523353 – Computer Networks

Lecture 3: Ethernet LANs - Part1

Dr. Parin Sornlertlamvanich

CompTIA Security+

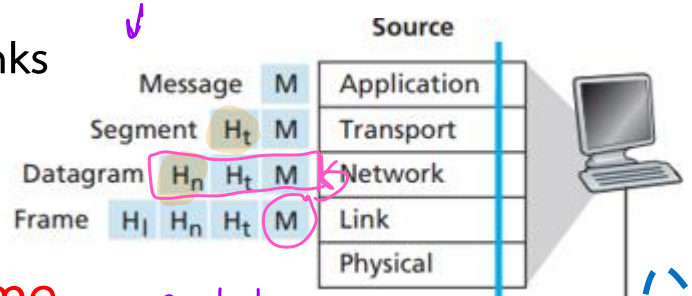
Huawei Certified HCIA-Datacom

parin.s@sut.ac.th

Link layer: introduction

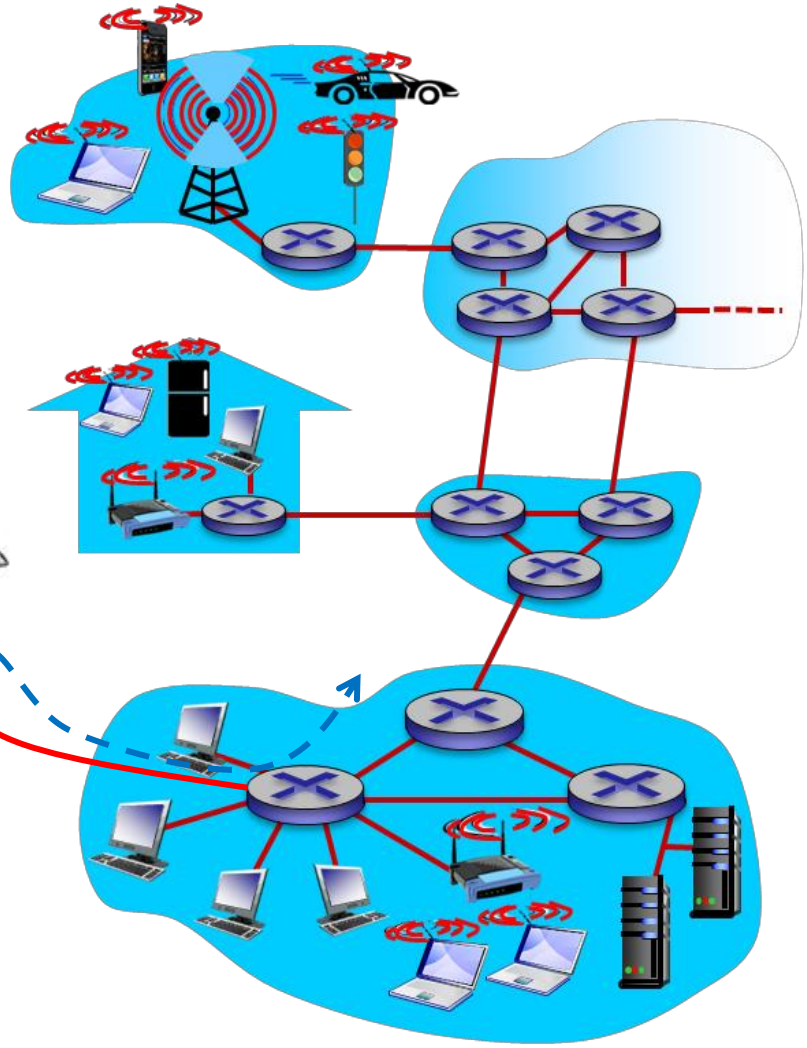
② Datalink

- Communication channels that connect adjacent nodes along communication path: links
  - Wired links
  - Wireless links
  - LANs



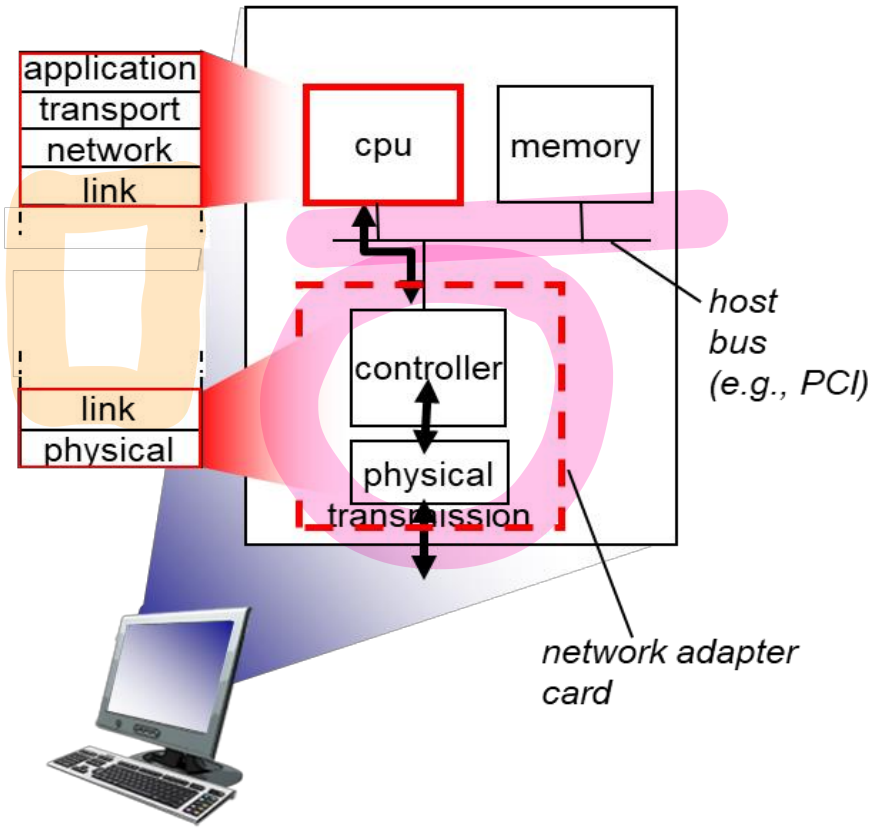
- Layer-2: frame
  - Encapsulates datagram

data-link layer has responsibility of transferring datagram from one node to *physically adjacent* node over a link

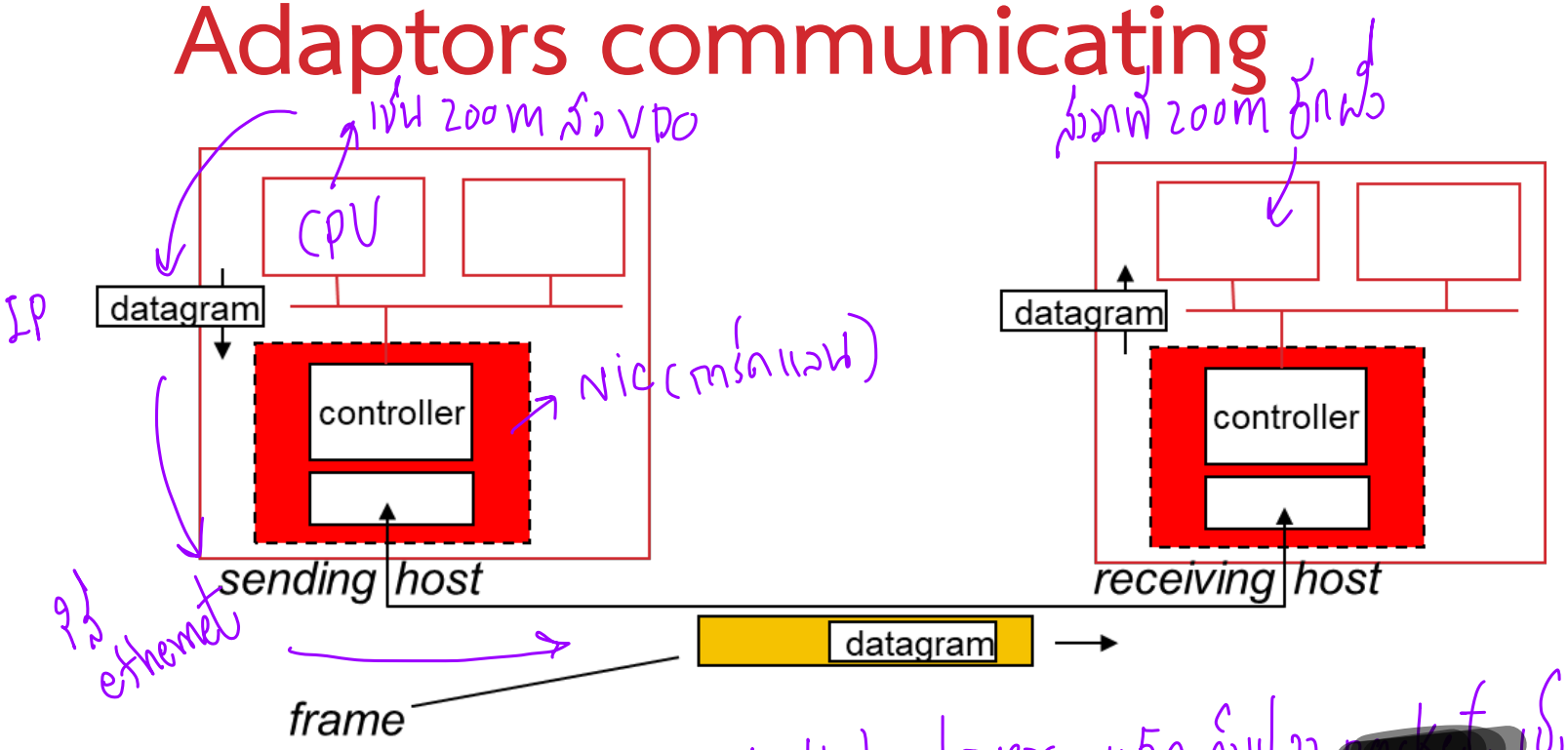


Where is the link layer implemented?

- In each and every host
- Link layer implemented in "Adaptor" (aka *Network Interface Card,* NIC) or on a chip
  - Ethernet card, 802.11 card
- Attaches into host's system buses
- Combination of hardware, software, firmware

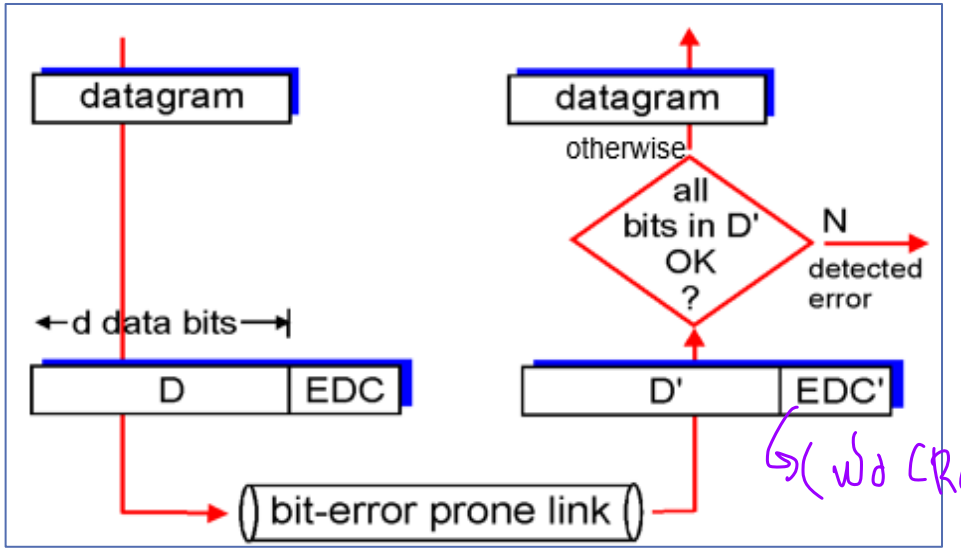


Adaptors communicating



- **Sending side:**
  - encapsulates datagram in frame
  - adds error checking bits, flow control, etc.
- **Receiving side:**
  - looks for errors, flow control, etc.
  - extracts datagram, passes to upper layer at receiving side

Error Detection and Correction (EDC)

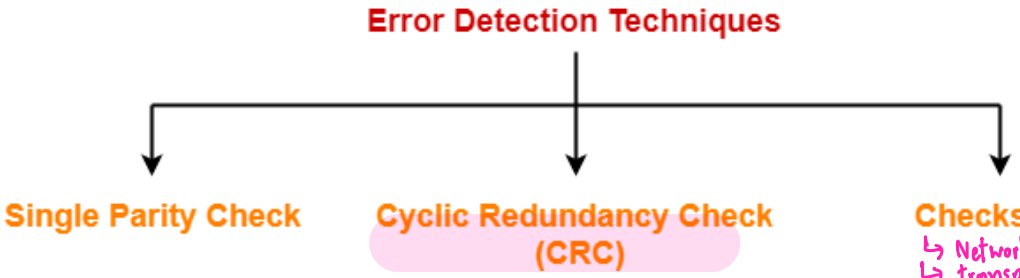


EDC - Error Detection and Correction bits (redundancy)

D - Data protected by error checking, may include header fields

Error detection not 100% reliable!

- Protocol may miss some errors, but rarely
- Larger EDC field yields better detection and correction



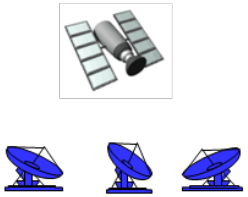
Multiple Access Links and Protocols

Two types of links

- 1. Point-to-point
  - PPP for dial-up access
  - Point-to-point link between Ethernet switch, host
- 2. Broadcast (shared wire or medium)
  - old-fashioned Ethernet
  - upstream Hybrid fiber-coaxial (HFC)
  - 802.11 wireless LAN

shared wire (e.g., cabled Ethernet)

shared RF (e.g., 802.11 WiFi)



shared RF (satellite)

humans at a cocktail party (shared air, acoustical)

Multiple Access Links and Protocols

Broadcast links

- Single shared broadcast channel
- Two or more simultaneous transmissions by nodes: interference
  - Collision if node receives two or more signals at the same time

Multiple Access Protocol

- Algorithm that determines how nodes share channel, i.e., determine when node can transmit
- Communication about channel sharing must use channel itself!
  - No out-of-band channel for coordination

Multiple Access Control (MAC) Protocols

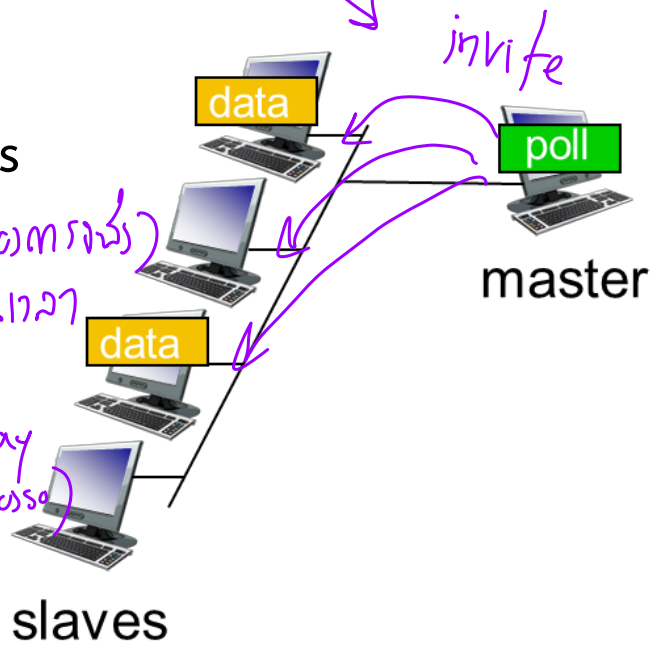
We can classify just about any MAC protocol as belonging to one of three categories

- **Channel Partitioning**
  - divide channel into smaller "pieces" (time slots, frequency, code)
  - allocate piece to node for exclusive use
- **Random Access**
  - CSMA protocol
  - Channel not divided, allow collisions
  - "Recover" from collisions
- **"Taking turns"**
  - Nodes take turns, but nodes with more to send can take longer turns
    - Polling
    - Token passing

“Taking turns” MAC protocols

Polling:

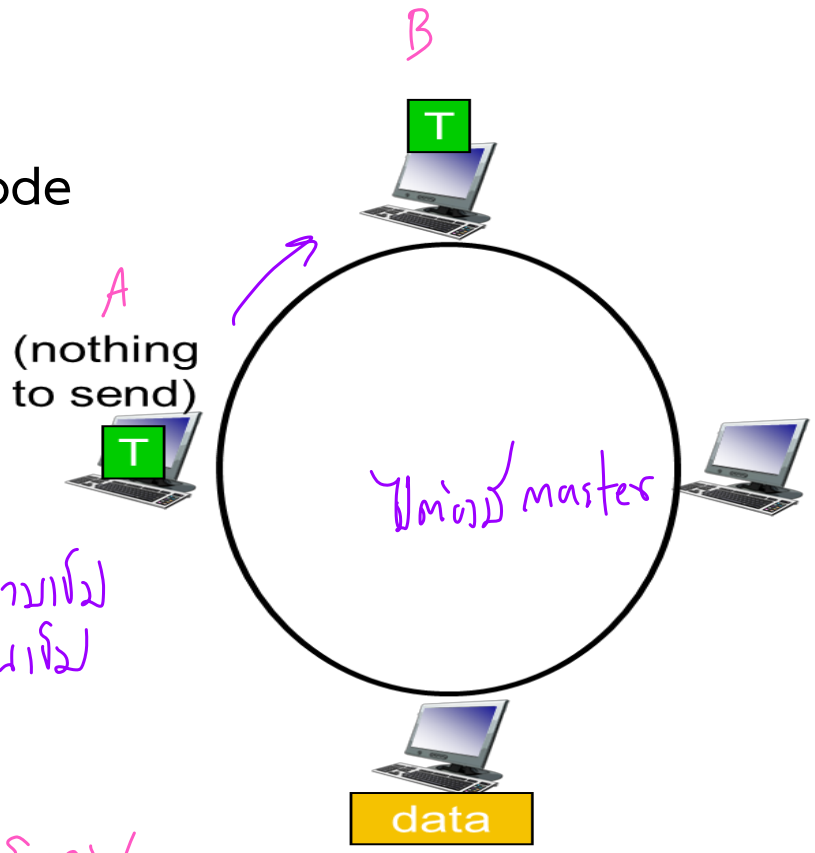
- master node “invites” slave nodes to transmit in turn
- typically used with “dumb” slave devices
- concerns:
  - polling overhead
  - latency
  - single point of failure (master)



“Taking turns” MAC protocols

Token passing:

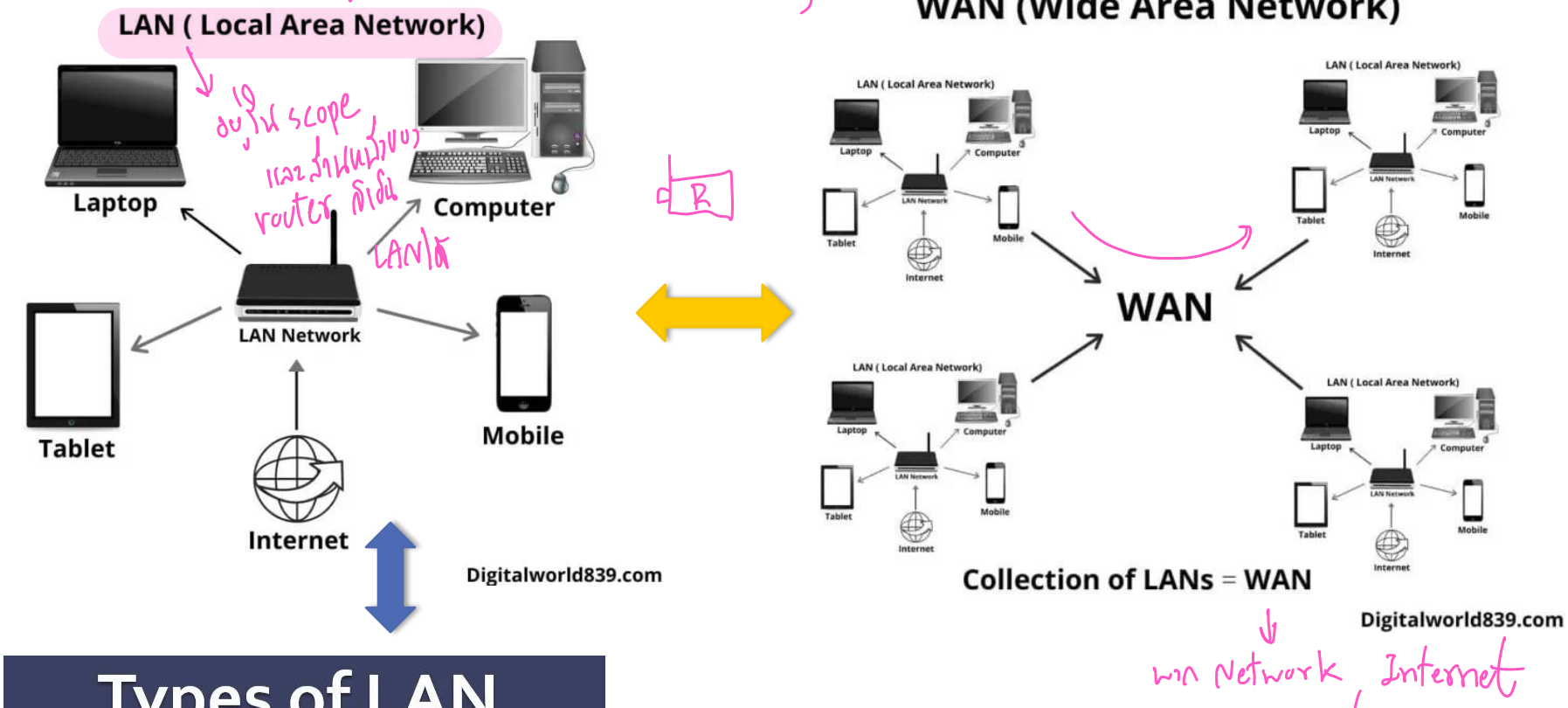
- control *token* passed from one node to next sequentially
- token message
- concerns:
  - token overhead
  - latency
  - single point of failure (token)

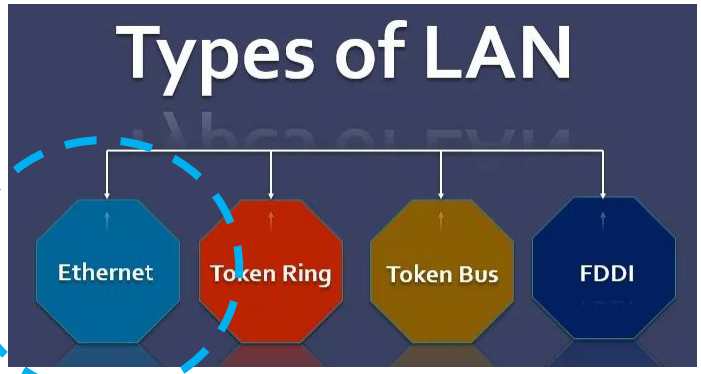


Summary of MAC protocols

- Channel partitioning, by time, frequency or code
  - Time Division, Frequency Division
- Random access (dynamic),
  - ALOHA, S-ALOHA, CSMA, CSMA/CD
  - carrier sensing: easy in some technologies (wire), hard in others (wireless)
  - CSMA/CD used in Ethernet
  - CSMA/CA used in 802.11
- Taking turns
  - polling from central site, token passing
  - Bluetooth, Fiber Distributed Data Interface (FDDI), token ring

Local Area Network (LAN)

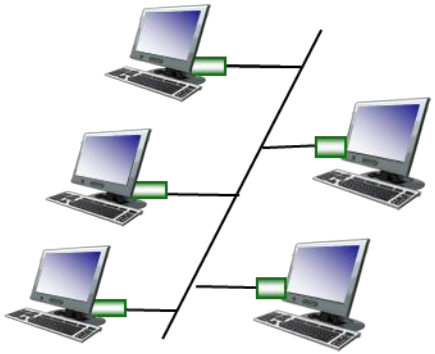




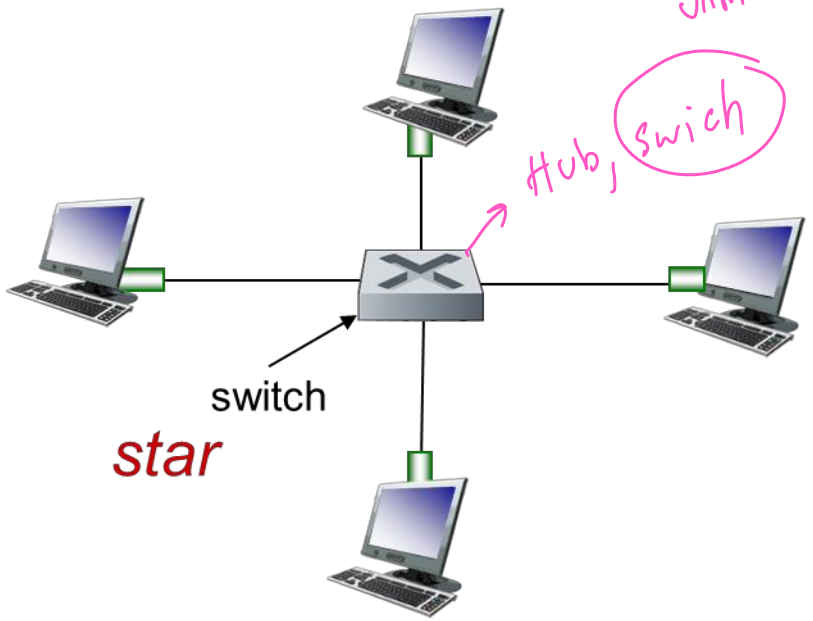
https://digitalworld839.b-cdn.net/wp-content/uploads/LAN-vs-WAN-vs-MAN-Comparison.jpg

Ethernet: physical topology

- Bus: popular through mid 90s
  - All nodes in same collision domain (can collide with each other)
- Star: prevails today
  - Active switch in center



bus: coaxial cable

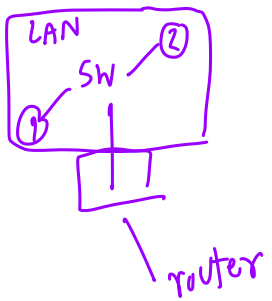


star

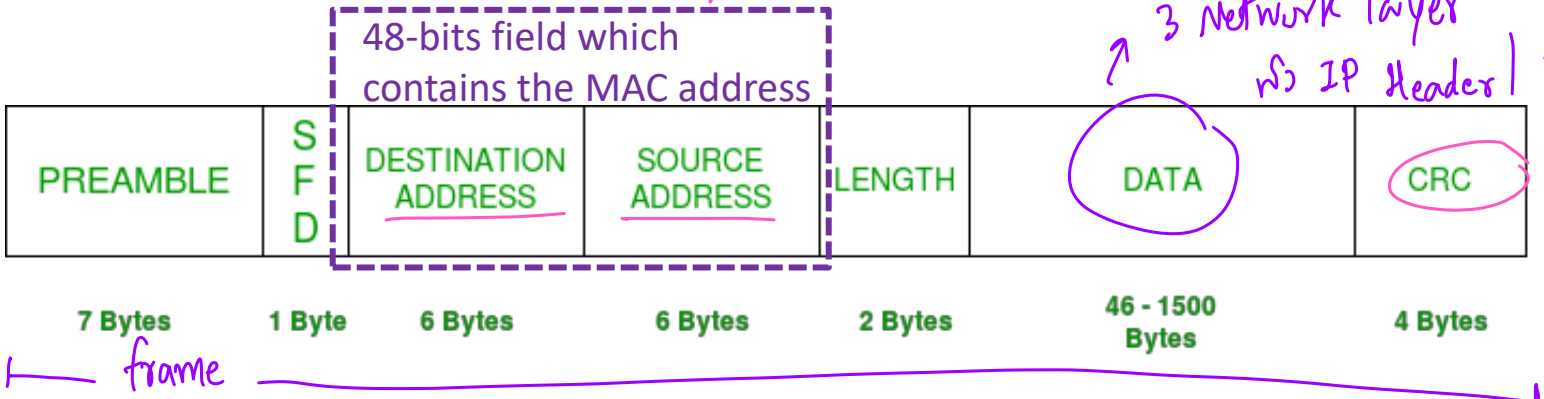
IP address vs. MAC addresses

- 32-bit IP address:
  - Network-layer address for interface
  - Used for layer 3 (network layer) forwarding
- MAC (or LAN or physical or Ethernet) address:
  - function: used 'locally" to get frame from one interface to another physically-connected interface (same network, in IP-addressing sense)
  - 48-bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
  - e.g.: 1A-2F-BB-76-09-AD

Hexadecimal (base 16) notation
(each "numeral" represents 4 bits)



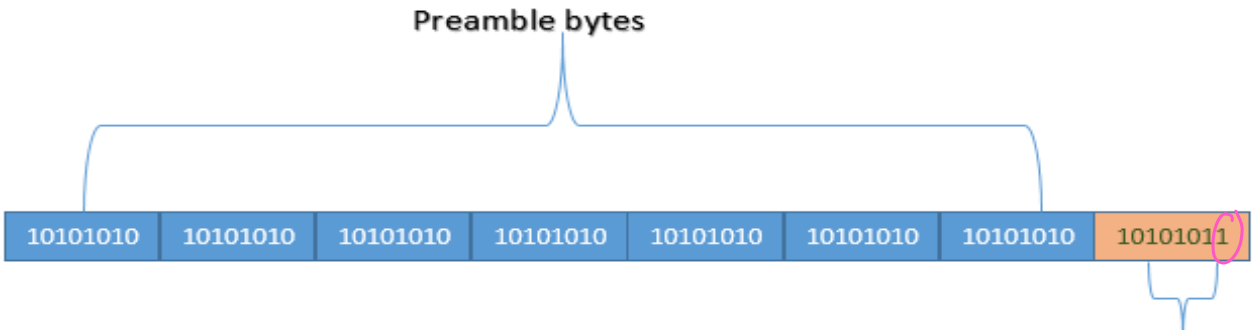
Ethernet (IEEE 802.3) frame structure



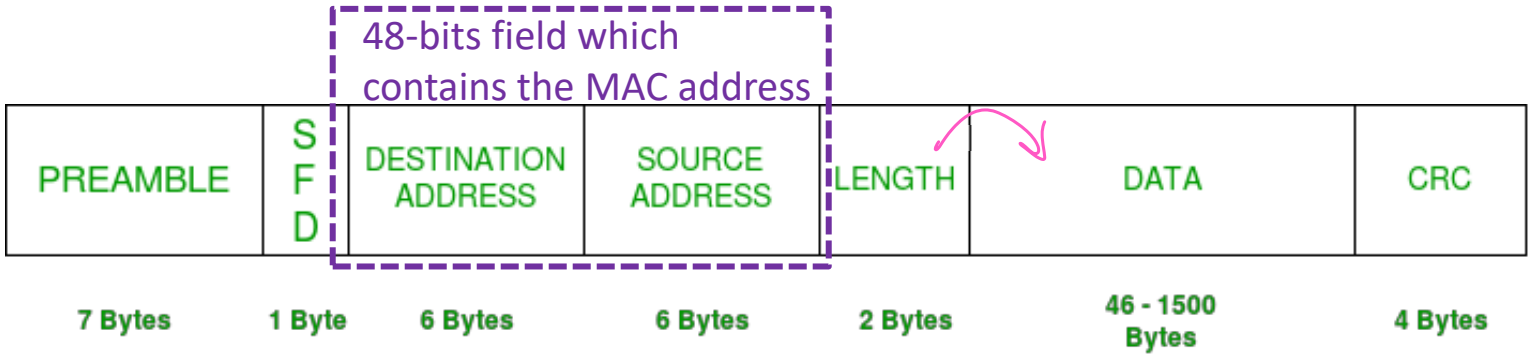
- Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame

- Preamble (7 bytes):

- 1-6 bytes with pattern 10101010 followed by one byte with pattern 10101011
- Used to synchronize receiver, sender clock rates



Ethernet (IEEE 802.3) frame structure (more)



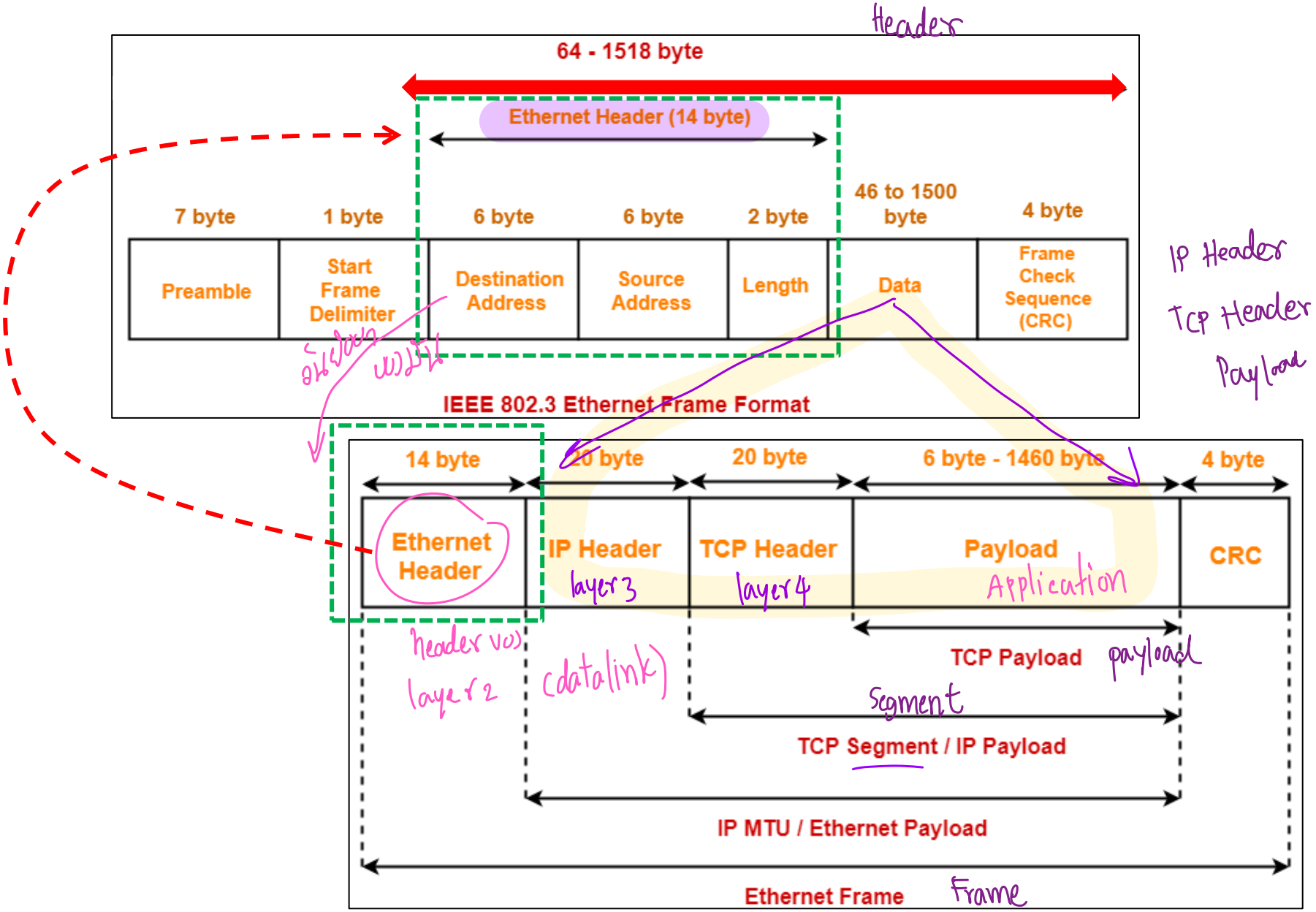
- Addresses: 6-byte source, destination MAC addresses
  - If adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to network layer protocol
  - otherwise, adapter discards frame

- Length/Type: Length is a 2-Byte field
  - Values of 1500 and below mean that it is used to indicate the data size
  - Values of 1536 and above indicate that it is used as an EtherType
  - 1501–1535 is undefined

- CRC: cyclic redundancy check at receiver
  - Error detected: frame is dropped

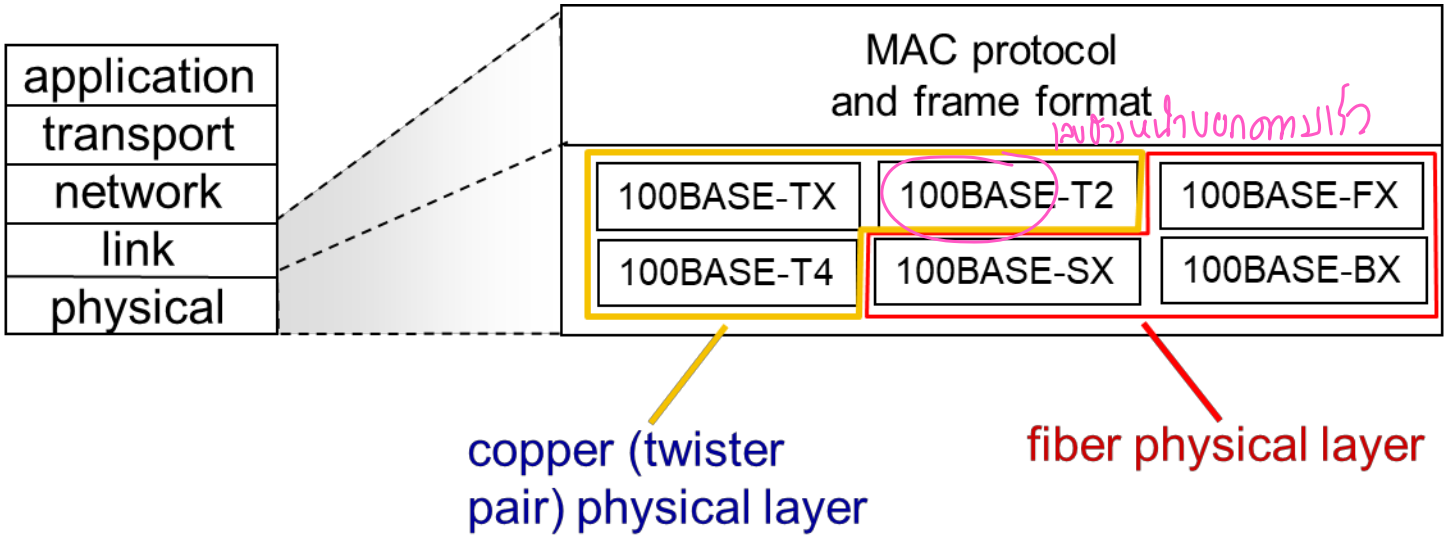
https://www.gatevidyalay.com/ethernet-ethernet-frame-format/

IP datagram sits inside the Ethernet payload field



802.3 Ethernet standards: link & physical layers

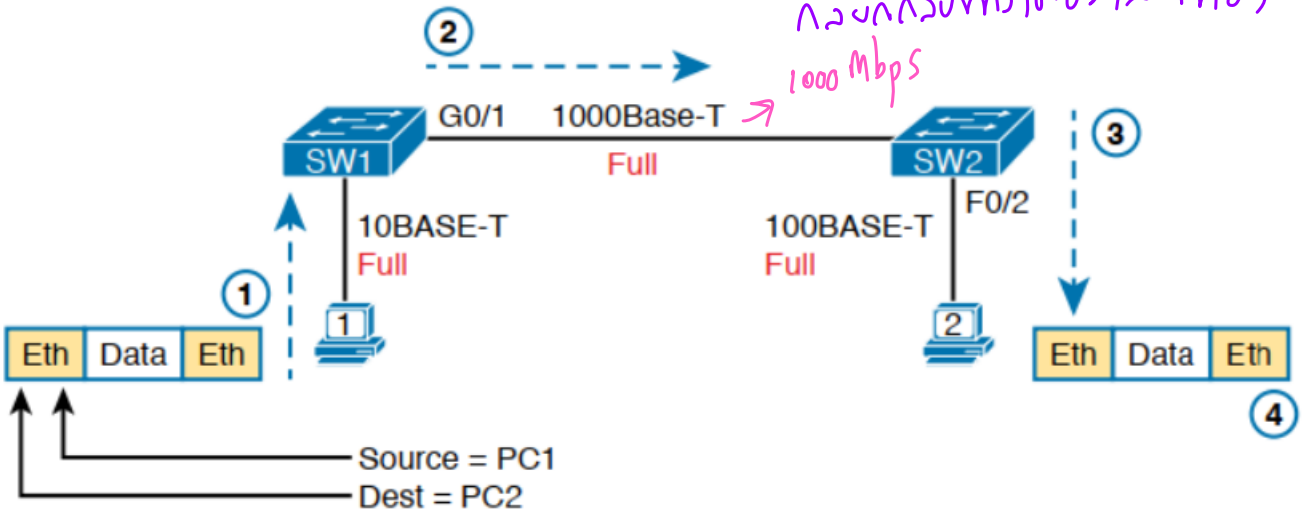
- Many different Ethernet standards
  - Common MAC protocol and frame format
  - Different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1Gbps, 10 Gbps, 40 Gbps, 100 Gbps
  - Different physical layer media: fiber, cable



Hub & Ethernet Switch

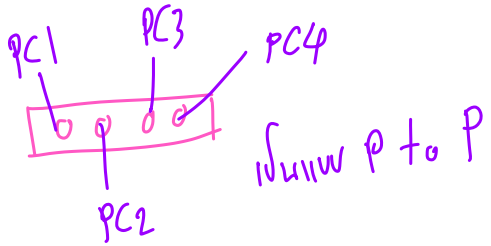
Sending Ethernet Frames

- LAN switches instead of some older LAN devices called LAN hubs
- More modern switches allows the use of full-duplex logic
  - faster and simpler than half-duplex logic



Half-duplex and Full-duplex

- **Half-duplex:**
  - Higher potential for collision
  - The device must wait to send if it is currently receiving a frame; in other words, it cannot send and receive at the same time.



- **Full-duplex: (no LAN hubs)**
  - Point-to-point only
  - Require full-duplex support on both ends
  - The device does not have to wait before sending; it can send and receive at the same time.

Using Half-duplex with LAN Hubs

- When the IEEE first introduced 10BASE-T in 1990, Ethernet switches did not exist yet

- LAN hubs forward data using physical layer standards rather than data-link standards and are therefore considered to be Layer 1 devices → พวก Hub
  - Hub repeats that electrical signal out all other ports (except the incoming port)
  - Hub has no concept of Ethernet frames

Using Half-duplex with LAN Hubs (2)

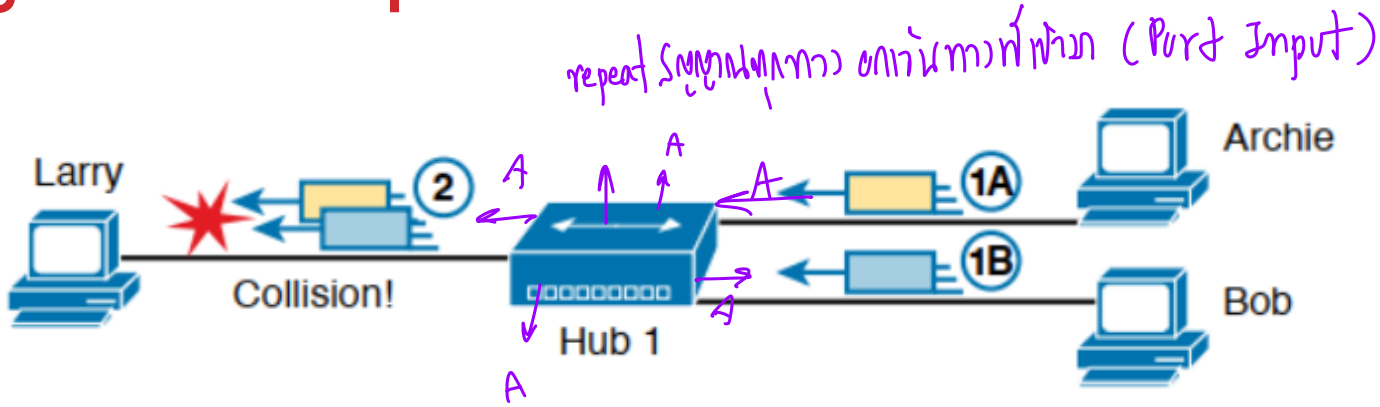
โบราณแล้ว

กระตุ้นสัญญาณ อย่างเดียว

มันไม่ได้ป้องกันการชน

- Hubs are a form of repeater for an Ethernet LAN which has multiple ports (they are sometimes also known as "multi-port repeaters"

Using Half-duplex with LAN Hubs (3)

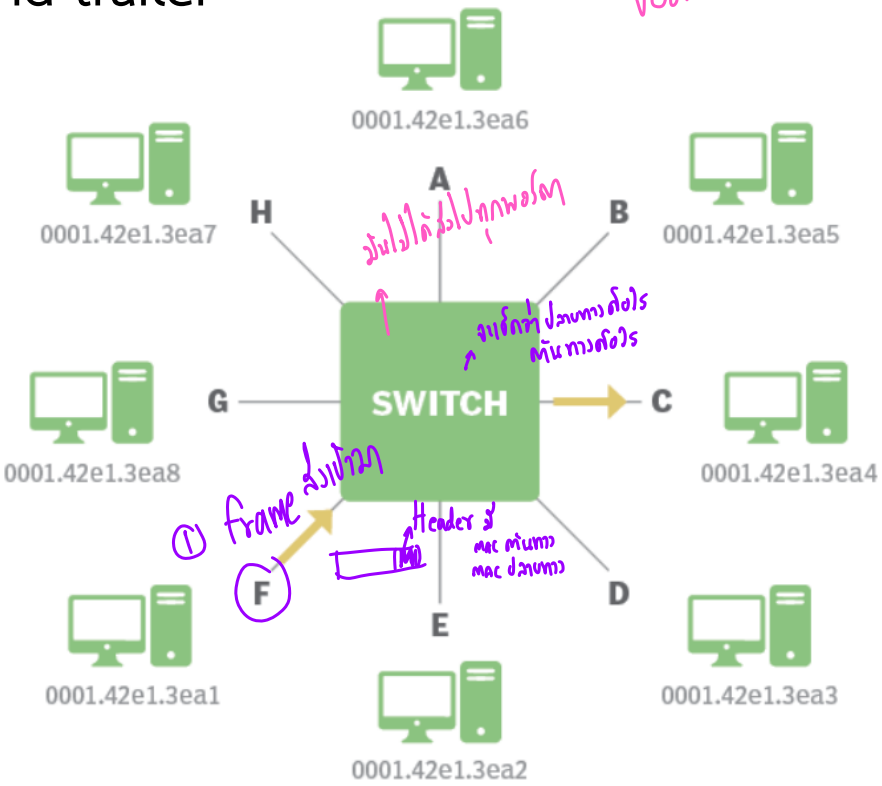


- If two or more devices transmitted a signal at the same instant, the electrical signal collides
  - Hub repeating both electrical signals out toward Larry on the left
- Hub floods each frame out all other ports (except the incoming port
  - Archie's frame goes to both Larry and Bob; Bob's frame goes to Larry and Archie

https://searchnetworking.techtarget.com/answer/Difference-between-a-router-switch-and-a-hub

To replace the hub with a LAN switch

- The switch operates as a Layer 2, meaning that it looks at the data-link header and trailer
  - MAC addresses



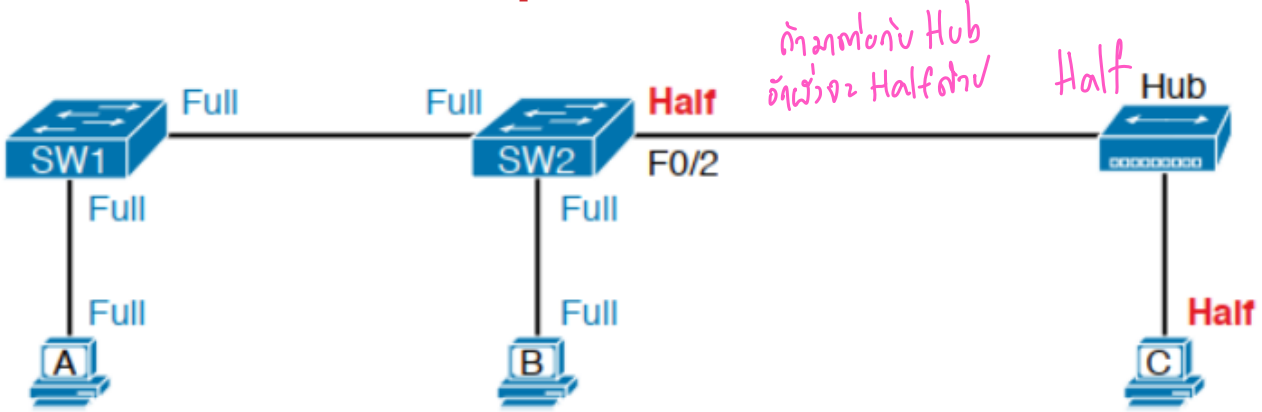
In this diagram of a **network switch**, the source, PC F - MAC 0001.42e1.3ea1, sends a packet to the destination, PC C - MAC 0001.42e1.3ea4. Only PC C receives the message because the switch has a table entry showing which port PC C is connected.

To replace the hub with a LAN switch

- However, the hub can prevent these collisions using half-duplex logic instead of full-duplex logic
  - half-duplex logic tells the nodes that if someone else is sending, wait before sending

- Example:
  - Archie began sending his frame early enough so that Bob received the first bits of that frame (from Archie)
    - Bob would notice that he was receiving a frame from someone else, and using half-duplex logic, would simply wait to send the frame
    - Nodes that use half-duplex logic actually use CSMA/CD

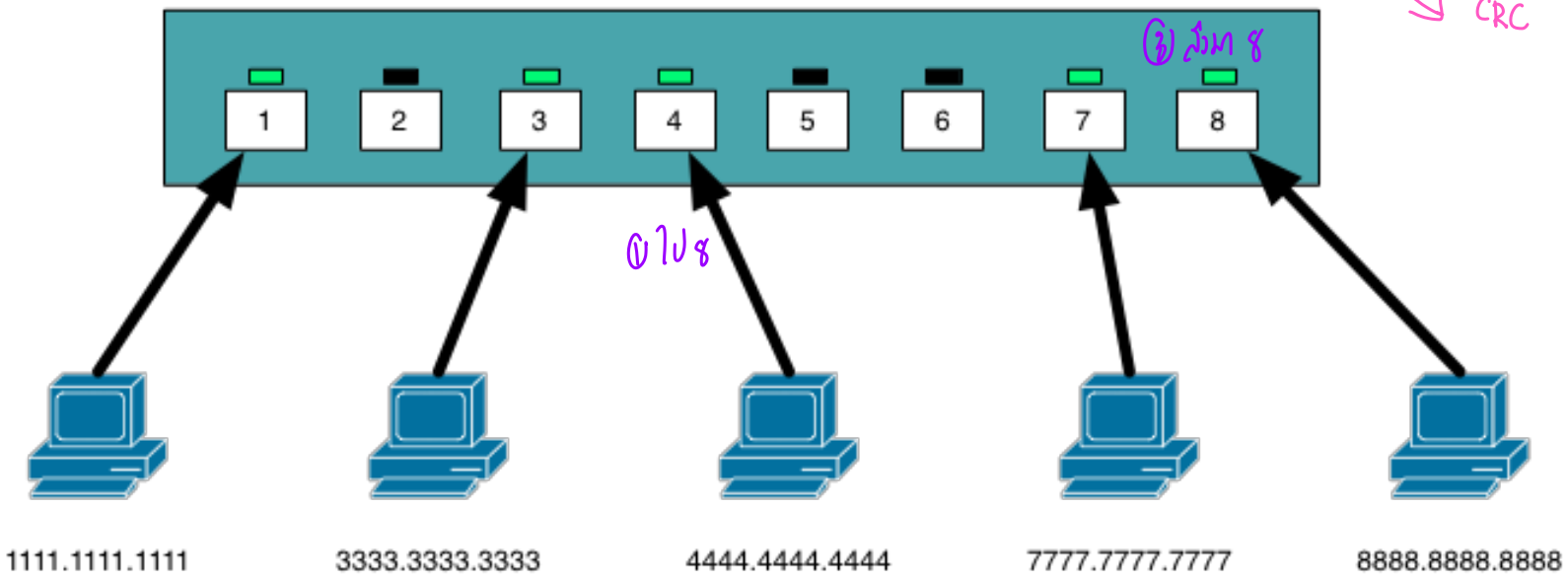
Full and Half Duplex in an Ethernet LAN



- Ethernet shared media (using hubs)
  - The devices connected to the hub share the network
    - They must use CSMA/CD
  - CSMA/CD enforces rules that allow only one device to successfully send a frame at any point in time

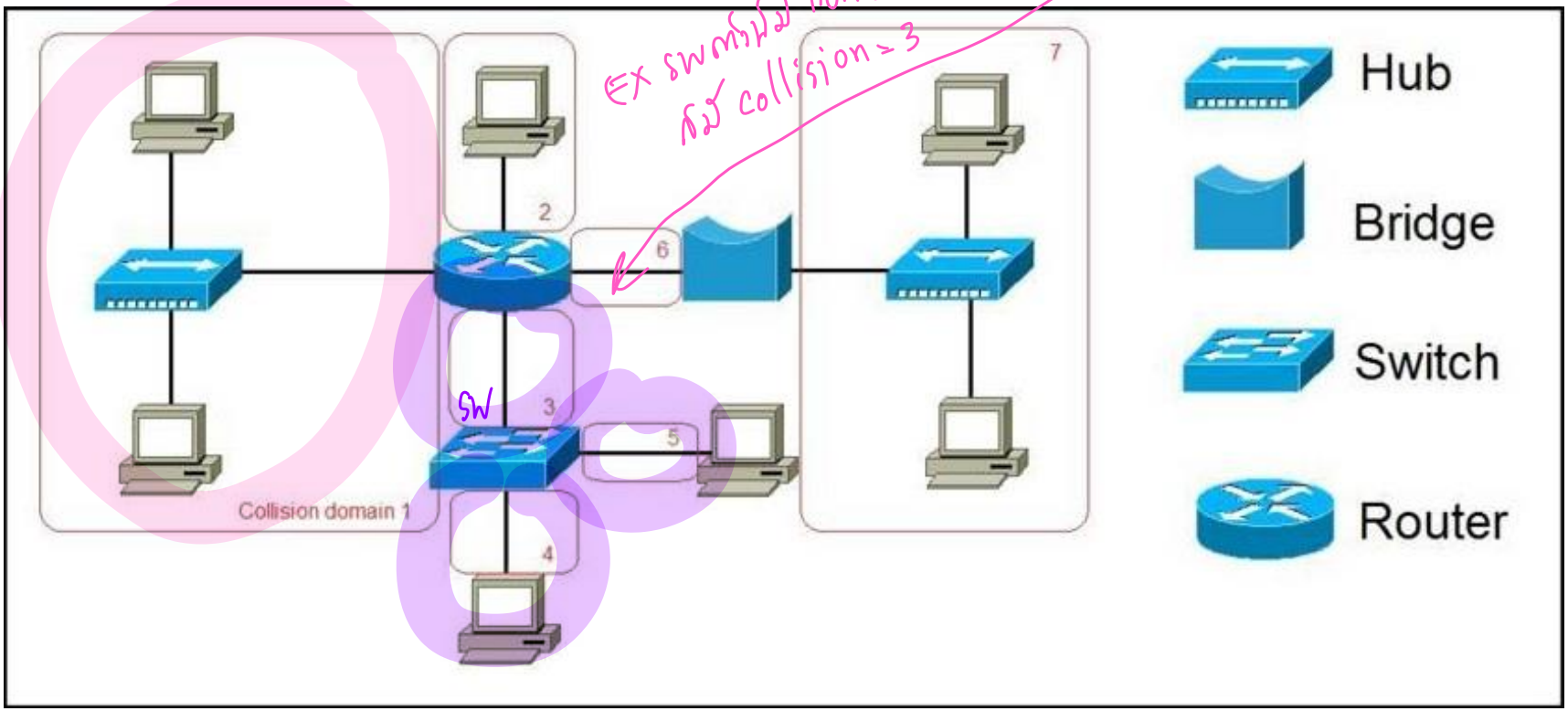
- Ethernet point-to-point (using switches)
  - Point-to-point link works independently of the others
  - Full-duplex logic, a frame can be sent on every point-to-point link in an Ethernet at the same time

Switching Table



Interface	MAC Address
Fa0/1	1111.1111.1111
Fa0/3	3333.3333.3333
Fa0/4	4444.4444.4444
Fa0/7	7777.7777.7777
Fa0/8	8888.8888.8888

Collision domain



https://geek-university.com/ccna/collision-domain-explained/

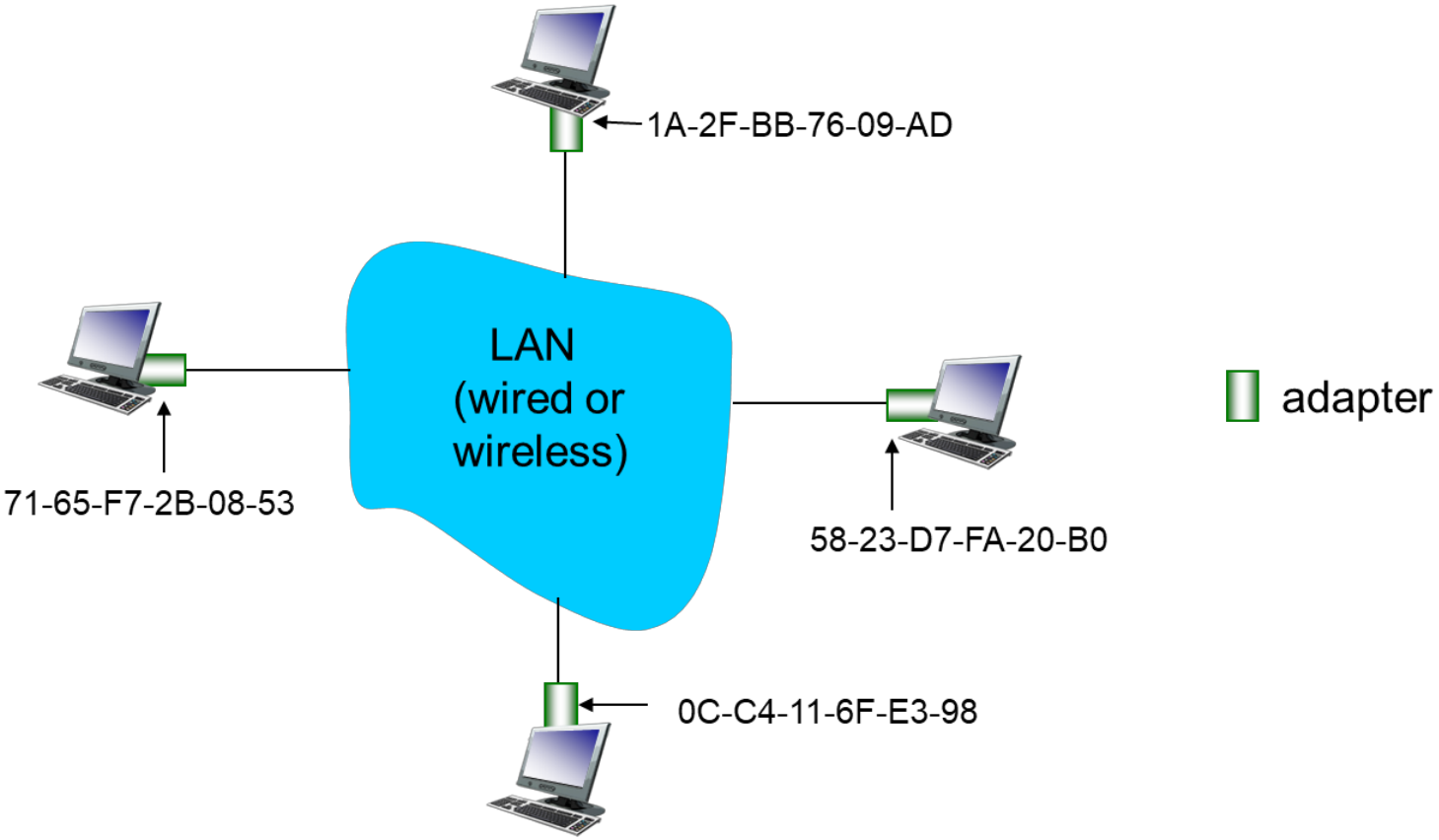
DataLink ↗ Node ที่เชื่อมกับ Link

↳ LAN → Ethernet LAN → MAC Address

Address Resolution Protocol (ARP)

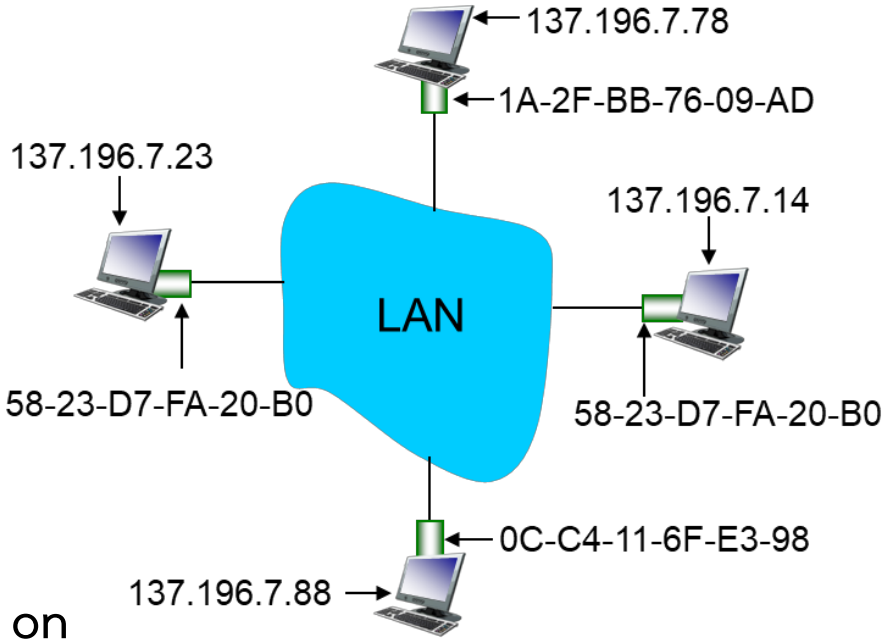
LAN addresses and ARP

- Each adapter on LAN has unique LAN address



ARP: Address Resolution Protocol

How to determine interface's MAC address, knowing its IP address?



- ARP table: each IP node (host, router) on LAN has table
  - IP/MAC address mappings for some LAN nodes:
    - < IP address; MAC address; TTL>
  - TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

- A wants to send datagram to B
  - B's MAC address not in A's ARP table.

I want to send to PC-B but I do not have the PC-B MAC address

Address Resolution Protocol

192.168.11.10

ขอ MAC Address ของ IP 192.168.11.11

192.168.11.1
CCCC.CCCC.CCCC

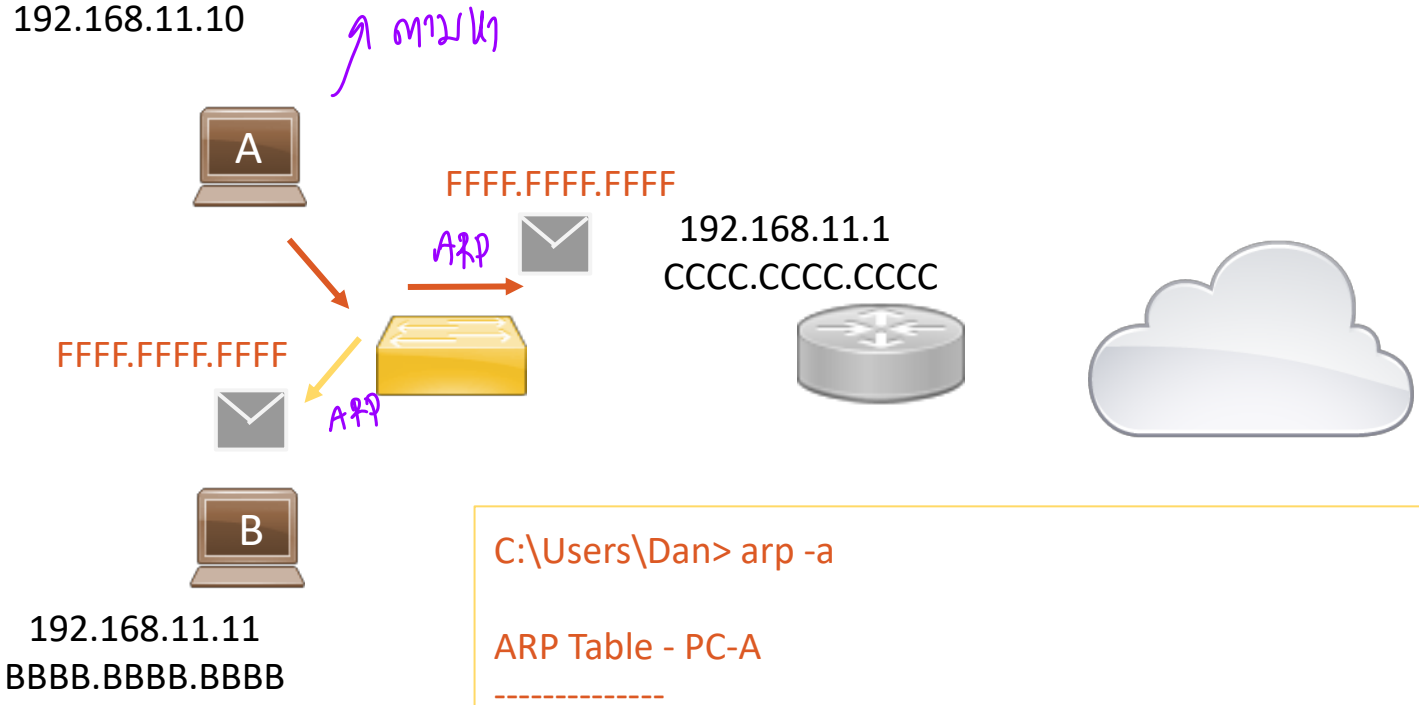
192.168.11.11
BBBB.BBBB.BBBB

```
C:\Users\Dan> arp -a

ARP Table - PC-A
-------------
??????????? ----------  ??????
??????????? ----------  ??????
```

- A broadcasts ARP query packet, containing B's IP address
  - destination MAC address = FF-FF-FF-FF-FF-FF
  - all nodes on LAN receive ARP query

Who has the MAC address
for 192.168.11.11? Tell 192.168.11.10

PC-A sends an ARP request



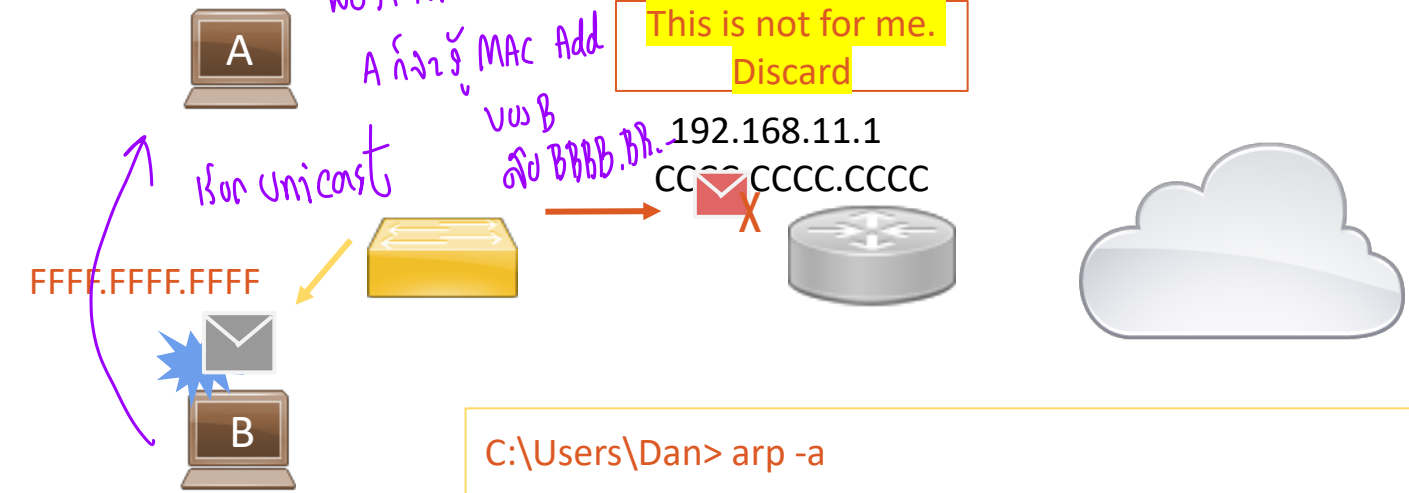

```
C:\Users\Dan> arp -a

ARP Table - PC-A
-------------
??????????? ----------  ??????
??????????? ----------  ??????
```

- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (unicast)

PC-B receives the ARP request

Who has the MAC address
for 192.168.11.11? Tell 192.168.11.10

192.168.11.10



192.168.11.11
BBBB.BBBB.BBBB

This is for me. I have it

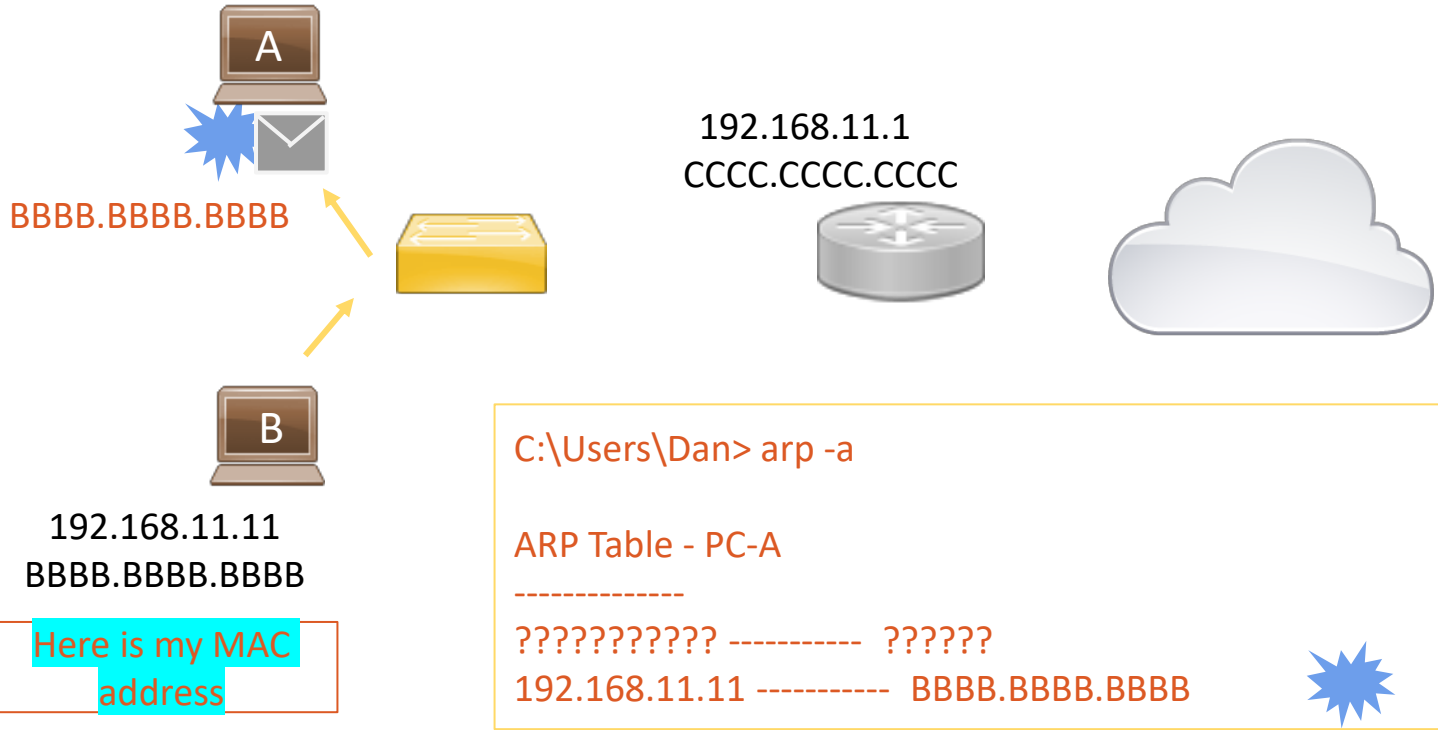
```
C:\Users\Dan> arp -a

ARP Table - PC-A
-------------
??????????? ----------  ??????
??????????? ----------  ??????
```

- B receives ARP packet, replies to A with its (B's) MAC address
  - frame sent to A's MAC address (unicast)

PC-B sends the ARP reply, and PC-A adds the MAC address to its ARP cache

I will add the MAC address to my ARP cache

192.168.11.10



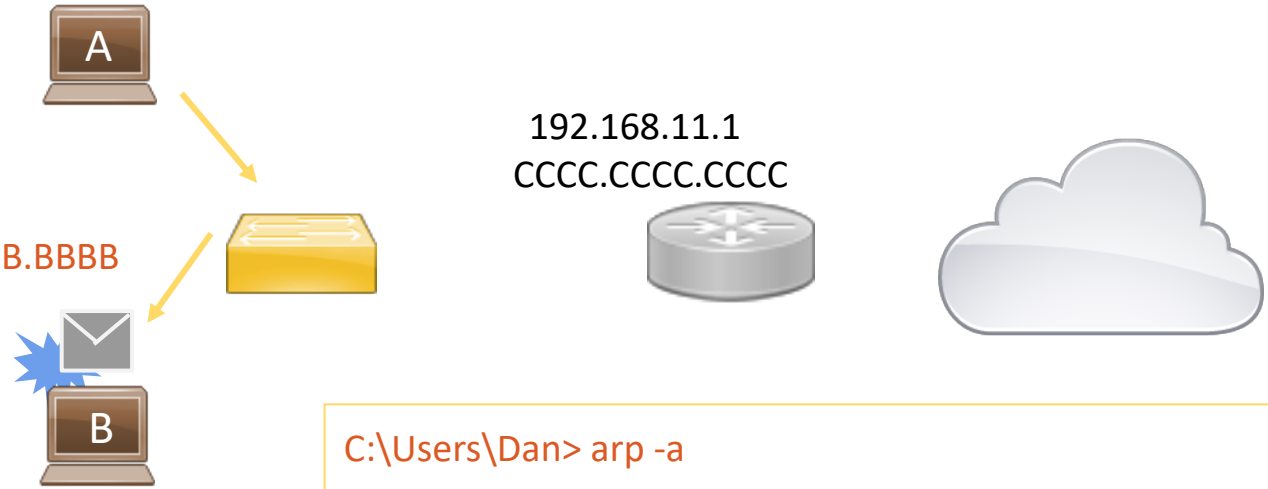

```
C:\Users\Dan> arp -a

ARP Table - PC-A
-------------
??????????? -----------  ??????
192.168.11.11 -----------  BBBB.BBBB.BBBB
```

- A caches (saves) IP-to-MAC pair in its ARP table until information becomes old (times out)
  - **soft state: information that times out (goes away) unless refreshed**

PC-A can now send to PC-B

Now I can deliver an Ethernet Frame to BBBB.BBBB.BBBB

192.168.11.10

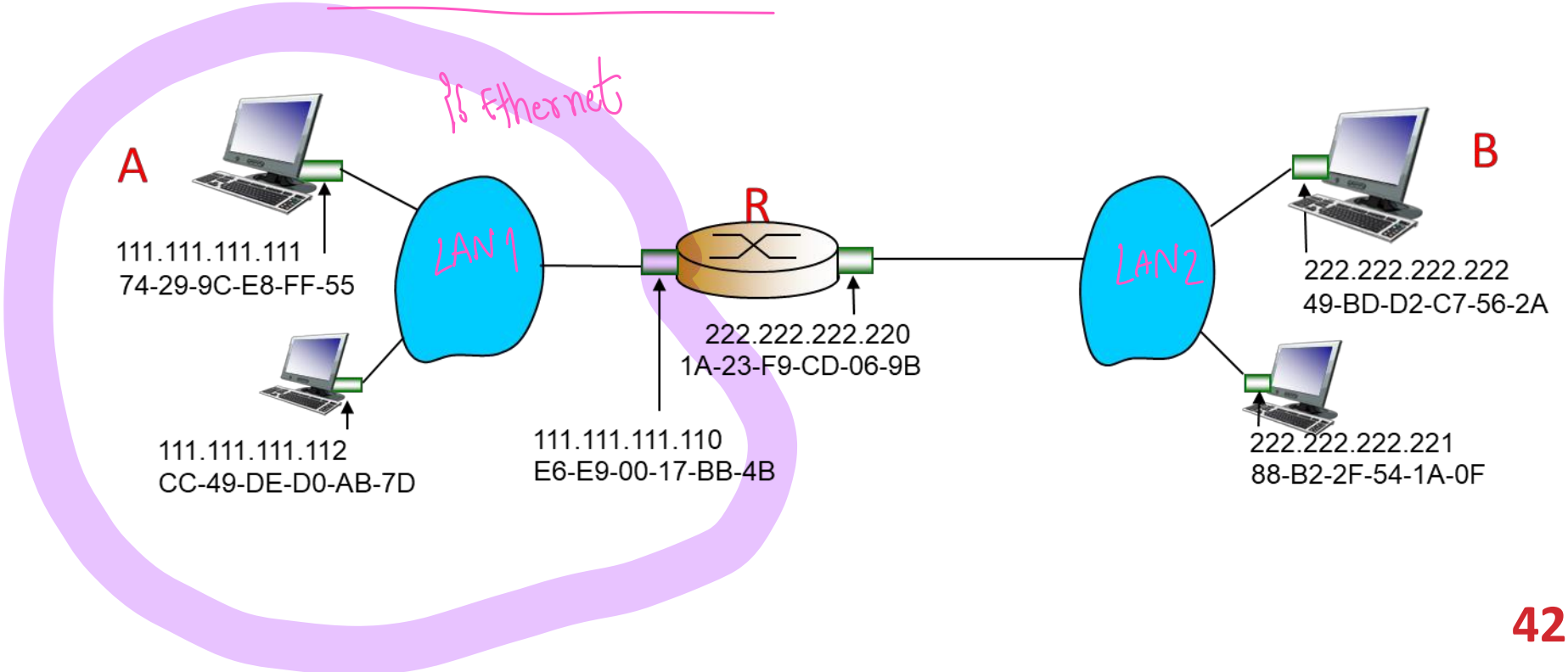


192.168.11.11
BBBB.BBBB.BBBB

```
C:\Users\Dan> arp -a

ARP Table - PC-A
-------------
192.168.11.1  ----------  ??????
192.168.11.11 ----------  BBBB.BBBB.BBBB
```

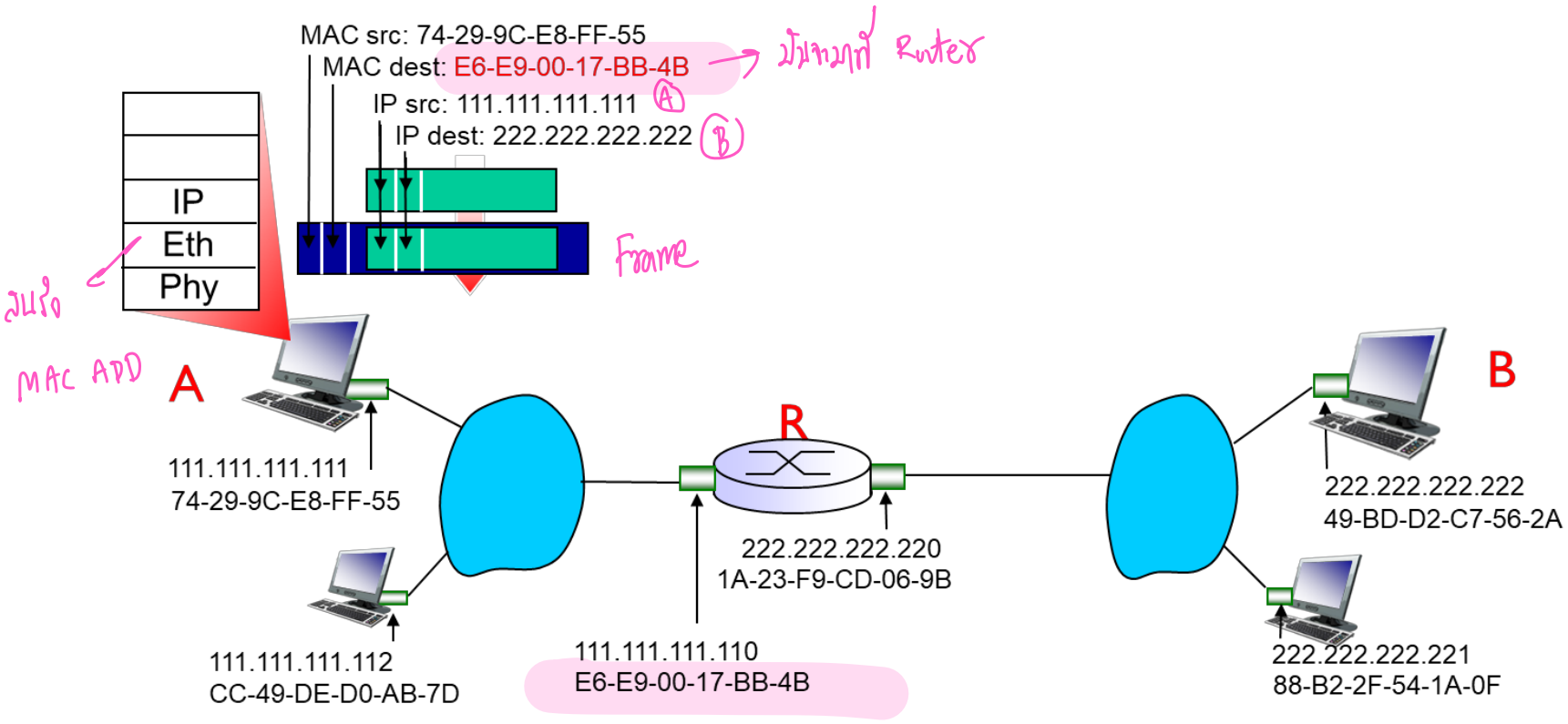
Addressing: Routing to another LAN

- Walkthrough: send datagram from A to B via R
  - focus on addressing – at IP (datagram) and MAC layer (frame)
  - assume A knows B's IP address
  - assume A knows IP address of first hop router, R (how?)
  - assume A knows R's MAC address (how?)



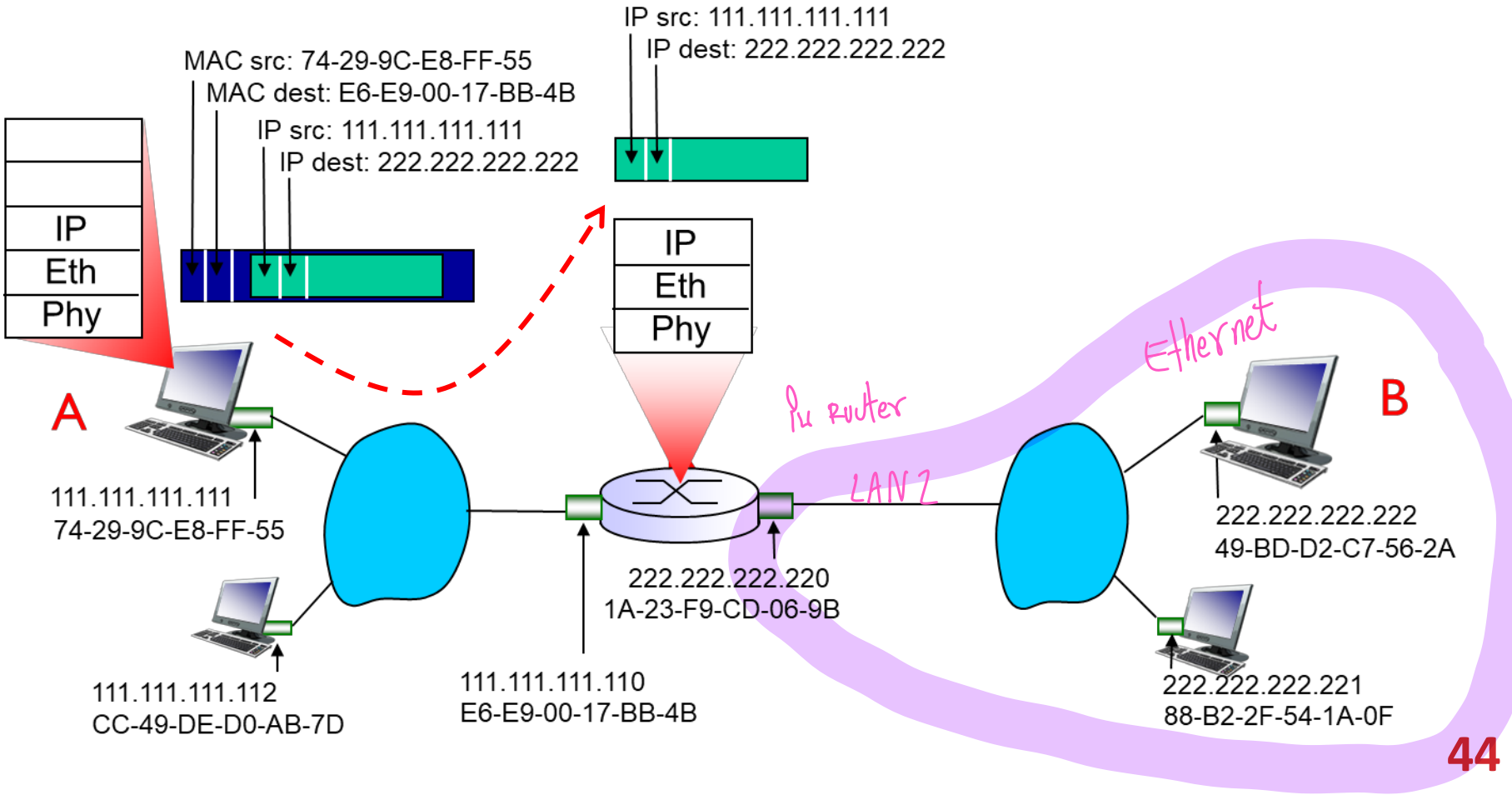
Addressing: Routing to another LAN

- A creates IP datagram with IP source A, destination B
- A creates link-layer frame with R's MAC address as destination address, frame contains A-to-B IP datagram



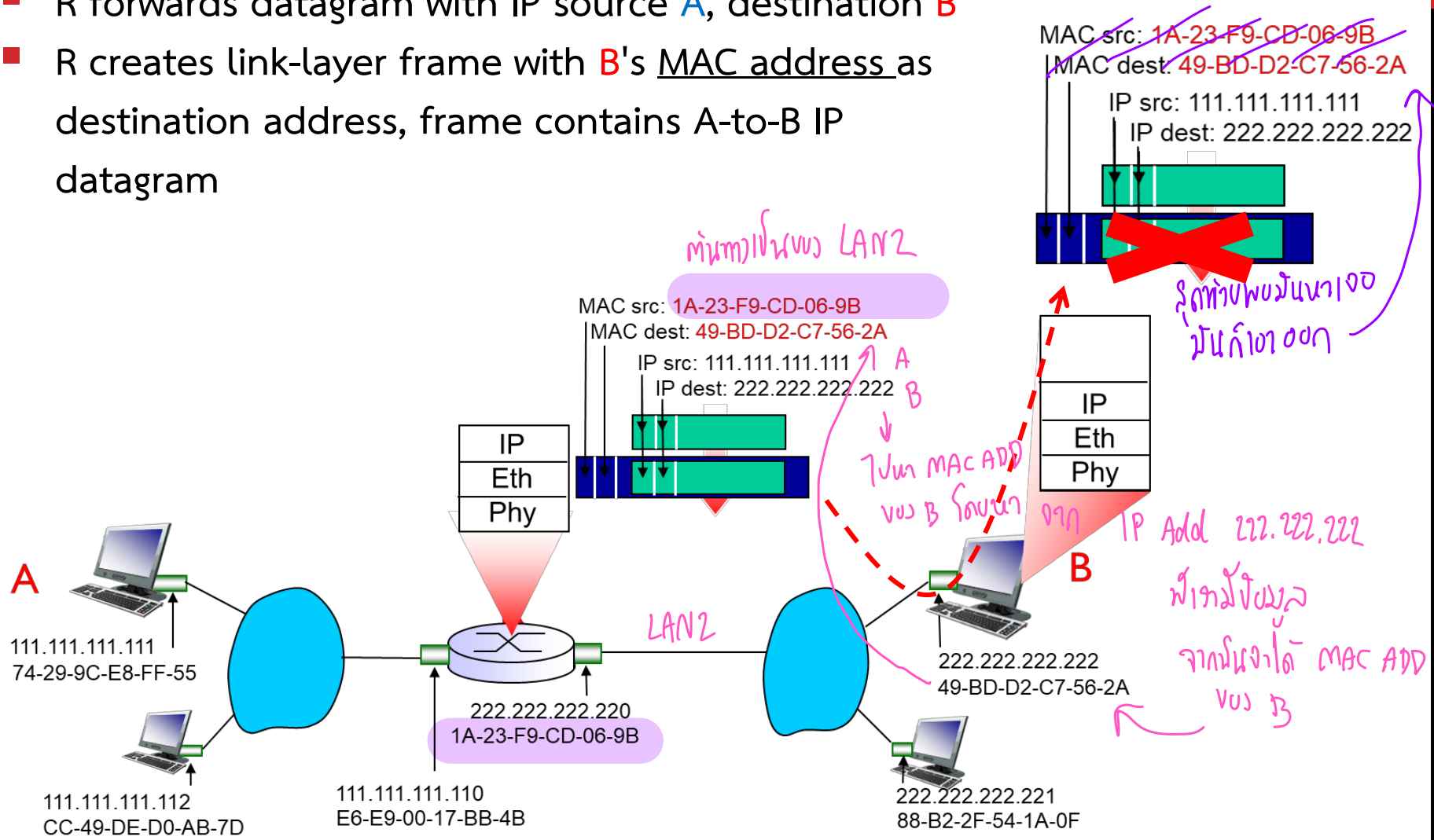
Addressing: routing to another LAN

- Frame sent from A to R
- Frame received at R, datagram removed, passed up to IP



Addressing: routing to another LAN

- R forwards datagram with IP source A, destination B
- R creates link-layer frame with B's MAC address as destination address, frame contains A-to-B IP datagram



Ethernet Virtual LANs (VLANs)

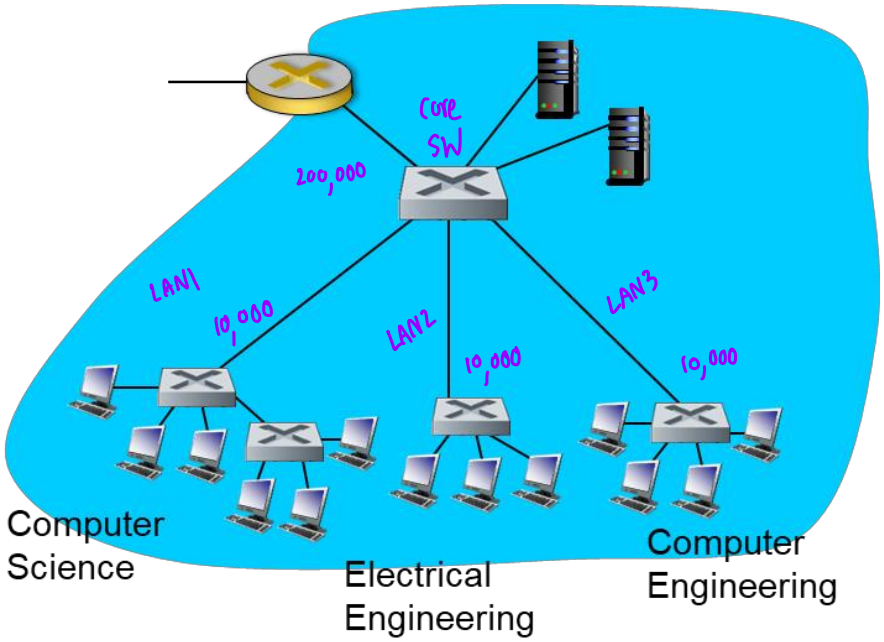
VLANs: motivation

Consider:

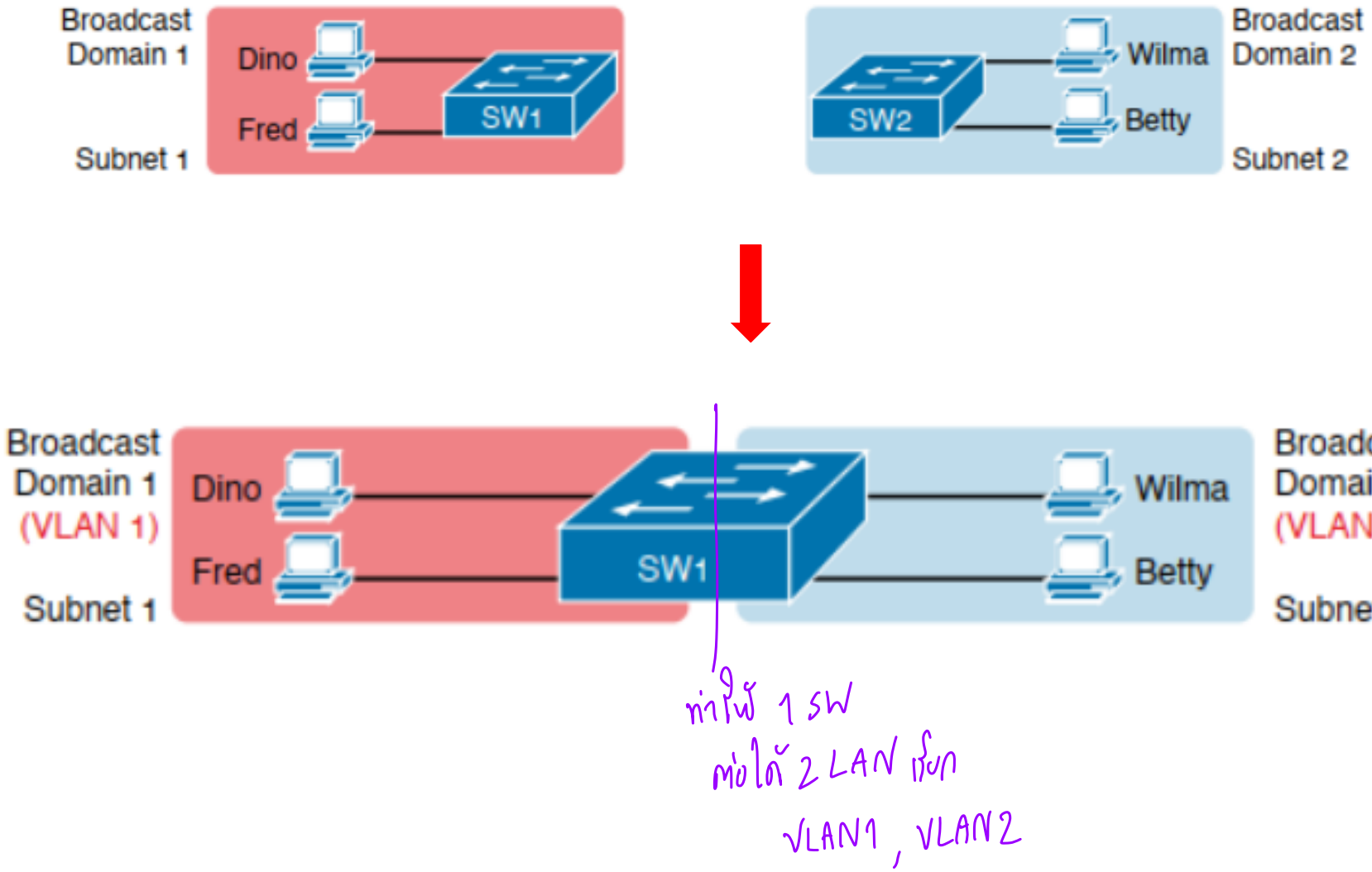
- CS user moves office to EE, but wants connect to CS switch?

subnet / industry

- Single broadcast domain:
  - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
  - security/privacy, efficiency issues



A switch using VLAN



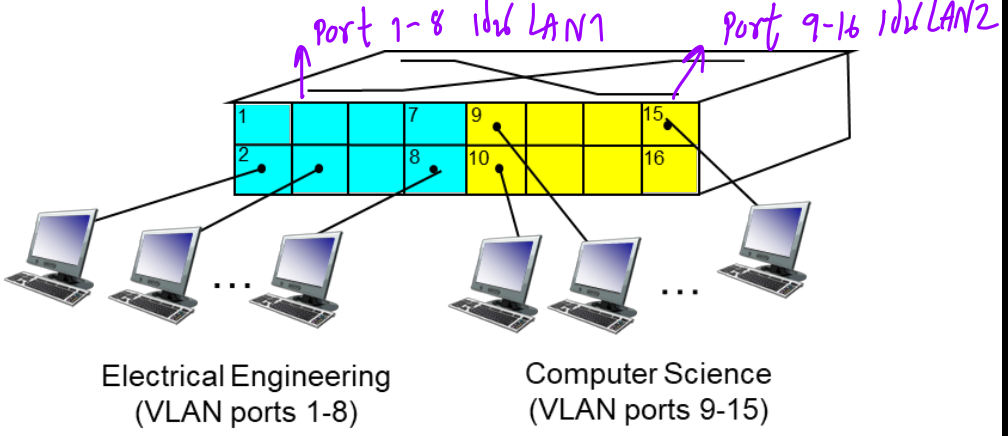
VLANs

Port-based VLAN:

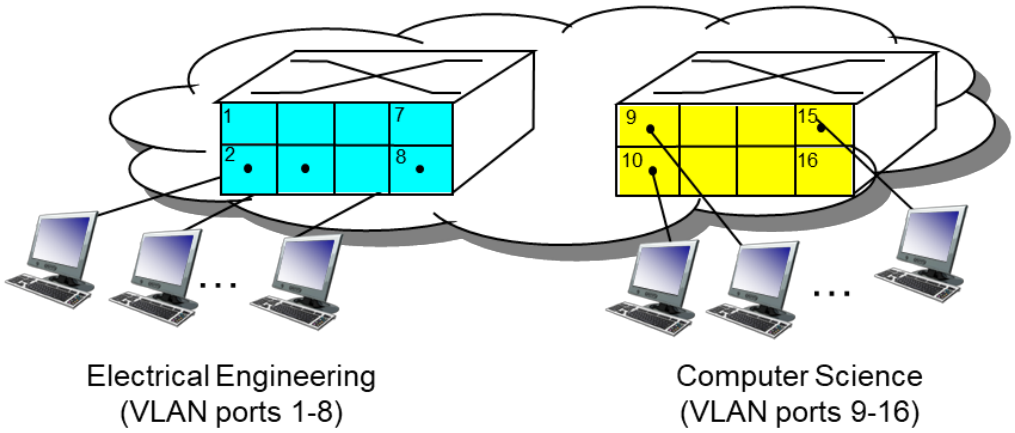
switch ports grouped (by switch management software) so that single physical switch .....

Virtual Local Area Network

Switch(es) supporting VLAN capabilities can be configured to define multiple *virtual* LANS over single physical LAN infrastructure.

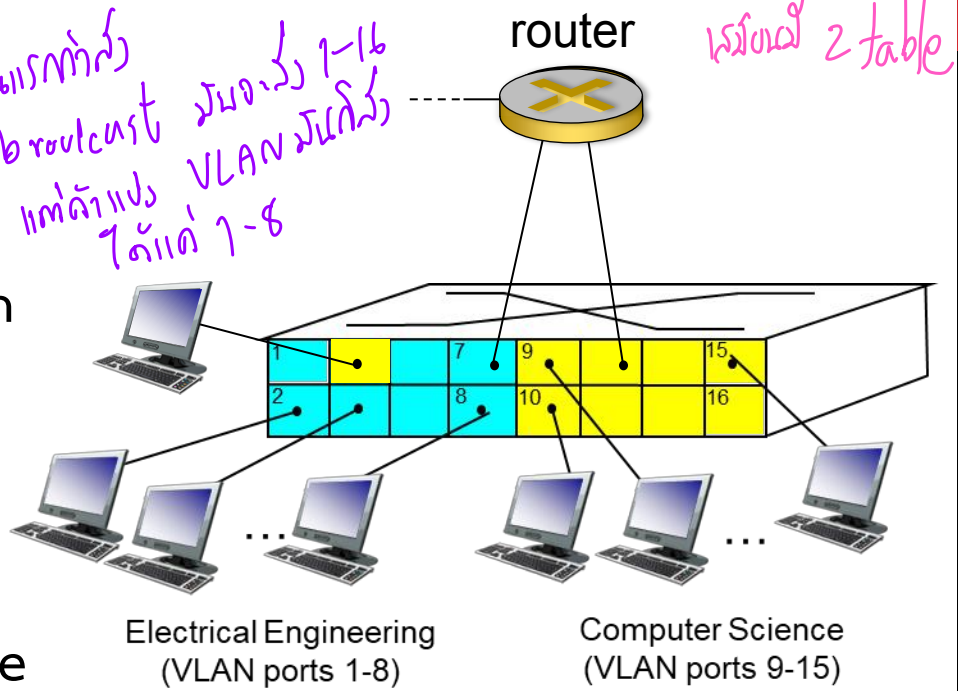


... operates as multiple virtual switches



Port-based VLAN

- Traffic isolation: frames to/from ports 1-8 can only reach ports 1-8
  - can also define VLAN based on MAC addresses of endpoints, rather than switch port



- Dynamic membership: ports can be dynamically assigned among VLANs

- Forwarding between VLANS: done via routing

Reference

- CCNA 200-301 Official Cert Guide, Volume 1 (2019)
  - By Wendell Odom
- Computer Networking Problems and Solutions (2017)
  - By Russ, Ethan Banks
- Computer Networking: A Top-Down Approach, Global Edition (2016)
  - By Keith Ross James Kurose

นางสาวนัฐชยา ผ่องกุศล B6226718

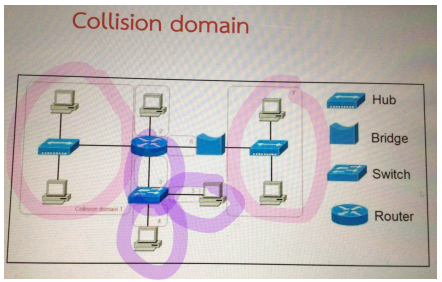
Classwork 3: Ethernet LANs - Part1 (ส่งเป็น PDF ไฟล์)

1. Collision domain ระหว่าง Hub และ Switch แตกต่างอย่างไร

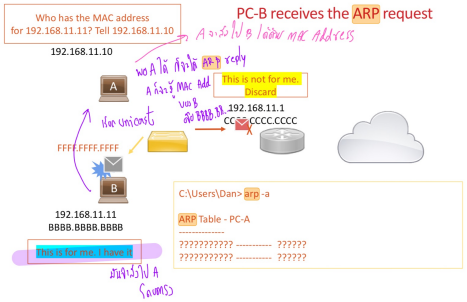
2. ARP ถูกใช้เพื่อจุดประสงค์ใด

3. Switch ที่ใช้ VLAN มีความแตกต่างอย่างไรจาก Switch ที่ไม่ใช้ VLAN

1. ของเขตที่ต่อกับ Hub มีโอกาสชนกันได้ แต่ switch จะมี collision domain ขึ้นอยู่กับ port ของ switch



2. ใช้หา MAC Address โดยมาจาก IP Address ที่เรารู้



3. Switch ที่ใช้ VLAN จะสามารถแบ่ง port ได้ คือ 1 switch มี 2 LAN ได้ เมื่อเรียกใช้ Broadcast ปกติจะส่งข้อมูลนั้นทั้งหมด แต่เมื่อใช้ VLAN ก็จะส่งข้อมูลเฉพาะของเขต port นั้นๆ