
Module 6

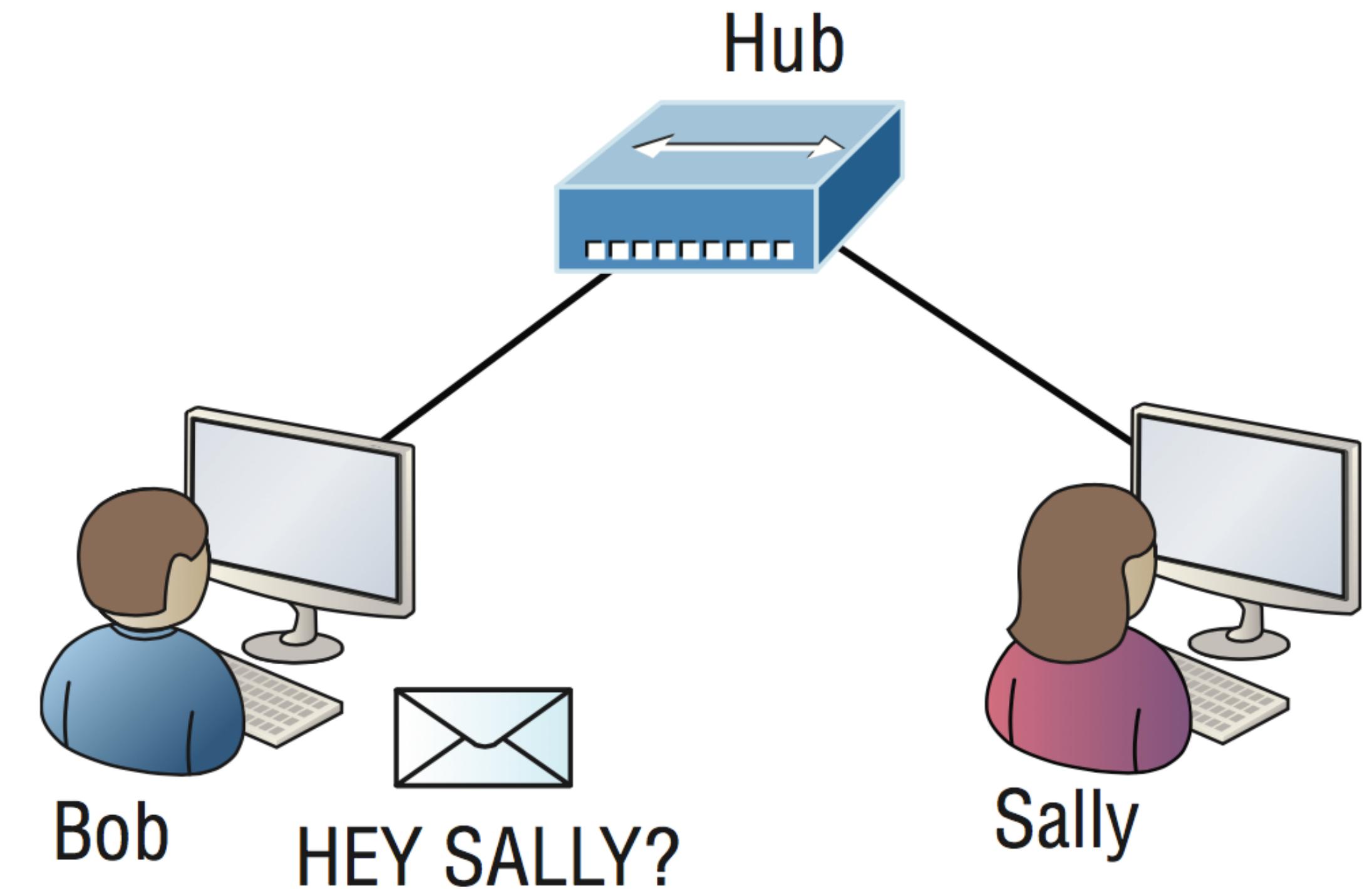
LAN Technology

Contents

- What is Security
- Threat
- Protection
- Email Security
- Cloud Security
- Software Security
- Secure Web Browsing
- Secure HTTP

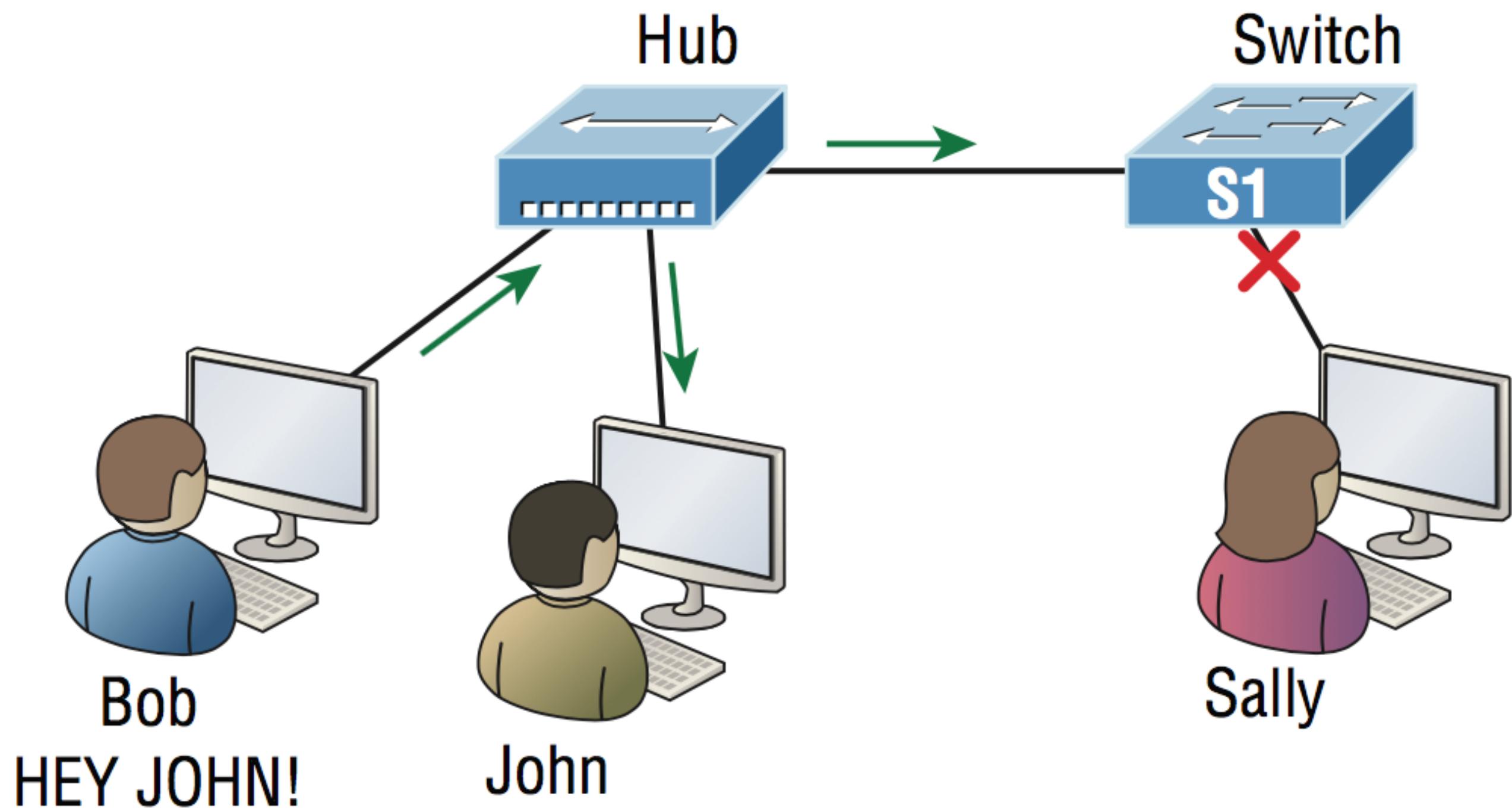
A very basic network

- Local Area Network via Hub
- Collision Domain



Network Segmentation

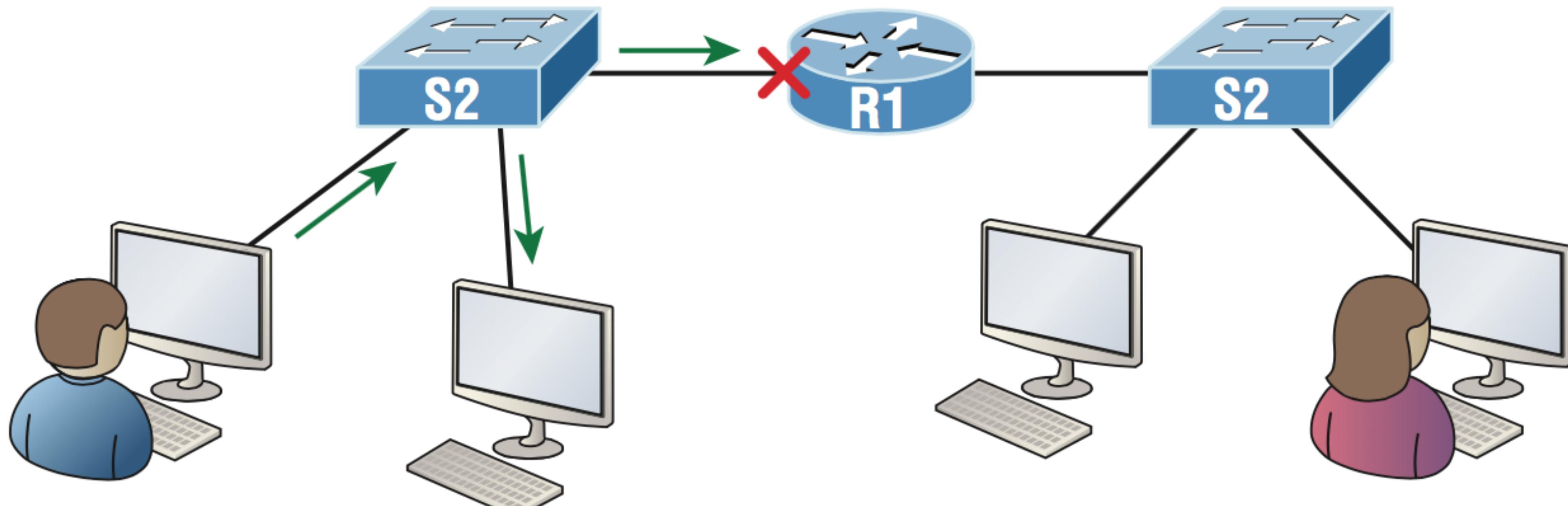
- Network Segmentation
 - Routers, Switches, Bridges



Network Segmentation

- Too many host in a collision or broadcast domain
- Broadcast storms
- Too much multicast traffic
- Low bandwidth
- Adding hubs for connectivity to the network
- ARP broadcast

Broadcast Domain

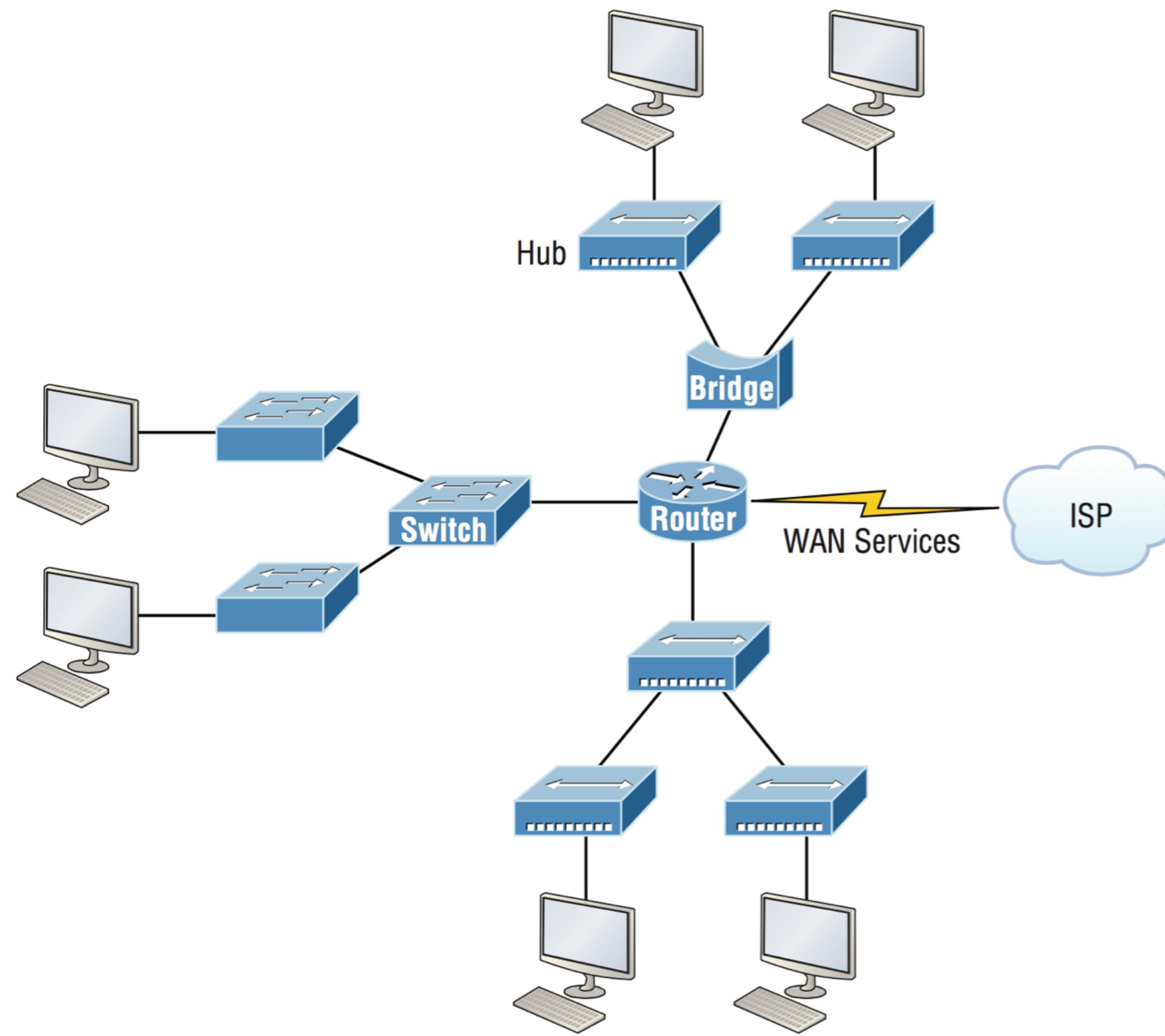


I LOVE SHOUTING!
... HEY EVERYONE!

Sure is nice and quiet here.

Inter-networking Devices

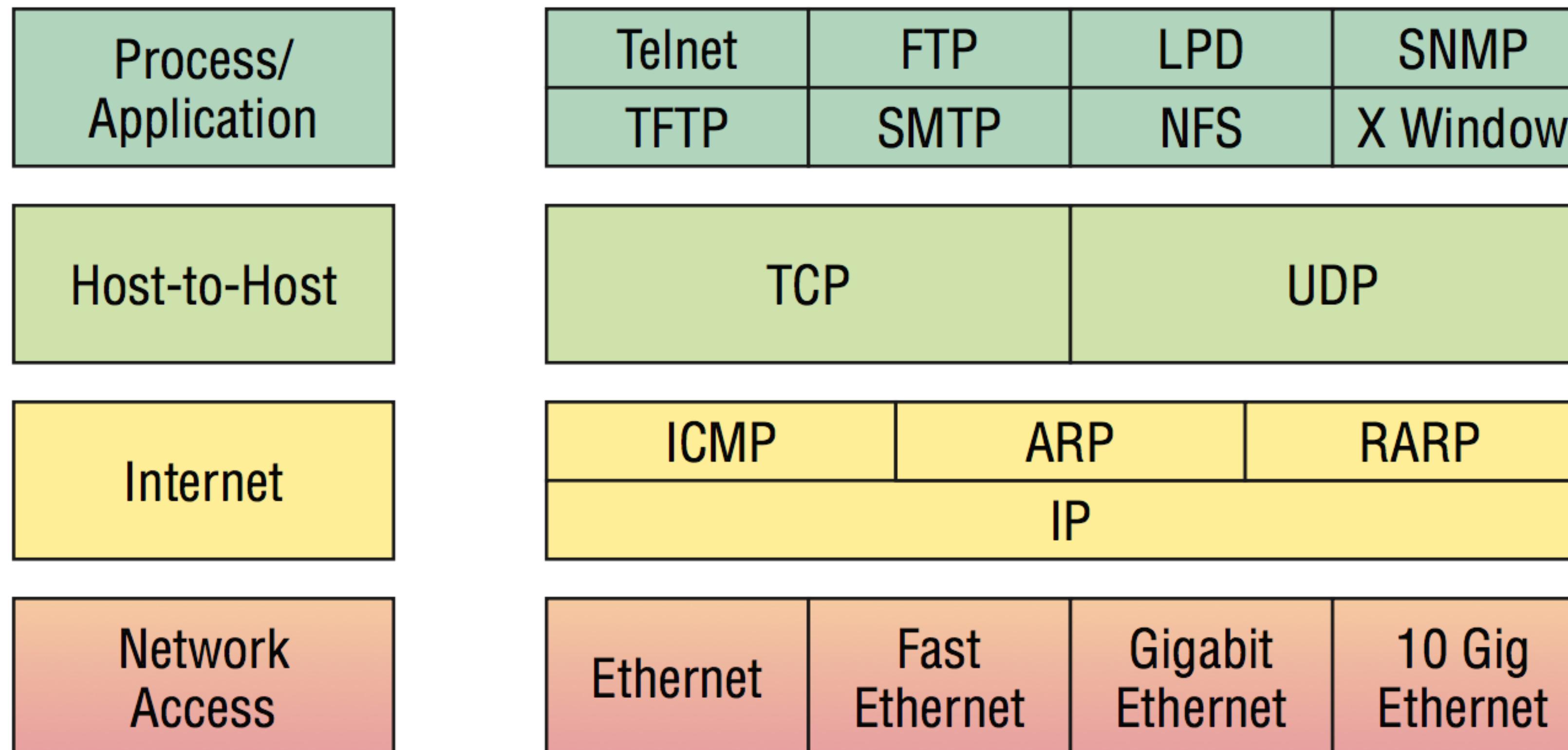
UbiN3\$
Ubiquitous Networked Embedded System



TCP/IP MODEL

PROTOCOL SUITE

DoD Model



TELNET

- **Telnet** is the chameleon of protocols—its specialty is terminal emulation.
 - It allows a user on a remote client machine, called the **Telnet client**, to access the resources of another machine, the Telnet server in order to access a command-line interface.
 - Telnet achieves this by pulling a fast one on the Telnet server and making the client machine appear as though it were a terminal directly attached to the local network.
 - This projection is actually a software image—a virtual terminal that can interact with the chosen remote host.
 - A drawback is that there are no encryption techniques

SECURE SHELL (SSH)

- **Secure Shell (SSH)** protocol

- sets up a secure session that's similar to Telnet over a standard TCP/IP connection and is employed for doing things like logging into systems, running programs on remote systems, and moving files from one system to another.
- And it does all of this while maintaining an encrypted connection.

FILE TRANSFER PROTOCOL (FTP) **UbIn3\$**

Ubiquitous Networked Embedded System

- **File Transfer Protocol (FTP)** actually lets us transfer files, and it can accomplish this between any two machines using it. But FTP isn't just a protocol; it's also a program.
- FTP is used by applications.
 - As a program, it's employed by users to perform file tasks by hand.
 - FTP also allows for access to both directories and files and can accomplish certain types of directory operations, such as relocating into different ones

FILE TRANSFER PROTOCOL (FTP)

- Users must then be subjected to an authentication login that's usually secured with passwords and usernames implemented by system administrators to restrict access.
- You can get around this somewhat by adopting the username **anonymous**, but you'll be limited in what you'll be able to access.

HTTP

- All those snappy websites comprising a graphics, text, links, ads and so on rely on the Hypertext Transfer Protocol (HTTP) to make it all possible.
- It's used to manage communications between web browsers and web servers and opens the right resource when you click a link, wherever that resource may actually reside.

HTTPS

- **Hypertext Transfer Protocol Secure (HTTPS)** is also known as Secure Hypertext Transfer Protocol.
 - It uses Secure Sockets Layer (SSL).
 - It's what your browser needs to fill out forms, sign in, authenticate, and encrypt an HTTP message when you do things online like make a reservation, access your bank, or buy something.

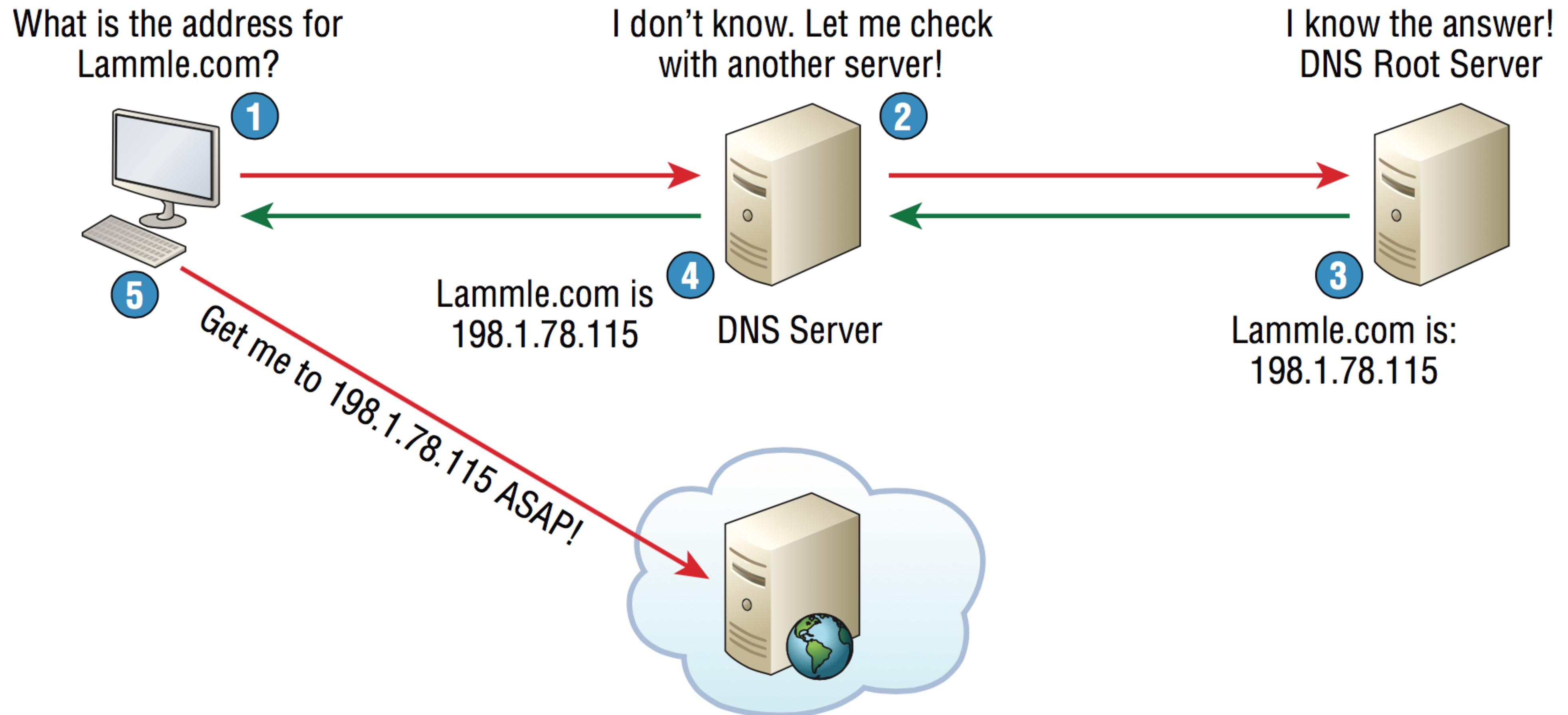
Network Time Protocol (NTP)

UbIn3\$
Ubiquitous Networked Embedded System

- Network is used to synchronize the clocks on our computers to one standard time source (typically, an atomic clock).
- **Network Time Protocol (NTP)** works by synchronizing devices to ensure that all computers on a given network agree on the time.
- This may sound pretty simple, but it's very important because so many of the transactions done today are time and date stamped.
- Network Monitoring System needs NTP

Domain Name System (DNS)

UbIn3\$
Ubiquitous Networked Embedded System



Dynamic Host Configuration Protocol **UbIn3\$**

Ubiquitous Networked Embedded System

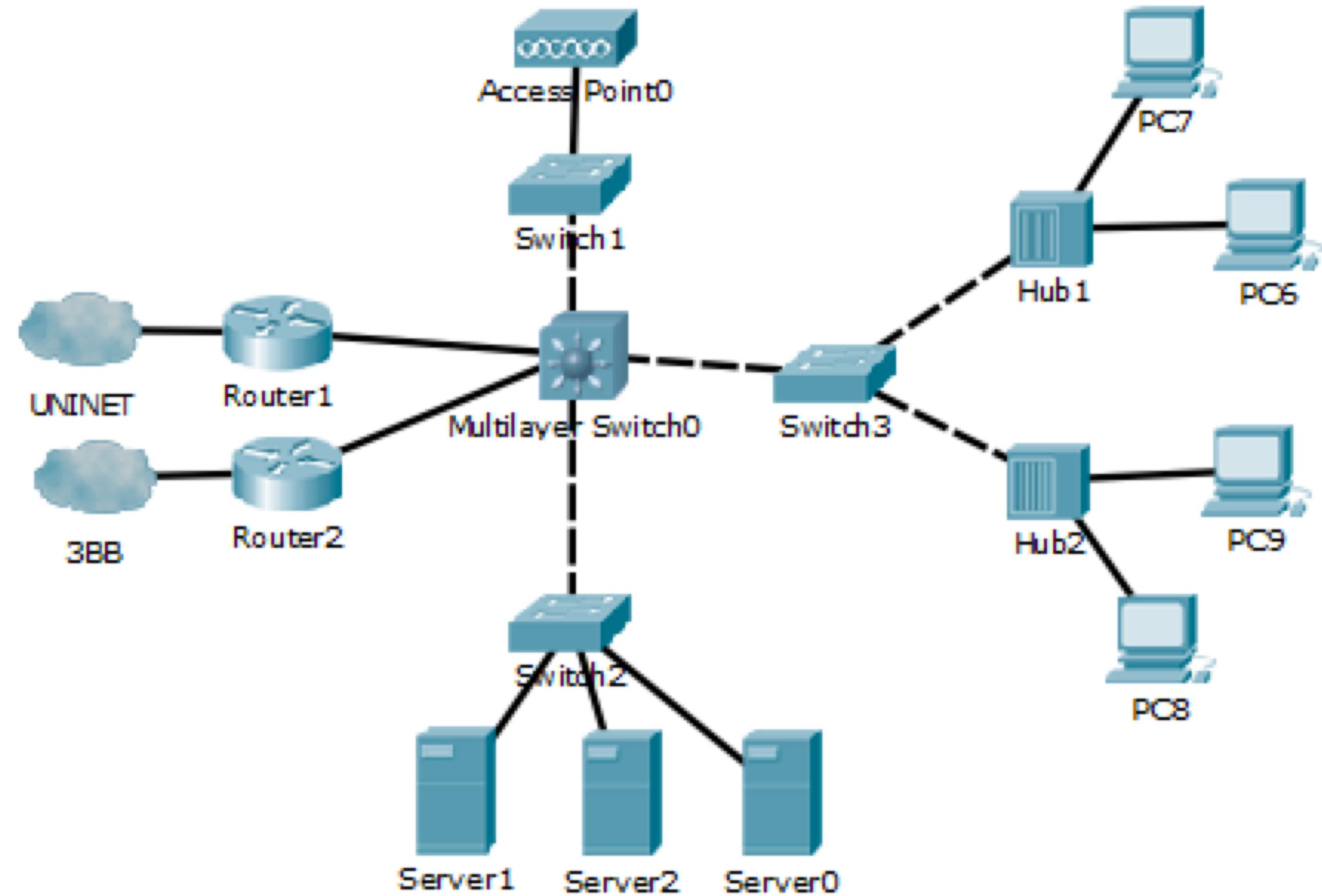
- **Dynamic Host Configuration Protocol (DHCP)** assigns IP addresses to hosts.
- It allows for easier administration and works well in small to very large network environments.
- Many types of hardware can be used as a DHCP server, including a Cisco router.
- DHCP server can provide:
 - IP address, Subnet mask, Domain name, Default gateway (routers), DNS server address

Local Area Network

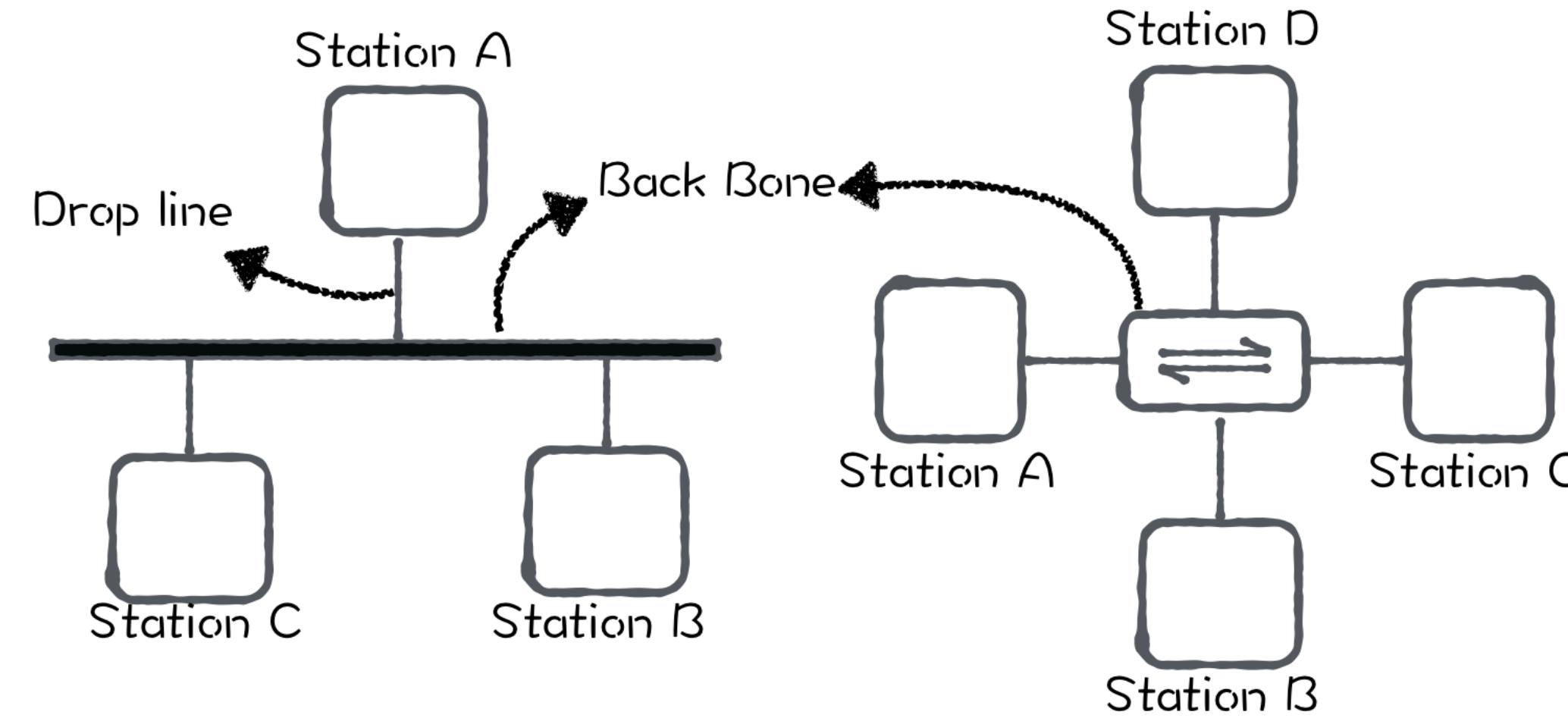
- **Local Area Network (LAN)** เป็นเครือข่ายที่เชื่อมโยงอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์ต่างๆ ไว้ด้วยกัน ภายในห้องถินเดียวกัน
 - อาจจะเชื่อมโยงภายในห้อง อาคาร ระหว่างอาคาร ซึ่งอยู่ในบริเวณใกล้เคียง
- นอกจากนี้อาจจะเป็นการเชื่อมต่อของอุปกรณ์ต่างๆ ที่อยู่ต่างพื้นที่ผ่านเครือข่ายโทรศัพท์สาธารณะ แต่เชื่อมโยงด้วยเทคโนโลยีบางอย่าง เช่น **Virtual Private Network** หรือ **VPN** ซึ่งเป็นผลในผู้ดูแลระบบสามารถตัดและจัดการระบบได้โดยบุคคลภายนอกองค์กรเดียวกัน
- ตัวอย่าง
 - การเชื่อมต่อเครือข่ายของมหาวิทยาลัยลักษณ์ มีเครือข่าย LAN หลักอยู่ที่ จังหวัดนครศรีธรรมราช นอกเหนือนี้ ยังมีเครือข่ายย่อยอีก 3 แห่ง ได้แก่ ภูเก็ต สุราษฎร์ธานี และ กรุงเทพฯ โดยเครือข่ายทั้งหมดนั้นเชื่อมต่อกันภายในตัวเครือข่าย LAN เดียวกัน ซึ่งจะเรียกเครือข่ายชั้นต้นว่า **Campus Network**

LAN

UbiN3\$
Ubiquitous Networked Embedded System

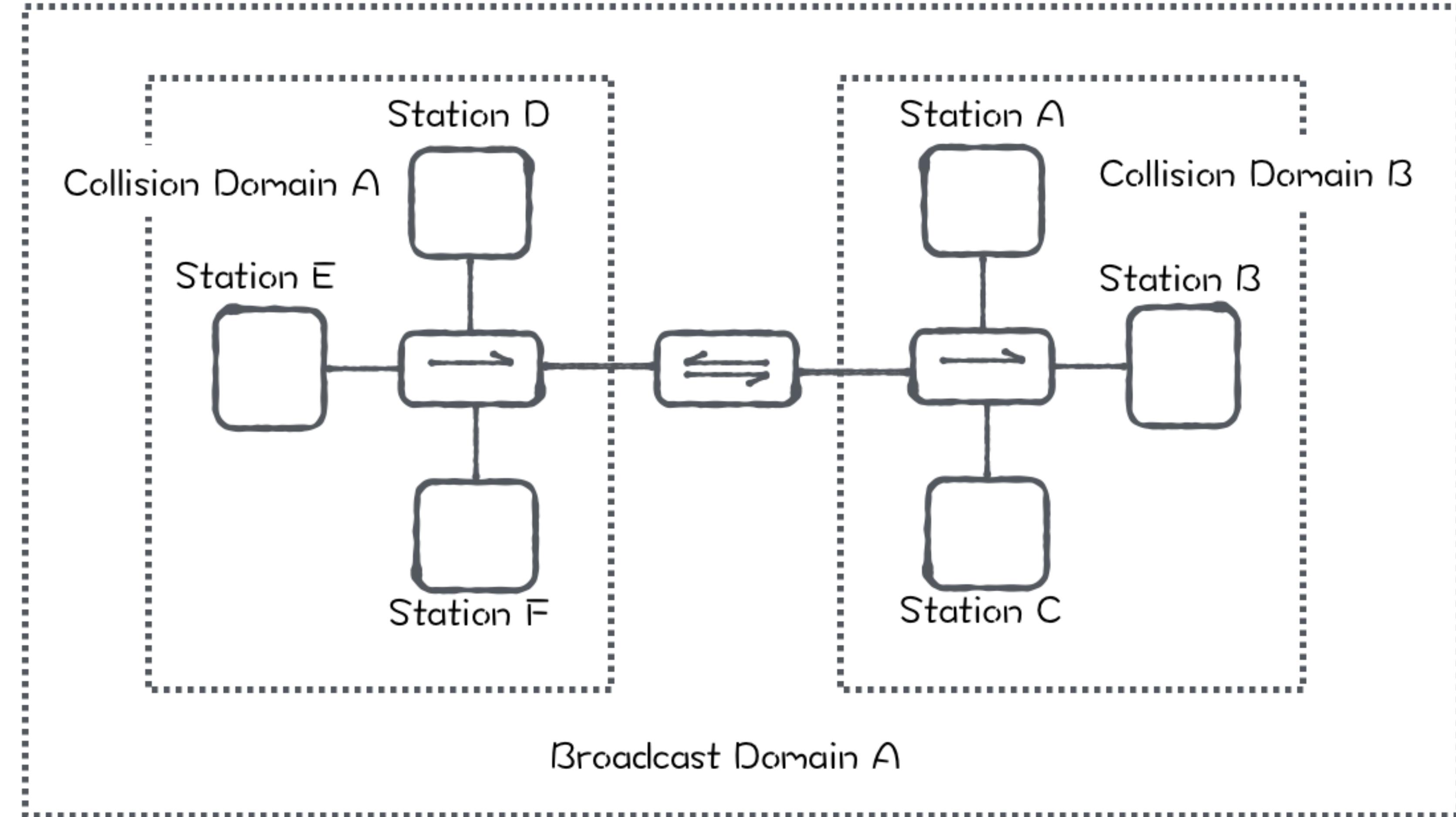


LAN Segment



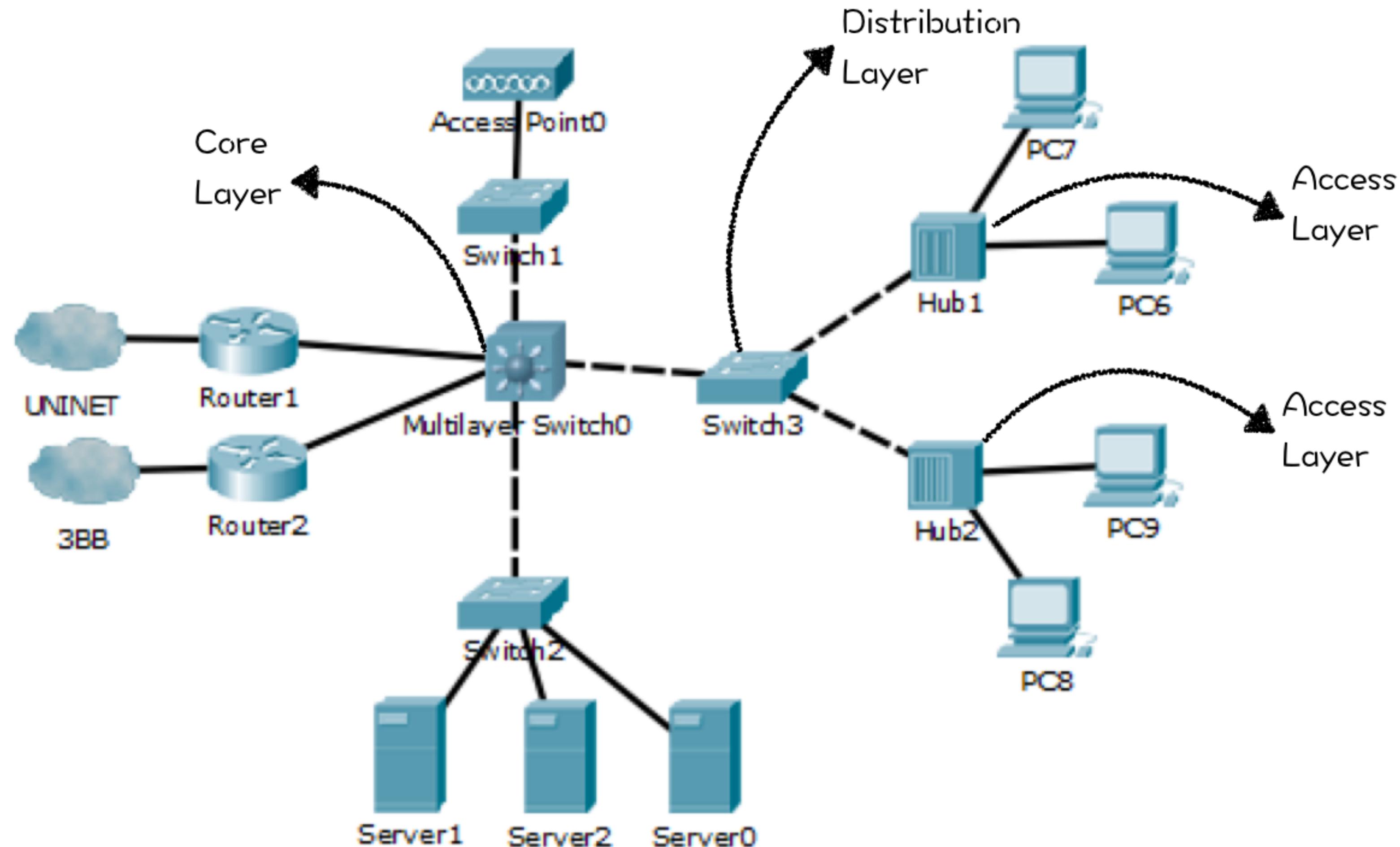
- LAN Segmentation หมายถึงการแบ่งเครือข่ายแลนออกเป็นส่วนๆ หรือเรียกว่า "เซกเมนต์ (Segment)" ใช้อุปกรณ์เครือข่ายต่างๆ
 - บริดจ์ (Bridge), สวิตซ์ (Switch) หรือ เรอะเตอร์ (Router)
- การจัดแบ่งเครือข่ายดังกล่าว มีผลต่อประเด็นของ Collision Domain และ Broadcast Domain

LAN Segment



Hierarchical Network Design

Ubiquitous Networked Embedded System



Hierarchical Network Design **UbIN3\$**

Ubiquitous Networked Embedded System

- **ชั้นการเข้าถึง (Access Layer)** เป็นชั้นที่อยู่ใกล้กับผู้ใช้มากที่สุด เป็นจุดที่นำเครื่องคอมพิวเตอร์ของผู้ใช้เข้าสู่ระบบเครือข่าย
- สำหรับ LAN และ Campus Network อุปกรณ์เครือข่ายที่ใช้งานในชั้นนี้คือ
 - สวิตซ์ชั้น 2 (L2-Switch) หรือ ฮับ (Hub) โดยจำนวนพอร์ตที่ใช้งาน ควรมีให้เท่ากันกับอุปกรณ์ของผู้ใช้
 - เชื่อมต่อกับอุปกรณ์เครือข่ายไร้สาย (Access Point)
- การเชื่อมต่อในกลุ่มนี้ จะมีพอร์ตอย่างน้อย 1 พอร์ต ใช้สำหรับเชื่อมต่อกับ Distribution Switch หรือ Core Switch ซึ่งเรียกพอร์ตนั้นว่า Up Link

Hierarchical Network Design **UbIn3\$**

Ubiquitous Networked Embedded System

- **ชั้นกระจาย (Distribution Layer)** เป็นชั้นที่รวม Access Switch ต่างๆ เข้าด้วยกัน เพื่อส่งผ่านไปยังชั้นแกน
- อุปกรณ์ในกลุ่มนี้ควรเป็นอุปกรณ์ที่มีประสิทธิภาพ มีฟังก์ชันเสริมการทำงานต่างๆ
 - InterVLAN, Routing, Access Control List (ACL) รวมถึง QoS เป็นต้น
- **ชั้นแกน (Core Layer)** เป็นหัวใจหลักของเครือข่าย ซึ่งมีหน้าที่เชื่อมต่อ Distribution Switch ต่างๆ เข้าด้วยกัน
 - อุปกรณ์ในชั้นนี้ ควรมีประสิทธิภาพสูง สามารถรับส่งข้อมูลได้รวดเร็ว

Hierarchical Network Design UbiN3\$

Ubiquitous Networked Embedded System

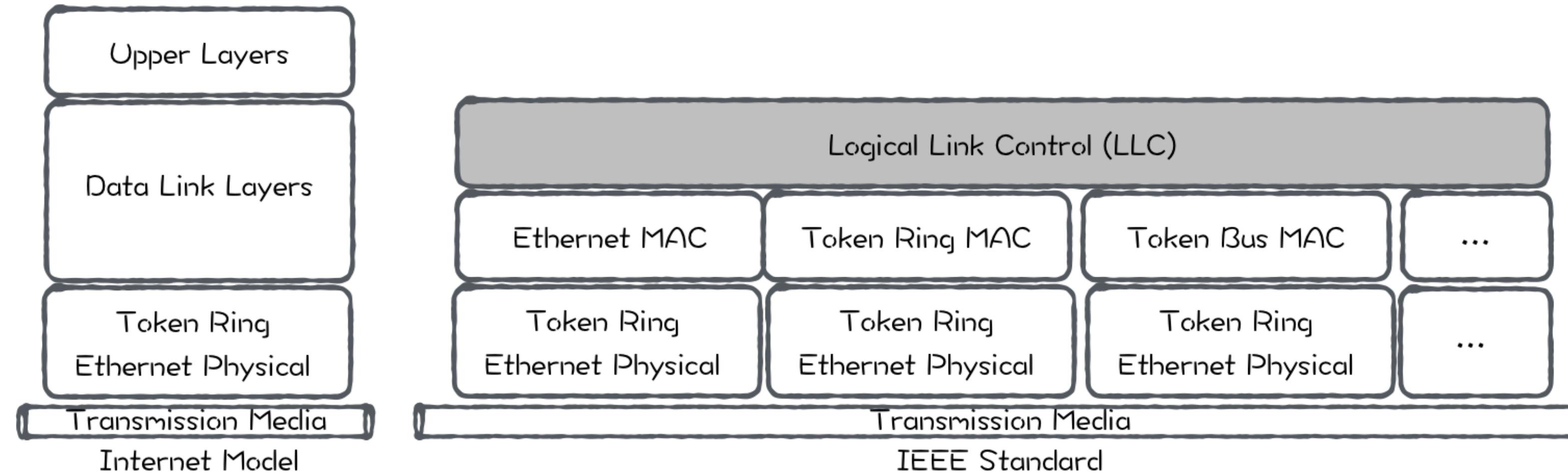
- ในทางปฏิบัติ องค์กรได้รวม ชั้นกระจาย (Distribution Layer) และ ชั้นแกน (Core Layer) ไว้ด้วยกัน
- เนื่องจากองค์กรมีขนาดเล็ก หรือมีข้อจำกัดของงบประมาณ
- สำหรับองค์กรที่มีขนาดใหญ่ อาจจะมีการใช้งานเราเตอร์เป็น Core Layer เพื่อจัดการเครือข่าย ให้มีประสิทธิภาพสูงสุด ซึ่งสิ่งที่ตามมาคือ งบประมาณและความรู้ความเข้าใจของผู้ดูแลระบบ จำเป็นต้องมีพร้อมเช่นกัน

Ethernet Technology

Ethernet

- อีเธอร์เน็ต (Ethernet) เป็นตระกูลของเทคโนโลยีเครือข่ายที่ใช้สำหรับการสื่อสารผ่านระบบเครือข่ายแลน โดยเริ่มต้นในยุค 80
- การอ้างอิงหมายเลขอารบิกของมาตรฐานนั้นอิงตามหน่วยงาน IEEE ซึ่งกำหนดหมายเลขเป็น IEEE 802 ซึ่งเกี่ยวข้องกับ LAN และ MAN
- นอกจากนี้ IEEE 802 นั้นยังกำหนดวิธีการขนส่งข้อมูลที่ขนาดของแพ็คเกจมีความแตกต่างกัน บริการและโปรโตคอลที่ระบุใน IEEE 802 นั้นมี 2 ชั้น
 - ชั้นภาษาภาพ
 - ชั้นเชื่อมโยง
- นอกจากนี้ IEEE 802 นั้นได้แบ่งชั้นเชื่อมโยงออกเป็นชั้นย่อยได้แก่
 - Logical Link Control หรือ LLC
 - Media Access Control หรือ MAC

Ethernet



- มาตรฐานในตระกูล IEEE 802 นั้นได้รับการออกแบบและพัฒนาโดย IEEE 802 LAN/MAN Standard Committee (LMSC)
- มาตรฐานต่างๆเหล่านี้ถูกพัฒนาและใช้งานในเทคโนโลยีต่างๆ ได้แก่ Ethernet Family, Token Ring, Wireless LAN, Bridging และ Virtual Bridged LAN

IEEE 802 Frame

- การสื่อสารข้อมูลผ่านอีเธอร์เน็ตนั้น ข้อมูลจะถูกแบ่งออกเป็นส่วนย่อยซึ่งเรียกว่าเฟรม (Frame) โดยแต่ละเฟรมนั้นประกอบด้วยส่วนต่างๆ ได้แก่ เลขที่อยู่ต้นทาง เลขที่อยู่ปลายทาง ส่วนของข้อมูล และกระบวนการตรวจสอบความถูกต้อง

IEEE 802 Frame

- **เลขที่อยู่ (Address)** ใช้สำหรับการกำหนดที่อยู่ของฝ่ายส่งและฝ่ายรับ ซึ่งการกำหนดเลขที่อยู่นี้เป็นเลขที่อยู่ของ NIC จะไม่ซ้ำกัน
- เลขที่อยู่นี้เรียกว่า MAC Address หรือ Physical Address ซึ่งมีขนาด 48 บิต โดยเขียนในรูปแบบของเลขฐาน 16 จำนวน 6 ใบต์ต่อเนื่องกันโดยคั่นแต่ละใบต์ด้วย ":"

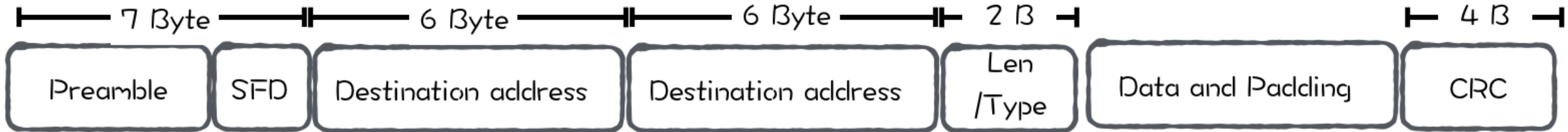
↳ Manufacturing ID ↳

06 : 01 : 02 : 01 : 2C : 4B

6 Bytes = 12 hex digits = 48 bits

IEEE 802 Frame

UbIn3\$
Ubiquitous Networked Embedded System

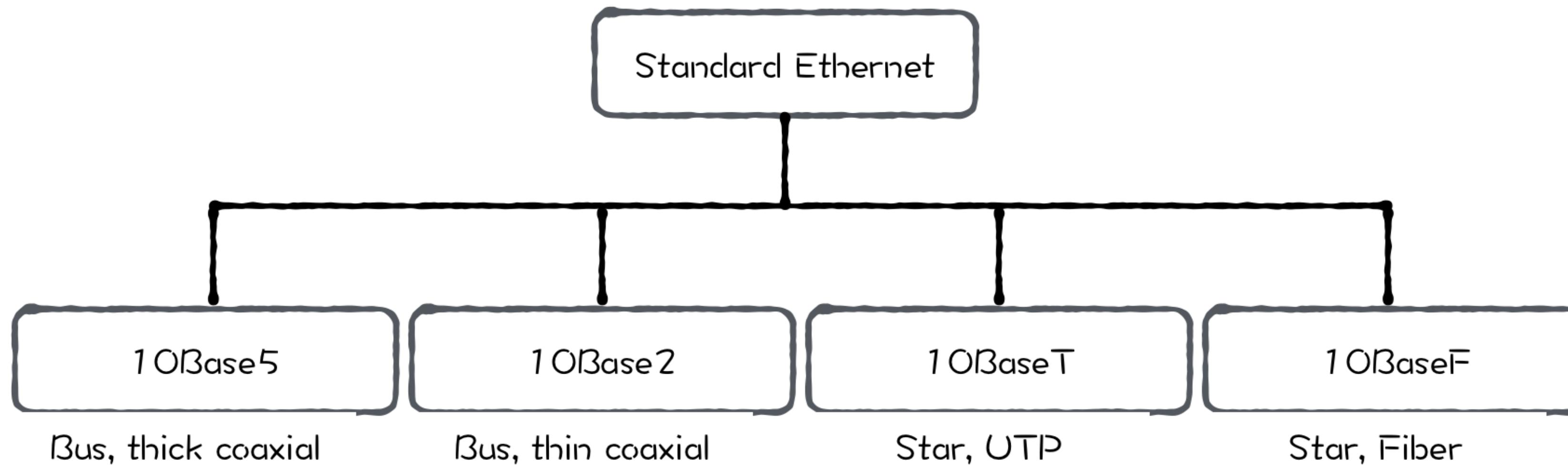


Preamble: 56bit of alternating 1s and 0s

SFD: Start frame delimiter (10101011)

- **Destination/Source Address** คือ MAC Address
- **ความยาว/ชนิดของข้อมูล** ขึ้นอยู่กับว่าการสื่อสารในชั้นนี้เป็นการสื่อสารโดยใช้เทคโนโลยีรุ่นใด หากเป็นเทคโนโลยีของ Ethernet II นั้นข้อมูลส่วนนี้คือ ความยาวของข้อมูล หากเป็นเทคโนโลยีแลนอื่นๆ กำหนดเป็นชนิดของข้อมูลที่อยู่ในส่วนของ Data
- **กระบวนการตรวจสอบความถูกต้อง** กำหนดโดยการใช้ Cyclic Redundant Check เพื่อสร้างข้อมูลพิเศษเพื่อใช้ในการตรวจสอบว่า ข้อมูลที่ส่งมานั้นแตกต่างจากฝ่ายส่งหรือไม่

Evolution of Ethernet



- การพัฒนาโปรโตคอลของอีเธอร์เน็ตมีวิวัฒนาการของมาตรฐานโดยขึ้นอยู่กับความต้องการของความเร็ว อุปกรณ์ลีอสาร
 - อีเธอร์เน็ตแบบมาตรฐาน (Standard Ethernet)
 - พาสต์อีเธอร์เน็ต (Fast Ethernet),
 - กิกะบิตอีเธอร์เน็ต (Gigabit Ethernet)

Standard Symbol

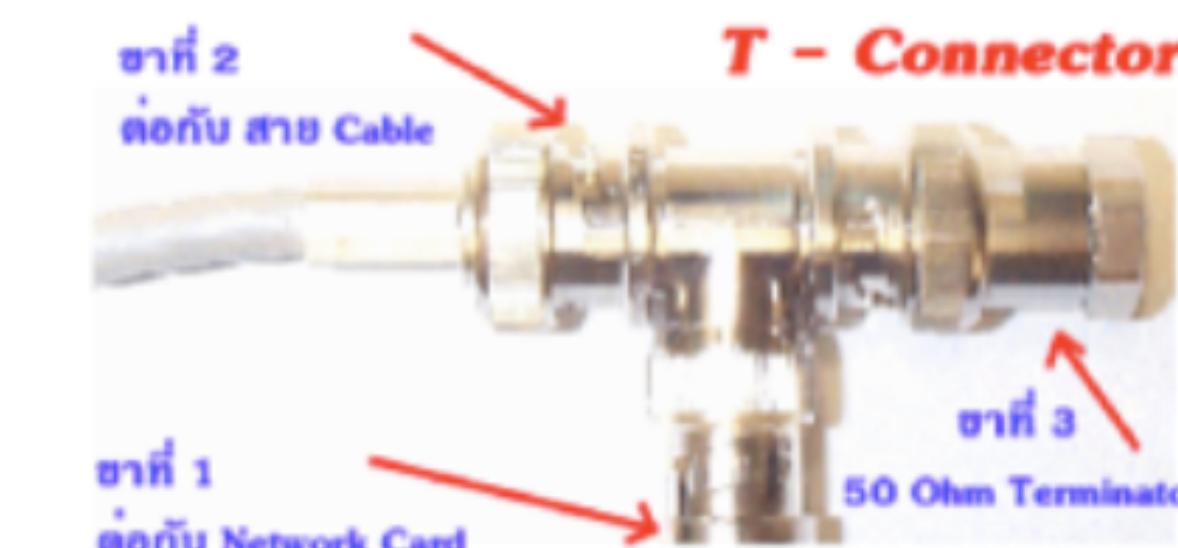
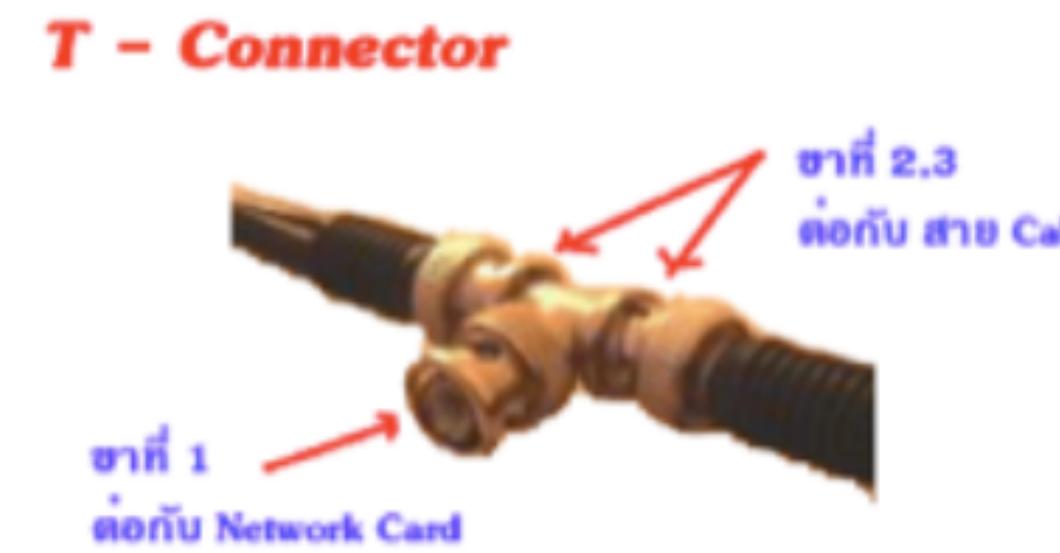
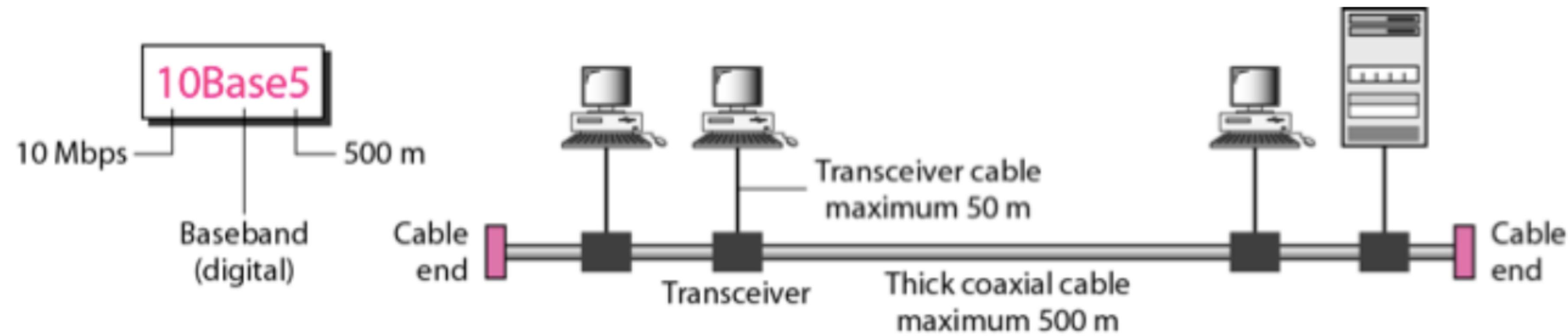
- การแทนสัญลักษณ์ของมาตรฐานนั้น มีองค์ประกอบทั้งหมด 3 ส่วนได้แก่ ความเร็ว รูปแบบการส่งข้อมูล และชนิดของสื่อ เช่น **10Base2** สามารถตีความได้ดังนี้
 - 10 หมายถึงความเร็วในการส่งข้อมูล มีหน่วยเป็น Mbps ซึ่งอาจจะมีค่าเป็น 10, 100 หรือ 1000 เป็นต้น
 - Base หมายถึงรูปแบบการเชื่อมต่อเครือข่ายซึ่งกำหนดค่าเป็น Base และ Broad
 - Base หมายถึงการเชื่อมต่อเครือข่ายแบบ Baseband เป็นการนิยามวิธีการสื่อสารแบบดิจิทัล ที่มีผู้ส่งเพียงเครื่องเดียวเท่านั้นที่สามารถใช้ช่องทางสื่อสารได้
 - Broad แทนการสื่อสาร BroadBand ซึ่งเป็นการสื่อสารแบบดิจิทัลเช่นกัน แต่ใช้สำหรับการสื่อสารแบบ Point-to-Point โดยใช้สำหรับการสื่อสารภายนอกองค์กร เช่นจากผู้ใช้บริการและองค์กรที่ใช้งานอินเตอร์เน็ตนั่นๆ
 - 2 เป็นสัญลักษณ์ที่ใช้แทนชนิดของสื่อที่ใช้สำหรับการสื่อสาร ได้แก่ 2 แทน Thin Coaxial, 5 แทน Thick Coaxial, T แทน UTP หรือ FX แทน Fiber optic เป็นต้น

Standard Ethernet

UbIn3\$
Ubiquitous Networked Embedded System

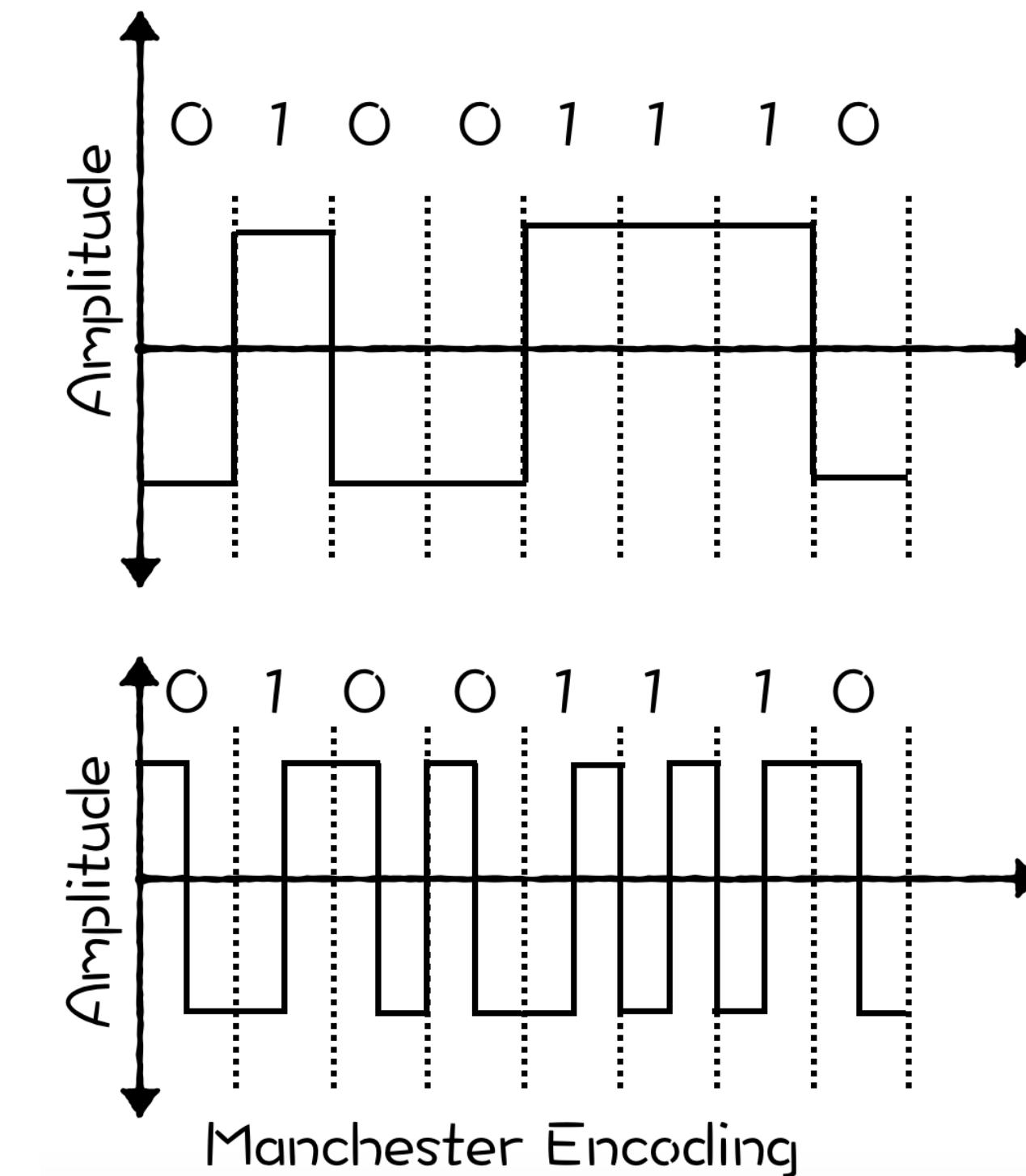
- **Standard Ethernet** เป็นมาตรฐานการเชื่อมต่อของอีเธอร์เน็ตในยุคแรกๆ เชื่อมต่อด้วยมาตรฐาน
- 10Base5/ 10Base2 เป็นการสื่อสารอีเธอร์เน็ตบนโทปโอลิย์แบบบัส โดยใช้สายโคคเอยล์แบบหนา หรือแบบบาง กำหนดความยาวของสายไม่เกิน 500 เมตร เช้ารหัสสัญญาณแบบ Manchester

Standard Ethernet



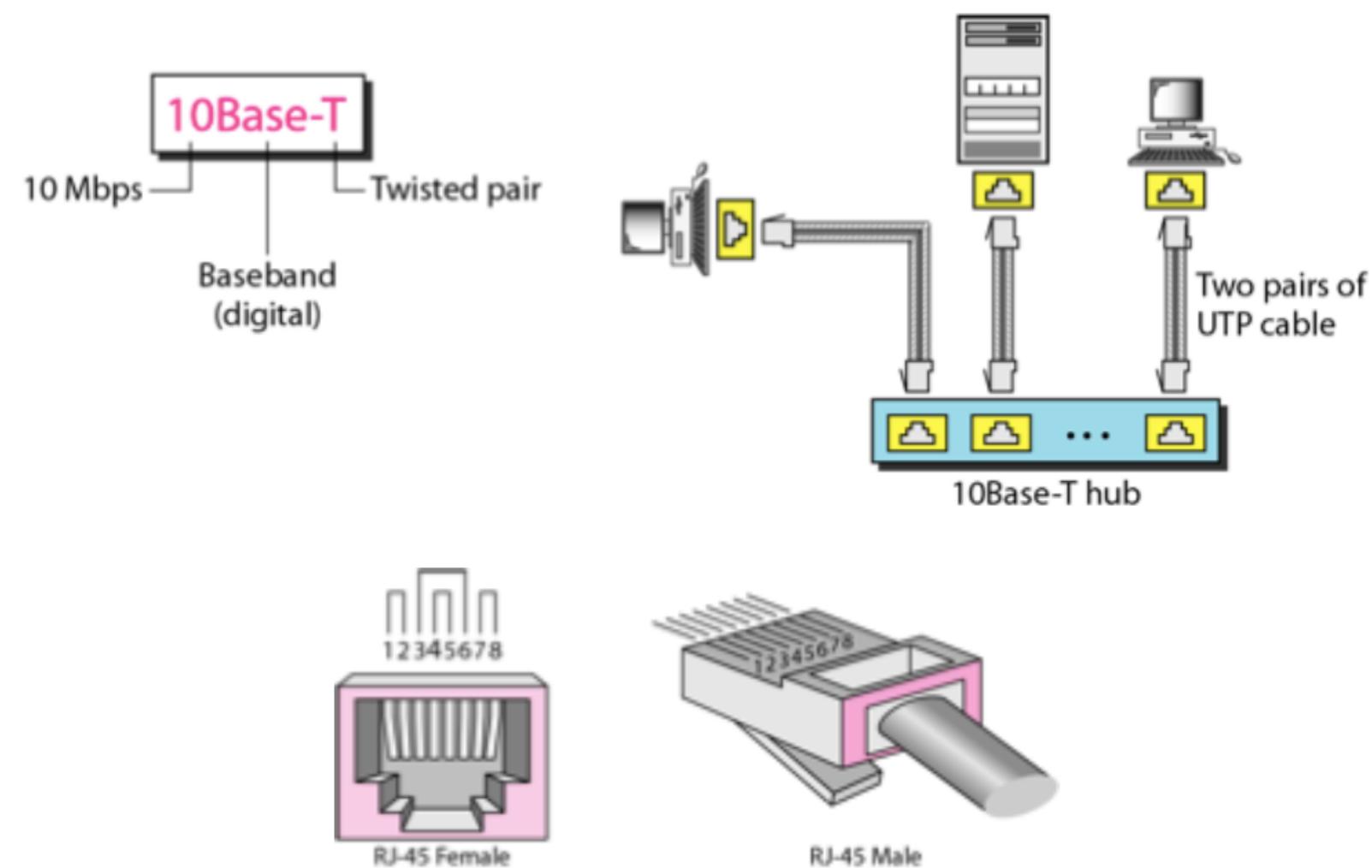
Manchester Encoding

- การเข้ารหัสสัญญาณเป็นการแก็บัญหา ในการนี้ที่สัญญาณที่ส่งผ่านลื่อนั้น เป็น 0 หรือ 1 ต่อเนื่องเป็นเวลานาน ซึ่งความถี่ของสัญญาณเป็น 0 ส่งผลให้ทางฝ่ายรับไม่สามารถประเมินได้ว่า ค่าที่ส่ง ในขณะนั้นคือค่าใด การเข้ารหัสแบบ Manchester
- การเข้ารหัสแบบ Manchester เป็นการเข้ารหัสแบบมีขั้ว (Polar Encoding) ซึ่งมีการเปลี่ยนสัญญาณหรือการกลับเฟสของคลื่นกางบิต เรียกวิธีการเข้ารหัสแบบนี้ว่า Biphase Encoding การเข้ารหัสแบบ Biphase มี 2 เทคนิคคือ
 - Manchester และ Differential Manchester
 - การเข้ารหัสแบบ Manchester นั้นมีหลักการคิดคือ หากข้อมูลเป็น 1 แล้ว จะเปลี่ยนแรงดันไฟจากลบเป็นบวกซึ่งจะเปลี่ยนกางบิต ในการกลับกันหากข้อมูลเป็น 0 จะเปลี่ยนแรงดันไฟจากบวกไปต่ำ โดยจะเปลี่ยนกางบิตเช่นกัน



Standard Ethernet

- 10BaseT/10BaseF เป็นการสื่อสารอีเรอร์เน็ตโทปโลยีแบบดาว โดยอุปกรณ์ต่อสาย UTP มีจำนวน 2 เส้นเชื่อมต่อกับชั้บ (Hub) ความยาวของสายไม่เกิน 100 เมตร เข้ารหัสสัญญาณแบบ Manchester แต่ถ้าใช้สายใยแก้วนำแสง ความยาวสายสามารถเพิ่มขึ้น 200 เมตร และเชื่อมต่อผ่านชั้บ เช่นกัน



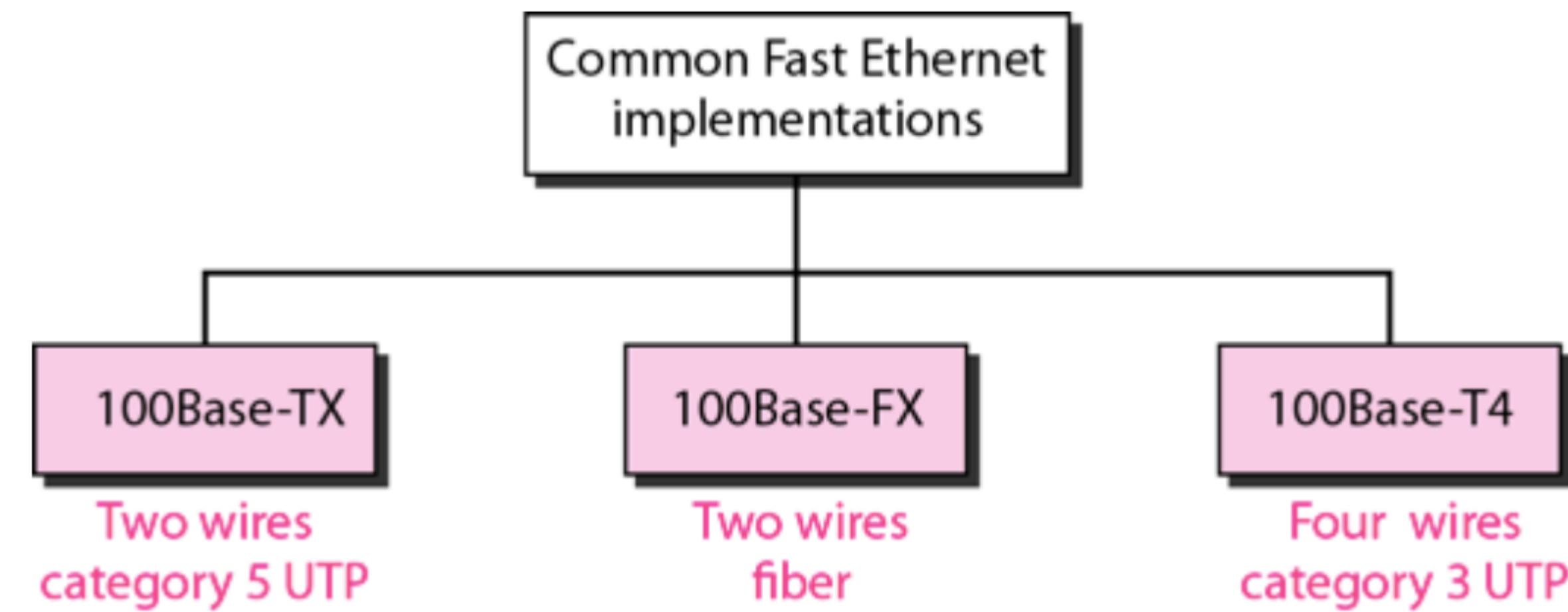
Fast Ethernet

- **Fast Ethernet** เป็นการออกแบบมาตรฐานของอีเรอร์เน็ตสำหรับการสื่อสารผ่านใยแก้วนำแสง โดยทาง IEEE เรียกมาตรฐานนี้ว่า IEEE 802.3b โดยที่มาตรฐานนี้ยังสามารถเชื่อมต่อกับ Standard Ethernet ได้เช่นเดิม
- กำหนดเลขที่อยู่แบบ 48 บิต รูปแบบของเฟรมและความยาวของเฟรมขึ้นตั้งแต่ 64 บิต กัน
- แต่ความเร็วของการสื่อสารปรับเพิ่มขึ้นเป็น 100 Mbps

Fast Ethernet

- การออกแบบโปรโตคอลชั้น MAC Sublayer แตกต่างกัน โดยที่ยกเลิกการเชื่อมต่อแบบบัสโดยยังคงใช้งานโทโพโลยีแบบดาวไว้เช่นเดิม
 - การเข้าใช้ของการสื่อสารเป็นแบบ Half Duplex โดยใช้เทคนิค CSMA/CS
 - การเชื่อมต่อของโหนดรองรับทั้งแบบ Point-to-Point หากโหนดสองตัวเชื่อมต่อผ่านสายโดยตรง
 - ถ้าจำนวนของโหนดมากกว่า สองตัวแล้วการเชื่อมต่อเป็นแบบดาว โดยเชื่อมผ่าน สวิตซ์หรือฮับ
- มาตรฐานของ Fast Ethernet
 - 100Base-TX, 100Base-FX, และ 100Base-T4

Fast Ethernet

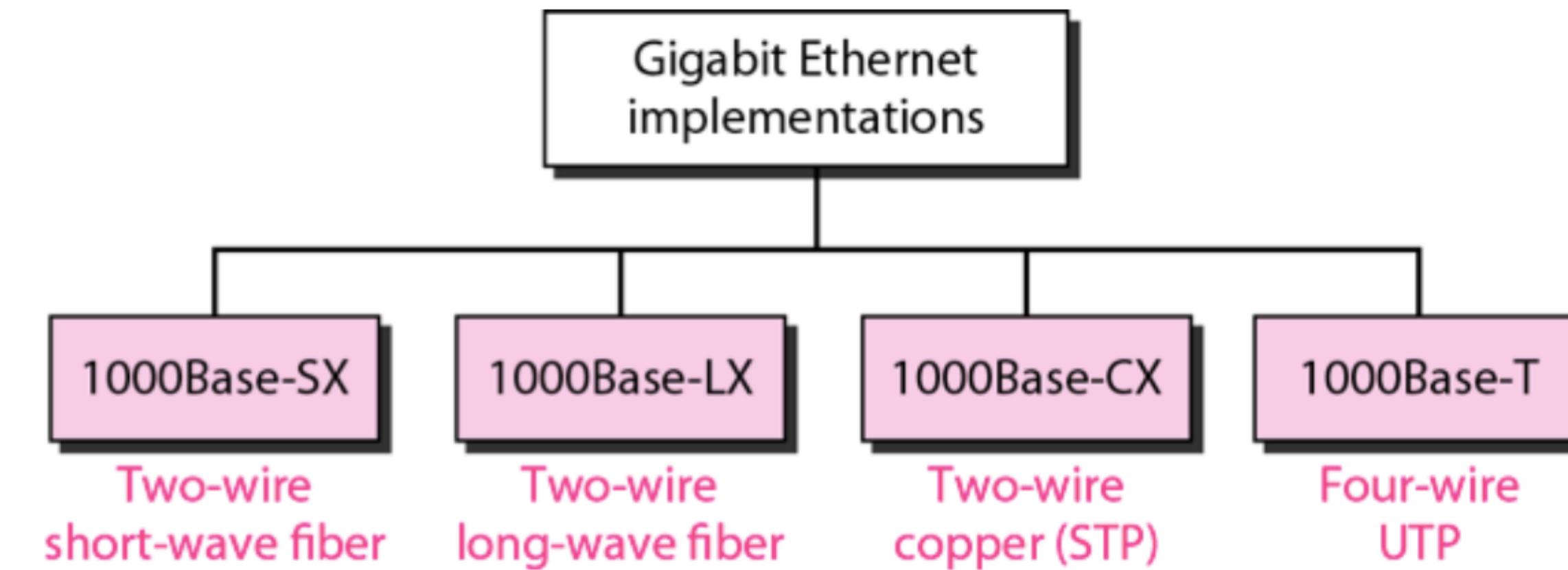


Characteristics	100Base-TX	100Base-FX	100Base-T4
Media	Cat 5 UTP or STP	Fiber	Cat 4 UTP
Number of wires	2	2	4
Maximum length	100 m	100 m	100 m
Block encoding	4B/5B	4B/5B	
Line encoding	MLT-3	NRZ-I	8B/6T

Gigabit Ethernet

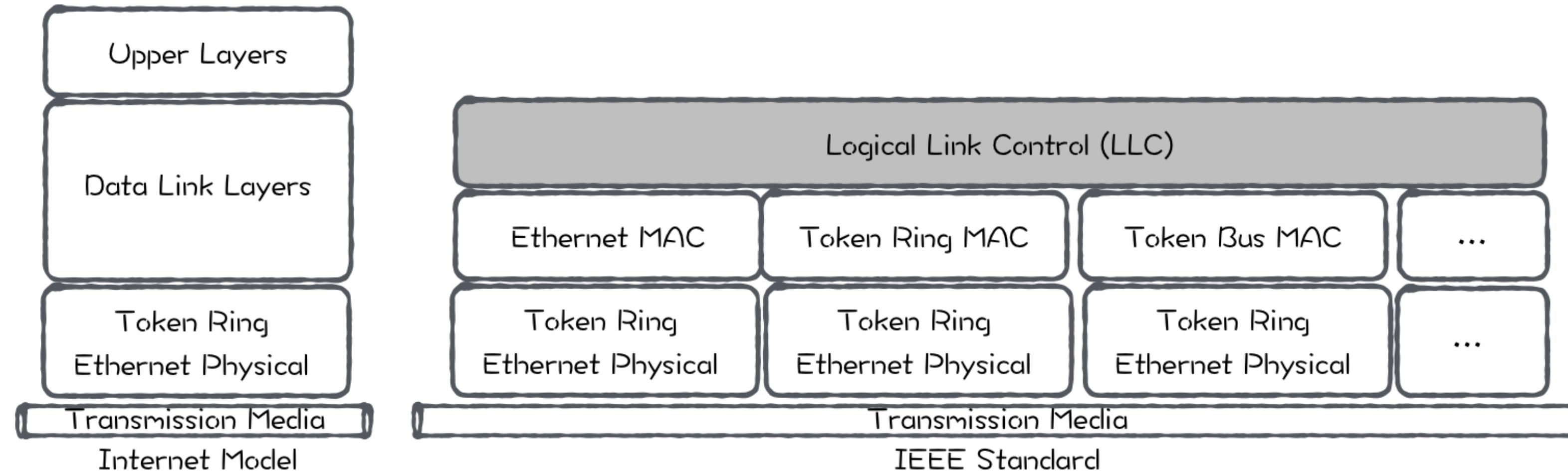
- **Gigabit Ethernet/10 Gigabit Ethernet** เป็นการพัฒนามาตรฐานของการสื่อสารข้อมูลอิเล็กทรอนิกส์ที่เพิ่มความเร็วในการสื่อสารในเครือข่าย Ethernet สามารถกำหนดความเร็วได้สูงถึง 1 Gbps และ 10 Gbps
- ปรับปรุงส่วนของ PHY Sublayer สื่อกลางที่ใช้เป็นสายแก้วนำแสง STP หรือ Cat-5 UTP
- การใช้ในแก้วนำแสงกำหนดระยะห่างของอุปกรณ์ไม่เกิน 5 กม แต่ถ้าใช้ Cat-5 UTP ระยะทางไม่เกิน 100 เมตร
- ในการนี้ที่ต้องการความเร็วของสายถึง 10 Gbps นั้นต้องใช้สายใยแก้วนำแสงเป็นสื่อกลางในการเชื่อมต่อ
- หากเชื่อมต่อแบบ Multimode นั้น สายสามารถขยายสูงสุดถึง 300 เมตร แต่ถ้าเป็นแบบ Single mode นั้น สายใยแก้วนำแสงสามารถขยายได้ถึง 40 กม

Gigabit Ethernet



<i>Characteristics</i>	<i>1000Base-SX</i>	<i>1000Base-LX</i>	<i>1000Base-CX</i>	<i>1000Base-T</i>
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

ข้อสังเกต



- การเปลี่ยนมาตรฐานของอีเธอร์เน็ต
 - การเปลี่ยนแปลงมาตรฐานนั้นเกิดขึ้น ในชั้น PHY Sublayer
 - การเปลี่ยนแปลงลีโอเพิ่มความเร็ว ในการส่งข้อมูล
 - การกำหนดเลขที่อยู่ รูปแบบของเฟรม หรือความยาวของแพ็คเกตนั้นยังคงเท่าเดิม
 - เพื่อ ให้มาตรฐานทั้งเก่าและใหม่ยังสามารถ ใช้งานร่วมกันได้

Switch

- ฮับ
- เชื่อมผ่านสาย UTP ซึ่งเชื่อมต่อช่องทางสื่อสารเดียวกัน หรือเรียกว่า Collision Domain
- หากโหนดใดๆ อย่างน้อยสองโหนดส่งข้อมูลพร้อมกัน ข้อมูลทั้งสองฝั่งจะชนกัน
- ทำให้เครื่องทั้งสองถอยไปตั้งหลัก นับถอยหลังแล้วส่งใหม่ เพื่อเลี่ยงการชนกันอีกครั้ง
- การใช้งานแบบดีวิดร์เป็นการใช้ร่วมกัน
 - หากเครื่องคอมพิวเตอร์ 10 เครื่องเชื่อมต่อเครือข่าย 100 Mbps และ เครื่องคอมแต่ละตัว จะส่งข้อมูลได้สูงสุด ไม่เกิน 10 Mbps

Switch

- อุปกรณ์พื้นฐานของการสื่อสารข้อมูลคือ บริดจ์
 - ในปัจจุบันอุปกรณ์ดังกล่าวไม่มีการใช้งานแล้ว
 - มีอุปกรณ์อื่นซึ่งมีหลักการทำงานเดียวกันเข้ามาแทน
 - สวิตช์ซึ่งทำงานในชั้นที่ 2 ของ OSI Model เนื่องจากการส่งต่อเพรอมนั้นพิจารณาจาก MAC Address

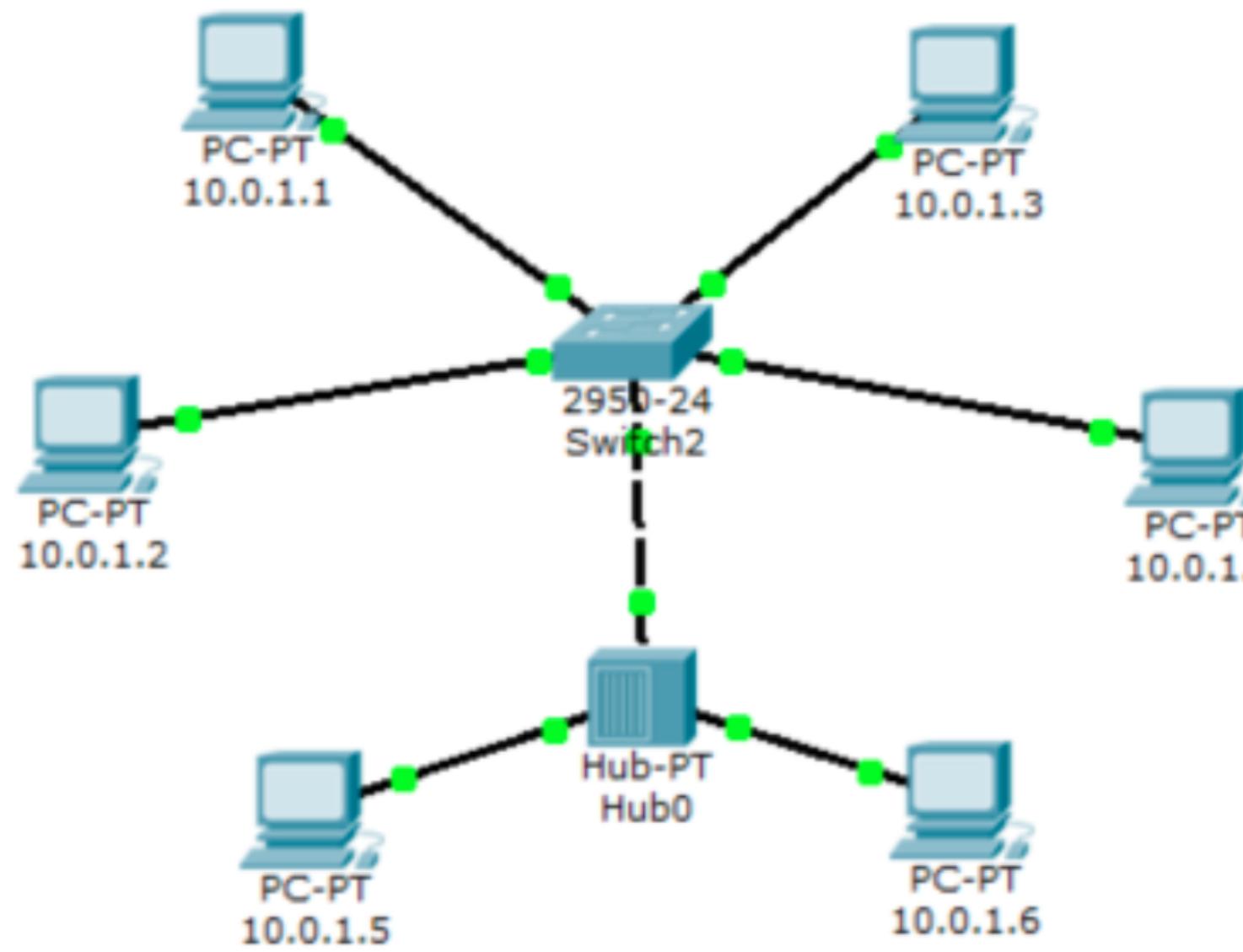
Switch

- ในการนี้ของสวิทซ์และบริดจ์นั้น พอร์ตแต่ละพอร์ตนั้นถือว่าต่าง Collision Domain กัน
 - การสื่อสารข้อมูลไม่ต้องใช้ร่วมกันกับใคร
 - หากโหนดต้องการส่งข้อมูลแล้ว เมื่อข้อมูลถูกส่งเข้าพอร์ต
 - สวิตซ์จะตรวจสอบหมายเลข MAC address ที่อยู่ในตาราง MAC Address หรือไม่
 - หากมี MAC Address ดังกล่าวเชื่อมต่อที่พอร์ตหมายเลขใดๆ ข้อมูลจะถูกส่งโดยตรงไปยังพอร์ตนั้นๆ
 - แต่ถ้าไม่มี MAC Address นั้นอยู่แล้ว ข้อมูลจะส่งผ่านไปยังทุกๆ พอร์ต เช่นเดียวกับ อับ
 - แต่การส่งข้อมูลในรอบต่อไป สามารถส่งต่อผ่านอับได้โดยที่ไม่ต้องตรวจสอบ MAC Address อีกครั้ง

MAC Address Learning

- ขั้นตอนการพิจารณาของสวิตช์จะพิจารณาจากหมายเลข MAC Address ที่เชื่อมต่อกับพอร์ตนั้นๆ แต่ข้อมูลของ MAC Address นั้นยังไม่มีการจัดเก็บในตอนต้น
- แต่จะทยอยเพิ่มเข้าไปในตารางจักระทั้งครบทุกพอร์ต
- โดยข้อมูลต่างๆ เหล่านี้นําไปใช้ในการเชื่อมต่อสวิตช์ครั้งแรกของอุปกรณ์ปลายทาง
- กระบวนการสร้างฐานข้อมูลของ MAC Address นี้เรียกว่า การเรียนรู้แอดเดรส (Address Learning)

ຕົວຢ່າງ



Switch#sh mac-address-table
Mac Address Table

Vlan	Mac Address	Type	Ports
---	-----	-----	-----
1	0001.4228.1053	DYNAMIC	Fa0/3
1	0009.7c59.46c9	DYNAMIC	Fa0/4
1	000b.be6b.0c44	DYNAMIC	Fa0/5
1	000c.cf28.338b	DYNAMIC	Fa0/5
1	0060.3e02.e81e	DYNAMIC	Fa0/1
1	0060.4778.86b3	DYNAMIC	Fa0/2

Virtual LAN (VLAN)

- Broadcast Domain หมายถึงขอบเขตของการส่งข้อมูลแบบกระจายไปถึงโหนดต่างๆ ทุกๆ โหนดที่อยู่ในเครือข่าย เพื่อให้โหนดทุกๆ ตัวได้รับเพرمไปประมวลผล
 - หากเครื่อง A และ B อยู่ใน Broadcast Domain เดียวกันแล้ว เครื่อง B จะได้รับ Broadcast Frame ที่ส่งมาจากเครื่อง A
- แต่ในการกรณีที่อุปกรณ์ต่างๆ ต้องการให้ใช้บริการต่างๆ ภายนอก Broadcast Domain เดียวกันแต่อุปกรณ์ต่างๆ นั้นอยู่ต่างพื้นที่กัน อาจจะอยู่กระจายไปทั่วอาคารหรืออาจจะอยู่ข้ามอาคาร
 - เครื่องคอมพิวเตอร์ของเจ้าหน้าที่ในมหาวิทยาลัยทุกๆ เครื่องกำหนดให้อยู่ในเครือข่าย LAN เดียวกันแต่ไม่สามารถกำหนดให้อยู่ในเครือข่าย LAN แบบปกติได้
- จำเป็นต้องสร้างเครือข่าย LAN แบบเสมือน (Virtual LAN หรือ VLAN) เพื่อความสะดวกในการจัดการการควบคุมสิทธิ์ในการเข้าถึงทรัพยากรต่างๆ ซึ่งจะส่วนไว้เฉพาะผู้ใช้ในเครือข่ายเฉพาะเท่านั้น

ประโยชน์

- ช่วยจำกัดการขยายขอบเขตของการกระจายของ Broadcast Frame เพื่อไม่ให้ส่งผลกระทบกับประสิทธิภาพโดยรวมของเครือข่าย
- เอพลิเคชันบนเครือข่าย รวมทั้งโปรโตคอลต่างๆ ได้แก่ TCP/IP, IPS/SPX หรือ IPv6 มักจะมีการส่ง Broadcast Frame ออกมาเป็นระยะๆ เพื่อประโยชน์ของโปรโตคอลนั้นๆ
- เมื่อการสื่อสารข้างต้นก่อให้เกิดประโยชน์แก่โปรโตคอล
- แต่ยังสร้างการรบกวนแก่ระบบเครือข่ายอีกด้วย หากไม่มีการกำหนดขอบเขตของ Broadcast Frame

ประโยชน์

- สร้างกลไกทางด้านความมั่นคง ได้ง่ายขึ้น เช่น การสร้าง ACL บนอุปกรณ์ในชั้นที่ 3 ของเครือข่าย สามารถลดความเสี่ยงของการดักจับข้อมูล ได้ง่ายขึ้น
- ผู้ใช้สามารถเคลื่อนย้ายไปยัง VLAN อื่นๆ ได้โดยการเปลี่ยน Configuration ของสิ่วตัวชี้นำนั้นๆ เท่านั้นโดยที่ไม่จำเป็นต้องแก้ไข ในชั้นกายภาพ
- ระบบเครือข่ายสามารถรองรับการขยายตัวในอนาคต ได้ง่าย เนื่องจาก ในชั้นต้นเครือข่ายถูกออกแบบมาเพื่อรับจำนวนโหนดน้อย เมื่อองค์กรขยายขึ้น หน่วยงานมีมากขึ้น การจัดการเครือข่ายจึงจำเป็นต้องขยายเช่นกัน ดังนั้นการเพิ่ม VLAN อีกวันเพื่อย้ายหน่วยงานย่อยๆ นั้นสามารถทำได้ง่ายขึ้น

หลักการแบ่ง VLAN

UbIn3\$
Ubiquitous Networked Embedded System

- การแบ่งตามตำแหน่งทางกายภาพ
- การแบ่งตามชั้นในอาคาร หรือแบ่งตามอุปกรณ์สวิตซ์ หรือแบ่งตามตำแหน่งที่ตั้งของหน่วยงาน เช่น เครื่องคอมพิวเตอร์ในอาคารชั้นที่ 2 อยู่ใน VLAN 2 และให้คอมพิวเตอร์ในอาคารชั้นที่ 3 อยู่ใน VLAN 3 เป็นต้น

หลักการแบ่ง VLAN

UbIn3\$
Ubiquitous Networked Embedded System

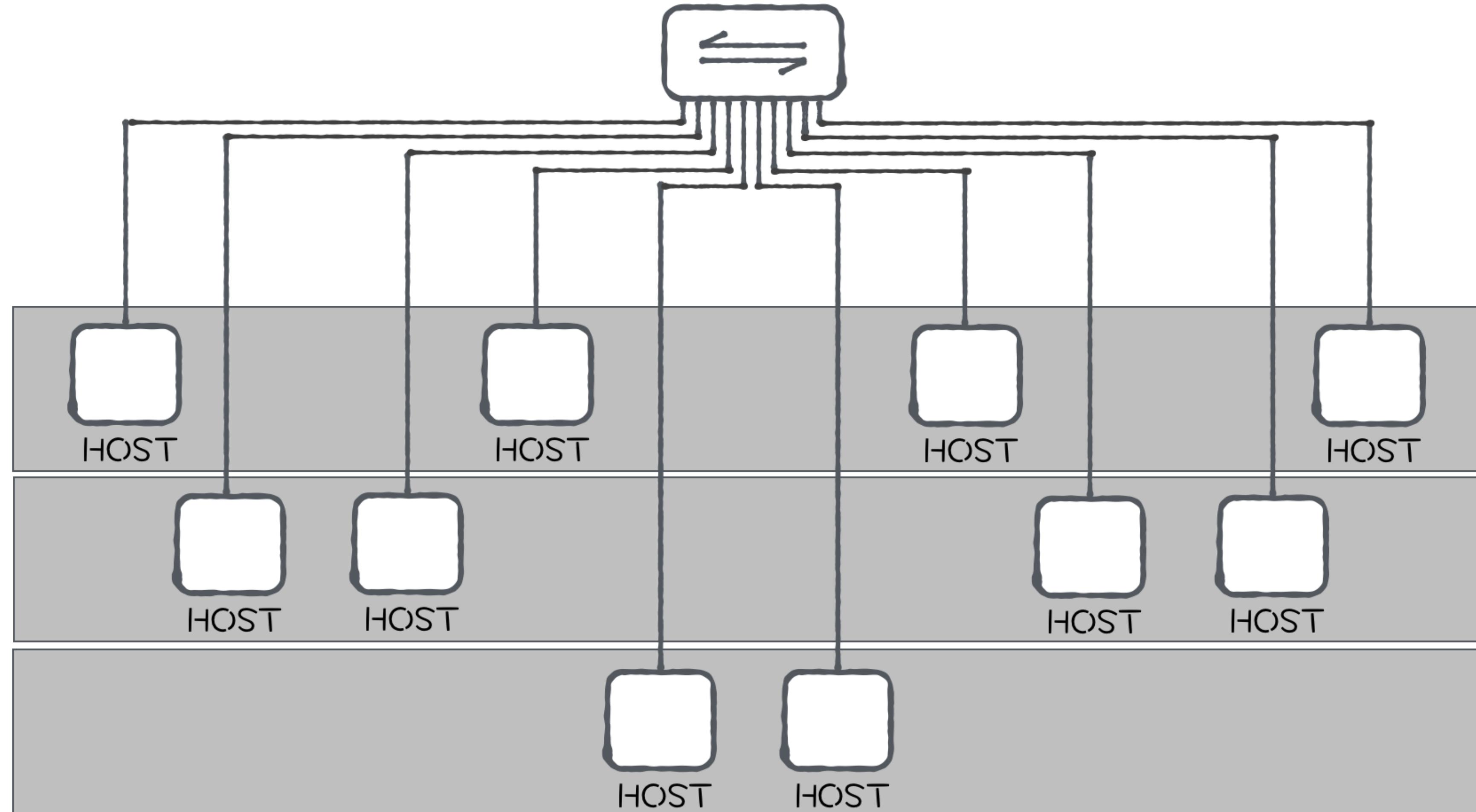
- การแบ่งตามหน่วยงาน
- เครื่องคอมพิวเตอร์แต่ละตัวจะเชื่อมต่ออยู่บนสวิตช์คนละตัวกัน และอยู่กันคนละชั้น สามารถนำมาร่วมกันเป็นสมาชิกของ VLAN เดียวกันได้ ซึ่งตำแหน่งทางกายภาพ ไม่มีผลกระทบต่อการจัดการระบบ

หลักการแบ่ง VLAN

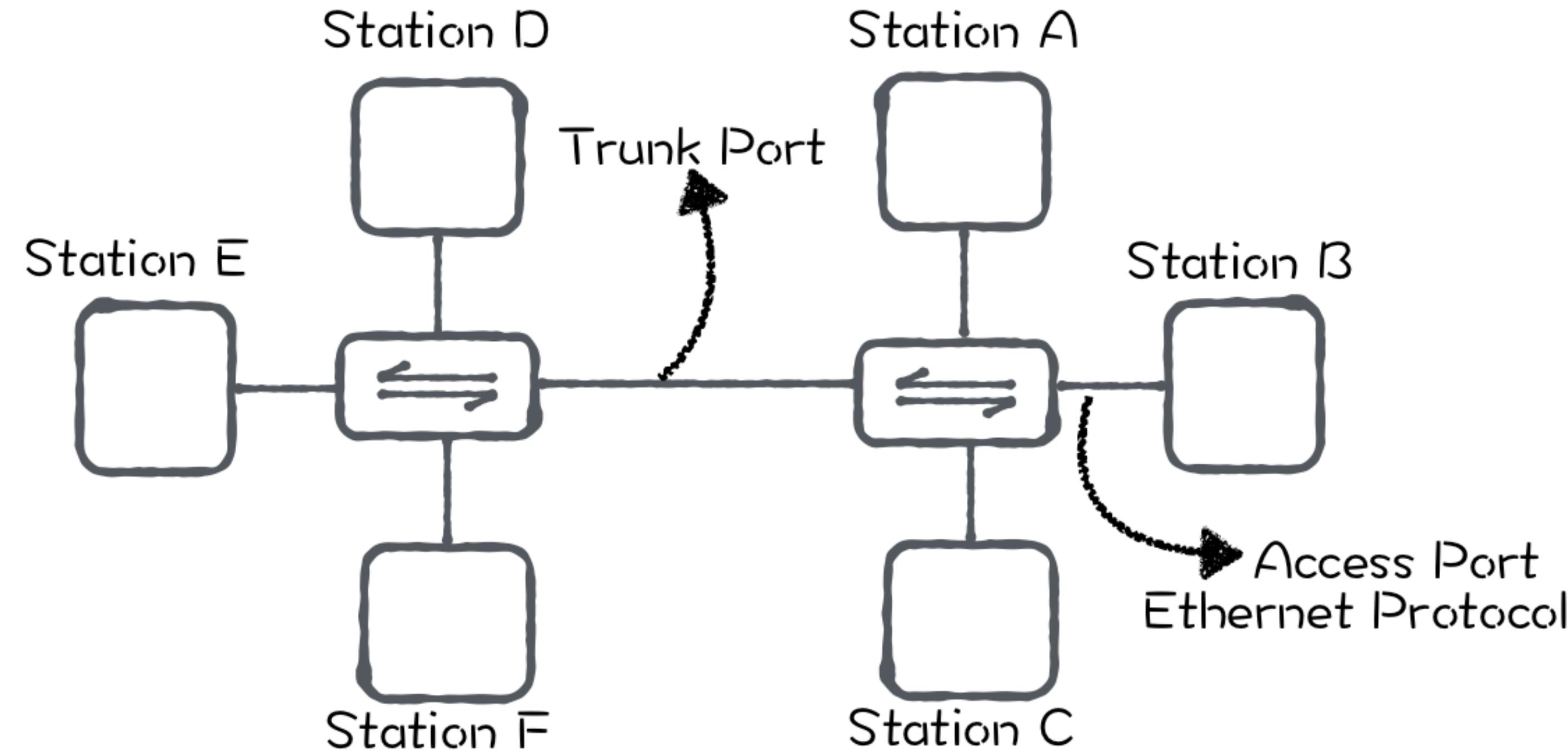
UbIn3\$
Ubiquitous Networked Embedded System

- การแบ่งตามการใช้งาน
- บางกลุ่มผู้ใช้ในองค์กรต้องการการใช้งานโปรแกรมเพียง 2 รายการเท่านั้น ในขณะอีกกลุ่มต้องการการใช้งานโปรแกรมในกลุ่มเดียวกัน 4 โปรแกรม และมีเครื่องพิมพ์แชร์ร่วมกัน ควรที่จะจัดให้อยู่ในเครือข่ายเดียวกัน
 -

ตัวอย่าง



Encapsulation



Wide Area Network

- Wide Area Network หมายถึงการเชื่อมต่อเครือข่ายแบบจุดต่อจุด โดยอุปกรณ์เครือข่ายแต่ละตัวอยู่ห่างกัน และเชื่อมต่อผ่านระบบเครือข่ายสาธารณะ หรือผู้ให้บริการ (Service Provider)
- การเชื่อมต่ออินเทอร์เน็ตของมหาวิทยาลัยลักษณ์ ผ่านอุปกรณ์เครือข่าย ซึ่งติดตั้งอยู่ที่มหาวิทยาลัย ผ่านเทคโนโลยี Leased Line เชื่อมต่อด้วยสายใยแก้วนำแสง ไปยังสำนักงานของผู้ให้บริการ (ในที่นี้คือ Uninet)
- นอกจากนี้ในประเทศไทยยังมีผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider หรือ ISP) หลายองค์กร ทั้งที่เป็นรัฐวิสาหกิจ และเอกชน

WAN Technology

UbIn3\$
Ubiquitous Networked Embedded System

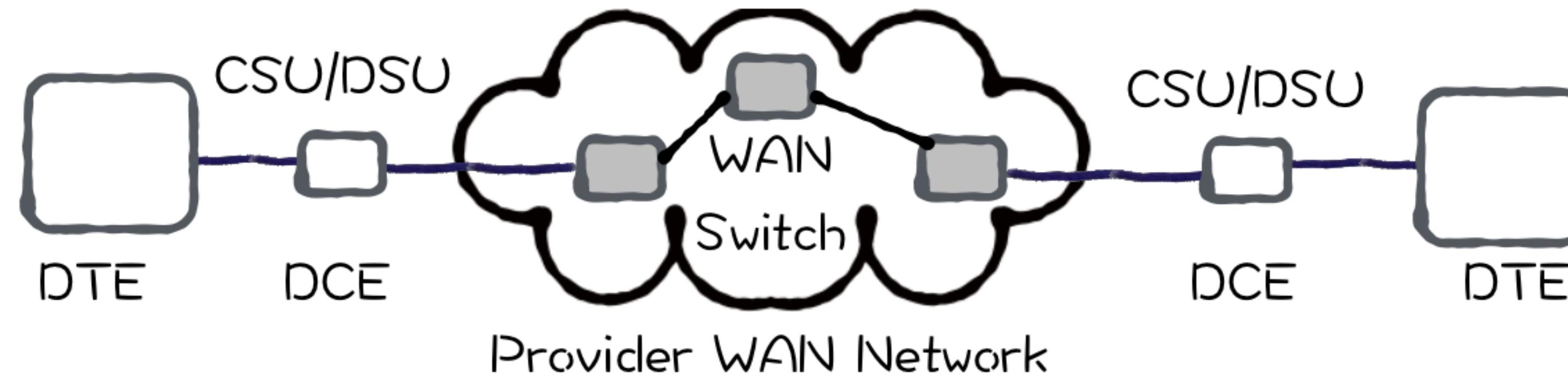
- เทคโนโลยีสำหรับเครือข่ายแบบกว้าง (Wide Area Network หรือ WAN) แบ่งออกเป็น 3 แบบได้แก่ Dedicated Circuit, Circuit Switching และ Packet Switching
 - **Dedicated Circuit** นั้นเป็นการเช่าวงจรดิจิทัล (Leased Line) โดยที่ทางผู้ให้บริการไม่จำเป็นต้องตั้งค่าวงจรใดๆ ก่อนส่งข้อมูล เพราะทางผู้ให้บริการได้ตั้งค่าต่างๆ ที่เกี่ยวข้องไว้แล้ว เราก็สามารถใช้สามารถรับส่งข้อมูลได้ทันที
 - **Circuit Switching** เป็นเครือข่ายที่ต้องการตั้งค่าเส้นทางก่อนการติดต่อกันปลายทางทุกครั้ง ได้แก่ Dial Up Modem เป็นต้น
 - **Packet Switching** เป็นเทคโนโลยีที่การเชื่อมต่อโดยใช้ X25 Switch หรือ Frame Relay Switch ในปัจจุบันเทคโนโลยีนี้กำลังเริ่มมีการใช้งาน หรือถูกแทนที่ด้วยเทคโนโลยีอื่นๆ

หลักการของ WAN

- อุปกรณ์ที่ใช้ในการเชื่อมต่อโดยส่วนใหญ่เป็นของผู้ให้บริการ โดยมีอุปกรณ์บางส่วนที่สำนักงานของผู้ใช้บริการ เป็นของผู้ให้บริการและผู้ให้บริการเป็นผู้กำหนดจุดเชื่อมต่อที่เหมาะสมไว้
- เครือข่ายแวนจะถูกสร้างขึ้นด้วยอุปกรณ์ที่เรียกว่า WAN Switch หรือ Router ส่วนวิธีการตั้งค่า และการเชื่อมต่อของวงจรนั้น ขึ้นอยู่กับชนิดของเครือข่าย
- อุปกรณ์ที่ใช้ในการเชื่อมต่อ มี 2 ประเภท
 - Data Terminal Equipment หรือ DTE ซึ่งได้แก่อุปกรณ์ปลายทางของผู้ใช้บริการ
 - Data Circuit Equipment หรือ DCE เป็นอุปกรณ์ที่ผู้ให้บริการเครือข่ายแวนจัดหมายให้ทางผู้รับบริการเพื่อเชื่อมต่อเน็ตเวิร์ค

1.

หลักการของ WAN



- อุปกรณ์ประเภท DTE เป็นอุปกรณ์ที่ทางผู้ให้บริการเป็นเจ้าของโดยตรง
- ตัวอย่างของ DTE ได้แก่ อุปกรณ์เราเตอร์ของผู้รับบริการ ซึ่งเชื่อมต่อไปยังเครือข่ายภายนอก
- ตัวอย่าง DCE ได้แก่ อุปกรณ์ Channel Service Unit/Data Service Unit หรือ CSU/DSU ซึ่งเป็นอุปกรณ์ที่เชื่อมต่อระหว่างเราเตอร์ของผู้รับบริการและ WAN Switch ของผู้ให้บริการ

Encapsulation

- เมื่อเปรียบเทียบกับการเครือข่ายแลนมีการห่อหุ้มแพ็คเก็ตโดยใช้โปรโตคอล Ethernet
- ในขณะที่เครือข่ายแวนที่เชื่อมต่อแบบวงจรเช่านั้น ห่อหุ้มด้วยโปรโตคอลจำนวน 2 ชนิดได้แก่ HDLC และ PPP
- **HDLC** เป็นรูปแบบการห่อหุ้มแพ็คเก็ตบนเครือข่ายแวนแบบที่ง่ายและตรงไปตรงมามากที่สุด
 - HDLC ถูกแก้ไขโดย CISCO ซึ่งใช้งานเฉพาะการลีโอสาระระหว่างอุปกรณ์ CISCO เท่านั้น

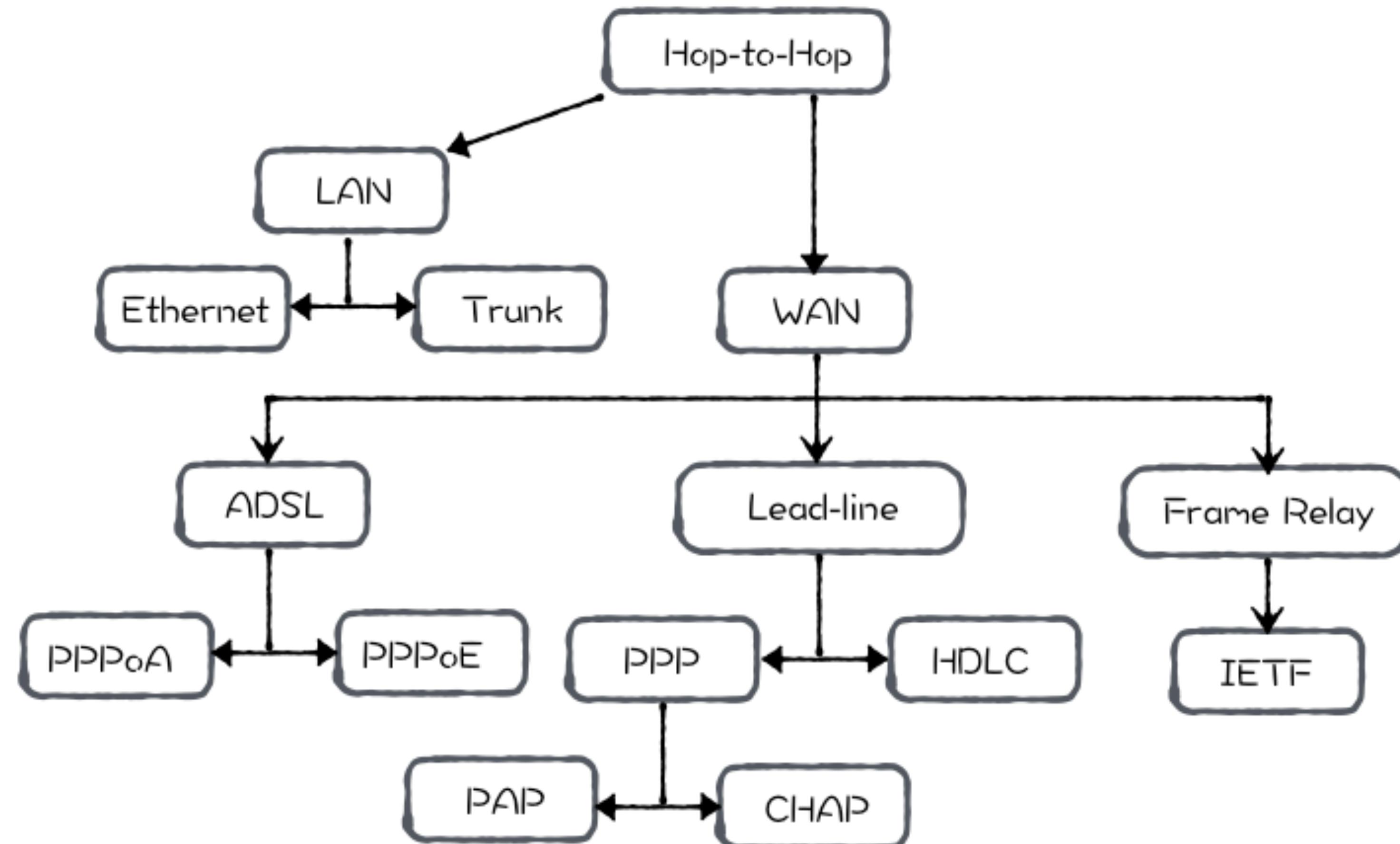
Encapsulation

- โปรโตคอล PPP เป็นโปรโตคอลที่นิยมใช้ในการเชื่อมต่อเครือข่ายแบบจุดต่อจุดซึ่งเป็นโปรโตคอลมาตรฐานที่ไม่อิงกับบริษัทใดๆ
- ถูกเลือกใช้ในการเชื่อมต่อเครือข่ายสำหรับผู้ให้บริการอินเทอร์เน็ต กับผู้ให้บริการอินเทอร์พ่าน ADSL
- การเชื่อมต่อโดยโปรโตคอล PPP เป็นการเชื่อมต่อโดยใช้สายโทรศัพท์ดังนั้นมีโอกาสที่จะถูกสัมരอย
 - ดังนั้นการเชื่อมต่อระหว่างอุปกรณ์ทั้งสองตัวนี้ต้องการกระบวนการตรวจสอบตัวตน (Authentication) ซึ่งมีโปรโตคอลที่ใช้สำหรับการตรวจสอบตัวตนจำนวน 2 ชนิดคือ Password Authentication Protocol หรือ PAP และ Challenge Handshake Authentication Protocol หรือ CHAP

Encapsulation

- โพรโตคอล PAP ผู้ใช้ต้องป้อนชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ก่อนการเชื่อมต่อ หลังจากที่ระบบได้ตรวจสอบตัวตนแล้วแล้ว ผู้ใช้สามารถเข้าใช้งานหรือปฏิเสธการใช้งานได้
- โพรโตคอล CHAP เป็นโพรโตคอลที่ความปลอดภัยมากกว่า PAP โดยที่รหัสผ่านและชื่อผู้ใช้จะถูกจัดเก็บไว้ในอุปกรณ์นั้นๆ โดยที่ไม่ถูกส่งออกผ่านเครือข่าย

Encapsulation Protocol



Wireless LAN

Wireless LAN

UbIn3\$
Ubiquitous Networked Embedded System

- การสื่อสารข้อมูลแบบไร้สาย ในเครือข่ายท้องถิ่น หรือ Wireless Local Area Network (WiFi)
- การเชื่อมต่อผ่าน WiFi อิงตามมาตรฐาน IEEE 802.11 ซึ่งเป็นมาตรฐานเดียวกันกับอีเธอร์เน็ตเช่นกัน
- การออกแบบมาตรฐาน IEEE 802.11 นี้ได้นำโมดูลต่างๆ ของ IEEE 802.3 กลับมาใช้ใหม่หลายโมดูล
- อีกทั้งยังสามารถนำมาเชื่อมต่อกับเทคโนโลยี Ethernet LAN ได้โดยง่าย
- การออกแบบพอร์ตคอลของ IEEE 802.11 นั้นไม่แตกต่างกับ 10BaseT, 100BaseT และ 1000BaseT
 - โดยมีโมดูลส่วนของ PHY และ MAC บางส่วนที่แตกต่างกัน

Wireless LAN

UbIn3\$
Ubiquitous Networked Embedded System

- การสื่อสารแบบไร้สายเป็นเทคโนโลยีที่กำลังจะเป็นซ่องทางหลักที่ประยุกต์ใช้งานในปัจจุบันและอนาคต
- นอกจากนี้เทคโนโลยี Internet of Thing เป็นการเน้นย้ำความต้องการของการเชื่อมต่ออุปกรณ์ต่างๆเข้าสู่เครือข่าย เพื่อใช้ผู้ใช้สามารถเชื่อมต่อเครือข่ายได้ตลอดเวลาและสถานที่ (Any Time Any Where)
- การพัฒนาของเทคโนโลยีมีหลายแนวทางได้แก่
 - ความเร็วในการสื่อสารข้อมูล ระยะห่างของแต่ละ Hop
 - พลังงานที่ใช้ในการสื่อสาร
- เทคโนโลยีของการสื่อสารแบบไร้สาย
 - IEEE 802.11 (WiFi), IEEE 802.15.1 (Blue Tooth) และ IEEE 802.15.4 (LowPAN)

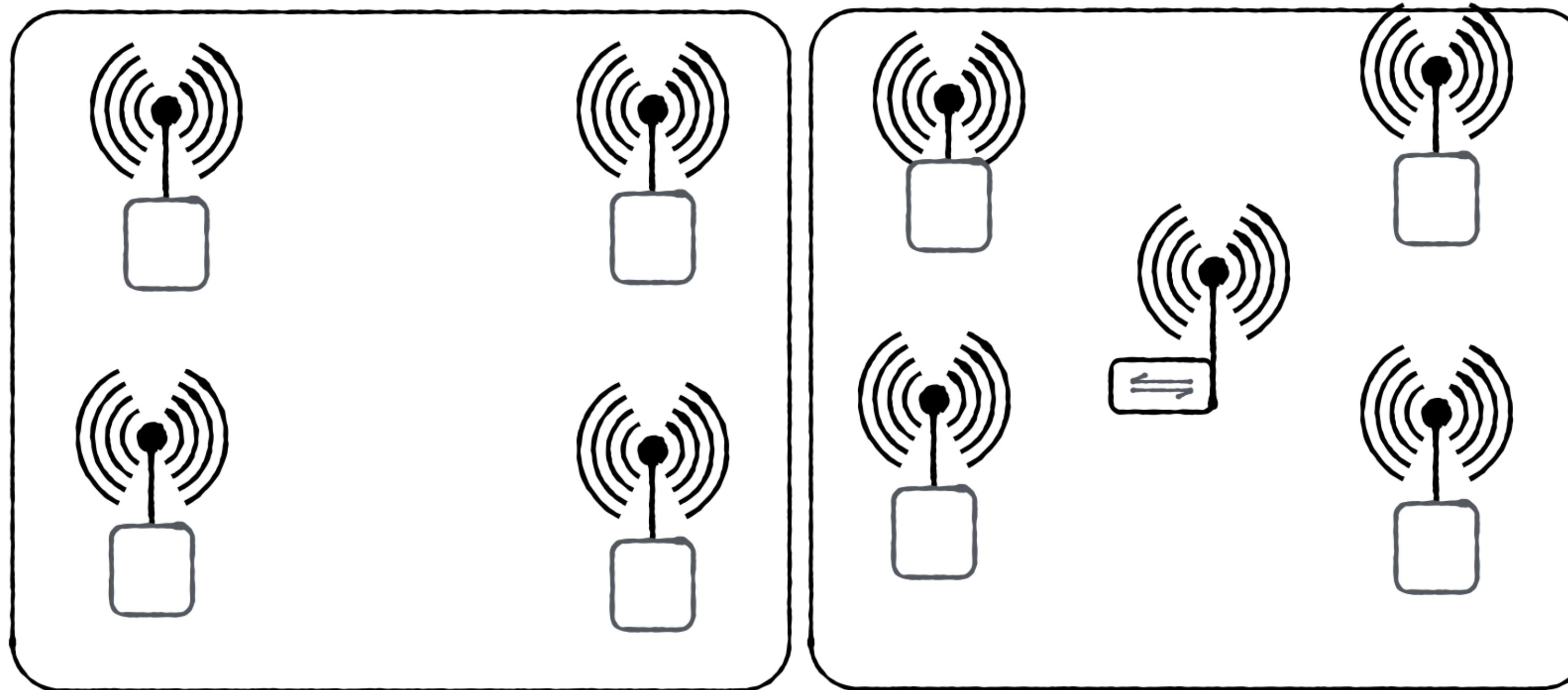
IEEE 802.11 Standard

- มาตรฐาน IEEE 802.11 เป็นมาตรฐานของการสื่อสาร WiFi ซึ่งประกอบด้วย 2 บริการ คือ Basic Service Set (BSS) และ Extended Service Set (หรือ ESS)
- **Basic Service Set (BSS)** คือ การเชื่อมต่อเครือข่ายไร้สาย โดยที่โหนดลูกได้แก่ คอมพิวเตอร์ มือถือ แท็บเลต เป็นต้น เพื่อต่อกับอุปกรณ์กลาง (Base Station) หรือ Access Point (AP) หรือโหนดลูกเชื่อมต่อกันเอง โดยตรง โดยที่ไม่ผ่านอุปกรณ์กลาง เรียกว่า การเชื่อมต่อแบบนี้ว่า สถาปัจยกรรมแบบ Ad Hoc

IEEE 802.11 Standard

BSS: Basic Service Set

AP: Access Point



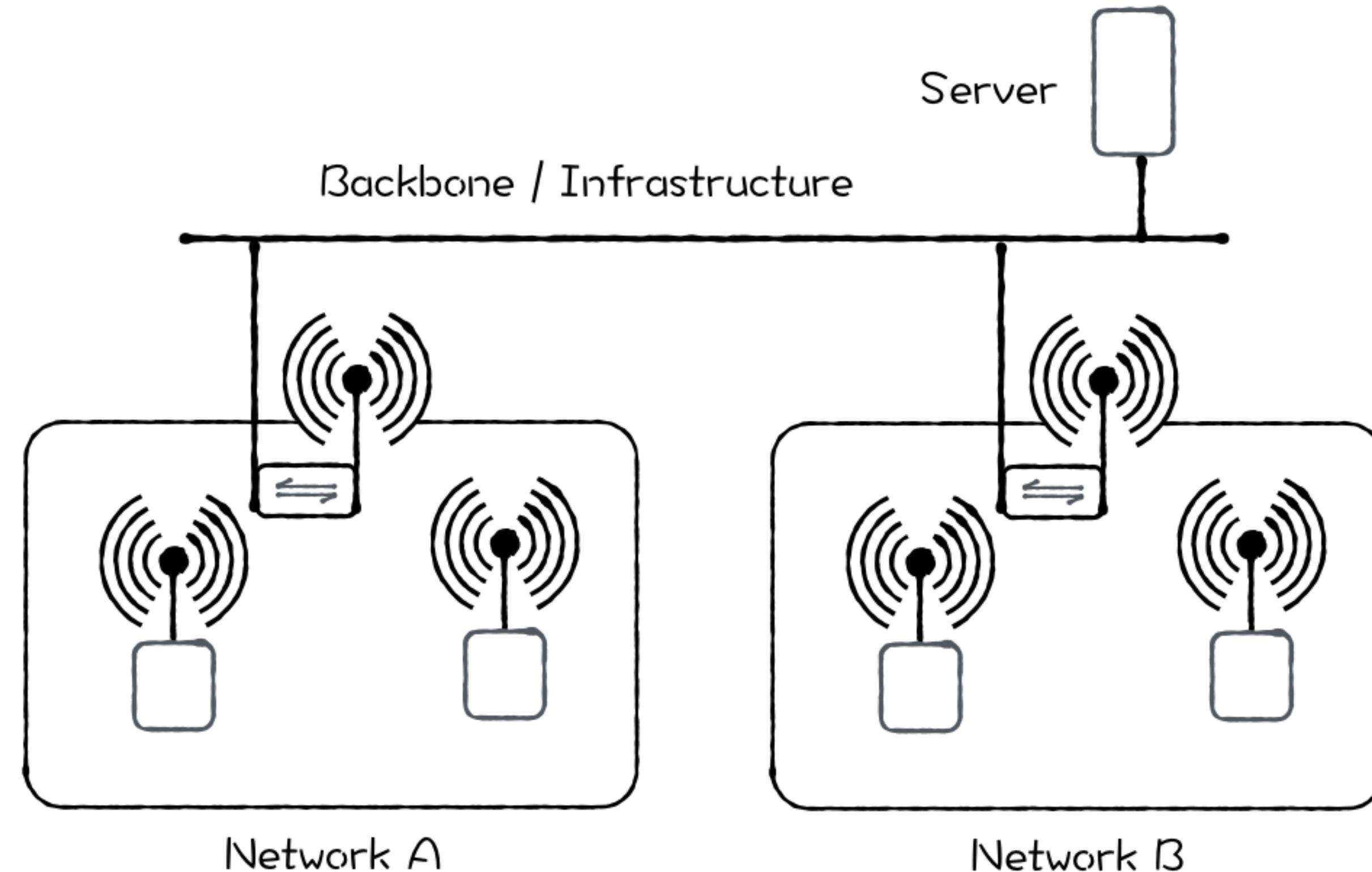
IEEE 802.11 Standard

UbIn3\$
Ubiquitous Networked Embedded System

- **Extended Service Set (ESS)** คือการเชื่อมต่อเครือข่ายแบบ BSS ตั้งแต่ 2 เครือข่ายขึ้นไปเชื่อมต่อกันกับ AP ตัวอื่น หรือ โครงข่าย BSS แต่ละตัวเชื่อมต่อกันผ่านเครือข่าย Wired LAN ระบบเครือข่ายแบบ ESS นี้เรียกอีกชื่อว่า **Infrastructure network**

IEEE 802.11 Standard

UbiN3\$
Ubiquitous Networked Embedded System



CSMA/CD

- Carrier Sense Multiple Access with Collision Detection
- ในการสื่อสารแบบมีสายนั้น โนนดแต่ละตัวเชื่อมต่อกับเครือข่ายสามารถตรวจนับแรงดันไฟฟ้าในสายส่งได้ หากมีโนนดใดๆ กำลังใช้ช่องทางอยู่นั้น แรงดันไฟฟ้าจะสูงกว่าปกติ

CSMA/CD

- การเข้าใช้ช่องสัญญาณของการสื่อสารแบบไร้สาย ใช้เทคนิค Carrier Sense Multiple Access with Collision Avoidance หรือ CSMA/CA
 - เทคนิคการเข้าใช้ช่องสัญญาณแบบเดียวกันกับการสื่อสารแบบมีสาย แต่ความแตกต่างระหว่างการสื่อสารแบบมีสายและไร้สายนั้นมีจุดต่างกัน
- ในการสื่อสารแบบไร้สายนั้น ไม่สามารถตรวจแรงดันในสื่อได้ จึงใช้เทคนิคอีกแบบคือ Collision Avoidance
 - โหนดที่ต้องการส่งข้อมูลต้องส่งสัญญาณไปแจ้ง AP ก่อนเพื่อจองช่องสัญญาณ หากช่องสัญญาณว่างแล้ว โหนดนั้นจะได้รับสิทธิ์ในการใช้ช่องสัญญาณ และส่งข้อมูลได้

Mobility

- การเคลื่อนย้ายโนนดต่างๆ โดยที่การเคลื่อนย้ายของโนนดนั้นไม่มีผลต่อการเชื่อมต่อ
- การลีอสารยังเกิดขึ้นได้แม้ว่าโนนดกำลังเคลื่อนย้ายอยู่ รูปแบบการเคลื่อนย้ายของโนนดแบ่งออกเป็น 3 ลักษณะ ได้แก่
 - No Transition Mobility
 - BSS Transition Mobility
 - ESS Transition Mobility

Mobility

