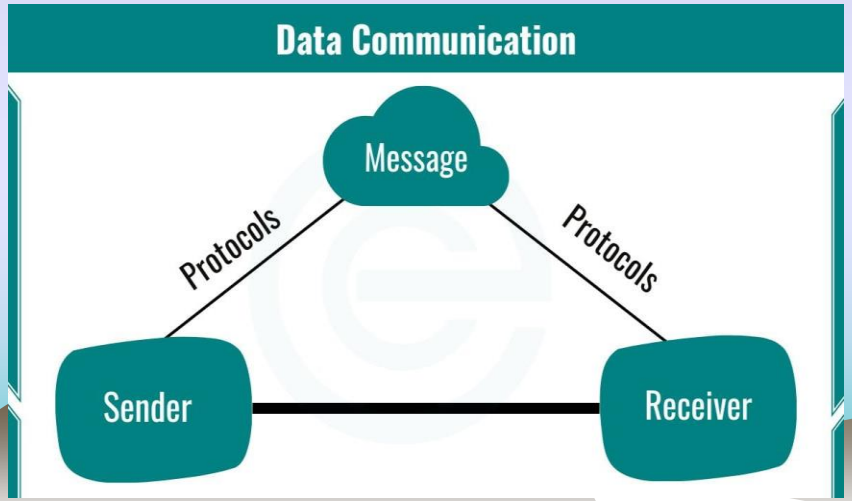
Data Communication
การสื่อสารข้อมูลและเครือข่ายคอมพิวเตอร์

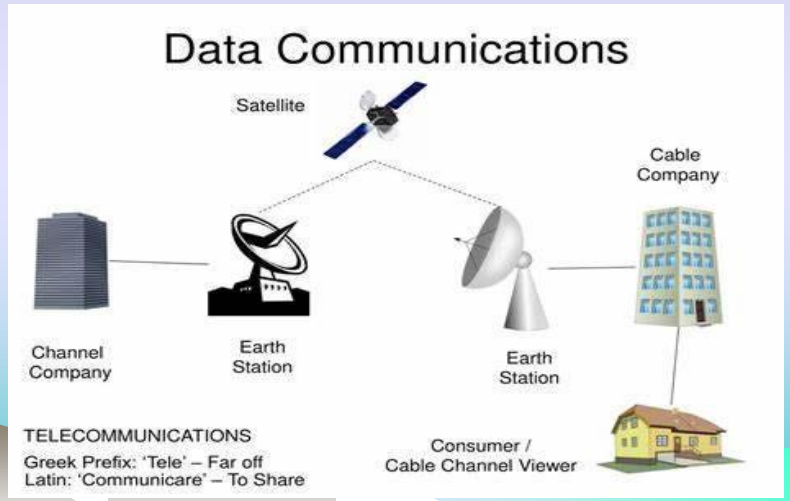
- ความรู้พื้นฐานของการสื่อสารข้อมูลทางอิเลคทรอนิกส์
- องค์ประกอบพื้นฐานของการสื่อสารข้อมูล
- การส่งข้อมูลแบบต่าง ๆ
- ความรู้พื้นฐานในการรับ-ส่งข้อมูล
- ช่องทางการรับ-ส่งสัญญาณ
- โปรโตคอล
- ระบบเครือข่าย LAN , MAN และ WAN
- โครงสร้างกายภาพของแลน
- อินเตอร์เนตและการใช้งาน

Dawn of the Net - How the Internet works

ความรู้พื้นฐานของการสื่อสารข้อมูลทางอิเลคทรอนิกส์

- การสื่อสารข้อมูลทางอิเลคทรอนิกส์ (Data Communications) คือ การแลกเปลี่ยนข้อมูลระหว่างต้นทางและปลายทาง โดยใช้อุปกรณ์ทางอิเลคทรอนิกส์ซึ่งเชื่อมต่อกันอยู่ด้วยสื่อกลางชนิดใดชนิดหนึ่ง
- เครือข่ายคอมพิวเตอร์ (Computer Network) คือระบบเชื่อมโยงระหว่างคอมพิวเตอร์ตั้งแต่ 2 ตัวขึ้นไป เพื่อสามารถทำการสื่อสารแลกเปลี่ยนข้อมูลอิเลคทรอนิกส์ได้



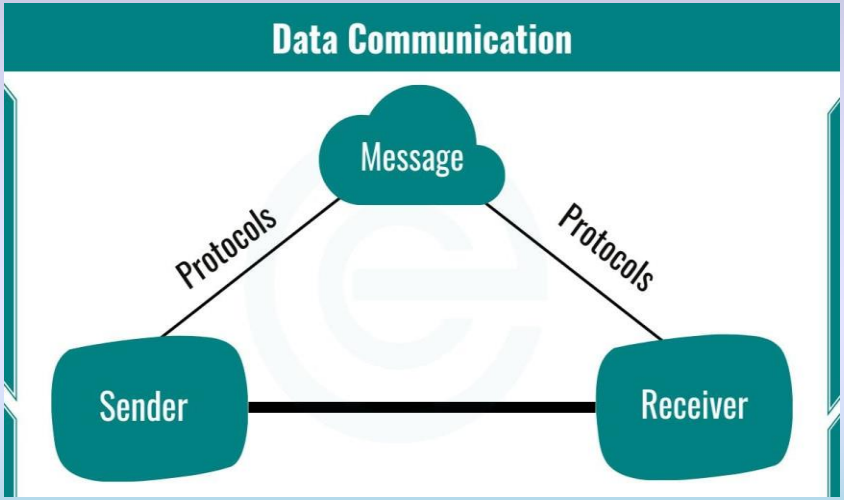


คำศัพท์ที่ควรทราบ

- Frequency : F = ความถี่ มีหน่วยเป็น เฮิร์ซ (Hertz : Hz)
  - **ช่วงความถี่ เรียกว่า spectrum**
  - **ในสเปกตรัมแบ่งเป็นช่วงๆ เรียกว่า band**
  - **ความกว้างของช่วงคลื่น = bandwidth**
- Amplitude : A = ความสูงของคลื่น
- bps = bit per second (bit = binary digit)
- channel = ช่องสัญญาณ
- protocol = วิธีการหรือรูปแบบที่ใช้ในการสื่อสาร

องค์ประกอบของการสื่อสาร

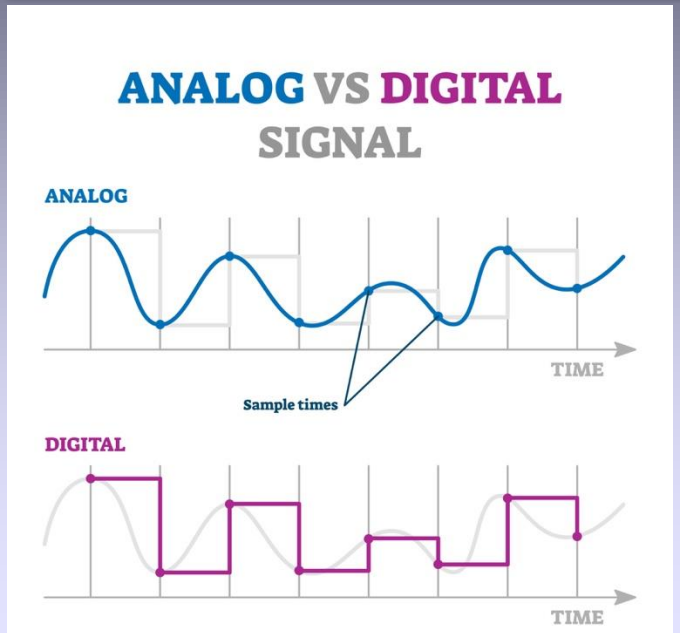
- ผู้ส่ง (Sender)
- ผู้รับ(Receiver)
- สื่อสัญญาณ หรือเส้นทางการส่ง หรือตัวกลาง (Medium)
- ข้อมูล (Data)
- โปรโตคอล (Protocol)



ชนิดของสัญญาณข้อมูล

จำแนกได้เป็น 2 ชนิดคือ

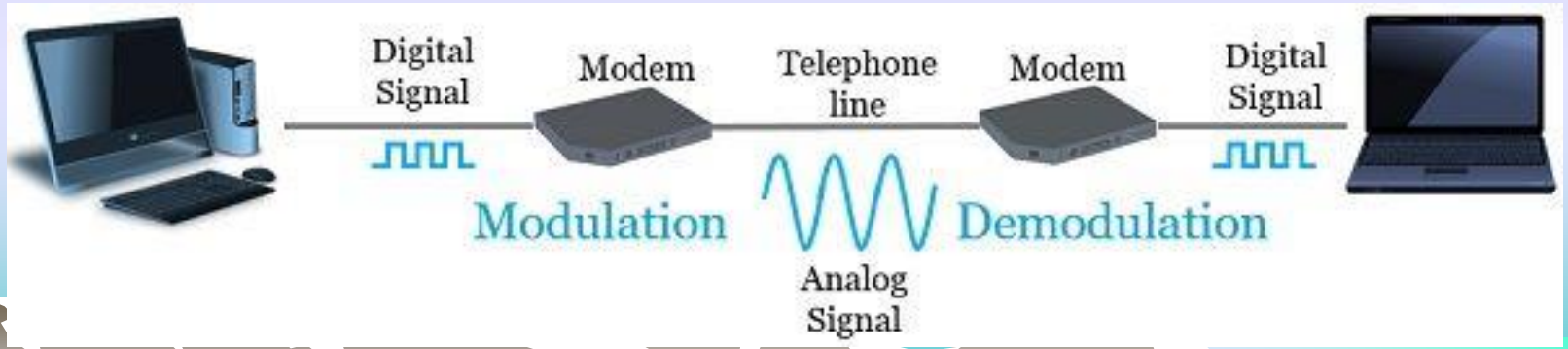
1. สัญญาณอนาล็อก (Analog signal)
2. สัญญาณดิจิตอล(Digital signal)



MODULATION & DEMODULATION

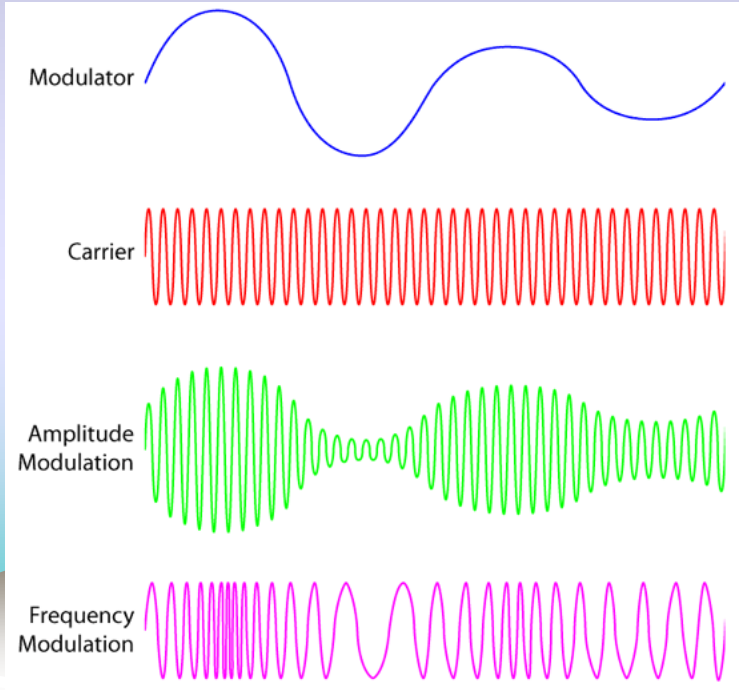
ในการส่งข้อมูลระหว่างเครื่องคอมพิวเตอร์โดยผ่ายสายสื่อสาร สัญญาณดิจิตอลต้องถูกแปลงเป็นสัญญาณอนาลอก ที่เรียกว่าคลื่นพาหะ(carrier wave) จากนั้นจึงแยกข้อมูลดิจิตอลจากคลื่นพาหะเพื่อให้เครื่องรับเข้าใจข้อมูล

- การแปลงสัญญาณจากดิจิตอลเป็นอนาลอก เรียกว่า มอดูเลชัน (Modulation) ซึ่งมีหลายวิธีเปลี่ยนคุณลักษณะของคลื่นพาหะมีหลายวิธี ได้แก่ วิธีการเปลี่ยนความถี่ และ วิธีการเปลี่ยนแอพลิจูด
- การแปลงสัญญาณจากอนาลอกเป็นดิจิตอล เรียกว่า ดีมอดูเลชัน (Demodulation) เป็นการแยกข้อมูลดิจิตัลออกจากคลื่นพาหะ



ในช่วงปลายศตวรรษที่สิบเก้ามนุษย์ค้นพบว่าเสียงสามารถส่งผ่านคลื่นอากาศได้จึงเริ่มยุคของวิทยุ วิทยุกลายเป็นรูปแบบการส่งสัญญาณที่ได้รับความนิยมมากที่สุดในช่วงแปดสิบปีแรกของศตวรรษที่ยี่สิบ มีสองวิธีหลักในการส่งสัญญาณวิทยุ AM (Amplitude Modulation) และ FM (Frequency Modulation)

- วิธีการเปลี่ยนความถี่คลื่น (Frequency Modulation : FM) เป็นวิธีการเปลี่ยนความถี่หรือจำนวนครั้งของการเกิดคลื่น ในช่วงเวลาหนึ่ง โดยช่วงของคลื่นที่ความถี่เพิ่มขึ้น จะหมายถึงการส่งข้อมูลที่เป็น 1
- วิธีการเปลี่ยนความสูงคลื่น (Amplitude Modulation : AM) เป็นวิธีการเปลี่ยนความสูงของคลื่น เมื่อมีการส่งข้อมุลที่เป็น 1 ซึ่งการส่งแบบนี้เหมาะจะใช้ส่งข้อมูลระยะไกล ได้ดีกว่าแบบ FM แต่อาจถูกรบกวนจากคลื่นสัญญาณอื่นได้ง่ายกว่า

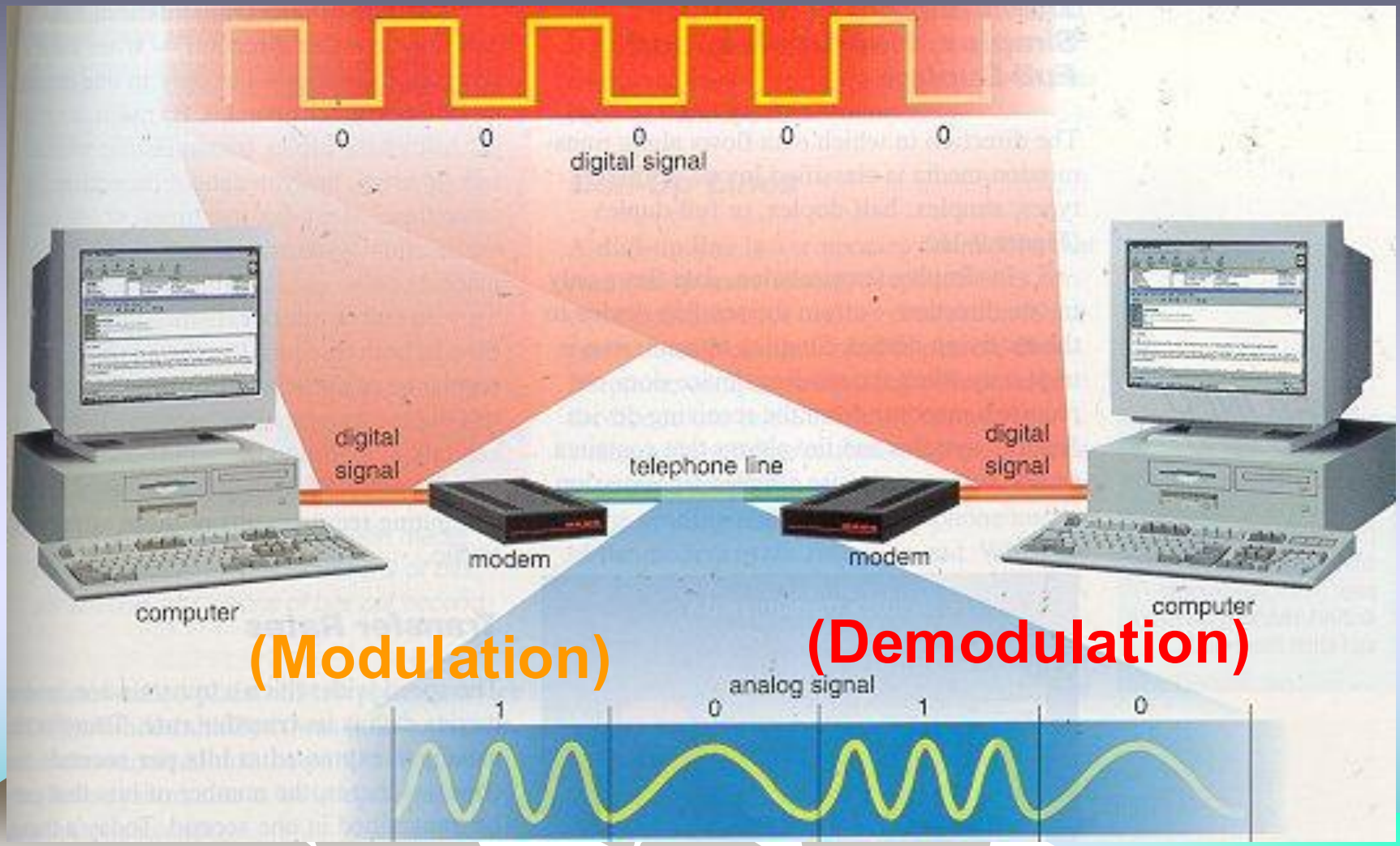


อุปกรณ์ที่ทำหน้าที่ในการแปลงสัญญาณจากดิจิตอลเป็นอนาลอก หรือจากอนาลอกเป็นดิจิตอล เรียกว่า **โมเด็ม** (MODEM มาจาก MOdulate-DEModulate) ซึ่งในปัจจุบันแบ่งได้เป็น 3 ประเภทใหญ่ ๆ คือ

1.โมเด็มที่ต่อภายนอก (External Modem)
2.โมเด็มที่ต่อแบบภายใน (Internal Modem)
3.โมเด็มไร้สาย (Wireless Modem)

ซึ่งมีความเร็วหลายระดับ ได้แก่ 9600 , 14400, 28800 bps หรือ 56000 Bps (56Kbps)

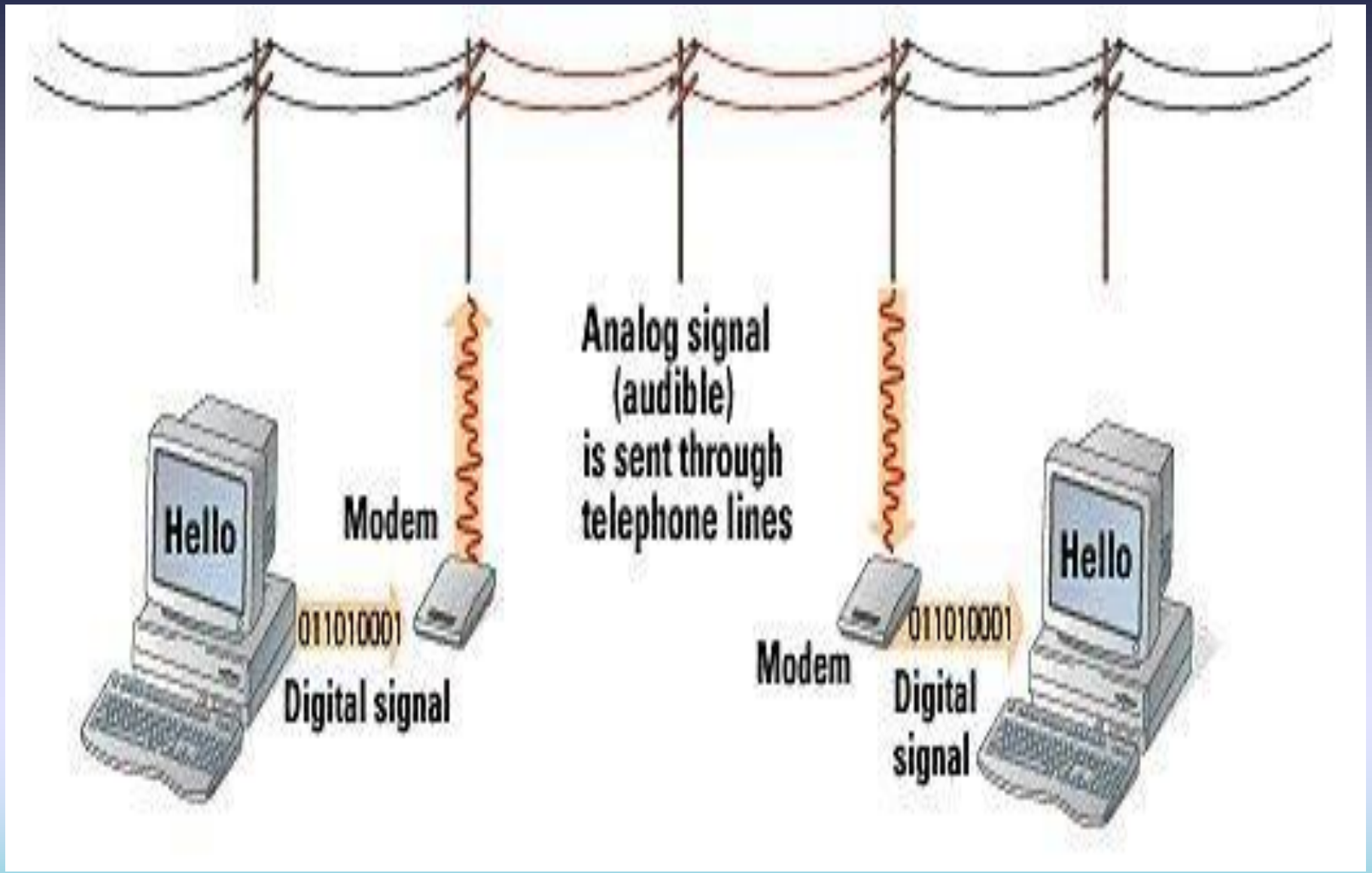
การสื่อสารผ่านสายโทรศัพท์



ความเร็วในการส่งผ่านข้อมูลของโมเด็ม

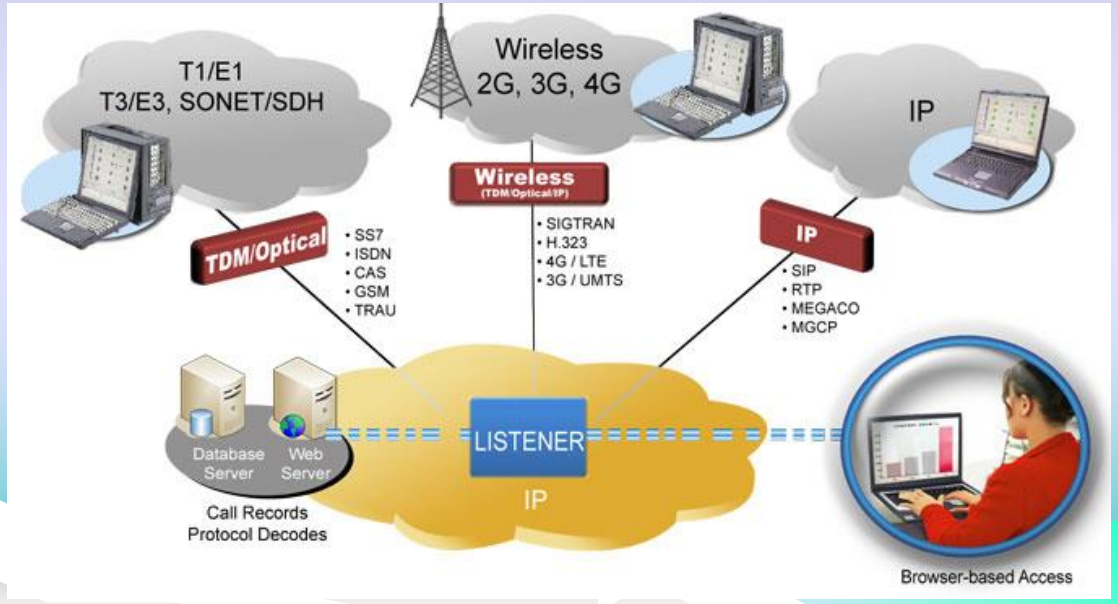
1. **bps** (bit per second) หมายถึง จำนวนบิตที่สามารถส่งได้ใน 1 วินาที (หมายถึงสัญญาณ **Digital)**

2. **Baud rate** หมายถึง จำนวนครั้งของการส่งสัญญาณใน 1 วินาที (หมายถึงสัญญาณ **Analog)**


Hello
Modem
011010001
Digital signal
Analog signal
(audible)
is sent through
telephone lines
Modem
011010001
Digital
signal
Hello

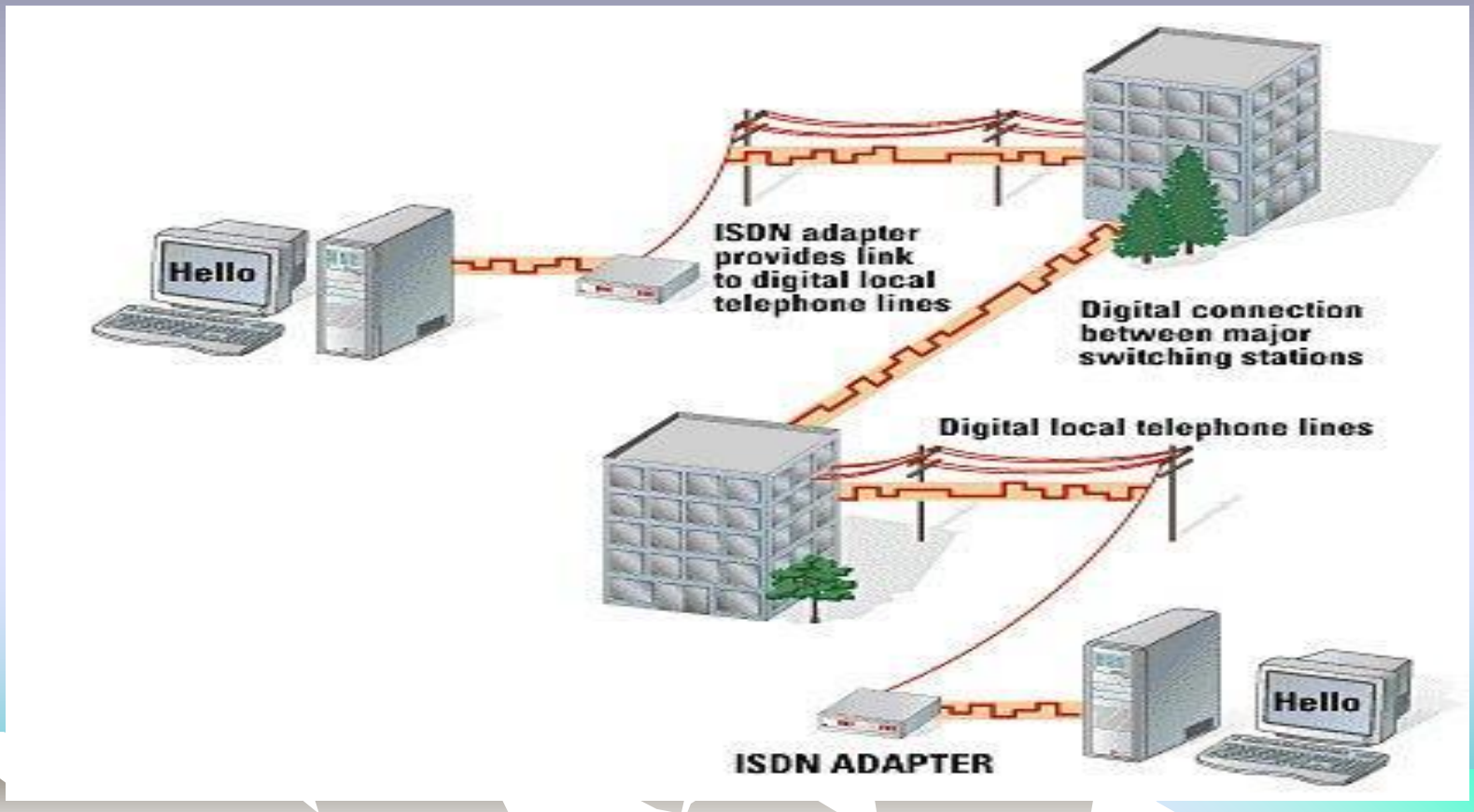
การเปลี่ยนจากระบบ Analog เป็น Digital

- การสื่อสารข้อมูลจะอยู่ในรูปของสัญญาณดิจิตอล (Digital) แทนที่จะเป็น Analog
- การส่งข้อมูลไม่จำเป็นต้องใช้ Modem แต่ต้องการเพียงแค่อุปกรณ์ที่ทำการจัดเรียงข้อมูลให้อยู่ในรูปที่สามารถส่งผ่านสายโทรศัพท์ได้
- ชนิดของ Digital line ที่เป็นที่รู้จักกันดีในปัจจุบันคือ ISDN, T1, และ T3



ISDN

- ISDN ย่อมาจาก Integrated Services Digital Network



การส่งข้อมูล (TRANSMISSION)

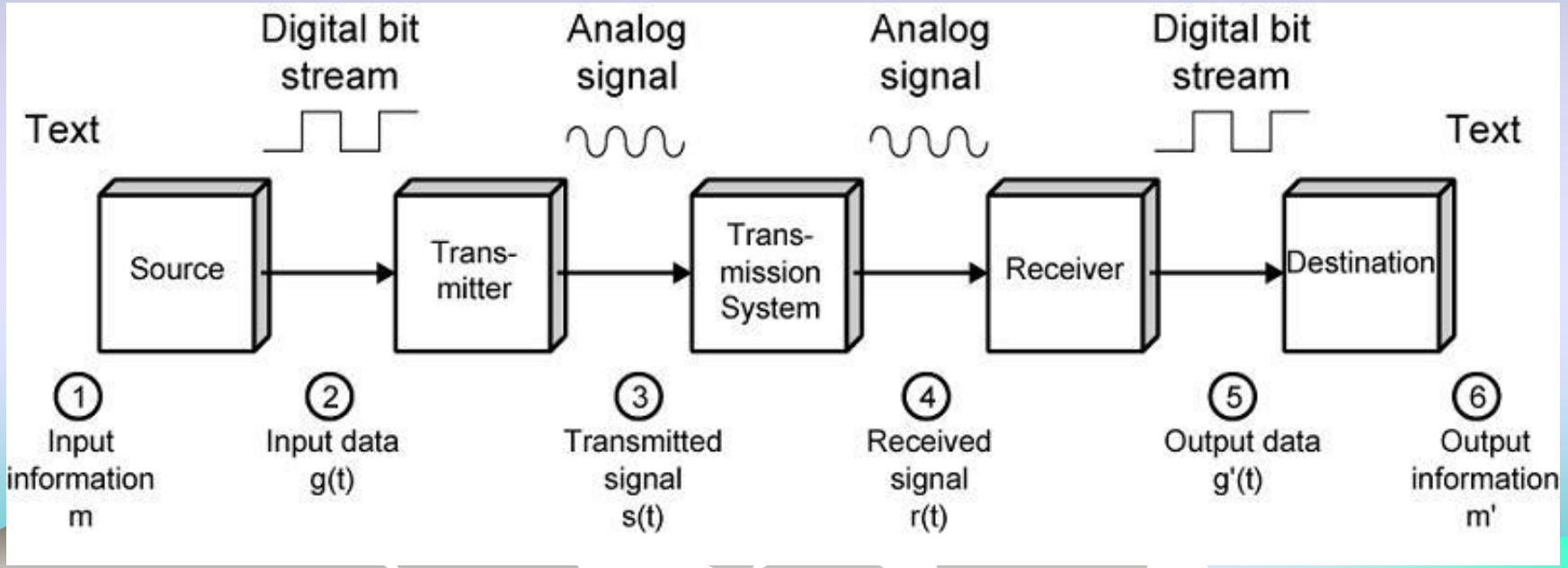
- **การส่งข้อมูล** หมายถึง การที่สายส่งสัญญาณในการสื่อสารจะเป็นตัวกลางที่จะนำเอาข้อมูลหรือข่าวสารจากจุดหนึ่งไปยังอีกจุดหนึ่งในระบบการสื่อสารข้อมูล

- การส่งสัญญาณแบบอนาลอก (Analog Transmission)

สัญญาณถูกส่งไปด้วยระดับแรงดันค่าต่าง ๆที่ต่อเนื่อง ส่วนมากจะอยู่ในรูปสัญญาณไฟฟ้า เช่น การพูดกันทางโทรศัพท์

- การส่งสัญญาณแบบดิจิตอล (Digital Transmission)

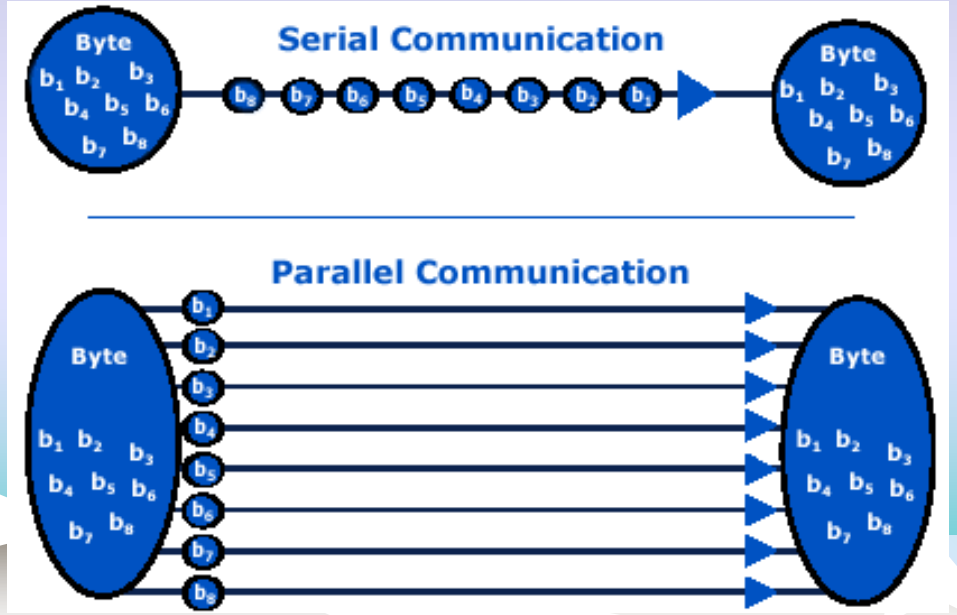
สัญญาณถูกส่งไปด้วยเลข 0 และ 1เท่านั้น มีการกำหนดรหัสไว้ อาจเรียกว่า สัญญาณพัลส์ (Pulse signal)



รูปแบบของการส่งผ่าน(รับส่ง)ข้อมูล

รูปแบบของสายส่งสัญญาณสื่อสารอาจประกอบด้วยสายส่งตั้งแต่หนึ่งสายขึ้นไป ซึ่งทำให้เกิดช่องทางการส่งข้อมูลได้มากกว่าหนึ่งช่องทาง รูปแบบของการส่งผ่านข้อมูลสามารถแบ่งได้เป็น 2 รูปแบบคือ

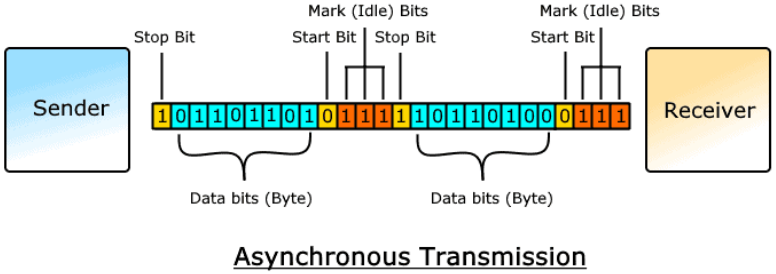
- การส่งผ่านข้อมูลแบบอนุกรม (Serial Transimision)
- การส่งผ่านข้อมูลแบบขนาน (Parallel Transimision)



วิธีการในการสื่อสารระหว่างอุปกรณ์

- การรับส่งข้อมูลแบบอนุกรม (Serial Transmission) เป็นการส่งข้อมูลทีละบิตต่อครั้ง หรือการส่งข้อมูลตัวอักขระแต่ละตัวเป็นกลุ่มบิต เรียงกันไปตามลำดับบนสายสื่อสารเพียงสายเดียว
  - การรับ-ส่งแบบไม่ประสานจังหวะ (Asynchronous Transmission) อาจเรียกว่าวิธีการส่ง-รับแบบระบุจุดเริ่มและจุดสิ้นสุด (start-stop transmission) มักใช้ในการติดต่อระหว่างคอมพิวเตอร์กับอุปกรณ์รอบข้าง โดยข้อมูลที่ติดต่อระหว่างอุปกรณ์เครือข่าย 2 ชิ้นนี้ จะประกอบขึ้นจาก 4 ส่วน คือ
    - บิตเริ่มต้น (start bit)
    - บิตของข้อมูลที่สื่อสาร (transmission data) 8 bit
    - บิตตรวจข้อผิดพลาด (error check bit)
    - บิตปิดท้าย (stop bit)

เป็นการสื่อสารที่ความเร็วต่ำ เนื่องจากสูญเสียช่องการสื่อสารไป 2 บิต



Asynchronous Transmission

- การรับ-ส่งแบบประสานจังหวะ (Synchronous Transmission) ข้อมูลสามารถส่งได้อย่างรวดเร็ว เนื่องจากทำการส่งแต่ละกลุ่มซึ่งเรียกว่า เฟรม (frameหรือ packets หรือ block) โดยมีข้อมูลเริ่มต้นและสิ้นสุดบอกในแต่ละกลุ่มข้อมูล รวมทั้งมีข้อมูลตรวจความผิดพลาดประจำกลุ่มด้วย มักใช้ในการติดต่อระหว่างคอมพิวเตอร์ต้องใช้อุปกรณ์ที่ทำงานซับซ้อน และมีราคาแพง

- การรับส่งข้อมูลแบบขนาน (Parallel Transmission) เป็นการส่งข้อมูลที่เร็ว เนื่องจากทุกบิตจะถูกส่งออกไปทีเดียวพร้อม ๆกัน(ตามจำนวนสายของสื่อ)แบบขนานกันไป ไม่ต้องเรียงกัน มักใช้ในการติดต่อระหว่างคอมพิวเตอร์กับอุปกรณ์รอบข้าง และใช้ส่งข้อมูลในระยะทางใกล้ ๆ แต่จะเสียค่าใช้จ่ายสูง เพราะต้องมีสายสื่อหลายเส้น

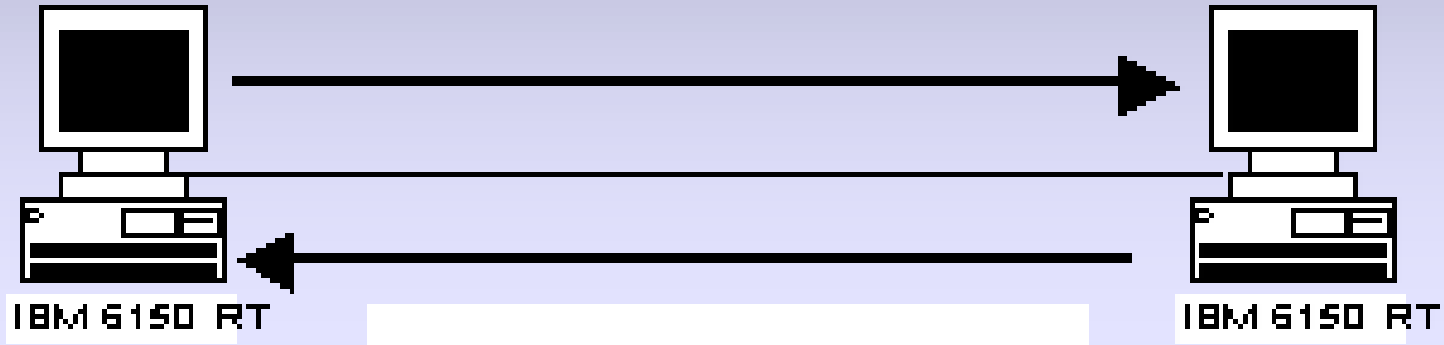
ทิศทางการสื่อสารข้อมูล

- แบบทิศทางเดียว (Simplex Transmission)

ประกอบด้วย หนึ่งหรือหลายช่องทางการส่ง สามารถส่งข้อมูลในเวลาใดเวลาหนึ่ง ไปในทิศทางเดียวเท่านั้น หรือพูดอีกนัยหนึ่งคือ ผู้ส่งสามารถส่งข้อมูลไปให้แก่ผู้รับเพียงฝ่ายเดียว ส่วนผู้รับไม่สามารถโต้ตอบกลับได้ เช่นการส่งวิทยุกระจายเสียง

- แบบกึ่งสองทิศทาง หรือ สองทิศทางสลับกัน (Half-duplex Transmission)

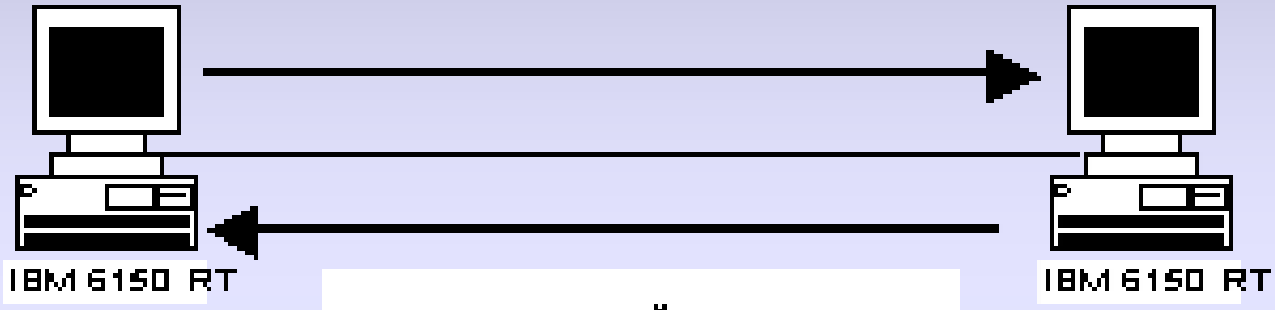
สามารถส่งข้อมูลในเวลาใดเวลาหนึ่ง ไปในทิศทางเดียวเท่านั้น ทั้งฝ่ายส่งและฝ่ายรับ หรือพูดอีกนัยหนึ่งคือ ผู้ส่งสามารถส่งข้อมูลไปให้แก่ผู้รับ ส่วนผู้รับก็สามารถโต้ตอบกลับได้ แต่ไม่สามารถส่งสวนทางกันได้ในเวลาเดียวกัน เช่นการส่งวิทยุของตำรวจ



สองทิศทางสลับกัน

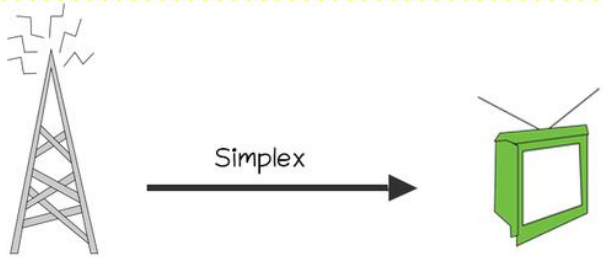
- แบบสองทิศทางพร้อมกัน (Full-duplex Transmission)

สามารถส่งข้อมูลในเวลาใดเวลาหนึ่ง ได้ทั้ง2ทิศทาง ทั้งฝ่ายส่งและฝ่ายรับ หรือพูดอีกนัยหนึ่งคือ ผู้ส่งและผู้รับ สามารถโต้ตอบสวนทางกันได้ในเวลาเดียวกัน เช่น การส่งสัญญาณโทรศัพท์

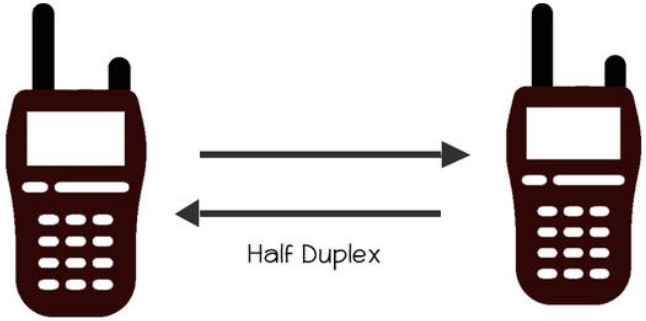


สองทิศทางส่งได้พร้อมกัน

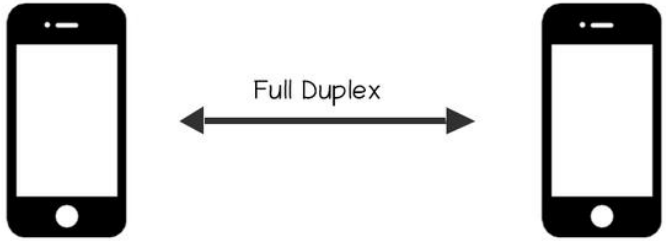
การส่งสัญญาณข้อมูล



Simplex : การสื่อสารแบบซิมเพล็กซ์ หรือการติดต่อสื่อสารแบบทางเดียว



Half-Duplex : การสื่อสารแบบฮาล์ฟดูเพล็กซ์ หรือการติดต่อสื่อสารแบบทางใดทางหนึ่ง



Full-Duplex : การสื่อสารแบบฟูลดูเพล็กซ์ หรือการติดต่อสื่อสารแบบสองทิศทาง

VRPRO SERVICE

ช่องทางการสื่อสาร/ตัวกลางการสื่อสาร (COMMUNICATION CHANNEL)

ตัวกลางการสื่อสารเป็นสื่อที่ใช้ต่อเชื่อมการสื่อสารระหว่างผู้ส่งกับผู้รับข้อมูล แบ่งเป็น 2 แบบ คือ

1.แบบมีสาย (Wired Media)

2.แบบไร้สาย (Wireless Media)

สื่อนำข้อมูลแบบมีสาย (WIRED MEDIA)

- สายคู่เกลียวแบบมีชีลด์ และไม่มีชิลด์ (Shielded and Unshielded Twisted-Pair Cable)

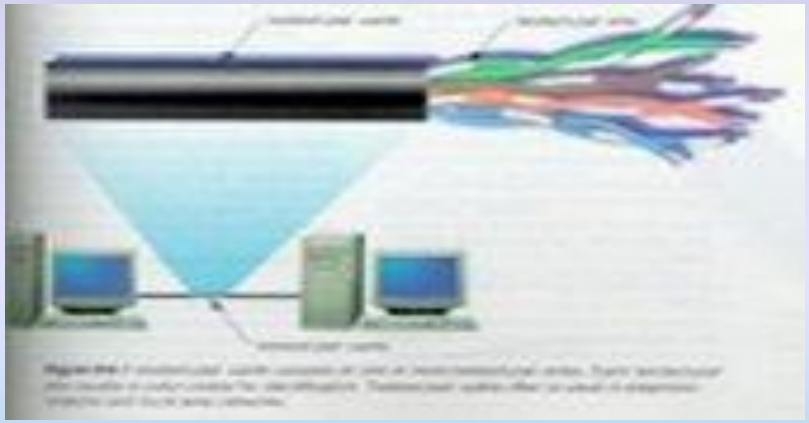
เป็นสายราคาถูกที่สุด ประกอบด้วยสายทองแดงที่มีฉนวนหุ้มจำนวน 2 เส้น นำมาพันกันเป็นเกลียว สามารถลดการรบกวนจากสนามแม่เหล็กไฟฟ้า

สายเกลียวคู่หนึ่งหมายถึงหนึ่งช่องทางการสื่อสาร ซึ่งอาจมีหลายสายมัดรวมกันเป็นสายใหญ่ เพื่อใช้งานพร้อมกัน

- สายคู่เกลียวแบบไม่มีชีลด์ (UTP) ใช้เดินสายโทรศัพท์และระบบเครือข่ายระยะใกล้ มีราคาต่ำ
- คู่เกลียวแบบมีชีลด์ (STP) มีฉนวนโลหะหุ้มภายนอก ทำให้ป้องกันสัญญาณรบกวนได้ดีขึ้น

Twisted pair: เป็นสายทองแดงบิดเกลียวหุ้มด้วยฉนวน

- ชนิดที่เป็นที่นิยม คือ **UTP** ซึ่งย่อมาจาก Unshielded Twisted-Pair
- Twisted-pair แบบที่มีฉนวนหุ้ม (Shield) เรียกว่า STP
- ข้อดีคือราคาถูก หาง่าย เช่น สายโทรศัพท์, สาย CAT 5
- อัตราการับ-ส่งข้อมูล 1-128 Mbps
- ข้อเสีย คือสัญญาณถูกรบกวนได้ง่าย



- สายโคแอกเชียล (Coaxial Cable) เรียกสั้น ๆว่า สายโคแอก

สามารถส่งได้ไกลกว่าและเร็วกว่าสายคู่บิดเกลียว แต่ราคาสูงกว่า ประกอบด้วยสายส่งข้อมูลที่เป็นทองแดงที่มีฉนวนหุ้มอยู่ตรงกลาง จากนั้นหุ้มด้วยตัวนำที่เป็นสายกราวนด์แล้วจึงหุ้มด้วยฉนวนอีกชั้นหนึ่ง ทำให้สามารถลดการรบกวนจากสนามแม่เหล็กไฟฟ้าได้ดีกว่า สามารถส่งข้อมูลและเสียงได้เร็ว

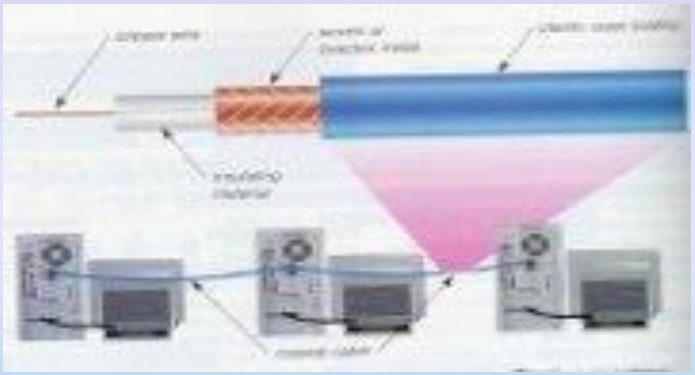
- สายชนิดความต้านทาน 50 โอห์ม เรียกว่า แบบช่วงสัญญาณแคบ (baseband) ใช้สำหรับส่งข้อมูลแบบดิจิตอล

- สายชนิดความต้านทาน 75 โอห์ม เรียกว่า แบบช่วงสัญญาณกว้าง (broadband) มีความกว้างของสัญญาณมากกว่า 4 KHz ใช้สำหรับส่งข้อมูลแบบอนาลอก

พบการใช้งานในสายเคเบิลทีวี การวางสายใต้ทะเลและใต้ดิน ปัจจุบันพบการใช้น้อยลงเนื่องจากแบบคู่เกลียวมีการพัฒนามากขึ้น

Coaxial: เป็นสายทองแดงหุ้มด้วยฉนวน

- อาจเรียกว่าสาย Coax เช่น สาย Cable TV
- แบ่งเป็นแบบ Thick และ Thin
- ข้อดี รับ-ส่งข้อมูลได้เร็วกว่าแบบแรกประมาณ 200 เมกะบิตต่อ วินาที
- ปัจจุบันใช้น้อยลง เนื่องจากความก้าวหน้าของ UTP ที่สามารถส่งข้อมูลได้เร็ว ติดตั้งง่ายกว่า มีราคาถูก จึงเป็นที่นิยมมากกว่า



สายใยแก้วนำแสง (Fiber Optic Cable)

ประกอบด้วยใยแก้วหรือพลาสติกอยู่ตรงกลาง จากนั้นหุ้มด้วยใยแก้วอีกชนิดหนึ่ง (cladding) แล้วจึงหุ้มด้วยฉนวนชั้นนอกสุด ใยแก้วทำหน้าที่เหมือนกระจกที่สะท้อนสัญญาณแสงให้สะท้อนไปมาจากจุดต้นทางไปจนถึงจุดปลายทาง สามารถส่งข้อมูลจำนวนมากๆได้เร็วมาก, ส่งได้ไกล (ไกลถึง 30 km.) และปลอดภัยจากสัญญาณรบกวน เนื่องจากใช้แสงเป็นตัวนำ

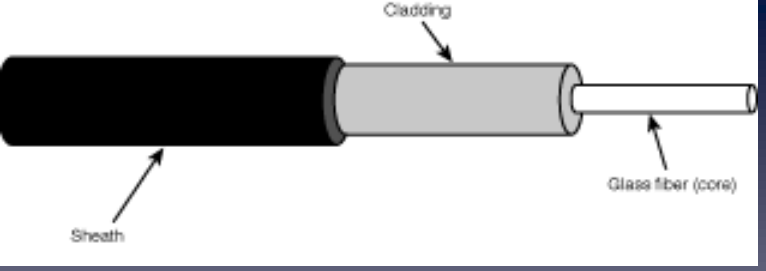
การสื่อสารข้อมูลโดยสายใยแก้ว ประกอบด้วย 3 ส่วน คือ

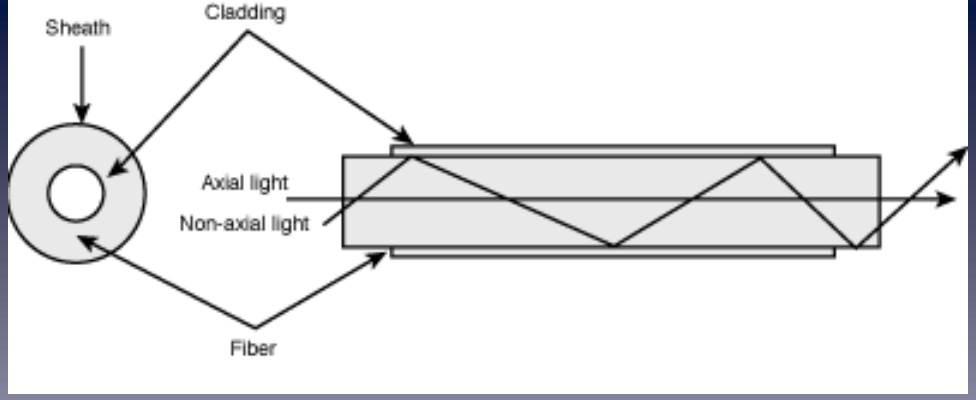
- **อุปกรณ์กำเนิดแสง**
- **สายใยแก้วนำแสง**
- **อุปกรณ์ตรวจจับแสง**

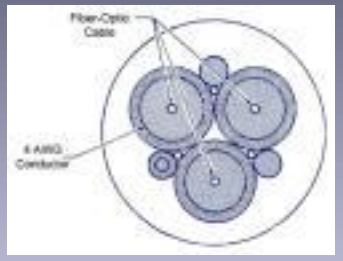
โดยปกติการส่งสัญญาณแสง(light pulse) ออกไป 1 ครั้งใช้แทน บิต “1” และการไม่ส่งสัญญาณแสงหมายถึงบิต “0”

สายใยแก้วที่ลำแสงเดินทางเป็นเส้นตรงไม่หักเห = single-mode fiber มีขนาด 8-10 ไมครอน สายใยแก้วที่มีหลายลำแสงส่งไปพร้อมๆกันได้ = multi-mode fiber มีขนาด 50 ไมครอน

ข้อเสียคือติดตั้งและบำรุงรักษายาก รวมทั้งมีราคาแพง


Cladding
Glass fiber (core)
Sheath


Sheath
Cladding
Axial light
Non-axial light
Fiber


Fiber-Optic Cable
4 AWG Conductor

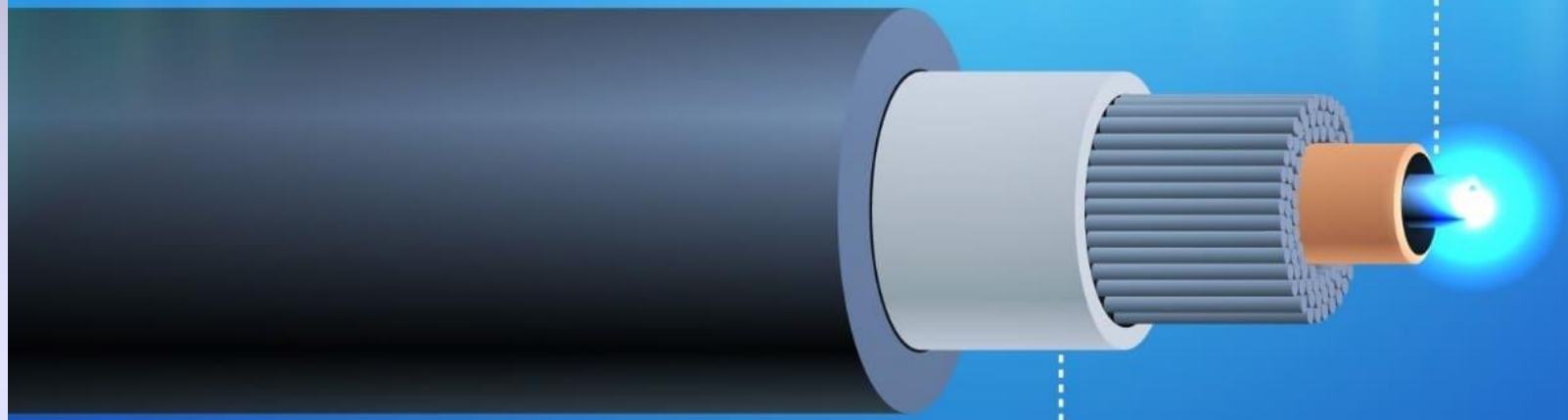
There are three major parts of a fiber optic cable

The Coating

It's a protective layer that protects the cable against mechanical stresses and environmental factors.

The Core

Central region where light pulses travel. It is made from material with a high refractive index.

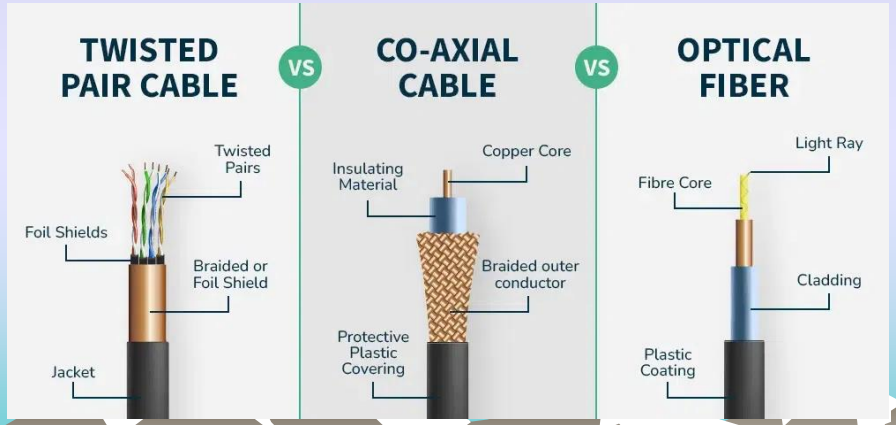


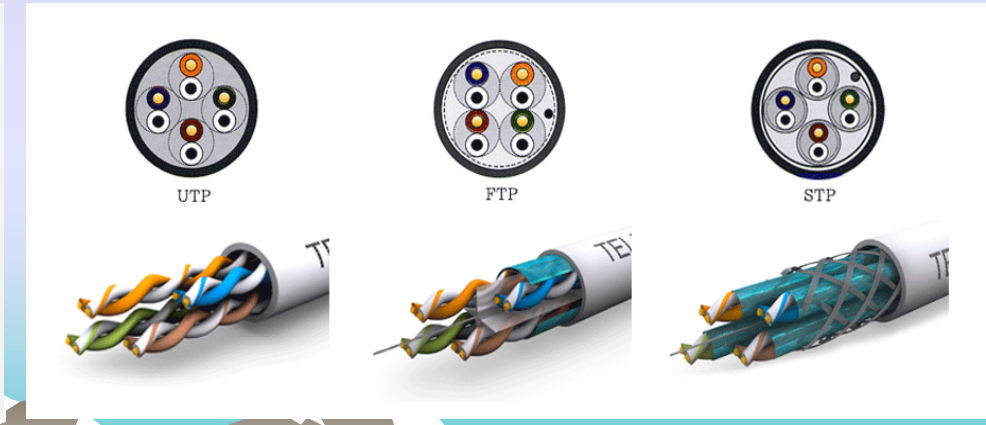
Cladding

Acting as an optical boundary, cladding contains the light within the core through total internal reflection.

ตารางเปรียบเทียบการใช้งานสายเคเบิลต่าง ๆ

Characteristics	UTP	STP	Coaxial Cables	Fiber Optic Cables
Bandwidth	10 Mbps - 100 Mbps	10 Mbps - 100 Mbps	10 Mbps	100 Mbps -1 Gbps
Maximum cable segment	100 meters	100 meters	200 - 500 meters	2 k.m. - 100 k.m.
Interference rating	Poor	Better than UTP	Better than Twisted Pair Cable	Very good as compared to any other cable
Installation cost	Cheap	Costly than UTP	Costlier than twisted pair wires	Costliest to install
Bend radius	360 degrees / feet	360 degrees / feet	360 degrees / feet or 30 degrees / feet	30 degrees / feet
Security	Low	Low	Low	High





Comparison	UTP	STP	FTP
Full Name	Unshielded twisted pair	Shielded twisted pair	Foil twisted pairs
Cable Shield	None	Braiding	Foil
Twisted Pair Shield	None	None	None
Crosstalk	High crosstalk	Low crosstalk	Low crosstalk
Termination	Easier to terminate and saves time	Difficult and takes a longer time	Difficult and takes a longer time
Bonding and Grounding	Not required	Necessary	Necessary
Data rate	Low	High	High
Application	Home network	Longer distance network	Longer distance network
Costs	Cheaper and does not require much maintenance	Moderately expensive	Moderately expensive

1. ชนิดติดตั้งภายในอาคาร (Indoor Cable)

สายสัญญาณสำหรับติดตั้งภายในอาคารนั้น เปลือกนอกมักนิยมทำจากวัสดุ PVC เนื่องจากมีความยืดหยุ่นและสามารถป้องกันการลามไฟได้ นอกจากนี้ได้มีข้อกำหนดหรือมาตรฐานป้องกันทางด้านอัคคีภัย

จึงต้องมีการใส่สารพิเศษเข้าไป ทำให้สามารถแบ่งชนิดของสายภายในอาคารที่ใช้กันแพร่หลาย 4 ชนิดด้วยกัน

- CM (Communication Metallic) เป็นสายที่สามารถป้องกันการลามไฟได้ในแนวราบ เหมาะสำหรับการใช้งานทั่วไป เช่นการติดตั้งสายแนวราบภายในชั้นเดียวกัน (Horizontal Wiring)
- CMR (Communication Metallic Riser) สายชนิดนี้สามารถป้องกันการลามไฟทั้งแนวราบและแนวดิ่ง มักใช้ในการเดินสายสัญญาณระหว่างชั้นในอาคารโดยผ่านช่องเดินสายของตัวอาคาร (Vertical Shaft)
- CMP (Communication Metallic Plenum)เป็นสายที่เหมาะสำหรับการติดตั้งเดินสายบนฝ้าเพดาน หรือบริเวณช่องว่างเหนือฝ้าที่มีอากาศไหลเวียน (Plenum Space) แต่ไม่สามารถป้องกันการลามไฟในแนวดิ่งได้
- LSZH (Low Smoke Zero Halogen)สามารถป้องกันการลามไฟได้ทั้งในแนวราบและแนวดิ่งเหมือน CMR แต่มีคุณสมบัติเพิ่มเติมคือเมื่อเกิดอัคคีภัย สายชนิดนี้จะมีควันน้อยและไม่ก่อให้เกิดสารพิษ

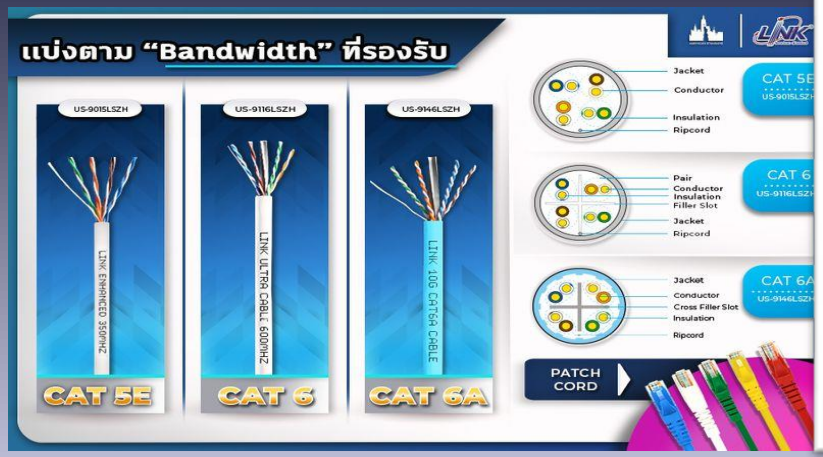
2. ชนิดติดตั้งภายนอกอาคาร (Outdoor Cable)

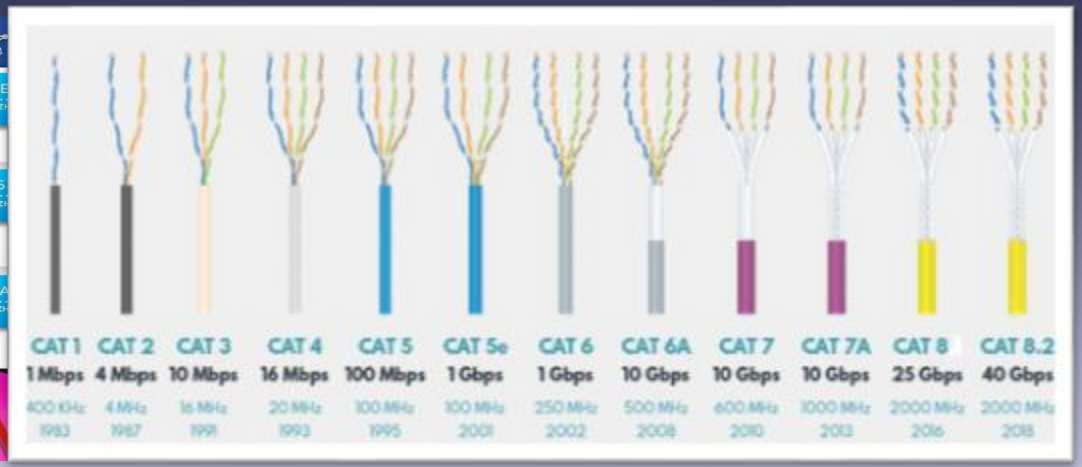
สายสัญญาณสำหรับติดตั้งภายนอกอาคารนั้น จะมีเปลือกนอกทำจากวัสดุ PE (Polyethylene) ซึ่งมีคุณสมบัติทนทานต่อสภาพแวดล้อมภายนอก ไม่สึกกร่อน แต่จะไม่สามารถป้องกันการลามไฟได้ ดังนั้นเราควรเลือกสายให้ถูกต้องตามชนิดของการใช้งาน

แบ่งตามลักษณะการป้องกันสัญญาณรบกวน

1. ชนิดไม่มีฉนวนป้องกันสัญญาณรบกวน : Unshield Twisted Pair (UTP) เป็นสายทองแดงคู่บิดตีเกลียวแบบไม่มีชิลด์ป้องกันสัญญาณรบกวน โดยตัวนำสัญญาณจะมี 8 เส้น (4คู่) เป็นทองแดงแท้ นิยมใช้กับระบบคอมพิวเตอร์ทั่วๆ ไป
2. ชนิดมีฉนวนป้องกันสัญญาณรบกวน : Foil Twisted Pair (FTP) เป็นสายทองแดงคู่ บิดตีเกลียวแบบมีชิลด์ป้องกันสัญญาณรบกวน นิยมใช้งานในพื้นที่ ที่มีสัญญาณรบกวนสูง เช่น โรงงานอุตสาหกรรม ติดตั้งผ่านเครื่องจักรขนาดใหญ่ ไฟฟ้าแรงสูง ปลั๊กไฟ ฯลฯ

3. แบ่งตาม Bandwidth ที่รองรับได้





1. Category 5E (CAT 5E)
เป็นสาย LAN (UTP) ทองแดงที่มีความเร็วต่ำ พัฒนามาจากสาย CAT 5 เดิม ออกแบบมาเพื่อรองรับ Bandwidth อยู่ที่ 100-200 MHz ความเร็วสูงสุดอยู่ที่ 1 Gbps ในระยะทางไม่เกิน 100 เมตร
2. Category 6 (CAT 6)
เป็นสาย LAN (UTP) ทองแดงที่มีความเร็ว ถูกผลิตขึ้นมาตามมาตรฐานของ Gigabit Ethernet ออกแบบมาเพื่อรองรับ Bandwidth อยู่ที่ 250 MHz ความเร็วสูงสุดอยู่ที่ 10 Gbps ในระยะทางไม่เกิน 55 เมตร
3. Category 6A (CAT 6A)
เป็นสาย LAN (UTP) ทองแดงที่มีความเร็ว ออกแบบมาเพื่อรองรับ Bandwidth อยู่ที่ 500 MHz ความเร็วสูงสุดอยู่ที่ 10 Gbps ในระยะทางไม่เกิน 100 เมตร
4. Category 8 (CAT 8)
เป็นสาย LAN (UTP) ทองแดงที่มีความเร็ว ออกแบบมาเพื่อรองรับ Bandwidth อยู่ที่ 2GHz ความเร็วสูงสุดอยู่ที่ 25/40 Gbps ในระยะทางไม่เกิน 30 เมตร

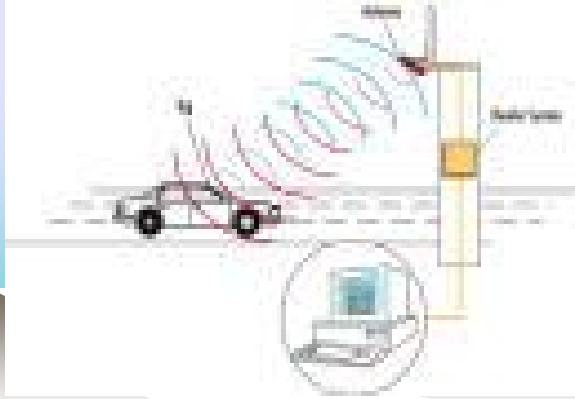
สื่อนำข้อมูลแบบไร้สาย (WIRELESS MEDIA)

คลื่นสัญญาณวิทยุ (Radio Wave)

เป็นช่วงคลื่นที่สร้างได้ง่าย ส่งได้ระยะทางไกล สามารถผ่านสิ่งกีดขวางได้ดี เดินทางออกจากแหล่งได้ทุกทิศทาง

ข้อเสียในตัวเอง ที่ความถี่ต่ำ สัญญาณคลื่นจะสามารถเดินทางผ่านวัตถุกีดขวางได้เป็นอย่างดี แต่กำลังสัญญาณจะลดลงอย่างรวดเร็วเมื่อเดินทางไกลออกไป ที่ความถี่สูงคลื่นจะเดินทางในแนวเกือบตรง แต่จะเกิดการสะท้อนเมื่อถูกขวางกั้น และจะถูกดูดซึมเมื่อเดินทางผ่านสายฝน

นอกจากนี้ คลื่นทุกความถี่ยังถูกรบกวนได้ง่ายจากการทำงานของมอเตอร์และอุปกรณ์ไฟฟ้า



การเชื่อมโยงแบบไร้สายด้วยคลื่นวิทยุ เข้าสู่ผู้ใช้ปลายทาง

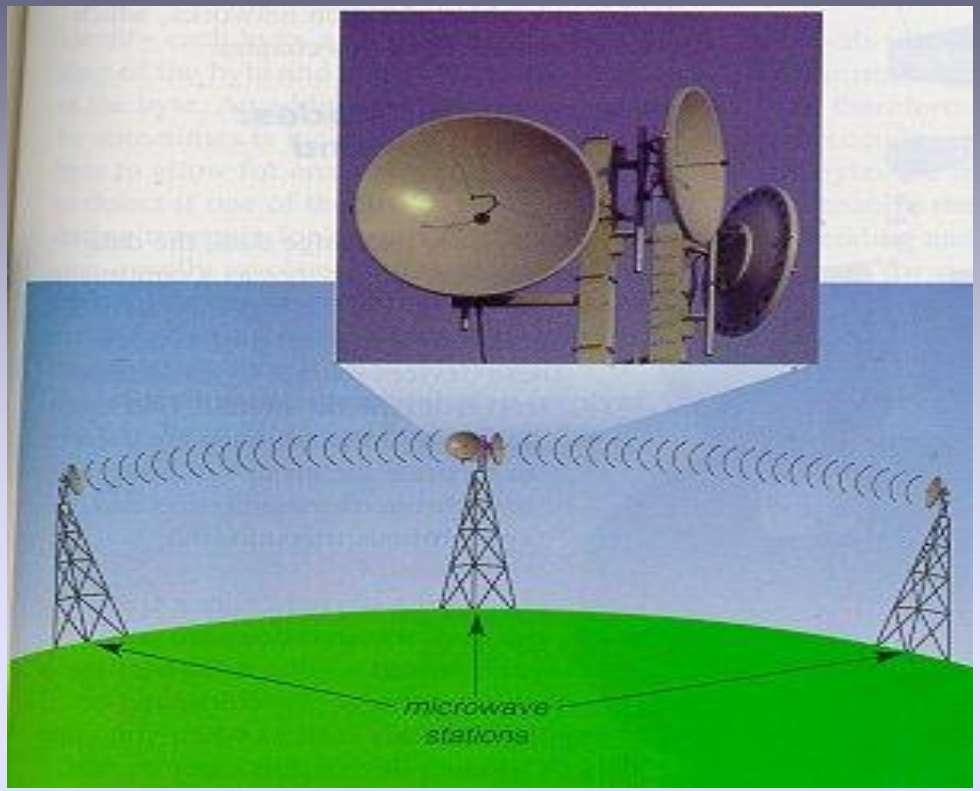
สัญญาณไมโครเวฟ (Microwave)

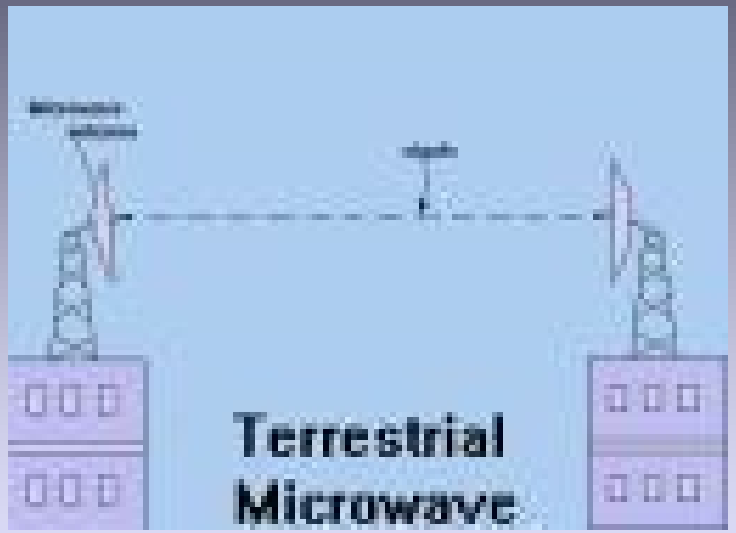
ใช้วิธีส่งสัญญาณที่มีความถี่สูงกว่าคลื่นวิทยุเป็นทอด ๆ จากสถานีหนึ่งไปสถานีหนึ่ง บ่อยครั้งจะถูกเรียกว่า สัญญาณแบบเส้นสายตา (line of sight) เนื่องจากสัญญาณที่ส่งไปได้ไม่ไกลกว่าเส้นขอบฟ้าโลก เพราะเดินทางเป็นเส้นตรง ดังนั้นสถานีจึงตั้งในที่สูง เพื่อช่วยให้ส่งได้ไกลขึ้น ปกติสถานีหนึ่งจะครอบคลุมพื้นที่สัญญาณประมาณ 30- 50 กม. สามารถส่งสัญญาณหลายความถี่ในทิศทางเดียวกันได้โดยไม่รบกวนกันเอง ราคาถูก ติดตั้งง่าย มีอัตราการส่งข้อมูลสูง

ข้อเสีย

สัญญาณอาจถูกรบกวนได้จาก อุณหภูมิ พายุและฝน และยังไม่สามารถผ่านสิ่งกีดขวางได้ และบางครั้งสัญญาณอาจมีการหักเหระหว่างทางได้

ปัจจุบันถูกนำมาใช้ ในบริการโทรศัพท์ทางไกล และ โทรศัพท์มือถือ


microwave
stations


Terrestrial
Microwave

- การส่งสัญญาณคลื่นอินฟาเรดและคลื่นสั้น (Infrared และ Millimeter wave)

เดินทางเป็นเส้นตรง ราคาถูก ง่ายต่อการผลิตใช้งาน ปลอดภัยจากการถูกลักลอบดักสัญญาณ

ข้อเสียไม่สามารถผ่านสิ่งกีดขวางได้ ระยะทางในการรับส่งไม่ไกลนัก

ปัจจุบันถูกนำมาใช้ ในการสื่อสารระยะใกล้ เช่น รีโมทควบคุมโทรทัศน์ รวมทั้งการนำไปใช้ในการส่งข้อมูลจากเครื่องคอมพิวเตอร์ ไปยังเครื่องพิมพ์ด้วย

การส่งสัญญาณผ่านคลื่นแสง (Lightwave Transmission)

ปัจจุบันเป็นการส่งข้อมูลระหว่างระบบเครือข่ายเฉพาะบริเวณสองแห่ง ที่อยู่ห่างกันโดยใช้แสงเลเซอร์ เป็นการสื่อสารแบบทางเดียว ถ้าให้เป็นการสื่อสารแบบสองทาง ทั้งผู้รับและผู้ส่งจะต้องมีอุปกรณ์ในการส่งและรับด้วย มีราคาถูกและมีช่วงกว้างของช่องสัญญาณสูงมากเมื่อเทียบกับแบบไมโครเวฟ

ข้อเสีย การติดตั้งอุปกรณ์ต้องใช้ผู้เชี่ยวชาญ และลำแสงเลเซอร์จะไม่ผ่านสายฝน หรือหมอกหนาได้ และอาจมีปัญหากับคลื่นความร้อนได้อีก

ระบบดาวเทียม (Satellite System)

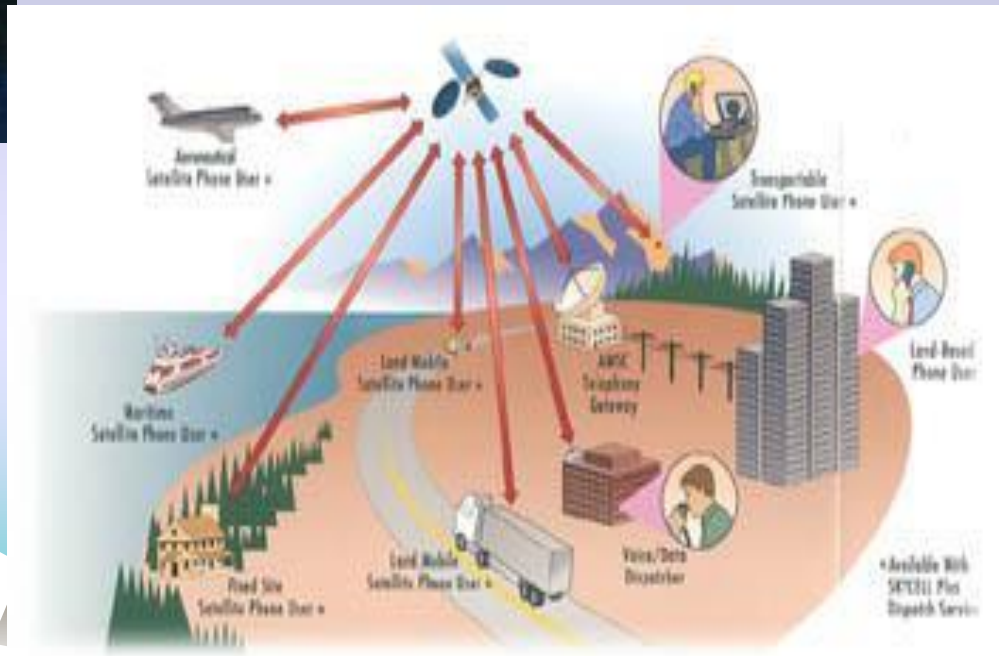
หลักการยิงสัญญาณคล้ายกับระบบไมโครเวฟ มี 2 แบบ คือ

- ดาวเทียมจะอยู่เหนือพื้นโลก 36000 กม. หมุนรอบโลกประมาณ 24 ชม. เรียกว่าดาวเทียมแบบประจำที่ (geosynchronous satellite) จะต้องโคจรห่างจากกัน 2 องศาเมื่อวัดจากแกนโลก เพื่อไม่ให้เกิดสัญญาณรบกวนกัน ดังนั้นจึงมีได้ 180 ดวง แต่ดาวเทียมแต่ละดวงสามารถรับและส่งสัญญาณหลายช่วงความถี่ในเวลาเดียวกัน และดาวเทียมอาจอยู่วงโคจรเดียวกันได้ถ้าใช้ความถี่ต่างกัน

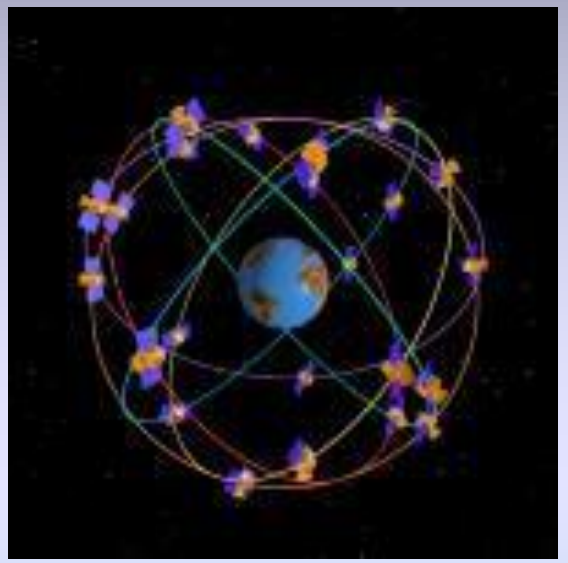
- ดาวเทียมโคจรระดับต่ำ อยู่ในระดับความสูง 750 km. โคจรผ่านขั้วโลกเหนือและขั้วโลกใต้ โดยทิ้งระยะห่างกัน 32 องศา

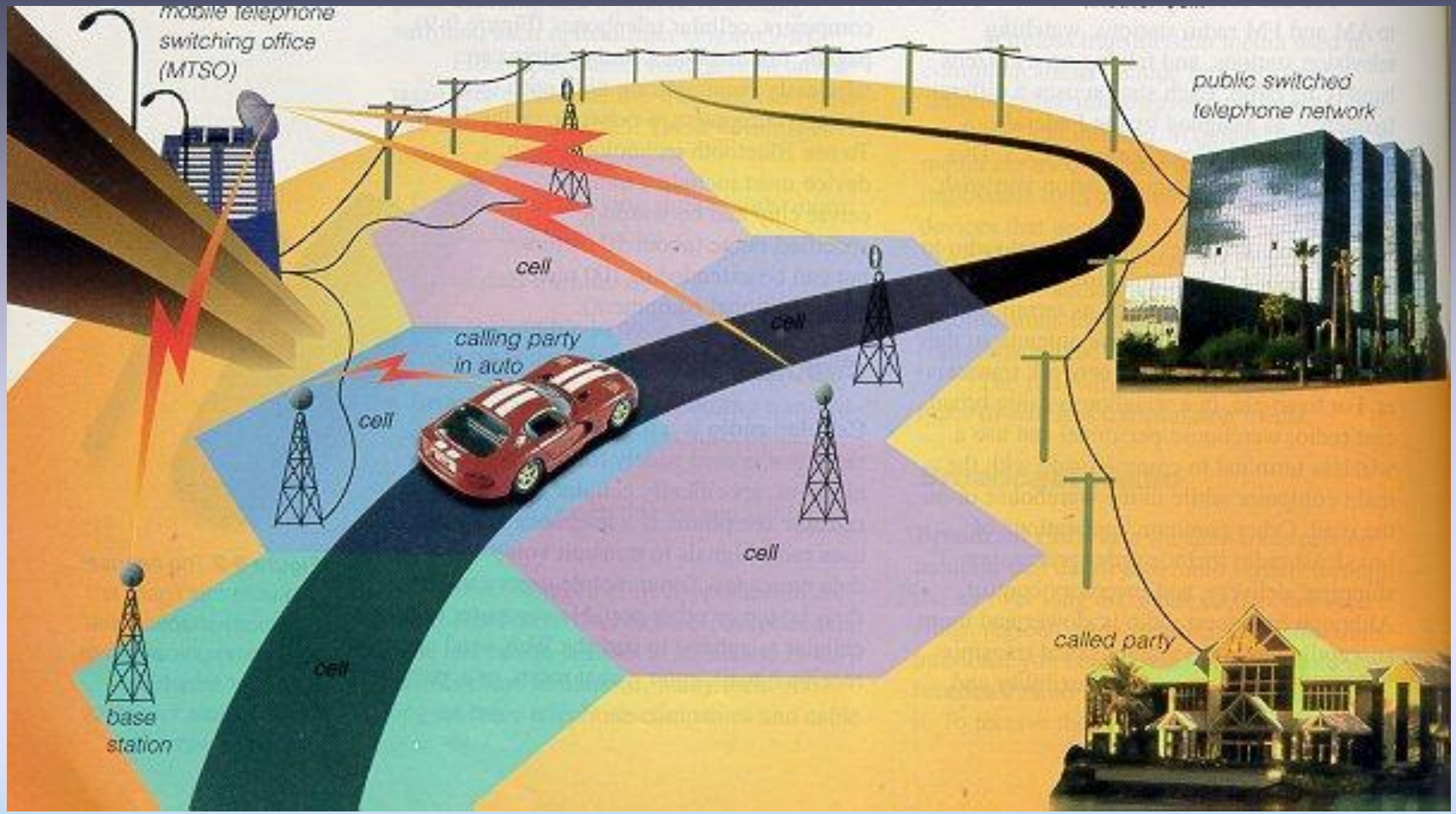
ในปัจจุบันมีการใช้สัญญาณดาวเทียม ในการส่งสัญญาณข้อมูลคอมพิวเตอร์ สัญญาณโทรทัศน์ รวมทั้งการใช้ในทางภูมิศาสตร์ ทางทหาร


communications satellite
microwave station
microwave station



GPS




mobile telephone
switching office
(MTSO)
public switched
telephone network
cell
cell
calling party
in auto
cell
cell
cell
called party
base
station

ข้อดีดาวเทียม คือ

- ค่าใช้จ่ายในการส่งสัญญาณคงที่ ไม่ว่าจะเป็นที่แห่งไหน
- การส่งสัญญาณดาวเทียมไม่ขึ้นอยู่กับระยะทาง
- เหมาะที่จะใช้ในพื้นที่ที่ไม่สามารถวางสายได้

ข้อเสีย คือ

- ถูกรบกวนได้จากสภาพอากาศ รวมทั้งตำแหน่งโคจรของดวงอาทิตย์
- ฝ่ายรับจะได้รับข้อมูลช้ากว่าที่เกิดขึ้นจริง (เกิดเวลาหน่วง= delay time)

หลักเกณฑ์การพิจารณาเลือกสื่อนำข้อมูล

สื่อในการสื่อสาร (Transmission media) ซึ่งในการเลือกช่องทางที่ต้องการต้องคำนึงถึง

- อัตราเร็วในการส่งผ่านข้อมูล (Transmission rate) ซึ่งมีตั้งแต่ Kbps ถึง Mbps
- ระยะทาง (Distance) ต้องคำนึงถึงระยะทางระหว่างอุปกรณ์ที่เชื่อมต่อกันด้วย
- ค่าใช้จ่าย (Cost) ค่าใช้จ่ายในการติดตั้งครั้งแรก และค่าใช้จ่ายประจำ
- ความสะดวกในการติดตั้ง (Ease of Installation)
- ความทนทานต่อสภาพแวดล้อม (Resistance to Environmental Conditions)

โปรโตคอล (Protocol)

Protocol คือกฎหรือวิธีที่กำหนดขึ้นเพื่อการสื่อสาร จะถูกสร้างขึ้นโดยเป็นส่วนหนึ่งของฮาร์ดแวร์หรือซอฟท์แวร์ ที่เราใช้ ซึ่งมีเนื้อหาครอบคลุมถึงวิธีการและกฎเกณฑ์ที่ถูกต้องในการรับ-ส่งข้อมูล มีองค์กรที่กำหนดมาตรฐานต่าง ๆ ได้แก่

- ISO(International Organization for Standardization) ทำหน้าที่กำหนดมาตรฐานสากลในหลาย ๆด้าน รวมทั้งในด้านของเครือข่ายคอมพิวเตอร์ กำหนดแบบจำลองสำหรับอ้างอิง OSI (Open System Interconnection) และชุดโปรโตคอล OSI
- ANSI (American National Standards Institute) กำหนดมาตรฐานของสหรัฐ

- EIA (Electronic Industries Association) กำหนดมาตรฐานทางด้านสัญญาณไฟฟ้า ได้แก่ RS-232

- IEEE (Institute of Electrical and Electronic Engineers) กำหนดมาตรฐานทางด้านเครือข่ายคอมพิวเตอร์ โดยมาตรฐานระบบ LAN ของ IEEE ได้แก่ IEEE 802.3, 802.4, 802.5 เป็นมาตรฐานใช้กันมาก IEEE 802.1X ใช้สำหรับพิสูจน์ตัวตนของอุปกรณ์ต่างๆที่เชื่อต่อกับเครือข่ายทั้งแบบ wireless LAN (ไวร์เลสแลน) และ LAN (แลน) โดยมีกลไกการทำงานจะอนุญาตให้เข้าถึงได้แค่อุปกรณ์ที่มีสิทธ์เข้าได้เท่านั้นหากอุปกรณ์ไหนไม่มีสิทธ์ก็จะสกัดกั้นออก

- ITU-T (International Telecommunication Union) เดิมคือ CCITT เป็นองค์กรกำหนดมาตรฐานทางด้านโทรคมนาคม ได้แก่ X.25, V.29(มาตรฐานของโมเด็ม)

- IAB (International Architecture Board) ทำหน้าที่กำหนดนโยบายและอนุมัติมาตรฐานของ internet เช่น TCP/IP (Transmission Control Protocol/Internet Protocol)

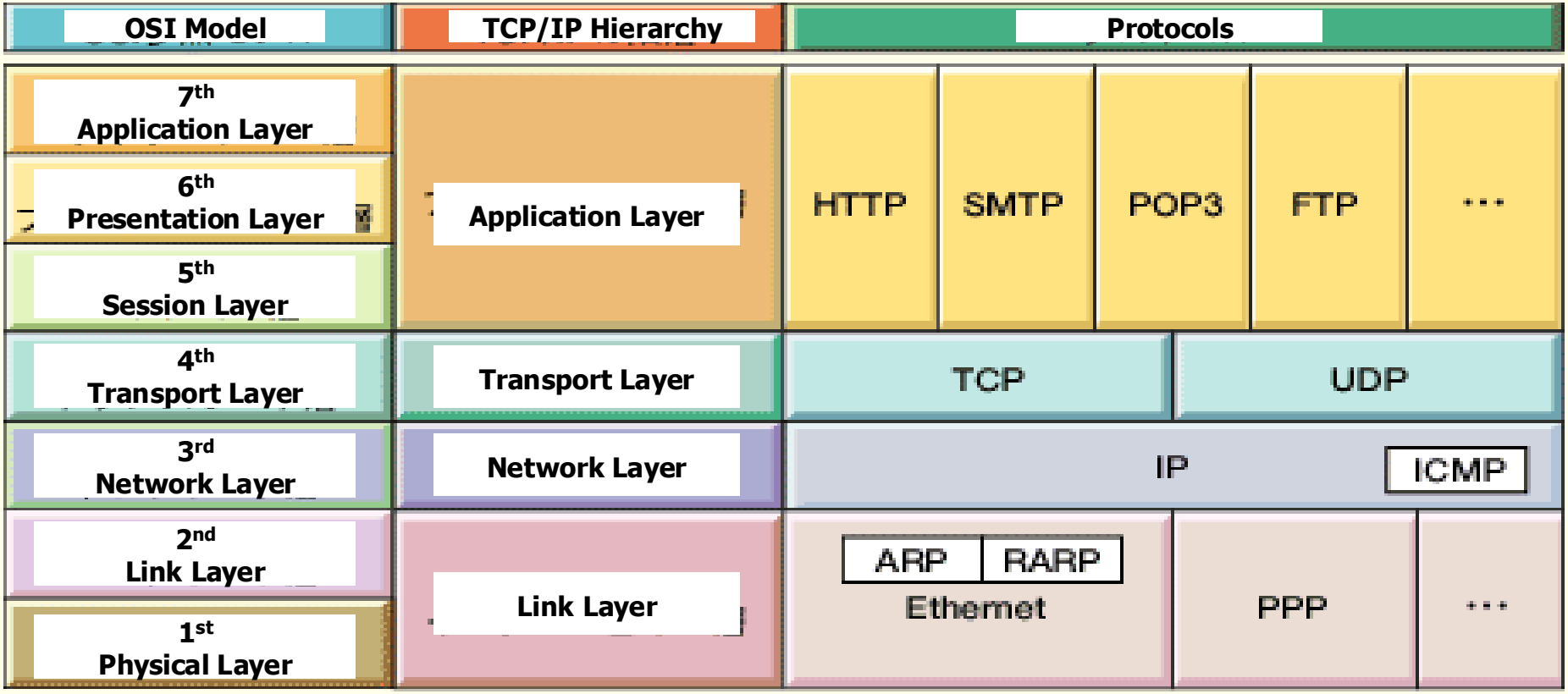
แบบจำลองสำหรับอ้างอิง OSI

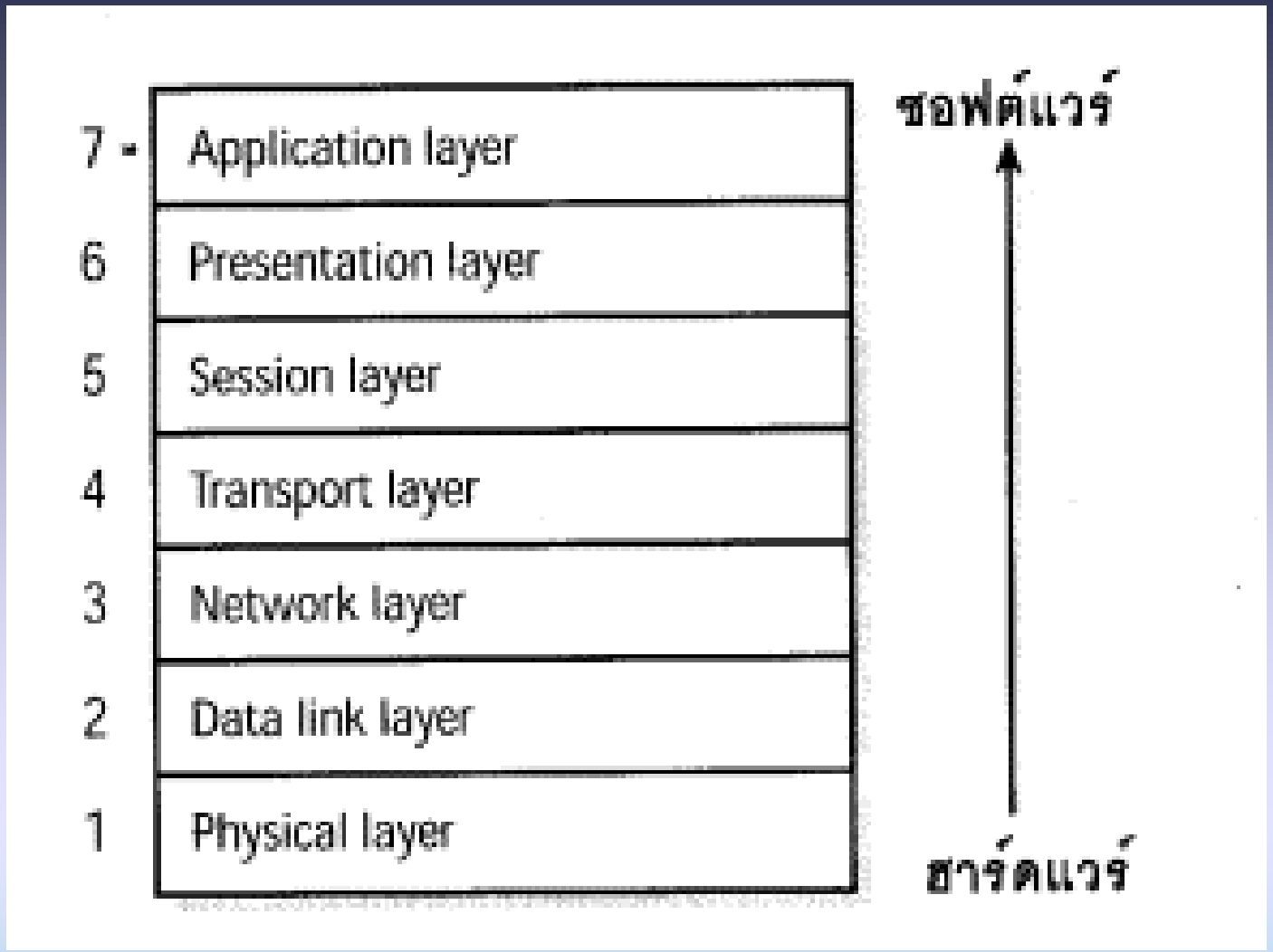
โดยโครงสร้างสถาปัตยกรรมเครือข่าย จะถูกออกแบบเป็นชั้น ซึ่งระบบเครือข่ายใดวางโครงสร้างตามแบบจำลองนี้ จะเป็นระบบเครือข่ายเปิด และอุปกรณ์ทางเครือข่ายจะสามารถติดต่อกันได้โดยไม่ขึ้นกับว่าเป็นอุปกรณ์ของบริษัทใด

- APPLICATION Layer เป็นชั้นการทำงานของซอฟต์แวร์ประยุกต์ซึ่งเกี่ยวกับระบบเครือข่าย เช่นการรับส่งข้อมูล, การจำลอง terminal
- PRESENTATION Layer เป็นชั้นการทำงานของระบบรักษาความลับและการแปลงข้อมูลรูปแบบต่าง ๆให้สามารถแลกเปลี่ยนกันได้ เช่น การแปลงระหว่าง EBCIDIC กับ ASCII

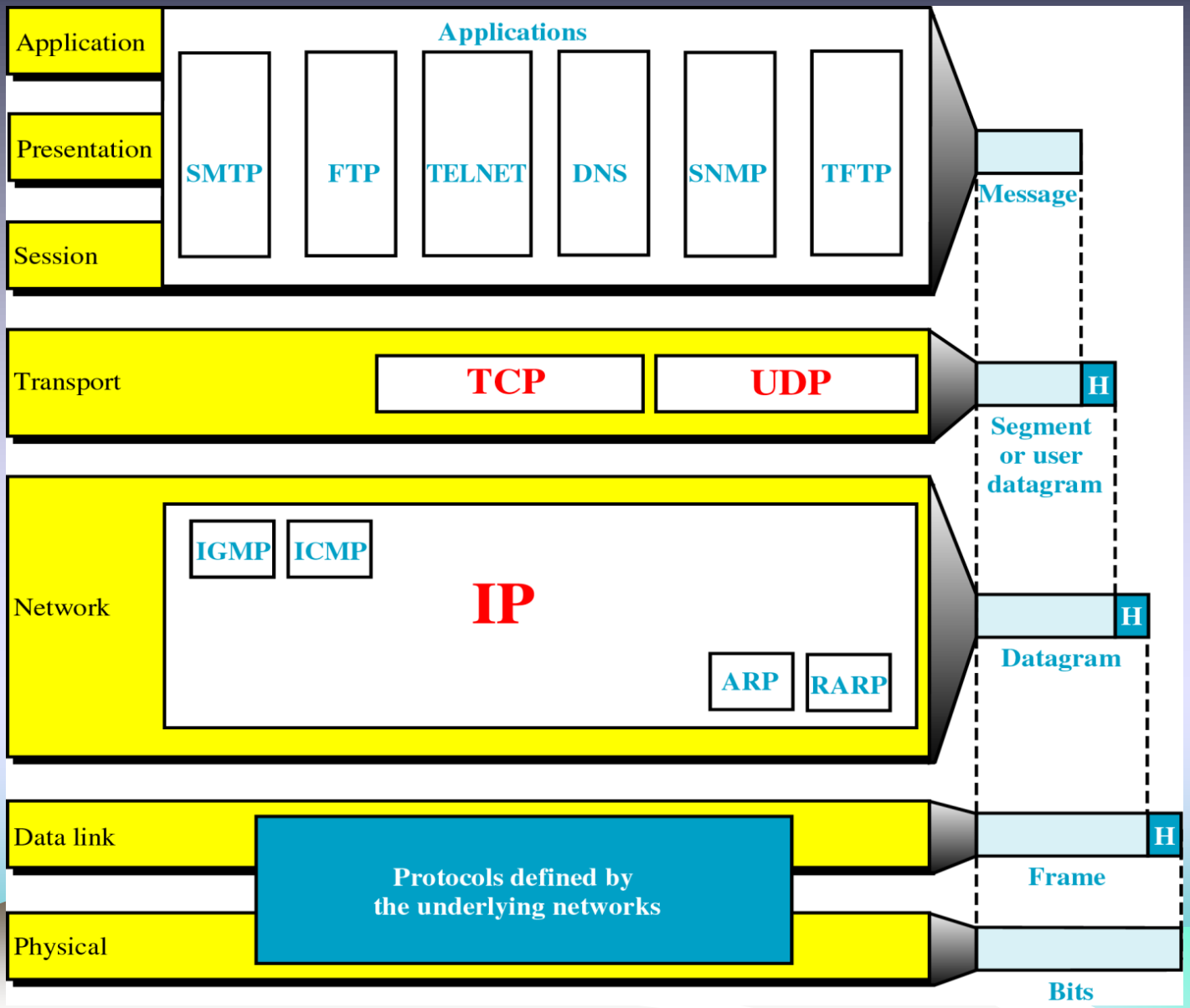
- SESSION Layer รับผิดชอบการควบคุมการติดต่อและประสานของข้อมูลที่ส่งผ่านระบบเครือข่าย เช่น การตรวจสอบลำดับก่อนหลังที่ถูกต้องของ packet
- TRANSPORT Layer รับผิดชอบการส่งถ่ายข้อมูลระหว่างจุด จะทำการตรวจสอบสามชั้นล่างว่ามีการทำงานที่ถูกต้อง และทำการส่งผ่านข้อมูลให้ชั้นที่สูงกว่าโดยซ่อนวิธีการทำงานที่เกิดขึ้นจริงในสามชั้นล่างไว้
- NETWORK Layer ทำการตรวจสอบการส่งข้อมูลผ่านเครือข่าย เช่น เวลาที่ใช้ในการ, การส่งต่อ(routing), การจัดการลำดับ (flow control)
- DATA LINK Layer รับผิดชอบการนำข้อมูลเข้าและออกจากตัวกลาง การจัดเฟรม การตรวจสอบและการจัดการข้อผิดพลาดของข้อมูล แบ่งเป็น 2ชั้นย่อย
    - LLC (Logical Link Control) รับผิดชอบการตรวจสอบข้อผิดพลาด
    - MAC (Media Access Control) วิธีส่งข้อมูลผ่านสื่อ
- PHYSICAL Layer เป็นชั้นการทำงานทางกายภาพของระบบการเชื่อมต่อ ทั้งในส่วนสัญญาณไฟฟ้า ระบบสายสัญญาณ และตัวเชื่อม

OSI AND TCP/IP




7 - Application layer
6 Presentation layer
5 Session layer
4 Transport layer
3 Network layer
2 Data link layer
1 Physical layer
ซอฟต์แวร์
ฮาร์ดแวร์

โปรโตคอล

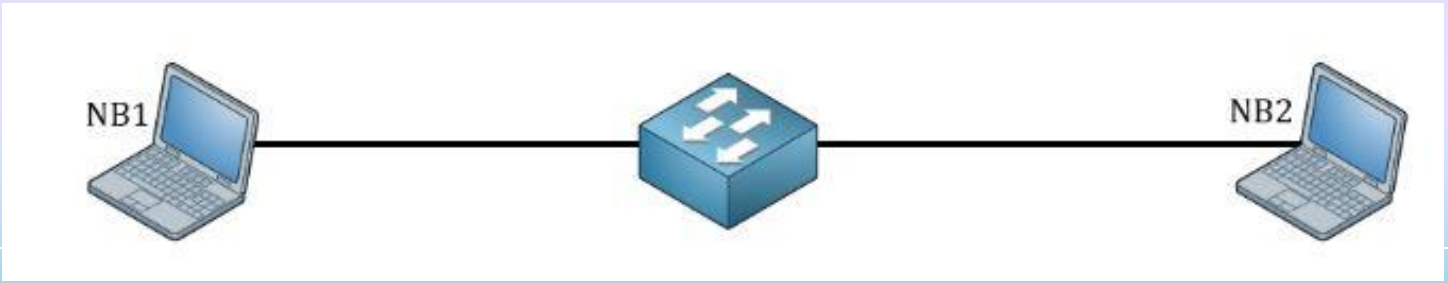

Application
Presentation
Session
Applications
SMTP
FTP
TELNET
DNS
SNMP
TFTP
Message
Transport
TCP
UDP
H
Segment or user datagram
Network
IGMP
ICMP
IP
ARP
RARP
H
Datagram
Data link
Protocols defined by the underlying networks
H
Frame
Physical
Bits

IP Protocol

- เป็นโปรโตคอลแบบ Connectionless Protocol และเป็นแบบ Unreliable
- มีการส่งข้อมูลโดยไม่มีการตรวจสอบ Error
- ไม่รองรับว่าข้อมูลที่ส่งไปจะถึงผู้รับหรือไม่
- ใช้ IP Address ในการระบุผู้ส่งและผู้รับข้อมูล
- Version ปัจจุบันคือ IP v.4

โปรโตคอล ARP (Address Resolution Protocol)

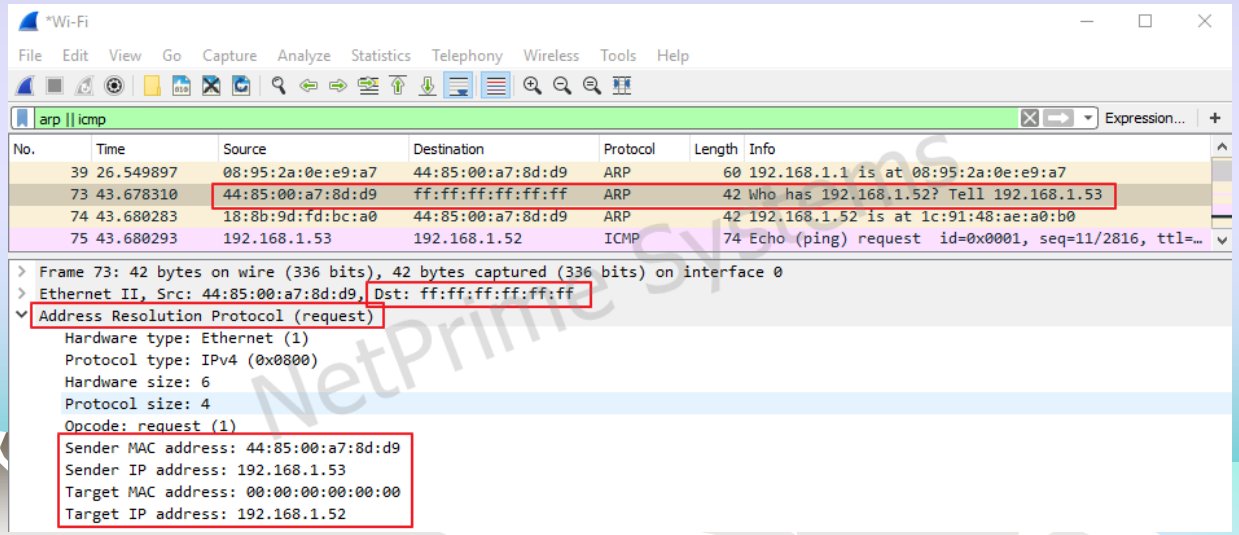
ARP โปรโตคอลที่ค้นหาหมายเลข Mac Address หรือ Physical Address ของเครื่องปลายทางที่เครื่องต้นทางต้องการส่งไปหา
ARP จะทำงานเมื่อมีการติดต่อสื่อสารบน LAN (Ethernet) ระหว่างเครื่องต้นทาง และ เครื่องปลายทาง ใช้ค้นหาและจับคู่ระหว่าง MAC Address กับ IP Address เพื่อให้ส่งถึงปลายทางในระดับ L2 ตาม OSI Model ได้ หรือ Link Layer ตาม TCP/IP



โปรโตคอล ARP (Address Resolution Protocol)

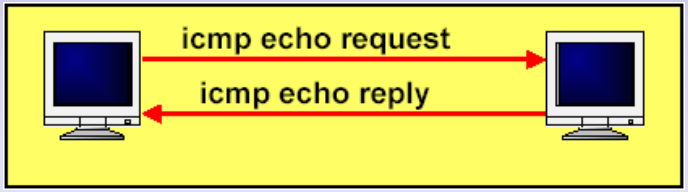
ที่ Network Layer เครื่อง NB1 จะสร้าง IP Packet ขึ้นมา โดยใน IP Packet จะระบุ Source IP address และ Destination IP address เพื่อใช้ในการส่งข้อมูล (Data)

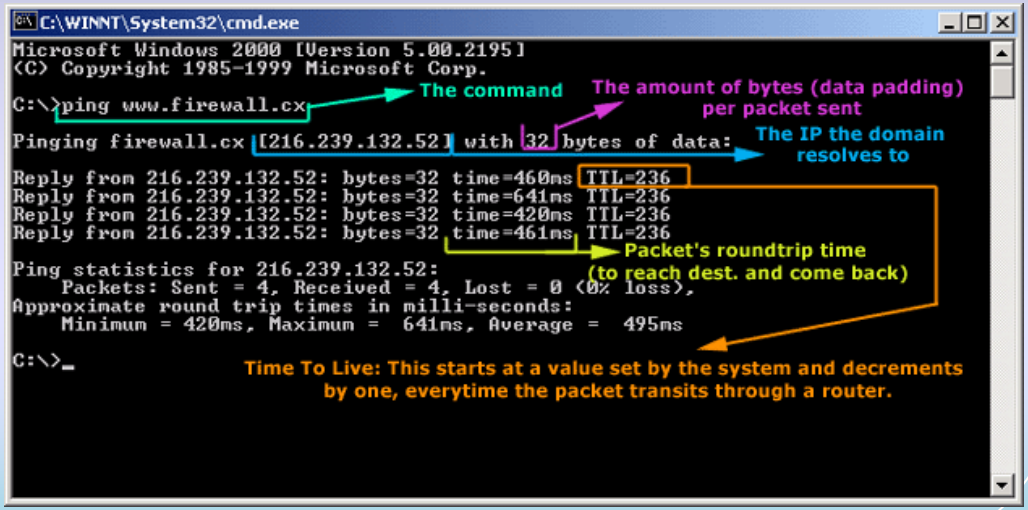
IP Packet ของ NB1 จะถูก Encapsulation ลงมาที่ Link Layer คือ Ethernet Frame โดยใน Ethernet Frame จะระบุ Source MAC address และ Destination MAC address



Internet Control Message Protocol (ICMP)

ICMP เป็นโปรโตคอลที่ใช้ในการตรวจสอบและรายงานสถานภาพของดาต้าแกรม โปรโตคอลนี้ทำงานในระดับ Network Layer เช่นเดียวกับ IP ในกรณีที่เกิดปัญหากับดาต้าแกรม เช่น เราเตอร์ไม่สามารถส่งดาต้าแกรมไปถึงปลายทางได้ ICMP จะถูกส่งออกไปยังโฮสต้นทางเพื่อรายงานข้อผิดพลาด ที่เกิดขึ้น





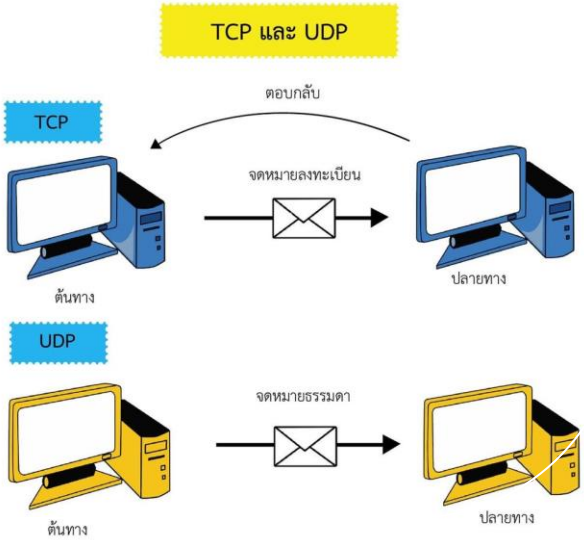
TCP and UDP

Transmission Control Protocol (TCP)

- มีการจัดแบ่งข้อมูลจากระดับ Application ให้มีขนาดพอเหมาะที่จะส่งไปบนเครือข่าย
- มีการสร้าง Connection กันก่อนที่จะมีการรับส่งข้อมูลกัน
- มีการใช้ Sequence Number เพื่อจัดลำดับการส่งข้อมูล
- มีการตรวจสอบว่าข้อมูลที่ส่งไปถึงปลายทางหรือไม่

User Datagram Protocol (UDP)

- ไม่มีการสร้าง Connection กันก่อนที่จะมีการรับส่งข้อมูลกัน
- ส่งข้อมูลด้วยความพยายามที่ดีที่สุด
- ไม่มีการตรวจสอบว่าข้อมูลที่ส่งไปถึงปลายทางหรือไม่



Network Port Number

ตัวอย่าง Well Known Ports (0-1023) จะเป็นพอร์ตสำหรับ applications ที่คุ้นเคยกัน เช่น

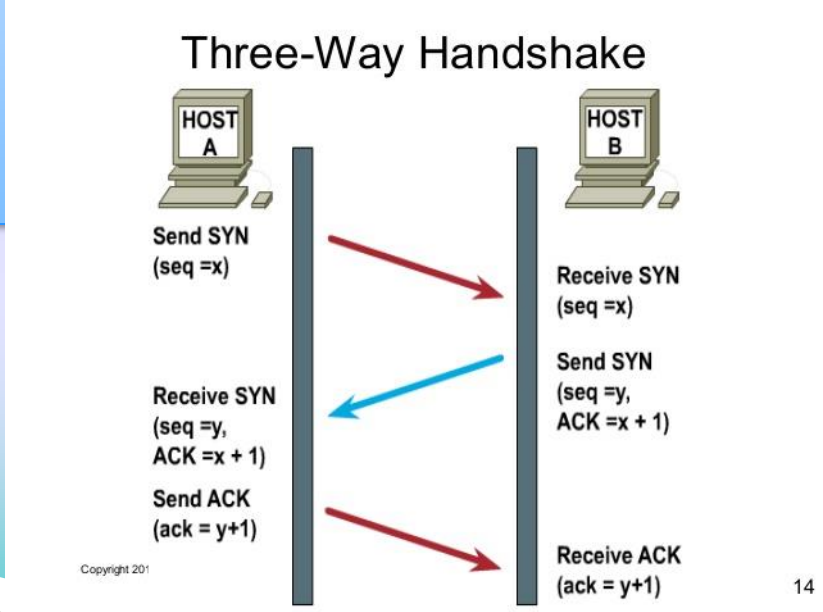
- TCP 20 and 21 (File Transfer Protocol, FTP)
- TCP 22 (Secure Shell, SSH)
- TCP 23 (Telnet)
- TCP 25 (Simple Mail Transfer Protocol, SMTP)
- TCP and UDP 53 (Domain Name System, DNS)
- UDP 69 (Trivial File Transfer Protocol, tftp)
- TCP 79 (finger)
- TCP 80 (Hypertext Transfer Protocol, HTTP)
- TCP 110 (Post Office Protocol v3, POP3)
- TCP 119 (Network News Protocol, NNTP)
- UDP 161 and 162 (Simple Network Management Protocol, SNMP)
- UDP 443 (Secure Sockets Layer over HTTP, https)

Tree-Way Handshake

เป็นวิธีในการสร้างช่องทางการสื่อสารสำหรับการรับส่งข้อมูลด้วยโพรโทคอล TCP สาเหตุที่เรียกว่า 3-Way Handshake เนื่องจากกระบวนการทำงานนั้นจะใช้ 3 ขั้นตอนด้วยกัน คือ

1. เครื่อง Client ส่งแพ็คเกต SYN เพื่อขอเชื่อมต่อไปยังเครื่อง Server
2. เครื่อง Server ส่งแพ็คเกต SYN/ACK ตอบกลับเครื่อง Client
3. เครื่อง Client ตอบกลับเครื่อง Server ด้วยแพ็คเกต ACK

หลังจากที่เครื่อง Server ได้รับแพ็คเกต ACK แสดงว่าการเชื่อมต่อเสร็จสมบูรณ์ จากนั้นเครื่อง Server ก็จะเริ่มรับส่งข้อมูลกับเครื่อง Client ได้



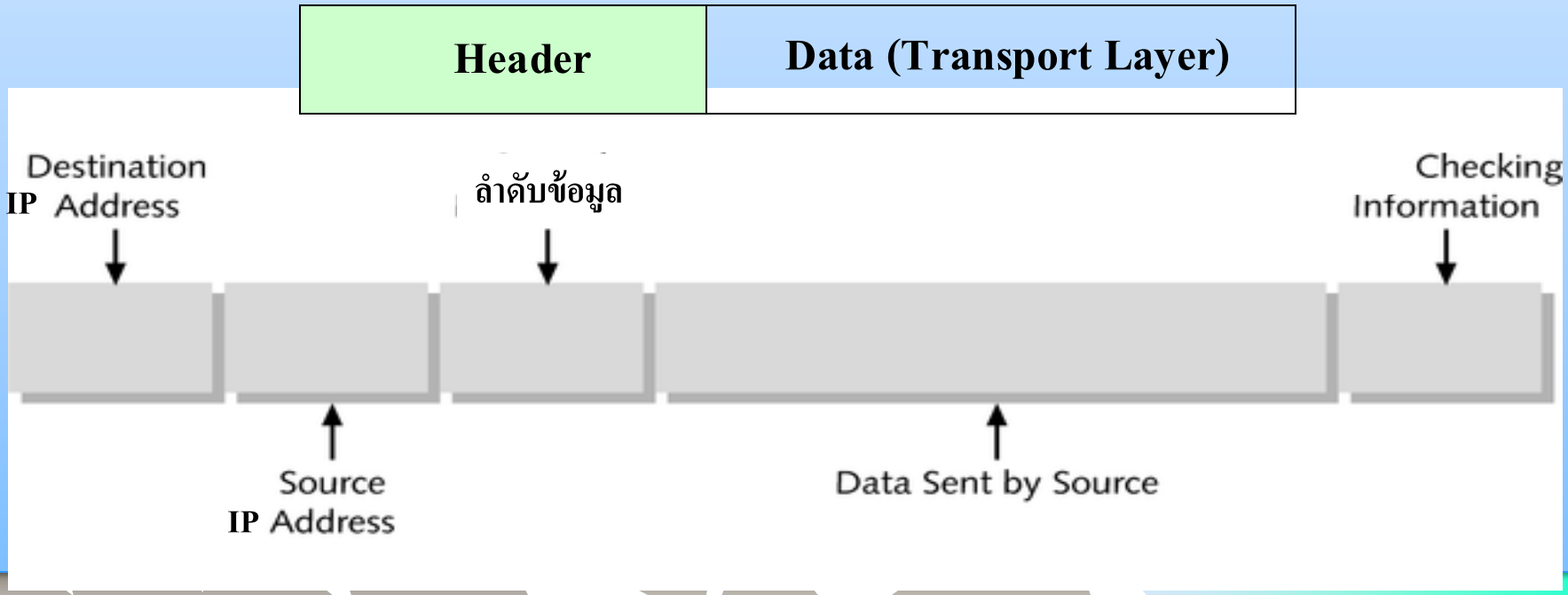
การส่งข้อมูลผ่านเครือข่าย

ในชั้นนี้จะมีหน้าที่ตรวจสอบการส่งข้อมูลผ่านเครือข่าย ดังนี้

1. การเลือกเส้นทางที่ดีที่สุด
2. ควบคุมความแออัดของข้อมูล โดยตรวจสอบปริมาณข้อมูลแต่ละเส้นทาง ทำการนับจำนวนของแพ็กเก็ต เพื่อนำมาจัดเส้นทางของข้อมูลใหม่
3. การจัดลำดับของข้อมูล ข้อมูลที่ส่งไปในแต่ละเส้นทางจะถูกจัดลำดับว่าเป็นข้อมูล ลำดับที่เท่าไร เมื่อถึงปลายทางแล้วก็จะถูกจัดเรียงลำดับ ให้ถูกต้องเหมือนต้นทาง

แพ็คเกต (Packet)

- แพ็คเกต (Packet) เป็นลักษณะของข้อมูลที่อยู่ในชั้น Network Layer
- ลักษณะของ Packet จะมีการ Encapsulation ในส่วน Header เข้าไปกับตัวข้อมูลที่ส่งมาจากชั้น Transport Layer



Internet Protocal (IP)

- เป็นโปรโตคอลประจำชั้น Network Layer ที่ทำหน้าที่ในการจัดส่งข้อมูลจากเครื่องต้นทางไปยังเครื่องปลายทางโดยอาศัย IP Address (เป็น Logical Address นั่นคือ วิธีการหาตำแหน่ง/เส้นทางของการส่งข้อมูลในชั้น Network)
- คอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อกันใน Internet ต้องมี IP Address ประจำเครื่อง ซึ่งเป็น Public address ที่ไม่ซ้ำกันเลยในโลกใบนี้ (เพื่อให้สามารถแยกอุปกรณ์แต่ละตัวได้)
- หน่วยงานที่รับผิดชอบคือ IANA (Internet assigned number authority) ซึ่งเป็นหน่วยงานกลางที่ควบคุมดูแล IPV4 ทั่วโลก
- แต่การดูแลจะแยกออกไปตามภูมิภาคต่าง ๆ สำหรับทวีปเอเชียคือ APNIC (Asia pacific network information center)

IP Address

- IP Address คือ หมายเลขประจำอุปกรณ์ในเครือข่าย (Logical Address) เช่น เครื่องคอมพิวเตอร์ หรือเราเตอร์ ที่ใช้บนเครือข่ายคอมพิวเตอร์ ซึ่งในแต่ละเครือข่ายจะต้องมีหมายเลข IP Address นี้ไม่ซ้ำกัน เช่น เครือข่ายอินเตอร์เน็ต
- ขนาดความยาวของ IP Address ที่ใช้ในปัจจุบันมีความยาวที่ 32 บิต หรือ 4 ไบต์ หรือเมื่อแปลงเป็นเลขฐานสิบแล้ว จะประกอบด้วยตัวเลข 4 ชุด โดยมีเครื่องหมาย “จุด” คั่นระหว่างชุดตัวเลข ตัวอย่าง เช่น 192.168.0.1
- ลักษณะของ IP Address มีการจำแนกออกเป็น Class จำนวน 5 class ได้แก่ Class A, B, C, D และ E
- IP Address ไม่ใช่หมายเลขที่ใช้อ้างอิงเครื่องใดเครื่องหนึ่งอย่างเฉพาะเจาะจง แต่ IP Address จะใช้บ่งชี้ตำแหน่งของการเชื่อมโยงระหว่างคอมพิวเตอร์กับเครือข่าย (ส่วนการอ้างอิงถึงตำแหน่งเครื่องจะเป็นการอ้างอิงที่ MAC Address)

IP Address

IP Address ประกอบไปด้วย 2 ส่วนหลัก คือ

1. ส่วนของหมายเลขเครือข่าย (NetID)
   - เป็นส่วนที่ใช้กำหนดหมายเลขของเครือข่าย
   - ใช้สำหรับการวางเส้นทางแพ็คเกตระหว่างเครือข่าย
   - ในส่วนนี้สามารถระบุ Class ของ IP Address ได้ (คือ Class Type เพื่อบอกให้ทราบว่า IP Address นี้อยู่ในคลาสใด)
2. ส่วนของหมายเลขโฮสต์ (HostID)
   - เป็นส่วนที่ใช้กำหนดหมายเลขของเครื่องคอมพิวเตอร์
   - เป็นการระบุตำแหน่งที่เฉพาะเจาะจงของอุปกรณ์หรือโฮสต์บนเครือข่าย

ลักษณะของ IP Address

- IP Address ขนาด 32 บิตนี้ สามารถใช้แทนหมายเลขแอดเดรสของอุปกรณ์ได้ถึง 4 พันล้านเครื่อง เท่ากับ 2^{32} (4,294,967,296)
- **แต่**ไม่สามารถนำ IP Address นั้นมาใช้งานได้ทั้งหมด เนื่องจากจะมีการสงวนหมายเลขบางส่วนไว้เพื่อการใช้งานเฉพาะอย่าง
- มีการเขียนให้อยู่ในรูปของเลขฐานสิบ เพื่อง่ายต่อการจดจำ

  10000000 . 00001011 . 00000011 . 00011111

  128 . 11 . 3 . 31
- ในแต่ละไบต์เมื่อนำมาแปลงเป็นเลขฐานสิบ จะมีค่าอยู่ระหว่าง 0 - 255

Class ของ IP Address

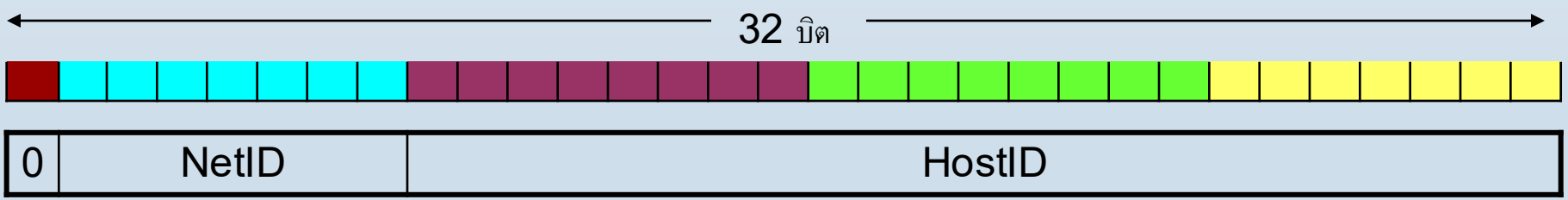
- Class ที่ใช้งานอยู่ มี 5 ชนิด คือ Class A - Class E
- โดยแต่ละ Class ออกแบบมาเพื่อรองรับความต้องการที่แตกต่างกันของแต่ละองค์กร
- ปัจจุบัน Class A และ Class B ถูกนำมาใช้งานเต็มหมดแล้ว
- เหลือแต่เพียง Class C ที่ยังสามารถใช้งานได้
- ส่วน Class D ถูกใช้เป็น Multicast Address (คือการแพร่ข่าวสารไปยังกลุ่มโหนดหลายๆ โหนดบนเครือข่าย)
- และ Class E สงวนไว้เพื่อใช้งานในอนาคต
- ในตำแหน่งไบต์แรก จะบ่งบอกว่า IP Address นั้นอยู่ใน Class ใด

IP Address : Class A

- Class A : **0**.0.0.0 – **127**.255.255.255
- บิตแรกของไบต์แรกต้องมีค่าเป็น 0 เพื่อใช้แทนว่าเป็น Class A

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
0	0	0	0	0	0	0	0	= Decimal 0
0	1	1	1	1	1	1	1	= Decimal 127

- มีส่วนของหมายเลขเครือข่าย (NetID) มีขนาด 7 บิต
- มีส่วนของหมายเลขโฮสต์ (HostID) มีขนาด 24 บิต



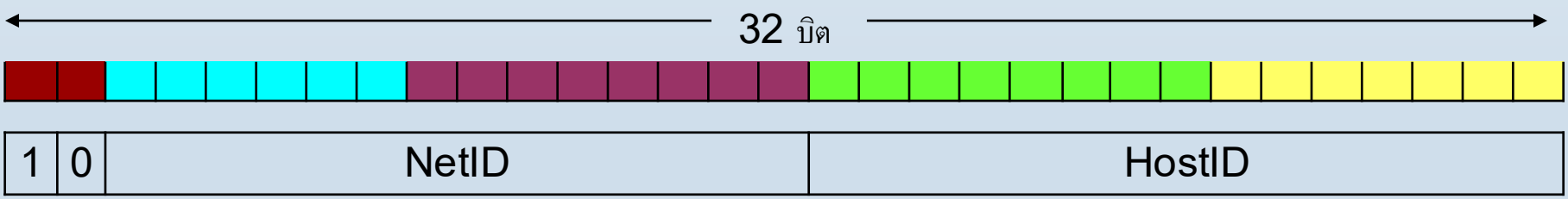
- ดังนั้น ในบิตแรกของ Class A จะมีค่าเป็น **0** เสมอ
- สามารถมีจำนวนเครือข่ายได้เท่ากับ 126 (2^7 - 2) เครือข่าย
- มีจำนวนของโฮสต์ได้ถึง 24 บิต (2^{24} – 2) หรือเท่ากับ 16,777,214 เครื่องต่อหนึ่งเครือข่าย
- นิยมนำไปใช้กับองค์กรขนาดใหญ่มากๆ ที่มีจำนวนเครื่องจำนวนมาก
- สาเหตุที่ต้องลบออก 2 ออกจาก HostID เนื่องจาก
  - Host ที่มี IP เป็น 0 ทั้งหมด จะถูกสงวนไว้สำหรับอ้างอิงหมายเลขเครือข่าย เช่น **121**.0.0.0
  - Host ที่มี IP เป็น 1 ทั้งหมด จะถูกสงวนไว้สำหรับการทำ Broadcast Address เช่น **121**.255.255.255
- สาเหตุที่ต้องลบออก 2 ออกจาก NetID ของ Class A เนื่องจาก
  - NetID ที่มี IP เป็น 0 ทั้งหมด และ 1 ทั้งหมด จะไม่นำมาใช้งาน

IP Address : Class B

- Class B : **128.0**.0.0 – **191.255**.255.255
- 2 บิตแรกของไบต์แรกต้องมีค่าเป็น 1 กับ 0 เพื่อใช้แทนว่าเป็น Class B

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
1	**0**	0	0	0	0	0	0	= Decimal 128
1	**0**	1	1	1	1	1	1	= Decimal 191

- มีส่วนของหมายเลขเครือข่าย (NetID) มีขนาด 14 บิต
- มีส่วนของหมายเลขโฮสต์ (HostID) มีขนาด 16 บิต



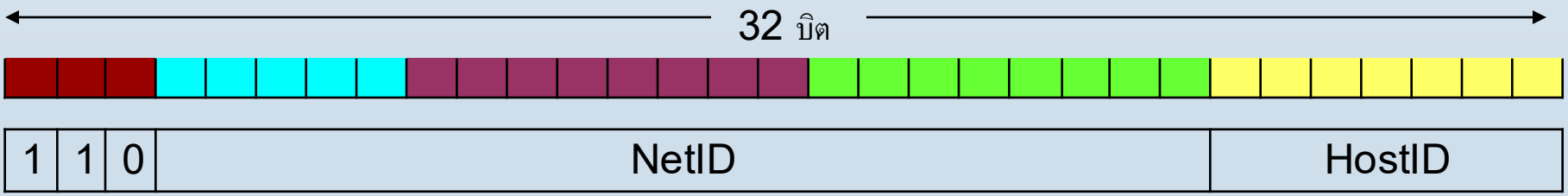
- ดังนั้น ในบิตแรกของ Class B จะมีค่าเป็น **1 0** เสมอ
- สามารถมีจำนวนเครือข่ายได้เท่ากับ 16,382 (2^{14} - 2) เครือข่าย
- มีจำนวนของโฮสต์ได้ถึง 16 บิต (2^{16} – 2) หรือเท่ากับ 65,534 เครื่อง
- นิยมนำไปใช้กับองค์กรขนาดกลาง เช่นสถาบันการศึกษา หน่วยงานของรัฐ
- สาเหตุที่ต้องลบออก 2 ออกจาก HostID เนื่องจาก
  - Host ที่มี IP เป็น 0 ทั้งหมด จะถูกสงวนไว้สำหรับอ้างอิงหมายเลขเครือข่าย เช่น **190.180**.0.0
  - Host ที่มี IP เป็น 1 ทั้งหมด จะถูกสงวนไว้สำหรับการทำ Broadcast Address เช่น **190.180**.255.255
- สาเหตุที่ต้องลบออก 2 ออกจาก NetID ของ Class B เนื่องจาก
  - NetID ที่มี IP เป็น 0 ทั้งหมด และ 1 ทั้งหมด จะไม่นำมาใช้งาน

IP Address : Class C

- Class C : **192.0.0**.0 – **223.255.255**.255
- 3 บิตแรกของไบต์แรกต้องมีค่าเป็น 1 1 0 เพื่อใช้แทนว่าเป็น Class C

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
1	**1**	**0**	0	0	0	0	0	= Decimal 192
1	**1**	**0**	1	1	1	1	1	= Decimal 223

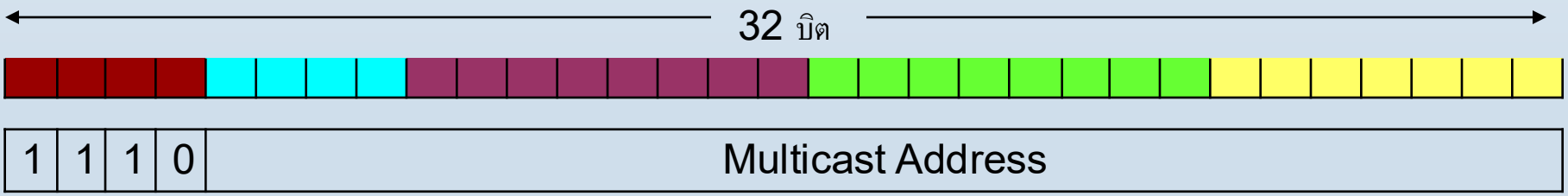
- มีส่วนของหมายเลขเครือข่าย (NetID) มีขนาด 21 บิต
- มีส่วนของหมายเลขโฮสต์ (HostID) มีขนาด 8 บิต



- ดังนั้น ในบิตแรกของ Class C จะมีค่าเป็น **1 1 0** เสมอ
- สามารถมีจำนวนเครือข่ายได้เท่ากับ 2,097,150 (2^{21} - 2) เครือข่าย
- มีจำนวนของโฮสต์ได้ถึง 8 บิต (2^8 – 2) หรือเท่ากับ 254 เครื่อง
- นิยมนำไปใช้กับองค์กรขนาดเล็กที่มีจำนวนเครื่องไม่มาก
- สาเหตุที่ต้องลบออก 2 ออกจาก HostID เนื่องจาก
  - Host ที่มี IP เป็น 0 ทั้งหมด จะถูกสงวนไว้สำหรับอ้างอิงหมายเลขเครือข่าย เช่น **192.168.4**.0
  - Host ที่มี IP เป็น 1 ทั้งหมด จะถูกสงวนไว้สำหรับการทำ Broadcast Address เช่น **192.168.4**.255
- สาเหตุที่ต้องลบออก 2 ออกจาก NetID ของ Class C เนื่องจาก
  - NetID ที่มี IP เป็น 0 ทั้งหมด และ 1 ทั้งหมด จะไม่นำมาใช้งาน

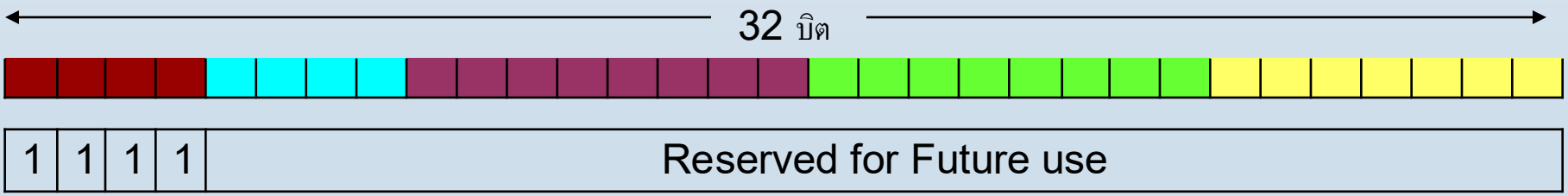
- Class D : **224**.0.0.0 – **239**.255.255.255
- 4 บิตแรกของไบต์แรกต้องมีค่าเป็น 1 1 1 0 เพื่อใช้แทนว่าเป็น Class D
- ใช้สำหรับเป็น Multicast Address

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
1	**1**	**1**	**0**	0	0	0	0	= Decimal 224
1	**1**	**1**	**0**	1	1	1	1	= Decimal 239

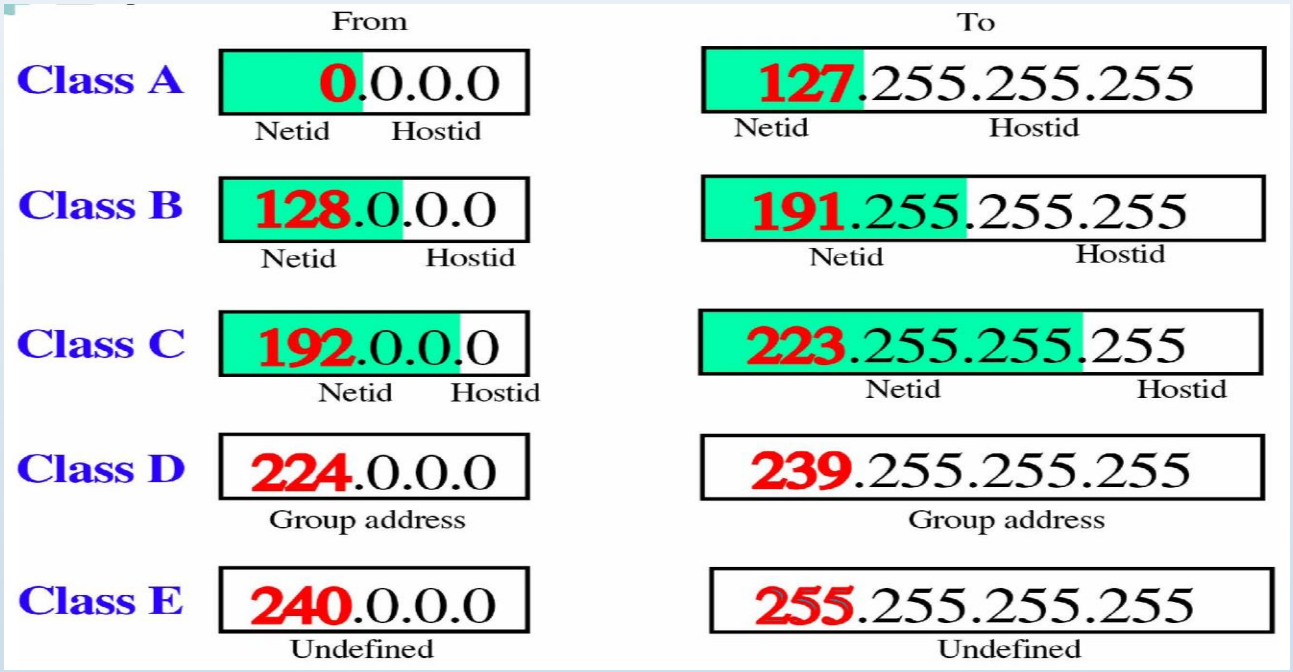


- Class E : **240**.0.0.0 – **255**.255.255.255
- 4 บิตแรกของไบต์แรกต้องมีค่าเป็น **1 1 1 1** เพื่อใช้แทนว่าเป็น Class E
- Class นี้ได้สงวนไว้ใช้ในอนาคต

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	
128	64	32	16	8	4	2	1	
1	**1**	**1**	**1**	0	0	0	0	= Decimal 240
1	**1**	**1**	**1**	1	1	1	1	= Decimal 255



สรุป IPAddress ที่ใช้งานในปัจจุบัน



สรุปรายละเอียด IPAddress

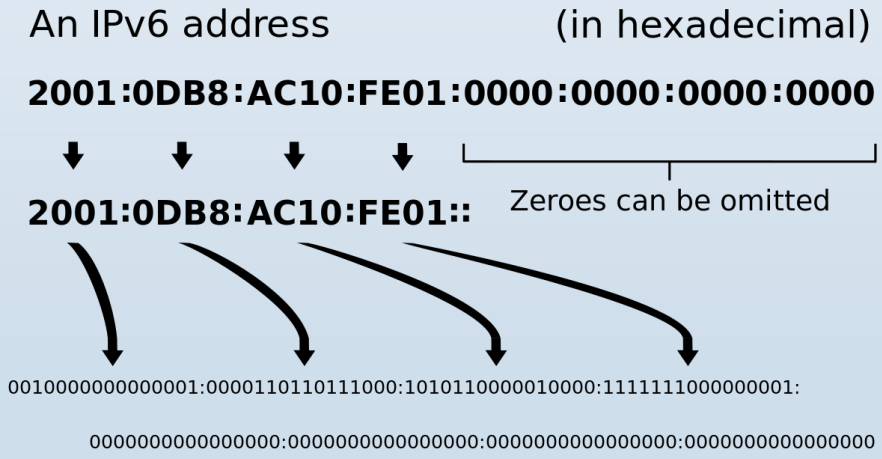
Address Type	First Decimal Value	Network Address (NetID)	Host Address (HostID)
Class A	0-127	126 address (7 bits)	16,777,214 address (24 bits)
Class B	128-191	16,382 address (14 bits)	65,534 address (16 bits)
Class C	192-223	2,097,150 address (21 bits)	254 address (8 bits)

สรุปรายละเอียด IP (V4) Address

- ส่วน Class D และ E เป็นหมายเลข IP Address ที่สงวนไว้ใช้งานเฉพาะอย่าง
- วิธีการเผยแพร่ข่าวสาร (กระจายข่าวสาร) ในเครือข่ายจะมีลักษณะดังนี้
  - **Unicast** คือ การแพร่กระจายข่าวสารไปยังเฉพาะโหนดใดโหนดหนึ่งในเครือข่าย (ระบุหมายเลข IP Address)
  - **Multicast** คือ การแพร่กระจายข่าวสารไปยังกลุ่มโหนดบางโหนดบนเครือข่าย (เช่น ส่งข่าวสารไปยังเครือข่ายย่อยโดยการระบุ NetID - ดูบทถัดไป)
  - **Broadcast** คือ การแพร่กระจายข่าวสารไปยังโหนดทุกโหนดบนเครือข่าย (เช่น การค้นหาบริการบนเครือข่าย แต่ไม่รู้ว่าอยู่ที่เครื่องใด โหนดที่ต้องการค้นหาจะส่งสัญญาณ Broadcast ไปทั่วเครือข่าย)

IP V6

- **Internet Protocol Version 6 address หรือ IPv6**
- IPv6 กำลังจะเข้ามาแทนที่ IPv4 ที่กำลังใช้งานกันอยู่ในปัจจุบัน อันเนื่องมากข้อจำกัดของ IPv4 ที่มี address ได้เพียงแค่ 32-bit แต่สำหรับ IPv6 แล้วมี address ได้ถึง 128-bit



IP V6

ชนิดของ IPv6 Address

1. **Unicast Address** เป็นการกำหนดที่ตัว network interface โดย IP จะระบุจะส่ง packet ไปยัง unicast address เดียว หลักการทำงานเหมือนกับ IPv4 unicast address ใช้ในการรับส่งข้อมูลแบบ one-to-one จากเครื่องหนึ่งไปยังอีกเครื่องหนึ่ง
2. **Anycast Address** กำหนดให้กับกลุ่มของ interface และมักจะใช้กับ node ที่อยู่ต่างกัน โดย packet ที่ส่งไปยัง unicast address จะถูกส่งไปยังสมาชิกใน network interface ซึ่งมักจะเป็น host ที่ใกล้ที่สุด อาศัยข้อมูล routing เป็นตัวบอกระยะห่าง anycast address ไม่สามารถระบุได้ชัดเนื่องจากมี format แบบเดียวกับ unicast address ซึ่งจะแตกต่างกันตรงใน network จะเห็นว่ามีการส่งไปหลายๆจุด
3. **Multicast Address** ใช้กับ host หลายๆตัว ซึ่งจะเป็นต้องสื่อสารกับ host เหล่านั้น โดย packet ที่ส่งไปหา multicast address จะถูกส่งไปทุก interface ที่อยู่ภายใต้ multicast group
4. **Loopback address** ใช้หมายเลข ::1/128 โดยมีหลักการทำงานเหมือนกับ loopback address บน IPv4 ทุกประการ (127.0.0.1)

รูปแบบของ IPv6

- IPv6 address จะแบ่งเป็น 8 กลุ่มด้วยกัน โดยใช้เลขฐาน 16 จำนวน 4 หลัก โดยแต่ละ group จะมีค่าเท่ากับ 16 bits และแบ่งโดย colons (:) แทน จุด (.) ใน IPv4

```
IPv4 - 172.16.100.1
IPv6 - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

เลขฐาน 16ที่ใช้จะเป็นตัวเล็กทั้งหมดตามคำแนะนำของ IETF ซึ่งเขียนในรูปแบบเต็มๆจะมี เลข 4หลักประกอบด้วยกัน 8ชุด แต่ในความเป็นจริงเราสามารถละ 0 ข้างหน้าทิ้งได้ ซึ่งไม่ทำให้ค่าเปลี่ยนแปลงdและสำหรับกลุ่มที่มีค่าเป็น 0 สามารถเว้นกลุ่มนั้นโดยเขียน :: ติดกันไปเลยก็ได้

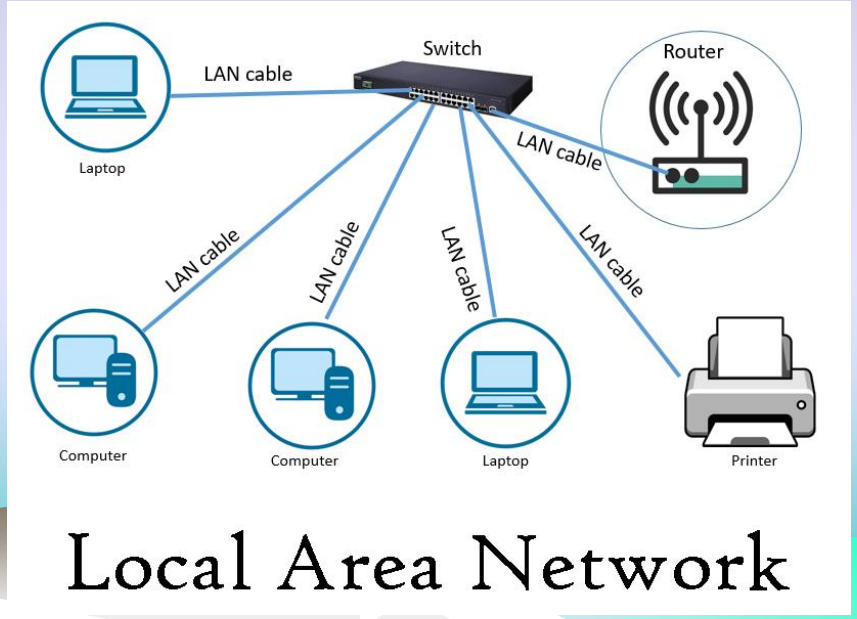
```
IPv6 - 2001:0db8:85a3:0000:0000:8a2e:0370:7334
IPv6 - 2001:db8:85a3:0:0:8a2e:370:7334
IPv6 - 2001:db8:85a3:::8a2e:370:7334
```

ชนิดของระบบเครือข่าย

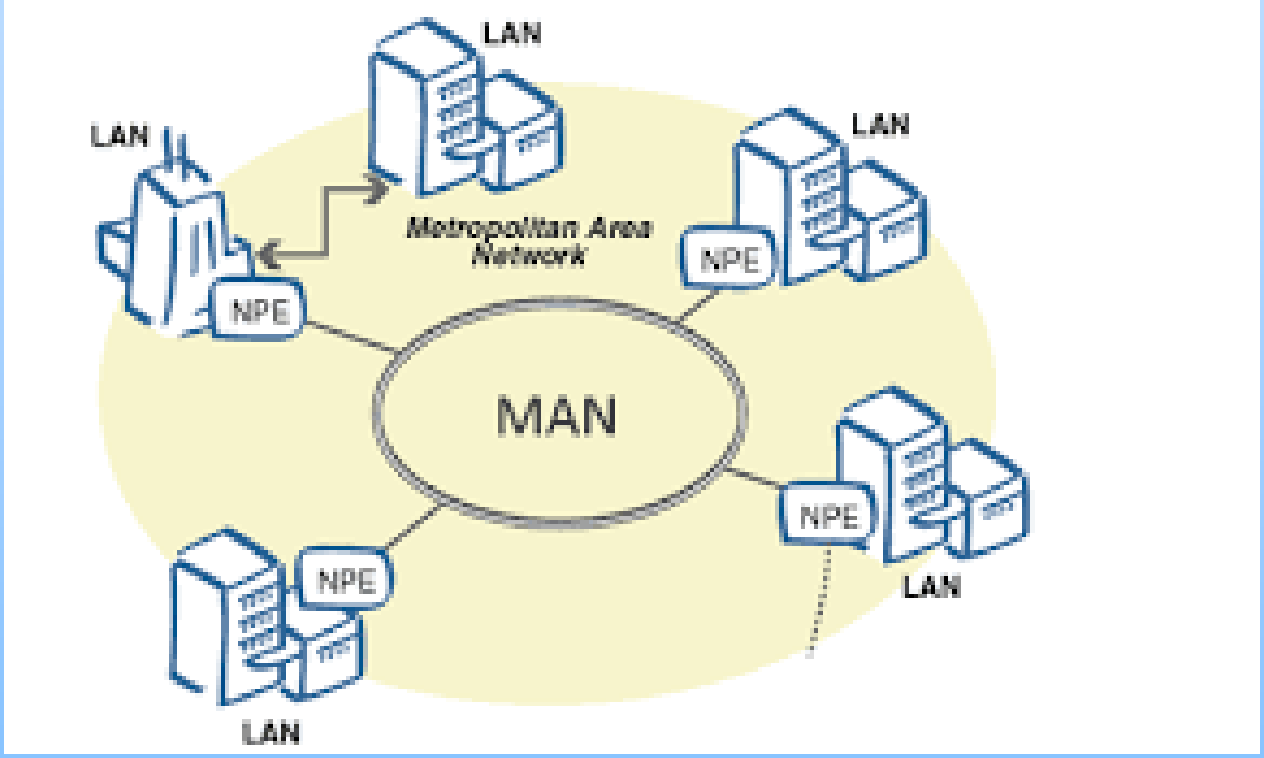
- LAN
- MAN
- WAN
- Internet

ชนิดของระบบเครือข่าย

●**LAN (Local Area Network)** เป็นเครือข่ายที่อุปกรณ์ทั้งหมดเชื่อมโยงกันในพื้นที่ใกล้ ๆกัน โดยส่วนมากเชื่อมโยงโดยใช้สายเคเบิลแบบต่าง ๆ ระบบ LAN ยังรวมถึงระบบเครือข่ายมหาวิทยาลัย (campus network) ซึ่งเป็นการเชื่อมโยงเครือข่ายแบบ LAN จากตึกต่าง ๆของมหาวิทยาลัย หรือบริเวณนิคมอุตสาหกรรม โดยใช้สาย fiber optic ในการเชื่อมโยง

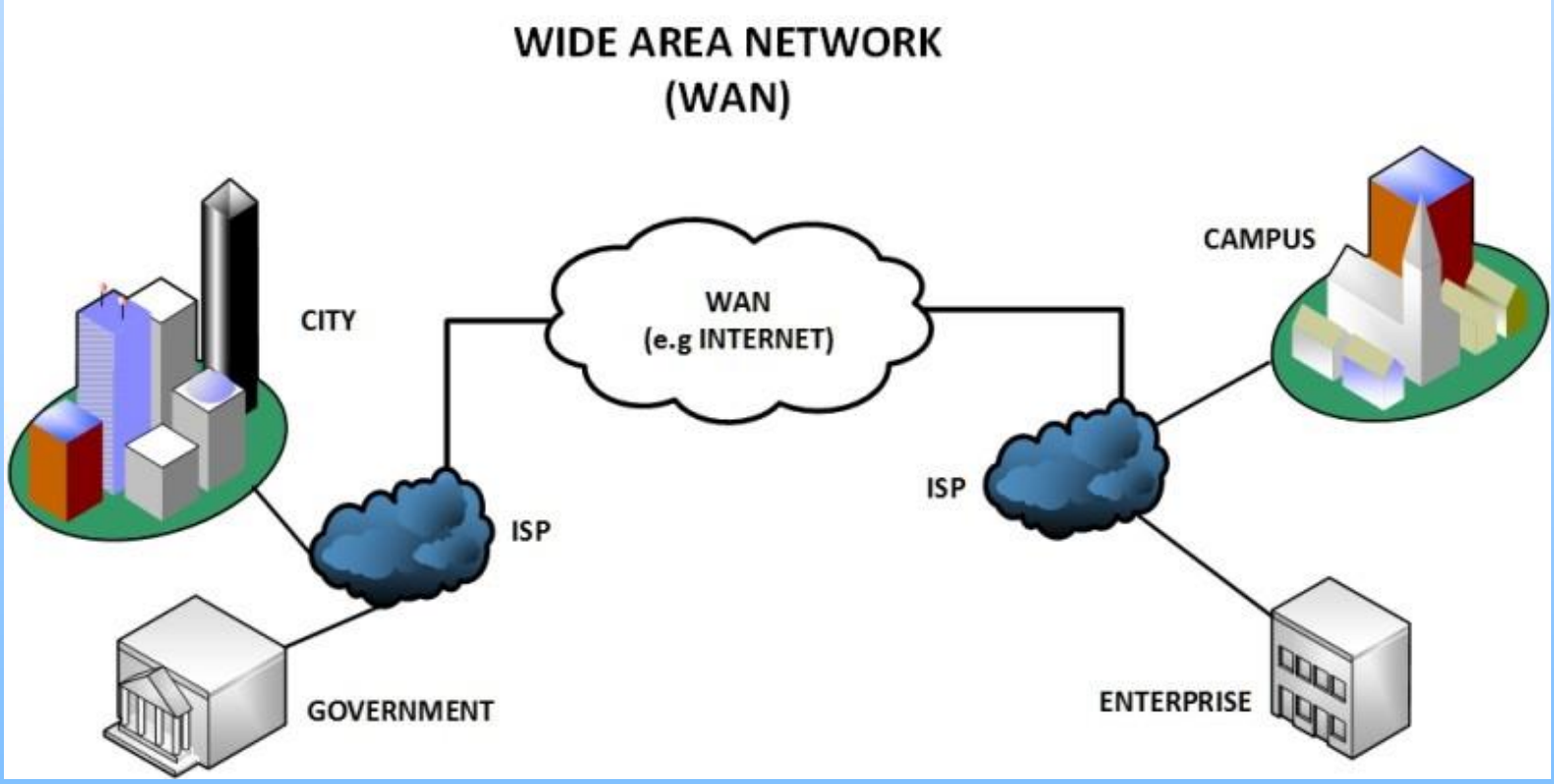


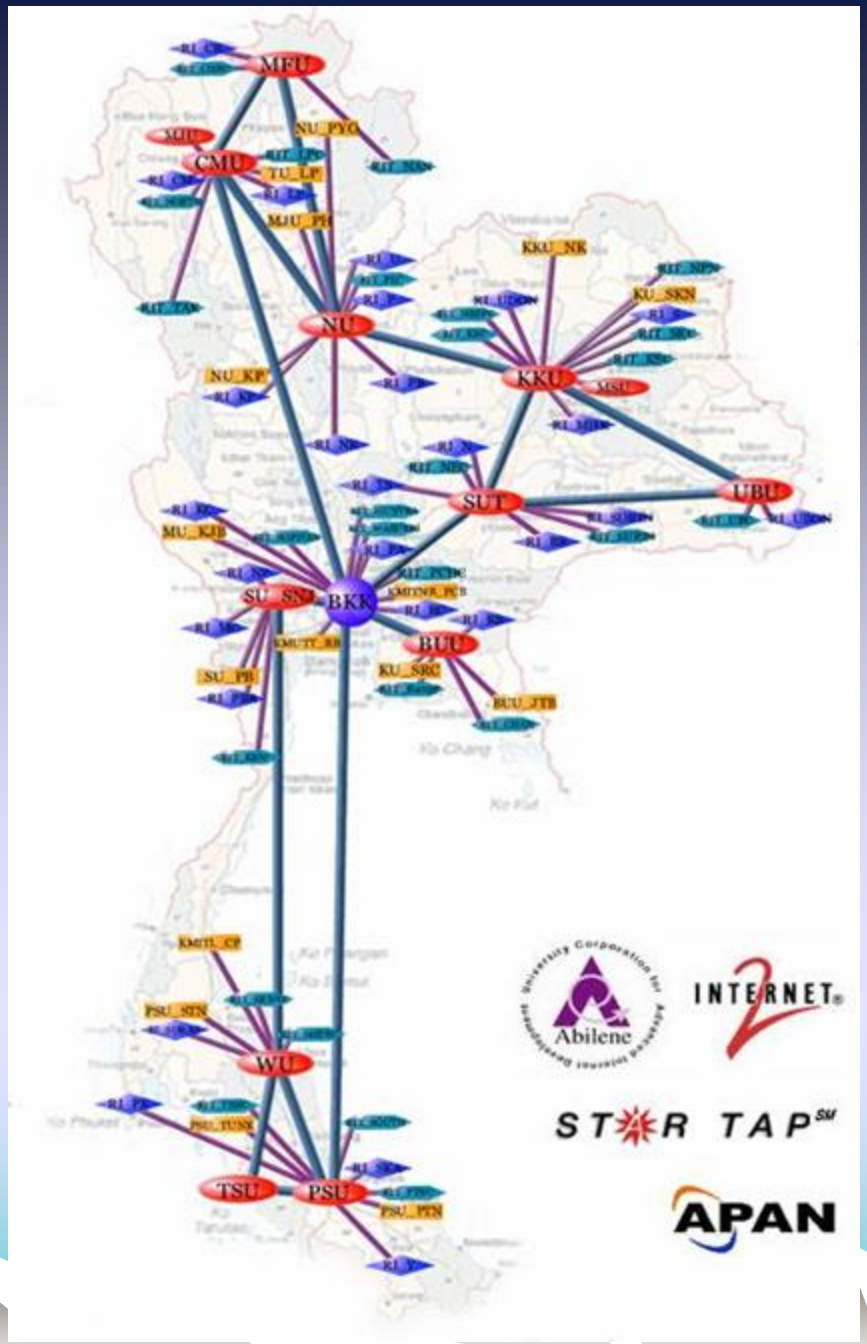
●**MAN (Metropolitan Area Network)** ระบบเครือข่ายบริเวณเมืองใหญ่ หรือย่านใจกลางธุรกิจ อาจถือเป็นระบบเครือข่ายแบบ WAN ระยะสั้น เป็นการเชื่อมโยงระหว่างตึกต่าง ๆ ด้วยการเชื่อมโยงความเร็วสูงผ่าน fiber optic และเป็นระบบเครือข่ายสาธารณะที่สามารถทำการเช่าใช้งานจากผู้ให้บริการได้



●**WAN (Wide Area Network)** ระบบเครือข่ายที่ประกอบด้วยเครือข่าย LAN ตั้งแต่ 2 วงขึ้นไปเชื่อมต่อกันระยะทางที่ไกลมาก ซึ่งจะเชื่อมต่อกันด้วยระบบเครือข่ายสาธารณะ เช่น สายโทรศัพท์ แบ่งเป็น 2 ประเภทใหญ่ ๆ คือ

- เครือข่ายส่วนตัว (Private Network) เป็นการจัดระบบเครือข่ายซึ่งมีใช้เฉพาะองค์กรที่เป็นเจ้าของเครือข่าย เช่นองค์กรที่มีสาขา
- เครือข่ายสาธารณะ (Public Data Network :PDNs) บางครั้งเรียก เครือข่ายมูลค่าเพิ่ม ซึ่งเป็นระบบเครือข่ายที่องค์กรได้รับสัมปทานจัดทำ เพื่อให้เช่าใช้ช่องทางการสื่อสาร สำหรับผู้ที่ไม่ต้องการวางโครงข่ายช่องทางการสื่อสารเอง

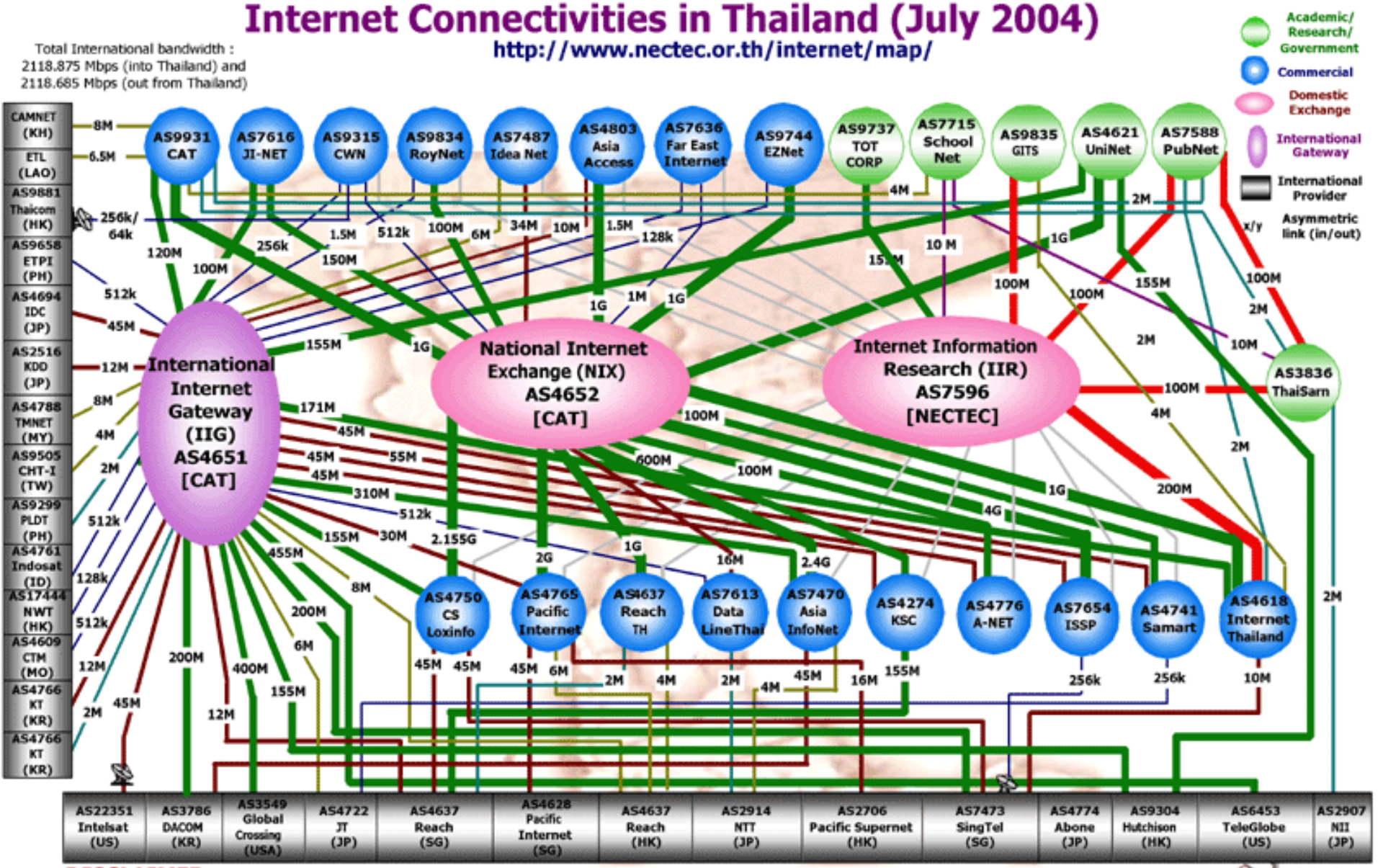



MFU
CMU
NU
KKU
SUT
UBU
BKK
BUU
WU
TSU
PSU
Abilene
INTERNET2
STAR TAP
APAN

Internet Connectivities in Thailand (July 2004)

http://www.nectec.or.th/internet/map/

Total International bandwidth :
2118.875 Mbps (into Thailand) and
2118.685 Mbps (out from Thailand)

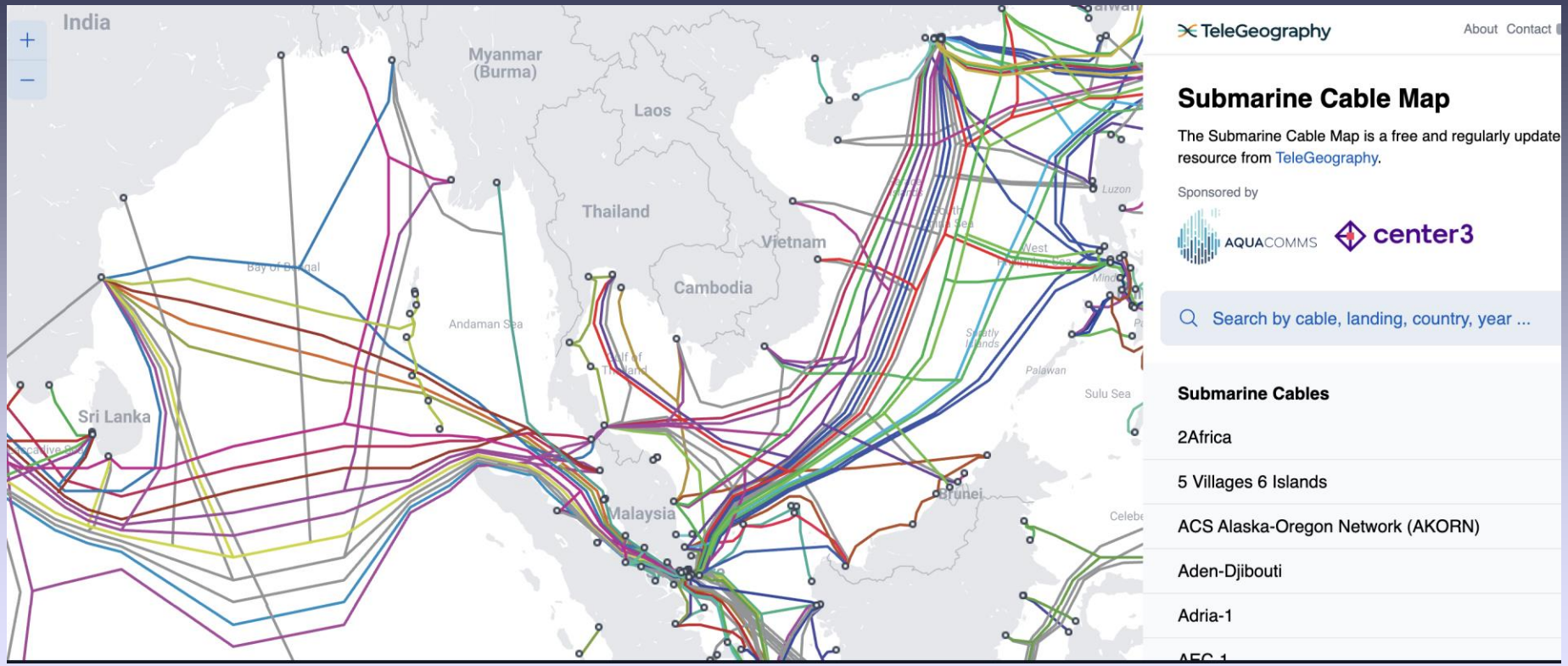


DISCLAIMER

Chart Date: 2004-07-01

This chart is designed, maintained and copyrighted by Chatchai Chan-In and Thaweesak Koanantakool NTL, NECTEC. All rights reserved. The information contained in this chart is based on actual measurements and estimation. We welcome update information, but reserve the rights to verify the accuracy of the given information. Please contact us at **netadmin@ntl.nectec.or.th** . For authoritative information please contact Communications Authority of Thailand.

https://www.submarinecablemap.com/

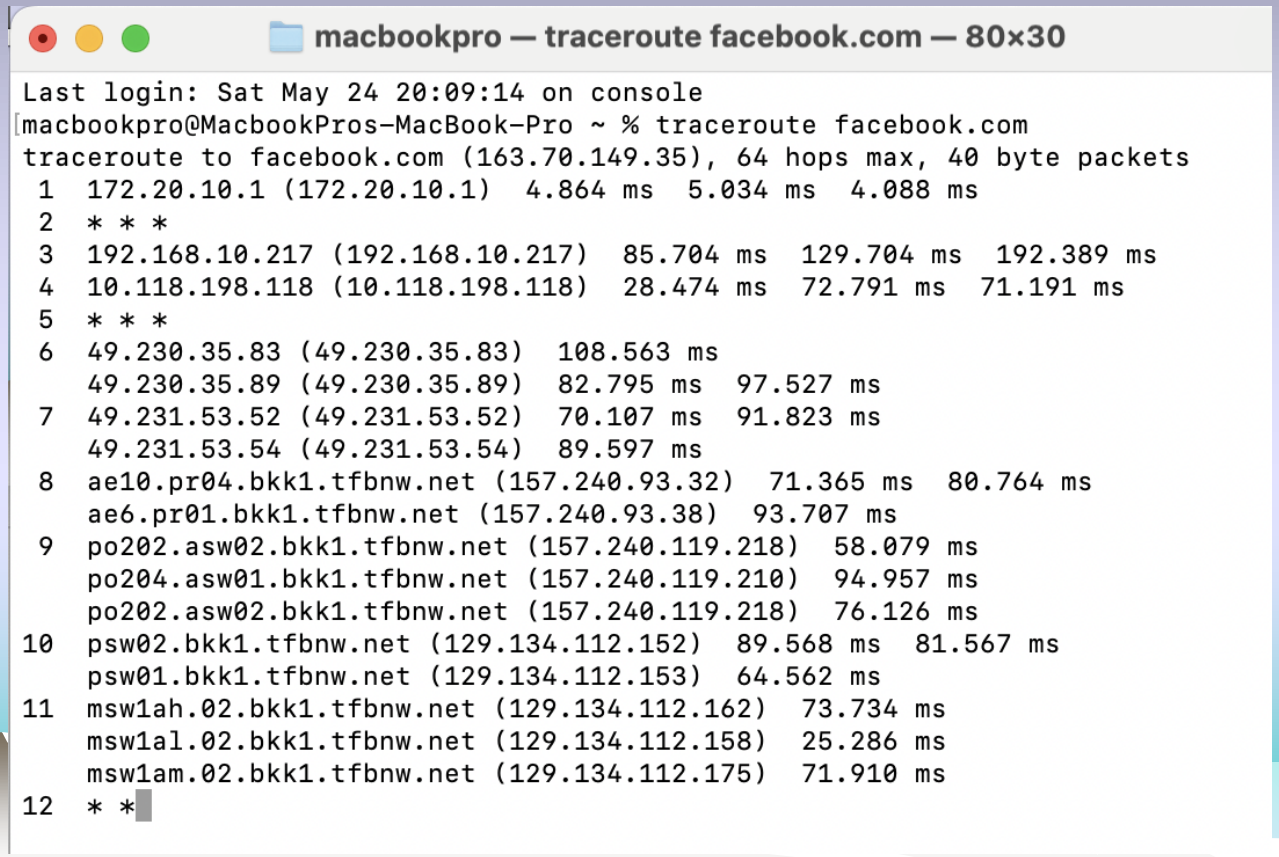


เครื่องมือตรวจสอบเส้นทาง (Traceroute / Looking Glass)

ใช้ตรวจสอบว่าเมื่อคุณเชื่อมต่อจากประเทศไทยไปยังเซิร์ฟเวอร์ต่างประเทศ ข้อมูลเดินทางผ่านเส้นทาง (hop) อะไรบ้าง

คำสั่งบนเครื่อง:

- Windows: tracert www.google.com
- Linux/macOS: traceroute www.google.com



ระบบ LAN
จุดประสงค์ของการใช้งานระบบ LAN

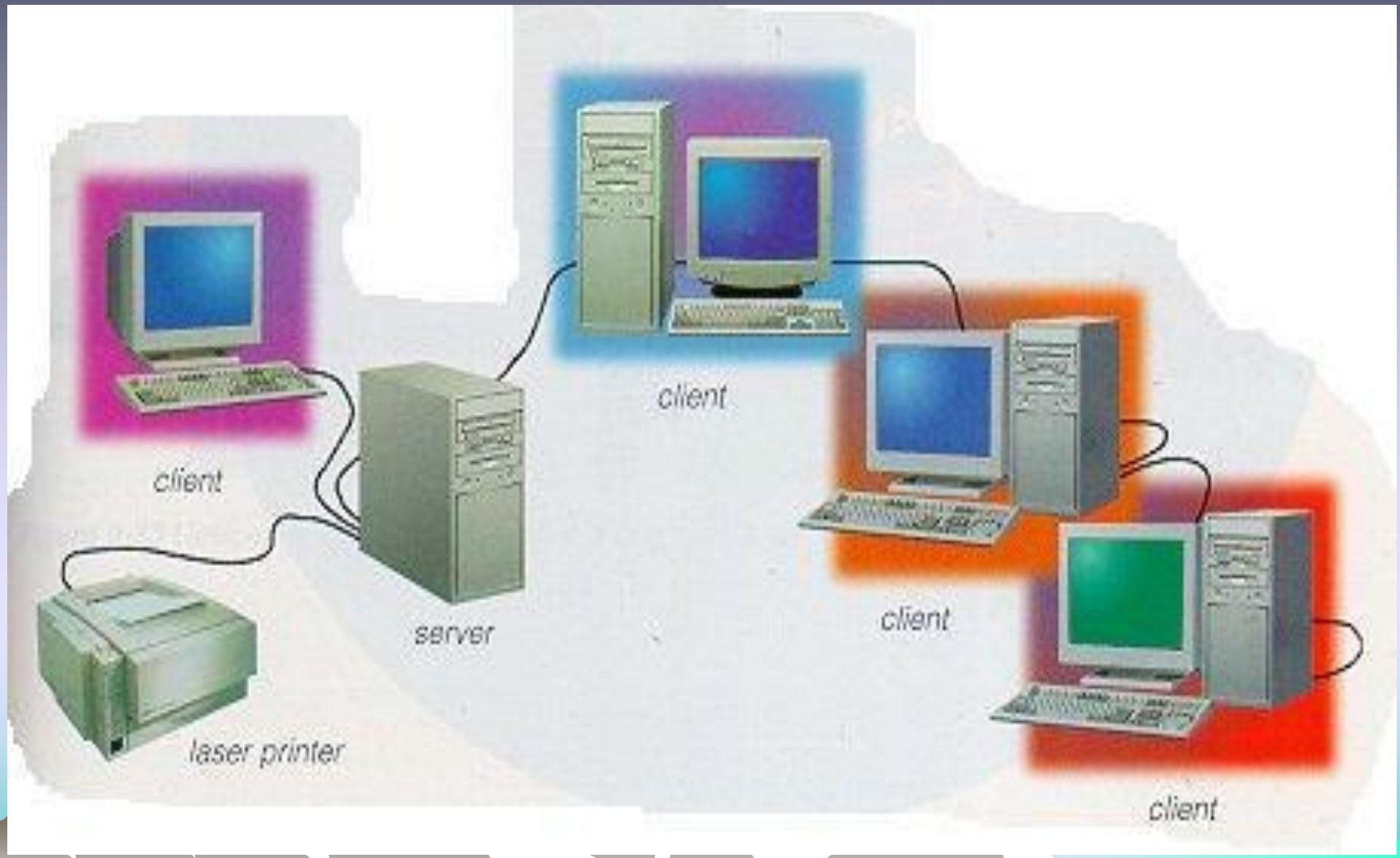
- สามารถใช้ hardware และ software ร่วมกันได้
- สามารถใช้ข้อมูลร่วมกันได้ แม้ว่าข้อมูลนั้นจะเก็บอยู่ในเครื่องคอมพิวเตอร์อื่น รวมทั้งสามารถจัดเก็บข้อมูลไว้เพียงที่เดียว
- สามารถไว้วางใจได้
- สามารถส่งข่าวสารระหว่างเครื่องในระบบได้
- สามารถคุยโต้ตอบกันระหว่างผู้ใช้
- ลดค่าใช้จ่ายโดยรวมขององค์กร

ประเภทของระบบ LAN

- **เครือข่ายแบบเครื่องลูกข่าย-เครื่องแม่ข่าย (client-server)**

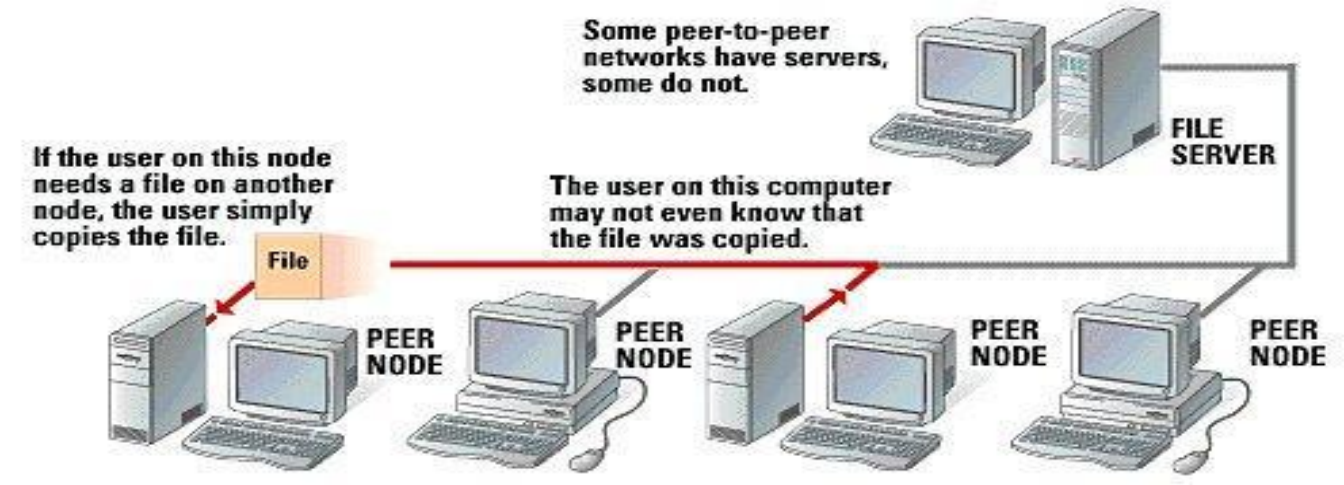
เครื่องPCจะทำหน้าที่เป็นเครื่องclient และ เครื่องPCที่มีความสามารถสูงจะทำหน้าที่เป็นเครื่อง server มีหน้าที่จัดการควบคุมการเรียกใช้ข้อมูลหรือซอฟต์แวร์และอุปกรณ์ทุกตัวที่ต่ออยู่ในระบบเครือข่าย รวมทั้งควบคุมความปลอดภัยของข้อมูล ซึ่งมี serverหลายแบบ ได้แก่

- file server ทำหน้าที่เก็บโปรแกรมและแฟ้มข้อมูลไว้ เพื่อให้เครื่องลูกเรียกใช้ได้
- database server ทำหน้าที่เก็บเฉพาะข้อมูล ให้เครื่องอื่น ๆเรียกใช้
- print server ทำหน้าที่ควบคุมการใช้งานเครื่องพิมพ์ที่ต่อกับระบบ


client
client
client
client
server
laser printer

- **เครือข่ายแบบเครื่องเพียร์ทูเพียร์ (Peer-to-Peer)**

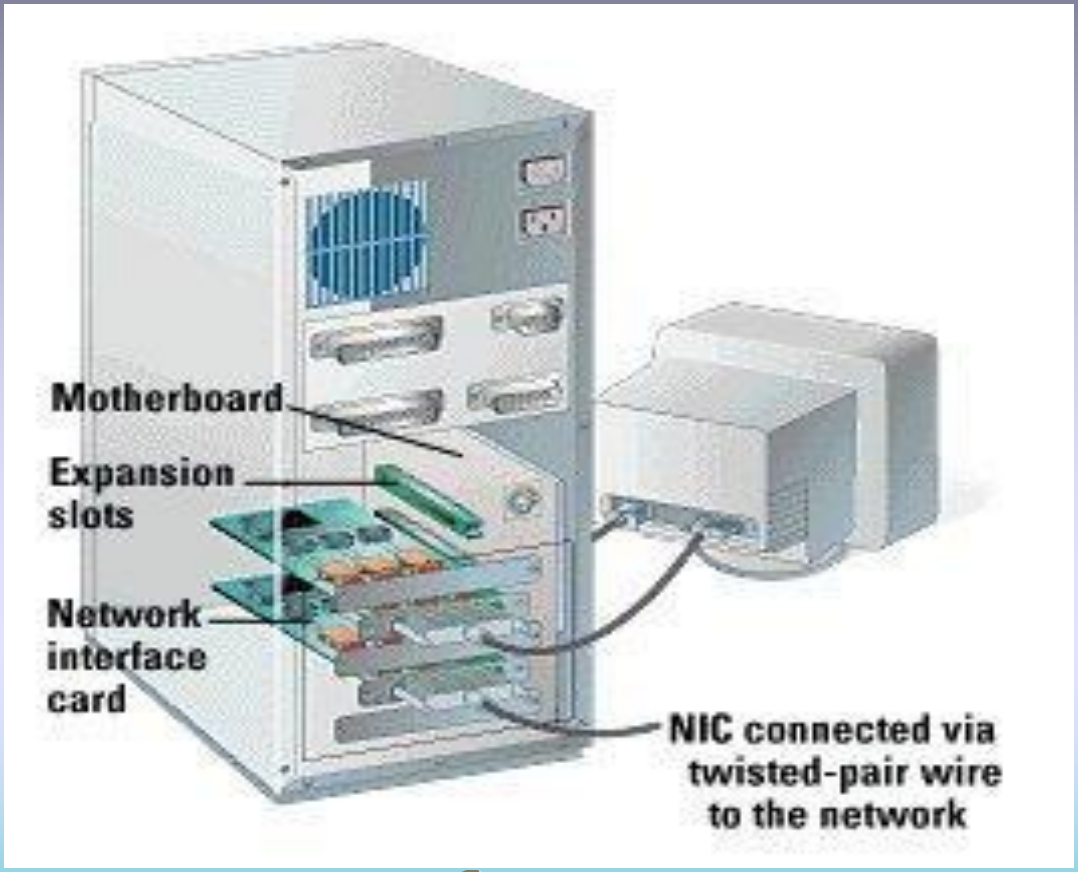
กำหนดให้เครื่องPCจทุกตัวที่ต่ออยู่ในระบบเครือข่าย มีฐานะเท่าเทียมกัน แต่ละเครื่องสามารถติดต่อสื่อสารกันได้โดยตรง โดยไม่ผ่านผู้ให้บริการ มีค่าใช้จ่ายถูกกว่า แต่ข้อเสียคือ มีความเร็วค่อนข้างช้า ถ้ามีการใช้งานเครือข่ายหนัก รวมทั้งควบคุมความปลอดภัยของข้อมูล

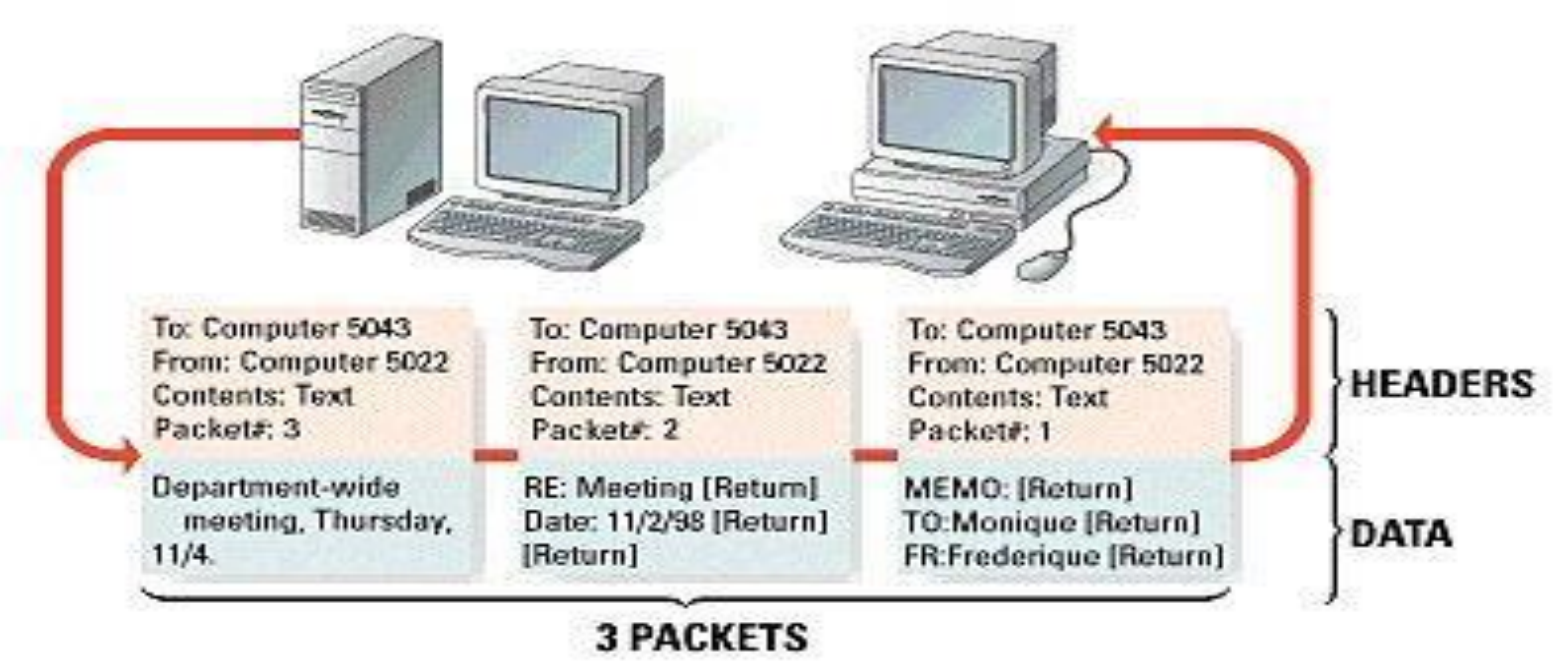


อุปกรณ์พื้นฐานในการเชื่อมโยงระบบเครือข่าย

- **การ์ดแลน** (**Network Interface Card หรือ NIC**) ใช้เชื่อมโยงคอมพิวเตอร์เข้ากับระบบเครือข่าย หน้าที่ควบคุมการรับ-ส่งข้อมูล ตรวจสอบความถูกต้องของข้อมูล
- **อุปกรณ์ในการเชื่อมโยง** (Link Media, Communication Channel) เช่น สายเคเบิลต่างๆ หรือการเชื่อมโยงแบบไร้สาย
- **ซอฟต์แวร์**ในการสื่อสาร เช่น ระบบปฏิบัติการเครือข่าย, Application SW
- **อุปกรณ์เสริม**อื่นๆ เช่น Hub, Switch, Router,โมเด็ม, โทรศัพท์, ไมโครโฟน, ลำโพง, กล้องวีดีโอดิจิตอล และอื่นๆ

อุปกรณ์พื้นฐานในการเชื่อมโยงระบบเครือข่าย





- ข้อมูลบนระบบเครือข่ายจะถูกแบ่งเป็นส่วนย่อย (**Packet)** แล้วส่งไปยังปลายทาง แล้วที่ปลายทางคอมพิวเตอร์จะทำการรวม Packet ที่ได้รับมาประกอบกลับรวมกันเป็นข้อมูลเดิม
- การสื่อสารระหว่างคอมพิวเตอร์ (ซึ่งอาจต่างชนิดกัน) สามารถเข้าใจกันได้ทุกเครื่องโดยใช้ภาษาหรือกฎเดียวกันหมดเรียกว่า **Protocol** เช่น TCP/IP IPX/SPX และ NetBEUI

โครงสร้างเครือข่าย (NETWORK TOPOLOGY)

- **โครงสร้างแบบบัส (Bus Topology)**

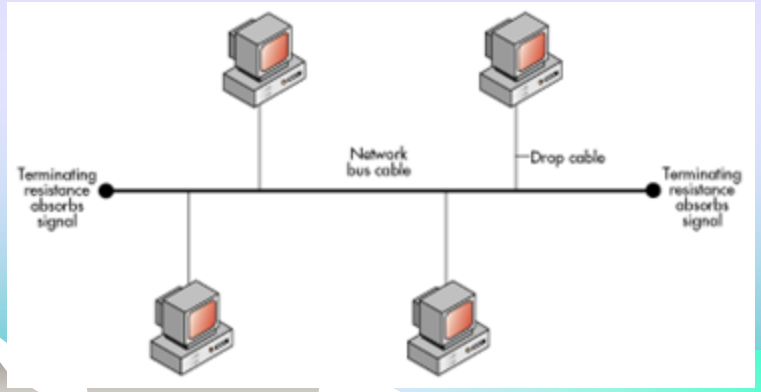
โครงสร้างที่เชื่อมต่อเครื่องPCแต่ละเครื่องด้วยสายเคเบิลที่ใช้ร่วมกัน การรับส่งข้อมูลจะผ่านไปมาระหว่างแต่ละเครื่อง โดยไม่ต้องผ่าน server ก่อน

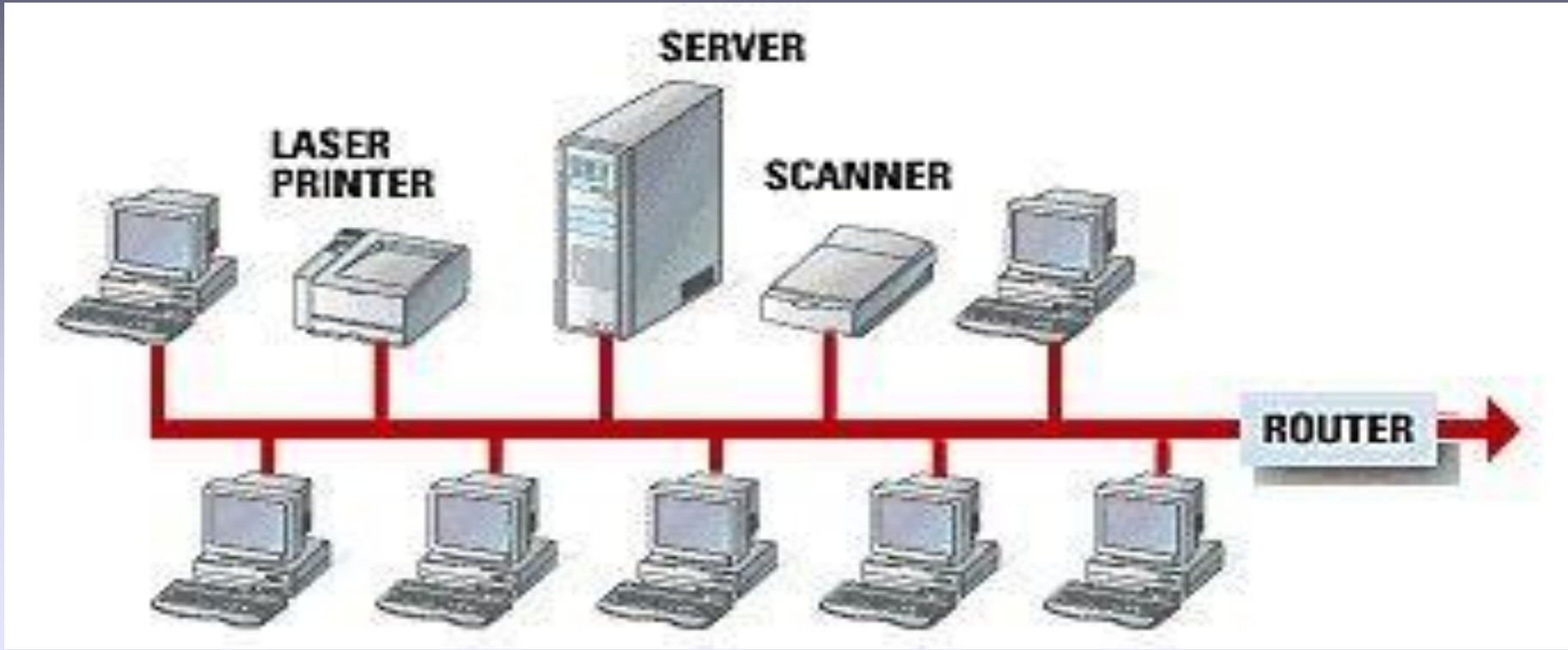
ข้อดี - ใช้สายเคเบิลน้อยที่สุด

- รูปแบบการวางสายง่าย และ สามารถขยายระบบได้ง่าย
- ถ้ามีเครื่องเสียก็ไม่มีผลอะไรต่อระบบโดยรวม

ข้อเสีย - ตรวจหาจุดที่มีปัญหาได้ยาด

- ระบบมีประสิทธิภาพลดลง ถ้ามีการจราจรของข้อมูลสูง




SERVER
LASER
PRINTER
SCANNER
ROUTER

โครงสร้างแบบดาว

- **โครงสร้างแบบดาว (Star Topology)**

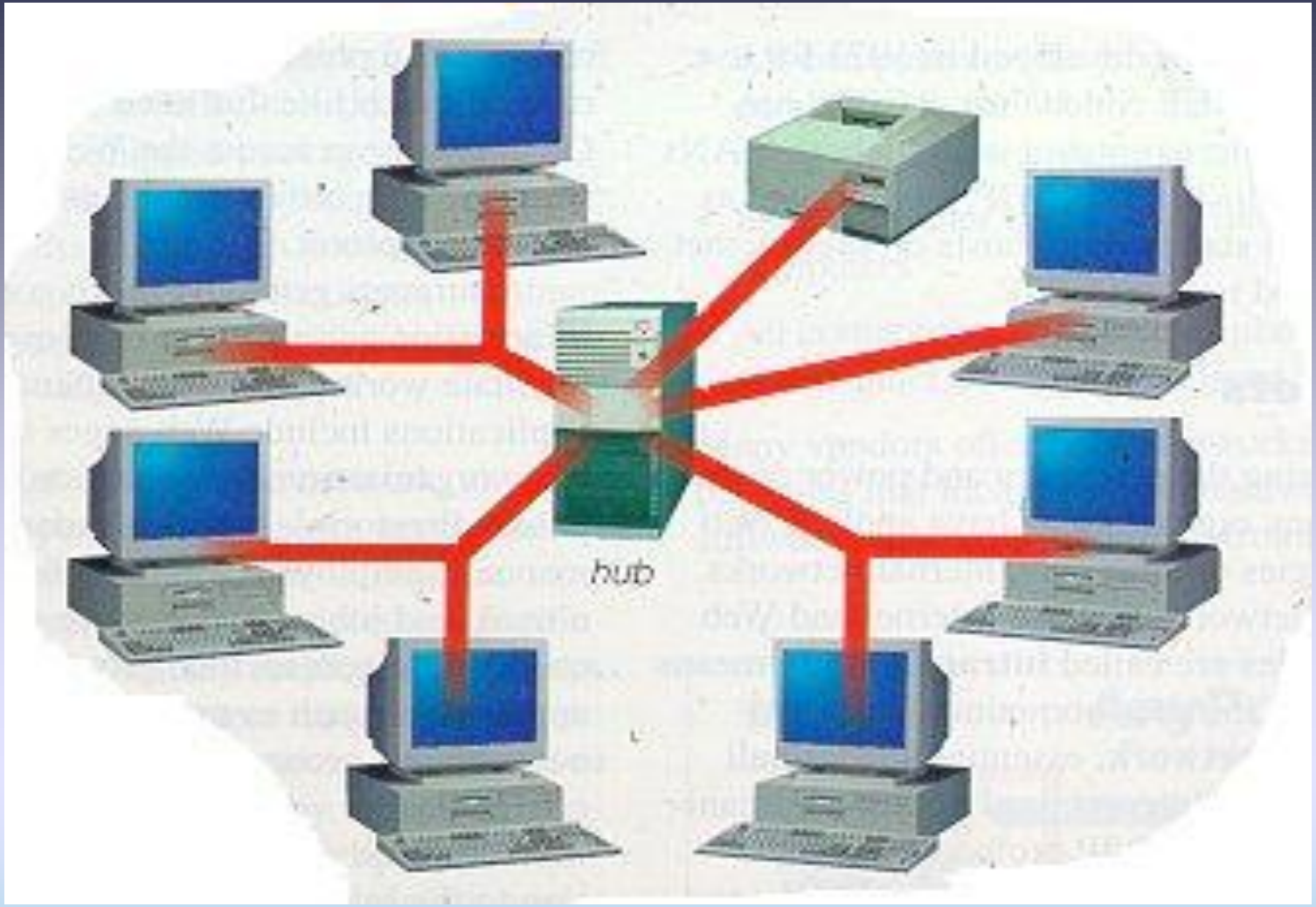
โครงสร้างที่เชื่อมต่อเครื่องPCแต่ละเครื่องเข้ากับเครื่อง server โดยใช้อุปกรณ์ hub การรับส่งข้อมูลทั้งหมดต้องผ่าน server เสมอ

ข้อดี - การเชื่อมต่อคอมพิวเตอร์เครื่องใหม่สามารถทำได้ง่าย และไม่กระทบกับเครื่องอื่นในระบบ

- ถ้ามีเครื่องเสียก็ไม่มีผลอะไรต่อระบบโดยรวม และ เปลี่ยนรูปแบบการวางสายได้ง่าย
- ตรวจสอบจุดที่เป็นปัญหาได้ง่าย
- รับส่งข้อมุลได้รวดเร็ว

ข้อเสีย - มีค่าใช้จ่ายสุง เนื่องจากค่าสายส่งข้อมูล

- ถ้า server เสียระบบเครือข่ายจะหยุดชะงักทั้งหมดทันที


hub

โครงสร้างแบบวงแหวน (Ring Topology)

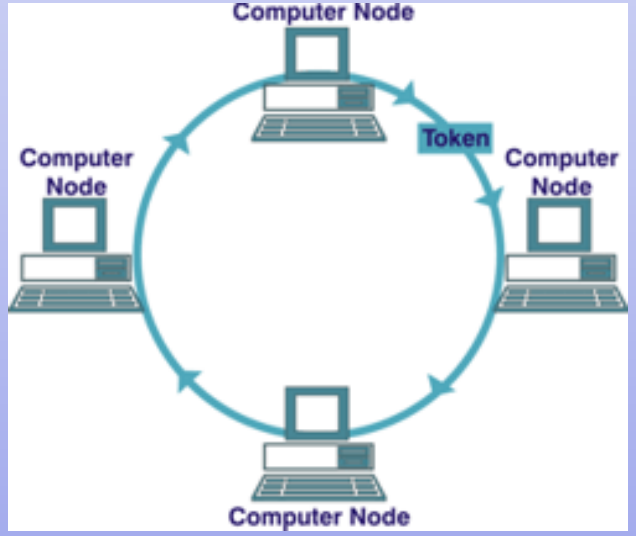
โครงสร้างที่เชื่อมต่อเครื่องPCแต่ละเครื่องเข้ากับเครื่อง server เข้าเป็นลักษณะวงแหวน การรับส่งข้อมูลทั้งหมดจะส่งผ่านกันไปในวงจนกว่าจะถึงเครื่องผู้รับที่ถูกต้อง

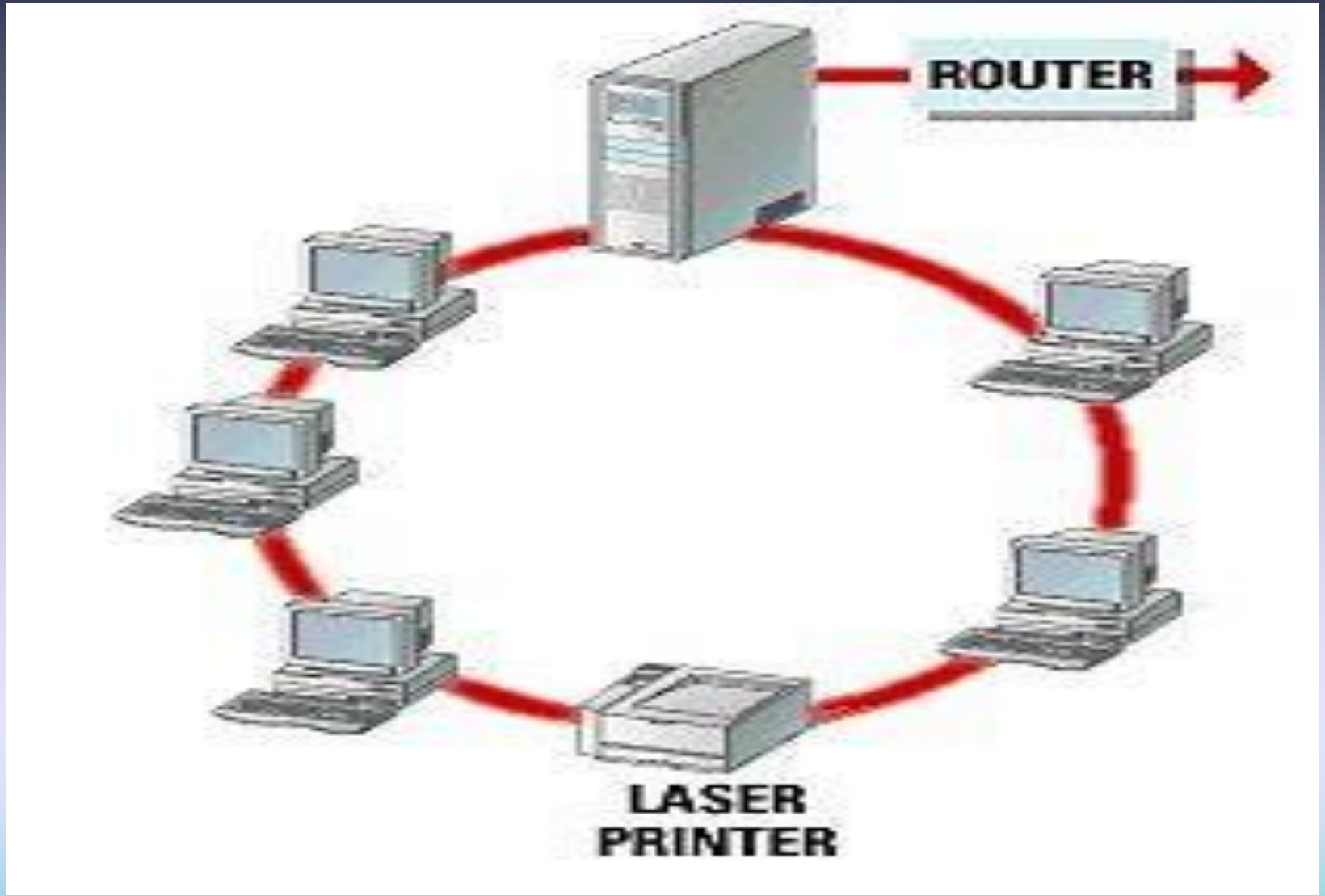
ข้อดี - ใช้สายเคเบิลน้อย

- ระบบมีประสิทธิภาพสูง แม้การจราจรของข้อมูลสูง ไม่มีการชนของข้อมูล เพราะข้อมูลวิ่ง ในทิศทางเดียว

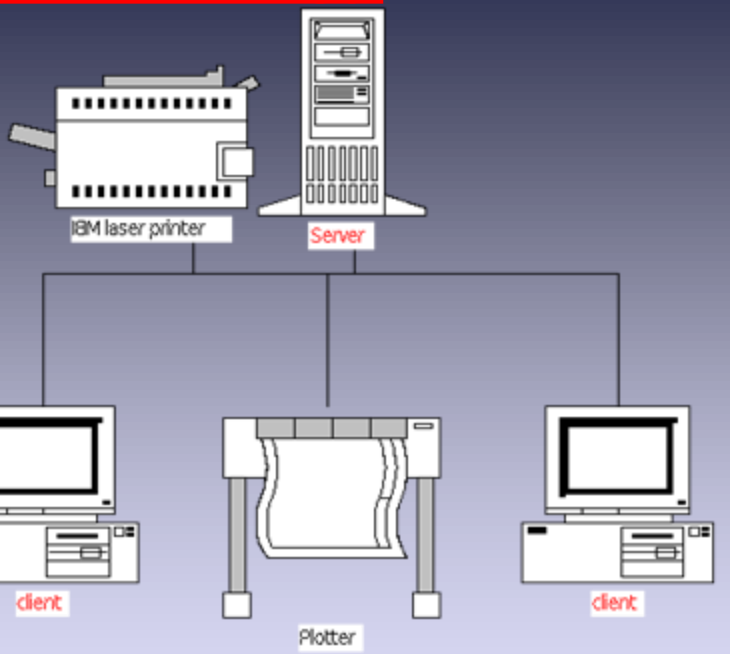
ข้อเสีย - ถ้า มีเครื่องที่มีปัญหา อาจมีผลให้ระบบเครือข่ายจะหยุดชะงักทั้งหมดทันที

- ตรวจหาจุดที่มีปัญหาได้ยาด
- เปลี่ยนรูปแบบการวางสายได้ยาก ต้องหยุดชะงักการทำงานของเครือข่าย

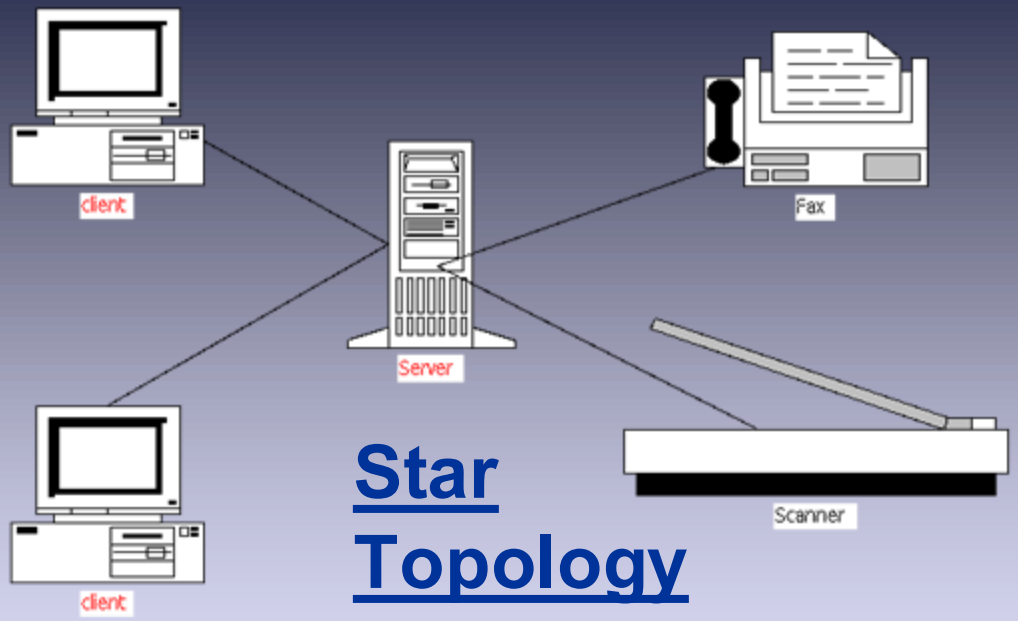



ROUTER
LASER
PRINTER

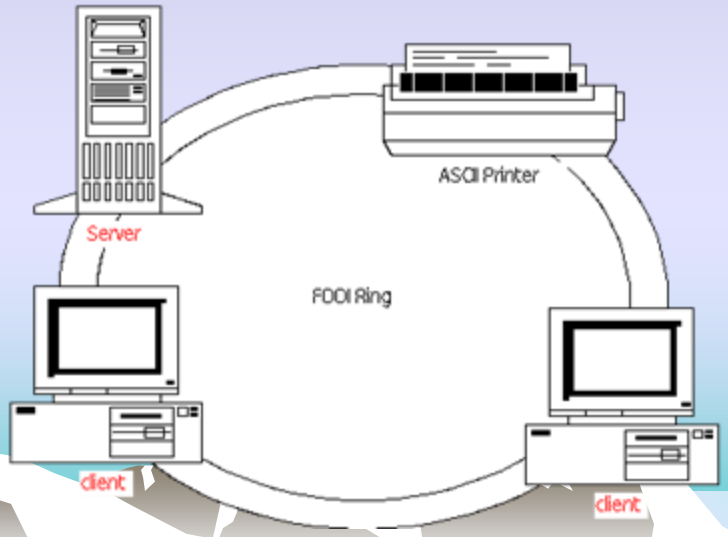
Bus Topology



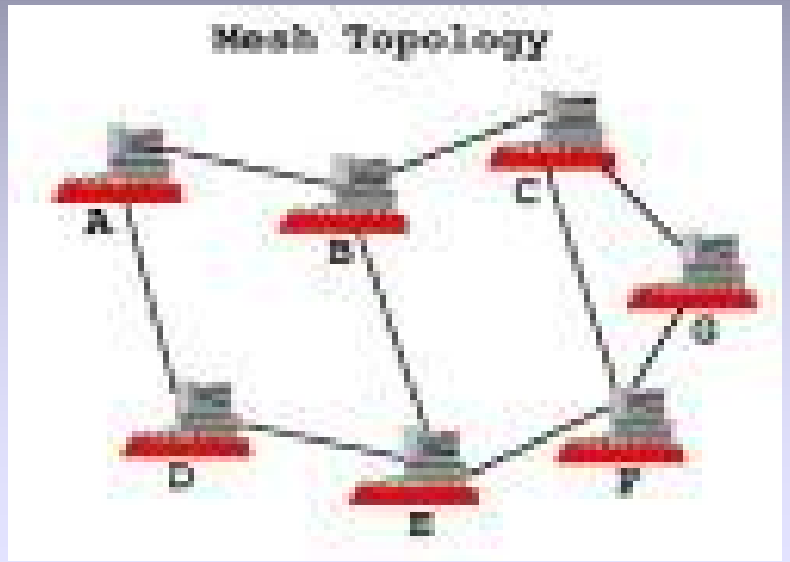
Star Topology



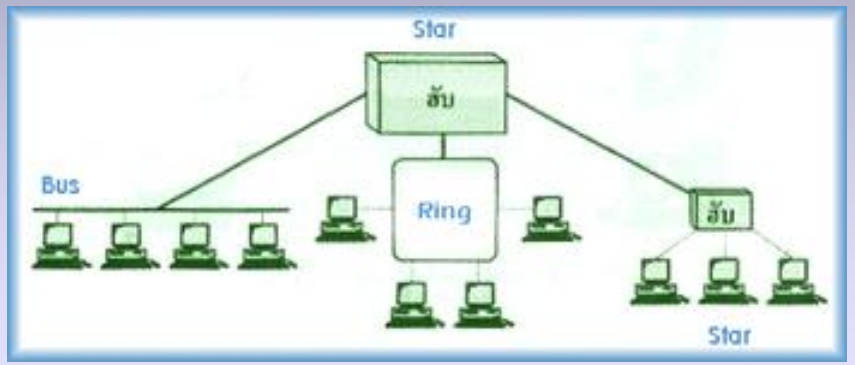
Ring Topology

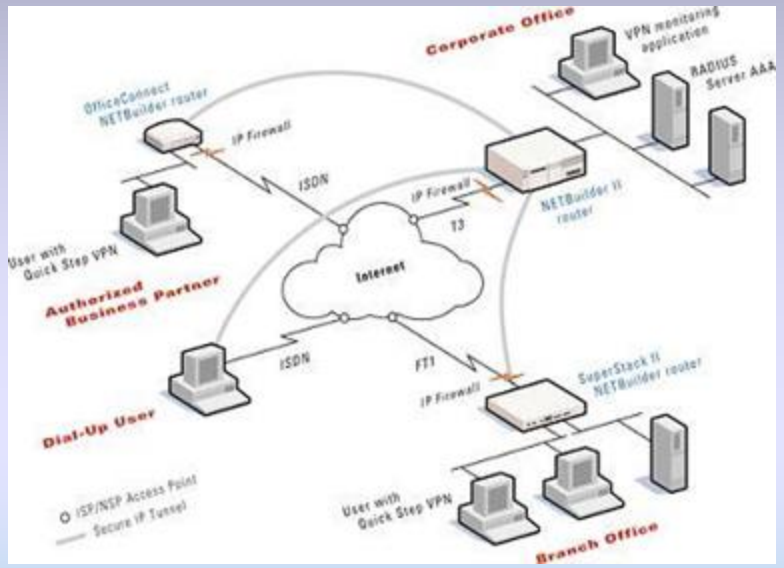


MESH TOPOLOGY



HYBRID TOPOLOGY





มาตรฐานการเชื่อมต่อเครือข่าย ที่เป็นที่นิยมแพร่หลาย

- **Ethernet**
  ความเร็ว 10 Mbps ใช้สาย 10base-2 , 10base-5
  10base-T หรือ UTP
- **Fast Ethernet**
  ความเร็ว 100 Mbps ใช้สาย 100base-T
- **Gigabit Ethernet** ความเร็ว 1000 Mbps

อุปกรณ์สื่อสารข้อมูล

- อุปกรณ์รวมสัญญาณ
- มัลติเพล็กเซอร์ (Multiplexer) นิยมเรียกว่า มัก (mux) เป็นอุปกรณ์ที่ใช้ในการรวมข้อมูลจากเครื่องเทอร์มินัลจำนวนหนึ่งเข้าด้วยกัน และส่งผ่านสายสื่อสารเช่น สายโทรศัพท์ และปลายทางของ มัก อีกตัวจะทำหน้าที่ แยกข้อมุลส่งไปยังจุดหมายปลายทาง
- Concentrator นิยมเรียกว่า คอนเซน สามารถทำการเก็บข้อมูลเพื่อส่งต่อ โดยใช้หน่วยความจำ buffer ทำให้สามารถเชื่อมต่อระหว่างอุปกรณ์ที่มีความเร็วสูงกับความเร็วต่ำได้
- Hub เรียกอีกอย่างว่า LAN Concentrator เพราะทำหน้าที่เหมือนคอนเซน แต่มีราคาถูกกว่า
- Front-End Processor พบมากในระบบขนาดใหญ่ เพื่อช่วยลดภาระในการติดต่อกับอุปกรณ์รอบข้างเครื่อง คอมพิวเตอร์หลัก

อุปกรณ์เชื่อมต่อเครือข่าย

- เครื่องทวนสัญญาณ (Repeater) เป็นอุปกรณ์ที่อยู่ในระดับ physical layer ทำหน้าที่ เป็นอุปกรณ์เชื่อมต่อสำหรับขยายสัญญาณให้กับเครือข่าย เพื่อเพิ่มระยะทางในการรับส่งข้อมูล

- บริดจ์ (Bridge) ใช้ในการเชื่อมต่อวง LAN เข้าด้วยกัน ทำให้สามารถขยายขอบเขต LAN ออกไปได้

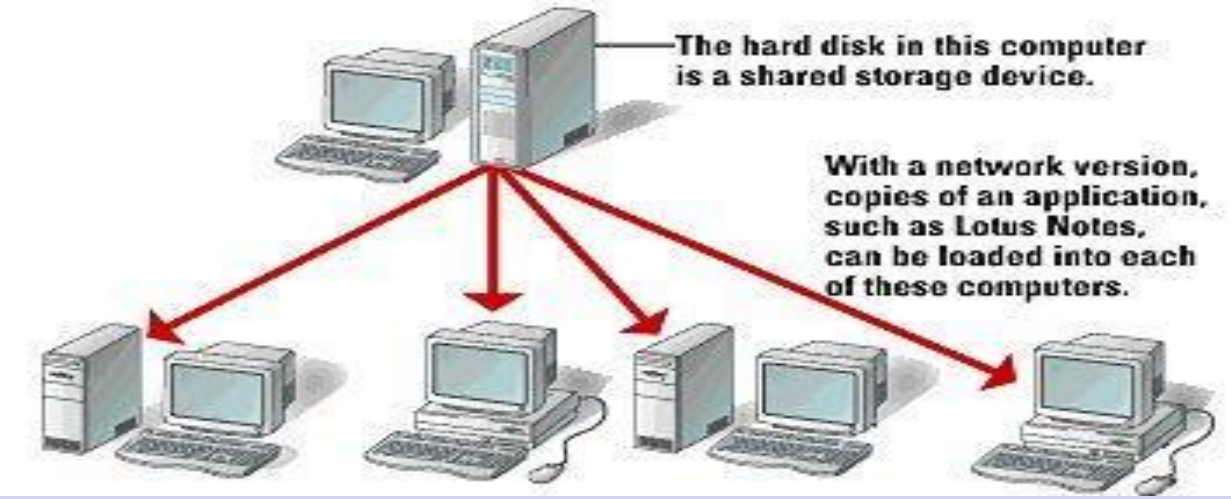
- Switch เรียกอีกอย่างว่า Ethernet Switch เป็น บริดจ์แบบหลายช่องทาง ช่วยลดการจราจรระหว่างเครือข่ายที่ไม่จำเป็น

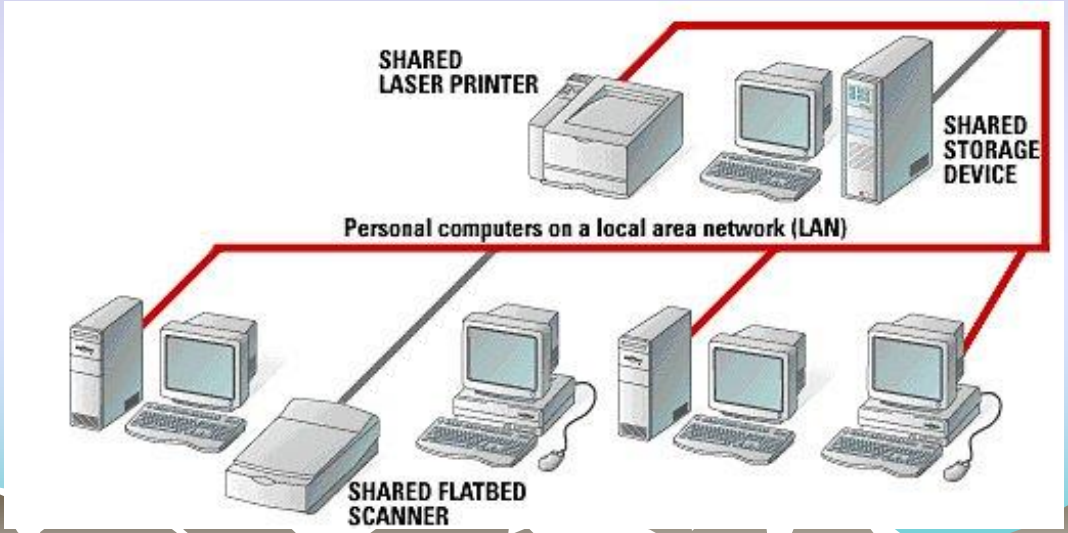
- Router เป็นอุปกรณ์ที่ทำงานในระดับ Network layer ทำให้สามารถใช้ในการเชื่อมต่อระหว่างเครือข่ายที่ใช้โปรโตคอลเครือข่ายต่างกัน และสามารถทำการกรองเลือกชนิดของข้อมูลที่ระบุไว้ ช่วยลดภาระปัญหา การจราจร ของข้อมูล และเพิ่มความปลอดภัยของเครือข่าย การจราจร

ประโยชน์ที่ได้รับจากระบบเครือข่าย

Simultaneous Access

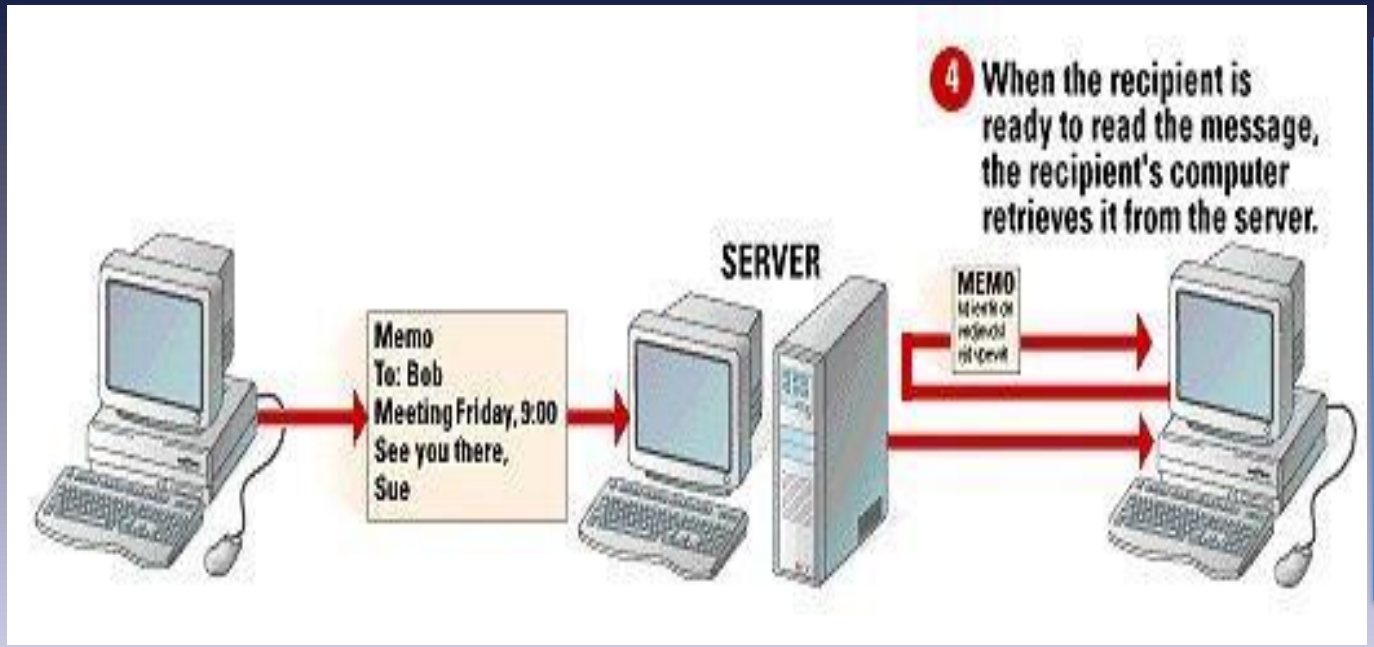
ผู้ใช้หลายคนสามารถใช้ข้อมูลจากที่ เดียวกันได้





Shared Peripheral Devices

การใช้อุปกรณ์ร่วมกัน



Personal Communication

การสื่อสารระหว่างบุคคล

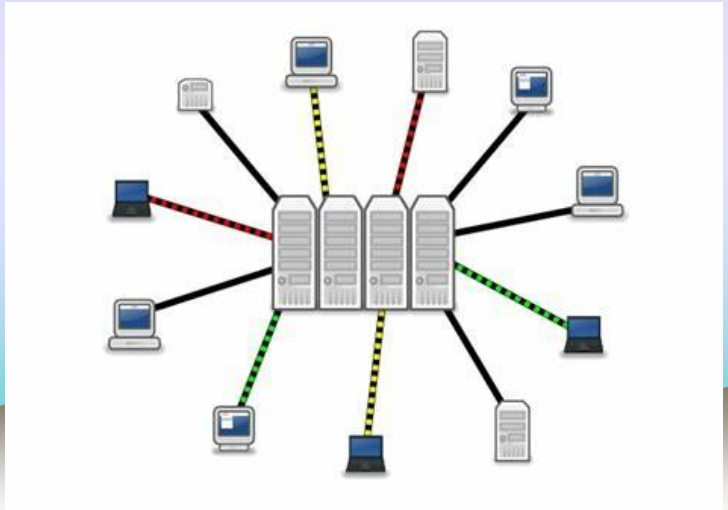
Personal Communication: Video Conferencing

การสื่อสารในกลุ่มผู้ใช้ที่อยู่ต่างสถานที่กัน โดยได้ทั้งภาพและเสียง

วิธีการประมวลผลของเครื่องคอมพิวเตอร์ในปัจจุบัน

- ระบบการประมวลผลข้อมูลที่ศูนย์กลาง (Centralized Data Processing)

  การประมวลผลทั้งหมดจะเกิดขึ้นที่เครื่องหลักเพียงเครื่องเดียว ในระยะแรกผู้ใช้ต้องไปใช้งานที่ศูนย์คอมพิวเตอร์เท่านั้น แต่ในปัจจุบัน จะเป็นการประมวลผลทางไกล (TeleProcessing) ซึ่งเป็นการทำให้ผู้ใช้สามารถเชื่อมต่อมาใช้งานคอมพิวเตอร์ที่ศูนย์กลางได้จากระบบการสื่อสารต่าง ๆ แต่การประมวลผลจะอยู่ที่ศูนย์เช่นเดิม เครื่องที่เชื่อมต่อเข้ามามีหน้าที่เพียงแสดงผลที่เครื่องศูนย์กลางส่งมาเท่านั้น

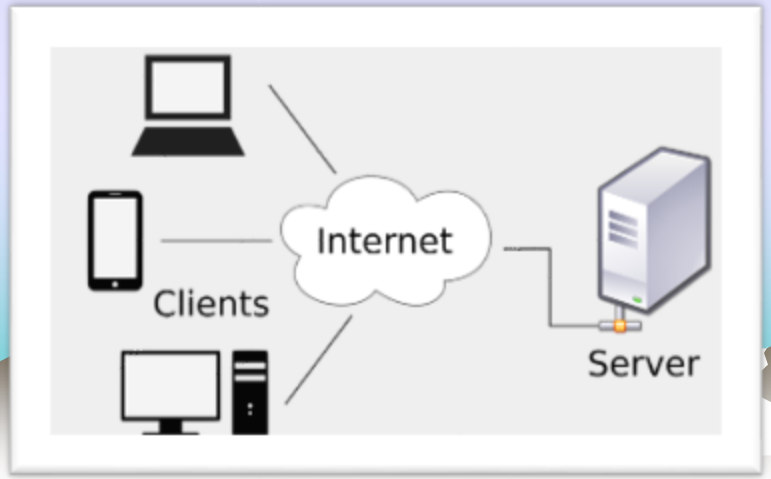


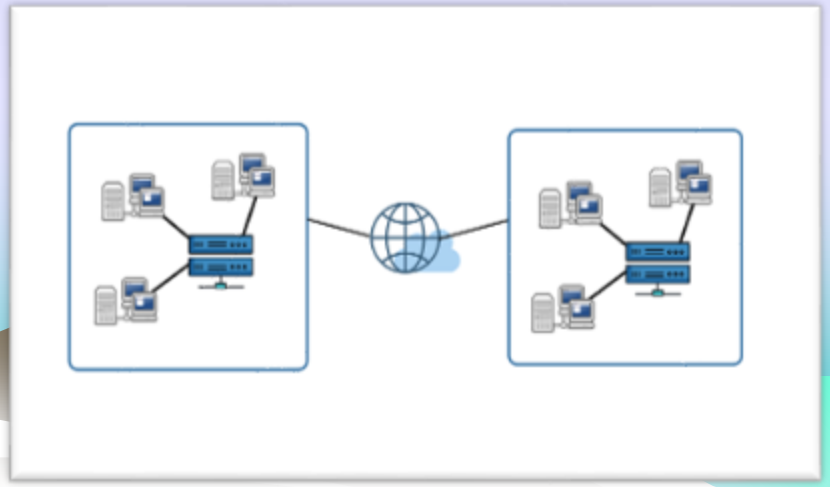
•ระบบการประมวลผลข้อมูลไคลเอนต์-เซิร์ฟเวอร์ (Client-Server Processing)

เป็นการแบ่งการประมวลผลมาทำงานที่เครื่องพีซี โดยเครื่องพีซีจะเรียกใช้งานโปรแกรมที่ทำหน้าที่คุยกับโปรแกรมที่คอมพิวเตอร์ศูนย์กลาง และรับหน้าที่ในการนำข้อมูลที่ผ่านการประมวลผลจาก server แล้วมาแสดงผลในรูปแบบต่าง ๆที่เหมาะสม รวมทั้งรับหน้าที่ในส่วนของการโต้ตอบและรับข้อมูลจากผู้ใช้ด้วย

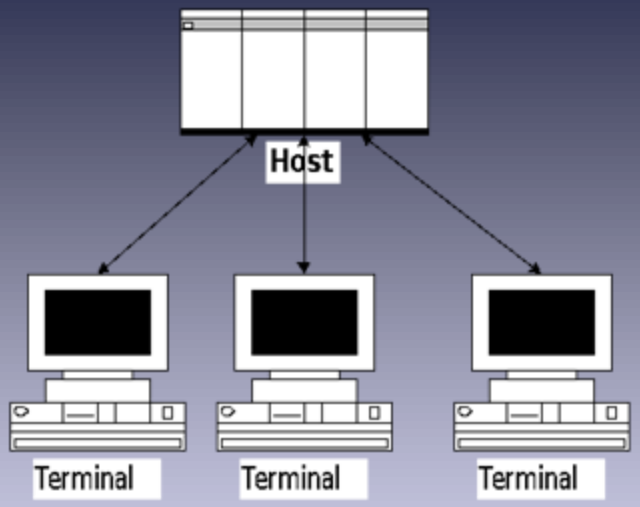
•ระบบการประมวลผลข้อมูลแบบกระจาย (Distributed Processing)

เป็นการกระจายภาระการประมวลผลไปยังเครื่องต่าง ๆ ที่เชื่อมต่อกันเป็นเครือข่าย และนำผลลัพธ์ที่ได้มารวมกัน ซึ่งเป็นการทำให้เพิ่มประสิทธิภาพในการประมวลผลของระบบโดยรวม รวมทั้งยังสามารถลดจำนวนข้อมูลที่ส่งผ่านเครือข่ายได้ด้วย

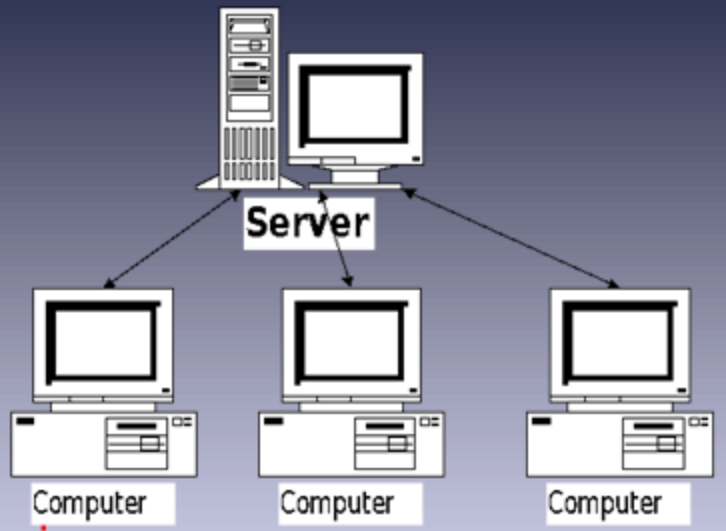




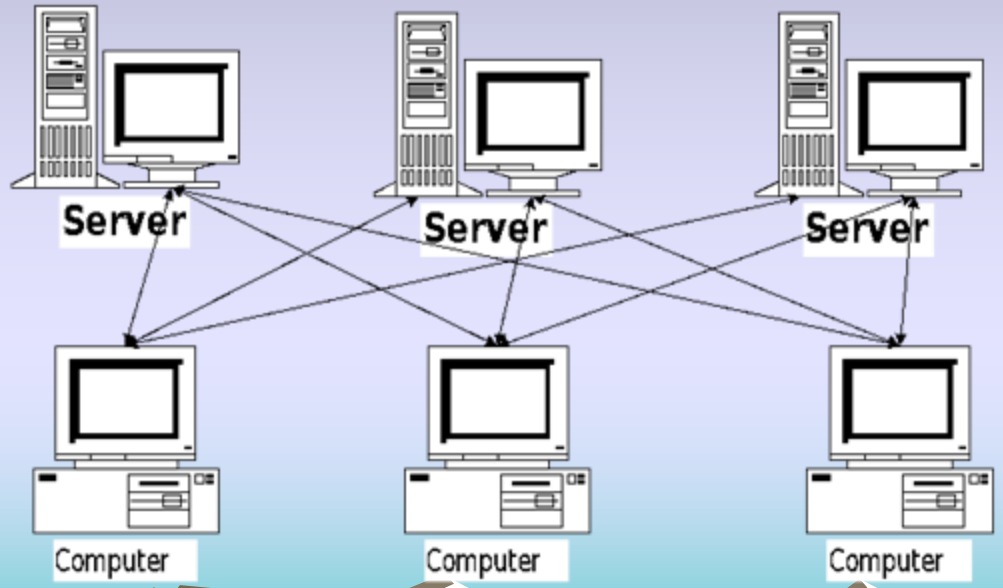
Centralized Processing



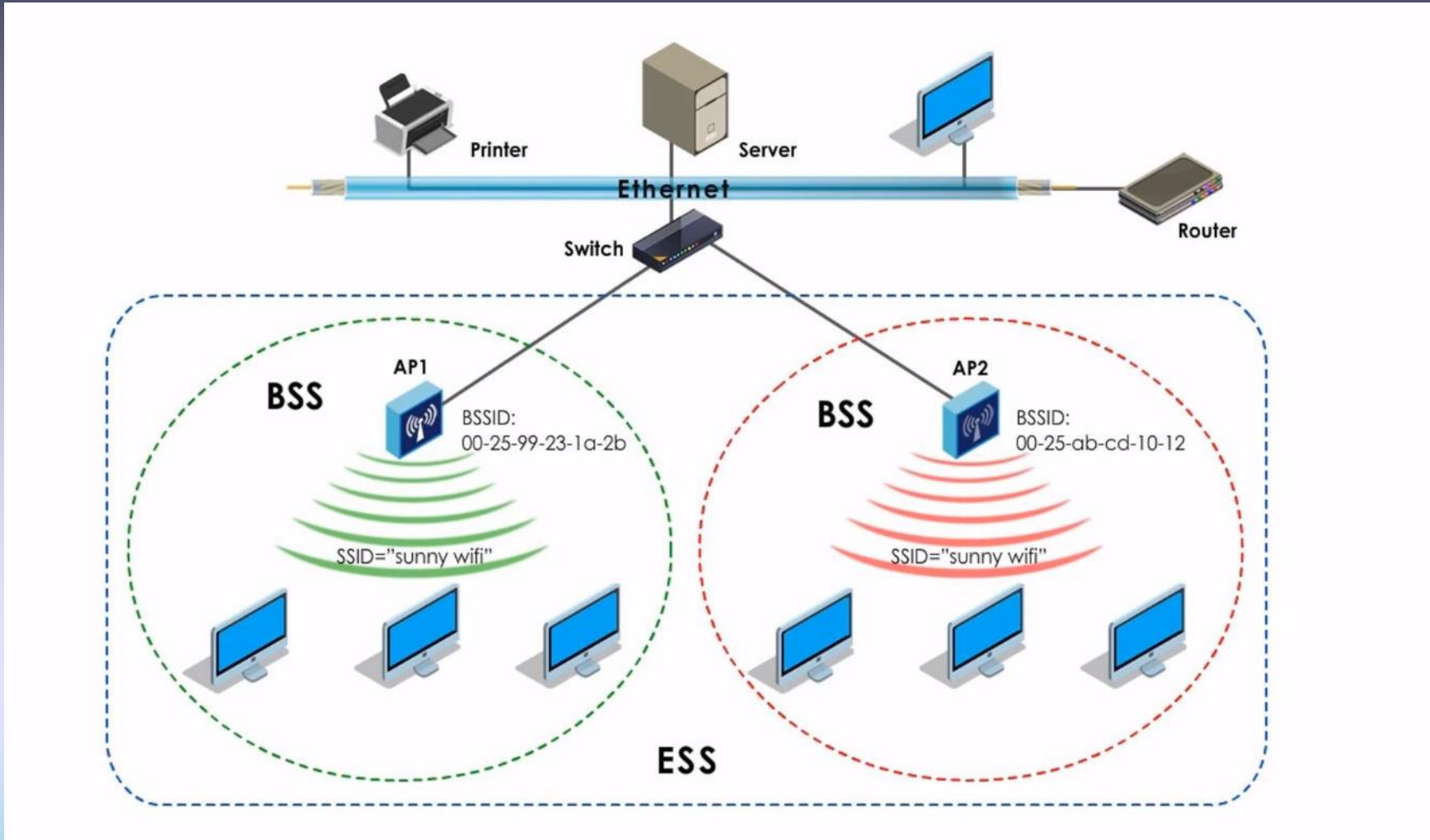
Client-Server Processing



Distributed Processing



SSID (Service Set Identifier) is the name of the network



คำสั่ง network เบื้องต้น

คำสั่ง	ใช้ทำอะไร	ตัวอย่าง
ipconfig (Windows) / ifconfig (Linux/mac)	ดู IP Address, Subnet, Gateway ของเครื่อง	ipconfig
ping	ตรวจสอบการเชื่อมต่อไปยังปลายทาง	ping 8.8.8.8
tracert (Windows) / traceroute (Linux/mac)	ดูเส้นทางของข้อมูล (hop) ที่เดินทางไปยังปลายทาง	tracert www.google.com
nslookup	ตรวจสอบ DNS (แปลงชื่อโดเมนเป็น IP)	nslookup www.google.com
netstat	ดูการเชื่อมต่อ (connection), port ที่กำลังเปิดอยู่	netstat -an
arp	ดู MAC Address ที่ cache ไว้ของอุปกรณ์ที่เชื่อมต่อกัน	arp -a
route	ดูหรือจัดการ Routing Table	route print
hostname	แสดงชื่อเครื่อง	hostname
curl	ทดสอบการร้องขอ HTTP/HTTPS	curl https://example.com
wget	ดาวน์โหลดไฟล์ผ่าน HTTP/HTTPS (ใช้บน Linux)	wget https://example.com/file.zip

คำสั่ง network เบื้องต้น

คำสั่ง	ใช้ทำอะไร	ตัวอย่าง
netsh (Windows)	ปรับแต่ง network adapter, firewall	netsh interface ip show config
ip a (Linux)	แสดง IP และ interface	ip a
dig (Linux/mac)	ตรวจสอบ DNS อย่างละเอียด (คล้าย nslookup)	dig google.com
nmap	สแกนพอร์ตหรือเครื่องในเครือข่าย	nmap 192.168.1.1