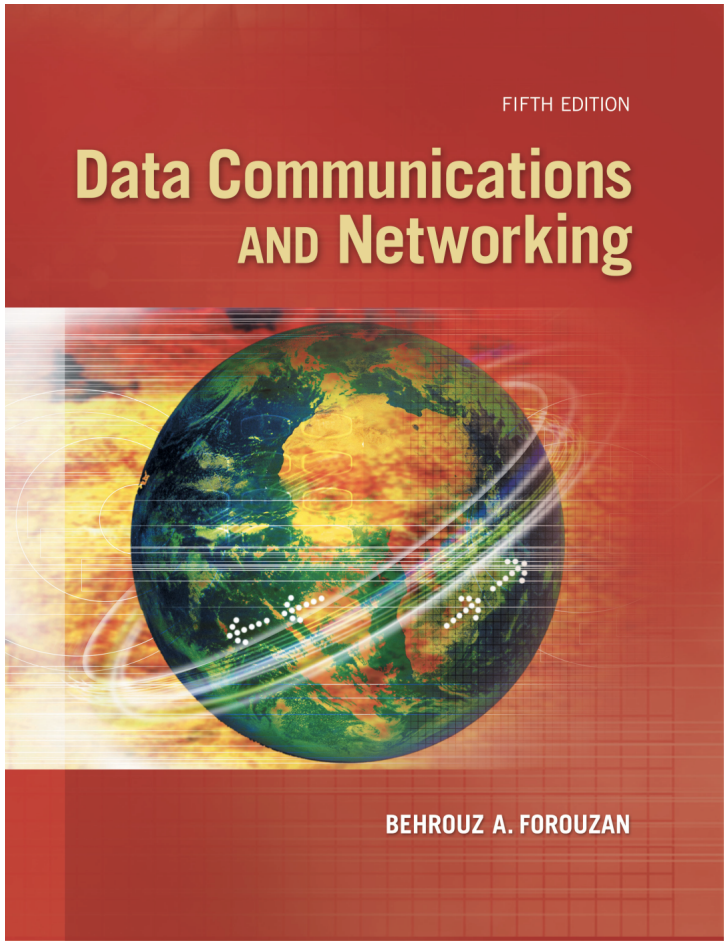
University of Human Development
College of Science and Technology
Department of Information Technology

Chapter 17

Data Communications and Networking

Network Connecting Devices



Course Administration and Policies

- You have to contact me through UHD email!
- dana.abd@uhd.edu.iq
- I will not respond you on social media!
- Put "Computer Network" in subject title when you send me emails.
- Course Notes (Class Slides), Labs and Solutions, Question Bank, Course Book and all other martials are available on the website at:

https://sites.google.com/a/uhd.edu.iq/dana-abd/home

Course Administration and Policies (cont.)

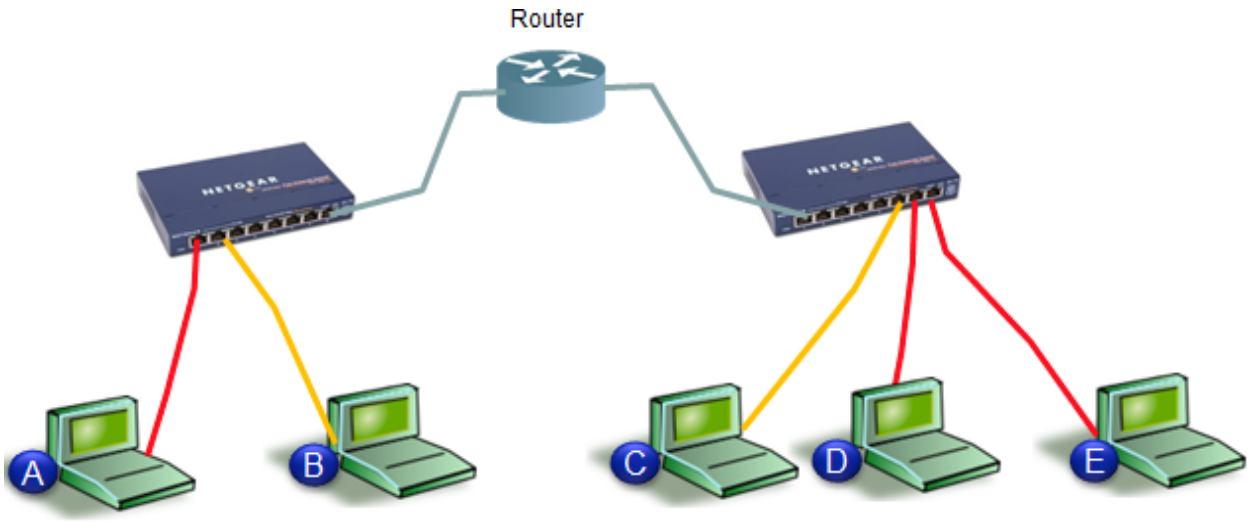
- During live class, please:
  - No speak with classmate
  - You have quiz every week (**TH+P**) if you do not have paper and pen I will get you out
  - If you have questions please raise your hand
  - Not get out during class
  - Turn off mobile devices
  - Be in class before I come to class if you late more than 10 minutes please do not come in class
  - Lecture break is 10 Minutes, more late do not come in
  - Group change or need permission will be done by head of department.

Grading

- **Grade Components:**
- **50% Pre-final and Quizes**
  - 20% - Theory Exam
  - 15% - Practical Exam
  - 10% - Mini-Exam (Quiz), every week
  - 5% - Presentation (By Group)
- **50% Final Exam**
  - 30% - Theory Exam
  - 20% - Practical Exam

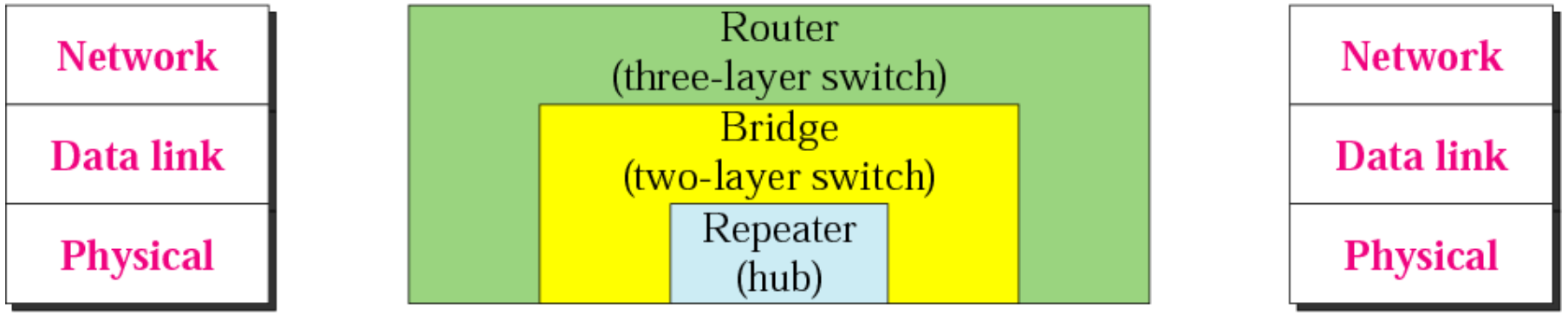
Networking Devices

- Hosts or LANs do not normally operate in isolation. They are connected to one another or to the Internet.
- To connect hosts or LANs, we use connecting devices.
- Connecting devices can operate in different layers of the Internet model.
  - It first describes hubs, Repeater and their features. The section then discusses link-layer switches, and Router.



Networking Devices

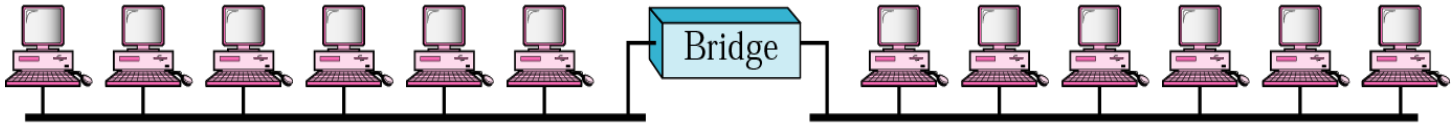
- Connecting devices
  - ***Repeaters*** (layer 1)
  - ***Hubs*** (layer 1)
  - ***Bridges*** (layer 2)
  - ***Switches*** (layer 2)
  - ***Routers*** (layer 3)



Networking Devices Repeaters

- **LAN segment** is a portion of a LAN to extend length/reach
- **LAN Repeaters** connect LAN segments
  - Two ports
  - Physical layer device
  - LAN segments must be of same type

a. Without bridging

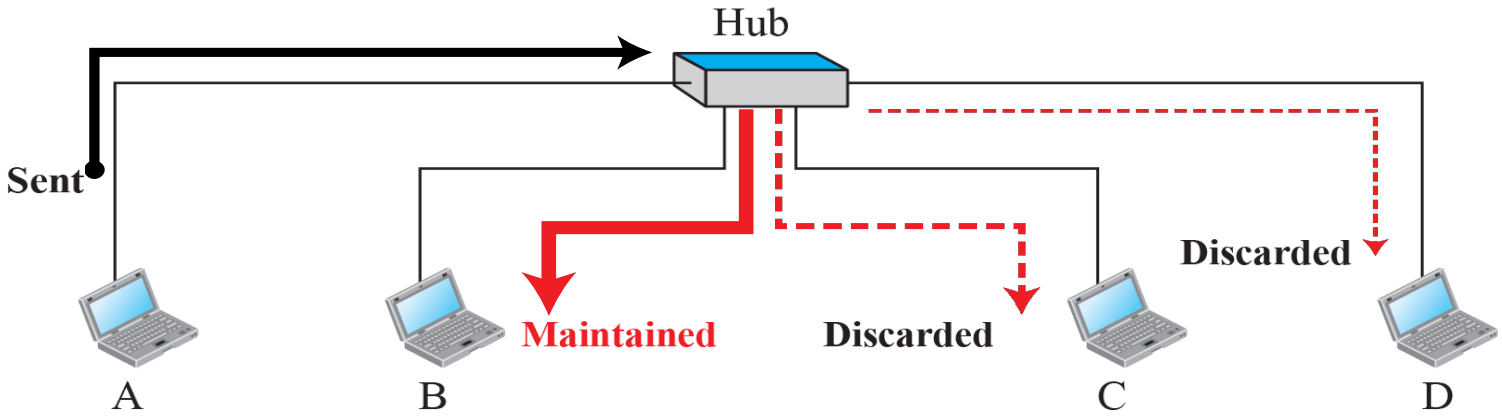


b. With bridging

Networking Devices Hubs

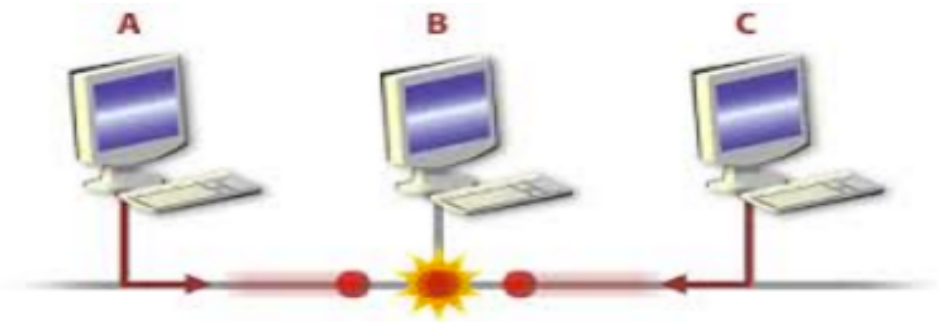
- **Hub** is a multi-port repeater
- Hubs connect more than two LAN segments
  - > than two ports
  - Physical layer device
  - LAN segments must be of same type
  - Operates in one ***collision domain***

A repeater and hub forwards every bit out of all ports; it has no filtering



LAN Networking Devices Collision Domains

- All devices connected to a Hub (or Hub network) are in the same ***collision domain***
- A ***collision domain*** is a set of LAN devices/hosts whose frames could collide with one another due to the broadcast based network topology
- Ethernet *collision domains* require *CSMA/CD* as the MAC protocol
- Ethernet *collision domains* operate at half duplex



LAN Networking Devices Bridge

- ***Bridge* = *repeater* + *2nd layer filter***
- ***2nd layer filter*** is able to read MAC addresses and decide if the frame should be forwarded or dropped based on entries in the ***MAC forwarding table***
  - ***MAC forwarding table*** associates port interface with host MAC address(es)
- Bridges can connect one LAN type to another
- Bridges separate *collision domains*
  - Improves the network bandwidth
  - Allows more hosts to be added to the LAN due to filtering

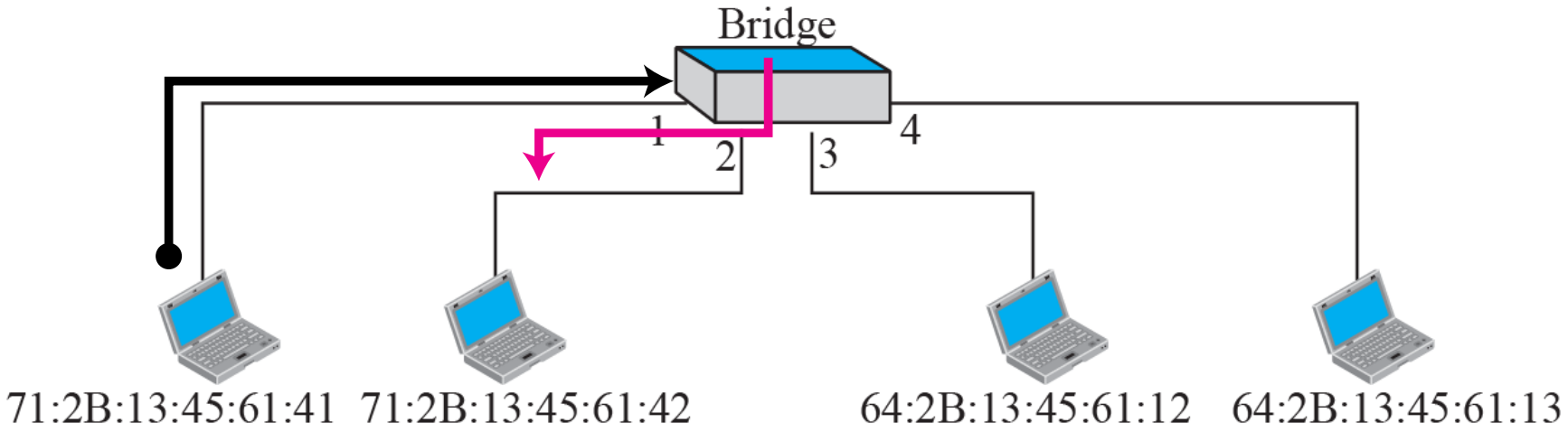
a. Without bridging

b. With bridging

LAN Networking Devices Bridge

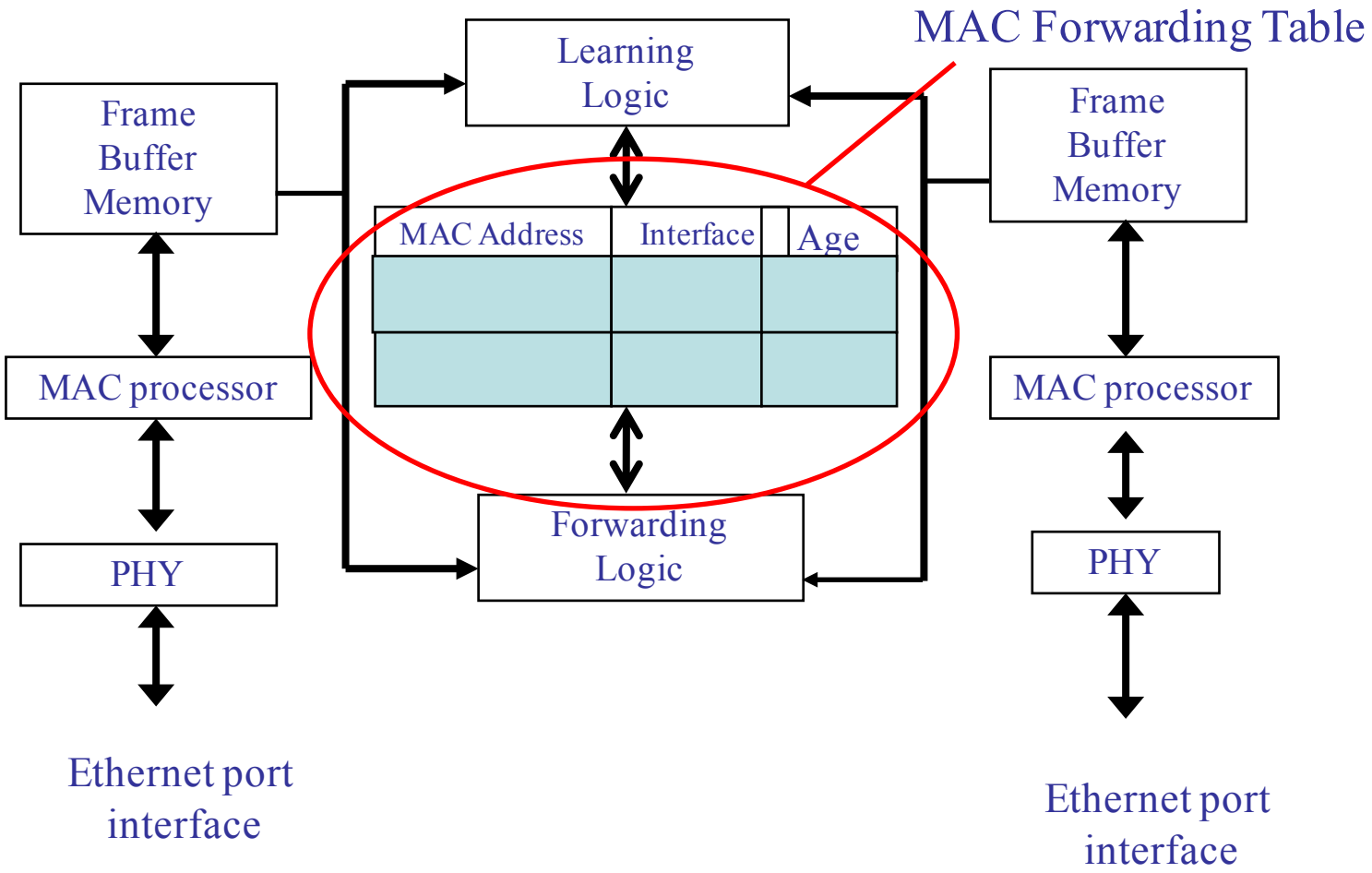
Bridge table

Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	2
64:2B:13:45:61:12	3
64:2B:13:45:61:13	4



LAN Bridge Functional Block Diagram

A bridge has a table used in filtering decisions



A bridge does not change the physical (MAC) addresses in a frame.

Principles of Bridging (Switching)

- ***Bridging*** (aka ***switching***) must at a minimum perform the following
  1. ***forward frames*** to a physical port based on MAC forwarding table
  2. ***Learning*** to update MAC Forwarding table
  3. prevent ***switching loops***

Switches vs. Hubs

- Switches vs. Hubs
  - How is Switch different than a Hub?
    - Broadcasting (and Security)
      - Hub broadcasts every packet to every device
      - Switch forwards packet out single port
    - Matching Data Rates
      - All ports on hub must run at same data rate
      - Switch ports can run at different rates (can buffer incoming packet at one data rate and re-transmit at another data rate).

Routers

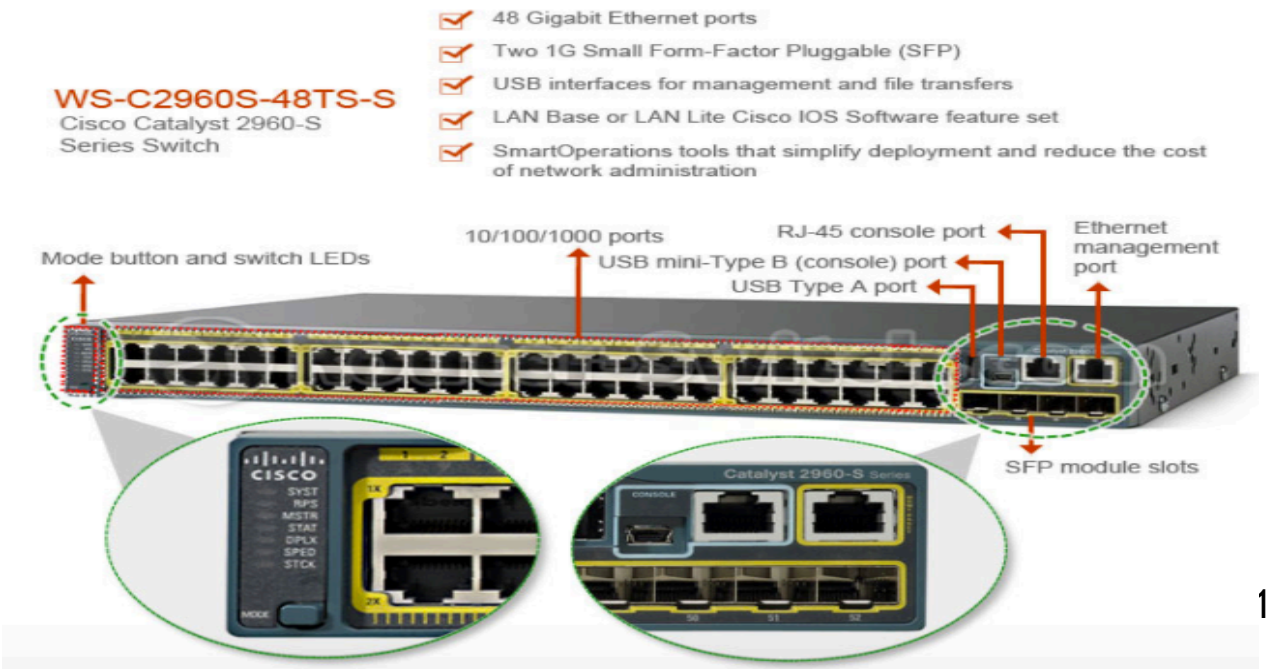
- Routers
  - The device that connects a LAN to a WAN or a WAN to a WAN.
  - A router accepts an outgoing packet, removes any LAN headers and trailers, and encapsulates the necessary WAN headers and trailers.
  - Because a router has to make wide area network routing decisions, the router has to dig down into the network layer of the packet to retrieve the network destination address.
  - ***A router is a three-layer (physical, data link, and network) device.***
  - ***A router changes the physical addresses in a packet and the CRC.***

Routers

- Routers (cont.)
  - Thus, routers are often called “layer 3 devices”. They operate at the third layer of TCP/IP model.
  - Thus, each time they receive a packet, they strip off the “layer 2” header (such as Ethernet), and then create a new “layer 2” header for the next hop to the next router (or destination).
  - Routers often incorporate firewall functions.

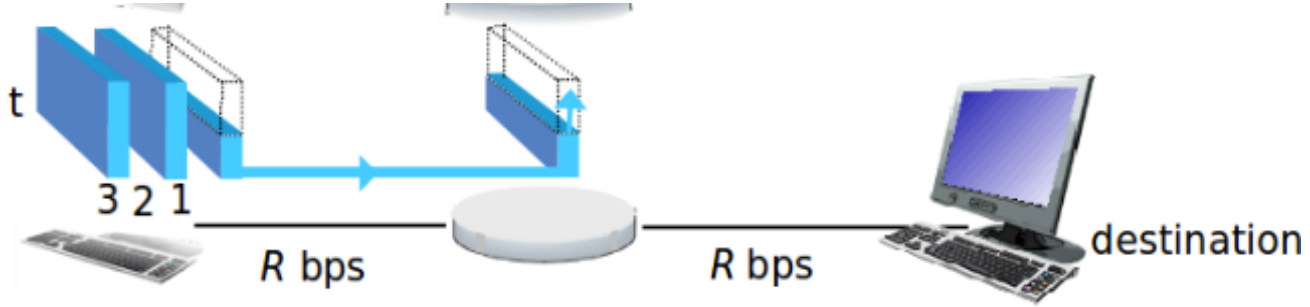
Routers v.s Switches

- Switches vs. Routers
  - How is Switch different than a Router?
    - Addressing
    - Switch uses layer 2 MAC addresses
    - Router uses layer 3 IP address
    - Speed & security
    - Switch forwards packets fast (~50-100 nsec).
    - Router takes more time (~1-50 msec) and provides other security features



2nd Layer Forwarding Methods

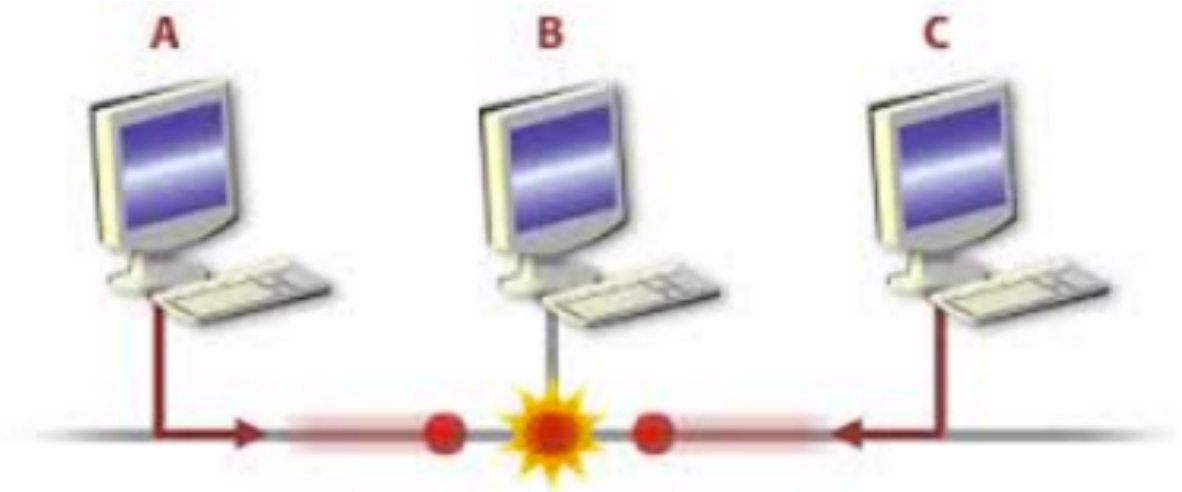
- Two general forwarding methods can be used in a switch/bridge
  - ***Store and forward switching***. Each inbound frame is completely buffered and then forwarded to the output port specified by the MAC table.
    - Error detection is performed.
    - If the frame has errors, it is dropped.



  - ***Cut-through switching***. Each inbound frame's header is buffered just enough to read the destination MAC address and then forwarded to the output port specified by the MAC table.
    - No error detection or frame size checking is performed
    - Fast processing

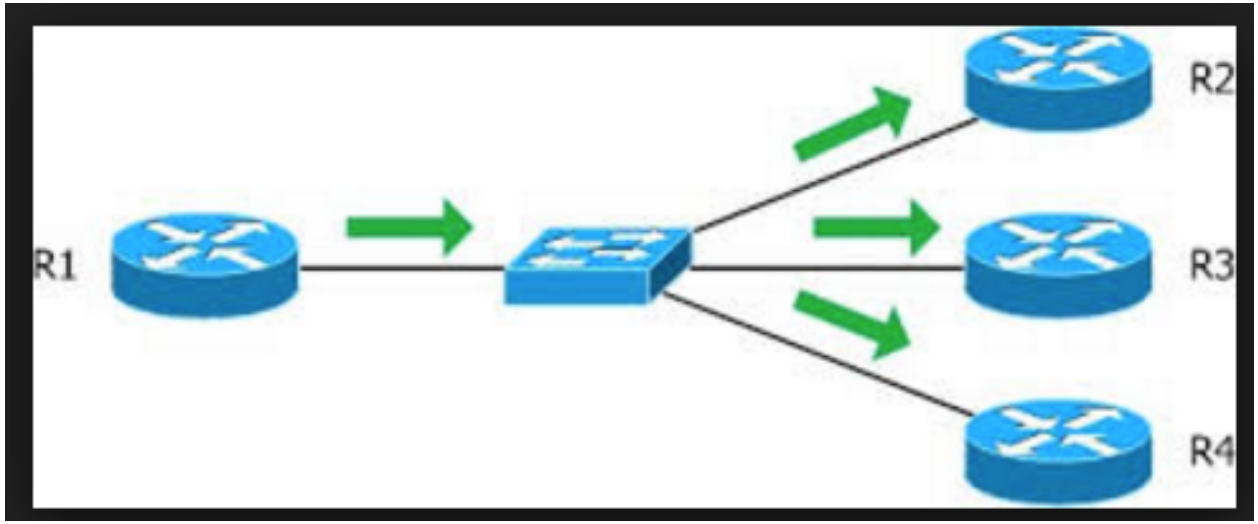
Collision Domain

- A collision domain is simply defined as any physical segment where a collision can occur.
  - Remember, if *any* two devices connected to a hub send a frame simultaneously, a collision *will* occur.
  - Thus, all ports on a hub belong to the same **collision domain**.



broadcast domain

- A broadcast domain is a logical segmentation of a network, dictating how far a broadcast frame can propagate.
  - Only a Layer-3 device, such as a router, can separate broadcast domains.
  - Both switches and hubs are belongs to only *one* **broadcast domain.**

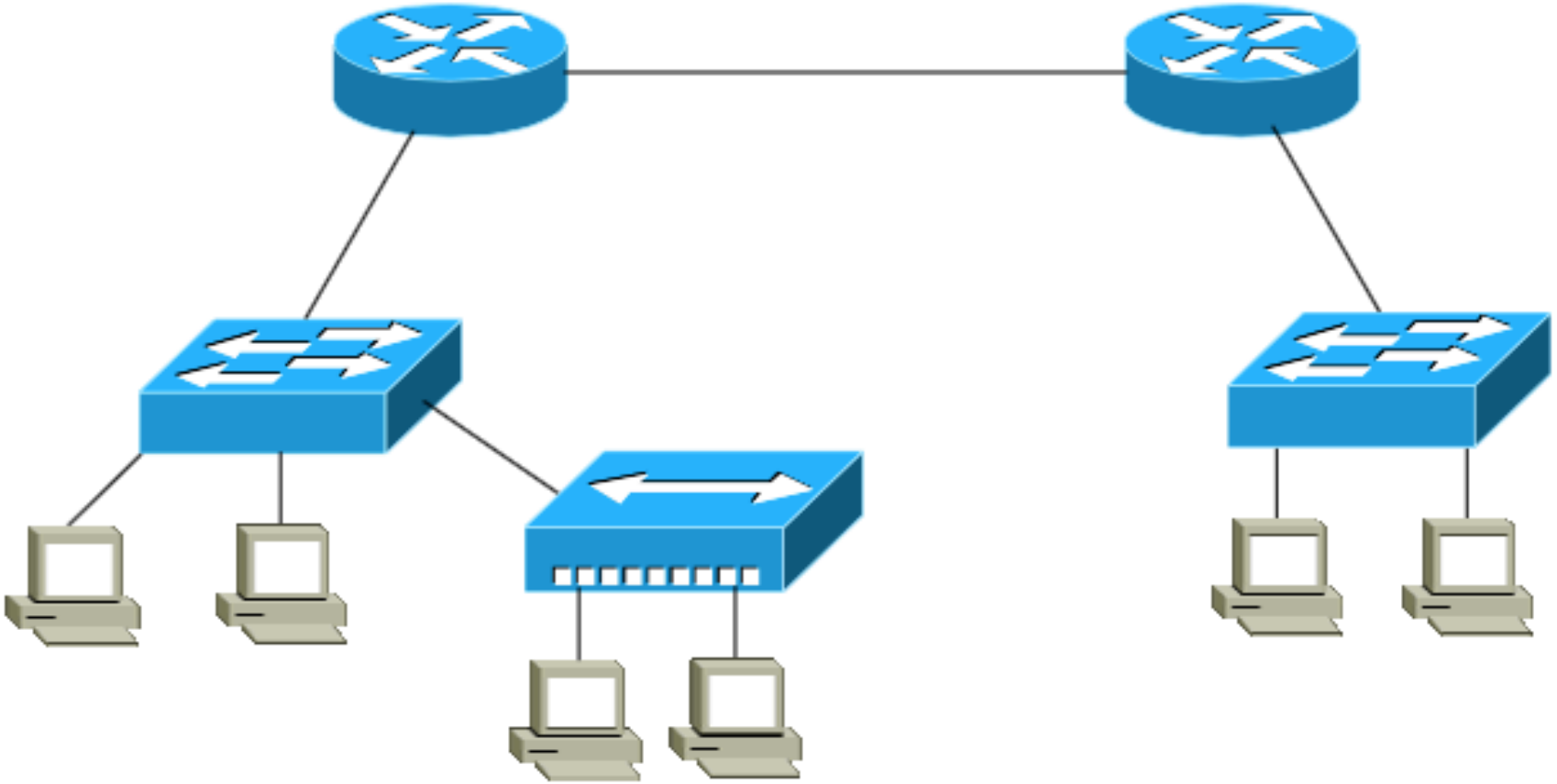


collision domain vs broadcast domain

- Remember that:
  - Routers separate *broadcast* and *collision* domains.
  - Each Routers interface is one *broadcast* domain and one *collision* domain.
  - Switches separate *collision* domains.
  - Each Switches interface is one *collision* domain.
  - Hubs belong to only one *collision* domain.
  - Switches and hubs both only belong to one *broadcast* domain.

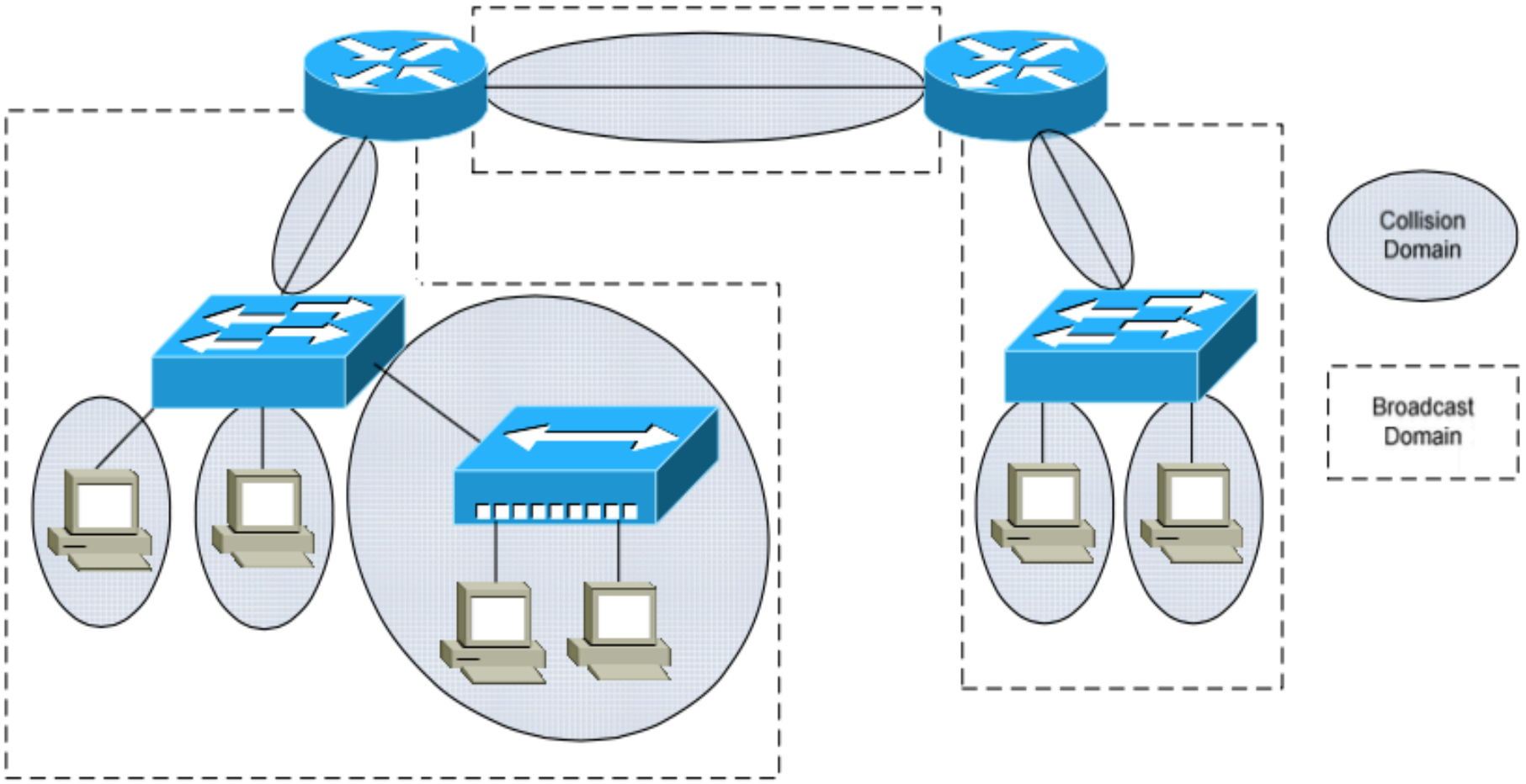
collision domain vs broadcast domain

Collision vs. Broadcast Domain Example

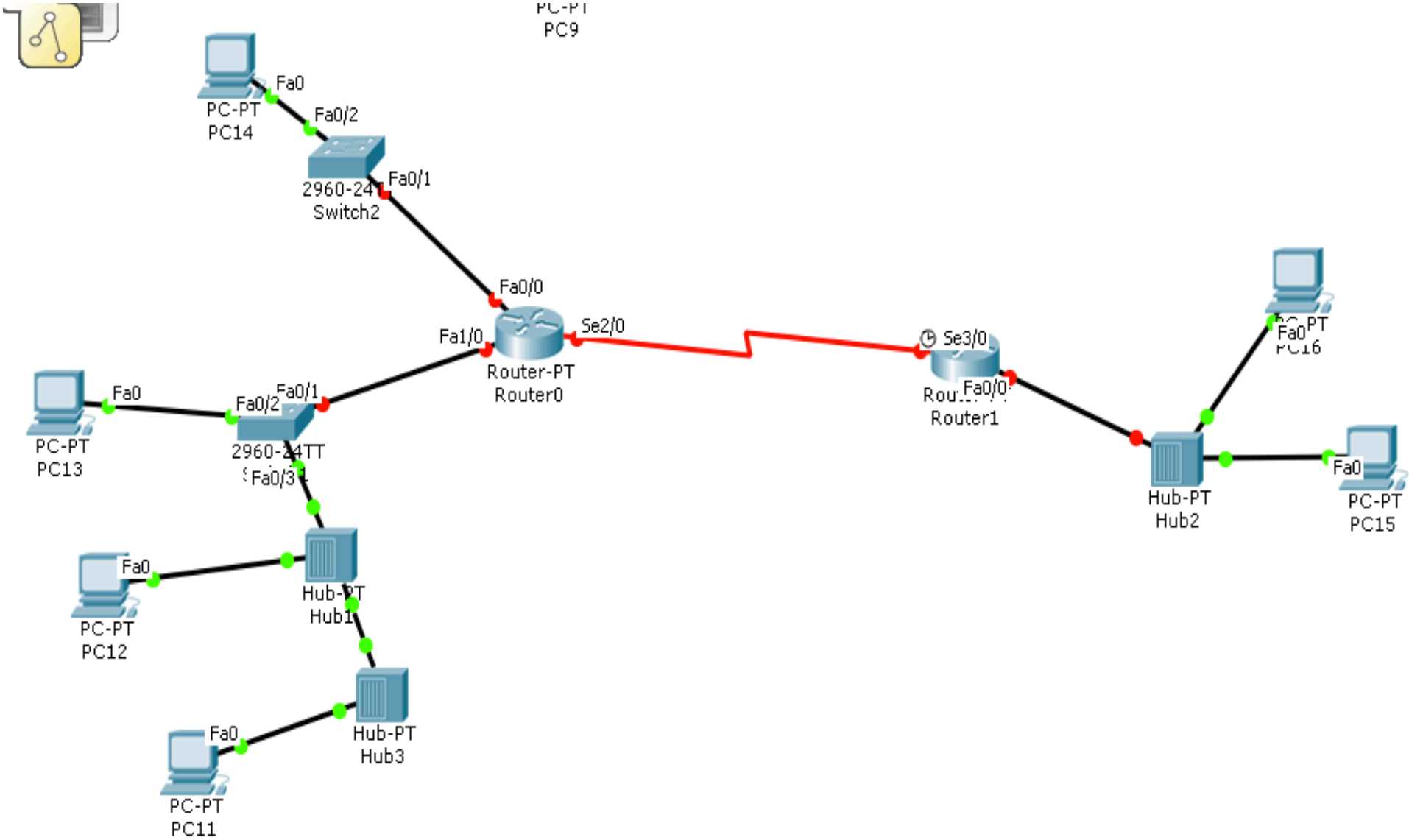


collision domain vs broadcast domain

In the above example, there are **THREE** broadcast domains, and **EIGHT** collision domains:



collision domain vs broadcast domain



MAC Address Learning Principles

- MAC forwarding table address entries are ***learned*** by monitoring source MAC addresses received at ingress (aka input) ports
  - MAC address ***learning*** populates the ***MAC forwarding table***

- MAC forwarding table entries are expired (aka removed) when frames from a source MAC address associated with an ingress port are not received within an ***aging time*** (aka "aged out")
  - Adapts to the mobility of end users
  - Default ***aging time*** = 5 minutes

- MAC address *learning* "stops" at the router interface
  - Ethernet switch does not learn the MAC addresses at the other side of the router
  - Ethernet switch learns one MAC address of the router that is directly connected to the switch's broadcast domain

Ethernet Flooding Principles

- How does the switch forward an ingress frame that has a Destination Address (DA) with no MAC forwarding table entry?

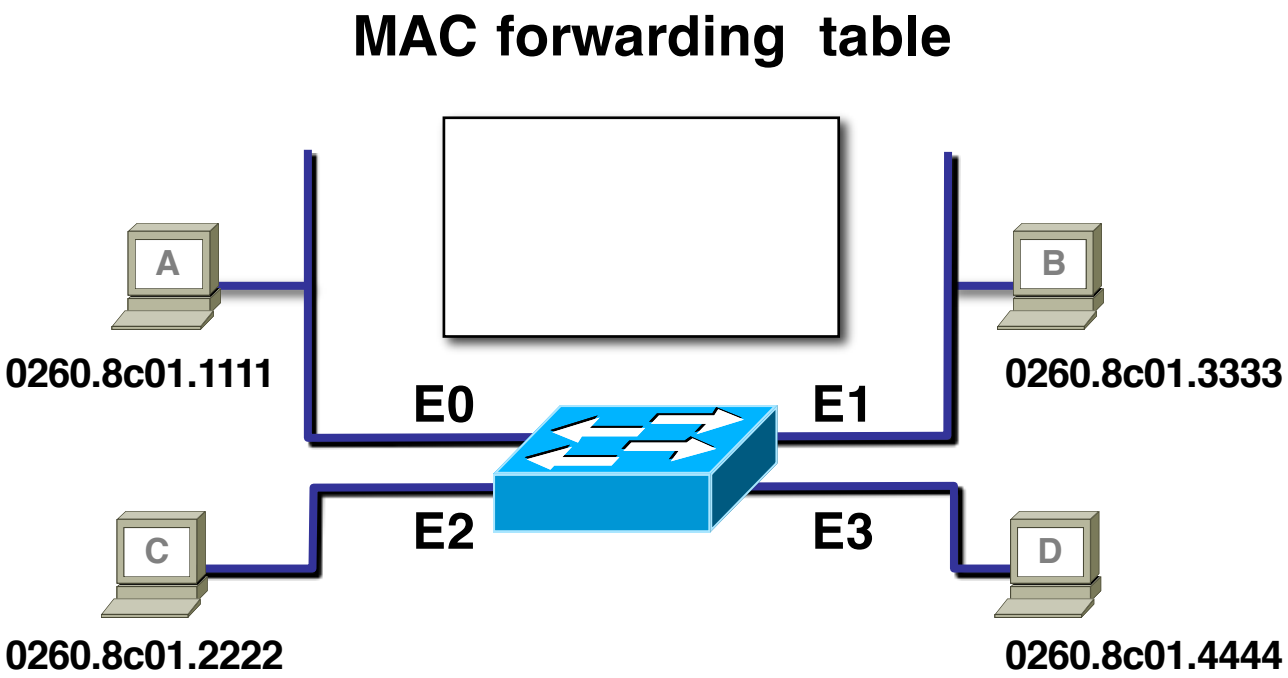
  Answer: →***Flooding***

- ***Flooding*** broadcasts unknown (aka unpopulated) MAC DA address frames to egress (aka output) ports associated with the ***broadcast domain***

- ***Broadcast domain*** consists of all ports that will be flooded

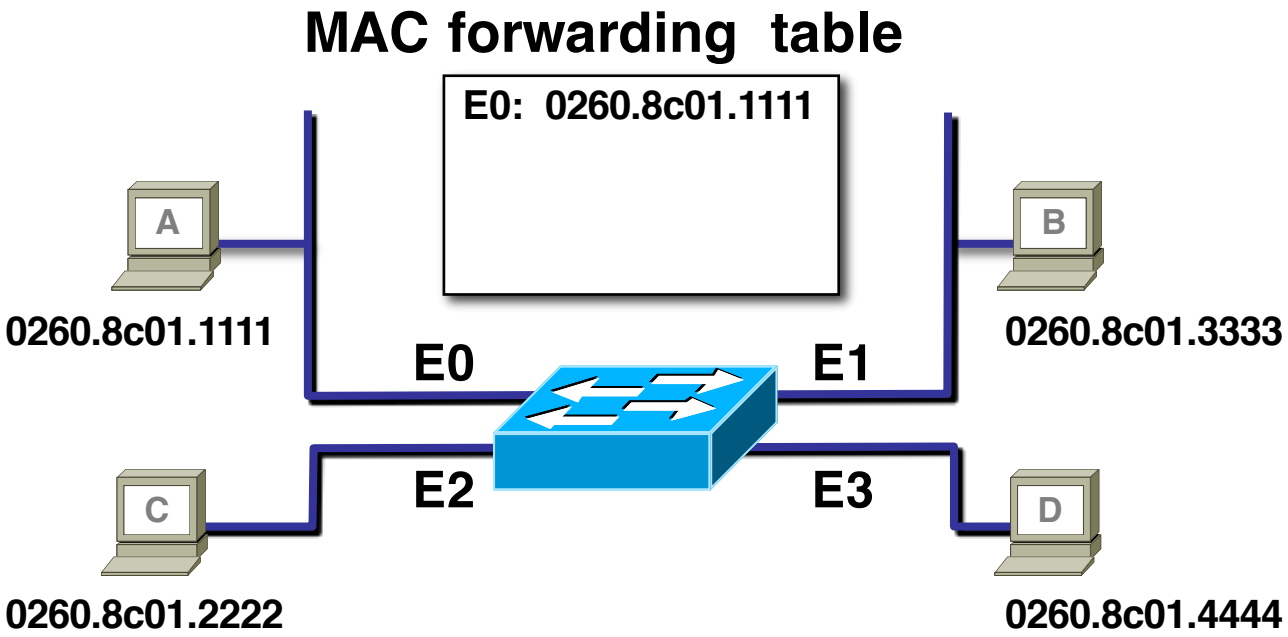
- ***Broadcast domain*** **= IP subnet (IMPORTANT!)**

How Bridges Learn Host Addresses and Locations?



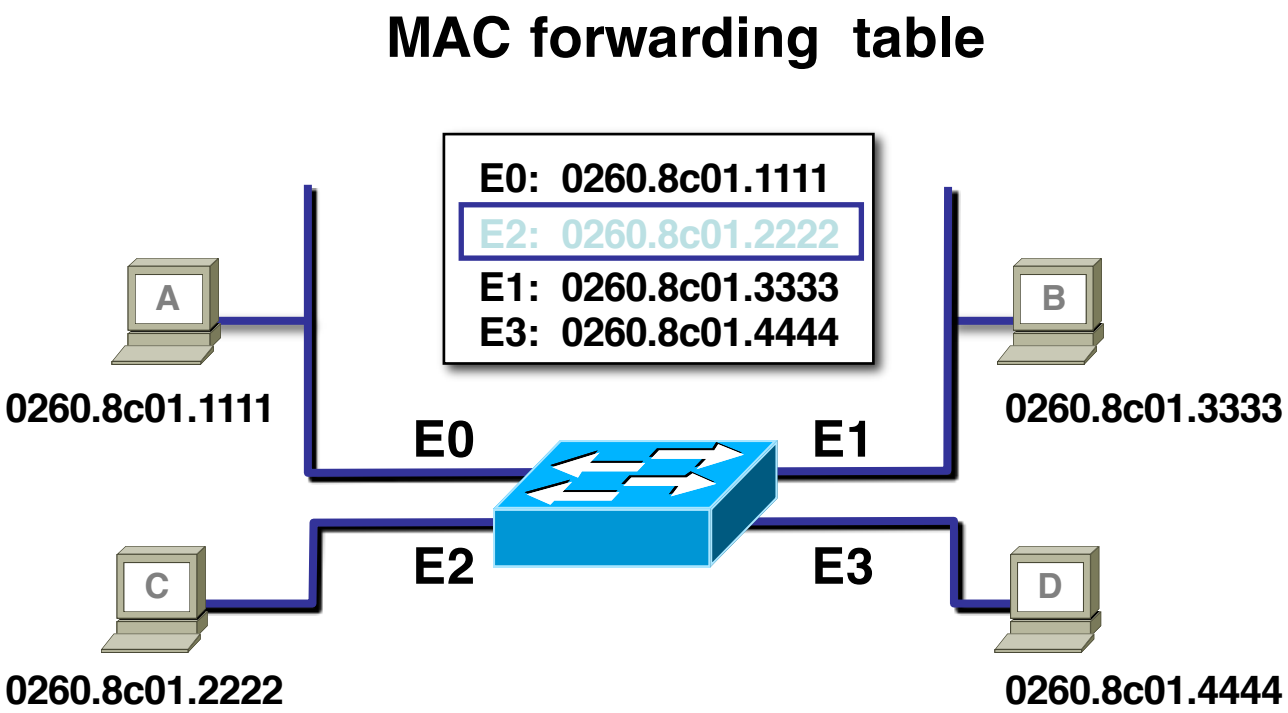
- **Initial MAC forwarding table is empty**

How Bridges Learn Host Addresses and Locations?



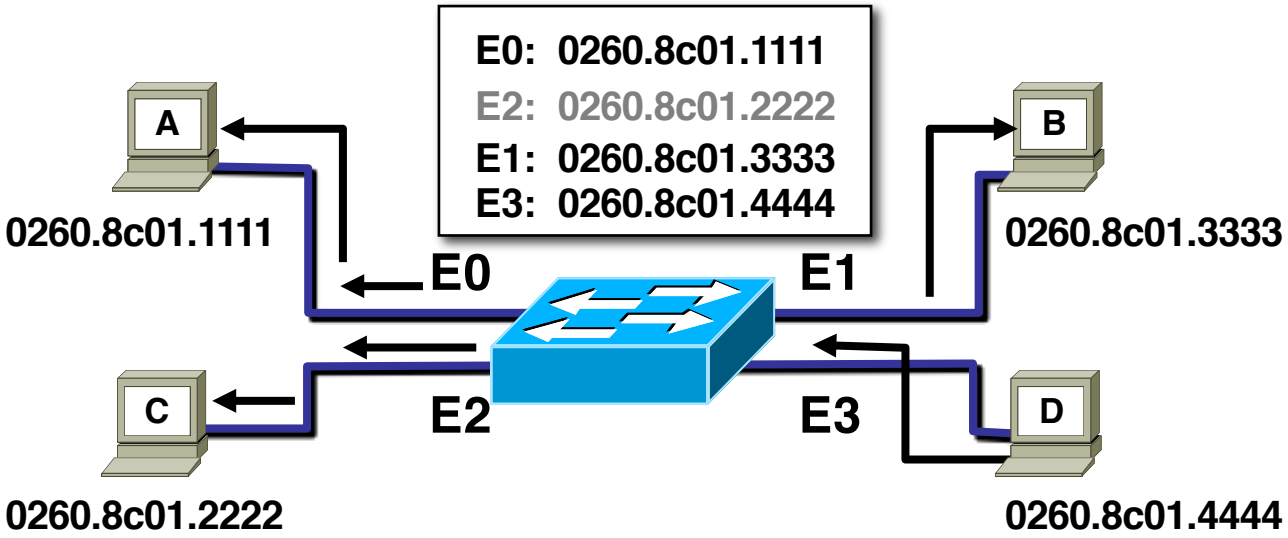
- Station A sends a frame to Station C
- Switch caches station A MAC address to port E0 by learning the source address of data frames
- The frame from station A to station C is flooded out to all ports except port E0 (unknown unicasts are flooded)

How Bridges Filter Frames?



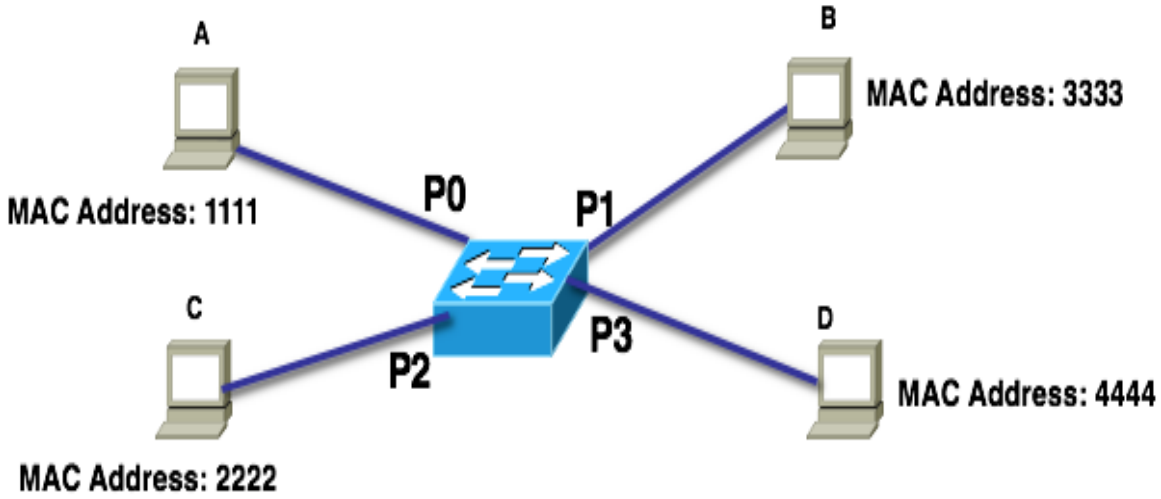
- Station A sends a frame to station C
- Destination is known, frame is not flooded

Broadcast Frames



- Station D sends a broadcast frame
- Broadcast frames are flooded to all ports other than the originating port

How Bridges Learn Host Addresses and Locations?



Assume that the MAC forwarding tables are initially empty.

Sequence step	Frame transmission	*Learn?* (YES or NO)	*Flood?* (YES or NO)
1	PC-B sends a frame to PC-C		
2	PC-C sends a frame to PC-D		
3	PC-A sends a frame to PC-D		
4	PC-A sends a frame to PC-B		
5	PC-D sends a frame to PC-B		
6	PC-C sends a frame to PC-A		
7	PC-B sends a frame to PC-D		

MAC address vs IP address

- IP addresses are logical and global.
  - IP address has not bound to hardware.
  - IP address of a device can be used by any other device on the entire Internet to communicate with it.
  - IP addresses are discoverable via DNS lookup, hyperlinks or scanning.
- MAC addresses are physical and local
  - MAC address burned into hardware by manufacturer
  - MAC address of a computer or server is only known to other devices on the same IP subnet (i.e. the same LAN).
  - MAC addresses do not cross routers – there is generally no way to discover MAC address of a device in another subnet.

Summary

- The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
- The IP address uniquely defines a host on the Internet.
- The port address identifies a process on a host.
- A specific address is a user-friendly address.
- A repeater is a connecting device that operates in the physical layer of the Internet model.
- A repeater regenerates a signal, connects segments of a LAN, and has no filtering capability.
- A link-layer switch is a connecting device that operates in the physical and data-link layers of the Internet model.
- A switch can forward and filter frames and automatically build its forwarding table.