SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

ICT259 Computer Networking

Seminar 2: Network Access and Ethernet

Ms Wong Yoke Moon

Network Access and Ethernet

Objectives:

- Explain the purpose and functions of the physical layer in a data network.
- Name the three main types of copper media used in networking.
- Identify the three types of UTP cables and their applications.
- Explain the purposes and functions of the data link layer in preparing for transmission on a data network.
- Summarize the functions of physical and logical topologies in LAN and WAN.
- Describe the characteristics and functions of the data link layer frame.
- Describe the function of each of the Ethernet sublayers.
- Outline the characteristics and purpose of the Ethernet MAC address.
- Demonstrate the learning, forwarding and filtering functions of an Ethernet switch.
- Describe the role of ARP in an Ethernet network.

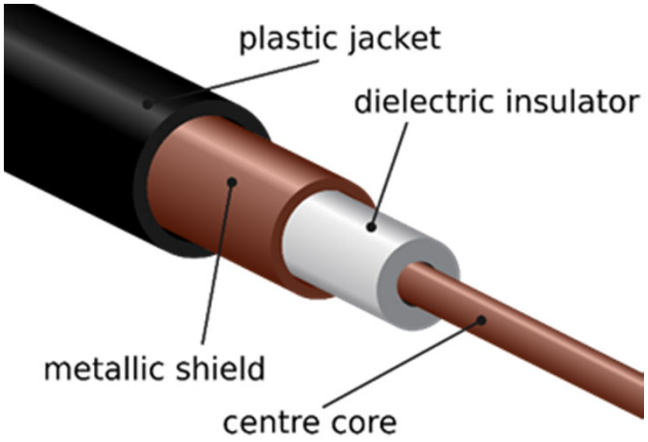
Network Media

Shielded Twisted-Pair (STP) Cable

- STP cable has a shield for each pair of wires, which are then wrapped in a foil shield to protect them from electromagnetic interference. The extra protection means that STP is more expensive and less flexible than UTP cable.

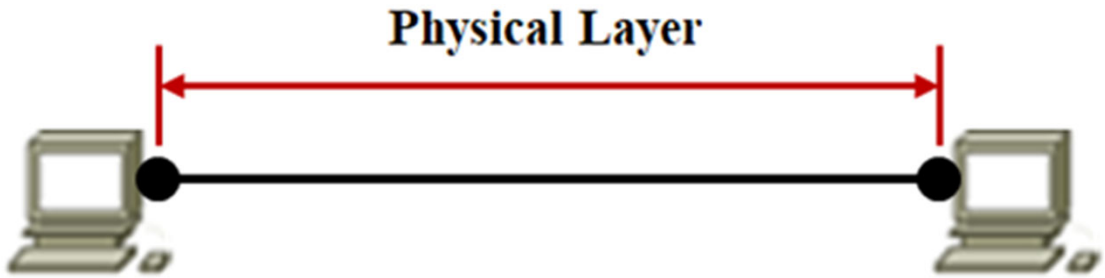
Coaxial Cable

- In coaxial cable, only the copper wire or centre core is used to transmit signals. Currently, coaxial cables are used in cable television network systems.



Physical Layer Protocols

- The physical layer is responsible for transmitting data onto the physical media by encoding binary bits into signals.
- Physical layer protocols define the rules or standards for the physical connections and the representation of data on the media.
- These rules describe the electrical, mechanical, functional and procedural aspects of the physical connections and media.
- These physical layer standards are implemented in hardware and are governed by many international organizations.
- Figure below shows the extent of the physical layer.



Network Media

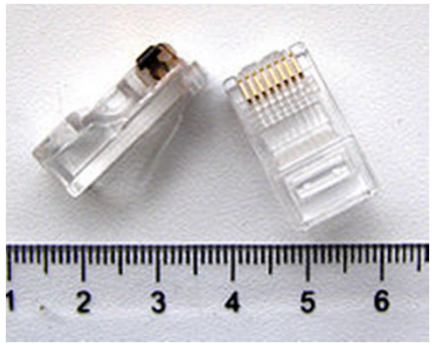
Three basic forms of network media: **copper** cable, **fiber-optic** cable and **wireless**.

Copper Media used in networking

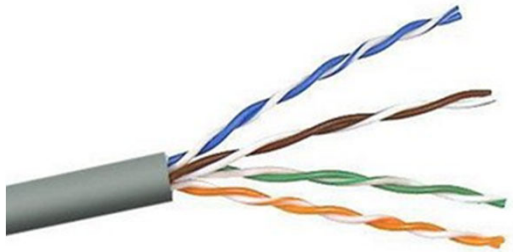
- Unshielded Twisted-Pair (UTP)
- Shielded Twisted-Pair (STP)
- Coaxial

Unshielded Twisted-Pair (UTP) Cable

- UTP cable is the most widely used media for LAN. It is terminated with RJ-45 connectors.
- The UTP cable has eight copper wires intertwined to form four pairs of wires. The eight wires are encased in a flexible plastic sheath that makes it highly flexible.



RJ-45 Connectors



Unshielded Twisted-Pair Cable

Network Media

UTP Categories

- UTP cables are classified into categories such as Category 5 (Cat 5) and Enhanced Category 5 (Cat 5e) based on the bandwidth rates they can support.
- The table below lists the properties of three major categories.

UTP Cable	Properties
Category 3 Cable (UTP)	• Used for voice communication • Most often used for phone lines
Category 5 and 5e Cable (UTP)	• Used for data transmission • Cat 5 supports 100 Mbps and can support 1000 Mbps, but it is not recommended • Cat 5e supports 1000 Mbps
Category 6 Cable (UTP)	• Used for data transmission • Supports 1000 Mbps to 10Gbps, although 10 Gbps is not recommended

Network Media

Types of UTP Cables

The three main types of UTP cables are:

- **Straight-through UTP** – Most widely used cable for networking. It is used to interconnect a host to a hub or switch, and a switch to a router.
- **Cross-over UTP** – It is used to interconnect similar devices, for example, a host to a host, a switch to a switch, or a router to a router. It is also used to connect a host to a router.
- **Rollover UTP** – It is used to connect a PC to the console port of a Cisco switch or router. This type of cable is used for configuring switches and routers.

IEEE 802

- Institute of Electrical and Electronics Engineers (IEEE) is a standard organization dedicated to creating standards in many industries.
- IEEE 802 is a family of standards that deal with local area networks and metropolitan area networks.
- These are the common 802 standards:
  - **802.3 Ethernet**
  - **802.11 Wireless LAN (WLAN)**
  - 802.15 Wireless Personal Area Network (WPAN) - Bluetooth
  - 802.16 Broadband Wireless Access

Network Media

Types of Wireless Media

- The IEEE **wireless standards** cover both the **physical and data link layers**.
- The IEEE wireless standards include:
  - **WiFi (IEEE 802.11 standard)** – Wireless LAN (WLAN) technology.
  - **Bluetooth** (IEEE 802.15 standard) – Wireless Personal Area Network (WPAN) technology, which allows devices to communicate and interoperate with one another over distances from 1 to 100 meters.
  - **WiMAX** (IEEE 802.16 standard) – Short for Worldwide Interoperability for Microwave Access (WiMAX), represents 4G or the "fourth generation" of wireless internet. It is essentially a wireless broadband.

Wireless LAN

For a wireless LAN to work, it requires:

- **Wireless Access Point (AP)** – A device that allows a WiFi device to connect to a wired network.
- **Wireless NIC adapters** – A wireless NIC adapter is a wireless network interface card used to connect to a radio frequency or RF network.

Data Link Layer Protocols

Purpose of the Data Link Layer

- To prepare data for the physical media.

Responsibility of the Data Link Layer

- Allow the upper layers to access the physical media
- Accept network layer packets and **package them into frames**
- Prepare the data for the physical network
- Control how data is placed and received on the physical media
- Exchange frames between nodes over a physical media
- **Remove** data link layer **header and trailer** and pass packet to the network layer protocol
- Perform error detection

Data Link Layer Protocols

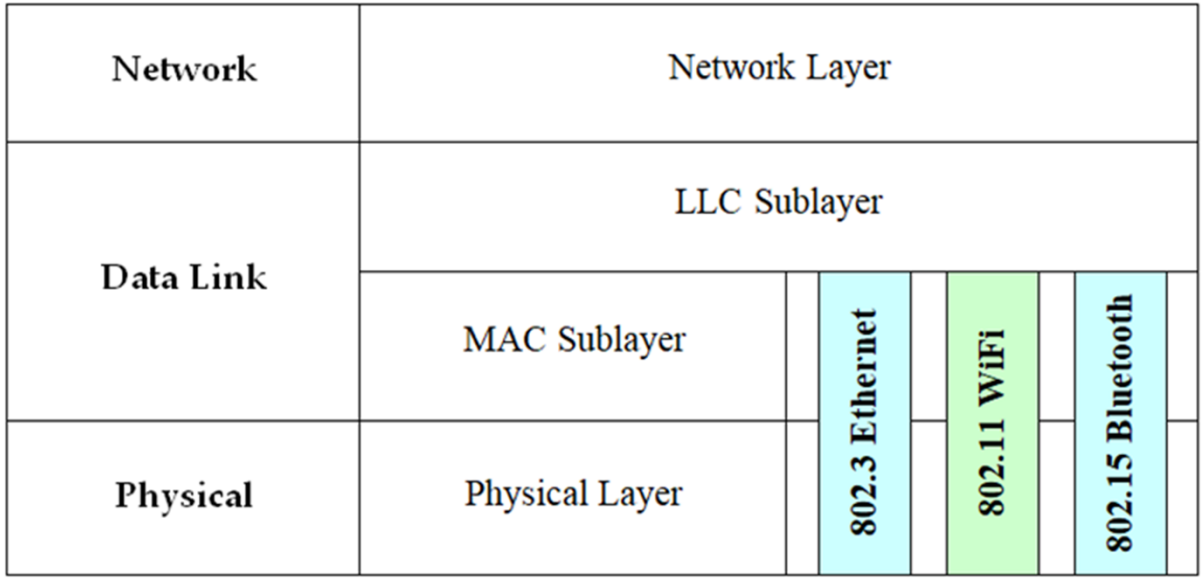
Data Link Sublayers

Data link layer has two sublayers:

1. **Logical Link Control (LLC)**
2. **Media Access Control (MAC)**

Logical Link Control (LLC)

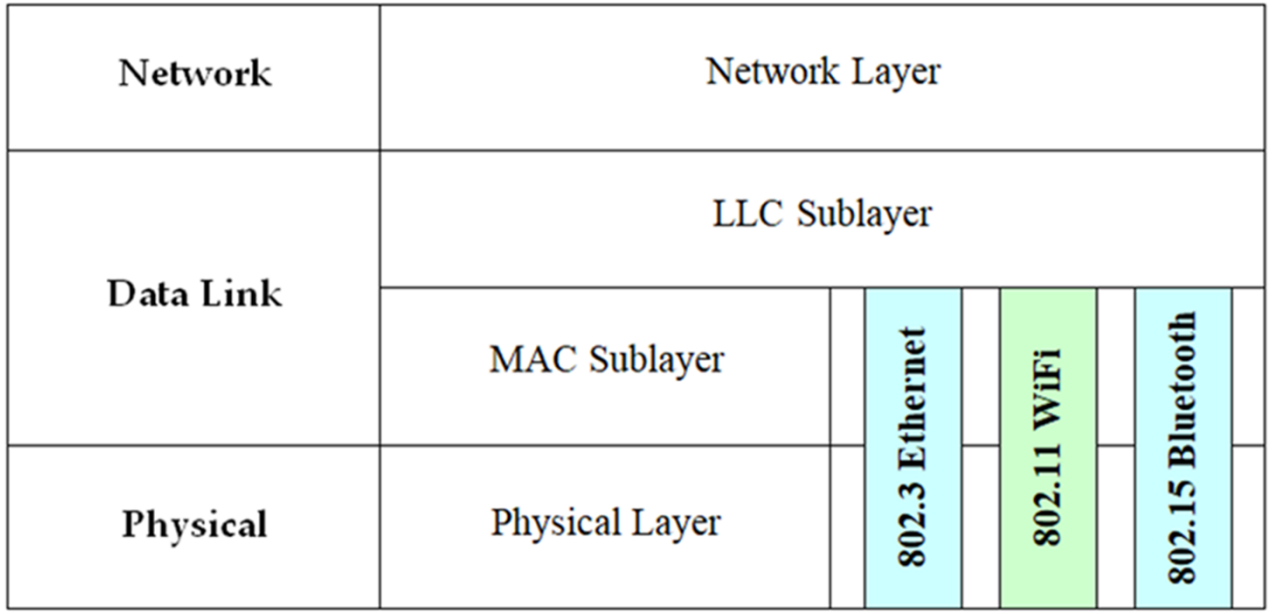
- This upper sublayer **interacts with the network layer**.
- This sublayer was created to provide **different physical layer technologies**, such as Ethernet, WiFi and Bluetooth, **a single method of accessing** the network layer and beyond.
- Thus, the LLC sublayer is **technology independent**.



Data Link Layer Protocols

Media Access Control (MAC)

- This lower sublayer transits **down to the physical media**.
- If multiple computers can access the network, then some form of **orderly access** to the media must be made. This is the job of the MAC sublayer to determine which computer can access the media at any one time.
- It provides also the **data link layer addressing**.
- **Different access methods** and addressing may be used for different Layer 1 technologies.
- Thus, the MAC sublayer is **technology dependent**.



Data Link Layer Protocols

Media Access Control Method

- The media access control method or in short the access method, is the technique used to **get the frame on and off the physical media**.
- As data travel from source host to destination host, it is possible for the data to traverse through different physical network or media, such as copper wires, optical fibers, and wireless.
- **Different access methods** may be required **for different media**.
- It is the responsible of the data link layer to **encapsulate the packet** into a frame **appropriate for the network** or media.
- **Different data link layer protocols** may be used **for different networks or media**.

Media Access Control

Topologies

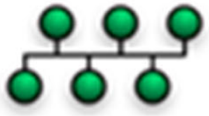
- The data link layer protocols define the rules for access to different media.
- The actual media access control method used depends on
  - **Topology** - The manner in which nodes are connected.
  - **Media sharing** – How the nodes share the media. The media sharing can be shared by many devices, or a point-to-point connection.

Physical and Logical Topologies

- Network **topology** refers to the **arrangement of network devices** and the interconnections between them.
- Network topologies can be viewed in two ways:
  - **Physical topology** – How network devices are **actually connected** together.
  - **Logical topology** – How **data flows** in the network.

Media Access Control

Common Network Topologies

Common Physical WAN Topologies	
	Point-to-Point topology – A permanent link between to end devices.
	Star topology – A central site interconnects branch sites using point-to-point links.
	Full mesh topology – Every device is interconnected to every other device using point-to-point link.
Common Physical LAN Topologies	
	Star topology – All end devices are connected to a central intermediate device, which is usually an Ethernet switch.
	Bus topology – All end devices are chained together, most likely by a coaxial cable and terminated by terminators on each end.
	Ring topology – All end devices are connected to their respective neighbour to form a closed loop.

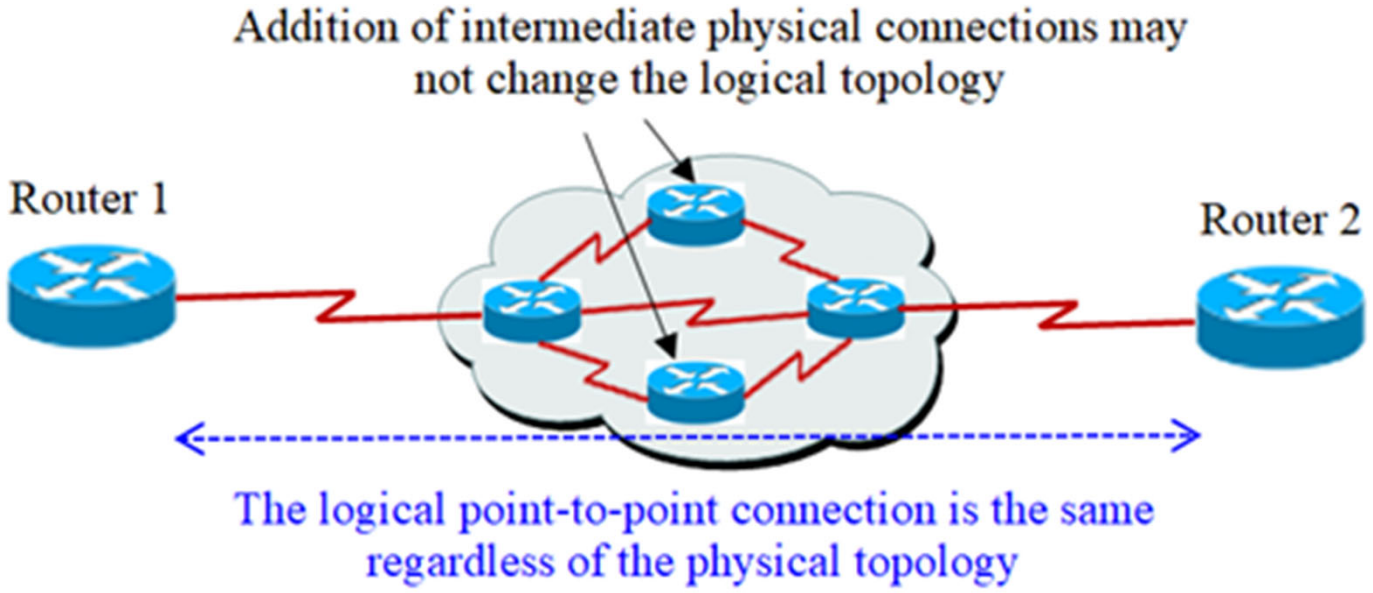
Physical Point-to-Point Topology

- Physical Point-to-Point topology has a direct connection between two end devices.

Media Access Control

Logical Point-to-Point Topology

- **Physical connections** in a network **do not affect the logical topology**.
- Some Layer 2 technologies **create *virtual circuit*** or logical connection within a network between two end devices.
- This **virtual circuit** is the **same regardless of the physical topology**.
- The **media access method** used by the data link layer protocol is **determined by the logical topology**, not the physical topology.
- This implies that the logical point-to point connection between two end devices may not necessarily be between two physical end devices at each end of a single physical link.



Media Access Control

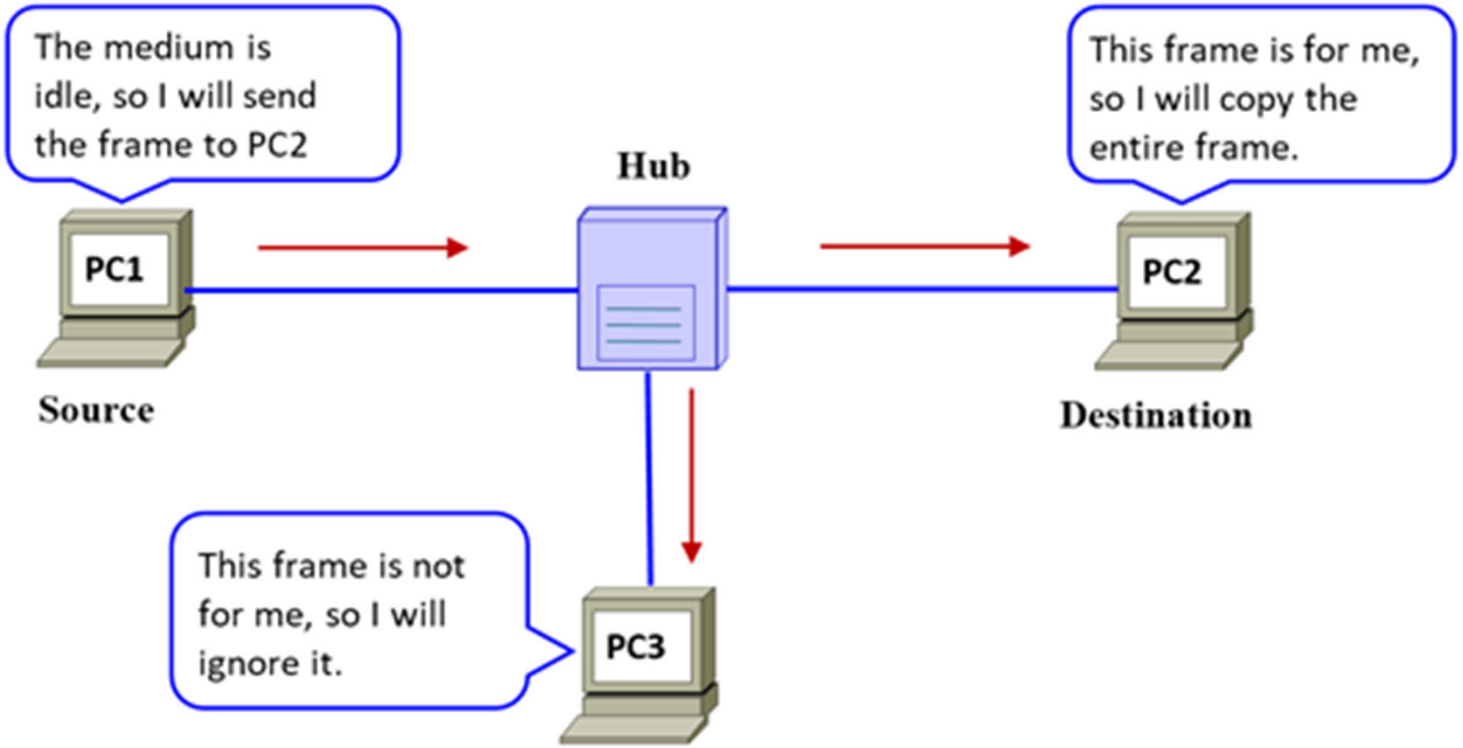
Contention-Based Access

- Some network topologies **share a common media** with many devices; such networks are called **multi-access networks**.
- Examples of multi-access networks are Ethernet LANs and WLANs.
- At any one time, **more than one device may be attempting to access the shared media**.
- As such, **rules are required** to govern how devices access the shared media.
- One popular access control method for shared media is **contention-based access**.
- In contention-based access, all devices **operating in half-duplex compete to use the medium**, but only one device can send at a time.
- There is a mechanism if more than one device sends at the same time.
- **WLANs and Ethernet LANs using hubs** are examples of contention-based access networks.

Media Access Control

Contention-Based Access – CSMA/CD

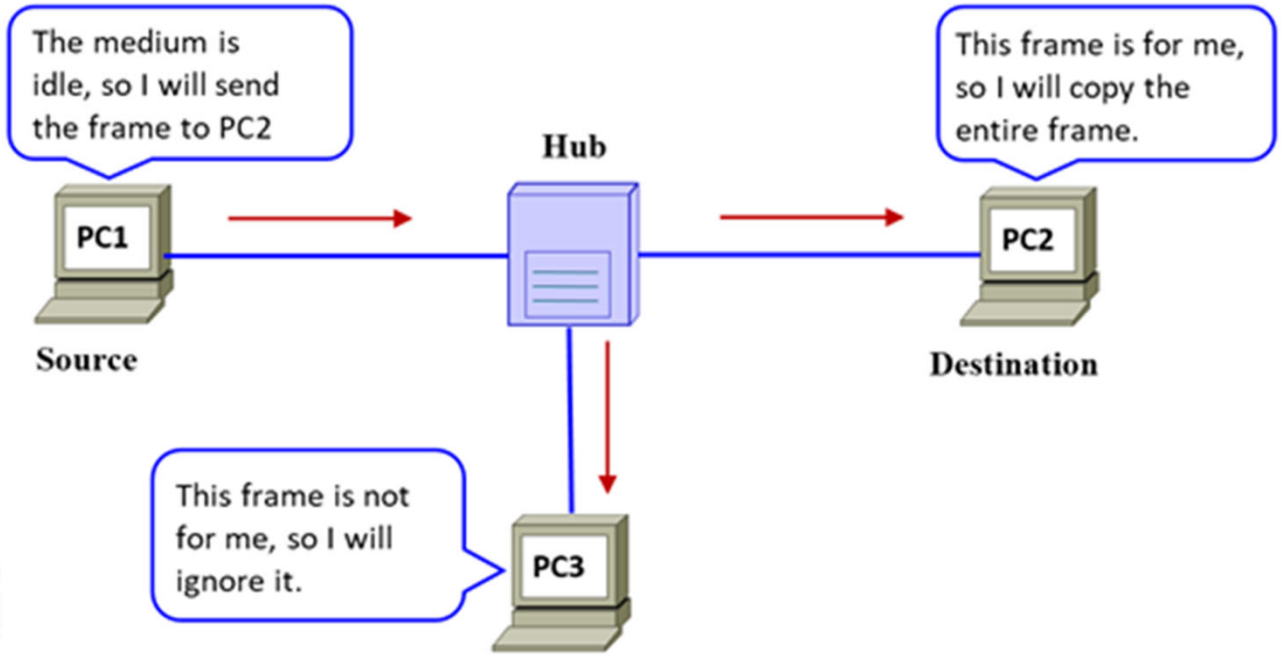
- ***Carrier Sense Multiple Access/Collision Detection (CSMA/CD)*** is a contention-based access method used in half-duplex Ethernet LANs.



Media Access Control

The process of CSMA/CD

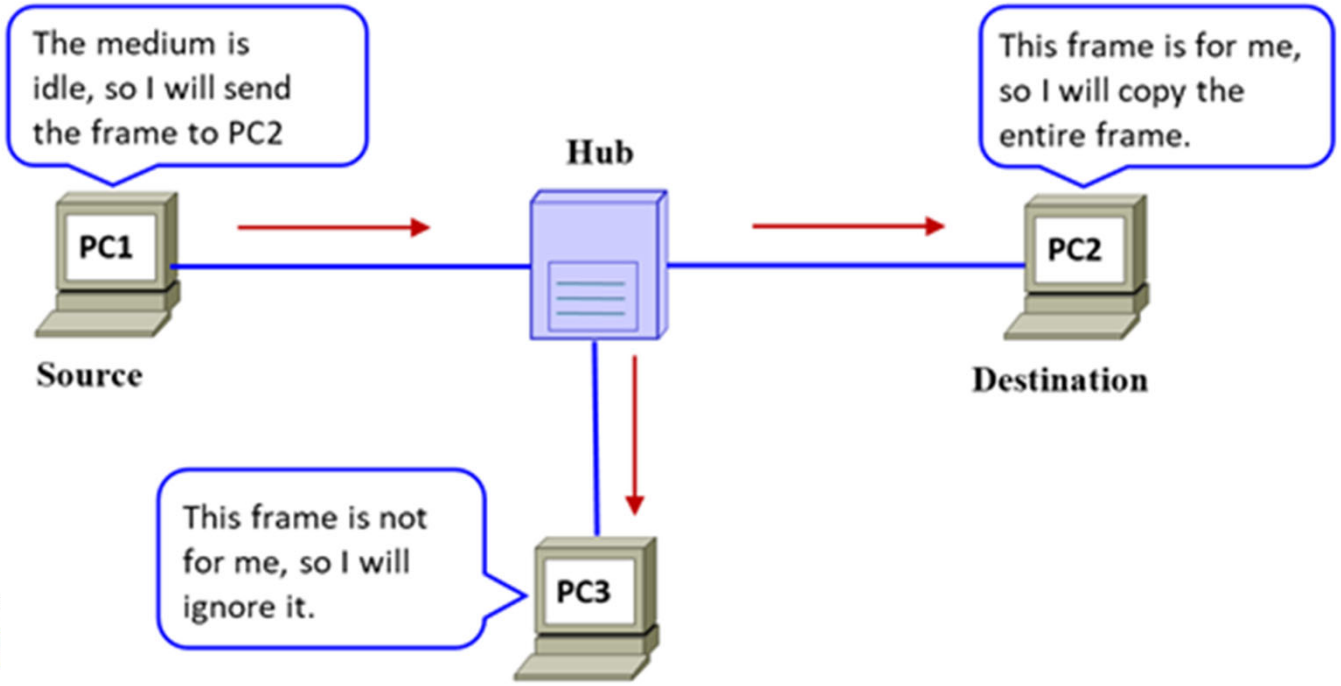
1. **All devices have access** to the network, which is the meaning of **Multiple Access (MA)**.
2. PC1 has an Ethernet frame to send to PC2.
3. PC1's NIC needs to determine if any device is sending on the medium. It **senses the medium** to detect for carrier signal, which is the meaning of **Carrier Sense (CS)**. If not signal is detected, it means it is not receiving transmissions from another device. It assumes the medium is **idle** and available.
4. PC1 **inserted the destination MAC address** of PC2 into the Ethernet header to form an Ethernet frame, and sends the frame.



Media Access Control

The process of CSMA/CD

5. The Ethernet **hub** receives the frame. The hub is a common connection point for all devices connected to it. Bits received on one port are regenerated (or repeated) and **sent out on all other ports**.
6. If another device, say PC3, wants to transmit, but detected an incoming signal; it must **wait until the medium is idle**.
7. Due to the regeneration of bits at the hub, all devices connected to the hub will receive the frame. Since the frame is destined for PC2, only **PC2 will accept and copy** the entire frame. All **other devices**' NIC will **ignore the frame**.

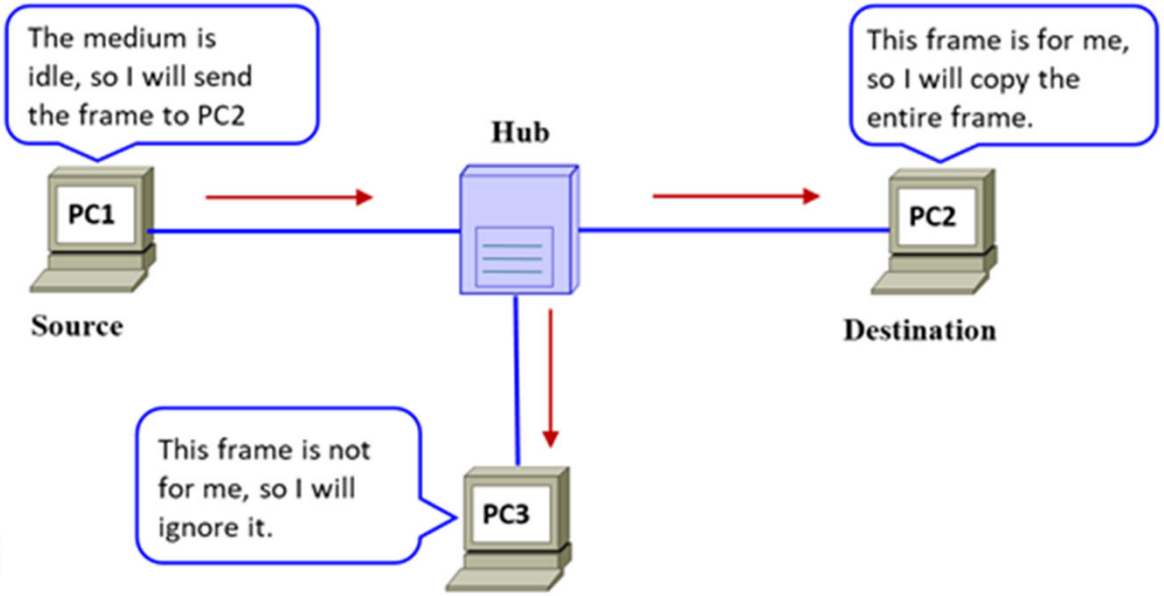


Media Access Control

The process of CSMA/CD

8. A **collision will occur**, if two devices transmit at the same time. There is a **mechanism** for the two devices **to detect the collision**, thus the **Collision Detection (CD)**. The data sent by both devices will be damaged. After a **random time interval**, both devices will attempt to **retransmit again**.

- Ethernet LAN using hubs is no longer popular due to its **poor performance** if the number of devices connected to the hub increases, which results in more collisions and retransmissions.
- To avoid this problem, **hubs are replaced by switches** because the switch and the host's NIC operate in full-duplex mode.



Media Access Control

Contention-Based Access – CSMA/CA

- ***Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)*** is a contention-based access method used by IEEE 802.11 **WLANs**.
- As the name implies, CSMA/CA **does not detect collisions**, but **avoid collision by waiting before transmitting**.

Media Access Control

The process of CSMA/CA

1. The CSMA portion of CSMA/CA is similar to CSMA/CD.
2. Before a device transmits data, it senses or **listens to the medium**. If the **medium is idle**, instead of immediately transmitting, it **waits a predefined period of time**. When this period of **time is up** and the medium is **still idle**, it **transmits**.
3. The transmitting device **includes a time duration** it needs for the transmission. All other wireless devices receive this information and know that the **medium will be unavailable during this period**.
4. If the device detects the medium is **busy**, it will **back off** and wait for a **random amount of time**.
5. If the **medium is idle when the random amount of time is up**, it **transmits** the data.
6. If the medium is still busy when the random amount of time is up, it will back off and wait for a random amount of time again, and the entire scenario is repeated.
7. Once the data is received by the receiving device, the receiver sends an **acknowledgment (ACK)** so that the sender knows that the frame is received.
8. If the **ACK is not received**, the sender assumes the data is lost and a **retransmission** is set up.

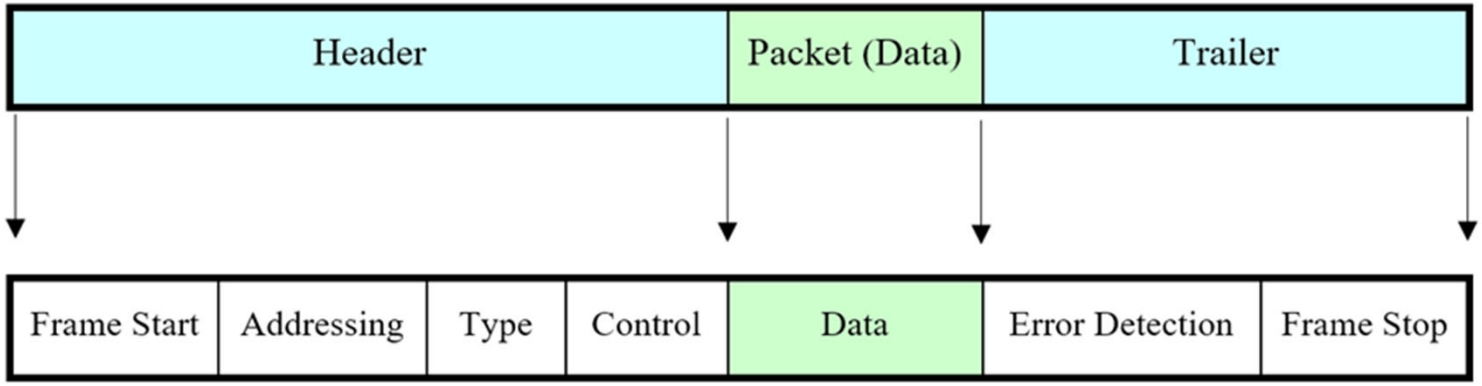
Media Access Control

Data Link Frame

- The data link layer prepares a packet or Layer 3 PDU for transmission across the physical media by **encapsulating a header and trailer to form a frame**.
- There are many **different data link layer protocols**, and each has its **own frame format** or structure.
- Regardless of the protocol used, each frame type has **three basic parts**:
  - Header
  - Data (Packet from layer 3)
  - Trailer
- The **contents** of the header and trailer vary **from** data link **protocol to protocol**.

Data Link Frame Fields

- **Framing** breaks a stream of binary bits into meaningful groupings or fields.
- These groupings help the receiving node to **make sense of the stream of binary bits** it is to receive. Figure below shows the fields of a generic frame.

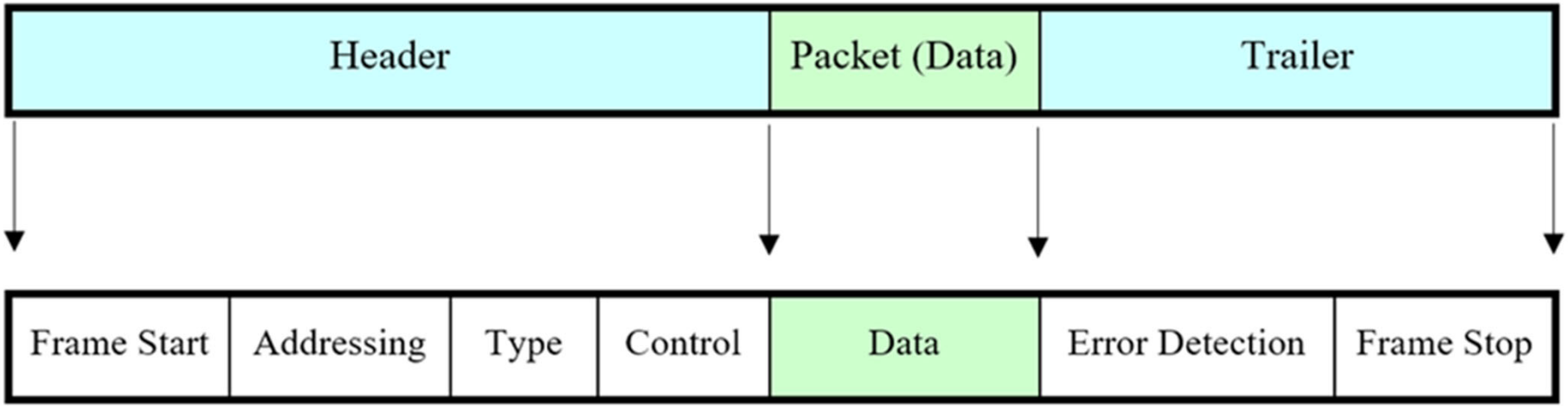


Media Access Control

Data Link Frame Fields

The field types of the generic frame include

- **Frame Start and Frame Stop flags** – Used to identify the beginning and end limits of the frame.
- **Addressing** – Indicates hardware or physical address of the source and destination nodes.
- **Type** – identifies the Layer 3 protocol encapsulated in the data field.
- **Control** – Identifies special **flow control services** such as quality of service (QoS).
- **Data** – This is the Layer 3 PDU (packet header, segment header and data).
- **Error Detection** – Used to detect any errors in transmissions. Also known as Frame Check Sequence (**FCS**). The source node computes a value based on the contents of the frame and places this value in the FCS field. Upon receiving the frame, the destination node performs a re-computation to check for errors.



Media Access Control

Layer 2 Address

- The Layer 2 address is the **physical or hardware address** of the device.
- The physical addresses of the source and destination nodes are **specified in the frame header**.
- Recall: Layer 2 addressing is point-to-point and it changes from hop to hop or network to network.

LAN and WAN Protocols

- Devices that operate at data link layer include the NICs on computers, Layer 2 switches and interfaces (or ports) on routers.

- Some common LAN data link layer protocols include
  - **Ethernet**
  - **802.11 Wireless**

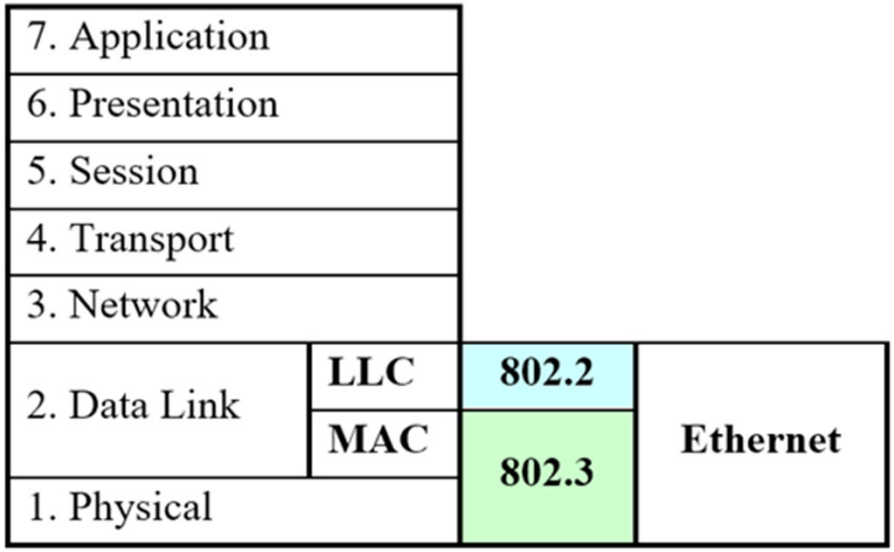
- Some common WAN data link layer protocols include
  - **Point-to-Point Protocol (PPP)**
  - **HDLC**
  - **Frame Relay**

Ethernet Protocol

Ethernet Standards

- Ethernet is a family of networking technologies defined in the IEEE **80.2.2** and IEEE **802.3** standards.
- Ethernet supports the following bandwidths:
  - 10 Mbps - Ethernet
  - 100 Mbps – Fast Ethernet
  - 1000 Mbps (1 Gbps) – Gigabit Ethernet
  - 10,000 Mbps (10 Gbps)
  - 40,000 Mbps (40 Gbps)
  - 100,000 Mbps (100 Gbps)

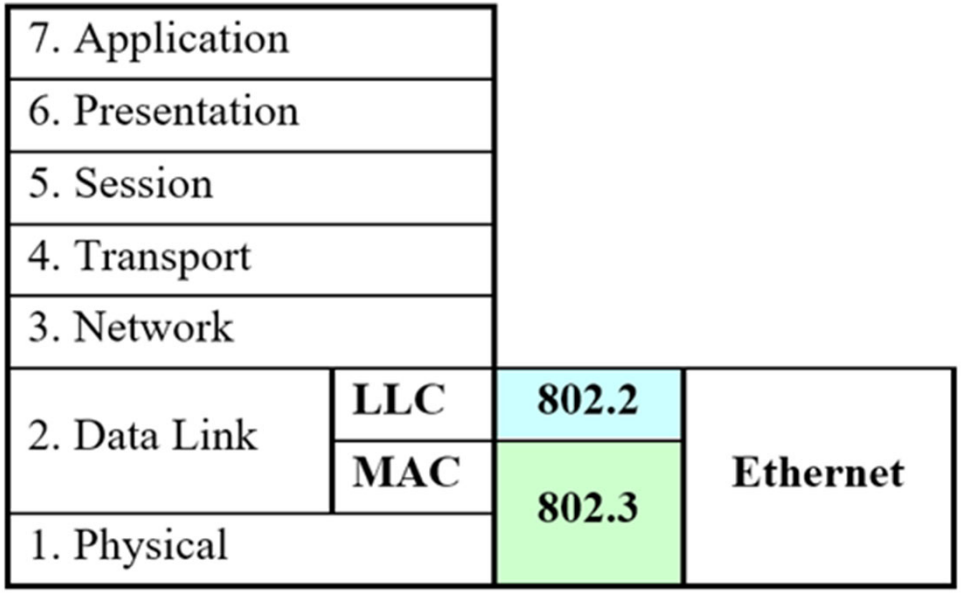
- The Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.



Ethernet Protocol

LLC Sublayer

- The LLC sublayer handles the communication between the **upper layers**, which is the networking **software**, and the **lower layers**, which is the device **hardware**.
- The LLC sublayer takes the layer 3 PDU, which is usually an IP packet, and adds a header with control information to help to transmit the packet to the destination node.
- **LLC** is implemented in **software** and is **independent of the hardware** at the lower layers.
- **LLC** can be considered as the **driver software** for the NIC of a computer. This driver software interacts with the hardware on the NIC to pass the data between the MAC sublayer and the physical media.



Ethernet Protocol

MAC Sublayer

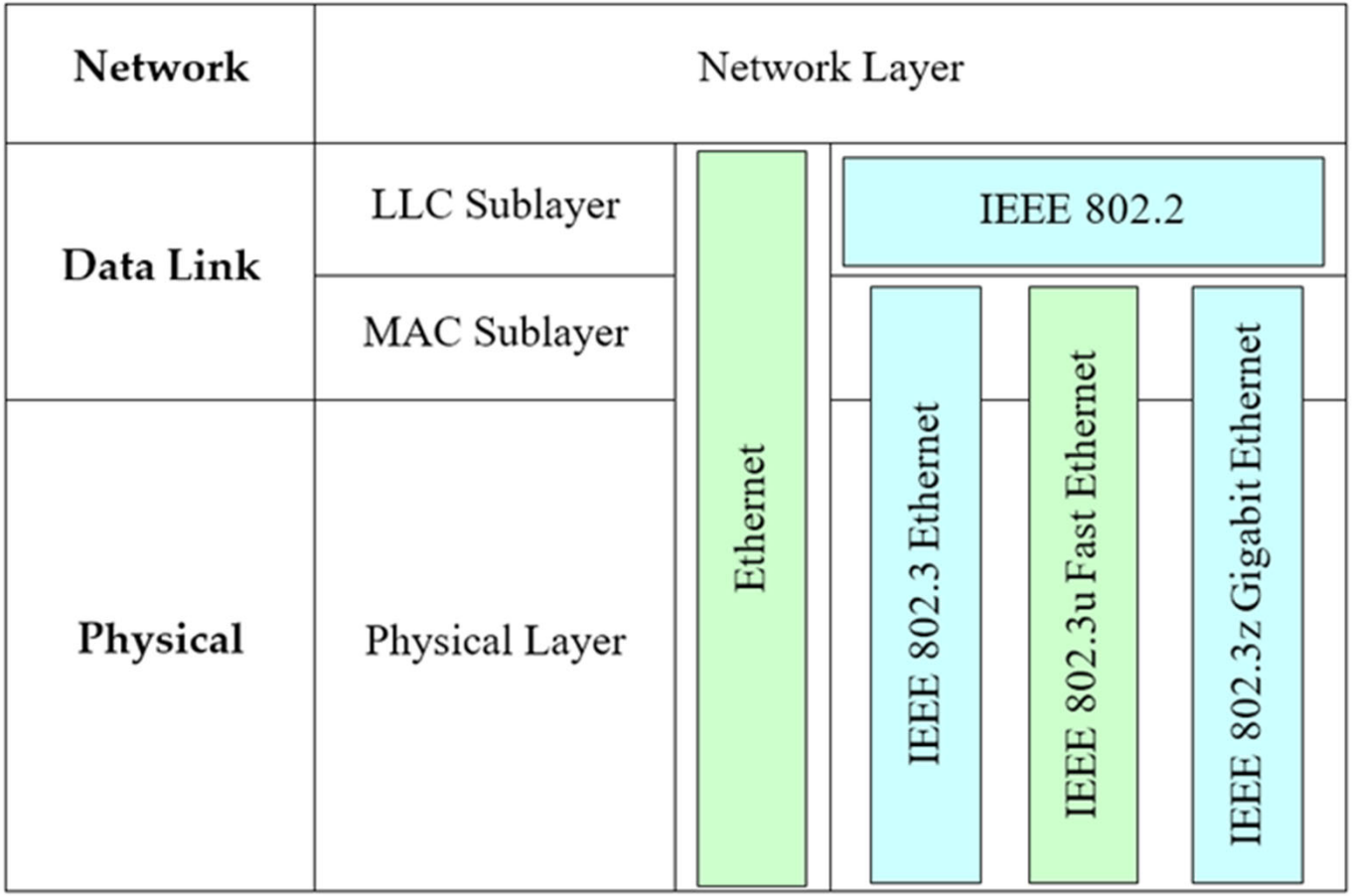
- **MAC** is implemented by **hardware**, usually in the computer NIC. Figure 2.2 shows the common IEEE Ethernet standards.

- Ethernet MAC sublayer has two main **responsibilities**:
  - **Data encapsulation**
    - Responsible for assembly of frame before transmission and disassembly upon receipt of frame.

  - **Media access control**
    - Responsible for **placing frames** on the media and **removing frames** from the media.
    - The **logical topology** of Ethernet is a **multi-access bus**, where all devices share a common media. It is a **contention-based network**. If half-duplex hubs are used in an Ethernet LAN, CSMA/CD will be the access method.

Ethernet Protocol

Common IEEE Ethernet Standards in the OSI Model



Ethernet Protocol

Ethernet Frame Fields

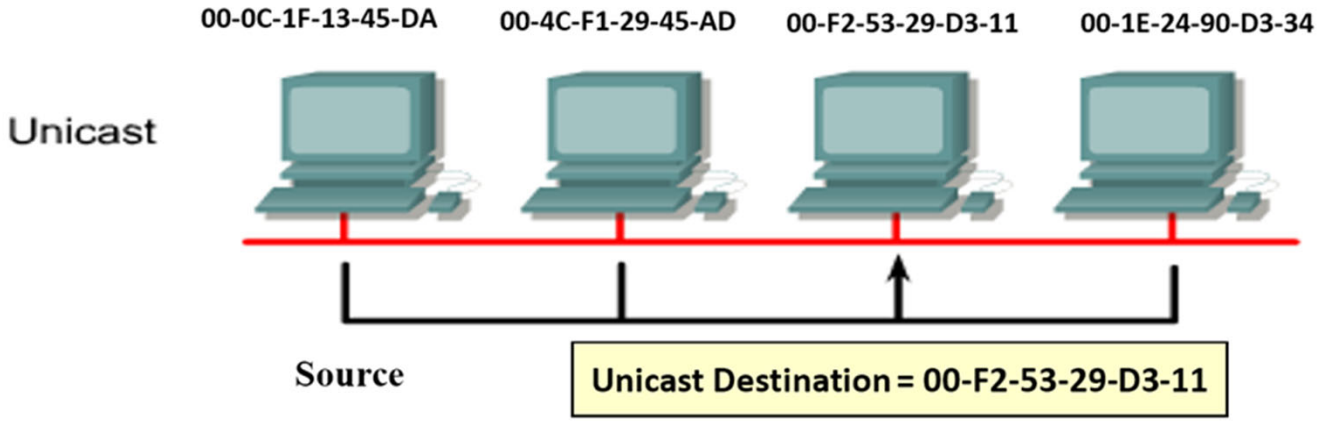
- The **Ethernet frame format** is almost **identical for all speeds** of the Ethernet.
- An Ethernet frame must be at **least 64 bytes** for collision detection to work, and can be a **maximum of 1518 bytes**. The description of each field is as follows:
  - **Preamble** – The Preamble is divided into two sections, with a Preamble (7 bytes) and a Start Frame Delimiter (SFD) of 1 byte. The Preamble controls the synchronization between sender and receiver. The SFD serves as a signal to the NIC that the data immediately following the SFD is the beginning of the actual frame. Both values are represented by the bit sequence "1010101010 …"
  - **Destination and Source Addresses** –The MAC address of the destination device and the MAC address of source device.
  - **Type** – Identifies the Layer 3 protocol encapsulated in the frame.
  - **Data** – The Layer 3 PDU or packet from a higher layer.
  - **Frame Check Sequence** – Also known as Cyclic Redundancy Check (CRC). CRC is a mechanism to check for transmission error upon arrival at the destination device.

Bit Sequence 1010101010…		Ethernet Frame (64 – 1518 Bytes)				
8 Bytes		6 Bytes	6 Bytes	2 Bytes	46 to 1500 Bytes	4 Bytes
Preamble (7 bytes)	SFD (1 byte)	Destination Address	Source Address	Type	Data	Frame Check Sequence

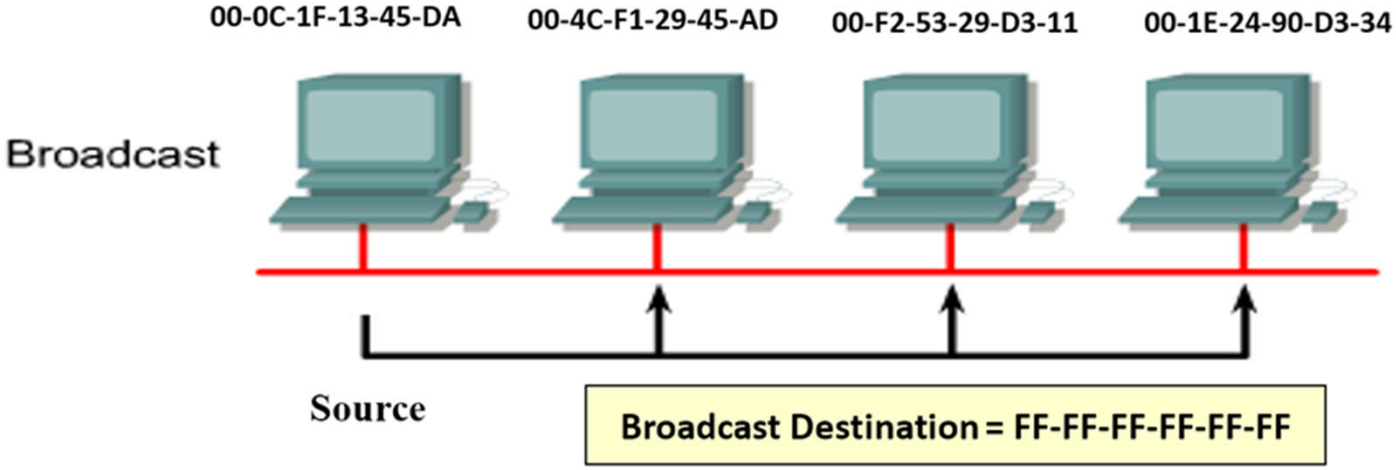
Ethernet Protocol

Layer 2 Communications

- **Unicast** - From one source to one destination, i.e. **One-to-One**.



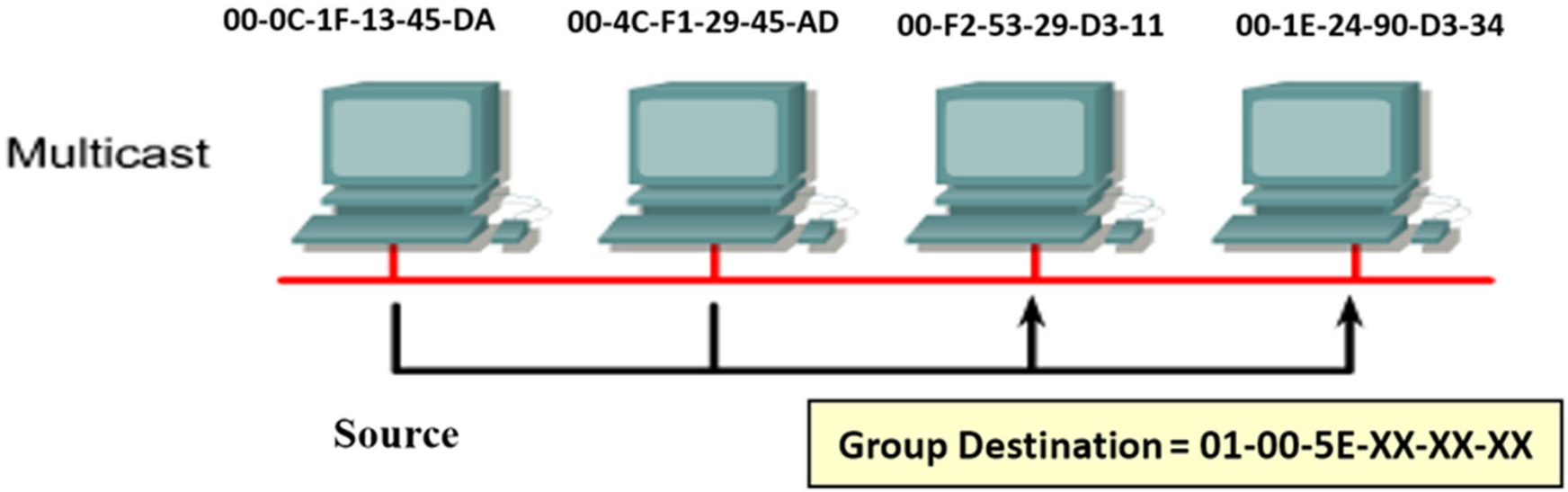
- **Broadcast** – From one source to all hosts in the network, i.e. **One-to-All**. The destination MAC address for broadcast is FF-FF-FF-FF-FF-FF.



Ethernet Protocol

Layer 2 Communications

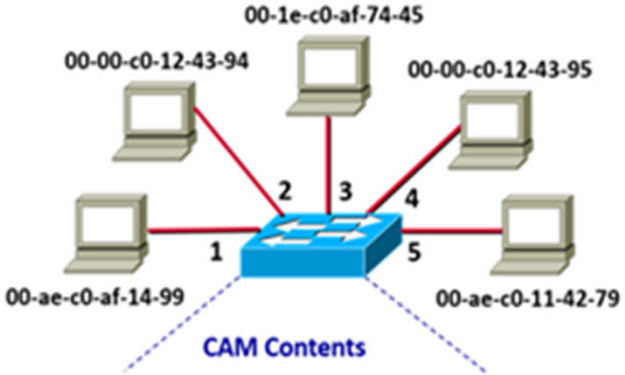
- **Multicast** - From one source to multiple hosts in a target group, i.e. **One-to-Many**. The multicast MAC address begins with **01-00-5E**.



LAN Switches

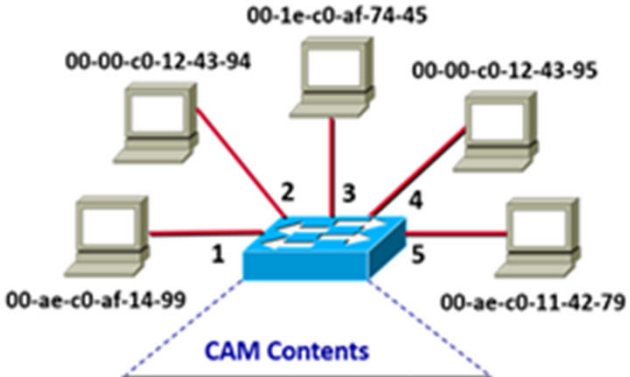
The MAC Address Table

- Every switch has a MAC address table stored in a memory called **Content Addressable Memory (CAM)**.
- The MAC address table shows the **MAC addresses** of nodes and their associated **ports**.
- When a switch is powered on, the MAC table is **empty**, meaning no port is mapped to any node.
- After all nodes have transmitted, all the MAC addresses and their associated ports will be shown in the MAC address table.



Host MAC Address	Port

Empty MAC Address Table



Host MAC Address	Port
00-ae-c0-af-14-99	1
00-00-c0-12-43-94	2
00-1e-c0-af-74-45	3
00-00-c0-12-43-95	4
00-ae-c0-11-42-79	5

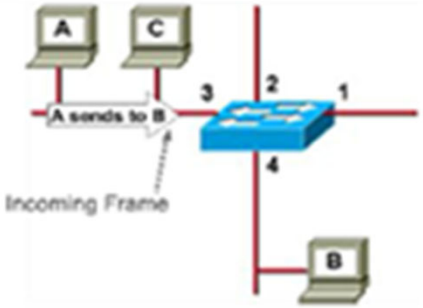
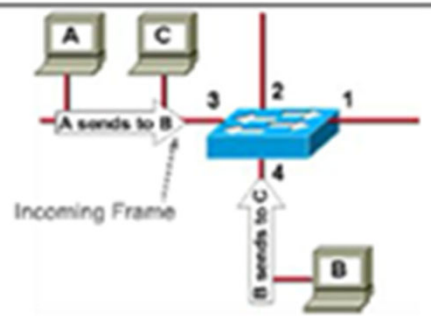
Filled MAC Address Table

Function of Switch

Learning MAC Addresses

- In learning, the switch examines the **source MAC address**, and enters the source MAC address and its attached port into the MAC address table.

Learning MAC Addresses

Illustration	Description
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3	• If node A transmits a frame to node B, it reaches the switch. The switch discovers that the frame was sent by node A from port 3. Hence, it records this in its CAM.
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3 MAC address of B | 4	• Subsequently, node B transmit a frame to node C, it reaches the switch. The switch discovers that the frame was sent by node B from port 4. Hence, it records in its CAM. • If node C did not transmit any frame, its MAC address and attached port will not be recorded in the MAC address table.

Function of Switch

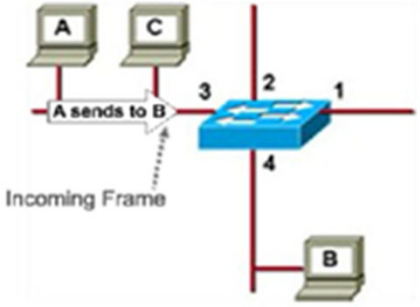
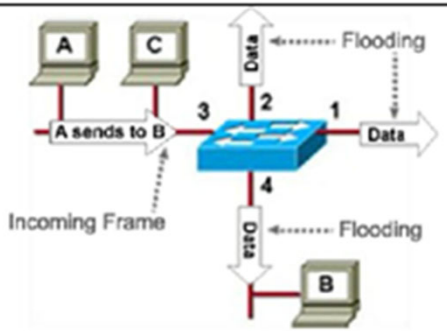
Forwarding Frames

- Forwarding is a decision making process based on the **destination MAC address**.

Forwarding Involving Unknown Destination MAC Address

- In forwarding, the switch examines the **destination MAC address** and consults the MAC address table for a match in the destination MAC address.
- If there is **no match**, it is taken as an unknown destination MAC address.
- If the **destination MAC address is unknown**, the frame is forwarded to all ports expect the incoming port.

Forwarding Involving Unknown Destination MAC Address

Illustration	Description
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3	As node A transmits a frame to node B, it reaches the switch.
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3	Since the switch does not know where node B is, it floods (or forwards the frame onto all ports, except the incoming ports).

Function of Switch

Forwarding Involving Broadcast and Multicast

- In forwarding, the switch examines the **destination MAC address**. If it is a broadcast or multicast, the frame is **forwarded to all ports expect the incoming port.**

Forwarding Involving Broadcast and Multicast

Illustration	Description
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3	Recall: Broadcast: Frame is to be sent to all nodes on the LAN. Multicast: Frame is to be sent to a group of nodes. Node A transmits a broadcast or multicast frame, it reaches the switch.
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3	The switch, upon receiving a broadcast or multicast, forwards the frame onto all ports, except the incoming ports.

Function of Switch

Forwarding Involving Known Destination MAC Address

- In forwarding, the switch examines the **destination MAC address** and consults the MAC address table for a match in the destination MAC address.
- When a node is transmitting to another node which has its destination MAC address in the MAC address table, the switch is handling a **known address**.
- The switch will **forward the frame to the port indicated** in the MAC address table.

Forwarding Involving Known Destination MAC Address

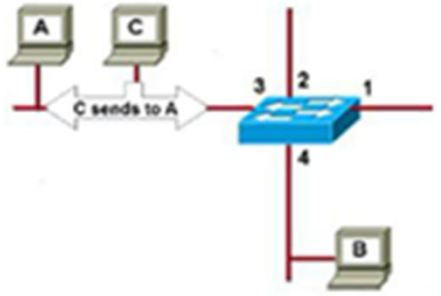
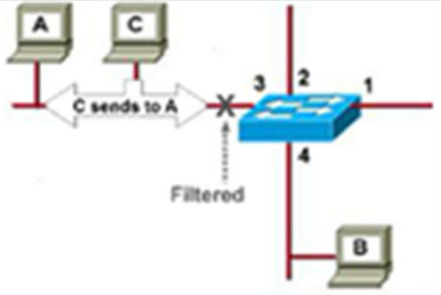
Illustration	Description
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3 MAC address of B | 4	As node A transmits a frame to node B, it reaches the switch.
 MAC Address Table in CAM Host MAC Address | Port MAC address of A | 3 MAC address of B | 4	The switch examines the destination MAC address of node B in the MAC address table, which is mapped to port 4, thus the frame is forwarded to port 4.

Function of Switch

Filtering Frames

- Filtering is a decision making process based on the **destination MAC address**.
- The process of not placing the frame out of the port is equivalent to **discarding the frame**.
- The switch examines the destination MAC address and consults the MAC address table for a match in the destination MAC address.
- If there is **a match** and the **incoming port is the same as the port indicated**, the frame is filtered.

Frame Filtering

Illustration	Description
 MAC Address Table in CAM: Host MAC Address / Port — MAC address of A / 3; MAC address of C / 3	• Node C transmits a frame to node A, it reaches the switch.
 MAC Address Table in CAM: Host MAC Address / Port — MAC address of A / 3; MAC address of C / 3	• The switch examines the destination MAC address and consults the MAC address table. Since there is a match and the incoming port is the same as the destination port, the frame is filtered. • Even though the frame is filtered, there is no harm done as node A has received the frame.

Example Involving Connected Switches

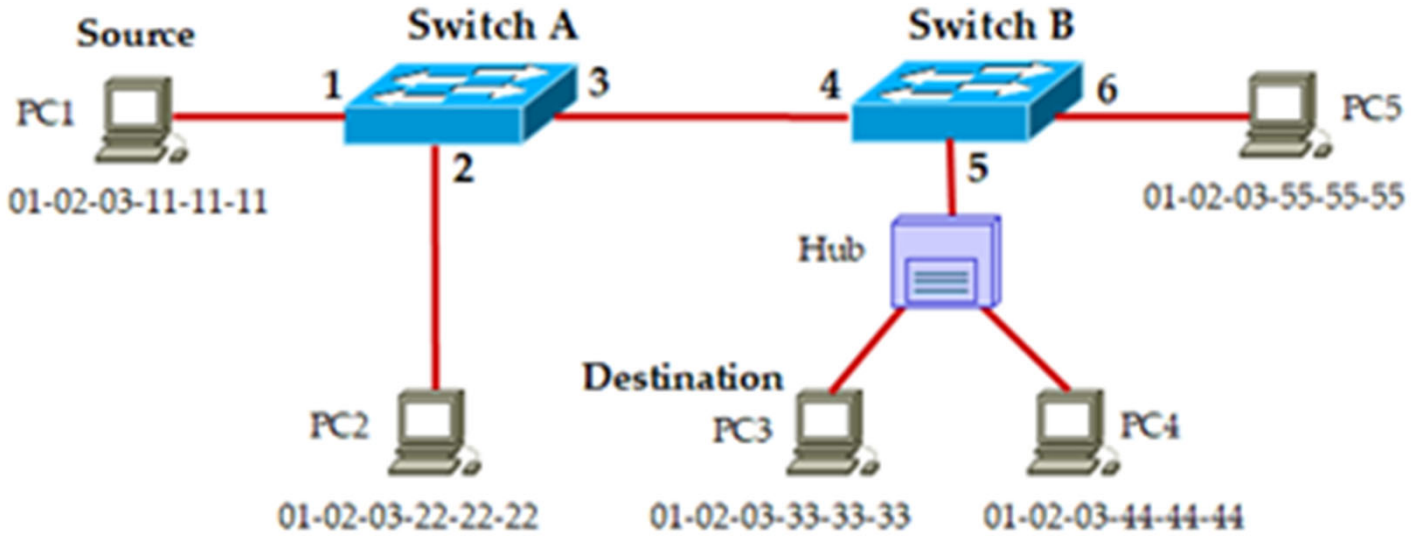
Example

For the scenario given below, explain how Switch A and Switch B respond if **PC1 is sending an Ethernet frame to PC3.**

Include any entry made to the MAC address tables during the process. Assume the MAC address tables of both switches were empty before the start of the process.

Switch A	
MAC Address	Port

Switch B	
MAC Address	Port



Example Involving Connected Switches

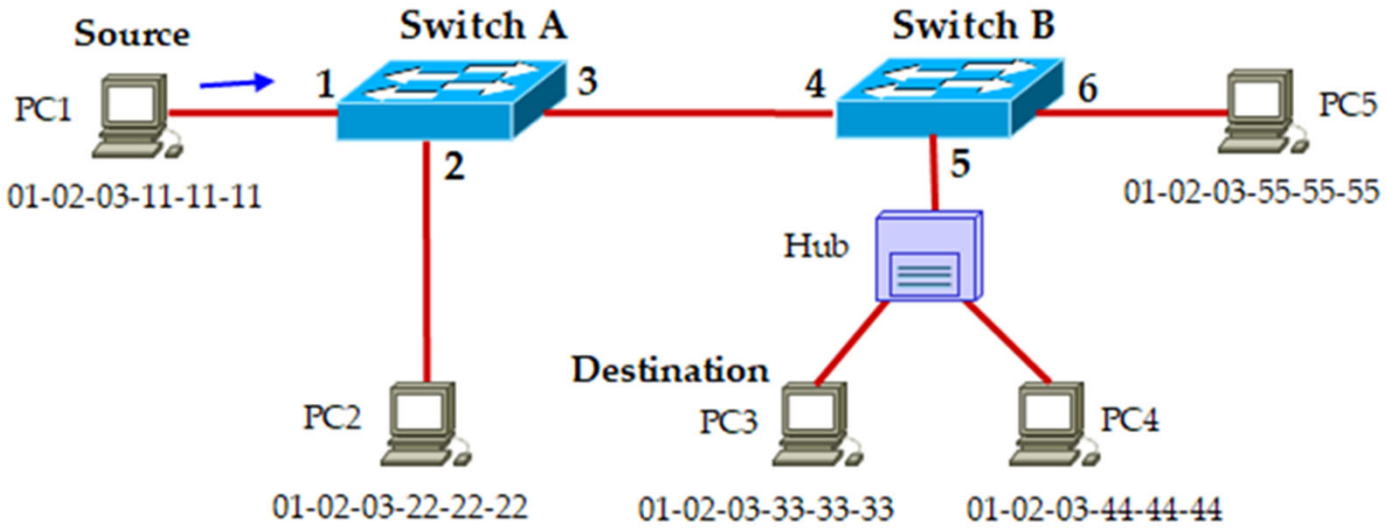
PC1 is sending an Ethernet frame to PC3

Learning MAC Address by Switch A

- As PC1 transmits a frame to PC3, it reaches Switch A.
- Since Switch A does not have a record of PC1's MAC address, Switch A enters PC1's MAC address and port 1 into the MAC address table

Switch A	
MAC Address	Port
01-02-03-11-11-11	1

Switch B	
MAC Address	Port



Example Involving Connected Switches

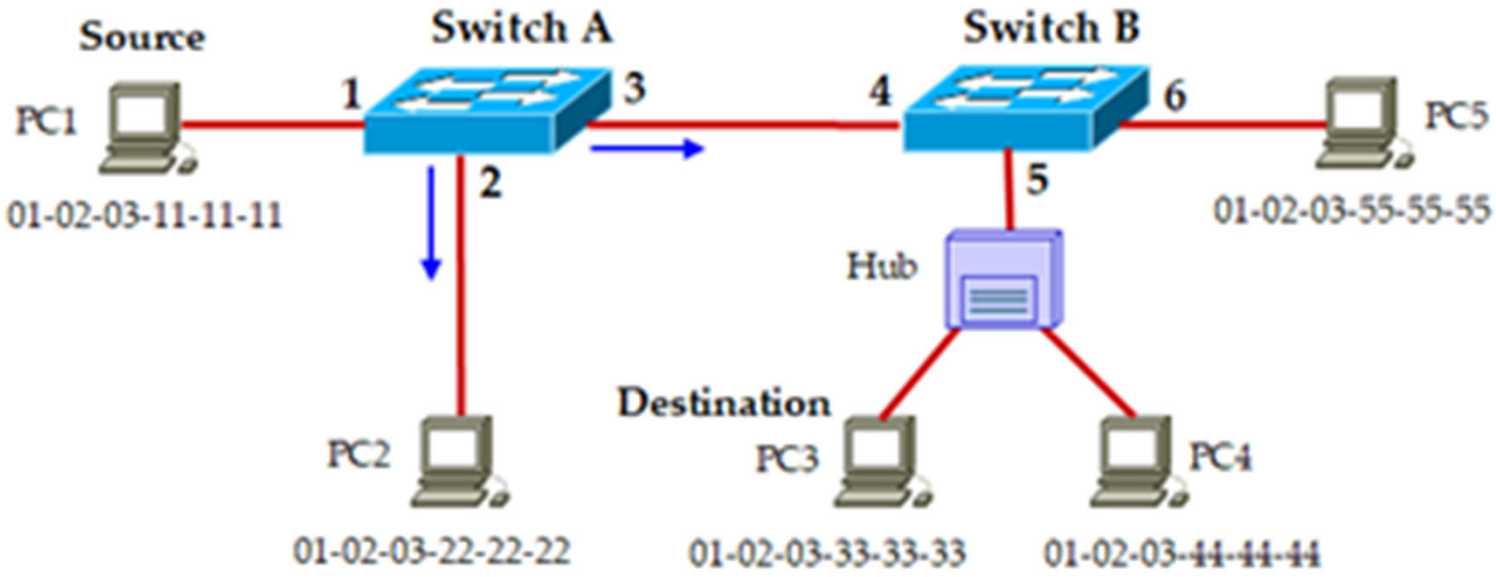
PC1 is sending an Ethernet frame to PC3

Flooding at Switch A

- Since Switch A has **no record of PC3** in its MAC address table, the frame is forwarded to all ports of Switch A except the incoming port.

Switch A	
MAC Address	Port
01-02-03-11-11-11	1

Switch B	
MAC Address	Port
01-02-03-11-11-11	**4**



Example Involving Connected Switches

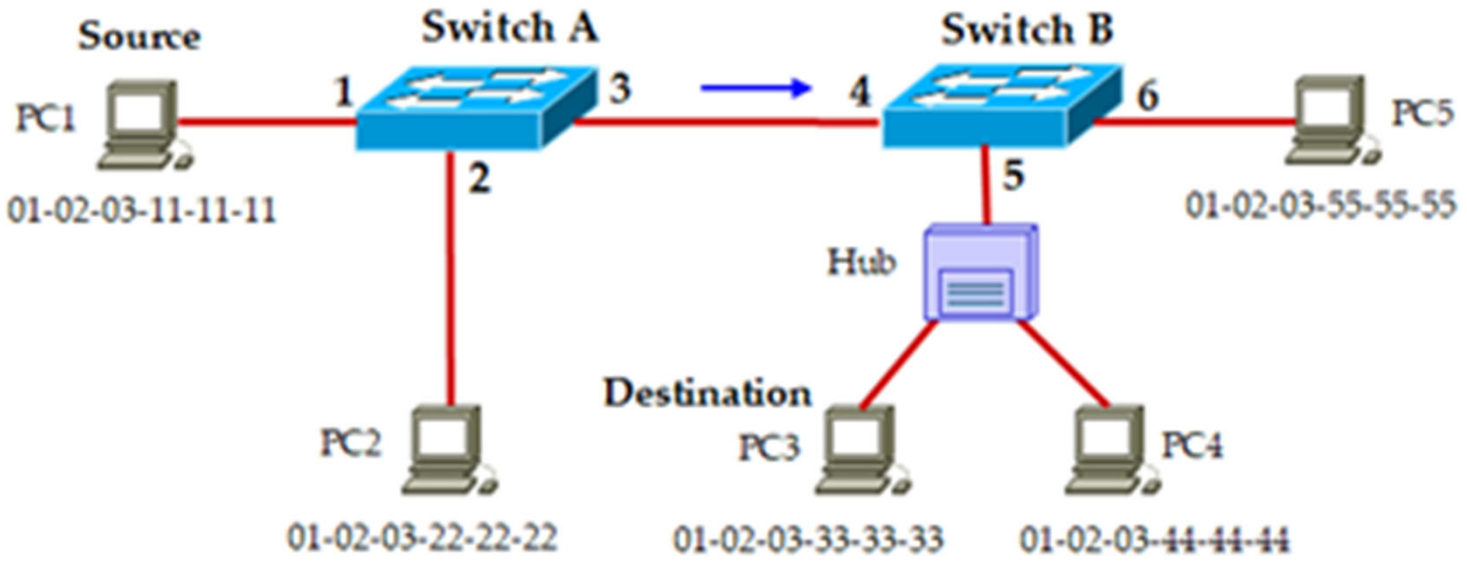
PC1 is sending an Ethernet frame to PC3

Learning at Switch B

- When the frame **arrives at Switch B**, **Switch B does not have a record of PC1's MAC address**, so it enters PC 1's MAC address and port 4 into its MAC address table.

Switch A	
MAC Address	Port
01-02-03-11-11-11	1

Switch B	
MAC Address	Port
01-02-03-11-11-11	4



Example Involving Connected Switches

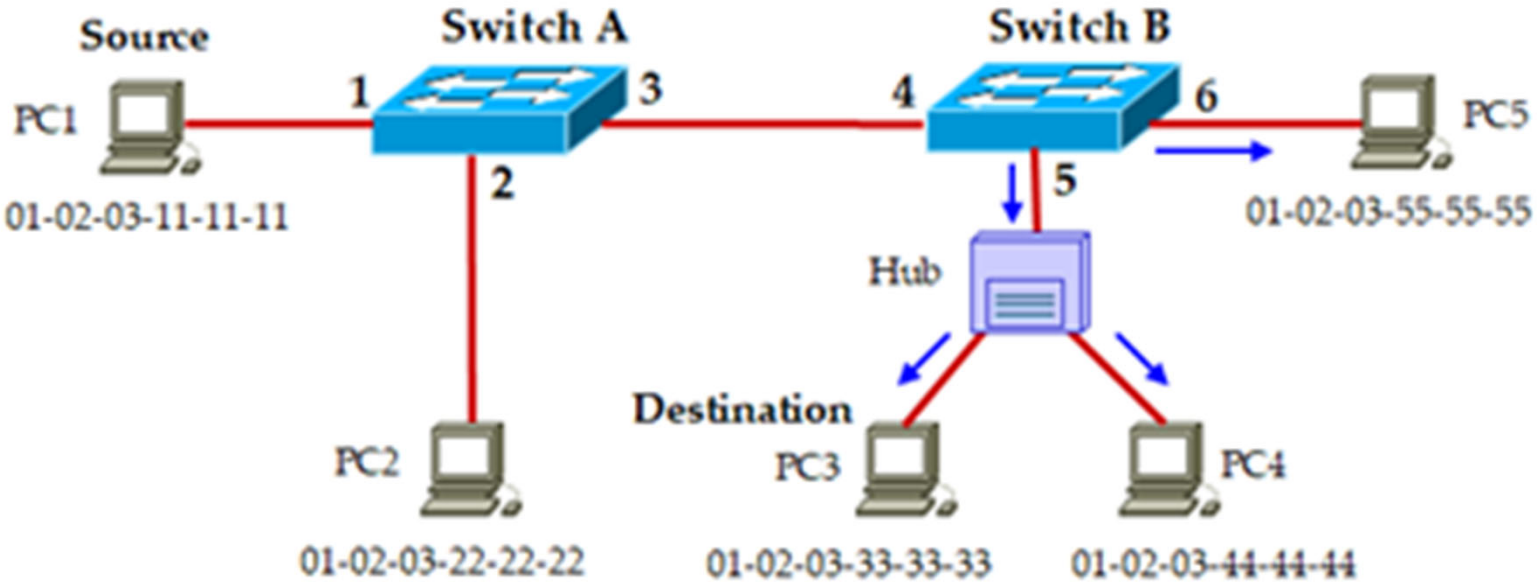
PC1 is sending an Ethernet frame to PC3

Flooding at Switch B

- Since **Switch B has no record of PC3** in its MAC address table, the frame is forwarded to all ports of Switch B except the incoming port.

Switch A	
MAC Address	Port
01-02-03-11-11-11	1

Switch B	
MAC Address	Port
01-02-03-11-11-11	4



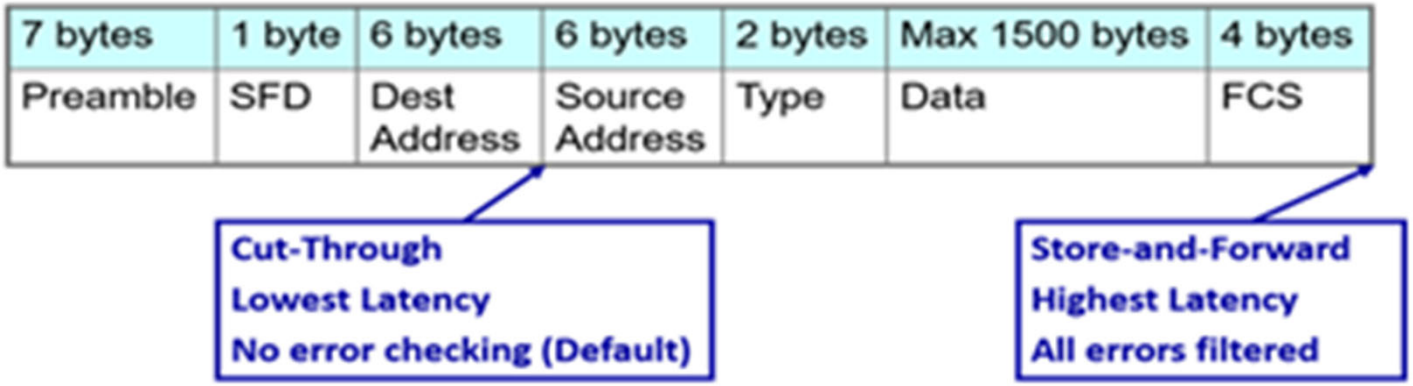
Switch Forwarding Methods

Store-and-forward switching

- Upon receiving the frame, the switch **copies the entire frame** into its buffer, **computes the CRC**, and **checks the length** of the frame.
- If the **CRC and frame length are valid**, the switch **looks up the destination address**, **determines the outgoing interface**, and **forwards the frame**.

Cut-through switching

- The switch begins to forward the frame as soon as the **destination address** and the **out-going interface** is determined.
- Cut-through switching is usually configured on switches on a **per-port basis**.
- Upon **reaching a** user-defined error **intolerant limit**, the switch will automatically **change to store-and-forward**.
- Once the **error rate drops** below the limit or within tolerant, the port will automatically **switch back to cut-through** switching mode.



Memory Buffering Techniques on Switches

Port-based memory buffering

- **Each port** on the switch **has a high-speed memory** to store frames until transmitted.
- Disadvantage: frames will be **dropped** when a port **runs out of storage**.

Shared memory buffering

- All frames are deposited into a **common memory buffer** that is shared by all ports on the switch.
- **Frames** are **linked dynamically** to the appropriate destination **port**.

Symmetric and Asymmetric Switching

LAN switching can be classified as ***symmetric*** or ***asymmetric*** based on the **data rate** on the switch ports.

Symmetric Switching

- Involves switching between **same data rate**, where all the ports on the switch have the same bandwidth, such as all 100 Mbps ports or all 1000 Mbps ports.

Asymmetric Switching

- Allows switching between **different data rates** on different ports.

Address Resolution Protocol (ARP)

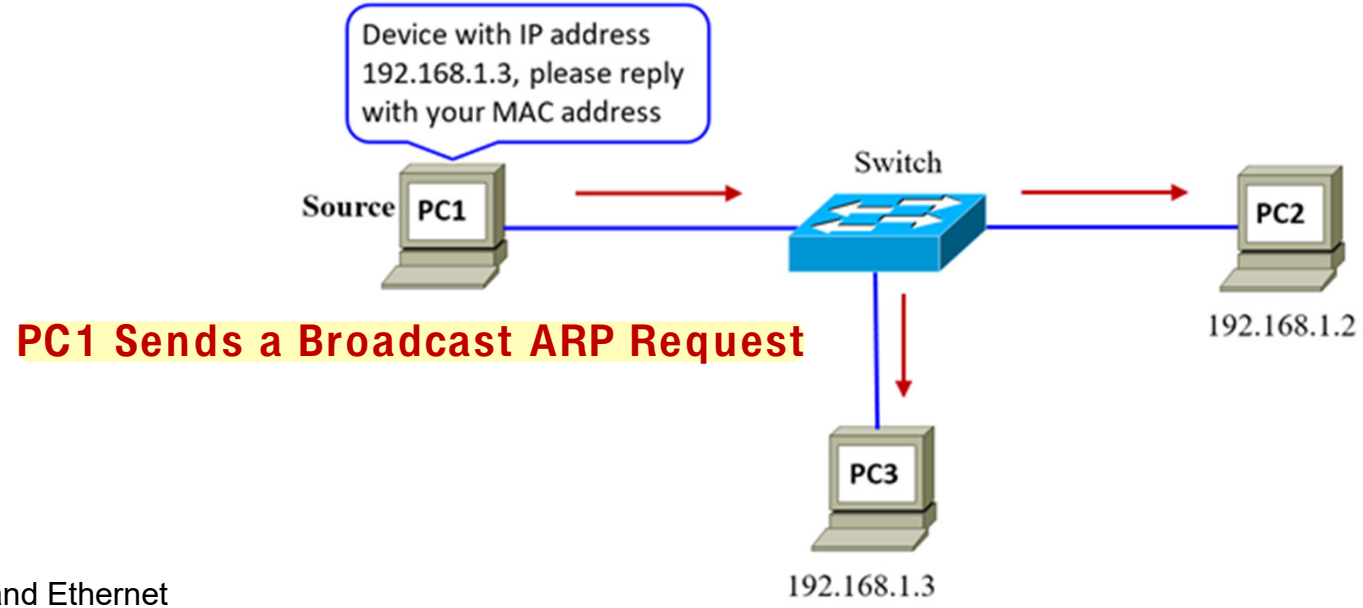
ARP Functions

- To send data to any device, the source must have both the **MAC and IP addresses of the destination device**.
- Sometimes, the **destination MAC address is not known**.
- The source device will **use ARP to determine the destination MAC** address.
- ARP provides two basic **functions**:
  - **Finding MAC addresses** from IPv4 addresses
  - **Maintaining** the **ARP table**

Address Resolution Protocol (ARP)

ARP Request

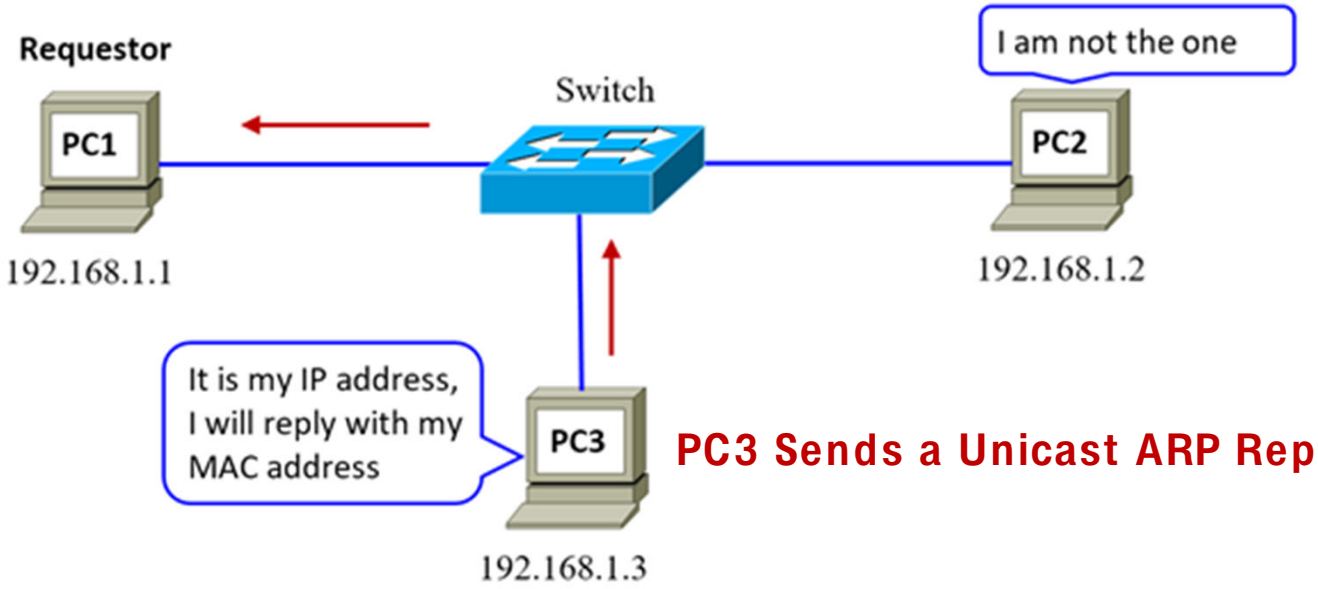
- When the data link layer received a packet from the network layer, using the destination IPv4 address in the packet, the source device **searches the ARP table** in its RAM **to find the MAC address**.
- If the source device is **able to find the destination IPv4** address and its corresponding MAC address, the destination MAC address will be used in the **frame encapsulation**.
- If the **IPv4 address is not found** in the ARP table, then the source device will send an **ARP request** by **broadcasting** the destination IPv4 to **all devices**.



Address Resolution Protocol (ARP)

ARP Reply

- Upon receiving the ARP request, devices with **no matching** IPv4 address will **ignore the ARP request**.
- The device with **matching IPv4** address will respond to the requesting device by sending a **unicast ARP reply with its MAC address**.
- Upon receiving the ARP reply, the requestor will **add** the IPv4 address and its corresponding MAC address **to its ARP table**.
- With the known MAC address, the data link layer can now **encapsulate** the packet into an Ethernet frame.
- If there is **no respond from any device**, the packet is **discarded** because a frame cannot be assembled.



PC3 Sends a Unicast ARP Reply

ARP Issues

ARP Broadcasts

- ARP request is **broadcasted** to all devices on the network. If large number of devices on the network is accessing network services at the same time, it can **affect the performance**.

ARP Spoofing or ARP Poisoning

- It is a **security risk**.
- ARP **does not keep track** of information to link **multiple communications** together. These create many possible attack points.
- An attacker can **reply** to an ARP request **with the MAC address of another device**, such as its own device. The receiver of the ARP reply will record the wrong MAC address to its ARP table and **send packets to the attacker's device**.
- Another possible attack point - an **attacker** can **send an ARP reply to** a target device (the **victim**) even though the target device has not sent any ARP request yet. It is possible for the **attacker** to **send fake ARP reply frames continuously** to the victim where the MAC address is forged to correspond to the attacker's device.
- Due to the vulnerability in ARP, **spoofing can take place on the source, destination, or anywhere in between where the traffic passes**. It is also possible to redirect traffic from the attacked device to a different destination.

Summary

- Purpose and functions of the physical layer in a data network
- Three main types of copper media used in networking
- Three types of UTP cables and their applications
- Purposes and functions of the data link layer in preparing for transmission on a data network
- Functions of physical and logical topologies in LAN and WAN
- Characteristics and functions of the data link layer frame
- Function of each of the Ethernet sublayers
- Characteristics and purpose of the Ethernet MAC address
- Learning, forwarding and filtering functions of an Ethernet switch
- Role of ARP in an Ethernet network

SUSS
SINGAPORE UNIVERSITY
OF SOCIAL SCIENCES

Thank You.