บทที่ 2

กรอบแนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 กรอบแนวคิดทฤษฎี

2.1.1 ความรู้พื้นฐานของการสื่อสารข้อมูล

2.1.1.1 ความรู้พื้นฐานของการสื่อสารข้อมูล

การสื่อสารข้อมูลทางอิเล็กทรอนิกส์ คือ การแลกเปลี่ยนข้อมูลระหว่างต้นทาง และปลายทาง โดยใช้อุปกรณ์ทางอิเล็กทรอนิกส์ซึ่งเชื่อมต่อกัน อยู่ด้วยสื่อกลางชนิดใดชนิดหนึ่ง ระบบเครือข่ายคอมพิวเตอร์ คือ ระบบการเชื่อมโยงระหว่าง คอมพิวเตอร์ ตั้งแต่สองตัวขึ้นไป เพื่อให้สามารถทำการสื่อสารแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ระหว่างกันได้

2.1.1.2 องค์ประกอบขั้นพื้นฐานของระบบสื่อสาร

องค์ประกอบขั้นพื้นฐานของระบบสื่อสารโทรคมนาคม สามารถจำแนกออกเป็นส่วนประกอบได้ดังต่อไปนี้

1. ผู้ส่งข่าวสาร หรือแหล่งกำเนิดข่าวสาร (Source) อาจจะเป็นสัญญาณต่าง ๆ เช่น สัญญาณภาพ ข้อมูล และเสียงเป็นต้น

2. ผู้รับข่าวสาร หรือจุดหมายปลายทางของข่าวสาร (Sink) ซึ่งจะรับรู้จากสิ่งที่ผู้ส่งข่าวสารหรือแหล่งกำเนิดข่าวสารส่งผ่านมาในการติดต่อสื่อสารบรรลุวัตถุประสงค์ ผู้รับสารหรือจุดหมายปลายทางของข่าวสารก็จะได้รับข่าวสารนั้น ๆ

3. ช่องสัญญาณ (channel) หมายถึงสื่อกลางหรือตัวกลางที่ข่าวสาร ข้อมูลเดินทางผ่าน เปรียบเสมือนเป็นสะพานที่จะให้ข่าวสาร ข้อมูลข้ามจากฝั่งหนึ่งไปยังอีกฝั่งหนึ่ง

4. การเข้ารหัส (Encoding) เป็นการช่วยให้ผู้ส่งข่าวสาร และผู้รับสารมีความเข้าใจตรงกันในการสื่อความหมาย การเข้ารหัส หมายถึง การแปลงข่าวสารให้ส่งไปในสื่อกลาง ทางผู้ส่งมีความเข้าใจต้องตรงกันระหว่างผู้ส่งและผู้รับ หรือมีรหัสเดียวกัน การสื่อสารจึงเกิดขึ้นได้

5. การถอดรหัส (Decoding) หมายถึงการที่ผู้รับข่าวสารแปลงพลังงานจากสื่อกลางให้กลับไปอยู่ในรูปข่าวสารที่ส่งมาจากผู้ส่งข่าวสาร โดยมีความเข้าใจหรือรหัสตรงกัน

6. สัญญาณรบกวน (Noise) เป็นสิ่งที่มีอยู่ในธรรมชาติ มักจะลดทอนหรือรบกวนระบบ อาจจะเกิดขึ้นได้ทั้งทางด้านผู้ส่งข่าวสาร ผู้รับข่าวสาร และช่องสัญญาณ

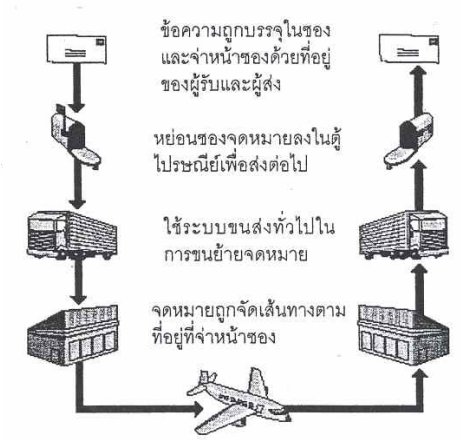
2.1.2 <u>มาตรฐานการสื่อสารข้อมูล</u>

การกำหนดมาตรฐานของการสื่อสารข้อมูลนั้น นับว่ามีความจำเป็นอย่างมาก สำหรับระบบเครือข่ายที่มี องค์ประกอบของอุปกรณ์ต่างๆ หลากหลายผู้ผลิต ซึ่งอุปกรณ์ทั้งหมดเหล่านั้นจะต้องทำงานเข้ากันได้ การกำหนดมาตรฐานต่างๆ นั้นจะเริ่มตั้งแต่โครงสร้างพื้นฐานของฮาร์ดแวร์ระบบเครือข่าย ได้แก่ ระบบสายเคเบิล อุปกรณ์ในการส่งสัญญาณข้อมูล ตลอดจนถึงเครื่องเซิร์ฟเวอร์ และซอฟต์แวร์ในการสื่อสารบนระบบเครือข่าย เพื่อเป็นการรับประกันว่าส่วนประกอบต่างๆ จะสามารถทำงานร่วมกันได้ ผู้ผลิตฮาร์ดแวร์และซอฟต์แวร์ระบบเครือข่ายจะต้องทำตามคำแนะนำตามมาตรฐานการออกแบบและสร้างผลิตภัณฑ์ ซึ่งกำหนดขึ้นโดย องค์กรมาตรฐานสากล (International Organization for Standardization - ISO) โดยมาตรฐานที่กำหนดขึ้นและได้ประกาศใช้ตั้งแต่ปี คศ.1984 เรียกว่า Open Systems Interconnection Reference Model เรียกสั้นๆ ว่า OSI Reference Model หรือ ISO/OSI Model

OSI Reference Model องค์การมาตรฐานนานาชาติ (The International Organization for Standardization) เป็นองค์กรที่ออกแบบโปรโตคอล OSI (Open System Interconnect) หรือโปรโตคอลการเชื่อมต่อเครือข่ายแบบเปิด จุดมุ่งหมายของการพัฒนามาตรฐานนี้ เพื่อให้คอมพิวเตอร์และอุปกรณ์เครือข่ายที่ผลิตโดยบริษัทต่าง ๆ สามารถทำงานร่วมกันได้ ชุดโปรโตคอลส่วนใหญ่นี้จะเรียกว่า “แบบอ้างอิง OSI (OSI Reference Model)” แบบอ้างอิงนี้จะแบ่งขั้นตอนการสื่อสารระหว่างคอมพิวเตอร์ออกเป็น 7 ขั้นตอนหรือเลเยอร์ (Layer) การแบ่งเป็นขั้นตอนต่าง ๆ เหล่านี้จะยึดหลักเหมือนกับการสื่อสารทั่วไป เช่น การรับส่งจดหมายทางไปรษณีย์ ก็จะมีขั้นตอน ดังแสดงในภาพข้างล่าง

ภาพที่ 2.1

ระบบการขนส่งจดหมาย



จากตัวอย่างการสื่อสารด้วยจดหมายนั้น จะเห็นว่าขั้นตอนของผู้ส่งกับขั้นตอนของผู้รับนั้นจะคล้าย ๆ กันเพียงแต่ลำดับเหตุการณ์นั้นเกิดขึ้นในทางตรงข้ามกันเท่านั้น การสื่อสารกันระหว่างคอมพิวเตอร์ก็จะเป็นไปในลักษณะคล้าย ๆ กัน กล่าวคือ จะแบ่งการทำงานออกเป็นขั้นตอนต่างๆ เพื่อให้ง่ายต่อการจัดการข้อความที่ส่ง

ภาพที่ 2.2

แบบอ้างอิง OSI

7	Application		7	Application
6	Presentation		6	Presentation
5	Session	Logical Flow	5	Session
4	Transport		4	Transport
3	Network		3	Network
2	Data Link		2	Data Link
1	Physical		1	Physical

Actual Flow

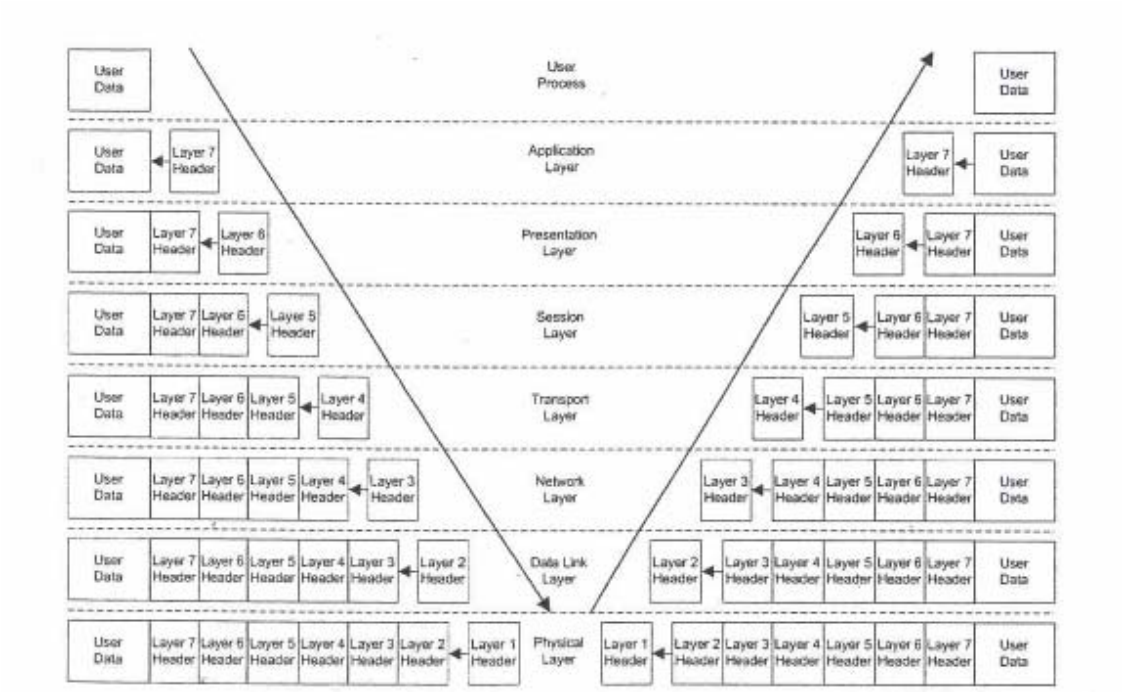
การสื่อสารกันระหว่างคอมพิวเตอร์สองเครื่องใด ๆ ในเครือข่ายจะมีขั้นตอนการสื่อสารจะเริ่มจากการที่ผู้ใช้มีข้อมูลที่ต้องการส่งไปยังผู้ใช้อีกคนหนึ่งที่ใช้คอมพิวเตอร์อีกเครื่องหนึ่ง ข้อมูลนั้นจะถูกส่งผ่านไปยังเลเยอร์ที่ 7 ในเลเยอร์นี้ข้อมูลก็จะถูกดัดแปลงและใส่ข้อมูลบางอย่างเพิ่มเติม แล้วจะถูกส่งต่อไปยังเลเยอร์ที่อยู่ต่ำกว่า จะทำอย่างนี้ไปเรื่อย ๆ จนถึงเลเยอร์ที่อยู่ต่ำกว่าข้อมูลก็จะถูกแปลงเป็นสัญญาณเพื่อส่งผ่านสายสัญญาณ หรือสื่อกลางที่เชื่อมกันระหว่างคอมพิวเตอร์สองเครื่องนี้ จนถึงเครื่องรับ ส่วนกระบวนการในการรับข้อมูลของเครื่องรับนั้นก็จะทำในทางตรงกันข้ามกับเครื่องส่งข้อมูล กล่าวคือจะเริ่มกระบวนการรับข้อมูลจากเลเยอร์ 1ก่อนและส่งต่อไปเรื่อย ๆ จนถึงเลเยอร์ 7 และส่งต่อให้แอพพลิเคชั่นของผู้ใช้ต่อไป

การทำงานในแต่ละเลเยอร์จะเป็นไปในรูปแบบที่ว่าแต่ละเลเยอร์จะคอยให้บริการให้กับ เลเยอร์ที่อยู่สูงกว่าและติดกัน โดยที่เลเยอร์ที่ใช้บริการจะไม่สนใจในรายละเอียดว่าเลเยอร์ที่ให้บริการจะมีวิธีการทำงานอย่างไร เพียงแค่รู้ว่าข้อมูลนั้นจะส่งถึงปลายทาง

การจัดเรียงโปรโตคอลเป็นชั้น ๆ หรือเลเยอร์นี้เพื่อจำลองการไหลของข้อมูลจากเครื่องส่งถึงเครื่องรับ แต่ละขั้นจะส่งข้อมูลต่อไปยังขั้นที่อยู่ติดกัน เช่น ถ้าเป็นการส่งข้อมูล ข้อมูลจะถูกส่งต่อไปยังขั้นที่อยู่ต่ำกว่าถัดลงไป แต่ถ้าเป็นการรับข้อมูล ข้อมูลก็จะส่งจากข้างล่างขึ้นข้างบน แต่ละขั้นจะมีจุดเชื่อมต่อกับขั้นที่อยู่ใกล้เคียง เพื่อให้การติดต่อสื่อสารสำเร็จได้ การติดต่อสื่อสารของแต่ละขั้นจะเป็นแบบเพียร์ทูเพียร์ (Peer-to-Peer) หมายความว่าโปรโตคอลชั้นที่อยู่ฝั่งส่งจะติดต่อกับโปรโตคอลชั้นเดียวกันที่อยู่ฝั่งรับ ข้อมูลที่อยู่ในชั้นนี้จะมีความหมายเฉพาะกับโปรโตคอลที่อยู่ระดับเดียวกันของฝั่งตรงกันข้ามเท่านั้น

ถึงแม้ว่าข้อมูลจะถูกส่งไปยังโปรโตคอลชั้นที่อยู่ติดกัน แต่ละชั้นจะคิดว่าเป็นเหมือนกับการส่งข้อมูลไปยังชั้นเดียวกันที่อยู่อีกฝั่งหนึ่ง เพื่อให้การสื่อสารแบบนี้เกิดขึ้นได้ แต่ละชั้นจะทำการเพิ่มข้อมูลบางอย่างให้กับข้อมูลที่ได้รับมาจากชั้นที่อยู่บน ข้อมูลส่วนที่เพิ่มมานี้เรียกว่า “ข้อมูลส่วนหัว (Header)” ซึ่งข้อมูลในส่วนนี้จะเข้าใจและนำไปใช้เฉพาะโปรโตคอลที่อยู่ระดับเดียวกันของอีกฝ่ายเท่านั้น ทางฝั่งผู้ส่งข้อมูลส่วนหัวจะถูกเพิ่ม ส่วนทางฝั่งรับข้อมูลส่วนหัวจะถูกนำออก กระบวนการตามภาพด้านล่าง

ภาพที่ 2.3
การใช้ข้อมูลส่วนหัวในการสื่อสารระหว่างชั้น



จากรูป ข้อมูลในชั้นที่ 4 จะประกอบด้วยข้อมูลที่ส่งผ่านมาจากชั้นที่ 5 แล้วเพิ่มข้อมูลส่วนหัวเพื่อเป็นข้อมูลให้ชั้นที่ 4 ของอีกฝั่งตรงกันข้าม เสร็จแล้วข้อมูลชุดใหม่นี้จะถูกส่งต่อไปยังชั้นที่ 3 เมื่อชั้นที่ 3 ได้รับข้อมูลก็จะทำการแบ่งข้อมูลเดิมนี้เป็นแพ็กเก็ตย่อย ๆ แล้วเพิ่มข้อมูลส่วนหัวให้แต่ละแพ็ตเก็ต ซึ่งข้อมูลส่วนหัวนี้จะมีที่อยู่ของคอมพิวเตอร์ที่ต้องการส่งข้อมูลนี้ไปถึงอยู่ หลังจากนั้นแพ็ตเก็ตเหล่านี้ก็จะถูกส่งต่อไปยังชั้นที่ 2 หรือชั้นเชื่อมโยงข้อมูล ซึ่งชั้นนี้ก็จะเพิ่มข้อมูลส่วนหัว และเปลี่ยนรูปแบบแพ็ตเก็ตให้เป็นเฟรม ซึ่งในแต่ละเฟรมก็จะมีที่อยู่ของคอมพิวเตอร์ในชั้นนี้ แล้วเฟรมก็จะถูกส่งต่อไปยังชั้นกายภาพ ซึ่งจะทำการแปลงเฟรมให้เป็นบิตต่อเนื่องเพื่อทำการส่งต่อไปบนสื่อนำสัญญาณไปยังปลายทางต่อไป ส่วนการทำงานของฝั่งสถานีรับก็จะตรงกันข้ามกับสถานีส่ง กล่าวคือ แต่ละชั้นจะเอาส่วนที่เป็นข้อมูลส่วนหัวที่ถูกเพิ่มโดยชั้นที่อยู่ระดับเดียวกันออก เมื่อข้อมูลมาถึงชั้นที่ 4 ข้อมูลก็จะอยู่ในรูปแบบเดิมเหมือนกับตอนที่อยู่ในชั้นที่ 4 ของฝั่งสถานีส่ง

ในปัจจุบันระบบเครือข่ายมีโปรโตคอลที่ใช้หลายประเภทซึ่งพัฒนาโดยบางองค์กรหรือบางบริษัทโครงสร้างของโปรโตคอลเหล่านี้ก็แบ่งเป็นชั้น ๆ หรือเลเยอร์คล้ายกับแบบอ้างอิง OSI แต่อาจจะไม่เหมือนกันทุกเลเยอร์ บางชุดโปรโตคอลอาจแบ่งขั้นตอนการรับส่งข้อมูลแค่ 4-5

ชั้นเท่านั้น แทนที่จะเป็น 7 ชั้นเหมือนแบบอ้างอิง OSI ซึ่งการทำงานของแต่ละชั้นอาจจะไม่เป็นเหมือนของ OSI ทุกอย่าง อย่างไรก็ตามแบบอ้างอิง ก็ถือได้ว่าเป็นชุดโปรโตคอลที่เป็นต้นแบบสำหรับการศึกษา

ชุดโปรโตคอล OSI ประกอบด้วยโปรโตคอลมาตรฐานหลายโปรโตคอล โปรโตคอลเหล่านี้เป็นส่วนหนึ่งของโครงการนานาชาติเพื่อพัฒนาโปรโตคอลและมาตรฐานอื่น ๆ เพื่อเอื้ออำนวยให้อุปกรณ์เครือข่ายที่ผลิตจากบริษัทต่าง ๆ สามารถทำงานร่วมกันได้ ข้อกำหนดของมาตรฐาน OSI ถูกจัดทำโดย 2 องค์กร คือ ISO และ ITU-T

ภาพที่ 2.4

OSI Protocols

OSI Reference Model		OSI Protocols
7	Application	CMIP, OS, FTAM, MHS, VTP
6	Presentation	Presentation Service/Presentation Protocols
5	Session	Session Service/Session Protocol
4	Transport	TP0, TP1, TP2, TP3, TP4, TP5
3	Network	CONP/CMNS, CLNP/CLNS, IS-IS, ES-IS
2	Data Link	IEEE 802.2, IEEE 802.3, IEEE 802.5, FDDI, X.25
1	Physical	IEEE 802.2, IEEE 802.3, IEEE 802.5, FDDI, X.25 Hardware Hardware Hardware Hardware

<u>Layer 7: ชั้นประยุกต์ (Application Layer)</u>

โปรโตคอลชั้นที่อยู่บนสุดของแบบอ้างอิง OSI คือชั้นประยุกต์ (Application Layer) ถึงแม้ว่าชื่อจะเป็นแอพพลิเคชั่นเลเยอร์ก็ไม่ได้รวมเอาแอพพลิเคชั่นของผู้ใช้ด้วย (User Application) แต่โปรโตคอลในชั้นนี้จะเป็นจุดเชื่อมต่อระหว่างแอพพลิเคชั่นของผู้ใช้กับกระบวนการการสื่อสารผ่านเครือข่าย ชั้นนี้อาจจะถือได้ว่าเป็นชั้นที่เริ่มกระบวนการติดต่อสื่อสาร เช่น เมื่อผู้ใช้ต้องการส่งอีเมล โปรแกรมที่ผู้ใช้ส่งอีเมลจะทำการติดต่อกับโปรโตคอลในชั้นประยุกต์เพื่อเริ่มกระบวนการทั้งหมด ตัวอย่างของโปรโตคอลที่ทำงานในเลเยอร์นี้

File Transfer, Access and Management (FTAM) ให้บริการเกี่ยวกับการถ่ายโอนไฟล์ระหว่างคอมพิวเตอร์และการอ่าน การเขียน หรือแม้กระทั่งการลบไฟล์ที่อยู่ในอีกเครื่องหนึ่งได้

Vernal Protocol (VTP) ให้บริการเกี่ยวกับการเข้าใช้แอพพลิเคชั่นที่อยู่อีกเครื่องหนึ่งโดยการจำลองเทอร์มินอลของเครื่องที่อยู่ห่างไกลกับผู้ใช้

Message Handing Service (MHS) ให้บริการเกี่ยวกับการรับส่งอีเมล

Directory Service (DS) ให้บริการเกี่ยวกับการจับคู่ระหว่างชื่อและที่อยู่ของคอมพิวเตอร์

Common Management Information Protocol (CMIP) ให้บริการข้อมูลเกี่ยวกับการจัดการเครื่อข่าย

Layer 6: ชั้นนำเสนอ (Presentation Layer)

โปรโตคอลในชั้นนี้จะรับผิดชอบเกี่ยวกับรูปแบบของข้อมูลที่รับส่งผ่านเครือข่าย เนื่องจากคอมพิวเตอร์ที่ต้องการแลกเปลี่ยนข้อมูลกันนั้นอาจมีวิธีการเข้ารหัส (Encoding) ที่ต่างกัน เช่น คอมพิวเตอร์บางเครื่องอาจใช้เข้ารหัสแบบ ASCII (American Code for Information Interchange) หรือบางเครื่องอาจใช้การเข้ารหัสแบบ EBCDIC (Extended Binary Coded Decimal Interchange Code) ดังนั้นก่อนการส่งข้อมูลโปรโตคอลในเลเยอร์นี้ก็จะแปลงข้อมูลให้อยู่ในรูปแบบที่เป็นมาตรฐาน ส่วนทางด้านฝ่ายรับก็จะต้องทำการแปลงกลับไปเป็นรูปแบบที่คอมพิวเตอร์เครื่องนั้นเข้าใจ นอกจากนี้เลเยอร์นั้ยังรับผิดชอบในการทำให้ข้อมูลที่เข้ารหัสเลขทศนิยมที่ต่างกันสามารถแลกเปลี่ยนข้อมูลกันได้

Layer 5: ชั้นเซสชั่น (Session Layer)

เซสชั่นเลเยอร์ (Session Layer) ทำหน้าที่ควบคุมการสื่อสารผ่านเครือข่ายที่กำลังเกิดขึ้นระหว่างสองฝั่ง การสื่อสารที่กำลังเป็นไปในช่วงขณะใดขณะหนึ่งจะเรียกว่า “เซสชั่น (Session)” แอพพลิเคชั่นทั้งสองฝั่งสามารถแลกเปลี่ยนข้อมูลหรือรับส่งแพ็ตเก็ตถึงกันและกันได้ในช่วงเวลาที่เซสชั่นยังอยู่ โดยเซสชั่นเลเยอร์จะรับผิดชอบเกี่ยวกับการสร้างเซสชั่น ควบคุมการแลกเปลี่ยนข้อมูล และยกเลิกเซสชั่นเมื่อการสื่อสารสิ้นสุด

เซสชั่นเลเยอร์สามารถกำหนดรูปแบบการสื่อสารว่าเป็นแบบทางเดียว (Unidirectional) หรือแบบสองทาง (Bi-directional) ในการสื่อสารแบบสองทางนั้นยังสามารถกำหนดได้ว่าการไหลของข้อมูลนั้นเป็นไปได้สองทางพร้อมกันหรือไหลได้ทางเดียวในขณะใดขณะหนึ่ง ในการจัดการเกี่ยวกับการที่ให้ข้อมูลไหลไปทางเดียวในขณะใดขณะหนึ่งนั้นก็โดยการใช้โทเคน (Token) เฉพาะฝั่งที่มีโทเคนเท่านั้นถึงจะมีสิทธิ์ส่งแพ็ตเก็ต

อีกฟังก์ชั่นหนึ่งของเซสชั่นเลเยอร์ คือ การควบคุมจังหวะการรับส่งข้อมูล (Synchronization) ฟังก์ชั่นนี้ก็มีประโยชน์ในกรณีอย่างเช่น สมมุติว่ากำลังมีการถ่ายโอนไฟล์ระหว่างสองเครื่อง แล้วเครื่องใดเครื่องหนึ่งเกิดล้มเหลวกะทันหัน การถ่ายโอนไฟล์นั้นอาจต้องเริ่มใหม่ แต่เซสชั่นเลเยอร์มีฟังก์ชั่นที่กำหนดจุดเริ่มต้นของกระบวนการถ่ายโอนไฟล์ได้ โดยเมื่อเปิดเครื่องใหม่ก็เริ่มกระบวนการถ่ายโอนไฟล์ต่อจากเมื่อคราวก่อนหน้านี้ได้

Layer 4: ชั้นเคลื่อนย้ายข้อมูล (Transport Layer)

ชั้นเคลื่อนย้ายข้อมูล หรือทรานสปอร์ตเลเยอร์ (Transport Layer) รับผิดชอบในการเคลื่อนย้ายข้อมูลระหว่างโพรเซสส์ของผู้รับและโพรเซสส์ของผู้ส่ง โพรเซสส์ในที่นี้จะหมายถึงโปรแกรมที่กำลังรันบนเครื่องคอมพิวเตอร์ ซึ่งในขณะใดขณะหนึ่งอาจจะมีหลายโพรเซสส์ที่กำลังทำงานอยู่ ดังนั้นชั้นนี้จะรับผิดชอบในการรับส่งข้อมูลให้ถึงโพรเซสส์ที่ต้องการ หน้าที่อีกอย่างของโปรโตคอลในชั้นนี้คือ การตรวจเช็คแพ็คเก็ตที่ละทิ้งโดยเราท์เตอร์ และทำการส่งข้อมูลใหม่อีกครั้ง

หน้าที่ที่สำคัญอีกอย่างหนึ่งของชั้นนี้คือ การจัดเรียงแพ็คเก็ตข้อมูลที่อาจเดินทางถึงฝ่ายรับโดยไม่เป็นลำดับ การที่แพ็คเก็ตเดินทางถึงปลายทางไม่เป็นลำดับนี้เกิดขึ้นได้ เนื่องจากแพ็คเก็ตแต่ละแพ็คเก็ตอาจจะเดินทางคนละเส้นทาง หรือแพ็คเก็ตบางแพ็คเก็ตอาจสูญหายระหว่างทางแล้วมีการส่งใหม่อีกครั้ง อย่างไรก็ตามชั้นเคลื่อนย้ายข้อมูลนี้สามารถตรวจเช็คลำดับและจัดเรียงแพ็คเก็ตเหล่านี้ให้เหมือนเดิมก่อนที่จะส่งต่อชุดข้อมูลไปให้ชั้นเซสชั่นต่อไป

โปรโตคอลในชั้นแบ่งออกเป็น 2 ประเภทคือ Connection-Oriented และ Connectionless โดยโปรโตคอลของ OSI ในชั้นนี้ประกอบด้วย 5 โปรโตคอล ตั้งแต่ TPO (Transport Protocol Class 0) ไปจนถึง TP4 โดยมีเพียง TP4 เท่านั้นที่ให้บริการแบบ Connectionless โปรโตคอลในชั้นนี้มีดังต่อไปนี้

TP0 โปรโตคอลทำหน้าที่เกี่ยวกับการแบ่งข้อมูลที่จะส่งเป็นส่วนย่อย (Segmentation) ในกระบวนการส่ง และจัดเรียงส่วนย่อยของข้อมูลให้ได้ลำดับเดิม (Reassembly) กระบวนการรับข้อมูล ส่วนย่อยของข้อมูลจะเรียกว่า “PDU (Protocol Data Unit)”

TP1 ทำหน้าที่เหมือน TP0 แต่มีฟังก์ชั่นที่เพิ่มขึ้นมาคือ การกู้คืนข้อมูลจากข้อผิดพลาด โดยจะทำการส่ง PDU อีกครั้งถ้าไม่ได้รับการตอบรับ หรืออาจสร้างการเชื่อมต่อใหม่ถ้าหากพบว่ามี PDU จำนวนมากที่ไม่ได้รับการตอบรับ

TP2 เหมือนกับ TP0 อีกทั้งยังทำ Multiplex และ De multiplex กระแสข้อมูลบนวงจรเสมือน (Virtual Circuit)

TP3 คือการรวมกันระหว่าง TP1 และ TP2

TP4 ทำหน้าที่เหมือนกับ TP3 แต่สามารถให้บริการได้ทั้งแบบ Connection-Oriented และ Connectionless โปรโตคอลนี้ทำหน้าที่คล้ายกับโปรโตคอล TCP (Transmission Control Protocol) ของชุดโปรโตคอลอินเตอร์เน็ต

โปรโตคอลในเลเยอร์นี้สามารถให้บริการได้หลาย ๆ แอพพลิเคชั่นในเวลาเดียวกัน โดยการกำหนดที่อยู่เพื่อให้สำหรับติดต่อกับแต่ละแอพพลิเคชั่นที่อยู่อีกฝั่งหนึ่ง โดยที่อยู่ในที่นี้ส่วนใหญ่จะเรียกว่า Port แต่การเชื่อมต่อเข้ากับพอร์ตจะเรียกว่า Socket

Layer 3: ชั้นเครือข่าย (Network Layer)

ชั้นเครือข่าย จะรับผิดชอบในการจัดการเส้นทางให้กับข้อมูลระหว่างสถานีส่งและสถานีรับ ถ้ามีเส้นทางเดียว เช่น ถ้ามีคอมพิวเตอร์แค่สองเครื่องเชื่อมต่อกันโดยตรง การจัดเส้นทางคงไม่ยากเพราะมีแค่เส้นทางเดียว แต่ถ้าเป็นเครือข่ายที่ซับซ้อนการจัดเส้นทางก็ไม่ใช่เรื่องยากนัก ชั้นนี้จะไม่มีกลไกใด ๆ ในการตรวจสอบข้อผิดพลาดของข้อมูล ดังนั้น ฟังก์ชันจึงเป็นหน้าที่ของชั้นเชื่อมโยงข้อมูล

ชั้นเครือข่ายจะรับผิดชอบในการกำหนดเส้นทางข้อมูลระหว่างสถานีส่งและสถานีรับที่อยู่คนละเครือข่าย การที่จะทำเช่นนี้ได้ต้องมีระบบการจัดการที่อยู่ (Addressing) ที่ไม่อยู่กับที่อยู่ที่ใช้ในชั้นเชื่อมโยงข้อมูล

การให้บริการในเลเยอร์นี้จะแบ่งออกเป็น 2 ประเภท คือ

1. Connectionless Network Service การให้บริการแบบ Connectionless หมายถึงการส่งข้อมูลแบบไม่มีการสร้างการเชื่อมต่อก่อน โดยหวังว่าแพ็คเก็ตจะส่งถึงปลายทางแน่นอน ดังนั้น จึงไม่สามารถรับรองได้ว่าข้อมูลจะส่งถึงปลายทางสำเร็จ ดังนั้น โปรโตคอลชั้นที่อยู่สูงกว่าจะต้องรับผิดชอบในการตรวจสอบข้อผิดพลาดเอง โปรโตคอลที่ให้บริการแบบนี้ เช่น CLNP (Connectionless Network Protocol) และ CLNS (Connectionless Network Service)

2. Connection - Oriented Network Service เป็นการให้บริการเครือข่ายโดยมีการรับรองว่าข้อมูลจะส่งถึงปลายทางแน่นอน ซึ่งก่อนที่จะมีการส่งข้อมูลแต่ละครั้งนั้น จะมีการสร้างเส้นทางการเชื่อมต่อระหว่างสองสถานีก่อน และเมื่อรับส่งข้อมูลสำเร็จก็จะมีการยกเลิกเส้นทางการเชื่อมต่อดังกล่าว โปรโตคอลประเภทนี้ คือ CONP (Connection - Oriented Network Protocol) และ CMNS (Connection – Mode Network Service)

Network Address คือที่อยู่ หรือหมายเลขที่บ่งบอกเฉพาะของคอมพิวเตอร์ที่อยู่ในเครือข่าย โดยจะแบ่งออกเป็น 2 ชั้นคือ NSAP (Network Service Access Point) และ NET

(Network-Entity Title) NSAP เป็นจุดสมมติที่เชื่อมต่อระหว่างชั้นทรานสปอร์ต และชั้นเครือข่าย NSAP เป็นที่ ๆ โปรโตคอลในชั้นเครือข่ายจะให้บริการกับโปรโตคอลในชั้นทรานสปอร์ต ซึ่งแต่ละ Entity ในชั้นทรานสปอร์ตจะถูกกำหนดให้มีหมายเลข NSAP ที่ไม่ซ้ำกัน ส่วน NET นั้นเป็นหมายเลขที่บ่งบอกเน็ตเวิร์คของระบบโดยรวม หมายเลขนี้จะใช้กับ IS (Intermediate System)

Layer 2: ชั้นเชื่อมโยงข้อมูล (Data Link Layer)

เลเยอร์ที่สองของแบบอ้างอิง OSI มีชื่อว่าชั้นเชื่อมโยงข้อมูล ชั้นนี้ก็มีหน้าที่เหมือนกับชั้นอื่น ๆ คือ รับและส่งข้อมูล ซึ่งชั้นนี้จะรับผิดชอบในการรับส่งข้อมูลและมีการตรวจสอบความถูกต้องของข้อมูลด้วย ทางด้านสถานีส่งข้อมูลจะจัดข้อมูลให้เป็นเฟรม (Frame) ซึ่งในเฟรมจะมีข้อมูลที่ทำให้เฟรมสามารถส่งไปยังสถานีรับผ่านเครือข่ายท้องถิ่น (LAN) อย่างถูกต้องและสำเร็จ การส่งข้อมูลสำเร็จในที่นี้หมายถึง การที่เฟรมข้อมูลส่งถึงปลายทางที่สถานีส่งต้องการโดยที่เฟรมข้อมูลไม่มีข้อผิดพลาด ดังนั้นเฟรมต้องมีข้อมูลที่ใช้ในการตรวจสอบข้อผิดพลาดของเฟรมข้อมูลนั้น ๆ ด้วย การส่งข้อมูลสำเร็จนั้นเหตุการณ์ต่อไปนี้ต้องเกิดขึ้น

1. สถานีรับเมื่อได้รับเฟรมแล้วต้องตรวจสอบข้อผิดพลาดของข้อมูล แล้วแจ้งให้สถานีส่งทราบ

2. สถานีส่งต้องได้รับการตอบรับจากสถานีรับว่าได้รับเฟรมข้อมูลถูกต้องแล้ว

ในระหว่างการรับส่งข้อมูลอาจมีเหตุการณ์ต่าง ๆ เกิดขึ้น เช่น ข้อมูลส่งไปไม่ถึงปลายทาง หรือบางส่วนของเฟรมเสียหายหรือเกิดข้อผิดพลาดขึ้น ชั้นเชื่อมโยงข้อมูลจะรับผิดชอบในการตรวจสอบ และแก้ไขข้อผิดพลาดต่าง ๆ เหล่านี้ ชั้นเชื่อมโยงข้อมูลนี้ยังรับผิดชอบในการจัดบิตต่อเนื่องที่ส่งผ่านมาจากชั้นกายภาพให้เป็นเฟรมเหมือนเดิม การจัดบิตต่อเนื่องให้เป็นเฟรมเหมือนเดิมจะใช้บัฟเฟอร์แล้วส่งข้อมูลทีละบิตจนครบเฟรม ชั้นกายภาพและชั้นเชื่อมโยงข้อมูลนี้เป็นขั้นตอนที่ต้องมีการสื่อสารข้อมูลทุกประเภท โดยไม่สนใจว่าจะเป็น LAN หรือ WAN โปรโตคอลมาตรฐานที่ทำงานในชั้นนี้ก็เหมือนกับชั้นกายภาพ คือ IEEE 802.2 LLC, IEEE 802.3 (อีเธอร์เน็ต), IEEE 802.5 (โทเคนริง), FDDI และ X.25

Layer 1: ชั้นกายภาพ (Physical Layer)

เลเยอร์ที่อยู่ล่างสุด คือ ชั้นกายภาพ (Physical Layer) จะรับผิดชอบเกี่ยวกับการส่งข้อมูลที่เป็นบิต หรือ 0 กับ 1 ในระบบเลขฐานสอง (Binary) ชั้นนี้จะรับข้อมูลจากเลเยอร์ที่ 2 หรือชั้นเชื่อมโยงข้อมูล (Data Link Layer) ซึ่งข้อมูลชุดหนึ่งจะเรียกว่า “เฟรม (Frame)” และทำการส่ง

เฟรมของข้อมูลนี้ทีละบิตแบบเรียงตามลำดับ เหตุการณ์นี้จะเกิดขึ้นทางฝั่งสถานีที่ส่งข้อมูล ส่วนทางฝั่งสถานีรับข้อมูล ชั้นกายภาพก็จะทำการรับข้อมูลที่ส่งมาทีละบิตและจัดส่งผ่านข้อมูลที่เป็นบิตนี้ต่อไปยังชั้นเชื่อมโยงเพื่อทำการโพรเซสส์ต่อไป

ชั้นนี้จะเห็นข้อมูลเป็นเลขฐานสอง หรือเลข 1 กับ 0 เท่านั้น ซึ่งจะไม่สนใจความหมายของข้อมูลเลย เลเยอร์นี้จะสนใจเฉพาะการที่จะแปลงข้อมูลให้เป็นสัญญาณไฟฟ้าหรือแสงขึ้นอยู่กับสื่อกลางที่ใช้ และสามารถส่งไปบนสื่อกลางหรือสายสัญญาณได้เท่านั้น ซึ่งมาตรฐานจะกำหนดเกี่ยวกับความกดดันไฟฟ้าที่เป็นตัวนำสัญญาณ ประเภทของสายสัญญาณและความต้านทานของสายสัญญาณ แม้กระทั่งลักษณะของหัวเชื่อมต่อสายสัญญาณด้วย เลเยอร์ที่หนึ่งเป็นขั้นตอนหรือกลไกที่จำเป็นในการส่งสัญญาณข้อมูลไปบนสัญญาณ และรับสัญญาณนั้นจากสายสัญญาณ

2.1.3 <u>ความรู้พื้นฐานเกี่ยวกับโปรโตคอล TCP/IP</u>

การเชื่อมต่อคอมพิวเตอร์ให้เป็นเครือข่ายด้วยสายสัญญาณนั้นเป็นขั้นตอนที่ง่ายของการสร้างเครือข่าย แต่ส่วนที่ท้าทาย คือ การพัฒนามาตรฐานเพื่อให้คอมพิวเตอร์และอุปกรณ์เครือข่ายที่ผลิตโดยบริษัทต่าง ๆ สามารถติดต่อสื่อสารกันได้ ซึ่งมาตรฐานนี้คือ โปรโตคอล (Protocol)

โปรโตคอลของเครือข่ายบางทีเรียกว่า “สถาปัตยกรรมเครือข่าย (Network Architecture)” เนื่องจากระบบเครือข่ายคอมพิวเตอร์ในปัจจุบันเป็นระบบที่ซับซ้อนมาก ทำให้ยากต่อการออกแบบโดยคน ๆ เดียว หรือคนกลุ่มเดียว เพื่อให้การพัฒนาระบบเป็นไปอย่างมีประสิทธิภาพและง่ายขึ้น จึงมีการแบ่งโปรโตคอลออกเป็นชั้น ๆ หรือเลเยอร์ (Layer) การทำงานในแต่ละเลเยอร์จะไม่ซ้ำซ้อนกัน ซึ่งเลเยอร์ที่อยู่ต่ำกว่าจะทำหน้าที่ให้บริการกับชั้นที่อยู่สูงกว่า โดยเลเยอร์ที่อยู่สูงกว่าไม่จำเป็นต้องทราบถึงรายละเอียดว่าเลเยอร์ที่ต่ำกว่ามีวิธีให้บริการอย่างไร เพียงแค่รู้ว่ามีบริการอะไรบ้าง และแต่ละบริการคืออะไรก็เพียงพอ ซึ่งแนวความคิดนี้จะเรียกว่า “เทคโนโลยีเลเยอร์ (Layer Technology)”

2.1.3.1 แบบจำลอง TCP/IP

TCP/IP Model มีแนวคิดพื้นฐานแตกต่างจาก OSI Model คือไม่ได้มีพื้นฐานของการสื่อสารแบบการสนทนา TCP/IP Model เป็นภาพแสดงถึงโลกของระบบเครือข่ายสากล (Internetworking) ที่ทำการเคลื่อนย้ายและกำหนดเส้นทางให้กับข้อมูลระหว่างเครือข่ายและ

ระหว่างเครื่องคอมพิวเตอร์ต่างๆ เมื่อเปรียบเทียบความสัมพันธ์ระหว่างทั้ง 2 โมเดล จะพบว่ามีบางเลเยอร์ที่มีการกำหนดคุณสมบัติที่เทียบได้ไกล้เคียงกัน แต่บางเลเยอร์ก็ไม่สามารถเทียบหาความสัมพันธ์กันได้เลย

ปัจจุบันโปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) เป็นโปรโตคอลที่นิยมใช้ในเครือข่ายมากที่สุด เนื่องจาก

1. เป็นโปรโตคอลระบบเปิด (Open System) ที่ไม่มีบริษัทใดบริษัทหนึ่งเป็นเจ้าของลิขสิทธิ์ และข้อกำหนดของทุกโปรโตคอลจะถูกพัฒนาโดยองค์กรสาธารณะและมีการตีพิมพ์ให้ทราบ

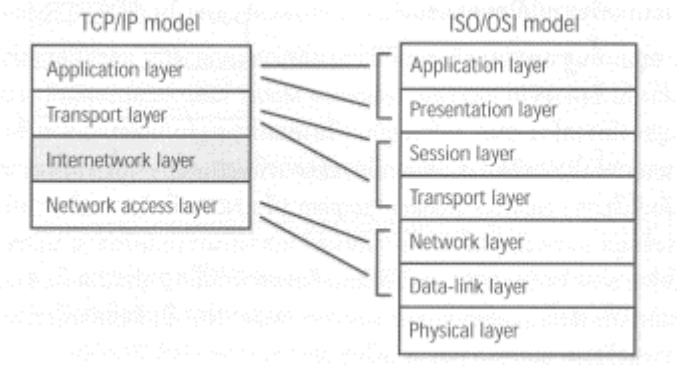
2. TCP/IP ถูกออกแบบมาเพื่อให้แพลตฟอร์มต่างกันสามารถสื่อสารกันได้ โปรแกรมบริการต่าง ๆ เช่น FTP (File Transfer Protocol) และ Telnet เป็นโปรแกรมที่ไม่ขึ้นต่อระบบเพียงแต่บริษัทนั้น ๆ พัฒนาระบบของตัวเองให้สามารถรองรับ TCP/IP ได้ก็สามารถสื่อสารกับระบบอื่นได้

3. โปรโตคอล TCP/IP ได้ถูกพิสูจน์แล้วว่าเป็นโปรโตคอลที่แข็งแกร่ง มีประสิทธิภาพสูง และมีความสามารถในการขยายตัวสูง ด้วยการใช้งานในเครือข่ายอินเตอร์เน็ต ซึ่งเป็นเครือข่ายที่ใหญ่ที่สุดในโลก

4. โปรโตคอล TCP/IP ได้กลายเป็นโปรโตคอลมาตรฐานกลางในการสื่อสารข้อมูลของคอมพิวเตอร์เนื่องจากเป็นภาษาที่ใช้ในระบบอินเตอร์เน็ต

ภาพที่ 2.5

Layer ต่าง ๆ ใน TCP/IP และ ISO/OSI Model



2.1.3.2 ชุดโปรโตคอล TCP/IP

ชุดโปรโตคอล TCP/IP (Transmission Control Protocol/Internet Protocol) ได้ถูกพัฒนามาแล้วกว่า 20 ปี ซึ่งเริ่มจากการวิจัยที่สนับสนุนโดยกระทรวงกลาโหมสหรัฐฯ จุดประสงค์ของการวิจัยนี้ก็เพื่อเชื่อมต่อคอมพิวเตอร์ที่ต่างแพลตฟอร์มกันให้สามาถสื่อสารกันผ่านเครือข่ายได้ ซึ่งสามารถทำได้โดยการแบ่งโปรโตคอลเป็นชั้นและเป็นการแยกการทำงานของแอพพลิเคชั่นของผู้ใช้ออกจากฮาร์ดแวร์ที่ใช้รับส่งข้อมูลผ่านเครือข่าย ชุดโปรโตคอลนี้จะมีการจัดรูปแบบที่แตกต่างจากแบบอ้างอิง OSI เล็กน้อย

การออกแบบชุดโปรโตคอล TCP/IP จะมุ่งเน้นไปที่การเชื่อมต่อระหว่างระบบที่ต่างกัน ในขณะที่แบบอ้างอิง OSI จะเน้นไปที่การแบ่งการทำงานของโปรโตคอลออกเป็นชั้น ๆ การออกแบบ TCP/IP ยังคงเป็นแบบชั้น ๆ เหมือนกัน แต่เมื่อถึงตอนทำจริง ๆ ก็จะให้ขึ้นอยู่กับการตัดสินใจของผู้ออกแบบ ซึ่งเป็นผลให้ชุดโปรโตคอล OSI เหมาะสำหรับใช้อธิบายสื่อสารระหว่างคอมพิวเตอร์ในเครือข่ายได้ดีกว่า ในขณะที่ชุดโปรโตคอล TCP/IP เป็นที่นิยมมากกว่าในการนำไปใช้จริง

ภาพที่ 2.6

ตารางเปรียบเทียบแบบอ้างอิง OSI and TCP/IP

<table>
<tr><th colspan="2">OSI Reference Model</th><th colspan="3">TCP/IP</th></tr>
<tr><td>7</td><td>Application</td><td rowspan="3">Application</td><td colspan="2" rowspan="3">FTP, Telnet, HTTP, SMTP, SNMP, DNS, etc.</td></tr>
<tr><td>6</td><td>Presentation</td></tr>
<tr><td>5</td><td>Session</td></tr>
<tr><td>4</td><td>Transport</td><td>Host – to – Host</td><td>TCP</td><td>UDP</td></tr>
<tr><td rowspan="2">3</td><td rowspan="2">Network</td><td rowspan="2">Internet</td><td>ICMP, IGMP</td><td rowspan="2">ARP
RARP</td></tr>
<tr><td>IP</td></tr>
<tr><td>2</td><td>Data Link</td><td rowspan="2">Network Access</td><td colspan="2" rowspan="2">Not Specified</td></tr>
<tr><td>1</td><td>Physical</td></tr>
</table>

TCP/IP จะแบ่งโปรโตคอลออกเป็น 4 ชั้นคือ ชั้นประยุกต์การใช้งาน (Application Layer), ชั้นเชื่อมต่อระหว่างโฮส (Host-to-host Layer), ชั้นอินเตอร์เน็ต (Internet Layer) และชั้นเข้าถึงเครือข่าย (Network Access Layer)

หลักการทำงานของโปรโตคอล TCP/IP คือ การสื่อสารจะเริ่มจากแอพพลิเคชั่นของผู้ใช้ส่งข้อมูลให้กับโปรโตคอลในชั้นแอพพลิเคชั่น หลังจากนั้นชั้นแอพพลิเคชั่นจะเพิ่มข้อมูลส่วนหัว

ซึ่งจะประกอบด้วย ชื่อของคอมพิวเตอร์ที่ต้องการสื่อสารด้วย และหมายเลขพอร์ตของเครื่องนั้น ข้อมูลก็จะถูกส่งต่อไปยังชั้นเชื่อมต่อโฮสต์ ซึ่งอาจจะใช้โปรโตคอล TCP หรือ UDP ขึ้นอยู่กับแอพพลิเคชั่นที่ใช้ เมื่อชั้นนี้ได้รับข้อมูลก็จะแบ่งข้อมูลออกเป็นส่วนย่อย ๆ ซึ่งแต่ละส่วนจะถูกเพิ่มข้อมูลส่วนหัวเข้าไป ข้อมูลส่วนย่อย ๆ นี้เรียกว่า Segment

ข้อมูลส่วนหัวของแต่ละ Segment จะถูกเพิ่มเข้าไปอย่างเหมาะสม หลังจากนั้นแต่ละ Segment ก็จะถูกส่งต่อไปให้ชั้นอินเตอร์เน็ต เมื่อข้อมูลมาถึงชั้นนี้ก็จะถูกเพิ่มข้อมูลส่วนหัวให้แต่ละ Segment เช่นกัน ข้อมูลที่เพิ่มเข้าไป เช่น หมายเลข IP, ประเภทของโปรโตคอลที่ใช้(TCP หรือ UDP) เป็นต้น ถ้าข้อมูลที่ส่งมามีการแบ่งย่อยอีกก็จะมีการเพิ่มข้อมูลที่เกี่ยวกับการแบ่งย่อยนี้เพิ่มเข้าไปด้วย ชุดข้อมูลที่อยู่ในชั้นนี้จะเรียกว่า Packet หลังจากนั้นแต่ละ Packet ข้อมูลก็จะส่งต่อไปให้ชั้นเข้าใช้เครือข่าย เพื่อทำการส่งข้อมูลไปตามช่องสื่อสารต่อไป เมื่อ Packet เดินทางไปถึงที่หมาย เครื่องปลายทางก็จะทำตามขั้นตอนที่ตรงกันข้ามกับเครื่องส่ง และข้อมูลก็จะถูกส่งผ่านต่อไปให้แอพพลิเคชั่นเพื่อนำข้อมูลไป Process ต่อไป

Layer 4: ชั้นประยุกต์การใช้งาน (Application Layer)

การทำงานของโปรโตคอลในชั้นนี้จะเป็นการเข้าใช้ทรัพยากรระยะไกล (Remote Access) และการแชร์ใช้ทรัพยากร (Resource Sharing) โปรโตคอลแอพพลิเคชั่นที่จัดอยู่ในชั้นนี้ได้แก่

HTTP (Hyper Text Transfer Protocol) ใช้สำหรับการรับส่งไฟล์เว็บเพจระหว่างเว็บบราวเซอร์และเว็บเซิร์ฟเวอร์

SMTP (Simple Mail Transfer Protocol) ใช้สำหรับการรับส่งอีเมล์ระหว่างเมล์เซิร์ฟเวอร์

POP (Post Office Protocol) ใช้สำหรับการดาวน์โหลดอีเมล์จากเมล์เซิร์ฟเวอร์

IMAP (Internet Message Access Protocol) ใช้สำหรับการดาวน์โหลดอีเมล์จากเซิร์ฟเวอร์

FTP (File Transfer Protocol) ใชสำหรับถ่ายโอนไฟล์ระหว่างโฮสต์

Telnet ใช้สำหรับการล็อกอินเข้าใช้โฮสต์ระยะไกล

Layer 3: ชั้นเชื่อมต่อระหว่างโฮส (Host-to-host Layer)

การทำงานในชั้นนี้จะคล้ายกับการทำงานในชั้นเซสชั่นและชั้นเคลื่อนย้ายข้อมูลของแบบอ้างอิง OSI ซึ่งในชั้นนี้จะมี 2 โปรโตคอลคือ TCP (Transmission Control Protocol) และ UDP (User Datagram Protocol) ซึ่งทั้งสองโปรโตคอลก็มีลักษณะการรับส่งข้อมูลที่แตกต่างกัน

โปรโตคอล TCP จะใช้การรับส่งข้อมูลแบบ Connection-Oriented ซึ่งการรับส่งข้อมูลแบบนี้จะหมายถึงการที่มีการสร้างการเชื่อมต่อก่อนที่จะส่งข้อมูลเพื่อให้แน่ใจว่าข้อมูลจะส่งถึงปลายทางอย่างแน่นอน และเมื่อทำการรับส่งข้อมูลเสร็จก็มีการยกเลิกการเชื่อมต่อที่สร้างไว้ ส่วนโปรโตคอล UDP จะใช้การรับส่งข้อมูลแบบ Connectionless หมายความว่าในแต่ละครั้งของการส่งข้อมูลจะไม่มีการสร้างการเชื่อมต่อกับเครื่องปลายทางก่อนส่ง ข้อมูลจะถูกส่งออกไปทันทีซึ่งมีการคาดหวังว่าเครื่องปลายทางจะได้รับข้อมูลที่ส่งไป ข้อแตกต่างระหว่างโปรโตคอล TCP และ UDP คือความเชื่อถือในการส่งข้อมูล การส่งแบบ TCP จะมีความเชื่อถือมากกว่า ในขณะที่การส่งแบบ UDP จะรวดเร็วกว่า แต่ก็มีโอกาสที่ข้อมูลอาจส่งไม่ถึงปลายทางได้

UDP เป็นอีกโปรโตคอลหนึ่งในชั้นเคลื่อนย้ายข้อมูล การรับส่งข้อมูลโดยใช้โปรโตคอล UDP เป็นการรับส่งข้อมูลที่มี Overhead น้อย โดยจะเรียกการเชื่อมต่อแบบนี้ว่า Datagram การสื่อสารแบบเรียบง่ายนี้อาจจะไม่เหมาะสำหรับบางแอพพลิเคชั่น แต่จะเหมาะสมกับแอพพลิเคชั่นที่มีระบบการเชื่อมต่อแบบ Connection-Oriented ในตัวเอง การใช้ UDP จะเหมาะสำหรับการใช้งานหลายอย่าง เช่น การประกาศชื่อคอมพิวเตอร์ของ NetBIOS,การกระจายข่าวสารของระบบ เป็นต้น เพราะการสื่อสารแบบนี้ไม่จำเป็นต้องมีการควบคุมการไหลของข้อมูล, การตอบกลับของผู้รับ, การจัดเรียงข้อมูลใหม่ หรือฟังก์ชันอื่น ๆ ที่ TCP มี

1. TCP (Transmission Control Protocol)

โปรโตคอล TCP (Transmission Control Protocol) เป็นโปรโตคอลที่ให้บริการแบบ Connection-Oriented ซึ่งเป็นการส่งข้อมูลที่เชื่อถือได้ TCP จะส่งข้อมูลทั้งหมดจนสำเร็จ ซึ่งถ้าข้อมูลมีขนาดใหญ่ก็จะถูกแบ่งย่อยเป็นหลายแพ็คเก็ต โปรโตคอล TCP จะทำหน้าที่ควบคุมการรับส่งแพ็คเก็ตข้อมูลย่อย ๆ เหล่านี้ สำหรับกลไกในการควบคุมการไหลของข้อมูล

เนื่องจาก TCP เป็นโปรโตคอลที่ให้บริการแบบ Connection-Oriented ดังนั้นก่อนที่จะมีการส่งข้อมูลจำเป็นที่ต้องสร้างเซสชั่นเพื่อเชื่อมต่อกับโฮสต์ปลายทางก่อน เซสชั่นเป็นการสร้างการสนทนาอย่างเป็นรูปแบบระหว่างทั้งสองโฮสต์เพื่อใช้สำหรับการกู้คืนข้อมูลเมื่อเกิดข้อผิดพลาดระหว่างการรับส่งข้อมูล ขั้นตอนในการสร้างเซสชั่นนี้จะมีอยู่ 3 ขั้นตอนซึ่งบางทีก็เรียกว่า “Three-Way Handshake”

1.โฮสต์ที่ต้องการส่งข้อมูลจะส่งแพ็คเก็ตไปยังโฮสต์ปลายทางเพื่อแจ้งให้ทราบว่าต้องการส่งข้อมูล

2. โฮสต์ปลายทางก็จะตอบตกลงกลับมาพร้อมทั้งรหัสที่จะใช้ในการรับส่งข้อมูล

3. โฮสต์ต้นทางก็จะส่งแพ็คเก็ตพร้อมรหัสที่ได้รับ เพื่อเป็นการยืนยันการเชื่อมต่อ หลังจากได้มีการสร้างเซสชั่นสำเร็จแล้วถึงจะเริ่มขบวนการรับส่งข้อมูลจริง ๆ ซึ่งการรับส่งข้อมูลแต่ละครั้งก็จะมีการยืนยันการรับข้อมูลจากโฮสต์ปลายทางทุกครั้ง เมื่อรับส่งข้อมูลเสร็จก็เป็นขั้นตอนการยกเลิกเซสชั่น ซึ่งจะคล้าย ๆ กับการสร้างเซสชั่น

ในแต่ละเซสชั่น โฮสต์ฝ่ายรับต้องตอบกลับทุก ๆ แพ็คเก็ตที่ได้รับภายในเวลาที่กำหนด เพื่อเป็นการยืนยันการรับข้อมูลทุก ๆ แพ็คเก็ตที่ส่ง ฝ่ายรับจะทำการเช็คความถูกต้องของแพ็คเก็ตข้อมูลทุกครั้ง และแจ้งให้ทราบถึงผลการตรวจสอบนั้น ถ้าฝ่ายส่งไม่ได้รับการตอบรับจากฝ่ายรับภายในเวลาที่กำหนด ฝ่ายรับก็จะคาดเอาว่าแพ็คเก็ตก็สูญหายระหว่างทาง ฝ่ายรับก็จะทำการส่งแพ็คเก็ตนั้นใหม่อีกครั้ง เพื่อทำให้มั่นใจได้ว่าข้อมูลทุก ๆ แพ็คเก็ตส่งถึงปลายทางอย่างสมบูรณ์ นอกจากนี้การแบ่งข้อมูลขนาดใหญ่ออกเป็นแพ็คเก็ตย่อย ๆ TCP ก็จะกำหนดหลายเลขลำดับ (Sequence Number) ให้แต่ละแพ็คเก็ตเพื่อใช้สำหรับการจัดรวมแพ็คเก็ตย่อย ๆ เหล่านั้นให้เป็นข้อมูลเหมือนเดิม นอกจากนี้หมายเลขลำดับยังใช้สำหรับการตรวจสอบว่าข้อมูลถูกส่งถึงปลายทางครบทุกแพ็คเก็ตหรือไม่

กลไกการตอบกลับแพ็คเก็ตนั้นมีอยู่ 2 ประเภท คือ PAR (Positive Acknowledgement and Retransmission) กลไกการทำงานคือ เมื่อฝ่ายส่งทำการส่งแพ็คเก็ตหนึ่ง ก็จะรอการตอบกลับจากฝ่ายรับ แล้วค่อยส่งแพ็คเก็ตต่อไป ถ้าไม่ได้รับการตอบกลับภายในเวลาที่กำหนดก็จะส่งแพ็คเก็ตนั้นอีกครั้ง ปัญหาของกลไกนี้คือ ถ้าข้อมูลประกอบด้วยหลาย ๆ แพ็คเก็ต และการที่ฝ่ายรับต้องส่งแพ็คเก็ตตอบรับต่อทุก ๆ แพ็คเก็ตที่ได้รับนั้นอาจเป็นการสิ้นเปลืองแบนด์วิธ และเป็นขบวนการที่ไร้ประสิทธิภาพเนื่องจากฝ่ายส่งจะใช้เวลาในการรอมากกว่าการส่งข้อมูล กลไกที่สองที่จะแก้ปัญหานี้เรียกว่า Sliding Window กลไกการทำงานคือ ฝ่ายรับสามารถยืนยันการรับแพ็คเก็ตโดยส่งแพ็คเก็ตเดียวสำหรับการยืนยันการรับหลายแพ็คเก็ต วิธีนี้จะช่วยลดจำนวนแพ็คเก็ตที่ต้องไหลเวียนในเครือข่าย และฝ่ายส่งสามารถส่งทีละหลาย ๆ แพ็คเก็ตก่อนที่จะรอการตอบรับ

เมื่อสร้างเซสชั่นสำเร็จ ขั้นตอนต่อไปคือการต่อรองเกี่ยวกับขนาดของ Window ซึ่งคือจำนวนไบต์ที่ฝ่ายรับได้รับก่อนที่จะทำการตอบกลับ หรือจำนวนไบต์ส่งสามารถส่งได้ก่อนที่จะรอการตอบกลับ การทำงานของ Sliding Window มีขั้นตอนดังนี้

1. เมื่อโฮสต์ต้องการที่จะส่งข้อมูล TCP จะย้ายข้อมูลไปไว้ที่บัฟเฟอร์ที่จะใช้ส่งข้อมูล ซึ่งข้อมูลส่วนนี้จะเรียกว่า Segment ซึ่งแต่ละ Segment อาจจะถูกแบ่งย่อยเป็นหลายแพ็คเก็ตซึ่งแต่ละแพ็คเก็ตก็จะถูกกำหนดหมายเลขลำดับ

2. ทุก ๆ แพ็คเก็ตใน Segment จะถูกส่งต่อไปให้โปรโตคอล IP เพื่อทำการส่งไปยังโฮสต์ปลายทาง

3. Segment ข้อมูลจะยังคงถูกเก็บไว้ที่บัฟเฟอร์จนกว่าจะได้รับการตอบรับจากโฮสต์ฝ่ายรับก่อนและโฮสต์ฝ่ายส่งจะตั้งเวลาเพื่อรอการตอบรับ ถ้าโฮสต์ฝ่ายรับไม่ตอบกลับภายในเวลาที่กำหนด ข้อมูลที่อยู่ในบัฟเฟอร์ก็จะถูกส่งใหม่อีกครั้ง

4. เมื่อแพ็คเก็ตเดินทางมาถึงฝ่ายรับ โฮสต์ฝ่ายรับก็จะใช้หมายเลขลำดับในการเรียบเรียงแพ็คเก็ตให้ได้เป็น Segment เหมือนเดิม

5. เมื่อโฮสต์ฝ่ายรับได้รับแพ็คเก็ตครบและตรวจสอบแล้วไม่มีข้อผิดพลาดใด ๆ ก็จะส่งแพ็คเก็ตตอบกลับไปยังโฮสต์ฝ่ายรับว่าได้รับข้อมูลครบหมดแล้ว

6. เมื่อโฮสต์ฝ่ายรับได้รับการตอบกลับ Segment ในบัฟเฟอร์ก็จะถูกลบทิ้งไปแล้วทำการส่ง Segment ถัดไปถ้ามี จนกว่าข้อมูลจะถูกส่งทั้งหมด

ขบวนการส่งข้อมูลแบบนี้จะทำให้มั่นใจได้ว่าข้อมูลจะถึงปลายทางอย่างแน่นอนและถูกต้อง ซึ่งการให้บริการแบบนี้เรียกว่า Connection-Oriented

ภาพที่ 2.7

ฟอร์แมตข้อมูลของแพ็คเก็ต TCP

32 bits

<table>
<tr><td colspan="3">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgement Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Flag</td><td>Window Size</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">Options + Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
</table>

ข้อมูลในส่วนหัวของโปรโตคอล TCP จะประกอบด้วยข้อมูลมากที่สุด 20 ไบต์ และประกอบด้วยส่วนต่าง ๆ ดังนี้

TCP Source Port (16 บิต) ส่วนนี้จะเป็นหมายเลขพอร์ตที่เป็นจุดเริ่มการสื่อสาร หมายเลขพอร์ตเมื่อรวมกับหมายเลข IP จะเป็นที่อยู่ของการส่งข้อมูลกลับ

TCP Destination Port (16 บิต) เป็นหมายเลขพอร์ตของเครื่องรับ ซึ่งพอร์ตนี้จะเป็นพอร์ตที่ใช้เชื่อมต่อกับแอพพลิเคชั่นที่จะนำข้อมูลที่ส่งไปให้นี้ไปทำการประมวลผลต่อไป

TCP Sequence Number (32 บิต) เป็นหมายเลขที่บอกลำดับแพ็คเก็ตที่จะใช้ โดยฝั่งเครื่องรับในการเรียงข้อมูลให้อยู่ในรูปแบบเดิม ในการส่งข้อมูลผ่านเครือข่ายที่สลับซับซ้อนนั้น แพ็คเก็ตแต่ละชุดอาจจะถูกส่งไปบนเส้นทางที่ต่างกัน ดังนั้น จึงเป็นไปได้ที่แพ็คเก็ตจะเดินทางมาถึงปลายทางไม่เป็นไปตามลำดับที่ส่ง หมายเลขนี้จะใช้ในการจัดเรียงแพ็คเก็ตเหล่านี้ให้อยู่ในลำดับเดิม

TCP Acknowledgement Number (32 บิต) เป็นหมายเลขลำดับแพ็คเก็ตถัดไปที่ทางฝั่งรับคาดหวัง ซึ่งเป็นการบอกเป็นนัยว่าแพ็คเก็ตที่มีหมายเลขลำดับก่อนหน้านี้ได้รับหมดแล้ว

Data Offset (4 บิต) เป็นตัวเลขที่บอกขนาดของข้อมูลส่วนหัว TCP Header ซึ่งมีหน่วยเป็น 32 บิต หรือ word

Reserved (6 บิต) ส่วนนี้จะถูกกำหนดให้เป็นศูนย์ตลอด ซึ่งข้อมูลส่วนนี้ไม่มีความหมายอะไรเพียงแต่เป็นการสงวนไว้ใช้ในอนาคตเมื่อมีการปรับปรุงโปรโตคอล

Flags (6 บิต) เป็นข้อมูลที่ใช้สำหรับควบคุมการรับส่งแพ็คเก็ต เช่น บิต SYN และ ACK ใช้สำหรับการสร้างการเชื่อมต่อ ส่วนบิต FIN เป็นการแจ้งการยกเลิกการเชื่อมต่อ เป็นต้น

Window Size (16 บิต) เป็นตัวเลขที่เครื่องปลายทางบอกให้เครื่องต้นทางทราบขนาดวินโดว์ที่เครื่องปลายทางสามารถรับข้อมูลได้

Checksum (16 บิต) เป็นข้อมูลที่ใช้ในการตรวจสอบข้อผิดพลาดของข้อมูลในส่วนตัว โดยเครื่องส่งจะทำการคำนวณค่า Checksum ของข้อมูลส่วนตัว เมื่อเครื่องปลายทางได้รับข้อมูลก็จะทำการคำนวณ Checksum ด้วยวิธีเดียวกัน แล้วทำการเปรียบเทียบข้อมูลค่าที่คำนวณได้กับที่อยู่ในฟิลด์นี้ ถ้าเหมือนกันแสดงว่าไม่มีข้อผิดพลาดในข้อมูลที่ได้รับ

Padding เป็นข้อมูลที่เพิ่มให้ข้อมูลส่วนหัวมีจำนวนบิตที่หารด้วย 32 ลงตัว

2. UDP (User Datagram Protocol)

โปรโตคอล UDP (User Datagram Protocol) จะให้บริการการส่งข้อมูลแบบ Connectionless หรือบางทีเรียกว่า Datagram ซึ่งจะเป็นการให้บริการแบบตรงกันข้ามกับ Connection-Oriented ของโปรโตคอล TCP การส่งข้อมูลแบบนี้จะเป็นแบบที่เชื่อถือไม่ได้ โดยจะพยายามส่งข้อมูลให้ดีที่สุด ในการรับส่งข้อมูลแต่ละครั้งนั้น จะไม่มีการสร้างเซสชั่นก่อน และไม่มีกลไกในการตอบกลับแพ็คเก็ตเหมือนโปรโตคอล TCP เหตุที่ตัดกลไกนี้ออกเพื่อเพิ่มประสิทธิภาพในการส่งข้อมูลนั่นเอง แต่ข้อเสียก็คือ การรับส่งเชื่อถือไม่ได้ เพราะแพ็คเก็ตอาจสูญเสียระหว่างทางซึ่งทางฝ่ายส่งจะไม่ทราบเลย ดังนั้นโปรโตคอลที่อยู่เหนือกว่าต้องรับผิดชอบเกี่ยวกับการตรวจสอบข้อผิดพลาดของการรับส่งข้อมูลเอง

ถึงแม้ว่าโปรโตคอล UDP จะมีความเชื่อถือน้อย แต่มันก็มีข้อดีหลายอย่าง เช่น ถ้าข้อมูลที่ต้องการส่งมีขนาดเล็กมากก็จะเป็นการเสียเวลา ถ้าต้องสร้างเซสชั่นการเชื่อมต่อระหว่าง 2 โฮสต์นั้นก่อนส่ง และอีกกรณีหนึ่งคือ การส่งข้อมูลแบบแพร่กระจาย หรือบรอดดาสต์ (Broadcast) และมัลติคาสต์ (Multicast) การสร้างเซสชั่นก็จะเป็นสิ่งที่เป็นไปได้ เนื่องจากเซสชั่นเป็นการเชื่อมต่อแบบ 2 โฮสต์เท่านั้น ดังนั้นการบรอดดาสต์ (Broadcast) และมัลติคาสต์ (Multicast) จะใช้โปรโตคอล UDP เท่านั้น

เนื่องจากโปรโตคอล UDP ไม่รับรองว่าข้อมูลจะส่งถึงปลายทาง ดังนั้นถ้าแอพพลิเคชั่นที่ใช้โปรโตคอลนี้ต้องการความเชื่อถือได้ของการส่งข้อมูล แอพพลิเคชั่นนั้นจะต้องควบคุมและตรวจสอบข้อผิดพลาดเอง ส่วนใหญ่แอพพลิเคชั่นที่ใช้โปรโตคอลนี้จะไม่ต้องการยืนยันการตอบรับ เช่น โปรโตคอลของระบบเครือข่ายของไมโครซอฟต์ เช่น การ Log on, Browsing และ Name Resolution เป็นต้น

ภาพที่ 2.8

ฟอร์แมตข้อมูลของแพ็ตเก็ค UDP

32 bits

Source Port	Destination Port
Length	Checksum
Data	

ข้อมูลในส่วนหัวของโปรโตคอล UDP นั้นแต่ละฟิลด์มีความหมายดังนี้

UDP Source Port Number (16 บิต) เป็นหมายเลขพอร์ตของเครื่องส่ง เมื่อรวมหมายเลขพอร์ตนี้กับหมายเลข IP ก็จะเป็นที่อยู่สำหรับเครื่องรับในการตอบกลับข้อความ

UDP Destination Port Number (16 บิต) เป็นหมายเลขพอร์ตของทางฝั่งเครื่องรับที่ใช้ในการส่งผ่านข้อมูลไปยังแอพพลิเคชั่นที่ต้องการติดต่อด้วย

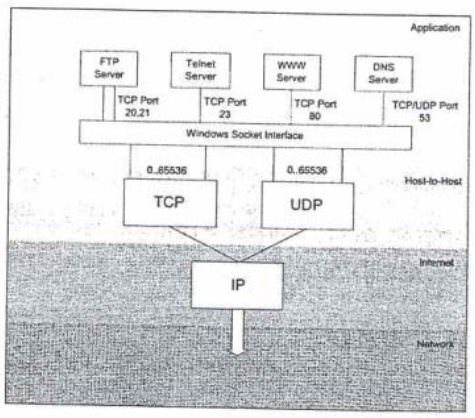
UDP Checksum (16 บิต) เป็นข้อมูลที่ใช้ในการตรวจสอบข้อผิดพลาดของข้อมูล เครื่องทางฝั่งรับจะทำการคำนวณหมายเลขนี้ด้วยวิธีเดียวกัน แล้วเปรียบเทียบกับค่าที่ส่งมา ถ้าหมายเลขเท่ากันแสดงว่าไม่มีข้อผิดพลาดในข้อมูลส่วนหัว

UDP Message Length (16 บิต) เป็นข้อมูลที่บอกความยาวของข้อมูลทั้งหมด ซึ่งจะเป็นข้อมูลที่ช่วยให้ทางฝ่ายรับทราบว่าข้อมูลควรมีขนาดเท่าใด

คอมพิวเตอร์ที่ใช้โปรโตคอล TCP/IP ส่วนใหญ่จะมีแอพพลิเคชั่นหลายตัวที่ใช้โปรโตคอล TCP/IP ในการสื่อสารกับเครื่องอื่น ซึ่งโปรโตคอล TCP/IP จะจัดการส่งข้อมูลไปยังแอพพลิเคชั่นที่เหมาะสม เพื่อให้ TCP/IP สามารถรองรับแอพพลิเคชั่นหลายแอพพลิชั่นในเครื่องเดียว จึงมีการใช้พอร์ตและซ็อกเก็ต (Port and Socket) เพื่อช่วยในการแยกแยะแอพพลิเคชั่น

ภาพที่ 2.9

รูปพอร์ต และซ็อกเก็ต (Post and Socket)



แอพพลิเคชั่นแต่ละตัวที่จะรับส่งข้อมูลผ่านเครือข่ายจะใช้หมายเลขพอร์ตตั้งแต่ 0 ถึง 65,536 ดังนั้นเพื่อให้การรับส่งข้อมูลถูกต้อง แอพพลิเคชั่นที่รันในเครื่องเดียวกันจะต้องใช้หมายเลขพอร์ตที่ต่างกันเพื่อช่วยลดความสับสน แอพพลิเคชั่นที่นิยมใช้กันทั่วไปส่วนใหญ่จะถูกกำหนดให้ใช้หมายเลขพอร์ตใดพอร์ตหนึ่ง ซึ่งองค์กรที่ทำหน้าที่กำหนดหมายเลขนี้คือ IANA

(Internet Assigned Numbers Authority) หมายเลขพอร์ตเหล่านี้จะถูกตีพิมพ์ใน RFC 1700 ซึ่งพอร์ตสำหรับแอพพลิเคชั่นที่นิยมใช้ทั่วไปดังตาราง

ภาพที่ 2.10

ตารางหมายเลขพอร์ตของบางแอพพลิเคชัน

พอร์ต	โปรโตคอล	แอพพลิเคชัน
20	TCP	FTP (Data)
21	TCP	FTP (Control)
23	TCP	Telnet
25	TCP	SMTP (อีเมล)
53	TCP/UDP	DNS (Domain Name System)
80	TCP	HTTP (เว็บเซิร์ฟเวอร์)
110	TCP	POP3 (อีเมล)
161	UDP	SNMP (Simple Network Management Protocol)

โปรโตคอล TCP/IP จะแยกแยะแอพพลิเคชั่นที่รันในแต่ละโฮสต์ โดยใช้ข้อมูล 3 ส่วนต่อไปนี้

1. หมายเลข IP ของโฮสต์นั้น
2. ประเภทของโปรโตคอลชันทรานสปอร์ต: TCP หรือ UDP
3. หมายเลขพอร์ตที่แอพพลิเคชั่นนั้นใช้

ตารางข้างต้นแสดงหมายเลขพอร์ตที่ใช้โดยทั่วไปโดยแอพพลิเคชั่นที่เป็นที่รู้จักโดยทั่วไป ส่วนเครื่องไคลเอนท์ที่เชื่อมต่อกับเซิร์ฟเวอร์จะใช้หมายเลขพอร์ตที่ต่างจากเซิร์ฟเวอร์ ซึ่งหมายเลขพอร์ตที่ใช้บนเครื่องไคลเอนท์จะถูกจัดการโดยระบบปฏิบัติการของเครื่องนั้น กล่าวคือ ถ้าไคลเอนท์จะเชื่อมต่อกับเว็บเซิร์ฟเวอร์ หมายเลขพอร์ตของเซิร์ฟเวอร์ที่ใช้ คือ พอร์ต 80 แต่เครื่องไคลเอนท์จะใช้หมายเลขพอร์ตอื่นที่ว่าง

Layer 2: ชั้นอินเตอร์เน็ต (Internet Layer)

การทำงานในชั้นอินเตอร์เน็ตนี้จะเทียบเท่ากับการทำงานในชั้นเครือข่าย (Network Layer) ของแบบอ้างอิง OSI ซึ่งชั้นนี้จะทำหน้าที่ในการส่งข้อมูลผ่านเครือข่ายต่าง ๆ ตามเส้นทางให้ถึงจุดหมาย ชุดข้อมูลที่อยู่ในชั้นนี้จะเรียกว่า Packet ซึ่งหน้าที่ของโปรโตคอลในชั้นนี้ก็คือ ส่งแพ็คเก็ตข้อมูลนี้ให้ถึงปลายทางโดยการจัดเส้นทางที่เหมาะสมให้กับแพ็คเก็ต โปรโตคอลหลักที่ทำงานในชั้นนี้ คือ IP (Internet Protocol)

การส่งแพ็คเก็ตในชั้นเครือข่ายจะเป็นแบบไม่มีการสร้างการเชื่อมต่อก่อนการส่ง หรือ Connectionless โดย Router จะเลือกเส้นทางที่ดีที่สุดในขณะนั้นให้กับแพ็คเก็ตนั้น ๆ การทำงานของชั้นนี้จะไม่มีการให้บริการตอบรับ, การควบคุมการไหลของข้อมูล, การเรียงลำดับแพ็คเก็ต เหมือนกับที่มีในโปรโตคอล TCP ซึ่งฟังก์ชั่นต่าง ๆ เหล่านี้จะเป็นหน้าที่ของโปรโตคอลที่ชั้นสูงกว่ารับผิดชอบ

นอกจากโปรโตคอล IP แล้ว ในชั้นอินเตอร์เน็ตนี้ยังมีโปรโตคอลอื่น ๆ ที่ช่วยให้การทำงานของโปรโตคอล IP เป็นไปด้วยดี เช่น

ICMP (Internet Control Message Protocol) ใช้สำหรับการรายงานข้อผิดพลาดในระหว่างการรับส่งแพ็คเก็ต IP

IGMP (Internet Group Message Protocol) ให้สำหรับการรายงานโฮสต์ที่เป็นสมาชิกในกลุ่มของ Multicast

ARP (Address Resolution Protocol) ใช้สำหรับการแปลงหมายเลข IP เป็นที่อยู่ในเลเยอร์ที่ 2 (MAC Address)

RARP (Reversed Address Resolution Protocol) ทำงานในทางตรงกันข้ามกับ ARP

Layer 1 ชั้นเข้าถึงเครือข่าย (Network Access Layer)

ตามมาตรฐานแล้วชุดโปรโตคอล TCP/IP ไม่ได้มีการกำหนดมาตรฐานสำหรับชั้นเข้าถึงเครือข่าย (Network Access) อย่างไรก็ตาม TCP/IP สามารถใช้ได้กับเน็ตเวิร์คหลายประเภท โดยเน็ตเวิร์คที่ใช้งานมากที่สุด คือ อีเธอร์เน็ต นอกจากนี้แพ็คเก็ตของ TCP/IP ยังสามารถส่งผ่านเน็ตเวิร์คอื่น ๆ ได้ เช่น FDDI, ATM, X.25, Frame Relay, PPP, SLIP และ ISDN เป็นต้น

2.1.4 ความรู้เบื้องต้นเกี่ยวกับเทคโนโลยีระบบความปลอดภัยบนเครือข่ายอินเทอร์เน็ต

2.1.4.1 นิยามของความมั่นคงปลอดภัยคอมพิวเตอร์

การปกป้องความมั่นคงปลอดภัยของระบบและข้อมูลภายในองค์กรถือเป็นเรื่องสำคัญในปัจจุบัน ทั้งนี้เนื่องจากการถูกคุกคามโดยผู้ไม่ประสงค์ดีหรือจากโปรแกรมบางประเภทได้เพิ่มมากขึ้นและอาจนำมาซึ่งความเสียหายอย่างมากต่อองค์กร ดังนั้นถ้าภายในระบบมีการควบคุมความปลอดภัยที่ดีจะช่วยลดโอกาสเสี่ยงต่อการถูกคุกคามได้

ในปัจจุบันระบบคอมพิวเตอร์ได้ถูกคุกคามมากขึ้นทั้งจากไวรัสคอมพิวเตอร์หรือจากผู้ไม่ประสงค์ดี ซึ่งความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Security) ช่วยปกป้องเครื่องคอมพิวเตอร์รวมไปถึงอุปกรณ์ต่างๆที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบหรือใช้ในความหมายความปลอดภัยทางข้อมูลสารสนเทศ (Information Security) ก็ได้ จุดประสงค์หลักของความปลอดภัยทางข้อมูลคือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่างๆภายในองค์กร (CIA-N) โดยมีรายละเอียดดังนี้

1. การรักษาความลับ (Confidentiality) คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้

2. การรักษาความสมบูรณ์ (Integrity) คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดย อุบัติเหตุหรือโดยเจตนา

3. ความพร้อมใช้ (Availability) คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้ได้ในเวลาที่ต้องการใช้งาน

4. การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) คือวิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

ในทางปฏิบัตินั้นสามารถกำหนดลักษณะของการควบคุมความมั่นคงปลอดภัย (Security Controls) ได้ 5 ระดับตามรูป

ภาพที่ 2.11

Security Pyramid

ที่มา: Doug Graham, "It's all about authentication", SANS Reading Room, 15 March 2003

และถือเป็นองค์ประกอบที่สำคัญส่วนหนึ่งของความมั่นคงปลอดภัยคอมพิวเตอร์ เพราะจัดเป็นการกำหนดและควบคุมทั้งบุคคลที่สามารถเข้าสู่ระบบและเข้าสู่ข้อมูลภายในระบบ และเพื่อกระทำการใดได้บ้าง อนุญาตตามระดับชั้นของความสำคัญของข้อมูล รวมไปถึงการจัดเก็บพฤติกรรมการใช้งานระบบของบุคคลนั้นต่อข้อมูลบนระบบทั้งหมด

1. การพิสูจน์ตัวตน (Authentication)

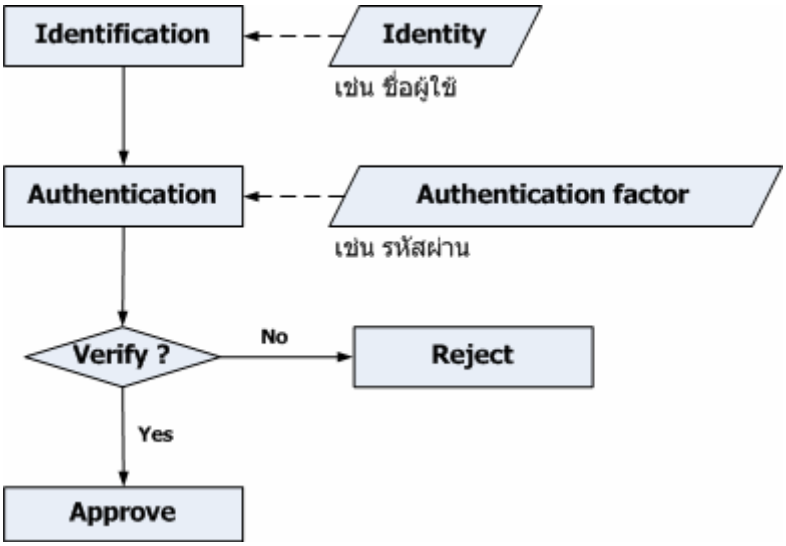
การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

1.1 การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (username)

1.2. การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

ภาพที่ 2.12

แผนผังแสดงกระบวนการการพิสูจน์ตัวตน



จากแผนผังแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้จะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐานที่ผู้ใช้นำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้จะถูกปฏิเสธจากระบบรหัสผ่านร่วมกับการใช้บัตร ATMเป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกัน

2. การกำหนดสิทธิ์ (Authorization)

การกำหนดสิทธิ์ คือขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตน และต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

3. การเข้ารหัส (Encryption)

การเข้ารหัส คือการเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วนที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้

หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่งที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่เข้ารหัสแล้วได้

4. การรักษาความสมบูรณ์ (Integrity)

การรักษาความสมบูรณ์ คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (Source) ไม่ว่าจะเป็นโดยบังเอิญหรือดัดแปลงโดยเจตนาที่อาจส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูลคือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะเข้าควบคุมการจัดการของข้อมูลได้

5. การตรวจสอบ (Audit)

การตรวจสอบ คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่นการตรวจสอบบัญชีชื่อผู้ใช้ โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

2.1.4.2 ประเภทของการพิสูจน์ตัวตน (Authentication Types)

2.1.4.2.1 ไม่มีการพิสูจน์ตัวตน (No Authentication)

ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น ถ้าเงื่อนไขต่อไปนี้เป็นจริง ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือ ข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้นๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

2.1.4.2.2 การพิสูจน์ตัวตนโดยใช้รหัสผ่าน (Authentication by Passwords)

รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นที่ทราบ

แต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่าย

เกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

2.1.4.2.3 การพิสูจน์ตัวตนโดยใช้ PIN (Authentication by PIN)

PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่นบัตร ATM และเครดิตการ์ดต่างๆ

การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่นฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

2.1.4.2.4 การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens (Authentication by Password Authenticators or Tokens)

Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง "รหัสผ่านซึ่งเปลี่ยนแปลงได้ (dynamic password)" อุปกรณ์ Token เป็นอุปกรณ์สำหรับสร้างรหัสลับ ที่สามารถใช้เข้าระบบได้เพียงครั้งเดียว (One Time Password) โดยก่อนที่ท่านจะใช้อุปกรณ์ Token ได้ท่านจะต้องทราบ "รหัส Token" ก่อนเพื่อใช้เข้าไปสร้างรหัสลับในอุปกรณ์ Token

ภาพที่ 2.13

Authenticators' หรือ token ที่ใช้สำหรับสร้างรหัสผ่านซึ่งเปลี่ยนแปลงได้

ที่มา: http://www.securecomputing.com/index.cfm?sKey=665

2.1.4.2.5 การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric traits)

ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่นการใช้ควบคู่กับการใช้รหัสผ่าน

2.1.4.2.6 การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว (One-Time Password: OTP)

One-Time Password ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำๆกัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้จะเข้าสู่ระบบ

การทำงานของ OTP คือเมื่อผู้ใช้ต้องการจะเข้าใช้ระบบ ผู้ใช้จะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง challenge string กลับมาให้ผู้ใช้ จากนั้นผู้ใช้จะนำ challenge string และรหัสลับที่มีอยู่กับตัวของผู้ใช้นำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า response ผู้ใช้ก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้ส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้ เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้เข้าสู่ระบบ

2.1.4.2.7 การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key cryptography)

เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

2.1.4.2 โพรโตคอลในการพิสูจน์ตัวตน (Authentication Protocol)

ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโตคอลในการพิสูจน์ตัวตน คือโพรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโตคอล

โพรโตคอลการพิสูจน์ตัวตนที่กล่าวถึงในเอกสารฉบับนี้ เน้นเฉพาะโพรโตคอลหลักที่นิยมใช้อย่างแพร่หลายบนอินเตอร์เน็ตในปัจจุบัน ประกอบไปด้วย

2.1.4.2.1 Secure Socket Layer (SSL)

Secure Sockets Layer (SSL) เริ่มพัฒนาโดย Netscape Communications เพื่อใช้ในโพรโตคอลระดับแอพพลิเคชันคือ Hypertext Transfer Protocol (HTTP) ซึ่งเป็นการสื่อสารผ่านเว็บให้ปลอดภัย พัฒนาในช่วงต้นของยุคการค้าอิเล็กทรอนิคส์กำลังได้รับความนิยมในโลกอินเตอร์เน็ต

SSL ทำให้เกิดการสื่อสารอย่างปลอดภัยระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ โดยการอนุญาตให้มีกระบวนการพิสูจน์ตัวตนร่วมกับการใช้งานลายเซ็นดิจิตอลสำหรับการรักษาความถูกต้องของข้อมูลและการเข้ารหัสข้อมูลเพื่อป้องกันความเป็นส่วนตัวระหว่างการสื่อสารข้อมูล

2.1.4.2.2 Secure Shell (SSH)

SSH เวอร์ชัน 1 พัฒนาขึ้นในปี 1995 โดย Tatu Ylonen ขณะที่เป็นนักวิจัยของมหาวิทยาลัยแห่งหนึ่งในฟินแลนด์ เพื่อแก้ปัญหาการดักจับรหัสผ่านที่เกิดขึ้นในระบบเครือข่าย และเผยแพร่ซอร์สโค้ดและเปิดให้ดาวโหลดไปใช้งานได้ฟรี ปลายปีเดียวกันได้จัดตั้งบริษัท SSH Communications Security, Ltd. (SCS) และเปิดตัว SSH เวอร์ชัน 2 ในต้นปี 1996 ในรูปของการค้า แต่ไม่สามารถทำงานร่วมกับ SSH เวอร์ชัน 1 ส่งผลให้มีการใช้งาน SSH เวอร์ชัน 1 แพร่หลายมากกว่าในเวลานั้น

2.1.4.2.3 Internet Protocol Security (IPsec)

IPsec เป็นส่วนเพิ่มขยายของ Internet Protocol (IP) ในชุดโพรโตคอล TCP/IP พัฒนาเพื่อเป็นส่วนหนึ่งของมาตรฐานของ IPv6 ซึ่งเป็นโพรโตคอลที่พัฒนาเพื่อใช้แทน IPv4 ที่ใช้ในปัจจุบันและกำหนดหมายเลข RFC เป็น RFC2401

IPsec ใช้โพรโตคอล 2 ชุดคือ Authentication Header (AH) และ Encapsulated Security Payload (ESP) เพื่อรองรับการพิสูจน์ตัวตน (Authentication) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความลับ (Confidentiality) ในระดับชั้นของ IP

2.1.4.2.4 Kerberos

การพิสูจน์ตัวตนแบบ Kerberos พัฒนาขึ้นโดย Massachusetts Institute of Technology หรือ MIT

ระบบ Kerberos ประกอบขึ้นจากสองส่วนหลักคือ

1. Ticket ใช้สำหรับการพิสูจน์ตัวตนของผู้ใช้ในระบบ และการเข้ารหัสข้อมูล

2. Authenticator ใช้ในการตรวจสอบ Ticket ว่าเป็นผู้ใช้คนเดียวกันที่ใช้ Ticket เป็นใบเบิกทางเข้าสู่ระบบและเป็นผู้ใช้ที่ระบบสร้างให้อย่างถูกต้อง

Kerberos เซิร์ฟเวอร์ มีสองส่วนบริการในการใช้งานคือ Authentication service (AS) สำหรับการพิสูจน์ตัวตนของผู้ใช้กับ Kerberos เซิร์ฟเวอร์ก่อนการเข้าใช้บริการ Ticket Granting Service (TGS) เป็นบริการที่ออก Ticket เพื่อให้ผู้ใช้นำไปใช้กับเซิร์ฟเวอร์ที่ต้องการ

การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ควรตระหนักเป็นอย่างยิ่งในปัจจุบัน เพราะโลกในยุคปัจจุบันเป็นโลกแห่งข้อมูลข่าวสาร การเก็บรักษาข้อมูลให้ปลอดภัยจึงเป็นสิ่งสำคัญกับตัวบุคคลและองค์กร เพราะฉะนั้นการที่จะอนุญาตให้บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลจึงเป็นสิ่งที่ควรระมัดระวัง เพราะข้อมูลบางอย่างของบุคคลและองค์กรมีความสำคัญและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้

การพิสูจน์ตัวตนจึงมีความสำคัญ เนื่องจากว่าการที่บุคคลใดบุคคลหนึ่งจะเข้าสู่ระบบได้ จะต้องได้รับการยอมรับว่าได้รับอนุญาตจริง การตรวจสอบหลักฐานจึงเป็นขั้นตอนแรกก่อนอนุญาตให้เข้าสู่ระบบ การยืนยันตัวตนยิ่งมีความซับซ้อนมาก นั่นก็หมายถึงว่าความปลอดภัยของข้อมูลก็มีมากขึ้นด้วย

2.1.5 <u>ประวัติความเป็นมาของ Internet Banking</u>

จุดเริ่มของการใช้บริการ Internet Banking นั้นเริ่มจาก ธนาคาร Security First Network Bank (SFNB) ซึ่งก่อตั้งในปี ค.ศ.1995 โดยมีทุนจดทะเบียน $ US 44.6 ล้านดอลลาร์ จุดเด่นของธนาคาร คือ ไม่มีสาขาย่อยที่คอยให้บริการลูกค้า การให้บริการทั้งหมดจะทำผ่านระบบเครือข่ายอินเทอร์เน็ตเพียงอย่างเดียว ธนาคารนี้จึงได้เติบโตขึ้นอย่างรวดเร็ว ภายใน 1 ปี หลังจากการก่อตั้ง ธนาคารได้มีจำนวนลูกค้าเพิ่มขึ้นจากไม่กี่ร้อยคน เป็นประมาณ 4,000 คน ซึ่งเป็นอัตราการเติบโตที่ดีมากสำหรับธนาคารที่เปิดขึ้นใหม่

การเติบโตอย่างรวดเร็วของ On-line Banking เช่น ธนาคาร SFNB นั้นได้สร้างความตื่นตระหนกให้กับธนาคารยักษ์ใหญ่เป็นอย่างมาก เนื่องจากเทคโนโลยีนี้ได้ทำให้ส่วนแบ่งการตลาดแบบท้องถิ่น (Banking Territory) ซึ่งเน้นความใกล้ชิดและความคุ้นเคยกับลูกค้าเพราะระบบ On-Line Banking สามารถให้บริการด้านการเงินได้ทั่วโลกโดยไม่จำกัดพื้นที่

ดังนั้นธนาคารยักษ์ใหญ่จึงเปลี่ยนกลยุทธ์และแนวคิดใหม่ทางการตลาดซึ่งต้องอาศัย On-Line Banking เป็นหลักอย่างเช่น ความสำเร็จอันงดงามในการประยุกต์ใช้เทคโนโลยีใหม่นี้ของธนาคาร Well Fargo ซึ่งใช้ระบบนี้เป็นตัวผลักดันจากระบบท้องถิ่นไปสู่ระดับโลกได้

Wells Fargo Online (www.wellsfargo.com) เป็นเว็บไซต์ให้บริการธนาคารออนไลน์ที่มีลูกค้าใช้บริการมากที่สุดในสหรัฐฯ ธนาคาร Wells Fargo เริ่มให้บริการโอนเงินผ่านโทรเลข ซึ่งเป็นจุดเริ่มต้นในการนำระบบอิเล็กทรอนิกส์มาใช้กับธนาคารเป็นครั้งแรก เมื่อปี 2532 ธนาคารเริ่มให้บริการธนาคารอิเล็กทรอนิกส์ที่เรียกว่า PC Banking ซึ่งเป็นการให้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบของธนาคาร อย่างไรก็ตาม PC Banking ไม่ได้รับความนิยมแพร่หลายมากนัก เนื่องจากลูกค้าไม่ได้รับความสะดวกในการเชื่อมต่อกับระบบเมื่ออยู่ต่างรัฐ ซึ่งมีอัตราค่าบริการโทรศัพท์ระหว่างรัฐสูง

ต่อมา ธนาคารได้ให้บริการศูนย์บริการลูกค้าทางโทรศัพท์ (Call Center) หรือที่เรียกว่าบริการธนาคารทางโทรศัพท์ (Telephone Banking) ซึ่งให้บริการลูกค้าทำธุรกรรมกับธนาคารผ่านทางโทรศัพท์ เช่น การสอบถามยอดเงินในบัญชี และการโอนเงิน เป็นต้น

เมื่อเดือนพฤษภาคม 2538 ธนาคาร Wells Fargo เป็นธนาคารแห่งแรกที่ริเริ่มให้บริการธนาคารทางอินเทอร์เน็ต ธนาคาร Wells Fargo หวังว่าบริการดังกล่าวช่วยลดค่าใช้จ่ายในการดำเนินงานและอำนวยความสะดวกให้แก่ลูกค้าเพิ่มขึ้น

ในปัจจุบัน ธนาคาร Wells Fargo ได้พัฒนารูปแบบในการให้บริการลูกค้าผ่านทางช่องทางใหม่ ๆ ดังต่อไปนี้

1. บริการธนาคารทางโทรศัพท์ (Telephone Banking) เป็นบริการให้ลูกค้าทำธุรกรรมกับธนาคารผ่านทางโทรศัพท์ ซึ่งลูกค้าสามารถโทรผ่านหมายเลขโทรศัพท์ที่ไม่ต้องเสียค่าใช้จ่ายใด ๆ ทั้งสิ้น (Toll-Free Number)

2. บริการสำนักงานสาขาของธนาคารในร้านขายของชำ (Grocery Store Branches) เป็นบริการสำนักงานสาขาในรูปแบบที่เล็กลง และให้บริการทำธุรกรรมบางอย่างเท่านั้น เช่น การฝากเงิน การถอนเงิน การโอนเงิน เป็นต้น

3. บริการธนาคารอินเทอร์เน็ต (Internet Banking) ให้บริการลูกค้าติดต่อทำธุรกรรมกับธนาคารผ่านทางอินเทอร์เน็ต โดยธนาคารจะไม่คิดค่าใช้จ่ายใด ๆ ทั้งสิ้น

จุดเด่นในการประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์ของธนาคาร Wells Fargo คือการเป็นผู้ริเริ่มให้บริการธนาคารทางอินเทอร์เน็ตให้แก่ลูกค้าเป็นรายแรก ๆ ทำให้ชื่อเสียงของธนาคารเป็นที่รู้จักในการให้บริการดังกล่าว

จุดเด่นอีกประการของธนาคาร Wells Fargo คือ การเน้นให้บริการแก่กลุ่มลูกค้ารายย่อย (Retail Banking) ซึ่งมีต้นทุนในการให้บริการสูงกว่าเมื่อเปรียบเทียบกับการให้บริการกลุ่มลูกค้าขนาดใหญ่ (Wholesale Banking) ธนาคารจึงต้องพัฒนาหาช่องทางใหม่ ๆ เพื่อช่วยลดค่าใช้จ่ายในการให้บริการลูกค้าอยู่เสมอ เช่น บริการธนาคารผ่านโทรศัพท์ บริการสำนักงานสาขาขนาดเล็กของธนาคารภายในร้านค้าปลีกขนาดใหญ่ และบริการธนาคารออนไลน์ เป็นต้น

การเริ่มต้นการสื่อสารผ่านเครือข่ายระบบเครือข่ายทางอินเตอร์เน็ตของธนาคารพาณิชย์ไทยนั้น เริ่มเข้ามาเป็นส่วนหนึ่งในการดำรงชีวิตประจำวัน และพฤติกรรมผู้บริโภคหันมานิยมซื้อขายสินค้า/บริการต่าง ๆ บนอินเตอร์เน็ตและชำระเงินผ่านบัตรเครดิต หรือบัญชีเงินฝาก ส่งผลให้ธุรกิจหลายประเภทเห็นช่องทาง และสนใจในการดำเนินธุรกิจผ่านสื่อนี้มากขึ้น ธุรกิจธนาคารพาณิชย์ก็เช่นเดียวกันได้มีการปรับตัวและพัฒนาบริการต่าง ๆ ผ่านสื่ออินเตอร์เน็ตเพื่อรองรับความต้องการของลูกค้า และเพิ่มศักยภาพรองรับการแข่งขันที่ทวีสูงขึ้น โดยการดำเนินธุรกิจธนาคารผ่านสื่ออินเตอร์เน็ต

ธนาคารพาณิชย์ได้มีการพัฒนานำเทคโนโลยีเข้ามาสู่ธุรกิจมากขึ้น ดังจะเห็นได้จาก

ยุคแรก ธนาคารพาณิชย์ในประเทศไทย ได้มีการพัฒนาระบบการทำงาน โดยการนำระบบคอมพิวเตอร์มาใช้ในกิจการธนาคาร เพื่อการจัดเก็บ และรวบรวมข้อมูลด้านบัญชี เงินฝาก สินเชื่อ และงานอื่น ๆ ภายในสำนักงาน ตลอดจนอำนวยความสะดวก รวดเร็วในการปฏิบัติ และขจัดปัญหาด้านการเก็บรักษาเอกสาร

ยุคที่ 2 ธนาคารพาณิชย์ได้พัฒนางานด้านคอมพิวเตอร์ให้ทันสมัย สอดคล้องกับสภาวะการณ์ที่เปลี่ยนแปลงในยุคของการพัฒนาด้านการสื่อสาร การเข้าถึงข้อมูลข่าวสารได้อย่างรวดเร็ว ประหยัดเวลา ลดค่าใช้จ่ายในการดำเนินงาน และนำคอมพิวเตอร์มาประยุกต์ใช้กับธุรกิจธนาคารได้อย่างมีประสิทธิภาพให้แก่ลูกค้าด้วยการเริ่มก้าวสู่ระบบที่เรียกว่า “ธนาคารอิเล็กทรอนิกส์” เพื่ออำนวยความสะดวกให้แก่ลูกค้าในการให้บริการของธนาคาร เมื่อนำบริการเงินด่วน หรือเอทีเอ็มเข้ามาให้บริการ และขยายบริการไปสู่ธนาคารทางโทรศัพท์

ยุคที่ 3 ภายหลังจากเผชิญปัญหาวิกฤตเศรษฐกิจที่ผ่านมา ธนาคารพาณิชย์ก็ได้พยายามปรับตัวและหันมาสนใจการดำเนินกลยุทธ์ทางการตลาดเชิงรุก เพื่อรองรับภาวะการแข่งขันที่สูงขึ้น ด้วยการนำเทคโนโลยีใหม่ ๆ เข้ามาเสริมการประกอบธุรกรรมของธนาคาร

สำหรับให้บริการลูกค้า และมุ่งเน้นกลุ่มลูกค้ารายย่อยมากขึ้น ซึ่งเป็นกลุ่มลูกค้าเป้าหมายในการเสริมสร้างรายได้ของธุรกิจ ดังนั้น ธนาคารพาณิชย์จึงให้ความสำคัญในเรื่องของอินเตอร์เน็ต และการจดทำเว็บไซต์ของตนเอง เพื่อบริการเผยแพร่ข่าวสารข้อมูล ประชาสัมพันธ์

โฆษณาผลิตภัณฑ์และบริการของธุรกิจธนาคารแก่ผู้สนใจ นับว่าเป็นช่องทางการตลาดรูปแบบใหม่และเป็นเครื่องมือในการดำเนินธุรกิจที่มีประสิทธิภาพอีกรูปแบบหนึ่งและพัฒนาไปสู่ธนาคารพาณิชย์อิเล็กทรอนิกส์ โดยใช้ชื่อแตกต่างกันไปเช่น (Electronic Banking = E-Banking) หรือ Internet Banking = I=Banking เข้ามาเสริมงานบริการลูกค้าเพื่อเสริมสร้างความแข็งแกร่งในด้านงานบริการลูกค้า ลดต้นทุนการดำเนินงาน เพื่อความเจริญก้าวหน้าในธุรกิจ และเสริมสร้างการดำเนินงานให้มีประสิทธิภาพมากขึ้น ด้วยการผนวกงานบริการและธุรกรรมทางการเงินผ่านสื่ออินเตอร์เน็ต

การพัฒนาระบบอินเตอร์เน็ตแบงกิ้งของธนาคารพาณิชย์ในประเทศไทย มีลักษณะค่อยเป็นค่อยไป แม้ว่าธนาคารพาณิชย์ส่วนใหญ่ให้ความสำคัญกับบริการดังกล่าว เนื่องจากเป็นช่องทางในการรักษา และขยายฐานลูกค้าของธนาคาร อีกทั้งยังเป็นช่วงสร้างเสริมรายได้จากค่าธรรมเนียม หรือการทำธุรกรรมออนไลน์ ทดแทนรายได้จากดอกเบี้ยที่ลดลง เพื่อสนองความต้องการของลูกค้า และรองรับการแข่งขันธุรกิจทั้งจากในและต่างประเทศ ด้วยการพัฒนาผลิตภัณฑ์ใหม่ ๆ ให้ลูกค้าเลือกใช้ตามความต้องการ และตรงกับกลุ่มเป้าหมายแต่ละกลุ่ม เพื่อรักษาและขยายส่วนแบ่งทางการตลาด โดยเฉพาะกลุ่มลูกค้ารายย่อยด้วยการพัฒนาบริการที่มีอยู่เดิม และบริการรูปแบบใหม่ขึ้น ธนาคารพาณิชย์เห็นถึงประโยชน์การให้บริการบนอินเตอร์เน็ตทำให้เกิดการดำเนินธุรกิจประเภท Business-to-business (B-to-B) และขยายไปสู่การดำเนินธุรกิจประเภท Business-to-Consumer (B-to-C) และ Consumer-to-consumer (C-to-C) เนื่องจากผู้ประกอบการ และผู้สนใจดำเนินธุรกิจเริ่มขยายช่องทางการค้าขายสินค้า/บริการผ่านสื่ออินเตอร์เน็ตมากขึ้น ทำให้ธนาคารทำการพัฒนาระบบการชำระเงินผ่านอินเตอร์เน็ต และการทำรายการต่าง ๆ กับธนาคารด้วยตนเอง

ประโยชน์ต่อธุรกิจธนาคารอินเตอร์เน็ตเป็นเครื่องมือทางการตลาดอีกประเภทหนึ่งที่ทำให้ธุรกิจเติบโตได้เร็วขึ้น เช่น

1. เป็นฐานจัดเก็บข้อมูลของลูกค้าและผู้สนใจอื่น ๆ ที่เข้ามาติดต่อกับธนาคารสำหรับการนำเสนอผลิตภัณฑ์และบริการอื่น ๆ ในครั้งต่อไป

2. สามารถเข้าถึงลูกค้าและให้บริการซื้อขายผลิตภัณฑ์ และบริการได้ทั่วโลกตลอด 24 ชั่วโมง

3. ช่วยลดต้นทุนค่าใช้จ่ายในการดำเนินงาน เช่น ประหยัดการใช้เช็ค, กระดาษบันทึก และลดปริมาณเอกสารต่างๆ เป็นต้น

โอกาสทางธุรกิจของผู้ประกอบการไทย ในปัจจุบันธนาคารพาณิชย์เริ่มที่จะให้บริการธนาคารทางอินเทอร์เน็ตมากขึ้น เช่น ธนาคารไทยพาณิชย์ ธนาคารเอเชีย และธนาคารกรุงไทย เมื่อพิจารณาโมเดลในการให้บริการแล้ว จะเห็นได้ว่าธนาคารทั้ง 3 แห่งมีการให้บริการที่คล้ายคลึงกับในต่างประเทศ เช่น การแพร่หลายของผู้ใช้อินเทอร์เน็ตในประเทศไทยยังมีน้อยจึงทำให้มีลูกค้าเข้ามาใช้บริการน้อยตาม กฎระเบียบข้อบังคับยังไม่เอื้ออำนวยเท่าที่ควร และการสมัครยังต้องการหลักฐานที่เป็นเอกสาร เป็นต้น ในอนาคตเมื่อปัญหาต่าง ๆ เหล่านี้ได้รับการแก้ไขแล้ว บริการธนาคารทางอินเทอร์เน็ตจะกลายเป็นช่องทางใหม่ในการให้บริการของธนาคารในประเทศไทย

2.1.6 <u>การวิเคราะห์เกี่ยวกับการลงทุน</u>

การวิเคราะห์การลงทุน (Capital investment analysis) หรืองบลงทุน (Capital Budgeting) เป็นกระบวนการในการวางแผนและการจัดสรรเงินลงทุนในโครงการต่างๆ ของธุรกิจ โดยเป็นการตัดสินใจเกี่ยวกับเงินลงทุนในธุรกิจที่ได้ลงทุนไปในปัจจุบัน ซึ่งเห็นผลสำเร็จในอนาคต หรือเป็นกระบวนการที่ผู้บริหารใช้ในการตัดสินใจ เพื่อประเมินความสัมพันธ์ระหว่างรายจ่าย และผลประโยชน์ที่ได้รับจากการลงทุนในโครงการต่างๆ เพื่อให้ได้ประโยชน์สูงสุดในการจัดสรรทรัพยากรสำหรับการลงทุนในระยะยาว

วิธีการประเมินโครงการลงทุน สามารถแยกได้เป็น 2 แบบ ดังนี้

1. แบบที่ไม่ได้คำนึงถึงมูลค่าปัจจุบัน (Not use present values) มี 2 วิธี คือ

1.1 วิธีอัตราผลตอบแทนถัวเฉลี่ย [Average rate of return (ARR)]

1.2 วิธีเงินสดคืนทุน (Cash payback) หรือระยะเวลาคืนทุน [Payback period (PB)]

2. แบบที่คำนึงถึงมูลค่าปัจจุบัน (Use present values) มี 2 วิธี คือ

2.1 วิธีมูลค่าปัจจุบันสุทธิ [Net present value (NPV)]

2.2 วิธีอัตราลดผลตอบแทนคิดลด [Internet rate of return (IRR)]

การประเมินโครงการลงทุนแบบที่คำนึงถึงมูลค่าปัจจุบันนั้นจะพิจารณาถึงมูลค่าตามเวลาของเงิน(Time value of money) โดยมีแนวคิดว่า เงินที่นำมาลงทุนในปัจจุบันและจะได้รับผลตอบแทนในอนาคตข้างหน้า โดยจำนวนเงินดังกล่าวหากได้รับในระยะเวลาต่างกันย่อมมีค่าไม่เท่ากัน ฝ่ายบริหารจะใช้วิธีการต่างๆ ในการประเมินโครงการลงทุนนั้น ซึ่งแต่ละวิธีจะมีข้อดีและข้อเสียที่แตกต่างกัน ตลอดจนมีการคำนวณที่สลับซับซ้อน การประเมินโครงการลงทุนนั้นสามารถ

ใช้เครื่องคอมพิวเตอร์ช่วยในการคำนวณซึ่งมีความรวดเร็วและทำได้ง่ายขึ้น เครื่องคอมพิวเตอร์สามารถช่วยในการวิเคราะห์ผลกระทบจากการเปลี่ยนแปลงในการประเมินโครงการลงทุนได้ แต่อย่างไรก็ตามผู้บริหารต้องตัดสินใจเลือกโครงการการลงทุนที่ให้ประโยชน์สูงสุดหรือมีความเสี่ยงน้อยที่สุด

การประเมินโครงการลงทุนแบบที่ไม่ได้มูลค่าปัจจุบัน ใช้ประเมินโครงการลงทุนเบื้องต้น เหมาะสำหรับการประเมินโครงการลงทุนระยะสั้น

2.1.6.1 การประเมินโครงการลงทุนแบบที่คำนึงถึงมูลค่าปัจจุบัน (Not use present values)

2.1.6.1.1 วิธีอัตราผลตอบแทนถัวเฉลี่ย [Average rate of return (ARR)] หรืออัตราผลตอบแทนทางการบัญชี (Accounting rate of return)

เป็นอัตราส่วนที่ใช้วัดกำไรสุทธิถัวเฉลี่ยเป็นเปอร์เซ็นต์ของการลงทุนในสินทรัพย์ถาวรถัวเฉลี่ย หรือเป็นอัตราส่วนระหว่างประมาณการกำไรสุทธิถัวเฉลี่ยต่อปีกับเงินลงทุนในสินทรัพย์ถาวรถัวเฉลี่ย ซึ่งสามารถคำนวณได้ดังนี้

$$\text{อัตราผลตอบแทนถัวเฉลี่ย} = \frac{\text{เงินลงทุนในสินทรัพย์} \quad \%}{\text{ประมาณการกำไรสุทธิถัวเฉลี่ยต่อปี}}$$

การประเมินกำไรสุทธิถัวเฉลี่ยต่อปี เป็นผลตอบแทนที่คาดว่าจะได้รับจากการลงทุนตลอดอายุของโครงการหลังจากหักค่าเสื่อมราคาออกแล้ว ดังนั้นตัวหารควรที่จะเป็นมูลค่าตามบัญชีถัวเฉลี่ย(Average Book Value) ตลอดอายุโครงการ ถ้าสมมุติว่าสินทรัพย์ที่นำมาลงทุนมีการคิดค่าเสื่อมราคาโดยวิธีเส้นตรง (straight-line-depreciation) และไม่มีมูลค่าซาก (No resident value) เงินลงทุนถัวเฉลี่ย (Average Investment) ตลอดอายุโครงการควรเท่ากับครึ่งหนึ่งของเงินลงทุนเริ่มแรก

2.1.6.1.2 ระยะเวลาคืนทุน [Payback period (PB)] กระแสเงินสดนั้นมีความสำคัญเพราะสามารถนำมาใช้ลงทุนซ้ำได้ (Reinvested) กล่าวคือ ทุนที่นำมาใช้ในการลงทุนต้องใช้เงินสดและผลตอบแทนจากเงินสดที "ได้รับในอนาคตนั้นสามารถนำกลับมาใช้ลงทุนได้อีกระยะเวลาคืนทุน (PB) หมายถึง การประมาณช่วงระยะเวลาของเงินที่ลงทุนไปที่จะได้รับเงินสดกลับคืนมาเท่ากับจำนวนที่ได้ลงทุน เพื่อให้การวิเคราะห์ง่ายขึ้นจะพิจารณาจากรายได้และค่าใช้จ่ายที่

เกี่ยวข้องกับสินทรัพย์ถาวรในการดำเนินงาน โดยสมมติให้รายได้และค่าใช้จ่ายดังกล่าวอยู่ในรูปของเงินสดทั้งหมด

$$\text{ระยะเวลาคืนทุน (PB)} = \frac{\text{จำนวนเงินที่ ได้ลงทุน}}{\text{กระแสเงินสดสุทธิที่คาดว่าจะได้รับต่อปี}}$$

ถ้ากระแสเงินสดรับมากกว่ากระแสเงินสดจ่าย เรียกว่า กระแสเงินสดสุทธิ (Net cash flow) ดังนั้นระยะเวลาของกระแสเงินสดที่คาดว่าจะได้รับในอนาคตเท่ากับเงินลงทุนเริ่มแรกในสินทรัพย์ถาวร

2.1.6.2 การประเมินโครงการลงทุนแบบที่คำนึงถึงมูลค่าปัจจุบัน

2.1.6.2.1 มูลค่าปัจจุบันสุทธิ [Net present value (NPV)] เป็นการวิเคราะห์โครงการลงทุนโดยการเปรียบเทียบเงินสดลงทุนเริ่มแรก (Initial cash investment) กับมูลค่าปัจจุบันของกระแสเงินสดสุทธิ (Net cash flow) มูลค่าปัจจุบันสุทธิ ในบางครั้งเรียกว่า วิธีคิดลดกระแสเงินสด (Discounted cash flow method) อัตราดอกเบี้ยหรืออัตราผลตอบแทนที่ใช้วิเคราะห์มูลค่าปัจจุบันจะกำหนดโดยฝ่ายบริหาร อัตรานี้โดยทั่วไปขึ้นอยู่กับปัจจัยตามลักษณะของธุรกิจ จุดมุ่งหมายของการลงทุนต้นทุนของการจัดหาเงินทุนเพื่อการลงทุน และอัตราผลตอบแทนขั้นต่ำที่ต้องการ (Minimum desired rate of return)

มูลค่าปัจจุบันสุทธิ (NPV) = มูลค่าปัจจุบันของกระแสเงินสดสุทธิรวม – จำนวนเงินลงทุน

2.1.6.2.2 อัตราผลตอบแทนคิดลด [Internal rate of return (IRR)] เป็นการใช้แนวคิดมูลค่าปัจจุบันในการคำนวณหาอัตราผลตอบแทนจากกระแสเงินสดสุทธิที่คาดว่าจะได้รับจากเงินลงทุนในโครงการ วิธีนี้ในบางครั้งเรียกว่า อัตราผลตอบแทนโดยปรับตามเวลา (Time-adjusted rate of return) วิธีนี้จะคล้ายกับวิธีมูลค่าปัจจุบันสุทธิคือ จะพิจารณาที่มูลค่าปัจจุบันของกระแสเงินสดสุทธิ แต่วิธีอัตราผลตอบแทนค่าลดจะเริ่มต้นด้วยการพิจารณากระแสเงินสดสุทธิและคิดย้อนหลังเพื่อคำนวณหาอัตราตอบแทนที่คาดไว้จากโครงการอัตราผลตอบแทนคิดลด (IRR) เป็นการคำนวณหาอัตราคิดลด ที่มีผลทำให้มูลค่าปัจจุบันของกระแสเงินสดที่ได้รับในอนาคตเท่ากับเงินลงทุนที่จ่ายเริ่มแรก สามารถเขียนเป็นสูตรได้ดังนี้

IRR; มูลค่าปัจจุบันของกระแสเงินสดสุทธิรวม = เงินลงทุนเริ่มแรก

2.1.7 บทบาททางกลยุทธ์สำหรับระบบเทคโนโลยีสารสนเทศ (Strategic Roles for Information Systems)

2.1.7.1 แนวคิดกลยุทธ์

แนวคิดกลยุทธ์ของการแข่งขันสามารถนำไปประยุกต์ใช้กับบทบาททางกลยุทธ์สำหรับระบบเทคโนโลยีสารสนเทศได้ ผู้จัดการสามารถส่งเสริมกลยุทธ์ทางการแข่งขันของบริษัทโดยใช้การลงทุนทางด้านเทคโนโลยีสารสนเทศได้ บริษัทจะสามารถนำกลยุทธ์ทางระบบเทคโนโลยีสารสนเทศมาใช้ให้เกิดความได้เปรียบทางการแข่งขัน สามารถสรุปการนำเทคโนโลยีสารสนเทศไปใช้เพื่อทำให้เกิดกลยุทธ์ทางการแข่งขันดังนี้

1. ต้นทุนต่ำ (Lower Costs) ใช้เทคโนโลยีเพื่อลดต้นทุนของขั้นตอนการทำธุรกิจได้อย่างมาก ลดต้นทุนของลูกค้า และผู้จัดหาสินค้า สร้างความเป็นผู้นำทางด้านต้นทุนต่ำ

2. ทำให้เกิดความแตกต่าง (Differentiate) พัฒนาคุณลักษณะใหม่ๆ ของเทคโนโลยีเพื่อทำให้สินค้าและบริการมีความแตกต่างออกไป ใช้คุณลักษณะของเทคโนโลยี เพื่อลดข้อได้เปรียบจากความแตกต่างของบริษัทคู่แข่ง และช่วยทำให้ตัวสินค้า และบริการเกิดความน่าสนใจและสร้างโอกาสทางการตลาด

3. สร้างความเจริญเติบโต (Promote Growth) ใช้เทคโนโลยีเพื่อบริหารจัดการกับการขยายธุรกิจออกไปสู่ระดับภูมิภาค และระดับโลก และใช้เทคโนโลยีเพื่อสร้างความหลากหลายและรวมเข้าเป็นอันหนึ่งอันเดียวกันกับสินค้าและบริการอื่นๆ

4. ปรับปรุงคุณภาพ และประสิทธิภาพ (Improve Quality and Efficiency) ใช้เทคโนโลยีเพื่อปรับปรุงคุณภาพของสินค้าและบริการอย่างทันทีทันใด และเกิดการปรับปรุงอย่างต่อเนื่อง นำไปสู่ประสิทธิภาพในกระบวนการทางธุรกิจ รวมทั้งลดระยะเวลาที่ใช้ในการคิดค้นพัฒนา ผลิต จัดส่งสินค้า และบริการ

2.1.7.2 การทำลายอุปสรรคทางธุรกิจ (Breaking Business Barriers)

ความสามารถที่สำคัญของเทคโนโลยีสารสนเทศคือสามารถทำลายอุปสรรคต่างๆ และนำไปสู่ความสำเร็จทางธุรกิจ เทคโนโลยีสามารถทำลายอุปสรรคทางด้านเวลา อุปสรรคทางด้านระยะทาง และอุปสรรคทางด้านต้นทุน ดังนี้

1. การทำลายอุปสรรคทางด้านเวลา (Breaking Time Barriers) เทคโนโลยีสารสนเทศสามารถลดระยะเวลาระหว่างขั้นตอนการดำเนินงาน การมุ่งความสนใจเกี่ยวกับการลด

ระยะเวลาและการทำงานที่รวดเร็วฉับไว จุดมุ่งหมาย คือ การทำให้ระยะเวลาการตอบสนองต่อความต้องการของลูกค้าสั้นลง และลดการลงทุนด้านการเก็บกักสินค้าให้เหลือน้อยที่สุด จะมีความได้เปรียบทางกลยุทธ์ การทำงานในเวลาอันรวดเร็ว หมายถึง ไม่มีความล่าช้าระหว่างการแยกแยะและการตอบสนองความต้องการ

2. การทำลายอุปสรรคทางด้านต้นทุน (Breaking Cost Barriers) เทคโนโลยีสารสนเทศสามารถทำให้หน่วยธุรกิจสามารถลดต้นทุนการทำธุรกิจได้อย่างไร การใช้อินทราเน็ตและเครือข่ายการสื่อสารระยะไกลอื่นๆ เพื่อเชื่อมโยงติดต่อกันในระหว่างส่วนธุรกิจที่สำคัญสามารถลดต้นทุนการผลิต การเก็บสินค้า การขนส่ง หรือการติดต่อกับบริษัทอื่นๆได้ ดังนั้นเทคโนโลยีสารสนเทศได้ช่วยบริษัทหลายๆแห่ง ประหยัดค่าแรงงาน ลดขนาดของคลังสินค้า ลดจำนวนศูนย์ขนส่งสินค้า และลดต้นทุนการติดต่อสื่อสาร

2.1.8 <u>ลักษณะบริการ Cash Management ของธนาคารพาณิชย์ไทย</u>

เป็นบริการสำหรับนิติบุคคล เพื่อเพิ่มประสิทธิภาพในการบริหารกระแสเงินสดของบริษัท ลดต้นทุน ลดความผิดพลาด และลดขั้นตอนในการบริหารงาน บริการ Cash Management ของธนาคารจะใช้ระบบเทคโนโลยี ของธนาคารเข้ามาช่วย ทำให้การบริหารกระแสเงินสดประจำวันของบริษัททั้งทางด้านการบริหารสภาพคล่องของบัญชีบริษัท ด้านขารับและขาจ่าย ให้เป็นระบบมากขึ้น ธนาคารจะจัดทำรายงานการทำรายการประจำวันส่งกลับบริษัทเพื่ออำนวยความสะดวกในการกระทบยอดและตรวจสอบบัญชี การวางแผนกระแสเงินสดของบริษัท ก็จะมีประสิทธิภาพมากขึ้น

บริการ Cash Management แบ่งเป็น 3 กลุ่ม ดังนี้

2.1.8.1 บริการด้านบริหารสภาพคล่อง (Liquidity Services)

เป็นบริการที่เพิ่มประสิทธิภาพในการบริหารกระแสเงินสดของบริษัท สามารถโอนเงินอัตโนมัติระหว่างบัญชีบริษัทจากบัญชีบริษัทแม่ไปบัญชีบริษัทลูก หรือบริษัทในเครือ โดยระบบจะบริหารบัญชีทั้งหมดให้กับบริษัทเพื่อให้บริษัทได้รับผลตอบแทนสูงสุด บัญชีที่ใช้อยู่ในรูปของบุคคลธรรมดา นิติบุคคล รวมทั้งบัญชีกระแสรายวัน หรือบัญชีออมทรัพย์ก็ได้

2.1.8.2 บริการด้านขารับ (Collection Services)

เป็นบริการที่เพิ่มประสิทธิภาพในการบริหารกระแสเงินสดที่เข้ามาบริษัทให้ดีขึ้น สะดวกในการส่งเช็คมาที่ธนาคารเพื่อการเรียกเก็บ, อำนวยความสะดวกในการเก็บเงินจากลูกค้าของบริษัท โดยธนาคารจะทำการหักเงินจากบัญชีของลูกค้าที่มีบัญชีอยู่กับธนาคารและนำเงินเข้า

บัญชีของบริษัทตามวันที่กำหนด และอำนวยความสะดวกและเพิ่มช่องทางในการชำระเงินค่าสินค้าและบริการให้กับลูกค้าของบริษัท

2.1.8.3 บริการทางด้านขาจ่าย (Payment Services)

เป็นบริการที่ช่วยลดขั้นตอนและเพิ่มประสิทธิภาพในการทำเช็คจ่ายค่าสินค้าและบริการให้กับ Supplier บริษัทเพียงแค่ส่งคำสั่งถึงธนาคารโดยมีรายละเอียดในการจ่ายเงิน หลังจากนั้นธนาคารจะทำการออกแคชเชียร์เช็คและสามารถให้ธนาคารจัดทำหนังสือรับรองการหักภาษี ตามคำสั่งของบริษัท

เป็นบริการที่อำนวยความสะดวกในการโอนเงินเข้าบัญชีพนักงานที่มีบัญชีกับธนาคาร และบัญชีผู้รับผลประโยชน์ บริษัทเพียงส่งคำสั่งถึงธนาคาร หลังจากนั้นธนาคารจะทำการโอนเงินตามคำสั่งของบริษัท

2.2 งานวิจัยที่เกี่ยวข้อง

งานวิจัยของรักษิตาพร วุฒิคงศิริกูล เรื่อง การศึกษาทัศนคติของผู้ประกอบการเกี่ยวกับการใช้บริการ Cash Management ผ่านระบบอิเล็กทรอนิกส์ของธนาคารพาณิชย์ไทย, หลักสูตรบริหารธุรกิจมหาบัณฑิต สาขาวิชาการจัดการธุรกิจผ่านอิเล็กทรอนิกส์ คณะบริหารธุรกิจ มหาวิทยาลัยรังสิต 2546

จากผลการศึกษาวิจัยพบว่า ผู้ประกอบการเลือกใช้บริการทางด้านอินเทอร์เน็ต เนื่องจาก มีการติดต่อได้สะดวกทุกที่ที่มีอินเทอร์เน็ตและสามารถติดต่อได้ทุกเวลาที่ต้องการ ไม่ต้องเสียเวลาและค่าใช้จ่ายในการเดินทางมาทำธุรกรรมที่ธนาคาร ช่วยให้บริษัทสามารถประหยัดต้นทุนได้มากขึ้น มีความปลอดภัยของระบบและข้อมูล สามารถเข้าใช้งานได้ง่าย อัตราความเร็วในการประมวลผลค่อนข้างเร็ว มีการแก้ไขข้อผิดพลาดได้รวดเร็ว ทำให้ข้อผิดพลาดน้อยลง โดยธุรกิจที่ใช้บริการทางด้าน Cash Management มีทุกประเภทธุรกิจ เช่น โรงงานอุตสาหกรรม, บริษัทเอกชน และหน่วยงานทางราชการ โดยขนาดขององค์กรขนาดเล็กตั้งแต่ 20 คน จนถึงองค์กรขนาดใหญ่ที่มีพนักงาน คนงานตั้งแต่ 1,000 คนขึ้นไป

งานวิจัยของปราณี วิวิธเกยูรวงศ์ เรื่อง ความคิดเห็นของลูกค้าที่มีต่อบริการธนาคารทางอินเทอร์เน็ตของธนาคารกรุงศรีอยุธยา จำกัด (มหาชน), บัณฑิตวิทยาลัย มหาวิทยาลัยเกษตรศาสตร์ 2546

จากผลการศึกษาทำให้ทราบว่า กระแสความนิยมในพาณิชย์อิเล็กทรอนิกส์มีมากขึ้น ทำให้อินเทอร์เน็ตกลายเป็นช่องว่างทางการตลาดที่มีความสำคัญช่องทางหนึ่ง และจากภาวะวิกฤตทางเศรษฐกิจที่ผ่านมา รวมทั้งการเข้ามาแข่งขันของธนาคารต่างชาติ ทำให้ธนาคารต้องหันมาพัฒนาปรับปรุงการให้บริการให้หลากหลายมากขึ้น โดยเฉพาะบริการผ่านเครือข่ายอินเทอร์เน็ต เพื่อให้สามารถตอบสนองความต้องการของลูกค้า และยังช่วยลดต้นทุนในการดำเนินงาน และเป็นการรักษาฐานลูกค้าเดิมไว้

งานวิจัยของคมกริช ตันทเสนีย์ เรื่อง การศึกษาวิจัยเฉพาะกรณีการรุกรานจากภายนอกโดยผ่านอินเตอร์เน็ตและผลกระทบต่อองค์กรธุรกิจระดับ SMEs, หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาการบริหารโทรคมนาคม วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์ 2545

จากผลการวิจัยปัญหาทางด้านความปลอดภัยขององค์กรระดับ SMEs นั้นมีการเพิ่มขึ้นของปัญหาทางด้านความปลอดภัย ขึ้นอยู่กับการใช้ทคโนโลยีสารสนเทศและอินเทอร์เน็ตที่เพิ่มมากขึ้นและภายในองค์กรของ SMEs เองมีความอ่อนแอทางด้านบุคลากรที่จะรู้และเข้าใจปัญหาทางด้านความปลอดภัย และสิ่งที่จำเป็นต่อการป้องกันความปลอดภัย จึงเป็นสาเหตุให้ Hacker สามารถที่จะโจมตีได้ง่าย อีกทั้งยังมีอีกหลายบริษัทที่ขาดการดูแลเอาใจใส่ในด้านความปลอดภัยจนกระทั่งได้รับผลกระทบจากการโจมตี ซึ่งผลกระทบที่เกิดขึ้น คือ การสูญเสียความน่าเชื่อถือขององค์กร, การเสียหายของข้อมูลที่สำคัญ, การเสียหายของระบบคอมพิวเตอร์, และค่าใช้จ่ายในการซ่อมแซมระบบที่เสียหายทั้งทางด้าน Hardware และ Software ภายในองค์กร

งานวิจัยของณัฐพล เหมือนบัว เรื่อง กรณีศึกษาการเพิ่มประสิทธิภาพเครือข่ายข้อมูล , หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาการบริหารโทรคมนาคม วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์ 2545

จากการศึกษาโครงสร้างระบบเครือข่าย การเพิ่มขนาดของ Bandwidth ที่สามารถรองรับการใช้งาน Application ต่าง ๆ ได้ ทำให้การรับ-ส่งข้อมูลไปยังปลายทางมีความเร็วเพิ่มขึ้น ทำให้ไม่เกิดปัญหาคอขวดหากมีการรับ-ส่งข้อมูลจำนวนมาก ๆ ซึ่งสามารถใช้เป็นแนวทางในการแก้ไขและเพิ่มประสิทธิภาพระบบเครือข่ายให้สามารถรองรับการใช้บริการได้อย่างเหมาะสม ช่วยในด้านการจัดสรรทรัพยากรเครือข่าย และจัดลำดับความสำคัญในการใช้เส้นทางรับ-ส่งข้อมูล

งานวิจัยของนฤศันส์ มิลินทางกูร เรื่อง ปัจจัยที่มีผลต่อบริการธนาคารทางอินเทอร์เน็ตกับกลุ่มประชากรที่ใช้บริการของธนาคารในเขตกรุงเทพมหานคร กรณีศึกษา ธนาคารไทยพาณิชย์ จำกัด (มหาชน), หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาการบริหารเทคโนโลยี วิทยาลัยนวัตกรรมอุดมศึกษา มหาวิทยาลัยธรรมศาสตร์ 2546

จากผลการศึกษาการใช้บริการของธนาคารทางอินเทอร์เน็ตทำให้ทราบถึง ปัญหาที่เกิดขึ้นในการใช้งานระบบ เช่น ปัญหาการเข้าใช้งาน Web Site ไม่ได้เป็นเวลานาน หรือระบบหลุดต้องใช้ระยะเวลานานจึงกลับมาใช้งานได้ตามปกติ บางรายถึงกับเลิกใช้บริการธนาคารทางอินเทอร์เน็ตเนื่องมาจากสาเหตุ คือ การใช้งานที่ค่อนข้างยาก มีความความซับซ้อนไม่สะดวกในการใช้งาน หรือไม่มีบริการเสริมที่เพียงพอต่อการใช้งาน และความไม่มั่นใจในระบบ ปัจจัยที่ทำให้มีผู้ใช้บริการใช้บริการทางด้านอินเทอร์เน็ตเพิ่มขึ้น ได้แก่ ต้องมีบริการทางการเงินที่หลากหลาย การใช้งานง่ายไม่ซับซ้อน การบริการไม่มีข้อผิดพลาด และระบบที่ใช้บริการมีความปลอดภัยและน่าเชื่อถือ