Data Communications And Computer Networks

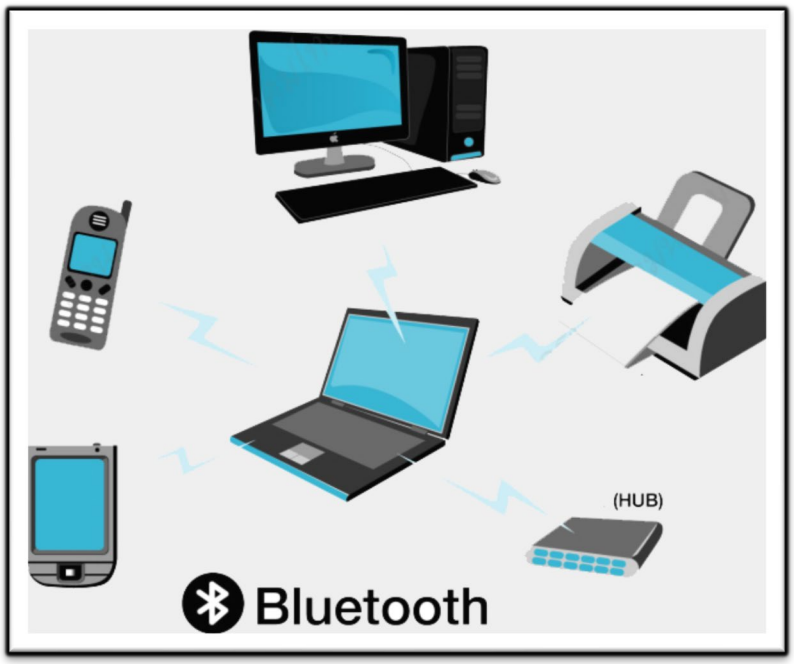
บทที่ 2

เครือข่ายคอมพิวเตอร์ (Computer Network)

เครือข่ายคอมพิวเตอร์

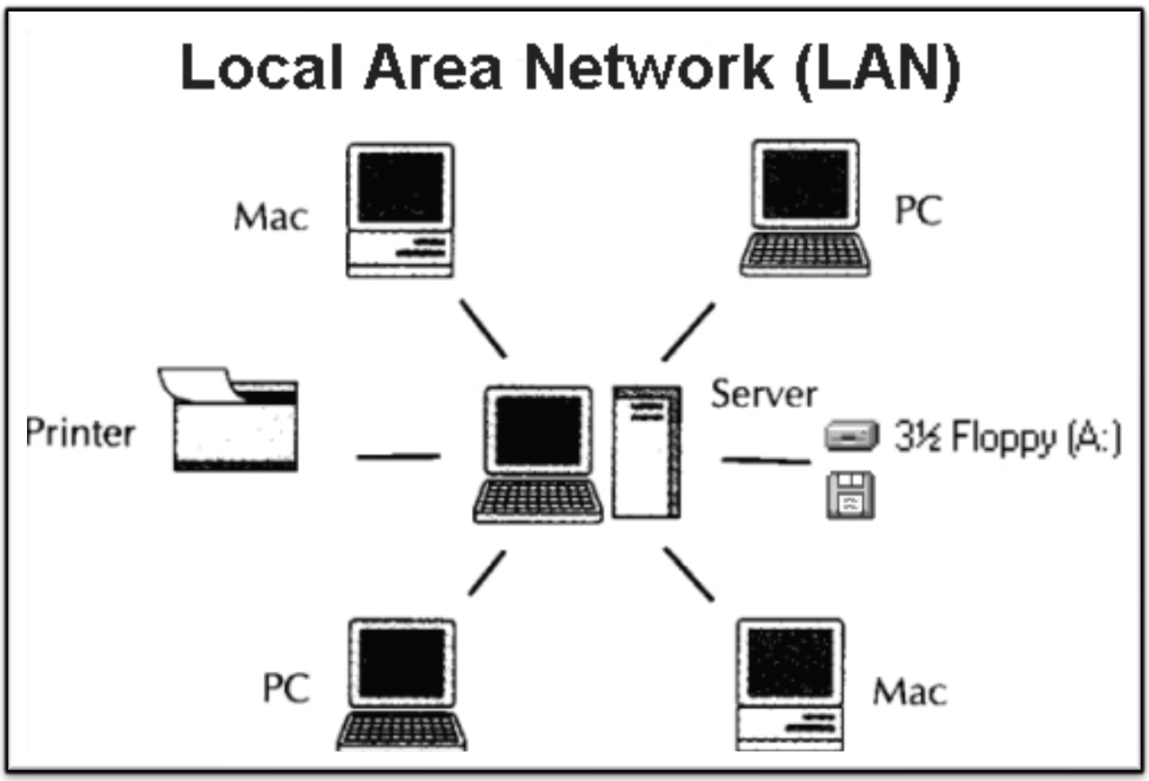
เครือข่ายคอมพิวเตอร์ (Computer Network) เป็นการเชื่อมต่อเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงเข้าด้วยกัน เพื่อให้สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลซึ่งกันและกันได้ เครือข่ายคอมพิวเตอร์แบ่งออกได้ตามสภาพการเชื่อมโยงเป็น 4 ชนิด ดังนี้

1. เครือข่ายส่วนบุคคล แพน (Personal Area Network : PAN) เป็นเครือข่ายเชื่อมต่อไร้สายส่วนบุคคลที่มีระยะใกล้ๆ เช่น การเชื่อมต่อคอมพิวเตอร์กับโทรศัพท์มือถือ เชื่อมต่อโทรศัพท์มือถือกับหูฟังบลูธูท เชื่อมต่อระหว่างโทรศัพท์มือถือเข้าด้วยกัน เป็นต้น



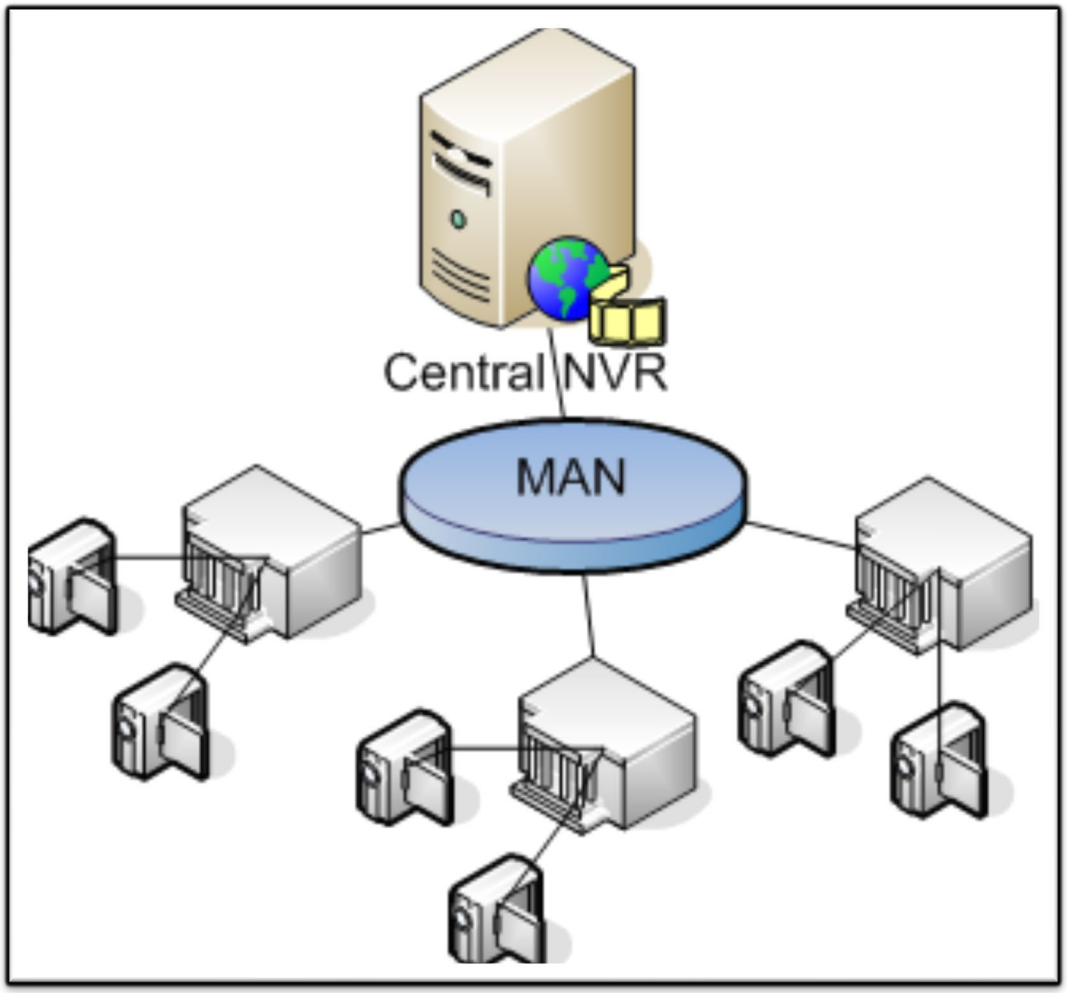
ภาพเครือข่าย Personal Area Network (PAN)

2. เครือข่ายเฉพาะที่ หรืออาจเรียกว่าเครือข่ายท้องถิ่น แลน (Local Area Network : LAN) เป็นการเชื่อมต่อเครือ ข่ายขนาดเล็ก ที่เชื่อมโยงอุปกรณ์ต่างๆ หรือคอมพิวเตอร์ในบริเวณใกล้ๆ กัน เข้าด้วยกัน เช่น ภายในห้อง ภายในอาคาร ระหว่างอาคาร โดยมีอุปกรณ์สำหรับเชื่อมโยงเครือข่าย เช่น สวิตช์ ฮับ เป็นต้น โดยการเชื่อมต่ออาจจะเป็นแบบใช้สายหรือแบบไร้สายก็ได้



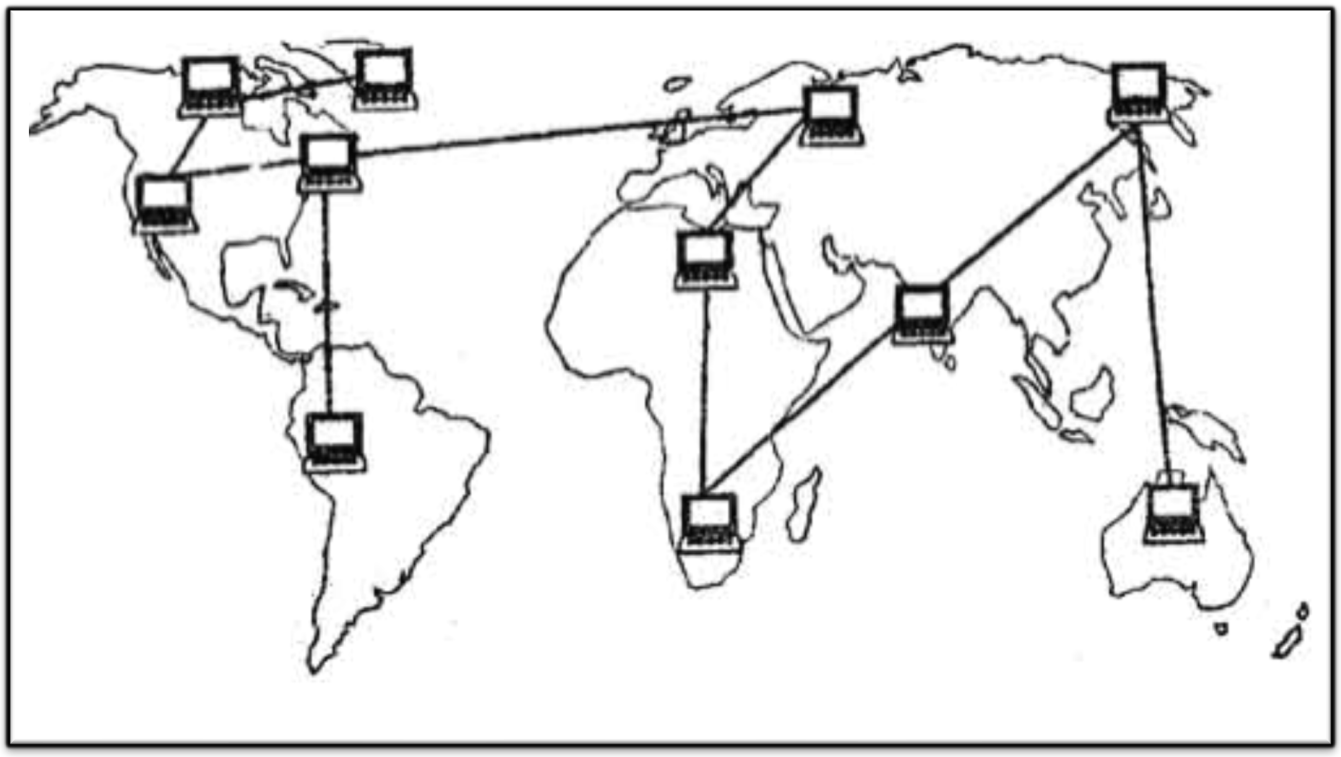
ภาพเครือข่าย Local Area Network (LAN)

3. เครือข่ายนครหลวงหรืออาจเรียกว่าเครือข่ายระดับเมือง แมน (Metropolitan Area Network : MAN) เป็นเครือข่ายเชื่อมโยงที่อยู่ห่างไกลกัน เช่น ภายในตำบล หรืออำเภอ ระยะเชื่อมโยงประมาณ 5-40 กิโลเมตร โดยการเชื่อมต่อจะเป็นแบบสายสัญญาณ เช่น สายใยแก้วนำแสง (fiber optic), สายโคแอกเชียล (Coaxial)



ภาพเครือข่าย Metropolitan Area Network (MAN)

4. เครือข่ายวงกว้าง แวน (Wide Area Network : WAN) เป็นเครือข่ายที่มีคอมพิวเตอร์จำนวนมาก ที่เชื่อมโยงในระยะที่ไกลมากๆ มีการติดต่อสื่อสารกันในบริเวณกว้าง เช่น เชื่อมโยงระหว่างจังหวัด หรือระหว่างประเทศ

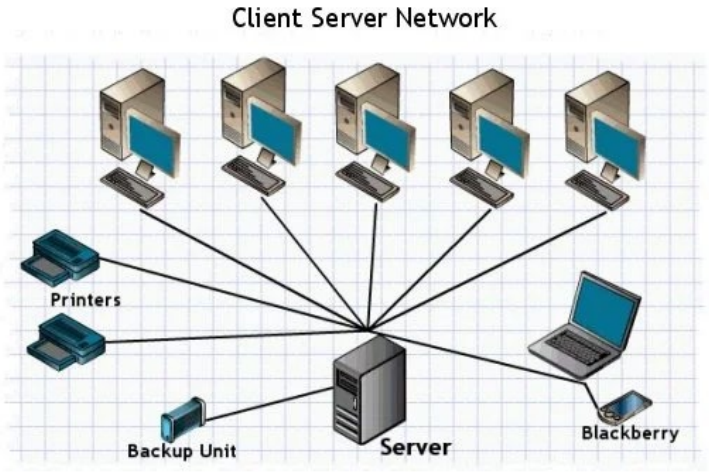


ภาพเครื่องข่าย Wide Area Network (Wan)

ประเภทของสถาปัตยกรรมเครือข่ายคอมพิวเตอร์

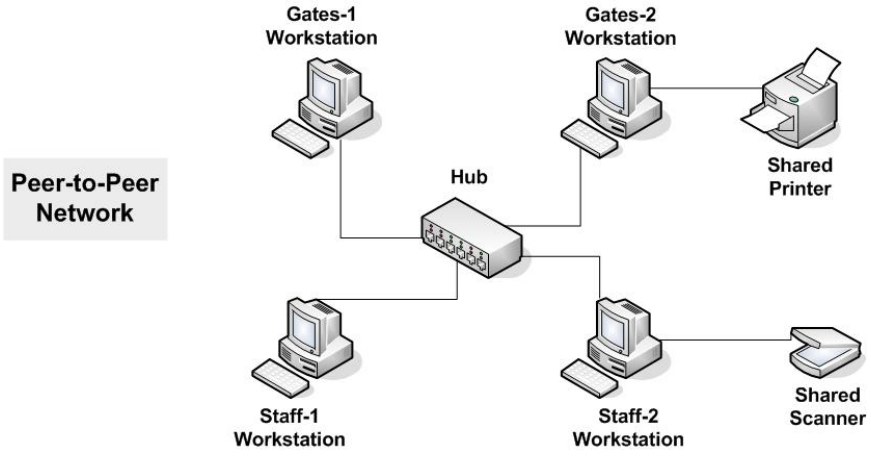
สถาปัตยกรรมไคลเอนต์-เซิร์ฟเวอร์

สถาปัตยกรรมไคลเอนต์-เซิร์ฟเวอร์เป็นสถาปัตยกรรมเครือข่ายคอมพิวเตอร์ประเภทหนึ่งซึ่งโหนดสามารถเป็นเซิร์ฟเวอร์หรือไคลเอนต์ได้ ที่นี่ โหนดเซิร์ฟเวอร์สามารถจัดการพฤติกรรมของไคลเอ็นต์โหนดได้



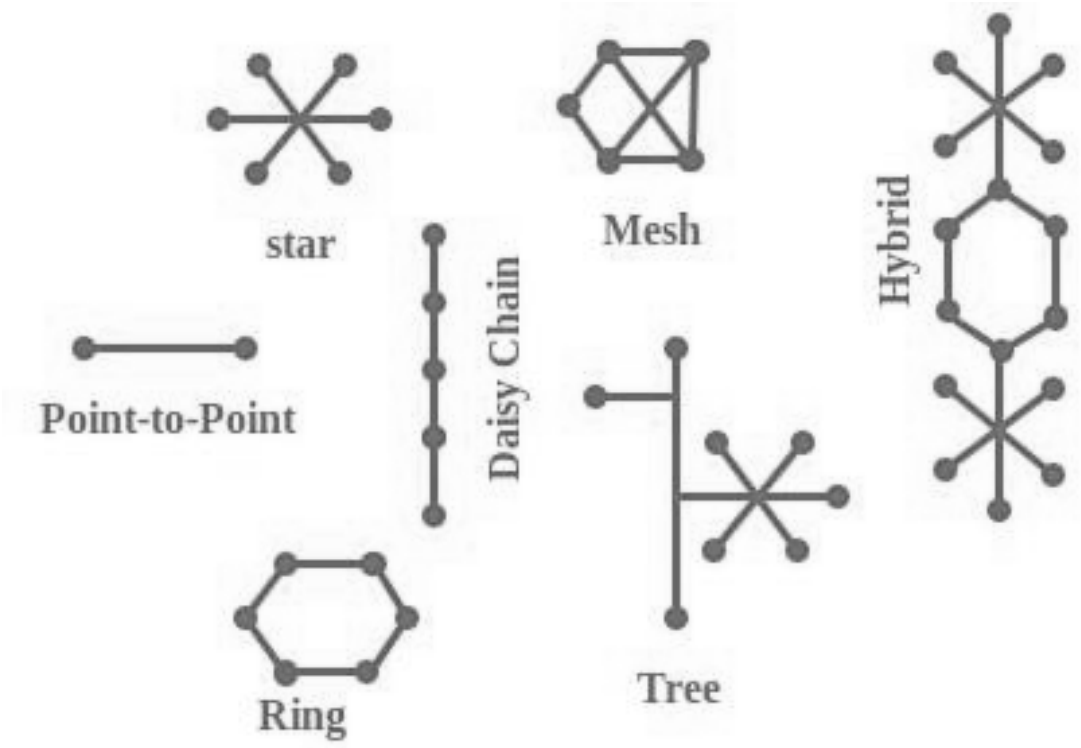
สถาปัตยกรรมแบบ Peer-to-Peer

ในสถาปัตยกรรม P2P (Peer-to-Peer) เป็นการเชื่อมต่อที่ไม่มีเซิร์ฟเวอร์กลาง อุปกรณ์แต่ละชิ้นมีอิสระสำหรับการทำงาน ทุกเครื่องมีสิทธิ์ เท่าเทียมกันหมด



โทโพโลยีเครือข่าย

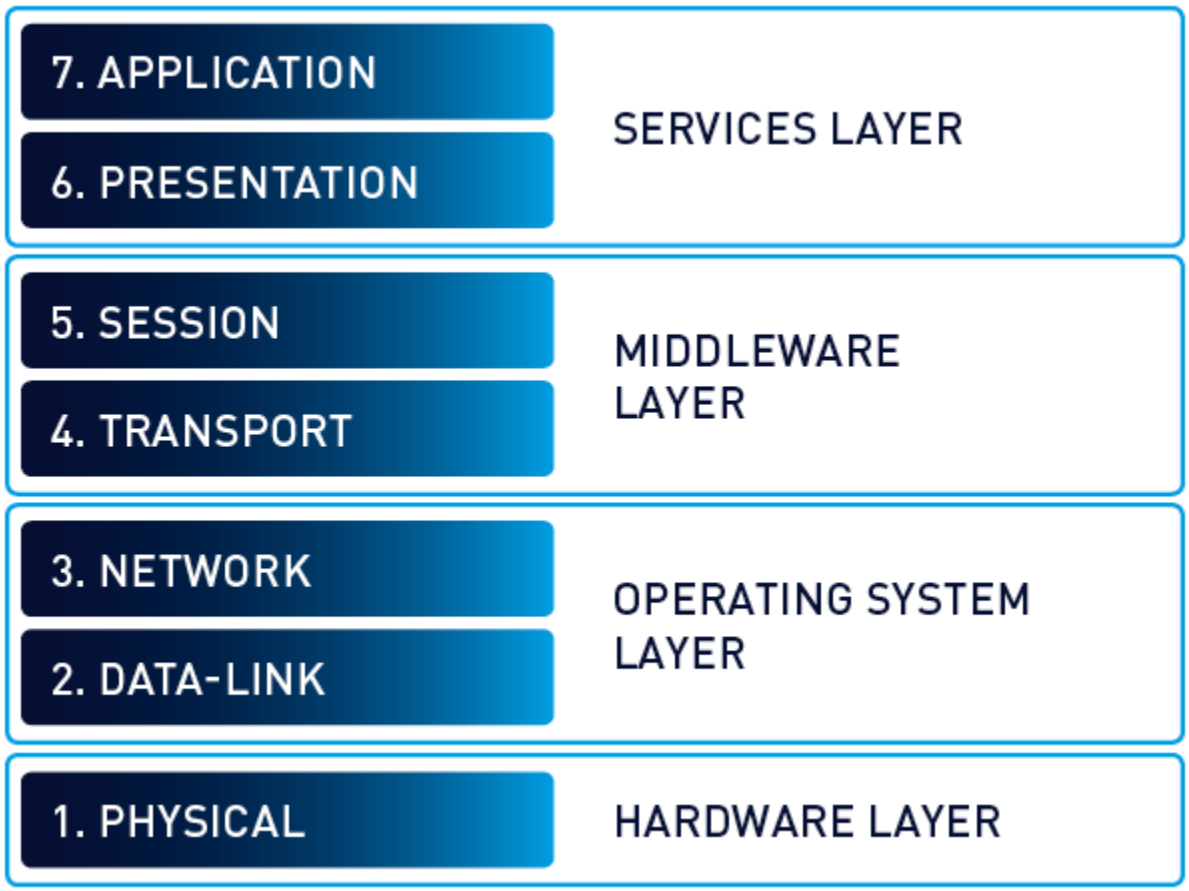
Network Topology คือการจัดเลย์เอาต์ของอุปกรณ์ต่าง ๆ ในเครือข่าย ตัวอย่างได้แก่ Bus, Star, Mesh, Ring และ Daisy chain



ภาพโทโพโลยีเครือข่าย

OSI Model

OSI Model (Open Systems Interconnection Model) คือรูปแบบการรับส่งข้อมูลระหว่างอุปกรณ์อิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นตัวกำหนดรูปแบบของผู้ส่งข้อมูล (Sender) และผู้รับข้อมูล(Receiver)จะแบ่งการทำงานออกเป็น 7 Layers โดย Layer 4-7 จะเน้นไปที่การติดต่อกับ User ผ่าน Software เป็นหลัก ส่วน Layer 1-3 จะเน้นที่การสื่อสารในระดับ Hardware เป็นหลัก โดยแต่ละ Layer จะมีบทบาท, หน้าที่และหลักการทำงานที่แตกต่างกันแต่จะทำงานร่วมกับ Layer ที่อยู่ติดกัน ดังนี้

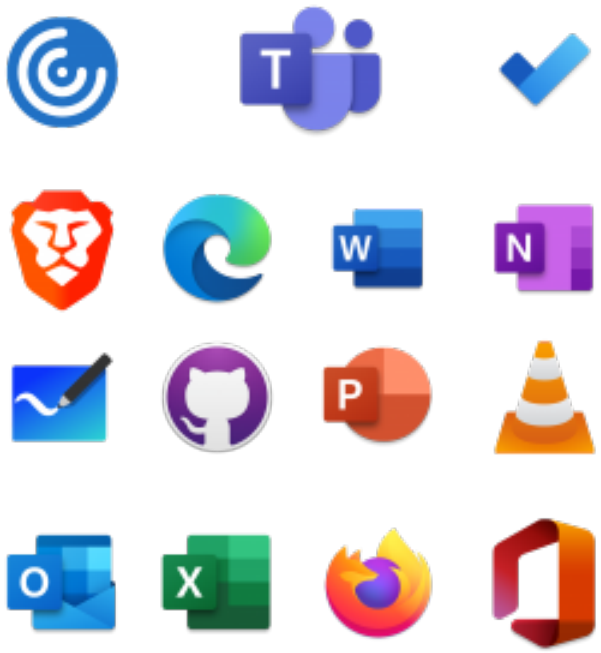


ภาพ 7 Segment Layer

1.Application-oriented layers (Layer 4-7) คือ กลุ่มของ Layers ที่ใช้สื่อสารการเชื่อมต่อข้อมูลระหว่าง Sender และ Receiver เข้ากับ Application ต่างๆ โดยจะเกี่ยวข้องกับ Software เป็นหลัก

Layer 7: Application Layer

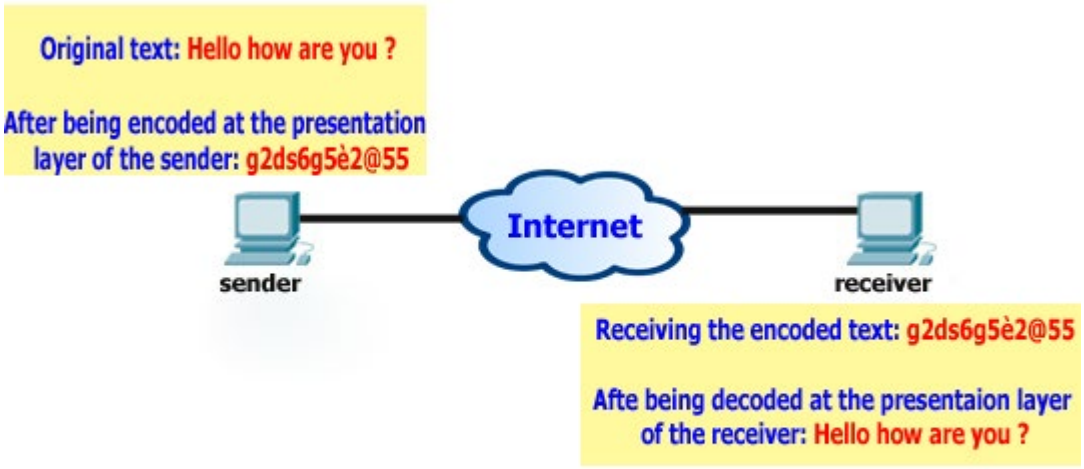
เป็น Layer ที่อยู่ใกล้กับ Users มากที่สุด โดยจะเป็น Protocol ต่างๆที่ใช้ในการสื่อสารกับ user เช่น HTTP, FTP นิยมใช้กับ Software เพื่อง่ายต่อการ Interact กับ Users เช่น หาก user ต้องการใช้ Protocol HTTP เพื่อท่องโลก internet ก็จะใช้ browser เช่น Firefox, Chrome, etc เพื่อเรียกใช้ Protocol ดังกล่าว



ภาพ Application Layer

Layer 6: Presentation Layer

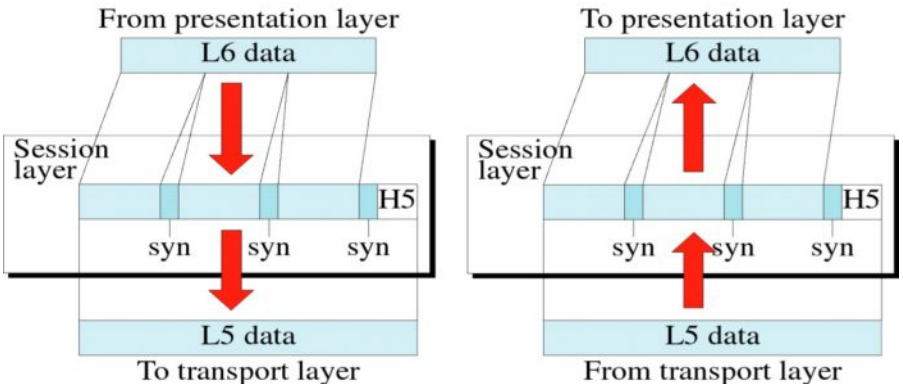
เป็น Layer ที่ใช้ในการ Translate ข้อมูลจาก/ไปยัง Application layer เช่น Sender พิมพ์ข้อความว่า “Hello, how are you?” layer นี้จะทำการแปลงข้อความเหล่านั้นเป็นรหัส และให้ Presentation layer จากฝั่ง Receiver เป็นตัวแปลงรหัสเหล่านั้นให้กลับมาเป็นข้อความ “Hello, how are you?” ให้ Receiver ได้รับ



ภาพ Presentation Layer

Layer 5: Session Layer

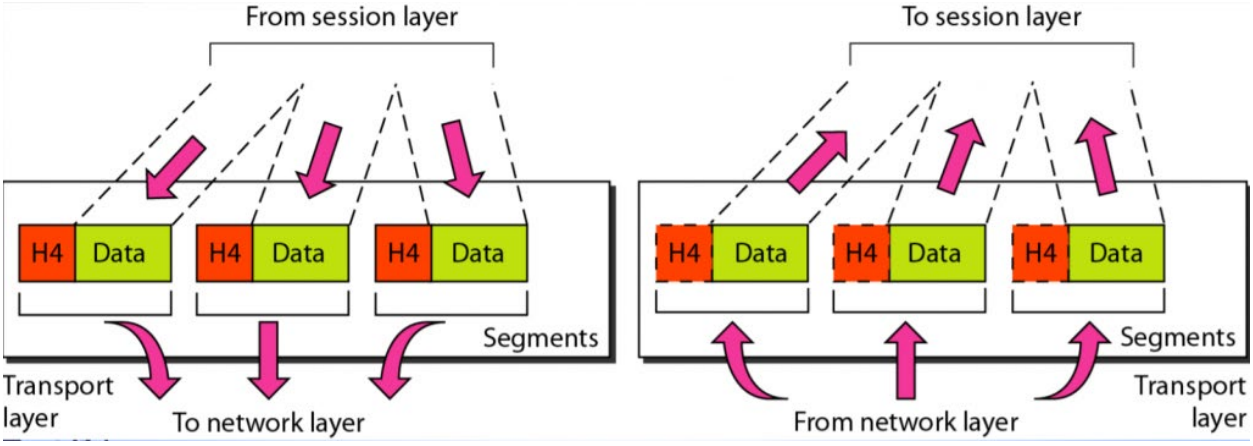
เป็น Layer ที่มีการ Sync ตามเงื่อนไขการใช้งานระหว่างเครื่องต้นทางกับเครื่องปลายทาง หรือจาก Layer 6 -> Layer 5 เช่น User ต้องการขอใช้บริการบางอย่างจาก Server เป็นเวลา 20 นาที ผ่านช่องทาง port 99, Server ก็จะส่งข้อความอนุญาตให้ User ดังกล่าวใช้บริการผ่าน port 99 ได้ (Start Session) เป็นเวลา 20 นาที หาก Session ที่ขอใช้งานเกิดหมดเวลา (End Session) ก็จะไม่สามารถใช้บริการต่อได้



ภาพ Session Layer

Layer 4: Transport Layer

เป็น Layer ที่จะควบคุมการขนส่งข้อมูลจาก Sender ไปยัง Receiver หรือจาก Receiver ไปยัง Sender เมื่อเกิดการรับส่งข้อมูล ตัว Transport layer จะทำการแบ่งชิ้นส่วนข้อความดังกล่าวเป็นชิ้นเล็กๆหลายๆชิ้นเรียกว่า “Segment” และทำการเพิ่มที่ L4 Header (ประกอบด้วย Protocol ที่ใช้, Source Port และ Destination Port) เข้าไปบน Segments แต่ละชิ้น เพื่อให้ง่ายต่อการส่งและตรวจสอบความถูกต้อง โดยวิธีการนี้เรียกว่า Segmentation

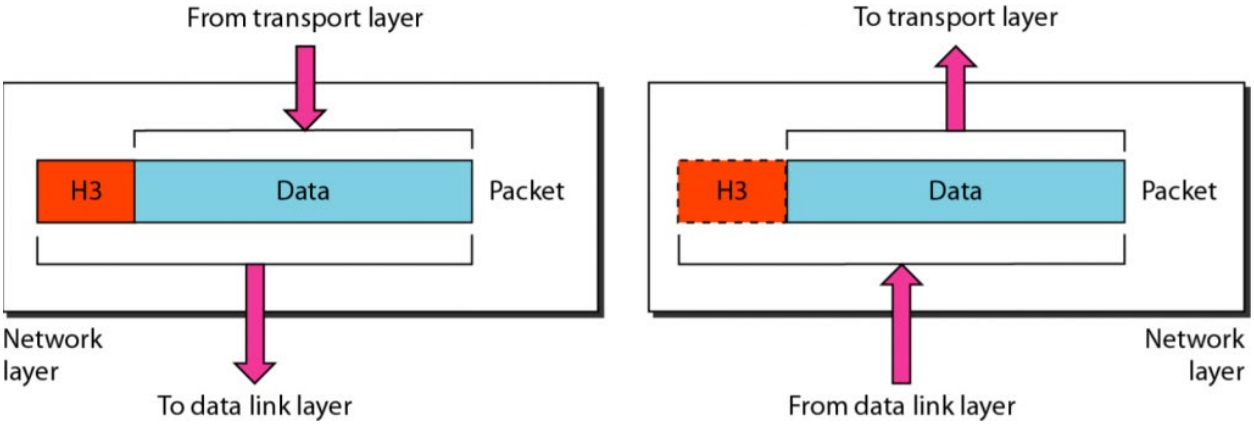


ภาพ Transport Layer

2. Network-dependent Layers (Layer 1-3) คือ กลุ่มของ Layers ที่ทำหน้าที่เชื่อมต่อคอมพิวเตอร์ของทั้ง Senders และ Receivers ผ่านระบบเครือข่ายทั้งแบบมีสายและไร้สาย โดยจะเกี่ยวข้องกับ Hardware เป็นหลัก ซึ่งสำหรับบุคลากรที่ทำงานสาย Network จะเน้นศึกษาที่ Layers เหล่านี้

Layer 3: Network Layer

เป็น Layer ที่ทำการสร้างช่องทางการเชื่อมต่อระหว่าง Network ของ Sender และ Receiver เข้าด้วยกันผ่าน IP Address รวมถึง โดย Layer นี้จะรับ Segments จาก Transport Layer มาเพิ่มเข้าที่ L3 Header (ประกอบด้วย Source IP และ Destination IP) และตั้งชื่อให้ใหม่ว่า “Packet” โดยอุปกรณ์ที่ทำหน้าที่บน Layer3 ได้แก่ Router, L3 Switch(Multilayer Switch), Wireless Router เป็นต้น

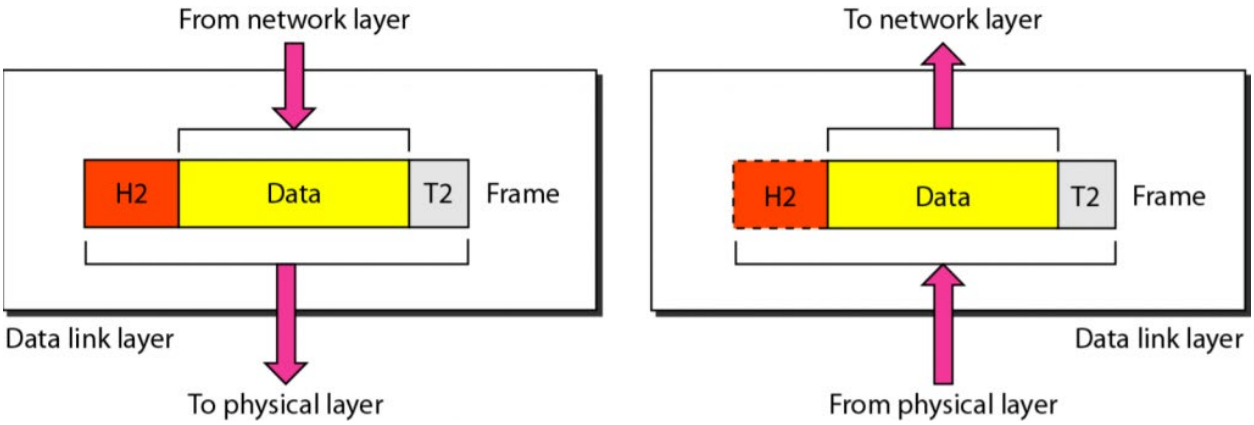


ภาพ Network Layer

Layer 2: Data link Layer

เป็น Layer ที่ทำการเชื่อมต่อข้อมูลแบบ node to node เช่น PC-Switch, Switch หรือ Switch-Router เป็นต้น โดยจะใช้ MAC Address ส่วนมากจะใช้สาย UTP เป็นตัวเชื่อมต่ออุปกรณ์เหล่านี้เข้าด้วยกัน โดย Layer นี้จะรับ Packet จาก Network Layer มาทำการเพิ่มที่ L2 Header และ L2 Trailer (ประกอบด้วย Source MAC, Destination

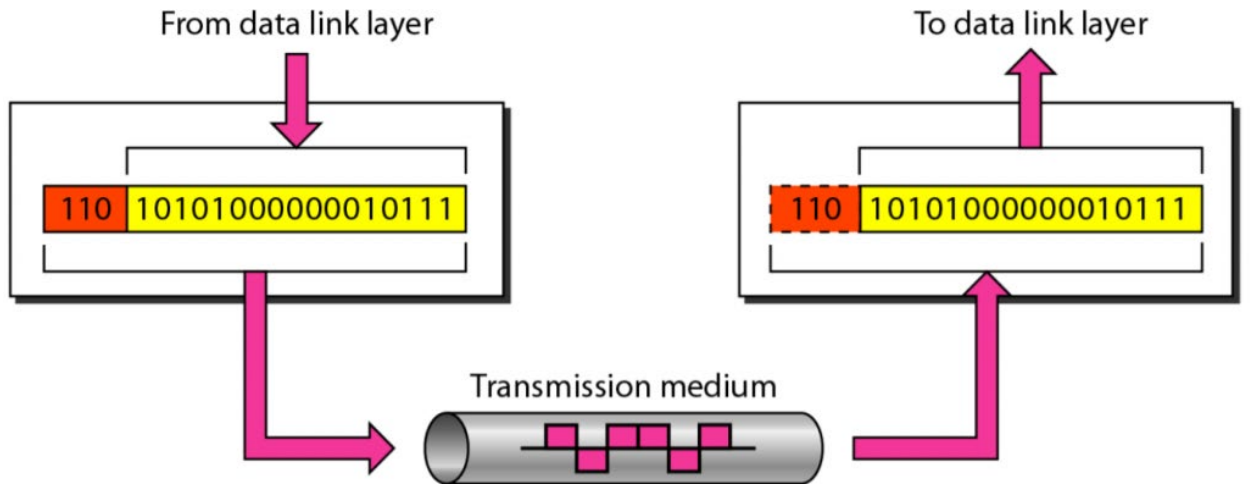
MAC, Tag VLAN, etc) และเรียกชื่อใหม่ว่า “Frame” โดยอุปกรณ์ที่ทำหน้าที่บน Layer2 ได้แก่ Switch, Bridge



ภาพ Data Link Layer

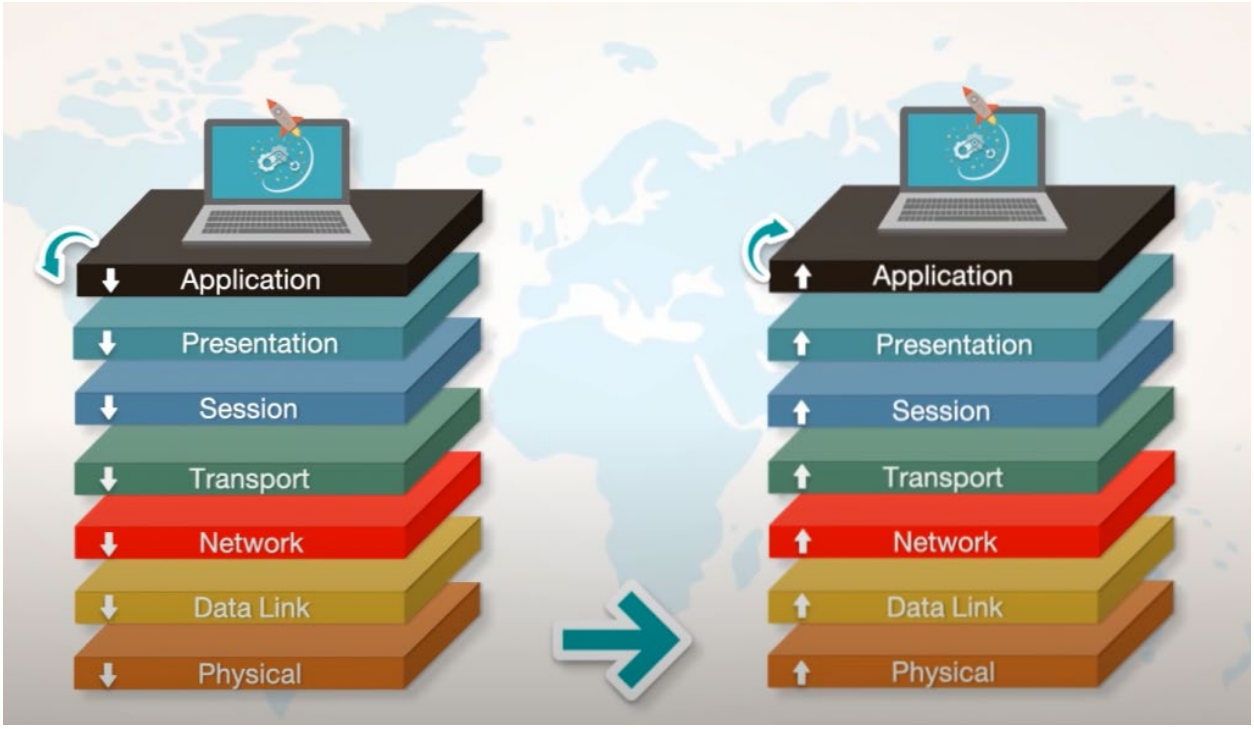
Layer 1: Physical Layer

เป็น Layer ที่ทำการนำ Frame ข้อมูลจาก Data Link Layer ส่งระหว่างอุปกรณ์ Network ผ่านตัวกลาง เช่น สาย UTP, สาย Fiber optic โดยเราเรียกสิ่งที่ส่งผ่านตัวกลางเหล่านี้ว่า “Bits”หรือ “Bytes” (8 Bits = 1 Byte)



ภาพ Physical Layer

โดยทั้ง 7 Layers มีหลักการทำงานที่สัมพันธ์กัน คล้ายกับการขึ้นลงบันได โดยจะเริ่มจากชั้น Application Layer จากฝั่ง Sender และจบที่ Application Layer จากฝั่ง Receiver



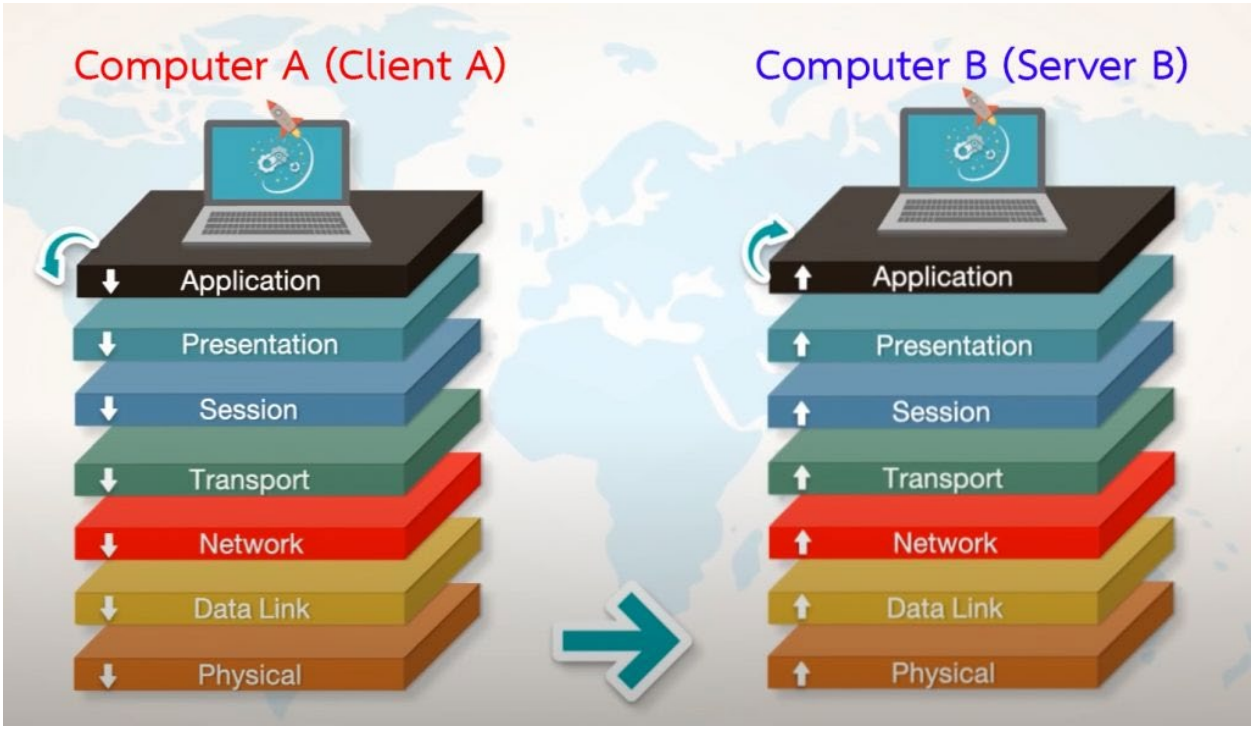
ภาพ 7 Layer Process

คำศัพท์ที่ควรรู้

Mac Address : Media Access Control Address

Physical Address : รหัสประจำตัวของอุปกรณ์ (Lan Card,Wireless Card) ที่ประกอบด้วยตัวเลขฐาน 16 มี 6 Bytes และรหัส 12 ตัว เช่น "2C:54:91:88:C9:E3"

ตัวอย่างเช่น Computer A (Client A) ต้องการติดต่อขอใช้บริการกับ Computer B (Server B)



Sender A

<Sender A> Application Layer:
ผู้ใช้กรอกข้อมูล Username/Password จากนั้นกด Enter
<Sender A> Presentation Layer:
Encode Username/Password ไปเป็น Data
<Sender A> Session Layer:
รอรับการ Synchronize จากปลายทาง
<Sender A> Transport Layer:
นำ Data มาแบ่งเป็นชิ้นเล็กๆจากนั้น แนบ L4 Header (มี Protocol, Source port,

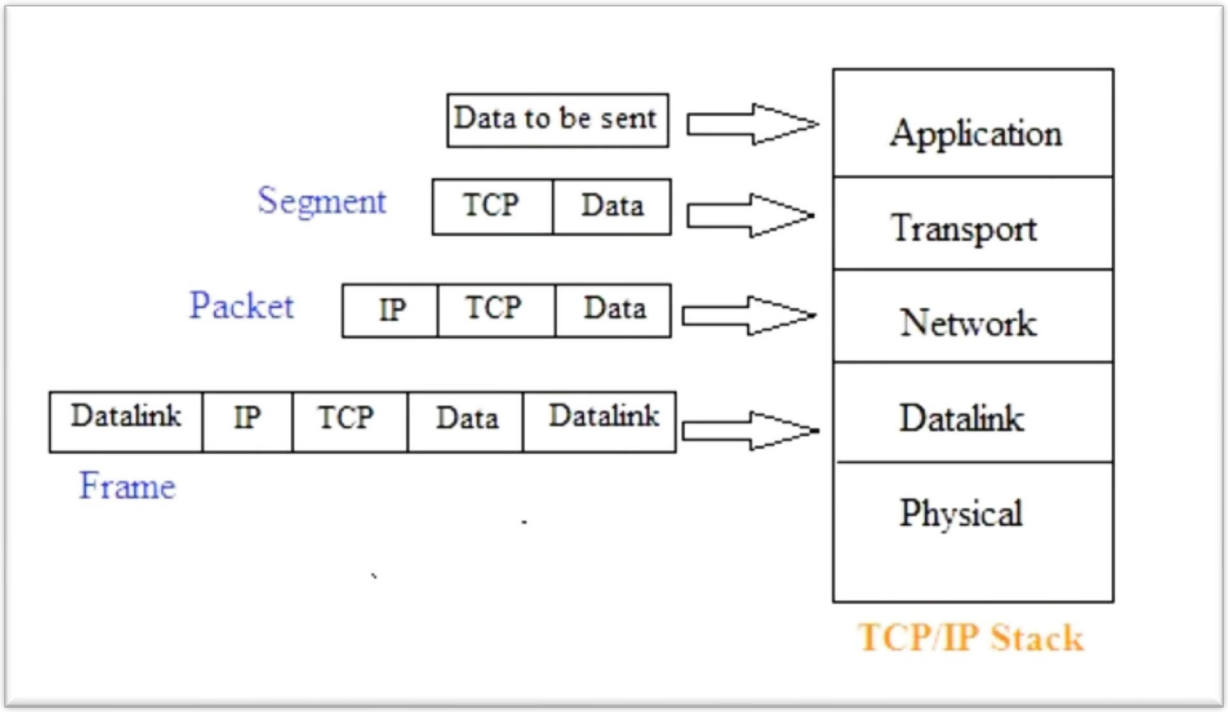
Destination port เป็นส่วนประกอบ) ลงไปเรียกแต่ละชิ้นว่า “Segment”
<Sender A> Network Layer:
นำ Segments มาแนบ L3 Header (มี Source IP, Destination IP เป็นส่วนประกอบ) เรียกว่า “Packet”
<Sender A> Data Link Layer:
นำ Packet มาแนบ L2 Header และ L2 Trailer (มี Source MAC, Destination MAC, ฯลฯ เป็นส่วนประกอบ) เรียกว่า “Frame”
<Sender A> Physical Layer:
นำ Frame ส่งผ่านสายนำข้อมูล เรียกว่า bits, Bytes (8 bits = 1 Bytes)

Receiver B

<Receiver B> Physical Layer:
รับ bits, Bytes ผ่านสายนำข้อมูล
<Receiver B> Data Link Layer:
รับ Frame มาทำการ แกะ L2 Header, L2 Trailer ออก เพื่อตรวจสอบ Source MAC, Destination MAC, ฯลฯ
<Receiver B> Network Layer:
รับ Packet มาทำการ แกะ L3 Header ออก เพื่อตรวจสอบ Source IP, Destination IP
<Receiver B> Transport Layer:
รับ Segment มาทำการ แกะ L4 Header ออก เพื่อตรวจสอบ Protocol, Source Port, Destination Port
<Receiver B> Session Layer:
รอรับการ Synchronize จากต้นทาง

<Receiver B> Presentation Layer:
ทำการ Decode Data ไปเป็น Username/Password เพื่อตรวจสอบในฐานข้อมูล
ว่า มีข้อมูล User ดังกล่าวหรือไม่
<Receiver B> Application Layer:
รายงานผลการข้อใช้บริการจาก Client A ให้ Server B ทราบ

จากนั้น Server B จะเปลี่ยนสถานะตัวเองจาก Receiver B ไปเป็น Sender B เพื่อส่งรายละเอียดการให้บริการกลับไปให้ Client A (Sender A ไปเป็น Receiver A) ผ่านทาง OSI Model ทั้ง 7 Layers (ครั้งนี้ Session Layer จะทำการ ส่งเงื่อนไขการให้บริการเพื่อ Sync ระหว่าง Server B และ Client A)



ภาพ OSI 7 Layer

อุปกรณ์เชื่อมต่อเครือข่าย

การเชื่อมต่อระหว่างเครื่องต่อกับเครื่อง หรือเครื่องต่อกับอุปกรณ์ต่อพ่วงต่างๆ ซึ่งในการเชื่อมต่อกัน เพื่อจุดประสงค์ในการรับ และส่ง ข้อมูลหรือสื่อต่างๆ โดยในเครือข่ายคอมพิวเตอร์จะมีอุปกรณ์ที่ใช้ในการเชื่อมต่อกัน หลากหลายแตกต่างกันตามการใช้งาน แต่ในทุกอุปกรณ์เชื่อมต่อสามารถทำให้เครื่องสามารถเชื่อมต่อกันได้ อุปกรณ์เครือข่ายที่ใช้สำหรับการเชื่อมต่อ เช่น เราเตอร์, สวิตช์, ฮับ และบริดจ์ เป็นต้น โดยตัวกลางที่ใช้ในการเชื่อต่อ คือ สาย หรือสัญญาน

สัญลักษณ์อุปกรณ์เครือข่าย/Network Icon

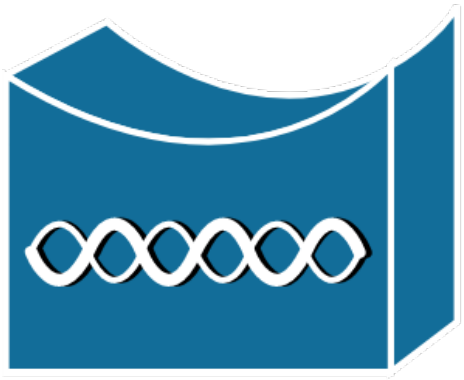
Router

Wireless Router

10 Base T Hub

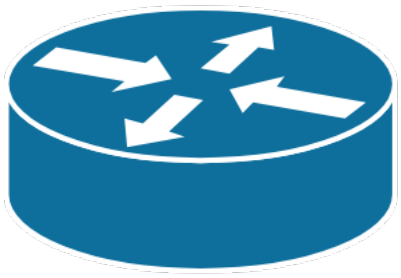
Switch

Bridge



Wireless Bridge

เราเตอร์ (Router)



เราเตอร์เป็นอุปกรณ์ที่ทำหน้าที่เชื่อมต่อ LAN หลายๆ เครือข่ายเข้าด้วยกันคล้ายกับสวิตช์แต่จะมีส่วนเพิ่มเติมคือ เราเตอร์สามารเชื่อมต่อ LAN ที่ใช้โปรโตคอลในการรับส่งข้อมูลเหมือนกัน แต่ใช้สื่อส่งข้อมูลหรือสายส่งต่างชนิดกันได้ เช่น เชื่อมต่อ Ethernet LAN ที่ใช้รับส่งข้อมูลแบบ UTP เข้ากับ Ethernet อีกเครือข่ายหนึ่งที่ใช้สายข้อมูลแบบ coaxial cable ได้

เราเตอร์ทำงานเสมือนเป็นเครื่องหรือโหนดหนึ่งใน LAN ซึ่งจะทำการรับข้อมูลเข้ามาแล้วส่งต่อไปยังปลายทาง โดยจะส่งในรูปแบบของ Packet ที่ต่างออกไปจากเดิม เพื่อไปผ่านสายสัญญาณแบบต่าง ๆ เช่น สายโทรศัพท์ที่ต่อผ่านโมเด็มก็ได้ ดังนั้นเราจึงอาจใช้เราเตอร์เพื่อเชื่อมต่อ LAN หลาย ๆ แบบเข้าด้วยกันได้ด้วย และจากการที่มันทำตัวเสมือนเป็นโหนด ๆ หนึ่งใน LAN ทำให้เราเตอร์สามารถทำงานอื่น ๆ อีกมาก เช่น รวบรวมข้อมูลเพื่อหาเส้นทางที่ดีที่สุดในการส่งข้อมูลต่อ หรือตรวจสอบว่าข้อมูลที่เข้ามานั้นมาจากไหน ควรจะให้ผ่านหรือไม่ เพื่อช่วยในเรื่องการรักษาความปลอดภัยด้วย

หน้าที่หลักของเราเตอร์คือ การหาเส้นทางที่ดีที่สุดในการส่งผ่านข้อมูล และเป็นตัวกลางในการส่งต่อข้อมูลไปยังเครือข่ายอื่น โดยในแต่ละเครือข่ายจะมีรูปแบบของ packet ที่แตกต่างกันตามโปรโตคอลที่ทำงานในระดับบน (ตั้งแต่เลเยอร์ที่ 3 ขึ้นไป) เช่น IP, IPX เมื่อมีการส่งข้อมูลก็จะบรรจุข้อมูลนั้นเป็น packet ในรูปแบบของเลเยอร์ที่ 2 เมื่อเราเตอร์ได้รับข้อมูลก็จะตรวจดูใน packet นี้เพื่อจะทราบว่าใช้โปรโตคอลแบบใด ซึ่งเราเตอร์

จะเข้าใจโปรโตคอลต่าง ๆ แล้ว จากนั้นก็จะตรวจดูเส้นทางส่งข้อมูลจากตาราง routing table ว่าจะต้องส่งข้อมูลนี้ไปยังเครือข่ายใดต่อจึงจะถึงปลายทางได้ แล้วจึงบรรจุข้อมูลลงเป็น packet ตามรูปแบบของเลเยอร์ที่ 2 อีกครั้งเพื่อส่งต่อไปยังเครือข่ายถัดไป

ไวเลส์ เราเตอร์ (Wireless Router)

ความแตกต่างของ เราเตอร์ กับ ไวเลส์เราเตอร์ ต่างกันตรงรูปแบบการเชื่อต่อโดยเราเตอร์ จะเชื่อมต่อผ่านสายสัญญาน ส่วนไวเลส์เราเตอร์ เชื่อต่อผ่านสัญญาน ไวไฟ แต่การทำงานทั่วไปจะเหมือนกัน

ฮับ (10 Base T Hub)

ความหมาย 10 คือ ความเร็วในการส่งข้อมูล 10 Mbps
Base คือ การส่งข้อมูลแบบ Baseband
T คือ Twisted Pair (UTP)
10 Base T จัดได้ว่าเป็นเครือข่ายที่นิยมใช้กันมากในปัจจุบัน เนื่องจากเป็นระบบเครือข่ายที่ติดตั้งง่ายและจำนวนสถานีที่ใช้งานจะต่อได้มาก กว่า ในความจริงแล้ว 10 Base T นั้นไม่ได้จัดอยู่ในมาตรฐาน Ethernet โดยตรง แต่เป็นเครือข่ายที่ผสมผสานระหว่าง Ethernet และ Star เข้าด้วย กัน ซึ่งจะมีอุปกรณ์ ตัวกลางที่เรียกว่า Concentrator หรือเรียกกันทั่วไปว่า HUB ที่คอยรับสัญญาณระหว่าง Workstation และ File Server โดยใน กรณีที่มีสายจากสถานีใดเสียหาย ก็จะไม่ส่งผลกระทบต่อระบบ

สวิทช์ (Switch)

Switch สำหรับ Industrial มักจะมีการออกแบบมาเพื่อให้มีการทำงานที่เร็วและมีประสิทธิภาพสูง สามารถรองรับการสื่อสารผ่านเครือข่าย Ethernet ได้มากกว่า 1000 Mbps (Gigabit Ethernet) โดยมีพอร์ตเชื่อมต่อ LAN หรือ WAN ที่มากมาย และสามารถรองรับการทำงานในระบบ Redundancy ได้ เพื่อเพิ่มความเชื่อมต่อเครือข่ายให้มีความเสถียรและมีประสิทธิภาพสูง

บริดจ์ (Bridge)

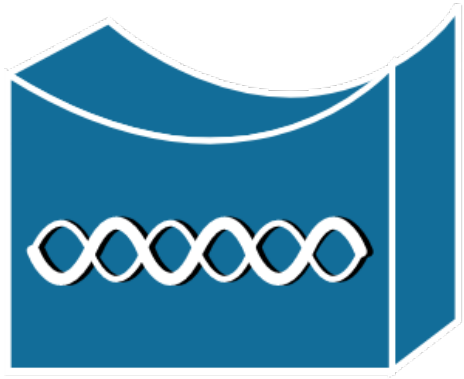
อุปกรณ์ Bridge เป็นสิ่งที่ใช้แก้ไขปัญหาในเรื่องสัญญาณที่วิ่งอยู่ในเครือข่ายมากเกินไปได้ โดยจะจัดแบ่งเครือข่ายออกเป็นเครือข่ายย่อยหรือ Network Segment (เน็ตเวิร์ก เซกเม้น) และจะทำการกลั่นกรองสัญญาณเท่าที่จำเป็นเพื่อส่งให้กับเครือข่ายย่อยที่ถูกต้องได้ ทำให้สัญญาณไม่มารบกวนกันหรือมีสัญญาณที่ไม่เกี่ยวข้องมาในเครือข่ายย่อย โดยไม่จำเป็น แต่ในทางกลับกัน ถ้ามีความจำเป็นต้องการสื่อสารกันข้ามเครือข่ายเป็นจำนวนมากแล้ว อุปกรณ์ Bridge ก็อาจกลายเป็นเสมือนคอขวดที่ทำให้เครือข่าย มีการทำงานช้าลงได้

บริดจ์ เป็นอุปกรณ์เชื่อมโยงเครือข่ายของเครือข่ายที่แยกจากกัน แต่เดิมบริดจ์ได้รับการออกแบบมาให้ใช้กับเครือข่ายประเภทเดียวกัน เช่น ใช้เชื่อมโยงระหว่าง Ethernet กับ Ethernet (อีเทอร์เน็ต) บริดจ์มีใช้มานานแล้ว หลังจากนั้นบริดจ์จึงเปลี่ยนมาเป็นเสมือนสะพานเชื่อมระหว่างสองเครือข่ายการติดต่อภายในเครือข่ายเดียวกันมีลักษณะการส่ง ข้อมูลแบบกระจาย Broadcasting (บรอดแคส) ดังนั้นจึงกระจายได้เฉพาะเครือข่ายเดียวกันเท่านั้นการรับส่งภายในเครือข่ายมีข้อกำหนดให้แพ็กเกจที่ส่งกระจายไปยังตัวรับได้ทุกตัว แต่ถ้ามีการส่งมาที่แอดเดรสต่างเครือข่ายบริดจ์จะนำข้อมูลเฉพาะแพ็กเกจนั้นส่งให้ บริดจ์จึงเป็นเสมือนตัวแบ่งแยกข้อมูลระหว่างเครือข่ายให้มีการสื่อสารภายในเครือข่าย ของตน ไม่ปะปนไปยังอีกเครือข่ายหนึ่ง เพื่อลดปัญหาปริมาณข้อมูลกระจายในสายสื่อสารมากเกินไป ในระยะหลังมีผู้พัฒนาบริดจ์ให้เชื่อมโยงเครือข่ายต่างชนิดกันได้ เช่น อีเทอร์เน็ตกับโทเก็นริง เป็นต้น หากมีการเชื่อมต่อเครือข่ายมากกว่าสองเครือข่ายเข้าด้วยกัน และ

เครือข่ายที่เชื่อมมีลักษณะหลากหลาย ซึ่งเป็นทั้งเครือข่ายแบบ LAN และ WAN อุปกรณ์ที่นิยมใช้ในการเชื่อมโยงคือ Router (เราเตอร์)

บริดจ์ทำหน้าที่เหมือนเป็นสะพาน เชื่อมระหว่างวงแลนเข้าหากัน จะเรียกง่ายๆ ก็คือ Bridge Mode (บริดจ์ โหมด) ทำให้วงแลน 2 วง ที่ต่างคนต่างทำงานกันเป็นปกติอยู่แล้ว สามารถเชื่อมต่อเข้าหากันได้ และต่างก็สามารถเข้าถึงอุปกรณ์ของอีกวงแลนหนึ่งได้

ไวเลส์บริดจ์ (Wireless Bridge)



ความแตกต่างของ บริดจ์ กับ ไวเลส์บริดจ์ ต่างกันตรงรูปแบบการเชื่อต่อโดยเรา บริดจ์ จะเชื่อมต่อผ่านสายสัญญาน ส่วนไวเลส์บริดจ์ เชื่อต่อผ่านสัญญาน ไวไฟ แต่การทำงานทั่วไปจะเหมือนกัน

VPN (Virtual Private Network)

VPN เป็นการสร้างการเชื่อมต่อเครือข่ายส่วนตัว ระหว่างอุปกรณ์ต่างๆ ผ่านอินเทอร์เน็ต โดยเราใช้ VPN เพื่อส่งข้อมูลอย่างปลอดภัยและไม่เปิดเผยตัวตนผ่านเครือข่ายสาธารณะ ซึ่งจะทำงานโดยปกปิดที่อยู่ IP ของผู้ใช้และเข้ารหัสข้อมูล เพื่อให้บุคคลที่ไม่ได้รับอนุญาตที่ได้รับข้อมูลดังกล่าวไม่สามารถอ่านได้

1. ความเป็นส่วนตัว (Privacy)

หากไม่มีเครือข่ายส่วนตัวเสมือน บุคคลที่สามสามารถบันทึกและขายข้อมูลส่วนบุคคลของคุณได้ เช่น รหัสผ่าน ข้อมูลบัตรเครดิต และประวัติการท่องเว็บ ดังนั้น VPN จึงใช้การเข้ารหัสเพื่อเก็บข้อมูลที่เป็นความลับนี้ให้เป็นส่วนตัว โดยเฉพาะอย่างยิ่งเมื่อเชื่อมต่อผ่านเครือข่าย Wi-Fi สาธารณะ

2. การปกปิดตัวตน (Anonymity)

ที่อยู่ IP ของคุณมีข้อมูลเกี่ยวกับตำแหน่งที่ตั้งและกิจกรรมการท่องเว็บของคุณ โดยเว็บไซต์ทั้งหมดบนอินเทอร์เน็ตติดตามข้อมูลนี้โดยใช้คุกกี้และเทคโนโลยีที่คล้ายคลึงกัน ซึ่งสามารถระบุตัวคุณได้ทุกเมื่อที่คุณเยี่ยมชมเว็บไซต์ต่างๆ ดังนั้นการเชื่อมต่อ VPN จะซ่อนที่อยู่ IP เพื่อปกปิดตัวตนของคุณบนอินเทอร์เน็ต

3. ความปลอดภัย (Security)

บริการ VPN ใช้การเข้ารหัสเพื่อปกป้องการเชื่อมต่ออินเทอร์เน็ตของคุณจากการเข้าถึงโดยไม่ได้รับอนุญาต นอกจากนี้ยังสามารถทำหน้าที่เป็นกลไกปิดการทำงาน โดยจะปิดโปรแกรมที่เลือกไว้ล่วงหน้าในกรณีที่พบกิจกรรมทางอินเทอร์เน็ตที่น่าสงสัย ซึ่งช่วยลดโอกาสที่ข้อมูลจะถูกโจมตีได้อีกด้วย โดยคุณสมบัติเหล่านี้ช่วยให้บริษัทต่างๆ สามารถให้การเข้าถึงระยะไกลแก่ผู้ใช้ที่ได้รับอนุญาตผ่านเครือข่ายธุรกิจของตนได้อีกด้วย

VPN ทำงานอย่างไร

การเชื่อมต่อ VPN จะเปลี่ยนเส้นทางแพคเก็ตข้อมูลจากเครื่องของคุณไปยังเซิร์ฟเวอร์ระยะไกลอื่น ก่อนที่จะส่งไปยังบุคคลที่สามผ่านทางอินเทอร์เน็ต โดยหลักการสำคัญที่อยู่เบื้องหลังเทคโนโลยี VPN ได้แก่

โปรโตคอลช่องทางการเชื่อมต่อ

เครือข่ายส่วนตัวเสมือนจะสร้างช่องทางการเชื่อมต่อข้อมูลที่ปลอดภัยระหว่างเครื่องในระบบของคุณกับเซิร์ฟเวอร์ VPN อื่นในตำแหน่งที่ตั้งที่อยู่ห่างออกไปหลายพันไมล์ เมื่อคุณออนไลน์ เซิร์ฟเวอร์ VPN นี้จะกลายเป็นต้นทางข้อมูลทั้งหมดของคุณ ผู้ให้บริการอินเทอร์เน็ต (ISP) และบริษัทภายนอกรายอื่นๆ จึงไม่สามารถมองเห็นรายละเอียดการใช้งานอินเทอร์เน็ตของคุณได้อีกต่อไป

การเข้ารหัส

โปรโตคอล VPN ต่างๆ เช่น IPSec จะแปลงข้อมูลของคุณก่อนที่จะส่งผ่านช่องทางการเชื่อมต่อข้อมูล โดย IPsec เป็นชุดโปรโตคอลในการรักษาความปลอดภัยการสื่อสารผ่านอินเทอร์เน็ตโปรโตคอล (IP) โดยการรับรองความถูกต้องและเข้ารหัสแต่ละแพคเก็ต IP ของสตรีมข้อมูล ซึ่งบริการ VPN จะทำหน้าที่เป็นตัวกรอง ทำให้ข้อมูลของคุณไม่สามารถอ่านได้ที่ปลายทางฝั่งหนึ่งและถอดรหัสได้เฉพาะที่ปลายอีกฝั่งหนึ่งเท่านั้น ซึ่งจะช่วยป้องกันการใช้ข้อมูลส่วนบุคคลในทางที่ผิด แม้ว่าการเชื่อมต่อเครือข่ายของคุณจะถูกโจมตีก็ตาม การรับส่งข้อมูลผ่านเครือข่ายจึงไม่มีความเสี่ยงที่จะถูกโจมตีอีกต่อไป และการเชื่อมต่ออินเทอร์เน็ตของคุณก็จะปลอดภัย