 Data link control layer

เลยอร์ระดับชั้นต่ำที่สุดของเลเยอร์พื้นฐานในโครงสร้าง **SNA** คือ **Data link control layer** ซึ่งมีหน้าที่เหมือนเป็น **peer** ใน **ISO/OSI Reference Model** ที่รับผิดชอบในการทำให้การโยกย้ายข้อมูลผ่านสื่อทางกายภาพและอุปกรณ์ระบบเครือข่าย ได้อย่างมีความน่าเชื่อถือ

3.4.7 Physical layer

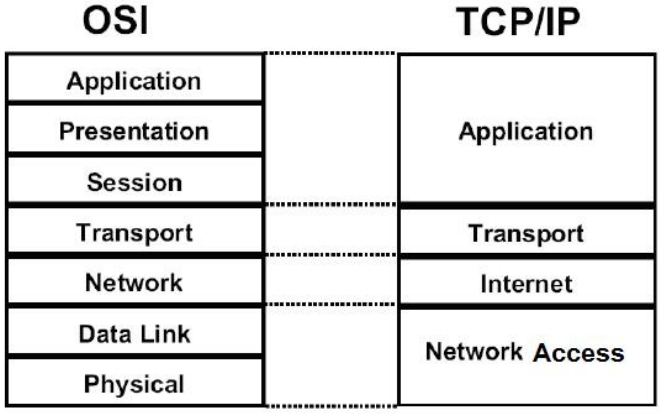
Physical layer ในโครงสร้าง **SNA** เป็นเลเยอร์ที่สองในส่วนขยายของโครงสร้างพื้นฐาน **SNA** ซึ่งมี 5 เลเยอร์ แต่จะไม่มีการทำให้เป็นผลสำเร็จได้โดยตรงเช่นเดียวกับ **Physical layer** ใน **ISO/OSI Reference Model** ที่รวบรวมโครงสร้างพื้นฐานทางกายภาพและการส่งสัญญาณทางไฟฟ้าที่ใช้บนระบบเครือข่าย

SNA อยู่บนพื้นฐานของจำนวนหน่วยที่แตกต่างกันบนระบบเครือข่ายและแต่ละหน่วยก็จะให้บริการที่แตกต่างกัน ซึ่งแตกต่างจาก **ISO/OSI Reference Model** ส่วนที่สำคัญของโครงสร้าง **SNA** จึงขึ้นอยู่กับเครื่องคอมพิวเตอร์เมนเฟรม ซึ่งในสภาวะแวดล้อมแบบ **mainframe/terminal** จะมีหน้าที่ในการสร้างการสนทนาทุกครั้งในการสื่อสาร ซึ่งหากมีการสื่อสารที่นอกเหนือจากนี้จะต้องอาศัย **controller** เพิ่มเติมที่เรียกว่า **Network Control Program** หรือ **NCP** ซึ่งรับภาระในการกำหนดเส้นทางการส่งข้อมูลและควบคุมเส้นทางผ่านโหนดตัวกลางบนระบบเครือข่าย นอกจากนั้นการพัฒนาโครงสร้าง **SNA** ให้เป็น **APPC** ยังจัดให้มี **nodes** อีก 2 ประเภทที่แตกต่างกัน คือ **End nodes (ENs)** ที่เชื่อมต่อเข้ากับระบบเครือข่ายเพื่อใช้ระบบเครือข่าย และ **Network nodes (NNs)** ซึ่งเชื่อมต่อเข้ากับระบบเครือข่ายเพื่อทำหน้าที่กำหนดเส้นทางการส่งข้อมูลและจัดการระบบเครือข่าย

อย่างไรก็ตามโครงสร้าง **SNA** จะมีการใช้ตัวย่อมากกว่าโครงสร้าง **ISO/OSI** ซึ่งไม่เพียงแต่ที่ได้อธิบายไปบ้างแล้ว แต่ยังมีบางตัวเป็นต้นว่า **PU (physical unit** ซึ่งหมายถึงอุปกรณ์และซอฟต์แวร์ของอุปกรณ์นั้น) และ **LU (logical unit** ซึ่งหมายถึงโปรแกรมประยุกต์หรือผู้ใช้) สำหรับรายละเอียดของเรื่องต่างๆ เหล่านี้และเรื่องอื่นที่เกี่ยวข้องกับโครงสร้าง **SNA** จะมีอยู่ในเอกสารที่เป็นหลักฐานของบริษัท **IBM**

3.5 TCP/IP Model หรือ Internet Reference Model

ด้วยเหตุที่มีการประกอบเป็นโครงสร้าง **SNA** เพื่อกำหนดและอธิบายการสื่อสารในสภาวะแวดล้อมของ **IBM** ที่ใช้เครื่องคอมพิวเตอร์เมนเฟรมเป็นพื้นฐาน การกำเนิดและวิวัฒนาการของเครือข่ายอินเตอร์เน็ตก็ทำให้เพิ่มไปสู่โครงสร้างแบบอื่น คือ **TCP/IP Reference Model** ซึ่งมักจะถูกกล่าวถึงว่าเป็น **Internet Reference Model**



รูปที่ 3 – 12 **Layers** ต่างๆ ใน **TCP/IP** และ **ISO/OSI Reference Model**

TCP/IP Model แตกต่างจากทั้ง **ISO/OSI model** และ **SNA model** ตรงที่ **TCP/IP** ไม่ได้มีพื้นฐานบนแนวความคิดของการสนทนาในการสื่อสารโดยกำหนดการเชื่อมต่อระหว่างโหนดที่สื่อสารกัน หรือกล่าวอีกอย่างหนึ่งได้ว่า **TCP/IP model** เป็นภาพแสดงให้เห็นโลกของระบบเครือข่ายสากล **(internetworking)** ที่ทำการเคลื่อนย้ายและกำหนดเส้นทางให้กับข้อมูลระหว่างเครื่องสถานีงาน **(workstation)** ต่างๆ และนี่ก็เป็นสิ่งแตกต่างอย่างสิ้นเชิงจากการเคลื่อนย้ายข้อมูลในโลกของความสัมพันธ์ **mainframe/terminal** หรือความสัมพันธ์แบบ **client/server** ซึ่ง

จัดตั้งการสนทนา รักษาการสนทนา และทำให้การสนทนาสิ้นสุดลง มีความสำคัญเพียงพอที่จะรับประกันสิทธิของ **protocol layer** ทั้งหมดในระบบเครือข่าย รูปที่ **3 – 12** แสดงความแตกต่างระหว่าง **TCP/IP** กับ **ISO/OSI Reference Model** โดยเปรียบเทียบ เลเยอร์ของโครงสร้างแต่ละแบบ ให้สังเกตว่าภาพที่แสดงจะไม่มีความสัมพันธ์ระหว่าง **TCP/IP internetworking layer** กับเลเยอร์ใดๆ ใน **ISO/OSI Reference Model** และให้สังเกตอีกว่าถึงแม้โครงสร้าง **TCP/IP** จะไม่มีเลเยอร์ที่เทียบได้กับ **Physical layer** ที่เห็นได้อย่างเด่นชัด แต่ระบบเครือข่ายใดๆ ก็ต้องอาศัยฮาร์ดแวร์ทางกายภาพและมีมาตรฐานการส่งสัญญาณข้อมูล

3.5.1 The network access layer

เป็นเลเยอร์ที่อยู่เหนือ **Physical layer** (ถ้าโครงสร้างนี้มี) ประกอบด้วยโปรโตคอลที่ต้องใช้ในการขนส่งและจัดส่งเฟรมข้อมูล และเป็นเลเยอร์ที่บรรจุโปรโตคอลซึ่งใช้ในการพิจารณาว่าจะส่งเฟรมข้อมูลได้อย่างไร และจะส่งผ่านไปยัง หรือเดินทางไปบนระบบเครือข่ายทางกายภาพอย่างแท้จริงได้อย่างไร สำหรับงานในการจัดส่งเฟรมข้อมูล เลเยอร์นี้จะต้องอาศัยการกำหนดที่อยู่อย่างถาวรให้กับการ์ดเชื่อมต่อระบบเครือข่าย หรือกล่าวอย่างสั้นๆ ได้ว่า **Network access layer** เป็นส่วนที่บรรจุโปรโตคอลซึ่งมีหน้าที่รับผิดชอบในการโต้ตอบกับ **Physical layer** โดยมีหน้าที่รับผิดชอบสำหรับรับทราบรายละเอียดที่จำเป็นในการสร้างและกำหนดแอดเดรสให้กับเฟรมข้อมูล

3.5.2 The internetwork layer

เป็นเลเยอร์ที่ไม่เหมือนกับเลเยอร์ใดๆ ใน **ISO/OSI model** และ **SNA model** เลเอยร์นี้เป็นส่วนของ **TCP/IP model** ที่ประกอบด้วยโปรโตคอลซึ่งมีหน้าที่รับผิดชอบในการกำหนดเส้นทางให้กับข้อมูลจากผู้ส่งไปยังผู้รับ คือกระบวนการซึ่งแพ็กเก็ตข้อมูลต้องการในการส่งอาจจะประกอบด้วยการ **hops** ผ่านสื่อกลางของระบบเครือข่ายหรือส่วนของระบบเครือข่าย ในเลเยอร์นี้แพ็กเก็ตข้อมูลจะถูกกล่าวถึงว่าเป็น **datagram** ซึ่งเป็นแพ็กเก็ตข้อมูลที่มีข่าวสารในส่วนหัว (**header**) และส่วนต่อท้าย (**trailer**) ประกอบอยู่ด้วยแล้ว การใช้เราท์เตอร์ กับเกตเวย์ในการส่ง **datagram** ไป-มาจากที่แห่งหนึ่งไปยังที่อีกแห่งหนึ่งก็ถูกรวมอยู่ในเลเยอร์นี้

3.5.3 The transport level

เช่นเดียวกับ **transport layer** ใน **ISO/OSI Reference Model** คือมีหน้าที่รับผิดชอบสำหรับความน่าเชื่อถือในการจัดส่ง **datagram** และสำหรับช่วยเหลือการสื่อสารของเครื่องคอมพิวเตอร์โดยการจัดตั้งการเชื่อมต่อหรือสร้างวงจรเสมือน (**virtual circuit**) การเชื่อมต่อที่ว่านี้จะเหมือนกับการสนทนาใน **ISO/OSI Reference Model** ที่จะเริ่มด้วยคำสั่งในการเปิดและสิ้นสุดด้วยคำสั่งในการปิด และจัดให้มีเส้นทางการส่งข้อมูลให้กับเครื่องคอมพิวเตอร์ผู้ส่งและเครื่องคอมพิวเตอร์ผู้รับ อย่างไรก็ตามในโลกของ **TCP/IP** นั้น แพ็กเก็ตข้อมูลจะถูกกำหนดเส้นทางการส่งจากแหล่งกำเนิดไปยังปลายทางผ่านเส้นทางที่ดีที่สุดในขณะนั้น การแลกเปลี่ยนข้อมูลในลักษณะนี้เรียกว่าการส่งข้อมูลโดยไม่จัดตั้งการเชื่อมต่อ (**connectionless**)

3.5.4 The application layer

แตกต่างจากเลเยอร์อื่นๆ ใน **TCP/IP model** ตรงที่สามารถเทียบได้กับ **Application layer** และ **Presentation layer** ใน **ISO/OSI Reference Model** โดย **Application layer** ใน **TCP/IP** จะบรรจุโปรโตคอลหลายแบบที่จัดให้โปรแกรมประยุกต์สามารถ **access** ระบบเครือข่ายและการให้บริการบนระบบเครือข่าย (เช่นเดียวกับ **Application layer** ใน **ISO/OSI Reference Model**) และมีมาตรฐานและวิธีในการเป็นตัวแทนของข้อมูลซึ่งสามารถรับรู้ซึ่งกันและกันได้อย่างมั่นใจ (เช่นเดียวกับ **presentation layer** ใน **ISO/OSI Reference Model**)

ถึงแม้ว่าโครงสร้าง **ISO/ISO, SNA** และ **TCP/IP** จะมีการกำหนดเลเยอร์ที่แตกต่างกัน แต่โครงสร้างเหล่านี้ก็ไม่กีดกันซึ่งกันและกัน ระบบเครือข่ายสมัยใหม่และระบบเครือข่ายสากลอาจจะต้องอาศัย **protocol** และการให้บริการที่เหมาะสมกับโครงสร้างมากกว่า **1** แบบ ตัวอย่างเช่น **LANs** ที่ใช้โปรโตคอล **TCP/IP** อาจจะใช้พื้นฐานการทำงานของระบบปฏิบัติการเครือข่ายที่ได้รับการออกแบบให้เป็นโครงสร้างแบบ **ISO/OSI Reference Model** และในอนาคตก็อาจจะมีซอฟต์แวร์และเกตเวย์ที่เหมาะสมในการแปลงข้อมูลให้สามารถสื่อสารกับระบบเครือข่ายซึ่งใช้พื้นฐานของบริษัท **IBM** ที่มีโครงสร้างแบบ **SNA**

3.6 Project 802.X

ในปี ค.ศ. **1985** สมาพันธ์คอมพิวเตอร์ของ **IEEE** ได้เริ่มโครงการเพื่อกำหนดมาตรฐานการติดต่อสื่อสารในระดับล่างระหว่างอุปกรณ์ เครื่องมือ อันหลากหลายของบริษัทต่างๆ เรียกว่า **Project 802** ทั้งนี้มิได้มีจุดมุ่งหมายที่จะยกเลิกหรือนำมาใช้แทนมาตรฐาน **OSI (Open System Interconnection)** เพียงแต่เป็นการกำหนดมาตรฐานชี้เฉพาะเจาะจงใน **Physical Layer** และ **Data Link Layer** ซึ่งเกี่ยวข้องกับการติดต่อสื่อสารของระบบเครือข่ายภายในโดยตรง สิ่งสำคัญของ **Project 802** คือ การจัดแยกการทำงานที่จำเป็นสำหรับการบริหารงานระบบเครือข่ายออกเป็นส่วนๆ เฉพาะงาน ส่วนต่างๆเหล่านี้ถูกกำหนดด้วยตัวเลขดังนี้

- **802.1** มาตรฐาน **internetworking**
- **802.2** มาตรฐานโดยทั่วไปของ **Data Link Layer** ใน **LLC sub-layer**
- **802.3** มาตรฐานโดยทั่วไปของ **Data Link Layer** ใน **MAC sub-layer** ที่ใช้การสื่อสารข้อมูลแบบ **CSMA/CD (Multiple Access with Collision Detection)**
- **802.4** กำหนด **MAC Sub-layer** สำหรับระบบเครือข่ายแบบ **Token Bus**
- **802.5** กำหนด **MAC Sub-layer** สำหรับระบบเครือข่ายแบบ **Token ring**
- **802.6** เป็นมาตรฐานของระบบเครือข่ายในเมือง **(Metropolitan Area Network – MAN)**
- **802.7** มาตรฐานสำหรับกลุ่มผู้ให้คำปรึกษาด้านเทคนิคด้าน **Broadband**
- **802.8** มาตรฐานสำหรับกลุ่มผู้ให้คำปรึกษาด้านเทคนิคด้าน **Fiber-Optic**
- **802.9** กำหนดมาตรฐานการบูรณาการระบบเครือข่าย **Voice/Data**
- **802.10** กำหนดมาตรฐานการรักษาความปลอดภัยระบบเครือข่าย
- **802.11** กำหนดมาตรฐานระบบเครือข่ายไร้สาย
- **802.12** กำหนดมาตรฐานลำดับความสำคัญในการ **access 100BaseVG-Any LAN**

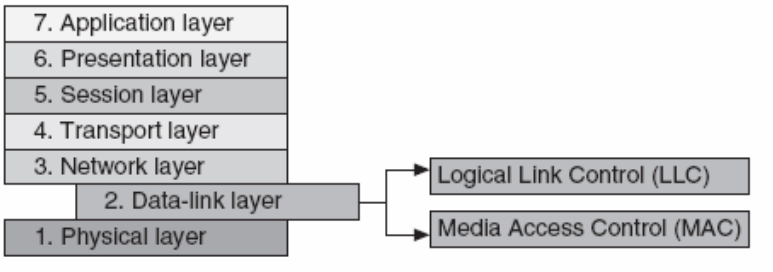
802.13 ไม่ได้ใช้

802.14 กำหนดมาตรฐานของ **Cable Modem**

802.15 กำหนดมาตรฐาน **WPAN (Wireless Personal Area Network)**

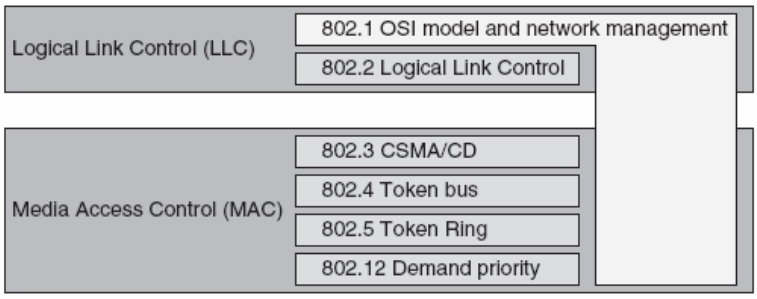
802.16 กำหนดมาตรฐานการสื่อสารไร้สายแบบ **Broadband**

Project 802 ได้แบ่ง **Data Link Layer** ออกเป็น 2 **Sub-layer** คือ **LCC (Logical Link Control)** และ **MAC (Media Access Control)** ดังแสดงตามรูปที่ **3 – 13**



รูปที่ **3 – 13** เปรียบเทียบ **Project 802** กับ **OSI**

นอกเหนือจาก **Sub-layer** ทั้งสองแล้ว **Project 802** ยังครอบคลุมถึงการควบคุมการทำงานของระบบเครือข่ายด้วย เช่นกำหนดมาตรฐานการติดต่อระหว่าง **LAN** กับ **MAN** ที่ใช้โปรโตคอลต่างกัน โดยแยกการทำงานในส่วนที่เกี่ยวข้องกับการบริหารงานระบบเครือข่ายภายในออกเป็นส่วนๆอย่างชัดเจน ดังแสดงตามรูปที่ **3 – 14**



รูปที่ **3 – 14 Project 802 Standards**

3.6.1 IEEE 802.1

802.1 เป็นส่วนหนึ่งของ **Project 802** ที่สนับสนุนการทำงานของระบบเครือข่ายที่สนับสนุนการทำงานของ **LAN** และ **WAN** โดยเฉพาะ ถึงแม้ว่าจะยังไม่สมบูรณ์ในขณะนี้แต่ก็ยังพยายามหาความแตกต่างระหว่างสถาปัตยกรรมของระบบเครือข่าย โดยที่ไม่จำเป็นต้องเปลี่ยนแปลงสิ่งที่มีอยู่แล้ว ไม่ว่าจะเป็นการกำหนดแอดเดรส (**Addressing**) การเข้าถึงกัน และการแก้ไขข้อผิดพลาดต่างๆ ที่เกิดขึ้น ก็ตาม

3.6.2 LLC (Logical Link Control) IEEE 802.2

IEEE Project 802 ใช้รูปแบบโครงสร้างของเฟรม **HDLC** และแบ่งฟังก์ชั่นการทำงานออกเป็น 2 กลุ่ม กลุ่มแรกรวบรวมการทำงานในส่วนของผู้ใช้ทั้งหมด เช่น **logical address, control information** และส่วนข้อมูล ในกลุ่มนี้ควบคุมการทำงานโดย **LCC** กำหนดให้เป็นมาตรฐาน **IEEE 802.2 LCC** ถือว่าเป็นชั้นบนในส่วน **IEEE 802** ที่ติดต่อสื่อสารใน **Data Link Layer**

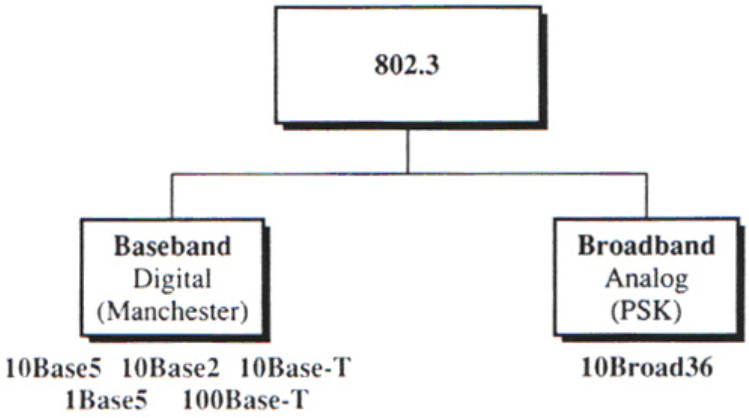
3.6.3 MAC (Media Access Control)

กลุ่มที่สองคือ **Media Access Control (MAC)** ทำหน้าที่จัดการการใช้สื่อร่วมกันของการสื่อสารข้อมูล **MAC** ประกอบด้วย **synchronization, flag, flow** และการควบคุมข้อผิดพลาดในการติดต่อสื่อสารที่อาจเกิดขึ้นโดยการเคลื่อนย้ายข้อมูลจากที่หนึ่งไปยังอีกที่หนึ่ง

3.6.4 IEEE 802.3

IEEE 802.3 รองรับการทำงานตามมาตรฐานของระบบเครือข่าย **LAN** ที่ได้รับการเริ่มต้นพัฒนาโดยบริษัท **Xerox** และต่อมาเป็นความร่วมมือระหว่างบริษัท **Digital Equipment Corporation (DEC), Intel** และ **Xerox** เรียกว่า ระบบเครือข่ายอีเธอร์เน็ต **(Ethernet)**

IEEE 802.3 แบ่งออกได้เป็น 2 ส่วนใหญ่ๆคือ **baseband** และ **boardband** ดังรูป



รูปที่ 3 – 15 IEEE 802.3

IEEE ยังแบ่งการทำงานในย่านการสื่อสารใน **baseband** ออกเป็น **5** ประเภท คือ **10Base5, 10Base2, 10Base-T, 1Base5** และ **100Base-T** (เลขตัวแรก **1, 10, 100** แสดงอัตราความเร็วในการส่งข้อมูลมีหน่วยเป็น **Mbps** และอักษรตัวสุดท้าย **2, 5, T** แสดงความยาวสูงสุดหรือประเภทของสายเคเบิล) สำหรับ **Broadband** มีการทำงานเพียงอย่างเดียวคือ **10Broad36**

3.7 IEEE 802.3 – อีเธอร์เน็ต (Ethernet)

ในปลายปี **1960** มหาวิทยาลัยฮาวายได้พัฒนา **WAN** ที่มีชื่อว่า "**ALOHA**" ซึ่งเชื่อมต่อระบบเครือข่ายข้ามทวีปขึ้นโดยใช้วิธีการ **access** แบบ **CSMA/CD** ระบบเครือข่ายนี้เป็นพื้นฐานของการพัฒนาสถาปัตยกรรมโครงสร้างแบบอีเธอร์เน็ต **(Ethernet)** ในปัจจุบัน และในปี **1972 Robert Metcalfe** และ **David Braggs** ได้วางแผนการเดินสายเคเบิลและการส่งสัญญาณข้อมูลที่ **PARC (Xerox Palo Alto Research Center)** และได้เสนอผลิตภัณฑ์อีเธอร์เน็ตขึ้นเป็นชิ้นแรกในปี **1975** ในนามของบริษัท **Xerox** ผลิตภัณฑ์นี้ได้รับการออกแบบให้มีความเร็วในการขนส่งข้อมูล **2.94 Mbps** เพื่อเชื่อมโยงเครื่องคอมพิวเตอร์ **100** เครื่องเข้าด้วยกันเป็นระยะทาง **1** กิโลเมตร จากการที่ปริษัท **Xerox** ประสบผลสำเร็จนี้จึงทำให้บริษัท **Xerox** ร่วมมือกับบริษัท **Intel Corp.** และ **Digital Corp.** ในการร่างมาตรฐานสำหรับผลิตภัณฑ์ **10-Mbps Ethernet** ซึ่งเป็นที่นิยมใช้อยู่จนถึงปัจจุบัน

3.7.1 CSMA/CD

CSMA/CD หมายถึง **Carrier Sense Multiple Access (with) Collision Detection** ซึ่งมีฟังก์ชันการทำงานบน **MAC Sub-layer** และเป็นวิธีที่โหนดของระบบเครือข่ายอีเธอร์เน็ต และ **LANs** อื่นๆ ต้องอาศัยในการ ให้ได้รับการ **access** เข้าไปยังระบบเครือข่ายเมื่อมีแพ็กเก็ตข้อมูลซึ่งจะทำการส่ง และทำให้มั่นใจว่าไม่มี 2 โหนด ที่พยายามจะทำการส่งสัญญาณข้อมูลในเวลาเดียวกัน

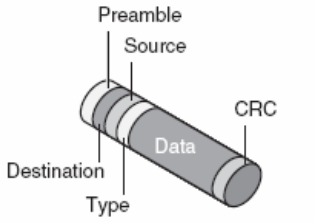
สำหรับความหมายที่แท้จริงของคำนี้ เราจะแยกอย่างไรเพื่อให้มีความหมายในด้านเทคโนโลยีและง่ายต่อการจำ ส่วนแรก **Carrier Sense** หมายความว่า โหนดบนระบบเครือข่ายจะเฝ้าฟังสัญญาณที่เป็นพาหะบนสายสื่อสารที่บ่งชี้ว่าระบบเครือข่ายไม่ว่าง ส่วนต่อไป **Multiple Access** หมายความว่าอาจจะมีมากกว่า **1** โหนด ที่ต้องการส่งสัญญาณข้อมูลในเวลาเดียวกัน ซึ่งในความเป็นจริงในกรณีนี้ ถ้ามี 2 โหนด ทำการส่งสัญญาณข้อมูลอย่างต่อเนื่อง แต่ละโหนดจะต้องอาศัยวิธี **Collision Detection** ในการตกลงใจในเหตุการณ์นั้นๆ

ในทางปฏิบัติ **CSMA/CD** จะทำให้ระบบเครือข่ายเป็นเหมือนบางสิ่งที่เหมือนกับคู่สนทนาทางโทรศัพท์ ที่ซึ่งทุกโหนดจะเปรียบได้กับบุคคลที่ต้องการ (หรือรอคอย) จะเข้ามามีส่วนร่วม เช่นเดียวกับการสนทนาทางโทรศัพท์ การส่งสัญญาณข้อมูลจะเดินทางไปทั้งสองทิศทาง และเช่นเดียวกับความอยากรู้อยากเห็นของเพื่อนบ้านในสายโทรศัพท์ ทุกโหนดจะเฝ้าฟังสัญญาณที่เป็นพาหะตัวนำอยู่ตลอดเวลา เมื่อโหนดหนึ่งมีบางสิ่งที่ต้องการจะส่ง ก็จะรอจนกว่าสายสื่อสารจะว่าง หมายความว่าจะไม่รู้สึกว่ามีสัญญาณพาหะตัวนำ ในเวลานั้น โหนดนั้นก็จะใส่การส่งสัญญาณข้อมูลของตนเองเข้าไปบนสายเคเบิล ถ้าโหนดนั้นเป็นเพียงโหนดเดียวที่ทำการส่งสัญญาณข้อมูลในเวลานั้น ทุกอย่างก็จะเป็นไปด้วยความเรียบร้อยและโหนดอื่นก็จะรอจนกว่าการส่งสัญญาณนั้นไปถึงปลายทางก่อนที่จะพยายามส่งข้อมูลใดๆ ของตนเอง ในบางครั้งอาจจะมี 2 โหนด ที่คิดว่าสายสื่อสารว่างในเวลาเดียวกันและพยายามที่จะส่งสัญญาณข้อมูลเหมือนกับการที่มีคน 2 คนในคู่สนทนาอาจจะเริ่มพูดพร้อมกันในขณะที่สายโทรศัพท์ว่างชั่วคราว เมื่อเกิดเหตุการณ์เช่นนี้ขึ้นบนระบบเครือข่าย **CSMA/CD** ผลก็คือข้อมูลจะเกิดการปะทะกันซึ่งทำให้การกระทำทุกอย่างหยุดลงและข้อมูลก็จะไม่มีคุณภาพ ในระบบเครือข่ายถ้าโหนดสามารถที่จะตรวจพบเหตุการณ์เช่นนี้และแปลความหมายได้ว่าเป็นการเกิดข้อมูลชนกัน แต่ละโหนดก็จะยกเลิกการส่งสัญญาณข้อมูลของตนเอง (เช่นเดียวกับการพูดว่า **oops** หรือพูดว่าขอโทษ) และโหนดทั้งคู่ก็จะถอยหลังกลับไปในช่วงเวลาแล้วแต่จะสุ่ม ก่อนที่จะพยายาม **access** เข้าไปยังระบบเครือข่ายอีกเพื่อทำการส่งสัญญาณข้อมูล ช่วงเวลาที่โหนดรอนี้เรียกว่า **deferral time** ซึ่งเป็นเวลาที่โหนดทั้งคู่ต้องเสียไปในการถอยกลับไปในช่วงระยะเวลาที่แตกต่างกันและจากนั้นโหนดใดโหนดหนึ่งก็จะสามารถที่จะทำการส่งได้อย่างสมบูรณ์ในการส่งครั้งที่สอง

ถึงแม้ว่า **CSMA/CD** จะฟังดูเหมือนต้องเป็นปากเสียงกันทั้งหมด และเป็นวิธีที่ซุ่มซ่ามในการจัดระเบียบการส่งสัญญาณในระบบเครือข่าย แต่ก็ได้ผลเมื่อสามารถควบคุมปริมาณผู้ใช้งานระบบเครือข่ายอีเธอร์เน็ต เมื่อวิธีการ **access** และการควบคุมทำงานได้ดีบนระบบเครือข่าย โดยไม่ต้องรับภาระในการขนส่งข้อมูลเป็นจำนวนมาก หรือการส่งสัญญาณขนาดเล็กหลายสัญญาณ จะต้องมีบางสิ่งที่รับผิดชอบสำหรับการชนกันของข้อมูล ในระบบเครือข่ายที่ยุ่งอยู่ตลอดเวลาจากการที่โหนดจำนวนมากทำการแลกเปลี่ยนแพ็กเก็ตข้อมูลจำนวนมาก ซึ่งก็อาจจะเพิ่มความน่าจะเป็นในการเกิดการชนกันของข้อมูล การที่สามารถตรวจพบและหลีกเลี่ยงการส่งสัญญาณข้อมูลในลักษณะนี้จะทำให้ระบบเครือข่ายทำงานช้าลง

3.7.2 คุณลักษณะของอีเธอร์เน็ต

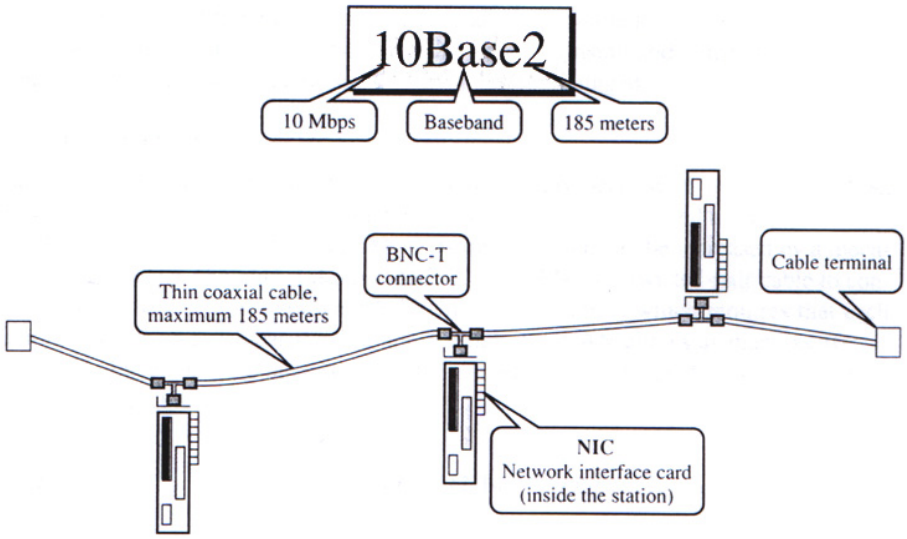
ในอดีต 4 – 5 ปีที่ผ่านมาสถาปัตยกรรมโครงสร้างระบบเครือข่ายแบบอีเธอร์เน็ตเป็นที่นิยมใช้อย่างแพร่หลายทั้ง **Topology** แบบบัส (**Bus**) และแบบดาว (**Star**) โดยส่งสัญญาณข้อมูลได้ด้วยความเร็ว **10 Mbps** โดยใช้เทคโนโลยี **CSMA/CD** ในการขนส่งข้อมูล และข้อมูลในเครือข่ายอีเธอร์เน็ตจะถูกแบ่งออกเป็นเฟรม (**Frame**) ที่มีความยาวระหว่าง **64 – 1518** ไบต์ โดยจะมีข้อมูล **18** ไบต์ที่เป็นส่วนของอีเธอร์เน็ต ดังนั้นข้อมูลจริงจะมีความยาวเพียง **46 – 1500** ไบต์ ดังแสดงตามรูปที่ **3 – 16** โดย **Preamble** เป็นส่วนที่ทำสัญลักษณ์แสดงว่าเป็นส่วนต้นของเฟรม **Source, Destination** คือ แอดเดรสต้นทางและปลายทาง ที่ใช้ในการระบุ **Network layer protocol (IP** หรือ **IPX)** และ **CRC(Cyclic Redundancy Check)** เป็นข้อมูลสำหรับตรวจสอบความถูกต้องของข้อมูล สถาปัตยกรรมโครงสร้างระบบเครือข่ายแบบอีเธอร์เน็ตตามมาตรฐาน **Project 802.x** จะมีอยู่ **3** แบบคือ **10Base2, 10Base5** และ **10BaseT**



รูปที่ **3 – 16 Ethernet II Frame**

3.7.3 10Base2 : Thin Ethernet

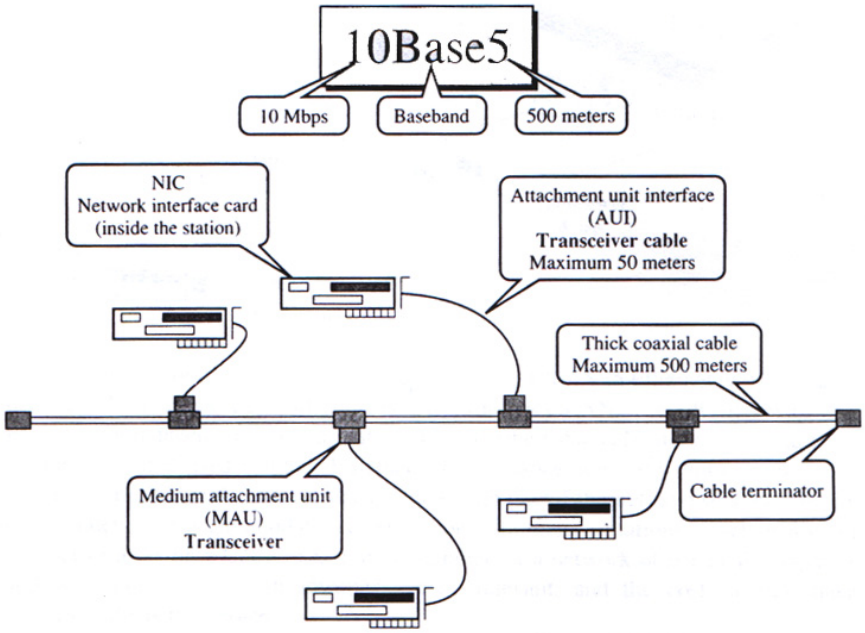
เรียกอีกอย่างหนึ่งว่า **Thin-Net** เป็นมาตรฐานของ **IEEE Project 802** ซึ่งอธิบายชนิดของสายที่ใช้ในการเชื่อมต่อระบบเครือข่ายภายในโดยใช้สายสัญญาณโคแอ็กเชียลแบบ **Thinnet** หมายความว่าสามารถรองรับการรับส่งข้อมูลได้ **10 Mbps** ในย่าน **Baseband** ใช้ในการเชื่อมต่อแบบ **Bus** โดยมีความห่างของแต่ละเซ็กเมนต์ไม่เกิน **500** เมตร ออกแบบให้มีราคาถูกกว่าแบบแรกและง่ายต่อการติดตั้งเพราะใช้สายขนาดเล็กกว่า



รูปที่ **3 – 17 10Base2 topology**

3.7.4 10Base5 : Thick Ethernet

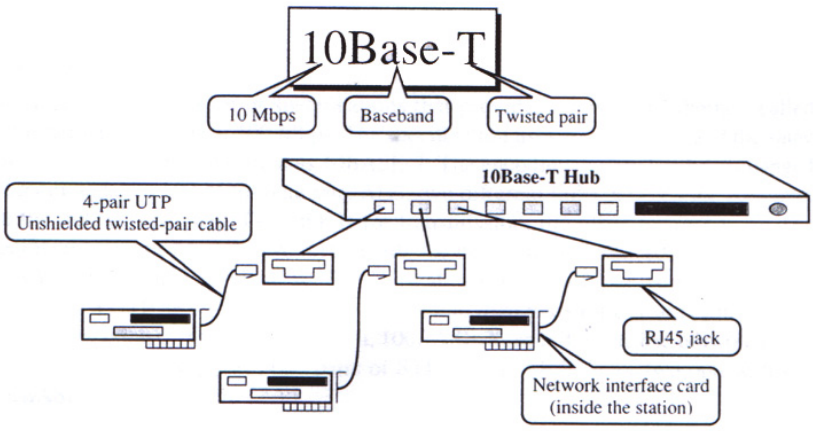
เรียกอีกอย่างหนึ่งว่า **Thick-Net** เป็นมาตรฐานของ **IEEE Project 802** ซึ่งอธิบายชนิดของสายที่ใช้ในการเชื่อมต่อระบบเครือข่ายภายในโดยใช้สายสัญญาณโคแอ็กเชียลแบบ **Thicknet** หมายความว่าสามารถรองรับการรับส่งข้อมูลได้ **10 Mbps** ในย่าน **Baseband** ใช้ในการเชื่อมต่อแบบ **Bus** โดยมีความห่างของแต่ละ **Segment** ไม่เกิน **500** เมตร และไม่ควรมีเกิน **5** เซ็กเมนต์ นั่นคือถ้าแต่ละเครื่องตั้งห่างกัน **2.5** เมตร จะทำให้สามารถมีเครื่องในระบบเครือข่ายได้ **1000** เครื่อง (**200** เครื่องต่อเซ็กเมนต์)



รูปที่ **3 – 18 10Base5 topology**

3.7.5 10Base-T : Twist-Pair Ethernet

เป็นสายที่เป็นที่นิยมในปัจจุบัน ถือว่าเป็นมาตรฐานของ **IEEE 802.3** ซึ่งอธิบายชนิดของสายที่ใช้ในการเชื่อมต่อระบบเครือข่ายภายในโดยใช้สายสัญญาณแบบ **Unshielded Twisted-Pair (UTP)** หมายความว่าสามารถรองรับการรับส่งข้อมูลได้ **10 Mbps** ในย่าน **Baseband** ใช้ในการเชื่อมต่อแบบดาว **(Star)** โดยมีระยะห่างระหว่างฮับกับเครื่องคอมพิวเตอร์ได้ไม่เกิน **100** เมตร



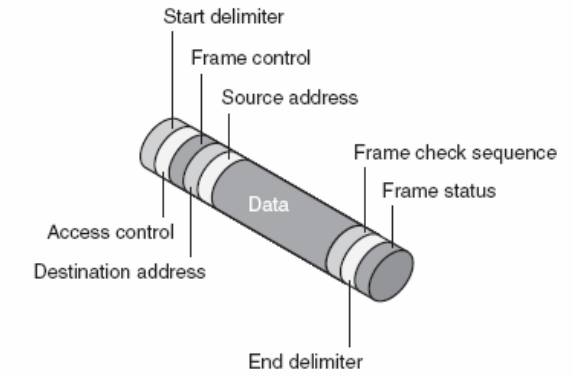
รูปที่ **3 – 19 10BaseT topology**

3.7.6 มาตรฐาน IEEE 100 Mbps

มาตรฐานใหม่ของอีเธอร์เน็ตกำลังผลักดันข้อจำกัดแบบเดิมให้สามารถขนส่งข้อมูลได้ด้วยความเร็วมากกว่า **10 Mbps** เพื่อรองรับการใช้งานโปรแกรมประยุกต์ที่ต้องการช่องสัญญาณข้อมูลมาก **(High Bandwidth)** เช่นโปรแกรมประเภท **CAD/CAM (Computer Aid Design/Computer Aid Manufacturing)** และการส่งสัญญาณภาพและเสียงในลักษณะมัลติมีเดีย **(Multimedia)** มาตรฐานเหล่านี้ได้แก่ **100BaseVG-AnyLAN** และ **100BaseTx** (หรือที่เรียกว่า **Fast Ethernet**) ที่สามารถใช้โครงสร้างพื้นฐานของระบบเครือข่ายอีเธอร์เน็ตเดิมได้ โดยเปลี่ยนเฉพาะสายสัญญาณและอุปกรณ์ระบบเครือข่ายเท่านั้น เช่น **100BaseT4** จะใช้สาย **UTP Cat4** และ **Cat5** ส่วน **100BaseFx** จะใช้สายเคเบิลใยแก้วนำแสง **(Fiber Optic)** เป็นต้น

3.8 IEEE 802.5 – โทเก้นริง (Token Ring)

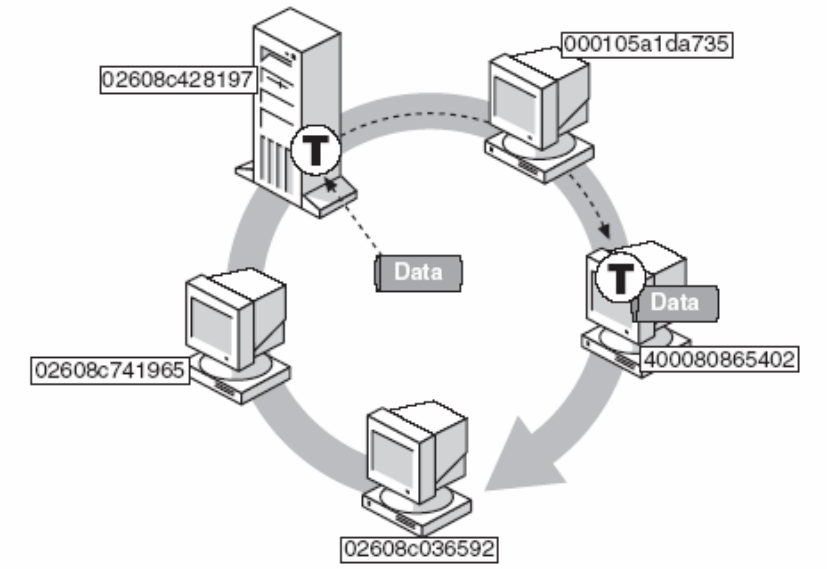
สถาปัตยกรรมโครงสร้างแบบโทเก้นริงได้ถูกพัฒนาขึ้นมาครั้งแรกในปี **1980** โดยบริษัท **IBM** ซึ่งมีลักษณะการเชื่อมต่อแบบดาว **(Star)** โดยมีเครื่องคอมพิวเตอร์เมนเฟรม หรือมินิคอมพิวเตอร์เป็นศูนย์กลาง ระบบเครือข่ายโทเก้นริงเป็นการดำเนินงานตามมาตรฐาน **IEEE 802.5** ซึ่งใช้วิธีการ **Token Passing** ในการ **access** ข้อมูล ดังนั้นการส่งข้อมูลทางตรรกะจึงทำในลักษณะวงแหวนด้วยความสามารถของฮับที่ใช้ จึงมีชื่อเรียกว่า **"Token Ring"** สำหรับรูปแบบของเฟรมข้อมูลพื้นฐานแสดงตามรูปที่ **3 – 20**



รูปที่ **3 – 20 Data Frame** ของ **Token Ring**

- **Start delimiter** เป็นสัญลักษณ์แสดงจุดเริ่มต้นของเฟรมข้อมูล
- **Access control** เป็นส่วนแสดงสิทธิก่อน-หลังของเฟรมข้อมูล
- **Frame control** บรรจุข้อมูลเกี่ยวกับ **Media Access Control** เพื่อให้เครื่องคอมพิวเตอร์เพียงเครื่องเดียวเท่านั้นที่สามารถ **access** เฟรมข้อมูลได้
- **Destination Address** ระบุแอดเดรสของเครื่องคอมพิวเตอร์ที่รับเฟรม
- **Source Address** ระบุแอดเดรสของเครื่องคอมพิวเตอร์ที่ส่งเฟรม
- **Data** ส่วนที่เป็นข้อมูลดิบ
- **Frame check sequence** บรรจุข้อมูล **CRC** สำหรับตรวจสอบการจัดลำดับการเรียงข้อมูล
- **End delimiter** เป็นสัญลักษณ์แสดงส่วนท้ายของเฟรม
- **Frame status** บอกให้ทราบสถานะของเฟรมว่าถูกคัดลอกไปแล้วหรือไม่

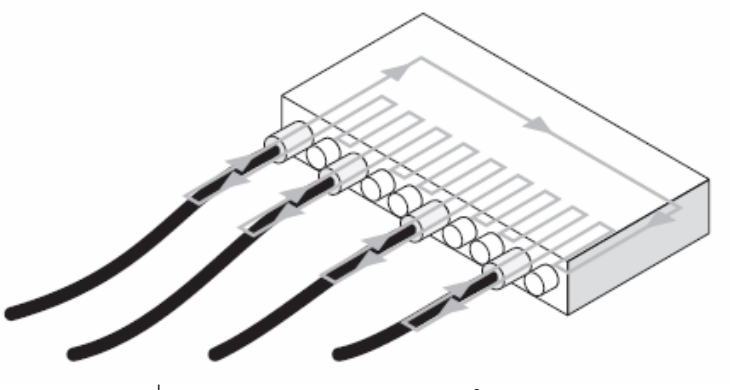
สำหรับการทำงานของระบบเครือข่ายโทเก้นริงเป็นดังนี้ เมื่อคอมพิวเตอร์ในโทเก้นริงเครื่องแรกเริ่มออนไลน์ ระบบเครือข่ายจะสร้างโทเก้น (**Token**) ให้กับเครื่องคอมพิวเตอร์นั้น และส่งให้ออกเดินทางไปรอบๆ วงแหวน เมื่อต้องการส่งข้อมูลให้กับเครื่องคอมพิวเตอร์เครื่องใด เครื่องคอมพิวเตอร์เครื่องนั้นจะทำการจับโทเก้นของเครื่องคอมพิวเตอร์ที่ต้องการส่งข้อมูลเอาไว้ จากนั้นคอมพิวเตอร์เครื่องส่งจะทำการส่งเฟรมข้อมูลส่งออกไปยังเครื่องคอมพิวเตอร์ผู้รับเครื่องนั้น เครื่องคอมพิวเตอร์ผู้รับจะทำการคัดลอกข้อมูลออกไป และอัพเดท **Frame Status** แล้วปล่อยโทเก้นให้เดินทางต่อไปในวงแหวน เมื่อคอมพิวเตอร์ผู้ส่งได้รับทราบว่าข้อมูลถูกคัดลอกไปแล้วจะทำการเก็บเฟรมข้อมูลเข้ามา และส่งโทเก้นอันใหม่ออกไปในวงแหวน ดังแสดงตามรูปที่ **3 – 21**



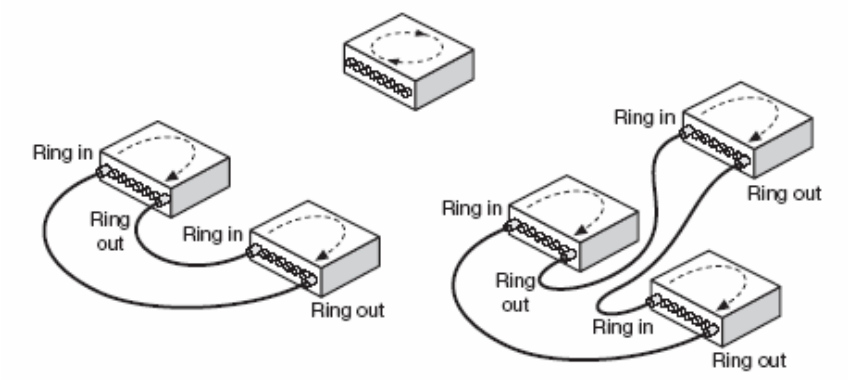
รูปที่ **3 – 21** การไหลตามเข็มนาฬิกาของโทเก้นไปรอบ **Logical Ring**

จะเห็นได้ว่าหลักการสำคัญในการทำงานของระบบเครือข่ายแบบโทเก้นริง คือการเฝ้าตรวจระบบเครือข่ายเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายจะได้รับมอบโทเก้นของตนเอง การตรวจสอบอย่างแรกคือจะมีเพียงโทเก้น **1** อันเท่านั้นที่ทำงานอยู่บนระบบเครือข่าย และการเดินทางของโทเก้นจะมีทิศทางเดียวกัน มาตรฐาน **802.5** กำหนดให้มีการเดินทางในทิศทางตามเข็มนาฬิกา กระบวนการตรวจสอบที่เรียกว่า "**Beaconing**" จะทำโดยเครื่องคอมพิวเตอร์แต่ละเครื่องทำการส่ง **Beacon announcement** ออกไปบนวงแหวนทุกๆ **7** วินาที ถ้าเครื่องคอมพิวเตอร์เครื่องนั้นไม่ได้รับ **Beacon** กลับมาแสดงว่าระบบถูกตัดการเชื่อมต่อ ทำให้ข้อมูลไม่สามารถเดินทางครบรอบได้ ซึ่งจะทำให้ระบบเครือข่ายแบบนี้ล่ม นอกจากนั้นเครื่องคอมพิวเตอร์แต่ละเครื่องยังต้องทำการเฝ้าตรวจโทเก้นในระบบเครือข่ายด้วยว่ามีโทเก้นใดที่ระบุแอดเดรสของตนเองเพื่อร้องขอการส่งข้อมูล

สำหรับฮับที่ใช้ในระบบเครือข่ายโทเก้นริงจะมีชื่อเรียกว่า **MAU** หรือ **MSAU (Multi Station Access Unit)** และ **SMAU (Smart Multi Station Access Unit)** ซึ่งมีการเชื่อมต่อสายภายในให้มีการหมุนเวียนโทเก้นในทิศทางตามเข็มนาฬิกา และเมื่อมีการเชื่อมต่อเข้ากับเครื่องคอมพิวเตอร์ในแต่ละจุดวงแหวนภายใน (**Inner Ring**) จะเปลี่ยนเป็นวงแหวนภายนอก (**Outer Ring**) โดยอัตโนมัติ ดังแสดงตามรูปที่ **3 – 22** สำหรับ **MAU** ของบริษัท **IBM** จะมีพอร์ตเชื่อมต่อ **10** พอร์ต และในระบบเครือข่ายสามารถเชื่อมต่อฮับได้มากถึง **33** ตัว ซึ่งในการขยายระบบเครือข่ายสามารถทำได้โดยใช้พอร์ต **Ring IN** และ **Ring OUT** ดังแสดงตามรูปที่ **3 – 23**



รูปที่ 3 – 22 การสร้างวงแหวนภายใน MAU

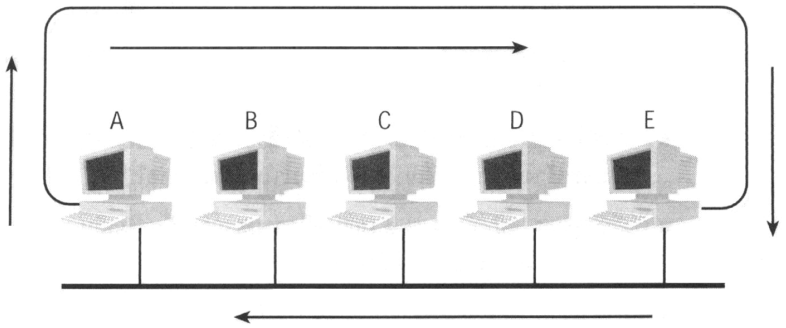


รูปที่ 3 – 23 การเพิ่ม MAU เพื่อขยายระบบเครือข่าย

3.9 IEEE 802.4 – ArcNet

บริษัท Data Point Corporation ได้พัฒนาโครงสร้างสถาปัตยกรรม ArcNet (Attached Resource Computer Network) ขึ้นในปี 1977 สำหรับจัดตั้งระบบเครือข่ายแบบเวิร์คกรุ๊ป (Workgroup) โดยมีการเชื่อมโยงแบบดาว (Star) การ์ดเชื่อมต่อระบบเครือข่าย ArcNet ได้มีการจดทะเบียนและผลิตออกขายตั้งแต่ปี 1983 ก่อนที่จะเริ่มมีมาตรฐาน IEEE 802 อย่างไรก็ตามโครงสร้างนี้จะมีความใกล้เคียงกับมาตรฐาน 802.4 โทเก้นบัส (Token Bus) ซึ่งใช้สายเคเบิลแบบ Broadband

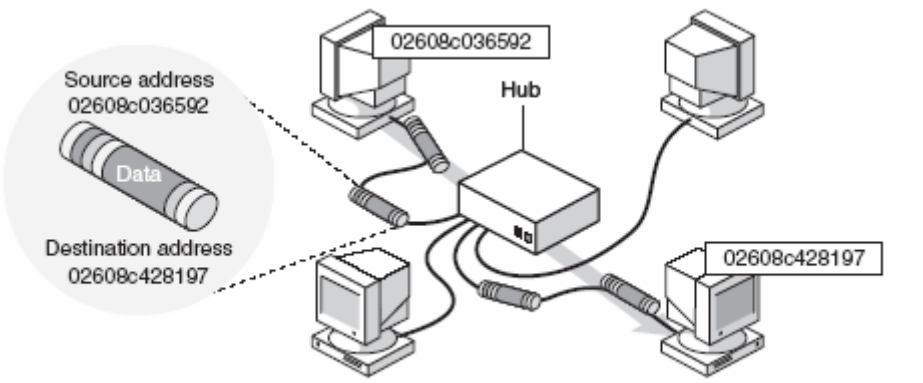
ในการ access ข้อมูล ArcNet ใช้วิธีการ Token Passing เครื่องคอมพิวเตอร์ในระบบเครือข่ายจะต้องมีโทเก้นสำหรับการส่งข้อมูล ข้อมูลจากเครื่องคอมพิวเตอร์ผู้ส่งจะถูกส่งผ่านเครื่องคอมพิวเตอร์เครื่องอื่นในระบบไปยังเครื่องคอมพิวเตอร์ผู้รับตามลำดับการเชื่อมโยง ดังแสดงตามรูปที่ 3 – 24



รูปที่ 3 – 24 สถาปัตยกรรมระบบเครือข่าย ArcNet แบบ Token Bus

Token Passing แตกต่างจากวิธี **CSMA/CD** ที่ใช้การช่วงชิง หมายความว่าผู้ใดก็ได้ที่ไปถึงที่นั่นเป็นคนแรก เพื่อให้ได้มาซึ่งการ **access** เข้าไปยังระบบเครือข่าย ระบบเครือข่ายซึ่งใช้วิธี **token passing** ในการส่งข้อมูลจะอาศัยการประสานงานกันมากขึ้นในวิธีการพิจารณา (หมายความว่าทุกคนมีโอกาสที่จะได้เล่น) ซึ่งทุกโหนดจะมีบทบาทในการจัดการการ **access** และหลีกเลี่ยงการเกิดข้อมูลปะทะกัน หัวใจสำคัญของวิธีการ **access** แบบนี้คือการใช้ เฟรมข้อมูลชนิดพิเศษที่มีขนาดเล็กเพียง **2-3** ไบต์ ที่เรียกว่า "โทเก้น **(token)**"

โทเก้น คือเฟรมพิเศษซึ่งมีเพียงอันเดียวบนระบบเครือข่ายในช่วงระยะเวลาหนึ่ง ซึ่งมีลักษณะเป็นท่อนสำหรับการถ่ายทอดลักษณะ และจะถูกส่งผ่านจากโหนดหนึ่งไปยังอีกโหนดหนึ่งในระบบเครือข่าย และจะเคลื่อนที่ไปในทิศทางเดียวตามลำดับที่กำหนดไว้ล่วงหน้าในรูปแบบของวงแหวนทางตรรกะ ในความเป็นจริงแล้วฟังก์ชันการทำงานของโทเก้นนับว่าเป็นจุดวิกฤตในการรักษาลำดับการจัดเรียงของโหนดบนระบบเครือข่าย เพราะว่าจะมีโหนดที่เก็บโทเก้นไว้เพียงโหนดเดียวที่ได้รับการอนุญาตให้ทำการส่งสัญญาณข้อมูล และเพื่อให้เกิดความเท่าเทียมกันระหว่างโหนดต่างๆ ในระบบเครือข่าย ดังนั้นโหนดที่เก็บโทเก้นไว้จะสามารถส่งข้อมูลได้เพียงแพ็กเก็ตเดียว ก่อนที่จะต้องส่งผ่านโทเก้นไปยังโหนดถัดไป สำหรับแพ็กเก็ตข้อมูลของระบบเครือข่าย **ArcNet** ประกอบด้วยแอดเดรสต้นทาง แอดเดรสปลายทาง และส่วนข้อมูล ดังแสดงตามรูปที่ **3 – 25**



รูปที่ **3 – 25** เส้นทางการเดินทางของโทเก้นบนระบบเครือข่าย **ArcNet**

ในทางปฏิบัติ ถ้าระบบเครือข่ายเงียบมากและไม่มีโหนดใดมีข้อมูลที่จะทำการส่งโทเก้นก็จะเคลื่อนที่รอบๆ วงแหวนไปเรื่อยๆ ในทางตรงกันข้ามถ้ามีโหนดใดโหนดหนึ่งมีข้อมูลที่จะทำการส่งก็จะรอจนกว่าจะได้รับโทเก้น แล้วก็จะนำโทเก้นออกจากการหมุนเวียนโดยการทำเครื่องหมายว่า "**busy**" ติดเข้าไปกับแพ็กเก็ตข้อมูล แล้วจึงส่งผ่านโทเก้นและเฟรมข้อมูลไปยังโหนดถัดไป ที่โหนดนี้จะรับทราบว่าโทเก้นไม่ว่างก็จะส่งผ่านข้อมูลไปยังโหนดต่อไป ซึ่งทำเช่นเดียวกันและเมื่อส่งต่อไปจนกระทั่งแพ็กเก็ตข้อมูลไปถึงเครื่องผู้รับที่ตั้งใจ ที่จุดนั้นเครื่องผู้รับจะแยกข้อมูลออกจากเฟรม ทำเครื่องหมายที่เฟรมว่าได้รับข้อมูลแล้ว และส่งต่อออกไป เมื่อเครื่องผู้ส่งได้รับเฟรมนั้นอีกครั้ง ก็จะตรวจสอบว่าข้อมูลได้รับแล้ว และทำเครื่องหมายว่า "**available for use**" และส่งออกไปยังโหนดถัดไป ถ้าโหนดนั้นมีข้อมูลที่จะทำการส่งก็จะทำกระบวนการทำเครื่องหมายโทเก้นว่า "**busy**" ส่งข้อมูล และรอเฟรมนั้นกลับมาด้วยเครื่องหมายการตอบรับว่าได้รับข้อมูลแล้ว และก็ส่งโทเก้นออกไปใหม่ ด้วยวิธีนี้แต่ละโหนดจะได้รับโอกาสในการส่งข้อมูลอย่างเท่าเทียมกันเมื่อใดก็ตามที่ได้รับโทเก้น และเนื่องจากจะมีเพียงโหนดเดียวที่เก็บโทเก้นไว้ ระบบเครือข่ายก็จะสามารถหลีกเลี่ยงการเกิดข้อมูลชนกันได้

สำหรับสายเชื่อมต่อมาตรฐานของระบบเครือข่าย **ArcNet** คือสายโคแอ็ก **RG-62 A/U 93Ω** อย่างไรก็ตาม โครงสร้างระบบเครือข่ายแบบนี้ยังสามารถสนับสนุนการใช้สายสัญญาณแบบสายคู่ตีเกลียวและเคเบิลใยแก้วนำแสงได้ ดังนั้นระยะห่างระหว่างเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายจึงขึ้นอยู่กับความสามารถของสายสัญญาณที่ใช้ การใช้สายโคแอ็กเชียล หัวต่อเชื่อม **BNC** และ **Active HUB** จะสามารถส่งข้อมูลต่อไปได้ไกลถึง **2000** ฟุต (**610** เมตร) ในขณะที่การใช้สาย **UTP** จะสามารถส่งข้อมูลต่อไปได้ไกลเพียง **800** ฟุต (**244** เมตร)

ในคุณลักษณะเฉพาะของ **IEEE token-passing** ถึงแม้ว่าคุณลักษณะเฉพาะ **IEEE 802.4 Token Bus** จะมีหมายเลขก่อนหน้าคุณลักษณะเฉพาะ **Token Ring (802.5)** แต่คุณจะได้พบกับระบบเครือข่ายโทเก้นริงก่อนเพราะว่าเป็นระบบเครือข่ายที่ใช้เป็นส่วนใหญ่ในระบบเครือข่ายที่ใช้เครื่อง **PC** เป็นพื้นฐาน

3.10 Isochronous Network – IEEE 802.9

คำว่า **isochronous** ตามพจนานุกรมของ **Webster** มาจากภาษากรีกว่า **isochronos – iso** แปลว่าเท่ากัน (**equal**) และ **chronos** แปลว่าเวลา (**time**) ในเรื่องของระบบเครือข่ายก็จะมีความหมายว่า **LANs** เหล่านี้มีผลกระทบต่อเวลา ในคุณลักษณะเฉพาะ **IEEE 802.9** คำว่า **isochronous** จะกล่าวถึง การรวมกันของเทคโนโลยี **ISDN (integrated Services Digital Network)** กับเทคโนโลยี **LAN** โดยเฉพาะอย่างยิ่งใน **physical layer** และ **LLC/MAC sub-layers**

Isochronous LANs โดยทั่วไปจึงถูกกล่าวถึงว่าเป็น **Integrated Services LAN (ISLAN)** ซึ่งมีจุดมุ่งหมายที่ทำให้ระบบเครือข่ายมีความสามารถในการส่งข้อมูลประเภทมัลติมีเดีย คุณลักษณะเฉพาะนี้เริ่มที่ คณะวิจัยของ **IEEE** เริ่มสำรวจเกี่ยวกับเรื่อง **Integrated Voice/Data (IVD)** ในกลางยุคปี **1980s** งานนี้รวมถึงการพัฒนามาตรฐานการรวมสัญญาณข้อมูลในสายคู่ตีเกลียวแบบไม่มีสิ่งห่อหุ้ม (**UTP**) ที่ทำให้เกิดเป็นคุณลักษณะเฉพาะ **IEEE 802** ที่ **MAC sublayer** และมาตรฐาน **ISDN** ที่กำหนดโดย **CCITT (CCITT** หมายถึงองค์กรชื่อว่า **Comite' Consultatif International Te'le'graphique et Te'le'phonique** ซึ่งในที่สุดก็เข้าสมทบกับหน่วยงานกำหนดมาตรฐานที่เรียกว่า **International Telecommunications Union-Telecommunication Standardization Sector** หรือ **ITU)** ในที่สุดความพยายามนี้ก็ได้รับการรับรองจาก **IEEE** ในปี **1993** และได้รับการเปลี่ยนชื่อเป็น **Integrated Services LAN (ISLAN)**

คุณลักษณะเฉพาะของ **ISLAN** ได้ถูกทบทวนโดยการรวบรวมอุปกรณ์ที่เรียกว่าเป็น **Integrated Services Terminal Equipment (ISTEs)** หากไม่คำนึงถึงบางสิ่งที่ทำให้เป็นไปไม่ได้ **ISTE** ก็เป็นเพียงชื่อโดยทั่วไปที่ใช้เรียกอุปกรณ์ที่เกี่ยวข้องกับมัลติมีเดีย ตัวอย่างเช่น โทรศัพท์ (**voice TE**) และเครื่องคอมพิวเตอร์ (**data TE**) คุณลักษณะเฉพาะนี้อธิบายโดยใช้ **topology** แบบดาว ซึ่งมีอุปกรณ์เหล่านี้ เชื่อมต่อเข้ากับ **Access Unit (AE)** และต่อเชื่อมเข้ากับ **backbone** ของระบบเครือข่ายผ่านทางสายคู่ตีเกลียว

ในเรื่องของเทคโนโลยี **ISDN** นั้น **IEEE 802.9** สามารถสนับสนุนได้ทั้ง **Basic Rate Interface (BRI) ISDN** และ **Primary Rate Interface (PRI) ISDN** (จะอธิบายในรายละเอียดต่อไปในภายหลัง) **ISDN** เป็นวิธีการจัดส่งข้อมูลหลายประเภท (เสียง ข้อมูล สัญญาณภาพ) ในรูปแบบดิจิตอลผ่านทางสายโทรศัพท์มาตรฐาน ลักษณะเด่นอย่างหนึ่งของ **ISDN** คือมีการจัดแบ่งสัญญาณข้อมูลออกเป็นช่องสัญญาณ (**channel**) **2** ประเภท คือ **B channel** และ **D channel** โดยที่ **B channel** จะนำข้อมูลด้วยความเร็ว **64 Kbps** และ **D channel** จะนำข้อมูล

และข่าวสารการควบคุมต่างๆ ด้วยความเร็ว **16 Kbps** รูปแบบของ **ISDN** ที่เรียกว่า **BRI** จะมี **B channel 2** ช่องสัญญาณ และ **D channel 1** ช่องสัญญาณ และในรูปแบบที่ราคาแพงกว่า ซึ่งเรียกว่า **PRI** จะมี **B channel 23** ช่องสัญญาณ (ในสหรัฐอเมริกา และญี่ปุ่น) หรือ **30** ช่องสัญญาณ (ในยุโรป) และมี **D channel 1** ช่องสัญญาณ และนี่คือความหมายและเหตุผลในการเรียก **IEEE 802.9** ว่า **Isochronous** ที่นี้ให้ลองคิดว่า ข้อมูล เช่นข้อความสามารถที่จะทำการส่งเป็นพักๆ อย่างฉับพลันในรูปแบบของแพ็กเก็ต ซึ่งถูกนำมาประกอบขึ้นใหม่ที่ปลายทางได้อย่างราบเรียบ แต่การกระทำในลักษณะนี้จะไม่เป็นความจริงสำหรับข้อมูลที่เป็นมัลติมีเดีย ที่ประกอบด้วยสัญญาณเสียงและสัญญาณภาพ ซึ่งสัญญาณทั้งคู่จะต้องได้รับการจัดส่งอย่างราบเรียบในช่วงเวลาที่แน่นอน ตัวอย่างเช่น สัญญาณภาพจะต้องได้รับการจัดส่งไปด้วยจำนวนเฟรมที่แน่นอนในเวลา **1** วินาที ถ้าการจัดส่งสัญญาณถูกขัดขวางหรือการส่งเฟรมไปถึงเมื่อใดก็ได้ตามใจชอบ การส่งสัญญาณข้อมูลนั้นจะถูกทำให้บิดเบือนไปและไม่สามารถที่จะมองเป็นภาพได้ เหตุการณ์เช่นเดียวกันก็เป็นความจริงสำหรับสัญญาณเสียง ซึ่งอาจกล่าวอีกอย่างหนึ่งได้ว่า สัญญาณเสียง **(audio)** และสัญญาณภาพ **(video)** จะขึ้นอยู่กับช่วงจังหวะเวลา และระบบเครือข่ายก็จะต้องสนับสนุนตามความต้องการนี้ จึงต้องเป็น **Isochronous**

3.11 IEEE 802.11 – ระบบเครือข่ายไร้สาย (Wireless Network)

การกล่าวถึงระบบเครือข่ายไร้สาย **(Wireless LAN)** หรือการเชื่อมต่อ **LAN** ที่อาจจะยากที่จะเข้าใจบ้างเล็กน้อย ซึ่งอาจจะกล่าวถึงเครื่องคอมพิวเตอร์แบบกระเป๋าหิ้วที่มีการ์ดเชื่อมต่อระบบเครือข่ายที่ส่งสัญญาณทางวิทยุ ไปยัง **access point** ที่รับสัญญาณวิทยุได้ และเชื่อมต่อกับระบบเครือข่ายที่ใช้สายเคเบิลแบบมาตรฐาน ในสถานการณ์การสื่อสารแบบผสมเช่นนี้ คือการสื่อสารซึ่งกันและกันระหว่างอุปกรณ์ไร้สายกับอุปกรณ์ที่ใช้สายเคเบิลเชื่อมต่อ ในทางตรงกันข้ามการอ้างถึงระบบเครือข่ายไร้สายตามจริงแล้วอาจจะกล่าวถึง **LAN** ที่ไม่มีการใช้สายเคเบิลในการเชื่อมต่อ ซึ่งคือระบบเครือข่ายประเภทที่จะอธิบายที่นี้ ซึ่งเป็นโครงสร้างตามคุณลักษณะเฉพาะของ **IEEE 802.11**

คุณลักษณะเฉพาะของ **IEEE 802.11** กำหนดระบบเครือข่ายไร้สายที่เทียบเคียงได้กับระบบเครือข่ายอีเธอร์เน็ต ที่ **LANs** เหล่านี้จะอาศัยเทคนิคที่มีความสัมพันธ์กับ **CSMA/CD** สำหรับการ **access** เข้าไปยังระบบเครือข่ายและควบคุมการช่วงชิงใน **MAC sublayer** อย่างไรก็ตาม **LAN** ไร้สายจะแตกต่างในการใช้วิธีที่เรียกว่า **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** แทนที่จะใช้ **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** ถึงแม้ว่า **CSMA/CA** จะค่อนข้างเหมือนกับ **CSMA/CD** ตรงที่ **nodes** ต่างๆ จะต้องเฝ้าฟังสื่อกลางในการนำสัญญาณและจะทำการส่งได้ก็ต่อเมื่อสายสัญญาณว่าง แต่ใน **CSMA/CA** นั้น **nodes** ต่างๆ ไม่ได้ทำเพียงฉกฉวยการใช้สายสื่อสารที่ว่างแล้วทำการส่งสัญญาณ แต่จะต้องเริ่มทำในสิ่งที่เหมือนกับการจับสิ่งของในอากาศ โดยการส่งข่าวสารสั้นๆ ที่เรียกว่า **RTS (Request To Send)** ซึ่งจะระบุผู้รับที่ตั้งใจไว้ในขณะเดียวกันก็จะเตือน **nodes** ทั้งหมดที่อยู่ในบริเวณใกล้เคียงให้หยุดรอในชั่วขณะหนึ่ง ในอีกทางหนึ่งผู้รับก็จะส่งสัญญาณ **CTS (Clear To Send)** กลับไปยัง **node** ที่ต้องการส่ง เมื่อกระบวนการนี้เสร็จสิ้น **node** นั้นก็จะทำการส่งสัญญาณข้อมูล ถ้าผู้รับได้รับข้อมูลอย่างถูกต้อง กระบวนการนี้ก็จะสิ้นสุดโดยการส่งสัญญาณตอบรับ **ACK (Acknowledge)** กลับไป ณ จุดนี้สื่อกลางก็จะว่างสำหรับ **node** อื่น

ในระบบเครือข่ายมาตรฐาน **IEEE 802.11** จะแบ่งระดับเทคโนโลยี ออกเป็น **4** ระดับ คือ **PHY (Physical Layer), MAC (Media Access Controller), OS** และ **Application**

3.11.1 PHY (Physical Layer)

PHY คือส่วนของฮาร์ดแวร์ที่แบ่งมาตรฐานออกเป็น **a, b, d, g** และ **IR** (อินฟาเรด) นั่นเอง โดยผู้ใช้ต้องเลือก **PHY** ที่มีมาตรฐานเดียวกันจึงจะทำงานร่วมกันได้ ใน **physical layer** นั้น **LANs** ไร้สายเหล่านี้จะอาศัยวิธีการส่งสัญญาณข้อมูลแบบไร้สายตามมาตรฐานต่างๆ ดังนี้

3.11.1.1 มาตรฐาน IEEE 802.11a

คือการส่งสัญญาณข้อมูลด้วยคลื่นวิทยุ ด้วยการออกอากาศในย่านความถี่วิทยุ **2.4 GHz** นอกจากนั้นการส่งสัญญาณคลื่นวิทยุยังแบ่งประเภทออกเป็น **Direct Sequence Spread Spectrum (DS)** และ **Frequency Hopping Spread Spectrum (FS)**

- **Direct Sequence Spread Spectrum (DS)** ใช้เทคนิค **modulation** (วิธีในการใส่ข้อมูลเข้าไปบนคลื่นวิทยุ) ซึ่งข้อมูลแต่ละบิตที่จะทำการส่งจะถูกแตกออกและเข้ารหัสเป็นส่วนหนึ่งของอนุภาคขนาดเล็กที่เรียกว่า **chips** ถึงแม้ว่ากระบวนการนี้จะยากที่จะบรรยายด้วยภาพ แต่ผลสุดท้ายข้อมูลที่เข้ารหัสในลักษณะนี้ก็จะสามารถส่งผ่านย่านความถี่ของคลื่นตัวนำได้ดีกว่าข้อมูลที่ไม่ถูกแตกเป็นชิ้นเล็กๆ นี้ นอกจากนั้นข้อมูลที่แท้จริงจะติดอยู่กับบิตย่อยๆ ที่เข้ารหัสนี้เป็นกระแสของข้อมูลที่สามารถทำการถอดรหัสได้โดยเครื่องรับที่จัดให้มีการใช้รหัสแบบเดียวกัน
- **Frequency Hopping Spread Spectrum (FS)** จะเข้าใจได้ง่ายกว่า ในกระบวนการนี้การส่งและรับสัญญาณคลื่นวิทยุจะกระโดดไปตามลำดับที่สอดคล้องกันจากความถี่หนึ่งไปยังอีกความถี่หนึ่งผ่านช่องสัญญาณการส่ง ในการหยุดแต่ละครั้งจะทำการส่งและรับสัญญาณก่อนที่จะเคลื่อนไปทำครั้งต่อไป เวลาที่ใช้ไปในแต่ละความถี่ (เรียกว่า **dwell time**) และการเลือกช่องสัญญาณในการส่งจะถูกกำหนดไว้ล่วงหน้าแล้วเพื่อที่จะให้ทุกคนในระบบเครือข่ายทราบว่าจะส่งไปที่ไหนและเมื่อใด **802.11a** มีจุดเด่นเหนือกว่า **802.11b** ในด้านความเร็วในการรับส่งข้อมูล ทำได้สูงสุด **54 Mbps** ใช้คลื่นความถี่วิทยุ **5 GHz** แต่มีข้อเสียคือระยะทางในการรับส่งข้อมูลสั้น ทำให้ต้องมีอุปกรณ์แม่ข่ายมากจุดเพื่อให้ครอบคลุมพื้นที่ ค่าใช้จ่ายจึงสูง

3.11.1.2 มาตรฐาน IEEE 802.11b

ล่าสุดได้รับการตั้งชื่อใหม่ว่า **Wi-Fi** คุณสมบัติของ **IEEE 802.11b** จะสามารถรับส่งข้อมูลได้ด้วยความเร็วสูงสุด **11 Mbps** โดยใช้คลื่นความถี่วิทยุที่ **2.4 GHz** ข้อเสียของมาตรฐานนี้ คือยังมีอุปกรณ์ไฟฟ้าชนิดอื่นใช้คลื่นความถี่เดียวกัน เช่น เตาไมโครเวฟ หรือโทรศัพท์มือถือ ซึ่งหากมีอุปกรณ์เหล่านี้อยู่ในบริเวณใกล้เคียง จะทำให้ความเร็วในการส่งข้อมูลลดลง ข้อดีคือใช้คลื่นความถี่วิทยุค่อนข้างต่ำ ทำให้สามารถส่งข้อมูลได้ในระยะไกล ช่วยให้ประหยัดค่าใช้จ่ายได้อีกส่วนหนึ่ง

3.11.1.3 มาตรฐาน IEEE 802.11g

คือการส่งสัญญาณข้อมูลด้วยคลื่นอินฟราเรด หรือคลื่นแสงที่มีลักษณะพิเศษ ความยาวคลื่นต่ำ การแพร่คลื่นของแสงอินฟราเรดที่ซึ่งทำการออกอากาศสัญญาณแสงที่โหนดต่างๆ ที่อยู่ในบริเวณนั้นสามารถรับ

ได้ โดยเฉพาะอย่างยิ่งการแพร่คลื่นของแสงอินฟราเรดนี้จะสะท้อนไปโดยรอบ สะท้อนผนัง พื้น เพดาน จนกระทั่งไปถึงผู้รับ วิธีนี้จะแตกต่างจากการส่งสัญญาณอินฟราเรดตามแนวเส้นเล็ง (**line of sight**) ซึ่งลำแสงอินฟราเรดจะต้องยิงออกไปในแนวเส้นตรงไปยังอุปกรณ์รับสัญญาณอินฟราเรดที่ติดอยู่กับเครื่องรับ (เช่น **VCR** หรือเครื่องคอมพิวเตอร์ที่ได้รับการออกแบบให้ใช้แป้นพิมพ์ไร้สาย) ถึงแม้ว่าการแพร่สัญญาณอินฟราเรดจะยอมให้เคลื่อนย้ายโหนดไปที่ใดก็ได้ตามต้องการ แต่สัญญาณนี้ก็ค่อนข้างจะอ่อนและเดินทางช้าเนื่องจากสัญญาณเกิดการสะท้อน โดยปกติการแพร่คลื่นของแสงอินฟราเรดจะมีระยะทางเพียงประมาณ **33** เมตร (**100** ฟุต)

ในปัจจุบันกำลังมีการพัฒนาเพื่อแก้ไขจุดอ่อนให้กับ **IEEE 802.11a** และ **802.11b** จุดเด่นของมาตรฐานนนี้ คือการใช้คลื่นความถี่ **2.4 GHz** เหมือนกับ **IEEE 802.11b** แต่มีความเร็วสูงกว่า อยู่ที่ **54 Mbps** เหมือน **IEEE 802.11a** เป็นที่คาดว่ามาตรฐาน **IEEE 802.11g** จะออกวางตลาดในเร็ววันนี้มาตรฐาน **IEEE 802.11g** เป็นมาตรฐานของเครือข่ายไร้สายระหว่างประเทศ กล่าวคือในบางประเทศจะมีข้อกำหนดเกี่ยวกับคลื่นวิทยุไม่ตรงกัน จึงมีการพัฒนาระบบนี้ให้สามารถนำเอาอุปกรณ์ไปใช้ในต่างประเทศได้โดยไม่ต้องเปลี่ยนอุปกรณ์

3.11.2 MAC (Media Access Controller)

MAC เป็นส่วนทำงานเกี่ยวกับระบบรักษาความปลอดภัยของเครือข่าย การจัดโครงสร้างหรือรูปแบบของข้อมูล การแปลงข้อมูล ในส่วนนี้ มาตรฐาน **IEEE 802.11** จะใช้ **MAC** เดียวกันทั้งหมด มาตรฐานส่วน **MAC** นั้นมีมาตรฐานกลุ่มย่อยอยู่ทั้งสิ้น **3** กลุ่ม คือ **e, h** และ **i**

3.11.2.1 IEEE 802.11e เป็นมาตรฐานสำหรับการกำหนดคุณภาพให้กับระบบเครือข่ายไร้สาย

3.11.2.2 IEEE 802.11h เป็นการเพิ่มความสามารถด้านคลื่นความถี่ระดับ **5 GHz** เข้าไปในตัว **MAC** ให้สามารถนำไปใช้งานในยุโรปได้ **IEEE 802.11eh** ปัจจุบันอยู่ในระหว่างการพัฒนา

3.11.2.3 IEEE 802.11i เป็นส่วนของการจัดการด้านการรักษาความปลอดภัยให้กับระบบเครือข่าย

3.11.3 OS และ Application

คือ ระบบปฏิบัติการภายในเครื่องและแอพพิเคชั่นควบคุมการสื่อสาร ซึ่งเหมือนกับมาตรฐานของเครือข่ายแบบมีสาย จะมีส่วนย่อยอยู่ **2** กลุ่มคือ **c** และ **f**

3.11.3.1 IEEE 802.11c เป็นมาตรฐานด้านการเพิ่มความสามารถทางภาษาให้กับระบบเครือข่ายไร้สาย

3.11.3.2 IEEE 802.11f เป็นเรื่องของการจัดการเกี่ยวกับ **Access Point** ซึ่งกำลังอยู่ในช่วงพัฒนา

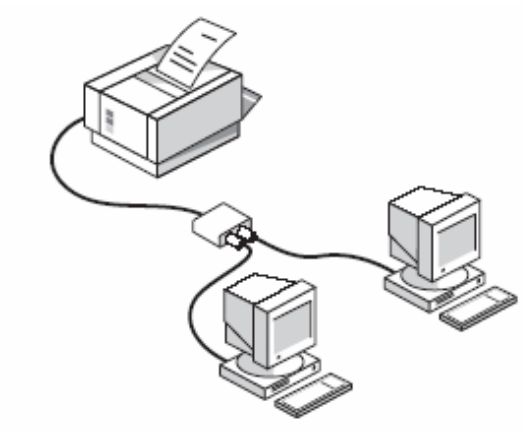
ดังนั้นระบบเครือข่ายในลักษณะนี้ที่เรียกว่า **WLANs (Wireless LANs)** จึงมีประโยชน์ในสถานการณ์ซึ่ง

- โหนดต้องการมีอิสระในการเคลื่อนย้าย เช่นในโรงพยาบาล ร้านค้าขนาดใหญ่ (การบันทึกรายการสินค้า) หรือในโรงงาน
- ต้องการการเชื่อมต่อระบบเครือข่ายในบริเวณที่ค่อนข้างวุ่นวาย เช่นในห้องโถงหรือห้องรับรองขนาดใหญ่
- การเชื่อมต่อไม่มีความน่าเชื่อถือ หรือขึ้นอยู่กับปัจจัยภายนอก เช่นในการปฏิบัติการทางทหาร
- ยากต่อการเชื่อมต่อระบบเครือข่ายได้ทั้งอาคารหรือแทบจะเป็นไปไม่ได้เลย

ในปัจจุบันระบบเครือข่ายไร้สายยังไม่เป็นที่แพร่หลายเท่าที่ควรแต่บางทีในอนาคตอาจจะได้รับความนิยมเพิ่มมากขึ้นเมื่อเวลาและเทคโนโลยีก้าวหน้าไปมากขึ้น

3.12 AppleTalk

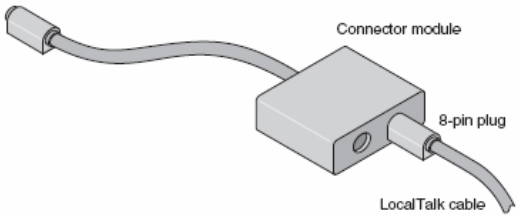
บริษัท **Apple Computer Inc.** ได้เปิดตัว **AppleTalk** ครั้งแรกในปี **1983** ในฐานะสถาปัตยกรรมระบบเครือข่ายสำหรับกลุ่มงานขนาดเล็ก การทำงานของระบบเครือข่ายได้ถูกสร้างลงในเครื่องคอมพิวเตอร์ **Macintosh** ทุกเครื่อง ในรูปของระบบปฏิบัติการของเครื่อง **Macintosh** ซึ่งหมายความว่าระบบปฏิบัติการของเครื่อง **Macintosh** ได้มีการรวบรวมโปรโตคอลต่างๆ ที่สอดคล้องกับ **OSI Reference Model** ไว้แล้วจึงทำให้สามารถเชื่อมต่อกันเป็นระบบเครือข่ายได้โดยง่าย ดังแสดงตามรูปที่ **3 – 26**



รูปที่ **3 – 26** ระบบเครือข่าย **AppleTalk**

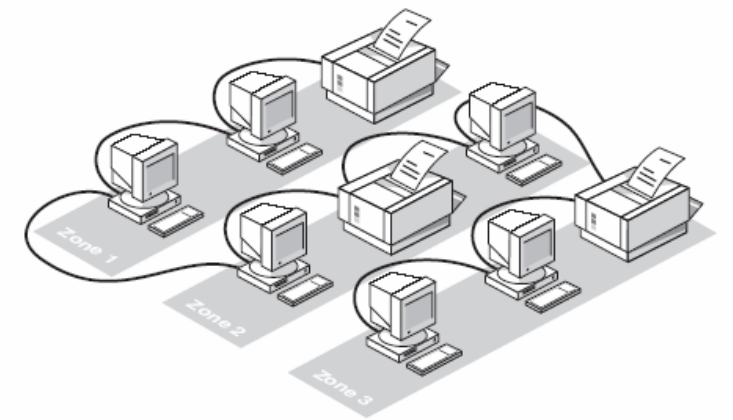
3.12.1 LocalTalk

LocalTalk เป็นระบบเครือข่ายซึ่งใช้วิธี **CSMA/CS** ในการ **access** ข้อมูลในระบบเครือข่ายที่มีโทโปโลยีแบบบัส การที่บริษัท แอปเปิล ผลิต **LocalTalk** รวมอยู่ในส่วนของฮาร์ดแวร์จึงทำให้มีราคาถูก แต่อย่างไรก็ตามอุปกรณ์การเชื่อมต่อก็จำเป็นต้องใช้อุปกรณ์ **Connector Module** ของบริษัท แอปเปิล ดังแสดงตามรูปที่ **3 – 25** วิธีการนี้จึงทำให้ธุรกิจขนาดใหญ่หันมาสนใจการเดินสายเคเบิลในองค์กรแทน



รูปที่ **3 – 27 Connector Module**

อย่างไรก็ตามยังมีผู้ที่นิยมการใช้เครื่องคอมพิวเตอร์ **Macintosh** อยู่เป็นจำนวนมากที่นำโครงสร้าง **LocalTalk** มาใช้เป็นระบบเครือข่ายขนาดใหญ่ภายในองค์กร โดยการจัดแบ่งโซน (**Zone**) และทำการเชื่อมต่อเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเข้าด้วยกันเป็นระบบเครือข่ายโดยไม่ต้องเดินสายเคเบิล ดังแสดงตามรูปที่ **3 – 28**



รูปที่ 3 – 28 การรวม 3 โซนเข้าด้วยกันเป็นระบบเครือข่ายขนาดใหญ่ขึ้น

3.12.2 AppleShare

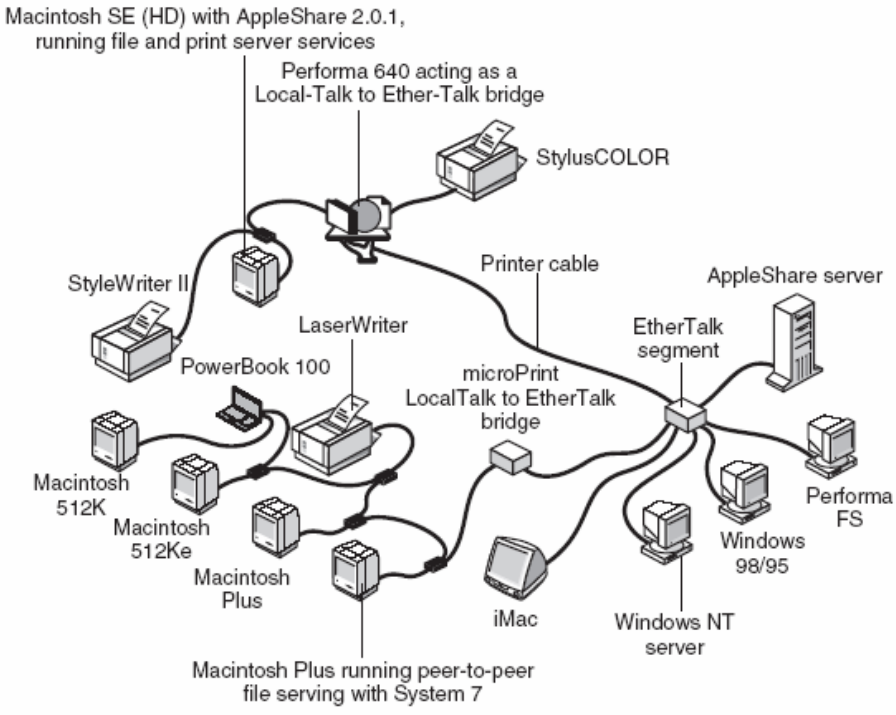
AppleShare เป็นเครื่องเซิร์ฟเวอร์บนเครือข่าย **AppleTalk** โดยมีซอฟต์แวร์ **AppleShare Print Server** เพิ่มเติมจากเครื่อง **Macintosh** ปกติ

3.12.3 EtherTalk

เป็นการ์ดระบบเครือข่ายเพิ่มเติมที่ช่วยให้เครื่องคอมพิวเตอร์ **Macintosh** สามารถเชื่อมโยงเข้ากับระบบเครือข่ายอีเธอร์เน็ต **802.3** ได้ โดยซอฟต์แวร์ของ **EtherTalk** ถูกรวมอยู่ในการ์ด

3.12.4 TokenTalk

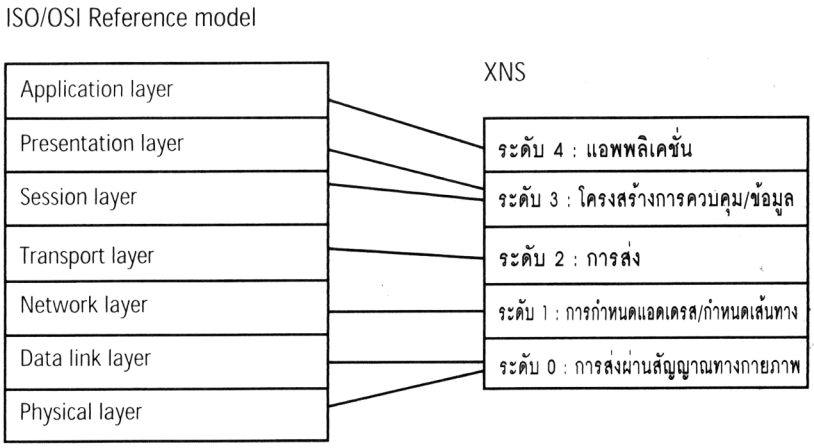
เป็นการ์ดต่อขยายที่ช่วยให้เครื่องคอมพิวเตอร์ **Macintosh** สามารถเชื่อมโยงเข้ากับระบบเครือข่ายโทเก้นริง **802.5** ได้ โดยซอฟต์แวร์ของ **TokenTalk** ถูกรวมอยู่ในการ์ด



รูปที่ 3 – 29 ระบบเครือข่าย **AppleTalk**

3.13 XNS (Xerox Network System)

XNS เป็นคำย่อของ Xerox Network System ซึ่งมีต้นกำเนิดจากบริษัท Xerox PARC เป็นชุดของโปรโตคอลที่กำหนดให้เป็น 5 เลเยอร์ จากเลข 0 ถึง 4 ถึงแม้ว่า XNS จะได้รับการพัฒนาขึ้นก่อนที่จะมี ISO/OSI Reference Model แต่ก็สามารถเทียบเคียงกับ OSI model ได้เป็นอย่างดี ดังแสดงตามรูปที่ 3 – 30



รูปที่ 3 – 30 เปรียบเทียบ OSI กับ XNS

3.13.1 ระดับ 0 (Level 0)

ระดับต่ำที่สุด เทียบได้กับ physical layer และ data link layer ของ ISO/OSI Reference Model ถึงแม้ว่า XNS จะมีเลเยอร์เหล่านี้ แต่ในตัวเองแล้วก็ไม่มีโปรโตคอลที่ทำงานบนเลเยอร์นั้นๆ จึงต้องอาศัยระบบเครือข่ายของตนเองในการจัดให้มีการส่งสัญญาณข้อมูลในโครงสร้างสถาปัตยกรรมของระบบเครือข่ายอีเธอร์เน็ต โทเก้นริง หรือโครงสร้างสถาปัตยกรรมแบบอื่น

3.13.2 ระดับ 1 (Level 1)

เทียบได้กับ Network layer ของ OSI Model ซึ่งถูกแสดงโดยโปรโตคอลของ XNS ที่เรียกว่า IDP (Internet Datagram Protocol) โดยที่ IDP จะกำหนดแอดเดรสให้กับแพ็กเก็ตข้อมูล และพิจารณาว่าจะใช้สื่อกลางการส่งสัญญาณข้อมูลแบบใด

3.13.3 ระดับ 2 (Level 2)

เทียบได้กับ Transport layer ประกอบด้วยโปรโตคอลที่ร่วมกันสนับสนุนการปฏิบัติงาน เช่น การจัดลำดับของแพ็กเก็ตข้อมูล การตรวจสอบความผิดพลาด การส่งสัญญาณข้อมูลที่เสียหายออกไปใหม่ และควบคุมอัตราการส่งสัญญาณข้อมูล โปรโตคอลต่างๆ เหล่านี้ คือ RIP (Routing Information Protocol), EP (Error Protocol), SPP (Sequenced Packet Protocol) และ PEP (Packet Exchange Protocol)

3.13.4 ระดับ 3 (Level 3)

เทียบอย่างหยาบๆ ได้กับ Session layer และ Presentation layer ประกอบด้วยโปรโตคอลที่เกี่ยวข้องกับการสร้างข้อมูล และควบคุมการโต้ตอบบนระบบเครือข่าย มีโปรโตคอลเพียงตัวเดียวที่ทำงานในเลเยอร์นี้ คือ CP (Courier Protocol)

3.13.5 ระดับ 4 (Level 4)

เทียบได้กับ **Application layer** ซึ่งประกอบด้วยโปรโตคอลจำนวนมากที่เกี่ยวข้องกับโปรแกรมประยุกต์ ประกอบด้วย **Printing Protocol** สำหรับการให้บริการการพิมพ์ **Filing Protocol** สำหรับการ **access** ไฟล์ และ **Clearinghouse Protocol** สำหรับการให้บริการชื่อของระบบเครือข่าย

3.14 DECnet

DECnet กล่าวถึงผลิตภัณฑ์ฮาร์ดแวร์และซอฟต์แวร์ รวมทั้งชุดโปรโตคอลสแต็ก (**Protocol Stack**) ที่ได้รับการออกแบบโดยบริษัท **Digital Equipment Corporation** (ปัจจุบันเป็นส่วนหนึ่งของบริษัท **Compaq Computer**) สำหรับโครงสร้างสถาปัตยกรรมระบบเครือข่ายดิจิตอล (**Digital Network Architecture - DNA**) โดยที่ **DECnet** ในเบื้องต้นได้รับการออกแบบเพื่อทำให้ เครื่องคอมพิวเตอร์ของบริษัท **Digital** สามารถสื่อสารซึ่งกันและกันได้ แต่หลังจากที่เปิดตัวออกมาในปี **1975** ก็ได้รับการปรับปรุงตามลำดับเป็นระยะ โดยกำหนดการสื่อสารบนระบบเครือข่ายอีเธอร์เน็ต ระบบเครือข่าย **FDDI (Fiber Distributed Data Interface)** และระบบ **WAN** ที่ให้บริการในลักษณะเครือข่ายส่วนตัว (**Private Network**) และเครือข่ายสาธารณะ (**Public Data Transmission**) โดย **DECnet** ได้มีการปรับปรุง **DECnet** หลายครั้ง แต่ละครั้งที่มีการปรับปรุงเรียกว่า เฟส (**Phase**) สำหรับเวอร์ชันในปัจจุบันคือ **DECnet Phase V** สามารถใช้โปรโตคอล **TCP/IP** และโปรโตคอลอื่นใน **OSI Reference Model** หรือโปรโตคอลของตนเองในการกำหนดเส้นทางการขนส่งข้อมูลได้

โปรโตคอลของ **DECnet** สนับสนุนทั้งโปรโตคอลใน **OSI Model** และโปรโตคอลที่บริษัท **Digital** จัดให้มีเป็นลำดับ นั่นคือสามารถสนับสนุนระบบเครือข่ายมาตรฐานอีเธอร์เน็ต โทเก้นริง และโปรโตคอลอื่นที่อาศัยอยู่ใน **Physical layer** และ **Data link layer** ของ **OSI Reference Model** อย่างไรก็ตามเพื่อที่จะรักษาความเข้ากันได้กับเฟสก่อนหน้านี้ **DECnet** จึงยังคงสนับสนุนโปรโตคอลของบริษัท **Digital** ซึ่งได้รับการพัฒนามาเป็นลำดับ ที่เรียกว่า **Digital Data Communication Messaging Protocol (DDCMP)** และทำงานใน **Data link layer**

ใน **Network layer** ที่อยู่เหนือขึ้นไป **DECnet** สนับสนุนการให้บริการแก่โปรโตคอลที่ต้องการการเชื่อมต่อและไม่ต้องการการเชื่อมต่อ ซึ่งประกอบด้วย **CLNP** และ **CMNP** ซึ่งเป็นโปรโตคอลของ **OSI Model** เช่นเดียวกัน สำหรับโปรโตคอลซึ่งพัฒนาใน **Phase IV (four)** ที่เรียกว่า **DECnet Phase IV routing Protocol** และเมื่อเลื่อนต่อไปด้านบน ใน **Transport Layer** ของ **OSI Model** นั้น **DECnet** จะรวมการสนับสนุนสำหรับโปรโตคอล **TPx** ของ **OSI** และสำหรับ **Network Service Protocol (NSP)** ของตัวเอง และในระดับสูงสุดของ **DECnet** จะรวมการสนับสนุนสำหรับ **DNA** และ **OSI session, presentation** และ **application**

แบบฝึกหัดท้ายบท

1. คอลัมน์ทางด้านซ้าย เป็นรายการของหลักการช่วยจำเลเยอร์ต่างๆ ในโครงสร้างสถาปัตยกรรม **OSI Reference Model** คือ "**All People Seem To Need Data Processing**" จงเขียนชื่อเลเยอร์ระดับต่างๆ ของ **OSI** ลงในคอลัมน์ด้านข้างพร้อมทั้งฟังก์ชันการทำงานของแต่ละเลเยอร์มาพอสังเขป

เครื่องมือช่วยจำ	**OSI Layer**	ฟังก์ชันการทำงาน
All **People** **Seem** **To** **Need** **Data** **Processing**		

2. คอลัมน์ทางด้านซ้ายจะแสดงรายการอุปกรณ์ระบบเครือข่ายมาตรฐาน จงเขียนว่าอุปกรณ์แต่ละตัวมีการทำงานในเลเยอร์ใดของ **ISO/OSI Reference Model** ลงในคอลัมน์ด้านข้าง

อุปกรณ์	**OSI Layer**
Gateway **NIC** **Hub** **Router** **IEEE 802.X**	

3. จงอธิบายพื้นฐานของมาตรฐาน **IEEE Project 802** แต่ละประเภทในตารางด้านล่าง

IEEE 802.X	**Basis for Standard**
802.1	
802.2	
802.3	
802.4	
802.5	
802.6	
802.7	
802.8	
802.9	
802.10	
802.11	
802.12	
802.13	
802.14	
802.15	
802.16	

4. ให้เปรียบเทียบโครงสร้างของ **SNA (System Network Architecture)** ของบริษัท **IBM** กับโครงสร้าง **OSI Reference Model** พร้อมทั้งอธิบายความเหมือนและความแตกต่างมาพอสังเขป
5. ให้เปรียบเทียบโครงสร้างของ **TCP/IP Model** กับโครงสร้าง **OSI Reference Model** พร้อมทั้งอธิบายความเหมือนและความแตกต่างมาพอสังเขป
6. จงอธิบายหลักการทำงานของการขนส่งข้อมูลบนระบบเครือข่ายด้วยวิธี **CSMA/CD (Carrier Sense Multiple Access (with) Collision Detection)** มาพอสังเขป
7. จงอธิบายหลักการทำงานของการขนส่งข้อมูลบนระบบเครือข่ายด้วยวิธี **Token Passing** มาพอสังเขป
8. **IEEE 802.11** ได้อธิบายคุณลักษณะเฉพาะของระบบเครือข่ายไร้สายโดยเทียบเคียงกับระบบเครือข่ายอีเธอร์เน็ต อยากทราบว่า ระบบเครือข่ายไร้สายใช้วิธีการใดในการ **access** เข้าไปยังระบบเครือข่าย อธิบายหลักการทำงานของวิธีการนั้นมาพอสังเขป
9. จงอธิบายโครงสร้างสถาปัตยกรรมของระบบเครือข่าย **AppleTalk**
10. ให้เปรียบเทียบโครงสร้างของ **XNS (Xerox Network System)** ของบริษัท **Xerox PARC** กับโครงสร้าง **OSI Reference Model** พร้อมทั้งอธิบายความเหมือนและความแตกต่างมาพอสังเขป

<u>จงเติมคำลงในช่องว่างให้ถูกต้อง</u>

11. โครงสร้าง **OSI Model** ได้จัดแบ่งการทำงานของระบบเครือข่ายออกเป็น _____ เลเยอร์
12. วัตถุประสงค์ในการทำงานของแต่ละเลเยอร์ในโครงสร้าง **OSI Model** คือให้บริการกับ _____ และป้องกันไม่ให้เลเยอร์ในระดับที่อยู่สูงกว่ามีรายละเอียดการให้บริการมากจนเกินไป
13. ที่แต่ละเลเยอร์จะทำการเพิ่ม _____ เข้าไปยังแพ็กเก็ตข้อมูล
14. ที่ _____ จะพิจารณาเส้นทางการขนส่งข้อมูลจากต้นทางไปยังปลายทาง
15. **Data link Layer** มีหน้าที่รับผิดชอบในการส่ง _____ จาก **Network Layer** ไปยัง **Physical Layer**
16. _____ จะระบุวิธีการที่สายเคเบิลจะเชื่อมต่อเข้ากับ **NIC**
17. **Project 802** ได้แบ่ง **Data link Layer** ออกเป็น **2 Sub-layer** คือ _____และ _____
18. **The** _____ **Sub-layer** จะสื่อสารโดยตรงกับ **NIC** และรับผิดชอบในการจัดส่งข้อมูลซึ่งไม่มีความผิดพลาดระหว่างเครื่องคอมพิวเตอร์ 2 เครื่องบนระบบเครือข่าย
19. **IEEE** _____ได้อธิบายครอบคลุมมาตรฐานของระบบเครือข่ายอีเธอร์เน็ต
20. **IEEE** _____ได้อธิบายครอบคลุมมาตรฐานของระบบเครือข่ายโทเก้นริง