



เครือข่ายคอมพิวเตอร์ เบื้องต้น



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

1. เครือข่ายคอมพิวเตอร์ (Computer Network)

ความหมายของระบบเครือข่ายคอมพิวเตอร์

กลุ่มของเครื่องคอมพิวเตอร์ เช่น คอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์พกพา สมาร์ทโฟน แท็บเล็ต ตั้งแต่สองเครื่องขึ้นไป รวมถึงอุปกรณ์ต่าง ๆ เช่น เครื่องพิมพ์ เครื่องสแกนที่ถูกลำมาเชื่อมต่อกันทั้งแบบมีสายและไร้สาย ตั้งแต่ขนาดเล็กที่เชื่อมต่อกันด้วยคอมพิวเตอร์ตั้งแต่ สองเครื่องเพื่อใช้งานในบ้านหรือในบริษัทเล็ก ๆ ไปจนถึงเครือข่ายขนาดใหญ่ที่เชื่อมต่อเครือข่ายต่าง ๆ จากทั่วโลกเข้าด้วยกัน ซึ่งเรียกว่า เครือข่ายอินเทอร์เน็ต (Internet)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

1. เครือข่ายคอมพิวเตอร์ (Computer Network)

1.1 หลักการทำงานของระบบเครือข่ายคอมพิวเตอร์



ระบบเครือข่ายคอมพิวเตอร์หนึ่งเครือข่ายจะมีการทำงานร่วมกันเป็นกลุ่มระหว่างคอมพิวเตอร์อย่างน้อยสองเครื่องขึ้นไป เรียกว่า กลุ่มงาน (Workgroup) เมื่อเชื่อมโยงหลาย ๆ กลุ่มงานเข้าด้วยกันจะเป็นเครือข่ายขององค์กร ซึ่งเรียกว่า เครือข่ายท้องถิ่น หรือแลน (Local Area Network : LAN) และเมื่อนำเครือข่าย ขององค์กร เชื่อมโยงกันผ่านระบบเครือข่ายของผู้ให้บริการ (Internet Service Provider : ISP) จะได้ เครือข่ายขนาดใหญ่และกว้างขึ้น หรือที่เรียกเครือข่ายบริเวณกว้าง หรือแวน (Wide Area Network : WAN)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

1. เครือข่ายคอมพิวเตอร์ (Computer Network)

การใช้งานเครือข่ายคอมพิวเตอร์เป็นไปอย่างหลากหลายและสามารถใช้ประโยชน์ได้มากมาย การแบ่งปันทรัพยากร ในการทำงานของเครือข่ายคอมพิวเตอร์นั้นจะต้องมีข้อตกลงในการสื่อสาร หรือเรียกว่าโพรโทคอล (Protocol) เพื่อให้อุปกรณ์คอมพิวเตอร์ต่าง ๆ ทำงานร่วมกันได้



รูปที่ 1.1 เครือข่ายคอมพิวเตอร์



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

1. เครือข่ายคอมพิวเตอร์ (Computer Network)



1.2 ประโยชน์ของระบบเครือข่ายคอมพิวเตอร์



การใช้อุปกรณ์ร่วมกัน (Sharing of peripheral devices)



การใช้โปรแกรมและข้อมูลร่วมกัน (Sharing of program and data)



การติดต่อสื่อสารระยะไกล (Telecommunication)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

1. เครือข่ายคอมพิวเตอร์ (Computer Network)



การประมวลผลแบบคลาวด์ (Cloud Computing)



สื่อใหม่และสังคมออนไลน์ (New Media and Social Network)



บริการและธุรกิจใหม่ (New Product and Service)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

การสื่อสารข้อมูลบนเครือข่ายคอมพิวเตอร์ประกอบไปด้วย 5 องค์ประกอบ

2.1 ผู้ส่งหรืออุปกรณ์ส่งข้อมูล (Sender)

ต้นทางของการสื่อสารโดยมีหน้าที่ในการให้กำเนิดข้อมูล
ข่าวสาร เช่น ผู้พูด คอมพิวเตอร์ โทรศัพท์ สมาร์ทโฟน เป็นต้น



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

2.2 ผู้รับหรืออุปกรณ์รับข้อมูล (Receiver)

ปลายทางที่รับข้อมูลแล้วนำไปดำเนินการต่อ เช่น ผู้ใช้ปลายทางได้รับข้อมูลข่าวสารแล้วนำมาใช้ในการตัดสินใจ คอมพิวเตอร์ปลายทางได้รับข้อมูลแล้วพิมพ์ทางเครื่องพิมพ์



หมายเหตุ

อุปกรณ์ส่งข้อมูล (Sender) หรืออุปกรณ์รับข้อมูล (Receiver) อาจใช้แทนด้วยคำว่าโฮสต์ (Host) หรือโหนด (Node) หรืออุปกรณ์ปลายทาง (End device หรือ Endpoint)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

2.3 ช่องทางการสื่อสาร (Communication Channel) หรือ สื่อกลางในการนำส่งข้อมูล (Media หรือ Medium)



สื่อกลางหรือเส้นทางที่ใช้เป็นทางผ่านในการรับส่งข้อมูลระหว่างผู้รับ (Receiver) และผู้ส่งข้อมูล (Transmitter) ปัจจุบันมีช่องทางการสื่อสารสำหรับการเชื่อมต่อเครือข่ายคอมพิวเตอร์ทั้งแบบมีสายและไร้สาย เช่น สายคู่บิดเกลียวชนิดหุ้มฉนวน (Shielded Twisted Pair : STP) สายคู่บิดเกลียวชนิดไม่หุ้มฉนวน (Unshielded Twisted Pair : UTP) สายใยแก้วนำแสง (Fiber Optic) อินฟราเรด ไมโครเวฟ Wi-Fi บลูทูธ ดาวเทียม เป็นต้น

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



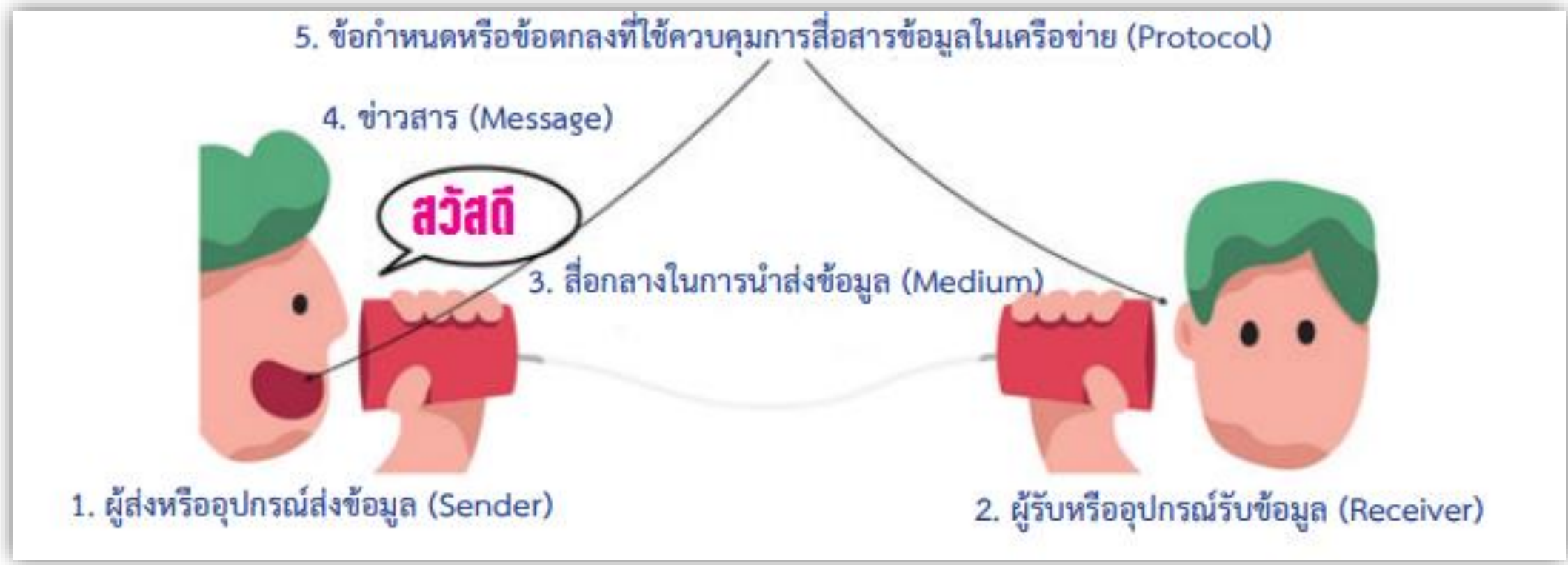
2.4 ข่าวสาร (Message) หรือข้อมูล (Data)

เนื้อหาสาระของข้อมูลที่ถูกส่งผ่านระบบเครือข่าย ซึ่งข่าวสารนี้มีหลากหลายรูปแบบ ขึ้นอยู่กับมาตรฐานความเข้าใจ ซึ่งเป็นที่ตกลงกันระหว่างผู้รับและผู้ส่ง เช่น

- @ ข้อความ (Text) คือ ข้อมูลที่อยู่ในรูปอักษรหรือเอกสาร
- @ เสียง (Voice) ทั้งในคลิปวิดีโอสื่อผสม (Multimedia) เสียงดนตรีหรือรหัสต่าง ๆ
- @ รูปภาพ (Image) ทั้งแบบที่เป็นภาพนิ่งหรือคลิปวิดีโอสื่อผสม (Multimedia) ข้อมูลทั้งรูปภาพ เสียงและข้อความเข้าด้วยกัน

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

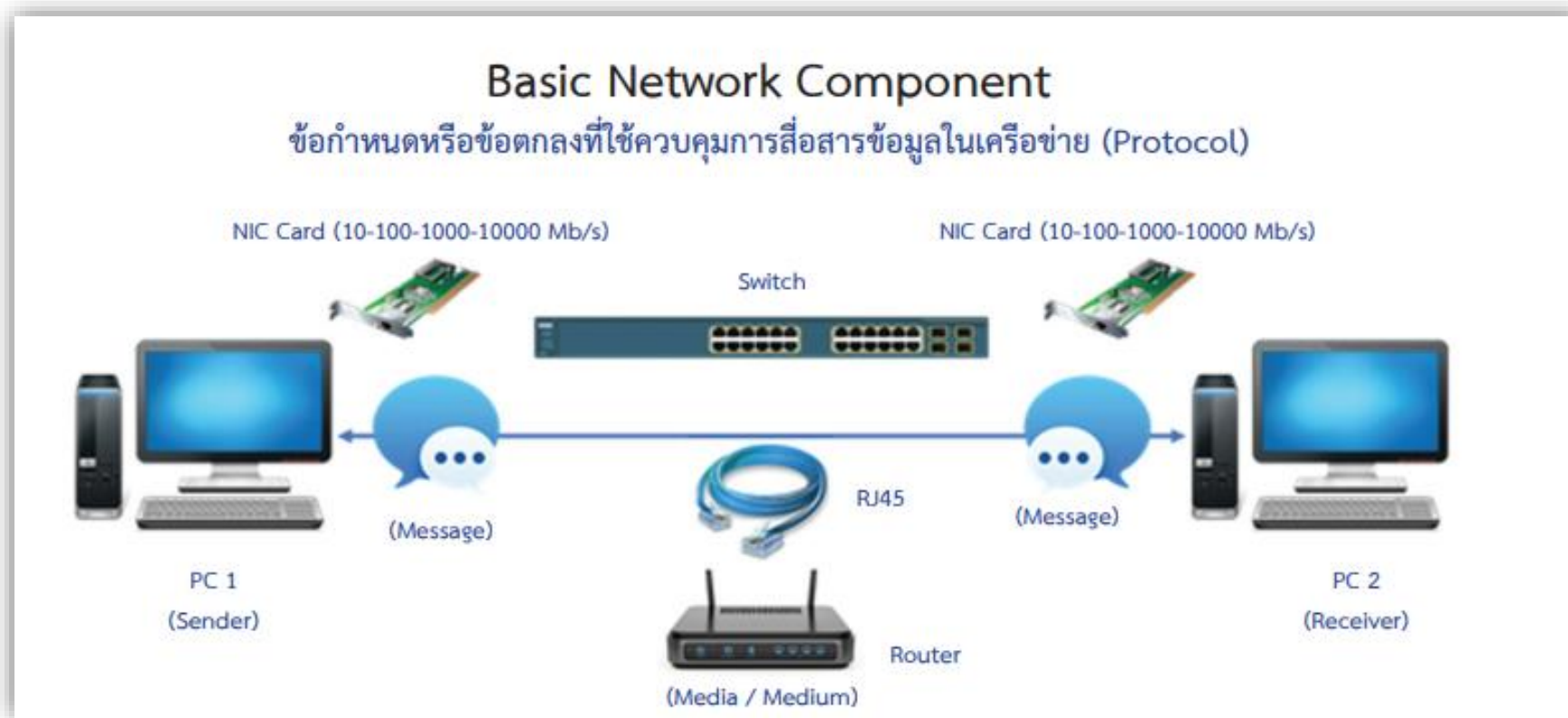
2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



รูปที่ 1.2 องค์ประกอบในการสื่อสารของมนุษย์

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



รูปที่ 1.3 องค์ประกอบของเครือข่ายคอมพิวเตอร์

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



2.5 ระเบียบวิธีหรือข้อตกลงในการสื่อสาร หรือโพรโทคอล (Protocol)

คอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่ใช้โพรโทคอลชนิดเดียวกันเท่านั้นจึงจะสามารถติดต่อและส่งข้อมูลระหว่างกันได้ โพรโทคอลจึงมีลักษณะคล้ายกับรูปแบบที่ใช้ในการสื่อสารของมนุษย์ที่ต้องใช้รูปแบบเดียวกันจึงจะสามารถสื่อสารกันได้เข้าใจ เปรียบเทียบง่าย ๆ



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์



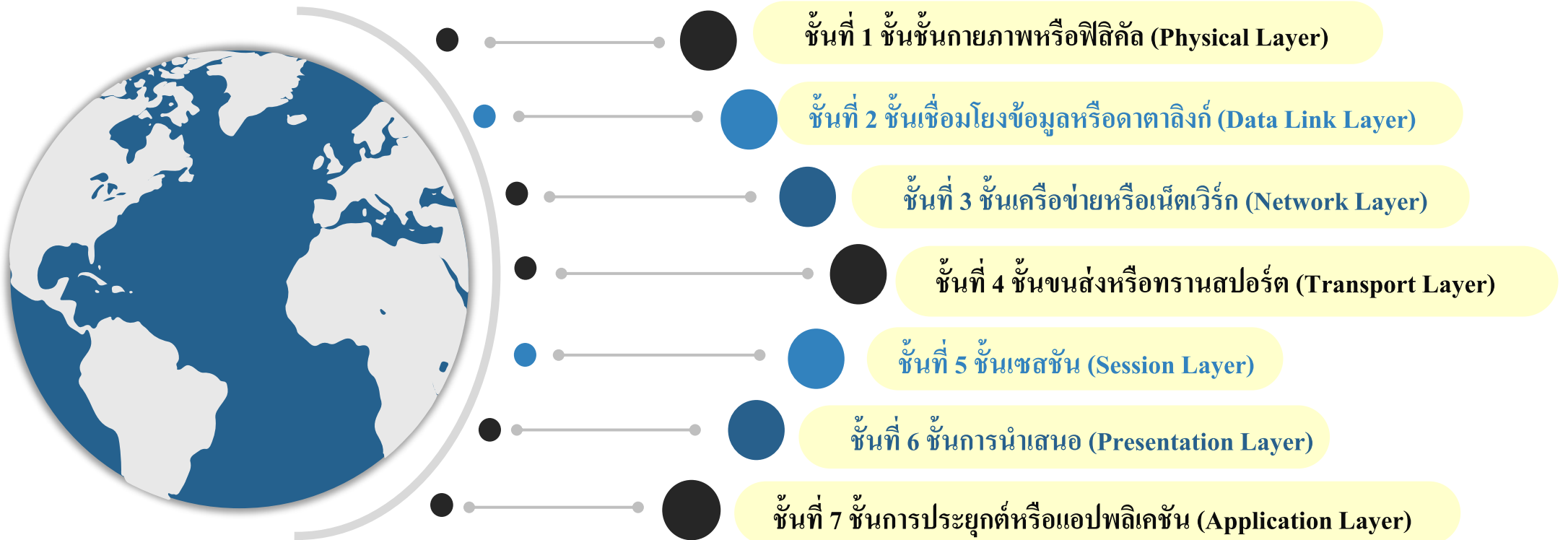
2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

ในระบบเครือข่าย โพรโทคอลจะเป็นตัวกำหนดคุณลักษณะหรือองค์ประกอบต่าง ๆ ที่ใช้ในการสื่อสารที่คอยควบคุมการให้บริการหรือเซอร์วิส (Services) รวมถึงกระบวนการหรือโปรเซส (Processes) ที่มีอยู่ในแต่ละอุปกรณ์ ช่วยกำหนดขนาดและรูปแบบของข้อความที่จะส่ง รูปแบบการแทนข้อมูล วิธีการในการรับส่งข้อมูลหรือกำหนดทิศทางการส่ง รูปแบบสัญญาณการรับส่ง การกำหนดหรือการอ้างอิงตำแหน่ง การแก้ไขข้อผิดพลาดในการส่งข้อมูล วิธีการส่ง ความเร็วในการรับส่งข้อมูล วิธีการรับและการตีความข้อมูล และความสำคัญนี้ องค์การที่ว่าด้วยเรื่องมาตรฐานระหว่างประเทศ (International Organization for Standardization : ISO) จึงได้กำหนดมาตรฐานการจัดระบบการเชื่อมต่อสื่อสารระหว่างระบบเปิด (Open System Interconnection : OSI)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

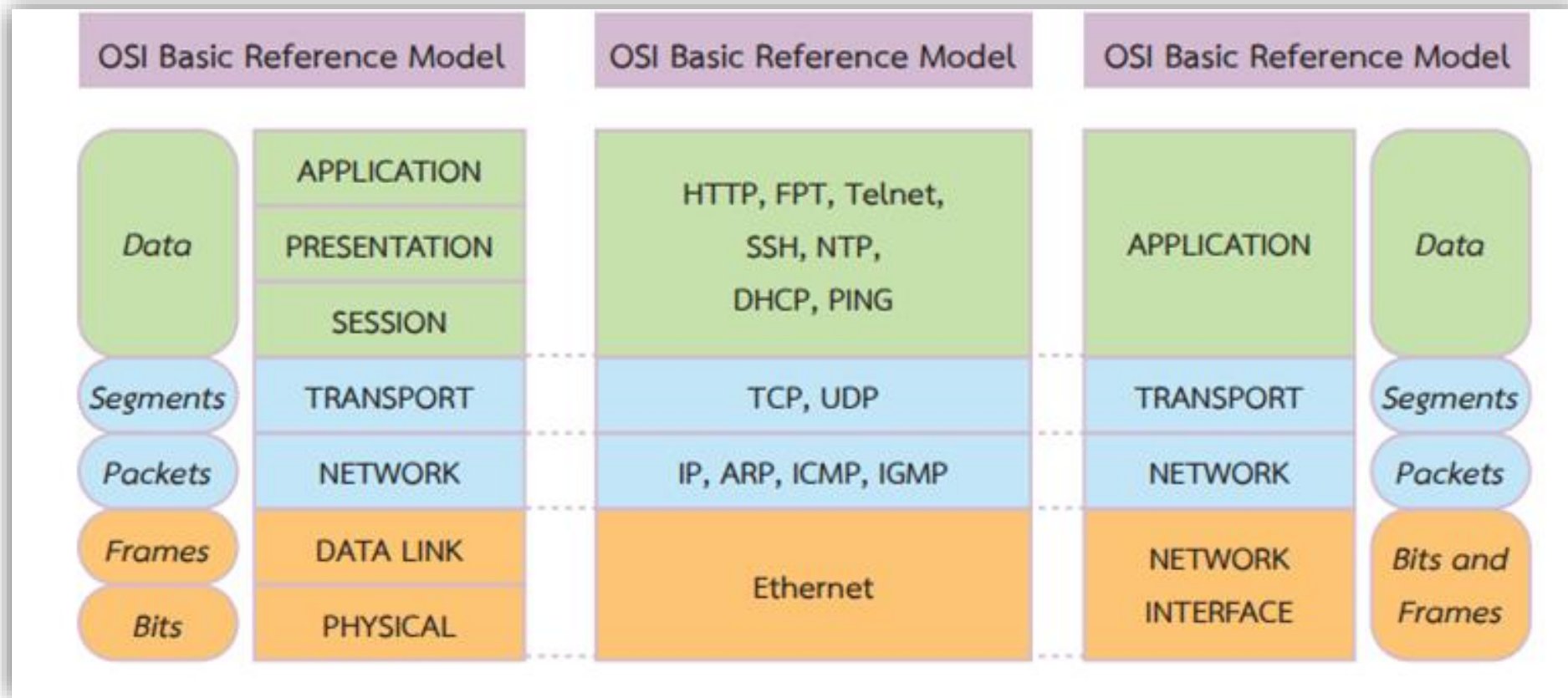
2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

2.5.1 โมเดล OSI การส่งข้อมูลข่าวสารโดยผ่านชั้นมาตรฐาน 7 ชั้น หรือเลเยอร์ (Layer) เรียงตามลำดับจากชั้นล่างสุดขึ้นไป ดังนี้



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



รูปที่ 1.4 เปรียบเทียบโมเดล OSI กับ TCP/IP

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

เพื่อสนับสนุนความหลากหลายของฟังก์ชันเครือข่าย ชั้นที่ 2 ชั้นเชื่อมโยงข้อมูลหรือดาตาลิงก์มักถูกแบ่งออกเป็น 2 ชั้นย่อย หรือซับเลเยอร์ (Sublayer) (รูปที่ 1.5) : Sublayer บน และ Sublayer ล่าง



ชั้นย่อยบน

การควบคุมการเชื่อมโยงตรรกะ (Logical Link Control : LLC) กำหนดกระบวนการของซอฟต์แวร์ (Software-processes) ที่เตรียมบริการสำหรับโพรโทคอลของชั้นเน็ตเวิร์ก จะวางแพ็กเก็ตที่ได้จากชั้นที่ 3 ลงในเฟรมที่ระบุโพรโทคอลของชั้นที่ 3 ที่ถูกใช้สำหรับเฟรมนั้นคือโพรโทคอลอะไร ข้อมูลนี้จะช่วยให้โพรโทคอลชั้น 3 ต่าง ๆ

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



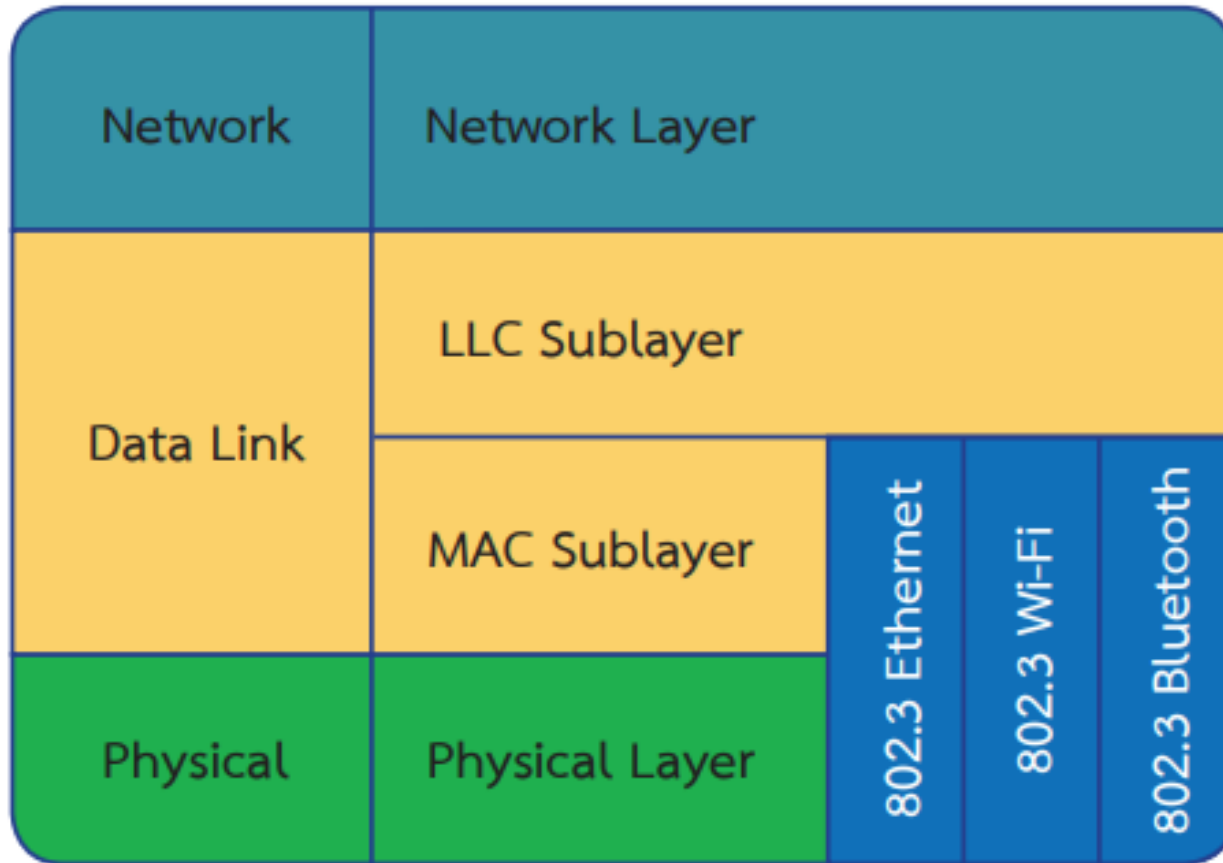
ชั้นย่อยล่าง

การควบคุมการเข้าถึงสื่อ (Media Access Control : MAC) กำหนดกระบวนการเข้าถึงสื่อ ซึ่งดำเนินการโดยฮาร์ดแวร์ ชั้นย่อยนี้ได้เตรียมแอดเดรสของชั้นที่ 2 ดาตาลิงก์และบอกขอบเขต (Delimiting) ของข้อมูลตามความต้องการของการส่งสัญญาณทางกายภาพของสื่อและบอกชนิดของโปรโตคอลของชั้นดาตาลิงก์ (Data Link protocol) ที่ใช้งาน

การแยกชั้นที่ 2 ชั้นเชื่อมโยงข้อมูล หรือดาตาลิงก์ออกเป็น 2 ชั้นย่อย ช่วยให้เฟรมชนิดหนึ่งที่กำหนดโดยชั้นบนเข้าถึงสื่อชนิดต่าง ๆ กันที่กำหนดโดยชั้นล่าง กรณีดังกล่าวพบเห็นได้ในเทคโนโลยีแลนทั่ว ๆ ไป รวมทั้งเทคโนโลยีอีเทอร์เน็ต (Ethernet) ซึ่งใช้กันมากที่สุดในแลน

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

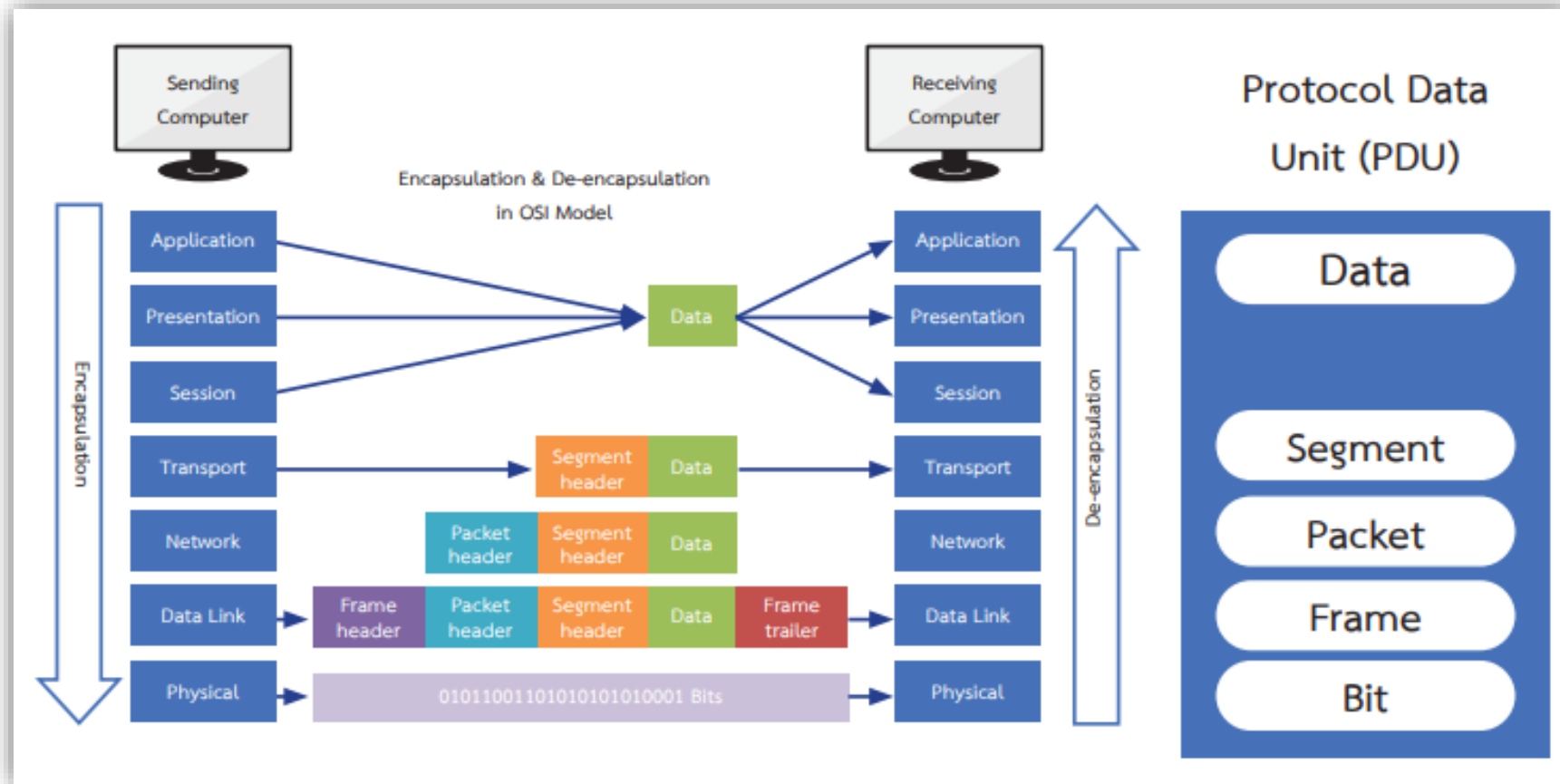
2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



รูปที่ 1.5 การแบ่งชั้นดาตาดังกล่าวออกเป็น 2 ชั้นย่อย คือ LLC และ MAC

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์



รูปที่ 1.6 การห่อหุ้ม (Encapsulation) ข้อมูลและการแกะข้อมูล (De-encapsulation) ในแต่ละชั้นของโมเดล OSI

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์



2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

ในการสื่อสาร การส่งข้อมูลขนาดใหญ่มากบนช่องทางการสื่อสารนั้นทำให้การใช้งานสื่อไม่มีประสิทธิภาพ ยกตัวอย่าง การส่งวิดีโอเพลง (Music Video) หรือข้อความอีเมล (e-mail message) ที่จะส่งข้ามเครือข่ายจากต้นทางไปยังปลายทางเป็นสตรีมของบิตที่ต่อเนื่องขนาดใหญ่ หากข้อความถูกส่งในลักษณะนี้ จะไม่มีอุปกรณ์อื่นใดที่จะสามารถส่งหรือรับข้อความบนเครือข่ายเดียวกันได้ในขณะที่กำลังมีการถ่ายโอนข้อมูล นอกจากนี้ หากการเชื่อมโยงในโครงสร้างพื้นฐานของเครือข่ายล้มเหลวในระหว่างการส่ง จะทำให้ข้อความที่กำลังส่งนั้นหายไป ทำให้ต้นทางจะต้องทำการส่งข้อความเดิมทั้งหมดอีกครั้งหรือเรียกว่าการส่งซ้ำหรือรีทรานสมิชัน (Retransmission)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

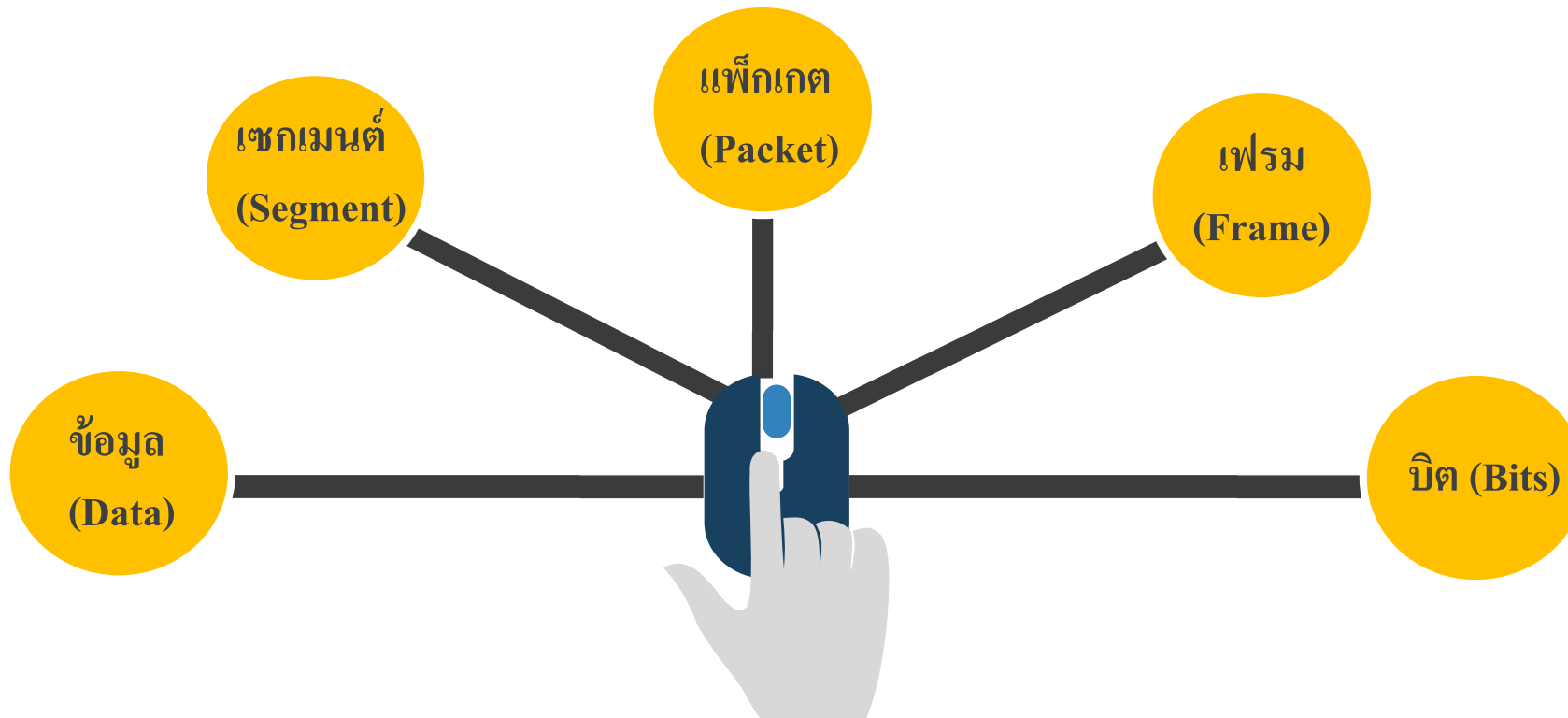


วิธีการที่ดีกว่าคือ การแบ่งข้อมูลวิดีโอเพลง (Music-Video) หรือข้อความอีเมล (e-mail Message) ออกเป็นข้อมูลชิ้นเล็ก ๆ (Data) ที่สามารถจัดการได้มากขึ้นเพื่อส่งผ่านเครือข่าย การแบ่งสตริมข้อมูลออกเป็นชิ้นเล็ก ๆ นี้เรียกว่าการแบ่งส่วนหรือการเซกเมนเตชัน (Segmentation) ซึ่งสามารถนำส่งเซกเมนต์เล็ก ๆ ของข้อความจากหลายแหล่งพร้อมกันได้ แต่อย่างไรก็ตามการส่งข้อมูลจากหลาย ๆ แหล่งพร้อมกันอาจทำให้เกิดการชนกันของเซกเมนต์เล็ก ๆ เหล่านั้นได้

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

แต่ละชั้นจะมี PDU ที่มีชื่อ รูปแบบ และข้อมูลในส่วนหัวที่เพิ่มเข้าไปใน PDU ที่แตกต่างกัน
ดังนี้



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

2.5.2 โมเดลโพรโทคอล TCP/IP (The TCP/IP Protocol Model)

โมเดลอินเทอร์เน็ต (Internet model) หรือสถาปัตยกรรมของชุดโพรโทคอล TCP/IP ที่กำหนด 4 ชั้น หรือเลเยอร์ที่ต้องมีสำหรับการสื่อสารที่ประสบความสำเร็จ จากล่างขึ้นบน ดังนี้

① ชั้นการเข้าถึงเครือข่ายหรือเน็ตเวิร์กแอ็กเซส (Network Access layer)

② ชั้นการเชื่อมต่อระหว่างเครือข่ายหรืออินเทอร์เน็ต (Internet layer)

③ ชั้นขนส่งหรือทรานสปอร์ต (Transport layer)

④ ชั้นการประยุกต์หรือแอปพลิเคชัน (Application layer)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์



2. องค์ประกอบของเครือข่ายคอมพิวเตอร์

โพรโทคอล ภายในชุดโพรโทคอลมีการทำงานร่วมกันอย่างไร คือ ดูการทำงานร่วมกันเหมือนเป็นสแต็ก (Stack) โมเดลโพรโทคอลโดยส่วนใหญ่จะอธิบายโพรโทคอลสแต็กที่เกี่ยวกับผู้ผลิตเฉพาะราย (Vendor-Specific Protocol แต่เนื่องจากโมเดล TCP/IP เป็นมาตรฐานเปิดที่ไม่มีบริษัทใดควบคุมรายละเอียดของคำนิยามของมาตรฐานและโพรโทคอล TCP/IP มีการกล่าวถึงในฟอรัมสาธารณะและถูกกำหนดไว้ใน RFC (Request for Comments) ที่ทุกคนสามารถเข้าถึงได้

หมายเหตุ

โมเดล TCP/IP มักถูกใช้อ้างอิงเฉพาะแค่เพียงชื่อ แต่ 7 ชั้นของโมเดล OSI นี้มักจะอ้างอิงกันโดยหมายเลขชั้นมากกว่าชื่อเรียกชั้น ตัวอย่างเช่น ชั้นฟิสิคัลจะถูกเรียกว่าชั้นที่ 1 ของโมเดล OSI

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. ประเภทของการสื่อสาร

3.1 การสื่อสารข้อมูลทิศทางเดียว (Simplex Transmission)

เป็นการติดต่อสื่อสารเพียงทิศทางเดียว
คือ ผู้ส่งจะส่งข้อมูลเพียงฝั่งเดียว โดยฝั่งรับ
ไม่มีการตอบกลับ เช่น เสียงตามสายการ
กระจายเสียงของสถานีวิทยุ เป็นต้น



รูปที่ 1.8 การสื่อสารข้อมูลทิศทางเดียว (Simplex Transmission)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. ประเภทของการสื่อสาร

3.2 การสื่อสารข้อมูลสองทิศทางสลับกัน (Half Duplex Transmission)

เป็นการส่งข้อมูลทั้งไปและกลับได้แต่สามารถส่งข้อมูลในเวลาใดเวลาหนึ่งไปในทิศทางเดียวเท่านั้น ทั้งฝ่ายส่งและฝ่ายรับ หรือผู้ส่งสามารถส่งข้อมูลไปให้แก่ผู้รับ ส่วนผู้รับจะสามารถโต้ตอบกลับได้ เมื่อผู้ส่งทำการส่งเสร็จแล้ว จะไม่สามารถส่งสวนทางกันได้ในเวลาเดียวกัน เช่น การใช้วิทยุสื่อสาร



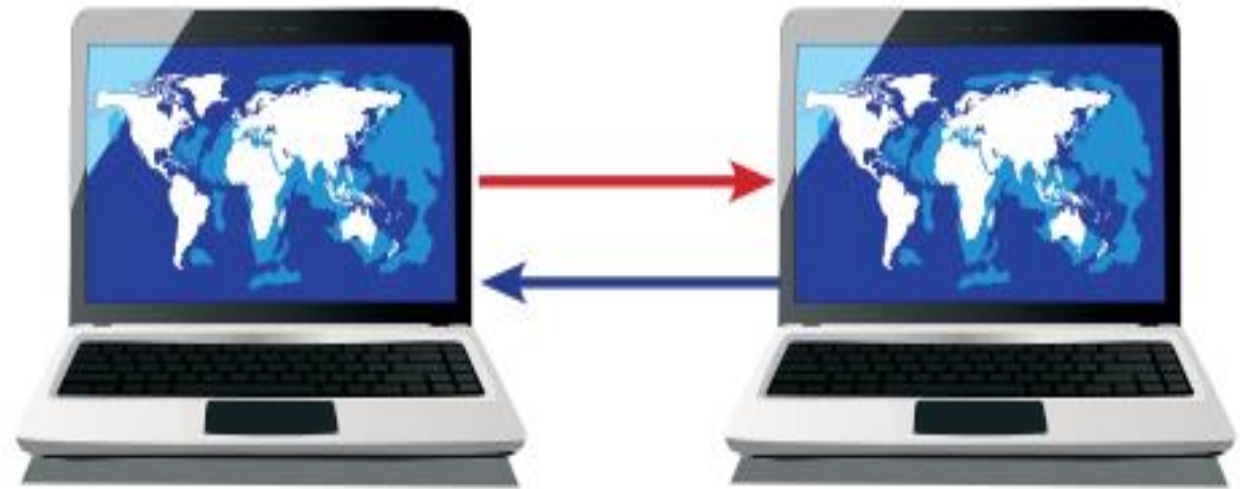
รูปที่ 1.9 การสื่อสารข้อมูลสองทิศทางสลับกัน (Half Duplex Transmission)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. ประเภทของการสื่อสาร

3.3 การสื่อสารข้อมูลสองทิศทางพร้อมกัน (Full Duplex Transmission)

คู่สนทนาสามารถส่งข้อมูลในเวลาใดเวลาหนึ่ง
ได้ทั้ง 2 ทิศทาง หรือสามารถโต้ตอบสวนทางกัน
ได้ในเวลาเดียวกันบนช่องทางการสื่อสารเดียวกัน
เช่น การพูดคุยผ่านโทรศัพท์ การทำ Video Call
หรือ การChat ผ่านโปรแกรมต่าง ๆ เป็นต้น



รูปที่ 1.10 การสื่อสารข้อมูลสองทิศทางพร้อมกัน (Full Duplex Transmission)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

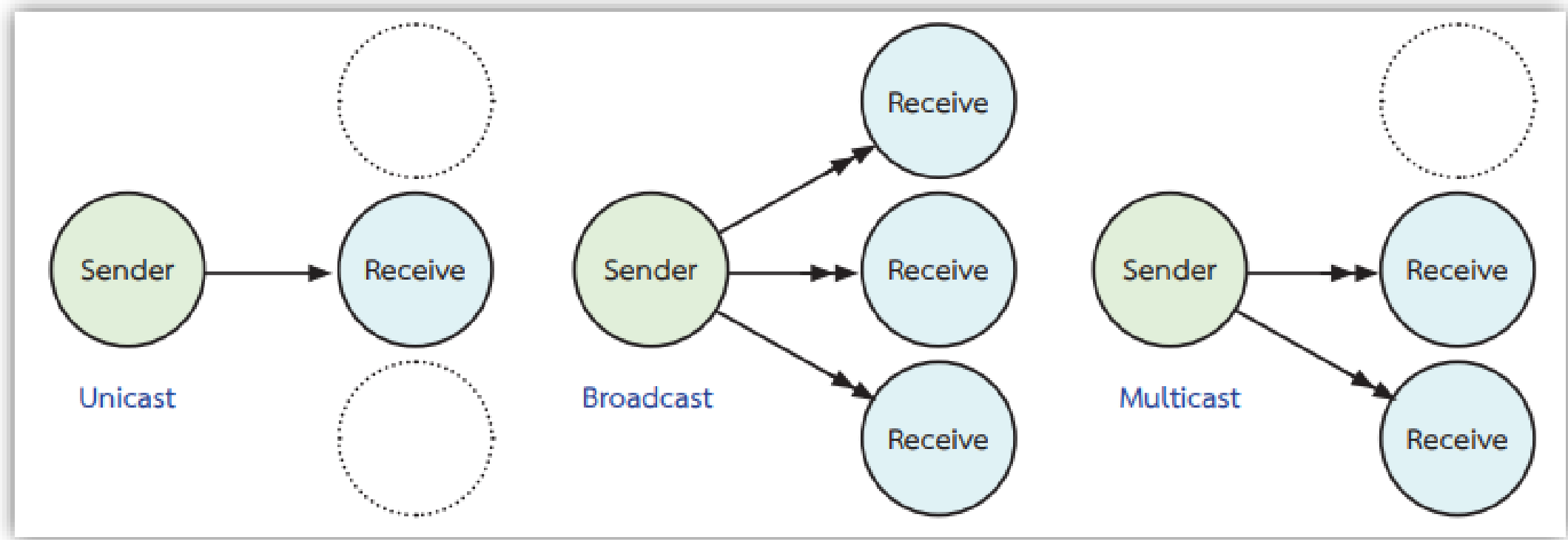


4. ตัวเลือกการส่งข้อความ

อาจต้องมีการส่งมอบข้อความในรูปแบบที่แตกต่างกัน ในบางครั้งต้องการที่จะสื่อสารข้อมูลกับบุคคลเพียงคนเดียว แต่ในบางครั้งเราอาจต้องการส่งข้อมูลไปยังหลาย ๆ บุคคลในเวลาเดียวกัน หรือแม้กระทั่งกับทุกคนที่อยู่ในพื้นที่เดียวกัน การสนทนาระหว่างคนสองคนเป็นตัวอย่างของการส่งแบบหนึ่งต่อหนึ่ง (One-to-one Delivery) แต่ผู้รับมีมากกว่าหนึ่ง และต้องการรับข้อมูลในเวลาเดียวกัน จำเป็นต้องใช้การส่งข้อความแบบหนึ่งต่อผู้รับจำนวนมาก (One-to-many Message Delivery) หรือหนึ่งต่อผู้รับทั้งหมด (One-to-all Message Delivery) โพรโทคอลเครือข่ายก็เช่นกัน จะใช้ตัวเลือกการส่งในการสื่อสารตามที่แสดงในรูปที่ 1.11

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4. ตัวเลือกการส่งข้อความ



รูปที่ 1.11 การส่งมอบข้อความในรูปแบบที่ต่างกัน

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4. ตัวเลือกการส่งข้อความ

มีบางครั้งที่ผู้ส่งข้อความต้องการแน่ใจว่าข้อความถูกส่งไปยังปลายทางได้สำเร็จเพราะข้อความนั้นมีความสำคัญ เช่น การส่งสินค้าต้องมีการยืนยันรายการสินค้าที่ส่ง จึงจำเป็นที่ผู้รับจะต้องตอบกลับการได้รับนั้นหรือเรียกว่า Acknowledgement กลับไปยังผู้ส่ง แต่ถ้าผู้ส่งไม่จำเป็นต้องได้รับการยืนยันจากผู้รับหรือที่เรียกว่า Unacknowledged เช่น การพูดคุยกันปกติไม่จำเป็นที่จะต้องตอบรับว่าเข้าใจในเรื่องที่กำลังคุยกันอยู่





5.

ประเภทของสัญญาณที่ใช้ในการสื่อสาร

การสื่อสารผ่านคอมพิวเตอร์ เป็นการสื่อสารด้วยสัญญาณไฟฟ้าผ่านสาย หรือ คลื่นวิทยุที่เป็นคลื่นแม่เหล็กไฟฟ้า หรือแม้แต่การใช้ใยแก้วนำแสงที่ต้นทางและปลายทางของสัญญาณ แสงเลเซอร์นั้นจะถูกแปลงกลับมาเป็นสัญญาณไฟฟ้า เพื่อให้การสื่อสารสมบูรณ์ทุกครั้ง การสื่อสารผ่านสัญญาณไฟฟ้านี้จะมีการส่งสัญญาณที่ใช้ในการสื่อสารอยู่ 2 ประเภท ดังนี้

5.1 สัญญาณแอนะล็อก (Analog Signal)

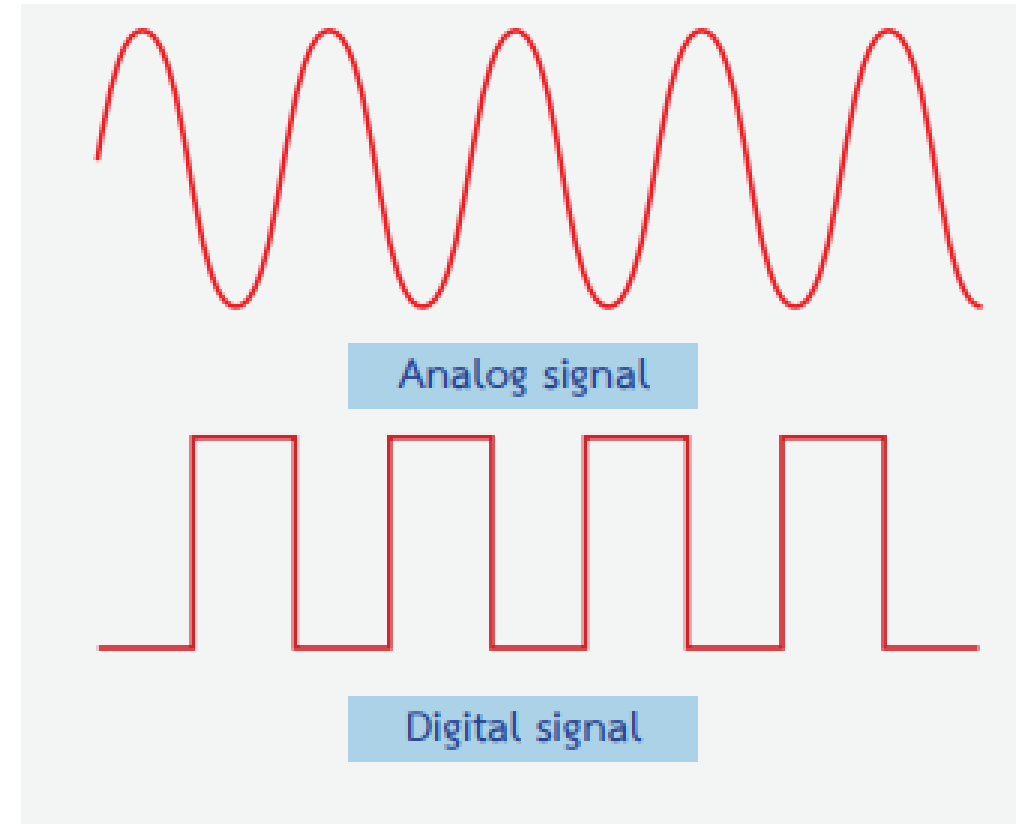
สัญญาณไฟฟ้าแบบนี้จะมีลักษณะเป็นคลื่นที่มีความเปลี่ยนแปลงของความสูง (Amplitude) และความถี่ (Frequency) เพื่อสื่อสารระหว่างต้นทางและปลายทาง ตัวอย่างเช่น การสื่อสารผ่านทางวิทยุสื่อสาร การออกอากาศจากสถานีวิทยุในระบบ AM หรือ FM

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

5. ประเภทของสัญญาณที่ใช้ในการสื่อสาร

5.2 สัญญาณดิจิทัล (Digital Signal)

เป็นสัญญาณที่ถูกแบ่งเป็นช่วง ๆ อย่างไม่ต่อเนื่อง (Discrete) โดยลักษณะของสัญญาณจะแบ่งออกเป็นสองระดับเพื่อแทนสองสถานะ คือ สถานะของบิต 0 และสถานะของบิต 1 ซึ่งแทนค่าด้วยการให้แรงดันทางไฟฟ้าที่แตกต่างกันเพียงสองระดับ แล้วนำมาถอดรหัสอีกครั้ง



รูปที่ 1.12 รูปแบบสัญญาณ Analog และ Digital

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

6. หน่วยงานกำกับดูแลด้านการสื่อสารและโทรคมนาคม

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union : ITU) มีหน้าที่ในการพัฒนามาตรฐานและกฎระเบียบ สำหรับการสื่อสารวิทยุและโทรคมนาคมระหว่างประเทศ การกำหนดแถบคลื่นความถี่วิทยุ (Allocation of the Radio Spectrum) และบริหารจัดการ กรณีที่จำเป็นสำหรับการเชื่อมโยงโครงข่ายระหว่างประเทศ เช่น บริการโทรศัพท์ใช้ระหว่างประเทศ อันเป็นภารกิจในเชิงโทรคมนาคม ในลักษณะเดียวกับการปฏิบัติงานของสหภาพสากลไปรษณีย์ ในกรณีของงานบริการไปรษณีย์



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

6. หน่วยงานกำกับดูแลด้านการสื่อสารและโทรคมนาคม

โดยในประเทศไทยได้มีการตั้งสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ หรือ “กสทช.” ขึ้นเมื่อปี พ.ศ. 2553 เป็นผู้ดูแลรับผิดชอบในการกำกับดูแล กำหนดนโยบาย ตรวจสอบ กำหนดหลักการต่าง ๆ ขึ้น รวมถึงพิจารณาการทำงาน การแข่งขันต่าง ๆ ของผู้ให้บริการ เพื่อไม่ให้เกิดความขัดแย้ง รวมถึงเพื่อป้องกันการค้าที่ไม่เป็นธรรม และช่วยเหลือผู้รับบริการให้ได้รับบริการอย่างเป็นธรรมและมีประสิทธิภาพอย่างสูงสุด



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

ระบบเครือข่ายคอมพิวเตอร์กลายเป็นปัจจัยสำคัญในการทำงานหรือแม้แต่การดำเนินชีวิตปกติของคนในยุคปัจจุบัน การทำความเข้าใจการทำงานของระบบเครือข่ายคอมพิวเตอร์ เพื่อให้เครือข่ายคอมพิวเตอร์ที่มีองค์ประกอบหลายอย่างทำงานสอดคล้องเหมาะสมภายใต้มาตรฐานเดียวกัน สามารถใช้งานได้อย่างเต็มความสามารถ ย่อมส่งผลให้การปฏิบัติงานทำได้ด้วยความราบรื่นมีประสิทธิภาพตามไปด้วย





ประเภทของเครือข่าย คอมพิวเตอร์



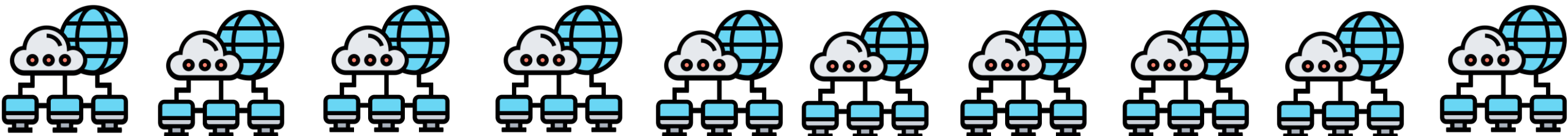
ประเภทของเครือข่ายคอมพิวเตอร์

1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์

1.1 เครือข่ายแบบลูกข่าย/แม่ข่ายหรือไคลเอนต์/เซิร์ฟเวอร์ (Client/Server)

ไคลเอนต์/เซิร์ฟเวอร์ คือ เครื่องผู้ให้บริการ หรือแม่ข่าย หรือเซิร์ฟเวอร์ (Server) และเครื่องผู้ให้บริการ หรือลูกข่าย หรือไคลเอนต์ (Client) เชื่อมต่อกัน และเครื่องผู้ให้บริการสามารถติดต่อร้องขอบริการจากเครื่องผู้ให้บริการ เครื่องผู้ให้บริการจะตอบสนองตามที่เครื่องผู้ขอใช้บริการร้องขอ

ไคลเอนต์ คือ เครื่องคอมพิวเตอร์ที่ไปร้องขอบริการและรับบริการอย่างใดอย่างหนึ่งจากเซิร์ฟเวอร์



ประเภทของเครือข่ายคอมพิวเตอร์

1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์

เครื่องเซิร์ฟเวอร์ คือ เครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง โดยบริการทรัพยากรให้กับเครื่องลูกข่าย เช่น บริการไฟล์ (File Server) การบริการงานพิมพ์ (Print Server) เป็นต้น เครื่องเซิร์ฟเวอร์อาจเป็นคอมพิวเตอร์ที่มีประสิทธิภาพสูงหรือคอมพิวเตอร์ทั่วไปก็ได้ขึ้นอยู่กับลักษณะการใช้งาน โดยเครื่องที่ออกแบบมาเพื่อใช้งานเป็นเครื่องเซิร์ฟเวอร์นี้มักจะมีสมรรถนะสูง รวมถึงถูกออกแบบมาเพื่อรองรับความทนทานต่อความผิดพลาด (Fault Tolerance) และมีระบบสำรองต่าง ๆ เช่น ระบบไฟสำรอง ระบบสำรองข้อมูล ในกรณีที่ข้อมูลหรือระบบงานมีความสำคัญมาก ๆ อาจมีการออกแบบระบบเซิร์ฟเวอร์สำรองขึ้นมาทั้งระบบ โดยออกแบบให้ทำงานคู่ขนานกับเครื่องเซิร์ฟเวอร์หลักที่เรียกว่า “Mirror Server” ในกรณีที่เครื่องหลักขัดข้อง เครื่องเซิร์ฟเวอร์สำรองจะทำงานแทนในทันที



ประเภทของเครือข่ายคอมพิวเตอร์

1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์

หน้าที่ของเครื่องเซิร์ฟเวอร์มีหลากหลายรูปแบบขึ้นอยู่กับการใช้งาน โดยคอมพิวเตอร์หนึ่งตัวอาจจะทำงานหลายประเภท แยกงานกันทำหรือใช้คอมพิวเตอร์เซิร์ฟเวอร์หลาย ๆ เครื่องทำงานเดียวกันก็ได้ เช่น

 ไฟล์เซิร์ฟเวอร์ (File Server) คือ เครื่องที่ให้บริการแฟ้มข้อมูลให้แก่เครื่องลูกข่าย

 พริ้นท์เซิร์ฟเวอร์ (Print Server) คือ เครื่องที่บริการงานพิมพ์ให้แก่เครื่องลูกข่าย โดยบันทึกงานพิมพ์เก็บไว้ในรูปแบบของสพูล (Spool) และดำเนินการพิมพ์งานตามลำดับคิว



ประเภทของเครือข่ายคอมพิวเตอร์

1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์

-  ดาตาเบสเซิร์ฟเวอร์ (Database Server) คือ เครื่องที่บริการฐานข้อมูลให้แก่เครื่องลูกข่าย
-  เว็บเซิร์ฟเวอร์ (Web Server) คือ เครื่องที่จัดเก็บข้อมูลด้านเว็บเพจขององค์กร
-  อีเมลเซิร์ฟเวอร์ (Email Server) คือ เครื่องที่จัดเก็บข้อมูลอีเมล
-  แพตช์เซิร์ฟเวอร์ (Patch Server) ให้บริการกำหนดการอัปเดตรุ่น (Version Patch) การทำงานให้กับเครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์อื่น



ประเภทของเครือข่ายคอมพิวเตอร์

1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์

เครื่องเซิร์ฟเวอร์ไม่จำเป็นจะต้องอยู่ที่เดียวกันกับเครื่องลูกข่าย นอกจากนี้ เครื่องเซิร์ฟเวอร์อาจประกอบด้วยคอมพิวเตอร์หลาย ๆ เครื่องช่วยกันทำงานประมวลผล หรือให้บริการข้อมูลผ่านระบบเครือข่ายที่เรียกว่า Cloud Computing เพื่อทำให้ระบบสามารถรองรับผู้ใช้บริการจำนวนมากได้ และสามารถขยายประสิทธิภาพของระบบได้ในเวลาอันรวดเร็ว เช่น เซิร์ฟเวอร์ที่ให้บริการ YouTube Facebook หรือระบบ Search Engine ของ Google



ประเภทของเครือข่ายคอมพิวเตอร์

1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์

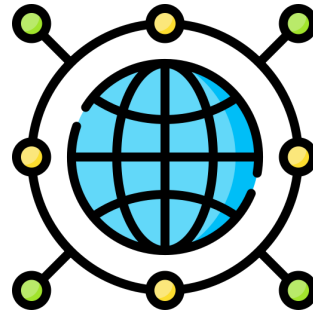


รูปที่ 2.1 ไคลเอนต์และเซิร์ฟเวอร์

ประเภทของเครือข่ายคอมพิวเตอร์

1.

รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์



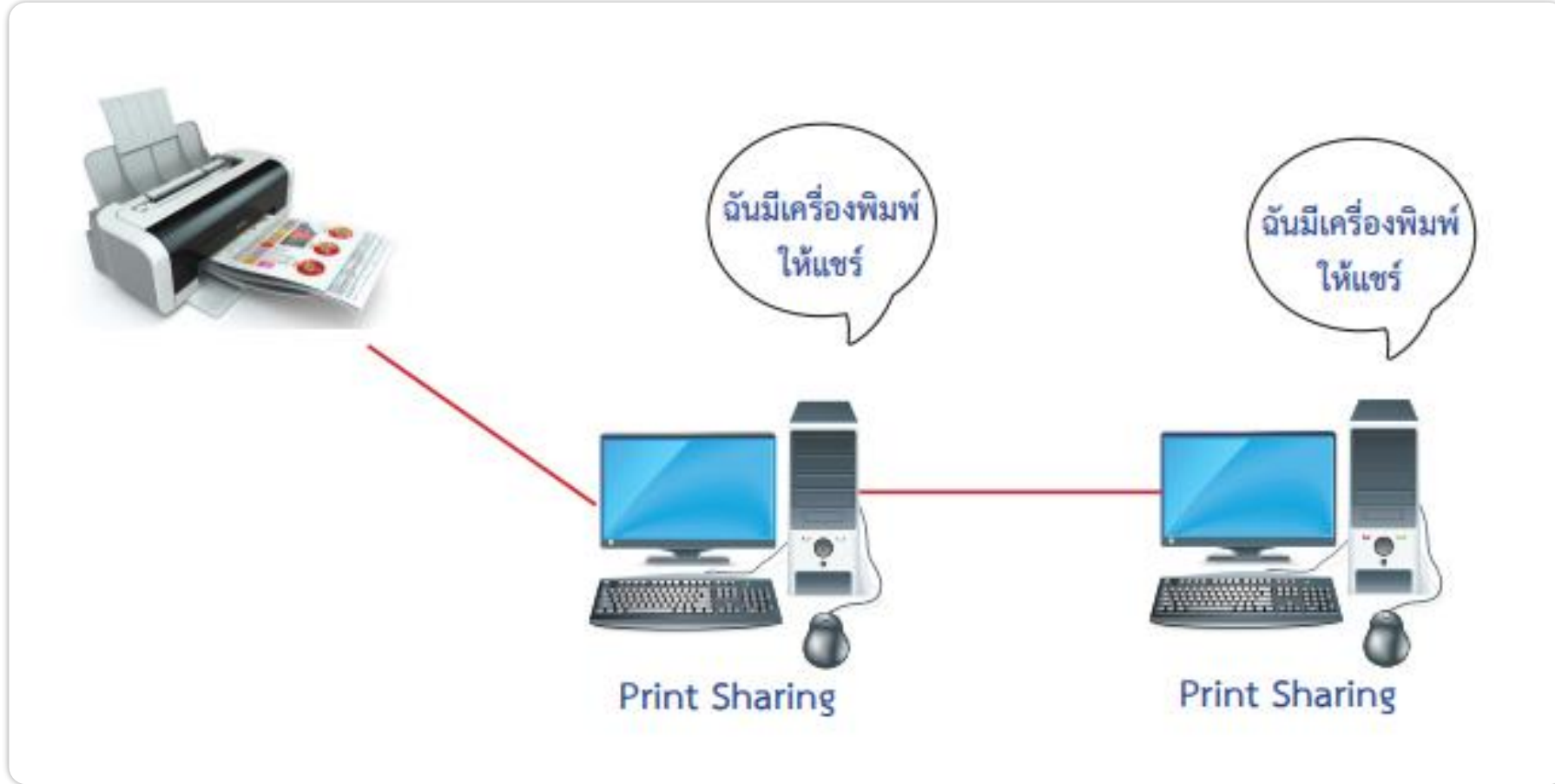
1.2 เครือข่ายแบบเพียร์-ทู-เพียร์ (Peer-to-Peer)

เพียร์-ทู-เพียร์ เป็นระบบเครือข่ายขนาดเล็กที่อยู่ในกลุ่มเดียวกันที่เรียกอีกอย่างหนึ่งว่า Workgroup โดยเครื่องคอมพิวเตอร์ทุกเครื่องจะมีความอิสระเท่าเทียมกัน นิยมใช้ในงานทั่วไปในสำนักงานขนาดเล็ก เนื่องจากเป็นระบบที่มีค่าใช้จ่ายถูก ส่วนมากนิยมนำมาใช้ในการแชร์ไฟล์และแชร์เครื่องพิมพ์

เครือข่ายแบบนี้จะเก็บไฟล์และการเชื่อมต่อกับอุปกรณ์ต่าง ๆ ไว้ที่เครื่องคอมพิวเตอร์ของผู้ใช้แต่ละคน โดยไม่มีคอมพิวเตอร์ส่วนกลางที่ทำหน้าที่นี้ ต่างคนต่างเก็บต่างใช้ แต่ผู้ใช้ในเครือข่ายสามารถเรียกใช้ไฟล์จากคอมพิวเตอร์เครื่องอื่นได้ ถ้าคอมพิวเตอร์เครื่องนั้นทำการแชร์ไฟล์เหล่านั้นไว้ เครือข่ายแบบเพียร์-ทู-เพียร์ เหมาะสำหรับองค์กรขนาดเล็กที่มีคอมพิวเตอร์เชื่อมต่อกันไม่เกิน 10 เครื่อง

ประเภทของเครือข่ายคอมพิวเตอร์

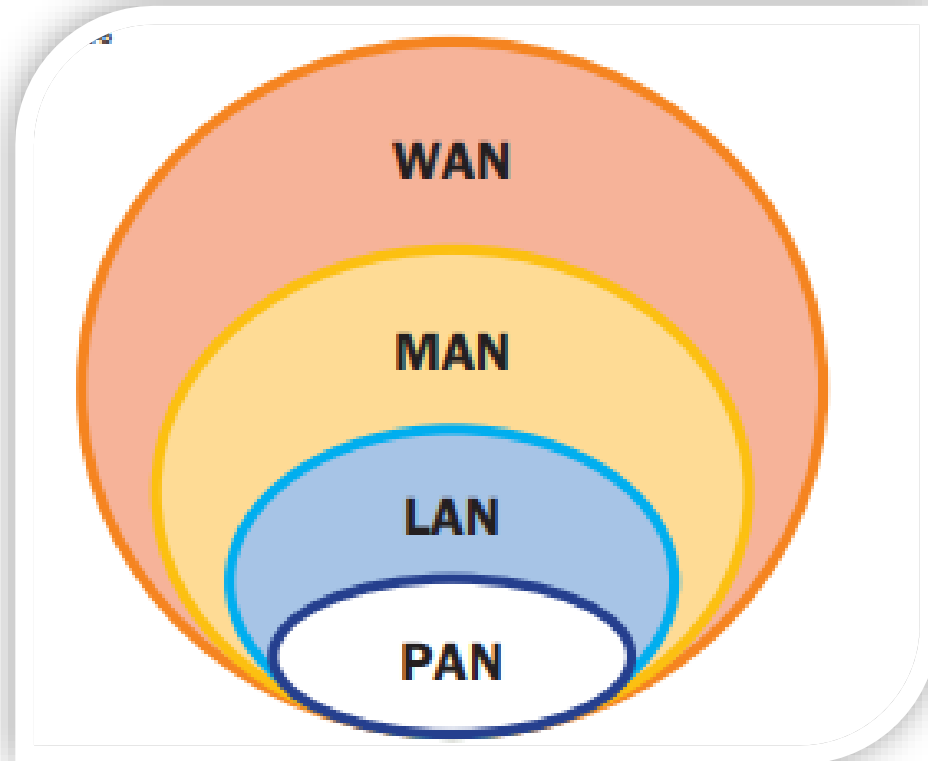
1. รูปแบบการเชื่อมต่อเพื่อให้บริการระบบเครือข่ายคอมพิวเตอร์



รูปที่ 2.2 เครือข่ายเพียร์-ทู-เพียร์แบบง่าย

ประเภทของเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม
แบ่งออกเป็น 4 ประเภท ดังนี้



รูปที่ 2.3 ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม

2.1 เครือข่ายส่วนบุคคลหรือแพน (Personal Area Network : PAN)

เครือข่ายส่วนบุคคลเป็นเครือข่ายที่ใช้สำหรับการสื่อสารระหว่างอุปกรณ์ที่ใช้งานอย่างใกล้ชิดกับผู้ใช้งาน บางทีอาจเรียกว่าเครือข่ายในบ้าน (Home Area Network : HAN)

เครือข่ายส่วนบุคคลแบบใช้สายอาจมีการเชื่อมต่ออุปกรณ์ต่าง ๆ เข้าด้วยกันผ่านพอร์ตต่าง ๆ เช่น USB อีเทอร์เน็ต



รูปที่ 2.4 เครือข่ายส่วนบุคคลแบบมีสาย

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม

เครือข่ายส่วนบุคคลแบบไร้สาย (Wireless Personal Area Network : WPAN) เป็นอีกหนึ่งเครือข่ายที่มีการใช้งานกันมากในปัจจุบัน เช่น การเชื่อมต่อสมาร์ทโฟนเข้ากับหูฟังบลูทูธ สมาร์ทโฟนกับสมาร์ทโฟน ฯลฯ โดย WPAN มีรัศมีการครอบคลุมประมาณ 10 เมตร WPAN สามารถใช้สำหรับการสื่อสารระหว่างอุปกรณ์หรือเป็นทางเข้าออกหรือพอร์ทัล (Portal) ไปยังเครือข่ายอื่น เช่น ระบบเครือข่ายท้องถิ่นหรือแลน และ/หรืออินเทอร์เน็ต เทคโนโลยีที่พบมากที่สุดภายใน WPAN คือ บลูทูธและอินฟราเรด โดยอินฟราเรดเป็นสื่อแสง ในขณะที่บลูทูธเป็นสื่อความถี่วิทยุ



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม

เทคโนโลยีที่ใช้สำหรับ WPAN ได้ถูกกำหนดโดยคณะกรรมการ IEEE 802.15 เช่น Bluetooth และ ZigBee โดย ZigBee เป็นอีกสื่อไร้สายที่อาจเกิดขึ้นได้ของเครือข่ายไร้สายที่มีต้นทุนต่ำระหว่างอุปกรณ์ในสถาปัตยกรรม WPAN

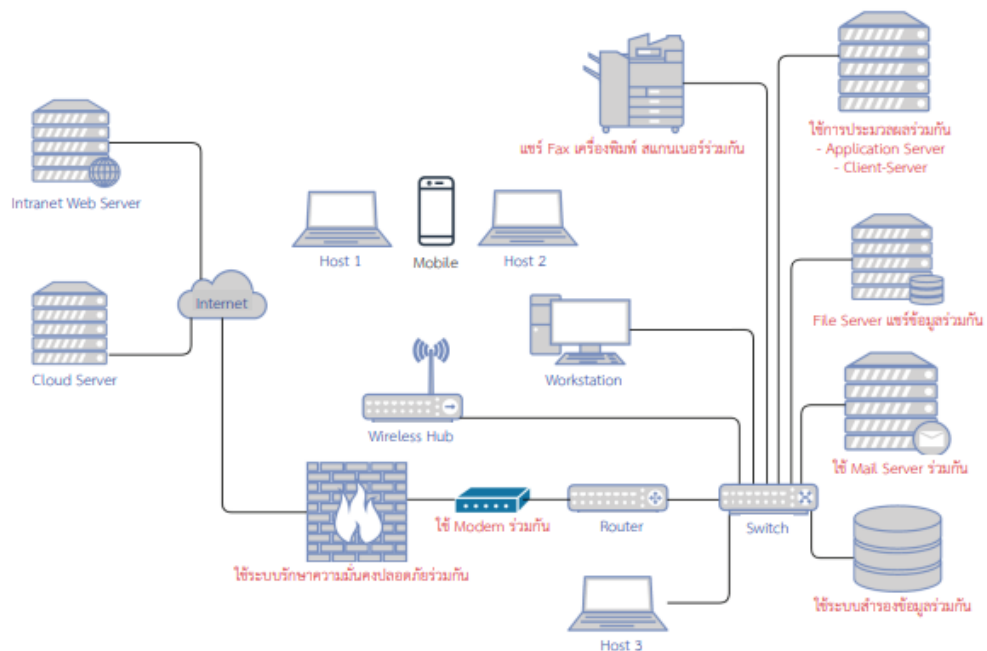


รูปที่ 2.5 เครือข่ายส่วนบุคคลแบบไร้สาย

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม

2.2 เครือข่ายท้องถิ่นหรือแลน (Local Area Network : LAN)



เป็นเครือข่ายระยะใกล้หรือเครือข่ายเฉพาะที่ ใช้กัน
อยู่ในบริเวณไม่กว้างนัก อาจอยู่ในองค์กรเดียวกัน หรือ
อาคารที่ใกล้กัน เช่น ภายในสำนักงาน ภายในโรงเรียน
หรือมหาวิทยาลัย เครือข่ายแลนมักบริการและจัดการโดย
หน่วยงานเจ้าของแลนนั่นเพียงรายเดียว หรืออาจมีการ
ว่าจ้างผู้ให้บริการภายนอกในการดูแลแทน

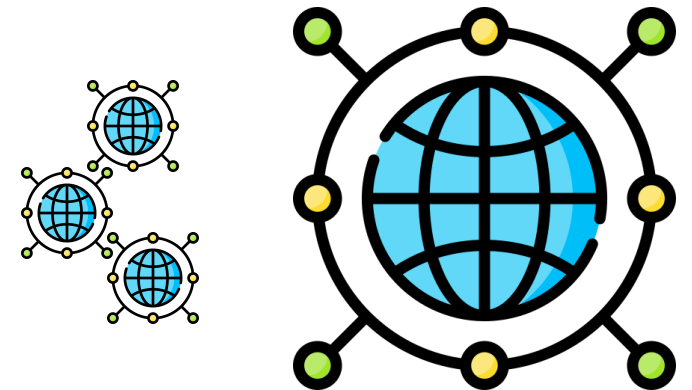
รูปที่ 2.6 เครือข่ายท้องถิ่นหรือแลน

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม

ระบบแลนช่วยให้ติดต่อกันได้สะดวก ช่วยลดต้นทุน และเพิ่มประสิทธิภาพในการทำงาน อุปกรณ์ต่าง ๆ ก่อให้เกิดประโยชน์และเพิ่มประสิทธิภาพการทำงานขององค์กรในหลายด้าน เช่น

- 📶 การใช้อุปกรณ์ร่วมกัน (Sharing of Peripheral Devices) ทำให้ผู้ใช้สามารถใช้อุปกรณ์ต่อพ่วงกับระบบคอมพิวเตอร์ร่วมกันได้อย่างมีประสิทธิภาพ เช่น เครื่องพิมพ์ สแกนเนอร์ เราเตอร์ โมเด็ม ทำให้ประหยัดค่าใช้จ่าย



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม

-  การใช้โปรแกรมและข้อมูลร่วมกัน (Sharing of Program and Data) ผู้ใช้สามารถใช้โปรแกรมและข้อมูลร่วมกันได้ โดยจัดเก็บโปรแกรมไว้ แหล่งเก็บข้อมูล เช่น ฮาร์ดดิสก์ของเครื่อง File Server ทำให้ไม่ต้องติดตั้งโปรแกรมลงในเครื่องคอมพิวเตอร์ที่ใช้ทำงาน ลดต้นทุนและความซ้ำซ้อนของข้อมูล
-  การประมวลผลร่วมกัน (Client Server) สามารถออกแบบโปรแกรมคอมพิวเตอร์ที่เชื่อมต่อกันบนเครือข่ายมาช่วยกันประมวลผลการทำงานของโปรแกรมต่าง ๆ ในองค์กร เพื่อเพิ่มประสิทธิภาพการทำงานโดยรวมและทำให้เกิดความคุ้มค่าในการลงทุนระบบมากที่สุด

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม

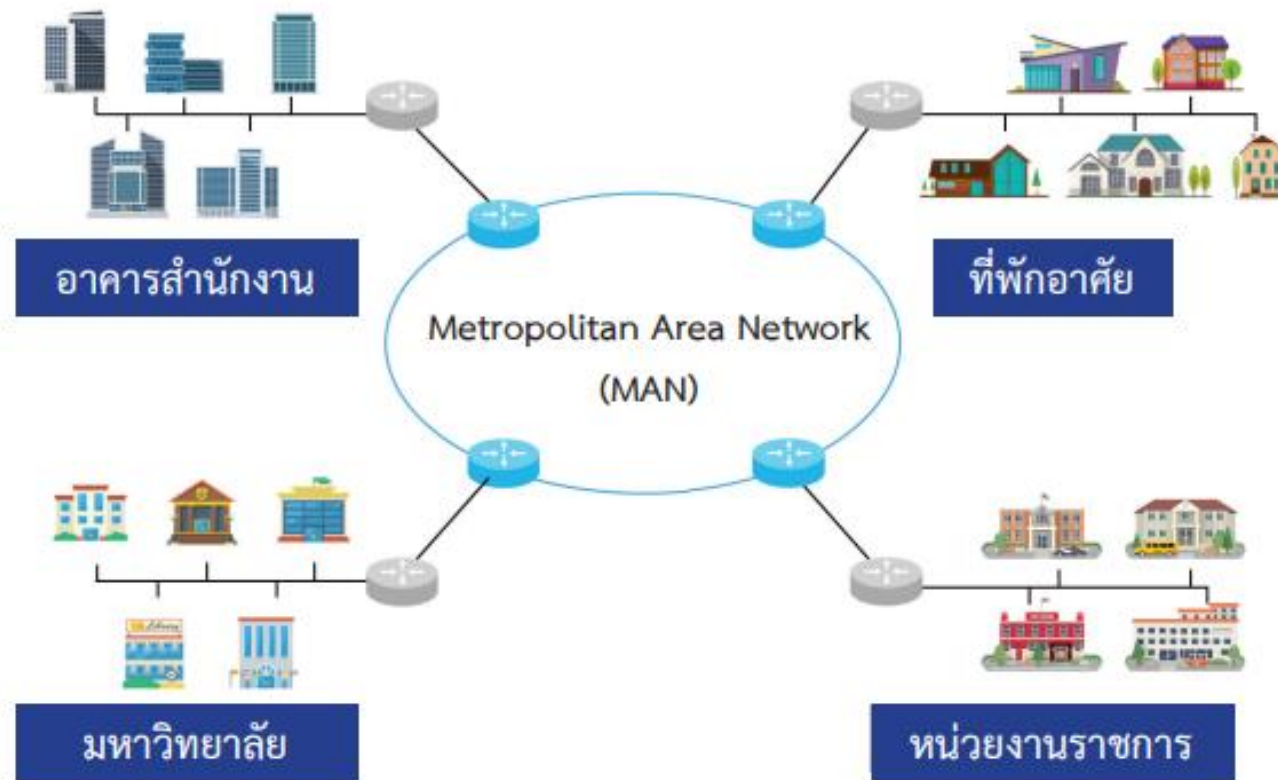
2.3 เครือข่ายระดับเมืองหรือแมน (Metropolitan Area Network หรือ MAN)

เป็นโครงสร้างพื้นฐานเครือข่ายที่ครอบคลุมพื้นที่ทางกายภาพที่มีขนาดใหญ่กว่าแลน แต่มีขนาดเล็กกว่าแวน (ครอบคลุมภายในเมือง หรือจังหวัดที่ใกล้เคียง ยกตัวอย่าง กรุงเทพมหานคร อาจจะมีเครือข่ายของตนเองที่เชื่อมต่อหน่วยงานต่าง ๆ ภายใต้การกำกับดูแลเข้าด้วยกัน เช่น หน่วยงานราชการ มหาวิทยาลัย ที่พักอาศัย และอาคารสำนักงาน) โดยทั่วไป MAN จะดำเนินการโดยองค์กรเดียว เช่น องค์กรขนาดใหญ่ระบบเคเบิลทีวีที่มีสมาชิกตามบ้านทั่วไปที่เราดูกันอยู่ทุกวันนี้จัดเป็นระบบเครือข่ายแบบ MAN



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม



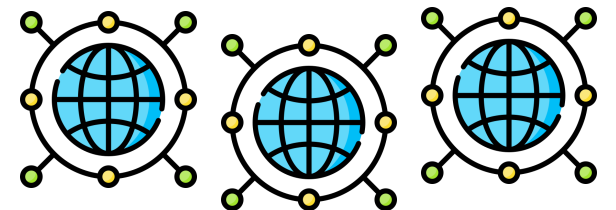
รูปที่ 2.7 เครือข่ายระดับเมืองหรือแมน

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม

2.4 เครือข่ายวงกว้างหรือแวน (Wide Area Network หรือ WAN)

เมื่อบริษัทหรือองค์กรมีสถานที่ตั้งที่มีการแยกจากกันโดยระยะทางภูมิศาสตร์ขนาดใหญ่อาจจำเป็นต้องใช้ผู้ให้บริการการสื่อสารโทรคมนาคม (Telecommunications Service Provider : TSP) ผู้ให้บริการ (Service Providers : SP) หรือผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers : ISP) ในการเชื่อมต่อระบบเครือข่ายในสถานที่ที่แตกต่างกัน ผู้ให้บริการโทรคมนาคมทำงานเครือข่ายในระดับภูมิภาคที่มีขนาดใหญ่ที่สามารถเชื่อมต่อระยะทางไกลได้ โดยดั้งเดิมแล้ว TSP ทำการขนส่งการสื่อสารด้วยเสียงและข้อมูลบนเครือข่ายที่แยกจากกัน แต่เมื่อมีการใช้บริการมากขึ้น ผู้ให้บริการเหล่านี้จะนำเสนอบริการเครือข่ายข้อมูลรวมกัน (Converged Information Network Services) ทั้งเสียง ข้อมูลและมัลติมีเดียให้กับสมาชิก

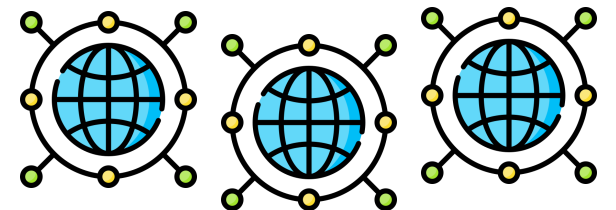


องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม

แต่ละองค์กรมักจะเข้าการเชื่อมต่อผ่านเครือข่ายผู้ให้บริการโทรคมนาคม เครือข่ายเหล่านี้ที่เชื่อมต่อระบบเครือข่ายในสถานที่แยกกันทางภูมิศาสตร์จะเรียกว่า เครือข่ายบริเวณกว้างหรือแวน (Wide Area Networks : WANs) แม้ว่าองค์กรนั้นจะดูแลรักษากำหนดนโยบายและการบริหารทั้งหมดบนเครือข่ายแลนที่ปลายทั้งสองของการเชื่อมต่อ แต่นโยบายภายในเครือข่ายผู้ให้บริการการสื่อสารจะถูกควบคุมโดย TSP

“แวน” ใช้อุปกรณ์เครือข่ายที่ออกแบบมาโดยเฉพาะเพื่อสร้างการเชื่อมต่อระหว่าง (Interconnection) แลนเข้าด้วยกันเพราะต้องมีการกำหนดค่า (Configuring) การติดตั้ง (Installing) และการบำรุงรักษา (Maintaining) โดยผู้ให้บริการโดยสรุป คุณลักษณะเฉพาะของแวน ได้แก่



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ที่ครอบคลุม

- ❏ แวนจะทำการเชื่อมต่อแลนต่าง ๆ เข้าด้วยกัน โดยแลนเหล่านั้นอยู่ในพื้นที่ทางภูมิศาสตร์กว้างหรือ ภูมิศาสตร์ที่แตกต่างกัน เช่น ระหว่างเมือง รัฐ จังหวัด ประเทศหรือทวีป
- ❏ แวนมักจะดำเนินการโดยผู้ให้บริการหลายราย
- ❏ โดยปกติแวนจะมีแบนด์วิดท์ที่ใช้การเชื่อมโยงต่ำ
- ❏ นอกเหนือจากนี้ ผู้ใช้งานไม่สามารถจะควบคุมอุปกรณ์ที่ใช้เชื่อมต่อในแวนได้

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

2. ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม



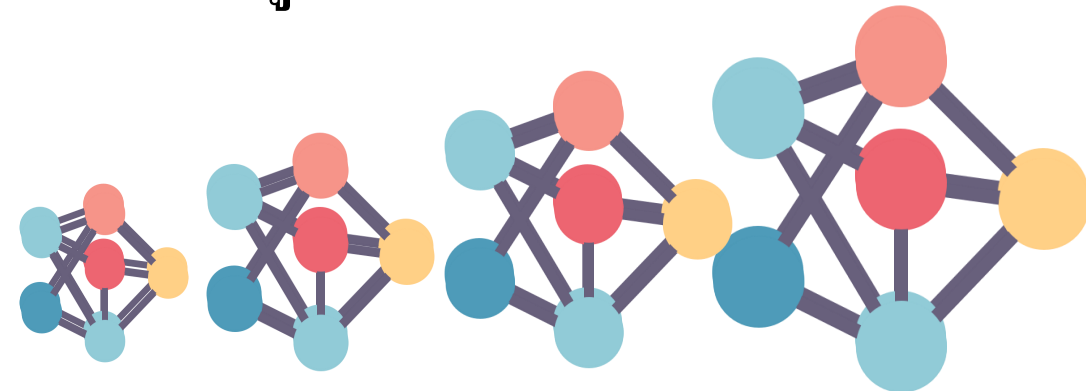
รูปที่ 2.8 เครือข่ายวงกว้างหรือแวน

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

3.1 อินเทอร์เน็ต (The Internet)

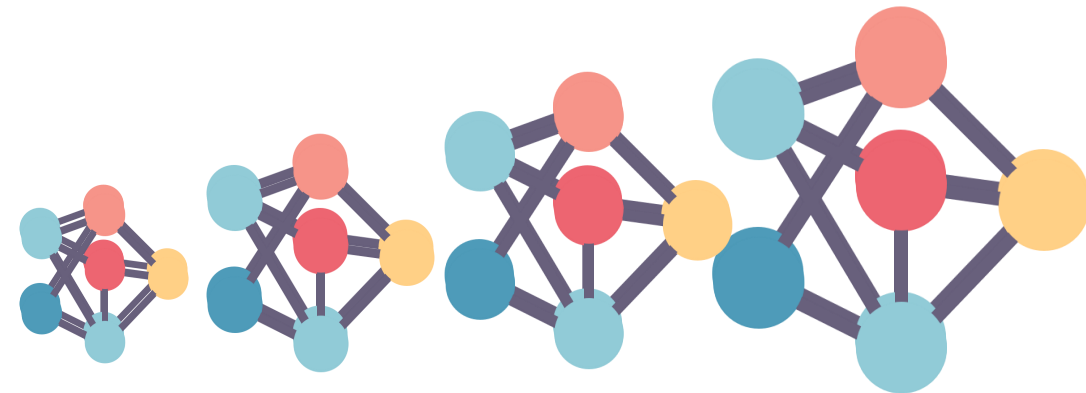
แม้ว่าการใช้ PAN LAN MAN หรือ WAN จะมีประโยชน์ แต่คนส่วนใหญ่ยังต้องการที่จะสื่อสารกับทรัพยากรบนเครือข่ายอื่นที่อยู่นอกเครือข่ายตนเอง ไม่ว่าจะเป็นเครือข่ายท้องถิ่น มหาวิทยาลัย หรือองค์กรล้วนต้องการเชื่อมต่อเครือข่ายภายนอกซึ่งสามารถจะกระทำได้โดยการใช้อินเทอร์เน็ต เพื่อจะเข้าถึงทรัพยากรของเครือข่ายอื่นบนอินเทอร์เน็ต เช่น การดูวิดีโอ การฟังเพลง การค้นหาข้อมูล การแลกเปลี่ยนไฟล์ การเล่นเกม เป็นต้น



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

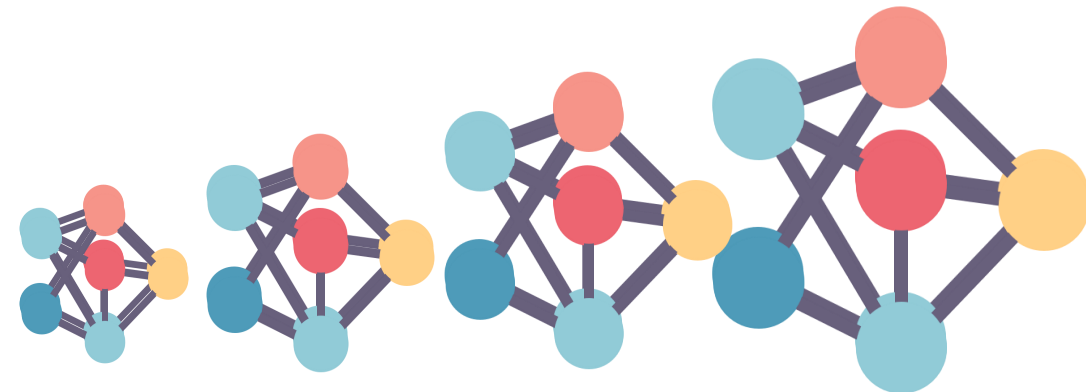
อินเทอร์เน็ตเป็นการรวบรวมเครือข่ายทั่วโลกที่เชื่อมต่อกัน เรียกว่า อินเทอร์เน็ตเวิร์ก (Internetworks) หรือเรียกย่อว่า “อินเทอร์เน็ต” (Internet) โดยได้รับความร่วมมือจากแต่ละเครือข่ายในการแลกเปลี่ยนข้อมูลโดยใช้มาตรฐานเดียวกัน ผ่านสายโทรศัพท์ สายเคเบิลทองแดง สายเคเบิลใยแก้วนำแสง การส่งสัญญาณไร้สาย และการเชื่อมโยงผ่านดาวเทียม ทำให้ผู้ใช้อินเทอร์เน็ตสามารถแลกเปลี่ยนข้อมูลในหลากหลายรูปแบบ



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

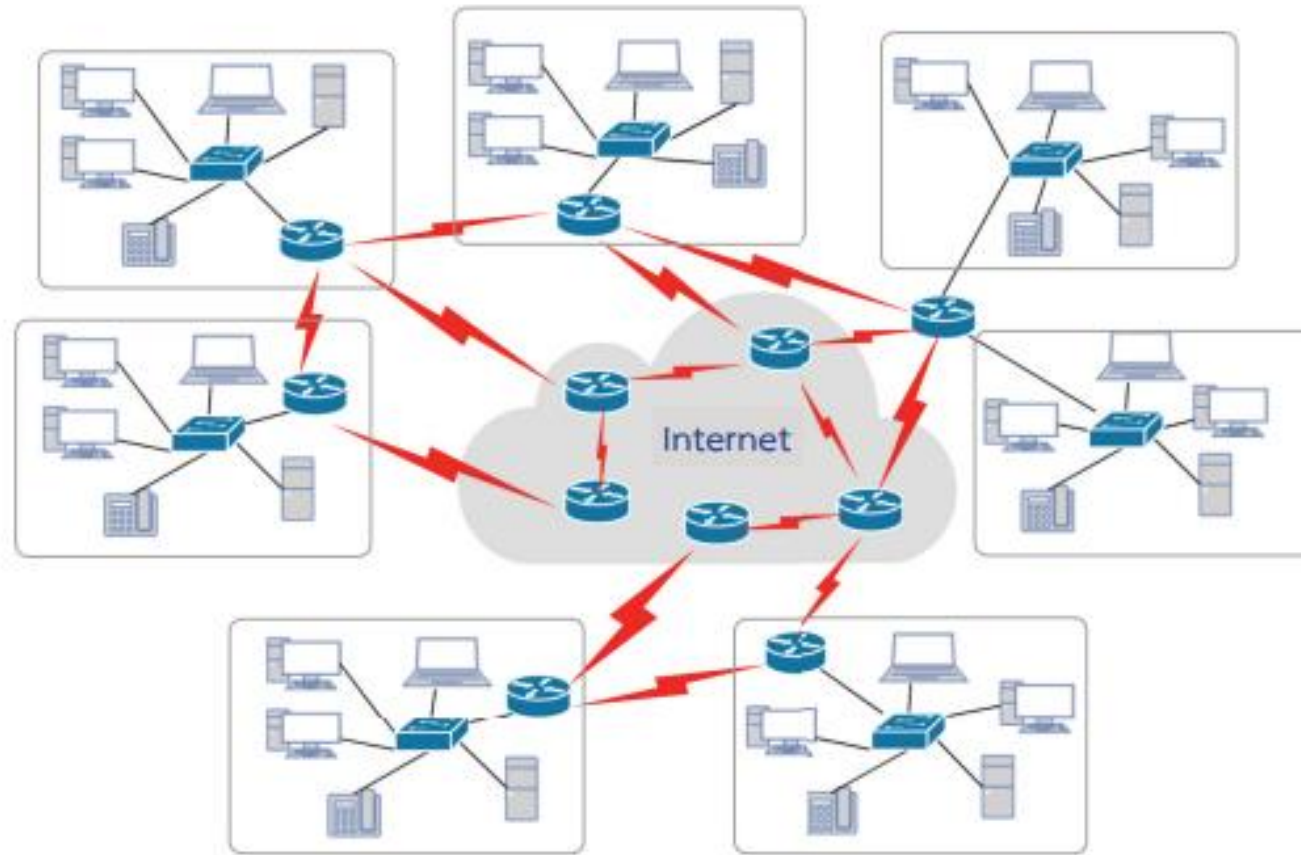
3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

อินเทอร์เน็ตเป็นกลุ่มของเครือข่ายและไม่ได้เป็นเจ้าของโดยบุคคลใดหรือกลุ่มใด เพื่อความมั่นใจในการสื่อสารที่มีประสิทธิภาพในโครงสร้างพื้นฐานที่มีความหลากหลายนี้ จำเป็นต้องมีเทคโนโลยีและมาตรฐานที่ใช้ที่สอดคล้องและเป็นที่ยอมรับกันทั่วไป โดยเป็นความร่วมมือของหน่วยงานการบริหารเครือข่ายจำนวนมาก มีองค์กรที่ได้รับการพัฒนาขึ้นเพื่อวัตถุประสงค์ในการให้ความช่วยเหลือในการบำรุงรักษาและดูแลโครงสร้างและมาตรฐานของโพรโทคอลและโพรเซสที่ใช้ในอินเทอร์เน็ต โดยองค์กรเหล่านี้รวมถึง Internet Engineering Task Force (IETF), Internet Corporation for Assigned Names and Numbers (ICANN) และ Internet Architecture Board (IAB) และองค์กรอื่น ๆ อีกมากมาย



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)



รูปที่ 2.9 อินเทอร์เน็ต

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

หมายเหตุ

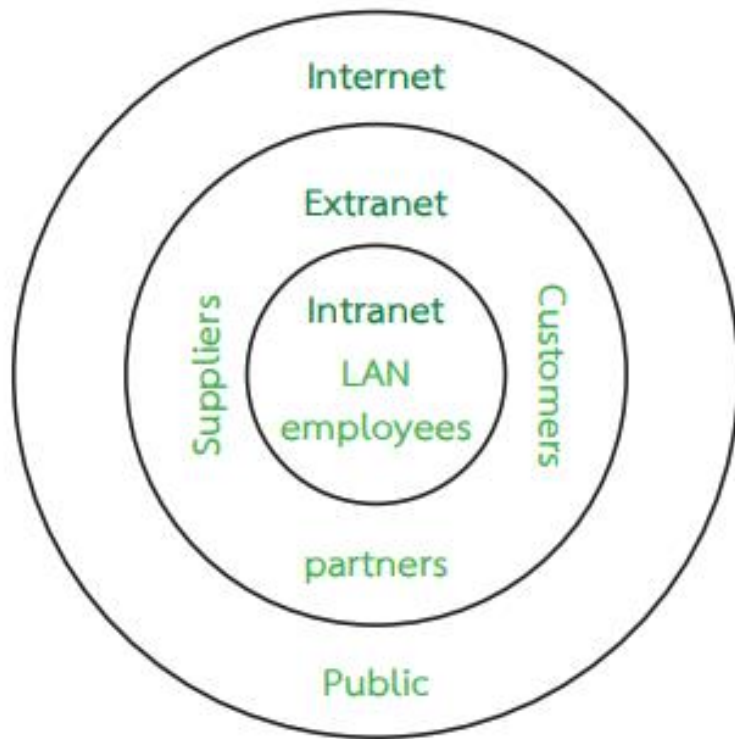
1. อินเทอร์เน็ตที่ใช้ตัวอักษร “i” ตัวเล็ก คือ internet ถูกนำมาใช้เพื่ออธิบายการเชื่อมต่อระหว่างเครือข่ายต่าง ๆ แต่เมื่อก้าวถึงเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อกันหรือเวปไซด์ไวด์เว็บในระดับโลก จะใช้ตัวอักษร “I” ตัวใหญ่ คือ Internet ซึ่งคือเครือข่ายของเครือข่าย (Network of Networks) ที่เชื่อมต่อกันทั่วโลก
2. คำต่อไปนี้อาจจะใช้แทนกัน Internetwork (เครือข่ายที่เชื่อมต่อกัน) Data Network (เครือข่ายข้อมูล) และ Network (เครือข่าย) โดยการเชื่อมต่อของสองเครือข่ายหรือมากกว่านั้นเข้าด้วยกันจะสร้างรูปแบบ Internetwork ขึ้น โดยอาจอ้างถึง Internetwork ว่าเป็นเครือข่ายข้อมูลหรือเป็นเพียงเครือข่ายที่เชื่อมต่อกัน เมื่อพิจารณาการสื่อสารในระดับสูง การใช้งานคำศัพท์ (Terms) นี้ขึ้นอยู่กับบริบทในเวลานั้นและคำศัพท์อาจมีการใช้สลับกันได้

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3.

อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

3.2 อินทราเน็ตและเอกซ์ทราเน็ต (Intranet and Extranet)



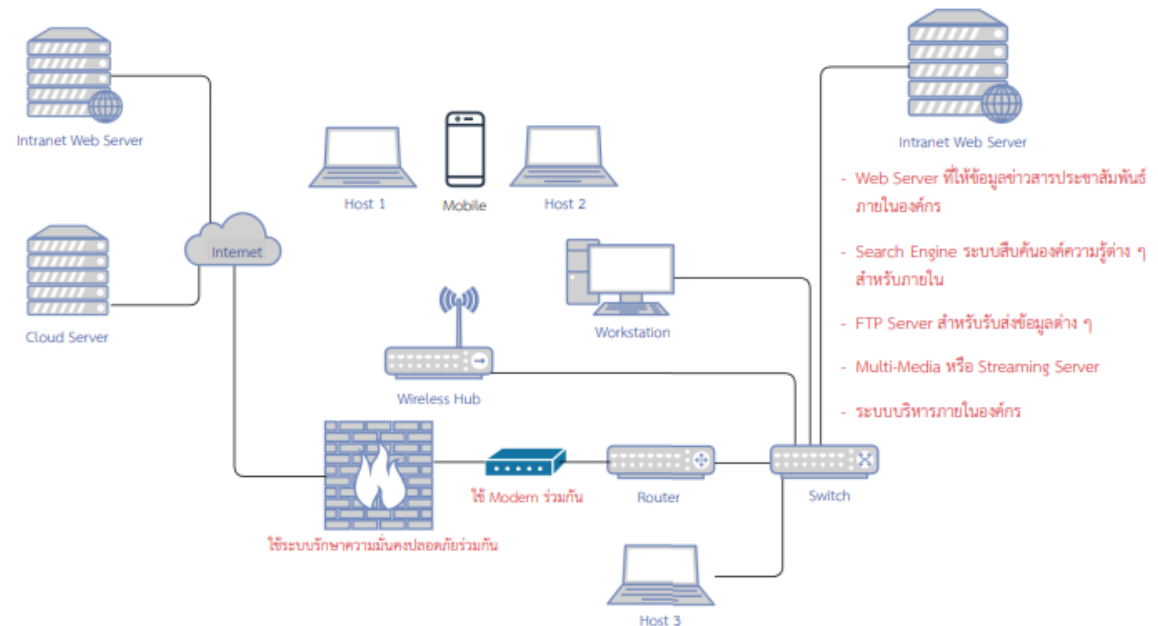
มีอีกคำศัพท์ที่เรียกประเภทของเครือข่ายอีก
สองคำที่มีความคล้ายคลึงกับคำว่าอินเทอร์เน็ต คือ
อินทราเน็ตและเอกซ์ทราเน็ต (รูปที่ 2.10)

รูปที่ 2.10 อินเทอร์เน็ต อินทราเน็ต และเอกซ์ทราเน็ต

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

อินทราเน็ตเป็นคำที่มักจะใช้เพื่ออ้างถึง การเชื่อมต่อส่วนตัวของแลนและแวนที่เป็น ขององค์กรหนึ่ง และถูกออกแบบมาให้สามารถ เข้าถึงได้เฉพาะสมาชิกขององค์กร พนักงาน หรือคนอื่น ๆ ที่ได้รับอนุญาต อินทราเน็ตโดย พื้นฐาน คือ อินเทอร์เน็ตที่จะสามารถเข้าถึงได้ จากภายในองค์กรเท่านั้น

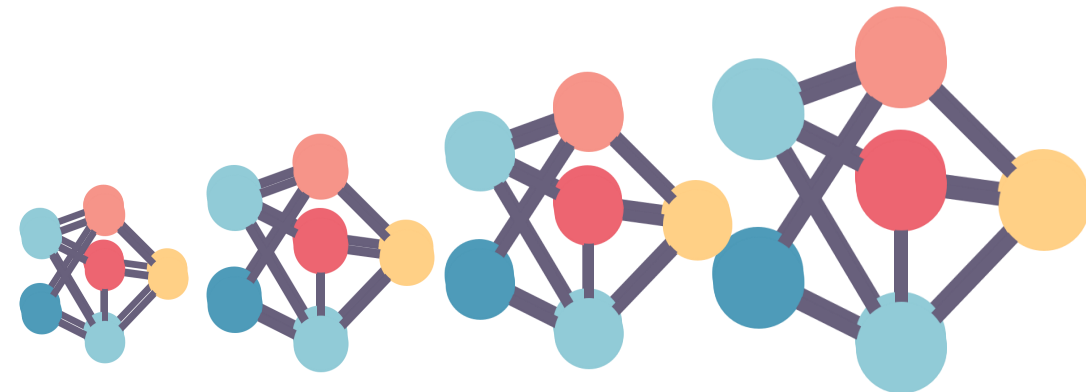


รูปที่ 2.11 การใช้งานเครือข่ายอินทราเน็ตในการปฏิบัติงานองค์กร

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

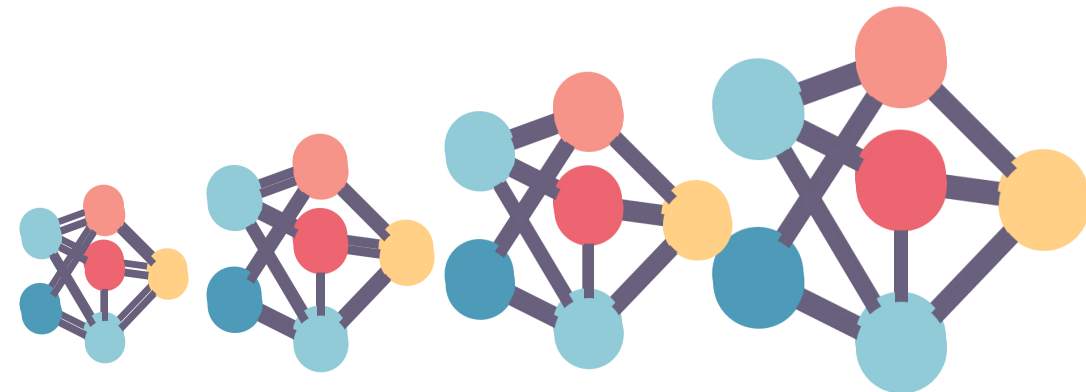
องค์กรอาจมีการเผยแพร่หน้าเว็บบนอินทราเน็ตเกี่ยวกับเหตุการณ์ภายใน นโยบายสุขภาพ และความมั่นคงปลอดภัย จดหมายข่าวสำหรับเจ้าหน้าที่ และไดเรกทอรีโทรศัพท์ของพนักงาน ตัวอย่างเช่น โรงเรียนอาจจะมีอินทราเน็ตที่มีข้อมูลเกี่ยวกับตารางเรียน หลักสูตรออนไลน์ และกระดานสนทนา อินทราเน็ตมักจะช่วยในการจัดการเอกสารกระดาษที่ไม่จำเป็นและเพิ่มความเร็วในการทำงาน พนักงานที่ทำงานนอกองค์กรอาจจะสามารถเข้าถึงอินทราเน็ตได้โดยใช้การเชื่อมต่อที่ปลอดภัยไปยังเครือข่ายภายในองค์กรโดยใช้วิธีการที่เรียกว่า VPN (Virtual Private Network)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

ส่วนเอกซ์ทราเน็ตนั้น องค์กรอาจจะใช้เพื่อเตรียมการเข้าถึงที่มีความมั่นคงปลอดภัยให้กับบุคคลที่ทำงานให้กับองค์กรอื่น แต่จำเป็นต้องใช้ข้อมูลขององค์กรของเรา ตัวอย่างของเอกซ์ทราเน็ต ได้แก่ บริษัทเตรียมการเข้าถึงเครือข่ายให้กับซัพพลายเออร์/ผู้รับเหมาภายนอก โรงพยาบาลเตรียมบริการระบบการจองให้กับแพทย์เพื่อที่แพทย์จะสามารถจัดการการนัดหมายสำหรับผู้ป่วยของตนเอง สำนักงานการศึกษาท้องถิ่นเตรียมงบประมาณและข้อมูลส่วนบุคคลให้กับโรงเรียนในเขตของพื้นที่ของตน



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

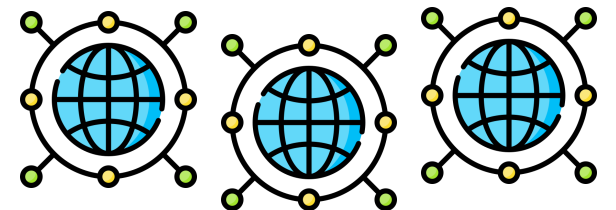
3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

3.3 การแบ่งโซนการทำงานของเครือข่าย (Zoning)

การใช้เครือข่ายในองค์กรต่าง ๆ มักมีการเชื่อมต่อกับระบบอินเทอร์เน็ต อินทราเน็ต ซึ่งอาจเกิดปัญหาในเรื่องของไวรัส และการถูกเจาะระบบหรือการแฮ็กเข้ามาในระบบโดยผู้ไม่ประสงค์ดี ดังนั้น เราจึงจำเป็นต้องมีการป้องกันโดยการจัดแบ่งระบบเครือข่ายออกเป็นโซน (Zone) เพื่อให้สามารถควบคุมและจัดการความมั่นคงปลอดภัยได้เหมาะสมยิ่งขึ้น โดยโซนนั้นแบ่งออกได้ 3 ประเภทหลัก ๆ ดังนี้

1. Internal Zone

ระบบเครือข่ายภายในองค์กร ซึ่งถือว่าเป็นโซนที่มีความมั่นคงปลอดภัยและน่าเชื่อถือสูงสุด อนุญาตให้เข้าถึงจากเครือข่ายภายในองค์กรเท่านั้น



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

2. External Zone

ระบบเครือข่ายภายนอก ซึ่งโดยส่วนใหญ่คืออินเทอร์เน็ต ซึ่งถือว่าเป็นโซนที่มีความมั่นคงปลอดภัยต่ำมากสำหรับองค์กร แต่เนื่องจากเราต้องมีการติดต่อกับเครือข่ายภายนอก จึงจำเป็นต้องมีการควบคุมการสื่อสารกับระบบเครือข่ายภายนอก เช่น คอมพิวเตอร์ ภายนอกองค์กร และเครือข่ายอินเทอร์เน็ตที่เราติดต่ออยู่ด้วย

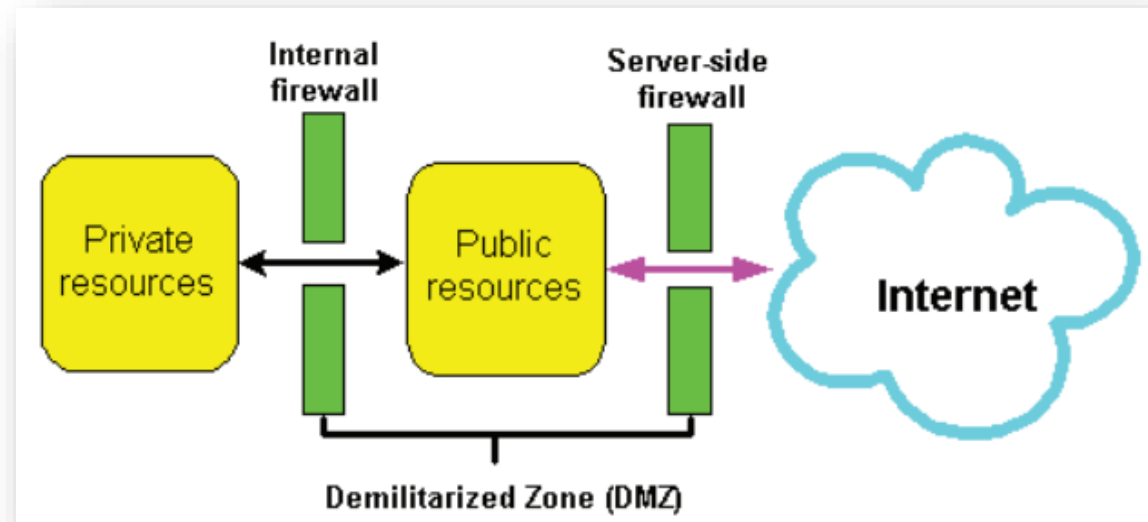
3. Demilitarized Zone (DMZ)

เป็นโซนที่องค์กรเตรียมการไว้สำหรับให้บริการกับผู้ให้บริการภายนอก และคนในองค์กรเองก็สามารถเข้าถึงโซนนี้ได้เช่นกัน ในโซนนี้มักจะมีอุปกรณ์จำพวกเซิร์ฟเวอร์ที่ให้บริการคนภายนอก เช่น เว็บเซิร์ฟเวอร์ อีเมล เซิร์ฟเวอร์ ผู้ดูแลระบบต้องดูแลความมั่นคงปลอดภัยโซนนี้อย่างระมัดระวังเพื่อไม่ให้เป็นจุดที่ใช้เข้าไปโจมตีเครือข่ายในองค์กรได้

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

3. อินเทอร์เน็ต (The Internet) อินทราเน็ต (Intranet) และเอกซ์ทราเน็ต (Extranet)

การป้องกันการเข้าถึงของแต่ละโซนมักมีอุปกรณ์รักษาความมั่นคงปลอดภัยในการป้องกันเครือข่ายด้วย เช่น ไฟร์วอลล์ (Firewall), IPS (Intrusion Prevention System) เป็นเทคโนโลยีที่ได้ออกแบบมาเพื่อให้ตรวจสอบการบุกรุก และแจ้งโจมตีตอบกลับหรือหยุดยั้งผู้บุกรุกได้ (ดูรายละเอียดไฟร์วอลล์ได้ในหน่วยการเรียนรู้ที่ 4)

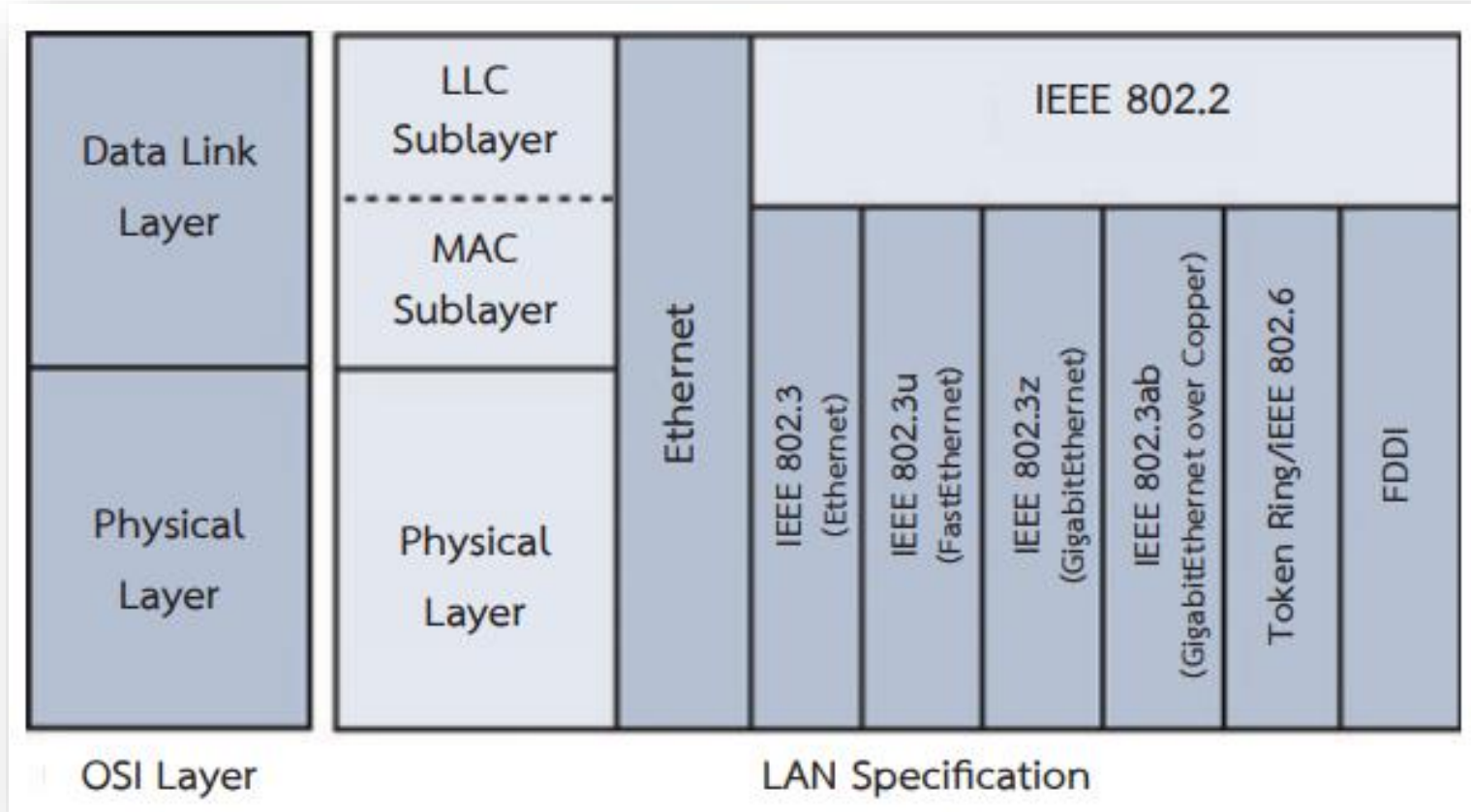


รูปที่ 2.12 ตัวอย่างการแบ่งโซนการทำงานของเครือข่าย

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN



รูปที่ 2.13 มาตรฐาน IEEE 802.2 และ IEEE 802.3

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์



4. มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

มาตรฐานของเครือข่ายคอมพิวเตอร์ถูกกำหนดโดยคณะกรรมการจากสถาบันวิศวกรรมไฟฟ้าและอิเล็กทรอนิกส์ (Institute of Electrical and Electronics Engineers : IEEE) หรือเรียกเป็นทางการคณะกรรมการมาตรฐาน LAN/MAN IEEE 802 (IEEE 802 LAN/MAN Standards Committee) โดยจะเน้นคุณสมบัติในระดับของอุปกรณ์การสื่อสารข้อมูล และการสื่อสารข้อมูลในเครือข่ายคอมพิวเตอร์ มาตรฐานจำนวนมากถูกกำหนดออกมาจากกลุ่มกรรมการกลุ่มนี้ และได้นำมาใช้กำหนดรูปแบบโครงสร้างระบบเครือข่ายปัจจุบัน โดยมาตรฐานที่สำคัญมีดังต่อไปนี้

- 📶 IEEE 802.1 (Higher Layer LAN Protocols) มาตรฐานด้านโพรโทคอลบนเครือข่ายท้องถิ่น (LAN)
- 📶 IEEE 802.2 (Logical Link Control) มาตรฐานด้านฟังก์ชันและโพรโทคอล LLC บนเครือข่ายท้องถิ่น

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4. มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

- 📶 IEEE 802.3 มาตรฐานกำหนดการสื่อสารข้อมูลในระดับฮาร์ดแวร์แบบ Carrier Sense Multiple Access with Collision Detect (CSMA/CD) ซึ่งเป็นการสื่อสารข้อมูลในระบบอีเทอร์เน็ต (Ethernet)
- 📶 IEEE 802.11 มาตรฐานเกี่ยวกับระบบเครือข่ายไร้สาย (Wireless LAN)
- 📶 IEEE 802.15 มาตรฐานสำหรับเครือข่ายไร้สายส่วนบุคคล (Wireless Personal Area Network: WPAN)
- 📶 IEEE 802.15.1 มาตรฐาน Bluetooth
- 📶 IEEE 802.15.3a มาตรฐาน Ultra Wide Band (UWB)
- 📶 IEEE 802.15.4 มาตรฐาน Zigbee

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4. มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

มาตรฐาน IEEE ที่มีการใช้กันอย่างแพร่หลายมากที่สุดในปัจจุบันในเครือข่ายแลน คือ อีเทอร์เน็ต (Ethernet) ที่ทำงานในดาตalinkเลเยอร์และฟิสิคัลเลเยอร์ ซึ่งเป็นตระกูลของเทคโนโลยีเครือข่ายที่กำหนดไว้ในมาตรฐาน IEEE 802.2 และ 802.3 โดยมาตรฐานอีเทอร์เน็ตจะรองรับแบนด์วิดท์ของข้อมูล เช่น

📶 10 Mb/s (Legacy Ethernet หรือ Classic Ethernet เป็น Ethernet แบบดั้งเดิม)

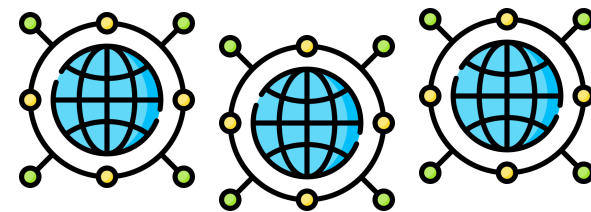
📶 100 Mb/s (Fast Ethernet)

📶 1,000 Mb/s (1 Gbps) (Gigabit Ethernet)

📶 10,000 Mb/s (10 Gbps)

📶 40,000 Mb/s (40 Gbps)

📶 100,000 Mb/s (100 Gbps) จนถึง 400,000 Mb/s (400 Gbps)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

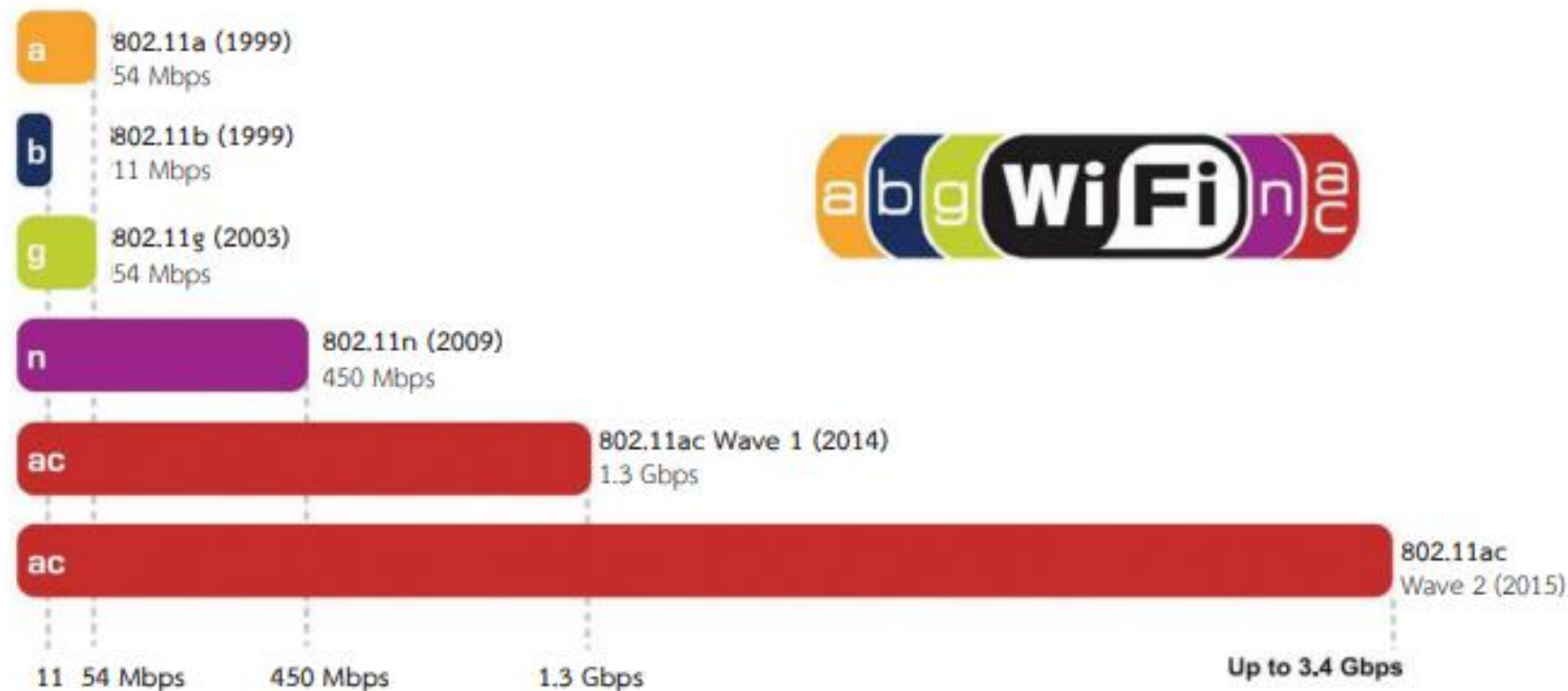


รูปที่ 2.14 วิวัฒนาการความเร็วของ IEEE 802.3

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN



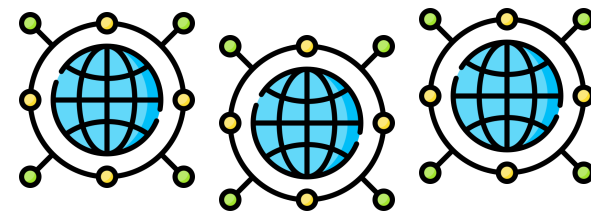
รูปที่ 2.15 วิวัฒนาการของ IEEE 802.11 ถึง IEEE 802.11ac Wave 2

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4. มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

ในขณะที่มาตรฐาน IEEE ที่เป็นที่ยอมรับและใช้งานอย่างแพร่หลายสำหรับเครือข่ายแลนไร้สายเป็นมาตรฐานที่อยู่ภายใต้ IEEE 802.11 ซึ่งเป็นมาตรฐานกลางในการทำงานของระบบเครือข่ายไร้สายกำหนดขึ้นโดย IEEE ที่ได้ถูกนำมาใช้เพื่อเชื่อมโยงอุปกรณ์เครือข่ายไร้สายเข้าด้วยกัน โดยมีการกำหนดมาตรฐานย่อยที่บ่งบอกความเร็วและความถี่ที่ใช้ในการสื่อสารข้อมูลตามลำดับดังนี้

1. เครือข่ายไร้สายที่ทำงานย่านความถี่ 5 GHz มีความเร็วในการรับส่งข้อมูล 54 Mbps โดยอัตราความเร็วในการรับส่งข้อมูลสามารถปรับระดับให้ช้าลงได้ เพื่อเพิ่มระยะทางการเชื่อมต่อให้มากขึ้น เช่น 54, 48, 36, 24 และ 11 Mbps เป็นต้น มีระยะการเชื่อมต่อในการกระจายสัญญาณของอุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point) อยู่ที่ 300 ฟุต ปัจจุบันแทบไม่มีอุปกรณ์ IEEE 802.11a ให้ใช้งานแล้ว



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

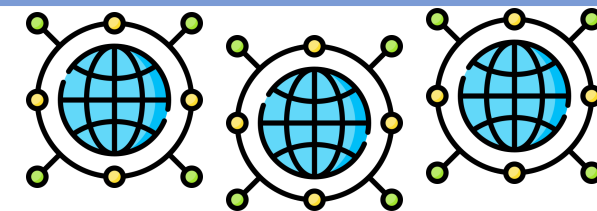
2. มาตรฐาน IEEE 802.11b

802.11b ใช้ความถี่ 2.4 GHz รับส่งข้อมูลด้วยความเร็ว 11 Mbps ขนาดของช่องสัญญาณกว้าง 22 MHz มาตรฐานนี้มีระบบเข้ารหัสข้อมูลแบบ WEP (Wired Equivalent Privacy) ที่ 128 บิต ในปัจจุบันแทบไม่มีอุปกรณ์ IEEE 802.11b ให้ใช้งานแล้ว

3. มาตรฐาน IEEE 802.11g

มาตรฐาน 802.11g ใช้ความถี่ 2.4 GHz ขนาดของช่องสัญญาณกว้าง 20 MHz รับส่งข้อมูลด้วยความเร็ว 36-54 Mbps ซึ่งเป็นความเร็วที่สูงกว่ามาตรฐาน 802.11b โดยมาตรฐาน 802.11g สามารถปรับระดับความเร็วในการสื่อสารลงเหลือ 2 Mbps ได้ (ตามสภาพแวดล้อมของเครือข่ายที่ใช้งาน) มาตรฐานนี้เป็นที่นิยมของผู้ใช้เป็นจำนวนมากและเข้ามาแทนที่ 802.11b ที่ความเร็วต่ำกว่า ในปัจจุบันแทบไม่มีอุปกรณ์ IEEE 802.11g ให้ใช้งานแล้ว

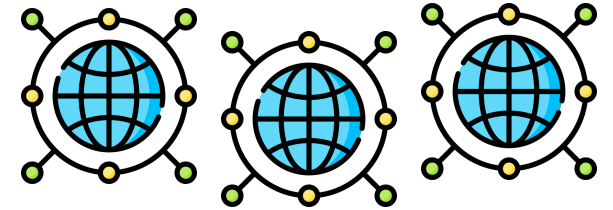
การสื่อสาร 802.11 a/b/g แบบเดิมนี้อาศัยเสาอากาศในการรับส่งเพียงแค่ 1 ต้น และฝั่งรับก็เช่นกัน จึงเรียกวิธีการแบบนี้ว่า SISO (Single Input Single Output)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN



4. มาตรฐาน IEEE 802.11n

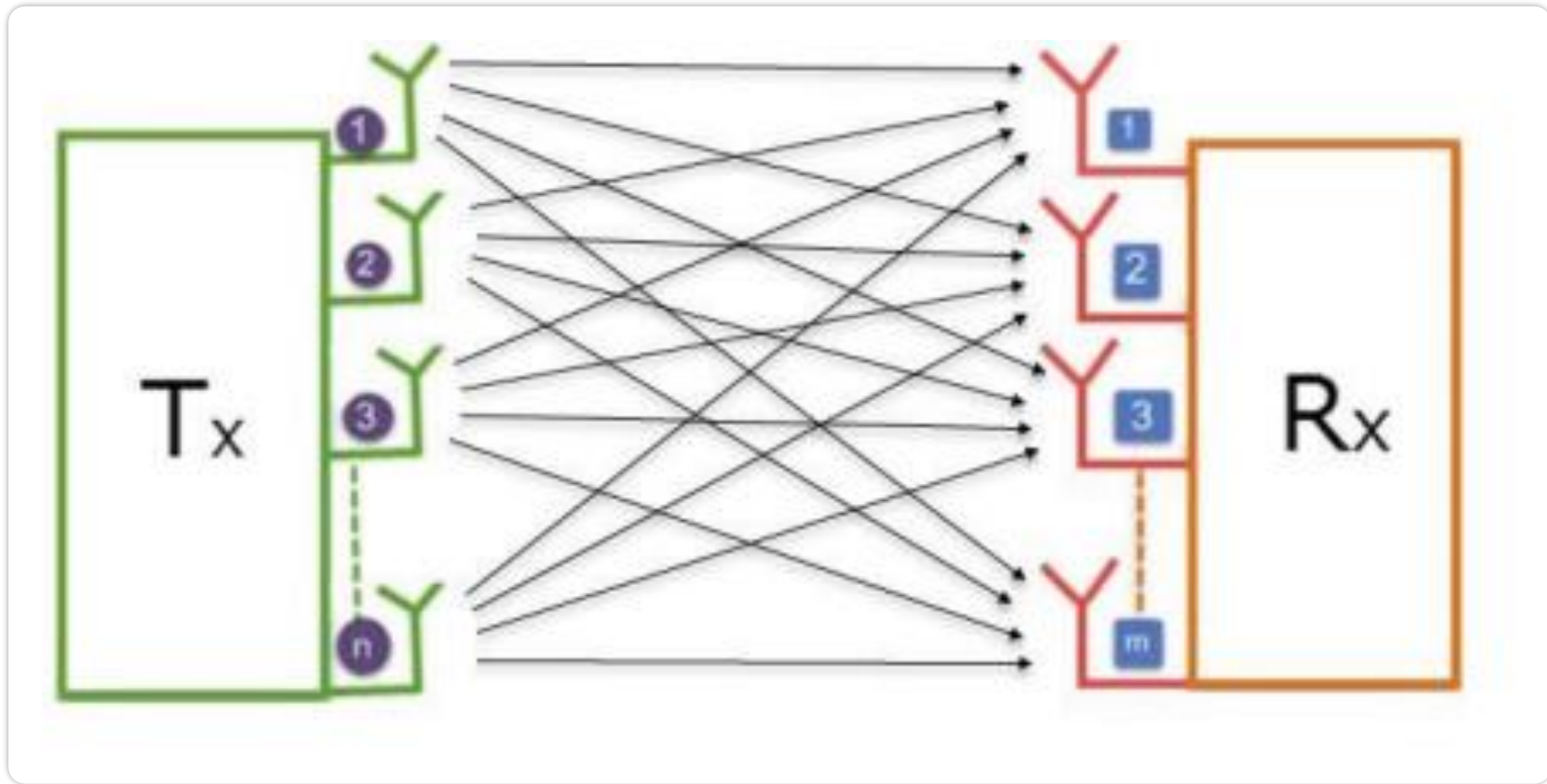
หรือเรียกว่ามาตรฐาน Wi-Fi4 ถือว่าเป็นมาตรฐานขั้นต่ำที่ใช้งานกันในปัจจุบัน มาตรฐานทำงานบนคลื่นความถี่ 2.4 และ 5 GHz และสามารถเลือกใช้ขนาดของช่องสัญญาณกว้าง 20 MHz หรือกว้างกว่าเดิมที่ 40 MHz รองรับความเร็วตั้งแต่ 300-600 Mbps มีเสาสัญญาณตั้งแต่ 2-4 เสา บนตัวอุปกรณ์กระจายสัญญาณไร้สาย หากผู้ใช้ต้องการใช้งานที่ความเร็วสูงสุด ผู้ใช้จำเป็นต้องมีเครื่องคอมพิวเตอร์พกพาหรืออุปกรณ์เคลื่อนที่ที่ต้องรองรับมาตรฐาน 802.11n ด้วยเช่นกัน และมาตรฐาน 802.11n สามารถทำงานร่วมกับ 802.11b/g ได้

ใน 802.11n มีการใช้ MIMO (Multiple-Input and Multiple-Output) ทำให้ Access Point มีเสาอากาศหลายต้นเพื่อส่งสัญญาณพร้อมกันหลายคลื่น และเครื่องรับก็รับพร้อมกันหลายคลื่น จึงส่งข้อมูลได้เร็วขึ้น เช่น ถ้าใช้ Access Point ที่รองรับการส่งสัญญาณ 4 สตรีม และใช้อุปกรณ์ที่รองรับ 4x4 ด้วย ความเร็วที่ได้จะสูงสุดตามที่เราเตอร์ให้บริการได้ แต่ส่วนมากอุปกรณ์สมาร์ทโฟนมักจะเป็นแบบ 1x1 เพราะพื้นที่ในเครื่องมีน้อย

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

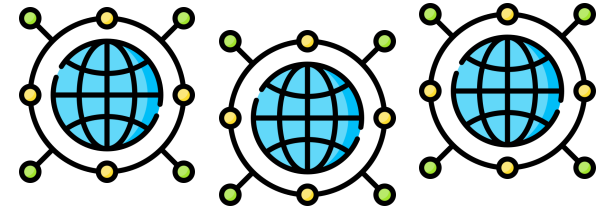


รูปที่ 2.16 ระบบ MIMO (Multiple-Input and Multiple-Output)

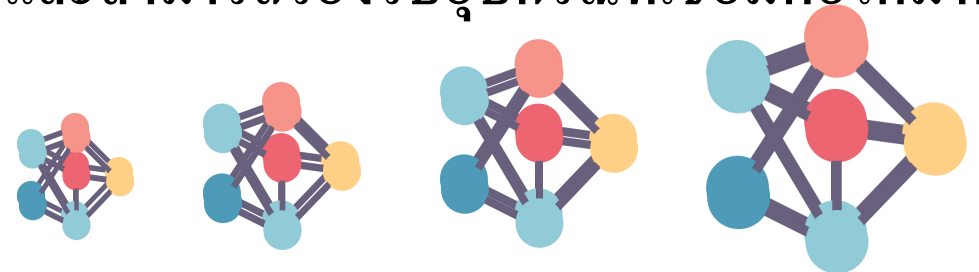
องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN



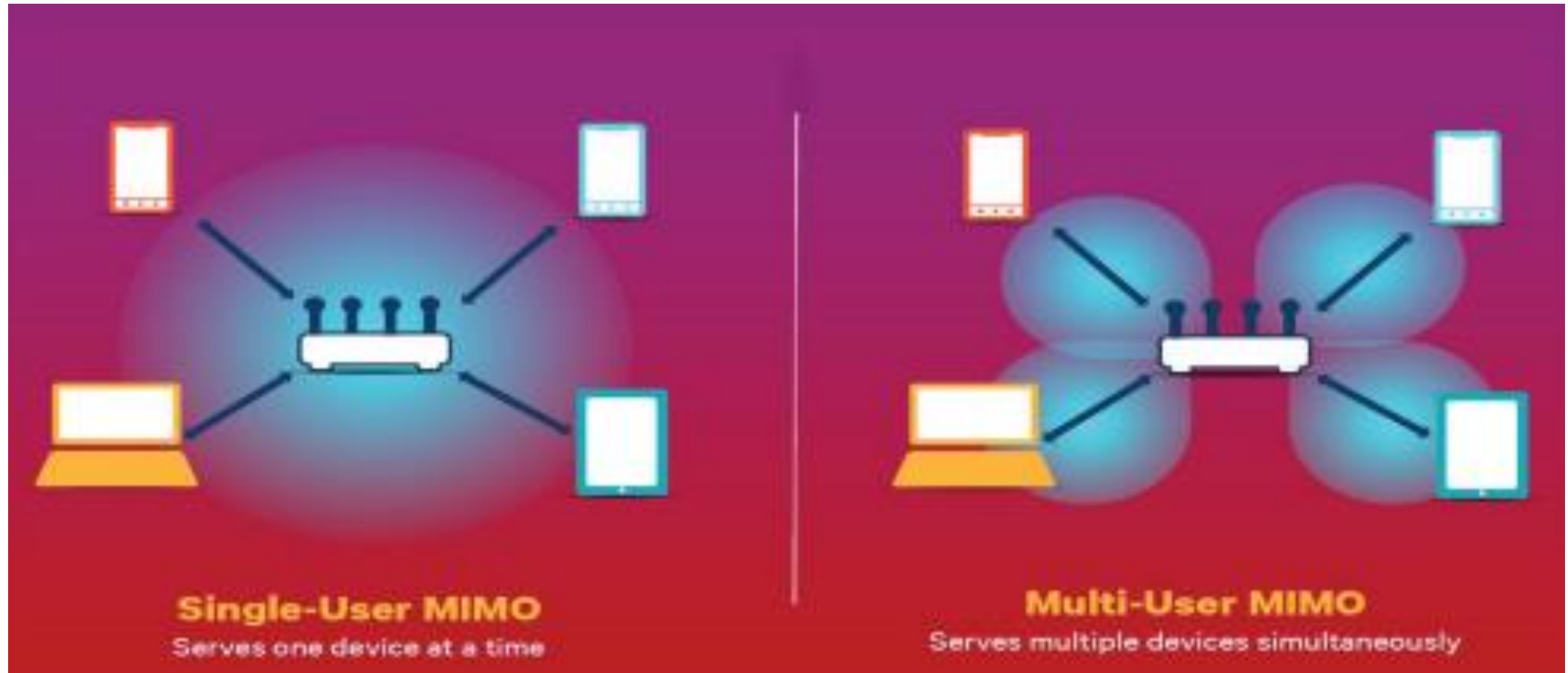
ในส่วนการทำงานของอุปกรณ์ Access Point เทคโนโลยีที่มีการใช้งานในการรับส่งสัญญาณกันส่วนใหญ่ มักเป็นแบบ Single-User MIMO หรือ SU-MIMO (Single-User Multiple-Input and Multiple-Output) คือ ในช่วงเวลาหนึ่ง Access Point จะสามารถรับ-ส่งข้อมูลกับอุปกรณ์ได้แค่ 1 ตัวเท่านั้น ดังนั้น เมื่อมีการเชื่อมต่อ อุปกรณ์หลายตัว Access Point จะส่งสัญญาณสลับไปสลับมาอย่างรวดเร็ว แต่ไม่ใช่ส่งพร้อมกันทุกอุปกรณ์ ส่งผลให้ เมื่อมีอุปกรณ์มาก Access Point จะสลับการสนทนากับทุกอุปกรณ์ไม่ทัน ส่งผลทำให้การสื่อสารไม่ราบรื่นหรือเรียกอาการนี้ตลึงสะกด แต่ Access Point รุ่นใหม่ทีรองรับการทำงานแบบ Multi-User MIMO หรือ MU-MIMO (Multi-User, Multi-Input and Multi-Output) สามารถรองรับจำนวนผู้ใช้งาน รับส่งข้อมูลกับหลาย ๆ อุปกรณ์พร้อมกัน ช่วยทำให้รับส่งข้อมูลได้เร็วขึ้น และสามารถรองรับอุปกรณ์ที่เชื่อมต่อได้มากกว่าเดิมด้วย



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

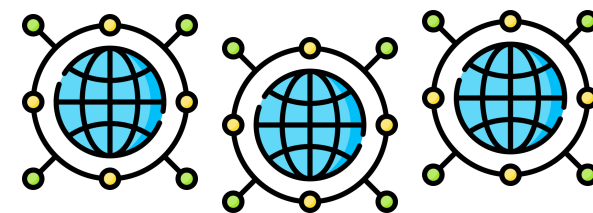


รูปที่ 2.17 เปรียบเทียบการทำงานระหว่าง Single-User MIMO และ Multi-User MIMO

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN



5. มาตรฐาน IEEE 802.11ac

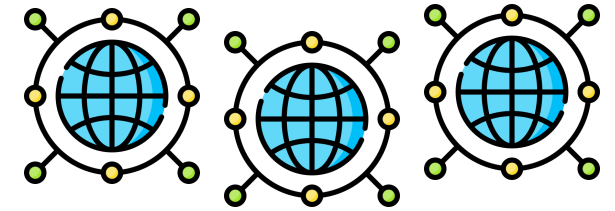
หรือเรียกว่ามาตรฐาน Wi-Fi5 หรือ Gigabit Wi-Fi ใช้ความถี่ 5 GHz แต่ปรับปรุงให้มีขนาดของช่องสัญญาณเพิ่มขึ้นจากเดิมที่มาตรฐาน 802.11n มีช่องสัญญาณ 40 MHz ให้ขยายเป็น 80-160 MHz ทำให้สามารถรับส่งข้อมูลได้ด้วยความเร็วสูงกว่าเดิม IEEE 802.11ac แบ่งออกเป็น 802.11ac Wave 1 และ 802.11ac Wave 2

โดย 802.11ac Wave 1 เป็นมาตรฐานของระบบเครือข่ายไร้สายใหม่ที่คาดว่าจะมาแทนที่มาตรฐาน IEEE 802.11n โดยใช้การมอดูเลตสัญญาณแบบใหม่ ปรับอัลกอริทึมให้ดีขึ้น ปรับช่องสัญญาณให้มีขนาด 80 MHz แทนของเดิมที่ขนาด 40 MHz ใน 802.11n ส่งผลให้มีอัตราการรับส่งข้อมูลสูงถึง 433 Mbps นอกจากนี้ 802.11ac Wave 1 ยังรองรับการรับส่งข้อมูลพร้อมกันถึง 4 ชุด (4 Spatial Streams) จึงทำความเร็วสูงสุดได้ถึง 1.73 Gbps

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN



มาตรฐาน 802.11n และ 802.11ac Wave 1 มีข้อจำกัดทางเทคโนโลยีที่เรียกว่า SU-MIMO 802.11ac Wave 2 ถูกออกแบบมาเพื่อแก้ไขเทคโนโลยี SU-MIMO โดยรองรับการใช้งานแบบ MU-MIMO (Multi-User Multiple-Input Multiple-Output) ทำให้ Access Point สามารถสื่อสารกับอุปกรณ์ได้หลายตัวพร้อมกัน ซึ่งทำให้รับส่งข้อมูลได้เร็วขึ้น ยังทำให้ Access Point สามารถรองรับอุปกรณ์ที่เชื่อมต่อได้มากกว่าเดิม เสมือนมีหลาย Access Point ในเครื่องเดียว

นอกจากนี้ 802.11ac Wave 2 จะทำการขยายช่องสัญญาณจาก Wave 1 คือ 80 MHz เป็น 160 MHz และเพิ่มอัตราการรับส่งข้อมูลพร้อมกันจากเดิม 4 ชุด เป็น 8 ชุด (8 Spatial Streams) ซึ่งเมื่อใช้ 2 ปัจจัยนี้เข้าด้วยกันและเพิ่มประสิทธิภาพของการทำ Beamforming¹ และเทคนิคเพิ่มเติม คาดว่ามาตรฐาน 802.11ac Wave 2 จะทำความเร็วสูงสุดที่ประมาณ 7-10 Gbps

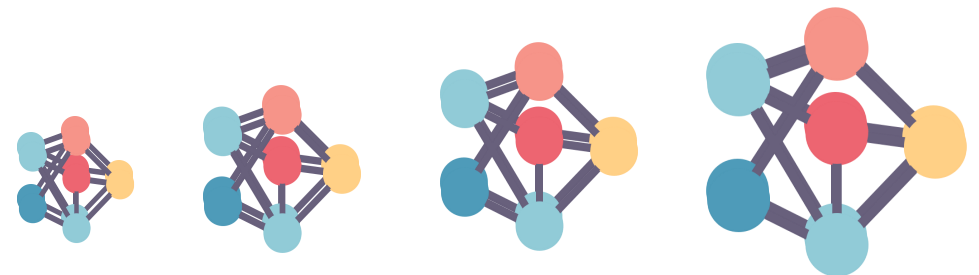
องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

4.

มาตรฐาน IEEE 802 สำหรับเครือข่าย LAN/MAN

6. มาตรฐาน IEEE 802.11ax

หรือเรียกว่ามาตรฐาน Wi-Fi6 เป็นมาตรฐานที่กำลังเริ่มได้รับความนิยม เนื่องจากการปรับปรุงต่อยอดจาก 802.11ac เดิม โดยทำงานที่ความถี่ 2.4 และ 5 GHz และรับส่งข้อมูลได้เร็วถึง 4.8 Gbps และอาจจะเร็วกว่า 4 เท่าเมื่อเทียบกับ IEEE 802.11ac โดยมีช่องสัญญาณที่กว้างถึง 160 MHz ด้วย 8x8 MU-MIMO ส่งผลให้สามารถรองรับการใช้งานพร้อมกันได้หลายอุปกรณ์ดีกว่าเดิม



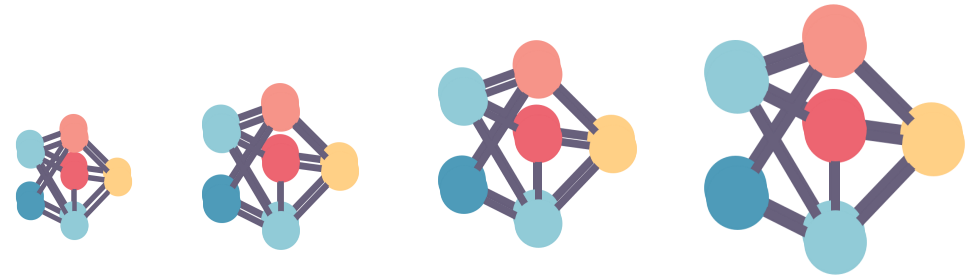
องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

5. รูปแบบการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ (Type of connection)

คือ วิธีการที่อุปกรณ์ตั้งแต่ 2 อุปกรณ์เชื่อมต่อกันด้วยสื่อส่งข้อมูล (Transmission Link) 1 สื่อ โดยสื่อส่งข้อมูลเป็นลักษณะทางกายภาพ (Physical) อาจเป็นแบบสายหรือแบบไร้สายก็ได้ สื่อส่งข้อมูลทำหน้าที่เป็นเส้นทางให้ข้อมูลข่าวสารเดินทางจากอุปกรณ์หนึ่งไปอีกอุปกรณ์หนึ่ง หรือไปยังอุปกรณ์หลาย ๆ ตัวได้ สื่อส่งข้อมูล ได้แก่ สายทองแดง สายใยแก้วนำแสง คลื่นแม่เหล็กไฟฟ้า (Wi-Fi, Bluetooth) เป็นต้น รูปแบบการติดตั้งสายมี 2 แบบ ได้แก่

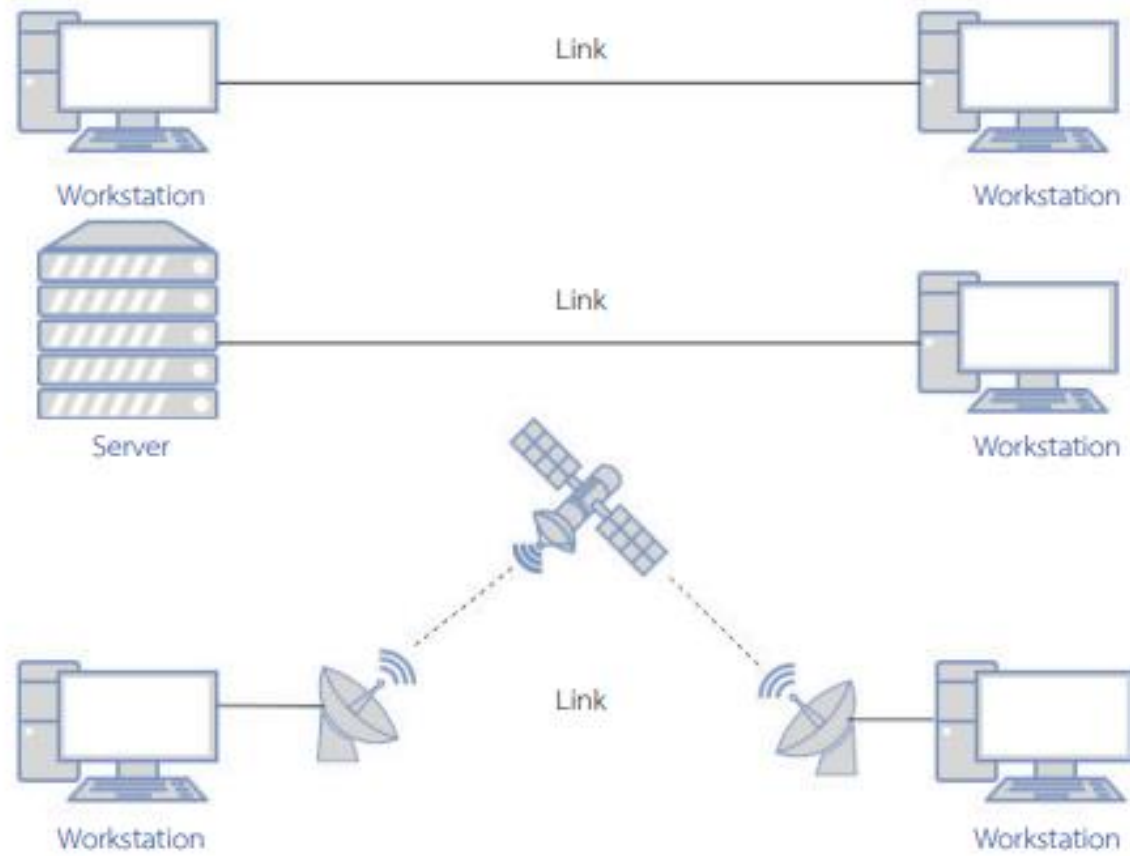
5.1 แบบจุดต่อจุด (point-to-point)

คือ วิธีเชื่อมต่อสื่อส่งข้อมูลระหว่างอุปกรณ์ 2 อุปกรณ์ โดยมีเส้นทางเพียง 1 เส้นทางนั้น เช่น ลักษณะการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์พีซีแต่ละเครื่องมีเพียงสาย 1 สายต่อเชื่อมโยงกันในการทำงาน การเชื่อมระหว่างคอมพิวเตอร์กับสมาร์ทโฟน หรือแท็บเล็ต เพื่อซิงค์ข้อมูลก็เป็นแบบจุดต่อจุดเช่นกัน



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

5. รูปแบบการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ (Type of connection)



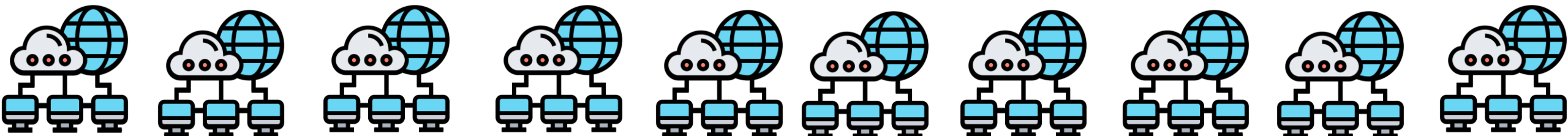
รูปที่ 2.18 ภาพเครือข่ายแบบ Point-to-Point

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

5. รูปแบบการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ (Type of connection)

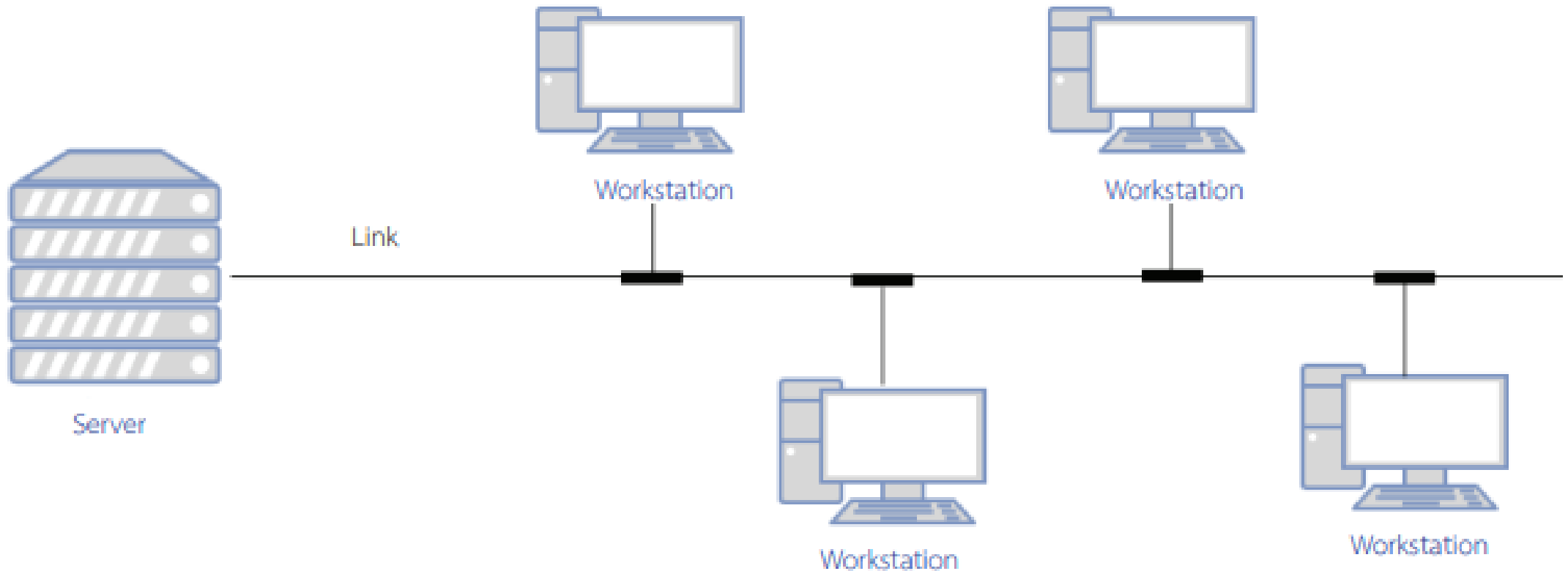
5.2 แบบหลายจุดหรือมัลติพอยต์ (Multipoint)

เรียกอีกอย่างว่า Multidrop line หมายถึง สื่อส่งข้อมูล 1 สื่อมีการเชื่อมต่อไปยังอุปกรณ์หลาย ๆ อุปกรณ์โดยใช้สื่อส่งข้อมูลเดียวกัน ถ้าสื่อส่งข้อมูลเป็นคลื่นวิทยุ เช่น การกระจายข้อมูลของ Access Point ผ่าน Wi-Fi สามารถทำได้โดยแบ่งความถี่ออกเป็นช่วงความถี่ของอุปกรณ์แต่ละตัว ซึ่งถือว่าเป็นการใช้สื่อส่งข้อมูลร่วมกันในแบบแบ่งส่วนที่เรียกว่า การแบ่งเป็นส่วน (Spatially Share) หรืออาจผลักดันกันใช้สื่อส่งข้อมูลโดยกำหนดระยะเวลาการใช้ที่เรียกว่า การแบ่งปันเวลา (Time Share)



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

5. รูปแบบการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ (Type of connection)



รูปที่ 2.19 ภาพการเชื่อมต่อแบบหลายจุดหรือมัลติพอยต์ (multipoint)

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

6. ความมั่นคงปลอดภัยการใช้งานเครือข่ายในการปฏิบัติงานขององค์กร

ในการใช้งานคอมพิวเตอร์ ไม่ว่าจะเป็นการใช้งานส่วนบุคคลหรือใช้งานกับระบบของหน่วยงาน ทั้งอุปกรณ์ขนาดใหญ่ เช่น คอมพิวเตอร์ หรืออุปกรณ์ส่วนบุคคล เช่น โทรศัพท์มือถือ เรื่องหนึ่งที่มีความสำคัญเป็นอย่างยิ่ง คือ การรักษาความมั่นคงปลอดภัยของข้อมูลและระบบไม่ให้เกิดความเสียหาย ทั้งด้วยความไม่ตั้งใจ หรือโดยเจตนาของผู้ไม่หวังดี เพราะปัจจุบันระบบคอมพิวเตอร์และเครือข่ายเป็นหัวใจหลักในการปฏิบัติงานของแทบจะทุกหน่วยงาน หากเกิดปัญหาขึ้นกับระบบเครือข่ายหรือระบบคอมพิวเตอร์จะส่งผลกระทบต่อ การปฏิบัติงานจนอาจส่งผลให้เกิดความเสียหายตามมาอีกมาก เนื่องจากมูลค่าของระบบเครือข่ายคอมพิวเตอร์ที่แท้จริงไม่ได้อยู่ที่ราคาอุปกรณ์ แต่มาจากข้อมูลและกระบวนการทำงานที่ก่อให้เกิดประโยชน์แก่องค์กร เช่น ข้อมูลบัญชีลูกหนี้ ข้อมูลสต็อกสินค้า หรือระบบการขายสินค้าที่ไม่สามารถทำงานได้เนื่องจากระบบสื่อสารขัดข้อง หากเสียหายไปจะส่งผลต่อการดำเนินงานขององค์กรในทันที



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

6. ความมั่นคงปลอดภัยการใช้งานเครือข่ายในการปฏิบัติงานขององค์กร

6.1 ความเสียหายทางกายภาพ

หมายถึง ความเสียหายที่เกิดขึ้นกับตัวอุปกรณ์ คอมพิวเตอร์ ฮับ สวิตช์ สายนำสัญญาณ ทำให้ระบบเสียหายไม่สามารถทำงานได้ ซึ่งความเสียหายอาจจะเกิดจากความตั้งใจและไม่ตั้งใจ โดยสามารถป้องกันความเสียหายทางกายภาพได้ในหลายระดับ ได้แก่

- 1) จัดให้มีระบบรักษาความมั่นคงปลอดภัยในพื้นที่จัดเก็บอุปกรณ์สำคัญ เช่น Server, Switch โดยมีการล็อกไม่ให้ผู้ไม่มีส่วนเกี่ยวข้องเข้าถึงได้
- 2) จัดสภาพแวดล้อมที่เหมาะสมกับการทำงานของอุปกรณ์ เช่น การติดตั้งระบบปรับอากาศ ระบบไฟฟ้าสำรองสำหรับอุปกรณ์เครือข่ายที่สำคัญและติดตั้งสายดินให้อุปกรณ์ทุกครั้ง
- 3) กำหนดและออกแบบเส้นทางการเดินสายสัญญาณให้เหมาะสม เช่น การร้อยท่อเก็บสาย การใส่สายในราง เลือกประเภทสายที่เหมาะสม

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

6. ความมั่นคงปลอดภัยการใช้งานเครือข่ายในการปฏิบัติงานขององค์กร

4) กรณีที่ระบบมีความสำคัญสูงอาจต้องติดตั้งระบบสำรองที่อยู่คนละพื้นที่กับไซต์หลักหรือแม้กระทั่งการทำไซต์สำรองเพื่อให้สามารถทำงานแทนกันได้ทันทีในกรณีที่เกิดเหตุไม่คาดคิด เช่น การจารกรรม จลาจล เพลิงไหม้ น้ำท่วม เป็นต้น

5) ติดตั้งสัญลักษณ์หรือเครื่องหมายบนอุปกรณ์ จุดเชื่อมต่อและสายสัญญาณต่าง ๆ เพื่อป้องกันความผิดพลาดในการเชื่อมต่อหรือใช้งาน

6) จัดทำคู่มือผู้ดูแลระบบและผู้ใช้งานให้ถูกต้องตรงตามข้อเท็จจริงเสมอ



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

6.

ความมั่นคงปลอดภัยการใช้งานเครือข่ายในการปฏิบัติงานขององค์กร

6.2 ความเสียหายของข้อมูล

ความเสียหายที่เกิดขึ้นกับโปรแกรมหรือข้อมูลโดยสาเหตุอาจจะเกิดจากไวรัสคอมพิวเตอร์การแฮ็กข้อมูล ซึ่งความเสียหายของข้อมูลนี้อาจมีมูลค่าสูงและส่งผลกระทบมากกว่าความเสียหายทางกายภาพ เพราะหากเกิดขึ้นแล้ว การแก้ไขหรือกู้ข้อมูลจะทำได้ยุ่งยากกว่าหรืออาจจะทำไม่ได้ ดังนั้นในหน่วยงานที่มีระบบเครือข่ายคอมพิวเตอร์ต้องกำหนดมาตรการป้องกันหรือรักษาความปลอดภัยที่เหมาะสม เช่น

1) การกำหนดรหัสผ่านเข้าระบบที่เหมาะสม ทั้งการเข้าใช้ Wi-Fi และรหัสผ่านผู้ใช้ที่เข้าใช้ระบบให้ได้มาตรฐาน ซึ่งการกำหนดรหัสผ่านที่ดีต้องมีความยาวมากกว่า 8 ตัวอักษร ยิงยาวยิ่งดี คาดเดายาก มีการผสมตัวอักษรพิเศษและไม่ควรเป็นข้อมูลพื้นฐาน เช่น วันเดือนปีเกิด เบอร์โทรศัพท์ตนเอง เป็นต้น

2) กำหนดสิทธิการใช้งานของผู้ใช้ (User) ให้เหมาะสมกับการทำงานแต่ละคน



องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

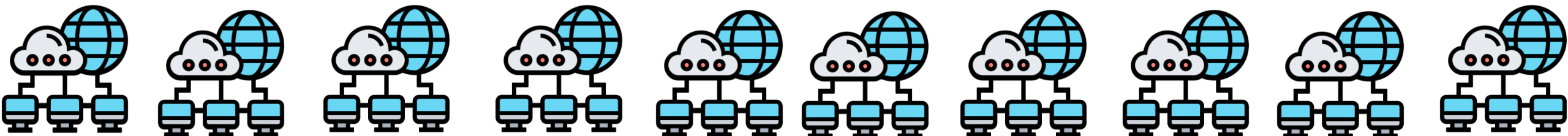
6. ความมั่นคงปลอดภัยการใช้งานเครือข่ายในการปฏิบัติงานขององค์กร

- 3) ตรวจสอบสื่อและอุปกรณ์ที่นำมาต่อเข้ากับระบบเครือข่าย เช่น คอมพิวเตอร์ ยูเอสบีไดรฟ์ ว่าปลอดภัยไม่มีไวรัสก่อนนำเข้ามาต่อกับระบบเครือข่าย
- 4) ติดตั้งไฟร์วอลล์และกำหนดมาตรการป้องกันการแฮ็กจากทั้งภายในและภายนอกองค์กร
- 5) ติดตั้งโปรแกรมแอนติไวรัสและอัปเดตโปรแกรมอย่างสม่ำเสมอ
- 6) มีระบบสำรองข้อมูลในหลายระดับ เช่น การสำรองข้อมูลรายวัน การสำรองข้อมูลรายสัปดาห์โดยสื่อที่ใช้สำรองข้อมูลควรจะถูกเก็บแยกออกจากระบบเครือข่าย เพื่อป้องกันการถูกทำลายโดยไวรัสที่ส่งผ่านเครือข่าย
- 7) กำหนดระเบียบการรักษาความมั่นคงปลอดภัยให้รัดกุมและบังคับใช้อย่างเคร่งครัด เช่น การห้ามนำสื่อหรือเครื่องคอมพิวเตอร์ที่ไม่ได้รับอนุญาตมาต่อกับระบบ
- 8) มีการฝึกอบรมและให้ความรู้เรื่องมาตรการรักษาความมั่นคงปลอดภัยข้อมูลแก่ผู้ใช้อย่างสม่ำเสมอ

องค์ประกอบของระบบเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

การทำให้อุปกรณ์คอมพิวเตอร์สื่อสารและทำงานร่วมกันเป็นเครือข่ายคอมพิวเตอร์ สามารถทำได้หลายวิธี หลายรูปแบบ ผู้ออกแบบระบบเครือข่ายต้องเข้าใจถึงรูปแบบการเชื่อมต่อ ประเภทของระบบเครือข่ายคอมพิวเตอร์ตามพื้นที่ครอบคลุม มาตรฐานต่าง ๆ ที่เกี่ยวข้อง เช่น IEEE 802 สำหรับเครือข่าย LAN/MAN รูปแบบการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ และการรักษาความมั่นคงปลอดภัยการใช้งานเครือข่ายในการปฏิบัติงานขององค์กร ซึ่งสิ่งเหล่านี้เป็นจุดเริ่มต้นที่ดีในการกำหนดแนวทางในการนำระบบเครือข่ายคอมพิวเตอร์ที่เหมาะสมมาใช้ในองค์กร





สื่อกลางเครือข่าย คอมพิวเตอร์



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

1.1 สายคู่บิดเกลียว (Twisted pair)

ประกอบด้วยเส้นลวดทองแดงที่หุ้มด้วยฉนวนพลาสติก 2 เส้นพันบิดเป็นเกลียว เพื่อลดการรบกวนจากคลื่นแม่เหล็กไฟฟ้าจากคู่สายข้างเคียงภายในเคเบิลเดียวกันที่เรียกว่าครอสทอล์ก (Crosstalk) หรือจากภายนอก

ครอสทอล์ก (Crosstalk) หมายถึง สัญญาณหนึ่งบนสายหนึ่งรบกวนสัญญาณบนอีกสายหนึ่ง สายคู่บิดเกลียวถูกออกแบบมาเพื่อลดปัญหานี้ โดยการบิดคู่สายเป็นเกลียว ทำให้สัญญาณรบกวนในแต่ละสายหักล้างกันเอง ถ้าจำนวนเกลียวต่อหน่วยความยาวยิ่งมาก จะป้องกันครอสทอล์กได้ดีขึ้น แต่จะทำให้ความยาวของสายที่ต้องใช้งานเพิ่มขึ้น



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

อัตราการส่งข้อมูลผ่านสายคู่บิดเกลียวจะขึ้นอยู่กับความหนาของสาย คือ สายทองแดงที่มีเส้นผ่านศูนย์กลางกว้าง จะสามารถส่งสัญญาณไฟฟ้ากำลังแรงได้ ทำให้สามารถส่งข้อมูลด้วยอัตราสูงโดยทั่วไปสำหรับการส่งข้อมูลแบบดิจิทัล สัญญาณที่ส่งเป็นลักษณะคลื่นสี่เหลี่ยม สายคู่บิดเกลียวสามารถใช้ส่งข้อมูลได้ถึงร้อยเมกะบิตต่อวินาที (Megabits per second : Mbps) ในระยะทางไม่เกินร้อยเมตร เนื่องจากสายคู่บิดเกลียวมีราคาไม่แพงมาก ติดตั้งใช้งานง่าย ใช้ส่งข้อมูลได้ดี จึงมีการใช้งานอย่างกว้างขวาง



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

1.1.1 สายคู่บิดเกลียวชนิดหุ้มฉนวน (Shielded Twisted Pair : STP)

เป็นสายทองแดงคู่บิดเกลียว (Twisted Pair) ที่หุ้มด้วยฟอยล์ (Foil Shields) และหุ้มทั้ง 4 คู่สายทั้งหมดด้วยลวดถักหรือฟอยล์ชั้นนอก (Braided or Foil Shield) ที่หนาอีกชั้น เพื่อป้องกันการรบกวนของคลื่นแม่เหล็กไฟฟ้า และมีปลอกนอก (Jacket) หุ้มอีกชั้น

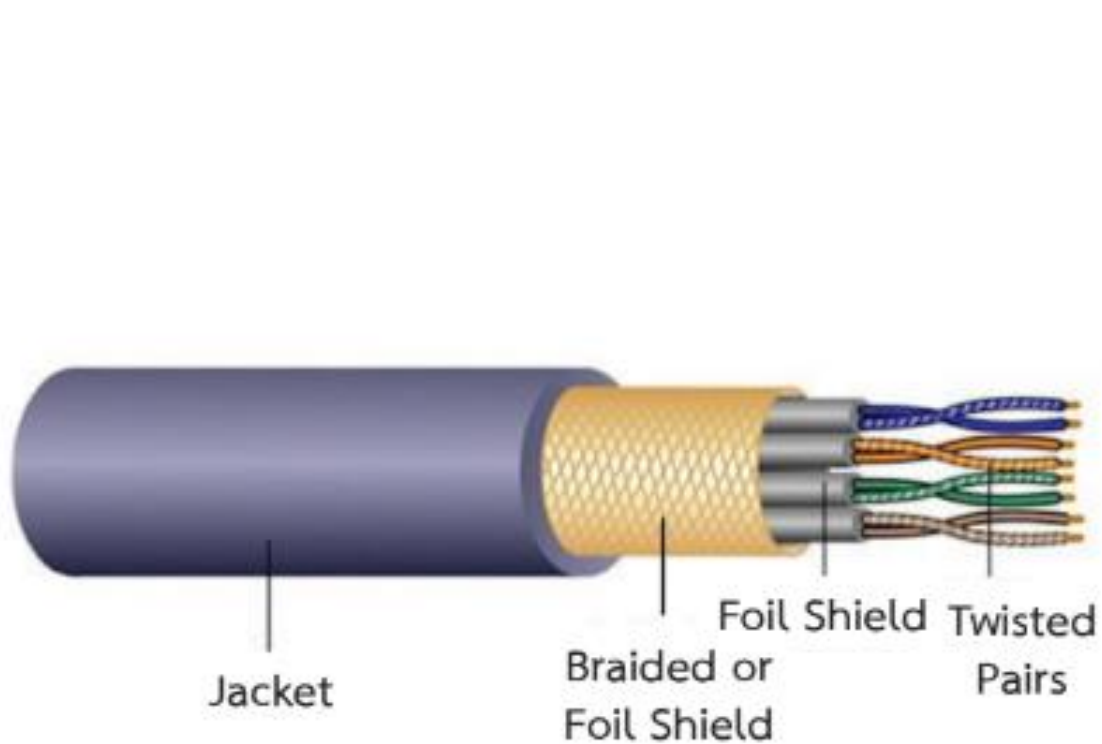
สาย STP เหมาะสำหรับการเชื่อมต่อกับระบบรักษาความมั่นคงปลอดภัย (Security) ระบบกล้องโทรทัศน์วงจรปิด (CCTV) ระบบเคเบิลทีวี (CATV) ทีวีรวม (TV MATV) และระบบควบคุมการเข้าถึง (Access Control System)



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



รูปที่ 3.1 สายคู่บิดเกลียวชนิดหุ้มฉนวน (Shielded Twisted Pair : STP)

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

1.1.2 สายคู่บิดเกลียวชนิดไม่หุ้มฉนวน (Unshielded Twisted Pair : UTP)

เป็นสายคู่บิดเกลียวมีฉนวนชั้นนอกที่บางอีกชั้นสำหรับสายทั้ง 8 เส้น ทำให้สะดวกในการโค้งงอ แต่สามารถป้องกันการรบกวนของคลื่นแม่เหล็กไฟฟ้าได้น้อยกว่าสายคู่บิดเกลียวชนิดหุ้มฉนวน แต่มีราคาต่ำกว่า จึงนิยมใช้ในการเชื่อมต่ออุปกรณ์ในเครือข่าย ตัวอย่างของสายคู่บิดเกลียวชนิดไม่หุ้มฉนวนที่เห็นในชีวิตประจำวัน คือ สายโทรศัพท์ที่ใช้ในบ้าน และสายแลนที่มี 8 เส้นที่เรียกตามหมวดหรือ CAT (Category) ซึ่งจะถูกแบ่งออกตามมาตรฐาน ANSI/TIA-568-C.2 แต่ละ Category นั้นจะต่างกันที่ระยะของสายและความสามารถที่รองรับความถี่ในการส่งสัญญาณ หรือเรียกว่า ความเร็วในการส่งสัญญาณ โดยมีหน่วยวัดเป็น MHz โดยปัจจุบันนิยมใช้ตั้งแต่ CAT5e ขึ้นไป



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย



รูปที่ 3.2 สายคู่บิดเกลียวชนิดไม่หุ้มฉนวน (Unshielded Twisted Pair: UTP)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

โครงสร้างของสายแลนพิจารณาจากตัวป้องกันสัญญาณรบกวน หากสายไม่มีตัวป้องกันสัญญาณรบกวนที่ดี จะทำให้ความเร็วตกและเดินสายได้ระยะทางสั้นลง ปกติแล้วสายแลนที่ได้มาตรฐาน ISO/IEC 11801 ed2.2 Annex E จะมีการตีเกลียวของสายแต่ละคู่เพื่อป้องกันสัญญาณรบกวนระดับหนึ่งอยู่แล้วซึ่งเรียกสายประเภทนี้ว่า UTP แต่ถ้าหากต้องการเดินสายแลนในจุดที่มีสัญญาณรบกวนสูง ๆ ไม่ควรนำสาย UTP แบบธรรมดามาใช้งาน



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

สาย UTP ที่นิยมใช้ในปัจจุบันมีดังนี้

ก) สาย Category 5e UTP

เป็นสายที่ไม่มีฉนวนป้องกันสัญญาณรบกวนจากภายนอก สายชนิดนี้เป็นสายที่มีจำนวน 4 คู่สาย 8 เส้น และมีขนาดของแกนทองแดงขนาดที่ 24AWG (0.51 mm) ซึ่งมีการผลิตแกนทองแดงแบบแกนเดี่ยว (Solid Conductor) ที่เหมาะกับการติดตั้งแบบทั่วไป และแบบแกนทองแดงแบบฝอย (Stranded Conductor) ที่เหมาะกับสายเชื่อมต่อภายในตู้สื่อสาร หรือที่เรียกว่าสาย Patch Cord ซึ่งจะสามารถบิดโค้งงอได้มากกว่าสายชนิดแกนเดี่ยว (Solid) สายชนิดนี้จะมีแบนด์วิดท์สูงสุด 350MHz ในบางยี่ห้อมาตรฐานที่ 100 MHz และความเร็วในการส่งสัญญาณที่ 100-1,000 Mbps หรือ Gigabit



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

ข) สาย Category6 UTP

เป็นสายที่ไม่มีฉนวนป้องกันสัญญาณรบกวนจากภายนอก สายชนิดนี้เป็นสายที่มีแกนกลางสำหรับแบ่งแยกช่องสัญญาณทั้ง 4 คู่สาย และมีจำนวน 4 คู่สาย 8 เส้น เหมือนกับ CAT5e แต่จะมีขนาดของแกนทองแดงที่ใหญ่กว่าชนิด CAT5e อยู่ที่ขนาด 23AWG (0.51 mm) ซึ่งมีการผลิตแกนทองแดงทั้งแบบแกนเดี่ยว (Solid Conductor) ที่เหมาะกับการติดตั้งแบบทั่วไป และแบบแกนทองแดงแบบฝอย (Stranded Conductor) ที่เหมาะกับสายเชื่อมต่อภายในตู้สื่อสาร หรือที่เรียกว่าสาย Patch Cord ซึ่งจะสามารถบิดโค้งงอได้มากกว่าสายชนิดแกนเดี่ยว (Solid) สำหรับสาย CAT6 จะมีแบนด์วิดท์สูงสุดที่ 650 MHz หรือมาตรฐานอยู่ที่ 250 MHz และความเร็วสูงสุดในการส่งสัญญาณที่ Full Speed 1,000 Mbps หรือ Full Gigabit



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



รูปที่ 3.3 มาตรฐานของลวดตัวนำไฟฟ้า AWG (American Wire Gauge)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หมายเหตุ

AWG (American Wire Gauge) หรือใช้คำย่อ Gauge ซึ่งเป็นหน่วยวัดขนาดของลวดตัวนำไฟฟ้าที่ใช้ในอเมริกาและแคนาดา และใช้กันอย่างแพร่หลายทั่วโลก โดยสามารถแปลงหน่วย AWG เป็นหน่วยวัดที่เราคุ้นเคย เช่น มิลลิเมตร (Millimeter) และตาราง-มิลลิเมตร (Sq. Millimeter) ได้ดังนี้

$$12 \text{ AWG} = 2.05 \text{ mm} = 3.309 \text{ sq.mm}$$

$$13 \text{ AWG} = 1.83 \text{ mm} = 2.624 \text{ sq.mm}$$

$$14 \text{ AWG} = 1.63 \text{ mm} = 2.081 \text{ sq.mm}$$

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หมายเหตุ

15 AWG = 1.45 mm = 1.650 sq.mm

16 AWG = 1.29 mm = 1.309 sq.mm

18 AWG = 1.02 mm = 0.822 sq.mm

20 AWG = 0.81 mm = 0.517 sq.mm

22 AWG = 0.65 mm = 0.325 sq.mm

23 AWG = 0.57 mm = 0.260 sq.mm

24 AWG = 0.51 mm = 0.204 sq.mm

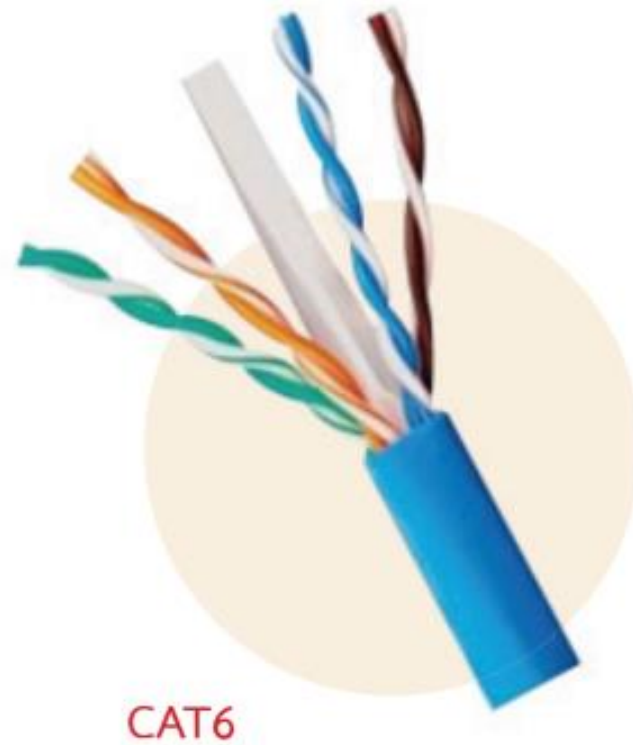
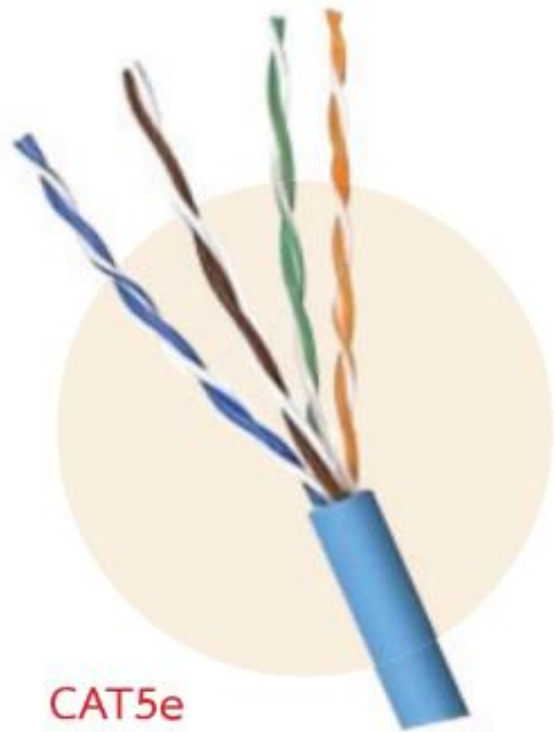
26 AWG = 0.40 mm = 0.128 sq.mm

สังเกตว่ายิ่ง AWG มีค่ามากขึ้น ขนาดของลวดตัวนำไฟฟ้าจะยิ่งเล็กลงเท่านั้น

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

จุดสังเกตระหว่าง CAT5e กับ CAT6



รูปที่ 3.4 ภาพแสดงสาย CAT5e กับ CAT6

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



สีของตัวสาย โดยส่วนใหญ่ในประเทศไทย สายชนิด CAT5e จะมีสีเทาและสีขาว ส่วนสายชนิด CAT6 จะมีสีฟ้าหรือน้ำเงินในบางยี่ห้อ



แกนทองแดงของสายชนิด CAT5e จะมีแกนทองแดงที่เล็กกว่าชนิด CAT6



สาย CAT6 จะมีพลาสติกแกนกลางที่คั่นระหว่างสายทั้ง 4 คู่ ส่วนสายชนิด CAT5e ไม่มี



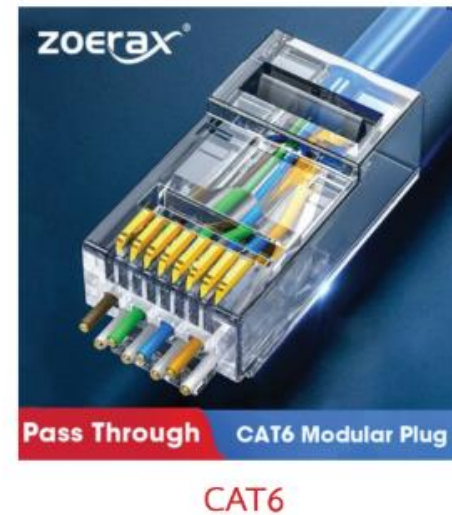
สาย CAT6 จะมีพลาสติกแกนกลางที่คั่นระหว่างสายทั้ง 4 คู่ ส่วนสายชนิด CAT5e ไม่มี

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

- 👤 สาย CAT6 จะมีพลาสติกแกนกลางที่คั่นระหว่างสายทั้ง 4 คู่ ส่วนสายชนิด CAT5e ไม่มี
 - ☁ CAT5e หน้าตัด แกนกลางของสายจะเรียงกันแบบแนวนอน
 - ☁ CAT6 หน้าตัดจะสลับฟันปลา ขึ้นลง ไม่เสมอกัน



รูปที่ 3.5 ภาพตัดของหัวต่อ RJ45 Plug

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

ค) สาย Category7

สาย CAT7, 7A รองรับการส่งข้อมูลความเร็วสูงสุด 10 Gbps ระยะทางสูงสุด 100 เมตร ความถี่ใช้งานสูงสุด 600-1,000 MHz ประกอบด้วยสายคู่บิดเกลียวที่หุ้มด้วยฟอยล์ ซึ่งช่วยป้องกัน Crosstalk อย่างสมบูรณ์เหมาะสำหรับศูนย์ข้อมูล (Data Center) มากกว่าการใช้งานที่บ้าน

ง) สาย Category8

CAT8 มีโครงสร้างที่มีชีลด์ (Shield) ป้องกันถึง 2 ชั้น คือ S/FTP ถ้าปกสายลงไปชั้นแรกจะเจอกับลวดถักที่สานกันเป็นฉนวนป้องกันชั้นแรก ถัดลงไปจะเป็นฟอยล์หุ้มสายคู่ บิดเกลียวเอาไว้อีกชั้นเป็น 2 ชั้น เพื่อรองรับการส่งข้อมูลความเร็วสูง โดยความเร็วสูงสุดอยู่ที่ 25 Gbps และ 40 Gbps ที่ระยะทาง 30 เมตร ความถี่ใช้งาน 2,000 MHz สายจึงมีขนาดใหญ่ถึง 22 AWG จึงเหมาะใช้ในงานที่ต้องการความเร็วสูง เช่น ศูนย์ข้อมูล หรือเชื่อมต่อระหว่างอุปกรณ์สวิตช์ ดังนั้นจึงรองรับอนาคตทางการสื่อสารที่ต้องการความเร็วสูงมาก ๆ ได้

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

สาย CAT8 มีความแตกต่างจากสายเคเบิลรุ่นก่อนหน้านี้อย่างมาก เนื่องจากสามารถรองรับความถี่ของสัญญาณได้สูงถึง 2 GHz (2,000 MHz) โดยมีการจำกัดช่องต่อที่ระยะ 30 เมตร จำนวน 2 ช่อง (Connector channels) และสาย CAT8 ต้องใช้สายชนิดหุ้มฉนวนเช่นกัน CAT8 สามารถรองรับความเร็วได้ที่ 25 Gbps หรือ 40 Gbps และยังช่วยลดค่าใช้จ่ายและการใช้พลังงานมากกว่าสาย Fiber อีกด้วย



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

ลักษณะทางกายภาพของสาย CAT8 จะมีความคล้ายคลึงกับสายแลนชนิดอื่น ๆ และใช้หัวต่อ RJ45 หรือหัวต่ออื่นที่ไม่ใช่ RJ45 ได้ และสาย CAT8 สามารถใช้งานร่วมกับสายชนิดก่อนหน้านี้คือ CAT6 และ CAT7 ได้ จึงไม่มีปัญหาในการใช้งานเมื่อเชื่อมต่อกัน

รองรับความเร็วสูงสุดถึง 40 Gbps ระยะทางไม่เกิน 30 เมตร และ 10 Gbps ระยะทางไม่เกิน 100 เมตร สาย CAT8 กำลังจะเข้ามาแทนที่ CAT6a เนื่องจากปริมาณข้อมูลที่เพิ่มขึ้นทุกวัน ทำให้ความเร็วในการส่งข้อมูลของศูนย์ข้อมูลจะต้องมากขึ้นด้วย ดังนั้นจะเน้นใช้งาน CAT8 ในศูนย์ข้อมูลเป็นหลัก



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

	Cat6	Cat8
แบนด์วิดท์	250 MHz	2000 MHz
ความเร็วสูงสุด	1 Gbps	40 Gbps
ระยะสูงสุดของสาย	328 ft. / 100 m	98 ft. / 100 m

	Cat6a	Cat8
แบนด์วิดท์	50 MHz	2000 MHz
ความเร็วสูงสุด	10 Gbps	40 Gbps
ระยะสูงสุดของสาย	328 ft. / 100 m	98 ft. / 100 m

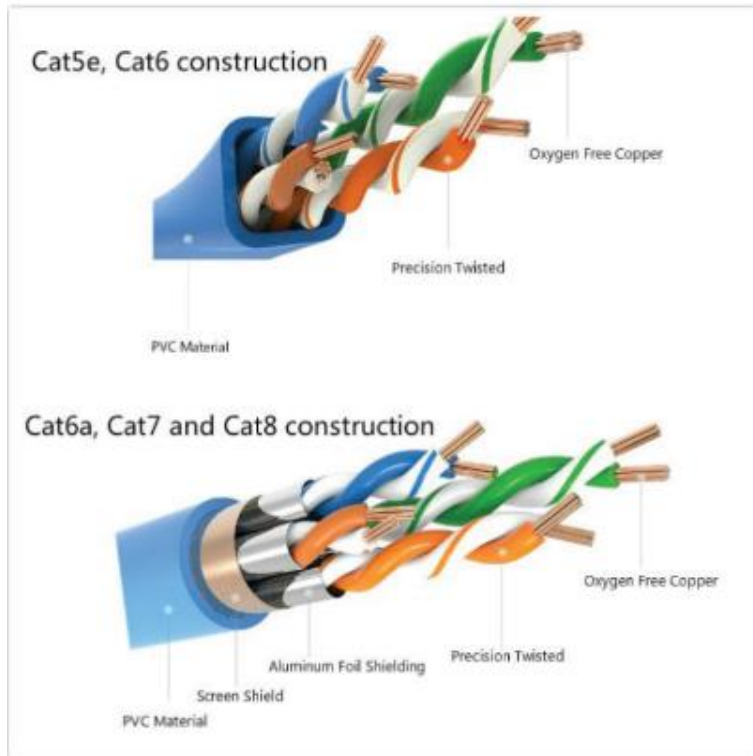
	Cat7	Cat8
แบนด์วิดท์	600 MHz	2000 MHz
ความเร็วสูงสุด	10 Gbps	40 Gbps
ระยะสูงสุดของสาย	328 ft. / 100 m	98 ft. / 100 m

ตารางที่ 3.1 เปรียบเทียบแบนด์วิดท์ ความเร็วสูงสุด และระยะสูงสุดของสายเมื่อเทียบกับ Cat8

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



สาย CAT5e และ CAT6 UTP เป็นสายที่นิยมใช้งานเป็นอย่างมาก ซึ่งมักเรียกว่าสายประเภท UTP แต่ด้วยการสื่อสารในปัจจุบันมีความเร็วมากขึ้น ตัวสายก็ใช้ความถี่ที่มากขึ้นในการรับส่งสัญญาณ จึงทำให้เกิดสัญญาณรบกวนของกลุ่มสายที่มากขึ้นด้วย

เพื่อแก้ปัญหาดังกล่าว จึงเกิดสายที่มีฟอยล์ (Foil) หรือเรียกว่าสกรีน (Screen) หุ้มคู่สายไว้ เรียกสายสัญญาณแบบนี้ว่า F/UTP (Foil Twisted Pair) และมีสายประเภท F/UTP, U/FTP, F/FTP ขึ้นมา

รูปที่ 3.6 เปรียบเทียบโครงสร้างของสาย CAT5e, CAT6 กับ CAT6a, CAT7 และ CAT8

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

แต่การเพิ่มพอยต์หุ้มสาย ส่งผลต่อการเพิ่มต้นทุนของสายสัญญาณ ผู้ผลิตบางรายจึงพยายามออกแบบโครงสร้างของสาย UTP ให้มีคุณสมบัติพิเศษในการป้องกันสัญญาณรบกวนระหว่างสายสัญญาณแต่ละเส้น (Alien Crosstalk) โดยอาจต้องตีเกลียวให้แน่นขึ้น ซึ่งทำให้ต้นทุนทองแดงยาวขึ้นและในบางกรณีต้นทุนโครงสร้างของสาย UTP อาจแพงกว่าสาย F/UTP ก็ได้ เช่น สาย UTP CAT6a จะแพงกว่าสาย F/UTP CAT6a

หรือในสาย CAT6 มีเพิ่มแกนพลาสติกตรงกลางสาย ซึ่งเรียกว่า Filler Slot หรือ Cross Filler ใช้แยกสายแต่ละคู่ออกจากกัน เพื่อป้องกันสัญญาณรบกวนระหว่างสายแต่ละคู่ที่อยู่ภายใน ทำให้ป้องกันสัญญาณรบกวนได้ดีและมีประสิทธิภาพสูง



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

แต่เมื่อสาย CAT6a ได้รับความนิยมและความถี่ที่ใช้งานสูงมากขึ้น ทำให้การผลิตสาย CAT6a แบบ UTP ต้องมีการตีเกลียวสายให้แน่นขึ้น ส่งผลให้ต้นทุนทองแดงที่ใช้เพิ่มขึ้นตามไปด้วย และยังต้องทำเปลือกสายกับ Filler ให้หนาขึ้น จนทำให้สายประเภท UTP ของ CAT6a มีราคาที่สูงกว่า FTP รวมไปถึงประสิทธิภาพในการป้องกันสัญญาณรบกวนนั้น สายประเภทมีฟอยล์สามารถป้องกันการรบกวนได้ดีกว่าและเมื่อผลิตสายประเภท FTP มีขนาดสายที่เล็กกว่า เพราะไม่ต้องมี Filler และเปลือกที่หนา จึงทำให้สาย CAT6a ที่มีโครงสร้างแบบ U/FTP หรือ F/FTP เป็นที่นิยมมากกว่า



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

ในอนาคต ตั้งแต่สาย CAT8 ขึ้นไป เราจะไม่พบสายประเภท UTP แล้ว เนื่องด้วยความถี่ที่สูงขึ้นมาก ทำให้มีความจำเป็นต้องใช้สายที่มีฟอยล์หุ้มเพียงอย่างเดียว

ดังนั้น สำหรับสาย CAT5e และ CAT6 การเลือกใช้สาย UTP เป็นทางเลือกที่คุ้มค่าและมีประสิทธิภาพ แต่สำหรับสาย CAT6a ขึ้นไป ควรเลือกใช้สายประเภท U/FTP หรือ F/FTP จะคุ้มค่ากว่า

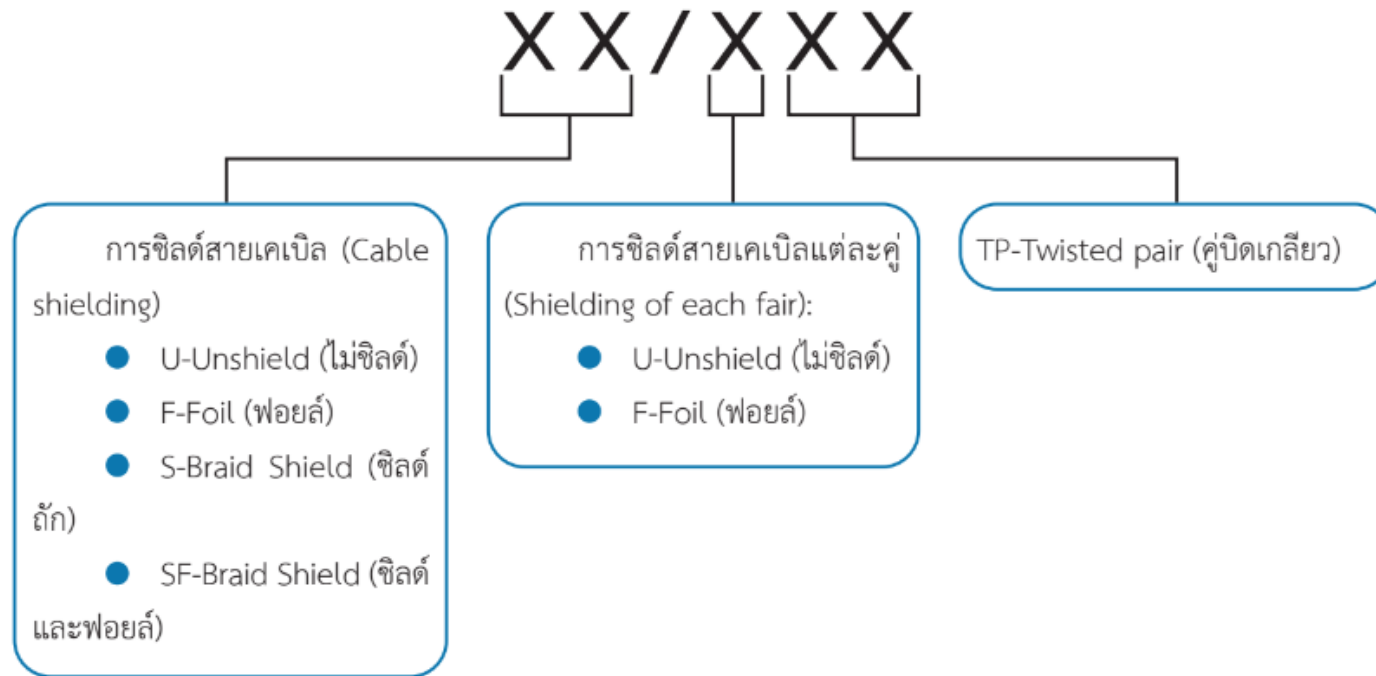


สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

เนื่องจากสาย UTP มีหลายประเภทมากขึ้น จึงกำหนดหลักการเรียกหรืออธิบาย ประเภทสาย UTP ดังนี้



รูปที่ 3.7 หลักการเรียกหรืออธิบายประเภทสาย UTP

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

ดังนั้น สาย UTP ทั่วไปจะเป็น ดังนี้

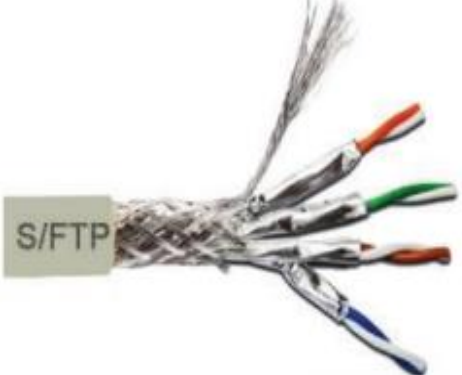
ประเภทสาย	คำอธิบาย
UTP Unshield Twisted Pair [U/UTP]	สายทองแดงคู่บิดตีเกลียว แบบไม่มีชีลด์ป้องกันสัญญาณรบกวน
Foil Twisted Pair (FTP) หรือ F/UTP	สายทองแดงคู่บิดตีเกลียว แบบมีชีลด์ฟอยล์และชีลด์ถักด้านนอก
SF/UTP (Shield and foil shield with unshielded twisted pairs)	สายทองแดงคู่บิดตีเกลียวแบบไม่มีชีลด์ แต่มีชีลด์ฟอยล์และชีลด์ถักภายนอก
U/FTP (Individual Foil Twisted Pair)	สายทองแดงคู่บิดตีเกลียว แบบมีชีลด์ฟอยล์แต่ละคู่สาย
F/FTP (Foil and Individual Foil Twisted Pair)	สายทองแดงคู่บิดตีเกลียว แบบมีชีลด์ฟอยล์แต่ละคู่สาย และมีชีลด์ฟอยล์ภายนอก
S/FTP (Shield over Individual Foil Twisted Pair)	สายทองแดงคู่บิดตีเกลียว แบบมีชีลด์ฟอยล์แต่ละคู่สาย และมีชีลด์ถักภายนอก

ตารางที่ 3.2 ลักษณะของสาย UTP ประเภทต่าง ๆ

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

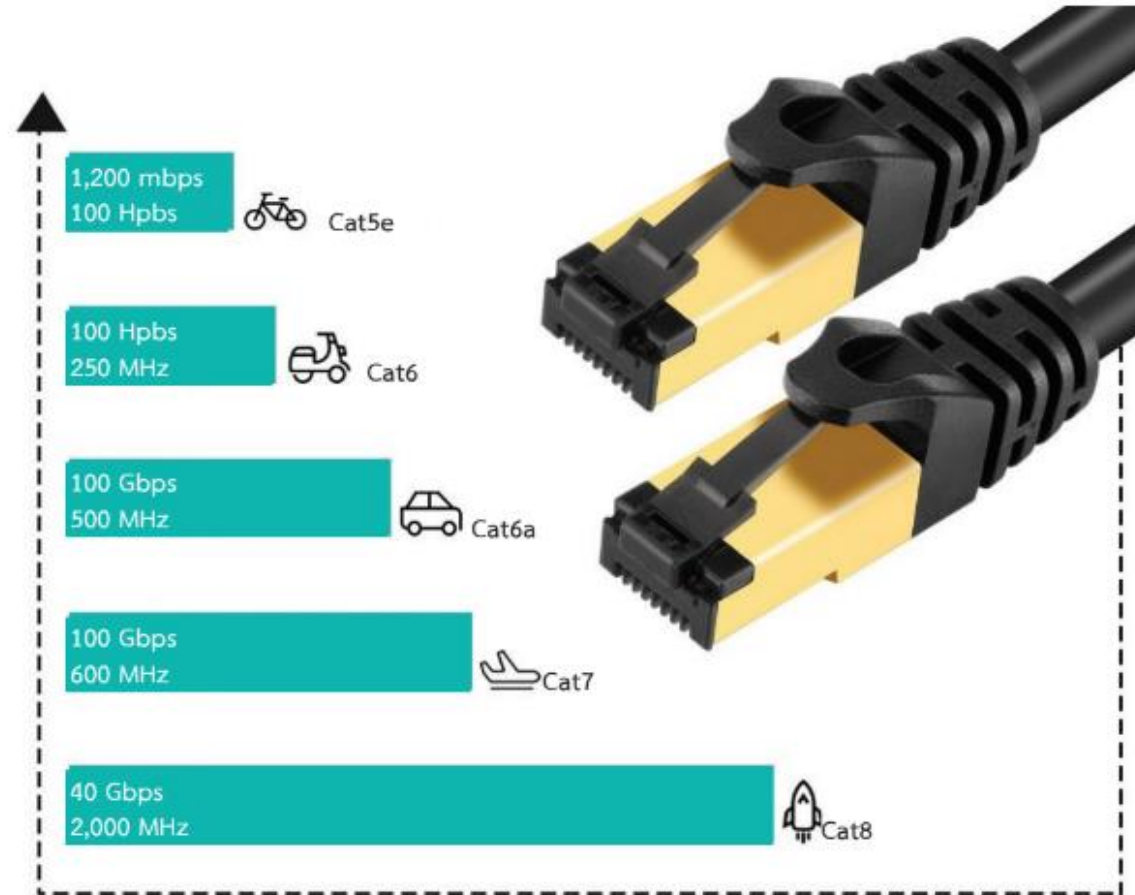
	ISO/IEC 11801	Cable Shielding	Pair Shielding			
	U/UTP	None	None		F/FTP	Foil Foil
	U/FTP	None	Foil			
	F/UTP	Foil	None		S/FTP	Braiding Foil

รูปที่ 3.8 สาย UTP ประเภทต่าง ๆ

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



รูปที่ 3.9 เปรียบเทียบความเร็วสาย UTP ประเภทต่าง ๆ

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

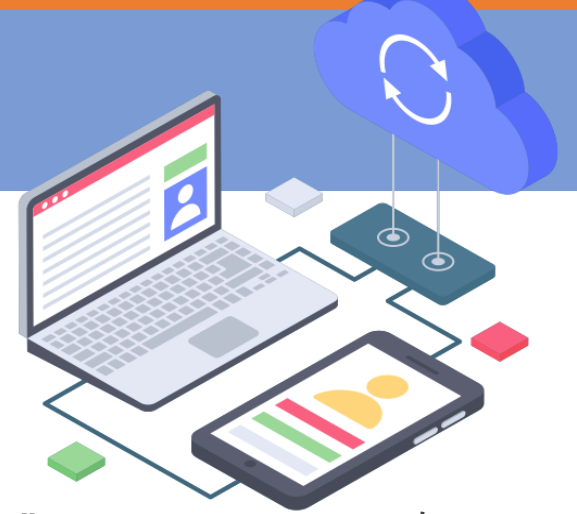
1.1.3 หัวต่อและพอร์ต (Registered Jack: RJ)

Registered Jack คืออุปกรณ์มาตรฐานในงานโทรคมนาคมที่ใช้เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์กับสายตีเกลียว

ก) หัวต่อ RJ11

สำหรับใช้กับสายโทรศัพท์ (ไม่ใช่สายคู่บิดเกลียว STP และ UTP ที่กล่าวในที่นี่ แต่ควรจะรู้จัก) เพื่อการติดต่อสื่อสารจากสายโทรศัพท์ผ่านโมเด็มไปยังอินเทอร์เน็ต โดย RJ11 ขนาดเล็กกว่า RJ45 (ซึ่งใช้กับสายคู่บิดเกลียว UTP) เนื่องจากตัวหัวต่อมีขาเพียง 4 ขา

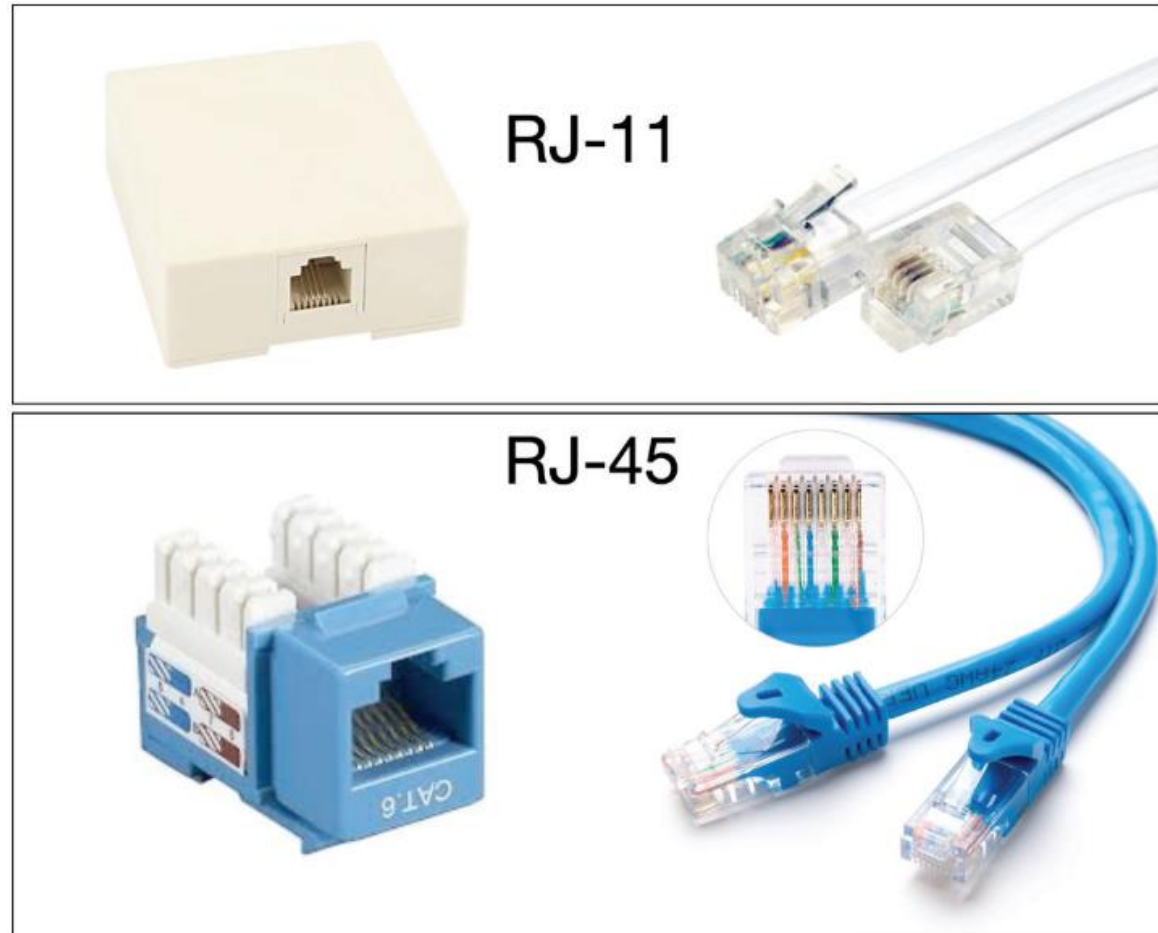
เนื่องจากการสื่อสารระบบแอนะล็อก ซึ่งมีความเร็วในการรับส่งข้อมูลต่ำมาก ปัจจุบันจึงไม่มีการใช้งานแล้วสำหรับการสื่อสารเครือข่ายคอมพิวเตอร์ แต่ยังมีใช้งานอยู่สำหรับโทรศัพท์บ้าน



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



รูปที่ 3.10 เปรียบเทียบหัวต่อและพอร์ต RJ11 และ RJ45

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

ข) หัวต่อ RJ45

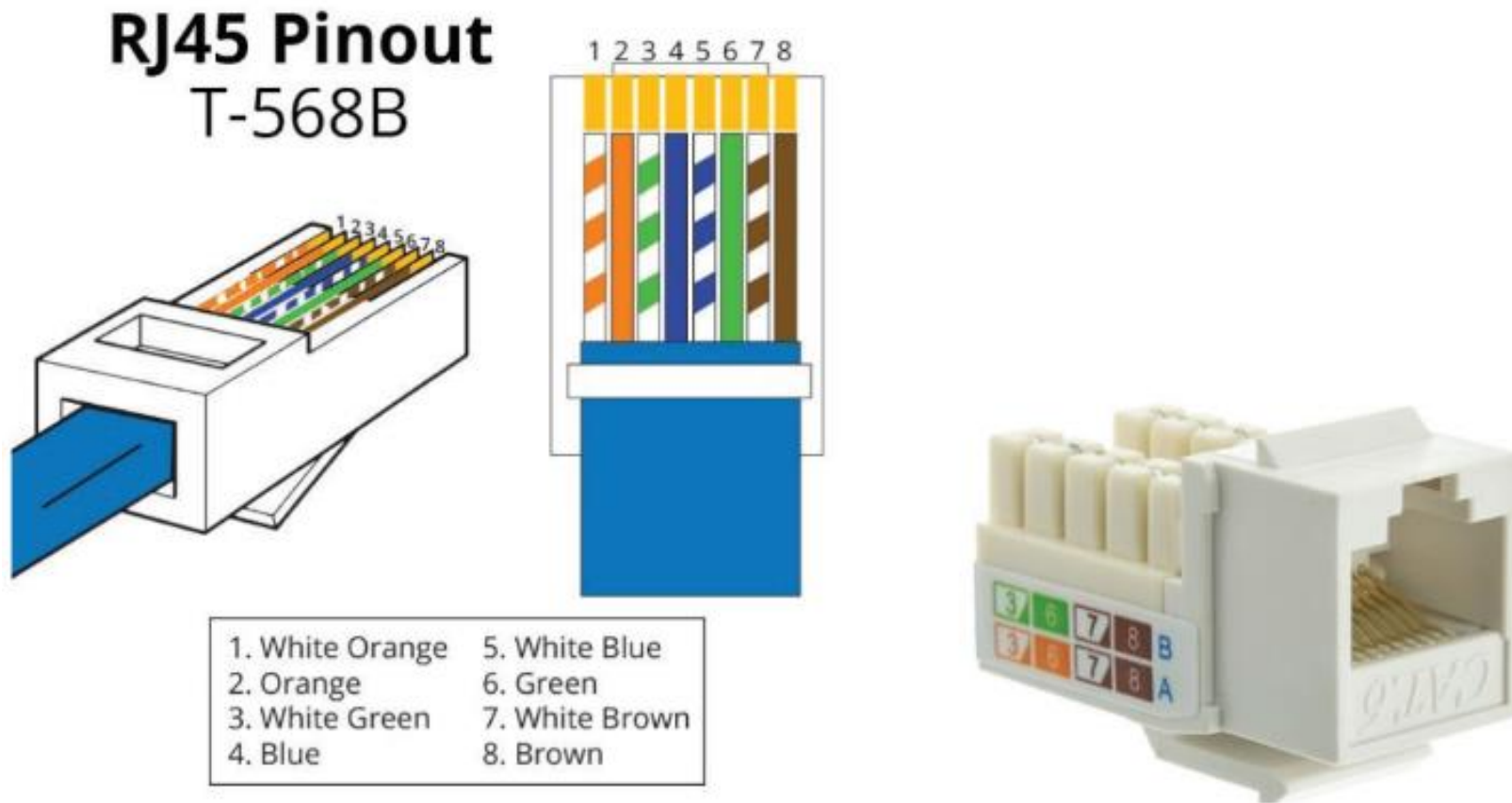
หรือหัวต่อตัวผู้ RJ45 (หรือ RJ45 connector หรือ RJ45 Jack Plug) คือ หัวต่อที่ใช้กับสายสัญญาณสายคู่บิดเกลียว UTP โดยเป็นหัวต่อสำหรับใส่ที่ปลายสาย UTP มีลักษณะเป็นพลาสติกสีเหลืองมกลายหัวต่อโทรศัพท์ แต่มีขนาดใหญ่กว่าเล็กน้อย และมี 8 พิน มีช่องสำหรับเสียบสายที่ด้านหลังด้านล่างเรียบ ส่วนด้านบนมีตัวล็อก ถ้าหันหน้าเข้าด้านหน้าของหัวต่อพิน 1 จะอยู่ทางซ้ายมือในขณะที่พิน 8 จะอยู่ทางขวามือ



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



รูปที่ 3.11 หัวต่อตัวผู้และตัวเมีย RJ45

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หัวต่อตัวเมีย RJ45 (RJ45 Jack Face) หรือโดยทั่วไปเรียกพอร์ต RJ45 มีลักษณะเป็นช่องเสียบสำหรับหัวต่อ RJ45 ตัวผู้ เมื่อมองจากด้านที่จะนำหัวต่อตัวผู้ไปเสียบ พिन 8 จะอยู่ทางซ้าย ส่วนพิน 1 จะอยู่ทางขวา

หัวต่อตัวเมียจะเป็นกล่องมีช่องสำหรับเสียบหัวต่อ ด้านในกล่องจะมีขั้ว ซึ่งจะเป็นส่วนที่เชื่อมกับสายนำสัญญาณ เพื่อเป็นช่องทางสื่อสารระหว่างตัวคอมพิวเตอร์กับอุปกรณ์ภายนอก มักพบ RJ45 Jack Face ในเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย เช่น เราเตอร์ (Router) ฮับ (Hub) สวิตช์ (Switch) มากกว่าที่จะต่อลอยอยู่กับสายเคเบิล



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

1.1.4 การใช้งานหัวต่อ RJ45

หัวต่อ RJ45 ไซสายแบบ CAT5 และสาย CAT6 เป็นสายเส้นเล็กจำนวน 8 เส้น บิดเกลียวคู่ทั้งหมด 4 คู่ รูปแบบในการเข้าหัวต่อ RJ45 มีอยู่ 2 แบบ คือ TIA/EIA 568A และ 568B ส่วนรายละเอียดเกี่ยวกับการเรียงลำดับสายจะแสดงดังนี้

พินที่	TIA/EIA 568A	TIA/EIA 568B
1	ขาวส้ม	ขาวเขียว
2	ส้ม	เขียว
3	ขาวเขียว	ขาวส้ม
4	น้ำเงิน	น้ำเงิน
5	ขาวน้ำเงิน	ขาวน้ำเงิน
6	เขียว	ส้ม
7	ขาวน้ำตาล	ขาวน้ำตาล
8	น้ำตาล	น้ำตาล

รูปที่ 3.12 มาตรฐาน TIA/EIA 568A และ 568B

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หมายเหตุ

ในอดีตจะมีการใช้แค่ 2 คู่สาย (4 เส้น) แต่ในปัจจุบันสำหรับการส่งข้อมูลที่ต้องการความเร็วสูงจะใช้งานทั้ง 4 คู่สาย (8 เส้น)

สื่อกลางเครือข่ายคอมพิวเตอร์



1. สื่อกลางประเภทมีสาย

การนำใช้สายสัญญาณตามมาตรฐาน TIA/EIA 568A และ 568B แบ่งออกเป็น 2 ประเภท ดังนี้

ก) สายครอส (Crossover Cable) หรือสายไขว้

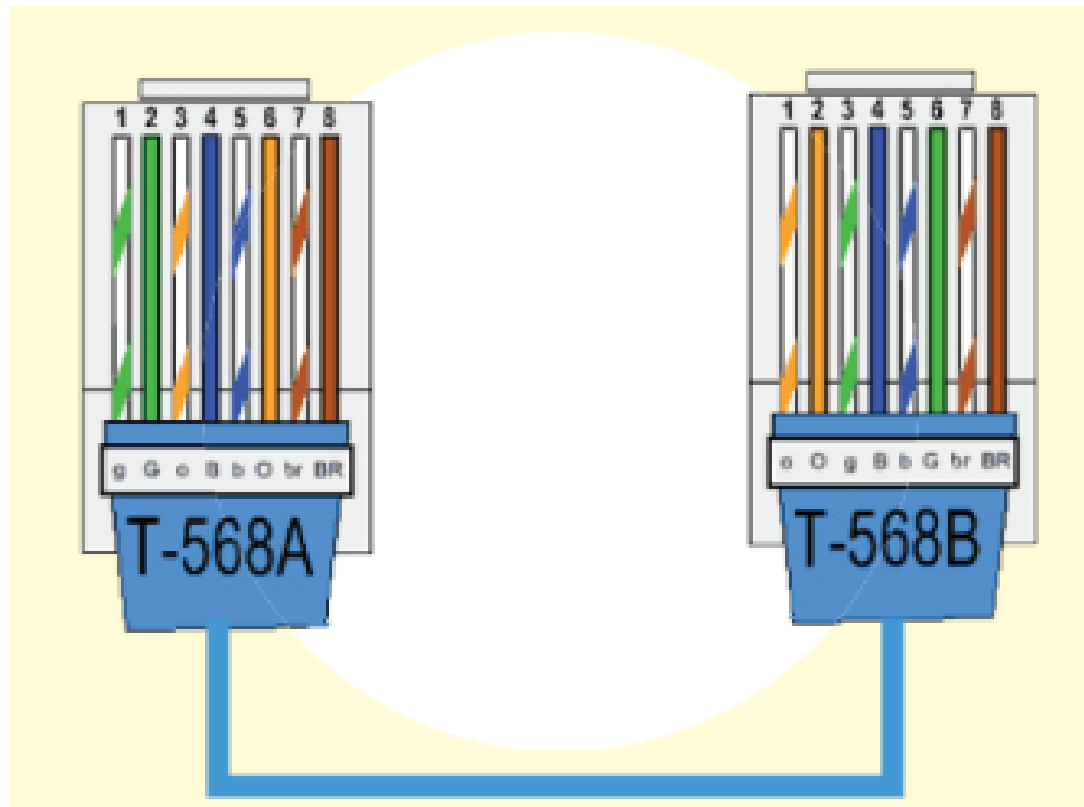
สำหรับเชื่อมต่ออุปกรณ์ที่เหมือนกัน เช่น การเชื่อมต่อโดยตรงระหว่างเครื่องคอมพิวเตอร์ 2 เครื่อง หรือระหว่างเครื่องคอมพิวเตอร์กับเราเตอร์ด้วยสาย UTP เพียง 1 เส้น โดยเสียบหัวต่อ RJ45 ไปที่การ์ดเน็ตของทั้งสองเครื่อง

เนื่องจาก MDI (Medium Dependent Interface) เป็นชนิดพอร์ตของการ์ดแลน ซึ่งคอมพิวเตอร์ และเราเตอร์ใช้ ทำให้อุปกรณ์ทั้งคอมพิวเตอร์และเราเตอร์เป็น MDI เหมือนกัน จึงใช้สายครอสในอุปกรณ์ประเภทเดียวกัน

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

รูปแบบการเข้าสาย UTP กับหัวต่อ RJ45 มีดังนี้



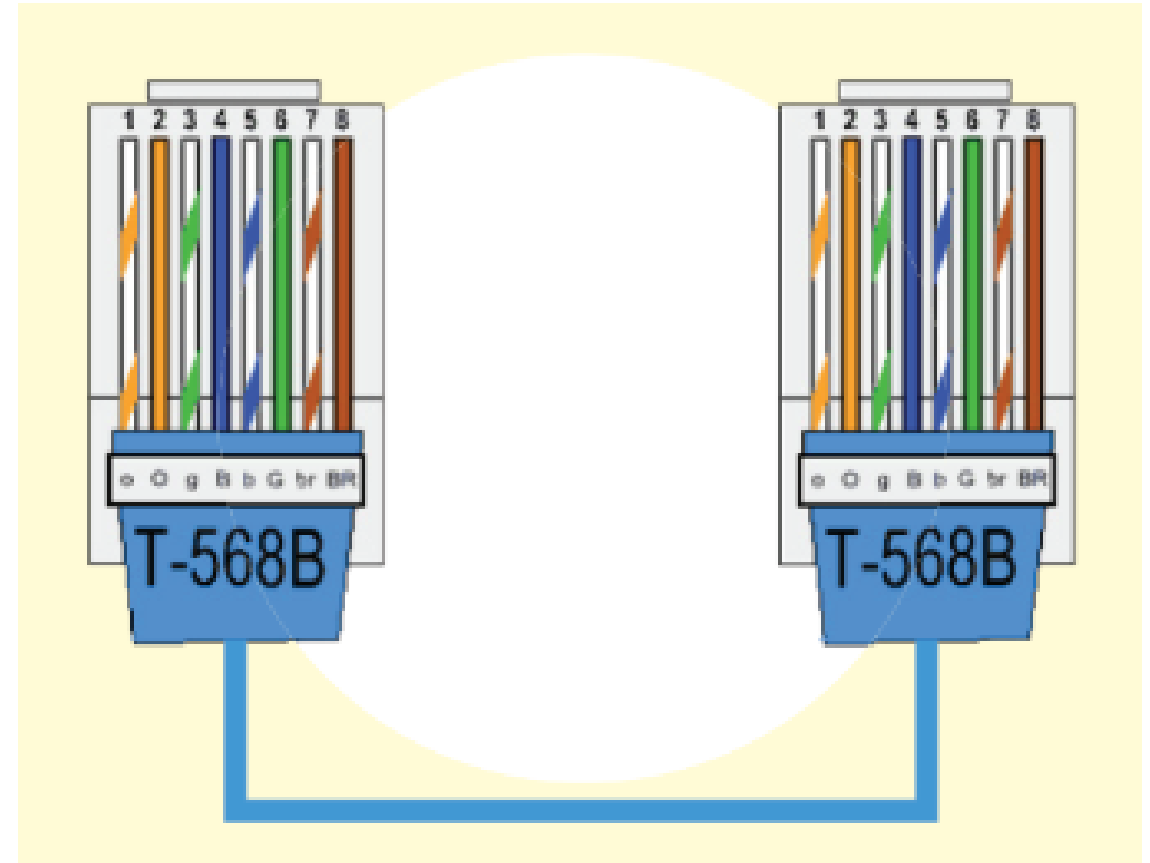
รูปที่ 3.13 สายครอส (Crossover Cable) หรือสายไขว้

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

ข) สายตรง (Straight-through Cable)

สำหรับต่ออุปกรณ์ที่ต่างกัน เช่น การเชื่อมต่อคอมพิวเตอร์เข้ากับสวิตช์ การเชื่อมต่อคอมพิวเตอร์เข้ากับฮับชนิดพอร์ตของการ์ดแลน ฮับและสวิตช์ใช้คือ MDIX (Medium Dependent Interface Crossover) (โดย X ตัวย่อของ Crossover) แต่คอมพิวเตอร์เป็น MDI



รูปที่ 3.14 สายตรง (Straight-through Cable)

สื่อกกลางเครือข่ายคอมพิวเตอร์

1. สื่อกกลางประเภทมีสาย

ในปัจจุบันอุปกรณ์เครือข่ายมีความฉลาดมากขึ้น สามารถทำการปรับการเชื่อมต่อหัวสายให้โดยอัตโนมัติ เรียกว่า ฟังก์ชัน auto-MDI/MDIX ซึ่งมีวงจรเพื่อปรับสายไขว้ให้กลับมาเป็นสายตรง หรือปรับสายตรงกลับมาเป็นสายไขว้ได้ แต่ถ้าทำงานกับอุปกรณ์เครือข่ายรุ่นเก่าจำเป็นต้องใช้สายในการเชื่อมต่อให้ถูก ไม่เช่นนั้นอาจส่งผลให้อุปกรณ์ไม่สามารถใช้งานได้



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

1.2 สายโคแอกเซียล (Coaxial)



เรียกสั้น ๆ ว่าสายโคแอก (Coax) โดยได้รับชื่อจากข้อเท็จจริงว่ามีสองตัวนำที่ใช้แกนเดียวกันร่วมกัน (Share the same axis) หรือเรียกสาย RG ซึ่งย่อมาจาก Radio Grade หมายถึง ท่อนำคลื่นความถี่ เป็น ตัวกลางเชื่อมโยงที่มีลักษณะเช่นเดียวกับสายที่ต่อจากเสาอากาศ สายโคแอกเซียลที่ใช้ทั่วไปมี 2 ชนิด ได้แก่ 50 โอห์ม ซึ่งใช้ส่งข้อมูลแบบดิจิทัล และชนิด 75 โอห์ม ซึ่งใช้ส่งข้อมูลสัญญาณแอนะล็อกสายโคแอกเซียล ประกอบด้วย



แกนกลางตัวนำทองแดง (Center Conductor) เป็นแกนกลางที่ใช้ในการส่งสัญญาณ



ตัวนำทองแดงจะล้อมรอบด้วยชั้นของวัสดุไดอิเล็กทริก (Dielectric Material) เป็นฉนวนไฟฟ้า ชนิดหนึ่งที่มีความยืดหยุ่น เพื่อป้องกันกระแสไฟรั่ว

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



จากนั้นฉนวนไฟฟ้าอาจจะถูกหุ้มด้วยฟอยล์ (Foil shield)



ฉนวนไฟฟ้าจะถูกหุ้มด้วยชีลด์ถัก (Braid Shield) ซึ่งอาจเป็นทองแดงถักทอ (Copper Braid) หรือฟอยล์โลหะ (Metallic foil) ที่ทำหน้าที่เหมือนเป็นสายเส้นที่สองในวงจร (Second Wire in the Circuit) และเป็นตัวป้องกัน (Shield) ให้กับตัวนำภายใน (Center Conductor) นอกจากนี้ยังช่วยลดปริมาณของสัญญาณรบกวนแม่เหล็กไฟฟ้าภายนอก



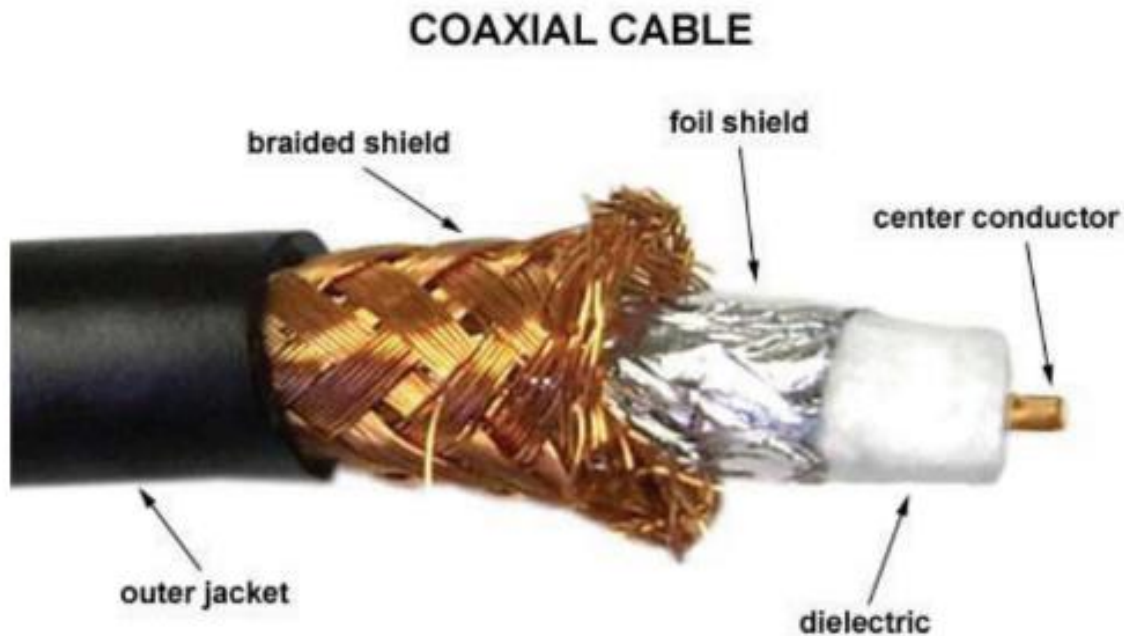
สายเคเบิลทั้งหมดจะถูกคลุมด้วยแจ็คเก็ตหุ้มสาย (Cable Jacket) ที่จะปกป้องจากความเสียหายเล็กน้อยทางกายภาพ



สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย



รูปที่ 3.15 สายโคแอกเชียล (Coaxial)



นิยมใช้กับงานระบบรักษาความมั่นคง
ปลอดภัย (Security) ระบบกล้องโทรทัศน์วงจรปิด
(CCTV) ระบบเคเบิลทีวี (CATV) ทีวีรวม (TV,
MATV) และระบบดาวเทียม (Satellite)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หัวต่อแบบ BNC ใช้สำหรับสายโคแอกเชียลซึ่งเป็นสายเส้นเดียวมีลวดทองแดงเป็นแกนกลางหุ้มด้วยฉนวนสายยาง หัวต่อ BNC จะเป็นโลหะรูปวงกลม มีเกลียวสำหรับล็อกและยังต้องใช้ตัวปิด (Terminator) (ความต้านทาน 50 โอห์ม) เพื่อปิดหัวและท้ายของสาย



รูปที่ 3.16 หัวต่อแบบ BNC

สื่อกลางเครือข่ายคอมพิวเตอร์

1.

สื่อกลางประเภทมีสาย

นอกจากนี้ ยังมีหัวต่อ
สำหรับสายโคแอกเชียลอีก
หลากหลาย (Coaxial Cable
Connector types)



รูปที่ 3.17 หัวต่อสำหรับสายโคแอกเชียลแบบต่าง ๆ
(Coaxial Cable Connector types)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

1.3 สายใยแก้วนำแสง (Fiber optic)

มีแกนกลางของสายซึ่งประกอบด้วยเส้นใยแก้วหรือพลาสติก (Fiber Core) ขนาดเล็กหลาย ๆ เส้นอยู่ร่วมกัน เส้นใยแต่ละเส้นมีขนาดเล็กเท่าเส้นผม ภายในกลวง และเส้นใยเหล่านั้นได้รับการห่อหุ้มด้วยเส้นใยอีกชนิดหนึ่งเรียกว่า แคลดดิง (Cladding) และหุ้มด้วยบัฟเฟอร์ (Buffer) หรือตัวกันกระแทกที่เคลือบแคลดดิงเอาไว้และวัสดุที่เสริมสร้างความแข็งแรง (Strengthening Materials) จากนั้นหุ้มด้วยแจ็คเก็ต (Jacket) หรือตัวหุ้มภายนอกสุดอีกที



สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

การส่งข้อมูลผ่านทางสื่อกลางชนิดนี้ จะใช้แสงเลเซอร์หรือ LED วิ่งผ่านช่องกลางของเส้นใยแต่ละเส้นและอาศัยหลักการหักเหของแสง โดยใช้ใยแก้วชั้นนอกเป็นกระจกสะท้อนแสง การให้แสงเคลื่อนที่ไปในท่อแก้วสามารถส่งข้อมูลด้วยอัตราความหนาแน่นของสัญญาณข้อมูลสูงมากและไม่ถูกรบกวนจากคลื่นแม่เหล็กไฟฟ้า การส่งข้อมูลด้วยใยแก้วนำแสงยังมีความเร็วสูงและความมั่นคงปลอดภัยสูง แต่ต้องระวังการบิดงอสายสัญญาณอาจจะทำให้เส้นใยหักและการติดตั้งเนื่องจากต้องใช้เครื่องมือพิเศษในการติดตั้งและต่อสาย

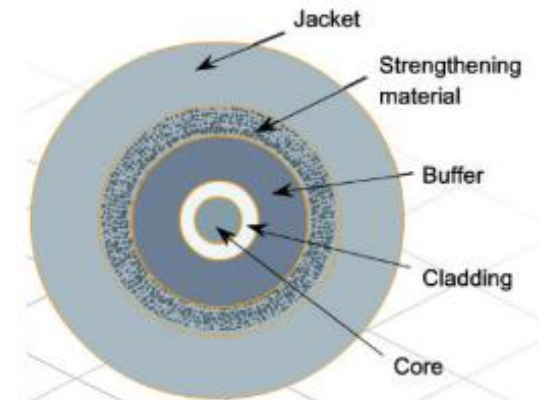
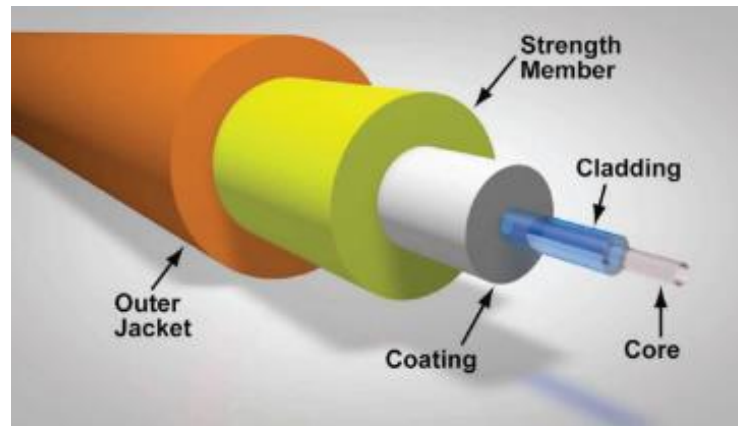


สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย



รูปที่ 3.18 สายใยแก้วนำแสง (Fiber optic cable)



รูปที่ 3.19 โครงสร้างของสายใยแก้วนำแสง

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

1.3.1 โครงสร้างของสายใยแก้วนำแสง (Fiber optic cable)

แม้ว่าสายใยแก้วนำแสง (Fiber Optic) หรืออปติกไฟเบอร์ ไฟเบอร์จะบางมาก แต่จะประกอบด้วยแก้วสองชนิดและชีลด์ป้องกันด้านนอก (Protective Outer Shield) ดังนี้

- **คอร์ (Core)** แกนกลางหรือเส้นใยหลัก (Fiber Core) ประกอบด้วยแก้วบริสุทธิ์และเป็นส่วนหนึ่งของใยแก้วนำแสงที่จะใช้นำพาแสง

- **แคลดดิง (Cladding)** หรือตัวหุ้มใยแก้ว กระจกที่ล้อมรอบเส้นใยหลักและทำหน้าที่เป็นตัวสะท้อน โดยพัลส์แสง (Light Pulses) หรือคลื่นแสงจะแพร่กระจายลงที่เส้นใยหลัก ส่วนแคลดดิงจะสะท้อน (Reflect) พัลส์แสงนั้น ซึ่งจะรักษาให้พัลส์แสงมีอยู่ในเส้นใยหลักในปรากฏการณ์ที่เรียกว่าการสะท้อนภายใน (Internal Reflection)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

 แจ็กเกต (Jacket) หรือตัวหุ้มภายนอก โดยปกติจะเป็นแจ็กเกตพีวีซี (PVC jacket) ที่ช่วยปกป้องเส้นใยหลักและแคลดดิ้ง

 นอกจากนี้ยังอาจรวมถึงวัสดุที่เสริมสร้างความแข็งแรง (Strengthening Materials) และบัฟเฟอร์ (Buffer) หรือตัวกันกระแทกที่เคลือบแคลดดิ้งเอาไว้ โดยมีวัตถุประสงค์เพื่อป้องกันใยแก้วจากรอยขีดข่วนและความชื้น

แม้ว่าความเสี่ยงในการทำงานที่มีรูปร่างโค้งคม (Susceptible to Sharp Bends) อาจทำให้สายเสียหายได้ คุณสมบัติของเส้นใยหลักและแคลดดิ้งได้มีการเปลี่ยนแปลงในระดับโมเลกุลที่จะทำให้แข็งแรงมาก ใยแก้วนำแสงได้รับการทดสอบผ่านกระบวนการผลิตอย่างเข้มงวด เพื่อความแข็งแรงอย่างน้อย 100,000 ปอนด์ต่อตารางนิ้ว (100,000 Pounds per Square Inch) ใยแก้วนำแสงมีความทนทานพอที่จะทนต่อการจัดการในระหว่างการติดตั้งและการใช้งานในสภาพแวดล้อมที่เลวร้ายในทุกเครือข่ายทั่วโลก

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

1.3.2 ประเภทของสื่อไฟเบอร์ (Types of Fiber Media)

พัลส์แสงเป็นตัวแทนของข้อมูลที่ถูกส่งเป็นบิตบนสื่อ ถูกสร้างขึ้นโดยใช้的一种方式ดังนี้



เลเซอร์ (Lasers)



ไดโอดเปล่งแสง (Light Emitting Diodes : LEDs)

ที่ฝั่งรับจะมีอุปกรณ์ทางอิเล็กทรอนิกส์ (Electronic) เป็นอุปกรณ์กึ่งตัวนำที่เรียกว่าโฟโตไดโอด (Photodiodes) จะทำการตรวจสอบพัลส์แสงและแปลงให้เป็นแรงดันไฟฟ้าที่จะสามารถสร้างขึ้นมาใหม่เป็นเฟรมข้อมูล (Reconstructed Into Data Frames)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หมายเหตุ

แสงเลเซอร์ (Laser Light) ที่ส่งผ่านสายเคเบิลใยแก้วนำแสงสามารถสร้างความเสียหายแก่สายตาของคนได้ ดังนั้น จึงต้องมีการดูแลเพื่อหลีกเลี่ยงการมองเข้าไปในส่วนท้ายของใยแก้วนำแสงที่ใช้งานอยู่

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

สายเคเบิลใยแก้วนำแสงสามารถแบ่งกว้าง ๆ ออกเป็นสองประเภท ดังนี้



ใยแก้วนำแสงโหมดเดียว (Single-Mode Fiber (SMF)) ประกอบด้วยแกนกลางขนาดเล็กมากและใช้เทคโนโลยีเลเซอร์ที่มีราคาแพงเพื่อส่งลำแสงเดี่ยวออกไป เป็นที่นิยมสำหรับระยะทางไกลทอดยาวหลายร้อยกิโลเมตร เช่น ต้องใช้ในโทรศัพท์ระยะไกล (Long Haul Telephony) และการใช้งานเคเบิลทีวี

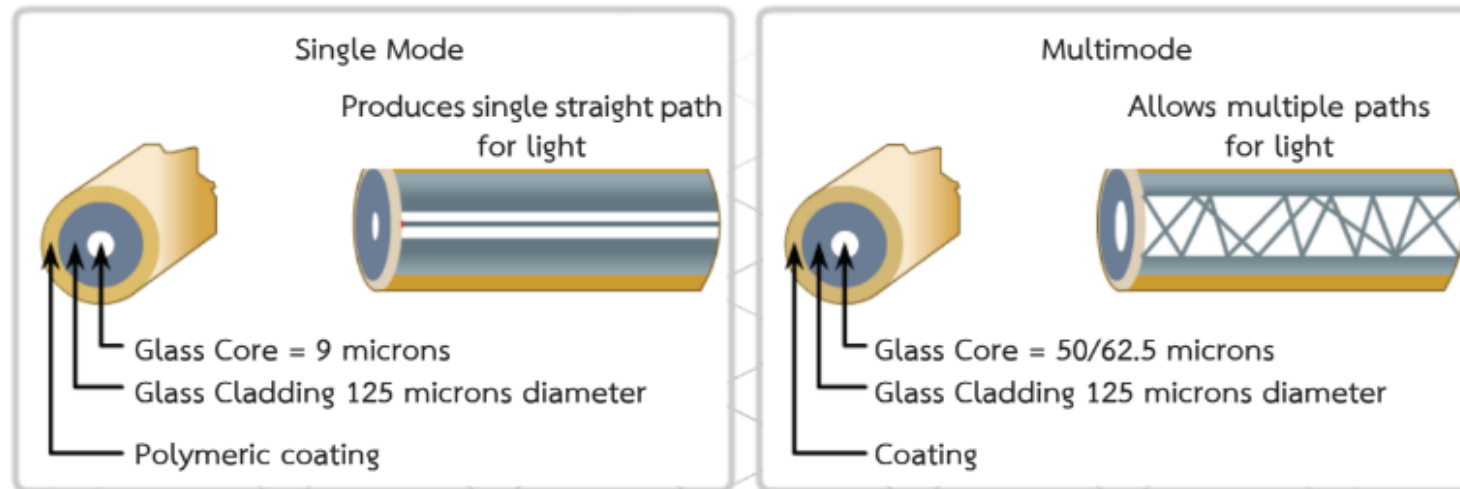


ใยแก้วนำแสงมัลติโหมด (Multimode Fiber (MMF)) ประกอบด้วยแกนกลางขนาดใหญ่และใช้ตัวส่ง LED เพื่อส่งคลื่นแสง โดยแสงจาก LED จะเข้าสู่ใยแก้วนำแสงมัลติโหมดในมุมที่แตกต่างกัน (Different angles) เป็นที่นิยมใน LAN เพราะสามารถใช้ LED ที่ต้นทุนต่ำเป็นตัวกำเนิดแสงได้ และจะให้แบนด์วิดท์ได้ถึง 10 Gbps กับความยาวของการเชื่อมโยงถึง 550 เมตร

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หนึ่งในความแตกต่างระหว่างใยแก้วนำแสงโหมดเดียวและใยแก้วนำแสงมัลติโหมด คือ ปริมาณของการกระจายตัว (Dispersion) โดยการกระจายตัวหมายถึงการแพร่กระจายออกมาจากพัลส์ของแสงในช่วงเวลา ถ้าการกระจายตัวมากขึ้นจะมีการสูญเสียความแรงของสัญญาณมากขึ้นด้วย ดังจะเห็นได้ว่า ใยแก้วนำแสงมัลติโหมดจะมีการกระจายตัวมากกว่าใยแก้วนำแสงโหมดเดียว



รูปที่ 3.20 ลักษณะของใยแก้วนำแสงโหมดเดียวและใยแก้วนำแสงมัลติโหมด (รูปจาก Cisco)

สื่อกลางเครือข่ายคอมพิวเตอร์

1. สื่อกลางประเภทมีสาย

หัวต่อสายใยแก้วนำแสง (Fiber optic connector) มีด้วยกันหลากหลายรูปแบบ บางส่วนที่ได้รับความนิยมแสดงดังรูป



รูปที่ 3.21 ตัวอย่างบางส่วนของหัวต่อสายใยแก้วนำแสง (Fiber optic connector)

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

2.1 สัญญาณไมโครเวฟ (Microwave)

เป็นสื่อกลางในการสื่อสารที่มีความเร็วสูง การส่งข้อมูลโดยอาศัยสัญญาณไมโครเวฟ ซึ่งเป็นสัญญาณคลื่นแม่เหล็กไฟฟ้าไปในอากาศพร้อมกับข้อมูลที่ต้องการส่งจะต้องมีสถานีที่ทพหน้าที่ส่งและรับข้อมูล เนื่องจากสัญญาณไมโครเวฟจะเดินทางเป็นเส้นตรงไม่มีสิ่งกีดขวางเส้นสายตา (Line-of-sight) ไม่สามารถเลี้ยวหรือโค้งตามขอบโลกที่มีความโค้งได้ จึงต้องมีสถานีรับส่งข้อมูลเป็นระยะ ๆ ส่งข้อมูลต่อกันเป็นทอด ๆ ระหว่างสถานีต่อสถานีจนกว่าจะถึงสถานีปลายทาง แต่ละสถานีจะตั้งอยู่ในที่สูง เช่น ดาดฟ้าตึกสูงหรือยอดดอยเพื่อหลีกเลี่ยงสิ่งกีดขวางจากแนวการเดินทางที่เป็นเส้นตรงของสัญญาณดังที่กล่าวมาแล้ว การส่งข้อมูลด้วยสื่อกลางชนิดนี้เหมาะกับการส่งข้อมูลในพื้นที่ห่างไกลมาก ๆ และทุรกันดาร

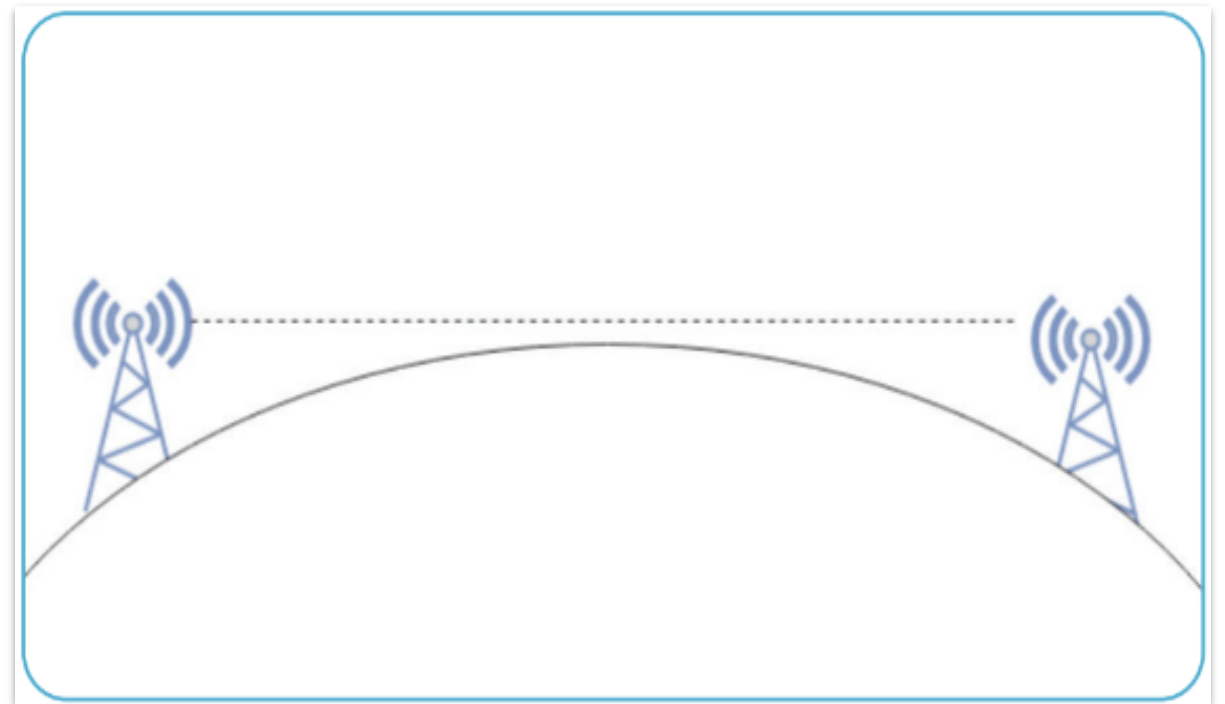


สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย



รูปที่ 3.22 จานรับส่งไมโครเวฟ (Microwave)



รูปที่ 3.23 การรับส่งไมโครเวฟ (Microwave)
ที่ต้องถ่ายทอดสัญญาณจากที่สูง

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

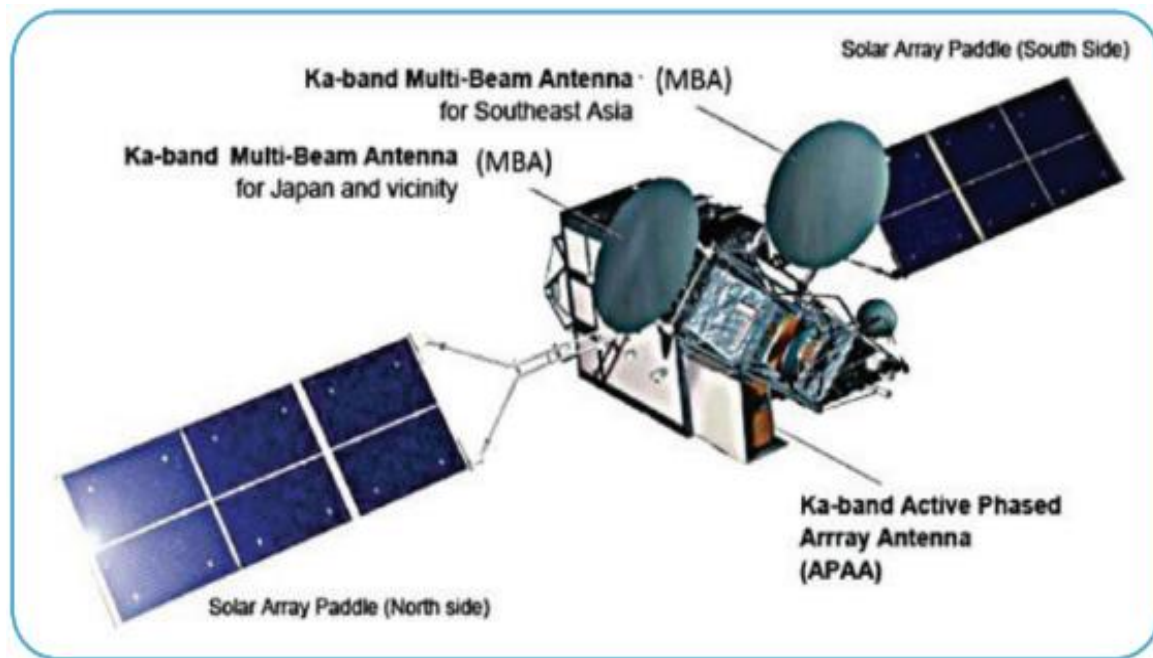
2.2 ดาวเทียม (Satellite)



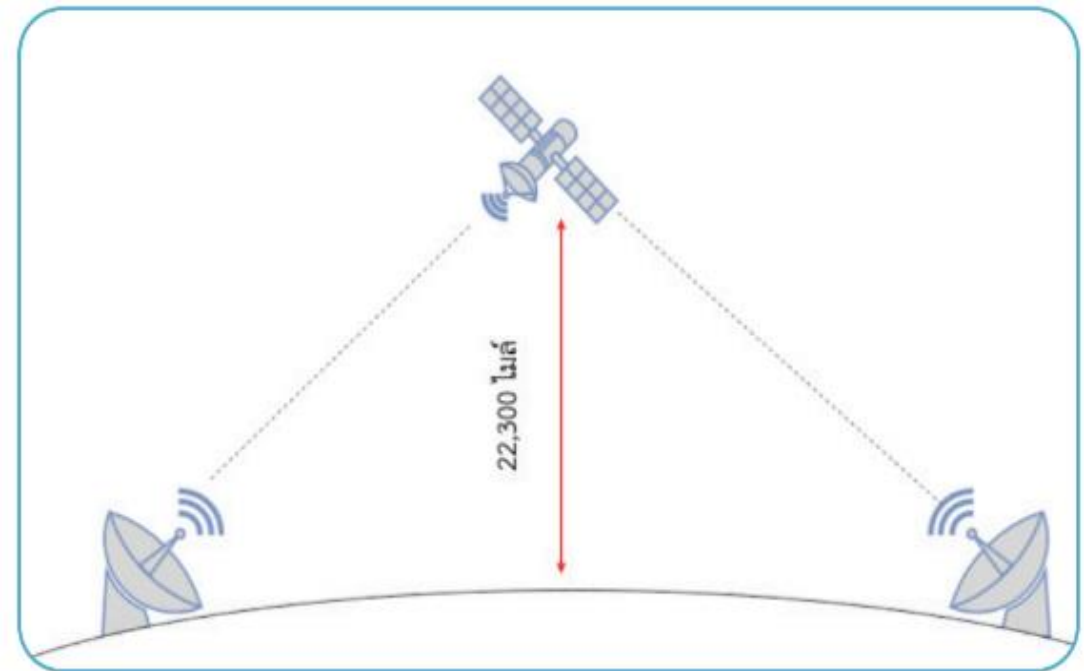
ได้รับการพัฒนาขึ้นมาเพื่อหลีกเลี่ยงข้อจำกัดของสถานีรับส่งไมโครเวฟบนผิวโลก การสร้างดาวเทียมเพื่อเป็นสถานีรับส่งสัญญาณไมโครเวฟบนอวกาศและทวนสัญญาณในแนวโคจรของโลก ในการส่งสัญญาณดาวเทียมจะต้องมีสถานีภาคพื้นดินทำหน้าที่รับและส่งสัญญาณขึ้นไปบนดาวเทียมที่โคจรอยู่สูงจากพื้นโลก 22,300 ไมล์ (หรือ 35,888.371 กิโลเมตร) โดยดาวเทียมเหล่านั้นจะเคลื่อนที่ด้วยความเร็วที่เท่ากับการหมุนของโลก จึงเสมือนกับดาวเทียมนั้นอยู่นิ่งอยู่กับที่ ขณะที่โลกหมุนรอบตัวเอง ทำให้การส่งสัญญาณไมโครเวฟจากสถานีหนึ่งขึ้นไปบนดาวเทียมและการกระจายสัญญาณจากดาวเทียมลงมายังสถานีตามจุดต่าง ๆ บนผิวโลกเป็นไปอย่างแม่นยำ ดาวเทียมสามารถโคจรอยู่ได้โดยอาศัยพลังงานที่ได้มาจากการเปลี่ยนพลังงานแสงอาทิตย์ด้วยแผงโซลาร์ (Solar panel)

สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย



รูปที่ 3.24 ส่วนประกอบพื้นฐานดาวเทียม
เพื่อการสื่อสาร



รูปที่ 3.25 ลักษณะการส่งสัญญาณของ
ดาวเทียมเพื่อการสื่อสาร

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

2.3 อินฟราเรด (Infrared หรือ I.R.)



การติดต่อสื่อสารข้อมูลโดยใช้คลื่นแสงอินฟราเรด มีลักษณะคล้ายกับการสื่อสารด้วยคลื่นไมโครเวฟ จึงต้องหันตัวรับและตัวส่งให้ตรงกันและไม่มีสิ่งกีดขวางเส้นสายตา (Line-of-sight) หรือขวางแสงอินฟราเรดการสื่อสารด้วยอินฟราเรดใช้ได้ในระยะทางที่ไม่ไกลนัก

ก่อนหน้านี้มีคอมพิวเตอร์และอุปกรณ์จำนวนมากที่สามารถใช้คลื่นแสงอินฟราเรดสื่อสารข้อมูลกันได้ เช่น คอมพิวเตอร์ โน้ตบุ๊ก คอมพิวเตอร์แบบพกพา เป็นต้น ซึ่งอุปกรณ์เหล่านี้ จะมีพอร์ต “IrDA (The Infrared Data Association)” สำหรับเชื่อมต่ออุปกรณ์ด้วยอินฟราเรด หรือสามารถซื้ออุปกรณ์ USB เป็น IrDA (USB to IrDA adapter) มาใช้งานได้

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย



แต่เนื่องจากข้อจำกัดในเรื่องระยะทาง ความเร็ว และต้องไม่มีอะไรมาบังเส้นทางส่งข้อมูลการใช้งาน อินฟราเรดในคอมพิวเตอร์จึงไม่เป็นที่นิยม แต่คุณสมบัติดังกล่าวกลับเป็นข้อดีและเหมาะสมในอุปกรณ์บางประเภท เช่น Remote Control ต่าง ๆ เพราะถ้าใช้การสื่อสารอื่น เช่น คลื่นวิทยุ ซึ่งไม่สามารถควบคุมทิศทางหรือมีอำนาจทะลุทะลวงกำแพงก็จะทำให้เกิดความผิดพลาดในการสั่งการ ลองนึกภาพถึงห้องติดกันที่มีโทรทัศน์ห้องละเครื่อง ถ้า Remote Control ห้องหนึ่งเปลี่ยนช่องแล้วสัญญาณควบคุมทะลุไปอีกห้องหนึ่งอาจจะทำให้สัญญาณเกิดการรบกวนกัน เช่นเดียวกับการปรับอุณหภูมิเครื่องปรับอากาศถ้าปรับตัวหนึ่งแล้วอีกห้องหนึ่งอุณหภูมิเปลี่ยนไปอาจไม่เหมาะสม

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

ตั้งขึ้นการสื่อสารด้วย Infrared ในปัจจุบันจึงนิยมใช้เฉพาะอุปกรณ์ประเภท Remote Control และเป็นการสื่อสารทางเดียวเป็นหลัก



รูปที่ 3.26 การสื่อสารด้วยแสงอินฟราเรด

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

2.4 สัญญาณวิทยุ (Wi-Fi)



เป็นเทคโนโลยีที่ได้รับความนิยมที่ช่วยอุปกรณ์อิเล็กทรอนิกส์ในการแลกเปลี่ยนข้อมูลหรือการเชื่อมต่ออินเทอร์เน็ตแบบไร้สายโดยใช้คลื่นวิทยุ คำว่า “Wi-Fi” เป็นเครื่องหมายการค้าของ Wi-Fi Alliance ที่ให้คำนิยามของวายเป็นว่าหมายถึง “ชุดผลิตภัณฑ์ใด ๆ ที่สามารถทำงานได้ตามมาตรฐานเครือข่ายคอมพิวเตอร์แบบไร้สาย (แลนไร้สาย) ซึ่งอยู่บนมาตรฐาน IEEE 802.11” อย่างไรก็ตาม เนื่องจากแลนไร้สายที่ทันสมัยส่วนใหญ่จะขึ้นอยู่กับมาตรฐานเหล่านี้ คำว่า “วายฟาย” จึงนำมาใช้ในภาษาอังกฤษทั่วไปสำหรับ “แลนไร้สาย” เดิมทีวายฟายออกแบบมาใช้สำหรับอุปกรณ์พกพาต่าง ๆ และใช้เครือข่ายแลนเท่านั้น แต่ปัจจุบันนิยมใช้วายฟายเพื่อต่อกับอินเทอร์เน็ต

สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย

โดยเฉพาะอย่างยิ่งอุปกรณ์พกพาต่าง ๆ เช่น คอมพิวเตอร์ส่วนบุคคล เครื่องเล่นเกม สมาร์ทโฟน แท็บเล็ต กล้องดิจิทัล และเครื่องเสียงดิจิทัล สามารถเชื่อมต่อกับอินเทอร์เน็ตได้ผ่านอุปกรณ์ที่เรียกว่า จุดเข้าถึงหรือแอ็กเซสพอยต์ (Access Point) หรือ ฮอตสปอต (Hotspot) และบริเวณที่ระยะทำการของ แอ็กเซสพอยต์ครอบคลุมอยู่ที่ประมาณ 45 ถึง 100 เมตร ในอาคาร (ขึ้นอยู่กับมาตรฐานและประเภทของ แอ็กเซสพอยต์) แต่จะมีระยะครอบคลุมที่มากกว่าหากเป็นพื้นที่โล่ง ในปัจจุบันมีการกำหนดมาตรฐานการเชื่อมต่อแบบต่าง ๆ เพื่อให้เหมาะสมกับเทคโนโลยีและการเลือกใช้งาน



สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย

ในการใช้งานฮอตสปอตตามจุดต่าง ๆ เช่น โรงแรม ร้านกาแฟ สนามบิน ผู้ใช้งานสามารถเชื่อมต่อเครือข่ายไร้สายได้เลย ซึ่งอาจเรียกฮอตสปอตแบบนี้ว่า Open Network หรืออาจมีการใส่ผู้ใช้และรหัสผ่านบนหน้าเว็บเรียกว่า Captive Portal หรือหน้า Internet Login ของผู้ให้บริการอินเทอร์เน็ต เพื่อใช้งานอินเทอร์เน็ตผ่านการพิสูจน์สิทธิ์ (Authentication)

อย่างไรก็ตาม ข้อมูลที่ส่งผ่านฮอตสปอตนั้นอาจถูกดักจับได้ เนื่องจากไม่ได้มีการเข้ารหัสข้อมูล (Data Encryption) ดังนั้น จึงต้องพึงระวังในการใช้งานฮอตสปอตสาธารณะ



สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

หากผู้ใช้งานต้องการเปิดใช้ฮอตสปอตของตนเองหรือเชื่อมต่อกับแอคเซสพอยต์ การเพิ่มความมั่นคงปลอดภัยในการใช้งานฮอตสปอต ต้องมีการเข้ารหัสข้อมูลที่วิ่งระบบเครือข่ายไร้สายนี้ เช่น

- 👤 WEP เป็นการเข้ารหัสแบบเก่า ที่ถูกถอดรหัสได้ง่ายที่สุด ควรหลีกเลี่ยงการใช้งาน

- 👤 WPA/TKIP หรือเรียกว่า WEP Enhanced เป็นการเข้ารหัสแบบเก่า ไม่แนะนำให้ใช้เช่นกัน

- 👤 WPA2/AES เป็นมาตรฐานการเข้ารหัสที่ใช้งานกันอยู่ในปัจจุบันสามารถถูกแฮ็กได้ แต่ต้องใช้เวลาค่อนข้างมากในการแฮ็ก

สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย

 WPA3 มาตรฐานการเข้ารหัสแบบใหม่ล่าสุด ที่มีความมั่นคงปลอดภัยมากที่สุด หากมี WPA3 ให้เลือกใช้ ผู้ใช้งานควรเลือกใช้งาน

 WPS (Wi-Fi Protected Setup) เป็นรูปแบบการเชื่อมต่อที่ทำให้แอคเซสพอยต์ที่มีปุ่ม WPS กับอุปกรณ์ Wi-Fi ที่มีปุ่ม WPS เช่นกัน สามารถเชื่อมต่อกันได้ทันทีโดยไม่ต้องใส่รหัสผ่าน (หากอุปกรณ์ที่ไม่มีปุ่ม WPS ต้องใส่รหัสเช่นเดิม นอกจากนี้ อาจต้องใส่รหัส WPS ที่ไม่ใช้รหัสผ่านที่ผู้ใช้งานตัวเองเพิ่มอีกด้วย)

อย่างไรก็ตาม การใช้งาน WPS มีช่องโหว่จากรหัส WPS ของแอคเซสพอยต์ที่มี 8 หลัก ทำให้ผู้ไม่ประสงค์ดีสามารถใช้โปรแกรมเดาสุ่มรหัส WPS โดยใช้เวลานานนัก หากไม่จำเป็นต้องใช้ WPS ผู้ใช้งานควรปิดฟังก์ชันการทำงานของ WPS

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

2.5 สัญญาณบลูทูธ (Bluetooth)



เป็นข้อกำหนดสำหรับอุตสาหกรรมเครือข่ายส่วนบุคคล (Personal Area Networks - PAN) แบบไร้สายบลูทูธช่วยให้อุปกรณ์อิเล็กทรอนิกส์สามารถเชื่อมต่อกันได้ เช่น โทรศัพท์มือถือ พีดีเอ คอมพิวเตอร์ส่วนบุคคล โดยผ่านทางสัญญาณบลูทูธนี้ ชื่อบลูทูธมาจากพระนามพระเจ้าฮารัลด์ บลูทูธ ของประเทศเดนมาร์กเพื่อเป็นการรำลึกถึงกษัตริย์บลูทูธผู้ปกครองประเทศกลุ่มสแกนดิเนเวีย ระบบบลูทูธถูกสร้างขึ้นมาเพื่อใช้กับโทรศัพท์มือถือ และเริ่มต้นจากประเทศในแถบนี้ บลูทูธจะใช้สัญญาณวิทยุความถี่สูง 2.4 GHz (จิกะเฮิรตซ์ (Gigahertz))

สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย

แต่จะแยกย่อยออกไปตามแต่ละประเทศ อย่างในแถบยุโรปและอเมริกาจะใช้ช่วง 2.400 ถึง 2.4835 GHz แบ่งออกเป็น 79 ช่องสัญญาณ และจะใช้ช่องสัญญาณที่แบ่งเพื่อส่งข้อมูลสลับช่องไปมา 1,600 ครั้งต่อ 1 วินาที ส่วนที่ญี่ปุ่นจะใช้ความถี่ 2.402 ถึง 2.480 GHz แบ่งออกเป็น 23 ช่องระยะทำการของบลูทูธจะอยู่ที่ 5-100 เมตร มีการป้องกันความมั่นคงปลอดภัย (Security) การสื่อสารโดยใช้การป้อนรหัสก่อนการเชื่อมต่อ และป้องกันการดักสัญญาณระหว่างสื่อสารโดยระบบจะสลับช่องสัญญาณไปมา และจะเลือกเปลี่ยนความถี่ที่ใช้อยู่ในการติดต่อเองอัตโนมัติ โดยไม่จำเป็นต้องเรียงตามหมายเลขช่องทำให้การดักฟังหรือลักลอบขโมยข้อมูลทำได้ยากขึ้น



สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย

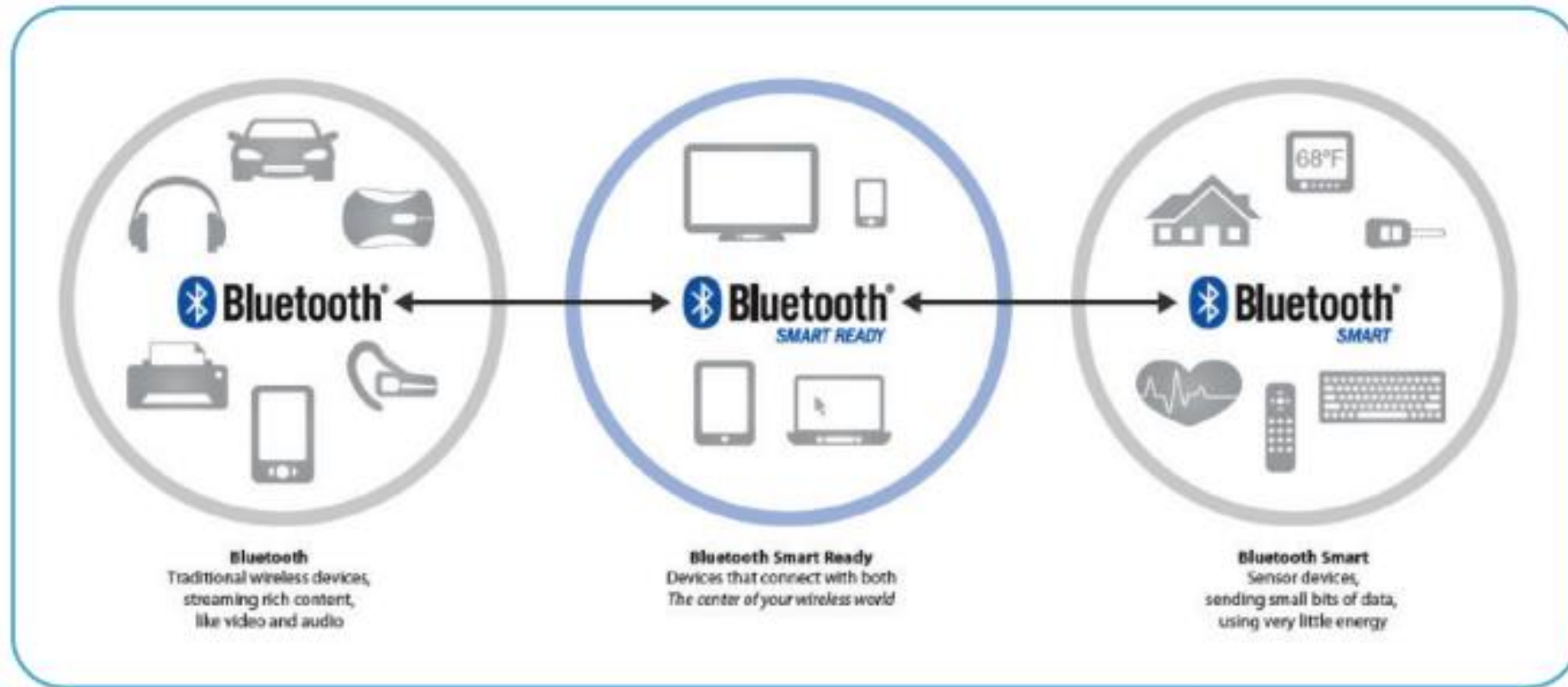
บลูทูธถูกออกแบบมาเพื่อใช้กับอุปกรณ์ที่มีขนาดเล็กเนื่องจากการขนส่งข้อมูลในจำนวนที่ไม่มาก อย่างเช่น ไฟล์ภาพ เสียง แอปพลิเคชันต่าง ๆ และสามารถเคลื่อนย้ายได้ง่ายเพียงอยู่ในระยะที่กำหนดไว้เท่านั้น (ประมาณ 5-100 เมตร) นอกจากนี้ยังใช้พลังงานต่ำกินไฟน้อยและสามารถใช้งานได้นาน โดยไม่ต้องนำไปชาร์จไฟบ่อย ๆ ด้วย ข้อกำหนดและคุณสมบัติของบลูทูธแบ่งเป็นรุ่นต่าง ๆ เช่น Bluetooth 4.0 Bluetooth 5.0 เป็นต้น



สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย



รูปที่ 3.27 การเชื่อมต่อสัญญาณบลูทูธ (Bluetooth)

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย

2.6 สัญญาณโทรศัพท์เคลื่อนที่ (Mobile Cellular)

วิวัฒนาการก่อนจะเป็นเทคโนโลยีสื่อสารไร้สาย 4G LTE และ 5G คำว่า G ย่อมาจาก Generation แปลว่า ยุค หรือช่วงสมัย ไม่ได้หมายถึงชื่อของเทคโนโลยี

 ยุค 1G (1st Generation) เป็นยุคที่ใช้ระบบแอนะล็อก (Analog) คือใช้สัญญาณวิทยุในการส่งคลื่นเสียง (Voice) โดยสามารถโทรออก-รับสายได้อย่างเดียว ไม่สามารถส่งผ่านข้อมูลใด ๆ ได้ทั้งสิ้น

 ยุค 2G (2nd Generation) เป็นยุคที่เปลี่ยนจากการส่งคลื่นวิทยุแบบแอนะล็อก (Analog) เป็นการเข้ารหัสดิจิทัล (Digital) แทน โดยผู้ใช้สามารถใช้งานทางด้านข้อมูล คือ สามารถส่งข้อความ SMS ได้นอกจากการโทรออก-รับสาย

สื่อกลางเครือข่ายคอมพิวเตอร์

2. สื่อกลางประเภทไร้สาย

 ยุค 3G (3rd Generation) เทคโนโลยีการสื่อสารในยุคที่ 3 เป็นยุคที่เริ่มแข่งขันเรื่องความเร็วในการเชื่อมต่อและการรับส่งข้อมูล โดยเน้นการเชื่อมต่อแบบไร้สายด้วยความเร็วสูง เพื่อรองรับการใช้งานกับอุปกรณ์สมัยใหม่ทำให้สามารถใช้งานด้านมัลติมีเดียสามารถส่งข้อมูลทั้งภาพและเสียงในระบบไร้สายด้วยความเร็วที่สูง ทำให้เกิดการใช้งานที่หลากหลาย ไม่ว่าจะเป็นการสนทนาผ่านวิดีโอคอล หรือดูหนังฟังเพลงผ่านอินเทอร์เน็ต

 ยุค 4G (4th Generation) เป็นมาตรฐานการสื่อสารด้วยอุปกรณ์ไร้สายขั้นต่ำในปัจจุบันสำหรับทั่วโลก เพราะในปัจจุบันกำลังก้าวไปสู่ยุค 5G โดยยุค 4G ระบบการสื่อสารด้วยมือถือสามารถรับส่งข้อมูลได้ปริมาณสูงในระดับหลายร้อยเมกะบิตต่อวินาที ทำให้การใช้งานเครือข่ายไร้สายทำได้อย่างสะดวกรวดเร็วในทุกที่ทุกเวลา (Anytime Anywhere) จนเกิดการเปลี่ยนแปลงพฤติกรรมของผู้บริโภคทั่วโลก ทั้งในด้านการรับชมสื่อแบบออนไลน์ สตรีมมิง การประชุม การทำงานทางไกล

สื่อกลางเครือข่ายคอมพิวเตอร์

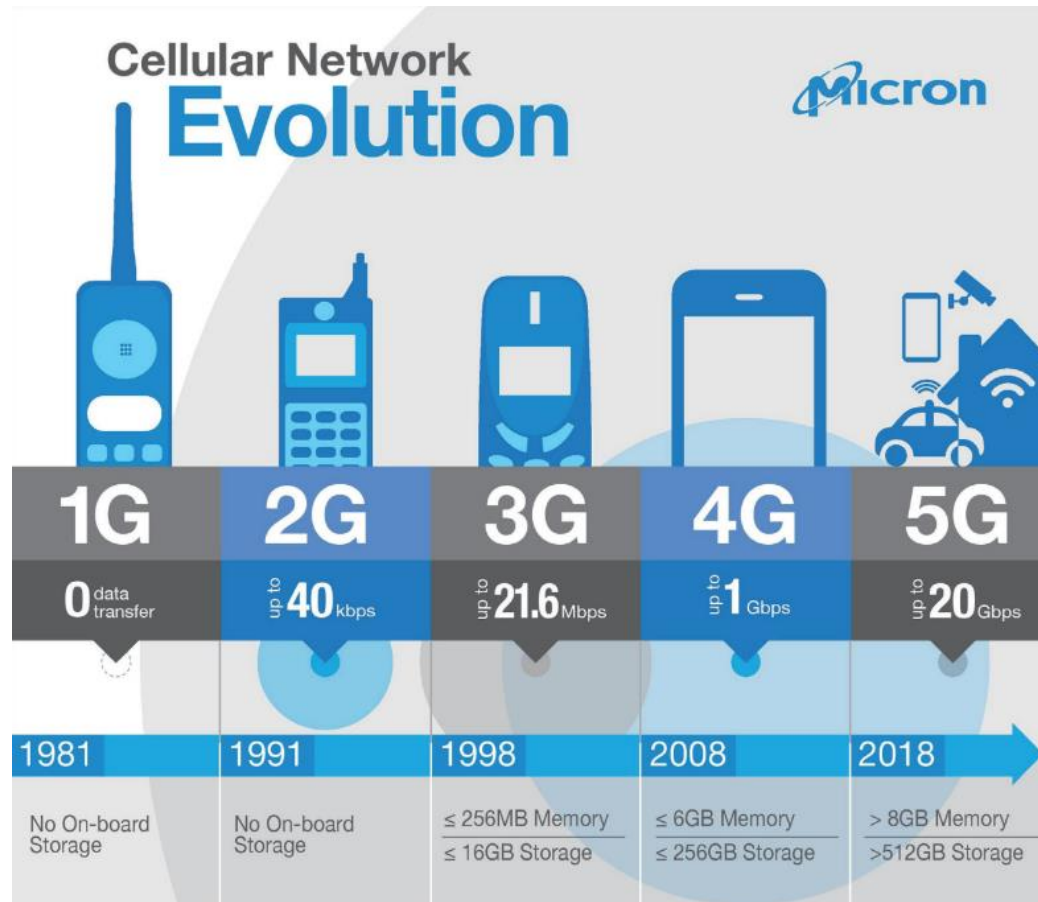
2. สื่อกลางประเภทไร้สาย

 ยุค 5G (5th Generation) สิ่งที่แตกต่างกันระหว่างยุค 4G สู่ยุค 5G นอกจากความเร็วในการรับส่งข้อมูลแล้ว 5G จะเน้นเรื่องความเร็วในการตอบสนองโดยลดเวลาหน่วง (Latency) ของการสื่อสารให้น้อยลงมาก ๆ เมื่อเทียบกับยุค 4G เพราะเป็นสิ่งจำเป็นต่อการพัฒนาระบบอัตโนมัติต่าง ๆ ที่จะเกิดขึ้น เช่น ระบบการควบคุมระยะไกลสำหรับพาหนะ การผ่าตัดระยะไกลที่เครื่องมือผ่าตัด ซึ่งถูกควบคุมด้วยแพทย์จะต้องทำงานตอบสนองให้แพทย์ได้อย่างรวดเร็วและแม่นยำ เป็นต้น

สื่อกลางเครือข่ายคอมพิวเตอร์

2.

สื่อกลางประเภทไร้สาย



รูปที่ 3.28 วิวัฒนาการของมือถือในแต่ละ Generation

สื่อกลางเครือข่ายคอมพิวเตอร์

3. หลักการพิจารณาการใช้สื่อกลาง

ตัวกลางหรือสื่อกลาง เป็นส่วนที่ทำให้เกิดการเชื่อมต่อระหว่างคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ในระบบเครือข่ายเข้าด้วยกันเพื่อส่งข้อมูลจากผู้ส่งไปสู่ผู้รับ โดยสื่อกลางที่ใช้ในการสื่อสารข้อมูลมีอยู่หลายประเภทแต่ละประเภทมีคุณสมบัติที่มีความแตกต่างกัน ไม่ว่าจะเป็นความเร็วและปริมาณข้อมูลที่สามารถรับส่งถึงกันได้ระยะทางที่สามารถรับส่งข้อมูลกันโดยมีประสิทธิภาพสูงสุด และต้นทุนในการใช้สื่อกลางประเภทต่าง ๆ หลักการเลือกสื่อกลางการสื่อสารข้อมูลที่เหมาะสมจะต้องคำนึงถึงปัจจัยต่าง ๆ ดังนี้



สื่อกลางเครือข่ายคอมพิวเตอร์

3.

หลักการพิจารณาการใช้สื่อกลาง

3.1 ความเร็วที่สื่อกลางนั้นสามารถรับส่งข้อมูลได้ (Speed)

โดยไม่จำเป็นจะต้องเป็นสื่อกลางที่มีความเร็วสูงสุด แต่ต้องมีความเร็วเพียงพอต่อการทำงาน และตอบสนองความต้องการของผู้ใช้ได้ เช่นการถ่ายทอดสด (Live) ผ่านสื่อสังคมออนไลน์ การรับชมภาพยนตร์จากบริการสตรีมมิงต่าง ๆ อาจจะไม่ต้องการความเร็วที่สูงมาก แต่ต้องการความเร็วที่คงที่สม่ำเสมอ ซึ่งความเร็วสำหรับการรับชมภาพยนตร์ Full HD ทั่วไปสามารถเริ่มต้นที่ 10 เมกะบิตต่อวินาที หรือการใช้งานควบคุมระบบอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things : IoT) อาจจะไม่ต้องการความเร็วสูง เพราะเป็นแค่คำสั่งเปิดปิดอุปกรณ์ แต่ถ้าเป็นการรับส่งไฟล์งานสำหรับองค์กร ก็อาจจำเป็นจะต้องมีความเร็วในการรับส่งข้อมูลสูงมากที่สุดเท่าที่จะมีงบประมาณ



สื่อกลางเครือข่ายคอมพิวเตอร์

3.

หลักการพิจารณาการใช้สื่อกลาง

3.2 เวลาหน่วง (Latency)



เวลาส่วนต่างระหว่างที่ข้อมูลเข้าไปประมวลผลในอุปกรณ์จนถึงออกมาจากอุปกรณ์ หรือบางทีที่หลาย ๆ คนอาจเรียกหรือเข้าใจว่า ความเร็วในการตอบสนอง (Response Time) ปัจจุบันมีการพัฒนาอุปกรณ์ที่ใช้การควบคุมระยะไกลที่จำเป็นจะต้องรับคำสั่งและทำงานด้วยความรวดเร็ว เช่น การควบคุมเครื่องจักร การผ่าตัดด้วยหุ่นยนต์ หรือแม้แต่การทำกิจกรรมบางประเภท เช่น การเล่นเกมออนไลน์ ต้องการการตอบสนองที่รวดเร็วของข้อมูล ดังนั้นในการเลือกใช้สื่อกลางต้องคำนึงถึงเรื่องความเร็วในการตอบสนองด้วยเช่นกัน ซึ่งการพัฒนาระบบ 5G จะเน้นในเรื่องนี้เป็นพิเศษ

สื่อกลางเครือข่ายคอมพิวเตอร์

3.

หลักการพิจารณาการใช้สื่อกลาง

3.3 สภาพแวดล้อมและระยะทาง (Environment and Distance)



เนื่องจากสื่อกลางที่ใช้ในการรับส่งข้อมูลแต่ละประเภทมีข้อดี ข้อเสีย และคุณสมบัติเฉพาะที่แตกต่างกัน ดังนั้นการเลือกใช้ต้องคำนึงถึงสิ่งเหล่านี้ด้วย เช่น ในโรงงานที่มีการรบกวนจากคลื่นแม่เหล็กไฟฟ้ามีพนักงันการใช้สื่อกลางแบบไร้สาย หรือแม้แต่วีลอสกลางที่มีสายเป็นทองแดงอาจจะเกิดปัญหาสัญญาณรบกวนได้ จึงจำเป็นจะต้องใช้สื่อกลางประเภทใยแก้วนำแสง ซึ่งจะไม่มีการรบกวนจากปัจจัยเหล่านี้ แต่มีราคาสูงกว่าและไม่สะดวกในการขยายระบบ เป็นต้น และหากระยะระหว่างตัวรับส่งข้อมูลมีระยะทางที่ไกลมาก ผู้ออกแบบระบบต้องพิจารณาถึงตัวทวนสัญญาณหรือรีพีตเตอร์ (Repeater) คือการนำสื่อกลางหลายประเภทมาใช้ร่วมกันเช่น การใช้ฮับ (Hub) สวิตช์ (Switch) เป็นต้น

สื่อกลางเครือข่ายคอมพิวเตอร์

3.

หลักการพิจารณาการใช้สื่อกลาง

3.4 ความมั่นคงปลอดภัยและเสถียรภาพการทำงานของระบบ (Security & Reliability)

ระบบการสื่อสารข้อมูลคอมพิวเตอร์เรียกได้ว่าเป็นหัวใจของการทำงานในแทบทุกองค์กร แม้แต่การดำเนินชีวิตของบุคคลธรรมดาทั่วไปการเลือกใช้สื่อกลางที่เหมาะสมมีความมั่นคงปลอดภัย สูงทั้งจากการถูกขโมยข้อมูลหรือการถูกทำลายให้เสียหายก็เป็นสิ่งจำเป็น และหากเป็นระบบสำคัญ ควรจะมีช่องทางหรือตัวกลางการสื่อสารสำรอง กรณีที่สื่อกลางหลักเสียหาย



สื่อกลางเครือข่ายคอมพิวเตอร์

3.

หลักการพิจารณาการใช้สื่อกลาง

3.5 ต้นทุน (Cost)

การออกแบบระบบสื่อสารข้อมูลย่อมต้องการระบบที่มีความเร็วและคุณสมบัติสูงสุดเท่าที่จะทำได้ แต่ต้องคำนึงถึงความคุ้มค่าในการลงทุนให้เหมาะสมด้วย เช่น การซื้อแพ็คเกจที่มีความเร็วสูงเกินไปโดยไม่จำเป็น หรือการเลือกใช้อุปกรณ์ สาย หรือโครงสร้างพื้นฐานที่ราคาสูงเกินไป นอกจากนี้ผู้ให้บริการอินเทอร์เน็ตส่วนใหญ่มักจะกำหนดความเร็วในการรับส่งข้อมูลที่แตกต่างกัน เพื่อให้ผู้ใช้สามารถกำหนดงบประมาณได้เหมาะสมกับการทำงานด้วย เช่น ผู้ใช้ตามบ้านอาจจะใช้ความเร็วด้านรับหรือดาวน์โหลด (Download) ที่ 1,000 เมกะบิตต่อวินาที ด้านส่งหรืออัปโหลด (Upload) แค่ 100 เมกะบิตต่อวินาทีก็เพียงพอ เพราะส่วนใหญ่จะใช้ดูหรือโหลดข้อมูล ไม่ค่อยได้ส่งไฟล์ขนาดใหญ่เท่าไร เป็นต้น



สื่อกลางเครือข่ายคอมพิวเตอร์



สรุปท้ายหน่วย

การใช้งานระบบเครือข่ายถือเป็นเรื่องจำเป็นสำหรับองค์กรรวมถึงการใช้งานภายในบ้านโดยเทคโนโลยีในปัจจุบันทำให้ประสิทธิภาพการทำงานของอุปกรณ์สูงขึ้นในราคาและขนาดที่เล็กลงอย่างไรก็ตามการเข้าใจคุณสมบัติและความสามารถของอุปกรณ์แต่ละประเภท แต่ละรุ่นยังมีความจำเป็นสำหรับผู้ใช้งาน โดยเฉพาะในสำนักงาน ถึงแม้เทคโนโลยีจะก้าวหน้ามากขึ้นเรื่อย ๆ เราไม่จำเป็นจะต้องเลือกใช้เทคโนโลยีล่าสุดหรือดีที่สุด เพราะอาจจะมีราคาสูงและเกินความจำเป็น สื่อกลางที่ใช้สำหรับระบบเครือข่ายเป็นเรื่องที่หลายคนมองข้าม แต่ในความเป็นจริงแล้วมีความสำคัญในการออกแบบระบบเครือข่ายเป็นอย่างมาก ทั้งในด้านราคาและความเหมาะสมกับงาน เช่น การเดินสายแลนที่ราคาเมตรละไม่กี่สิบบาทสามารถทำงานได้ดีกว่าการใช้ Wireless Access Point ราคาเป็นหมื่นบาท แต่อาจจะไม่สวยงามหรือไม่เหมาะสมกับบางพื้นที่ เป็นต้น ดังนั้นเพื่อให้สามารถเลือกใช้เทคโนโลยีที่เหมาะสมกับงานและงบประมาณมากที่สุด จึงต้องศึกษาและทำความเข้าใจกับสื่อกลางการสื่อสารข้อมูลด้วยเช่นกัน



อุปกรณ์ระบบเครือข่าย
คอมพิวเตอร์และตัวกลาง
การเชื่อมต่อเครือข่ายคอมพิวเตอร์

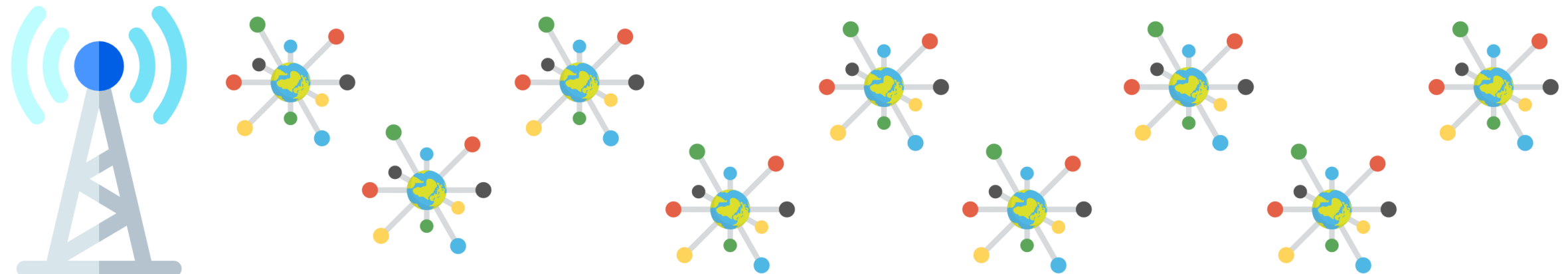


อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

ในระบบเครือข่ายคอมพิวเตอร์จะประกอบไปด้วยอุปกรณ์ต่าง ๆ ที่ถูกนำมาเชื่อมต่อกันมากมาย เพื่อให้สามารถทำงานรวมกันได้ ยิ่งระบบเครือข่ายคอมพิวเตอร์มีขนาดใหญ่ยิ่งมีจำนวนอุปกรณ์และประเภทอุปกรณ์ที่หลากหลาย ซึ่งสามารถแบ่งออกได้เป็น 3 ประเภท ดังนี้



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.1 เครือข่ายคอมพิวเตอร์ (Computer Network)

คือ อุปกรณ์ที่ผู้ใช้ใช้งานโดยตรง อุปกรณ์เหล่านี้เป็นอินเทอร์เน็ตเฟสหรือการเชื่อมต่อระหว่างมนุษย์และระบบเครือข่ายคอมพิวเตอร์ ตัวอย่างบางส่วนของอุปกรณ์ปลายทาง เช่น

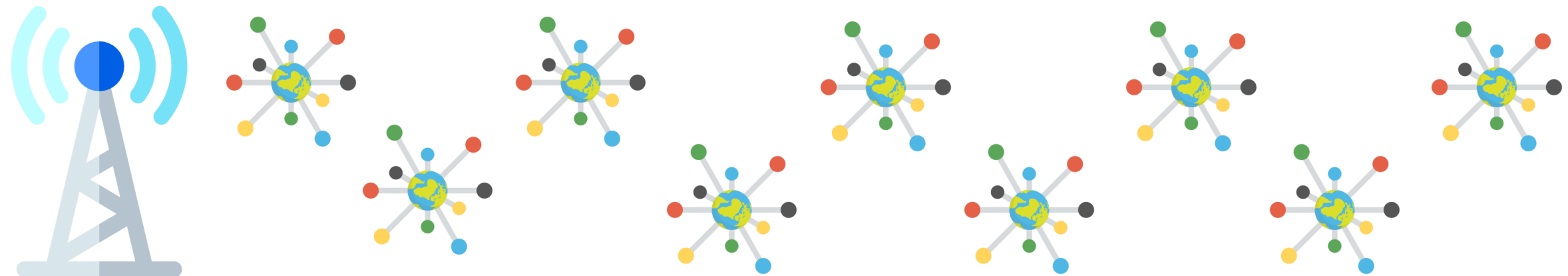
-  คอมพิวเตอร์
-  เครื่องพิมพ์เครือข่าย
-  โทรศัพท์
-  กล้องรักษาความมั่นคงปลอดภัย
-  อุปกรณ์มือถือ (เช่น สแกนเนอร์, บาร์โค้ดแบบไร้สาย, PDA)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

ในบริบทของระบบเครือข่าย อุปกรณ์ปลายทางจะเรียกว่า “โฮสต์” (Host) หรือ “โหนด” (Node) อุปกรณ์โฮสต์เป็นทั้งต้นทางหรือปลายทางของข้อมูลที่ถูกส่งผ่านระบบเครือข่าย เพื่อให้แยกความแตกต่างของโฮสต์หนึ่งออกจากอีกโฮสต์ในระบบเครือข่าย แต่ละโฮสต์บนเครือข่ายจะมีการระบุที่อยู่หรือแอดเดรส (Address) เช่น IP address เป็นต้น เมื่อโฮสต์เริ่มต้นการสื่อสารจะใช้แอดเดรสของโฮสต์ปลายทางเพื่อระบุตำแหน่งที่ข้อมูลจะถูกส่งไป



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

โฮสต์สามารถทำหน้าที่เป็นเครื่องลูกข่ายหรือไคลเอนต์ (Client) เครื่องแม่ข่ายหรือเซิร์ฟเวอร์ (Server) หรือทั้งสองอย่าง โดยซอฟต์แวร์ที่ติดตั้งบนโฮสต์จะกำหนดบทบาทที่จะเป็นของโฮสต์บนระบบเครือข่าย เซิร์ฟเวอร์เป็นโฮสต์ที่มีซอฟต์แวร์ที่ใช้ในการติดตั้งที่ช่วยให้โฮสต์เหล่านั้นสามารถที่จะให้ข้อมูลและการบริการ เช่น อีเมลหรือเว็บเพจให้กับโฮสต์อื่นในระบบเครือข่าย ส่วนไคลเอนต์เป็นโฮสต์ที่ได้ติดตั้งซอฟต์แวร์ที่ช่วยให้โฮสต์เหล่านั้นสามารถขอและแสดงข้อมูลที่ได้รับจากเซิร์ฟเวอร์ ซึ่งหน่วยการเรียนรู้นี้จะอธิบายเพิ่มเติมเฉพาะคอมพิวเตอร์เท่านั้น เนื่องจากเป็นอุปกรณ์ที่ผู้ใช้งานมีความคุ้นเคยและมีโอกาสใช้งานบ่อยที่สุด



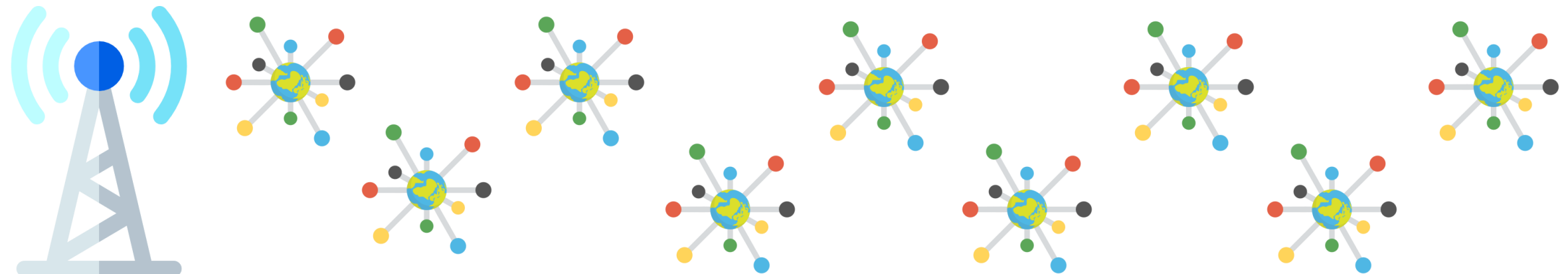
อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

เครื่องเซิร์ฟเวอร์ คือ เครื่องคอมพิวเตอร์ที่ทำหน้าที่ให้บริการอย่างใดอย่างหนึ่งหรือหลายอย่าง โดยบริการทรัพยากรให้กับเครื่องลูกข่าย เช่น บริการไฟล์ (File Server) การบริการงานพิมพ์ (Print Server) เป็นต้น (ตามที่กล่าวถึงในหน่วยการเรียนรู้ที่ 2)

เครื่องไคลเอนต์ คือ เครื่องลูกข่ายที่ขอใช้บริการจากเครื่องเซิร์ฟเวอร์ ซึ่งเครื่องไคลเอนต์อาจเป็นคอมพิวเตอร์ส่วนบุคคล (PC) หรืออาจเรียกเครื่องไคลเอนต์ว่า สถานีงาน (Workstation หรือ Terminal) ซึ่งหมายถึง

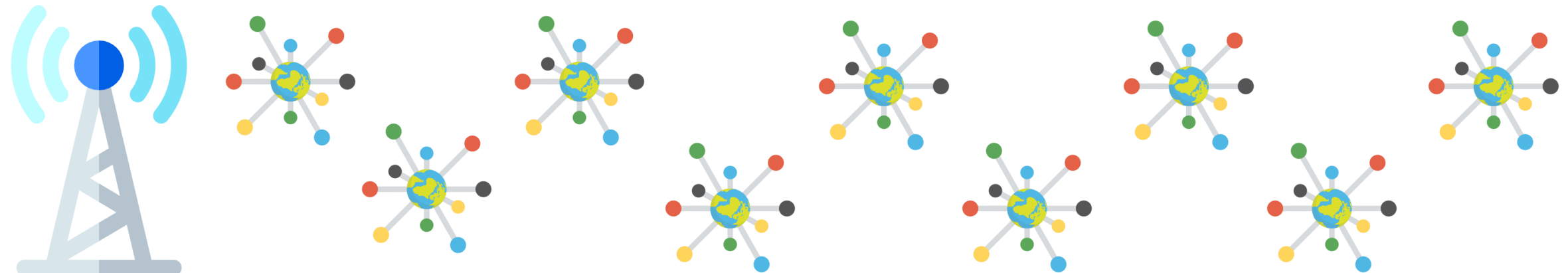


อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

อุปกรณ์หรือเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ทำหน้าที่เป็นสถานีปลายทางหรือสถานีงานที่ได้รับการบริการจากเครื่องคอมพิวเตอร์แม่ข่าย โดยเครื่องเวิร์กสเตชัน (Workstation) มักมีหน่วยประมวลผลหรือซีพียูของตัวเอง ส่วนเทอร์มินัล (Terminal) ประกอบด้วยจอภาพและแป้นพิมพ์เท่านั้น ไม่มีหน่วยประมวลผลกลางของตัวเอง ต้องใช้หน่วยประมวลผลของคอมพิวเตอร์ศูนย์กลาง



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.2 อุปกรณ์ตัวกลาง (Intermediary Devices)

นอกจากอุปกรณ์ปลายทางที่เราคุ้นเคยแล้ว ระบบเครือข่ายยังต้องพึ่งพาอุปกรณ์ตัวกลาง (Intermediary Devices) ที่เตรียมการเชื่อมต่อและการทำงานเบื้องหลัง เพื่อให้แน่ใจว่าชุดข้อมูลส่งผ่านระบบเครือข่ายไปได้ อุปกรณ์เหล่านี้เชื่อมต่อโฮสต์จากแต่ละระบบเครือข่ายและสามารถเชื่อมต่อหลาย ๆ ระบบเครือข่ายเข้าด้วยกัน โดยจะสร้างเป็น Internetwork (การเชื่อมต่อเครือข่ายเข้ากับเครือข่าย) หรือเรียกว่า “อินเทอร์เน็ต” (Internet) ซึ่งเป็นเครือข่ายที่ใหญ่ที่สุดในโลก อุปกรณ์ตัวกลางเหล่านี้ผู้ใช้สามารถที่จะจับต้องได้ แต่ไม่สามารถใช้งานได้โดยตรง ตัวอย่างของอุปกรณ์เครือข่ายตัวกลาง เช่น



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

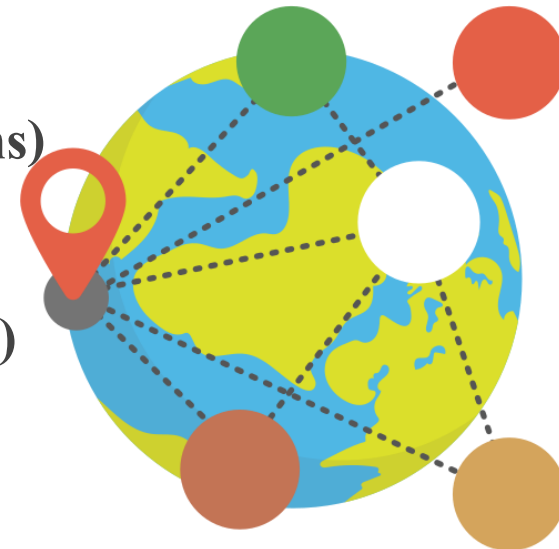
อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

🌐 อุปกรณ์สำหรับการเข้าถึงเครือข่าย (Network Access Devices) เช่น ฮับ (Hub) สวิตช์ (Switch) และจุดเชื่อมต่อไร้สายหรือไวร์เลสแอคเซสพอยต์ (Wireless Access Point)

🌐 อุปกรณ์เชื่อมต่อระหว่างเครือข่าย (Internetworking Devices) เช่น เราเตอร์ (Router)

🌐 เซิร์ฟเวอร์สำหรับการสื่อสารและโมเด็ม (Communication Servers and Modems)

🌐 อุปกรณ์รักษาความมั่นคงปลอดภัย (Security Devices) เช่น ไฟร์วอลล์ (Firewall)



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

บทบาทของตัวกลางอุปกรณ์ คือ การจัดการข้อมูลขณะที่ข้อมูลไหลผ่านระบบเครือข่าย โดยอุปกรณ์เหล่านี้ใช้แอตเตรซของโฮสต์ปลายทางร่วมกับข้อมูลเกี่ยวกับการเชื่อมต่อเครือข่ายเพื่อกำหนดเส้นทางที่ข้อความควรใช้ผ่านเครือข่าย โดยมีหน้าที่และกระบวนการดังนี้

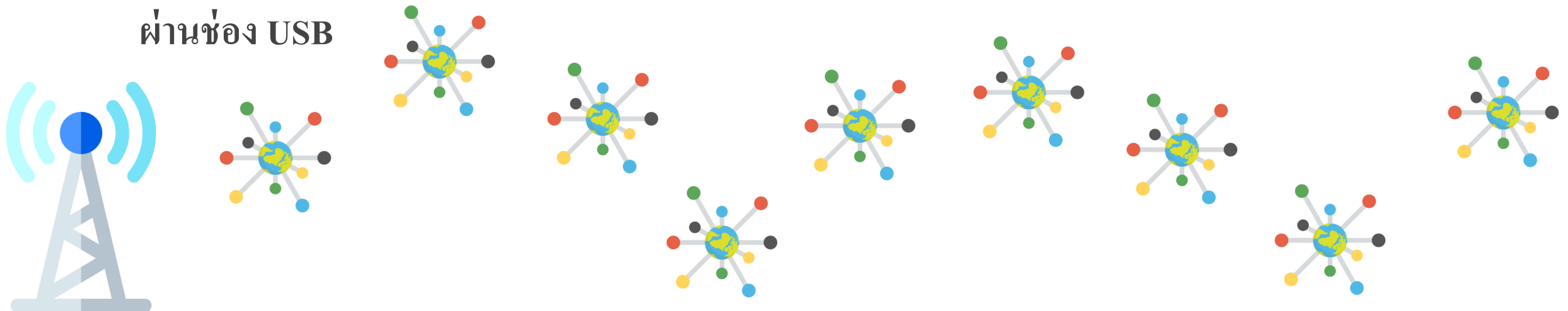
- 🌐 สร้างและทวนส่งต่อสัญญาณข้อมูล
- 🌐 เก็บดูแลรักษาข้อมูลเกี่ยวกับเส้นทางที่มีอยู่โดยผ่านเครือข่ายและ Internetwork
- 🌐 แจ้งอุปกรณ์อื่น ๆ ถึงข้อผิดพลาดและความล้มเหลวในการสื่อสาร
- 🌐 กำหนดทิศทางของข้อมูลไปตามทางเดินสำรองเมื่อมีความล้มเหลวการเชื่อมต่อ
- 🌐 จำแนกและกำหนดทิศทางของข้อความตามลำดับความสำคัญ (Quality of Service : QoS)
- 🌐 อนุญาตหรือปฏิเสธการไหลของข้อมูลตามการตั้งค่าการรักษาความมั่นคงปลอดภัย

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2.

การ์ดเชื่อมต่อเครือข่าย (Network Interface Card: NIC)

หรือเรียกว่า การ์ดแลน หมายถึง แผงวงจรสำหรับใช้ในการเชื่อมต่อทั้งแบบมีสายและไร้สายกับเครือข่าย ซึ่งติดตั้งไว้ในเครื่องคอมพิวเตอร์ที่ต้องการเชื่อมต่อกับเครือข่าย ทั้งที่เครื่องแม่ข่ายหรือเครื่องลูกข่ายหน้าที่ของการ์ดนี้คือแปลงสัญญาณจากคอมพิวเตอร์ส่งผ่านไปตามสายสัญญาณหรือแบบไร้สาย ทำให้คอมพิวเตอร์ในเครือข่ายแลกเปลี่ยนข้อมูลกันได้ โดยผู้ใช้สามารถเพิ่มการ์ดแลนลงในเครื่องคอมพิวเตอร์ของตนเองได้โดยเสียบการ์ดแลนช่อง PCI Slot บนเมนบอร์ด หรือผ่านช่อง USB





2.

การ์ดเชื่อมต่อเครือข่าย (Network Interface Card: NIC)

เนื่องจากการเชื่อมต่อเครือข่ายถือเป็นสิ่งสำคัญในการทำงานคอมพิวเตอร์ ดังนั้นผู้ผลิตเมนบอร์ดคอมพิวเตอร์ส่วนใหญ่จึงมักจะมีการ์ดแลนสำหรับการเชื่อมต่อแบบมีสาย หรือการ์ดแลนเชื่อมต่อแบบไร้สายมาให้จากโรงงานแล้ว เช่นเดียวกับสมาร์ทโฟนที่จะมีการติดตั้งการ์ดแลนเชื่อมต่อแบบไร้สายมาพร้อมใช้งานแล้ว การที่จะติดตั้งการ์ดแลนเพิ่มเติมบนคอมพิวเตอร์มักจะเกิดจากความต้องการในการต่อวงแลนมากกว่า 1 วง (เนื่องจากในการเชื่อมต่อหนึ่งการ์ดแลน สามารถเชื่อมต่อได้แค่เครือข่ายเดียวเท่านั้นในขณะใดขณะหนึ่ง) หรืออาจต้องการเชื่อมต่อกับอินเทอร์เฟซ (Interface) แบบพิเศษ เช่น Fiber Optic นอกจากนี้ ในความเป็นจริงแล้วอุปกรณ์เกือบทุกตัวทั้งอุปกรณ์ปลายทางและอุปกรณ์ตัวกลางที่เชื่อมต่อระบบคอมพิวเตอร์จำเป็นที่จะต้องมีการ์ดแลน ซึ่งอาจจะใช้สำหรับเชื่อมต่อแบบมีสายหรือไร้สายเพื่อให้สามารถเชื่อมต่อได้ แต่อาจจะอยู่ในรูปแบบที่แตกต่างกัน เช่น ฝังในตัวอุปกรณ์ต่าง ๆ หรืออยู่ในพอร์ตของแต่ละอุปกรณ์

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2.

การ์ดเชื่อมต่อเครือข่าย (Network Interface Card: NIC)



รูปที่ 4.1 การ์ดเชื่อมต่อแบบไร้สาย



รูปที่ 4.2 ตัวอย่าง USB ตัวรับ Wi-Fi

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

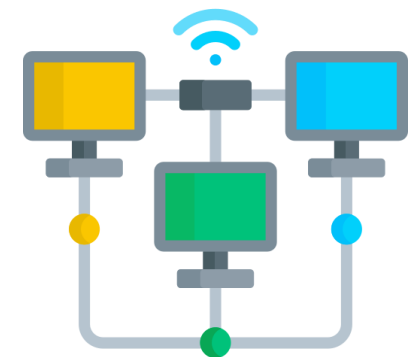
อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.1 อุปกรณ์ตัวกลาง (Intermediary Devices)

เป็นอุปกรณ์สำหรับคอมพิวเตอร์ที่ทำให้คอมพิวเตอร์สามารถเชื่อมต่อกับเครือข่ายอื่นได้ มีดังนี้

3.1.1 โมเด็มแบบแอนะล็อก (Analog Modem)

เป็นอุปกรณ์ที่ทำให้คอมพิวเตอร์สามารถเชื่อมต่อกับเครือข่ายอื่นได้ ซึ่งเป็นอุปกรณ์ที่ใช้ในอดีตในยุคแรก ๆ ที่ผู้ใช้งานจะต้องใช้คอมพิวเตอร์ต่อกับโทรศัพท์บ้านผ่านโมเด็ม เพื่อเชื่อมต่อไปยังผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) โมเด็มมาจากคำว่า Modulator/Demodulator



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

Modulation คือ การแปลงสัญญาณดิจิทัล (Digital) จากเครื่องคอมพิวเตอร์ต้นทางให้กลายเป็นสัญญาณแอนะล็อก (Analog) แล้วส่งไปตามสายโทรศัพท์ และ **Demodulation** คือ การเปลี่ยนจากสัญญาณดิจิทัลที่ได้จากสายโทรศัพท์ให้กลับไปเป็นสัญญาณแอนะล็อก เพื่อส่งต่อไปยังเครื่องคอมพิวเตอร์ปลายทาง สัญญาณจากคอมพิวเตอร์เป็นสัญญาณดิจิทัลมีแค่ 0 กับ 1 เท่านั้น เมื่อเปลี่ยนมาเป็นสัญญาณแอนะล็อกอยู่ในรูปที่คล้ายกับสัญญาณไฟฟ้าของโทรศัพท์ เนื่องจากข้อจำกัดด้านเทคโนโลยีทำให้โมเด็มแบบแอนะล็อกทำงานรับส่งข้อมูลได้เพียง 64-128 kbps จึงทำให้ได้รับความนิยมน้อยลงจนไม่มีผู้ใช้แล้ว



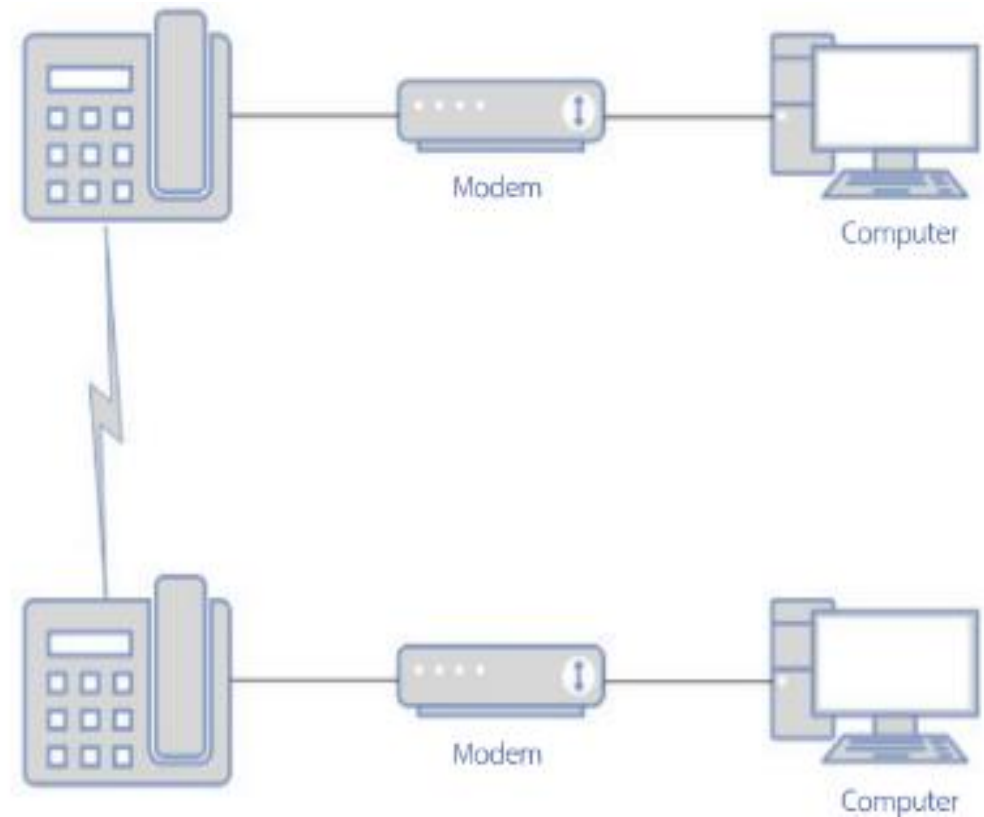
อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



รูปที่ 4.3 รูป Analog Modem



รูปที่ 4.4 การทำงานของโมเด็ม

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.1.2 โมเด็มแบบดิจิทัล (Digital Modem)

ใช้รับและส่งข้อมูลผ่านสายเชื่อมสัญญาณแบบดิจิทัลการเชื่อมต่อโมเด็มแบบนี้ผู้ใช้ไม่จำเป็นต้องหมุนโทรศัพท์ไปที่ผู้ให้บริการอินเทอร์เน็ต โดยโมเด็มจะทำการเชื่อมต่อให้อัตโนมัติเมื่อมีการใช้งานสามารถส่งข้อมูลด้วยความเร็วสูงตั้งแต่ 128 kbps จนถึงมีความเร็วมากกว่า 1,000 Mbps ซึ่งขึ้นอยู่กับเทคโนโลยีที่ใช้ในการเชื่อมต่อด้วย โดยทั่วไปจะเป็นโมเด็มที่ติดตั้งภายนอก (External Modem) และมักจะรวมความสามารถของ Router Switch และ Wireless Access Point มาด้วย เช่น



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.1.2 โมเด็มแบบดิจิทัล (Digital Modem)

🌐 **ดีเอสแอล (Digital Subscriber Line : DSL)** เป็นโมเด็มที่ได้รับความนิยมในการใช้งานในบ้านและสำนักงานขนาดเล็ก โดยสามารถรับและส่งข้อมูลดิจิทัลด้วยความเร็วสูงกว่าการเชื่อมต่อผ่านโมเด็มแบบหมุนโทรศัพท์

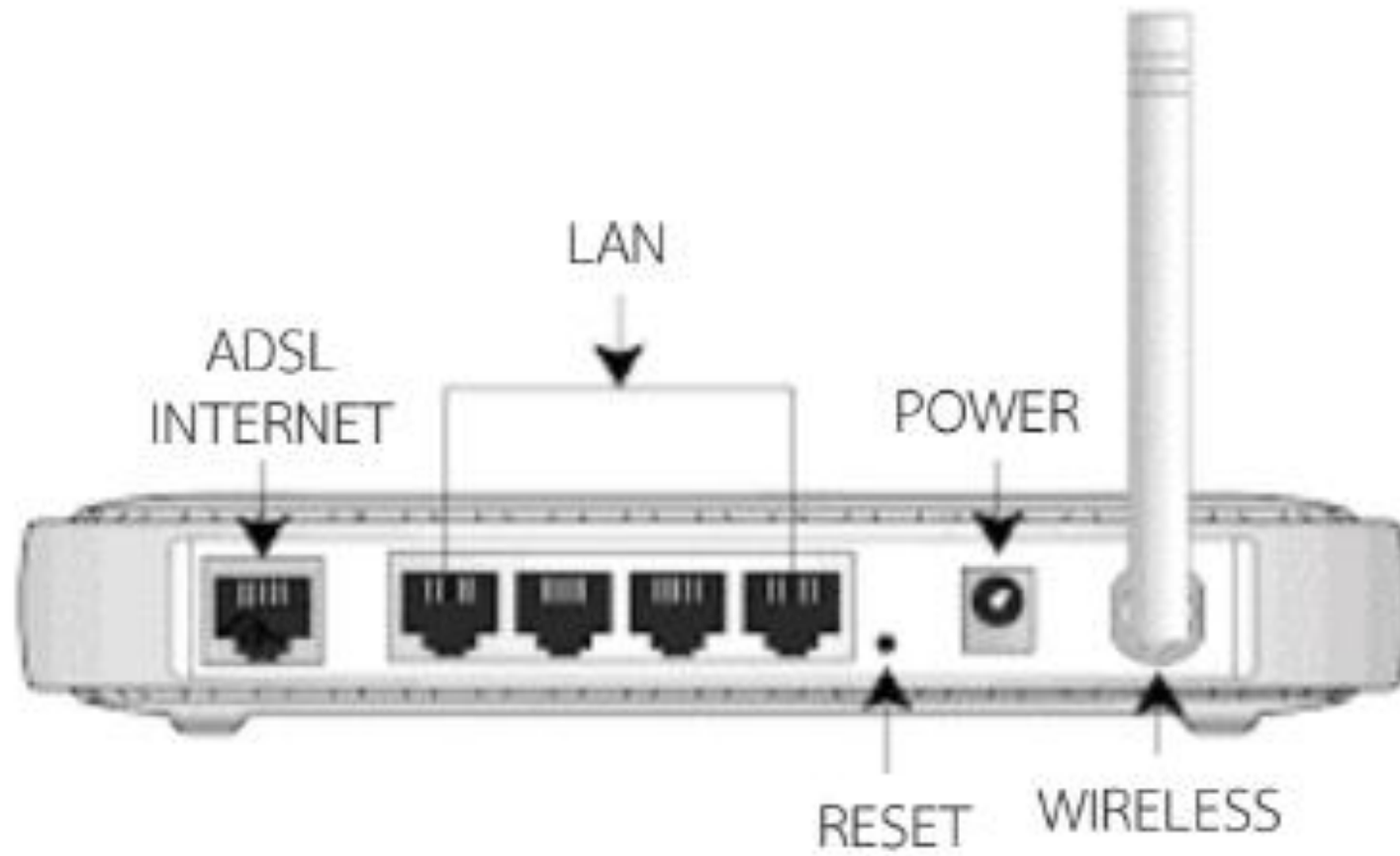
🌐 **เคเบิลโมเด็ม (Cable Modem)** เป็นโมเด็มทำหน้าที่รับและส่งข้อมูลดิจิทัลจากคอมพิวเตอร์ผ่านทางสายเคเบิลทีวี บางครั้งเรียกว่าบรอดแบนด์โมเด็ม (Broadband Modem)



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



รูปที่ 4.5 ADSL Modem

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

🌐 **ONU หรือ Optical Network Unit** หรืออาจเรียกว่าโมเด็มสำหรับสายไฟเบอร์อปติก (Fiber Optic) เป็นอุปกรณ์ที่โซ่ปลายทางหรือเป็นอุปกรณ์ที่วางไว้ที่บ้าน เพื่อให้ใช้งานอินเทอร์เน็ตในระบบ FTTx สามารถรองรับความเร็วได้สูงกว่าโมเด็มสำหรับ DSL มาก เนื่องจากสายสัญญาณที่เข้ามาเป็นสายไฟเบอร์อปติก โดยผู้ใช้งานจะได้รับ ONU มาจากผู้ให้บริการอินเทอร์เน็ต เนื่องจากอุปกรณ์ปลายทางและต้นทางในระบบนี้จะต้องมีการจับคู่กันในระบบสื่อสารให้ถูกต้องจึงจะใช้งานได้



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



รูปที่ 4.6 Optical Network Unit

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

ก่อนที่จะรู้จักการทำงานของอุปกรณ์เครือข่ายอื่น ๆ เราควรเข้าใจหลักการของโดเมนการชน (Collision Domain) และโดเมนการbroadcast (Broadcast Domain)

โดเมนการชน (Collision Domain) คือ การเกิดโอกาสการชนกันของข้อมูลที่ถูกส่งจากเครื่องคอมพิวเตอร์ที่มีการเชื่อมต่อกันผ่านสื่อที่ใช้งานร่วมกันในเวลาเดียวกัน (Shared Media) เช่น ตัวทวนสัญญาณ (Repeater) ฮับ (Hub) เพราะฮับมีพอร์ต (Port) และสื่อกลางที่ใช้ทำงานร่วมกันของอุปกรณ์ หากอุปกรณ์ใดอุปกรณ์หนึ่งกำลังส่งข้อมูลผ่านฮับอยู่ อุปกรณ์อื่น ๆ ที่จะส่งข้อมูลต้องรอให้อุปกรณ์ที่ส่งอยู่ก่อนหน้าทำการส่งเสร็จสมบูรณ์ก่อน



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

หากส่งข้อมูลออกมาในขณะที่อุปกรณ์อื่นกำลังส่งข้อมูลผ่านฮับอยู่จะเกิดการชนกัน (Collision) ของสัญญาณ ดังนั้นจึงเรียกการเชื่อมต่อด้วยฮับว่าอยู่ในโดเมนการชนเดียวกัน หรือเรียกว่าอยู่ในส่วนหรือเซกเมนต์ (Segment) เดียวกัน การใช้งานสามารถเชื่อมต่อฮับหลายตัวต่อเข้าด้วยกัน แต่อุปกรณ์ทั้งหมดยังคงอยู่ในโดเมนการชนเดียวกัน แต่โดเมนการชนนั้นจะมีขนาดใหญ่ขึ้นและความเร็วในการรับส่งข้อมูลของอุปกรณ์จะถูกแชร์มากขึ้นด้วย ซึ่งส่งผลให้ความเร็วที่อุปกรณ์ที่เชื่อมต่ออยู่กับฮับนั้นจะลดลงตามไปด้วย แต่อุปกรณ์สวิตช์แต่ละพอร์ตจะแยกการทำงานออกจากกัน



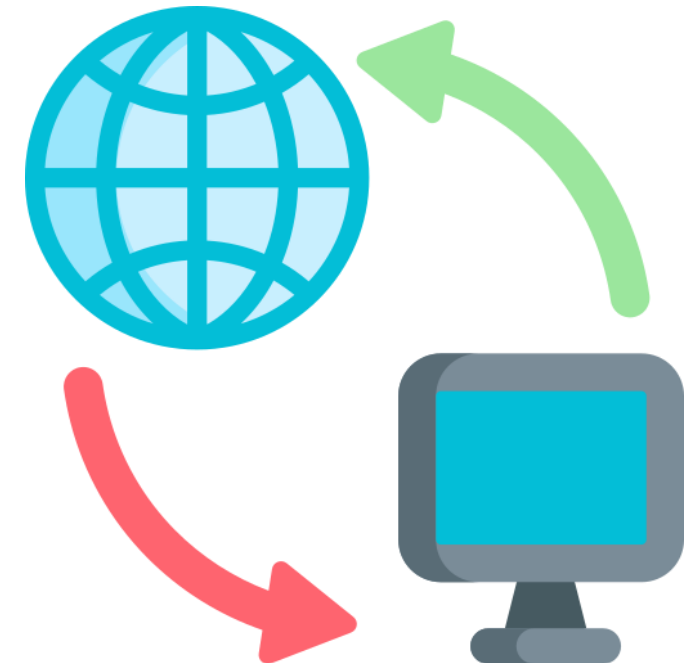
อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

ทำให้จำนวนโดเมนการชนของสวิตช์เป็นไปตามจำนวนพอร์ตที่มีของสวิตช์ ยิ่งโดเมนการชนมากขึ้น จะเพิ่มความเร็วในการทำงานให้กับอุปกรณ์เครือข่ายมากขึ้น เพราะไม่ต้องแชร์ความเร็วที่มีรวมกัน เช่น

- 🌐 ตัวทวนสัญญาณ 2 พอร์ตเชื่อมต่อกันอยู่ จะมี 1 โดเมนการชน
- 🌐 ฮับ 4 พอร์ตเชื่อมต่อกันอยู่ จะมี 1 โดเมนการชน
- 🌐 บริดจ์ 2 พอร์ตเชื่อมต่อกันอยู่ จะมี 2 โดเมนการชน
- 🌐 สวิตช์ 4 พอร์ตเชื่อมต่อกันอยู่ จะมี 4 โดเมนการชน
- 🌐 เราเตอร์ 4 พอร์ตเชื่อมต่อกันอยู่ จะมี 4 โดเมนการชน



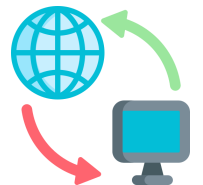
อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

อุปกรณ์ที่สามารถป้องกันหรือจัดการโดเมนการชนนั้นจะทำงานที่ชั้นที่ 2 ของโมเดล OSI ขึ้นไป ซึ่งจะเห็นวาบรีดจ์ สวิตช์ และเราเตอร์มีความสามารถดังกล่าว ในขณะที่ตัวทวนสัญญาณและฮับนั้น ไม่สามารถป้องกันหรือจัดการโดเมนการชนได้ ดังนั้น ทั้งตัวทวนสัญญาณและฮับนั้น ทำงานที่ชั้นที่ 1 ของโมเดล OSI

อุปกรณ์ที่ทำงานที่ชั้นที่ 2 ของโมเดล OSI จะกรองข้อมูลจากหมายเลข Media Access Control address (MAC address) ก่อนที่จะส่งต่อไปให้กับอุปกรณ์ปลายทางเครือข่ายย่อยที่ถูกต้อง โดยหมายเลข MAC address นี้ฝังมาบนการ์ดแลน เป็นหมายเลขที่ไม่ซ้ำกันและมีหมายเลขเดียวในโลก คล้ายกับหมายเลขบัตรประชาชนของเรา ไม่ว่าเราจะไปที่ไหนเราก็ยังมีหมายเลขบัตรประชาชนนี้ที่ไม่ซ้ำกับใคร และมีหมายเลขเดียวในโลก



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

โดเมนการbroadcast (Broadcast Domain) คือ การกระจายสัญญาณเพื่อให้เครื่องคอมพิวเตอร์ทั้งหมดในเครือข่ายแลนนั้นสื่อสารกันได้ผ่านการbroadcast (Broadcasting) เช่น หากเครือข่ายของเรามีการเชื่อมต่อด้วยสวิตช์ 4 พอร์ต หากต้องการให้ทั้ง 4 พอร์ตของสวิตช์นั้นคุยกันได้ จะต้องทำการbroadcast หรืออาจเรียกว่าการฟลัดดิ้ง (Flooding) ในกรณีที่เป็นการทำงานที่ชั้นที่ 2 ของโมเดล OSI

โดเมนการbroadcast จะทำการbroadcast ได้เฉพาะในกรณีที่อยู่ภายในขอบเขตเครือข่ายเดียวกัน เช่น เครือข่ายของแต่ละคณะ ที่อาจจะมีการแบ่งแยกการดูแลออกจากกันตามแต่ละคณะ เราอาจจะสามารถทำการbroadcast ข้ามขอบเขตเครือข่ายได้

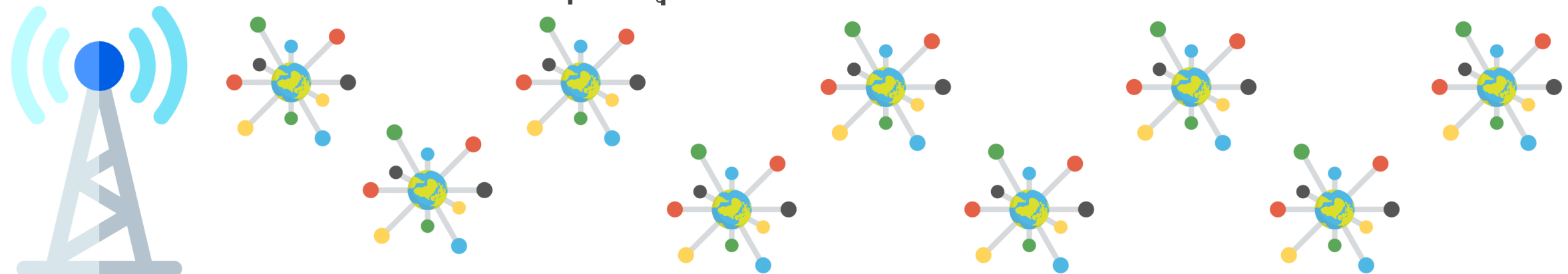


อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

โดยหากเครื่อง A และ B อยู่ในโดเมนการ broadcast เดียวกัน เครื่อง B จะได้รับเฟรม broadcast (Broadcast Frame) จากเครื่อง A ตัวอย่าง หากเป็นอุปกรณ์ฮับ เมื่อได้รับเฟรม broadcast ฮับจะส่งออกไปทุกพอร์ตของอุปกรณ์ หากเป็นอุปกรณ์สวิตช์ (โดยเริ่มต้นที่มีเพียง 1 VLAN เท่านั้น) เมื่อได้รับเฟรม broadcast สวิตช์จะส่งต่อสัญญาณ (Forward) ไปทุกพอร์ตที่มีการเชื่อมต่ออยู่ (ยกเว้นพอร์ตที่รับเฟรม broadcast เข้ามา) หากเป็นเราเตอร์ เมื่อได้รับเฟรม broadcast เราเตอร์จะ ไม่มีการส่งต่อไปยังพอร์ตอื่น ๆ ซึ่งสรุปได้ดังนี้



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

- ตัวทวนสัญญาณ 2 พอร์ตเชื่อมต่อกันอยู่จะมี 1 โดเมนการชน และ 1 โดเมนการบรอดคาสต์
- ฮับ 4 พอร์ตเชื่อมต่อกันอยู่ จะมี 1 โดเมนการชน และ 1 โดเมนการบรอดคาสต์
- บริดจ์ 2 พอร์ตเชื่อมต่อกันอยู่ จะมี 2 โดเมนการชน และ 1 โดเมนการบรอดคาสต์
- สวิตช์ 4 พอร์ตเชื่อมต่อกันอยู่ จะมี 4 โดเมนการชน และ 1 โดเมนการบรอดคาสต์
- เราเตอร์ 4 พอร์ตเชื่อมต่อกันอยู่ จะมี 4 โดเมนการชน และ 4 โดเมนการบรอดคาสต์

อุปกรณ์ที่สามารถป้องกันหรือจัดการโดเมนการบรอดคาสต์นั้นจะทำงานที่ชั้นที่ 3 ของโมเดล OSI ขึ้นไปซึ่งจะเห็นว่าเราเตอร์มีความสามารถดังกล่าว

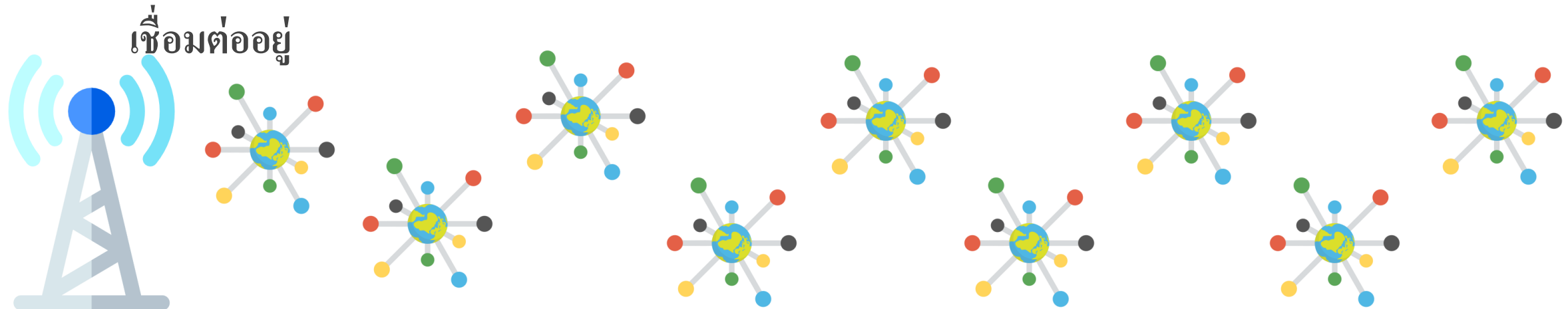


อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

อุปกรณ์ที่ทำงานที่ชั้นที่ 3 ของโมเดล OSI จะกรองข้อมูลจากหมายเลข IP Address ก่อนที่จะส่งต่อไปให้กับอุปกรณ์ปลายทางเครือข่ายที่ถูกต้อง โดย IP Address นี้จะเปลี่ยนไปทุกครั้งตามแต่ละผู้ให้บริการเครือข่าย เพื่อบอกให้รู้ว่าตอนนี้อุปกรณ์นั้นเชื่อมต่อกับเครือข่ายใด เช่น เมื่ออุปกรณ์นั้นเชื่อมต่อกับเครือข่ายในวิทยาลัย จะได้ IP Address มาหนึ่งหมายเลข เช่น 192.168.10.5 และเมื่อเรากลับบ้านและนำอุปกรณ์นั้นไปเชื่อมต่อกับเครือข่ายที่บ้าน จะได้ IP address มาหนึ่งหมายเลข เช่น 10.10.10.5 เป็นต้น ซึ่งหมายเลข IP Address นี้จะแตกต่างกันไปตามแต่ละเครือข่ายที่อุปกรณ์นั้นเชื่อมต่ออยู่

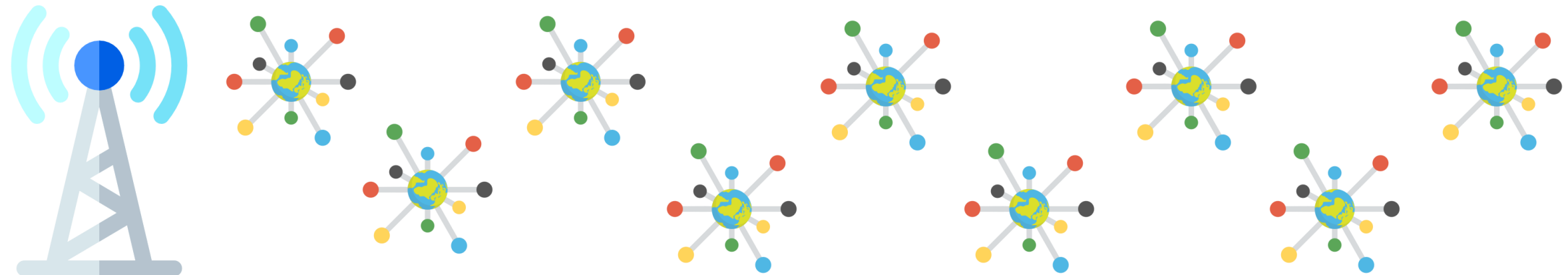


อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

นอกจากนี้ ในการที่อุปกรณ์ในระบบเครือข่ายจะสามารถเชื่อมต่อกับระบบเครือข่ายอื่นได้ จำเป็นต้องมีการกำหนดทางออกหรือเรียกว่าเกตเวย์ (Gateway) ซึ่งโดยปกติจะต้องมีการกำหนดค่า IP Address ของเกตเวย์ที่ใช้เป็นทางออกเริ่มต้นสำหรับอุปกรณ์ต่าง ๆ ซึ่งเรียกว่า เกตเวย์เริ่มต้น (Default Gateway) อุปกรณ์ที่ทำหน้าที่เกตเวย์อาจจะเป็นเครื่องคอมพิวเตอร์ที่มีโปรแกรมการตั้งค่าเฉพาะ หรืออาจเป็นอุปกรณ์ตัวกลาง เช่น เราเตอร์อุปกรณ์นั้นเชื่อมต่ออยู่



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.2 ตัวทวนสัญญาณ (Repeater)

ทำหน้าที่รับสัญญาณดิจิทัล ขยายสัญญาณแล้วส่งต่อออกไปยังอุปกรณ์อื่น เนื่องจากการส่งสัญญาณผ่านสื่อตัวกลางนั้น เมื่อระยะทางมากขึ้น ความแรงของสัญญาณจะลดลง ทำให้ประสิทธิภาพในการรับส่งข้อมูลลดลงหรือไม่สามารถรับส่งข้อมูลได้ ดังนั้น จึงใช้ตัวทวนสัญญาณที่รับข้อมูลแล้วนำมาเพิ่มกำลังส่งเพื่อขยายระยะทางให้มากขึ้น ตัวทวนสัญญาณมีทั้งแบบที่ไวทวนสัญญาณแบบผ่านตัวกลางแบบมีสายและแบบไร้สาย

การทำงานของตัวทวนสัญญาณอยู่ในชั้นกายภาพหรือฟิสิคัล (Physical Layer) ซึ่งเป็นชั้นที่ 1 ของโมเดล OSI เมื่อเชื่อมต่อเครือข่ายด้วยตัวทวนสัญญาณ ทำให้มี 1 โดเมนการชน และ 1 โดเมนการ broadcast



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

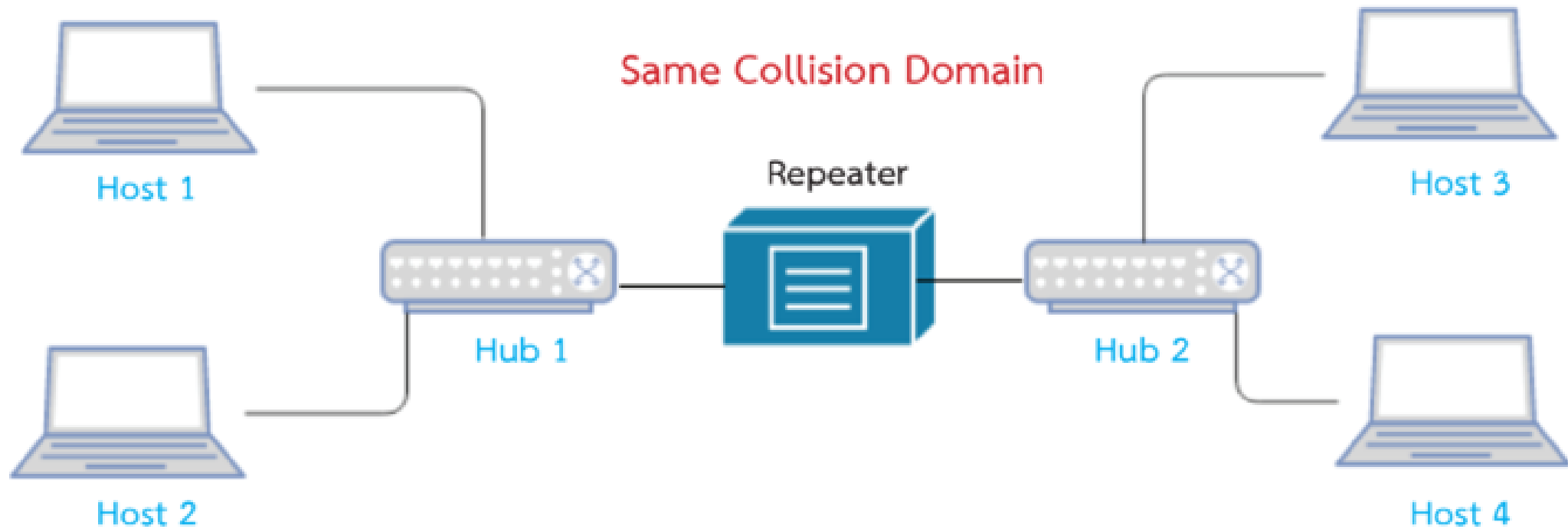


รูปที่ 4.7 ตัวทวนสัญญาณ (Repeater)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



รูปที่ 4.8 ภาพการทำงานของเครื่องทวนสัญญาณ (Repeater)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.3 ฮับ (Hub)



เป็นอุปกรณ์เชื่อมต่อที่ใช้เป็นจุดรวมและแยกสายสัญญาณ ใช้เป็นจุดรวมการเชื่อมต่อสายสัญญาณระหว่างเครื่องแม่ข่ายกับเครื่องเวิร์กสเตชันต่าง ๆ เพื่อให้เกิดความสะดวกในการเชื่อมต่อของเครือข่ายแบบดาว (Star) โดยใช้ฮับเป็นศูนย์กลางในการเชื่อมต่อทุกเครื่อง (คล้ายปลั๊กพวงไฟฟ้า) ด้วยสาย UTP (Unshielded Twisted Pair) หรือ CAT5, CAT6 กับหัวต่อแบบ RJ-45 ในการรับส่งข้อมูล ฮับจะเป็นเสมือนตัวทวนสัญญาณ (Repeater) ในตัวด้วย เพราะถ้าเราเชื่อมต่ออุปกรณ์ในระบบเครือข่ายโดยใช้สาย UTP ที่มีระยะทางสายยาวมากเกินไปจะทำให้สัญญาณที่ผ่านไปในสายลดลง จำเป็นจะต้องมีการทวนสัญญาณด้วยการนำฮับมาต่อไว้ระหว่างทาง แต่การทวนสัญญาณนี้มีข้อจำกัดเรื่องของจำนวนฮับที่นำมาพ่วงใช้งานและระยะทางด้วยเช่นกัน การทำงานของฮับจะอยู่ในชั้นกายภาพหรือฟิสิคัล (Physical Layer) ซึ่งเป็นชั้นที่ 1 ของโมเดล OSI ให้มี 1 โดเมนการชน และ 1 โดเมนการบรอดคาสต์ เช่นเดียวกับตัวทวนสัญญาณ

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



3. อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

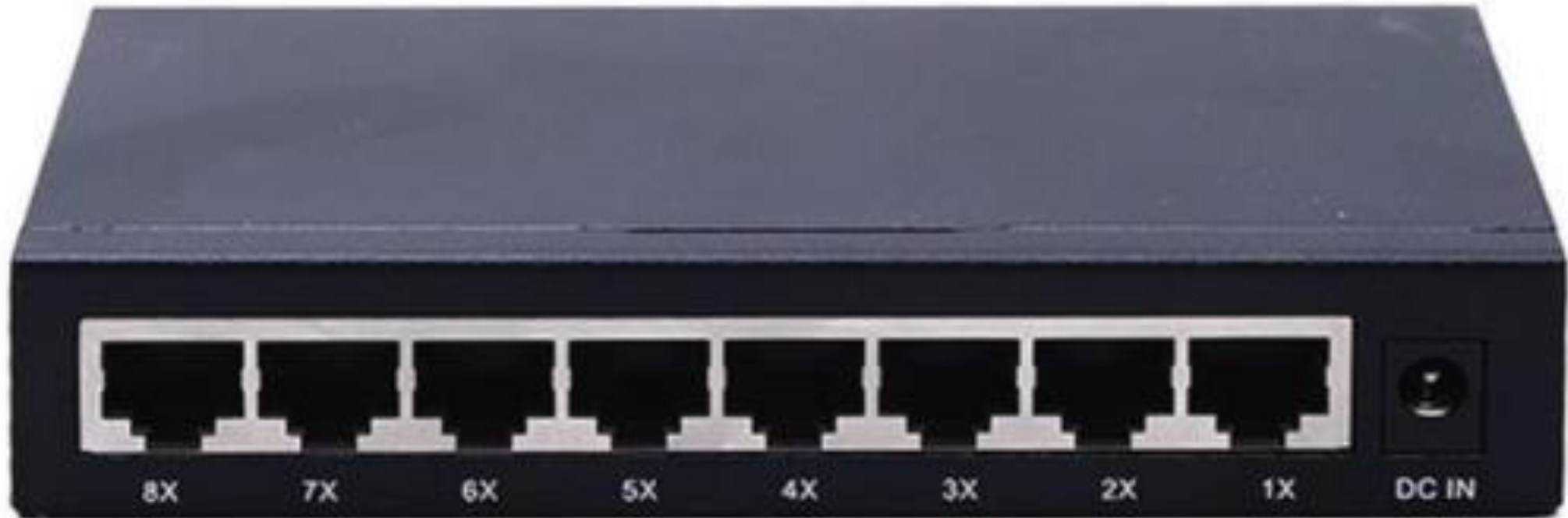
อัตราความเร็วในการรับส่งข้อมูลของฮับจะมีตั้งแต่ 100 Mbps (Megabit per Second) จนถึง 1,000 Mbps และจะมีจำนวนช่องขนาดเล็กตั้งแต่ 4 ช่อง หรือเรียกว่า ฮับ 4 พอร์ต (Port) และอื่น ๆ ตามจำนวนพอร์ตที่มีให้ใช้งาน เช่น 8 พอร์ต 12 พอร์ต 16 พอร์ต และ 24 พอร์ต การใช้งานฮับสามารถต่อใช้งานได้ทันทีโดยไม่ต้องตั้งค่าใด ๆ

ข้อเสียของฮับ คือ ความเร็วในการรับส่งข้อมูลของอุปกรณ์จะถูกแชร์เท่ากันทุกเครื่องขึ้นอยู่กับจำนวนเครื่องที่อยู่งานผ่านฮับ เช่น ฮับมีความเร็วการรับส่งข้อมูลอยู่ที่ 100 Mbps มีเครื่องเชื่อมต่ออยู่ 4 เครื่องแต่ละเครื่องจะมีความเร็วในการรับส่งข้อมูลอยู่ 25 Mbps เป็นต้น เนื่องจากการใช้สื่อร่วมกัน (Shared Media) ระหว่างอุปกรณ์ต่าง ๆ

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

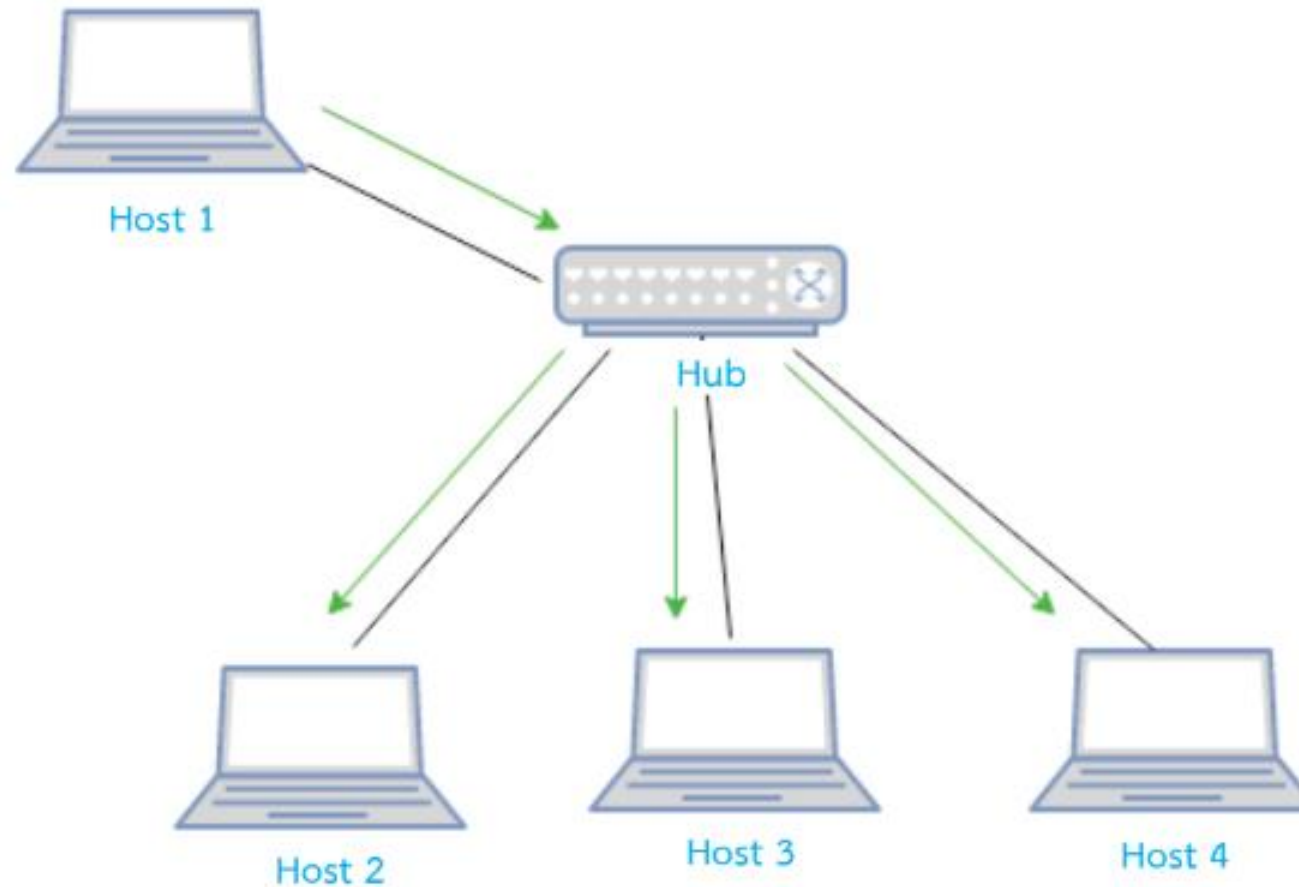


รูปที่ 4.9 ฮับ (Hub)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

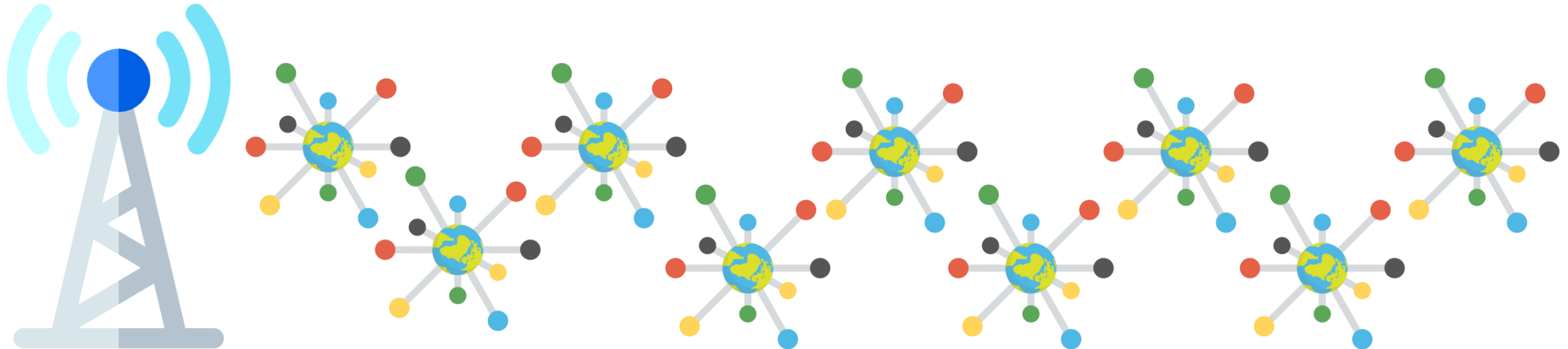


รูปที่ 4.10 การทำงานของฮับ (Hub)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3. อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

ในยุคเริ่มต้น ราคาอุปกรณ์สวิตช์ที่มีลักษณะคล้ายกับฮับแต่มีคุณสมบัติดีกว่ายังมีราคาสูงอยู่จึงทำให้มีการใช้ฮับอย่างแพร่หลาย แต่ในปัจจุบันฮับไม่ค่อยได้รับความนิยมจนแทบไม่มีการใช้งานฮับแล้ว เนื่องจากราคาอุปกรณ์สวิตช์มีราคาถูกลงมาก รวมถึงความเร็วและประสิทธิภาพการทำงานของอุปกรณ์สวิตช์ที่สูงมากด้วยเช่นกัน



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.4 บริดจ์ (Bridge)



เป็นอุปกรณ์ที่ใช้ในการเชื่อมต่อสองเครือข่ายเข้าด้วยกันในยุคแรก คล้ายกับเป็นสะพานเชื่อมสองฟากฝั่งเข้าด้วยกัน จึงเรียกอุปกรณ์นี้ว่า “บริดจ์” ซึ่งแปลว่า สะพาน เครือข่ายสองเครือข่ายที่นำมาเชื่อมต่อกันจะต้องเป็นเครือข่ายชนิดเดียวกัน และใช้โปรโตคอลในการรับส่งข้อมูลเหมือนกัน เช่น ใช้ในการเชื่อมต่อเครือข่ายตามมาตรฐานอีเทอร์เน็ตสองเครือข่ายเข้าด้วยกัน เพื่อให้สามารถขยายขอบเขตของแลนออกไปได้โดยประสิทธิภาพโดยรวมลดลงไม่มากนัก เนื่องจากการติดต่อกับเครื่องที่อยู่ในเซกเมนต์ (Segment) เดียวกันจะไม่มี การส่งข้ามไปยังต่างเซกเมนต์ ทำให้แต่ละพอร์ตของฮับอยู่ต่างโดเมนการชน โดยบริดจ์จะตรวจสอบข้อมูลที่ส่งโดยพิจารณาจากที่อยู่ของผู้รับปลายทาง

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



3. อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

หากพบว่าเป็นเครื่องคอมพิวเตอร์ที่อยู่คนละเครือข่ายย่อยก็จะขยายสัญญาณ (เช่นเดียวกับตัวทวนสัญญาณ) แล้วจึงส่งต่อให้ข้อมูลไปยังอีกพอร์ตที่มีการเชื่อมต่ออยู่ โดยไม่ได้สนใจว่าจะมีเครื่องคอมพิวเตอร์ปลายทางเชื่อมต่ออยู่ในอีกฝั่งของพอร์ตนั้นหรือไม่ การทำงานของบริดจ์จะอยู่ในชั้นที่ 2 ของโมเดล OSI ดังนั้น ทำให้มี 2 โดเมนการชนและ 1 โดเมนการบรอดคาสต์ การใช้งานบริดจ์นั้นสามารถต่อใช้งานได้ทันทีโดยไม่ต้องตั้งค่าใด ๆ

โดยการทำงานของบริดจ์นั้นสามารถช่วยลดปริมาณข้อมูลบนเครือข่ายแลนและแบ่งเครือข่ายออกเป็นเครือข่ายย่อย รวมถึงกรองข้อมูลเท่าที่จำเป็นเพื่อส่งต่อไปให้กับเครือข่ายย่อยที่ถูกต้อง โดยบริดจ์พิจารณาจากหมายเลข MAC Address ที่ฝั่งมากับการ์ดแลน

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

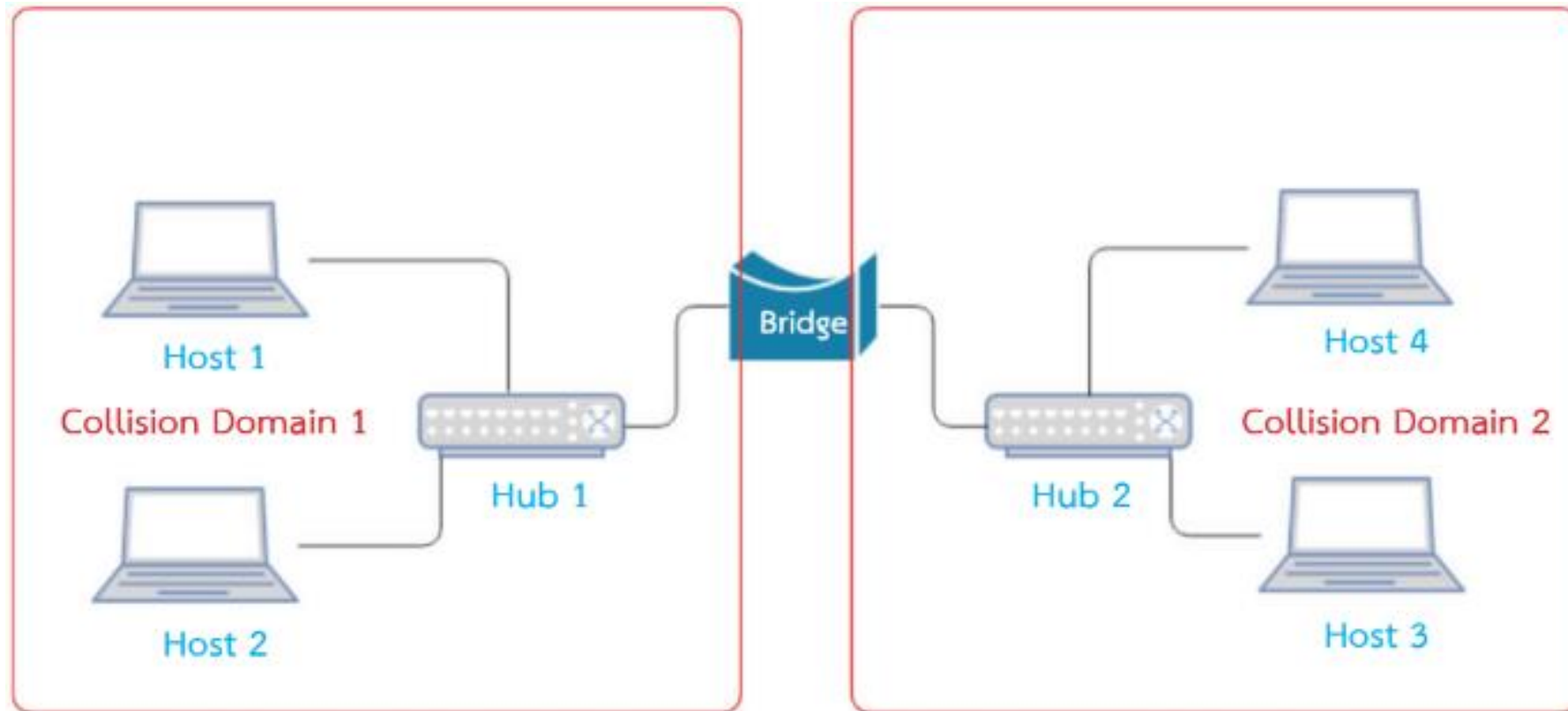


รูปที่ 4.11 บริดจ์ (Bridge)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



รูปที่ 4.12 การทำงานของบริดจ์ (Bridge)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.5 สวิตช์ (Switch) หรืออีเทอร์เน็ตสวิตช์ (Ethernet Switch)

เป็นอุปกรณ์ที่ทำหน้าที่กระจายช่องทางการสื่อสารข้อมูลหลายช่องทางหรือหลายพอร์ตในระบบเครือข่ายคล้ายกับฮับ

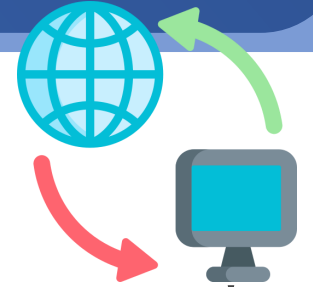
แต่มีความแตกต่างที่ในแต่ละพอร์ตจะมีความสามารถและประสิทธิภาพในการส่งข้อมูลได้สูงกว่า โดยเฉพาะในเครือข่ายที่มีอุปกรณ์ต่อพ่วงอยู่เป็นจำนวนมาก เพราะฮับจะส่งสัญญาณไปยังคอมพิวเตอร์ที่ต่อพ่วงอยู่ในทุกพอร์ต แต่สวิตช์จะส่งข้อมูลตรงไปยังพอร์ตต้นทางและปลายทางโดยตรง (ในกรณีที่เราทราบว่าปลายทางเชื่อมต่ออยู่ในพอร์ตใดของสวิตช์ แต่ฮับจะมีการเก็บสถานะว่าแต่ละพอร์ตมีอุปกรณ์ใดต่ออยู่) เพราะในสวิตช์มีตารางเส้นทาง (Route Table) และหน่วยความจำของสวิตช์ที่บันทึกไว้ว่าแต่ละพอร์ตมี IP Address หรือ MAC Address ใดเชื่อมต่ออยู่



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



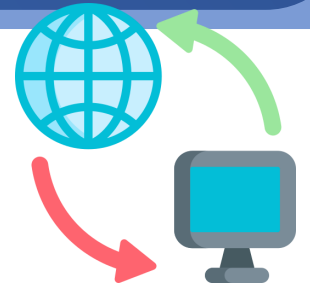
ซึ่งทำให้การส่งข้อมูลเป็นไปได้อย่างรวดเร็ว และยังไม่เป็นการส่งข้อมูลในลักษณะกระจายไปทุกเครื่องของเครือข่ายที่เรียกว่า การbroadcast (Broadcasting) ทำให้จำนวนข้อมูลที่อยู่ในระบบมีน้อยกว่าและมีประสิทธิภาพสูงกว่าฮับ และทำให้แต่ละพอร์ตของสวิตช์อยู่ต่างโดเมนการชน การทำงานของสวิตช์จะอยู่ในชั้นที่ 2 ของโมเดล OSI ดังนั้น ทำให้มีโดเมนการชนตามจำนวนพอร์ตที่มีบนสวิตช์นั้น และ 1 โดเมนการbroadcast

สวิตช์ไม่ได้แชร์ความเร็วในการรับส่งข้อมูลตามจำนวนพอร์ตที่เชื่อมต่ออยู่เหมือนฮับ โดยแต่ละพอร์ตของสวิตช์มีความเร็วการรับส่งข้อมูลที่แยกเป็นอิสระต่อกันตามความสามารถของอุปกรณ์ เช่น ระบบเครือข่ายใช้มาตรฐานความเร็ว 100 Mbps และมีเครื่องคอมพิวเตอร์ที่ต่อในระบบ 5 เครื่อง แต่ละเครื่องจะสื่อสารกันภายในสวิตช์ด้วยความเร็วเท่ากับ 100 Mbps เท่ากันทุกเครื่อง

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



การใช้งานสวิตช์นั้นสามารถต่อใช้งานได้ทันทีโดยไม่ต้องตั้งค่าใด ๆ แต่สามารถกำหนดค่าด้านความมั่นคงปลอดภัยเพิ่มเติม แต่เราจำเป็นต้องศึกษาเพิ่มเติมในการกำหนดค่าดังกล่าวของอุปกรณ์แต่ละรุ่นแต่ละยี่ห้อ

นอกจากนี้ หากกล่าวถึงอุปกรณ์สวิตช์ โดยทั่วไปคืออุปกรณ์ที่ทำงานที่ชั้นที่ 2 ของโมเดล OSI เรียกว่า L2 Switch หรือสวิตช์ แต่ก็ยังมีสวิตช์ที่ทำงานที่ชั้นที่ 3 ของโมเดล OSI เรียกว่า L3 Switch หรือ MultilayerSwitch ซึ่งมีความสามารถในการทำงานของอุปกรณ์ชั้นที่ 3 เช่นเดียวกับอุปกรณ์เราเตอร์ แต่อาจจะมีความสามารถและประสิทธิภาพบางประการที่น้อยกว่าเราเตอร์

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

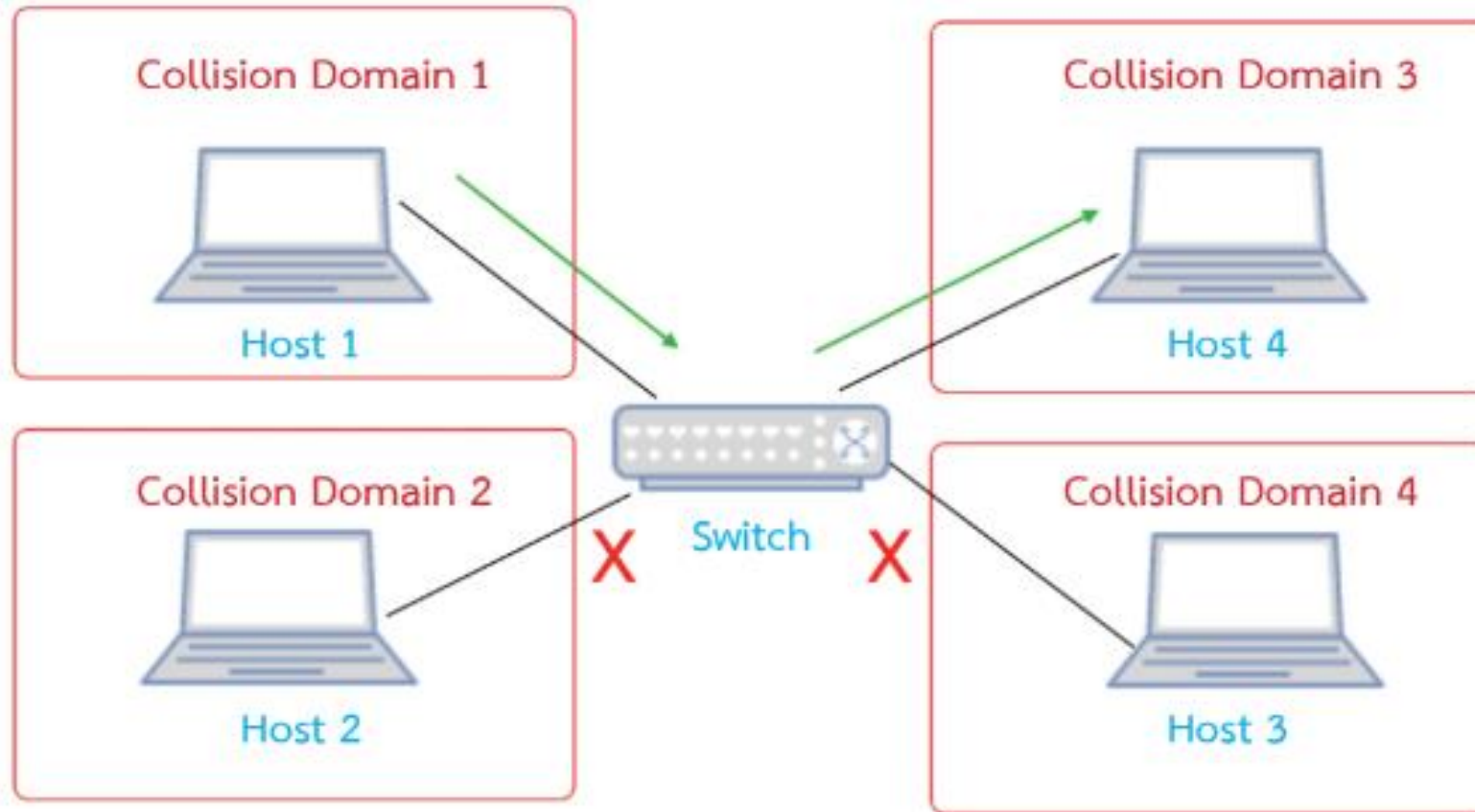


รูปที่ 4.13 อิเทอร์เน็ตสวิตช์

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

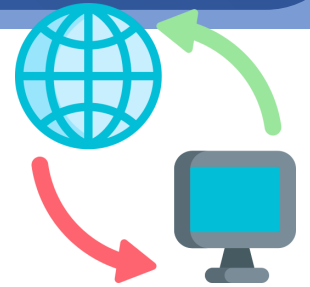


รูปที่ 4.14 การทำงานของอีเทอร์เน็ตสวิตช์

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



3.6 เราเตอร์ (Router)

เราเตอร์ (Router) เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่อระบบเครือข่ายแลนเข้าด้วยกัน ทั้งแลนที่ใช้โปรโตคอลในการรับส่งข้อมูลเหมือนกัน แต่ใช้สื่อส่งข้อมูลหรือสายส่งต่างชนิดกันได้ เช่น เชื่อมต่อ Ethernet LAN ที่ใช้รับส่งข้อมูลแบบ UTP เข้ากับ Ethernet อีกเครือข่ายหนึ่งโดยผ่านสายสื่อสารในรูปแบบสาย Coaxial cable หรือสาย Fiber Optic ได้ หรือแลนที่ใช้คนละโปรโตคอลในการทำงาน

เราเตอร์ทำงานที่ชั้นที่ 3 ตามโมเดล OSI หน้าที่หลักของเราเตอร์ คือ การหาเส้นทางที่ดีที่สุด (Best path) ในการส่งผ่านข้อมูล และเป็นตัวกลางในการส่งต่อข้อมูลไปยังเครือข่ายอื่น โดยในแต่ละเครือข่ายจะมีรูปแบบของแพ็กเก็ตที่แตกต่างกันตามโปรโตคอลที่ทำงานในระดับบน (ตั้งแต่ชั้นที่ 3 ขึ้นไป) เช่น IP, IPX หรือ AppleTalk เราเตอร์จะใช้ที่อยู่ทางตรรกะ (Logical Address) หรือหนึ่งในตัวอย่างที่เราคุ้นเคยคือ IP Address

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



เราเตอร์จะทำการรับข้อมูลเข้ามาซึ่งตามขั้นที่ 3 ตามโมเดล OSI เรียกว่า แพ็กเกต (Packet) แล้วพิจารณาจากที่อยู่หรือ IP Address ของปลายทาง เทียบกับเส้นทางส่งข้อมูลจากตารางเส้นทาง (Routing Table) ว่าจะส่งข้อมูลนั้นออกไปทางใดจึงจะสามารถไปถึงปลายทางนั้นได้ เมื่อมีการส่งข้อมูลออกไปมีการเปลี่ยนรูปแบบของขั้นที่ 2 ตามโมเดล OSI ซึ่งเรียกหน่วยข้อมูลในขั้นที่ 2 ว่าเฟรม (Frame) และบรรจุและทำการห่อหุ้ม (Encapsulation) ให้อยู่ในรูปแบบแพ็กเกต โดยแต่ละเฟรมจะถูกเปลี่ยนแปลงที่อยู่ทางกายภาพหรือ MAC Address ของต้นทางและปลายทางใหม่ให้สอดคล้องกับเครือข่ายที่จะส่งเฟรมนั้นออกไป โดยรูปแบบและขนาดเฟรมจะต้องสอดคล้องกับช่องทางการสื่อสาร เช่น Coaxial Cable, UTP, Fiber Optic, Wi-Fi เป็นต้น

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

ลักษณะการทำงานของเราเตอร์นั้นนอกจากจะเชื่อมต่อแล้ว ยังเก็บสถานะของเครือข่ายแต่ละเซกเมนต์และสามารถทำการกรอง (Filter) หรือเลือกเฉพาะชนิดของข้อมูลที่ระบุไว้ว่าให้ผ่านไปได้ ทำให้ช่วยลดปัญหาการจราจรที่คับคั่งของข้อมูลและเพิ่มระดับความมั่นคงปลอดภัยของเครือข่าย โปรดจำไว้

โปรดจำไว้

หน่วยข้อมูลโปรโตคอล (Protocol Data Unit : PDU) ที่ส่งออกจากเราเตอร์เรียกว่าแพ็กเก็ต (Packet) จะไม่มีการเปลี่ยนแปลง IP Address ต้นทางและปลายทางตลอดการสื่อสาร และหน่วยข้อมูลในชั้นที่ 2 เรียกว่าเฟรม (Frame) จะมีการเปลี่ยนแปลงที่อยู่ทางกายภาพหรือ MAC Address ของต้นทางและปลายทางเสมอให้สอดคล้องกับเครือข่ายที่จะส่งเฟรมนั้นออกไป

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

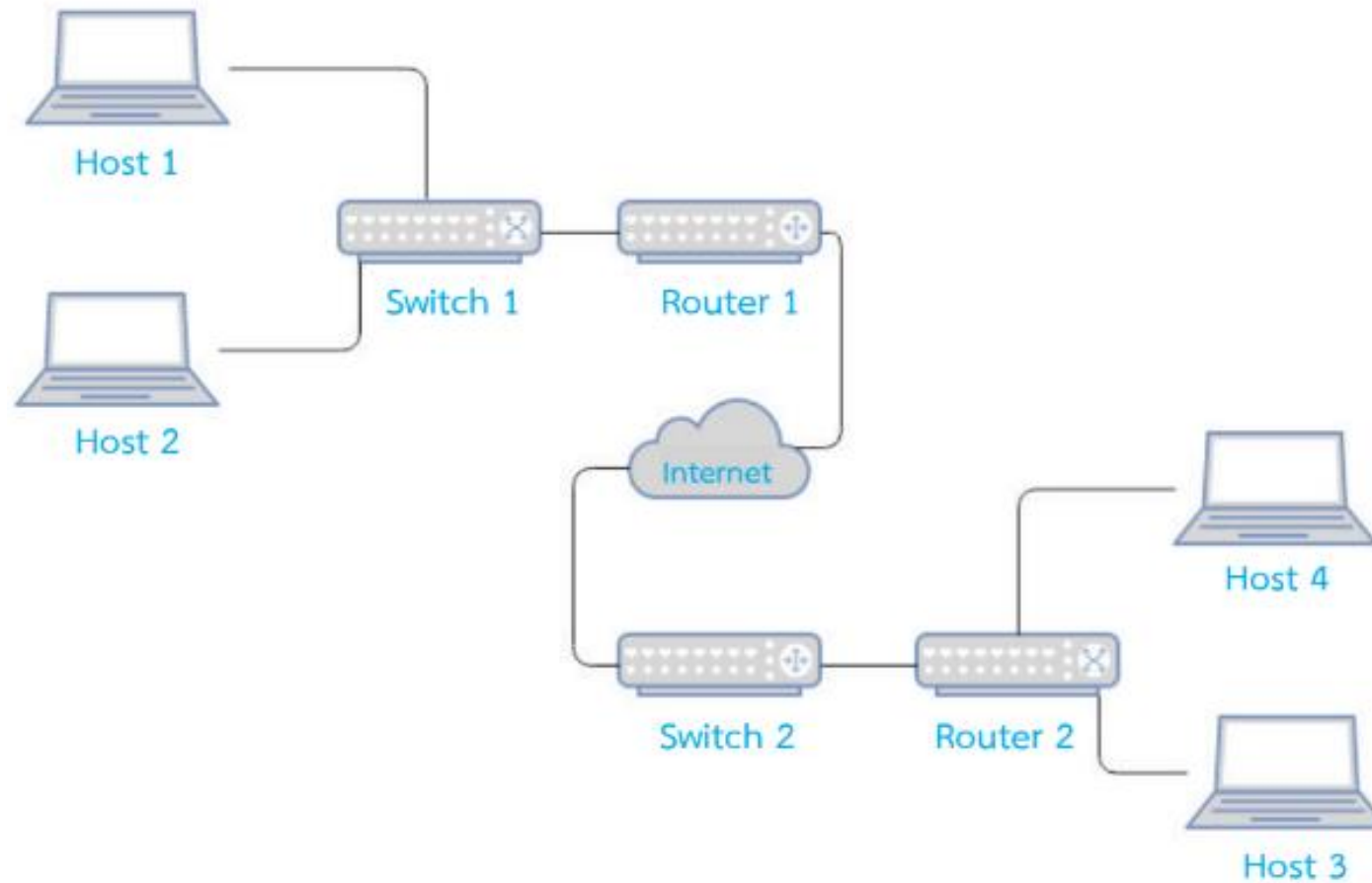


รูปที่ 4.15 เราเตอร์ (Router)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



รูปที่ 4.16 การทำงานของเราเตอร์ (Router)

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3. อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.7 อุปกรณ์เข้าใช้งานเครือข่ายไร้สาย (Wireless Access Point)

ทำหน้าที่เสมือนฮับเชื่อมเครื่องคอมพิวเตอร์ไร้สายและอุปกรณ์เครือข่ายไร้สาย (Wireless LAN) แบบต่าง ๆ เข้าด้วยกัน โดยสามารถกระจายสัญญาณ Wi-Fi หรือเชื่อมต่อกับอุปกรณ์อื่นแบบมีสายผ่านอีเทอร์เน็ตพอร์ต ช่วยทำให้อุปกรณ์ที่ทำงานทั้งแบบมีสายและไร้สายสามารถสื่อสารและทำงานรวมกันได้ผ่าน Wireless Access Point นี้ แต่ Wireless Access Point จะไม่มีพอร์ตที่สามารถเชื่อมต่อเครือข่ายแวนหรืออินเทอร์เน็ตได้ หากเป็น Wireless Access Point ที่มีพอร์ตเชื่อมต่อเครือข่ายแวนหรืออินเทอร์เน็ตได้ จะเรียกว่า Wi-Fi Router



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

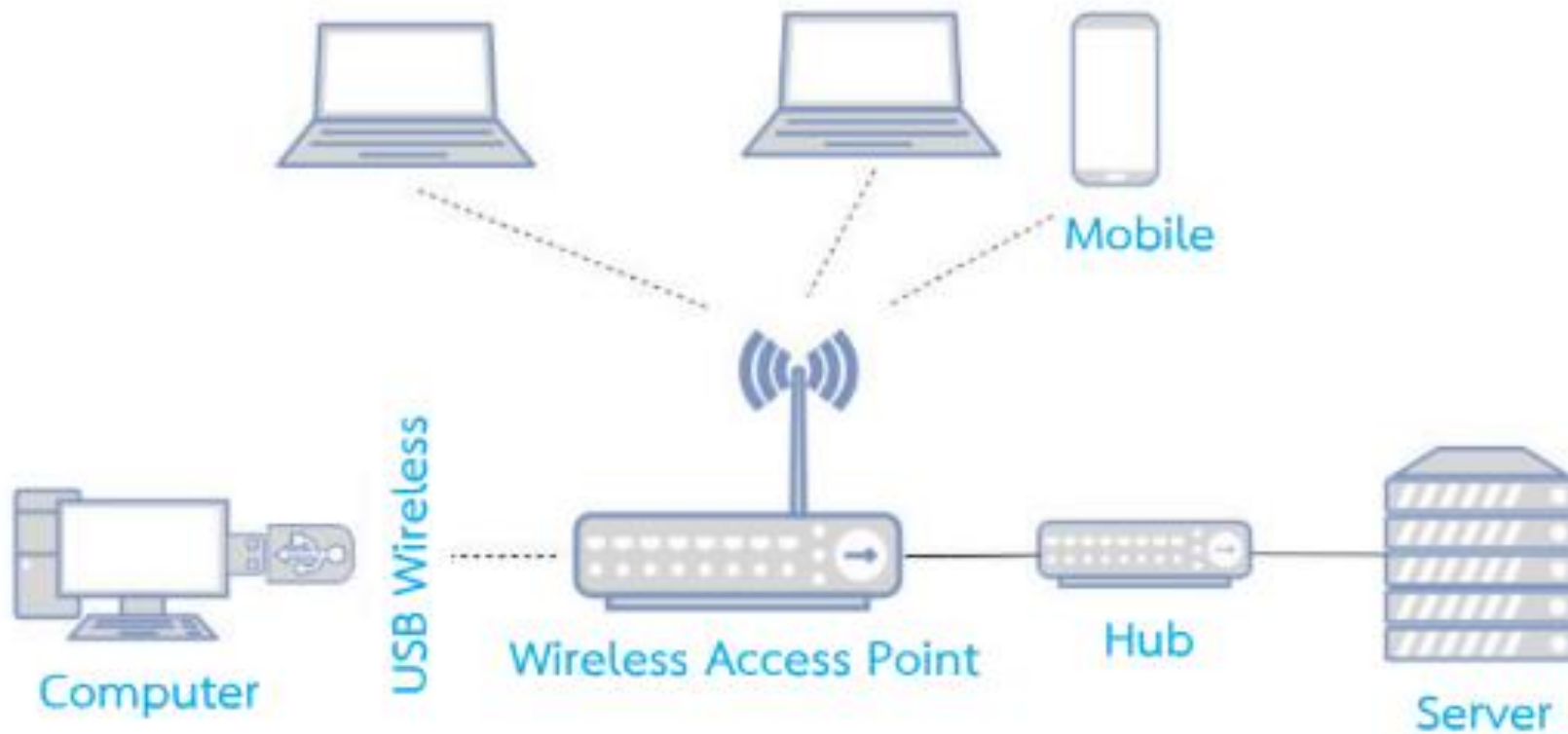


รูปที่ 4.17 อุปกรณ์เข้าใช้งานเครือข่ายไร้สายแบบ Wi-Fi Router

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

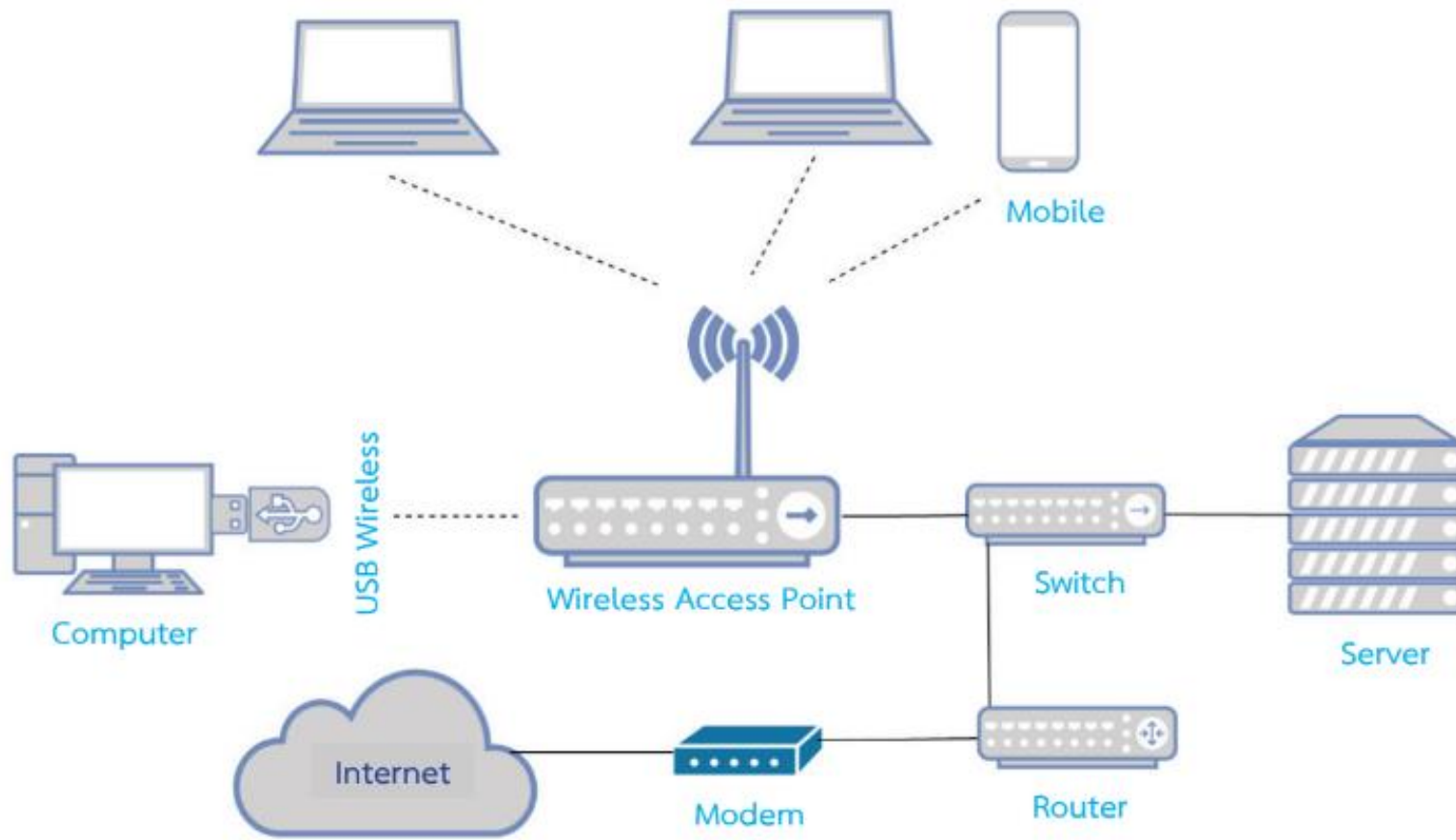


รูปที่ 4.18 การทำงานของอุปกรณ์ Wireless access point

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

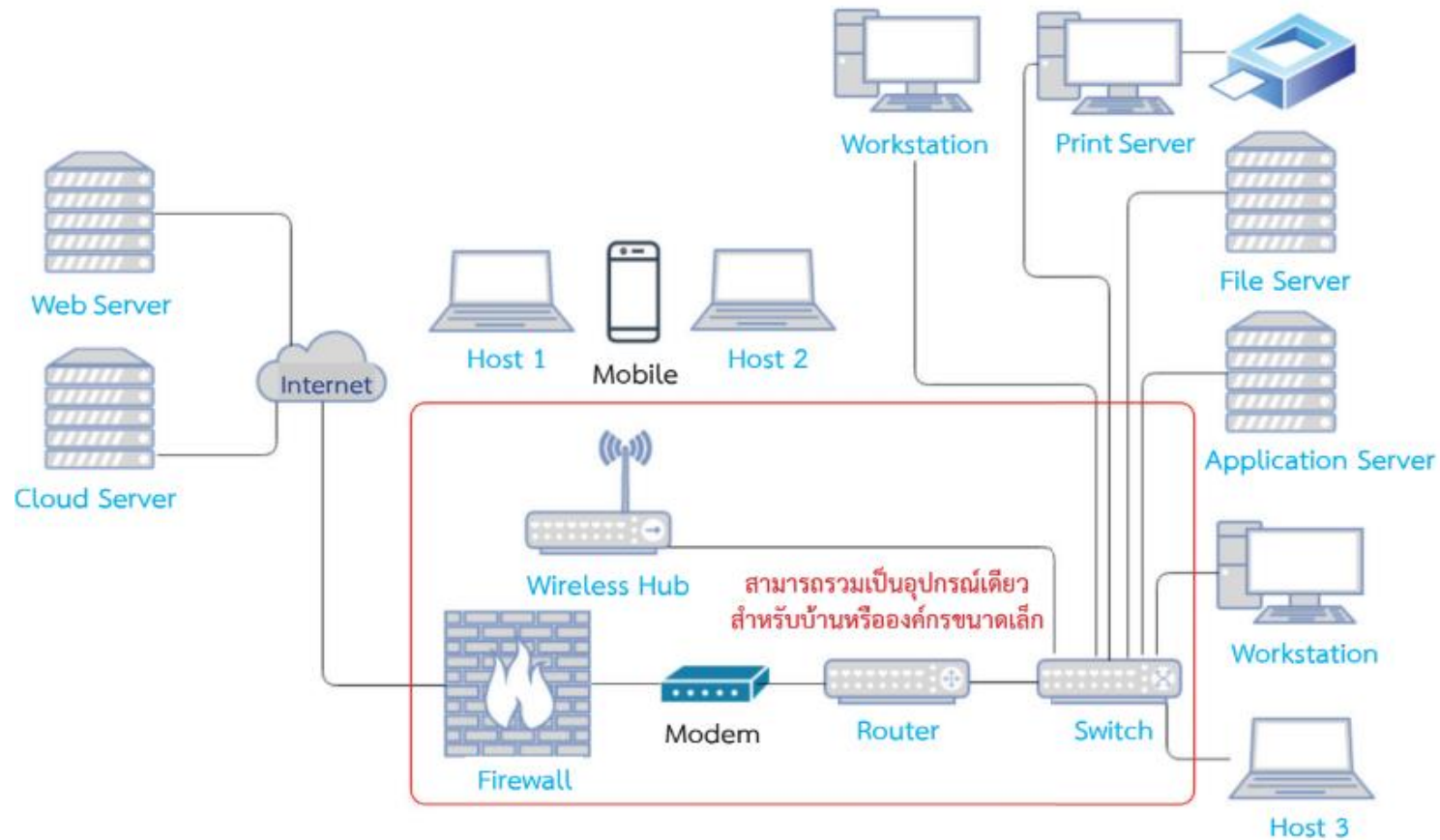


รูปที่ 4.19 การทำงานของอุปกรณ์ Wi-Fi Router

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



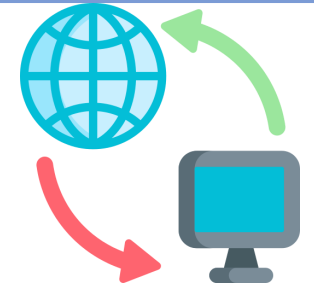
รูปที่ 4.20 ตัวอย่างการติดตั้งระบบเครือข่ายในองค์กร

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.8 ไฟร์วอลล์ (Firewall)



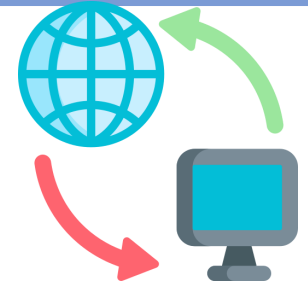
การใช้งานอินเทอร์เน็ตมีปริมาณเพิ่มสูงขึ้นทุกวัน องค์กรยังใช้งานอินเทอร์เน็ตอยู่เกือบตลอดเวลา ทั้งการติดต่อสื่อสาร การประชาสัมพันธ์ การทำงาน และกิจกรรมส่วนตัว อย่างไรก็ตามการโจรกรรมข้อมูลหรือภัยคุกคามจากเครือข่ายยังคงเกิดขึ้นอยู่ตลอดเวลาด้วยเช่นกัน ดังนั้น องค์กรจำเป็นต้องมีระบบเพื่อป้องกันภัยคุกคามเหล่านั้น หนึ่งในเทคโนโลยีที่ถูกนำมาใช้งาน คือ ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์ คือ ซอฟต์แวร์หรือฮาร์ดแวร์บนระบบเครือข่าย ทำหน้าที่เป็นตัวควบคุมและคัดกรองข้อมูลที่เข้า-ออกภายในเครือข่าย โดยต้องมีการกำหนดเกณฑ์โดยผู้ดูแลระบบให้กับไฟร์วอลล์ ไฟร์วอลล์เป็นเสมือนกำแพงที่ทำหน้าที่ป้องกันไม่ให้คอมพิวเตอร์ที่ไม่ได้รับอนุญาตที่อยู่อีกด้านของไฟร์วอลล์นั้นเข้ามาเชื่อมต่อยังคอมพิวเตอร์ที่อยู่ภายใต้ขอบเขตของไฟร์วอลล์นั้น อุปกรณ์ที่ทำหน้าที่ไฟร์วอลล์อาจจะรวมเอาฟังก์ชันการทำงานเป็นเกตเวย์ไว้ในตัวด้วย

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



3.8.1 การแบ่งประเภทไฟร์วอลล์ตามชั้นของโมเดล OSI

โดยทั่วไปจะถูกแบ่งรูปแบบการทำงานออกเป็น 2 ประเภท ได้แก่ ไฟร์วอลล์ระดับเครือข่าย (Network) และไฟร์วอลล์ระดับแอปพลิเคชัน (Application) โดยมีหลักการทำงานที่แตกต่างกันดังนี้

1) **ไฟร์วอลล์ระดับเครือข่าย (Network)** ไฟร์วอลล์จะตัดสินใจอนุญาตให้ทราฟฟิกใด ๆ ผ่านเข้ามาในเครือข่ายนั้น โดยจะตรวจสอบ IP Address ของผู้ส่งและผู้รับ รวมถึงโปรโตคอล (Protocol) ในแต่ละแพ็กเก็ต ไฟร์วอลล์ประเภทนี้มีความเร็วสูงตรวจสอบและวิเคราะห์แพ็กเก็ตในการเข้าถึงเครือข่าย

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์



2) **ไฟร์วอลล์ระดับแอปพลิเคชัน (Application) หรือ “Proxy Server”** สามารถตรวจสอบเข้าถึงเครือข่ายได้อย่างละเอียดมากกว่าระดับเครือข่าย โดยทำงานในระดับชั้นที่ 7 ของโมเดล OSI ผู้ดูแลระบบสามารถตั้งข้อกำหนดและบังคับใช้นโยบายความมั่นคงปลอดภัยได้มากกว่า แต่ไฟร์วอลล์ประเภทนี้จะมีความยุ่งยากในการกำหนดค่าการใช้งานมากกว่าไฟร์วอลล์ระดับเครือข่าย (คำศัพท์ทางเทคนิคเรียกว่า มีความโปร่งใส (Transparent) น้อย) เพราะอาจต้องตั้งค่าที่เครื่องไคลเอนต์ให้มีการเข้า-ออกเครือข่ายผ่าน Proxy Server นี้ อย่างไรก็ตาม ไฟร์วอลล์ระดับแอปพลิเคชันรุ่นใหม่ ๆ มีความสามารถในการทำงานที่โปร่งใสสำหรับผู้ใช้งานมากขึ้น ซึ่งผู้ใช้งานอาจจะไม่ต้องกำหนดค่าใด ๆ ก็สามารถใช้งานเครือข่ายได้เลย

อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3. อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

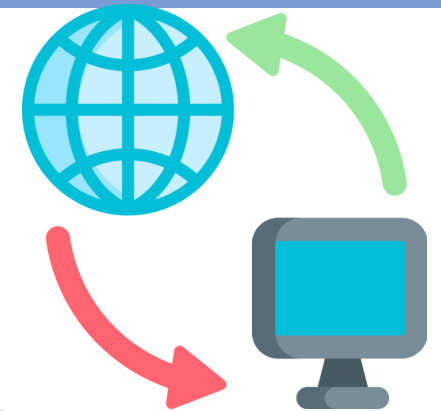
3.8.2 การแบ่งประเภทไฟร์วอลล์ตามการทำงาน

1) Packet Filtering Firewall

เป็นไฟร์วอลล์ที่จะทำการตรวจสอบแพ็กเก็ต (Packet) ว่าตรงกับเงื่อนไขหรือเกณฑ์ที่ผู้ดูแลระบบกำหนดไว้หรือไม่ ถ้าผ่านเกณฑ์ทั้งหมด ข้อมูลก็จะถูกปล่อยเข้ามาในเครือข่าย ถ้าไม่ผ่านเกณฑ์จะถูกปฏิเสธการเข้าถึงระบบเครือข่ายภายในองค์กร

2) Circuit-Level Gateway

ใช้ตรวจสอบเส้นทางการเชื่อมต่อเครือข่าย โดยทำหน้าที่พิจารณาความน่าเชื่อถือของการเชื่อมต่อโดยสร้างการจำลองเส้นทางการเชื่อมต่อ แต่ไฟร์วอลล์ประเภทนี้ไม่สามารถตรวจสอบแพ็กเก็ตได้ด้วยตนเองได้ การตรวจสอบแพ็กเก็ตจะทำงานชั้นที่ 4 (Transport Layer เป็นชั้นที่ทำหน้าที่จัดระเบียบแพ็กเก็ต) ในโมเดล OSI เป็นหลัก



อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3) Stateful Inspection Firewall

เป็นไฟร์วอลล์ที่ใช้ตรวจสอบแพ็กเก็ตซึ่งสามารถตรวจสอบได้ว่าแพ็กเก็ตนี้มีการร้องขอออกจากเครือข่ายภายในหรือไม่ โดยนำข้อมูลของแพ็กเก็ตมาเทียบกับรายการแพ็กเก็ตที่เคยร้องขอการเชื่อมต่อออกไปภายนอกมาตรวจสอบ หากตรงกันจะปล่อยให้มีการเชื่อมต่อเข้ามายังเครือข่ายภายใน หนึ่งในตัวอย่างการใช้งานที่แพร่หลาย คือ ไฟร์วอลล์ที่มีการใช้งานบน Microsoft Windows 10

4) Application-Level Gateway

เป็นไฟร์วอลล์ที่ใช้เพื่อตรวจสอบเส้นทางการส่งข้อมูลและเนื้อหาของแพ็กเก็ต นอกจากนั้นยังทำหน้าที่กรองและปิดกั้นการโจมตีที่มองไม่เห็นบนเครือข่ายในโมเดล OSI อีกด้วย



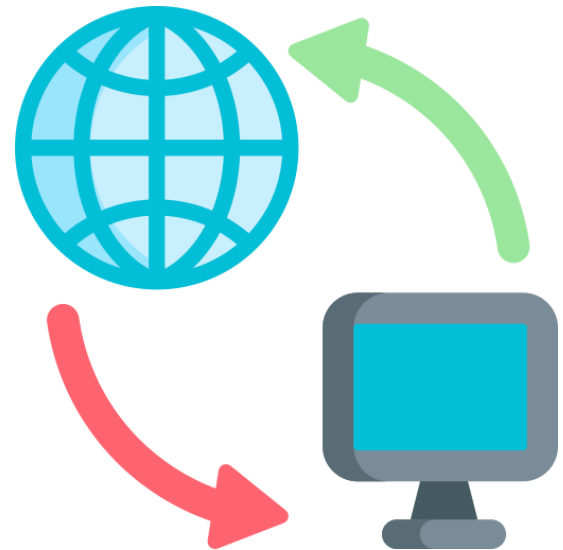
อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์และตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

3.

อุปกรณ์ตัวกลางการเชื่อมต่อเครือข่ายคอมพิวเตอร์

5) Next-Generation Firewall

ไฟร์วอลล์ที่รวมการตรวจสอบเส้นทางเครือข่ายและแพ็กเก็ตไว้ด้วยกัน โดยสามารถตรวจสอบแพ็กเก็ตในเชิงลึก (Deep Packet Inspection) เป็นวิธีการขั้นสูงในการตรวจสอบแพ็กเก็ตและเครือข่าย เป็นการรวมรูปแบบการตรวจสอบแพ็กเก็ตที่หลากหลาย รวมถึงการตรวจจับป้องกันมัลแวร์ และไวรัส โดยการตรวจสอบที่มาของการเชื่อมต่อผ่าน IP Address ของผู้เชื่อมต่อที่ขอเข้ามายังเครือข่ายภายใน



สื่อกลางเครือข่ายคอมพิวเตอร์



สรุปท้ายหน่วย

การใช้งานภายในบ้านหรือองค์กรที่มีเครือข่ายขนาดเล็กสามารถใช้อุปกรณ์เพียงตัวเดียวเพื่อทำงานเป็นไฟร์วอลล์ โมเด็ม และเราเตอร์จนถึงเป็นตัวกระจายสัญญาณไร้สายได้ การติดตั้งเครือข่ายจึงทำได้ง่ายมาก อย่างไรก็ตาม การเข้าใจคุณสมบัติและความสามารถของอุปกรณ์แต่ละประเภทแต่ละรุ่นก็ยังมีความจำเป็นสำหรับผู้ใช้อยู่ เพื่อให้สามารถเลือกใช้เทคโนโลยีที่เหมาะสมกับงานและงบประมาณมากที่สุด

ผู้ออกแบบระบบเครือข่ายต้องระลึกอยู่เสมอว่าประสิทธิภาพสูงสุดของระบบเครือข่ายจะขึ้นอยู่กับประสิทธิภาพต่ำสุดของอุปกรณ์ที่ต่อเชื่อมอยู่ในระบบ เช่น การใช้บริการอินเทอร์เน็ตความเร็วสูงขนาด 1 Gbps แต่กลับใช้สวิตช์ที่รองรับการทำงานสูงสุดที่ 100 Mbps ระบบจะทำงานได้สูงสุดที่ 100 Mbps เท่านั้น หรือกรณีที่พบบ่อย คือ การที่เครือข่ายไร้สายในบ้านที่รองรับความเร็วสูงสุดที่ 500-600 Mbps แต่อุปกรณ์ปลายทาง เช่น สมาร์ทโฟนสามารถรับสัญญาณความเร็วสูงสุดได้เพียง 100-300 Mbps ย่อมส่งผลให้ผู้ใช้ไม่ได้รับประสิทธิภาพการทำงานที่สูงสุดตามที่ผู้ให้บริการติดตั้งมา

สื่อกลางเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย



อีกกรณีหนึ่งที่ต้องคำนึงถึงคือ ความจำเป็นในการเลือกใช้อุปกรณ์และความเร็วให้เหมาะสมกับการทำงาน เพราะมักจะพบว่าแอปพลิเคชันส่วนใหญ่ในปัจจุบันยังไม่ต้องการความเร็วในการรับส่งข้อมูลสูงมากนัก เช่น การดูสตรีมมิงภาพยนตร์ในระดับ 4K ต้องการแบนด์วิดท์เพียง 50 Mbps เท่านั้น แต่ต้องการเสถียรภาพหรือความนิ่งของความเร็ว หรือเกมออนไลน์ส่วนใหญ่ต้องการแบนด์วิดท์ในระดับเพียง 10 Mbps แต่ต้องการความเร็วในการตอบสนองที่ดีมาก ๆ หรือเวลาหน่วง (Latency) ที่ต่ำมาก ๆ เป็นต้น

หากผู้ออกแบบระบบเข้าใจถึงความต้องการทรัพยากรเครือข่ายของแอปพลิเคชันต่าง ๆ ที่จะใช้งาน ก็จะส่งผลให้เกิดความคุ้มค่าในการใช้ทรัพยากรและการลงทุนในระบบเครือข่ายมากที่สุดเช่นกัน



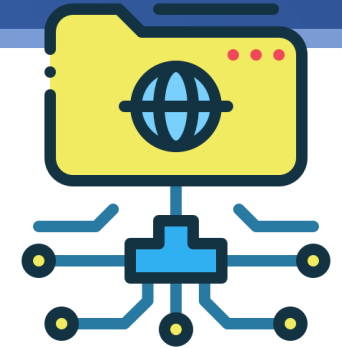
โปรโตคอลและรูปแบบ การเชื่อมต่อเครือข่าย คอมพิวเตอร์



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



1.1 ความหมายของโพรโทคอล



โพรโทคอล คือ ข้อตกลงที่ใช้ควบคุมการสื่อสารข้อมูลในเครือข่าย เพื่อให้การสื่อสารของระบบคอมพิวเตอร์แต่ละเครื่องสื่อสารกันได้ โพรโทคอลจะทำหน้าที่สื่อกลางในการสื่อสารเพื่อให้อุปกรณ์ต่าง ๆ สามารถทำงานร่วมกันได้อย่างราบรื่นในเครือข่ายคอมพิวเตอร์ อุปกรณ์จะสื่อสารกันได้อย่างไรก็การ ทำงานเชื่อมต่อเป็นเครือข่ายเข้าด้วยกัน การกำหนดรูปแบบการสื่อสาร ขนาดของแพ็กเก็ตการสื่อสารรวมถึงการสร้าง ดูแลรักษาและแก้ไขปัญหาของการสื่อสาร และอื่น ๆ อีกมากมาย

การเชื่อมต่อระหว่างระบบและอุปกรณ์หรือเป็นผู้ผลิตคนละรายกันมีความแตกต่างกัน หากขาด โพรโทคอลที่ทำงานร่วมกันได้ก็ทำให้การสร้างเครือข่ายเป็นเรื่องยากมาก ดังนั้นจะเห็นว่าโพรโทคอลเป็นสิ่งที่ สำคัญมากสำหรับเครือข่ายคอมพิวเตอร์



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

1.2 ความสำคัญของโพรโทคอล



หน่วยงานกำหนดมาตรฐานสากล คือ International Standards Organization (ISO) กำหนดโครงสร้างทั้งหมดที่จำเป็นต้องใช้ในการสื่อสารข้อมูลและเป็นระบบเปิด เพื่อให้ผู้ผลิตต่าง ๆ สามารถแยกผลิตได้ตามความถนัดของตนเอง แต่ต้องสามารถนำไปใช้ร่วมกันได้ เช่น บางรายเชี่ยวชาญในการพัฒนาซอฟต์แวร์บางรายเชี่ยวชาญการผลิตอุปกรณ์ หรือรูปแบบในการเก็บไฟล์ข้อมูล เป็นต้น



ระบบเครือข่ายคอมพิวเตอร์จะถูกออกแบบให้มีโครงสร้างที่แน่นอน และเพื่อเป็นการลดความซับซ้อนระบบเครือข่ายส่วนมากจึงแยกการทำงานออกเป็นชั้นหรือเลเยอร์ (Layer) โดยกำหนดหน้าที่ในแต่ละชั้นไว้อย่างชัดเจน แบบจำลองสำหรับอ้างอิงแบบ OSI (Open System Interconnection Reference Model) จะบรรยายถึงโครงสร้างของสถาปัตยกรรมเครือข่ายในอุดมคติ ซึ่งระบบเครือข่ายที่เป็นไปตามสถาปัตยกรรมนี้จะเป็นระบบเครือข่ายแบบเปิด และอุปกรณ์ในระบบเครือข่ายจะสามารถทำงานร่วมกันได้โดยไม่ขึ้นกับว่าเป็นอุปกรณ์ของผู้ขายรายใด

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

1.3 ตัวอย่างของโพรโทคอลหรือมาตรฐานที่นำมาใช้งาน

ในการทำงานตามแบบจำลองสำหรับ
อ้างอิงแบบ OSI นั้น แต่ละชั้นล้วนมี
โพรโทคอลหรือมาตรฐานที่ใช้ในการ
ทำงาน ยกตัวอย่างบางส่วนได้ดังนี้

ชั้นที่	ชั้นหรือเลเยอร์	ตัวอย่างของโพรโทคอลหรือมาตรฐานที่นำมาใช้งาน
7	ชั้นการประยุกต์หรือแอปพลิเคชัน (Application layer)	HTTP, HTTPS, NNTP, FTP, DHCP, NTP, Telnet, SSH, SNMP, SMTP, POP3, IMAP
6	ชั้นการนำเสนอหรือพรีเซนเตชัน (Presentation layer)	ASCII, MIME, BMP, GIF, JPEG, PNG, WAV, AVI, MPEG, TLS
5	ชั้นเซสชัน (Session layer)	RPC, PPTP, SCP, SDP
4	ชั้นขนส่งหรือทรานสปอร์ต (Transport layer)	TCP, UDP, SCTP, RTP, RTCP
3	ชั้นเครือข่ายหรือเน็ตเวิร์ก (Network layer)	IPv4, IPv6, ICMP, ARP
2	ชั้นเชื่อมโยงข้อมูลหรือดาตาลิงก์ (Data link layer)	CSMA/CD, CSMA/CA, LLDP, CDP, Ethernet
1	ชั้นกายภาพหรือฟิสิคัล (Physical layer)	USB, OTN, IEEE.802.11, IEEE.802.3, EIA RS-232, Bluetooth physical layer

ตารางที่ 5.1 ตัวอย่างของโพรโทคอลหรือมาตรฐานที่นำมาใช้งานในแต่ละชั้นของโมเดล OSI

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

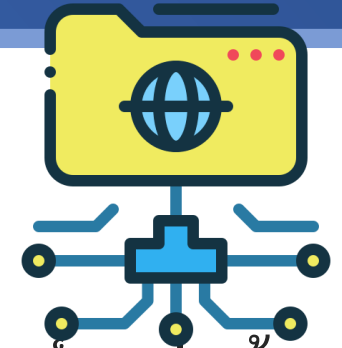
โพรโทคอล (Protocol)

1.3.1 ชั้นการประยุกต์หรือแอปพลิเคชัน (Application layer protocol)

ชั้นนี้เป็นส่วนติดต่อระหว่างโปรแกรมประยุกต์ของเครือข่ายกับผู้ใช้ โดยคอมพิวเตอร์จะแปลงข้อมูลที่ที่ได้รับจากผู้ใช้เข้าสู่ระบบ เช่น การเข้าใช้งานระบบคอมพิวเตอร์ที่อยู่ในเครือข่าย การถ่ายโอนข้อมูลและอีเมล ตัวอย่างโพรโทคอลที่นิยมใช้งาน เช่น

 HTTP (Hypertext Transfer Protocol) เป็นโพรโทคอลสำหรับการถ่ายโอนข้อมูลผ่านอินเทอร์เน็ตและเว็บไซต์ (www) มักจะเรียกใช้โพรโทคอลนี้ผ่านโปรแกรมเว็บเบราว์เซอร์ (Browser)

 HTTPS (Hypertext Transfer Protocol Secure) เป็นโพรโทคอลสำหรับการถ่ายโอนข้อมูลผ่านอินเทอร์เน็ตและเว็บไซต์ (www) เช่นเดียวกับ HTTP แต่มีการเพิ่มการรักษาความมั่นคงปลอดภัย (Security) ทำให้ช่วยรักษาความสมบูรณ์ถูกต้องของข้อมูลผู้ใช้และเก็บข้อมูลไว้เป็นความลับระหว่างคอมพิวเตอร์ของผู้ใช้กับเว็บไซต์



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



ดังนั้นผู้ใช้ที่ต้องการออนไลน์อย่างปลอดภัยและเป็นส่วนตัวระหว่างที่ใช้เว็บไซต์ จึงควรเลือกใช้ HTTPS เพื่อปกป้องเนื้อหาในเว็บไซต์ตลอดระยะเวลาการเชื่อมต่อของผู้ใช้กับเว็บไซต์ ข้อมูลที่ส่งด้วย HTTPS จะได้รับการรักษาความมั่นคงปลอดภัยผ่านโพรโทคอล Transport Layer Security (TLS) ซึ่งให้การปกป้องหลัก 3 ชั้นดังนี้

🌐 การเข้ารหัส (Encryption) หมายถึง การเข้ารหัสข้อมูลที่แลกเปลี่ยนเพื่อรักษาความปลอดภัยจากผู้ลักลอบดูข้อมูล ซึ่งขณะที่ผู้ใช้เรียกดูเว็บไซต์จะไม่มีใครสามารถ “ดักฟัง” การสนทนาติดตามกิจกรรมหรือขโมยข้อมูลของการสนทนานี้ได้

🌐 ความถูกต้องครบถ้วน (Integrity) หมายถึง จะไม่สามารถแก้ไขหรือทำให้ข้อมูลเสียหายในช่วงที่ถ่ายโอนข้อมูลไม่ว่าจะมีเจตนาหรือไม่ก็ตาม

🌐 การตรวจสอบสิทธิ์ (Authentication) หมายถึง การพิสูจน์ว่าผู้ใช้สื่อสารกับเว็บไซต์ที่ต้องการโดยจะป้องกันการโจมตีแบบแทรกกลางการสื่อสาร



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

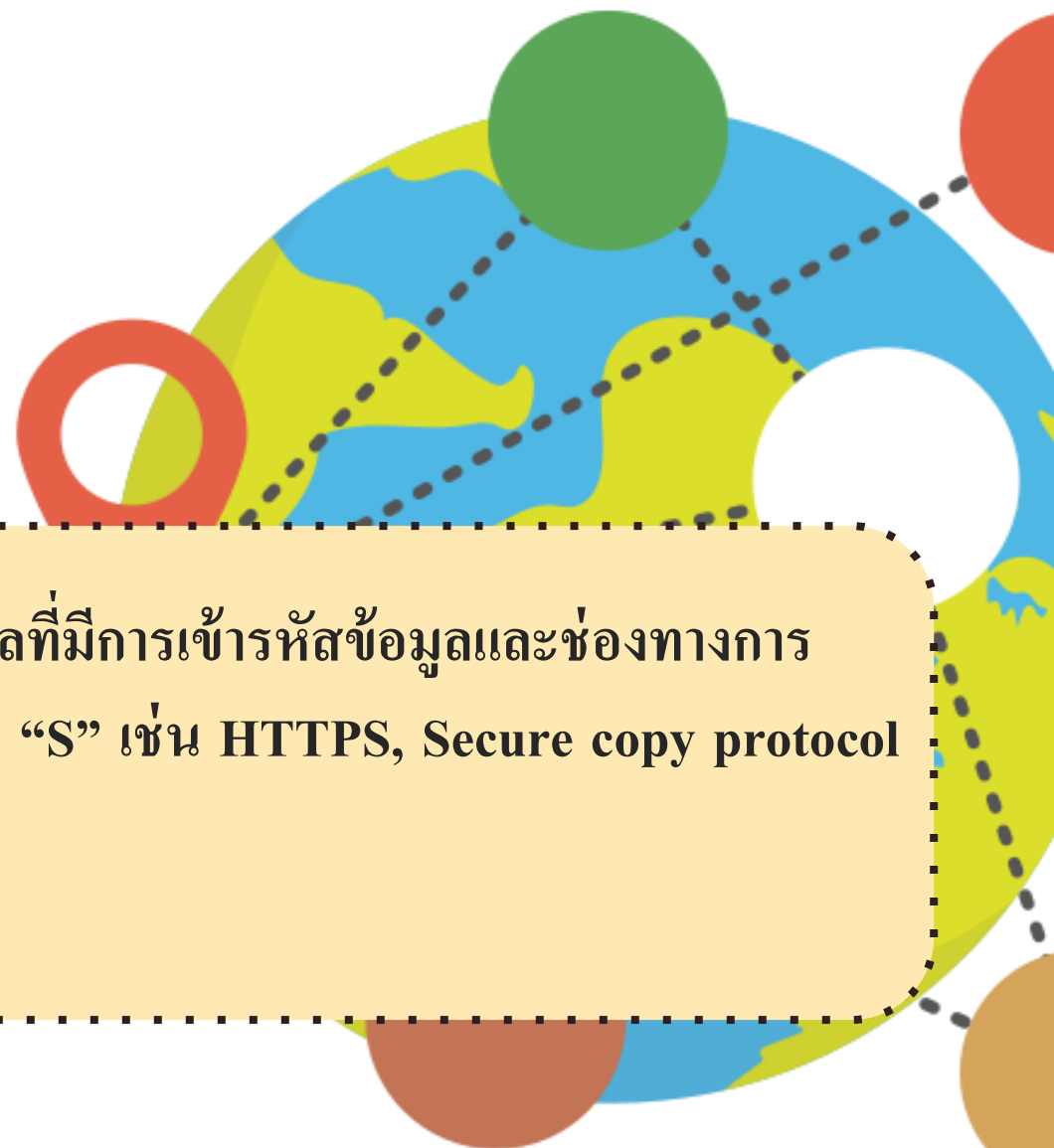
1.

โพรโทคอล (Protocol)

คุณสมบัติเหล่านี้ทำให้ผู้ใช้เกิดความเชื่อมั่น
ส่งผลต่อการดำเนินกิจกรรมหรือธุรกรรมทางธุรกิจตามมา

หมายเหตุ

หากต้องการความมั่นคงปลอดภัยควรเลือกใช้โพรโทคอลที่มีการเข้ารหัสข้อมูลและช่องทางการสื่อสาร โดยโพรโทคอลเหล่านี้มักขึ้นต้นหรือลงท้ายตัวอักษร “S” เช่น HTTPS, Secure copy protocol (SCP), SFTP (SSH File Transfer Protocol)



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

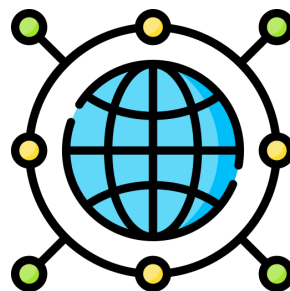


 **NNTP (Network News Transfer Protocol)** โปรโตคอลที่ใช้โอนย้ายข่าวสารระหว่างกันข้ามเครือข่ายอินเทอร์เน็ต

 **FTP (File Transfer Protocol)** โปรโตคอลที่ใช้ในการโอนย้ายแฟ้มระหว่างกัน จะใช้งานบ่อยในการอัปโหลดไฟล์ขึ้นเครื่องแม่ข่าย

 **DHCP (Dynamic Host Configuration Protocol)** โปรโตคอลที่ใช้แจกจ่ายและขอรับบริการค่า IP address สำหรับการเข้าถึงเครือข่าย

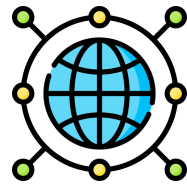
 **Domain Name System (DNS)** โปรโตคอลที่ใช้สำหรับแปลงชื่อเครื่องหรือ URL ที่ผู้ใช้ร้องขอให้ เป็น IP address



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

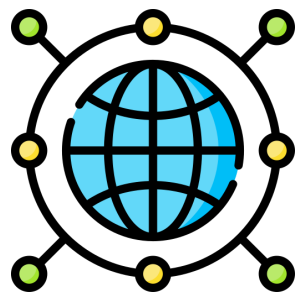
1.

โปรโตคอล (Protocol)



เนื่องจากการทำงานของเครือข่ายข้อมูลแต่ละอุปกรณ์จะระบุด้วยหมายเลข IP address เพื่อให้อุปกรณ์เหล่านั้นสามารถมีส่วนร่วมในการส่งและรับข้อความผ่านทางเครือข่ายได้ แต่คนส่วนใหญ่จะพบความยากในการจำตัวเลข IP address นี้ ดังนั้น ชื่อโดเมน (Domain names) จึงถูกสร้างขึ้นมาหรือคือ URL ที่ผู้ใช้งานพิมพ์ผ่านเว็บเบราว์เซอร์

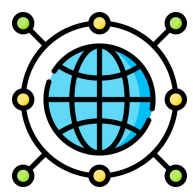
 **NTP (Network Time Protocol)** โปรโตคอลสำหรับการเทียบเวลามาตรฐานและตั้งค่าเวลาบนโฮสต์ที่ต้องการโดยอัตโนมัติผ่านระบบเครือข่าย มักใช้ในองค์กรเพื่อช่วยทำให้เวลาในเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายนั้นมีค่าตรงกัน



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

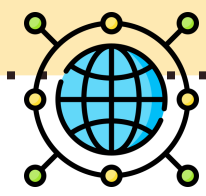
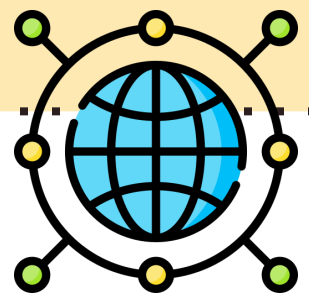
โปรโตคอล (Protocol)



Telnet โปรโตคอลที่เป็นบริการที่ช่วยให้ผู้ใช้งานสามารถเชื่อมต่อกับคอมพิวเตอร์แม่ข่ายอุปกรณ์เครือข่าย เช่น เราเตอร์ สวิตช์ หรือโฮสต์อื่น ๆ โดยใช้การเข้าถึงจากระยะไกล (Remote access) ซึ่งมักหมายถึงการที่ผู้ใช้งานไม่ได้อยู่ที่อุปกรณ์ตัวที่ต้องการทำงานด้วย อาจจะทำผ่านอินเทอร์เน็ตหรือเครือข่ายอื่น ๆ โดยผู้ใช้งานพิมพ์คำสั่ง Telnet สำหรับการเข้าถึงโปรแกรมและการบริการต่าง ๆ ที่อยู่บนโฮสต์ระยะไกลได้

ควรหลีกเลี่ยง

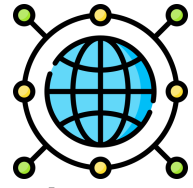
การใช้ Telnet เนื่องจากไม่ได้มีการเข้ารหัสการสื่อสาร (Encryption) ทำให้สามารถถูกดักจับอ่านข้อมูลได้



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



 **SSH (Secure Shell)** โปรโตคอลที่เป็นบริการที่ช่วยให้ผู้ใช้งานสามารถเชื่อมต่อโฮสต์อื่น ๆ โดยใช้การเข้าถึงจากระยะไกล (Remote access) ได้เช่นเดียวกับ Telnet แต่มีความมั่นคงปลอดภัยกว่าเนื่องจากการเข้ารหัสการสื่อสาร (Encryption) และมีการบังคับให้ผู้ใช้งานต้องทำการใส่ชื่อผู้ใช้งานและรหัสผ่านเพื่อการพิสูจน์ตัวตน (Authentication) ก่อนเข้าใช้งาน

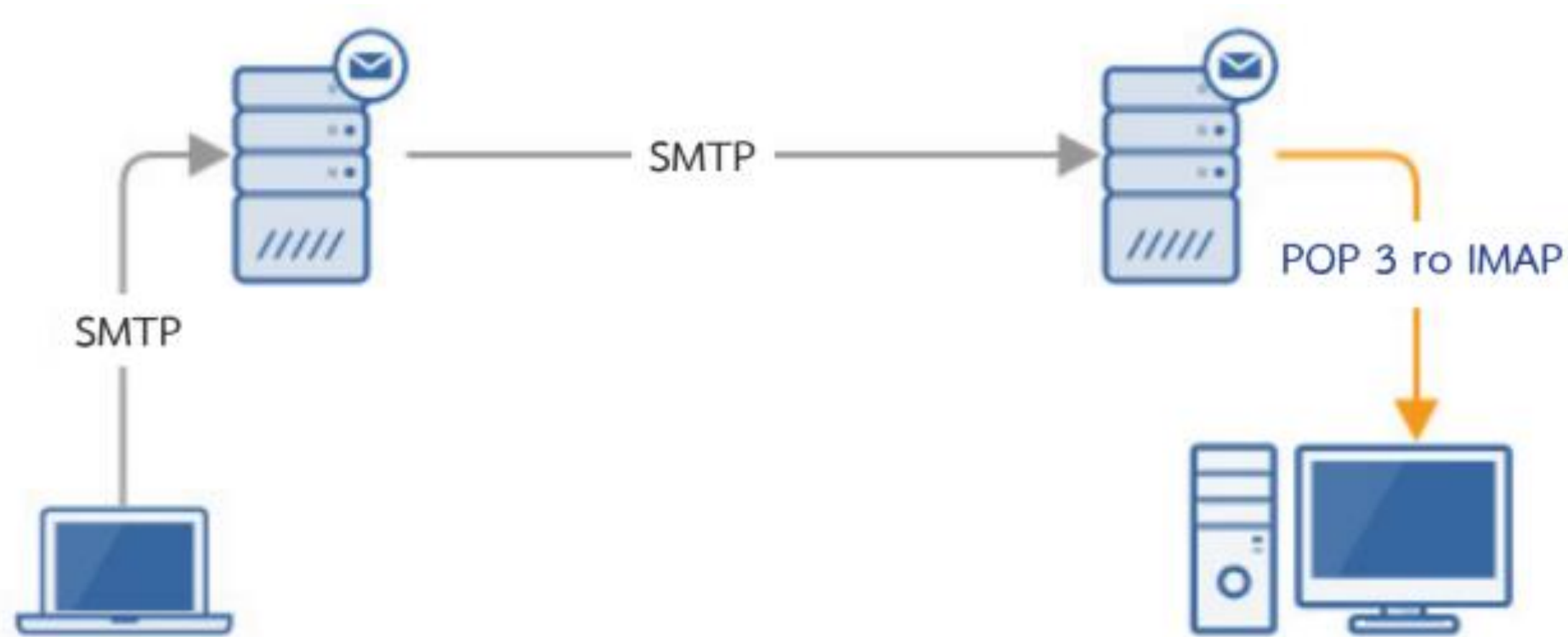


 **SNMP (Simple Network Management Protocol)** ใช้สำหรับแลกเปลี่ยนข้อมูลเกี่ยวกับการจัดการเครือข่ายระหว่างอุปกรณ์เครือข่ายหรือกลุ่มของชุดคำสั่งอย่างง่ายสำหรับการจัดการ หรือรวบรวมข้อมูลจากเอเจนต์ ผู้ใช้งานสามารถใช้จัดการอุปกรณ์เครือข่ายได้จากระยะไกล (Remote) ปัจจุบัน SNMP ได้รับความนิยมและใช้งานกันอย่างแพร่หลายในการจัดการ โดยมีอุปกรณ์หลายชนิดบนระบบเครือข่ายที่สนับสนุนการใช้งาน SNMP ได้แก่ Router, Switch, Server, Workstation และ Printer นอกจากนี้อุปกรณ์ที่ออกมาใหม่ ๆ มักจะสนับสนุน SNMP ด้วย ซึ่งช่วยให้ผู้ดูแลระบบสามารถจัดการอุปกรณ์ วิเคราะห์ปัญหา และให้ข้อมูลเพื่อใช้สำหรับวิเคราะห์สถานะของเครือข่ายในปัจจุบันและวางแผนเพื่อทำการขยายเครือข่ายในอนาคตได้อย่างมีประสิทธิภาพ



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1. โปรโตคอล (Protocol)

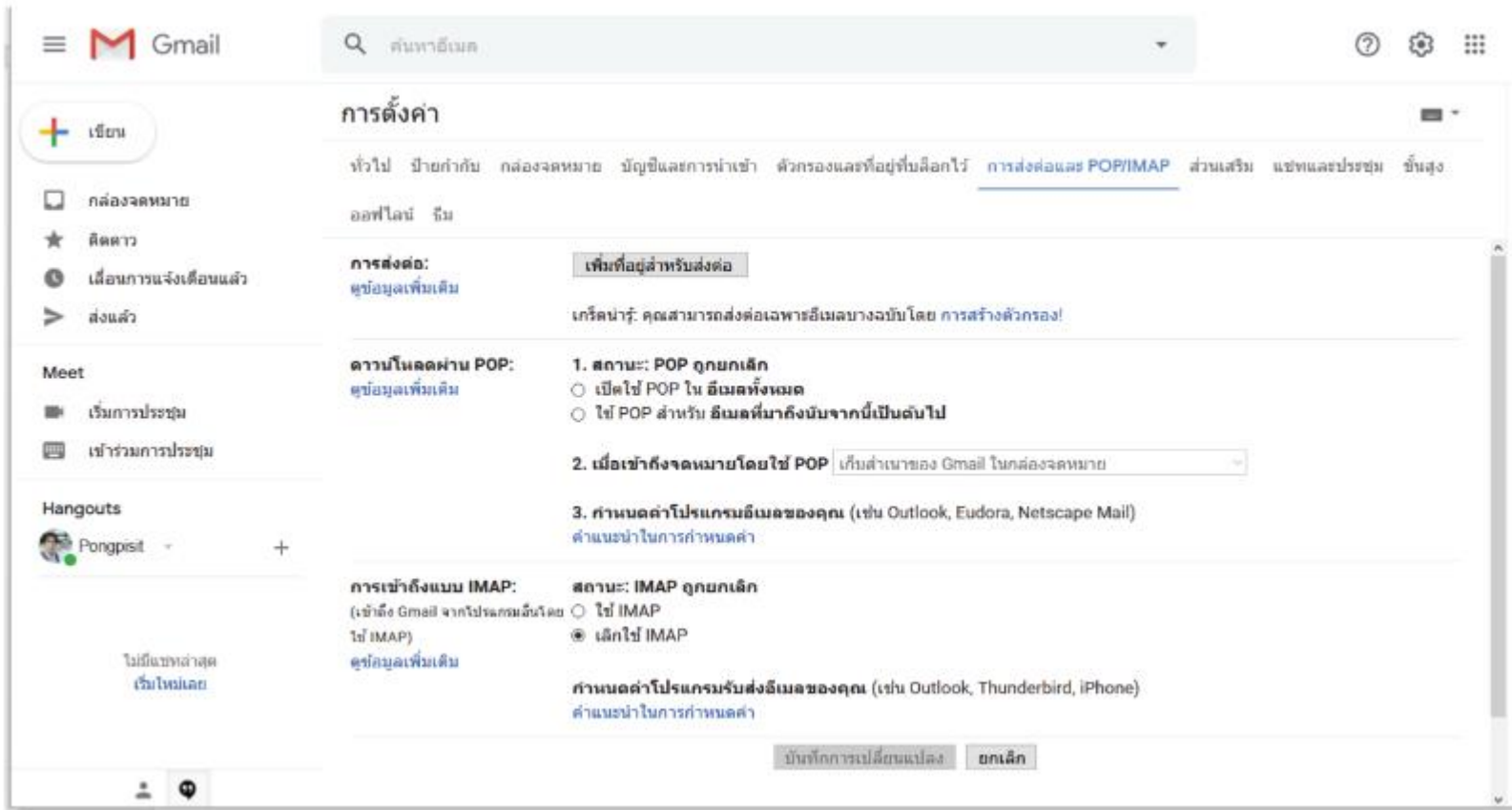


รูปที่ 5.1 การใช้โปรโตคอล SMTP ในการส่งอีเมล และใช้ POP 3 หรือ IMAP สำหรับดึงอีเมลมาอ่าน

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

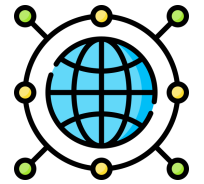
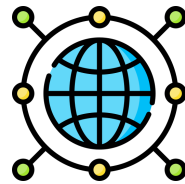


รูปที่ 5.2 ตัวอย่างหน้าจอการตั้งค่าการเข้าถึงอีเมลของ Gmail โดยใช้ POP หรือ IMAP

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



หมายเหตุ

การตั้งค่าการเข้าถึงแบบ IMAP และเปลี่ยนการตั้งค่า SMTP เพื่ออ่านข้อความ Gmail ในโปรแกรมรับส่งอีเมลอื่น ๆ เช่น Microsoft Outlook และ Apple Mail เมื่อใช้การเข้าถึงแบบ IMAP ผู้ใช้จะอ่านข้อความ Gmail ได้ในหลากหลายอุปกรณ์โดยระบบจะซิงก์ข้อความแบบเรียลไทม์ด้วย



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

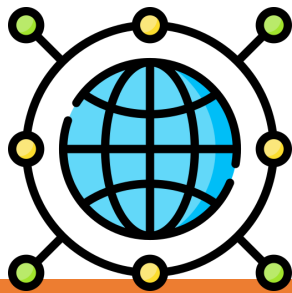


1.3.2 ชั้นการนำเสนอหรือพรีเซนเตชัน (Presentation Layer)

หน้าที่ของชั้นนี้ คือ แปลงข้อมูล (Data conversion) ที่ส่งมาให้อยู่ในรูปแบบที่โปรแกรมของเครื่องผู้รับเข้าใจ รวมทั้งการจัดรูปแบบการนำเสนอข้อมูล (Character code translation) โดยกำหนดรูปแบบภาษาชนิด และวิธีการเข้าถึงข้อมูลของเครื่องผู้ส่งให้เครื่องผู้รับเข้าใจ เช่น การนำเสนอผ่านเว็บ เป็นต้น การบีบอัดข้อมูล (Data compression) การเข้ารหัสและถอดรหัสข้อมูล (Encryption and decryption)

ดังนั้น ในชั้นนี้โพรโทคอลและมาตรฐานส่วนใหญ่จะเป็นการกำหนดรูปแบบไฟล์ต่าง ๆ เช่น ASCII, MIME, BMP, GIF, JPEG, PNG, WAV, AVI และ MPEG เป็นต้น

นอกจากนี้ยังรวมถึง Transport Layer Security (TLS) ที่กล่าวไปก่อนหน้านี้ในการทำงานร่วมกับ HTTPS



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

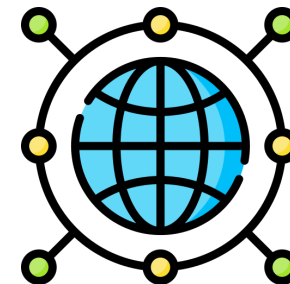
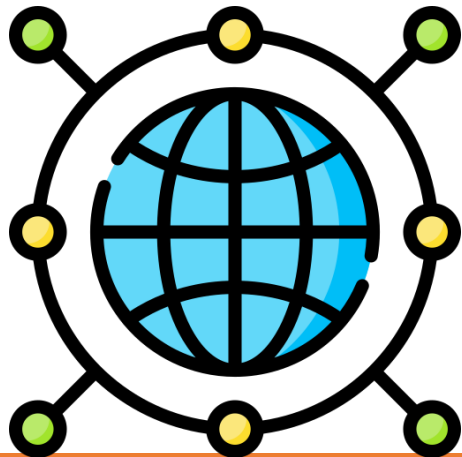
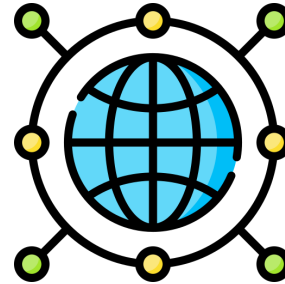
1.

โพรโทคอล (Protocol)

1.3.3 ชั้นเซสชัน (Session Layer)

ทำหน้าที่สร้างการติดต่อระหว่างเครื่องต้นทางและปลายทาง ตลอดจนดูแลการส่งข้อมูลระหว่างเครื่องทั้งสองให้ถูกต้องและมีประสิทธิภาพ โดยกำหนดขอบเขตการรับส่ง คือ กำหนดจุดผู้รับและผู้ส่งโดยจะเพิ่มเติมรูปแบบการรับส่งข้อมูลว่าเป็นแบบข้อมูลชุดเดียว หรือหลายชุดพร้อม ๆ กัน เช่น โมดูล (Module) ของการนำเสนอผ่านเว็บ

ตัวอย่างโพรโทคอลในชั้นนี้ เช่น Remote procedure call protocol (RPC), Point-to-Point Tunneling Protocol (PPTP), Session Control Protocol (SCP), Session Description Protocol (SDP) เป็นต้น

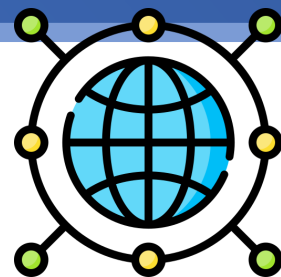


โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

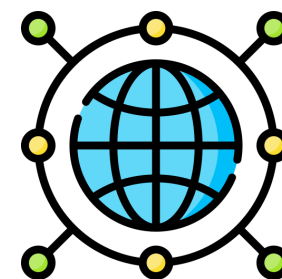
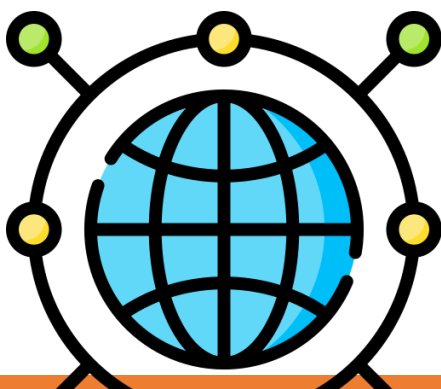
โพรโทคอล (Protocol)



1.3.4 ชั้นขนส่งหรือทรานสปอร์ต (Transport Layer)

บทบาทของทรานสปอร์ตเลเยอร์ในการห่อหุ้ม (Encapsulation) ข้อมูลที่มาจากแอปพลิเคชัน (Application Data) เพื่อที่จะให้สามารถใช้งานได้โดยเน็ตเวิร์กเลเยอร์ นอกจากนี้ ทรานสปอร์ตเลเยอร์ยังมีฟังก์ชันต่าง ๆ เช่น

- 🌐 ทำให้หลาย ๆ แอปพลิเคชันสื่อสารผ่านเครือข่ายในเวลาเดียวกันในอุปกรณ์ตัวเดียวกันได้
- 🌐 ทำให้แน่ใจว่าข้อมูลทั้งหมดที่จะได้รับโดยแอปพลิเคชันที่ต้องการ (ถ้าจำเป็น) ข้อมูลนั้นจะมีความน่าเชื่อถือ และในลำดับที่ถูกต้องขึ้นอยู่กับลักษณะของแอปพลิเคชันว่ามีความจำเป็นหรือไม่ เพราะบางแอปพลิเคชันต้องการความเร็วแต่ไม่ต้องครบถ้วน ในขณะที่บางแอปพลิเคชันต้องการความครบถ้วนของข้อมูลแม้ว่าต้องใช้เวลาในการรอ



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

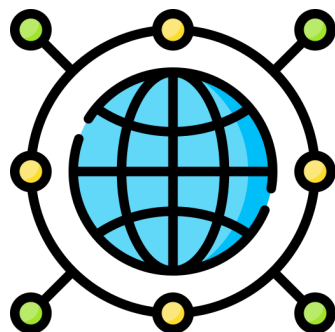
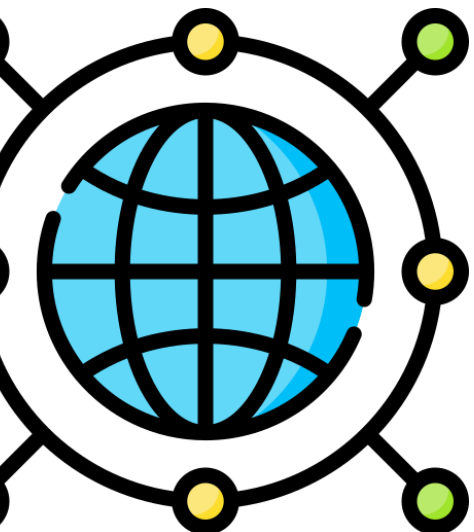
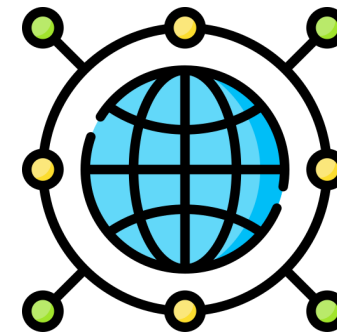
โพรโทคอล (Protocol)



ใช้กลไกในการจัดการข้อผิดพลาด (Error Handling Mechanism)

ในชั้นนี้มีอยู่โพรโทคอลหลากหลาย เช่น SCTP (Stream Control Transmission Protocol), RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol), TCP (Transfer Control Protocol) และ User Datagram Protocol (UDP) เป็นต้น

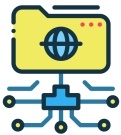
โดยจะกล่าวเพิ่มเติมถึงโพรโทคอลในชั้นนี้ที่รู้จักกันอย่างแพร่หลาย คือ TCP และ UDP เท่านั้น



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



Transmission Control Protocol (TCP)

TCP เป็นโปรโตคอลเชิงเชื่อมต่อ (Connection-oriented protocol) อธิบายไว้ใน RFC 793 โดย TCP มีโอเวอร์เฮด (Overhead) เพิ่มขึ้นเพื่อที่จะให้บริการฟังก์ชันต่าง ๆ โดย TCP คือ การนำส่งที่เรียงลำดับ (Same order delivery) การนำส่งที่เชื่อถือได้ (Reliable delivery) และการควบคุมการไหล (Flow control) ดังนั้น จึงส่งผลให้การสื่อสารของ TCP จะเป็นรูปแบบ 1 ต่อ 1 หรือยูนิคาสต์ (Unicast) แต่ละเซกเมนต์ของ TCP มีโอเวอร์เฮด 20 ไบต์ ในส่วนหัวที่ห่อหุ้ม (Encapsulation) ข้อมูลแอปพลิเคชันเลเยอร์ในแต่ละเซกเมนต์ของ UDP มีโอเวอร์เฮดเพียง 8 ไบต์ แอปพลิเคชันที่ใช้ TCP เช่น



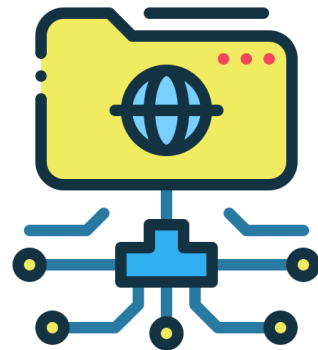
Web Browser



E-mail



File Transfer

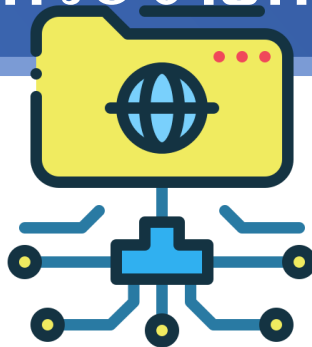


หน่วยข้อมูลโปรโตคอล (Protocol Data Unit : PDU) ของ TCP จะเรียกว่า เซกเมนต์ (Segment)

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



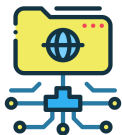
User Datagram Protocol (UDP)

UDP เป็นโปรโตคอลที่ไม่ต้องมีการเชื่อมต่อ (Connectionless) อธิบายไว้ใน RFC 768 โดย UDP มีความได้เปรียบในเรื่องการจัดข้อมูลด้วยโอเวอร์เฮดต่ำ ขึ้นข้อมูลในการติดต่อสื่อสารใน UDP.เรียกว่า ดาตาแกรม (Datagram) โดยดาตาแกรมเหล่านี้จะถูกส่งด้วยวิธีการ “Best..effort” โดยทรานสปอร์ตเลเยอร์โปรโตคอลนี้ การสื่อสารของ UDP สามารถทำได้ทั้ง 3 รูปแบบ ได้แก่ ยูนิคาสต์ (Unicast) มัลติคาสต์ (Multicast) และบรอดคาสต์ (Broadcast) แอปพลิเคชันที่ใช้ TCP เช่น

 Domain Name System (DNS)

 Video Streaming

 Voice over IP (VoIP)

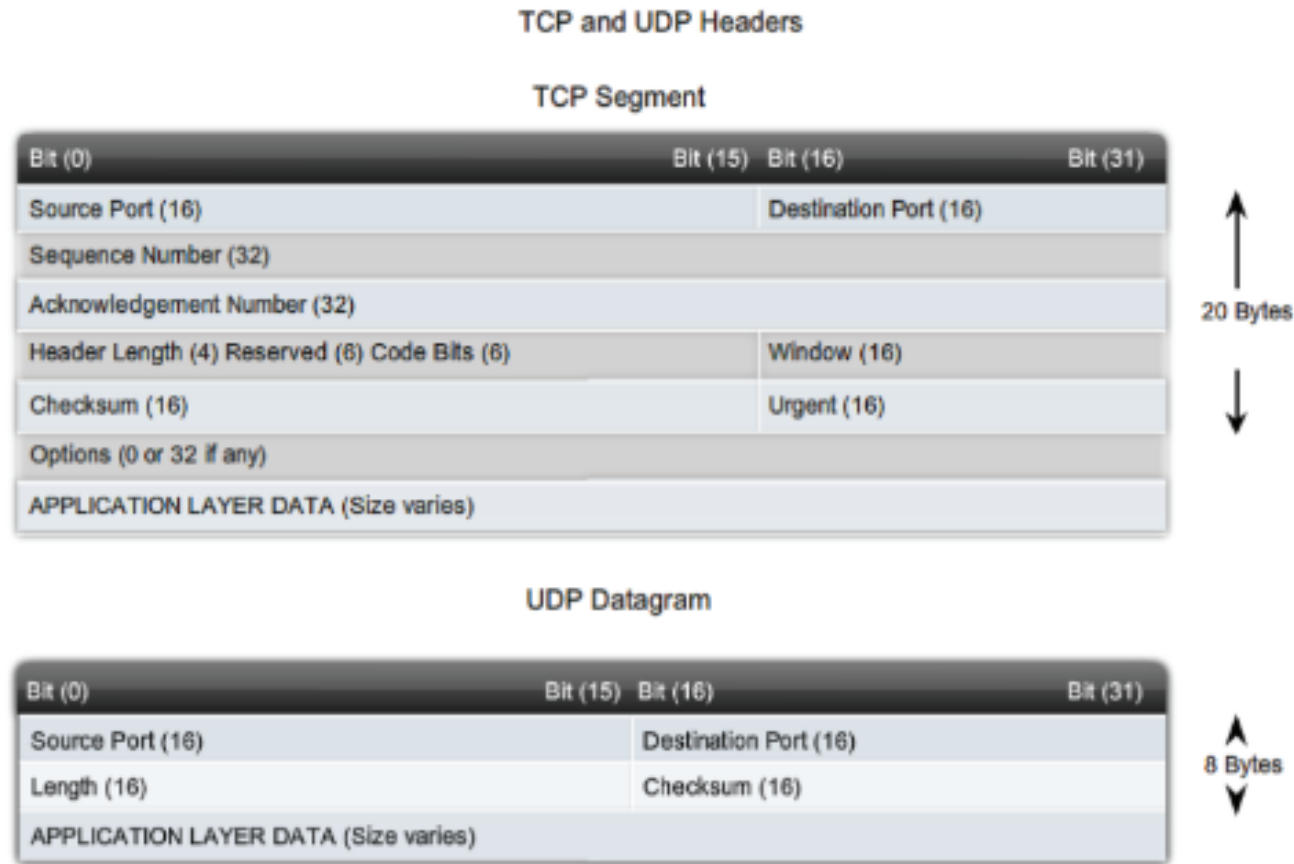


หน่วยข้อมูลโปรโตคอล (Protocol Data Unit : PDU) ของ UDP จะเรียกว่า ดาตาแกรม (Datagram)

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

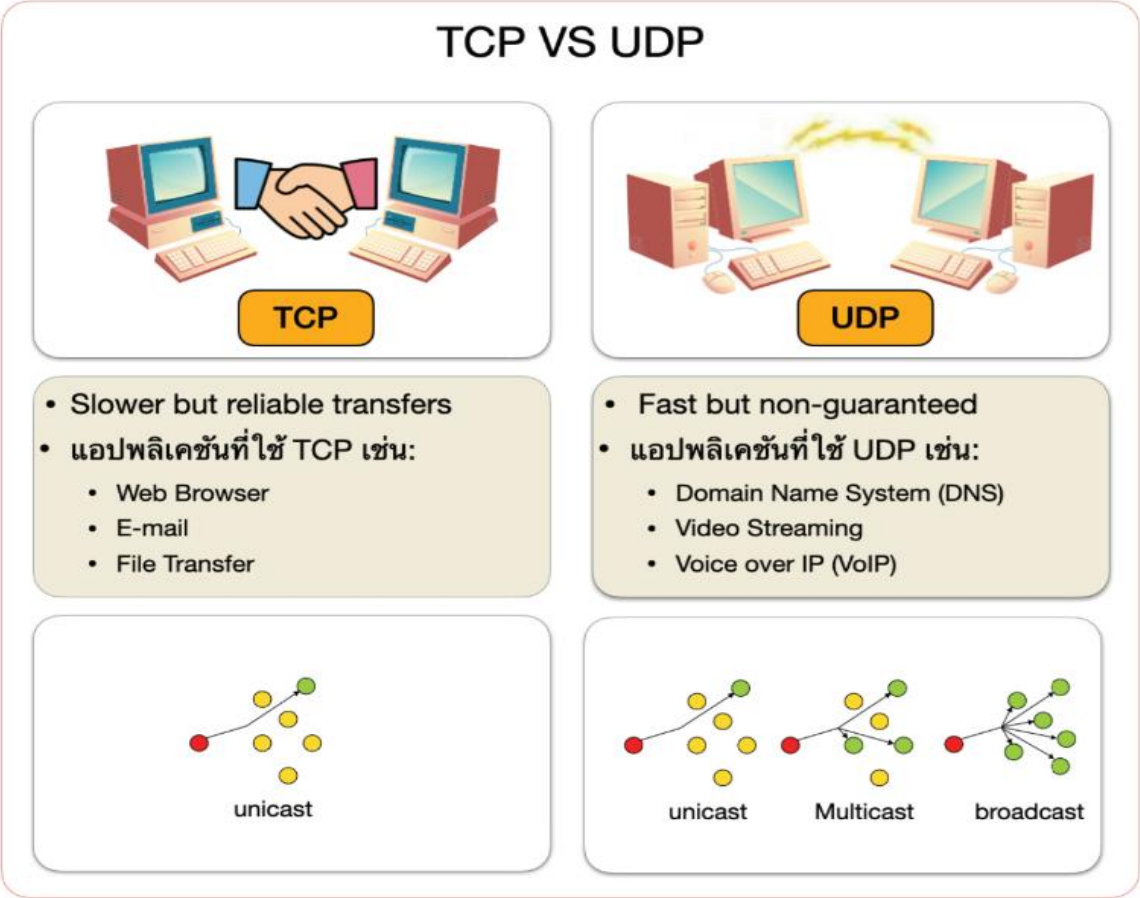


รูปที่ 5.3 TCP header และ UDP header (รูปจาก Cisco)

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



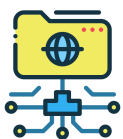
รูปที่ 5.4 เปรียบเทียบการทำงานของ TCP และ UDP

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



แอดเดรสของพอร์ต (Port Addressing)

TCP และ UDP อยู่บนพื้นฐานของบริการที่ขึ้นอยู่กับแอปพลิเคชันต่าง ๆ ที่มีการติดต่อสื่อสารกันเพื่อแยกความแตกต่างของเซกเมนต์และดาตาแกรมสำหรับแต่ละแอปพลิเคชัน ทั้ง TCP และ UDP จะมีฟิลด์ส่วนหัวคือหมายเลขพอร์ต (Port number) เป็นตัวระบุเอกลักษณ์ (Unique identifier) ที่ไม่ซ้ำกันที่ใช้ระบุแอปพลิเคชันเหล่านี้ได้

ในส่วนหัวของแต่ละเซกเมนต์หรือดาตาแกรมมีพอร์ต (Port) ต้นทางและพอร์ตปลายทาง หมายเลขพอร์ตต้นทางคือหมายเลขสำหรับการสื่อสารที่เกี่ยวข้องกับแอปพลิเคชันที่มีต้นกำเนิดในคอมพิวเตอร์นั้น หมายเลขพอร์ตปลายทางเป็นหมายเลขสำหรับการสื่อสารที่เกี่ยวข้องกับแอปพลิเคชันปลายทางในคอมพิวเตอร์ปลายทาง

หมายเลขพอร์ตได้รับมอบหมายในรูปแบบต่าง ๆ ขึ้นอยู่กับว่าข้อความเป็นคำขอหรือการตอบสนองขณะที่กระบวนการที่เซิร์ฟเวอร์ (Server process) มีหมายเลขพอร์ตแบบคงที่ที่กำหนดไว้ให้กับแต่ละ Server process เช่น TCP พอร์ต 80 เป็นพอร์ตเริ่มต้นที่กำหนดให้การใช้งานเว็บที่ให้บริการ (Web-serving application) ผู้ใช้ไคลเอนต์ จะเลือกหมายเลขพอร์ตแบบไดนามิกสำหรับการสนทนา



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



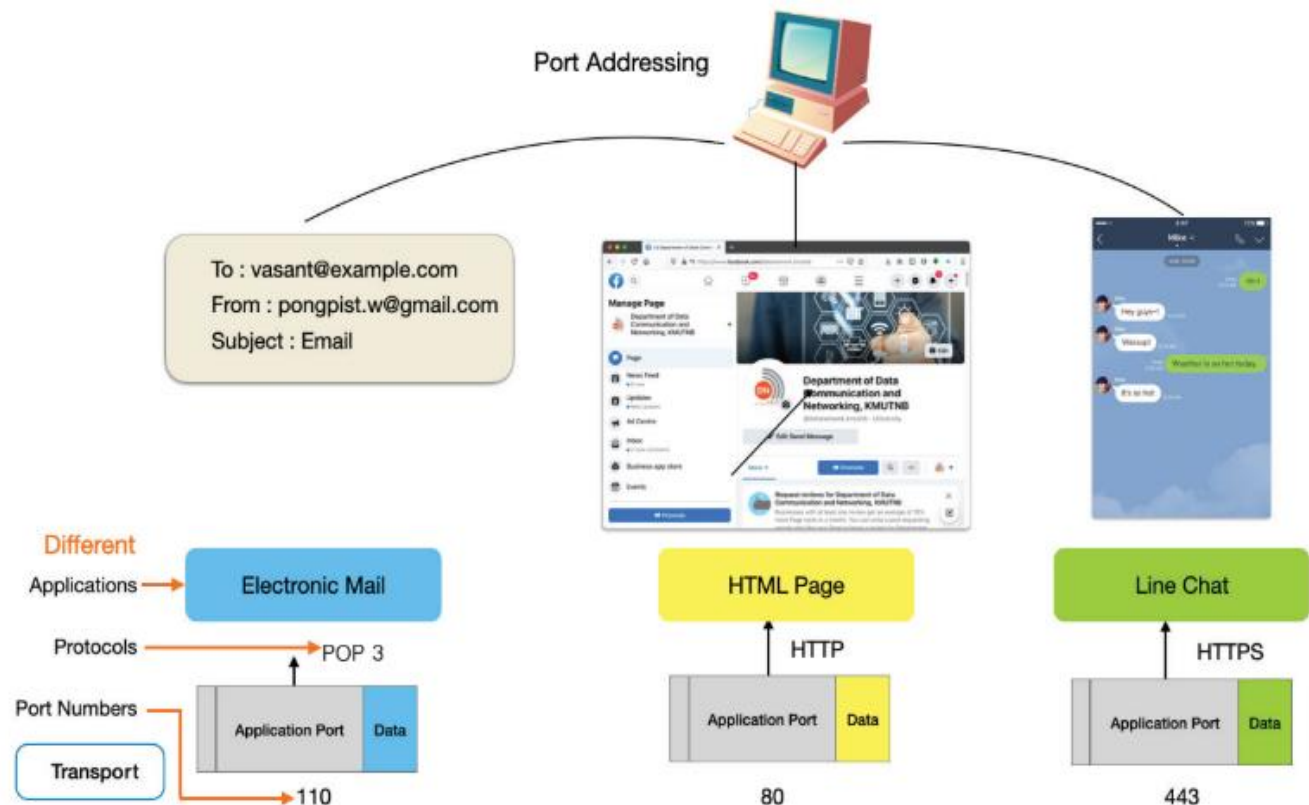
เมื่อแอปพลิเคชันไคลเอนต์จะส่งคำขอไปยังแอปพลิเคชันเซิร์ฟเวอร์ พอร์ตปลายทางที่มีอยู่ในส่วนหัว คือ หมายเลขพอร์ตที่กำหนดให้กับซอฟต์แวร์หรือดีมอนการให้บริการ (Service daemon) ที่ทำงานบนโฮสต์ปลายทาง โดยซอฟต์แวร์ไคลเอนต์ (Client software) ต้องทราบหมายเลขพอร์ตที่เกี่ยวข้องกับ Server process ที่ปลายทาง หมายเลขพอร์ตปลายทางนี้ถูกกำหนดค่าโดยอย่างไรอย่างหนึ่ง ตามค่าเริ่มต้น (Default) หรือด้วยตนเอง (Manually) ตัวอย่างเช่น เมื่อโปรแกรมเว็บเบราว์เซอร์ทำการร้องขอไปยังเว็บเซิร์ฟเวอร์ เบราว์เซอร์จะใช้ TCP และหมายเลขพอร์ต 80 (นอกจากมีระบุไว้เป็นอย่างอื่น) ซึ่งเป็นเพราะ TCP พอร์ต 80 เป็นพอร์ตเริ่มต้นที่กำหนดให้การใช้งานเว็บที่ให้บริการ (Web-serving applications) โดยส่วนใหญ่



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



ข้อมูลของ Applications จะถูกส่งตรงไปยังแต่ละ Applications อย่างถูกต้อง เพราะ Applications แต่ละตัวใช้ Port ที่แตกต่างกัน

รูปที่ 5.5 การกำหนดหมายเลขพอร์ตให้กับแต่ละแอปพลิเคชัน

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

หมายเหตุ

บางแอปพลิเคชันอาจมีการให้บริการพร้อมกันมากกว่าหนึ่งพอร์ต เช่น Line Chat อาจมีการให้บริการบนพอร์ต 443 และพร้อมกับพอร์ตอื่นด้วย

แอปพลิเคชันมีการกำหนดพอร์ตเริ่มต้นไว้ (Default port) รูปที่ 5.5 แสดงการกำหนดหมายเลขพอร์ตให้กับแต่ละแอปพลิเคชันทำให้ ณ เวลาใดเวลาหนึ่งแต่ละพอร์ตมีเพียงแอปพลิเคชันเดียวเท่านั้นที่ทำงานได้ และนี่เป็นเหตุผลที่ทำให้สามารถใช้หลาย ๆ แอปพลิเคชันหรือโปรแกรมพร้อมกันโดยที่ไม่มีการส่งข้อมูลผิดไปยังโปรแกรมอื่น

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



อย่างไรก็ตาม หากมีโปรแกรมที่ให้บริการลักษณะเดียวกัน แล้วต้องการให้โปรแกรมเหล่านั้นทำงานพร้อมกัน บนเครื่องเดียวกันก็สามารถทำได้ แต่ต้องกำหนดให้ทำงานที่หมายเลขพอร์ตต่างกันยกตัวอย่าง หากต้องการให้มี โปรแกรมให้บริการเว็บ (Web server program) สองตัวทำงานพร้อมกันทั้ง IIS (Internet Information Services) และ Apache โดยปกติ หากเราลงโปรแกรมใดในเครื่องก่อนโปรแกรมนั้นจะทำงานก่อน และมักจะได้หมายเลขพอร์ตเฉพาะสำหรับบริการนั้น โดยค่าเริ่มต้นสำหรับการให้บริการเว็บจะใช้หมายเลขพอร์ต 80 ถ้าวาง IIS ในเครื่องก่อน จะทำให้ IIS ทำงานที่หมายเลขพอร์ต 80 และถัดมา เมื่อลง Apache จำเป็นต้องเปลี่ยนค่าหมายเลขพอร์ต เป็นหมายเลขอื่น เช่น 8080 8000 เป็นต้น



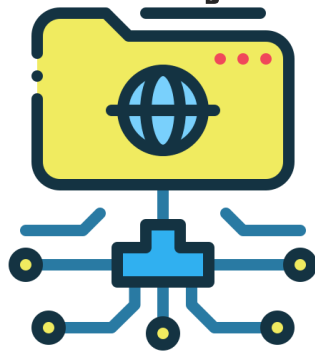
โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



พอร์ตต้นทางในส่วนหัวของเซกเมนต์หรือดาตาแกรมของไคลเอนต์จะถูกสร้างขึ้น โดยการสุ่มจากหมายเลขพอร์ตที่มากกว่า 1,023 ตราบใดที่ไม่ได้ขัดแย้งกับพอร์ตอื่น ๆ ที่ใช้งานบนระบบไคลเอนต์สามารถเลือกหมายเลขพอร์ตใด ๆ จากช่วงของหมายเลขพอร์ตเริ่มต้นที่ใช้โดยระบบปฏิบัติการ หมายเลขพอร์ตนี้ทำหน้าที่เหมือนที่อยู่ของผู้ส่งสำหรับแอปพลิเคชันที่ร้องขอ ชั้นเลเยอร์จะติดตามพอร์ตนี้และแอปพลิเคชันที่ริเริ่มการร้องขอเพื่อที่ว่าเมื่อการตอบสนองจะถูกส่งกลับก็สามารถส่งต่อไปยังแอปพลิเคชันที่ต้องการ หมายเลขพอร์ตของแอปพลิเคชันที่กำลังร้องขอถูกใช้เป็นหมายเลขพอร์ตปลายทางในการตอบสนองกลับมาจากเซิร์ฟเวอร์



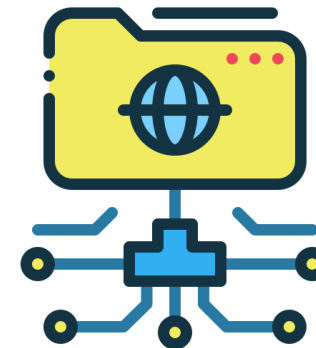
โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



การรวมกันของหมายเลขพอร์ตทรานสปอร์ตเลเยอร์และ IP address ของเน็ตเวิร์กเลเยอร์ถูกกำหนดให้โฮสต์ระบุกระบวนการเฉพาะที่ไม่ซ้ำกันทำงานบนอุปกรณ์โฮสต์นั้น การรวมกันนี้เรียกว่าซ็อกเก็ต (Socket) บางครั้งเราอาจพบคำศัพท์ หมายเลขพอร์ตและซ็อกเก็ตที่ใช้แทนกันได้ ในบริบทของหลักสูตรนี้ คำศัพท์ซ็อกเก็ตอ้างอิงถึงการรวมกันที่มีค่าไม่ซ้ำกันของ IP address และหมายเลขพอร์ต คู่ของซ็อกเก็ต (Socket pair) ประกอบด้วย IP address และหมายเลขพอร์ตต้นทางและปลายทาง นอกจากนี้ยังเป็นค่าที่ไม่ซ้ำกันและใช้ระบุการสนทนาระหว่างสองโฮสต์



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



ตัวอย่างดังรูปที่ 5.6 ไคลเอนต์ที่มี IPv4 address 10.3.4.9 เปิดเว็บเบราว์เซอร์ เพื่อทำการร้องขอเว็บเพจ HTTP จากเว็บเซิร์ฟเวอร์ที่มี IPv4 address 10.2.3.4 โดยค่าเริ่มต้น เว็บเซิร์ฟเวอร์จะให้บริการ http ที่พอร์ต 80 ดังนั้นปลายทางของซ็อกเก็ตจะถูกกำหนดให้เป็น 10.2.3.4:80

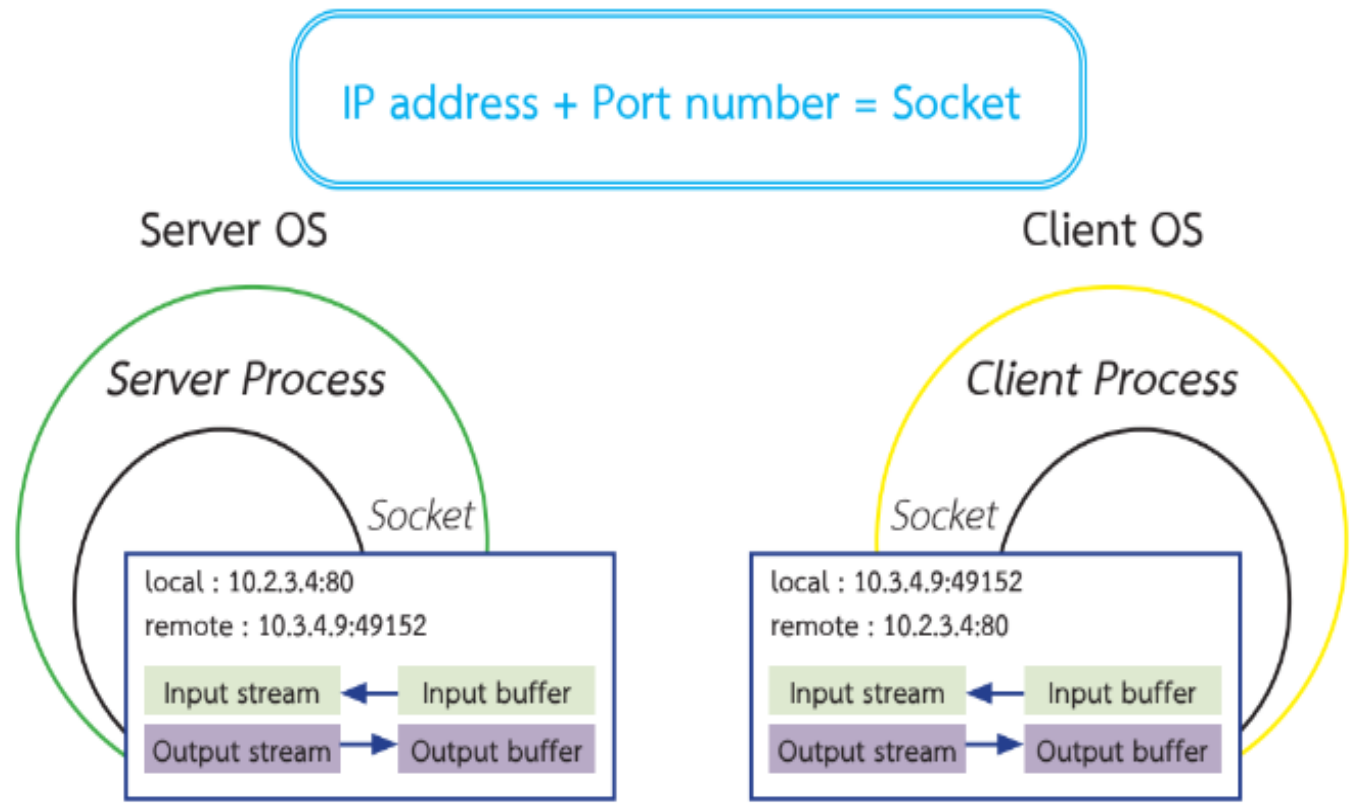
ที่เว็บเบราว์เซอร์ของไคลเอนต์ 10.3.4.9 ที่ร้องขอเว็บเพจ สมมติให้ได้รับหมายเลขพอร์ตแบบไดนามิกที่ถูกกำหนดให้เว็บเบราว์เซอร์เป็น 49152 ซ็อกเก็ตสำหรับต้นทางจะเป็น 10.3.4.9:49152 และที่เว็บเซิร์ฟเวอร์ ค่าสำหรับซ็อกเก็ตนี้จะสลับกัน คือ ต้นทางเป็น 10.2.3.4:80 และปลายทางจะเป็น 10.3.4.9:49152



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



รูปที่ 5.6 การสร้างคู่ของซ็อกเกต (Socket pair) ระหว่างไคลเอนต์และเว็บเซิร์ฟเวอร์

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

หมายเลขพอร์ต (Port Number) คืออะไร



คือ เลขฐานสองจำนวน 16 บิต ทำให้หมายเลขพอร์ต (Port Number) มีได้ตั้งแต่ 0-65535 (มาจาก $2^{16} = 65536$ ค่าที่เป็นไปได้) แต่ละหมายเลขพอร์ตจะถูกกำหนดโดยเฉพาะจากระบบปฏิบัติการ (Operating System : OS) และมีหน่วยงานกลางที่กำกับดูแลอย่างองค์การกำหนดหมายเลขอินเทอร์เน็ต (Internet Assigned Numbers Authority : IANA) เป็นหน่วยงานกลางในการประสานการใช้พอร์ตว่าหมายเลขพอร์ตใดสำหรับบริการใด

มีหลายประเภทที่แตกต่างกันของหมายเลขพอร์ตดังนี้

พอร์ตที่รู้จักกันดี (Well Known Ports) (หมายเลข 0-1023) - หมายเลขเหล่านี้จะสงวนไว้สำหรับบริการและแอปพลิเคชันมักใช้สำหรับแอปพลิเคชันเช่น HTTP (เว็บเซิร์ฟเวอร์) POP 3/SMTP (e-mail server) และ Telnet โดยมีการกำหนดพอร์ตที่รู้จักกันเหล่านี้สำหรับแอปพลิเคชันฝั่งเซิร์ฟเวอร์ (Server application) ส่วนแอปพลิเคชันฝั่งไคลเอนต์ (Client application) สามารถตั้งโปรแกรมให้ร้องขอการเชื่อมต่อกับพอร์ตที่เจาะจงและบริการที่เกี่ยวข้อง

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

พอร์ตที่ลงทะเบียน (Registered Ports) (หมายเลข 1024-49151) - หมายเลขพอร์ตเหล่านี้ได้รับมอบหมายโดยผู้ใช้งานหรือแอปพลิเคชันเอง คือ แต่ละแอปพลิเคชันที่ผู้ใช้เลือกที่จะติดตั้ง (นอกเหนือไปจากแอปพลิเคชันสำหรับการใช้งานทั่วไปที่จะได้รับพอร์ตที่รู้จักกันดี) และในกรณีเมื่อพอร์ตเหล่านี้ไม่ได้มีการใช้งานทรัพยากรเซิร์ฟเวอร์ พอร์ตเหล่านี้อาจจะถูกเลือกแบบไดนามิกโดยไคลเอนต์ให้เป็นพอร์ตต้นทางของไคลเอนต์

พอร์ตไดนามิกหรือพอร์ตส่วนตัว (Dynamic or Private Ports) (หมายเลข 49152-65535) - รู้จักกันในชื่อ Ephemeral Ports โดยพอร์ตเหล่านี้จะมอบหมายแบบไดนามิกไปยังไคลเอนต์แอปพลิเคชันเมื่อเริ่มการเชื่อมต่อ ซึ่งไม่ได้เป็นเรื่องธรรมดามากนักสำหรับไคลเอนต์ที่เชื่อมต่อไปยังบริการโดยใช้พอร์ตแบบไดนามิกหรือพอร์ตส่วนตัว (แม้ว่าบางโปรแกรมแชร์ไฟล์แบบ peer-to-peer จะใช้งาน)



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

ประเภทหมายเลขพอร์ต	หมายเลขพอร์ต
พอร์ตที่รู้จักกันดี (Well Known Ports)	0-1023
พอร์ตที่ลงทะเบียน (Registered Ports)	1024 -49151
พอร์ตไดนามิกหรือพอร์ตส่วนตัว (Dynamic or Private Ports)	49152-65535

ตารางที่ 5.2 ประเภทหมายเลขพอร์ตและหมายเลขพอร์ตที่ใช้งานได้

หมายเหตุ

สามารถดูเพิ่มเติมจากเว็บไซต์ของทาง IANA ว่ามีพอร์ตใดที่พบการใช้งานบ่อยและเป็นพอร์ตมาตรฐานที่ควรรู้ <https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt>

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

หมายเลขพอร์ต	โปรโตคอลหรือแอปพลิเคชันที่ใช้งาน
20	File Transfer Protocol (FTP) Data Transfer
21	File Transfer Protocol (FTP) Command Control
22	Secure Shell (SSH) Secure Login
23	Telnet remote login service, unencrypted text messages
25	Simple Mail Transfer Protocol (SMTP) E-mail routing
53	Domain Name System (DNS) service
67, 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP) used in the World Wide Web
110	Post Office Protocol (POP 3)

ตารางที่ 5.3 ตัวอย่างพอร์ตที่รู้จักกันดี

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

หมายเลขพอร์ต	โปรโตคอลหรือแอปพลิเคชันที่ใช้งาน
119	Network News Transfer Protocol (NNTP)
123	Network Time Protocol (NTP)
143	Internet Message Access Protocol (IMAP) Management of digital mail
161	Simple Network Management Protocol (SNMP)
194	Internet Relay Chat (IRC)
443	HTTP Secure (HTTPS) HTTP over TLS/SSL

ตารางที่ 5.3 ตัวอย่างพอร์ตที่รู้จักกันดี (ต่อ)

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

1.3.5 ชั้นเครือข่ายหรือเน็ตเวิร์ก (Network layer)

ชั้นเครือข่ายหรือเน็ตเวิร์กใช้ระบุที่อยู่หรือจัดการแอดเดรส (Addressing) โดยส่วนใหญ่ที่ใช้กันในเครือข่ายอินเทอร์เน็ตมักหมายถึง IPv4 address และ IPv6 และกระบวนการที่ช่วยให้ข้อมูลชั้นทรานสปอร์ตสามารถที่จะบรรจุลงแพ็กเก็ต เรียกว่ากระบวนการนี้ว่า การห่อหุ้ม (Encapsulation) และจากนั้นชั้นเน็ตเวิร์กจึงทำการขนส่งแพ็กเก็ตต่อไป การห่อหุ้มจะช่วยให้เนื้อหาของข้อมูลถูกส่งผ่านไปยังปลายทางภายในเครือข่ายหรือบนเครือข่ายอื่นด้วยโอเวอร์เฮดที่ต่ำ

บทบาทอื่นของชั้นเน็ตเวิร์ก เช่น ตรวจสอบวิธีการที่จะแบ่งเครือข่ายเพื่อจัดการการไหลของแพ็กเก็ตข้อมูลภายในเครือข่าย วิธีการสื่อสารระหว่างเครือข่าย โดยการสื่อสารระหว่างเครือข่ายนี้จะเรียกว่าการจัดการเส้นทางหรือการค้นหาเส้นทางหรือเราติง (Routing)



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

คุณลักษณะของไอพี (Characteristics of IP)



การให้บริการของชั้นเน็ตเวิร์กที่นำมาใช้โดยชุดโพรโทคอล TCP/IP คือ อินเทอร์เน็ตโพรโทคอลรุ่น 4 (Internet Protocol version 4 : IPv4) เป็นไอพีรุ่นที่ใช้กันอย่างแพร่หลายอย่างยาวนานจนถึงปัจจุบัน และมีความพยายามในการเปลี่ยนแปลงมาใช้ไอพีรุ่น 6 (IPv6) กันมากขึ้น

IPv6 ถูกพัฒนาและมีการใช้งานในบางพื้นที่ โดย IPv6 จะมีการนำไปใช้งานควบคู่ไปกับ IPv4 และอาจแทนที่ IPv4 ในอนาคต แต่อย่างไรก็ตาม IPv4 ยังเป็นโพรโทคอลชั้นที่ 3 ที่มีการใช้งานในการนำพาข้อมูลของผู้ใช้ผ่านทางอินเทอร์เน็ตมากที่สุด ดังนั้น จึงใช้ IPv4 เป็นตัวอย่างสำหรับโพรโทคอลชั้นเน็ตเวิร์ก

อินเทอร์เน็ตโพรโทคอลถูกออกแบบมาเป็นโพรโทคอลที่มีโอเวอร์เฮดต่ำ จะทำหน้าที่เพียงเท่าที่จำเป็นในการส่งมอบแพ็กเก็ตจากต้นทางไปยังปลายทางบนระบบที่มีการเชื่อมต่อกันของเครือข่าย โพรโทคอลไม่ได้ถูกออกแบบเพื่อติดตามและจัดการการไหลของแพ็กเก็ต ฟังก์ชันเหล่านี้จะทำโดยโพรโทคอลอื่นในชั้นอื่น ๆ

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

ลักษณะพื้นฐานของ IPv4

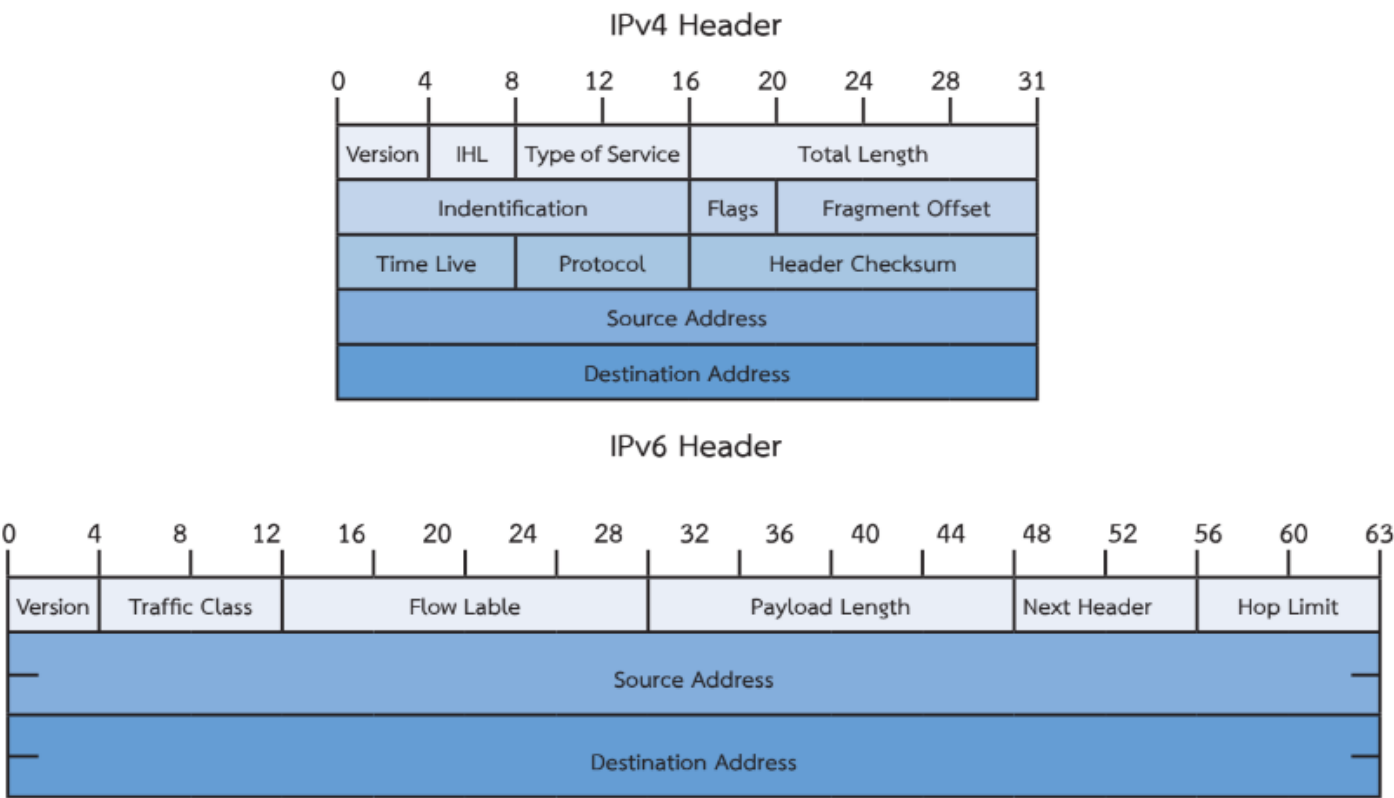
- 🌐 ไม่มีการสร้างการเชื่อมต่อ (Connectionless) ไม่มีการเชื่อมต่อที่จัดตั้งขึ้นก่อนที่จะส่งแพ็กเก็ตข้อมูล
 - 🌐 พยายามให้ดีที่สุด (Best Effort) เชื่อใจไม่ได้ (Unreliable) คือ พยายามทำดีที่สุดแล้วในการส่งข้อมูล แต่ถ้าไม่ถึงก็ไม่รับผิดชอบอะไร จึงไม่มีโอเวอร์เฮดที่ใช้ในการรับประกันการส่งมอบแพ็กเก็ต
 - 🌐 อิสระจากสื่อ (Media Independent) ทำงานเป็นอิสระจากสื่อที่ใช้ส่งข้อมูล สามารถส่งบนสื่อใดก็ได้ไม่ว่าเป็นสายเคเบิลทองแดง สายใยแก้วนำแสง คลื่นวิทยุ หรืออื่น ๆ
- แต่ละอุปกรณ์ในเครือข่ายต้องมีแอดเดรสที่ไม่ซ้ำกัน ที่เน็ตเวิร์กเลเยอร์แพ็กเก็ตของการสื่อสารจะต้องมีการระบุด้วยแอดเดรสต้นทางและปลายทางที่สื่อสารกันโดยในแต่ละแพ็กเก็ต IPv4 (รูปที่ 5.7) มีแอดเดรสต้นทาง (Source address) ขนาด 32 บิต และแอดเดรสปลายทาง (Destination address) ขนาด 32 บิตในส่วนหัวของแพ็กเก็ตของชั้นที่ 3 นี้ ในขณะที่ IPv6 มีแอดเดรสต้นทางและแอดเดรสปลายทางขนาด 128 บิต



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



รูปที่ 5.7 เปรียบเทียบเฮดเดอร์ (Header) ของ IPv4 และ IPv6

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

แอดเดรสเหล่านี้ถูกนำมาใช้ในเครือข่ายข้อมูลในรูปแบบไบนารี (Binary) หรือเลขฐานสอง ภายในอุปกรณ์ ที่เรียกว่าเลขฐานสองเนื่องจากตัวเลขหนึ่งตัวจะแทนค่าได้สองค่าคือ 0 และ 1 เป็นรูปแบบที่คอมพิวเตอร์เข้าใจซึ่งเป็นค่าดิจิทัลทางตรรกะ ทำให้ค่าเลขฐานสองนี้ถูกนำไปใช้สำหรับการตีความของอุปกรณ์คอมพิวเตอร์ แต่สำหรับมนุษย์นั้น สตริงขนาด 32 บิต เป็นเรื่องยากที่จะตีความและยิ่งยากที่จะจำ ดังนั้นจึงแทนค่าของ IPv4 address โดยใช้รูปแบบเลขฐานสิบหรือเลขทศนิยม (Decimal) และแบ่งด้วยจุด (เช่นเดียวกันกับเลขฐานสอง) ที่เรียกว่าเลขฐานสิบเนื่องจากตัวเลขหนึ่งตัวจะแทนค่าได้สิบค่าคือ 0 ถึง 9



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

เลขฐานสิบที่มีจุด (Dotted Decimal)

รูปแบบเลขฐานสองจำนวน 32 บิต ต่อเนื่องกันที่คอมพิวเตอร์เข้าใจนั้นจะใช้แทน IPv4 address แต่ในการที่จะทำให้ IPv4 address นี้ใช้งานง่ายสำหรับมนุษย์ จึงมีการแสดง IPv4 address เป็นเลขฐานสิบที่มีจุดที่แยกแต่ละไบต์ (Byte) ของเลขฐานสอง ซึ่งที่เรียกว่าออกเตต (Octet หมายถึง แปด) โดยมีจุดแบ่งที่เรียกว่า Octet เพราะแต่ละไบต์หรือ 8 บิต จะถูกแทนค่าด้วยเลขฐานสิบ

ตัวอย่างเช่น IPv4 address

11000000101010000000101000000011

จะเห็นว่ายากมากที่เราจะจำได้ทั้งหมด หรือแม้กระทั่งจะแบ่งจำทีละ 8 บิต โดยมีการเว้นวรรค เช่น

11000000 10101000 00001010 00000011

ดังนั้น IPv4 address จะแสดงในเลขฐานสิบที่มีจุดเป็น

192 .168 .10 .3 (เวลาใช้งานจริงจะเขียนติดกันเป็น 192.168.10.3)



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โปรโตคอล (Protocol)

จะเห็นว่าเราสามารถจดจำตัวเลขฐานสิบได้ง่ายกว่า อันที่จริงแล้วถ้าเป็นชื่อเราคงจำได้ง่ายกว่านี้มาก เช่น โฮสต์ kmutnb.ac.th แต่คอมพิวเตอร์จะไม่รู้จักว่าโฮสต์ kmutnb.ac.th คือ IPv4 address อะไรเพื่อที่คอมพิวเตอร์จะรู้จัก IPv4 address ของโฮสต์ kmutnb.ac.th นั้นจำเป็นต้องใช้โปรโตคอล DNS (Domain Name System) เพื่อแปล (Resolve) ชื่อโฮสต์เป็นแอดเดรสที่คอมพิวเตอร์รู้จัก อย่างไรก็ตามอุปกรณ์ในเครือข่ายใช้ตรรกะแบบเลขฐานสอง แต่รูปแบบเลขฐานสิบที่มีจุดจะถูกใช้ เพื่อให้่ายขึ้นสำหรับคนที่จะใช้และจำแอดเดรสเหล่านี้



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

หมายเหตุ

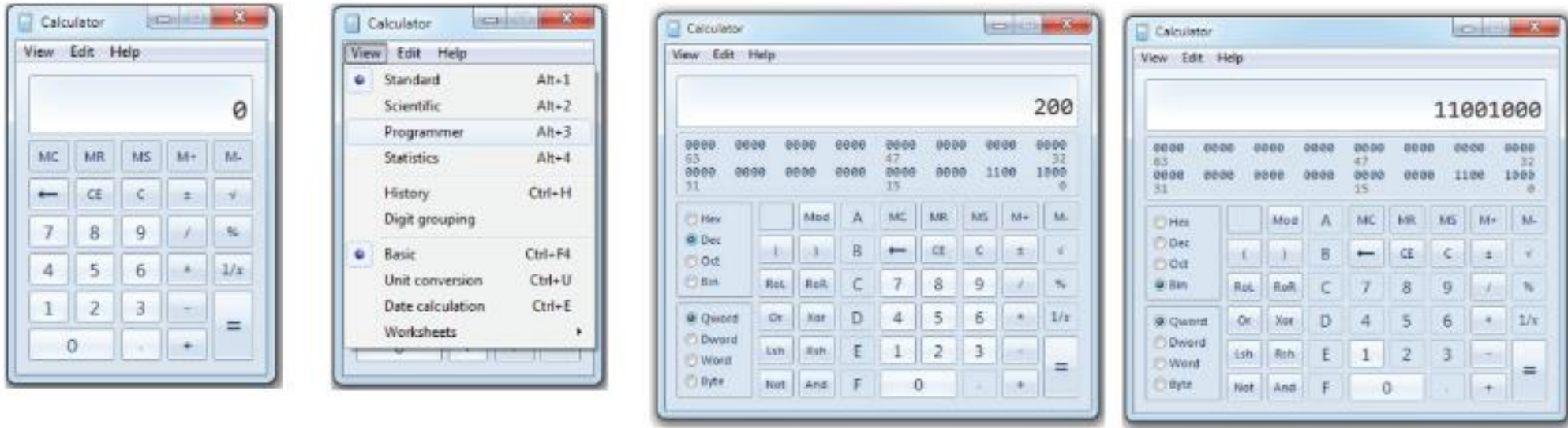
สามารถหาคำตอบการแปลงตัวเลขฐานสิบเป็นฐานสองได้ด้วยการใช้โปรแกรมเครื่องคิดเลข (Calculator) ที่อยู่บน Microsoft Windows ดังรูปที่ 5.8 โดยปกติเมื่อเรียกโปรแกรมเครื่องคิดเลขขึ้นมา โปรแกรมจะอยู่ในการทำงานแบบ Standard ให้ทำการเปลี่ยนการทำงานเป็น Programmer โดยเลือกจากเมนู View > Programmer จากนั้นให้พิมพ์ตัวเลขฐานสิบที่ต้องการแปลงลงไปในตัวอย่างคือ 200 ทำการเลือกการแปลงโดยเลือก Bin (Binary) จะได้ค่า 11001000 นอกจากนี้ยังสามารถเปลี่ยนเป็นเลขฐานอื่น ๆ ได้อีก โดย Hex=Hexadecimal (เลขฐานสิบหก) Dec=Decimal (เลขฐานสิบ) Oct=Octal (เลขฐานแปด) และ Bin=Binary (เลขฐานสอง)



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



รูปที่ 5.8 การใช้โปรแกรมเครื่องคิดเลขในการแปลงเลขฐานสิบเป็นเลขฐานสอง

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



ส่วนประกอบของไอพีแอดเดรส

ในแต่ละไอพีแอดเดรสจะประกอบไปด้วย 2 ส่วน ดังนี้



ส่วนบอกเครือข่ายหรือเน็ตเวิร์กพอร์ชัน (Network Portion) ซึ่งประกอบไปด้วยบิตจำนวนหนึ่ง เรียกว่าบิตของเครือข่ายหรือเน็ตเวิร์กบิต (Network bit) คือ ส่วนที่บอกให้รู้ว่าไอพีแอดเดรสนั้นอยู่ในเครือข่ายใดโดยที่เลเยอร์ 3 กำหนดให้โฮสต์แอดเดรส (Host address) ที่อยู่ในเครือข่ายเดียวกันต้องมีรูปแบบของบิตที่เหมือนกันในเน็ตเวิร์กพอร์ชันของโฮสต์แอดเดรส (Host address) เปรียบเทียบให้เห็นตัวอย่างง่าย ๆ คือรหัสโทรศัพท์ทางไกล ถ้าขึ้นต้นด้วย 02 คือ กรุงเทพมหานคร จังหวัดนนทบุรี ปทุมธานี และสมุทรปราการ ถ้าขึ้นต้นด้วย 036 คือจังหวัดลพบุรี สิงห์บุรี และสระบุรี เป็นต้น ถ้าขึ้นต้นด้วย 02 เราจะได้ทันทีว่าอยู่ในจังหวัดใด

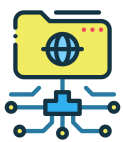


โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



ในแต่ละไอพีแอดเดรสจะประกอบไปด้วย 2 ส่วน ดังนี้

 **ส่วนบอกเครือข่ายโฮสต์หรือโฮสต์พอร์ชัน (Host Portion)** ซึ่งประกอบไปด้วยบิตจำนวนหนึ่ง เรียกว่า บิตของโฮสต์หรือโฮสต์บิต (Host bit) จำนวนบิตที่เปลี่ยนแปลงได้ในเครือข่ายนั้น เปรียบเทียบให้เห็นตัวอย่างง่าย ๆ กับเบอร์โทรศัพท์ 02 555 2000 หมายเลข 02 หมายถึง กรุงเทพมหานคร จังหวัดนนทบุรี ปทุมธานี และสมุทรปราการ ส่วน 555 2000 หมายถึงเบอร์โทรประจำเครื่องที่ระบุถึงมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ในการใช้งานจริงเราไม่สามารถกดแค่เบอร์ 555 2000 จำเป็นต้องกด 02 ก่อนจึงจะสามารถติดต่อได้หมายเลขโทรศัพท์ในเครือข่ายนั้นจะเปลี่ยนไปเรื่อย ๆ ตามที่เครือข่ายนั้นสามารถรองรับหรือถูกกำหนดการทำงานมา นอกจากนี้จำนวนบิตของโฮสต์พอร์ชันจะใช้ในการกำหนดจำนวนของโฮสต์ที่สามารถมีได้ภายในเครือข่ายนั้น ซึ่งจะอธิบายในภายหลัง



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



ในเครือข่ายไอพีก็เช่นกันต้องมีส่วนบอกเครือข่ายเพื่อบอกให้รู้ว่าเครือข่ายนั้นอยู่ที่ใดและในการที่จะสื่อสารกับโฮสต์ปลายทางที่ต้องการก็ต้องใช้ส่วนบอกเครือข่าย แต่การใช้ส่วนบอกเครือข่ายนั้นไม่สามารถใช้งานได้โดยลำพัง ในการใช้งานต้องมีส่วนบอกเครือข่ายก่อนโดยเริ่มจากบิตที่มีค่าสูง (High-order bits) แล้วตามด้วยส่วนบอกเครือข่ายโฮสต์

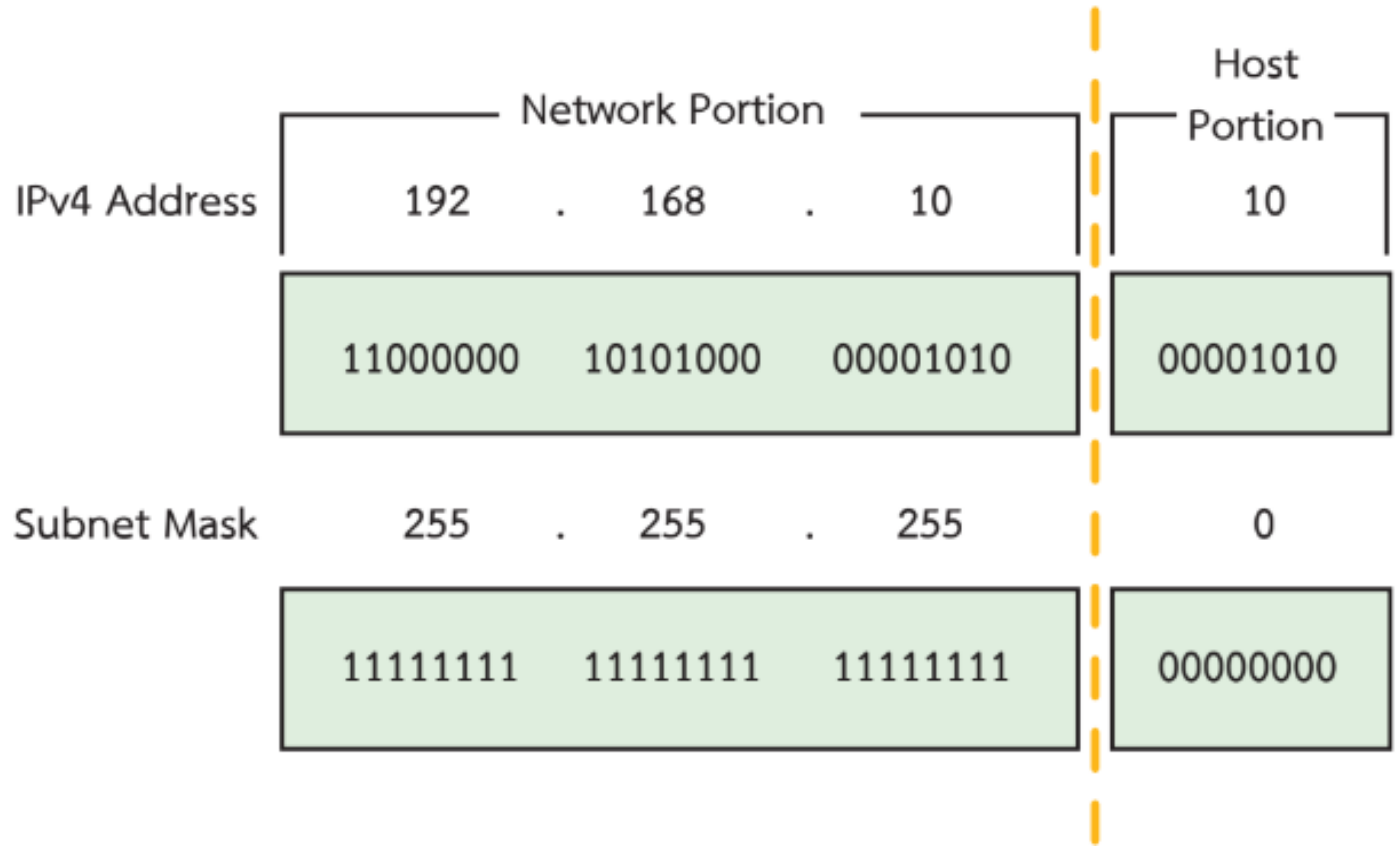
ดังตัวอย่างในรูปที่ 5.9 ไอพีแอดเดรส 192.168.10.10 จะประกอบด้วยเน็ตเวิร์กพอร์ชัน 192.168.10 และโฮสต์พอร์ชัน 10 นอกจากนี้ ยังมีสิ่งที่เรียกว่าซับเน็ตมาสก์ (Subnet Mask) ด้วย ซึ่งจะอธิบายในภายหลังต่อไป



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



รูปที่ 5.9 ไอพีแอดเดรสจะประกอบด้วยเน็ตเวิร์กพอร์ชันและโฮสต์พอร์ชัน (รูปจาก Cisco)

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)



เมื่อแสดงถึง IPv4 address จะมีการแสดงความยาวของเน็ตเวิร์กบิตหรือพรีฟิกเลงท์ (Prefix length) กับแอดเดรสเสมอ Prefix length คือ จำนวนของบิตในแอดเดรสที่ใช้ในการบอกเน็ตเวิร์กพอร์ชันเรียกว่าเน็ตเวิร์กบิต (Network.Bits) โดยการเขียน Prefix length จะมีเครื่องหมาย / นำหน้า ตัวอย่างเช่น ใน 192.168.10.10/24 คา/24 คือ Prefix length ซึ่งบอกว่า 24 บิตแรกเป็นเน็ตเวิร์กพอร์ชัน ส่วนที่เหลืออีก 8 บิตหรือ Octet สุดท้ายเป็นโฮสต์พอร์ชัน เรียกบิตเหล่านี้ว่า โฮสต์บิต (Host Bits)



สิ่งที่ถูกนำมาใช้เพื่อระบุเน็ตเวิร์กพอร์ชันของ IPv4 address ที่อยู่ในอุปกรณ์เครือข่ายต่าง ๆ ซึ่งมันถูกเรียกว่า ซับเน็ตมาสก์ (Subnet Mask) โดยซับเน็ตมาสก์ประกอบด้วย 32 บิตเช่นเดียวกับไอพีแอดเดรสแต่ ซับเน็ตมาสก์จะเป็นการแทนค่าของ Prefix length โดยการแทนค่า 1 จำนวนเท่ากับที่ระบุใน Prefix length เริ่มจากบิตที่มีค่ามากที่สุดไปจนถึงบิตที่มีค่าน้อยที่สุด ส่วนนอกเหนือจากนี้จะแทนด้วยค่า 0

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โปรโตคอล (Protocol)

ตัวอย่างเช่น Prefix length คือ /24 ดังนั้น แทนค่า 1 จำนวน 24 บิต ที่เหลือเป็นค่า 0 จะได้ซับเน็ตมาสก์ คือ 11111111.11111111.11111111.00000000 แปลงเป็นเลขฐานสิบได้คือ 255.255.255.0

เครือข่ายไม่ได้รับการกำหนด /24 Prefix เสมอ ทั้งนี้ขึ้นอยู่กับจำนวนของโฮสต์บนเครือข่าย โดย Prefix ที่ถูกกำหนดอาจจะแตกต่างกัน การมีจำนวน Prefix ที่แตกต่างกันจะมีช่วงโฮสต์ที่ใช้งานได้แตกต่างกัน

โปรดจำไว้

ในการกำหนดค่าให้กับแต่ละอุปกรณ์ ต้องกำหนดค่า IP address และ Subnet Mask ด้วยคำแนะนำ เพื่อให้ง่ายแก่การใช้งาน ผู้เรียนสามารถใช้เครื่องมือในการช่วยคำนวณเกี่ยวกับ IP address ได้ โดยใช้ คำค้นหาเช่น “ipv4 calculator” ในกูเกิล จะมีหลายเว็บไซต์ให้เลือกใช้งาน ในที่นี้ขอยกตัวอย่างเว็บไซต์ <http://jodies.de/ipcalc>

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



ในช่องแรก คือ Address (Host or Network)

ในช่องสอง คือ Netmask (i.e. 24)

เราสามารถทดลองใส่ค่า IPv4 address ในตัวอย่างข้างต้น คือ 192.168.10.10/24 โดยใส่

Address (Host or Network) = 192.168.10.10

Netmask (i.e. 24) = 24



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

จะแสดงค่าที่เกี่ยวข้องกับ IPv4 address นี้ที่เราสามารถเอาไปใช้งานได้ อธิบายพอสังเขปได้ดังนี้

หมายเลข IPv4 address ที่สามารถนำไปกำหนดค่าให้กับโฮสต์ต่าง ๆ ได้คือ ค่าตั้งแต่ HostMin : 192.168.10.1 - HostMax: 192.168.10.254 ซึ่งหมายถึงจำนวนโฮสต์ที่มีได้ในเครือข่ายนี้ คือ 254 โฮสต์ อีก 2 หมายเลขที่ไม่สามารถกำหนดให้กับโฮสต์ใด ๆ ได้นั้นคือหมายเลขเครือข่าย (Network address) และหมายเลขบรอดคาสต์ (Broadcast address)

- 🌐 Subnet Mask สำหรับโฮสต์หรือเครือข่ายนี้ คือ Netmask : 255.255.255.0
- 🌐 หมายเลขเครือข่ายของ 192.168.10.10/24 คือ Network : 192.168.10.0/24
- 🌐 หมายเลขบรอดคาสต์สำหรับเครือข่ายนี้ คือ Broadcast : 192.168.10.255



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

Address (Host or Network)Netmask (i.e. 24)Netmask for sub/supernet (optional)

192.168.10.10 / 24move to:

CalculateHelp

Address: 192.168.10.1011000000.10101000.00001010.00001010

Netmask: 255.255.255.0 = 2411111111.11111111.11111111.00000000

Wildcard: 0.0.0.25500000000.00000000.00000000.11111111

=>

Network: 192.168.10.0/2411000000.10101000.00001010.00000000 (Class C)

Broadcast: 192.168.10.25511000000.10101000.00001010.11111111

HostMin: 192.168.10.111000000.10101000.00001010.00000001

HostMax: 192.168.10.25411000000.10101000.00001010.11111110

Hosts/Net: 254 (Private Internet)

IP-Calculator

Version 0.35.2 2005/07/07

รูปที่ 5.10 ตัวอย่างการใช้โปรแกรมคำนวณเกี่ยวกับ IPv4 address

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

ประเภทของ IPv4 address ที่กำหนดให้กับโฮสต์ได้

IPv4 address ที่กำหนดให้กับโฮสต์ได้หรือเรียก IPv4 โฮสต์แอดเดรส (IPv4 host address) แบ่งออกเป็น 2 ประเภท คือ แอดเดรสสาธารณะหรือพับบลิคแอดเดรส (Public address) และแอดเดรสส่วนตัวหรือไพรเวตแอดเดรส (Private address)

แอดเดรสสาธารณะ (Public address) ถูกกำหนดไว้สำหรับใช้ในเครือข่ายที่สามารถเข้าถึงได้บนอินเทอร์เน็ต (Accessible on the Internet) สามารถส่งออกไปยังอินเทอร์เน็ตได้หรือเรียกว่า เราเอเบิล (Routable) และต้องไม่ซ้ำกันเลย (Unique) สำหรับเครือข่ายที่เชื่อมต่อกับอินเทอร์เน็ต ในภาษาเฉพาะของคนทำงานด้านเครือข่ายอาจเรียกว่า ไอพีจริง

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

แอดเดรสส่วนตัว (Private address) เป็นบล็อกของแอดเดรสที่ถูกนำมาใช้ในเครือข่ายภายในองค์กร ซึ่งแอดเดรสเหล่านี้ไม่สามารถเข้าถึงได้จากอินเทอร์เน็ต (Limited or no Internet access) และในขณะเดียวกัน Private address เหล่านี้ก็ไม่สามารถที่จะใช้ในการออกสู่อินเทอร์เน็ตได้ จึงทำให้องค์กรต่าง ๆ สามารถมี Private address ซ้ำกันได้ ซึ่งแตกต่างจาก Public address ที่ในเครือข่ายในโลกนี้จะมีเพียงแค่อุปกรณ์เดียวเท่านั้นที่มี Public address นี้ ในภาษาเฉพาะของคนทำงานด้านเครือข่ายอาจเรียกว่า ไอพีปลอม

โดย Private address มีบล็อกของแอดเดรสดังนี้

-  10.0.0.0 ถึง 10.255.255.255 (10.0.0.0 /8)
-  172.17.0.0 ถึง 172.31.255.255 (172.17.0.0 /12)
-  192.168.0.0 ถึง 192.168.255.255 (192.168.0.0 /16)



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

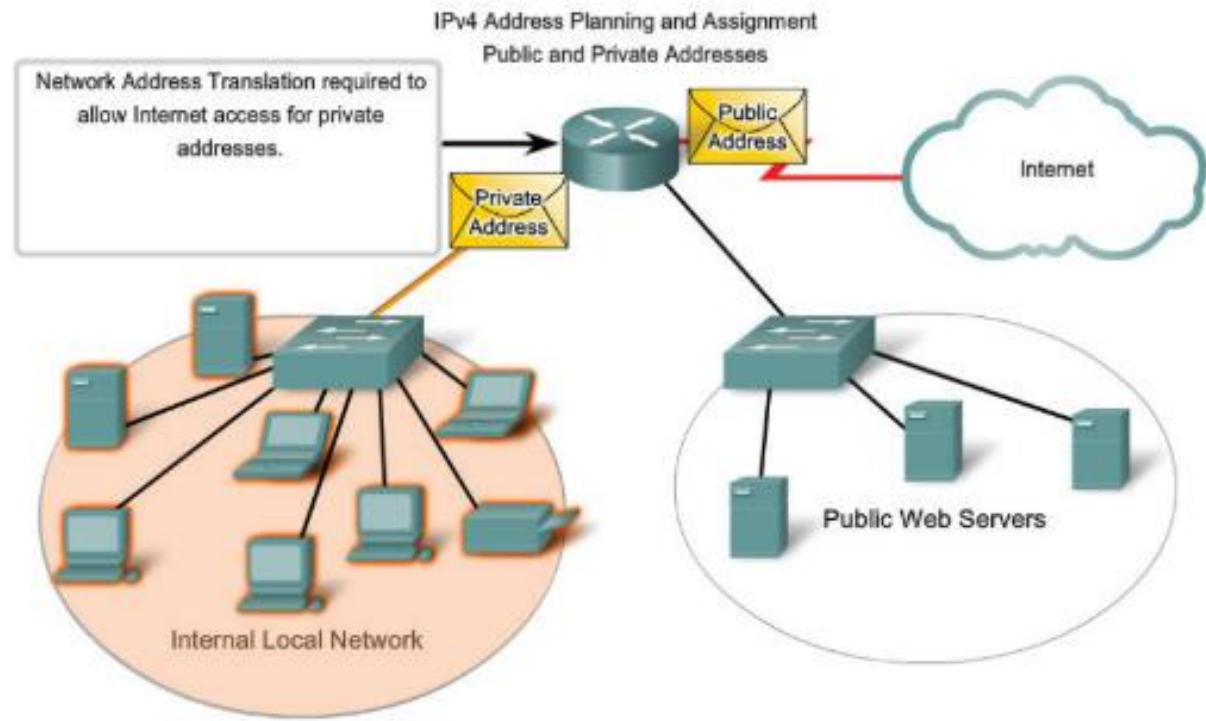
นอกจากนี้ การนำ Private address มาใช้อาจช่วยในเรื่องของการรักษาความมั่นคงปลอดภัยได้ เพราะโฮสต์ที่อยู่ภายนอกองค์กรไม่สามารถเข้าถึง Private address เหล่านั้นได้โดยตรง อีกประการหนึ่ง คือ IPv4 public address นั้นไม่เพียงพอกับการใช้งานในปัจจุบัน ซึ่ง IPv4 public address จำเป็นต้องใช้สำหรับการสื่อสารในเครือข่ายอินเทอร์เน็ต แต่เนื่องจากมีจำนวนจำกัด ดังนั้นในเครือข่ายปัจจุบันส่วนใหญ่จะใช้ IPv4 private address (ตามมาตรฐาน RFC 1918) ในองค์กร



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



รูปที่ 5.11 การทำงานของ NAT ในการแปลงระหว่าง IPv4 private address และ IPv4 public address

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

Network Address Translation (NAT)

ปัญหาของการใช้ IPv4 private address คือ ไม่สามารถต่อออกอินเทอร์เน็ต การที่จะต่อออกอินเทอร์เน็ตได้นั้นจำเป็นต้องใช้การแปลงแอดเดรสของเครือข่ายที่เรียกว่า Network Address Translation (NAT) ซึ่งเป็นวิธีการที่ใช้สำหรับแปลง (Translation) ระหว่าง IPv4 private address ให้เป็น IPv4 public address สำหรับออกอินเทอร์เน็ต และแปลง IPv4 public address ให้เป็น IPv4 private address สำหรับการสื่อสารกลับเข้าไปในเครือข่ายขององค์กร โดยที่จะมีการตั้งค่าการทำงานของ NAT ที่เราเตอร์สำหรับเข้า-ออกองค์กรที่ต่อออกไปยังเครือข่ายของผู้ให้บริการ (ISP)



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

IPv6 address และระบบเลขฐานสิบหก (Hexadecimal Number System)

ค่าแอดเดรสสามารถดูได้จากเอกสาร RFC 2373 “IP Version 6 Addressing Architecture” IPv6 address ที่มีจำนวน 128 บิตนั้นมีการแสดงค่าที่แตกต่างจาก IPv4 ซึ่งมี 32 บิต โดยการใช้การแบ่งเลขฐานสองทีละชุด ชุดละ 8 บิต แล้วแปลงเป็นเลขฐานสิบและคั่นด้วยจุด “.” จะได้ IP address ออกมา เช่น 192.168.1.1 แต่ใน IPv6 จะแบ่งเลขฐานสองทีละชุด ชุดละ 16 บิต และแทนค่าด้วยเลขฐานสิบหก (Hexadecimal) และคั่นแต่ละชุดด้วยโคลอน “:” เช่น FE80:0000:0000:0000:0123:4567:89AB:CDEF

ดังนั้น ก่อนอื่นจำเป็นที่จะต้องเรียนรู้การแปลงจากเลขฐานสองไปเป็นเลขฐานสิบหก แสดงดังรูปที่ 5.12 ที่เรียกว่าเลขฐานสิบหกเนื่องจากค่า 1 ตำแหน่งสามารถแทนได้ที่ 16 ค่า คือจาก 0 ถึง F โดยที่ A=10, B=11, C=12, D=13, E=14 และ F=15 และค่าเลขฐานสิบหก 1 เลขสามารถใช้แทนค่าของเลขฐานสองได้ที่ละ 4 บิต (คือจำนวนครึ่งของไบต์) โดยค่าที่ต่ำสุดคือ 0000=0 และค่าที่สูงสุดคือ 1111=F

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

Representing Hexadecimal Values		
Hexadecimal	Decimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Hexadecimal Conversions of Binary Octets		
Hexadecimal	Decimal	Binary
00	0	0000 0000
01	1	0000 0001
02	2	0000 0010
03	3	0000 0011
04	4	0000 0100
05	5	0000 0101
06	6	0000 0110
07	7	0000 0111
08	8	0000 1000
0A	10	0000 1010
0F	15	0000 1111
10	16	0001 0000
20	32	0010 0000
40	64	0100 0000
80	128	1000 0000
C0	192	1100 0000
CA	202	1100 1010
F0	240	1111 0000
FF	255	1111 1111

รูปที่ 5.12 เปรียบเทียบเลขฐานสอง ฐานสิบ และเลขฐานสิบหก (รูปจาก Cisco)

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)

ตัวอย่างการแปลงเลขฐานสองทีละ 8 บิต ไปเป็นเลขฐานสิบหกจะทำการแบ่งเลขฐานสองออกทีละ 4 บิต จากนั้นจึงแปลงเป็นเลขฐานสิบหก และสามารถแปลงให้เป็นเลขฐานสิบได้ด้วยเช่นกัน

การแสดงความหมายของ IPv6 (IPv6 Address Representation)

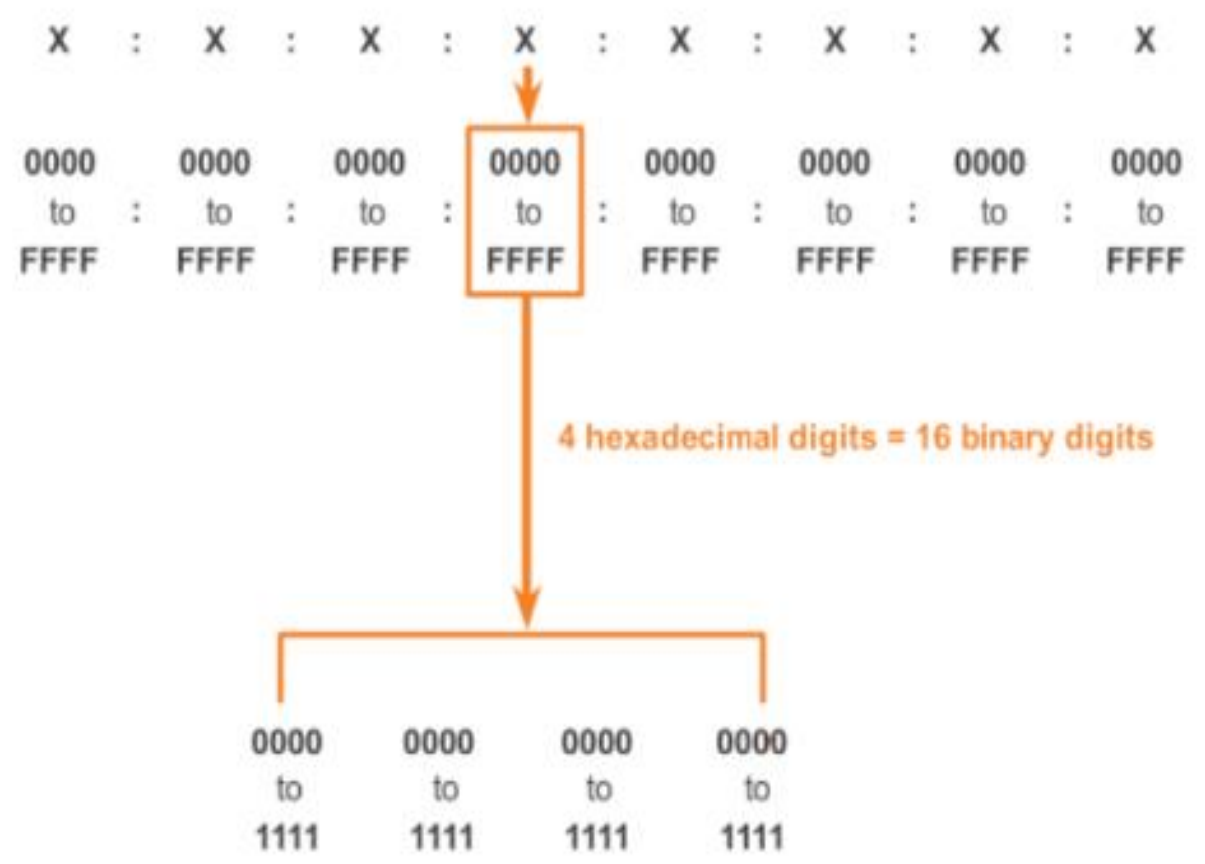
รูปแบบการแสดงความหมายของ IPv6 address จะทำการแบ่งเลขฐานสองจำนวน 128 บิต ออกมาชุดละ 16 บิต (แล้วแบ่งออกทีละ 4 บิต อีกครั้งเพื่อให้ทำการแปลงง่ายขึ้น) แทนค่าด้วยเลขฐานสิบหก (บางครั้งเรียกเลขฐานสิบหก 4 ตัวที่แทนค่าเลขฐานสอง 16 บิตนี้ว่า Hextet) ได้ 8 ชุด โดยการเขียนเลขฐานสิบหกนี้จะเขียนตัวพิมพ์ใหญ่หรือตัวพิมพ์เล็กได้ และใช้เครื่องหมายที่คั่นแต่ละชุดด้วยโคลอน “:”



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



รูปที่ 5.13 รูปแบบ IPv6 ประกอบด้วย 8 Hextet และคั่นด้วยโคลอน “:” (รูปจาก Cisco)

1.

โปรโตคอล (Protocol)

ตัวอย่าง การแสดงความหมายของ IPv6 address จากเลขฐานสอง 128 บิต

```
0010000111011010000000001101001100000000000000001011110011101100000010
101010100000000011111111111110001010011001110001011111
```

แบ่งเป็นชุดละ 16 บิต ได้ 8 ชุด ดังนี้

ฐาน 2	0010 0001 1101 1010	0000 0000 1101 0011	0000 0000 0000 0000	0010 1111 0011 1011
ฐาน 16	21DA	00D3	0000	2F3B
ฐาน 2	0000 0010 1010 1010	0000 0000 1111 1111	1111 1110 0010 1001	1001 1100 0101 1111
ฐาน 16	02AA	00FF	FE29	9C5F

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)

ทำการแปลงเป็นเลขฐาน 16 และใช้โคลนกัน จะได้การแสดงความหมายของ IPv6 address ดังนี้

21DA:00D3:0000:2F3B:02AA:00FF:FE29:9C5F หรือ 21da:00d3:0000:2f3b:02aa:00ff:fe29:9c5f

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

ICMP (Internet Control Message Protocol)

อีกตัวอย่างหนึ่งของโพรโทคอลในชั้นนี้ คือ ICMP ซึ่งเป็นโพรโทคอลที่ใช้ในการสอบถามข้อมูลข่าวสารระหว่างกันของระบบเครือข่ายและเครื่องคอมพิวเตอร์ โดย ICMP เป็นโพรโทคอลสำหรับการส่งข้อความตรวจสอบสถานะการเชื่อมต่อกันระหว่างอุปกรณ์โดยจะแสดงผลลัพธ์ออกมา เช่น ผ่านการใช้งานคำสั่งการปิง (Ping) ซึ่งเป็นคำสั่งสำหรับการตรวจสอบการเชื่อมต่อกันระหว่างเครื่องต้นทางและเครื่องปลายทางและ traceroute ซึ่งเป็นคำสั่งในการตรวจสอบเส้นทางที่ใช้จากเครื่องต้นทางติดต่อไปยังเครื่องปลายทางในความเป็นจริง ICMP message มีด้วยกันหลายประเภท แต่ในหลักสูตรนี้จะกล่าวถึงการแจ้งสถานะการเชื่อมต่อระหว่างอุปกรณ์โดย ใช้การ ping หรือ traceroute เท่านั้น (ดูรายละเอียดการใช้งานในหน่วยการเรียนรู้ที่ 7 การใช้โปรแกรมประยุกต์)

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

ARP (Address Resolution Protocol)

Address Resolution Protocol หรือ ARP (อ่านว่าอาร์ฟหรือเออาร์พี) ทำหน้าที่ในการแปลง IP address ให้เป็น MAC address

จำไว้ว่าแต่ละโหนดบนเครือข่าย IP ต้องมีทั้ง MAC address และ IP address ซึ่งโหนดต้องใช้ทั้งสองแอดเดรสนี้เพื่อที่จะส่งข้อมูล โหนดต้องใช้ MAC address และ IP address ของตัวเองในฟิลด์ Source และต้องใช้ทั้ง MAC address และ IP address ของผู้รับสำหรับฟิลด์ Destination ในขณะที่ IP address ของปลายทางจะใช้สำหรับเลเยอร์ที่สูงกว่าของโมเดล OSI

โหนดต้นทางต้องการวิธีการหา MAC address ของปลายทางสำหรับการเชื่อมโยงอีเทอร์เน็ต นี่คือจุดประสงค์ของการใช้ ARP

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โปรโตคอล (Protocol)

ARP จะอาศัยการทำงานส่งข้อความของอีเทอร์เน็ต (Ethernet) แบบbroadcast ซึ่งเรียกว่า ARP request และยูนิคาสต์ ARP reply

โปรโตคอล ARP มีสองฟังก์ชันพื้นฐาน

- 🌐 การแปลง (Resolving) IPv4 address ไปเป็น MAC address
- 🌐 การดูแลรักษาตารางของการแมป (Maintaining a table of mappings)

หมายเหตุ

บางครั้ง ARP ถูกพิจารณาว่าทำงานที่ชั้นหรือเลเยอร์ที่ 2.5 คือระหว่างชั้นดาตalink และชั้นเน็ตเวิร์ก และใน IPv6 address ไม่มีการใช้งาน ARP แล้ว แต่ใช้โปรโตคอลชื่อ Neighbor Discovery Protocol (NDP) ที่มีหลักการเดียวกัน

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โพรโทคอล (Protocol)

1.3.6 ชั้นเชื่อมโยงข้อมูลหรือดาตาลิงก์ (Data link layer)

อีเทอร์เน็ต (Ethernet) เป็นเทคโนโลยีแลนที่ได้รับความนิยมที่สุดในโลก จากเริ่มต้นที่ความเร็ว 10 Mbps จนพัฒนาถึง 400 Gbps และสามารถใช้กับสายได้หลากหลายประเภท รวมถึงมีการใช้งานที่นอกเหนือจากเครือข่ายแลนไปจนถึงการใช้งานในแมน

อีเทอร์เน็ตทำงานในชั้นดาตาลิงก์และฟิสิคัล มาตรฐานของอีเทอร์เน็ตโพรโทคอลจะกำหนดหลายแง่มุมของการสื่อสารเครือข่ายรวมทั้งรูปแบบเฟรม (Frame format) ขนาดของเฟรม (Frame size) ระยะเวลา (Timing) และการเข้ารหัส (Encoding) เมื่อมีการส่งข้อความระหว่างโฮสต์บนเครือข่ายอีเทอร์เน็ตโฮสต์จะจัดรูปแบบข้อความให้อยู่ในเลย์เอาต์ของเฟรมที่ถูกระบุไว้ตามมาตรฐาน ซึ่งเฟรม คือ หน่วยข้อมูลโพรโทคอล (Protocol Data Unit : PDU) ของชั้นดาตาลิงก์นี้

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โปรโตคอล (Protocol)

หมายเหตุ

ในการทำงานของชั้นดาตalink จะต้องสามารถระบุแต่ละอุปกรณ์ที่กำลังทำการสื่อสารกัน โดยใช้หมายเลขทางกายภาพ ซึ่งคือ MAC address โดยข้อมูล MAC address ต้นทางและปลายทางจะถูกเพิ่มเข้าไปในส่วนหัวของเฟรม

อีเทอร์เน็ตจะประกอบด้วยมาตรฐานที่ชั้นล่างเหล่านี้ จะเป็นการดีที่สุดที่จะเข้าใจด้วยการอ้างอิงถึงโมเดล OSI ซึ่งโมเดล OSI จะแยกฟังก์ชันของชั้นดาตalink เกี่ยวกับการจัดการแอดเดรส (Addressing) การจัดการเฟรม (Framing) การเข้าถึงสื่อ (Accessing the media) ออกจากมาตรฐานฟิสิกส์เลเยอร์ของสื่อ

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

โปรโตคอล (Protocol)

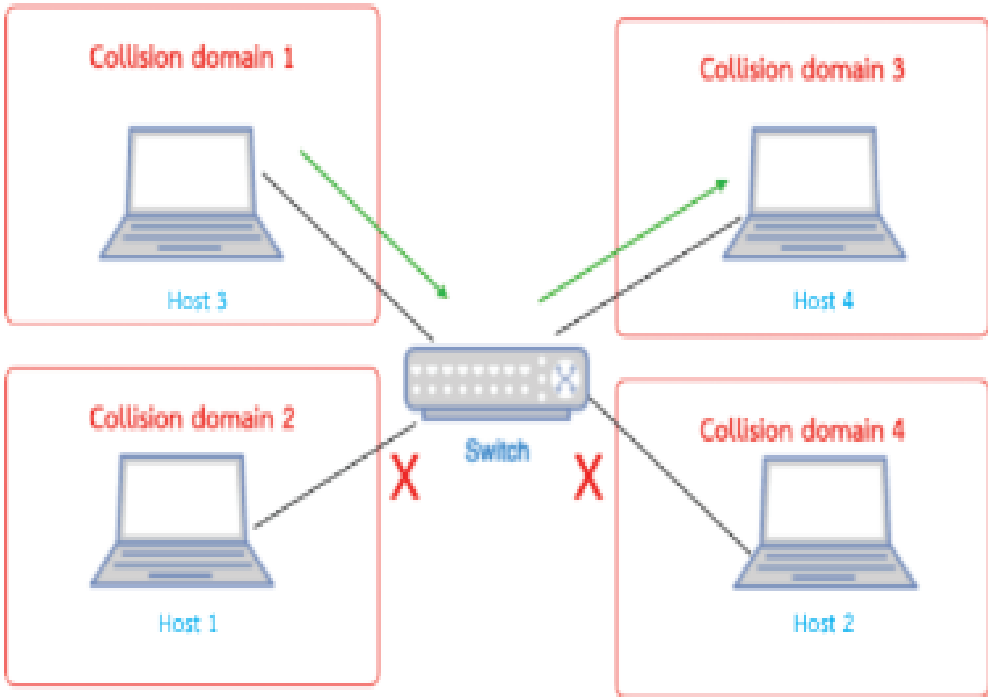
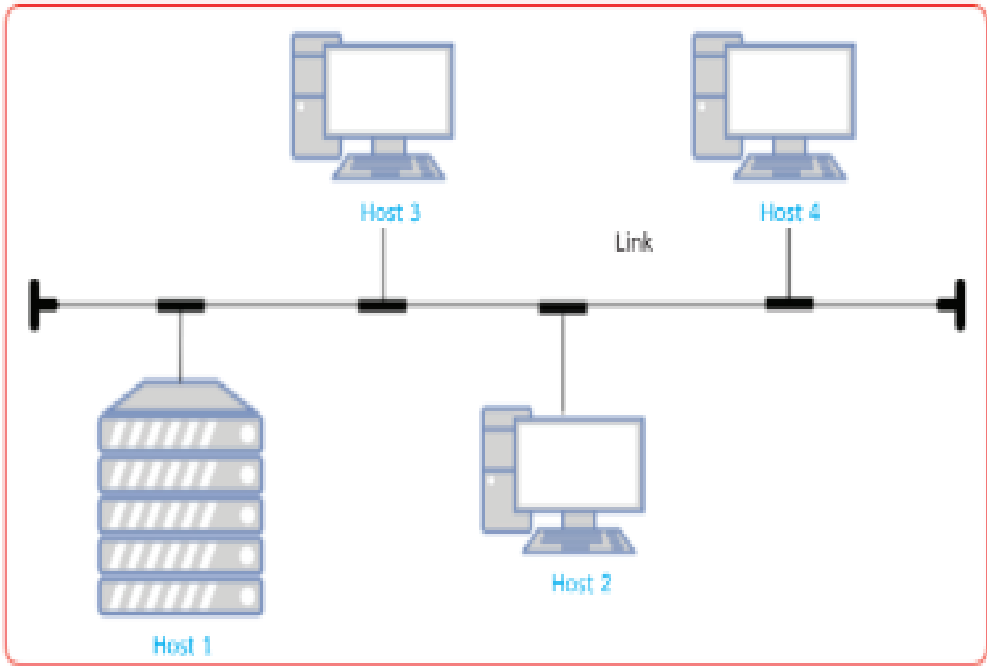
มาตรฐานอีเทอร์เน็ตจะกำหนดทั้งโปรโตคอลชั้นที่ 2 และเทคโนโลยีของชั้นที่ 1 อย่างไรก็ตามข้อกำหนดของอีเทอร์เน็ต (Ethernet specifications) จะสนับสนุนสื่อ แบบด์วิธที่ ชั้นที่ 1 และชั้นที่ 2 ที่แตกต่างจากนี้ได้รูปแบบเฟรมและแบบแผนของแอคเครสชั้นพื้นฐานจะเหมือนกันแม้ว่าจะทำงานกับอีเทอร์เน็ตที่แตกต่างกัน

ลักษณะและการทำงานของอีเทอร์เน็ตที่มีวิวัฒนาการมาจากเทคโนโลยีการสื่อสารข้อมูลที่ใช้สื่อร่วมกัน (Shared media) โดยมีการเชื่อมต่อกันในลักษณะบัส (Bus Topology) (ดูเพิ่มเติมเรื่อง Bus Topology ในหัวข้อที่ 2) และมีการแย่งชิงการใช้สื่อ (Contention-based) โดยใช้โปรโตคอล CSMA/ Collision Detection (CSMA/CD) มาเป็นเทคโนโลยีฟูลดูเพล็กซ์ที่มีแบนด์วิธที่สูง (High bandwidth, Full-duplex technology) ซึ่งมักใช้การเชื่อมต่อกันในลักษณะดาว (Star Topology) ในปัจจุบัน

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โปรโตคอล (Protocol)



รูปที่ 5.14 โครงสร้างการเชื่อมต่ออินเทอร์เน็ตในอดีตรูปแบบบัสมาเป็นแบบดาวที่ได้รับความนิยมในปัจจุบัน

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

โพรโทคอล (Protocol)



ใน CSMA/Collision Detection (CSMA/CD) อุปกรณ์จะตรวจสอบสื่อสำหรับการมีอยู่ของสัญญาณข้อมูล หากไม่มีสัญญาณข้อมูล แสดงให้เห็นว่าสื่อนั้นว่าง อุปกรณ์จะสามารถส่งข้อมูลได้ หากมีการตรวจพบสัญญาณ แสดงให้เห็นว่ามีอุปกรณ์อื่นกำลังส่งในเวลาเดียวกัน อุปกรณ์ทั้งหมดจะหยุดส่งและจะลองส่งอีกครั้งในภายหลัง รูปแบบดั้งเดิมของอีเทอร์เน็ตถูกพัฒนาขึ้นโดยวิธีการนี้ ซึ่งมีการใช้สื่อร่วมกันและสื่อนั้นมีลักษณะแบบ Half-duplex คือ ณ ขณะหนึ่งบนสื่อนั้น จะทำได้เพียงแค่ส่งหรือรับสัญญาณเท่านั้นไม่สามารถที่จะรับและส่งได้พร้อม ๆ กัน



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

1.

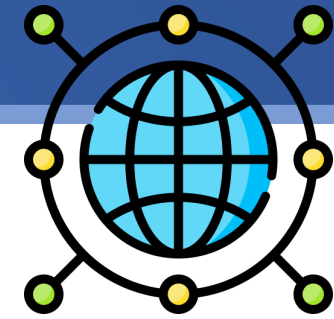
โพรโทคอล (Protocol)

จากการใช้งานอย่างแพร่หลายร่วมกับเทคโนโลยีสวิตช์ในเครือข่ายสมัยใหม่ ในปัจจุบันไม่จำเป็นต้องใช้ CSMA/CD ในเครือข่ายแลนใช้ร่วมกับเทคโนโลยีสวิตช์ การเชื่อมต่อแบบมีสายเกือบทั้งหมดระหว่างอุปกรณ์ในเครือข่ายจะมีการเชื่อมต่อแบบ Full-duplex คือ อุปกรณ์สามารถส่งและรับพร้อมกันได้ตลอดเวลาของวันนี้จะไม่มี การชนกันเกิดขึ้น

อย่างไรก็ตาม การเชื่อมต่อเครือข่ายแลนไร้สาย (Wireless LAN) ยังคงมีการชนกันของข้อมูล อุปกรณ์ในเครือข่ายไร้สายจะใช้กลไกการเข้าถึงสื่อแบบ CSMA/Collision Avoidance (CSMA/CA)

ตัวอย่างอื่นของโพรโทคอลในชั้นนี้ คือ LLDP (Link Layer Discovery Protocol) และ CDP (Cisco Discovery Protocol) ซึ่งเป็นโพรโทคอลที่สามารถตรวจสอบได้ว่าอุปกรณ์ที่เชื่อมต่อกันอยู่โดยตรงเป็นอุปกรณ์อะไร รุ่นอะไร มี IP Address อะไรบ้าง ต่างกันที่ CDP เป็นโพรโทคอลที่ทำงานได้กับอุปกรณ์ยี่ห้อ Cisco เท่านั้น LLDP เป็นมาตรฐาน IEEE 802.1AB ใช้กับอุปกรณ์ได้ทุกยี่ห้อ

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



1.

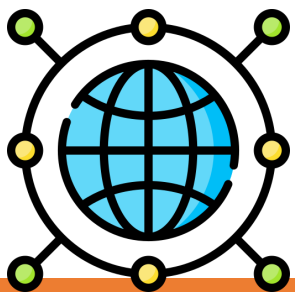
โพรโทคอล (Protocol)



1.3.7 ชั้นกายภาพหรือฟิสิคัล (Physical layer)

ทำหน้าที่กำหนดลักษณะทางกายภาพในการเชื่อมต่อเครือข่าย เช่น ขนาดพิน จำนวนพิน ประเภทหัวต่อ (Connector) การประสานจังหวะการทำงานหรือซิงโครไนเซชัน (Synchronization) (ซึ่งเมื่อนำข้อมูลที่ได้จากโพรโทคอลในแต่ละชั้นมาประกอบรวมกันจะได้ดังรูป) และแปลงข้อมูลในรูปของสัญญาณดิจิทัลแต่ละบิตให้ผ่านตัวกลางแต่ละชนิดได้ เช่น แปลงเป็นสัญญาณไฟฟ้ากรณีที่อยู่กลางเป็นสายทองแดงแปลงเป็นสัญญาณแสงกรณีที่อยู่กลางเป็นสายใยแก้วนำแสง แปลงเป็นสัญญาณคลื่นวิทยุกรณีที่อยู่กลางเป็น Wi-Fi

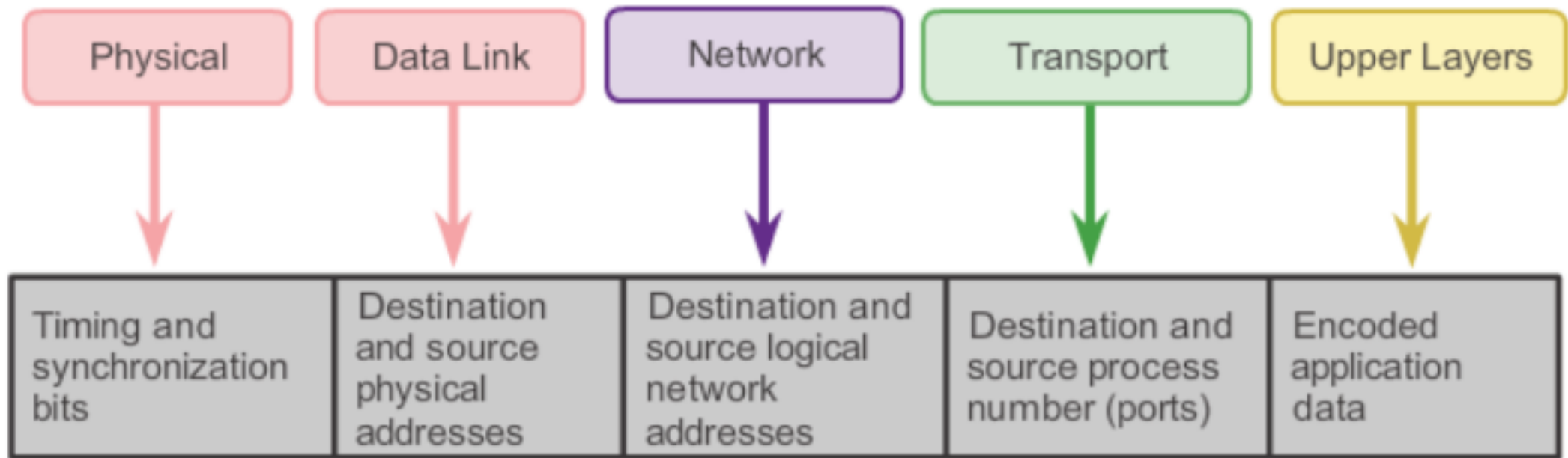
ดังนั้นในชั้นนี้ มักจะใช้เป็นมาตรฐานในการผลิตอุปกรณ์ต่าง ๆ เช่น USB, OTN (Optical Transport Network), IEEE 802.11, IEEE 802.3, EIA RS-232 และ Bluetooth physical layer เป็นต้น



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

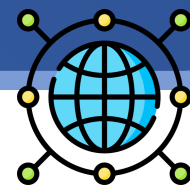
1.

โพรโทคอล (Protocol)



รูปที่ 5.15 ข้อมูลที่ถูกห่อหุ้มด้วยส่วนหัวของแต่ละชั้นในโมเดล OSI (รูปจาก Cisco)

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์



2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

โทโพโลยี (Topology) หรือรูปแบบการเชื่อมต่อเครือข่าย เป็นลักษณะทั่วไปที่กล่าวถึงการเชื่อมต่อคอมพิวเตอร์ทางกายภาพว่ามีรูปแบบหน้าตาอย่างไร เพื่อให้สามารถสื่อสารร่วมกันได้ เครือข่ายแลนจะมีรูปแบบของโทโพโลยีหลายแบบด้วยกัน โดยมีข้อดีข้อเสียที่แตกต่างกัน ซึ่งผู้ออกแบบระบบควรศึกษาและเลือกใช้โทโพโลยีที่เหมาะสม โดยปกติโทโพโลยีที่นิยมใช้กันบนเครือข่ายแลนมีอยู่ 6 แบบ ดังนี้

2.1 แบบบัส (Bus Topology)

เป็นการเชื่อมต่อคอมพิวเตอร์ทุกเครื่องบนสายสัญญาณหลักเส้นเดียวที่เรียกว่า บัส (Bus) ที่ปลายทั้งสองด้านปิดด้วยอุปกรณ์ที่เรียกว่าอุปกรณ์ปิดหัวสาย (Terminator) เพื่อป้องกันสัญญาณรบกวนเข้ามาในสายสัญญาณ โทโพโลยีแบบบัสเป็นโทโพโลยีที่ได้รับความนิยมในยุคแรก ๆ โดยไม่มีอุปกรณ์เครือข่ายเป็นศูนย์กลางในการเชื่อมต่อ หากโหนดใดหยุดทำงานก็ไม่มีผลกับโหนดอื่นในเครือข่าย



โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

ข้อดี

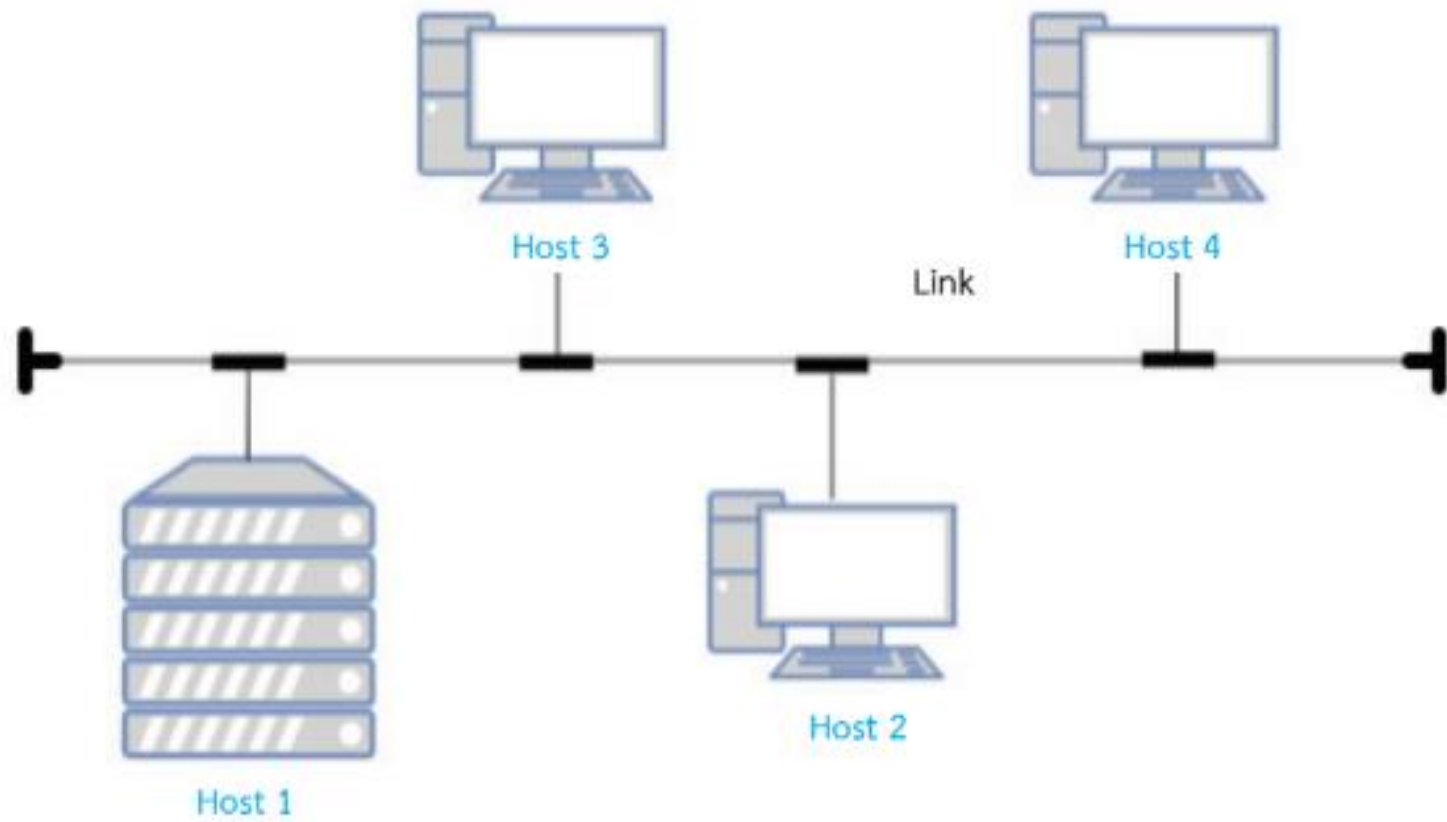
1. สามารถติดตั้งได้ง่าย เพราะเป็นโครงสร้างเครือข่ายที่ไม่ซับซ้อน
2. การเดินสายติดตั้งสามารถทำได้ง่าย
3. ง่ายต่อการเพิ่มโหนดใหม่เข้าไปในระบบ โดยโหนดนี้สามารถใช้สายส่งข้อมูลที่มีอยู่แล้วได้

ข้อเสีย

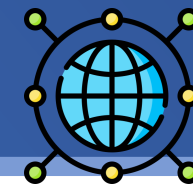
1. ถ้ามีสายเส้นใดเส้นหนึ่งหลุดหรือขาด จะทำให้ระบบเครือข่ายทั้งหมดหยุดการทำงานลง
2. ถ้าระบบเกิดข้อผิดพลาดจะหาข้อผิดพลาดได้ยาก โดยเฉพาะถ้าเป็นระบบเครือข่ายขนาดใหญ่

2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

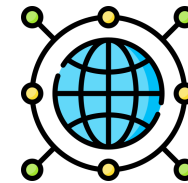


รูปที่ 5.16 ภาพโครงสร้างเครือข่ายแบบบัส (Bus Topology)



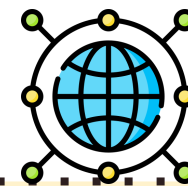
2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์



2.2 แบบดาว (Star topology)

เป็นการเชื่อมต่อโหนดหรือจุดต่าง ๆ ออกจากอุปกรณ์ที่เป็นศูนย์กลาง เช่น ฮับหรือสวิตช์ อุปกรณ์ในระบบเครือข่ายจะมีสายสัญญาณเชื่อมต่อกับศูนย์กลาง โดยไม่มีการใช้สายสัญญาณร่วมกัน หากอุปกรณ์ใดเกิดความเสียหายจะไม่มีผลกระทบกับโหนดอื่น ๆ ปัจจุบันนิยมใช้อุปกรณ์สวิตช์เป็นตัวยุติเชื่อมต่อจากคอมพิวเตอร์แม่ข่าย และกระจายไปยังเครื่องลูกข่าย



ข้อดี

ง่ายต่อการให้บริการ เพราะมีศูนย์กลางอยู่ที่สวิตช์เครื่องเดียวและเมื่อเกิดความเสียหายที่คอมพิวเตอร์เครื่องใดเครื่องหนึ่ง คอมพิวเตอร์เครื่องอื่นจะไม่มีผลกระทบอันใดเพราะใช้สายคนละเส้น

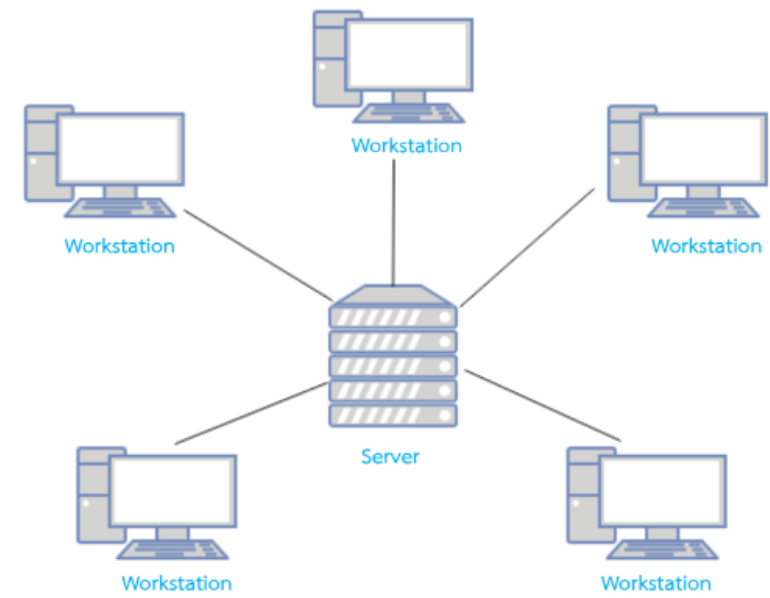


2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

ข้อเสีย

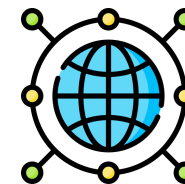
หากอุปกรณ์หลัก เช่น สวิตช์ขัดข้อง ระบบจะไม่สามารถทำงานต่อไปได้ ต้องเปลี่ยนอุปกรณ์ใหม่มาทดแทน



รูปที่ 5.17 ภาพโครงสร้างเครือข่ายแบบดาว (Star Topology)



2. รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์



2.3 แบบวงแหวน (Ring Topology)

เป็นการเชื่อมต่อเครือข่ายเป็นรูปวงแหวนในเครือข่าย โหนดแรกเชื่อมต่อกับโหนดตัวถัดไป และโหนดตัวถัดไปเชื่อมต่อกับโหนดที่อยู่ถัดไปอีก จนกระทั่งถึงโหนดสุดท้ายจะวนไปเชื่อมต่อกับโหนดแรก การรับส่งข้อมูลในเครือข่ายจะต้องผ่านทุกโหนด แต่ละโหนดต้องคอยตรวจสอบข้อมูลที่ส่งมา ถ้าไม่ใช่ของตนเองต้องส่งผ่านไปยังโหนดอื่นต่อไป

ข้อดี

ใช้สายน้อย นิยมเชื่อมต่อด้วยสายสัญญาณใยแก้วนำแสง เพราะสามารถส่งข้อมูลทางเดียวกันด้วยความเร็วสูง

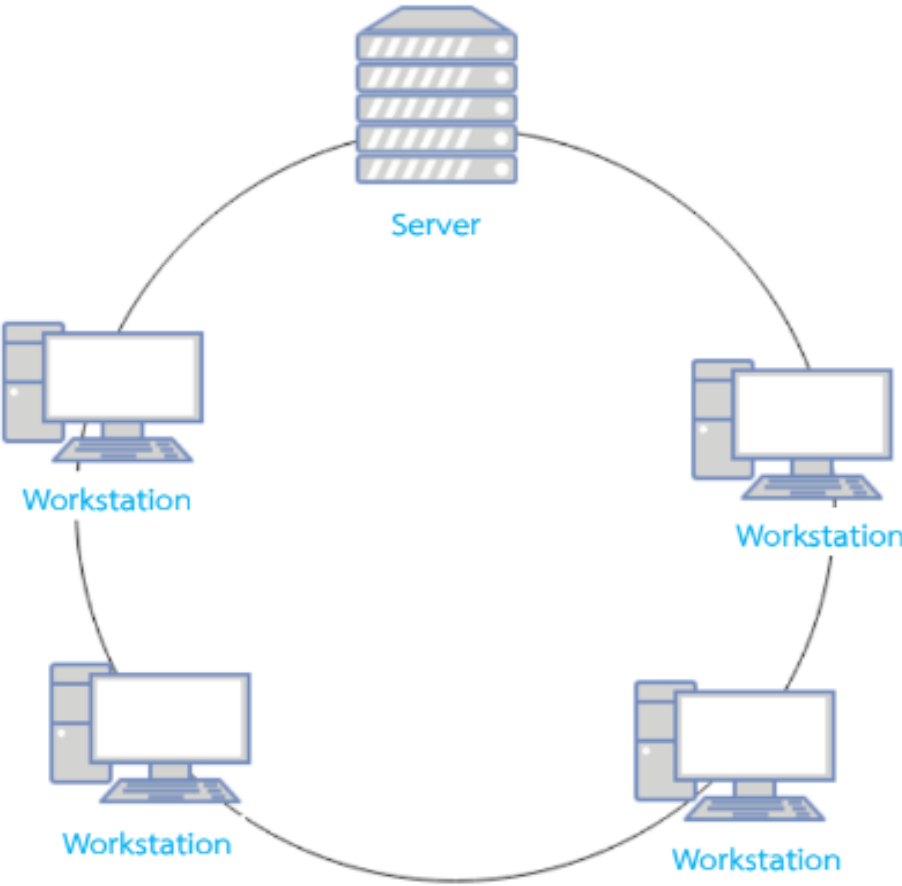
ข้อเสีย

ถ้าโหนดใดเสียระบบจะไม่สามารถทำงานต่อไปได้จนกว่าจะแก้ไขจุดเสียนั้น



2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์



รูปที่ 5.18 ภาพโครงสร้างเครือข่ายแบบวงแหวน (Ring Topology)

โปรโตคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2. รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

2.4 โทโพโลยีแบบตาข่ายหรือเมช (Mesh Topology)

เป็นรูปแบบการเชื่อมต่อที่ดีที่สุดในแง่ของความเร็วและเสถียรภาพการทำงาน สามารถป้องกันการผิดพลาดที่อาจจะเกิดขึ้นกับระบบได้ดีที่สุด เพราะทุกโหนดในเครือข่ายจะมีสายเชื่อมถึงกันทุกโหนดหากมีโหนดในเครือข่ายขัดข้องหรือสายเส้นใดเส้นหนึ่งขาด ระบบยังคงทำงานได้

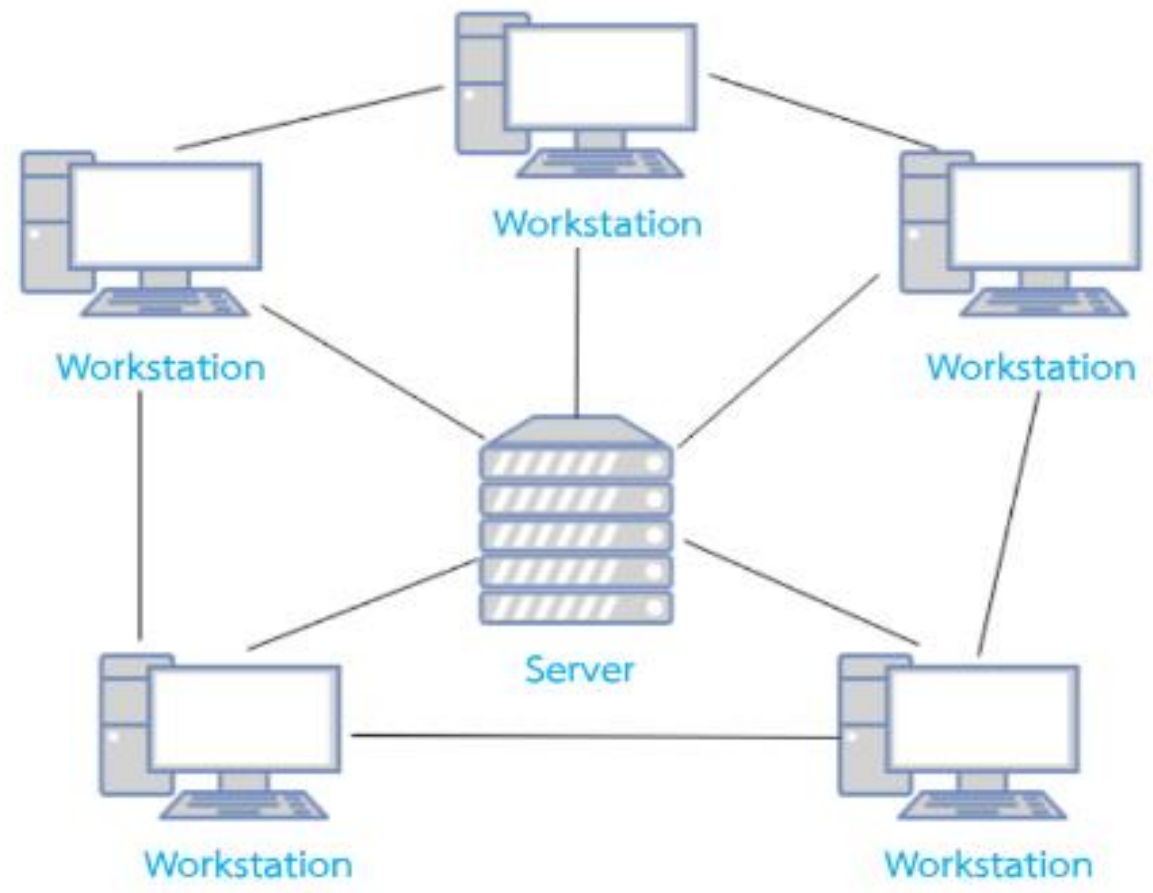
โดยมีสูตรคำนวณจำนวนจุดในการเชื่อมต่อดังนี้ $N(N-1)/2$ โดย N คือจำนวนโหนดที่เชื่อมต่อกันอยู่เช่น เชื่อมต่อ 5 โหนดเข้าด้วยกันจะต้องมีการเชื่อมต่อทั้งหมด $5(5-1)/2 = 10$ จุด

หากเป็นเครือข่ายแบบที่ใช้สาย ระบบจะเห็นว่าจะสิ้นเปลืองมากเพราะต้องใช้การ์ดแลนและสายหลายชุดต่อหนึ่งโหนด ในการใช้งานจริง อาจจะไม่ได้ออกแบบแบบเมชสมบูรณ์ (Full Mesh) จึงใช้การเชื่อมต่อแบบเมชบางส่วน (Partial mesh) โดยไม่จำเป็นต้องต่อโหนดให้เข้าถึงกันทุกจุด แต่เลือกเชื่อมต่อเฉพาะจุดที่สำคัญๆ เท่านั้น นอกจากนี้ยังได้มีการนำโทโพโลยีแบบเมชมาใช้กับเครือข่ายไร้สาย โดยเฉพาะกับเราเตอร์และ Access Point โดยใช้ความถี่ของ Wi-Fi ยาน 2.4 GHz และ 5 GHz แทนสายสัญญาณหลายเส้น

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2.

รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์



รูปที่ 5.19 โครงสร้างโทโพโลยีแบบเมช (Mesh Topology)



2. รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

2.5 โทโพโลยีแบบทรี (Tree Topology)

มีลักษณะเชื่อมโยงคล้ายกับโครงสร้างอื่น ๆ โดยนำข้อดีของโครงสร้างแบบบัส วงแหวน และดาวมารวมกันเพื่อให้สามารถสร้างระบบเครือข่ายขนาดใหญ่ได้ โดยมีแกนหลักหรือแบกโบน (Back Bone) เป็นแบบบัส หรือวงแหวนที่สามารถเชื่อมต่อเครือข่ายในระยะไกลด้วยความเร็วสูงได้ (เช่น Fiber Optic) แล้วไปขยายเครือข่ายระยะใกล้ที่มีอุปกรณ์จำนวนมากด้วยโทโพโลยีแบบดาว

ข้อดี

1. รองรับการขยายเครือข่ายขนาดใหญ่
2. สามารถกำหนดและบริหารจัดการประสิทธิภาพของเครือข่ายได้ดี

โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2. รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

ข้อเสีย

1. ความยาวของแต่ละเซกเมนต์อาจแตกต่างกันไปขึ้นอยู่กับสายสัญญาณที่ใช้
2. หากสายสัญญาณ Black bone เสียหาย เครือข่ายจะไม่สามารถสื่อสารกันได้จึงควรมีสายหรือระบบสำรอง
3. การติดตั้งทำได้ยากและซับซ้อนกว่าโทโพโลยีแบบอื่น

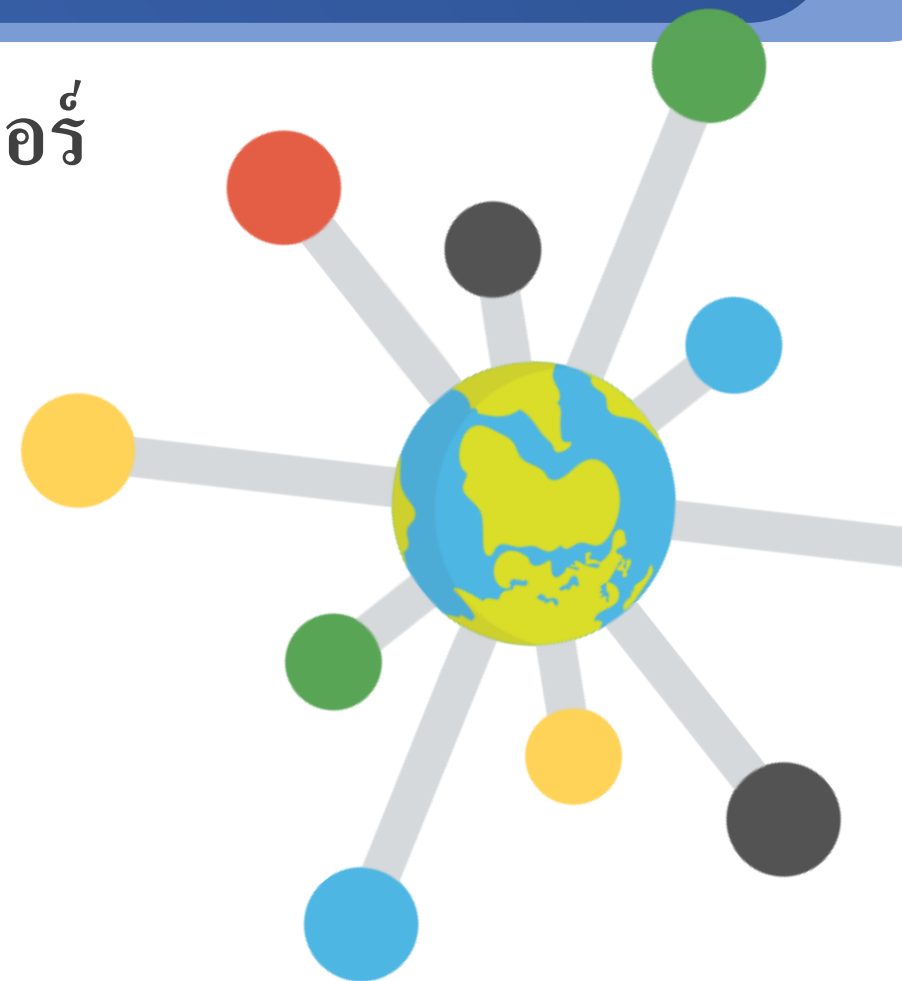


โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

2. รูปแบบการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์

2.6 เครือข่ายแบบผสม (Hybrid Network)

เป็นเครือข่ายคอมพิวเตอร์ที่ผสมผสานระหว่างรูปแบบต่าง ๆ หลายแบบเข้าด้วยกัน คือ จะมีเครือข่ายคอมพิวเตอร์ย่อยหลาย ๆ เครือข่ายเพื่อให้เกิดประสิทธิภาพสูงสุดในการทำงานเครือข่ายบริเวณกว้างซึ่งเครือข่ายที่ถูกเชื่อมต่ออาจจะอยู่ห่างกันคนละจังหวัด หรืออาจจะอยู่คนละประเทศก็ได้



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

ในการสื่อสารข้อมูล ไม่ว่าจะเป็นการสื่อสารด้วยภาษามนุษย์หรือการสื่อสารผ่านระบบคอมพิวเตอร์ นอกจากจะมีการเชื่อมต่อด้วยอุปกรณ์ ข้อความที่จะสื่อสาร และสื่อกลางในการสื่อสาร การที่จะทำให้อุปกรณ์หลากหลายยี่ห้อหลายรุ่นสามารถทำงานด้วยกันได้ซึ่งเป็นสิ่งสำคัญที่จะต้องกำหนดให้เป็นมาตรฐานเดียวกัน นั่นคือ ระเบียบวิธีหรือข้อตกลงที่ใช้ในการสื่อสารข้อมูลหรือเรียกว่า โพรโทคอล เพื่อทำให้อุปกรณ์ต่าง ๆ ในเครือข่ายคอมพิวเตอร์สามารถทำงานร่วมกันได้อย่างราบรื่น

โดยการทำงานรับส่งข้อมูลในระบบเครือข่ายจะมีโพรโทคอลกำหนดไว้อย่างชัดเจนเพื่อให้ผู้ส่งและผู้รับข้อมูลเข้าใจกติกาตรงกัน เช่น โพรโทคอล HTTP สำหรับการดูเว็บไซต์ HTTPS สำหรับการเข้าชมเว็บไซต์ที่ต้องการความมั่นคงปลอดภัยของข้อมูล หรือ SMTP สำหรับการเรียกดูอีเมล เป็นต้น



โพรโทคอลและรูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

นอกจากโพรโทคอลแล้ว หัวใจสำคัญของการที่จะทำให้การสื่อสารข้อมูลมีประสิทธิภาพทั้งในด้านความเร็วและเสถียรภาพการทำงาน คือ รูปแบบการเชื่อมต่อเครือข่ายคอมพิวเตอร์หรือโทโพโลยีการออกแบบโทโพโลยีในระบบเครือข่ายนั้นจำเป็นจะต้องสอดคล้องกับสภาพทางกายภาพของพื้นที่และอุปกรณ์ที่จะถูกติดตั้งในระบบเครือข่าย ซึ่งการออกแบบที่ดีนอกจากจะพิจารณาถึงการใช้งานในปัจจุบันแล้ว ต้องพิจารณาความต้องการใช้งานในอนาคตอีกด้วย





การติดตั้งระบบปฏิบัติการ เครือข่ายคอมพิวเตอร์



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

1.

ประเภทของระบบปฏิบัติการ



1.1 การทำงานของระบบปฏิบัติการ



ระบบปฏิบัติการ (Operating system) หรือโอเอส (OS) เป็นระบบซอฟต์แวร์ที่ทำหน้าที่จัดการอุปกรณ์คอมพิวเตอร์ ซอฟต์แวร์และบริการโปรแกรมคอมพิวเตอร์ ระบบปฏิบัติการมีหน้าที่หลัก ๆ คือการจัดสรรทรัพยากรในเครื่องคอมพิวเตอร์ เพื่อให้บริการซอฟต์แวร์ประยุกต์ ในเรื่องการรับส่งและจัดเก็บข้อมูลกับฮาร์ดแวร์ เช่น การส่งข้อมูลภาพไปแสดงผลที่จอภาพ การส่งข้อมูลไปเก็บหรืออ่านจากหน่วยจัดเก็บข้อมูล เช่น ฮาร์ดดิสก์ หรือ SSD การรับส่งข้อมูลในระบบเครือข่าย การส่งสัญญาณเสียงไปออกลำโพง หรือจัดสรรพื้นที่ในหน่วยความจำตามที่ซอฟต์แวร์ประยุกต์ร้องขอ รวมทั้งทำหน้าที่จัดสรรเวลาการใช้ CPU ในกรณีที่อนุญาตให้ซอฟต์แวร์ประยุกต์หลาย ๆ ตัวทำงานพร้อม ๆ กัน



1. ประเภทของระบบปฏิบัติการ

ระบบปฏิบัติการช่วยทำให้ตัวซอฟต์แวร์ประยุกต์ไม่ต้องจัดการเรื่องเหล่านั้นด้วยตนเอง เพียงแค่เรียกใช้บริการจากระบบปฏิบัติการก็พอ ทำให้พัฒนาซอฟต์แวร์ประยุกต์ได้ง่ายขึ้น ดังนั้นระบบปฏิบัติการถือว่าเป็นหัวใจหลักในการกำหนดประสิทธิภาพโดยรวมของคอมพิวเตอร์ การเลือกระบบปฏิบัติการที่เหมาะสมกับระบบงานจึงเป็นสิ่งจำเป็น

ระบบปฏิบัติการแบ่งออกเป็น 2 ลักษณะ ได้แก่ มาตรฐานแบบเปิด (Open Source) และมาตรฐานแบบปิด (Proprietary) ซึ่งข้อแตกต่าง คือ การพัฒนาระบบปฏิบัติการแบบเปิดจะมีการเผยแพร่ต้นฉบับโปรแกรม (Source Code) ที่เปิดเผยหลักการหรือแหล่งที่มาของเทคโนโลยีของซอฟต์แวร์นั้นให้บุคคลภายนอกได้ใช้ ภายใต้เงื่อนไขบางประการที่เปิดโอกาสให้ผู้ใช้ทำการแก้ไข ดัดแปลง และเผยแพร่ซอร์ซโคดได้ ภายใต้เงื่อนไขข้อตกลงทางกฎหมาย ส่วนใหญ่ระบบปฏิบัติการแบบ Open Source



1. ประเภทของระบบปฏิบัติการ

จะถูกพัฒนามาจากระบบยูนิกซ์ (Unix) ที่ชื่อลินุกซ์ (Linux) ซึ่งโดยปกติจะไม่มีค่าใช้จ่ายในการใช้งาน แต่มีผู้พัฒนาระบบปฏิบัติการบางบริษัททำการปรับแต่ง Linux ให้ใช้งานได้สะดวกมากขึ้นด้วยการเพิ่มโปรแกรมรรถประโยชน์หรือยูทิลิตี้ (Utility) แลวนำมาเผยแพร่ฟรี แต่จะเก็บค่าบริการสำหรับการบริการบางอย่าง เช่น Linux Red Hat เป็นต้น

การพัฒนาระบบปฏิบัติการแบบปิด (Proprietary) จะดำเนินการโดยบริษัทเอกชนบริษัทเดียวที่พัฒนาระบบปฏิบัติการของตนเอง เช่น บริษัทเจ้าตลาดสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลโดยส่วนใหญ่คือ Microsoft ที่เป็นเจ้าของระบบปฏิบัติการ Microsoft Windows และคอมพิวเตอร์ส่วนบุคคลตระกูล Mac ของบริษัท Apple ที่ใช้ระบบปฏิบัติการ Mac OS หรือ OS X ซึ่งถูกพัฒนาจากระบบ UNIX แต่จำกัดการใช้งานสำหรับเครื่อง Mac เท่านั้นจึงถือเป็นระบบปฏิบัติการมาตรฐานแบบปิดเช่นกัน

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

1.

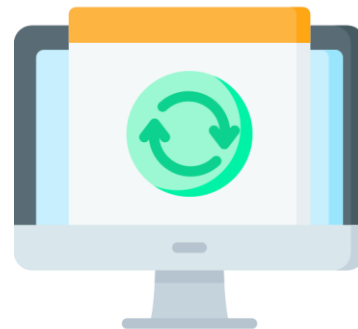
ประเภทของระบบปฏิบัติการ

สามารถแบ่งระบบปฏิบัติการคอมพิวเตอร์ในเครือข่ายออกเป็น 2 ลักษณะ ดังนี้



 ระบบปฏิบัติการสำหรับเครื่องแม่ข่าย หรือ Server ได้แก่ Windows Server 2019 ของ Microsoft, Linux Server ที่เป็นระบบ Open Source

 ระบบปฏิบัติการสำหรับเครื่องลูกข่าย แบ่งเป็น 2 แบบหลัก คือ Windows 10 สำหรับเครื่อง PC Mac OS สำหรับเครื่องคอมพิวเตอร์ Mac ของ Apple สำหรับระบบ Closed Source และ Linux สำหรับ Open Source



2.

ระบบปฏิบัติการ Windows Server 2019

เป็นระบบปฏิบัติการที่ใช้สำหรับเครื่องแม่ข่ายซึ่งพัฒนาโดยบริษัท Microsoft ซึ่งก่อนหน้านี้ได้พัฒนาระบบปฏิบัติการสำหรับเครื่องแม่ข่ายควบคู่กับระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลโดยใช้ชื่อว่า Microsoft Windows

ระบบปฏิบัติการที่ใช้กับเครื่องแม่ข่ายในยุคเริ่มต้น ใช้ชื่อ Windows NT ซึ่งเริ่มใช้ในปี 1998 Windows 2000, 2003, 2012 ที่เปิดตัวในปี 2000, 2003, 2012 ตามชื่อรุ่น และระบบปฏิบัติการรุ่นล่าสุดที่ใช้สำหรับเครื่องแม่ข่าย คือ Windows Server 2019



2.

ระบบปฏิบัติการ Windows Server 2019

ในมาตรฐานระบบปิด ผู้ใช้จะต้องจ่ายค่าลิขสิทธิ์ให้กับเจ้าของระบบปฏิบัติการซึ่ง Microsoft ได้กำหนดค่าใช้จ่ายในแบบฉบับ License โดยตรงจาก Microsoft และจะมีให้เลือกใช้อยู่ 2 แบบด้วยกันคือ

1. **แบบ Volume** ซึ่งจะเป็นแบบซื้อขาด เหมือนซื้อโปรแกรมทั่วไปมาใช้งาน

2. **แบบ Services Provider License Agreement (SPLA)** ซึ่งจะเหมือนการเช่าโปรแกรมมาใช้งาน ปัจจุบัน Microsoft ผลักดันผลิตภัณฑ์ของตนในรูปแบบการให้บริการผ่าน Cloud มากขึ้น อย่าง Microsoft Office ก็มีการให้บริการผ่าน Cloud ซึ่งเวอร์ชันเต็ม หรือ License ก็ต้องมีการเช่าโปรแกรมเช่นกัน



2.

ระบบปฏิบัติการ Windows Server 2019

นอกจากจะแบ่งรูปแบบตามลักษณะความสะดวกในการจ่ายเงินแล้ว Microsoft ยังแบ่งรูปแบบ Windows Server ให้เลือกตามขนาดขององค์กรคือ

-  องค์กรขนาดใหญ่ เหมาะสมกับ Windows Server Datacenter
-  องค์กรขนาดกลาง หรือธุรกิจทั่วไป เหมาะสมกับรุ่น Standard Edition
-  องค์กรขนาดเล็ก มีผู้ใช้ไม่เกิน 20 – 25 คน เหมาะสมกับรุ่น Essential Edition



2.

ระบบปฏิบัติการ Windows Server 2019

2.1 การติดตั้งระบบปฏิบัติการ Windows Server 2019



การติดตั้งระบบปฏิบัติการ ผู้ติดตั้งจะต้องตรวจสอบคุณสมบัติของเครื่องคอมพิวเตอร์ที่จะทำการติดตั้งก่อนว่ามีคุณสมบัติหรือมีสเปก (Specification) เหมาะสมกับระบบปฏิบัติการหรือไม่ จากนั้นเตรียมระบบปฏิบัติการที่จะติดตั้ง โดยเตรียมแผ่นโปรแกรมระบบปฏิบัติการหรือ USB Drive ที่สามารถบูตเข้าระบบปฏิบัติการได้

การติดตั้งระบบปฏิบัติการหรือแอปพลิเคชันต่าง ๆ ผู้ผลิตมักจะอนุญาตผู้ใช้สามารถติดตั้งโปรแกรมได้โดยไม่ต้องมีหมายเลขประจำตัวแสดงสิทธิ์ในการทำงาน (License Number หรือ Series Number) เพื่ออำนวยความสะดวกและให้ผู้ใช้ได้ทดสอบการทำงานก่อน

2.

ระบบปฏิบัติการ Windows Server 2019



ในระหว่างการทดสอบระบบก็จะมีข้อจำกัดบางอย่างในการใช้งาน เช่น ในกรณีของ Microsoft Office ปรับแต่งคุณสมบัติบางอย่างไม่ได้ หรือบันทึกข้อมูลไม่ได้ และเมื่อผู้ใช้เริ่มใช้งานระบบปฏิบัติการไประยะหนึ่งหากไม่ได้บันทึกข้อมูลหมายเลขประจำตัวแสดงสิทธิ์ในการใช้งานในระบบเพื่อลงทะเบียนออนไลน์ที่เรียกว่า Activate โปรแกรมหรือระบบปฏิบัติการนั้นก็อาจจะใช้ไม่ได้ ดังนั้นก่อนการติดตั้งควรเตรียมหมายเลขประจำตัวแสดงสิทธิ์ในการใช้งานให้พร้อมและคอมพิวเตอร์ที่ติดตั้งโปรแกรมจะต้องเชื่อมต่อกับอินเทอร์เน็ตเพื่อให้สามารถ Activate และ Update โปรแกรมได้ทันที



2.

ระบบปฏิบัติการ Windows Server 2019

นอกจากนี้ คอมพิวเตอร์แต่ละยี่ห้อ แต่ละรุ่นจะมีโปรแกรมสำหรับปรับแต่งอุปกรณ์หรือช่วยให้ระบบปฏิบัติการรู้จักอุปกรณ์ต่าง ๆ ที่เรียกว่า Driver ซึ่งตอนติดตั้งควรเตรียมโปรแกรม Driver ให้พร้อม จากนั้นจึงเริ่มดำเนินการติดตั้งระบบปฏิบัติการ ดังนี้

1. กำหนดให้เครื่องคอมพิวเตอร์บูตจากสื่อที่บรรจุตัวติดตั้งระบบปฏิบัติการ เช่น USB หรือ CD-ROM โดยศึกษาวิธีการกำหนดค่าระบบจากคู่มือประจำเครื่องคอมพิวเตอร์
2. ใส่แผ่น CD หรือ USB ตัวติดตั้งระบบปฏิบัติการ จากนั้น เปิดเครื่องคอมพิวเตอร์ เมื่อคอมพิวเตอร์โหลดโปรแกรมเบื้องต้นหรือบูทระบบแล้วจะปรากฏหน้าจอให้เลือกภาษา ให้เลือกเป็นภาษาอังกฤษ

2.

ระบบปฏิบัติการ Windows Server 2019

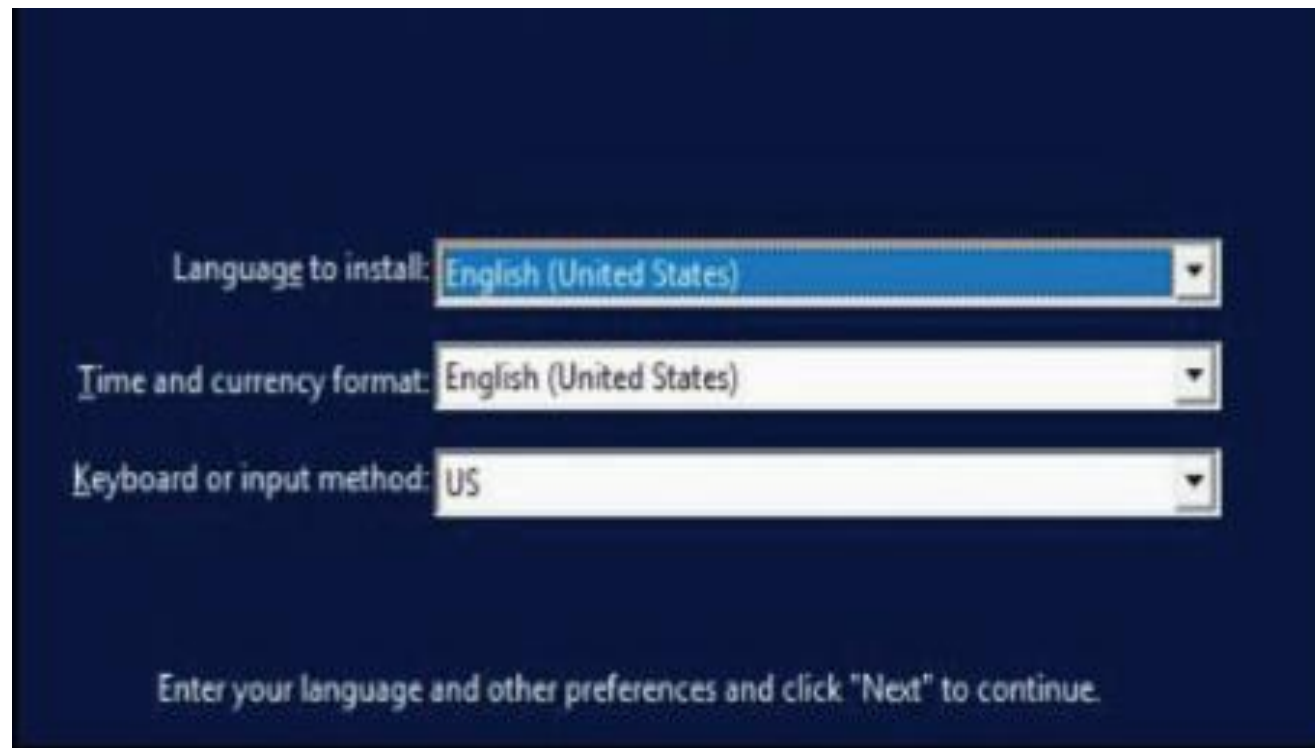


รูปที่ 6.1 หน้าจอการเลือกภาษาที่ใช้ในการติดตั้ง

2.

ระบบปฏิบัติการ Windows Server 2019

3. จากนั้น ในการแสดงผลระหว่างติดตั้งตามรูป เลือกสกุลเงิน และแป้นพิมพ์จากนั้น ให้กดปุ่ม Next



รูปที่ 6.2 หน้าจอการเลือกภาษา สกุลเงิน และแป้นพิมพ์ที่จะใช้

2.

ระบบปฏิบัติการ Windows Server 2019

4. คลิกเมาส์ที่ปุ่ม Install Now

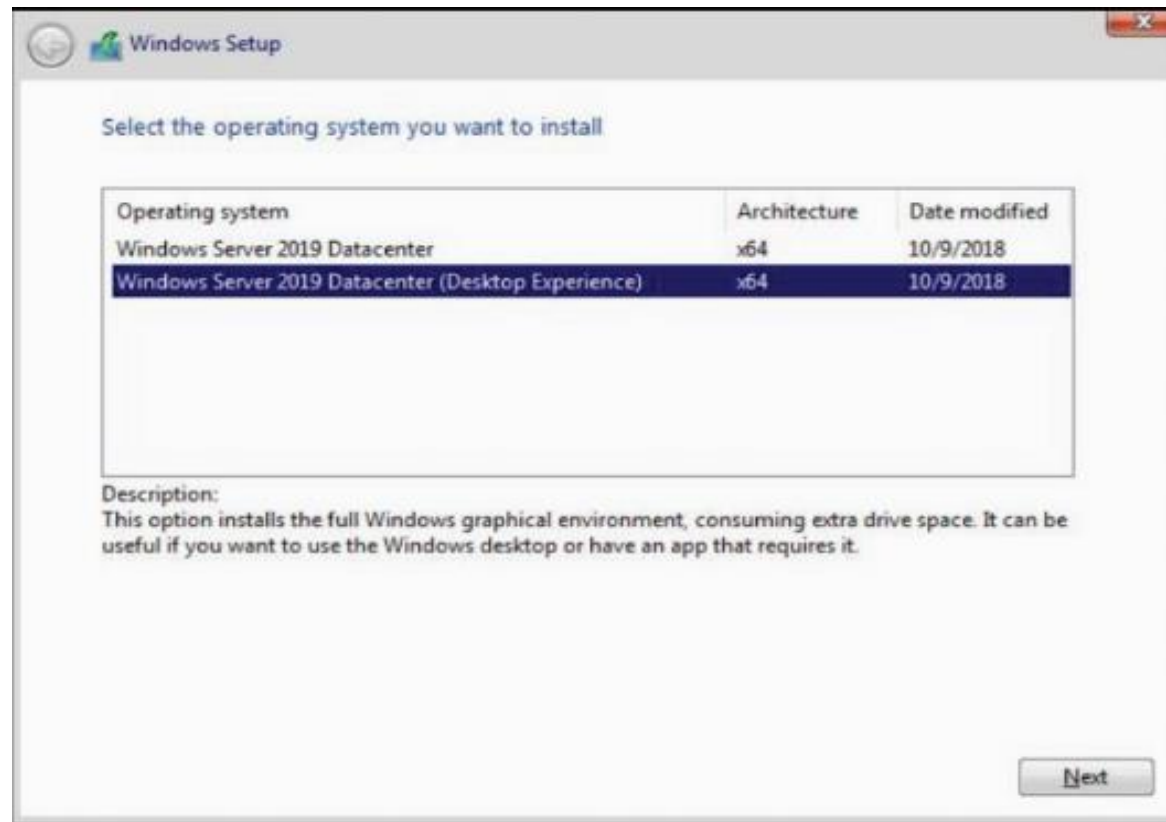


รูปที่ 6.3 หน้าจอเริ่มต้นการ Install

2.

ระบบปฏิบัติการ Windows Server 2019

5. เลือกชนิดของระบบปฏิบัติการจากนั้น คลิก Next

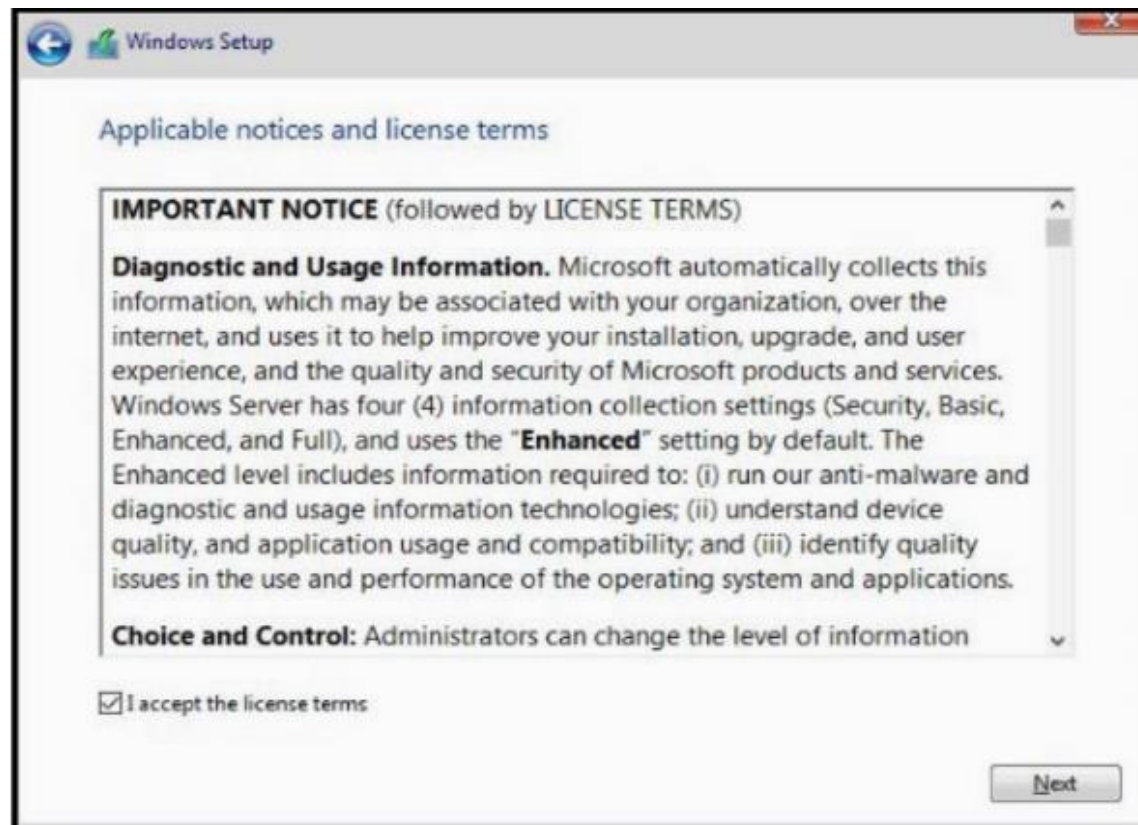


รูปที่ 6.4 หน้าจอการเลือกชนิดของระบบปฏิบัติการ

2.

ระบบปฏิบัติการ Windows Server 2019

6. อ่านข้อตกลงเกี่ยวกับลิขสิทธิ์ แล้วเลือก I accept the license terms จากนั้น คลิก Next



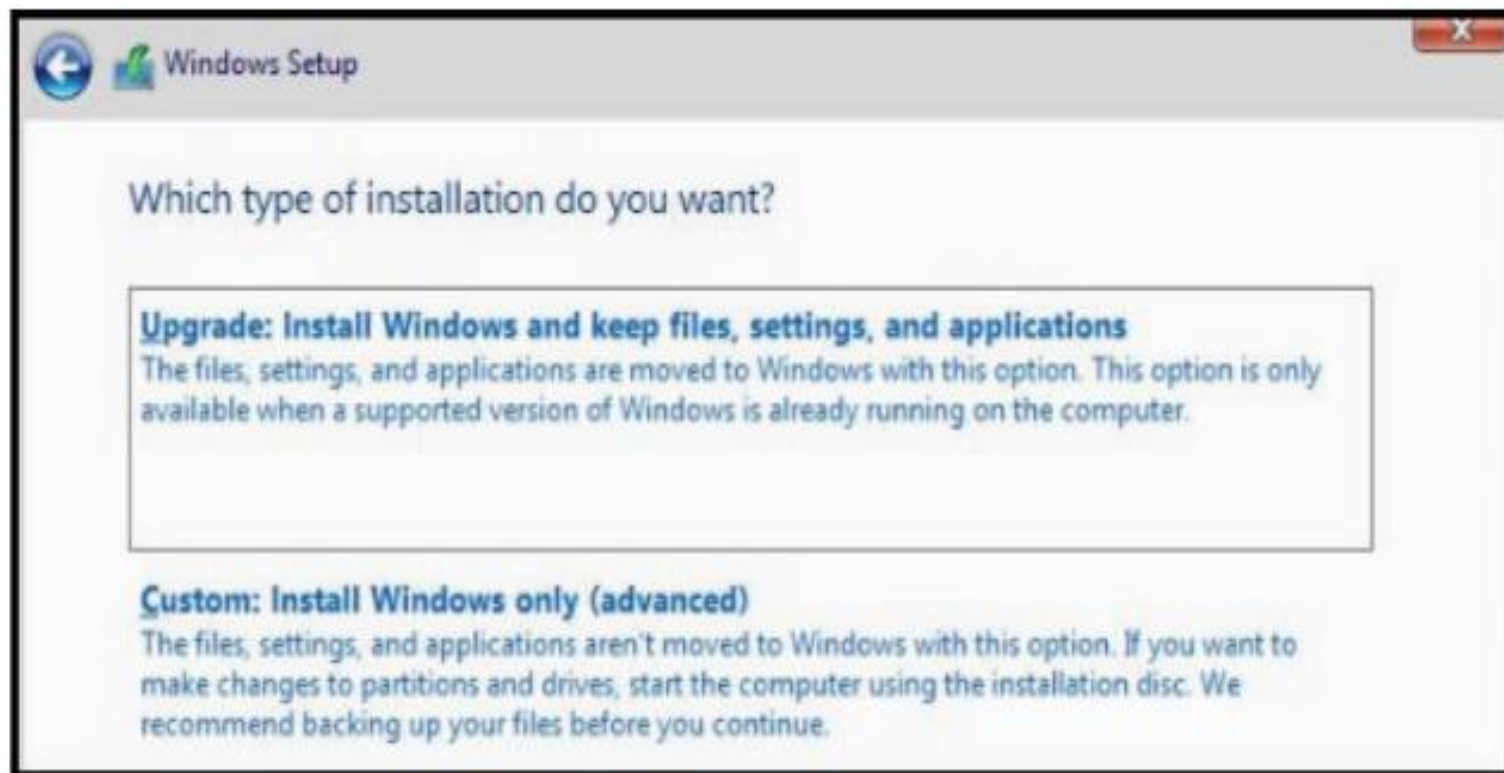
รูปที่ 6.5 หน้าจอข้อตกลงเกี่ยวกับลิขสิทธิ์

2.

ระบบปฏิบัติการ Windows Server 2019

7. หน้าต่างเลือกประเภทการติดตั้งจะปรากฏขึ้นมา Which type of installation do you want?

window, ให้เลือก Custom: Install Windows only (advanced)

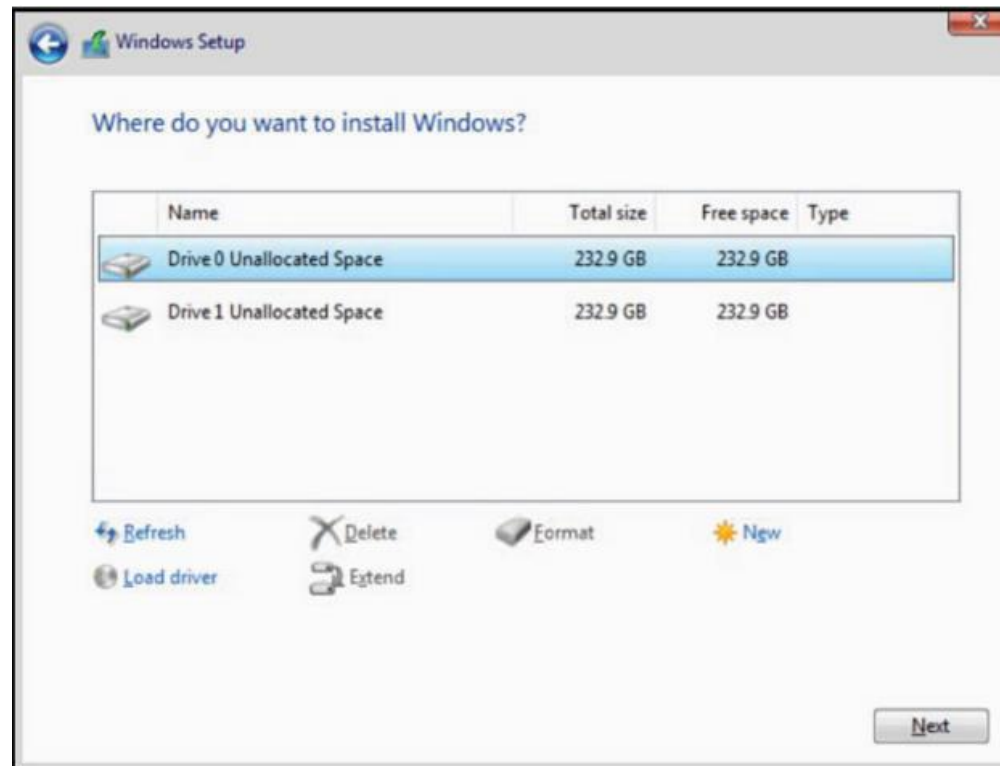


รูปที่ 6.6 หน้าจอการเลือกประเภทการติดตั้ง

2.

ระบบปฏิบัติการ Windows Server 2019

8. เลือกพื้นที่ของ Hard Disk ที่จะติดตั้งระบบปฏิบัติการ โดยเลือกพื้นที่ว่างซึ่งสามารถลบข้อมูลทิ้งได้ หรือใช้ Hard Disk ใหม่



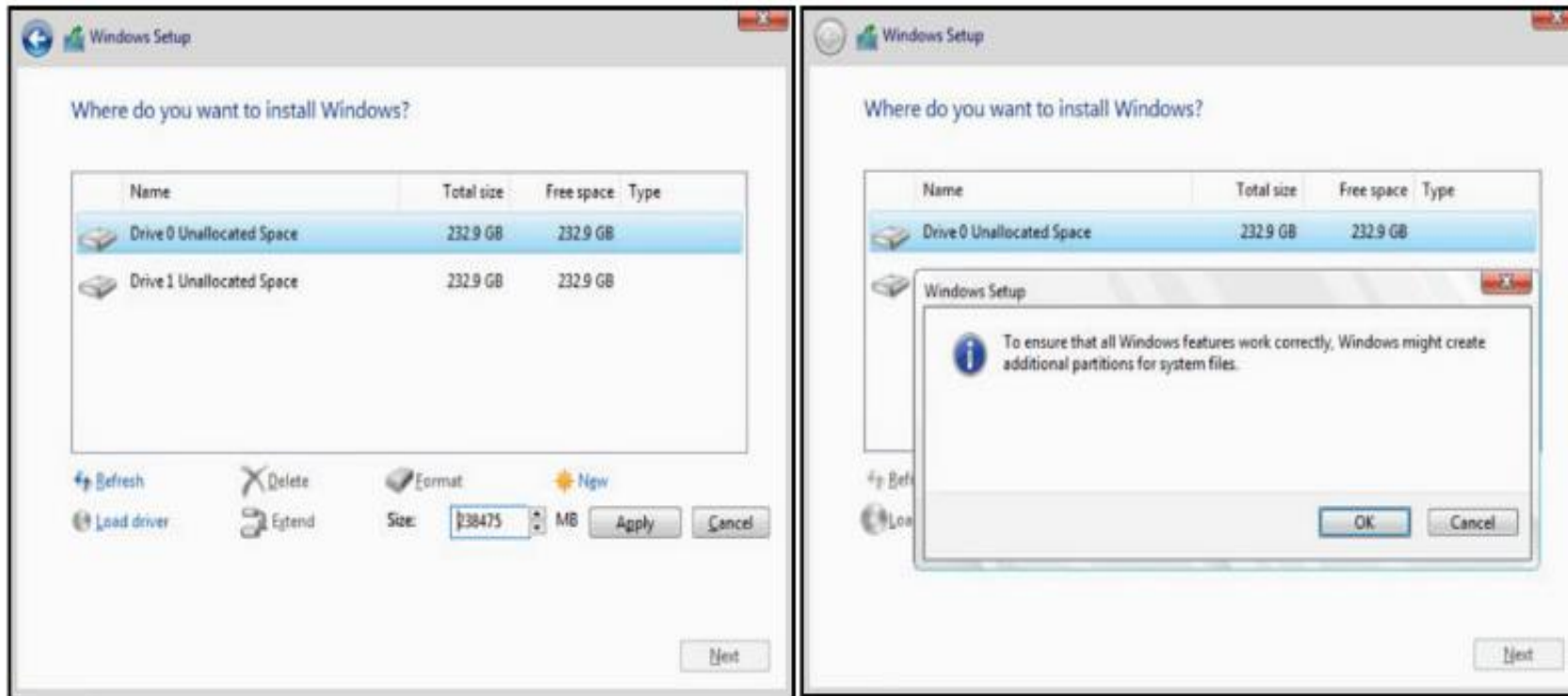
รูปที่ 6.7 หน้าจอการเลือกพื้นที่ของ Hard Disk ที่จะติดตั้งระบบปฏิบัติการ

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2.

ระบบปฏิบัติการ Windows Server 2019

9. กำหนดขนาดของพื้นที่จัดเก็บระบบปฏิบัติการให้เหมาะสม จากนั้น กดปุ่ม Apply แล้วกด OK เพื่อ Format Hard Disk เพื่อเตรียมติดตั้งระบบปฏิบัติการ



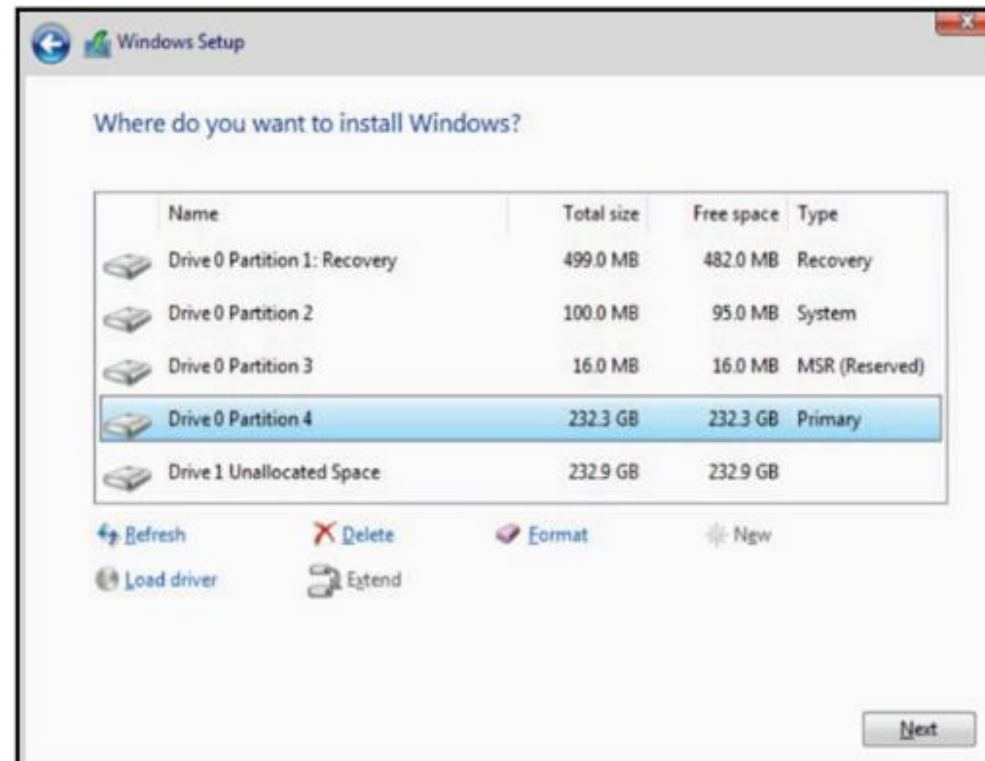
รูปที่ 6.8 หน้าจอการกำหนดขนาดของพื้นที่จัดเก็บระบบปฏิบัติการ

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2.

ระบบปฏิบัติการ Windows Server 2019

10. จากนั้นเลือกพื้นที่ติดตั้งระบบปฏิบัติการและกด Next โปรแกรมจะเริ่มติดตั้งระบบปฏิบัติการหลังการติดตั้งเสร็จ เครื่องจะรีบูตหนึ่งครั้ง

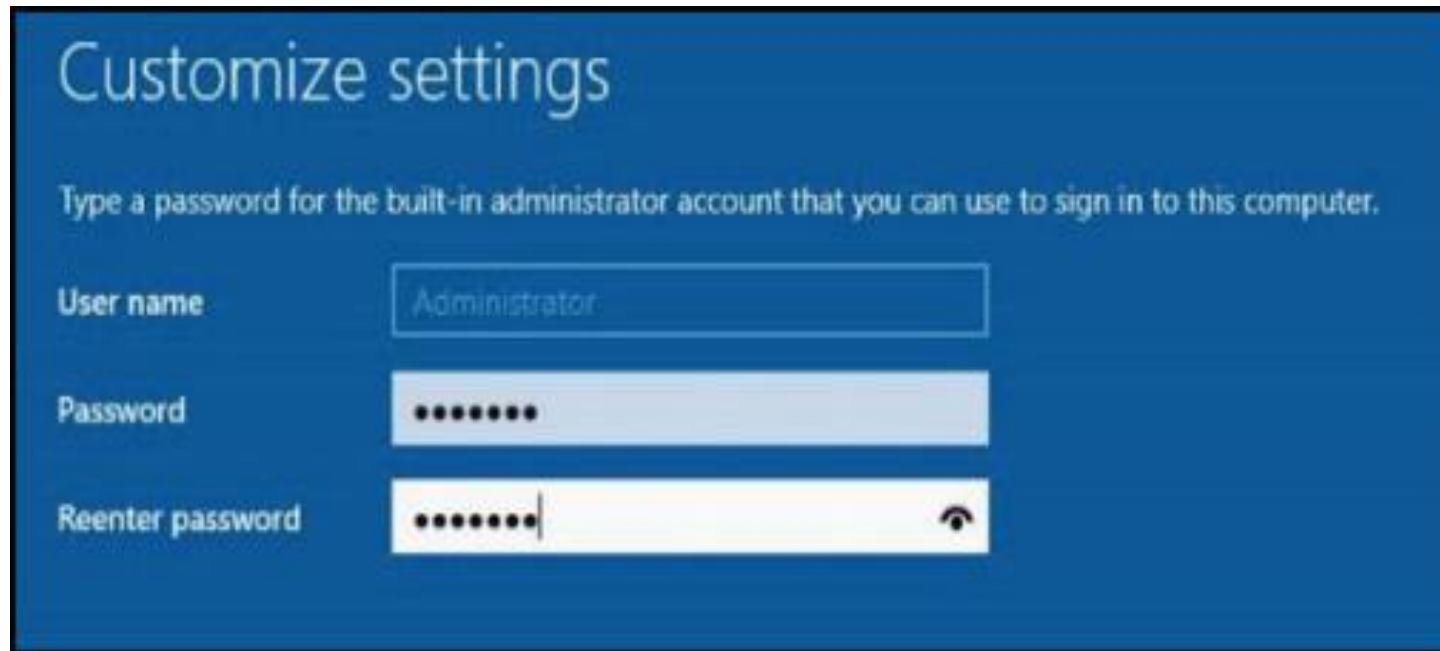


รูปที่ 6.9 หน้าจอการเลือกพื้นที่ติดตั้งระบบปฏิบัติการ

2.

ระบบปฏิบัติการ Windows Server 2019

11. เมื่อติดตั้งระบบปฏิบัติการเสร็จในครั้งแรกและระบบบูตกลับมาแล้ว ให้กดปุ่ม **Ctrl+Alt+Delete** พร้อมกันเพื่อเข้าสู่หน้าจอกำหนดรหัสผ่านสำหรับผู้ดูแลระบบให้พิมพ์รหัสผ่านที่กำหนดไว้ลงไปช่อง **Password** และ **Reenter password** ให้เหมือนกันแล้ว กดปุ่ม **Enter**

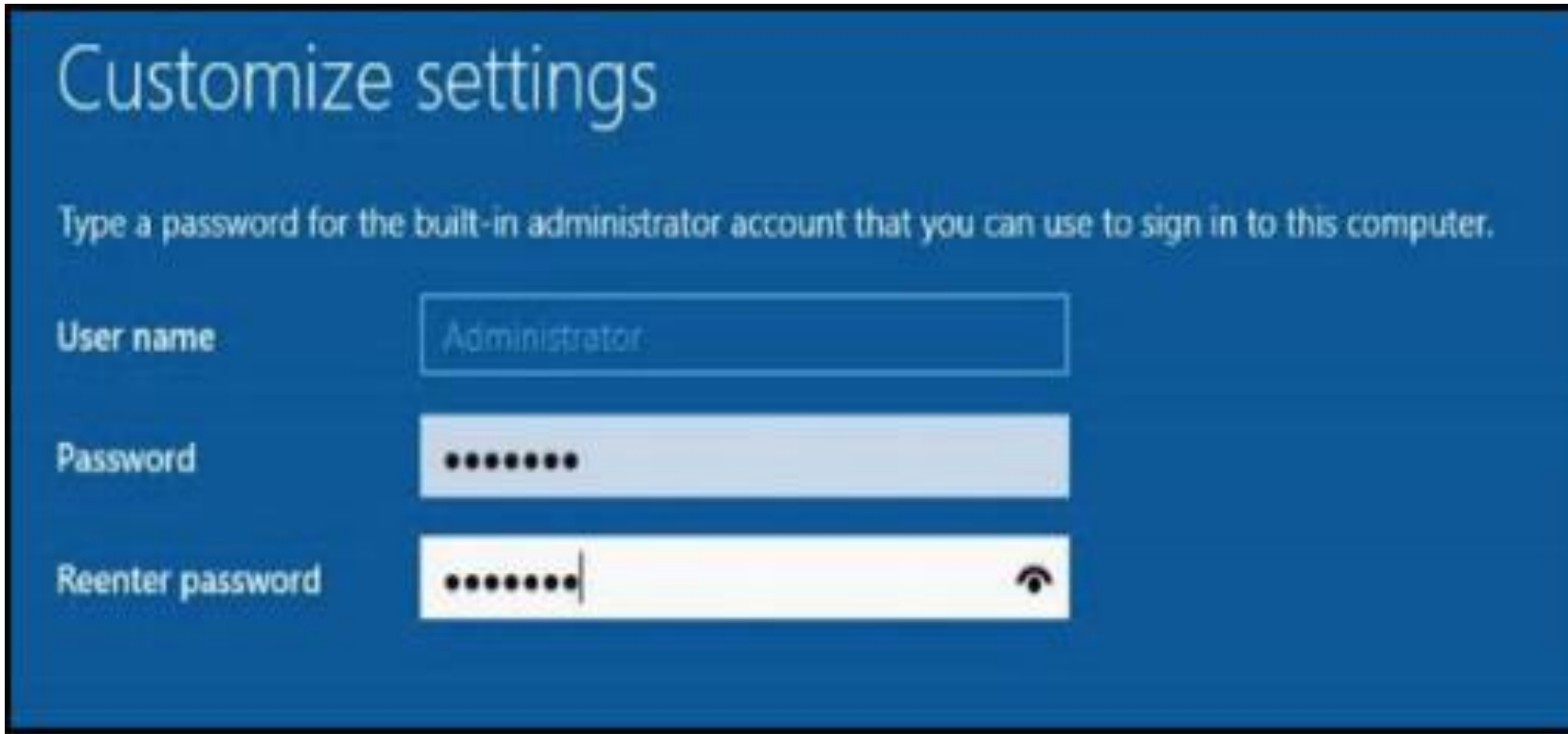


รูปที่ 6.10 หน้าจอกำหนดรหัสผ่านสำหรับผู้ดูแลระบบ

2.

ระบบปฏิบัติการ Windows Server 2019

12. เสร็จสิ้นการติดตั้ง Windows Server 2019



Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name

Password

Reenter password

รูปที่ 6.10 หน้าจอกำหนดรหัสผ่านสำหรับผู้ดูแลระบบ



3. ระบบปฏิบัติการ Windows 10

ระบบปฏิบัติการ Windows 10 เป็นระบบปฏิบัติการที่ใช้สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งพัฒนาโดยบริษัท Microsoft โดยมีชื่อระบบปฏิบัติการแตกต่างกันไปในแต่ละรุ่น เช่น Windows XP, Windows 7, Windows 8, Windows 10 และ Windows 11

Windows 10 สามารถใช้งานได้กับอุปกรณ์ทั้งที่เป็น PC Notebook และ Tablet ที่รองรับระบบปฏิบัติการในมาตรฐาน X86 ทั้งแบบ 32 บิต และ 64 บิต

Windows 10 มีการแยกรุ่นเพื่อให้เหมาะสมต่อการใช้งาน รวมไปถึงให้เหมาะสมกับแต่ละอุปกรณ์การแยกแ่รุ่นดังกล่าวนี้ทำให้ Windows 10 ในแต่ละรุ่นสำหรับแต่ละอุปกรณ์นั้นมีความสามารถแตกต่างกันออกไป ดังนี้

หมายเหตุ

ผู้เรียนสามารถนำหลักการของ Windows 10 ไปประยุกต์ใช้กับ Windows 11 ได้

3. ระบบปฏิบัติการ Windows 10

3.1 Windows 10 Home

Windows 10 Home สำหรับการใช้งานในบ้านทั่วไป หรือสำหรับผู้ทั่วไป Windows 10 Home มีฟีเจอร์หรือความสามารถดังต่อไปนี้

- 🔗 ใช้งานได้กับทั้งคอมพิวเตอร์ PC แท็บเล็ต และอุปกรณ์จำพวก 2-in-1
- 🔗 รองรับการใช้งานผู้ช่วยดิจิทัล Cortana (เฉพาะภาษาอังกฤษ)
- 🔗 มาพร้อมกับเว็บเบราว์เซอร์ Microsoft Edge
- 🔗 ใช้ฟีเจอร์ Continuum tablet mode สำหรับอุปกรณ์ที่รองรับหน้าจอแบบสัมผัสได้
- 🔗 ฟีเจอร์ Windows Hello ที่เป็นฟีเจอร์ทางด้านความมั่นคงปลอดภัยผ่านการจดจำใบหน้า

การสแกนม่านตา และการสแกนลายนิ้วมือ เพื่อใช้ในการ Login เข้าสู่ระบบ (แต่มีข้อจำกัดว่าอุปกรณ์นั้น ๆ ต้องมากับกล่อง ระบบสแกนม่านตา และระบบสแกนลายนิ้วมือที่ Microsoft รองรับด้วย)



3. ระบบปฏิบัติการ Windows 10

รองรับ Universal Windows apps โดยมีแอปพลิเคชันอย่าง Photos, Maps, Mail, Calendar, Music และ Video ให้ใช้งานทันที

มาพร้อมกับแอปพลิเคชันสำหรับการเล่นเกมอย่าง Xbox ที่ให้ผู้ใช้สามารถทำการเล่นเกมได้อย่างต่อเนื่องทั้งจาก Xbox 360 หรือ Xbox One



รูปที่ 6.11 Windows 10 Home

3. ระบบปฏิบัติการ Windows 10

3.2 Windows 10 Pro



Windows 10 Pro สำหรับคอมพิวเตอร์ PC แท็บเล็ต และอุปกรณ์จำพวก 2-in-1 มีความสามารถพื้นฐานเหมือนรุ่น Home แต่เพิ่มความสามารถที่เกี่ยวข้องกับทางด้านธุรกิจ ช่วยให้ผู้ใช้สามารถจัดการควบคุมอุปกรณ์และแอปพลิเคชันต่าง ๆ ได้อย่างมีประสิทธิภาพและประสิทธิผลมากกว่า โดยฟีเจอร์ที่ถูกเพิ่มเข้ามาในรุ่น Pro ได้แก่

- 🔒 ฟีเจอร์สำหรับการป้องกันข้อมูลทางด้านธุรกิจที่สำคัญของผู้ใช้เพิ่มเติม
- 🔒 สนับสนุนการ remote และ mobile productivity scenarios
- 🔒 มาพร้อมกับเทคโนโลยีคลาวด์ขั้นสูงกว่า
- 🔒 สนับสนุนการใช้งานฟีเจอร์ Choose Your Own Device (CYOD) programs และ prosumer customers สำหรับองค์กร

3. ระบบปฏิบัติการ Windows 10



รูปที่ 6.11 Windows 10 Home

3. ระบบปฏิบัติการ Windows 10

3.3 Windows 10 Enterprise



Windows 10 รุ่น Enterprise เป็นเวอร์ชันที่อัปเดตความสามารถและฟีเจอร์ต่าง ๆ สำหรับองค์กรขนาดใหญ่เพิ่มขึ้นมาจาก Windows 10 Pro เพื่อที่จะให้รองรับการใช้งานในระดับองค์กรมากขึ้น สำหรับฟีเจอร์และความสามารถใหม่ ๆ ที่เพิ่มขึ้นมาบน Windows 10 Enterprise ได้แก่

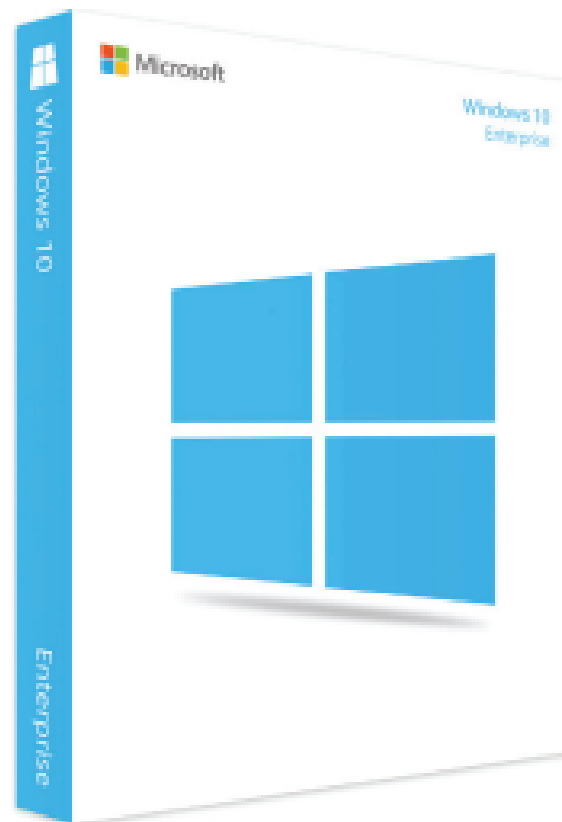
- เพิ่มความสามารถในการป้องกันความมั่นคงปลอดภัยให้กับอุปกรณ์ ตัวตนผู้ใช้งาน แอปพลิเคชัน และข้อมูลสำคัญของบริษัทในระดับสูง

- รองรับลูกค้าแบบ Volume Licensing (ซื้อสิทธิ์การใช้งานแบบเป็นจำนวนได้ตามที่บริษัทหรือองค์กรต้องการ)

- มาพร้อมกับ Windows Update for Business

- ผู้ใช้จะได้รับการเข้าถึงการให้บริการทางด้านต่าง ๆ เช่น ความช่วยเหลือจาก Microsoft อย่างเต็มรูปแบบ

3. ระบบปฏิบัติการ Windows 10



รูปที่ 6.13 Windows 10 Enterprise

3. ระบบปฏิบัติการ Windows 10

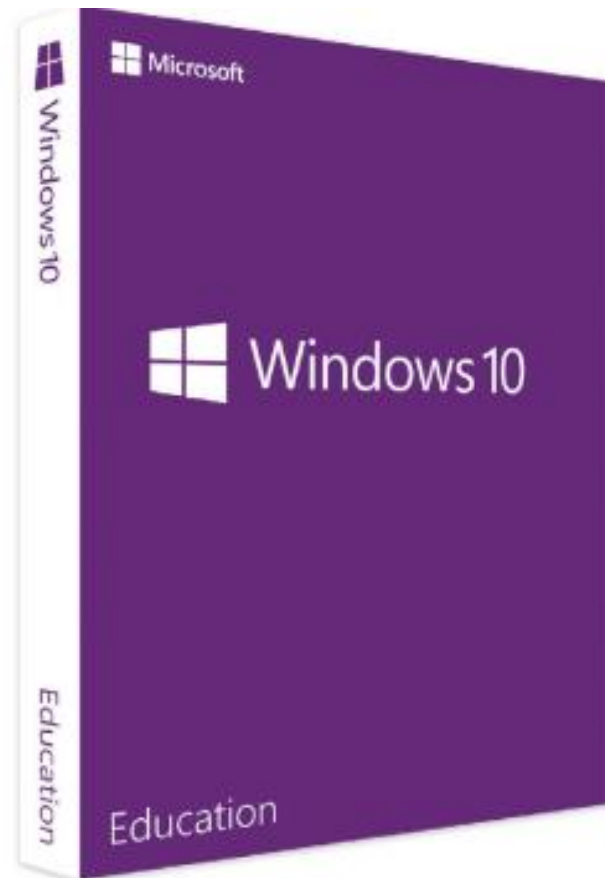
3.4 Windows 10 Education



Windows 10 Education มีคุณสมบัติเหมือน Windows 10 Enterprise แต่จะถูกปรับปรุงให้เหมาะสมกับการใช้งานในโรงเรียน และสถานศึกษา เพื่อให้ตอบสนองกับความต้องการใช้งานทางด้านการเรียนรู้เป็นหลักสำหรับบุคลากร ผู้ดูแลระบบ อาจารย์ และนักเรียนนักศึกษา ทั้งนี้ Windows 10 Education จะถูกใช้งานสำหรับในสถานศึกษาเท่านั้น ส่วนเครื่องของนักเรียนนักศึกษาที่ใช้งานร่วมในระบบด้วยนั้นจะเป็น Windows 10 Home หรือ Pro

Windows 10 Education จำหน่ายในรูปแบบ Academic Volume Licensing เท่านั้น

3. ระบบปฏิบัติการ Windows 10



รูปที่ 6.14 Windows 10 Education

3. ระบบปฏิบัติการ Windows 10

ตารางแสดงคุณลักษณะของ Windows แต่ละรุ่น

Features	Home	Pro	Enterprise	Education
Device Encryption ⁶	✓	✓	✓	✓
Domain Join		✓	✓	✓
Group Policy Management		✓	✓	✓
BitLocker ²		✓	✓	✓
Enterprise Mode Internet Explorer (EMIE)		✓	✓	✓
Assigned Access 8.1		✓	✓	✓
Remote Desktop		✓	✓	✓
Direct Access			✓	✓
Windows To Go Creator			✓	✓
AppLocker			✓	✓
BranchCache			✓	✓

3. ระบบปฏิบัติการ Windows 10

การใช้ซอฟต์แวร์ถูกลิขสิทธิ์เป็นสิ่งจำเป็นสำหรับองค์กร เพราะนอกจากจะเป็นสิ่งที่ถูกกฎหมายแล้วยังเป็นการป้องกันความมั่นคงปลอดภัยของข้อมูลและระบบเครือข่ายจากโปรแกรมไม่พึงประสงค์ด้วยโปรแกรม Windows 10 จะมีโปรแกรมป้องกันไวรัสที่ชื่อ Windows Defender ติดตั้งมาด้วย โดยระบบจะทำการอัปเดตฐานข้อมูลไวรัสและแก้ไขช่องโหว่ในระบบต่าง ๆ ที่ถูกพบโดยอัตโนมัติสำหรับผู้ใช้ที่ใช้โปรแกรมถูกลิขสิทธิ์ และถึงแม้จะมีโปรแกรม Anti-Virus ที่ดีเพียงใดหากพฤติกรรมของผู้ใช้มีความเสี่ยง เช่น การใช้ซอฟต์แวร์เถื่อนซึ่งอาจจะมีการฝังไวรัสมาด้วย ก็จะทำให้ระบบมีช่องโหว่ให้ไวรัสเข้ามาทำลายข้อมูลได้ ดังนั้นการใช้โปรแกรมลิขสิทธิ์จากผู้แทนจำหน่ายที่น่าเชื่อถือจึงเป็นสิ่งจำเป็น



3. ระบบปฏิบัติการ Windows 10

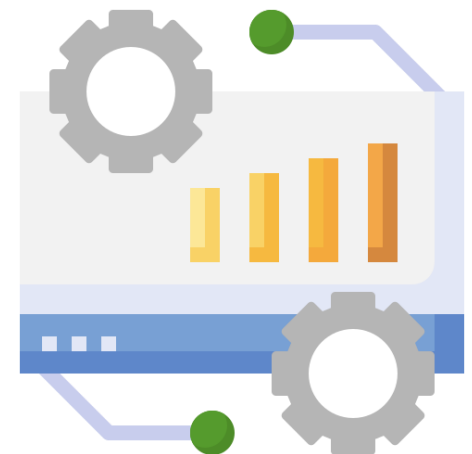
การใช้ระบบปฏิบัติการที่ถูกลิขสิทธิ์ย่อมมีค่าใช้จ่าย จึงจำเป็นต้องเลือกระบบปฏิบัติการที่เหมาะสมกับการทำงาน เพราะหากซื้อระบบปฏิบัติการที่มีความสามารถมากเกินไปก็จะเป็นการสิ้นเปลืองโดยใช่เหตุ แต่หากซื้อระบบปฏิบัติการที่ขาดคุณสมบัติที่เหมาะสมก็อาจจะทำให้การทำงานไม่เต็มประสิทธิภาพเช่นกัน



4. การติดตั้งระบบปฏิบัติการ Windows 10

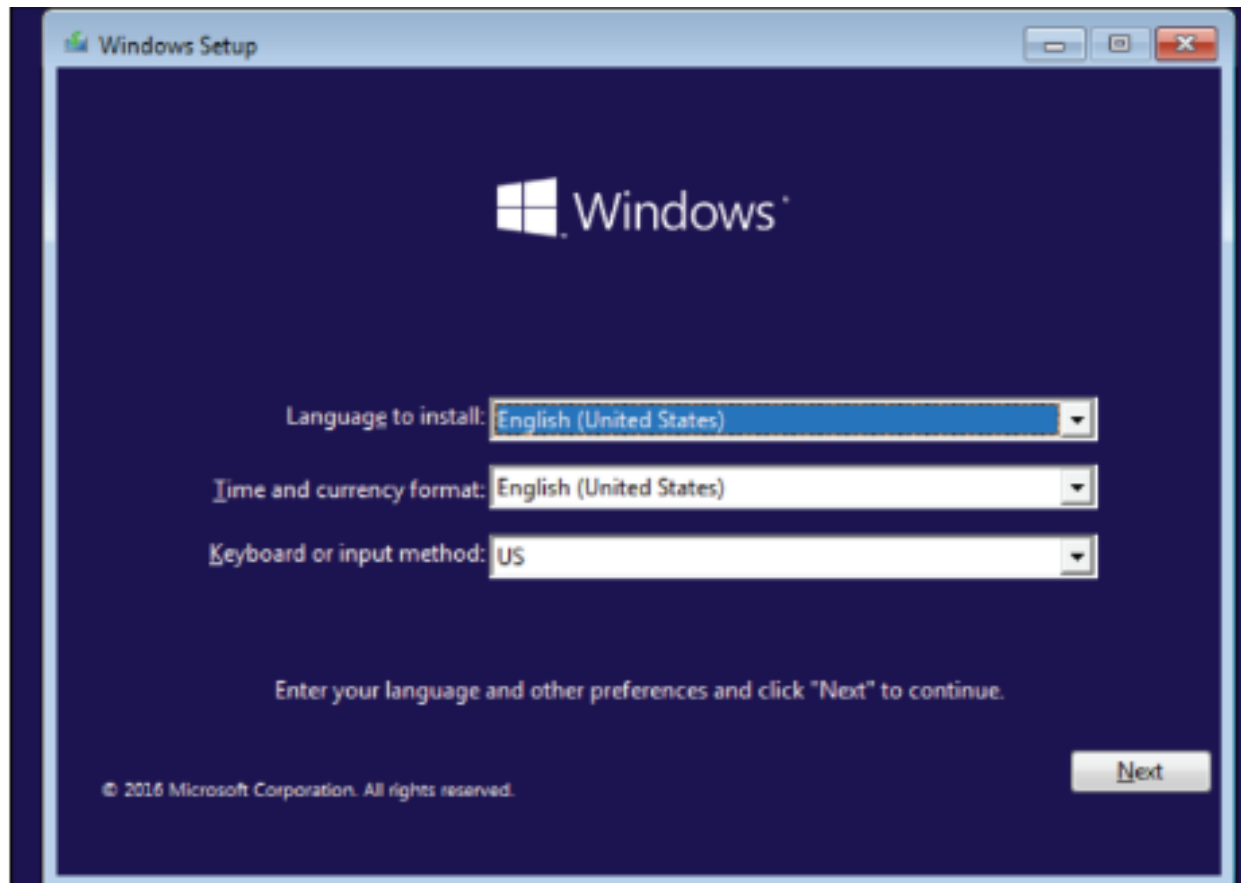
เตรียมการเช่นเดียวกับการติดตั้งระบบปฏิบัติการ Windows Server 2019 จากนั้นทำตามขั้นตอนต่อไปนี้

1. กำหนดให้เครื่องคอมพิวเตอร์บูตจากสื่อที่บรรจุตัวติดตั้งระบบปฏิบัติการ เช่น USB หรือ CD-ROM โดยศึกษาวิธีการกำหนดค่าระบบจากคู่มือประจำเครื่องคอมพิวเตอร์
2. ใส่แผ่น CD หรือ USB ตัวติดตั้งระบบปฏิบัติการ จากนั้นเปิดเครื่องคอมพิวเตอร์ เมื่อคอมพิวเตอร์โหลดโปรแกรมเบื้องต้นหรือบูตระบบแล้วจะปรากฏหน้าจอให้เลือกภาษา ให้เลือกเป็นภาษาอังกฤษ



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

4. การติดตั้งระบบปฏิบัติการ Windows 10



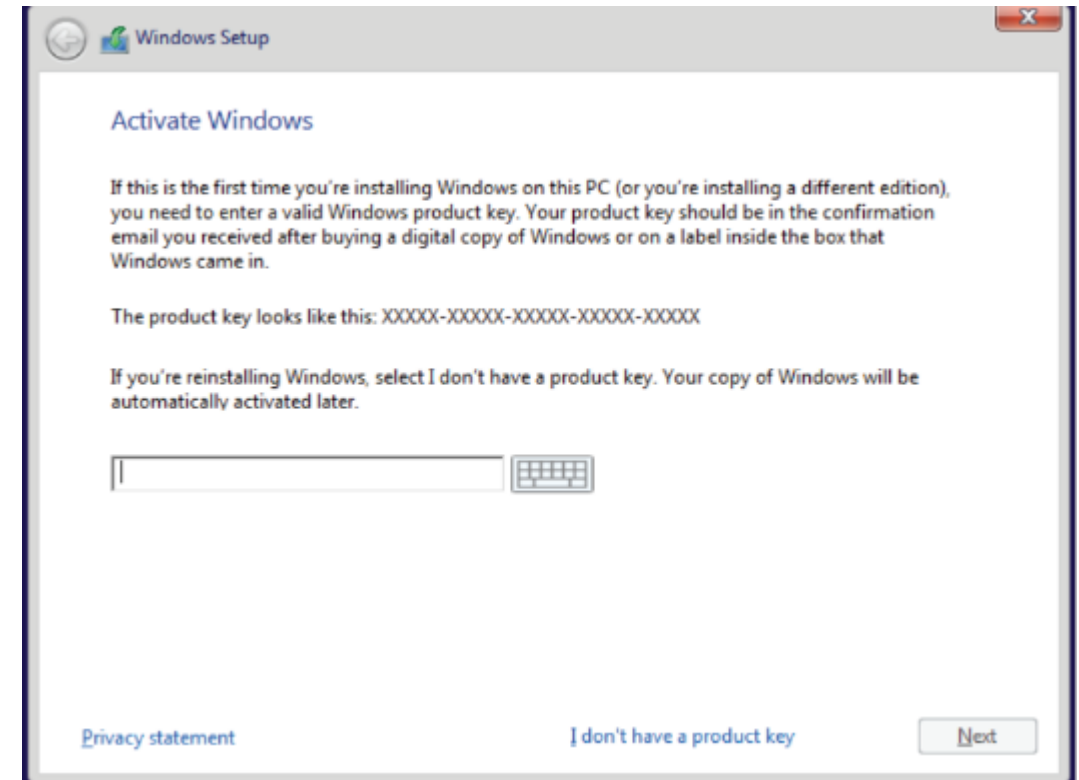
รูปที่ 6.15 เลือกภาษาให้เลือกเป็นภาษาอังกฤษ

4. การติดตั้งระบบปฏิบัติการ Windows 10

3. จากนั้นในการแสดงผลระหว่างติดตั้งตามรูปเลือก
สกุลเงิน และแป้นพิมพ์ จากนั้นให้คลิกที่ Next

4. คลิกเมาส์คลิกที่ Install Now

5. ระบบจะให้ใส่หมายเลขประจำตัวหรือ Product Key ซึ่งจะได้จากผู้จำหน่าย (ส่วนใหญ่จะติดอยู่ที่กล่องผลิตภัณฑ์) หรือส่งมาทางอีเมลกรณีที่ซื้อแบบออนไลน์ ซึ่งในขั้นตอนนี้อาจจะยังไม่ต้องใส่ Product Key ก็ได้ แต่จะยังไม่สามารถใช้ Windows ได้อย่างเต็มประสิทธิภาพ



รูปที่ 6.16 ใส่หมายเลขประจำตัวหรือ Product Key

4. การติดตั้งระบบปฏิบัติการ Windows 10

6. อ่านข้อตกลงเกี่ยวกับลิขสิทธิ์ แล้วเลือก I accept the license terms จากนั้นคลิก Next

7. หน้าต่างเลือกประเภทการติดตั้งจะปรากฏขึ้นมา Which type of installation do you want ? ให้เลือก

Custom: Install Windows only (advanced)

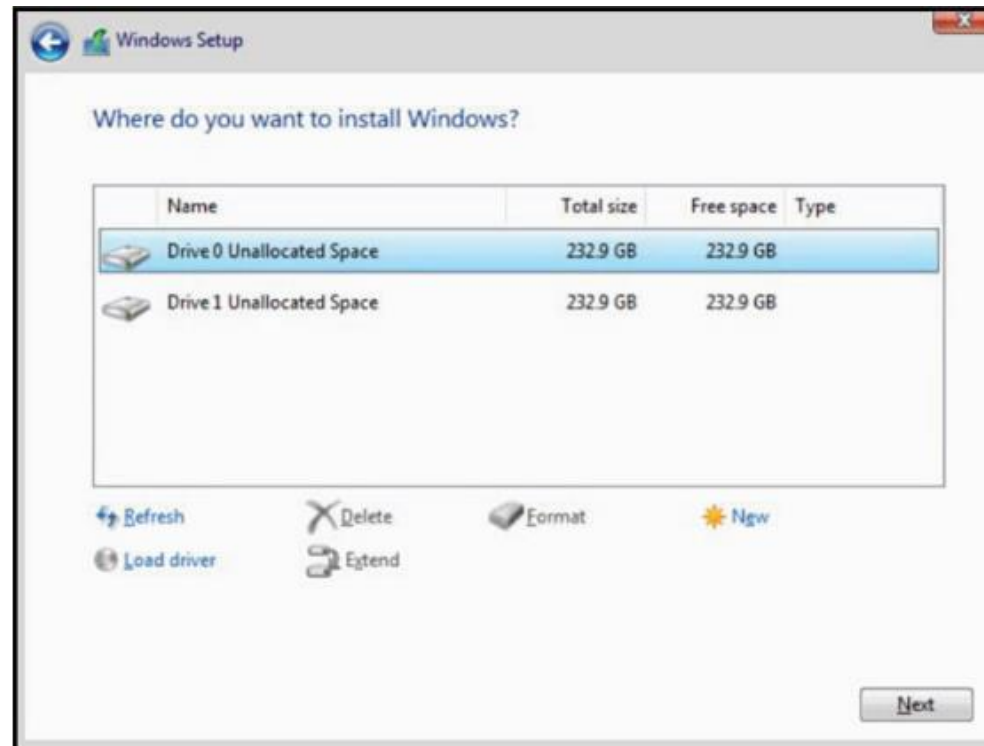


รูปที่ 6.17 เลือก Custom: Install Windows only (advanced)

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

4. การติดตั้งระบบปฏิบัติการ Windows 10

8. เลือกพื้นที่ของ Hard Disk ที่จะติดตั้งระบบปฏิบัติการ โดยเลือกพื้นที่ว่างซึ่งสามารถลบข้อมูลทิ้งได้ หรือใช้ Hard Disk ใหม่

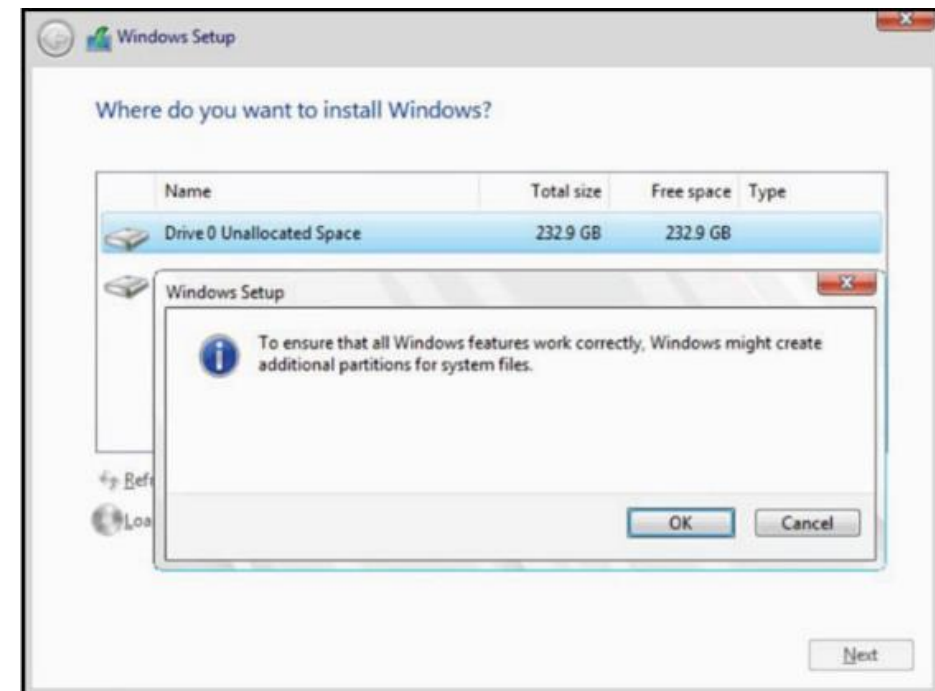
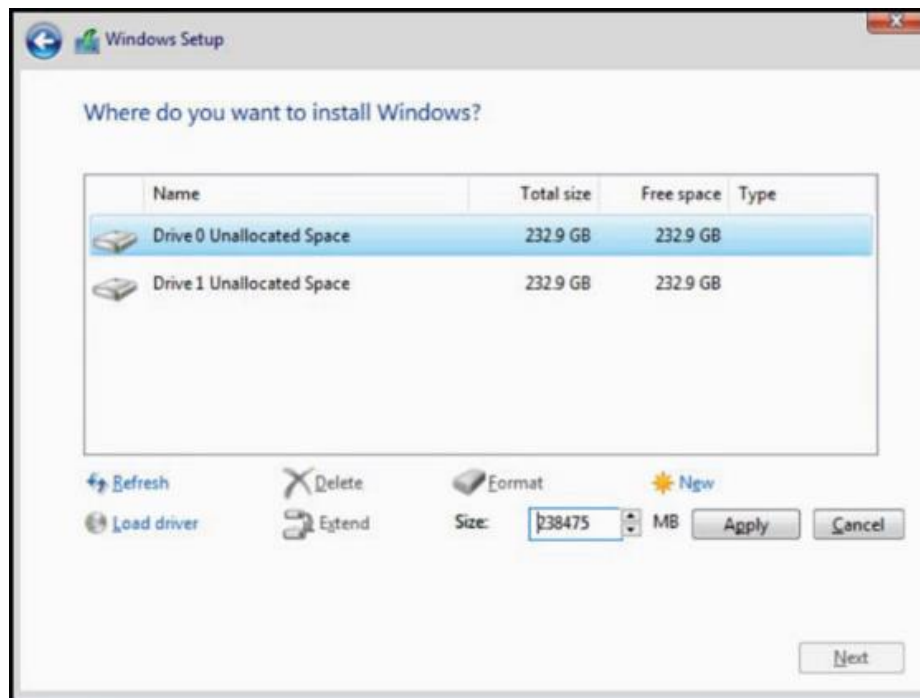


รูปที่ 6.18 เลือกพื้นที่ของ Hard Disk

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

4. การติดตั้งระบบปฏิบัติการ Windows 10

9. กำหนดขนาดของพื้นที่จัดเก็บระบบปฏิบัติการให้เหมาะสม จากนั้นคลิกที่ Apply แล้วกด OK เพื่อ Format Hard Disk และเตรียมติดตั้งระบบปฏิบัติการ

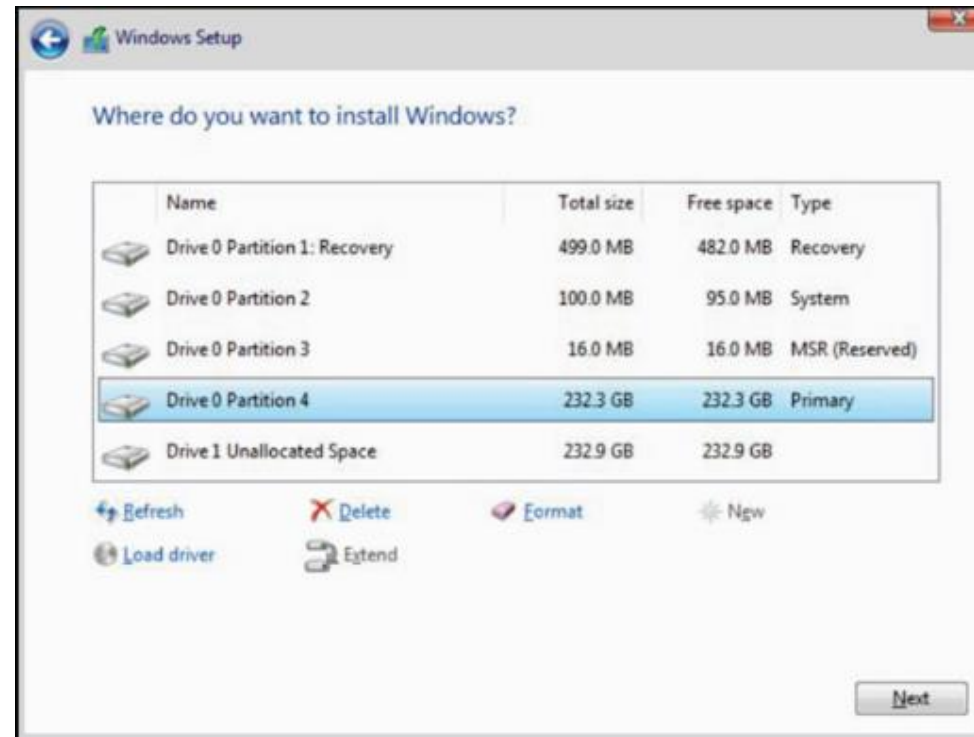


รูปที่ 6.19 การ Format Hard Disk

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

4. การติดตั้งระบบปฏิบัติการ Windows 10

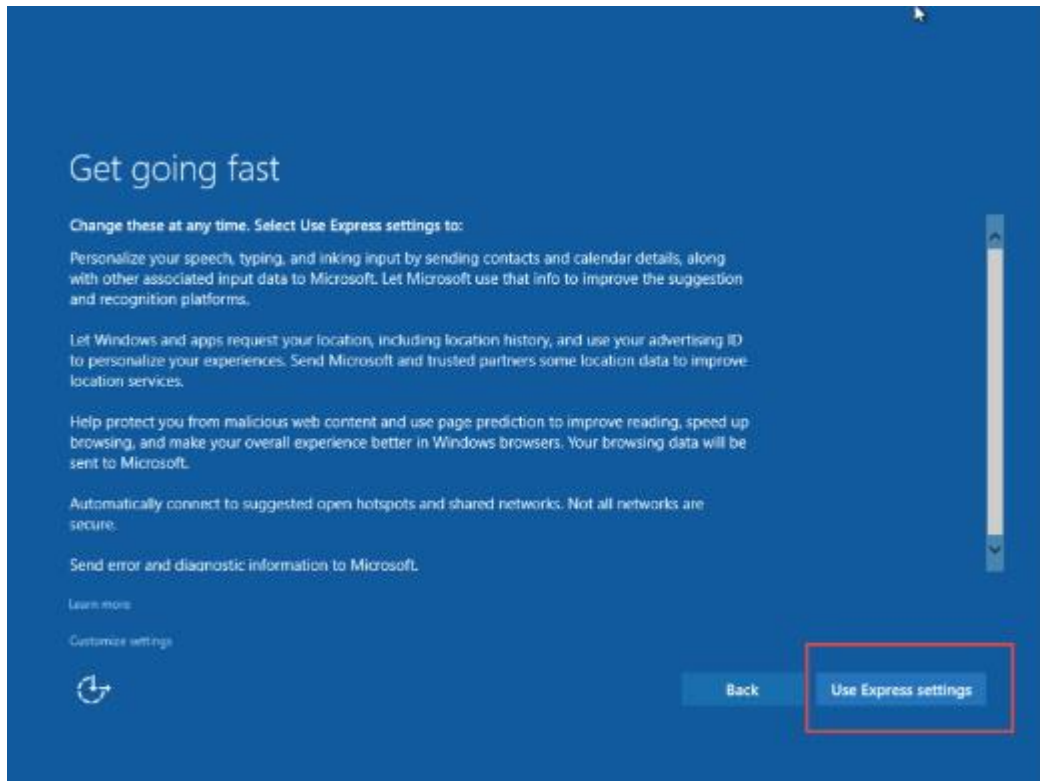
10. จากนั้นเลือกพื้นที่ติดตั้งระบบปฏิบัติการและกด Next โปรแกรมจะเริ่มติดตั้งระบบปฏิบัติการหลังการติดตั้งเสร็จเครื่องจะรีบูตหนึ่งครั้ง



รูปที่ 6.20 เลือกพื้นที่ติดตั้งระบบปฏิบัติการ

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

4. การติดตั้งระบบปฏิบัติการ Windows 10



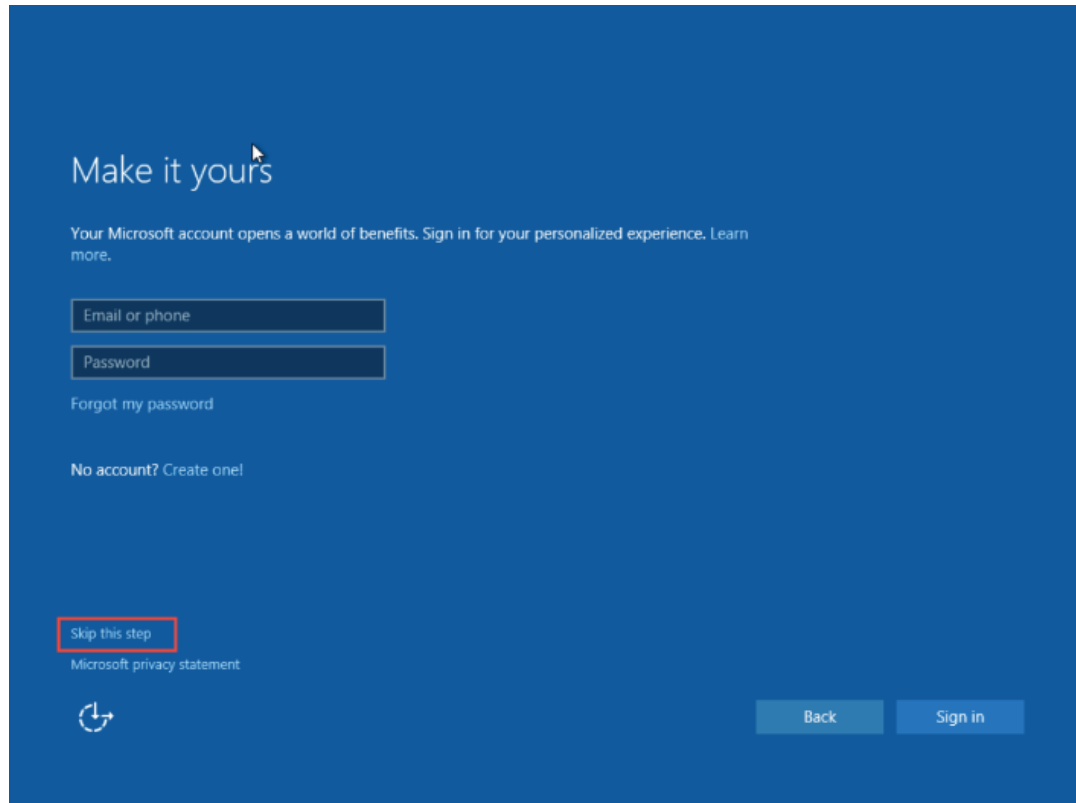
รูปที่ 6.21 เลือก Use Express Settings

11. หลังจากคอมพิวเตอร์ลง Windows 10 เสร็จแล้ว คอมพิวเตอร์จะทำการ Restart ตัวเองอัตโนมัติ และเข้าสู่หน้า Settings ให้ทำการใส่ License Windows 10 หรือ Activate Key ให้ตรงกับ Editions ที่ได้ทำการลง Windows 10 ถ้ายังไม่มี Key ให้กด Do this later

12. ระบบจะให้เลือกวิธีการกำหนดค่าต่าง ๆ ของ การติดตั้ง ให้ทำการเลือก Use Express Settings

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

4. การติดตั้งระบบปฏิบัติการ Windows 10



รูปที่ 6.22 เลือก Skip This Step

13. ถ้าเป็นคอมพิวเตอร์ส่วนตัวทำการเลือก I own it

14. ระบบจะให้เลือกว่าจะ Sign in เข้าสู่ Windows ด้วยวิธีการลงทะเบียนเข้าใช้งานผ่านบัญชี Microsoft Account เช่น การใช้อีเมลที่เป็น Hotmail MSN Outlook เข้าสู่ระบบ

ถ้าไม่ต้องการใช้หรือไม่มี Microsoft Account ให้ข้ามไปเพื่อใช้บัญชีเฉพาะเครื่องที่เรียกว่า Account Local โดยการกด Skip This Step ไปก่อน (Microsoft Account สร้างฟรี)

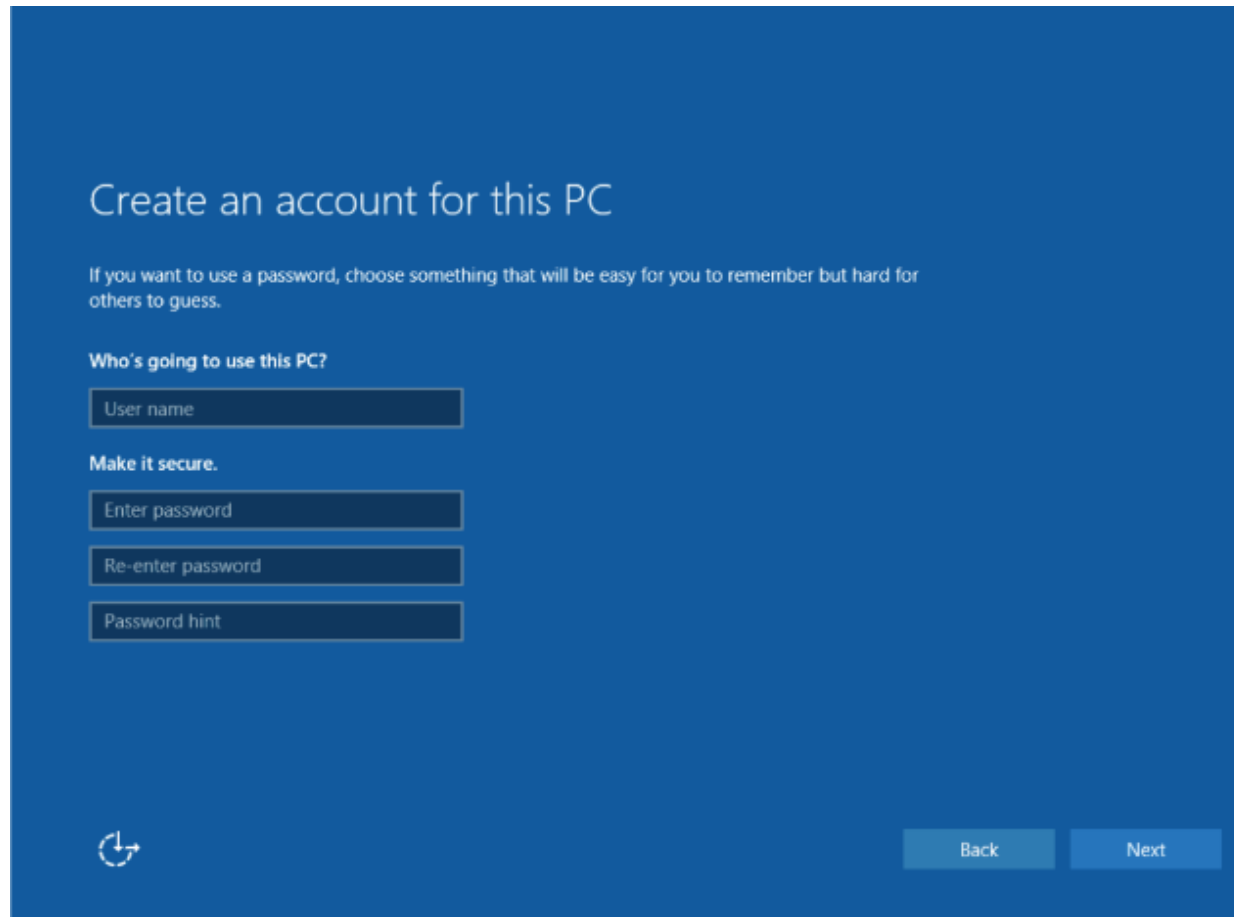
4. การติดตั้งระบบปฏิบัติการ Windows 10

15. ขั้นตอนการสร้าง Account Local

- เลือก Your Account
- User name : ใส่ชื่อที่ต้องการ
- Password : ใส่ Password ที่เราต้องการ
- Re-enter Password : ยืนยัน Password อีกครั้ง
- Password hint : ใส่คำบอกใบ้รหัส Password เพื่อกรณีลืม Password ด้านบน อย่าใส่ Password ตรง ๆ



4. การติดตั้งระบบปฏิบัติการ Windows 10



Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

User name

Make it secure.

Enter password

Re-enter password

Password hint

Back Next

รูปที่ 6.23 ขั้นตอนการสร้าง Account Local

4. การติดตั้งระบบปฏิบัติการ Windows 10

16. สามารถเข้าใช้งาน Windows 10 ได้แล้ว แต่เพื่อให้ประสิทธิภาพการทำงานของระบบสูงสุดผู้ใช้งานต้องติดตั้ง Driver ของอุปกรณ์ เช่น Mainboard, Wireless, LAN, Display Card, Sound Card ให้ครบก่อนเริ่มใช้งานจริง



รูปที่ 6.24 เสร็จสิ้น

5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต



สมาร์ทโฟน แท็บเล็ต เป็นคอมพิวเตอร์ที่ประกอบไปด้วยหน่วยประมวลผล หน่วยความจำ หน่วยจัดเก็บข้อมูล และส่วนแสดงผล เช่นเดียวกับคอมพิวเตอร์ส่วนบุคคลทั่วไป และต้องใช้ระบบปฏิบัติการเช่นเดียวกัน แต่ด้วยสถาปัตยกรรมฮาร์ดแวร์และจุดประสงค์ในการใช้งานทำให้ไม่นิยมที่จะเอาระบบปฏิบัติการของเครื่องคอมพิวเตอร์ส่วนบุคคลมาใช้กับโทรศัพท์มือถือ (มีมือถือ/แท็บเล็ต บางรุ่นใช้ Windows แต่ไม่ประสบความสำเร็จในเชิงการตลาด) ระบบปฏิบัติการที่ใช้ในอุปกรณ์สมาร์ทโฟน แท็บเล็ต ได้แก่ Android, iOS, Windows Phone, BlackBerry, Symbian, webOS, MeeGo, QNX และ Harmony Os เป็นต้น

ในปัจจุบันระบบปฏิบัติการสำหรับสมาร์ทโฟน แท็บเล็ต ที่ได้รับความนิยมจะแบ่งเป็น 2 ระบบคือ Android ที่ถูกใช้กับโทรศัพท์สมาร์ทโฟนหลากหลายยี่ห้อในท้องตลาด และระบบปฏิบัติการ IOS ที่ใช้กับมือถือแท็บเล็ตของบริษัท Apple Computer



5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

5.1 ระบบปฏิบัติการ Android



แอนดรอยด์ (Android) คือ ระบบปฏิบัติการแบบเปิดเผยซอร์สแวร์ต้นฉบับ (Open Source) โดยบริษัท กูเกิล (Google Inc.) แอนดรอยด์เป็นระบบปฏิบัติการระบบเปิดจึงทำให้ได้รับความนิยมเป็นอย่างสูง และมีอุปกรณ์ที่ใชระบบปฏิบัติการแอนดรอยด์จำนวนมาก หลากหลายระดับ หลายราคา รวมทั้งสามารถทำงานบนอุปกรณ์ที่มีขนาดหน้าจอ และความละเอียดแตกต่างกันทำให้ผู้บริโภคสามารถเลือกได้ตามต้องการ

รูปที่ 6.25 สัญลักษณ์
ระบบปฏิบัติการ Android

5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต



ระบบปฏิบัติการแอนดรอยด์ถูกพัฒนาโดยบริษัท แอนดรอยด์ (Android Inc.) เมื่อ พ.ศ. 2546 โดย แอนดี้ รูบิน (Andy Rubin) ผู้ให้กำเนิดระบบปฏิบัติการนี้ ต่อมาบริษัท กูเกิล ได้ซื้อกิจการบริษัท แอนดรอยด์ เมื่อเดือนสิงหาคม พ.ศ. 2548 โดยบริษัทแอนดรอยด์ได้กลายมาเป็นบริษัทลูกของบริษัทกูเกิล

ระบบปฏิบัติการแอนดรอยด์เป็นระบบปฏิบัติการที่พัฒนามาจากระบบปฏิบัติการลินุกซ์ (Linux Kernel) ซึ่งเป็นระบบปฏิบัติการที่ออกแบบมาเพื่อทำงานเป็นเครื่องแม่ข่าย (Server) เพื่อให้กลายเป็นระบบปฏิบัติการบนอุปกรณ์พกพา (Mobile Operating System)



5.

ระบบปฏิบัติการสำหรับสมาร์ตโฟนและแท็บเล็ต



ข้อดีของอุปกรณ์ที่ใช้ระบบปฏิบัติการแอนดรอยด์ คือ การที่เป็นระบบเปิด มีนักพัฒนาเป็นจำนวนมากที่ร่วมกันพัฒนาแอปพลิเคชันสำหรับใช้งานในระบบ และตัวอุปกรณ์แอนดรอยด์เองสามารถเชื่อมต่ออุปกรณ์อื่น ๆ เช่น เครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อส่งถ่ายข้อมูลได้ง่าย การเพิ่มพื้นที่จัดเก็บ ข้อมูลด้วย memory card (ปัจจุบันไม่นิยมในเครื่องราคาแพง เพราะทำให้ประสิทธิภาพของเครื่องด้อยลง) นอกจากนี้ ยังมีอุปกรณ์ให้เลือกในท้องตลาดในหลายแบบหลายราคาอีกด้วย





5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

ข้อเสียของอุปกรณ์ที่ใช้ระบบปฏิบัติการแอนดรอยด์ คือ เนื่องจากเป็นระบบเปิดทำให้การพัฒนาแอปพลิเคชันทำได้ไม่ยากและการควบคุมมาตรฐานทำได้ยาก ทำให้แอปพลิเคชันใน Play Store ของ Android มีแอปพลิเคชันบางส่วนที่ด้อยคุณภาพ ในบางกรณีอาจจะพบความพยายามในการแฝงโฆษณาหรือขโมยข้อมูลลูกค้า ทำให้ผู้ใช้ต้องใช้ความระมัดระวังในการเลือกใช้แอปพลิเคชันของแอนดรอยด์ในแง่ผู้พัฒนาเนื่องจากอุปกรณ์ที่ใช้ระบบปฏิบัติการแอนดรอยด์มีหลากหลายแบบ ทั้งขนาดหน้าจอและสเปกเครื่อง (Specification) ทำให้นักพัฒนาระบบต้องตรวจสอบโปรแกรมเพิ่มมากขึ้น



5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

5.2 ระบบปฏิบัติการ iOS

ระบบปฏิบัติการไอโอเอส (iOS) มีชื่อเดิมว่า iPhone OS เริ่มต้นด้วยการเปิดตัวของ iPhone เมื่อวันที่ 29 มิถุนายน พ.ศ. 2550 เป็นระบบปฏิบัติการสำหรับสมาร์ทโฟนของแอปเปิล ต่อมาได้ถูกนำมาใช้ในอุปกรณ์อื่น ได้แก่ iPod และ iPad (ปัจจุบัน iPad ใช้ระบบปฏิบัติการ iPad OS) ซึ่งผลิตและจำหน่ายโดยบริษัท Apple Computer เท่านั้น



รูปที่ 6.26 สัญลักษณ์ระบบปฏิบัติการ iOS

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

ข้อดี

ข้อดีของ iOS การที่เป็นระบบปฏิบัติการระบบปิดที่ใช้กับอุปกรณ์เฉพาะทำให้การพัฒนาแอปพลิเคชันสามารถควบคุมคุณภาพได้ดี ทั้งในแง่ของประสิทธิภาพการทำงานและคุณภาพการใช้งาน

ข้อเสีย

ข้อเสียของ iOS เนื่องจากเป็นระบบเฉพาะทำให้อุปกรณ์ของแอปเปิล (บริษัท Apple) ควบคุมขอบเขตการทำงานของระบบปฏิบัติการ เช่น การเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลกับเครื่องคอมพิวเตอร์ที่ต้องกระทำผ่านโปรแกรม iTunes และไม่สามารถเพิ่มขนาดของพื้นที่จัดเก็บได้ โดยจะถูกกำหนดตั้งแต่วันที่ซื้อครั้งแรก อย่างไรก็ตาม ด้วยการพัฒนาประสิทธิภาพของระบบเครือข่ายการเชื่อมต่อทำให้ปัจจุบันมีการทดแทนขนาดของพื้นที่จัดเก็บและการแลกเปลี่ยนข้อมูลให้สามารถกระทำผ่านระบบไร้สาย Cloud Service ต่าง ๆ เช่น iCloud Dropbox Google Drive ได้

5. ระบบปฏิบัติการสำหรับสมาร์ตโฟนและแท็บเล็ต

5.3 ระบบปฏิบัติการ Linux

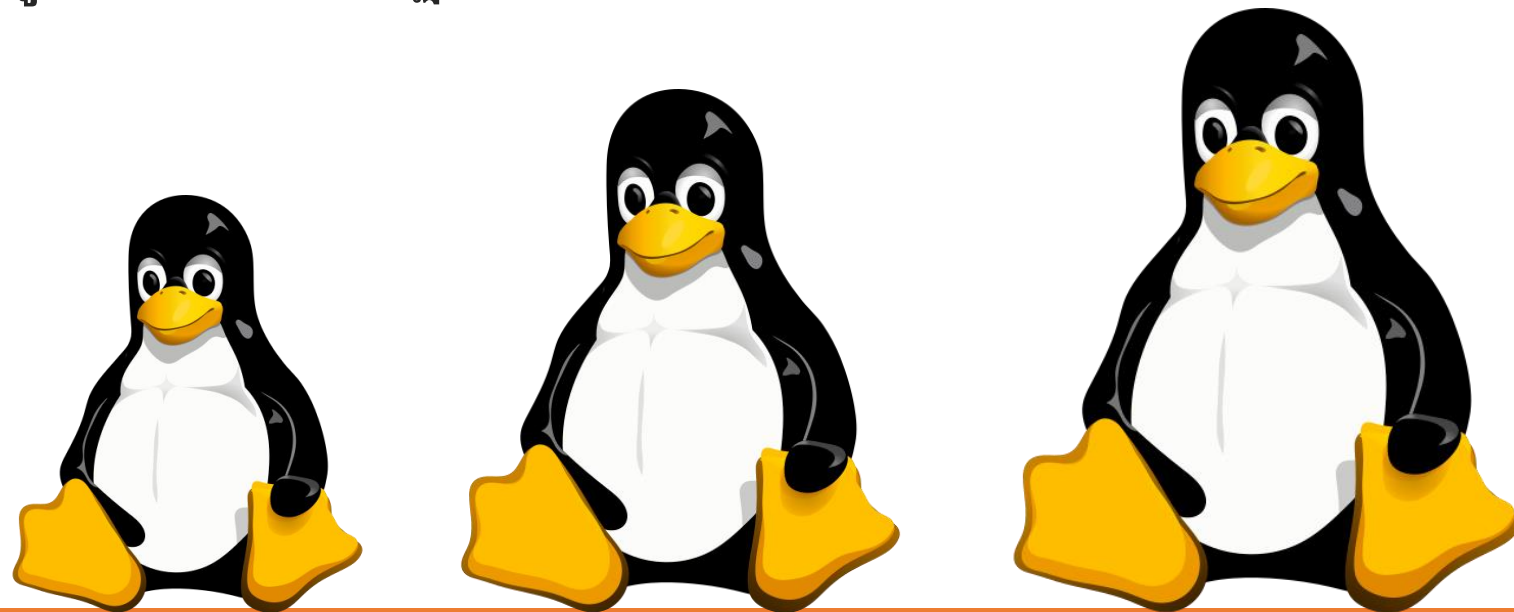
เริ่มพัฒนาโดยชาวฟินแลนด์ ชื่อ ลินุส โตร์วัลดส์ (Linus Torvalds) เมื่อยังเป็นนักศึกษาคอมพิวเตอร์
ที่มหาวิทยาลัยเฮลซิงกิ



รูปที่ 6.27 สัญลักษณ์ระบบปฏิบัติการ Linux

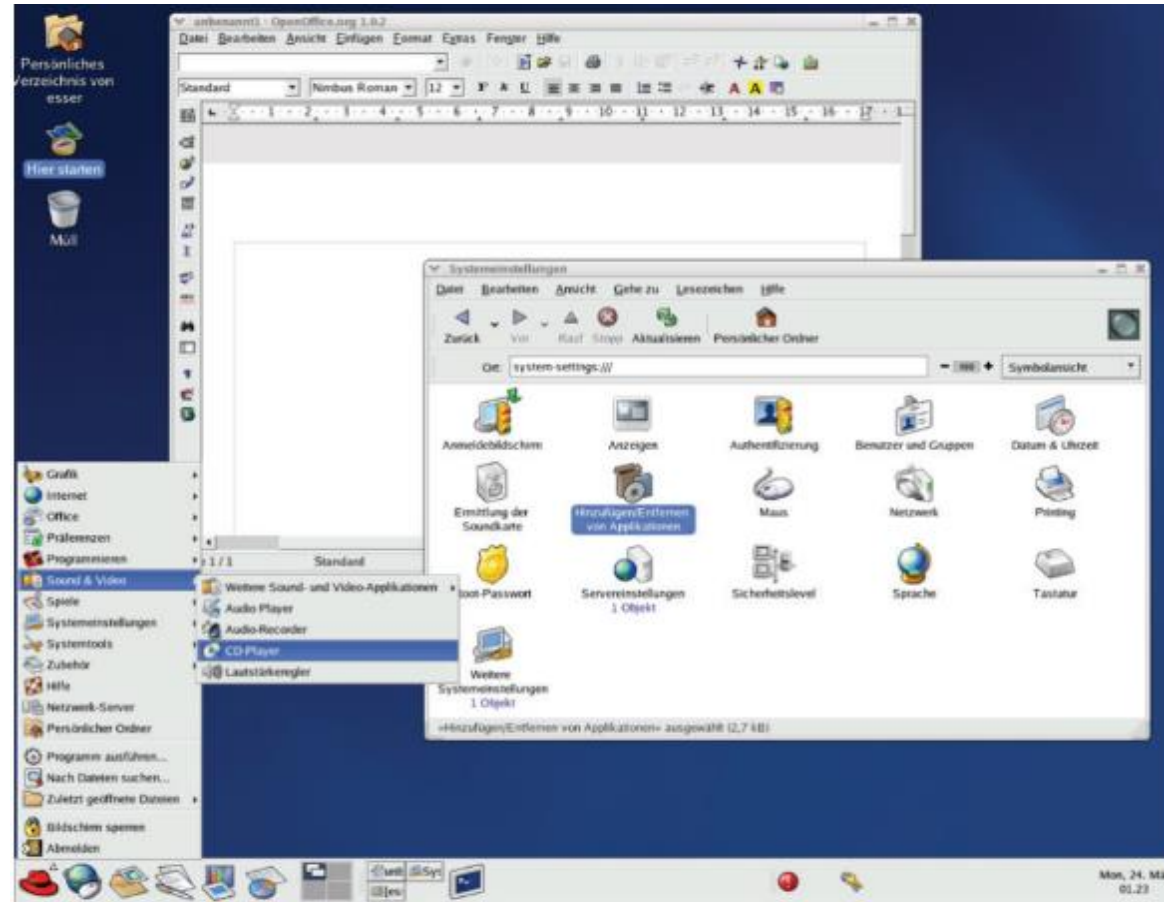
5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

ระบบปฏิบัติการ Linux สามารถใช้งานกับอุปกรณ์คอมพิวเตอร์ได้หลากหลายชนิด ทั้งนำมาทำเป็นเครื่องแม่ข่าย เครื่องลูกข่าย โน้ตบุ๊ก แท็บเล็ต โดยมีแอปพลิเคชันสำหรับใช้งานครอบคลุมการทำงานในองค์กร เหมือนกับระบบปฏิบัติการอื่น และใช้ทรัพยากรระบบหรือสเปกเครื่องที่ต่ำกว่าระบบปฏิบัติการ Windows อย่างเห็นได้ชัด ทั้งระบบปฏิบัติการสำหรับเครื่องลูกข่าย และระบบปฏิบัติการสำหรับเครื่องแม่ข่าย



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

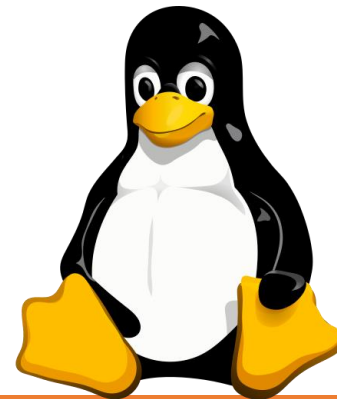
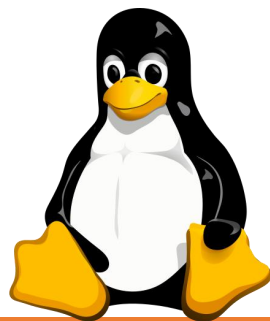


รูปที่ 6.28 ภาพส่วนติดต่อผู้ใช้ของ Linux Red Hat

5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

เนื่องจากระบบปฏิบัติการ Linux เป็นระบบปฏิบัติการระบบเปิดที่มีผู้ร่วมนำไปพัฒนาหลากหลาย ทำให้มีส่วนประกอบต่าง ๆ แยกออกจากกัน ทั้งโปรแกรมรรถประโยชน์หรือเรียกว่า โปรแกรมยูทิลิตี้ (Utility program) ที่ช่วยให้ผู้ใช้สามารถทำงานได้สะดวกขึ้นและแอปพลิเคชันสำหรับทำงานในองค์กร ทำให้ผู้ใช้ประสบปัญหาในการนำองค์ประกอบเหล่านี้มาใช้งาน จึงเกิดมีผู้ให้บริการรวบรวมโปรแกรมเหล่านี้เข้าด้วยกันที่เรียกว่า Distributions เช่น Red Hat, Mandrake, Slackware หรือของไทย เช่น TLE Distributions จะเก็บค่าบริการจากการให้คำปรึกษาหรือแก้ไขปัญหาที่เกิดขึ้นกับการใช้งานระบบ Open Source แต่ไม่ได้เก็บค่าลิขสิทธิ์การใช้งานซอฟต์แวร์



5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

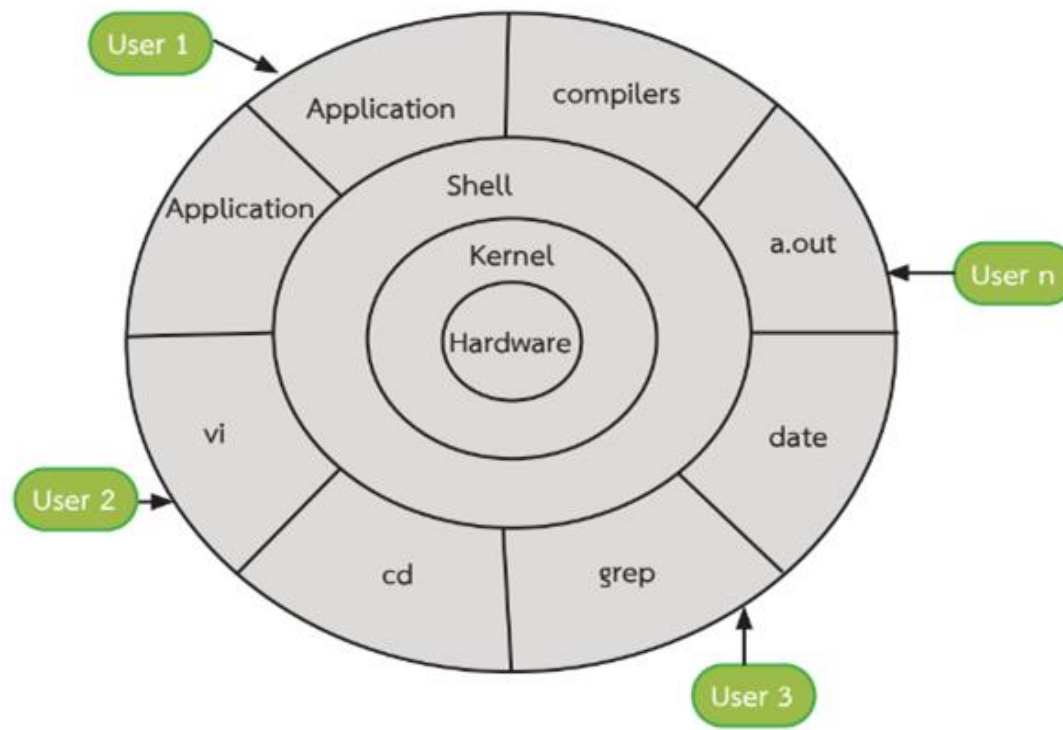


รูปที่ 6.29 ภาพสัญลักษณ์ของ Linux Distributions ต่าง ๆ

5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

1. โครงสร้างของลินุกซ์



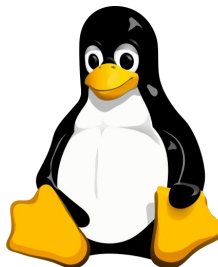
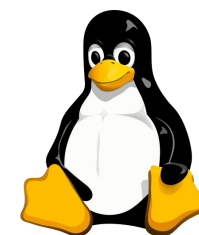
รูปที่ 6.30 โครงสร้างของระบบปฏิบัติการ Linux

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

สามารถแบ่งออกได้ดังนี้

1.1 ฮาร์ดแวร์ (Hardware) คือ อุปกรณ์ต่าง ๆ ที่เรามองเห็นและประกอบขึ้นเป็นคอมพิวเตอร์ทั้งส่วนประกอบภายในและภายนอก เช่น CPU แรม ฮาร์ดดิสก์ การ์ดจอ อุปกรณ์ต่อเสริมต่าง ๆ เป็นต้น

1.2 เคอร์เนล (Kernel) เป็นส่วนประกอบที่สำคัญของระบบ มีหน้าที่ควบคุมการทำงานทั้งหมดของระบบตั้งแต่การจัดสรรทรัพยากรของระบบบริการ โพรเซสงาน (Process) การจัดการไฟล์และอุปกรณ์ อินพุต เอาต์พุต และบริหารหน่วยความจำ เคอร์เนลจะควบคุมอุปกรณ์ฮาร์ดแวร์ของเครื่องทั้งหมดจึงขึ้นอยู่กับฮาร์ดแวร์ ถ้าเปลี่ยนฮาร์ดแวร์รุ่นใหม่ เคอร์เนลจะต้องเปลี่ยนด้วย ภายในเคอร์เนลประกอบไปด้วยโมดูล (Module) ต่าง ๆ ซึ่งอาจเรียกโมดูลว่า ไดรเวอร์ (Driver) มีหน้าที่เป็นตัวกลางในการติดต่อกันระหว่างแอปพลิเคชัน หรือระบบปฏิบัติการกับอุปกรณ์ฮาร์ดแวร์ทั้งหมด



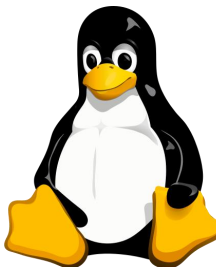
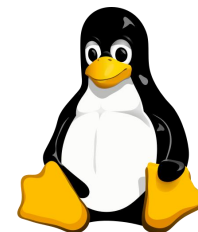
5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

1.3 เชลล์ (Shell) ทำหน้าที่ติดต่อระหว่างผู้ใช้กับเคอร์เนล โดยรับคำสั่งจากผู้ใช้ทางอุปกรณ์อินพุต เช่น คีย์บอร์ด เมาส์ และส่งให้เคอร์เนล ของระบบปฏิบัติการเป็นตัวแปลคำสั่ง (Command interpreter) ทำการแปลให้เป็นภาษาที่เครื่องเข้าใจ นอกจากนี้ เชลล์ยังควบคุมและกำหนดทิศทางของอินพุตและเอาต์พุตว่าจะให้เข้าหรือออกมาทางใด เช่น กำหนดให้เอาต์พุตออกทางหน้าจอ หรือเก็บลงในไฟล์

เชลล์แบ่งออกเป็น 2 ประเภท ดังนี้

1. Command line ผู้ใช้จะติดต่อไปยังเคอร์เนลผ่านทางอินเทอร์เฟซแบบคำสั่ง (Command Line Interface : CLI)

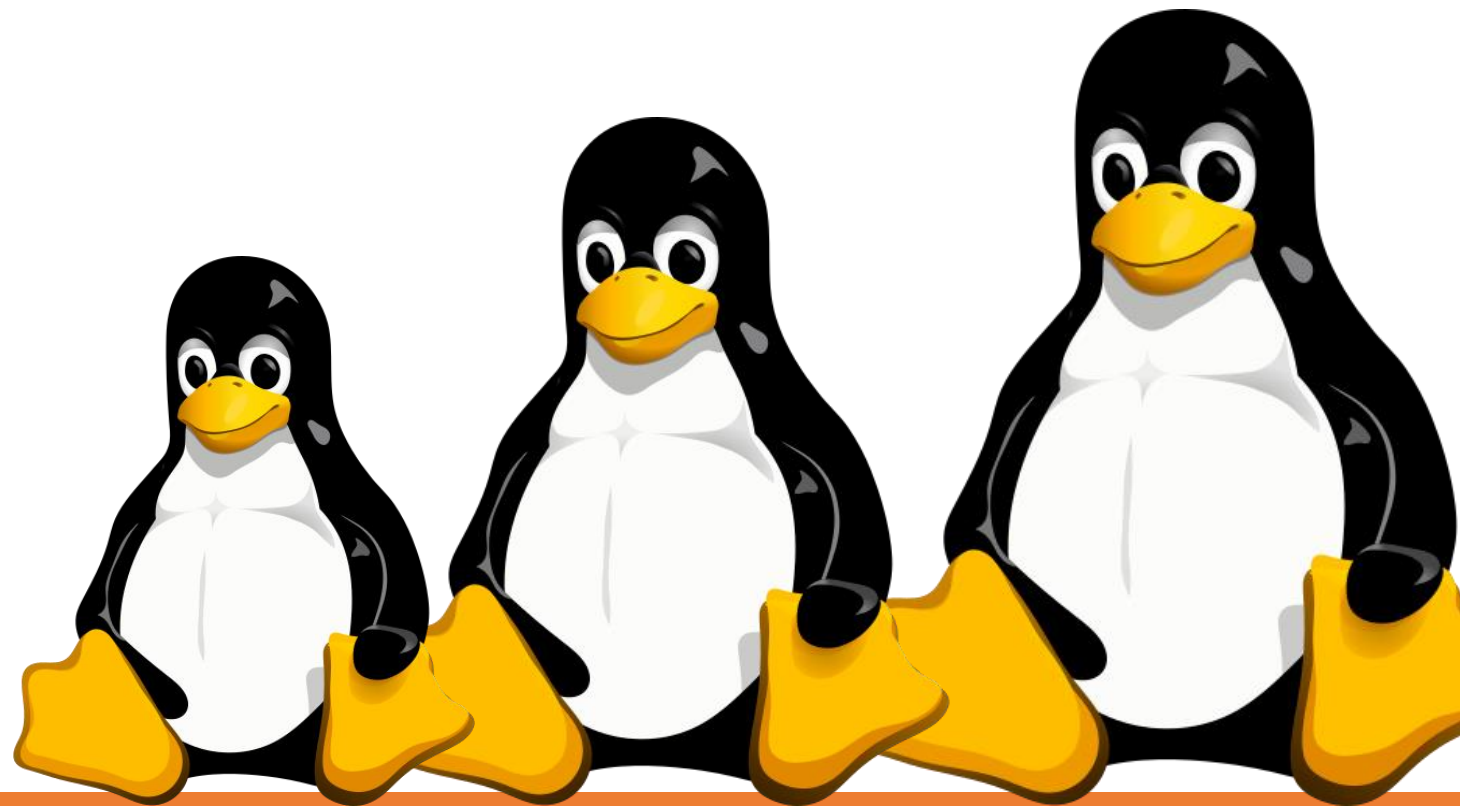
2. Graphic ผู้ใช้ติดต่อผ่านอินเทอร์เฟซแบบกราฟิก (Graphical User Interface : GUI)



5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

1.4 โปรแกรมประยุกต์ (Application) คือ โปรแกรมเพื่อใช้ในงานต่าง ๆ บนลินุกซ์ เช่น สำหรับงานเอกสาร งานกราฟิก เป็นต้น โปรแกรมประยุกต์เหล่านี้มีการพัฒนาร่วมกันโดยนักพัฒนาทั่วโลกและเผยแพร่ให้ดาวน์โหลดไปใช้งานได้ฟรี



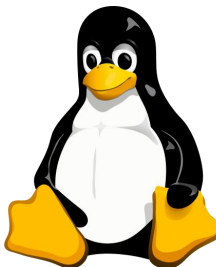
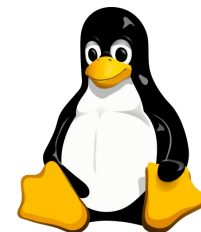
5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

2. ส่วนประกอบหลักของระบบปฏิบัติการ Linux

🌀 **Bootloader** เป็นซอฟต์แวร์ที่ทำหน้าที่จัดการเรื่องการบูต (Boot) ของคอมพิวเตอร์สำหรับผู้ใช้ ก็คือหน้าจอที่แสดงขึ้นมาช่วงที่กำลังเริ่มเข้าสู่ระบบปฏิบัติการ

🌀 **Kernel** เปรียบเสมือนคำเรียกของ “Linux” เพราะเป็นระบบส่วนกลางที่ทำหน้าที่จัดการทรัพยากรต่าง ๆ เช่น CPU, memory และอุปกรณ์ต่อเสริมต่าง ๆ เป็นเลเยอร์ต่ำสุดที่อยู่ใกล้กับฮาร์ดแวร์มากที่สุด

🌀 **Daemons** เป็นส่วนที่ทำงานอยู่เบื้องหลัง (Background service) เริ่มทำงานตั้งแต่ระหว่างที่บูต และเริ่ม login เข้าสู่ระบบ

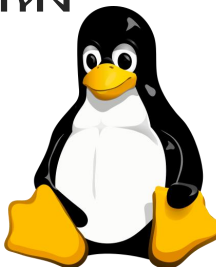
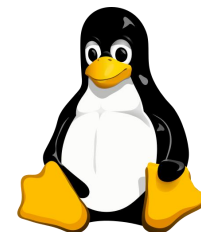


5. ระบบปฏิบัติการสำหรับสมาร์ตโฟนและแท็บเล็ต

๑ **Shell** คือ การทำงานของคำสั่งที่ทำให้ผู้ใช้สามารถควบคุมและสั่งการผ่านการพิมพ์ตัวอักษรเข้าไป (Command line) ซึ่งเป็นส่วนหนึ่งที่ทำให้ผู้ใช้กังวลในการใช้งานเนื่องจากไม่สามารถจดจำคำสั่งและเข้าใจการใช้คำสั่ง แต่ใน Linux desktop รุ่นใหม่ไม่จำเป็นต้องใช้ Command line แล้ว

๑ **Graphical Server** เป็นระบบที่ช่วยเสริมการแสดงผลบนจอแสดงผล ลินุกซ์ใช้ Graphical server ที่เรียกว่า “X” หรือ “X-server”

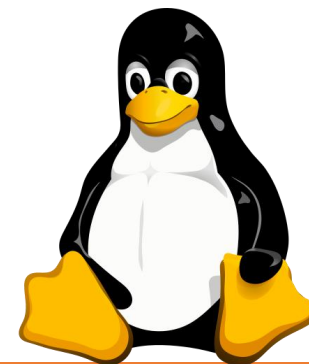
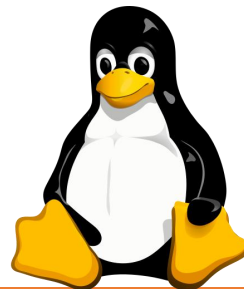
โดย X คือ แอปพลิเคชันที่จัดการจอแสดงผลกราฟิกหนึ่งจอขึ้นไปและอุปกรณ์อินพุตหนึ่งอุปกรณ์ขึ้นไป (เช่น แป้นพิมพ์ เมาส์) ที่เชื่อมต่อกับคอมพิวเตอร์ ทำงานเป็นเซิร์ฟเวอร์และสามารถทำงานบนเครื่องคอมพิวเตอร์นี้หรือบนเครื่องอื่นในเครือข่ายบริการสามารถสื่อสารกับเซิร์ฟเวอร์ X เพื่อแสดงอินเทอร์เฟซแบบกราฟิกและรับอินพุตจากผู้ใช้



5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

🔗 Desktop Environment คือ ส่วนที่ผู้ใช้ใช้งานจริงโดยมีให้เลือกได้หลากหลาย ซึ่งก็คือ ชุดของแอปพลิเคชันต่าง ๆ ที่ถูกจับมารวมกัน เช่น managers, configuration tools, web browsers, games

🔗 Applications Desktop environment นั้นไม่ได้จัดแอปพลิเคชันมาครบเหมือน Window หรือ Mac เนื่องจาก Linux มีซอฟต์แวร์ที่มีคุณภาพที่ง่ายต่อการค้นหาแล้วติดตั้ง Linux ที่ได้รับความนิยมส่วนใหญ่มักจะมีเครื่องมือที่ใช้สำหรับค้นหาและติดตั้งแอปพลิเคชันติดมาให้ เช่น Ubuntu Linux จะมี software center คือ apt ที่ใช้ในการดาวน์โหลดและติดตั้งแอปพลิเคชันจากศูนย์กลาง

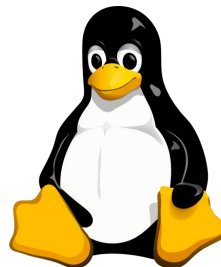
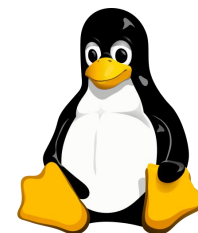


5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

3. แอปพลิเคชันที่ทำงานบนระบบปฏิบัติการ Linux

แอปพลิเคชันที่ทำงานบนระบบปฏิบัติการ Linux มีอยู่จำนวนมากและส่วนใหญ่เปิดให้ใช้ฟรีตั้งแต่โปรแกรมสำหรับทำงานในสำนักงานทั่วไป โปรแกรมทำภาพ ตัดต่อภาพยนตร์ จนถึงงานออกแบบทางวิศวกรรม เช่น

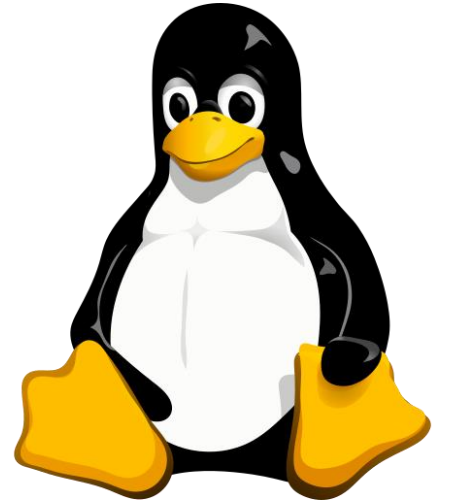
- 1) โปรแกรมทำแอนิเมชัน ได้แก่ Blender 3D, Pencil, KpovModeler, Synfig (2D), Stopmotion
- 2) โปรแกรมสำหรับทำงานด้านเสียง ได้แก่ Audio CD Extractor (ripper), Sound Converter, Freqtweak, Hipo iPod Management Tool
- 3) โปรแกรมทำงานด้านวิดีโอ ได้แก่ VLC, Wink, XBMC, Media Center, Acidrip, Gnome Subtitles



5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

- 4) โปรแกรมทำงานด้านกราฟิก ได้แก่ GIMP, Hlugin, Comix, QCad, Inkscape
- 5) โปรแกรมทำงานสำนักงาน ได้แก่ OpenOffice, KOrganizer, xPDF, AbiWord
- 6) โปรแกรมเบราว์เซอร์ ได้แก่ Opera, Firefox Thunderbird (สำหรับรับส่งอีเมล)



ข้อดีของการใช้ Linux

- ๑ ลินุกซ์เป็นระบบปฏิบัติการแบบเปิด (Open Source) ที่ผู้ใช้สามารถนำไปใช้ได้ฟรี จึงไม่ผิดกฎหมายลิขสิทธิ์
- ๑ ไม่ค่อยมีปัญหาเรื่องไวรัสหรือการแฮ็กข้อมูล เนื่องจากไม่ค่อยเป็นเป้าหมาย (ผู้ใช้ควรตรวจสอบการ Update Patch ความมั่นคงปลอดภัยอย่างสม่ำเสมอ) แต่อาจถูกโจมตีได้เช่นกัน
- ๑ ไม่ต้องการระบบฮาร์ดแวร์สเปกสูงมาก สามารถปรับแต่งการทำงานของระบบได้อย่างหลากหลาย
- ๑ เป็นระบบปฏิบัติการที่มีเสถียรภาพสูง ใช้ทรัพยากรระบบน้อย จึงนิยมนำไปใช้เป็นเครื่องแม่ข่าย

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

ข้อเสียของการใช้ Linux

- ❖ ผู้ใช้ส่วนใหญ่ไม่ค่อยรู้จักและไม่มีความคุ้นเคยในการใช้งาน ทำให้การเริ่มต้นใช้งานต้องปรับตัวและเรียนรู้ใหม่บ้าง
- ❖ ผู้ดูแลระบบที่เข้าใจการบริหารจัดการ Linux มีน้อยกว่าผู้ที่ทำงานกับระบบปฏิบัติการอื่น เช่น Windows



5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

5.4 ระบบปฏิบัติการ macOS

เป็นระบบปฏิบัติการที่ใช้เฉพาะเครื่องคอมพิวเตอร์ที่ผลิตและจำหน่ายโดย บริษัท แอปเปิลคอมพิวเตอร์ จำกัด เช่น Apple Macintosh, Mac Book, Mac Mini



รูปที่ 6.31 คอมพิวเตอร์ของ Apple ที่ใช้ระบบปฏิบัติการ macOS

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

ระบบปฏิบัติการแมคโอเอส (macOS) ถูกออกแบบมาให้มีส่วนติดต่อผู้ใช้ (Interface) แบบกราฟิก (Graphic) ในอดีตก่อนหน้านี้ ระบบปฏิบัติการที่ใช้กับคอมพิวเตอร์ส่วนบุคคลจะการใช้การรับคำสั่งจากผู้ใช้แบบ Command Line ทำให้ยุ่งยากในการจดจำและเข้าใจ macOS จึงถูกพัฒนาขึ้นเพื่อใช้กับคอมพิวเตอร์ของ Apple รุ่น Macintosh โดยคอมพิวเตอร์รุ่นนี้ถูกออกแบบมารองรับการทำสื่อสิ่งพิมพ์และงานดนตรี

ระบบปฏิบัติการ macOS ถูกพัฒนาอย่างต่อเนื่องให้ใช้งานได้กับเครื่องคอมพิวเตอร์สำหรับทำงานและคอมพิวเตอร์ที่ใช้เป็นเครื่องแม่ข่ายในชื่อระบบปฏิบัติการ MAC OS X Server โดยต่อมาแอปเปิลได้ยุติการพัฒนา ระบบปฏิบัติการสำหรับเซิร์ฟเวอร์เนื่องจากไม่ค่อยประสบความสำเร็จในการทำตลาด



5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

แมคโอเอส (macOS) ก่อนหน้าเรียกว่า แมคโอเอสเท็น (Mac OS X) ถึง พ.ศ. 2554 และโอเอสเท็น (OS X) ถึง พ.ศ. 2559 จึงเปลี่ยนชื่อเป็น macOS ซึ่งเป็นระบบปฏิบัติการรุ่นล่าสุดในตระกูลแมคโอเอสประกอบด้วย 2 ส่วนหลัก คือ แกนกลาง ดาร์วิน (Darwin) ซึ่งเป็นสภาพแวดล้อมการทำงานแบบยูนิกซ์ที่เป็นโอเพนซอร์ซ และส่วนติดต่อผู้ใช้แบบอควา (Aqua) ซึ่งเป็นลิขสิทธิ์ของบริษัท แอปเปิล

แอปเปิลยังได้สร้างแมคโอเอสรุ่นปรับปรุงเพื่อนำไปใช้ในอุปกรณ์ของแอปเปิล 4 ตัว ได้แก่ แอปเปิลทีวี ไอโฟน ไอพอดทัช และไอแพด โดยที่ไอโฟนและไอพอดทัชจะใช้รุ่นของแมคโอเอสที่เรียกว่า iOS ซึ่งระบบปฏิบัติการที่แก้ไขนี้จะมีแต่สิ่งที่เป็นเท่านั้น ไดรเวอร์และส่วนประกอบอื่นที่ไม่จำเป็นจะถูกนำออกไป



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต



รูปที่ 6.32 ระบบปฏิบัติการ macOS ล่าสุด (2021) macOS Big Sur

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต



ในส่วนของการใช้งานแอปพลิเคชัน ถึงแม้ macOS จะไม่สามารถติดตั้งโปรแกรมที่ถูกสร้างมาสำหรับระบบปฏิบัติการ Windows ได้ แต่เนื่องจากจำนวนผู้ใช้ macOS มีมากพอสมควร ผู้สร้างมีแอปพลิเคชันรายใหญ่จึงมักจะทำแอปพลิเคชันแบบเดียวกันกับที่ใช้กับ Windows แต่เป็นเวอร์ชันสำหรับระบบปฏิบัติการ macOS ขึ้นมา เช่น Microsoft Office, Photoshop AutoCAD เป็นต้น

รูปที่ 6.33 โปรแกรม Microsoft Office For Mac

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

ข้อดีสำหรับผู้ใช้งานทั่วไปในการใช้งานระบบปฏิบัติการ macOS คือ ระบบจะมีโปรแกรมที่ใช้ในสำนักงานที่ทำงานเหมือน Microsoft Office มาให้เลยโดยไม่ต้องซื้อเพิ่มคือ Pages ใช้แทน Microsoft Word, Numbers ใช้แทน Excel และ Keynote ใช้แทน PowerPoint นอกจากนี้ยังมีโปรแกรมสำหรับตัดต่อภาพยนตร์ชื่อ iMovie และโปรแกรมสำหรับแต่งเพลงทำดนตรีชื่อ Garage Band มาให้ด้วย

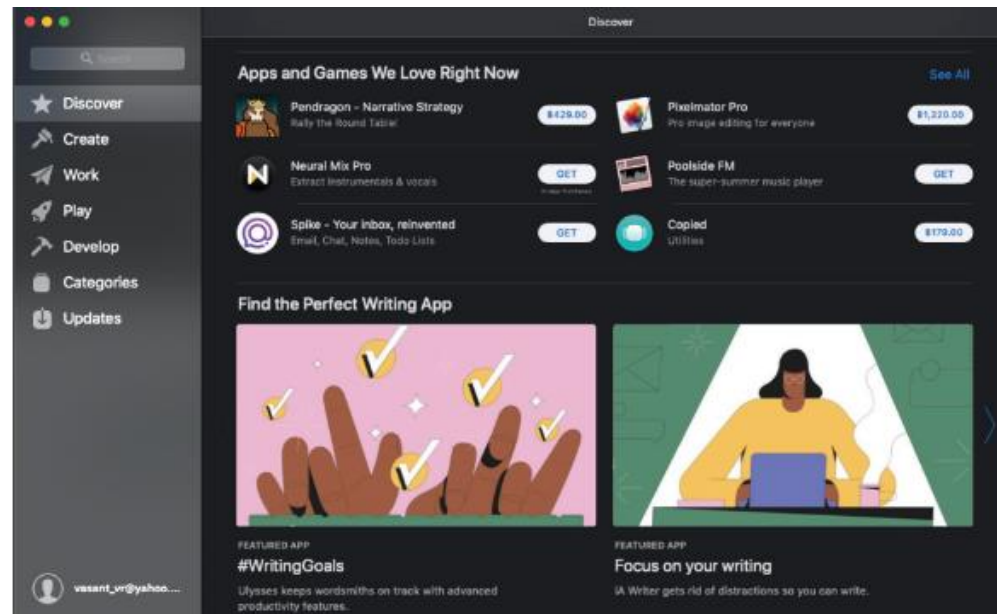


รูปที่ 6.34 โปรแกรมประยุกต์ที่แถมมากับ
ระบบปฏิบัติการ macOS

5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

1. การติดตั้งแอปพลิเคชันระบบปฏิบัติการ macOS

ระบบปฏิบัติการ macOS กำหนดให้ผู้ใช้เข้าไปโหลดแอปพลิเคชันผ่าน Apple App Store เหมือนกับโทรศัพท์มือถือ Android ที่มี Play Store โดยใน Apple App Store จะมีทั้งโปรแกรมฟรี และโปรแกรมเสียเงิน อย่างไรก็ตาม ผู้ใช้ยังสามารถที่จะติดตั้งโปรแกรมด้วยตนเองจากโปรแกรมติดตั้งเหมือน Windows เช่นกัน



รูปที่ 6.35 App Store สำหรับระบบปฏิบัติการ macOS



5.

ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

2. ข้อดีของระบบปฏิบัติการ macOS

- 1) เป็นระบบปฏิบัติการที่ถูกออกแบบมาเฉพาะรุ่นคอมพิวเตอร์ ทำให้มีการทำงานร่วมกันระหว่าง Hardware และ Software เป็นอย่างดี ส่งผลให้ระบบมีความเสถียรและประสิทธิภาพการทำงานดี
- 2) ส่วนผู้ติดต่อผู้ใช้ออกแบบมาให้เรียนรู้ได้ไม่ยากและมีมาตรฐานเดียวกัน ทำให้การใช้งานง่ายสำหรับผู้เริ่มต้น
- 3) เนื่องจากมีพื้นฐานมาจาก UNIX ทำให้มี Utility สำหรับการดูแลระบบ การพัฒนาภาษาคอมพิวเตอร์ และประสิทธิภาพที่ดีของระบบ UNIX จึงเหมาะสำหรับนักพัฒนาโปรแกรม
- 4) ไม่ค่อยเป็นเป้าโจมตีของผู้ผลิตไวรัสหรือแฮกเกอร์เนื่องจากไม่ค่อยเป็นที่นิยมในการทำงานภาคธุรกิจ (แต่ถูกโจมตีได้เช่นกัน)
- 5) ตัวระบบปฏิบัติการมาพร้อมกับโปรแกรมประยุกต์สำหรับการทำงานในสำนักงานจึงไม่ต้องจัดซื้อเพิ่ม เมื่อรวมค่าลิขสิทธิ์แล้วจึงมีราคาไม่สูงมากอย่างที่หลายคนเข้าใจ





5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

3. ข้อเสียของระบบปฏิบัติการ macOS

- 1) มีผู้ใช้อย่างไม่มาก ทำให้การสนับสนุนจากผู้เชี่ยวชาญอาจจะหายากกว่า Windows
- 2) อาจจะมีปัญหาเรื่องการจัดวางเอกสารหรือการแลกเปลี่ยนข้อมูลเอกสารระหว่าง Windows และ macOS (ส่วนใหญ่เป็นเรื่องของรูปแบบเอกสารภาษาไทย)
- 3) การหาแอปพลิเคชันเฉพาะทางบางประเภทจะยุ่งยากกว่า Windows



หมายเหตุ

ข้อควรปฏิบัติในการใช้ระบบปฏิบัติการ มีดังนี้

1. เลือกใช้ระบบปฏิบัติการให้เหมาะสมกับสเปกของเครื่องและลักษณะการใช้งาน หากเลือกระบบปฏิบัติการที่มีฟังก์ชันการทำงานมากแต่ไม่ได้ใช้ก็เป็นการสิ้นเปลือง หรือถ้าเลือกระบบปฏิบัติการที่มีฟังก์ชันน้อยเกินไปก็จะไม่สามารถใช้งานอุปกรณ์ได้อย่างมีประสิทธิภาพ เช่น ระบบปฏิบัติการ Windows แบบ 32 บิต สามารถใช้งานหน่วยความจำได้เพียง 4 GB เท่านั้น



5. ระบบปฏิบัติการสำหรับสมาร์ทโฟนและแท็บเล็ต

หมายเหตุ

ข้อควรปฏิบัติในการใช้ระบบปฏิบัติการ มีดังนี้

2. เลือกใช้ระบบปฏิบัติการที่มีลิขสิทธิ์หรือเป็นระบบ Open Source ที่มีข้อมูลการใช้งานที่น่าเชื่อถือ เพื่อป้องกันปัญหาที่จะเกิดขึ้นต่อระบบงาน ข้อดีของการใช้ระบบปฏิบัติการที่มีลิขสิทธิ์ ได้แก่

2.1 ระบบปฏิบัติการที่ถูกลิขสิทธิ์ไม่ต้องใช้โปรแกรมอื่นที่เรียกว่าแคร็ก (Crack) มาเจาะระบบให้ใช้งานได้ ดังนั้นจึงช่วยลดความเสี่ยงต่อการมีไวรัสหรือถูกขโมยข้อมูล เพราะโปรแกรมแคร็กอาจจะเป็นไวรัสหรือสร้างช่องโหว่ด้านความมั่นคงปลอดภัยแก่ระบบของเราได้

2.2 ระบบปฏิบัติการที่มีลิขสิทธิ์สามารถ Update Patch ด้านความมั่นคงปลอดภัยจากผู้ผลิตได้ ทำให้ลดความเสี่ยงที่จะถูกเจาะระบบหรือไวรัสลดลง

2.3 การใช้ระบบปฏิบัติการละเมิดลิขสิทธิ์ และผิดกฎหมาย อาจจะถูกดำเนินคดีได้



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

สิ่งที่ทำให้คอมพิวเตอร์และอุปกรณ์ประเภทสมาร์ตโฟนแตกต่างจากอุปกรณ์อิเล็กทรอนิกส์อื่น ๆ คือ การมีซอฟต์แวร์ระบบปฏิบัติการ ซึ่งช่วยให้สามารถใช้งานอุปกรณ์เหล่านี้ในหลากหลายรูปแบบด้วยแอปพลิเคชันต่าง ๆ ได้ เครื่องคอมพิวเตอร์แบบเดียวกันแต่ถ้ามีการติดตั้งระบบปฏิบัติการที่ต่างกันจะทำให้การทำงานแตกต่างกันออกไปอย่างสิ้นเชิง ดังนั้นการเลือกระบบปฏิบัติการที่จะนำมาใช้งานจึงเป็นสิ่งสำคัญเป็นอย่างยิ่ง

ในการเลือกใช้ระบบปฏิบัติการรวมถึงซอฟต์แวร์ที่ใช้กับระบบเครือข่ายคอมพิวเตอร์ นอกจากจะต้องดูเรื่องความเหมาะสมของงาน ประสิทธิภาพการทำงานของระบบแล้ว สิ่งหนึ่งที่จะต้องตระหนัก คือ การเคารพต่อทรัพย์สินทางปัญญาและกฎหมายลิขสิทธิ์





การใช้โปรแกรมประยุกต์



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

1. ความหมายของโปรแกรมประยุกต์

โปรแกรมประยุกต์ หมายถึง โปรแกรมที่พัฒนาขึ้นเพื่อให้เครื่องคอมพิวเตอร์ทำงานตามความต้องการของผู้ใช้ ที่เป็นงานทั่วไปและงานเฉพาะด้าน ขึ้นอยู่กับลักษณะงานและจุดมุ่งหมาย การนำโปรแกรมประยุกต์ไปใช้งานนอกจากเป็นการเพิ่มประสิทธิภาพในการทำงานแล้วยังเป็นการอำนวยความสะดวกแก่ผู้ปฏิบัติงานอีกด้วย เช่น โปรแกรมเพื่องานด้านการฝากถอนเงินโดยเครื่องรับจ่ายเงินอัตโนมัติ จะเกี่ยวข้องกับการฝากหรือถอนเงิน รวมทั้งการควบคุมยอดเงินคงเหลือในบัญชีเงินฝากของลูกค้าธนาคาร ตัวอย่างของโปรแกรมประยุกต์เพื่อใช้งานในด้านต่าง ๆ ได้แก่



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

1.

ความหมายของโปรแกรมประยุกต์



โปรแกรมการคำนวณน้ำประปา ค่าไฟฟ้า ค่าโทรศัพท์



โปรแกรมเพื่อใช้บริหารบุคคลของหน่วยงาน



โปรแกรมเพื่อการลงทะเบียนเรียนของนักศึกษา



โปรแกรมเพื่อแสดงยอดขายสินค้าของบริษัท



โปรแกรมประยุกต์เงินเดือนพนักงาน



โปรแกรมประยุกต์เพื่อจัดซื้อสินค้าหรือพัสดุ

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

ก่อนหน้านี้เว็บเบราว์เซอร์จะมีหน้าที่สำหรับใช้ดูข้อมูลต่าง ๆ ผ่านเครื่องแม่ข่ายให้บริการเว็บ (Web Server) ที่ให้บริการผ่าน World Wide Web (WWW) หรือเทียบง่าย ๆ เหมือนเป็นโทรศัพท์เป็นห้องสมุดให้เราเข้าไปดูข้อมูล แต่เป็นสถานีโทรศัพท์ที่มีนับล้าน ๆ ช่อง ผู้ใช้ส่วนใหญ่จะไม่ค่อยสนใจรายละเอียดในการใช้งานเว็บเบราว์เซอร์หรือเลือกโปรแกรมเว็บเบราว์เซอร์มากนัก ผู้ใช้มักจะใช้โปรแกรมที่ติดตั้งมากับระบบปฏิบัติการ เช่น IE หรือ Internet Explorer ที่ติดตั้งมากับระบบปฏิบัติการ Windows หรือ Safari ที่มาพร้อมกับ Mac OS ต่อมาเมื่อมีโปรแกรมงานเว็บเบราว์เซอร์ฟรีจาก Mozilla ชื่อ Firefox เข้ามาทำให้ใช้โดยข้อดีของเว็บเบราว์เซอร์



2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

(ในยุคแรก) เริ่มมีผู้ผลิตโปรแกรมสำเร็จรูปหลายรายสร้างโปรแกรมเว็บเบราว์เซอร์มาให้เราได้ใช้มากขึ้นเรื่อย ๆ โดยเฉพาะเมื่อ Google สร้างเว็บเบราว์เซอร์ของตนเองที่ใช้ชื่อว่า Google Chrome ทำให้เกิดการแข่งขันเรื่องความสามารถของโปรแกรมเว็บเบราว์เซอร์มากขึ้นตามลำดับ



รูปที่ 7.1 โปรแกรมเว็บเบราว์เซอร์ที่ได้รับความนิยม

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

สาเหตุที่ทำให้เราให้ความสำคัญกับโปรแกรมเว็บเบราว์เซอร์มากขึ้น เพราะว่าเทคโนโลยีการสื่อสารในปัจจุบันมีความก้าวหน้าอย่างรวดเร็ว ทำให้เกิดบริการใหม่ ๆ บนเครือข่ายอินเทอร์เน็ต นอกเหนือจากการดูข้อมูล ไม่ว่าจะเป็นความบันเทิง การช้อปปิ้งออนไลน์ จนถึงการทำธุรกรรมการเงิน หรือแม้แต่การเข้าไปดูข้อมูลต่าง ๆ จากอินเทอร์เน็ตเองก็ตาม เพราะเว็บเบราว์เซอร์เป็นเหมือนประตูสู่โลกภายนอกของคอมพิวเตอร์ส่วนบุคคลหรือระบบเครือข่ายในองค์กร ในขณะเดียวกันก็เป็นช่องทางให้เกิดการเข้ามาของผู้ไม่ประสงค์ดีทั้งแบบที่โจมตีโดยตรง (แฮ็กข้อมูล) หรือการทำผ่านมัลแวร์ที่แนบมากับข้อมูลที่ใช้เข้าไป ดูทำให้ผู้ใช้ต้องเข้าใจกลไกการทำงานหรือความสามารถต่าง ๆ ของโปรแกรมเว็บเบราว์เซอร์เพื่อความระมัดระวังปลอดภัยในการใช้งานอินเทอร์เน็ต





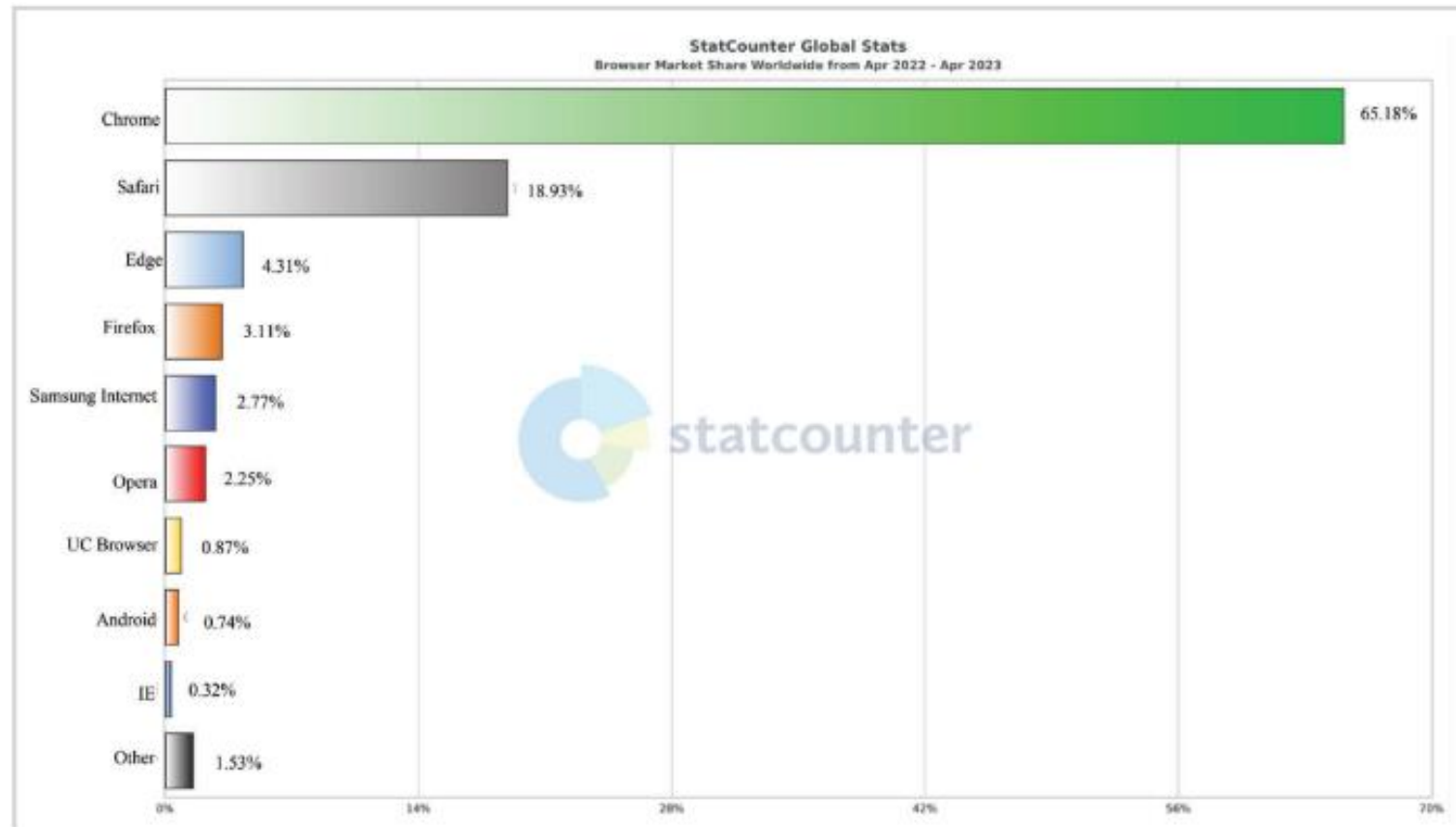
2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

ความสามารถและบริการของเว็บเบราว์เซอร์ที่เพิ่มขึ้นผ่านระบบ World Wide Web บวกกับความเร็วในการใช้งานอินเทอร์เน็ตในปัจจุบันที่มีมากขึ้น จนกระทั่งเราสามารถทำงานต่าง ๆ ผ่านเว็บเบราว์เซอร์ได้โดยไม่ต้องใช้โปรแกรมเสริมอื่น เช่น กรณีโน้ตบุ๊กของ Google ที่ชื่อว่า Chrome Book เมื่อเปิดเครื่องผู้ใช้จะเข้าไปใช้โปรแกรมพื้นฐาน เช่น ผ่านทางเว็บเบราว์เซอร์โดยมีโปรแกรมให้ใช้งานผ่าน Google Docs

ตัวอย่างโปรแกรมเว็บเบราว์เซอร์ ได้แก่ Opera, Avast Secure Browser, Google Chrome, Mozilla Firefox, Safari และ Microsoft Edge โดยเว็บเบราว์เซอร์ชั้นนำที่เป็นที่นิยมจะมีคุณสมบัติที่ใกล้เคียงกัน โดยเฉพาะเรื่องความมั่นคงปลอดภัย แต่จะแตกต่างกันในรายละเอียดปลีกย่อยที่จะช่วยให้ผู้ใช้สามารถปรับแต่งได้เหมาะสมกับการทำงานของตนมากที่สุด เช่น การโหลดโปรแกรมเสริมเพื่อเพิ่มความสามารถต่าง ๆ ให้เว็บเบราว์เซอร์ ที่เรียกว่า Add-on ใน Firefox หรือ Extension ใน Google Chrome

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์



รูปที่ 7.2 อันดับเว็บเบราว์เซอร์ที่มีผู้ใช้งานเยอะสุดประจำเดือนตั้งแต่ เม.ย. 2022 ถึง เม.ย. 2023

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

หัวใจสำคัญของการใช้เว็บเบราว์เซอร์นอกจากเรื่องความเร็วแล้วยังมีเรื่องที่หลายคนไม่ทราบหรือละเลย คือ การปรับแต่งเพื่อความมั่นคงปลอดภัยของข้อมูล หรือความเป็นส่วนตัวของผู้ใช้ ซึ่งโปรแกรมเว็บเบราว์เซอร์มาตรฐานจะมีส่วนนี้อยู่และจะเปิดใช้ค่ามาตรฐานระดับความมั่นคงปลอดภัยในระดับปานกลาง และให้ผู้ใช้ปรับเปลี่ยนเองได้ภายในเมนูการตั้งค่าของโปรแกรม โดยจะขอยกตัวอย่างการปรับตั้งค่าจากโปรแกรม Google Chrome เนื่องจากมีผู้นิยมใช้มาก (โปรแกรมอื่นจะปรับแต่งใกล้เคียงกัน)





2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

2.1 การท่องเว็บให้ปลอดภัยด้วย HTTPS

ปกติแล้วมักจะคุ้นเคยกับโปรโตคอล HTTP ซึ่งเมื่อพิมพ์ชื่อเว็บไซต์ในเว็บเบราว์เซอร์ โปรแกรมจะเติมโปรโตคอลให้เอง เช่น ถ้าเราพิมพ์ `www.kmutnb.ac.th` ระบบจะเติม `http://www.kmutnb.ac.th/` และถ้าตรวจพบว่าเว็บไซต์มีบริการด้านความมั่นคงปลอดภัยที่เรียกว่า HTTPS ระบบจะปรับที่อยู่ของเว็บไซต์เป็น `https://www.kmutnb.ac.th/` โดยอัตโนมัติ HTTPS (Hypertext Transfer Protocol Secure) คือ โปรโตคอลการสื่อสารอินเทอร์เน็ตที่ช่วยรักษาความสมบูรณ์ถูกต้องของข้อมูลผู้ใช้และเก็บข้อมูลไว้เป็นความลับระหว่างคอมพิวเตอร์ของผู้ใช้กับเว็บไซต์ ผู้ใช้คาดหวังประสบการณ์ออนไลน์ที่มีความมั่นคงปลอดภัยและเป็นส่วนตัวระหว่างที่ใช้เว็บไซต์ผู้ใช้ควรหลีกเลี่ยงเว็บไซต์ที่ไม่ใช้โปรโตคอล HTTPS เนื่องจากการรับส่งข้อมูลต่าง ๆ ระหว่างการท่องเว็บไซต์จะสามารถถูกดักข้อมูลไปได้ง่าย

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์



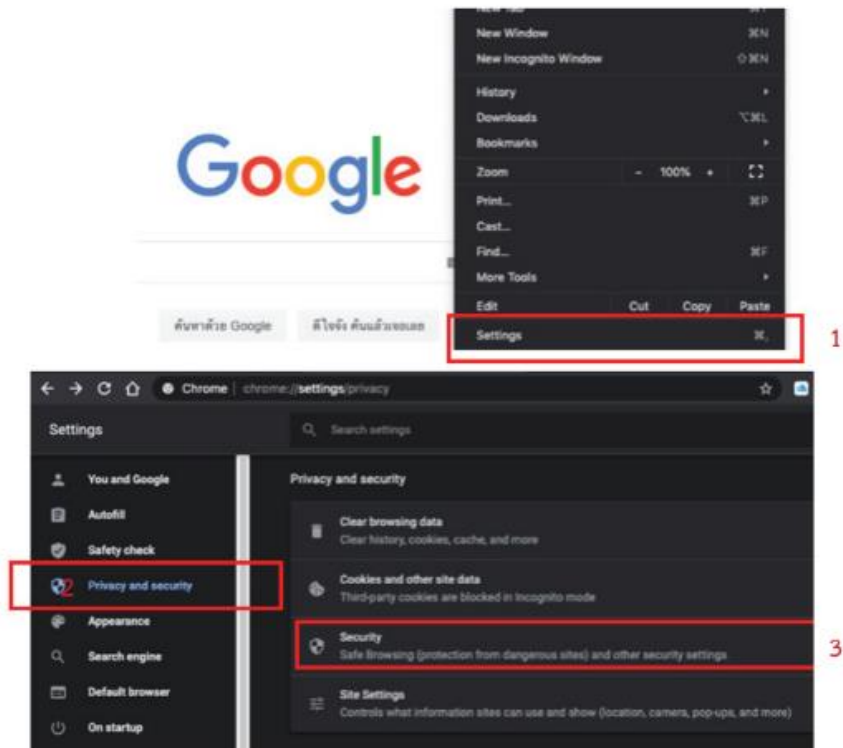
การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

2.2 การตรวจสอบและตั้งค่าความมั่นคงปลอดภัยเบื้องต้นของเว็บเบราว์เซอร์

ไปที่ Settings -> Privacy & Security ->

Security

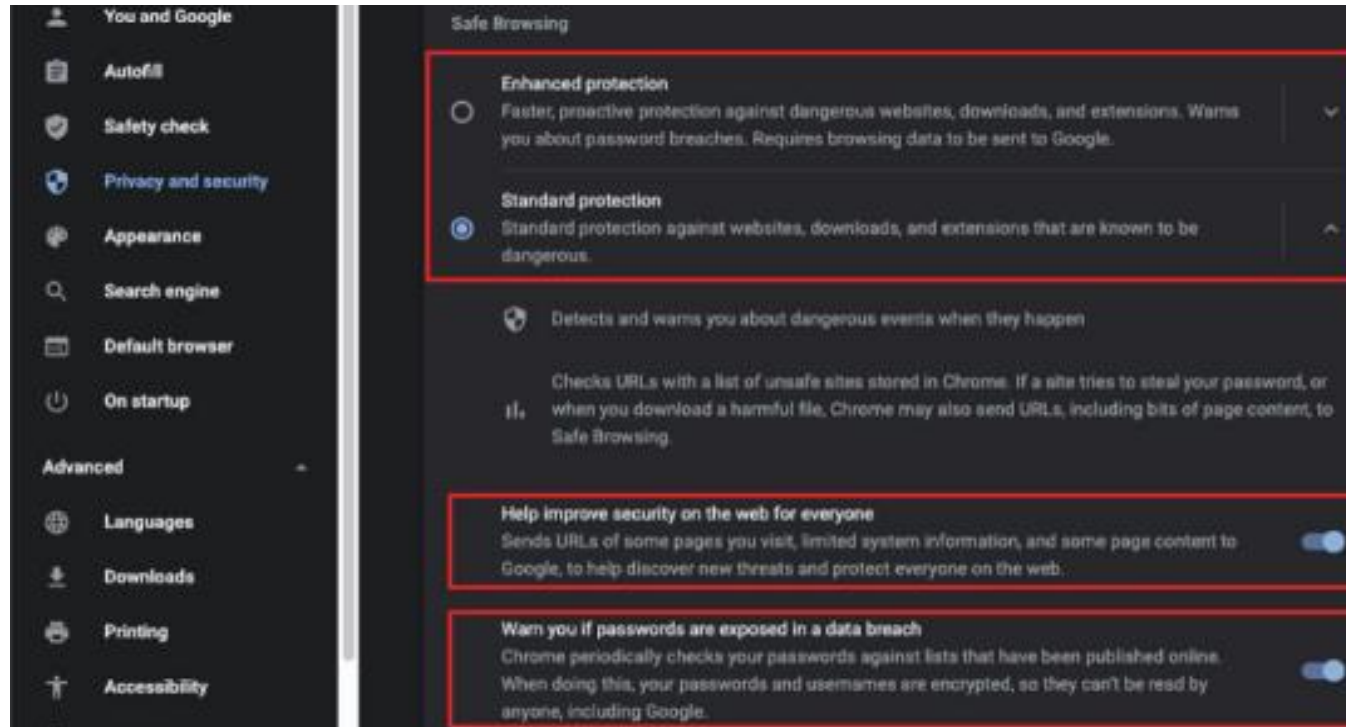


รูปที่ 7.4 การตั้งค่าความมั่นคงปลอดภัยเบื้องต้นของเว็บเบราว์เซอร์

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

✦ ตรวจสอบค่าระบบรักษาความมั่นคงปลอดภัยถูกเปิดใช้งานในแบบ Standard และมีการเปิดใช้งานตามภาพเป็นอย่างน้อย



รูปที่ 7.5 การลบประวัติการท่องเว็บไซต์

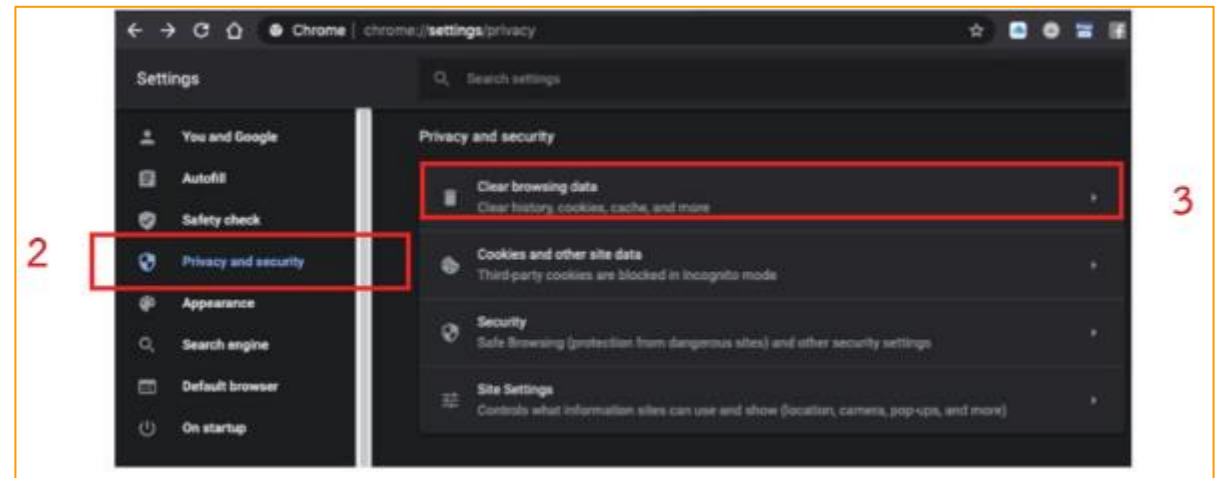
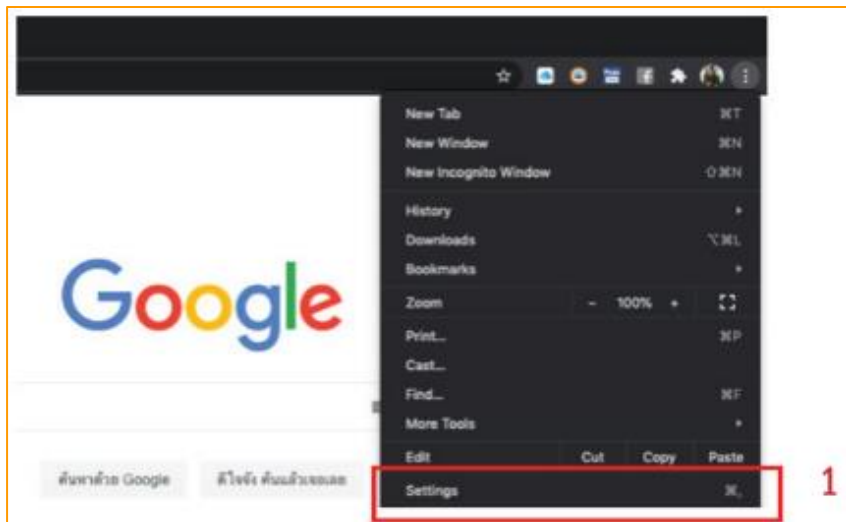
การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

2.3 การลบประวัติการท่องเว็บไซต์

ทั้งในกรณีที่เครื่องของตนเองหรือการไปใช้เครื่องคอมพิวเตอร์ของผู้อื่นแล้วต้องการจะลบประวัติการใช้งาน เพื่อป้องกันข้อมูลที่ใช้งานรั่วไหลไปยังบุคคลอื่นทำได้ ดังนี้

⚙ Settings -> Privacy and Security -> Clear browsing data

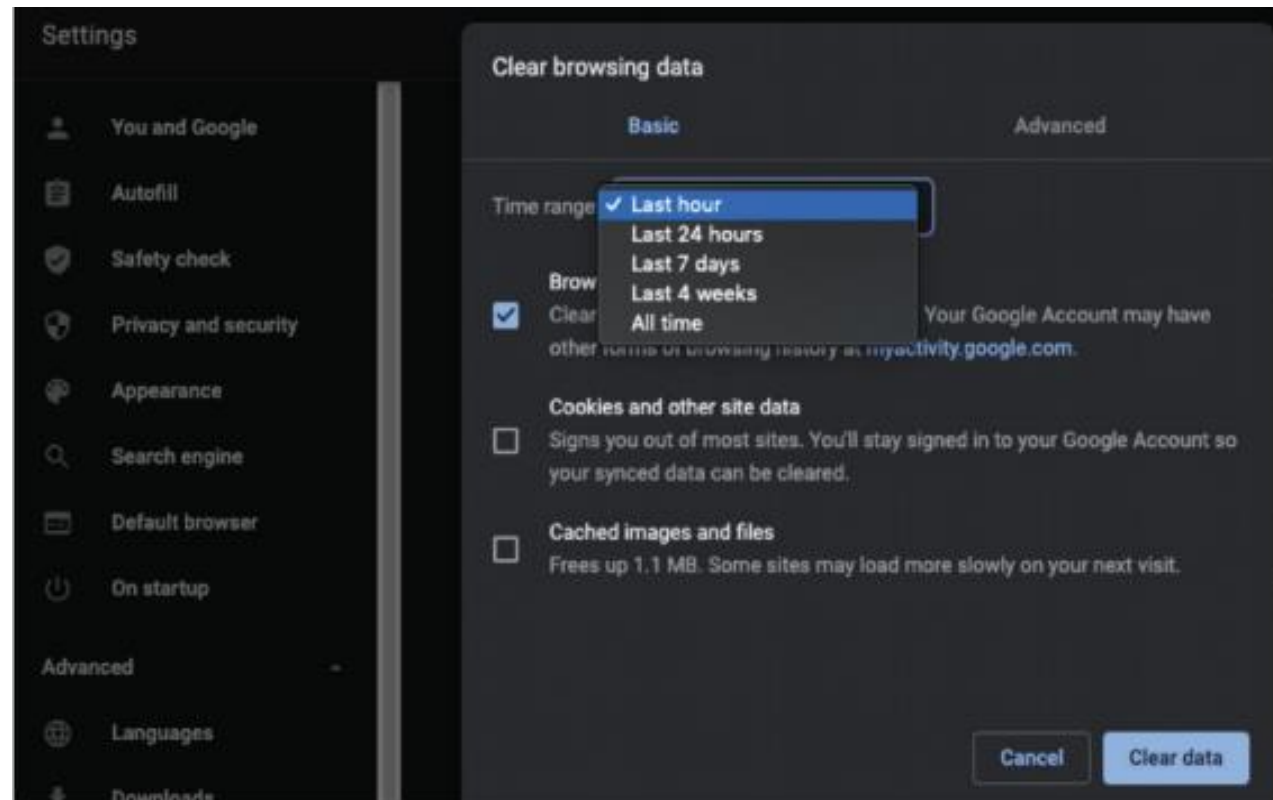


รูปที่ 7.6 Settings -> Privacy and Security -> Clear browsing data

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

✦ ผู้ใช้สามารถกำหนดระยะเวลาที่ต้องการลบประวัติการเข้าใช้งานในระบบได้



รูปที่ 7.7 การกำหนดระยะเวลาที่ต้องการลบประวัติการเข้าใช้งาน



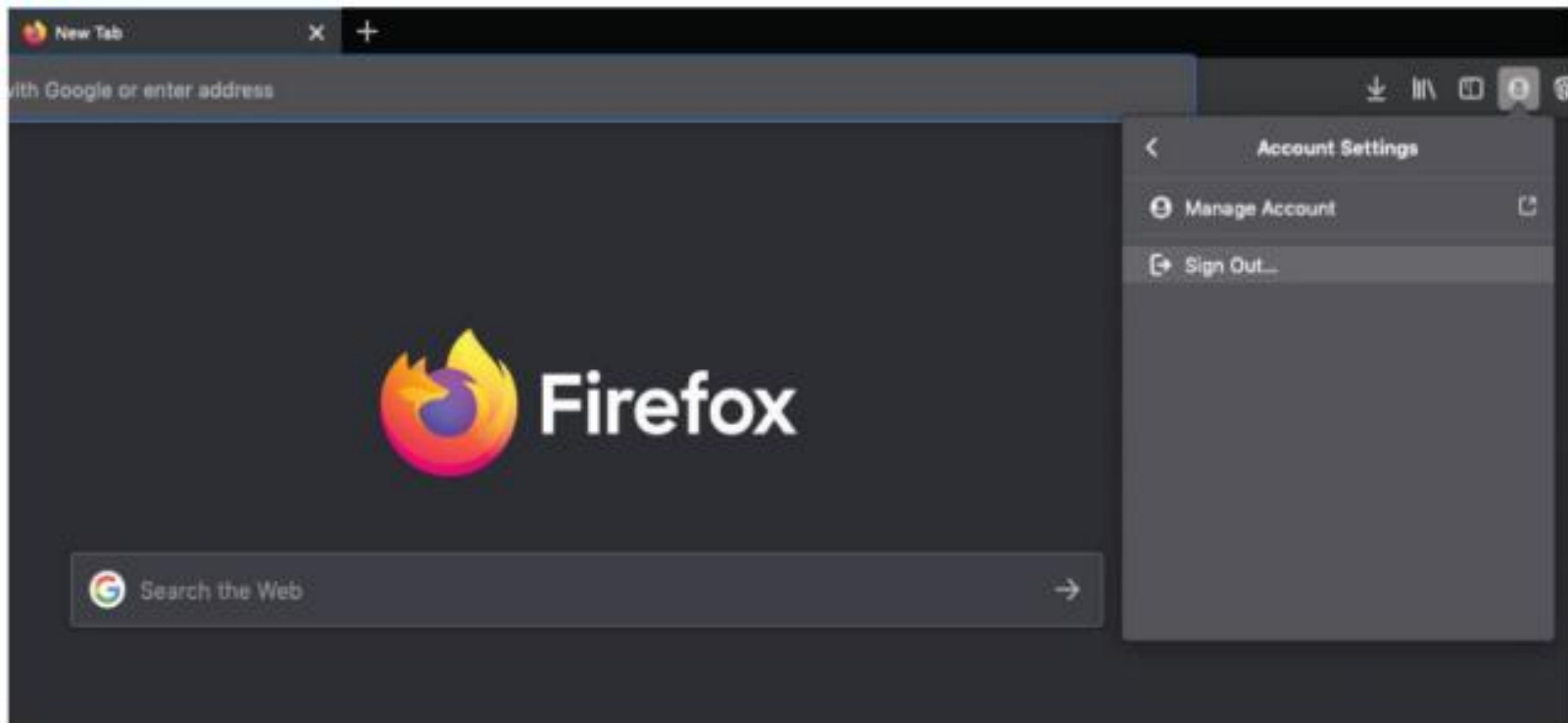
2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์

2.4 การใช้งานร่วมกันของเว็บเบราว์เซอร์ในหลายอุปกรณ์

เว็บเบราว์เซอร์ในหลายอุปกรณ์สมัยใหม่จะมีความสามารถที่เรียกว่าการ Synchronize ข้อมูลของผู้ใช้ ไปยังอุปกรณ์อื่นเพื่ออำนวยความสะดวกให้กับผู้ใช้ที่มีอุปกรณ์คอมพิวเตอร์หลายเครื่อง เช่น โน้ตบุ๊ก เครื่องตั้งโต๊ะและสมาร์ทโฟน ถ้าผู้ใช้งานลงชื่อเข้าใช้เว็บเบราว์เซอร์ด้วยบัญชีเดียว (สามารถสมัครได้ฟรี) เช่น การลงชื่อด้วย Gmail ใน Google Chrome ข้อมูลของผู้ใช้ทั้งประวัติการเข้าชม บุ๊กมาร์ก จนถึงรหัสผ่านต่าง ๆ จะถูกส่งผ่านไปปรากฏในทุกอุปกรณ์ที่ผู้ใช้งานลงชื่อเข้าใช้ไปใช้งาน อย่างไรก็ตามสิ่งที่ต้องระมัดระวังคืออุปกรณ์ที่ลงชื่อเข้าใช้ด้วยบัญชีของเว็บเบราว์เซอร์ จะต้องมั่นใจว่ามีความมั่นคงปลอดภัยในแง่กายภาพ คือไม่มีบุคคลอื่นสามารถเข้าไปใช้งานได้ เพราะอาจจะทำให้ข้อมูลรั่วไหลหรือมีการเข้าถึงข้อมูลส่วนบุคคลต่าง ๆ ได้ หากเป็นอุปกรณ์คอมพิวเตอร์ส่วนบุคคลอาจแนะนำให้ใช้การ Synchronize ข้อมูลผ่านเว็บเบราว์เซอร์

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

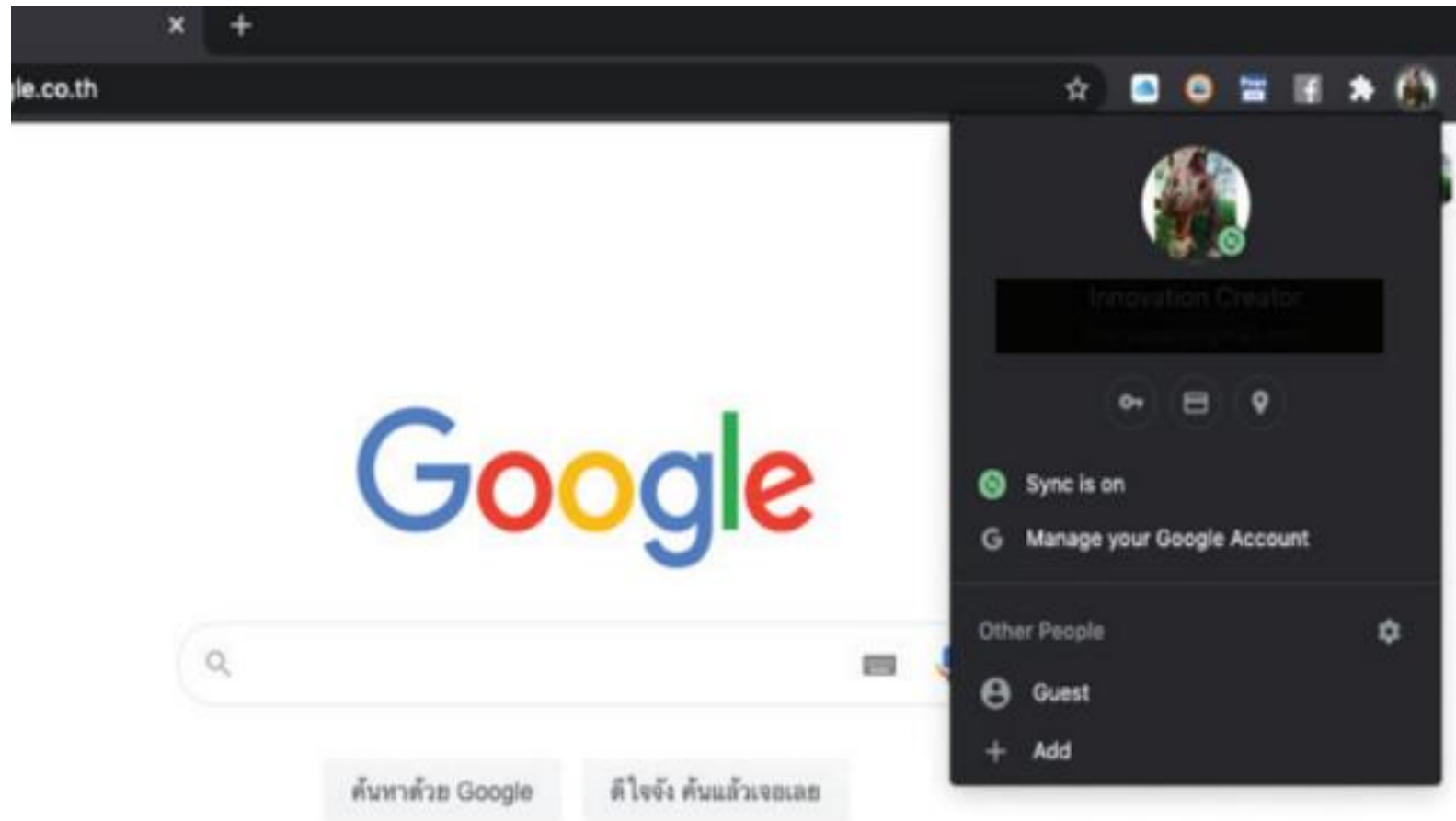
2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์



รูปที่ 7.8 การใช้งานร่วมกันของเว็บเบราว์เซอร์ในหลายอุปกรณ์

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

2. การใช้งานโปรแกรมประเภทเว็บเบราว์เซอร์



รูปที่ 7.9 การลงชื่อเข้าใช้งานเพื่อ Sync ข้อมูลในเว็บเบราว์เซอร์

3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

บริการต่าง ๆ เกิดขึ้นมากมายทั้งที่เป็นลักษณะการให้บริการผ่านเว็บไซต์ หรือการใช้งานบนเครื่องคอมพิวเตอร์แต่รับส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์ ซึ่งในปัจจุบันโปรแกรมประยุกต์ที่ถูกใช้งานผ่านระบบเครือข่ายนับได้ว่าแทบจะครอบคลุมการทำงานแทบทุกด้าน ได้แก่

3.1 โปรแกรมประยุกต์ด้านการทำธุรกิจ

ในการใช้งานระบบคอมพิวเตอร์ตั้งแต่เริ่มแรกจนถึงปัจจุบัน การใช้งานโปรแกรมประยุกต์ด้านธุรกิจจะเป็นวัตถุประสงค์หลัก โดยโปรแกรมที่นิยมใช้งาน ได้แก่ Word Processing โปรแกรมสำหรับคำนวณหรือ Spread Sheet โปรแกรมนำเสนองาน หรือ Presentation เช่น PowerPoint, Keynote

โปรแกรมประยุกต์เหล่านี้เรามักจะคุ้นเคยการทำงานในแบบที่ต้องติดตั้งบนเครื่องคอมพิวเตอร์แต่ในปัจจุบันผู้ใช้สามารถที่จะใช้งานโปรแกรมเหล่านี้ผ่านเว็บเบราว์เซอร์ได้ ซึ่งมีทั้งแบบฟรีและแบบที่ต้องเสียเงินค่าบริการรายปี

3.

โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

1. โปรแกรม Google Docs หรือ Google Documents “ฟรี” บริการออนไลน์ในการทำงานโปรแกรมประเภท Office จากค่าย Google เพียงแค่อีเมลของ Google ก็สามารถใช้บริการได้ฟรีผ่านทางเครือข่ายอินเทอร์เน็ต แลยังมีพื้นที่ในการจัดเก็บข้อมูลอย่าง “Google Drive” ฟรีอีกด้วย

เปรียบเทียบ Microsoft Office กับ Google Docs		
Program	Microsoft Office	Google Docs
งานจดหมาย	Microsoft Word	Docs
งานตาราง คำนวณ	Microsoft Excel	Sheets
งานนำเสนอ	Microsoft PowerPoint	Slides

3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

วิธีใช้งาน Google Docs

1. เปิดโปรแกรม “เว็บเบราว์เซอร์” แนะนำให้ใช้ Google Chrome

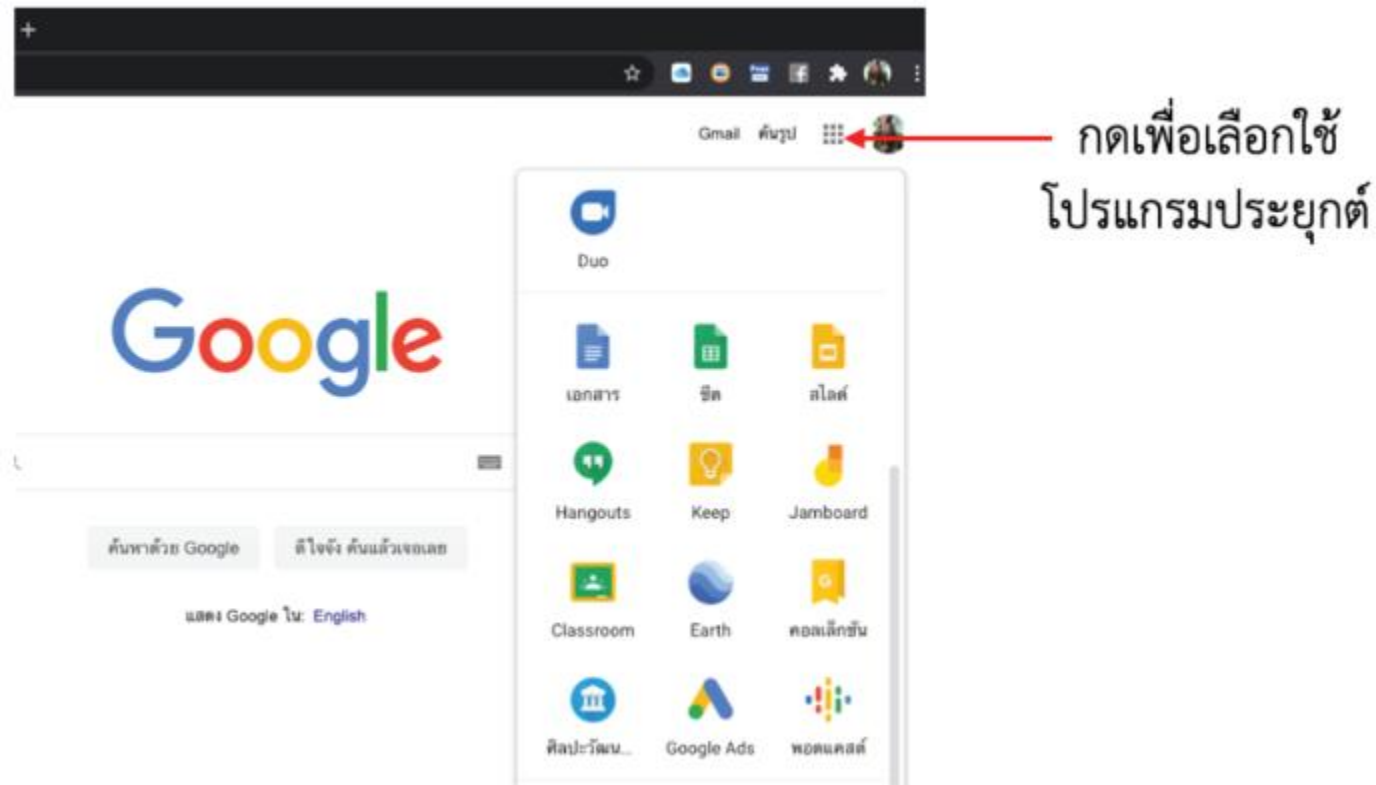
2. คลิก Login เพื่อเข้าบัญชี Google ด้วย Gmail

3..ที่มุมขวามือของหน้าจอ จากนั้นคลิกเลือกโปรแกรมที่ต้องการจากเมนูด้านซ้ายมือ ไม่ว่าจะเป็น Docs, Sheets หรือ Slides

4..นอกจากนี้ ยังมีโปรแกรม Forms ซึ่งเป็นโปรแกรมที่สามารถนำมาประยุกต์ใช้งานได้หลากหลาย เช่น การทำฟอร์มรับสมัคร เก็บข้อมูล หรือแม้แต่การทำแบบทดสอบออนไลน์อีกด้วย



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์



รูปที่ 7.10 วิธีใช้งาน Google Docs



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

2. โปรแกรม Office 365 เป็นการให้บริการโปรแกรมชุด Microsoft Office ที่สามารถใช้งานได้ทุกที่ผ่านเว็บเบราว์เซอร์และระบบอินเทอร์เน็ต โดยผู้ใช้เพียงแคมีบัญชี Microsoft ซึ่งลงทะเบียนโดยใช้ E-mail และสมัครการใช้บริการ Office 365 ก็สามารถใช้โปรแกรม Microsoft Office ได้โดยไม่ต้องติดตั้งโปรแกรมชุด Office ในเครื่องคอมพิวเตอร์หรือสมาร์ทโฟนและยังมีพื้นที่เก็บข้อมูลบนคลาวด์ให้สูงถึง 1 TB ทำให้ผู้ใช้สามารถเก็บเอกสารของตนไว้ได้อย่างมากมายทั้งสำหรับใช้งานจริงหรือใช้สำหรับสำรองข้อมูล อย่างไรก็ตาม Office 365 เป็นโปรแกรมที่ผู้ใช้จะต้องเสียค่าบริการรายปี โดยค่าใช้จ่ายเริ่มต้นเพียงปีละ 300 บาทต่อคน (แบบ Family) หากผู้ใช้มีความคุ้นเคยกับการใช้โปรแกรมตระกูล Microsoft Office ก็เป็นตัวเลือกที่น่าสนใจเพราะหนึ่งบัญชี (E-mail) สามารถลงชื่อใช้งานอุปกรณ์พร้อมกันได้ถึง 5 อุปกรณ์

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

3.

โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

รุ่นล่าสุด: ผู้ใช้สูงสุด 6 คนในพีซีหรือ Mac

Microsoft 365 Family

฿2,899.00 /ปี

ซื้อทันที

หรือซื้อในราคา ฿289.99 ต่อเดือน

ลองใช้ฟรี 1 เดือน >

การสมัครใช้งานเป็นการชำระเงินรายปีสำหรับผู้ใช้งานสูงสุด 6 คนในพีซีหรือ Mac มีแอปพลิเคชันประสิทธิภาพสูงที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS และแอปพลิเคชันที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS และแอปพลิเคชันที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS

รวมแอปพลิเคชันฟรี

Word Excel PowerPoint OneNote

Outlook Access (พีซีเท่านั้น) Publisher (พีซีเท่านั้น)

บริการที่รวม

OneDrive Skype

Microsoft 365 Personal

฿2,099.00 /ปี

ซื้อทันที

หรือซื้อในราคา ฿209.99 ต่อเดือน

การสมัครใช้งานเป็นการชำระเงินรายปีสำหรับผู้ใช้งานสูงสุด 1 คนในพีซีหรือ Mac มีแอปพลิเคชันประสิทธิภาพสูงที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS และแอปพลิเคชันที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS และแอปพลิเคชันที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS

รวมแอปพลิเคชันฟรี

Word Excel PowerPoint OneNote

Outlook Access (พีซีเท่านั้น) Publisher (พีซีเท่านั้น)

บริการที่รวมอยู่

OneDrive Skype

Office Home & Student 2019

ซื้อครั้งเดียวสำหรับ Mac และพีซี

฿4,299.00

ซื้อทันที

การซื้อครั้งเดียว

มีทุกแอปพลิเคชันที่พร้อมใช้งานสำหรับการใช้งานที่บ้านและที่ทำงานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS และแอปพลิเคชันที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS และแอปพลิเคชันที่พร้อมใช้งานบนพีซีและ Mac ที่ติดตั้งระบบปฏิบัติการ Windows หรือ macOS

รวมแอปพลิเคชันฟรี

Word Excel PowerPoint

บริการที่รวมอยู่

(ไม่มี)

รูปที่ 7.11 ตัวอย่างราคาของค่าบริการ Office 365 (ราคาอาจจะมีการเปลี่ยนแปลงตามโปรโมชั่น)



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

3.2 โปรแกรมประยุกต์ด้านการสื่อสาร

อินเทอร์เน็ตถูกออกแบบมาสำหรับการทำงานระยะไกล ซึ่งในปัจจุบันด้วยความเร็วในการสื่อสารที่เพิ่มมากขึ้นทำให้สามารถบริการการสื่อสารผ่านเครือข่ายอินเทอร์เน็ตเต็มรูปแบบ ทั้งภาพ เสียงการประชุม หรือการนำเสนอต่าง ๆ โดยเฉพาะเมื่อเกิดวิกฤตการณ์โรคโควิด-19 ระบาด ทำให้ความจำเป็นในการใช้การสื่อสารระยะไกลแบบกลุ่มเพิ่มสูงขึ้นจนกลายเป็นปัจจัยสำคัญในการขับเคลื่อนทั้งภาคธุรกิจและการศึกษา เช่น การประชุมออนไลน์ การเรียนการสอนทางไกล โดยโปรแกรมประยุกต์ที่ได้รับความนิยมในการสื่อสารระยะไกลแบบกลุ่ม ได้แก่





3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

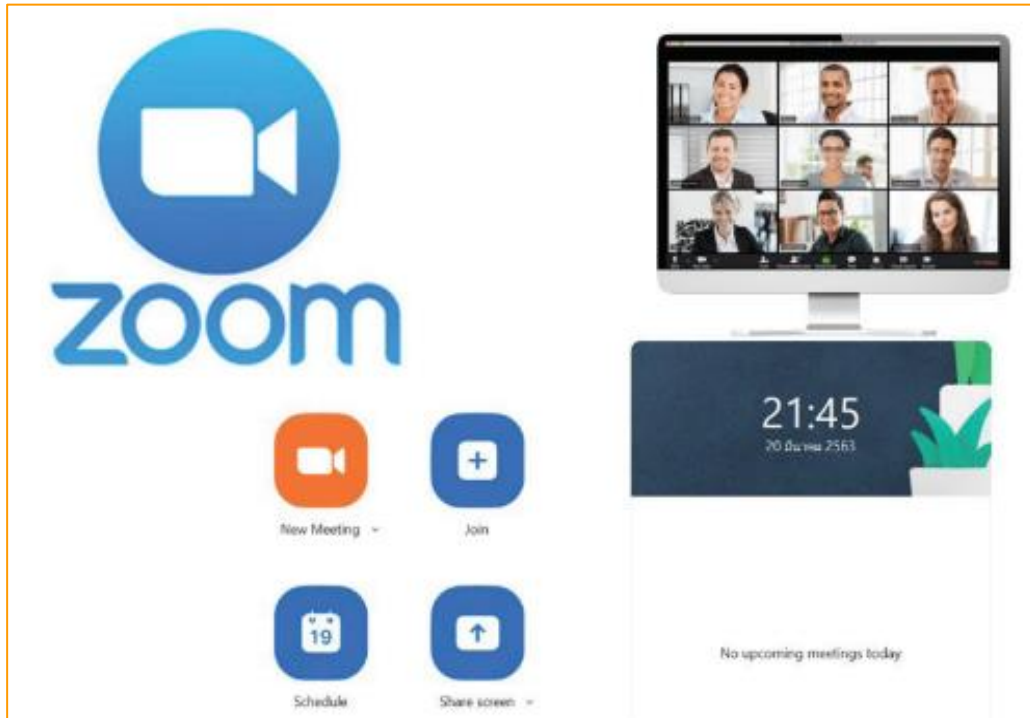
1. โปรแกรม Zoom

เป็นโปรแกรมประชุมทางไกลผ่านระบบคลาวด์ เป็นซอฟต์แวร์สำหรับสื่อสารกันในลักษณะของ Video Conference เหมาะสำหรับใช้ประชุมหรือห้องเรียนผ่านเครือข่ายคอมพิวเตอร์ที่มีระบบตอบโต้เพื่ออำนวยความสะดวกในการประชุมหรือการเรียนการสอน เช่น ระบบแชร์หน้าจอของผู้เข้าประชุม ระบบยกมือ ระบบพูดคุยกันเองระหว่างผู้เรียน และระบบควบคุมเสียง/ภาพของผู้เข้าประชุมหรือผู้เรียน เป็นต้น Zoom Cloud Meetings สามารถใช้งานได้หลายแพลตฟอร์ม ทั้งบนคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟนซึ่งมีคุณสมบัติในการทำงาน Video Conference, Chat Room, Schedule และ Share Screen



การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์



รูปที่ 7.12 โปรแกรมชุม

อีกทั้งยังสามารถเชิญผู้เข้าร่วมประชุมได้โดยไม่ต้องสมัครเป็นสมาชิก เพียงแค่ผู้เข้าร่วมจะต้องมี PM (Personal Meeting ID) และ Password หรือ URL จากผู้ที่เป็นเจ้าภาพการประชุมหรือเรียกว่า โฮสต์ (Host) และติดตั้งแอปพลิเคชันของ Zoom ก็สามารถเข้าร่วมประชุมได้ ทำให้ Zoom เหมาะสำหรับการใช้งานประชุมหรือสร้างห้องเรียนผ่านเครือข่ายคอมพิวเตอร์เป็นอย่างมาก



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

โปรแกรมซูมมีบัญชีฟรีสำหรับผู้เริ่มต้น สามารถจัดการประชุมทางไกลได้มากถึง 100 คน โดยจำกัดระยะเวลาไม่เกินครั้งละ 40 นาที ซึ่งเพียงพอที่จะใช้ในการประชุมหรือการเรียนการสอนทั่วไป (สามารถต่อกลับมาได้) และหากต้องการใช้ซูมเพื่อการประชุมระยะเวลานาน ๆ ผู้ที่เป็นเจ้าภาพการประชุม (Host) สามารถที่จะสมัครสมาชิกเพื่อใช้งานแบบโปร (Professional) ซึ่งมีราคาเริ่มต้นที่ประมาณเดือนละ 400 บาท

2. โปรแกรม Google Meet

เป็นโปรแกรมที่ใช้สำหรับการประชุมเช่นกัน โดยการให้บริการจาก Google ซึ่งพัฒนามาจากโปรแกรม Google Duo โดยเน้นการใช้งานในภาคธุรกิจคือมีความสามารถในการแชร์หน้าจอและแชร์เอกสารระหว่างการประชุม เป็นต้น



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

Google ไม่ได้บังคับให้ผู้ร่วมประชุมทุกคนที่ต้องเป็นผู้ใช้ผลิตภัณฑ์ Gmail ของ Google แต่หากเป็นสมาชิกของ Google อยู่แล้วจะใช้งาน Feature ต่าง ๆ ได้มากกว่า โดยทาง Google ได้ออกแบบไว้สำหรับกลุ่มผู้ใช้งาน 3 ประเภท ดังนี้

1. ระดับธุรกิจ : สำหรับบริษัท องค์กร ทั้งขนาดเล็กและขนาดใหญ่
2. สถาบันการศึกษา : โรงเรียน มหาวิทยาลัย และสถาบันการศึกษาอื่น ๆ
3. ผู้ใช้งานทั่วไป : สำหรับติดต่อสื่อสารกับเพื่อน ญาติ และผู้นัดหมายอื่น ๆ

หากต้องการใช้งาน Google Meet ให้เต็มประสิทธิภาพ ผู้ใช้จะต้องสมัครใช้บริการ G Suite ของ Google เช่นเดียวกันกับโปรแกรม Zoom แต่ราคาถูกกว่า

3.

โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

เลือกรุ่นที่เหมาะสมกับคุณ ทดลองใช้ฟรี 14 วัน

ทุกแพ็คเกจประกอบด้วย

Gmail Drive Meet Calendar Chat Jamboard Docs Sheets Slides Keep Sites Forms

Business Starter	Business Standard	Business Plus	Enterprise
฿113.50 THB ฿227*	฿272.40 THB ฿454*	฿681 THB	
ต่อผู้ใช้/เดือน โดยมีระยะเวลาสูงสุด 1 ปี	ต่อผู้ใช้/เดือน โดยมีระยะเวลาสูงสุด 1 ปี	ต่อผู้ใช้/เดือน โดยมีระยะเวลาสูงสุด 1 ปี	ติดต่อฝ่ายขาย
เริ่มต้นทดลองใช้ฟรี	เริ่มต้นทดลองใช้ฟรี	เริ่มต้นทดลองใช้ฟรี	
✓ มีเนตเวิร์กที่กำหนดและปลอดภัย ✓ การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ 100 คน ✓ พื้นที่เก็บข้อมูลขนาด 30 GB ต่อผู้ใช้ ✓ การควบคุมความปลอดภัยและการจัดการ ✓ การสนับสนุนระดับมาตรฐาน	✓ มีเนตเวิร์กที่กำหนดและปลอดภัย ✓ การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ + มีผู้เข้าร่วมได้ 150 คน ✓ พื้นที่เก็บข้อมูลขนาด 2 TB ต่อผู้ใช้** ✓ การควบคุมความปลอดภัยและการจัดการ ✓ การสนับสนุนระดับมาตรฐาน (ชำระเงินเพื่ออัปเกรดเป็นการสนับสนุนระดับสูง)	✓ มีเนตเวิร์กที่กำหนดและปลอดภัย + eDiscovery, การเก็บรักษาข้อมูล ✓ การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ + มีผู้เข้าร่วมได้ 500 คน การติดตามการเข้าร่วม ✓ พื้นที่เก็บข้อมูลขนาด 5 TB ต่อผู้ใช้** ✓ การควบคุมความปลอดภัยและการจัดการที่เพิ่มประสิทธิภาพ รวมถึงห้องปฏิบัติการและการจัดการปลายทางขั้นสูง ✓ การสนับสนุนระดับมาตรฐาน (ชำระเงินเพื่ออัปเกรดเป็นการสนับสนุนระดับสูง)	✓ มีเนตเวิร์กที่กำหนดและปลอดภัย + eDiscovery, การเก็บรักษาข้อมูล, การเข้ารหัส S/MIME ✓ การประชุมทางวิดีโอที่มีผู้เข้าร่วมได้ + มีผู้เข้าร่วมได้ 500 คน การติดตามการเข้าร่วม การลดเสียงรบกวน สตรีมมิงแบบสดภายในโดเมน ✓ พื้นที่เก็บข้อมูลตามต้องการ** ✓ การควบคุมความปลอดภัย การจัดการ และการปฏิบัติตามข้อกำหนดขั้นสูง รวมถึงฟองน้ำ, DLP, เซลล์ข้อมูล และการจัดการปลายทางระดับองค์กร ✓ การสนับสนุนขั้นสูง (ชำระเงินเพื่ออัปเกรดเป็นการสนับสนุนระดับพรีเมียม)

คุณจะได้รับสิทธิ์จาก Business Starter, Business Standard และ Business Plus ได้สูงสุด 300 คน ส่วนแพ็คเกจ Enterprise จะไม่มีจำนวนผู้ใช้ขึ้นสำหรับเรื่องสูงสุด

มูลค่า Google Workspace อาจแตกต่างกันไปขึ้นอยู่กับพื้นที่และช่วงเวลา

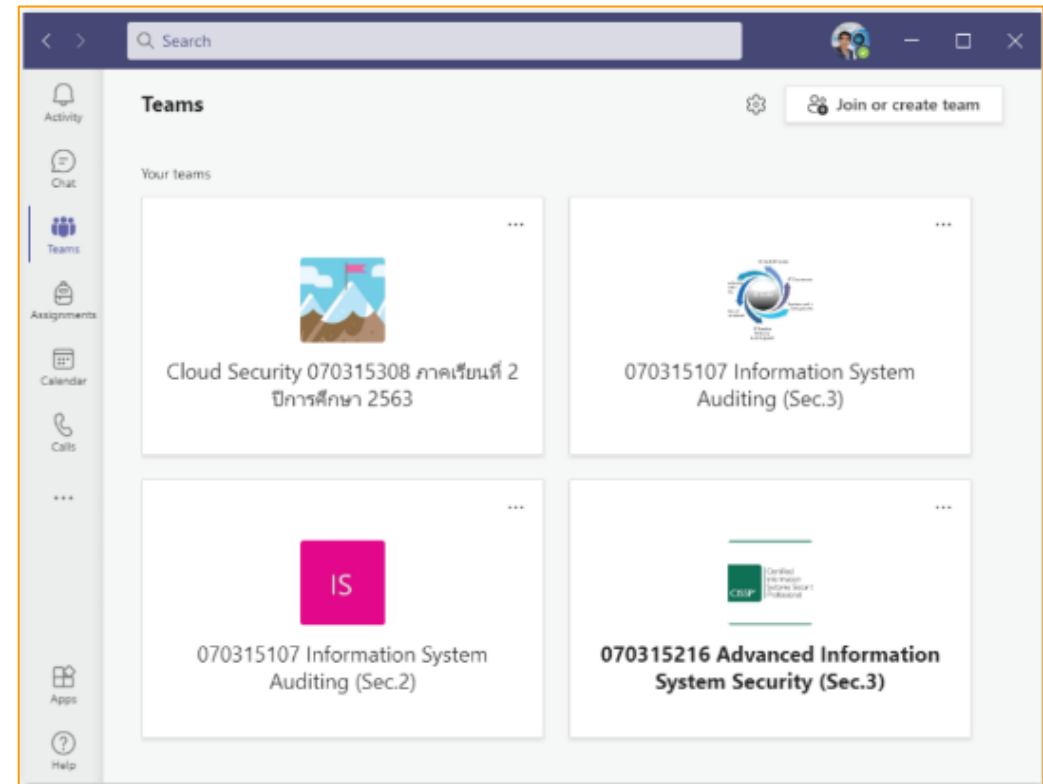
รูปที่ 7.14 ราคาค่าบริการของ Google Workspace ที่มีการรวม Google Meet เป็นส่วนหนึ่งของบริการ

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

3. Microsoft Team

เป็นแอปพลิเคชันสื่อสารระดับองค์กรที่มีข้อดีในด้านการทำงานร่วมกับ Office 365 โดยมีคุณสมบัติใกล้เคียงกับโปรแกรมประชุมทางไกลอื่น เช่น การแชร์หน้าจอ การทำงานเอกสารร่วมกัน การแชร์ไฟล์และด้วยความสามารถที่จะทำงานร่วมกับโปรแกรม Office ได้ ทำให้มีความคล่องตัวในการใช้งานแอป และเวิร์กโฟลว์ (Workflow) โดยผู้ใช้ที่มีบัญชี Office 365 สามารถที่จะใช้งาน Microsoft Team ได้ทันที



รูปที่ 7.15 ตัวอย่างหน้าจอของ Microsoft Team

3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

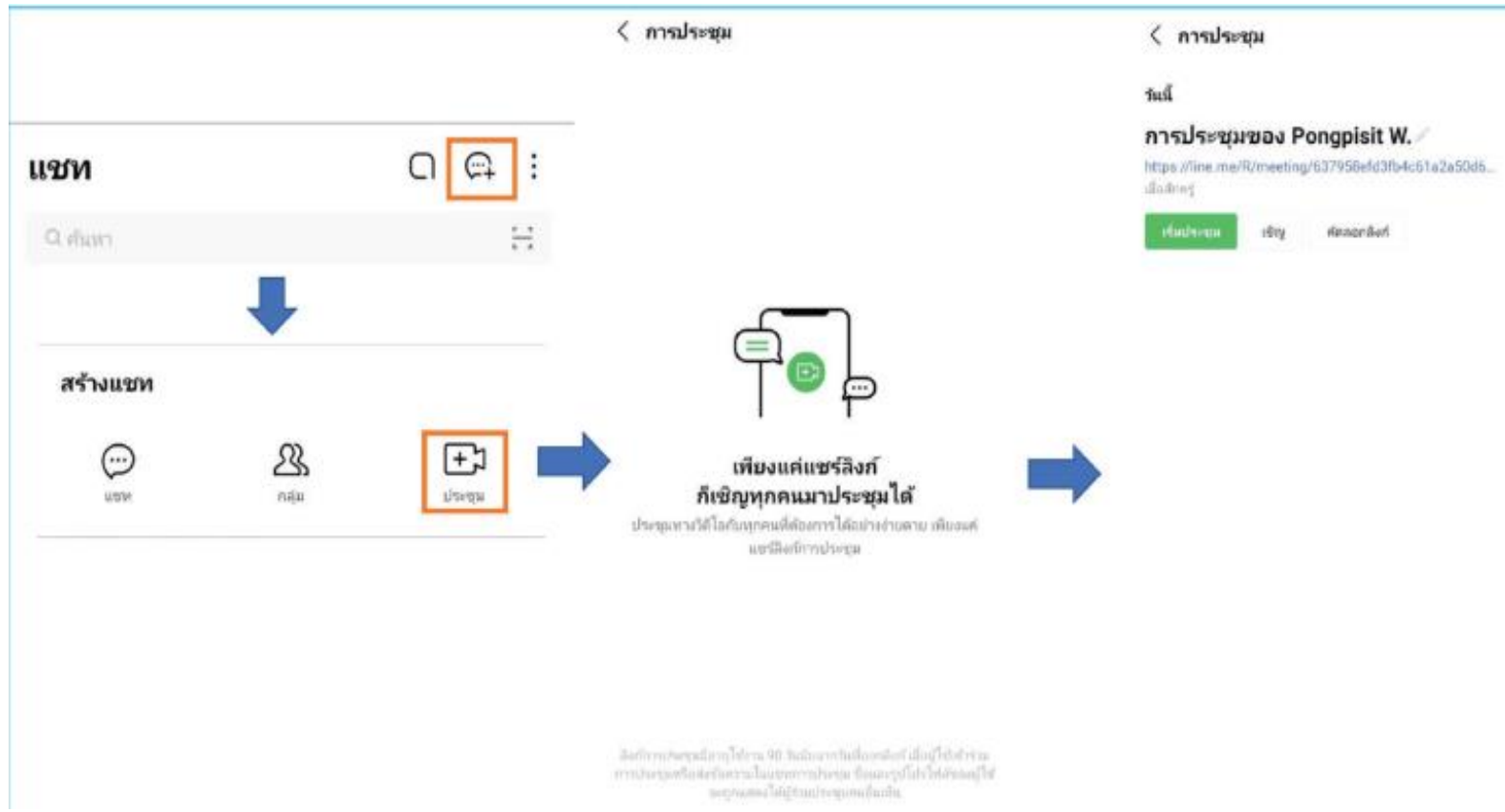
4. Line Meeting

เป็นแอปพลิเคชันด้านการสื่อสารอื่น ๆ นอกจากโปรแกรมสื่อสารและการประชุมเฉพาะทางที่มีอยู่ในตลาดแล้ว ผู้ให้บริการการสื่อสารข้อมูลส่วนบุคคล เช่น Line Facebook Messenger ก็พัฒนาการให้บริการประชุมกลุ่มขึ้นมาเช่นกัน Line จะใช้ชื่อว่า Line Meeting ซึ่งปรากฏอยู่ในโปรแกรม Line โดยผู้ใช้สามารถเชิญเพื่อนเข้าประชุมได้ทันทีโดยไม่ต้องสร้างกลุ่มและไม่จำเป็นต้องเป็นเพื่อนกันใน Line เพียงแต่มีลิงก์หรือ QR Code ที่เชิญโดยโฮสต์ สำหรับการประชุมก็สามารถเข้าประชุมได้ และสามารถรองรับการประชุมได้พร้อมกันถึง 500 คน โดยสามารถแชร์สกรีนได้ แต่จะขาดความสามารถบางอย่าง เช่น การควบคุมเสียงผู้เข้าประชุมโดยโฮสต์ เป็นต้น



3.

โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์



รูปที่ 7.16 การเรียกใช้ Line Meeting



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

5. Messenger Rooms

เป็นความสามารถที่เพิ่มขึ้นมาใน Facebook Messenger ให้สามารถสร้างห้องประชุมออนไลน์ ซึ่งรองรับการประชุมได้พร้อมกันถึง 50 คน ไม่จำกัดเวลา โดยมีความสามารถพิเศษคือการมีสติ๊กเกอร์สนุก ๆ พร้อมด้วยระบบ AR ซึ่งผู้ใช้งานสามารถแชร์ข้อมูลของการประชุมผ่าน Room ได้ผ่าน News Feed ของ Facebook โดยตรง หรือจะเข้าไปแชร์ที่ Group หรือ Event ของ Facebook

จากการที่มีโปรแกรมประยุกต์ด้านการสื่อสารให้เลือกหลากหลายโดยแต่ละโปรแกรมจะมีข้อดีข้อเสียที่แตกต่างกัน ดังนั้นผู้ใช้งานหรือองค์กรจะต้องพิจารณาเลือกโปรแกรมที่เหมาะสมกับตนเองมากที่สุด โดยข้อพิจารณาหลักจะประกอบไปด้วย

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์



รูปที่ 7.17 การประชุมผ่าน Messenger Rooms



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

1. ผู้เข้าร่วมประชุมมีความพร้อมที่จะใช้โปรแกรมใด เช่น การประชุมที่จัดขึ้นเป็นประจำภายในองค์กร ผู้ใช้น่าจะมีความพร้อม สามารถเรียนรู้การใช้โปรแกรมสำหรับการประชุมมาตรฐาน เช่น Zoom หรือถ้าหน่วยงานที่มีการใช้งาน office 365 อยู่แล้วก็ควรจะใช้ Microsoft Team เพื่อให้เกิดประโยชน์สูงสุดแต่ถ้าเป็นการประชุมกับบุคคลภายนอกเป็นครั้งคราวอาจจะเลือกใช้ระบบง่ายที่บุคคลทั่วไปมีใช้อยู่แล้ว เช่น การประชุมผ่าน Line เป็นต้น

2. รูปแบบและระยะเวลาการประชุม เป็นการประชุมที่ต้องการความร่วมมือหรือเป็นทางการและสำคัญในการนำเสนอ หน่วยงานจำเป็นจะต้องใช้โปรแกรมที่สามารถควบคุมการประชุมได้เป็นอย่างดี เช่น การปิดเสียงของผู้เข้าร่วมประชุมเพื่อให้ผู้เข้าประชุมได้รับฟังเสียงจากผู้นำการประชุมอย่างชัดเจน เป็นต้น



3. โปรแกรมประยุกต์ที่ใช้ในเครือข่ายคอมพิวเตอร์

3. ปัจจัยอีกอย่างหนึ่งที่จะต้องคำนึงถึง คือ ระบบอินเทอร์เน็ตของผู้จัดการประชุมหรือโฮสต์โดยสำหรับการประชุมผ่านระบบคลาวด์ ผู้ที่เป็นโฮสต์ไม่จำเป็นจะต้องมีความเร็วอินเทอร์เน็ตสูงมากนักแต่ระบบจะต้องมีเสถียรภาพที่ดี มีความเร็วคงที่ โดยความเร็วที่เหมาะสมเริ่มที่ประมาณ 4 Mbps ขึ้นไป

4. ควรเตรียมตัวก่อนการประชุม เช่น หากที่ไม่มีเสียงรบกวน มีแสงสว่างพอเหมาะ และมีความเป็นส่วนตัวพอสมควร

5. เพื่อประสิทธิภาพในการสื่อสาร ผู้เข้าร่วมประชุมทุกคนควรใช้หูฟังและ Microphone หรือหากใช้ลำโพงภายนอกต้องปิดไมโครโฟนทุกครั้งที่ตนเองพูดเสร็จ เพื่อป้องกันเสียงก้องหรือเสียงจากผู้เข้าประชุมไปรบกวนสมาธิผู้อื่น

4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

เพื่อปกป้องผู้ใช้งานให้มีการใช้งานระบบอินเทอร์เน็ตได้อย่างมั่นคงปลอดภัย ไม่ตกเป็นเหยื่อจากผู้ไม่หวังดี จึงจำเป็นที่ผู้ใช้งานอินเทอร์เน็ตจะต้องมีความตระหนักรู้ เพื่อสามารถป้องกันข้อมูลส่วนตัวและลดความเสี่ยงในการใช้งาน โดยได้ประยุกต์แนวทางจากที่สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) และคำแนะนำและแนวทางปฏิบัติด้าน Password จากเอกสาร NIST Special Publication 800-63B Rev3 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐฯ (National Institute of Standards and Technology: NIST) โดยมีคำแนะนำ ดังนี้



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์



4.1 การตั้งรหัสผ่านที่คาดเดาได้ยาก

โดยทั่วไปเพื่อความมั่นคงปลอดภัยควรตั้งรหัสผ่านอย่างน้อย 8 ตัวอักษร รหัสผ่านยิ่งยาวยิ่งเดายากหลีกเลี่ยงการตั้งรหัสผ่านด้วยหมายเลขโทรศัพท์ ชื่อเล่น ชื่อสัตว์เลี้ยง หรือคำพูดใดก็ตามที่สามารถระบุตัวตนของเราได้ วิธีการตั้งรหัสผ่านที่เดายาก

1. ในการตั้งรหัสผ่านควรมีตัวเลขประกอบด้วย การตั้งรหัสผ่านที่ดีควรประกอบไปด้วย

1) ตัวอักษรพิมพ์เล็ก

3) ตัวเลข

2) ตัวอักษรพิมพ์ใหญ่

4) ตัวอักษรพิเศษ ผสมกัน



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

โดยมีความยาวอย่างน้อย 8 ตัวอักษรขึ้นไป ยกตัวอย่างเช่น การนำประโยคในเนื้อเพลงมาเปลี่ยนแปลงรูปแบบตามหลักการทั้ง 4 รูปแบบ จะทำให้รหัสผ่านนั้นมีความยากในการคาดเดาจากผู้ไม่ประสงค์ดี ตัวอย่างเช่น ประโยคเดิม คือ all my Yesterday เรียบเรียงใหม่เป็น A11mYe47erd@y หรือประโยคเดิม ผมรักคุณมากนะครับ เรียบเรียงใหม่เป็น z,iyd86I,kdot8iy[เป็นต้น

โปรดจำไว้

ความยาวของรหัสผ่านสำคัญกว่าความยาก เนื่องจากยิ่งรหัสผ่านยาว ยิ่งเดารหัสผ่านได้ยาก การบังคับให้รหัสผ่านใหม่มีความยากกลับยิ่งทำให้ความมั่นคงปลอดภัยลดลง เพราะผู้ใช้อาจเพิ่มตัวอักษรบางตัวลงไป หรืออาจทำการจดบันทึกไว้เนื่องจากจำไม่ได้ และใช้รหัสผ่านซ้ำกันกับระบบอื่น ๆ



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

2. ไม่จำเป็นต้องรีเซตรหัสผ่านใหม่ทุก 3 เดือนหรือ 6 เดือน เนื่องจากการจดจำรหัสผ่านดี ๆ ถือเป็นเรื่องยากอยู่แล้ว เมื่อต้องมีหลาย ๆ รหัสผ่านที่ต้องจำ อาจทำให้ผู้ใช้เพิ่มตัวอักษรบางตัวลงไป หรืออาจทำการจดบันทึกไว้เนื่องจากจำไม่ได้ และใช้รหัสผ่านซ้ำกันกับระบบอื่น ๆ ทำให้มีความเสี่ยงมากกว่าเดิม

อย่างไรก็ตาม อาจยังคงมีนโยบายการรักษาความมั่นคงปลอดภัยของบางองค์กรที่กำหนดให้รหัสผ่านที่มีการใช้งานต้องควรเปลี่ยนรหัสผ่านเป็นระยะ ๆ อย่างน้อยทุก ๆ 90 วัน ในฐานะผู้ใช้งานขององค์กรเราก็ต้องปฏิบัติตาม แต่องค์กรควรพิจารณาข้อเสนอแนะที่ไม่บังคับให้ผู้ใช้ต้องเปลี่ยนรหัสผ่านบ่อย ๆ แต่ให้เปลี่ยนเฉพาะในกรณีที่จำเป็น เช่น พบว่าข้อมูลรั่วไหล หรือพบการล็อกอินที่ผิดปกติ

3. ระมัดระวังการใส่รหัสผ่านบนเครื่องคอมพิวเตอร์สาธารณะหรือเครื่องคอมพิวเตอร์ของบุคคลอื่น

4. ควรตั้งรหัสผ่านสำหรับการใช้งานกับบัญชีธนาคารออนไลน์ ไม่ซ้ำกับบัญชีเว็บ อีเมล เว็บเกม หรือแม้กระทั่งเว็บเครือข่ายสังคมออนไลน์

4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

4.2 คำแนะนำในการพิสูจน์ตัวตนด้วยรหัสผ่าน



NIST ได้ให้คำแนะนำการใช้พิสูจน์ตัวตนด้วยรหัสผ่านเมื่อผู้ใช้ทำการล็อกอิน ดังนี้

1. เปิดใช้งาน “แสดงรหัสผ่านขณะพิมพ์” ควรเปิดให้มีฟีเจอร์ “แสดงรหัสผ่านขณะพิมพ์” เพื่อเพิ่มโอกาสให้ผู้ใช้พิมพ์รหัสผ่านยาว ๆ ได้ถูกต้องในทีเดียว
2. เปิดให้ “วาง” รหัสผ่านในช่องที่ต้องกรอกได้ ยิ่งการใส่รหัสผ่านทำได้ง่าย ผู้ใช้ยังมีแนวโน้มที่จะตั้งรหัสผ่านยาวและยากมากยิ่งขึ้น การเปิดให้ “คัดลอก” และ “วาง” รหัสผ่านในช่องที่ต้องกรอกได้จึงเป็นผลดีมากกว่า
3. ใช้การป้องกันรหัสผ่านรวดเร็ว ต้องมีการตรวจสอบรหัสผ่านใหม่กับรายการแบล็กลิสต์ เช่นคำในพจนานุกรม คำที่ใช้ตัวอักษรเรียงกัน คำที่ใช้เป็นชื่อต่าง ๆ ข้อความที่มักใช้บ่อย หรือรหัสผ่านที่เคยหลุดออกมาสู่สาธารณะ การใช้เครื่องมือตรวจสอบรหัสผ่านที่เคยรวดเร็วก็เป็นทางเลือกที่ช่วยให้การตั้งรหัสผ่านใหม่มีความมั่นคงปลอดภัยมากยิ่งขึ้น



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

6. ใช้การพิสูจน์ตัวตนแบบ 2 ปัจจัย (2-Factor Authentication: 2FA) หรือตรวจสอบสิทธิ์แบบหลายปัจจัยได้ (Multi-factor authentication: MFA) ใช้การยืนยันตัวตน 2 จาก 3 ปัจจัยต่อไปนี้เพื่อทำการพิสูจน์ตัวตน

- 1) สิ่งที่คุณรู้ (Something you know) เช่น รหัสผ่าน หรือพิน
- 2) สิ่งที่คุณมี (Something you have) เช่น มือถือ หรือโทเคน
- 3) สิ่งที่คุณเป็น (Something you are) เช่น ลายนิ้วมือ หรือสแกนใบหน้า

เช่น ใช้รหัสผ่าน (สิ่งที่คุณรู้) และใช้รหัสผ่านครั้งเดียว (One Time Password: OTP) ผ่านมือถือ (สิ่งที่คุณมี) หรือลายนิ้วมือ (สิ่งที่คุณเป็น) ในการเข้าใช้งาน ยิ่งใช้หลายปัจจัยยิ่งมีความมั่นคงปลอดภัยโดย อนุญาตให้ตั้งรหัสผ่านได้ต่ำสุด 8 ตัวอักษร แต่ถ้าไม่เปิดใช้ MFA ควรกำหนดให้ตั้งรหัสผ่านที่มีความยาวไม่ต่ำกว่า 14 ตัวอักษร

นอกจากนี้ควรใช้การพิสูจน์ตัวตนแบบ 2FA เพื่อปกป้องข้อมูลส่วนบุคคลที่สามารถเข้าถึงได้แบบออนไลน์



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

4.3 ภัยร้ายจาก "ฟิชชิง" (Phishing)

เป็นการหลอกลวงในรูปแบบการปลอมแปลง อีเมล หรือข้อความที่สร้างขึ้นหลอกให้ผู้ใช้งานเปิดเผยข้อมูลทางการเงินหรือข้อมูลส่วนตัวต่าง ๆ เช่น บัญชีใช้งานและรหัสผ่าน (Username/Password), ข้อมูลบัตรเครดิตหรือหมายเลขบัตรประจำตัวอื่น ๆ โดยอ้างว่าที่ผู้ใช้งานอาจเคยติดต่อ เช่น เว็บไซต์ธนาคารเว็บไซต์ ที่เคยซื้อขายสินค้าบริการยืนยันข้อมูลส่วนตัวให้เป็นปัจจุบัน โดยอ้างให้เข้าใจผิดว่าหากไม่ดำเนินการอาจก่อให้เกิดความเสียหายต่าง ๆ โดยคนร้ายมักใส่ hyperlink ให้ดูเหมือน URL ขององค์กรนั้น ๆ โดยเป็นเว็บไซต์ปลอม (Spoofed Website) เพื่อหลอกให้กรอกข้อมูลลงไป

วิธีป้องกัน ไม่ควรใช้ลิงก์ในอีเมลเพื่อเข้าใช้งานยังเว็บไซต์ และหากผู้ใช้งานสงสัยควรจะติดต่อทางโทรศัพท์ไปยังองค์กรนั้น ๆ โดยตรงและควรใช้งานผ่านการพิมพ์ URL ขององค์กรนั้นใหม่ทุกครั้งที่ใช้งาน

4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

4.4 วิธีป้องกันการถูกขโมยข้อมูลส่วนบุคคล



1. ตรวจสอบรายการใช้งานอยู่เสมอในการใช้งานเว็บไซต์ต่าง ๆ ที่ต้องกรอกข้อมูลและรหัสผ่านก่อนใช้งานทุกครั้ง จะมีข้อมูลประวัติการใช้งานของเรา จึงควรตรวจสอบประวัติข้อมูลการใช้งานเพื่อสังเกตความผิดปกติ
2. หลีกเลี่ยงการใช้ข้อมูลส่วนตัวที่มากเกินไปในการทำธุรกรรมทางเว็บไซต์ควรหลีกเลี่ยงการให้ข้อมูลส่วนตัวเกินจำเป็น เนื่องจากหากให้ข้อมูลส่วนตัวของเรามากก็就会有ความเสี่ยงมากขึ้น
3. ระมัดระวังอีเมลที่สอบถามข้อมูลส่วนบุคคล หากได้รับอีเมลจากบุคคลที่ไม่รู้จัก สอบถามเกี่ยวกับข้อมูลส่วนบุคคล ไม่ควรตอบข้อมูลส่วนบุคคลกลับทางอีเมล และหากอีเมลดังกล่าวมาจากธนาคารหรือองค์กรที่เราเคยใช้บริการ ก็ควรติดต่อสอบถามทางโทรศัพท์เพื่อให้มั่นใจว่าไม่ถูกหลอกสอบถามข้อมูลส่วนบุคคลทางอีเมล



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

4. ควรระมัดระวัง Wi-Fi Hotspot ปลอม ซึ่งเป็นภัยคุกคามที่มีหลักการคล้ายกับ Phishing ปัจจุบันมีผู้ใช้งานอุปกรณ์มือถือมากขึ้น คนร้ายจึงทำการปล่อยสัญญาณ Wi-Fi ฟรีในที่สาธารณะ ซึ่งคนร้ายจะเตรียมเว็บไซต์ปลอมสำหรับการใช้บริการอินเทอร์เน็ตฟรี ทำให้คนร้ายนำเอาข้อมูลที่ได้ไปทดลองดูมัลแวร์กับเว็บไซต์ต่าง ๆ ซึ่งอาจจะนำความเสียหายมาสู่ผู้เข้าใจผิดได้

5. ทำลายเอกสารที่มีข้อมูลส่วนบุคคล ควรระมัดระวังเอกสารหรือจดหมายส่วนตัวที่ระบุข้อมูลส่วนบุคคล เช่น หมายเลขบัตรเครดิต บัญชีผู้ใช้งาน หรือแม้แต่การแจ้งรหัสผ่านทางจดหมาย ควรเก็บรักษาในที่ปลอดภัยจากบุคคลภายนอก และหากไม่มีความจำเป็นต้องเก็บไว้เป็นหลักฐานหรือช่วยเตือนความจำเป็นควรทำลายในลักษณะไม่สามารถนำกลับมาอ่านใหม่ได้ เช่น การย่อยทำลายเอกสารให้เป็นชิ้นเล็ก เป็นต้น



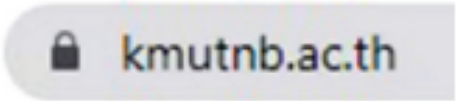
4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

4.5 วิธีป้องกันการถูกฉ้อโกงทางเว็บไซต์

1. ศึกษาข้อมูล ความน่าเชื่อถือในสินค้าและผู้ขาย อาจใช้วิธีการส่งอีเมล หรือโทรศัพท์ไปสอบถามรายละเอียดสินค้าหรือบริการ เพื่อสังเกตความรวดเร็วในการตอบกลับและการมีตัวตนเองของธุรกิจนั้น ๆ และทำการค้นหา รีวิวเพิ่มเติมเกี่ยวกับสินค้า บริการหรือผู้ขายรายนั้น ๆ ในอินเทอร์เน็ต
2. การจ่ายชำระเงินผ่านระบบควรสังเกตว่าระบบดังกล่าวมีความมั่นคงปลอดภัยหรือเข้ารหัสเสมอหรือไม่ เช่น อาจสังเกตจาก https หรือเครื่องหมายแม่กุญแจที่ปรากฏบนเว็บไซต์ที่ใช้งานอยู่

4. หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

สัญลักษณ์ https เมื่อเปิดจากเว็บเบราว์เซอร์ที่แตกต่างกัน	เว็บเบราว์เซอร์ที่ใช้งาน
	Google Chorme
	Mozilla Firefox
	Microsoft Edge

ตารางที่ 7.1 สัญลักษณ์ https เมื่อเปิดจากเว็บเบราว์เซอร์ที่แตกต่างกัน



4.

หลักการป้องกันข้อมูลส่วนตัวจากการใช้งานเครื่องคอมพิวเตอร์

3. หากสามารถเลือกชำระเงินแบบบัตรเดบิต (Debit Card) หรือบัตรเครดิต (Credit Card) ก็ควรเลือกชำระใช้บัตรเครดิตเสมอ เนื่องจากหากมีปัญหาในสินค้าที่สั่งซื้อ เจ้าของบัตรอาจจะสามารถปฏิเสธการชำระเงินได้ ในขณะที่กรณีบัตรเดบิตมีความเสี่ยงกว่าเนื่องจากจะถูกหักเงินจากบัญชีเงินฝากธนาคารทันทีที่ชำระผ่านบัตรเดบิต รวมทั้งควรตรวจสอบใบแจ้งหนี้ทุกรอบบัญชี เพื่อตรวจสอบรายการที่อาจผิดปกติ
4. ศึกษาว่าเว็บไซต์ที่กำลังจะซื้อสินค้าหรือบริการดังกล่าวมีกฎระเบียบเกี่ยวกับการรับประกันความพึงพอใจในสินค้าหรือไม่ มีนโยบายการรับคืนและคืนเงินทันทีเมื่อลูกค้าแจ้งความไม่พอใจในสินค้าหรือไม่
5. ใช้ความระมัดระวังอย่างสูงหากพบการเสนอขายสินค้าบนเว็บไซต์ที่ราคาขายต่ำกว่าความเป็นจริง อย่างมาก รวมถึงสินค้าหรือบริการที่วัดอ้างสรรพคุณเกินจริง

การติดตั้งระบบปฏิบัติการเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

การที่เราจะใช้ประโยชน์จากคอมพิวเตอร์ได้ นอกจากจะมีระบบปฏิบัติการที่เหมาะสมแล้วสิ่งที่สำคัญไม่น้อยกว่ากัน คือ โปรแกรมประยุกต์สำหรับการปฏิบัติงาน ซึ่งนอกจากผู้ใช้จะต้องเลือกโปรแกรมประยุกต์ให้เหมาะสมกับงานของตนเองแล้ว สิ่งที่ต้องคำนึงถึงโดยเฉพาะการใช้งานโปรแกรมประยุกต์บนระบบเครือข่ายก็คือ ความมั่นคงปลอดภัยของระบบงานและข้อมูลที่ถูกรับส่งหรือถูกบันทึกไว้บนระบบเครือข่าย เพราะข้อมูลเหล่านี้ อาจจะเป็นความลับทางการค้า รหัสผ่านการทำธุรกรรมการเงิน ซึ่งหากหลุดไปยังบุคคลที่ไม่ประสงค์ดีก็จะสร้างความเสียหายแก่ผู้ใช้และองค์กรอย่างมหาศาล





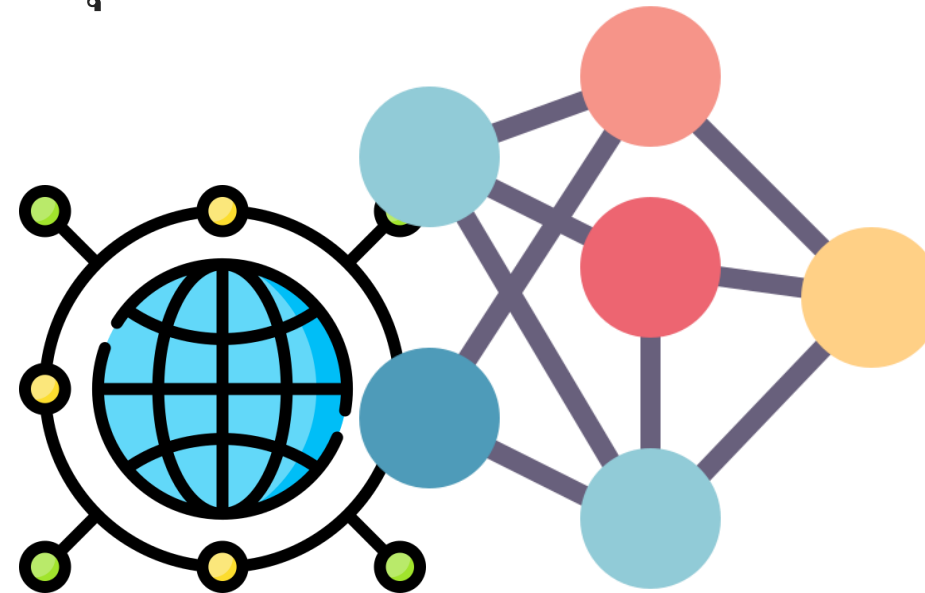
โปรแกรมการตลาดประโยชน์ บนเครือข่ายคอมพิวเตอร์



โปรแกรมลดประโยชน์บนเครือข่ายคอมพิวเตอร์

1. ความหมายของโปรแกรมยูทิลิตี้บนเครือข่าย

โปรแกรมยูทิลิตี้ (Utility program) หรือเรียกว่าโปรแกรมลดประโยชน์ หมายถึง โปรแกรมที่ใช้สำหรับอำนวยความสะดวกให้กับผู้ใช้ในการทำงานการบริหารจัดการเครือข่าย และระบบคอมพิวเตอร์ สามารถช่วยให้ระบบเครือข่ายหรือการใช้งานมีประสิทธิภาพเพิ่มขึ้น สำหรับโปรแกรมยูทิลิตี้ที่ช่วยการทำงานในระบบเครือข่ายมีหลายประเภททั้งบนเครื่องคอมพิวเตอร์ และอุปกรณ์พกพาอย่างสมาร์ทโฟนหรือแท็บเล็ต



โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

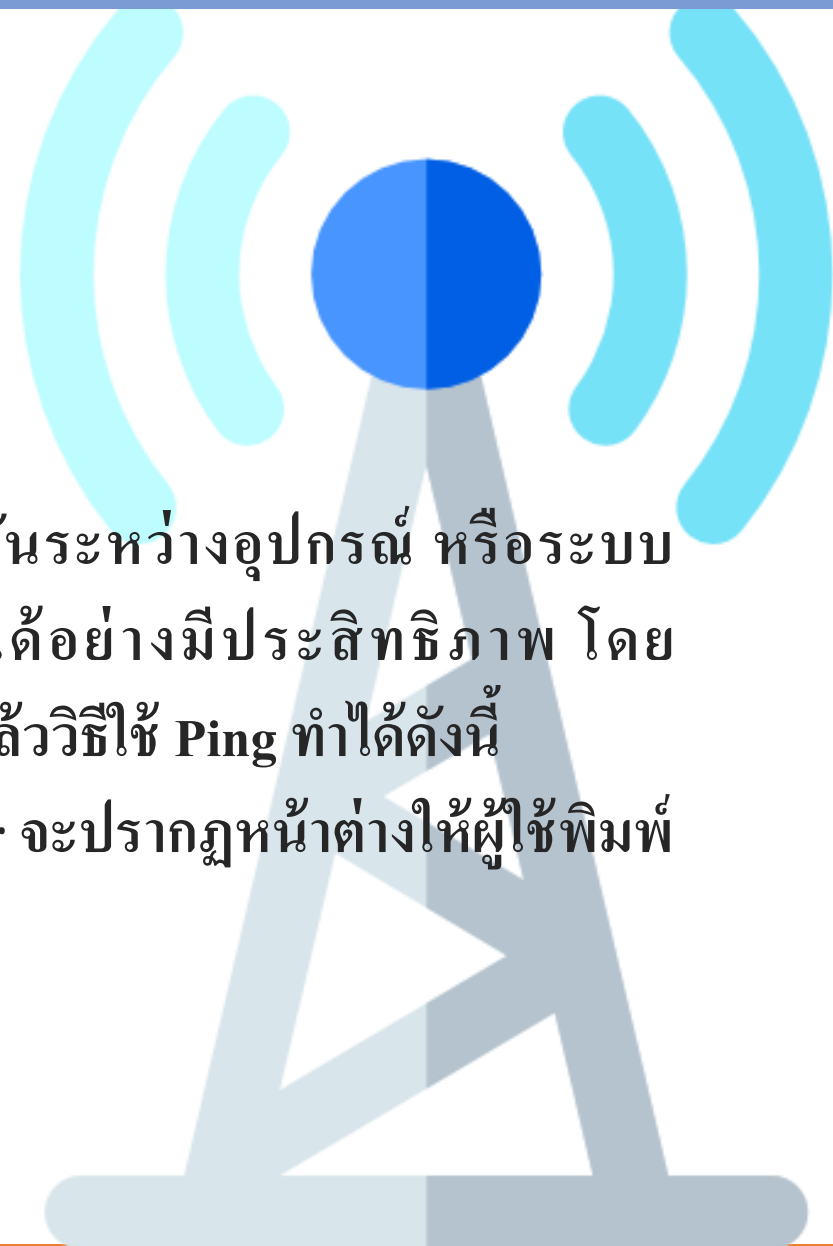
2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

มีทั้งที่ติดมากับระบบปฏิบัติการและที่ต้องติดตั้งเพิ่ม

2.1 Ping

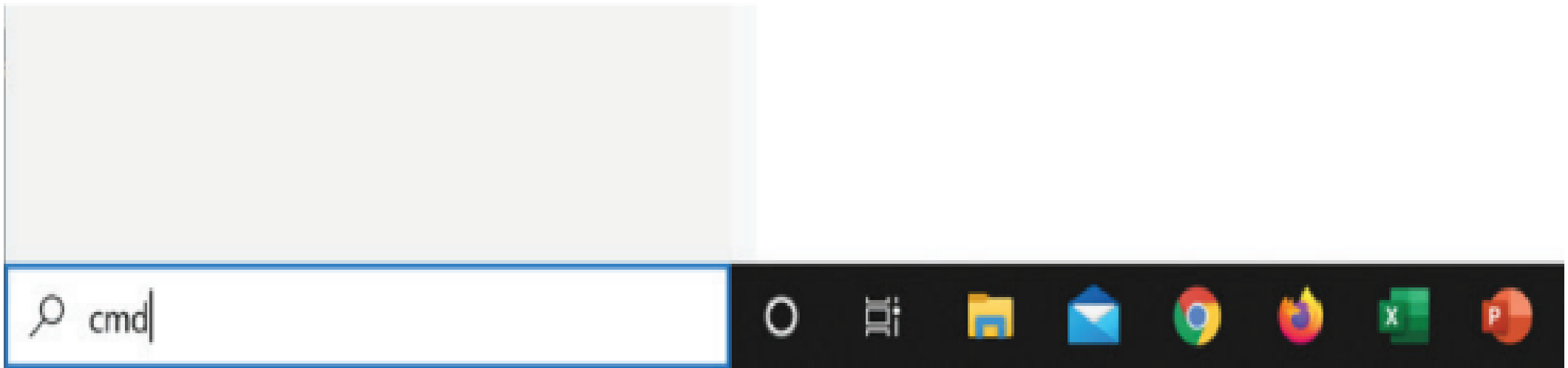
เป็นโปรแกรมคำสั่งพื้นฐานที่ไว้ใช้ตรวจสอบการเชื่อมต่อกันระหว่างอุปกรณ์ หรือระบบเครือข่ายในส่วนของความเร็วและเส้นทางการรับ - ส่งข้อมูลได้อย่างมีประสิทธิภาพ โดย Microsoft.Windows ทุกเครื่องจะมีโปรแกรมนี้เป็นโปรแกรมพื้นฐานอยู่แล้ววิธีใช้ Ping ทำได้ดังนี้

พิมพ์คำว่า cmd ในช่อง search ของ Window แล้วกดปุ่ม Enter จะปรากฏหน้าต่างให้ผู้ใช้พิมพ์คำสั่งได้



โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

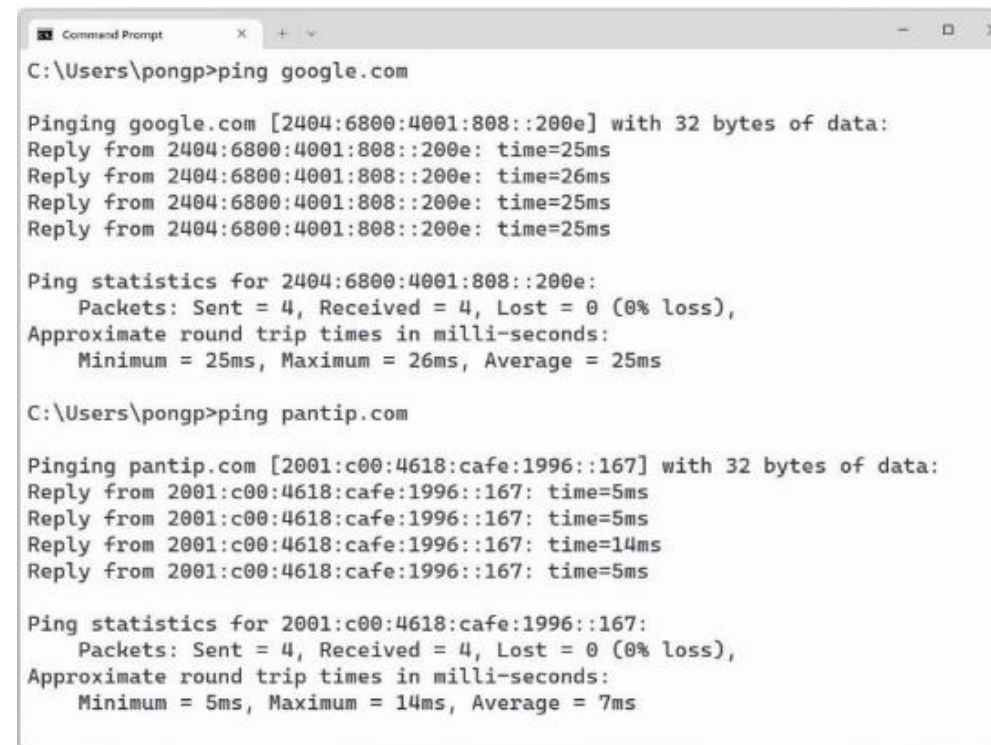


รูปที่ 8.1 การค้นหาโปรแกรมคำสั่งพื้นฐานที่ใช้ตรวจสอบการเชื่อมต่อกันระหว่างอุปกรณ์

โปรแกรมตรวจประโชยน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

ในหน้าต่างคำสั่งให้พิมพ์ Ping ตามด้วย IP address หรือชื่อเว็บไซต์ปลายทางที่เราต้องการจะตรวจสอบ เช่น ping www.google.com แล้ว กด Enter หากไม่มีอะไรผิดปกติ ระบบเครือข่ายใช้งานได้ระบบจะรายงานผลความเร็วของการเชื่อมต่อ จำนวน 4 ครั้ง ซึ่งจากภาพจะเห็นได้ว่าการเข้าถึง pantip.com ใช้เวลาประมาณ 7 ms (ms = หนึ่งในพันวินาที) ในขณะที่ เข้า goole.com ใช้เวลาประมาณ 25 ms ซึ่งช้ากว่า



```
C:\Users\pong>ping google.com

Pinging google.com [2404:6800:4001:808::200e] with 32 bytes of data:
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms

Ping statistics for 2404:6800:4001:808::200e:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 26ms, Average = 25ms

C:\Users\pong>ping pantip.com

Pinging pantip.com [2001:c00:4618:cafe:1996::167] with 32 bytes of data:
Reply from 2001:c00:4618:cafe:1996::167: time=5ms
Reply from 2001:c00:4618:cafe:1996::167: time=5ms
Reply from 2001:c00:4618:cafe:1996::167: time=14ms
Reply from 2001:c00:4618:cafe:1996::167: time=5ms

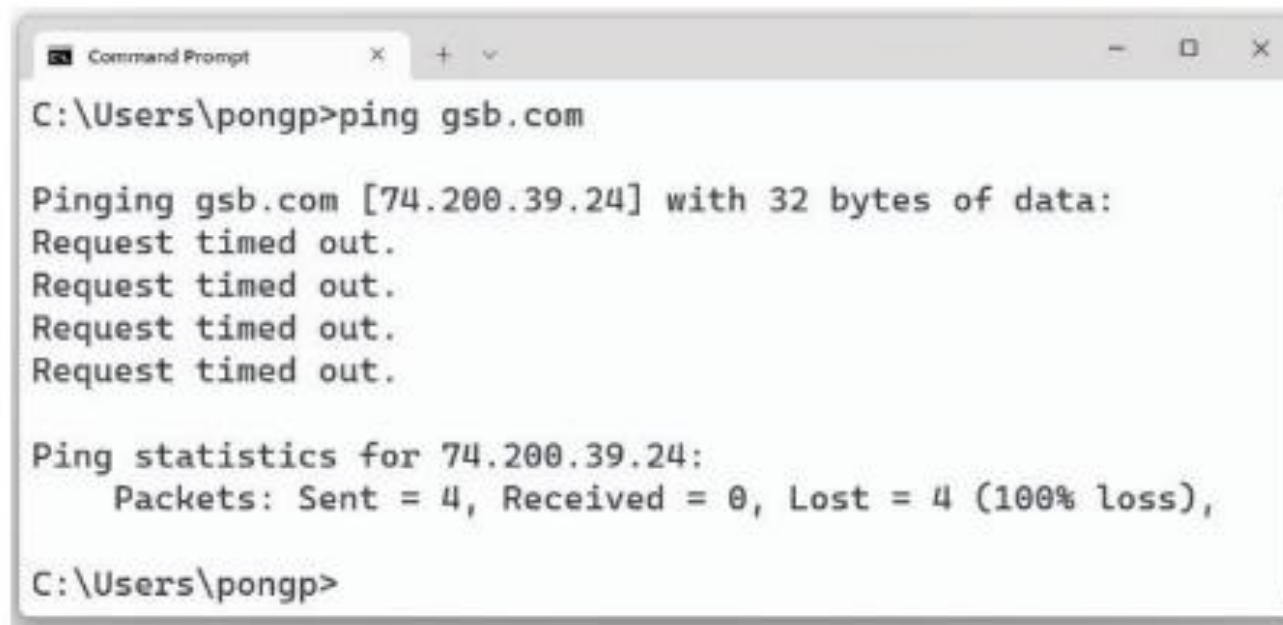
Ping statistics for 2001:c00:4618:cafe:1996::167:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 14ms, Average = 7ms
```

รูปที่ 8.2 ระบบรายงานผลความเร็วของการเชื่อมต่อ

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

กรณีที่เครือข่ายมีปัญหาหรือผู้ให้บริการปลายทางไม่พร้อมให้บริการ ระบบจะแสดงสถานะกลับมาเป็น timed out ดังนี้



```
Command Prompt
C:\Users\pongp>ping gsb.com

Pinging gsb.com [74.200.39.24] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 74.200.39.24:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\pongp>
```

รูปที่ 8.3 กรณีเครือข่ายมีปัญหาระบบจะแสดงสถานะกลับมา

โปรแกรมตรวจประโชยน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยู่ทิลิตี่สำหรับตรวจสอบระบบเครือข่าย

```
C:\Users\pong>ping /?

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
          [-r count] [-s count] [[-j host-list] | [-k host-list]]
          [-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
          [-4] [-6] target_name

Options:
  -t          Ping the specified host until stopped.
              To see statistics and continue - type Control-Break;
              To stop - type Control-C.
  -a          Resolve addresses to hostnames.
  -n count    Number of echo requests to send.
  -l size     Send buffer size.
  -f          Set Don't Fragment flag in packet (IPv4-only).
  -i TTL      Time To Live.
  -v TOS      Type Of Service (IPv4-only. This setting has been deprecated
              and has no effect on the type of service field in the IP
              Header).
  -r count    Record route for count hops (IPv4-only).
  -s count    Timestamp for count hops (IPv4-only).
  -j host-list Loose source route along host-list (IPv4-only).
  -k host-list Strict source route along host-list (IPv4-only).
  -w timeout  Timeout in milliseconds to wait for each reply.
  -R          Use routing header to test reverse route also (IPv6-only).
              Per RFC 5095 the use of this routing header has been
              deprecated. Some systems may drop echo requests if
              this header is used.
  -S srcaddr  Source address to use.
  -c compartment Routing compartment identifier.
  -p          Ping a Hyper-V Network Virtualization provider address.
  -4          Force using IPv4.
  -6          Force using IPv6.
```

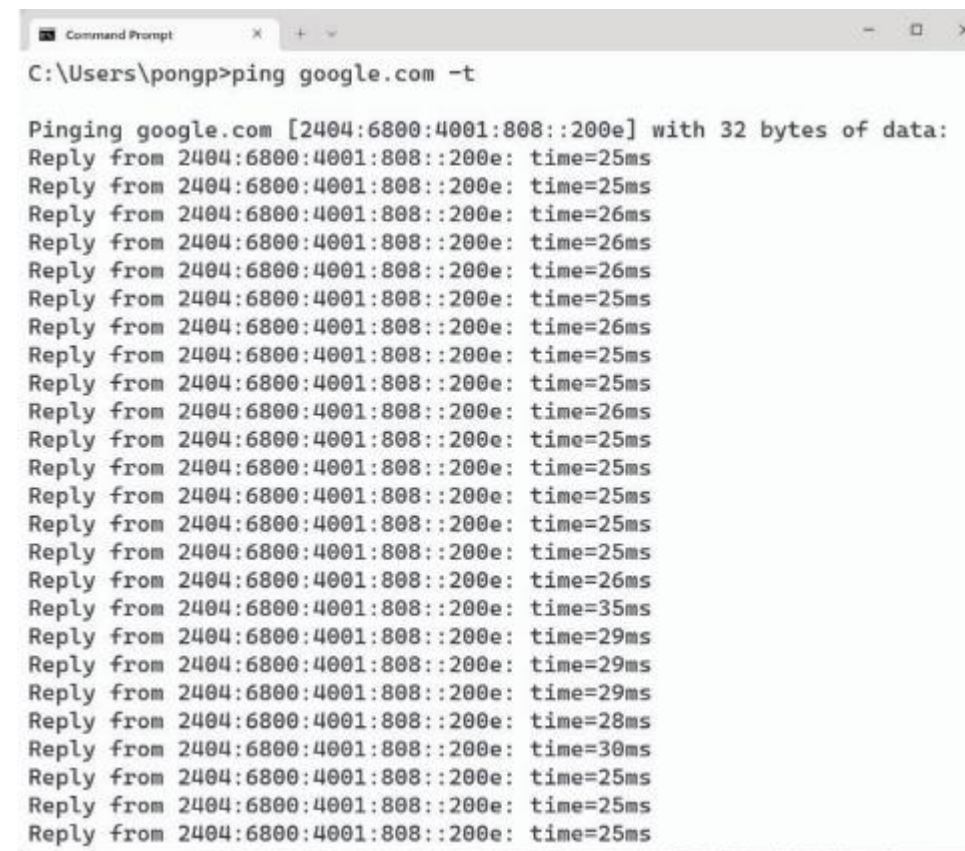
นอกจากนี้ คำสั่ง Ping ยังมีตัวเลือกเสริมต่าง ๆ (Option) เพื่อเพิ่มความสามารถในตรวจสอบระบบเครือข่ายให้มากขึ้น เช่น การใช้ ping ตามด้วยคำสั่ง -t หมายถึงให้ส่งข้อมูลทดสอบไปเรื่อย เพื่อตรวจสอบว่าสัญญาณในระบบเครือข่ายมีความเร็วสม่ำเสมอหรือไม่

รูปที่ 8.4 การใช้คำสั่ง ping ตามด้วยคำสั่ง -t

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

การใช้คำสั่ง `ping xxx.xxx.xxx.xxx -t` (xxx คือ IP address หรือเว็บไซต์ปลายทาง) แล้วพบว่า สัญญาณไม่เสถียร เวลาช้าเร็วแตกต่างกันมาก จนถึงขั้นหยุดทำงานในบางช่วง (Request Timed Out) ซึ่งหากเจอปัญหานี้ เราสามารถใช้ คำสั่ง `Tracert` ในการค้นหาสาเหตุเบื้องต้นของปัญหาได้



```
Command Prompt
C:\Users\pong>ping google.com -t

Pinging google.com [2404:6800:4001:808::200e] with 32 bytes of data:
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=26ms
Reply from 2404:6800:4001:808::200e: time=35ms
Reply from 2404:6800:4001:808::200e: time=29ms
Reply from 2404:6800:4001:808::200e: time=29ms
Reply from 2404:6800:4001:808::200e: time=29ms
Reply from 2404:6800:4001:808::200e: time=28ms
Reply from 2404:6800:4001:808::200e: time=30ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
Reply from 2404:6800:4001:808::200e: time=25ms
```

รูปที่ 8.5 การใช้คำสั่ง `ping xxx.xxx.xxx.xxx -t`

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

2.2 Tracert

มีรูปแบบใช้งานคล้ายกับคำสั่ง ping โดยพิมพ์คำว่า cmd ในช่อง search ของ Window แล้วกดปุ่ม Enter จะปรากฏหน้าต่างให้ผู้ใช้พิมพ์คำสั่งได้ จากนั้นพิมพ์ tracert ตามด้วยเว็บไซต์หรือ IP address ปลายทางที่ต้องการตรวจสอบ โปรแกรมจะรายงานเส้นทางและระยะเวลาที่ข้อมูลผ่านไปแต่ละจุดอย่างละเอียด เพื่อให้เราทราบว่าข้อมูลมีความล่าช้า หรือสัญญาณขาดหายไปจุดใด

หมายเหตุ

tracert จะทำงานได้กับการเชื่อมต่ออุปกรณ์ในเส้นทางไม่เกิน 30 จุด

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

```
Command Prompt
C:\Users\pongp>tracert google.com

Tracing route to google.com [2404:6800:4001:808::200e]
over a maximum of 30 hops:

  1    8 ms    7 ms    7 ms  2001:fb1:fc0:d3:39cb:1b1d:9b93:cff0
  2    7 ms    8 ms    7 ms  2001:fb1:fe0:d::6d
  3    5 ms    5 ms    4 ms  2001:fb1:fe0:d::6c
  4   66 ms    6 ms    5 ms  2001:fb0:1099:99::301
  5    8 ms    8 ms    7 ms  2001:fb0:1099:99::360
  6    8 ms    8 ms    8 ms  2001:fb0:1:19:171:102:254:65
  7    8 ms    7 ms    6 ms  2001:fb0:1:25:171:102:254:232
  8    *      *      *     Request timed out.
  9    8 ms    *      *     2405:4000:800:1::2
 10   26 ms   26 ms   26 ms  2406:4000:900:3::167
 11   27 ms   26 ms   26 ms  2001:4860:1:1::3a0
 12   26 ms   26 ms   27 ms  2404:6800:8078::1
 13   27 ms   27 ms   27 ms  2001:4860:0:1::fee
 14   29 ms   27 ms   27 ms  2001:4860:0:116a::c
 15   31 ms   28 ms   27 ms  2001:4860::1c:4000:ecba
 16   27 ms   26 ms   26 ms  2001:4860:0:1::1603
 17   25 ms   25 ms   25 ms  kul08s12-in-x0e.1e100.net [2404:6800:4001:808::200e]

Trace complete.
```

รูปที่ 8.6 การใช้คำสั่ง tracert

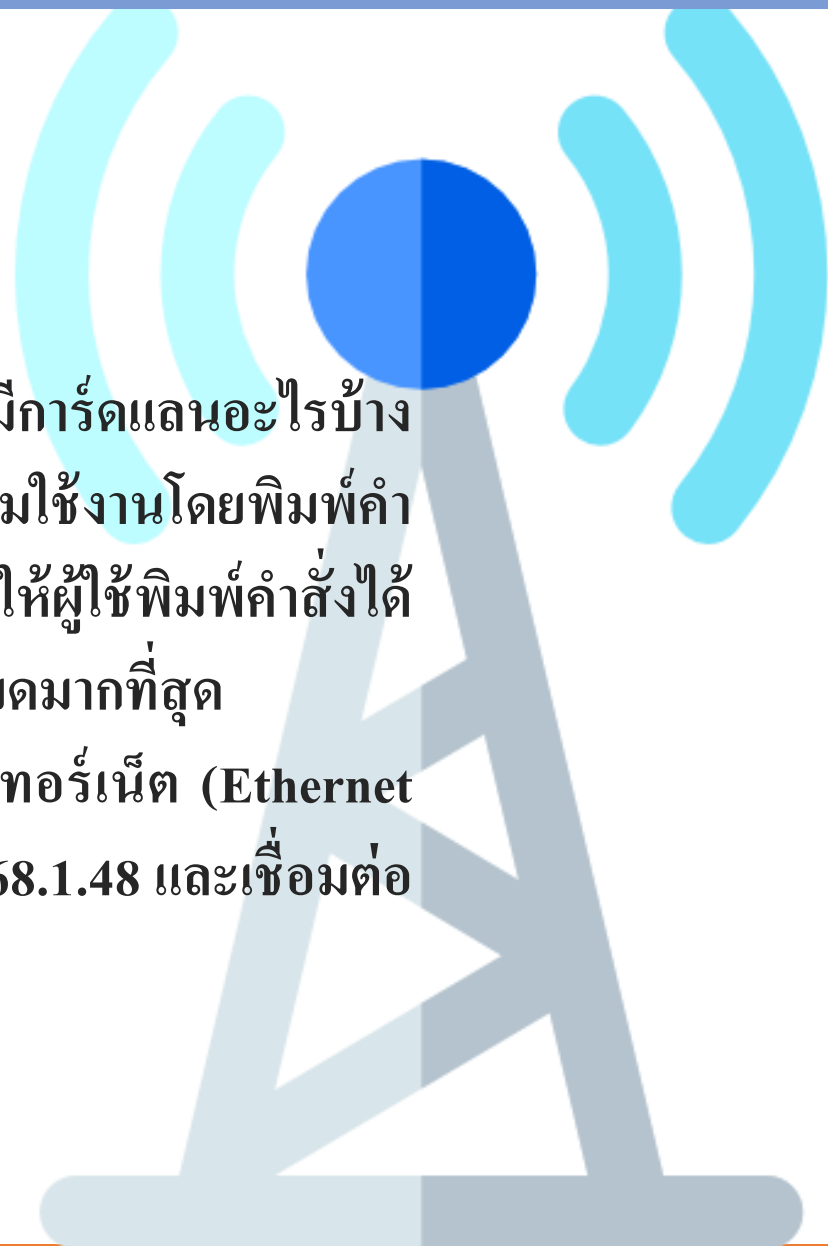
โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

2.3 คำสั่ง ipconfig

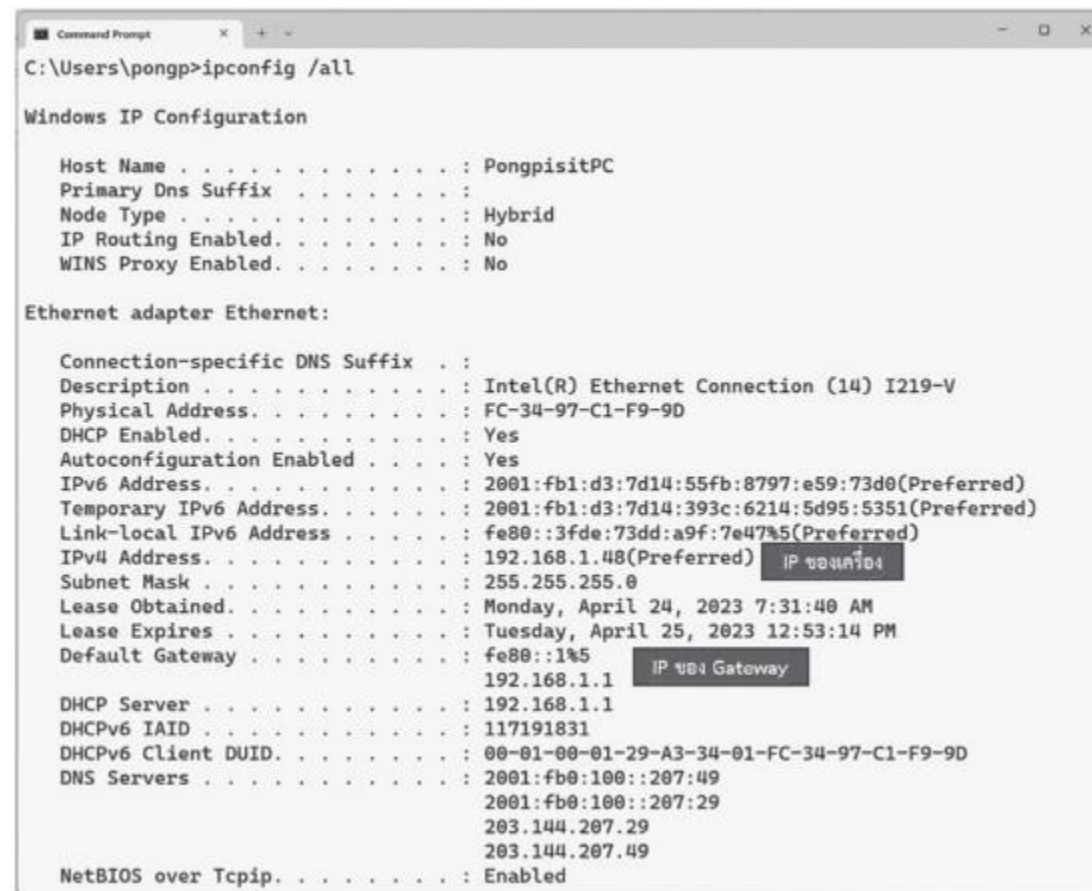
เป็นคำสั่งที่ใช้เรียกดูข้อมูลเกี่ยวกับคอมพิวเตอร์ที่เราใช้งานอยู่ว่ามีการ์ดแลนอะไรบ้าง มีการเชื่อมต่อหรือเปิดใช้งานอยู่หรือไม่ และมีการกำหนดค่าอะไรไว้ การเริ่มใช้งานโดยพิมพ์คำว่า cmd ในช่อง search ของ Window แล้วกดปุ่ม Enter จะปรากฏหน้าต่างให้ผู้ใช้พิมพ์คำสั่งได้ จากนั้นพิมพ์ ipconfig หรือพิมพ์ ipconfig /all เพื่อให้ระบบแสดงรายละเอียดมากที่สุด

จากตัวอย่างจะเห็นว่าคอมพิวเตอร์เครื่องนี้ มีการ์ดแลนแบบอีเทอร์เน็ต (Ethernet adapter Ethernet) หนึ่งตัวเชื่อมต่อใช้งานอยู่และมี IP address คือ 192.168.1.48 และเชื่อมต่อกับอินเทอร์เน็ตผ่าน Default Gateway ที่มี IP address 192.168.1.1



โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย



```
Command Prompt
C:\Users\pong>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PongpisitPC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . :
Description . . . . . : Intel(R) Ethernet Connection (14) I219-V
Physical Address. . . . . : FC-34-97-C1-F9-9D
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2001:fb1:d3:7d14:55fb:8797:e59:73d0(Preferred)
Temporary IPv6 Address. . . . . : 2001:fb1:d3:7d14:393c:6214:5d95:5351(Preferred)
Link-local IPv6 Address . . . . . : fe80::3fde:73dd:a9f:7e47%5(Preferred)
IPv4 Address. . . . . : 192.168.1.48(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, April 24, 2023 7:31:40 AM
Lease Expires . . . . . : Tuesday, April 25, 2023 12:53:14 PM
Default Gateway . . . . . : fe80::1%5
                             192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 117191831
DHCPv6 Client DUID. . . . . : 00-01-00-01-29-A3-34-01-FC-34-97-C1-F9-9D
DNS Servers . . . . . : 2001:fb0:100::207:49
                             2001:fb0:100::207:29
                             203.144.207.29
                             203.144.207.49
NetBIOS over Tcpip. . . . . : Enabled
```

รูปที่ 8.7 ตัวอย่างคอมพิวเตอร์ที่มี Wireless lan card หนึ่งตัวเชื่อมต่อใช้งานอยู่

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

2.4 โปรแกรมตรวจความเร็วอินเทอร์เน็ต

หรือที่เรียกกันสั้น ๆ ว่า Speed Test ซึ่งมีให้ใช้ทั้งที่เป็นแอปพลิเคชันบนมือถือ และผ่านเว็บเบราว์เซอร์ตัวอย่างแอปพลิเคชัน ได้แก่ Speedtest by Ookla หรือเข้าไปที่เว็บไซต์ Speedtest.net ซึ่งโปรแกรมเหล่านี้จะสามารถทดสอบความเร็วอินเทอร์เน็ต ทั้งจากการใช้สัญญาณโทรศัพท์มือถือและทดสอบผ่านสัญญาณจากผู้ให้บริการผ่านทางสาย เช่น DSL, Fiber optic, เครือข่ายแลน หรือสัญญาณ Wi-Fi ที่ติดตั้งตามสำนักงาน หรือผ่านสัญญาณมือถือ อย่างไรก็ตาม การทดสอบความเร็วอินเทอร์เน็ตขึ้นอยู่กับหลายปัจจัย ซึ่งผู้ทดสอบจะต้องทำความเข้าใจให้ดีก่อนที่จะแปลผลการทดสอบ โดยเฉพาะการทดสอบความเร็วผ่าน Wi-Fi เช่น

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

1. ความถี่และมาตรฐานสัญญาณ Wi-Fi ที่ใช้ในการทดสอบ ถ้าเป็น Wi-Fi 2.4 GHz ถึงแม้จะสามารถทำความเร็วสูงสุดได้ที่ 450 Mbps หรือ 600 Mbps ในขณะที่ Wi-Fi 5 GHz รองรับความเร็วสูงสุด 1,300 Mbps แต่ทั้งหมดเป็นผลทดสอบจากห้องทดลอง (Lab) ที่ไม่มีสัญญาณรบกวนและระยะทางระหว่างอุปกรณ์จะใกล้กันมาก โดยอุปกรณ์รับส่งจะต้องมีประสิทธิภาพเทียบเท่ากัน ซึ่งในทางปฏิบัติแทบจะเป็นไปไม่ได้โดยเฉพาะกับอุปกรณ์ขนาดเล็ก เช่น มือถือ หรือ แม้แต่โน้ตบุ๊ก



โปรแกรมลดประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

2. ความเร็วสูงสุดของอุปกรณ์ที่ใช้ทดสอบอาจจะต่ำกว่าความเร็วที่ผู้ให้บริการส่งมา เช่น การทดสอบกับ อุปกรณ์ขนาดเล็ก เช่น มือถือ มักจะพบว่ามือถือส่วนใหญ่สามารถรับสัญญาณได้ด้วยความเร็วสูงสุดผ่าน Wi-Fi ประมาณ 100-200 Mbps ในขณะที่โน้ตบุ๊กจะทำความเร็วได้ประมาณ 500-600 Mbps สำหรับผู้ที่มีอินเทอร์เน็ตบ้านความเร็วสูงแล้วต้องการใช้งานให้เต็มประสิทธิภาพ ทางเลือกที่เหมาะสมคือ การใช้สายแลนต่อเข้ากับ Gigabit Switch เท่านั้น เนื่องจากมือถือและการ์ดแลนไร้สายส่วนใหญ่ยังไม่รองรับมาตรฐาน 802.11ax หรือ Wi-Fi-6 หรือถ้ารองรับจะมีราคาสูงกว่าทั่วไป



โปรแกรมตรวจประโชยน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย



รูปที่ 8.8 แอปพลิเคชัน Speedtest by Ookla

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

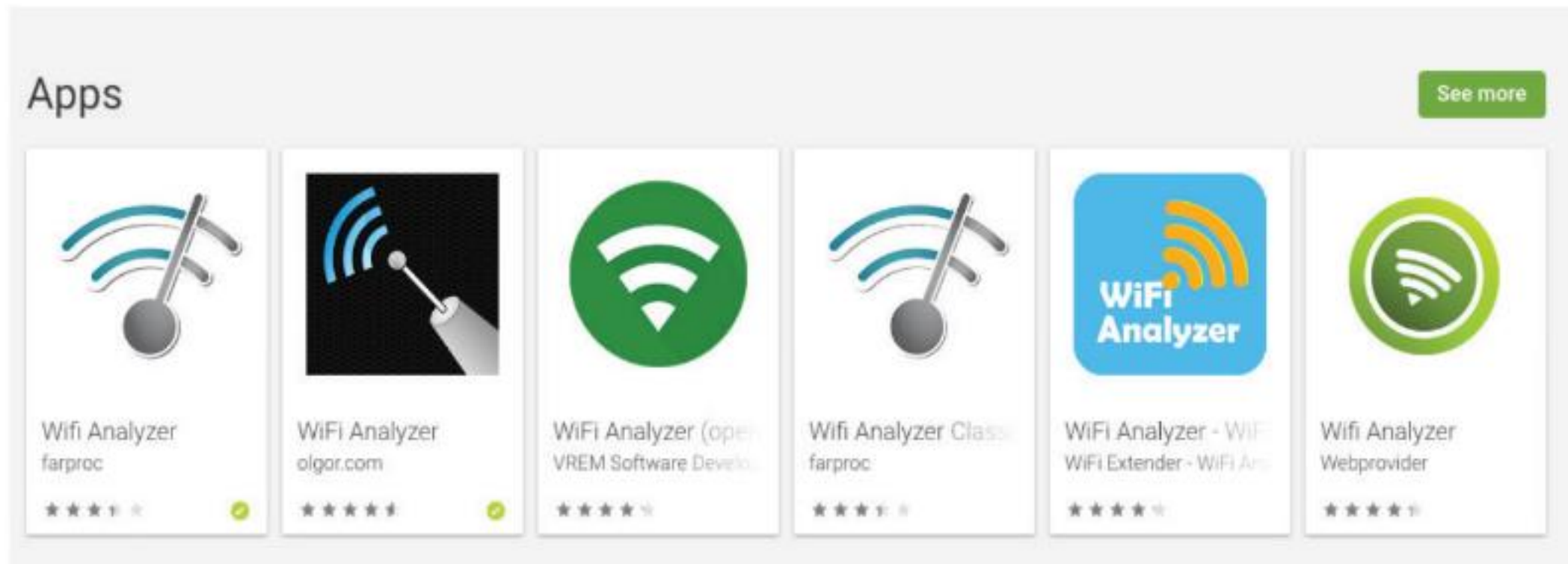
2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

2.5 โปรแกรมสำหรับวิเคราะห์สัญญาณ Wi-Fi (Wi-Fi Analyzer)

ในปัจจุบันสำนักงานและบ้านเรือนส่วนใหญ่จะมีการติดตั้งอุปกรณ์กระจายสัญญาณ Wi-Fi เพื่อใช้งานเนื่องจากสัญญาณ Wi-Fi เป็นคลื่นความถี่ซึ่งในบางพื้นที่ที่มีการติดตั้งอุปกรณ์กระจายสัญญาณเป็นจำนวนมาก มักพบปัญหาเกิดสัญญาณรบกวนกันเนื่องจากใช้ช่องสัญญาณเดียวกัน หาก Wi-Fi เราเตอร์ (Wi-Fi Router) มีระบบที่เปลี่ยนช่องอัตโนมัติสามารถแก้ปัญหาเหล่านี้ได้บ้าง แต่ทางที่ดีผู้ใช้ เจ้าของบ้านหรือผู้ดูแลระบบควรจะทราบและสามารถประเมินสถานะของเครือข่ายไร้สายที่อยู่รอบ ๆ บริเวณที่ใช้งาน อยู่ซึ่งจะช่วยให้สามารถปรับแต่งอุปกรณ์กระจายสัญญาณ Wi-Fi ที่ทำงานอยู่ในบริเวณเดียวกันให้สลับช่องความถี่ใช้งานไม่ให้ทับซ้อนกัน จึงจะทำให้ประสิทธิภาพการทำงานของระบบโดยรวมสูงขึ้นทั้งในแง่ความเร็วและระยะทางรับส่งข้อมูล

โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย



รูปที่ 8.9 โปรแกรมสำหรับวิเคราะห์สัญญาณ Wi-Fi

โปรแกรมลดประโยชน์บนเครือข่ายคอมพิวเตอร์

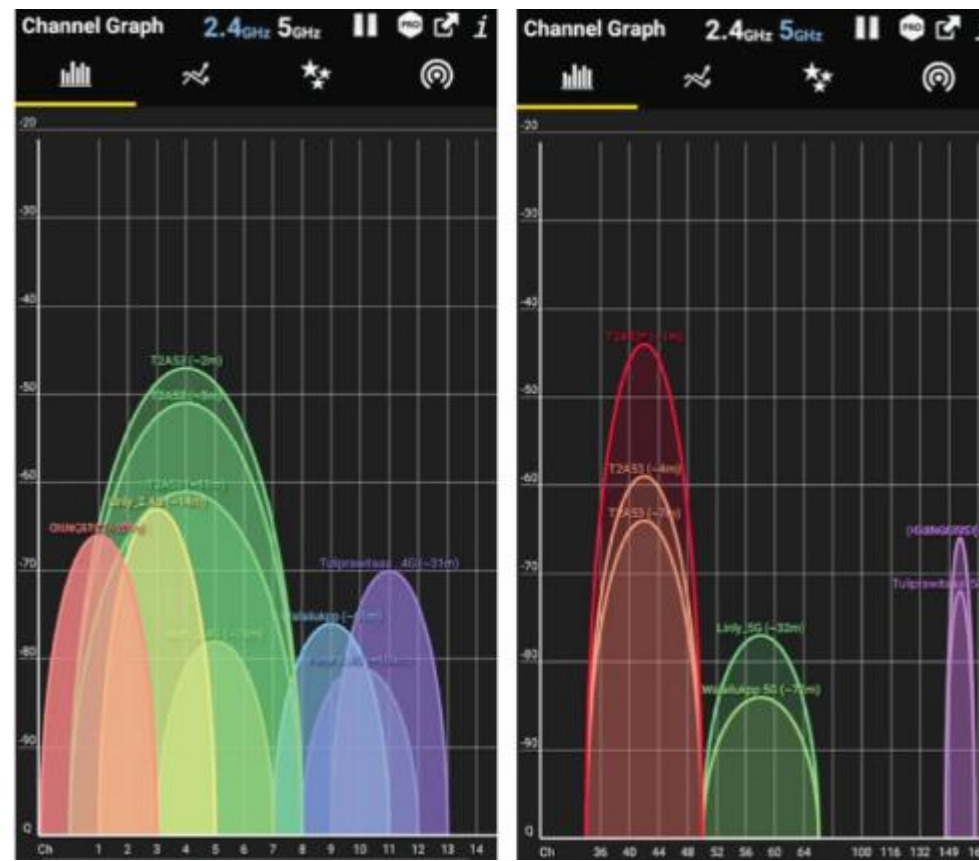
2. โปรแกรมยุติสิทธิ์สำหรับตรวจสอบระบบเครือข่าย

โปรแกรมสำหรับวิเคราะห์สัญญาณ Wi-Fi ส่วนใหญ่จะให้ดาวน์โหลดและใช้งานฟรี โดยโปรแกรมจะมีรายได้จากการโฆษณา เมื่อเปิดใช้งานจะปรากฏหน้าจอแสดงกราฟให้เห็นว่ารอบ ๆ บริเวณนั้นมี Wi-Fi ช่องไหนถูกใช้งานบ้าง และสัญญาณมีการทับซ้อนกันที่ช่องไหน หากพบว่าสัญญาณบริเวณนั้นช่องไหนมีผู้ใช้น้อย เราก็สามารถปรับแต่งอุปกรณ์กระจายสัญญาณ Wi-Fi ให้ไปใช้ช่องนั้นได้



โปรแกรมตรวจประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย



รูปที่ 8.10 ความหนาแน่นของช่องสัญญาณ Wi-Fi จากโปรแกรม Wi-Fi Analyzer

โปรแกรมลดประโยชน์บนเครือข่ายคอมพิวเตอร์

2. โปรแกรมยูทิลิตี้สำหรับตรวจสอบระบบเครือข่าย

จากภาพจะเห็นได้ว่ารอบบริเวณนี้มีการใช้งานความถี่ย่าน 2.4 GHz หนาแน่นมาก หากจะมีการติดตั้งอุปกรณ์กระจายสัญญาณใหม่ในย่าน 2.4 GHz ก็ควรจะกำหนดให้ใช้ช่อง 8 แต่ในย่าน 5 GHz ยังมีช่องสัญญาณว่างอยู่เป็นจำนวนมาก หากสามารถใช้ช่องสัญญาณในย่านนี้จะดีมาก แต่ข้อจำกัดของย่าน 5 GHz คือระยะทางระหว่างอุปกรณ์กระจายสัญญาณกับอุปกรณ์ต้องอยู่ห่างกันไม่มาก



โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

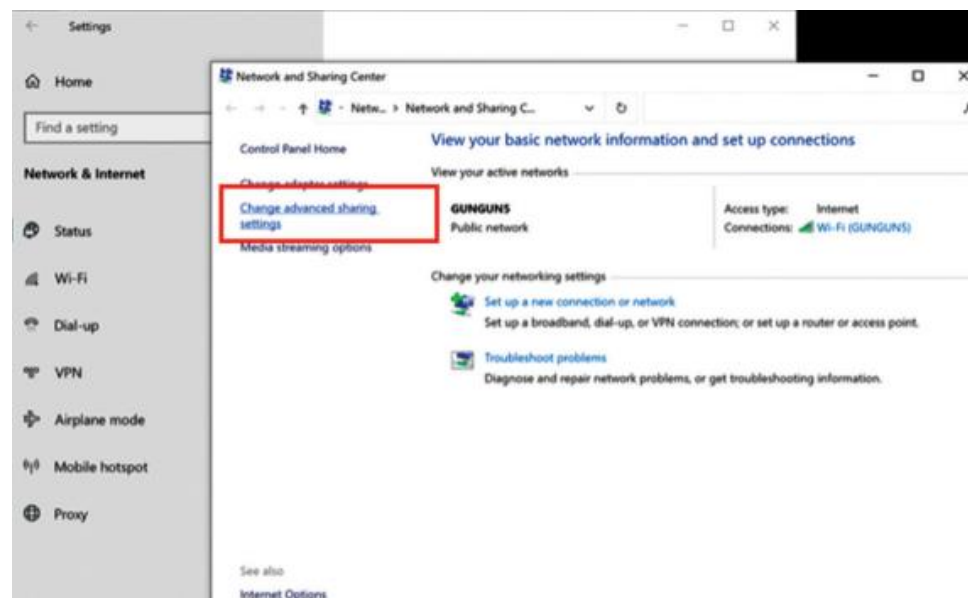
3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย

3.1 การแชร์เพิ่มข้อมูลบน Windows 10

สามารถอนุญาตให้คอมพิวเตอร์เครื่องอื่นที่อยู่บนเครือข่ายเดียวกันเข้าถึงเพิ่มข้อมูลในเครื่องของเราได้ โดยใช้ความสามารถพื้นฐานของ Windows 10 โดยทำการกำหนดค่าดังนี้

1) ไปที่ Control panel จากนั้นเลือก Network and Sharing Center

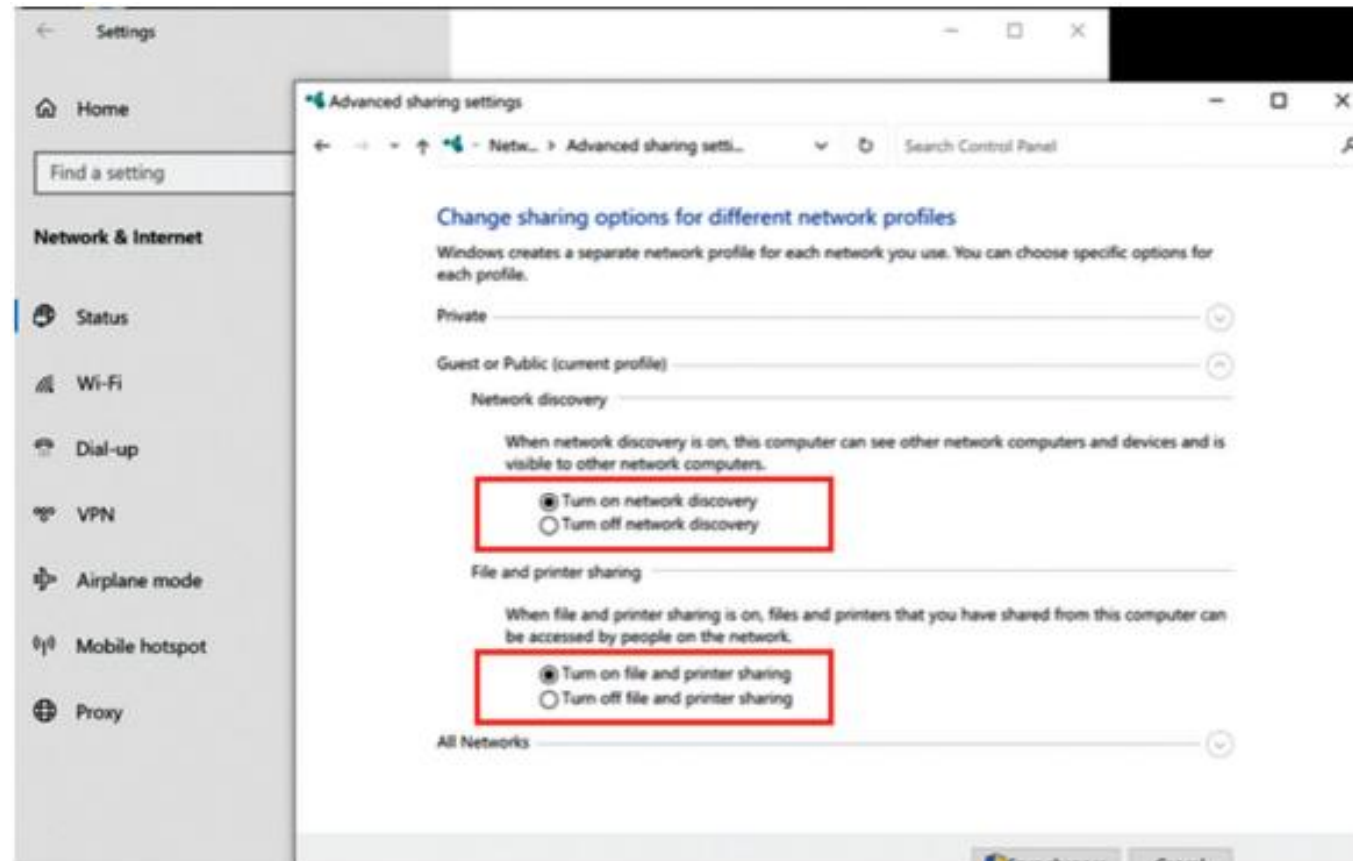


โปรแกรมบรรดประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย

2) ตั้งค่าการมองเห็นให้คอมพิวเตอร์เครื่องอื่นเห็นได้และเปิด File Sharing

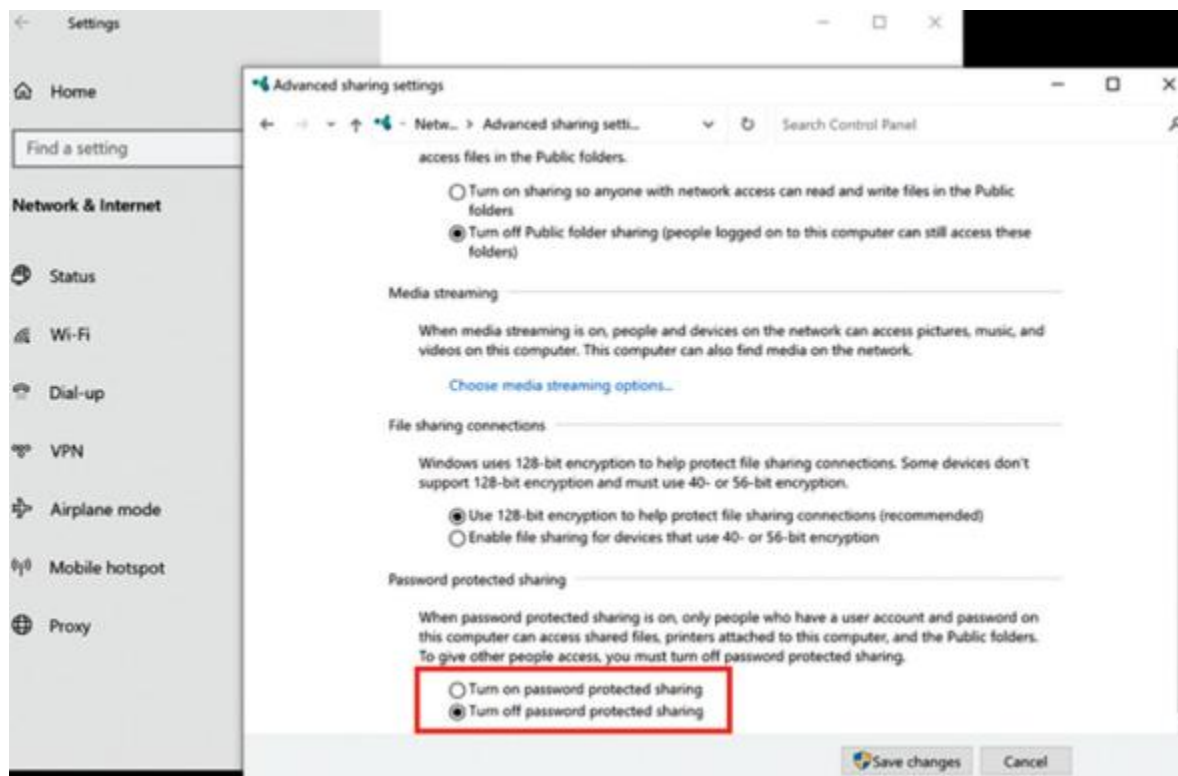


โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานแฟ้มข้อมูลบนเครือข่าย

3) ที่ All Networks ตั้งค่าที่หัวข้อ Password protected sharing ให้ตั้งค่าตามรูปด้านล่างแล้วกด Save Changes

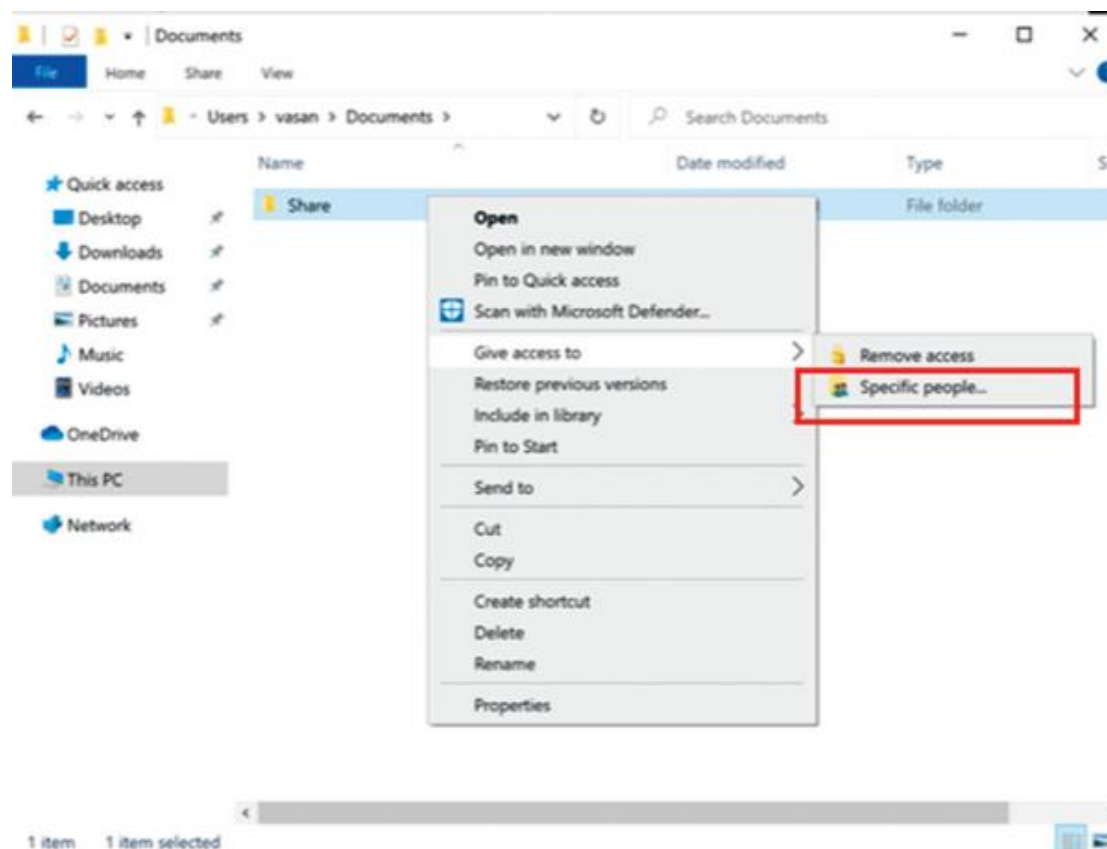


โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานแฟ้มข้อมูลบนเครือข่าย

4) จากนั้นไปที่ Folder ที่เราต้องการจะแชร์กับคนอื่น แล้วให้กดปุ่มเมาส์ขวาเลือก Give Access to Specific People

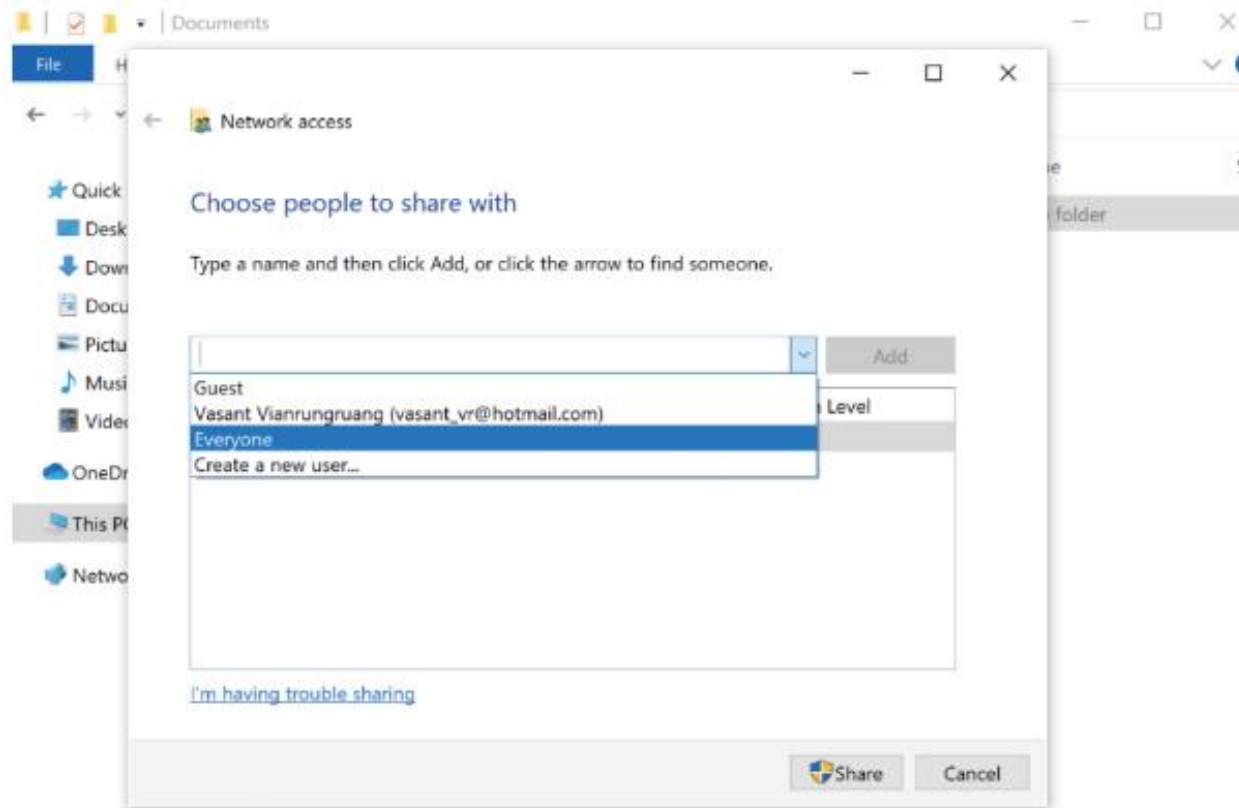


โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานแฟ้มข้อมูลบนเครือข่าย

5) เลือกว่าจะให้ผู้ใดคนไหนเข้าสู่แฟ้มข้อมูลในเครื่องเราได้

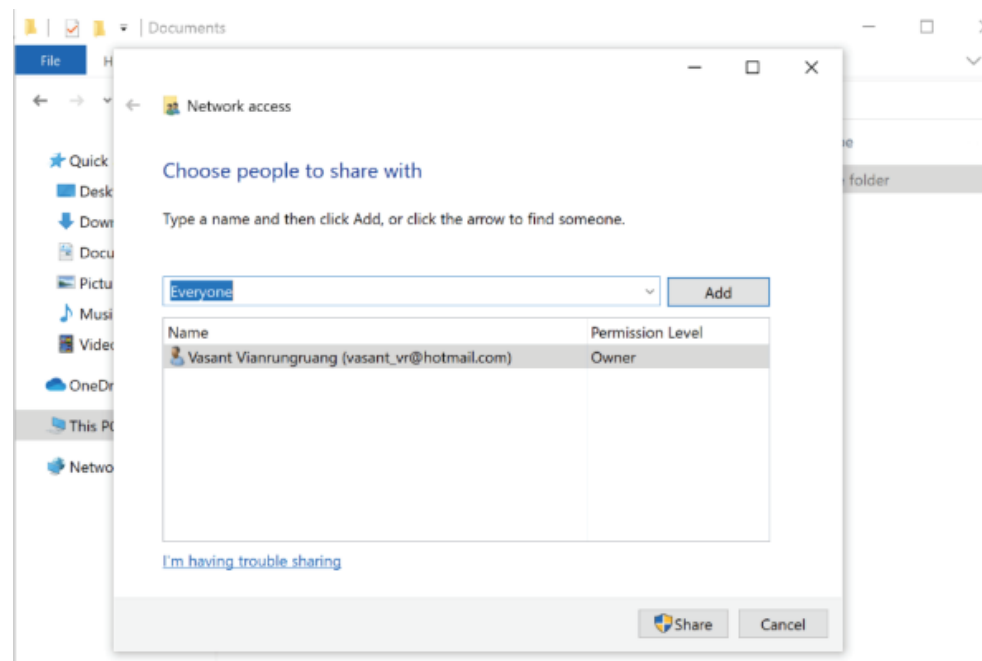


โปรแกรมบรรดประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานแฟ้มข้อมูลบนเครือข่าย

6) จะเลือกเพิ่มทีละคนหรือจะให้ทุกคนในเครือข่ายก็ได้



เมื่อเสร็จแล้วผู้ใช้ที่กำหนดจะสามารถเข้าถึงแฟ้มข้อมูลในโฟลเดอร์ที่กำหนดไว้ได้ ด้วยการไปที่
Windows Explorer > จากนั้นทำการพิมพ์ \\ชื่อเครื่อง\Folder ที่แชร์ และทำการ Enter เพื่อเข้าใช้งาน

โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย

3.2 ยูทิลิตี้สำหรับเก็บข้อมูลบนคลาวด์ (Cloud Storage)

Cloud Storage คือ ที่เก็บข้อมูลบนอินเทอร์เน็ต เช่น Dropbox, Google Drive, iCloud Drive และ OneDrive เราสามารถนำไฟล์ขึ้นไปจัดเก็บไว้บนคลาวด์ นำไฟล์กลับมาใช้งาน หรือแชร์ให้ผู้อื่นใช้ได้สะดวก ผู้ใช้เพียงมีอินเทอร์เน็ตและบัญชีผู้ใช้งานสำหรับแต่ละบริการของ Cloud Storage จึงทำให้บริการของ Cloud Storage ได้รับความนิยมเป็นอย่างมาก ผู้ให้บริการ Cloud Storage ส่วนใหญ่มักจะให้ผู้ใช้งานใช้บริการฟรี แต่จำกัดขนาดของข้อมูลที่ถูกจัดเก็บหรือปริมาณการรับส่งข้อมูล แต่หากต้องการพื้นที่จัดเก็บข้อมูลบนคลาวด์เพิ่มขึ้นสามารถจ่ายเงินซื้อพื้นที่เพิ่มขึ้นได้



โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย



รูปที่ 8.11 ยูทิลิตี้สำหรับเก็บข้อมูลบนคลาวด์ (Cloud Storage)

โปรแกรมถอดประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย

ผู้ให้บริการส่วนใหญ่จะมีโปรแกรมหรือยูทิลิตี้ให้ผู้ใช้งานติดตั้ง โดยเมื่อติดตั้งโปรแกรมแล้วระบบจะสร้างไฟล์เตอร์ขึ้นมาในเครื่องของผู้ใช้ หากผู้ใช้ต้องการจะเก็บข้อมูลไว้ในระบบคลาวด์ก็เพียงแค่เอาไฟล์นั้นไปใส่ไว้ในไฟล์เตอร์ดังกล่าว ระบบจะทำการสำรองข้อมูลไปเก็บไว้บนคลาวด์ให้เองโดยอัตโนมัติ ซึ่งระยะเวลาของการนำข้อมูลขึ้นสู่ระบบจะขึ้นอยู่กับความเร็วของระบบอินเทอร์เน็ตและขนาดของเพิ่มข้อมูล

ประโยชน์ของ Cloud Storage มีดังนี้

⚙ ใช้สำหรับเก็บข้อมูลในกรณีที่พื้นที่จัดเก็บบนอุปกรณ์ไม่เพียงพอ เช่น เราสามารถเก็บภาพของเราจากโทรศัพท์มือถือไว้กับ Google Photo ซึ่งเป็นส่วนหนึ่งของ Google Drive เพื่อให้พื้นที่ในมือถือเรามีที่ว่างได้



โปรแกรมรองรับประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย

⚙️ ช่วยในการทำงานออนไลน์และการส่งข้อมูลระหว่างอุปกรณ์ทำได้ง่ายขึ้น เช่น การถ่ายภาพบนมือถือแล้วเปิดดูบนคอมพิวเตอร์สามารถทำได้แทบจะในทันทีถ้าผู้ใช้คลาวด์ลงชื่อด้วยบัญชีเดียวกันหรือการแก้ไขงานแล้วอีกแผนกหนึ่งที่อยู่ห่างไกลกันมาก ๆ ก็สามารถส่งข้อมูลหรือแก้ไขงานร่วมกันได้ทันที เป็นต้น

⚙️ ใช้สำหรับแชร์หรือส่งข้อมูลขนาดใหญ่ ๆ ให้กันในกลุ่มโดยเมื่อเรานำเพิ่มข้อมูลไปเก็บไว้ใน Cloud Storage แล้ว เราสามารถที่จะส่งลิงก์ (Link) สำหรับเข้าถึงข้อมูลไปยังผู้ร่วมงานให้สามารถมาโหลดข้อมูลที่เราฝากไว้ไปได้ โดยการแชร์นี้จะสามารถกำหนดได้ว่าผู้อื่นสามารถที่จะเข้าถึง แก้ไข หรือลบข้อมูลได้หรือไม่ หรือแค่โหลดได้อย่างเดียว



โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานเพิ่มข้อมูลบนเครือข่าย

- ⚙ ใช้สำหรับทำงานร่วมกัน บริการ Cloud Storage บางรายสามารถเปิดให้ผู้ใช้ทำงานร่วมกัน เช่น การแก้ไขเพิ่มข้อมูลพร้อมกันได้ ทำให้เพิ่มประสิทธิภาพในการทำงาน
- ⚙ ใช้สำหรับสำรองข้อมูลในการทำงาน เช่น หากมีงานสำคัญที่ต้องใช้เพิ่มข้อมูลระหว่างการเดินทางเราสามารถสำรองข้อมูลขึ้นระบบคลาวด์ นอกเหนือจากข้อมูลที่มีอยู่ในโน้ตบุ๊ก หรืออุปกรณ์จัดเก็บข้อมูลอื่นหากอุปกรณ์เสียหายเราก็จะสามารถนำข้อมูลมาใช้ได้ทันที
- ⚙ เป็นที่สำรองข้อมูลเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นได้กับข้อมูลในระบบหรือข้อมูลต้นฉบับแต่การใช้งานคลาวด์ส่วนใหญ่เป็นในลักษณะการ Synchronize คือ ถ้ามีการเปลี่ยนแปลงข้อมูลที่ต้นทางข้อมูลที่ปลายทางก็จะถูกเปลี่ยนแปลงเช่นกัน ดังนั้นหากต้องการจะใช้ระบบ Cloud Storage ในการสำรองข้อมูลต้องศึกษาและกำหนดเงื่อนไขการสำรองข้อมูลให้ดี



โปรแกรมอรรถประโยชน์บนเครือข่ายคอมพิวเตอร์

3.

โปรแกรมยูทิลิตี้สำหรับการใช้งานแฟ้มข้อมูลบนเครือข่าย

ผู้ให้บริการ	ฟรี (GB)	ราคาเริ่มต้น (เดือน)	ความจุ เริ่มต้น	ใช้งานได้หลาย OS	แก้ไขข้อมูลออนไลน์ได้
Dropbox	2	330	1 TB	X	
iCloud Drive	5	35	50 GB		
Google Drive	15	70	100 GB	X	X
Microsoft OneDrive	5	35 (365 Family)	1 TB	X	X

ตารางที่ 8.1 เปรียบเทียบผู้ให้บริการระบบ Cloud Storage

หมายเหตุ

ราคาค่าบริการอาจเปลี่ยนแปลงตามแต่ละช่วงเวลา

โปรแกรมลดประโยชน์บนเครือข่ายคอมพิวเตอร์

สรุปท้ายหน่วย

เพื่อให้การทำงานของเครือข่ายมีประสิทธิภาพ ผู้ใช้ระบบเครือข่ายจำเป็นต้องรู้จักและสามารถใช้งานโปรแกรมยูทิลิตี้ที่ช่วยสำหรับตรวจสอบประสิทธิภาพการทำงานพื้นฐานของเครือข่าย เช่น ความเร็วในการรับส่งข้อมูล (Transfers Rate) ความเร็วในการตอบสนองของระบบเครือข่าย (Latency) หรือโปรแกรมยูทิลิตี้ที่ช่วยในการวิเคราะห์ปัญหา หาจุดอ่อนหรือคอขวดของระบบ ซึ่งโปรแกรมยูทิลิตี้เหล่านี้ใช้งานไม่ยากและส่วนใหญ่เป็นเครื่องมือฟรีที่มีมากับระบบปฏิบัติการหรือสามารถดาวน์โหลดได้ฟรี

