- March 15th, 2021
    - Ethernet
        - Last class the topic of discussion was data link layer
            - There are some parallels between data link layer and transport layer
            - Data link layer needs to provide services such as flow control, error detection, and error correction
                - These services are NOT unique to data link layer, and are also offered by the transport layer via TCP
            - Data link layer (also) provides specific/unique services
                - These unique services are required in situations where the transmission medium is shared, and multiple devices are connected
                    - The data link layer needs to determine which device gets to transmit at what time
        - This lecture focuses on two very dominant data link layer protocols
            - Ethernet
            - WLAN
                - Wireless local area network
    - IEEE 802 Protocol Suite
        - Ethernet and wireless lines/links are all part of the IEEE 802 protocol suite
            - It is a family of IEEE standards for body, personal, local area networks and metropolitan area networks
        - The IEEE 802 protocol suite corresponds to the lower 2 layers; data link layer and physical layer
            - In comparison, the TCP/IP protocol suite includes the application layer, transport layer, network layer, and data link layer
                - Up to the data link layer is the TCP/IP protocol suite
            - The data link layer in IEEE 802 protocol suite is actually the bottom layer in TCP/IP
                - It also specifies the physical layer of different technologies for local area networks
                    - 802.2 Logical Link Control (LLC)
                    - 802.3 Ethernet
                    - 802.11 Wireless Local Area Networks (WLAN)
                    - 802.15 Wireless Personal Area Networks (WPAN)
                        - i.e. Bluetooth, Zigbee, Body area networks, etc.
        - Within the IEEE 802 protocol suite, there is ethernet, wireless LAN (WLAN), and wireless personal area networks (WPAN)
            - Example of WPAN: Bluetooth
        - In order to make the layers on the services more scalable, the IEEE 802 protocol suite further divides/splits the data

link layer into 2 parts:

1. The top part corresponds to logical link control (LLC)
    - It is a sub-layer of the data link layer
    - It is across different data link layer technologies within the IEEE 802 protocol suite
    - It implements common services across different types of networks, whether it is ethernet or wireless LAN (WLAN) or wireless personal area network (WPAN)
        - i.e. Framing is a common service that is useful across all different technologies
        - i.e. Flow control or error detection MAY be implemented in the logical logical control
            - However, not all IEEE 802 technologies require flow control or error detection
                - But, if needed, this functionality can be implemented in the logical link control (LLC) layer
2. The bottom part corresponds to the media access control (MAC) layer
    - This part is below the logical link control layer, but it is still part of the data link layer
    - The media access control (MAC) and physical layer, when combined, are specific to the respective technology that is being dealt with
        - Ethernet, wireless LAN (WLAN), or wireless personal area network (WPAN), such as Zigbee or Bluetooth, have their own separate media access control and physical layer technology

- i.e. Diagram of TCP/IP & IEEE 802 Protocol Suite

```
    |-------------|
    | Application |
    |-------------|
    | Transport   |
    |-------------|
    | Network     |
    |-------------|
    | Data Link   |---------- LLC
    |             |---------- MAC
    |-------------|
    | Physical    |---------- PHY
    |-------------|

    |-----|------------------------------------|
    | LLC | IEEE 802.2 Logical Link Control (LLC) |
    |-----|----------|--------|---------|---------|
    | MAC | 802.3    | 802.11 |         | 802.15  |
    |-----|----------|--------| * * * * |---------|
    | PHY | Ethernet | WLAN   |         | WPAN    |
    |     |          |        |         |         |
    |-----|----------|--------|---------|---------|
```

  - The data link layer and the physical layer are fastly developing areas of industrial standard, as well as research
- Ethernet
  - Is the dominant wired local area network (LAN) technology
    - In other words, it is a very common data link layer technology
      - Most people deal with ethernet on a day-to-day basis, either directly or indirectly
  - The cost of ethernet network interface cards (NIC) has significantly decreased over time
    - On Amazon, a 1 Gpbs card can be purchased for roughly $20, and a 10 Gbps card can be purchased for roughly $100
      - Plus, ethernet network interface cards are becoming cheaper and cheaper, with time
      - Commonly, ethernet cards come pre-installed in laptops and desktop computers
  - Ethernet technology dates back to the late 70s and early 80s
    - It was one of the first widely used LAN technology
    - Ethernet pre-dates the TCP/IP protocol suite, because link layer technology provides connectivity among neighbouring devices
      - The entire TCP/IP protocol stack is not needed if communication and the exchange of information is restricted to the local environment/area
  - In addition to ethernet cards getting cheaper and better, the data rate, or throughput, provided by ethernet is also increasing overtime
    - 10 years ago, ethernet technology supported a throughput of 10 Mbps
      - Now, 400 Gbps is possible and used
        - However, 400 Gbps is quite expensive and tends to be utilized inside the core network among routers
  - i.e. Ethernet Diagram From Its Inventor

```
                |--- Tap
                |
                |   |--- Transceiver Station
                |   |
        * * *   |   |
          *     V   V                  |---|------|
          *     /||---|           |---||   |      |
          * ___/ || x |-----------| I || C |      |
          *    \ ||   |-----------|   ||   |      |
          *     \||---| Interface |-|-||   |      |
          *             Cable       |  |---|------|
          *                         |    |
          *                         |    |
          *                         |    |--- Controller
          *                         |
          *                         |--- Interface
          *
          *
          *
          *
          *                                     Terminator -----|
          *                                                     |
          *                                                     |
          *         |-----|     |-----|     |-----|             |
          *         |     |     |     |     |     |             |
          *         |-----|     |-----|     |-----|             |
          *          |---|       |---|       |---|              |
          *            |           |           |                |
          *            |           |           |                V
          *  <-------  V           V           V   ------>      *
          * * * * * * * * * * * * * * * * * * * * * * * * * * * *
                            |                     |             *
                            |                     |
                            |                     |
                            |                     |
                        The Ether             The Ether
```

- This is the sketch of the inventor of Ethernet
  - The inventor of ethernet is Metcalfe
- The story behind this sketch is that Metcalfe was in a cafe, and he started to think about how to interconnect devices through wires
  - Then, he drew this down on a piece of napkin
    - Supposedly, this is how ethernet was started
- According to the drawing, there are devices that have some kind of interface, and they are connected through some kind of bus topology
  - This is the earliest incarnation of ethernet; this dates back 20 years ago
  - Devices are connected through a shared medium, and utilize copper wires or even twisted pairs
- Currently, the most commonly used form of ethernet is switched ethernet

- Bus VS. Star Topology
  - Throughout the mid 90s, bus topology was very popular
    - In a bus topology, workstations with an ethernet interface interface interconnect via (some kind of) copper wire
    - Since bus topology is a shared medium, we have to determine what/which host gets to transmit
      - There has to be a way to arbitrate the medium access among different network interfaces that are connected along the bus
    - i.e. Diagram of Bus Topology

```
|---|       |---|       |---|       |---|
| H |       | H |       | H |       | H |
                  |---|       |---|       |---|       |---|
                    |           |           |           |
                    |           |           |           |
                    |           |           |           |
                ============================================
```

  - Currently, the star topology is the standard, and it has become more prevalent
    - In a star topology, devices can be connected through ethernet hubs or switches
      - Ethernet switches are the dominant devices used to interconnect other devices, like consumer electronics, in the Internet
      - Hubs similar to ethernet switches, and they can connect multiple devices
        - However, they are very limiting, because hubs are physical computers that cannot isolate different interfaces connected to them
        - Also, hubs are cheaper than ethernet switches
    - i.e. Diagram of Star Topology

```
                                 |-----|
                                 |  H  |
                                 |-----|
                                  |---|
                                  | I |
                                  |---|
                                    |
                                    |
                                    |
                                    |
                                    |
            |-----||---|         |-----|         |---||-----|
            |  H  || I |---------| LAN |---------| I ||  H  |
            |-----||---|         |-----|         |---||-----|
                                    |
                                    |
                                    |
                                    |
                                    |
                                  |---|
                                  | I |
                                  |---|
                                 |-----|
                                 |  H  |
                                 |-----|
```

  - In any network topology, whether the topology is bus or
star,
    devices interconnect with one another through hubs or switches
- Hubs VS. Switches
  - Assume that you want to connect devices in your home, or in

a lab, with Ethernet. The goal is to create your own local area network, via ethernet, and not Wi-Fi. To accomplish this, you have 2 options:

1. Ethernet Hubs
    - Hubs are layer-1 devices
        - This means that it only sees the signal on one port, that may be connected to the hub, replicates/duplicates the signal, and sends it to all other ports on the hub, which may have devices connected to them
            - Hubs are not intelligent, because they canno recognize ethernet frames. All they do is repeat the signal to other ports and devices
            - Devices connected to a hub are not directly connected to each other, but they do have physical connectivity
        - Since hubs are layer-1 devices, they have the same problem as bus topologies
            - Any transmission in a bus network topology will get replicated through the hub, and get sent to other devices, through the wires that are connected to the hub
            - The issue is that concurrent transmissions are not possible
                - If multiple devices are connected to the hub, and transmitting at the same time, then the hub will replicate the signal, and send it to all connected devices
    - Computers/devices connected by hubs are in the same contention domain
        - This means that they need to be able to resolve the contention, otherwise concurrent transmission may experience collision
            - This is a severe limitation of hubs
                - However, it may still be useful to connect local computers via a hub, because it is very cheap
    - i.e. Diagram of Ethernet Hub

```
                        |
                        |
                        |
                        V
                |--------------|
                | Message For  |
                | Computer "A" |
                |--------------|
                        |
                        |
                        |
                         |
                         V
                      |-----|
                      | Hub |
  |--------------|    |-----|    |--------------|
  | Message For  |   /   |   \   | Message For  |
  | Computer "A" |  /    |    \  | Computer "A" |
  |--------------| /     |     \ |--------------|
       ___________/      |      \_________
      /                  |                \
     /                   |                 \
    /                    |                  \
   /                     |                   \
   |                     V                   |
   |             |--------------|            |
   |             | Message For  |            |
   |             | Computer "A" |            |
   |             |--------------|            |
   |                     |                   |
   |                     |                   |
   |                     |                   |
   |                     |                   |
   |                     |                   |
   V                     V                   V
|----------|       |----------|      |----------|
| Computer |       | Computer |      | Computer |
| "A"      |       | "B"      |      | "C"      |
|----------|       |----------|      |----------|
```

    - In the diagram, 3 computers, "A", "B", & "C", are connected to a hub
    - An incoming message for computer "A", will be replicated/duplicated by the Hub, and then sent to all connected computers
    - Assume that both computer "A" and "B" transmit at the same time.
        - The packets sent from "A" will be replicated by the hub and sent to "B". Similarly, the packets from "B" will be replicated by the hub and sent to "A". This will result in some kind of collision between these packets
            - Therefore, computers connected by hubs are in the same contention domain
  - Simply put, hubs are physical layer repeaters
  - In terms of price, hubs are very cheap

2. Ethernet Switches
    - Are layer-2 devices that forward the messages to the selected port
        - This is possible because switches implement the bottom layer of the TCP/IP protocol suite

- i.e. Data link layer and physical layer

- Can interpret data link layer frames
  - For incoming frames, switches can determine which outgoing port the frame needs to be forwarded/delivered to
    - From this perspective, switches have some similarities between routers. However, switches operate at layer-2, rather than layer-3
      - Note: Layer-3 is the network layer
  - Switches are more intelligent than hubs
- Can forward messages to selected ports, and to computers that are connected by switches
- Computers that are connected to the same switch are in the same broadcast domain
  - This means that if a frame with its destination address is set to the broadcast address, it will be sent to all other ports, and will be received by the devices that are connected to the ports
    - The broadcast address corresponds to a destination address of FF:FF:FF:FF:FF
      - It is all 1's
    - In other words, all the devices that are connected to a switch can receive the broadcast message
      - Thus, these devices are within the same broadcast domain
- Unlike hubs, switches offer a point-to-point connectivity between a switch and the devices conneced to it, via a wire
  - This connection is a dedicated link, and it has full duplexity
  - Simply put, devices/computers and switches can transmit concurrently on the same wire
- When devices are connected to different ports on the switch, they can talk/communicate in parallel
- They key difference between a switch and a hub is that switches decide what to do with an incoming frame, and which port to forward it to
  - This is why switches are more expensive than hubs, because they are more intelligent
  - In general, switches are a better approach to connect your local devices
- i.e. Point-to-point link between a computer and a switch
- i.e. Diagram of Switch

```
                        |--------------|
                        | Message For  |
                        | Computer "A" |
                        |--------------|
                              |
                              |         |------------|
    |--------------|          |  _______| Computer A |
    | Message For  |          V /       |------------|
    | Computer "A" |           /
    |--------------|          /
                    |--------|          |------------|
    --------------->| Switch |----------| Computer B |
                    |--------|          |------------|
                              \
                               \
                                \_______|------------|
                                        | Computer C |
                                        |------------|
```

- Switches allow devices to talk in parallel
    - It is possible to have an incoming message for 'A', an incoming message for 'B', and an incoming message for 'C'
        - All incoming messages are sent to their respective destinations without experiencing any collision

- Even though there are a number of differences between hubs and switches, ultimately, both connect segments of LANs

- Ethernet Frame Structure
    - Sending adapter encapsulates IP datagram (or other network layer protocol packet) in Ethernet frame
    - i.e Diagram of Ethernet Frame

8	6	6	2	n	4
Preamble	Destination Address	Source Address	Type	Data	CRC

- The purpose/job of the 'Preamble' field is to indicate the beginning of the link frame, or when it has started
    - At the data link layer, it is very important to be able to separate frames, and be able to identify the start or end of an ethernet frame
    - In addition, the 'preamble' field contains information that allows the sender and receiver to synchronize their clocks
        - This allows them to decode the data that has been sent over the medium
    - In Ethernet, the 'preamble' field is 7 bytes long
        - It consists of a pattern of interleaving 1's and 0's, followed by 1 byte
            - i.e. 1010101011
        - The 'preamble' is used to synchronize the sender's clock with the receiver's clocks
            - Assuming that '1' indicates a high voltage and '0' indicates a low voltage, by interleaving

0's and 1's, the sender and receiver can synchronize their transmissions

- From a decoding point-of-view, it is important to be able to tell when a bit starts, and when a bit ends
- To be able to do this, the sender and receiver's respective clocks must be synchronized
  - If the clocks are not synchronized, then they may not be able to decode the pattern correctly

- Ethernet Frame Structure (More)
  - i.e Diagram of Ethernet Frame

```
         8           6            6        2      n     4
   |----------|-------------|---------|------|------|-----|
   | Preamble | Destination | Source  | Type | Data | CRC |
   |          | Address     | Address |      |      |     |
   |----------|-------------|---------|------|------|-----|
```

  - Destination & Source Address
    - After the 'preamble' is the destination address, and then source address
    - Both of them are their respective MAC layer address
    - Each address is 6 bytes long
    - The addresses are used to address the device that a particular frame is destined to
      - In a local area network (LAN), the destination address is used to determine whether a network interface should pass the frame to the appropriate upper layer protocols
        - i.e. If the destination address is a broadcast address, containing all 1's, then the frame will be passed to the upper layer(s). On the other hand, if the destination address differs from the MAC address that is associated with a particular device's network interface card (NIC), then the operating system (OS) will drop the frames, and prevent them from further processing
        - On the contrary, if a device is set to 'promiscuous mode', then the network interface card (NIC) will allow all frames to be passed on to the upper layer(s), irrespective of the frames' destination address
          - Promiscuous mode can be turned on via Wireshark
          - However, turning on promiscuous mode will add extra overhead, and processing, to a system
        - Typically, devices only accept frames that have a destination address that corresponds to its

own network interface, or a broadcast address

- A destination address that does not match the network interface is dropped

- Type
  - After the first 3 fields, preamble, destination address, and source address, is the 'type' field
  - The type field indicates the type of ethernet frames
    - i.e. Ethernet II, 802.2 LLC frame, etc.
- Data
  - Can contain almost anything, and has a variable size as a result
    - i.e. If the TCP/IP protocol suite is used on top of Ethernet, then the data could be the IP packet/ datagram coming from the network layer
  - Typically, the size of the payload is limited
    - i.e. Wireshark displays the typical maximum segment size (MSS) in the TCP layer
    - In TCP, the maximum segment size (MSS) is not limited because of the transport layer, it is due to the restrictions of the data link layer
      - i.e. For Ethernet, the typical maximum payload size is 1500 bytes.
      - To compute the maximum segment size (MSS) in TCP, simply subtract the length of the IP header, and then the length of the TCP header
        - This is how you may get something like 1460 bytes for MSS
    - Ethernet frames also have a lower bound, or a minimum size, of 46 bytes
      - If the data is less than 46 bytes, then it is padded with zeros until it reaches a size of 46 bytes
      - The lower bound is related to collision detection in a shared medium ethernet
    - Limiting the maximum size of an ethernet frame is inefficient because it already contains its own information, which has its own overhead
      - i.e. The preamble is 8 bytes, the addresses are 12 bytes, the type is 2 bytes, and the CRC is 4 bytes
- CRC
  - Stands for cyclical redundancy check (CRC)
  - It is an error detection mechanism that determines if there is any bit error within the ethernet frame
    - This helps the receiver to determine whether the frame has been received correctly without any errors
      - If there is a bit error, or the frame fails the cyclical redundancy check (CRC), then the corresponding frame is dropped
  - The size of the 'CRC' field is 4 bytes

  - All the fields in Ethernet frames are overhead
    - It is overhead on top of actual data that needs to be sent from the network layer
      - Considering the MSS, the overhead is simply too much
    - Currently, ethernet technology supports 1/10/100 Gbps connections for local area networks. The throughput that is çurrently available is much greater than the old days. Thus, current standards support 'jumbo frames'
      - Jumbo frames allow an MSS of up to 9000 bytes, which is much greater than the typical MSS of 1500 bytes that is allowed for current frames/packets
        - Thus, the actual MSS can change depending on what technology is deployed
        - Jumbo frames are used because limiting the maximum size is inefficient
- Unreliable, Connectionless Service
  - Using Ethernet as a data link layer technology provides some messaging services for the data link layer
    - Recall from previous lectures that the data link layer is concerned with the connectivity between physical devices that are in the same local area network. On the other hand, the transport layer is concerned with connectivity among end systems, and the processes on those systems that are not necessarily connected, but are reachable via multiple hops
  - Compared to other technologies, Ethernet is very simple, because it does not do reliable data transfer or connection setup/tear down
    - This is one of the many reasons why ethernet interface cards are cheap and inexpensive
  - Ethernet does not support any kind of connection setup or connection tear down
    - This is done to make things simple
      - As long as two entities are physically connected, they can send data to each other at anytime
    - There is no handshake between the sender's adapter, and the receiver's adapter
      - It is connectionless
    - In contrast, technologies like Bluetooth are connection oriented
      - i.e. If a device, such as a phone, wants to send a large amount of data to another device, then they need to setup a connection. The devices must go through some kind of handshake, where messages are exchanged between the devices, and a connection is setup after the exchange
        - A similar procedure takes place for something as simple as connecting wireless headphones to a smartphone, via Bluetooth
  - Ethernet does NOT ensure reliability of data transfer; it

does not even support it
    - Data that is transmitted over ethernet can be lost or corrupted for a variety of reasons. However, ethernet does not make any attempt, at the data link layer, to recover lost messages or fix corrupted messages. It does not utilize (negative) acknowledgements to notify the transmitter if a frame has been successfully received.
        - Although, it does perform error detecion to detect corruption of messages.
    - As a result, from a network layer point of view, the stream of frames that is passed on to the network layer may have gaps in between
        - The gaps correspond to lost frames due to collisions, or the frame may have been dropped at the data link layer, due to corruption.
        - Ethernet makes no attempt to "fill-in" the gaps. It relies on the upper layer protocol (i.e. TCP) to perform packet retransmission if necessary
            - If TCP is used, then the applications exchanging data with one another won't notice the gaps
                - If UDP is used, then the applications will notice gaps in the data stream
  - Reliability in wireless LAN (WLAN) is different than reliability in ethernet
    - The key difference in reliability between these two transmission mediums is the bit error rate. A wire, whether it is copper or high-speed optical fiber, the bit error rate tends to be extremely low. Where as, the bit error rate for wireless technologies are high
    - The assumption is that bits are unlikely to be corrupted when transmitted over a wire. Thus, the chances of packet loss or corruption over a wire in ethernet is extremely low. Therefore, there is no need to implement reliable data transfer
        - However, packet loss/corruption does occur in a wire, but it is so rare that implementing reliable data transfer does not make sense due to the added complexity, and increase in hardware cost
            - Simply put, it makes no sense to implement reliable data transfer for an event so rare that it occurs once in 10s of gigabytes of data transfer
        - Not implementing reliable data transfer is an engineering decision to tradeoff reliability for cost and ease of use
- Medium Access Control In Ethernet
  - Depending on what type of ethernet technology is being utilized, bus topology or star topology using hops, issues such as medium access need to be handled

  - In either topology, all devices and hosts that are connected to the ethernet will be part of the same (shared) medium
    - Thus, transmission on a particular device will be heard by all other devices on the medium, causing concurrent transmission to suffer from collision
      - Therefore, instead of letting all devices go crazy and send whatever data they want, shared medium ethernet has a mechanism called carrier sensing multiple access with collision detection (CSMA/CD)
  - Note: In a shared medium ethernet, the nodes are half duplex so they cannot send/transmit and receive at the same time. The nodes must take turns when it comes to transmissions
- The issue of medium access control is less problematic when dealing with point-to-point connections in a star topology with switches
  - This is because switches are effective at isolating the communication between switch ports and devices that connect to the ports
    - Thus, all pairs of devices to their ports are point-to-point, and concurrent transmissions are allowed on different links
      - Therefore, point-to-point ethernets are full duplex, which allows devices to send/transmit and receive at the same time
  - Instead, the issue is, "How does the switch know which port a device is connected to?", and not, "What device gets to talk at what time?"
    - When a switch receives a frame with a certain destination MAC address, the switch needs to be intelligent, and figure out which outgoing port the frame needs to be forwarded to?
      - This is similar to routers that operate on the network layer. Upon receiving a packet, the routers need to decide which outgoing interface a particular packet needs to be forwarded to, based on its destination IP address
        - Similarly, ethernet switches need to figure out which outgoing port a frame needs to be forwarded to
      - Ethernet switches use an algorithm to intelligently determine which port a packet needs to be forwarded
- Even though switch ethernet is the best, most dominant technology used to connect devices, it is important to learn about shared medium
  - This is because shared medium is common in wireless networks, and there are a lot of things that can be

learned from 'CSMA/CD'. By understanding how 'CSMA/CD' works, it becomes easier to understand a more sophisticated medium access control in wireless LAN called 'CSMA/CA'. The difference between 'CSMA/CD' and 'CSMA/CA' is the last letter. The 'D' in 'CD' stands for detection, and the 'A' in 'CA' stands for avoidance
    - Hence, it is useful to learn 'CSMA/CD', so it becomes easier to build upon the current knowledge of 'CSMA/CD' from shared medium ethernet to discuss medium access control in wireless LAN
- CSMA (Carrier Sense Multiple Access)
  - The purpose of medium access control, or 'CSMA/CD', in ethernet is to determine who gets to transmit
    - Since the medium is shared, concurrent transmissions will cause collisions
      - The shared medium problem is analogous to conversing in real life, talking to others in a Zoom meeting, and socializing with a group of friends. So, what cues do humans use to decide when it is their turn to talk? What happens when two people talk at the same time? How is this conflic resolved? What communication strategies do humans use to ensure that communication goes smoothly.
        Some ideas are:
        - Employ a meeting organizer that determines who gets to talk
          - This is a good idea, but it is not used in ethernet. However, it is used in other protocols, like token-based protocols, such as token buses; which were invented by IBM
            - The general idea is that a token is passed around, and whoever holds it is allowed to talk, while everyone else listens
            - This idea is too complicated for the minimalistic approach taken by ethernet, which does not require arbitration or tokenization
        - Talk when other people are not talking
          - This is common sense, and generally regarded as good social etiquette
            - Do not talk when other people are talking
          - If someone wants to talk, they listen to see if other people are talking or not
            - If there is a period of silence, then someone else can start talking
        - If two people are talking at the same time, then both of them immediately stop talking. But, how do they restart the conversation again?

                - Typically, they wait for a period of time, and then start talking. However, it is likely that 2 people can start talking again at the exact same time. They wait again, and maybe they wait a little longer. It is probable that one person is very eager to talk, and the other person is not eager, and can wait or defer their talk
        - 'CSMA/CD' functions very similar to humans in their day-to-day interactions, and conversations in a Zoom meeting or a phone call with multiple friends
            - The general idea is to avoid transmission of data when other devices are transmitting, because concurrent transmissions will result in collisions, and packets will not get delivered.
            - If collision is detected, because multiple devices are simultaneously transmitting, then those devices immediately stop transmitting
                - Continuing to transmit is a waste of resources, because the packets won't be delivered
            - After collision is detected and transmission is ceased, 'CSMA/CD' has a mechanism called backoff, which allows the transmitter to wait a period of time before it attempts to transmit again
                - If, after the timer ends, another device is transmitting, then the other devices will wait for the transmitting device to stop
        - 'CSMA' stands for Carrier Sense Multiple Access
            - Simply put, it means "listen before transmitting", or "listen before talking"
                - If a channel is sensed as idle, then the entire frame is transmitted
                - If the channel is busy, then you defer the transmission until the channel/medium becomes idle
        - The downside to 'CSMA/CD' is that it does not eliminate all possible collisions or concurrent transmissions
            - Even though devices will wait until the medium is available, it is possible that multiple devices will start transmitting at the same time, which will cause collisions
                - Since all devices are waiting for an idle medium, upon detecting it, they will all start transmitting, which will result in a collision
    - Collision In CSMA
        - CSMA reduces, but does not eliminate collisions
            - Propagation delay is a one of many reasons why collisions still occur in CSMA
                - Note: Propagation delay is the time it takes for the information/message to travel through the medium

  - Assume there are 4 devices ('A', 'B', 'C', & 'D') in a bus topology network
    - Devices that are further away from the receiver, their messages will take longer to transmit than messages sent from devices that are closer to the receiver
    - At time 't_0', 'B' decides that the medium is idle, so it transmits a frame
      - Note: The entire network is using CSMA, including 'B'
      - The transmission time, of any frame, is the length of the frame, L, divided by the throughput of the ethernet medium, R
        - The equation is: (L/R)
    - Surrounding devices on the bus will see a (start) signal transmitted from 'B' at different times
      - Also, the signal will end at different times relative to the devices
        - Both start signal and end signal are different for all devices on the bus topology, because of propagation delay
      - i.e. For 'B' the signal starts transmitting at time 't_0', but for 'D' the signal starts transmitting at time 't_1'
        - This is propagation delay; the signal takes time to propagate from 'B' to 'D'
    - Due to propagation delay, collision may still happen because the devices think that the medium is idle, which prompts them to start transmitting
      - When 'B' starts to transmit, the other devices are not notified until later. So, 'D' starts to transmit its data as well. After some time, 'D' receives the transmission from 'B', but it is already too late, because 'D' started its own transmission
        - As a result, transmission from 'D' will collide with 'B', because they overlap.
        - This is why there are (still) collisions in CSMA
  - When collision is detected devices will listen to the medium, and when they start transmitting, they will see whether there is something beyond what they are transmitting
    - This is how ethernet interfaces detect collisions
      - Based on things like power level detected from the wire, devices can determine if another signal is present, which indicates that another device is transmitting. Thus, a collision is present
    - When collision occurs, the receiver cannot decode anything, because the two, or more, sources of information overlap with one another
- CSMA/CD
  - i.e. Flowchart of CSMA/CD Protocol

```
              |---------|             NO
```

```
    |----->| Packet? |<-----------------------------|
    |      |---------|                              |
    |              |                                | NO
    |              |                                |
    |              |       clear                    |
    |              V         |                      |
    |           |---------|  |  |------|     |-----------|
    |           | Sense   |---->| Send |---->| Detect    |
    |    |----->| Carrier |     |------|     | Collision |
    |    |      |---------|                  |-----------|
    |    |                                          |
    |    |                                          |
    |    |                                          | YES
    |    |                                          |
    |    |                                          V
    |    |                            |------------------|
    |    |        attempts < 16       | Jam channel      |
    |    |----------------------------| b=CalcBackOff(); |
    |                                 | wait(b);         |
    |                                 | attempts++;      |
    |                                 |------------------|
    |                                               |
|---------|                                         |
| Discard |          attempts == 16                 |
| Packet  |<----------------------------------------|
|---------|
```

  - This is the flowchart of the 'CSMA/CD' protocol
  - `b` is the wait period
    - It is calculated by the 'CalcBackOff()' function
    - It is roughly equal to:
      `b` ~ (0, 2^(attempt - 1) * slot_time)
  - `attempts` is a counter that keeps track of how attempts the CSMA/CD protocol has made to send/transmit the frame/packet
- Upon detection of collision, the (ethernet) interface should immediately stop transmitting
- The (ethernet) interface determines whether a packet needs to be transmitted or not
  - Potentially, the device driver will pass a frame to the network interface queue, and the interface will sense the medium/carrier
- The purpose of sensing the medium is to determine if there is any transmission that is currently ongoing in the medium
  - If the medium is clear (i.e. No transmissions), then the device will go ahead and send/transmit the frame
- After starting a transmission, the sender will continue to monitor the medium, to see if there is any other simultaneous transmission
  - It does this by utilizing mechanisms such as

checking the power level in the medium

- If there is no collision, then the sender can assume that there is a very high chance that there is no other ongoing transmission, and its own transmission was successful
  - In ethernet, because connectivity is wire-based, as long as there is no collision, then the chance of packet corruption is very low
    - Thus, in the absence of collision, a link layer frame will be successfully delivered
  - Since the transmission is successful, the value of 'attempts' is set to 0
- Upon successful transmission of a packet, the sender moves onto the nex packet in the queue, and attempts to transmit it
  - The value of 'attempts' is 0
- In the situation where other devices transmit their frames over the medium, causing a collision, the ethernet device will perform 'jamming'
  - Collision can be caused by multiple senders transmitting their frames at once over the medium
    - This is similar to real life, where multiple people are talking in a (Zoom) meeting
  - The process of 'jamming', jams the channel
- After jamming the channel, the sender will determine a value to wait, for a period of time, before making its next attempt
  - This value is determined via a function called 'CalcBackOff()'
- The 'CalcBackOff()' function calculates a value from the following interval randomly: `0 - 2^(attempt - 1)`
  - If the initial 'attempt' value is 0, then the right-end of the interval is 1; an arbitrary value from 0 to 1 is selected
  - Note: The result of the 'CalcBackOff()' function should always be an integer
  - If the value of 'attempt' equals 3, then the interval ranges from 0 to 7
    - A value is uniformly selected from this interval and the result is multipled by the slot time
  - The result from the 'CalcBackOff()' function, and subsequent operations, is the amount of time, or the number of slots multiplied by the slot time that the sender will wait until it attempts the next transmission
- The 'attempts' value is reflective of how many tries, or retransmissions, have been done
  - It is also indirectly indicates congesion in the network
    - Thus, it is a good idea to adjust the backoff

interval, `b`, based on the value of `attempts`

- Assuming that the medium experiences collisions, by the end of this procedure, the 'attempts' value will increase
  - The bigger the size of the 'attempts' value, the bigger the size of the interval
    - This is because a value in the interval is uniformly chosen; the average amount of time that the sender will wait is roughly: ((2^(attempts - 1)) / 2)
    - On average, the larger the interval, the longer the wait time
    - This makes sense, because more collisions must mean that more people are attempting to transmit their frames, and the network might be congested
      - Thus, it is better to wait an extended period of time. The general idea is to let others do their retransmission before attempting to do your own retransmission
        - If a sender insists on immediate retransmission, then there is a good chance that collision will be experienced again and again
  - In ethernet, the maximum value of `attempts` is 16
    - It will try 16 times, and if the packet still cannot be sent/transmitted without experiencing collisions, then the packet is dropped
      - This is describes the unreliable nature of the data link layer protocol; it does not guarantee reliable data transfer
    - After 16 failed attempts, it will give up and try the next packet

- March 17th, 2021
  - CSMA (Carrier Sense Multiple Access)
    - The content discussed is carrier sense multiple access with collision detection in a shared medium Ethernet
    - The basic idea behind CSMA/CD is that a station or transceiver needs to listen to the medium before it can begin transmitting frames/packets
      - Transmission is allowed only if the medium/channel is sensed to be idle
      - If the medium/channel is busy, then the station/sender needs to defer its transmission
    - The golden rule of CSMA/CD is too NOT interrupt other stations/senders when they are transmitting
    - CSMA does not eliminate all collisions, it just reduces them
  - Collision In CSMA
    - During the transmission, the station/sender continues to listen to the medium to detect whether there are any

collision(s)

- It is possible that another station/sender tries to transmit/send its own frames/packets

- CSMA/CD reduces, but does not eliminate, collisions
  - i.e. If 2 stations both sense an idle medium, and start transmitting at the same time, then a collision may occur
  - i.e. The first station's transmission may propagate to the second station after the second station has started transmitting
    - Transmission may differ by a small time interval

- CSMA/CD
  - i.e. Flowchart of CSMA/CD Protocol

```
           |---------|              NO
    |----->| Packet? |<-----------------------------|
    |      |---------|                              |
    |              |                                | NO
    |              |                                |
    |              |       clear                    |
    |              V         |                      |
    |           |---------|  |  |------|     |-----------|
    |           | Sense   |---->| Send |---->| Detect    |
    |    |----->| Carrier |     |------|     | Collision |
    |    |      |---------|                  |-----------|
    |    |                                          |
    |    |                                          |
    |    |                                          | YES
    |    |                                          |
    |    |                                          V
    |    |                            |------------------|
    |    |        attempts < 16       | Jam channel      |
    |    |----------------------------| b=CalcBackOff(); |
    |                                 | wait(b);         |
    |                                 | attempts++;      |
    |                                 |------------------|
    |                                               |
|---------|                                         |
| Discard |          attempts == 16                 |
| Packet  |<----------------------------------------|
|---------|
```

- To resolve contention, CSMA/CD utilizes a mechanism called exponential backoff
- Upon collision detection, the station will continuously send some signals through the medium to jam the channel
- The purpose of jamming the channel is to ensure that other stations are able to detect the collision
  - After this, the stations will choose a value from an interval in the range: 0 - (2^(attempts - 1))
    - On average, this value willl increase as more retransmissions are needed. Stations/senders

will wait for the calculated period of time, and then attempt retransmission

        - This mechanism is similar to exponential increase, and not exponential decrease
          - Although, there is an exponential decrease in the throughput of the transmission from the station/sender
- Collision In CSMA/CD
  - Question: What is the purpose of jamming?
    - Jamming is needed even after detection of collision. It informs all other stations that they should not transmit
  - Assume there are 4 stations: 'A', 'B', 'C', & 'D'
    - After determining that the medium is idle, Station `B` makes its first transmission at time 't_0'
    - At time 't_1', before the wave from station/sender `B` arrives at station/sender `D`, `D` makes its first transmission
      - When the wave from station/sender `D` propagates to station/sender `B`, then `B` will be able to detect collision, because `B` is continually listening to the medium, even after it makes its first transmission
        - Station/sender `B` will know that a collision has occured, because of the extra energy in the transmission medium, on top of its own energy
        - Upon detecting collision, station/sender `B` will stop transmitting its own data, and start transmitting a jamming signal for a short period of time
          - The jamming signal from station/sender `B` will be propagated through the medium, and it will be detected by other stations
            - Upon reception of this jamming signal, station `D` will stop transmitting its own data, and begin transmitting a jamming signal, for a short time period
      - Station/sender `B` and `D` can tell that collision has occurred
    - After the jamming signal is sent, the transmitting stations/senders will abort all transmissions, and the medium will be idle
- Limits On CSMA/CD Network
  - The actual characteristics of ethernet in a shared medium context is dictated by topology
    - Traditionally, in a shared medium context, the stations are connected through a bus topology
      - There are limitations on the distance of the buses, because as signals propagate through the medium it tends to attenuate, and the actual propagation delay on the transmission medium will depend on the

physical length of the link

      - i.e. If station `A` were to send a packet, at time `C`, to station `B`, then `B` will see the mediu to be idle until time `t + D`, which can be calculated by the length of the link divided by the speed of light
        - This is the primary cost for collision in a shared medium; stations don't immediately know if another station is broadcasting. To them, the medium is idle
- Assume that are 4 stations - 'A', 'B', 'C', & 'D' - in a bus topology
  - For station `B` to be able to detect a transmission from station `D`, it will have to wait until the signal from station `D` propagates to station `B`
    - Now, suppose that the frame `B` transmits/sends is short, meaning that station `B` will finish its transmission before the signal from `D` arrives. In this situation, `B` would wrongly assume that its transmission is successful, because station `B` does not see an overlay of transmission power, which is the result of signals coming from station `D`
  - If `B` finishes its transmission at a particular time, then from its point-of-view everything seems OK
    - However, this is not nescessarily the situation for the intended destination of the frame sent from `B`. For instance, if station `C` is the destination address for all frame(s), then the collision between the signals sent by `B` and `D` starts around a different time. It is at this time that station `C` will see a signal coming from `B` and `D`
    - The transmission from station `B` will finish at a particular time, and can be modeled by the equation: (t_0 + L/R)
      - Part of the frame sent from `B` will experience collision from `D`. When this happens, station `C` will not be able to correctly decode the data from station `B` or `D`, because their frames are partially overlapped
        - From the point-of-view of station `B`, it assumes that the transmission is successful and collision free, because it thinks that there are no other signals on the wire. However, from the receiver's point-of-view, it cannot decode the frame from station `B`
          - This is a huge problem
        - This is precisely the reason why frames must have a minimum frame size. The frame sizes need to be sufficiently large so that this situation will not happen

- If the maximum propagation delay in the network, like a bus topology, is known, then it can be used to determine the minimum frame length. The maximum distance is determined by the signal propagation attenuation in the medium
  - Ethernet frames have minimum size, due to this reason

- If a frame is shorter than the minimum frame size, then it needs to be padded with zeros, at the end,
  - This makes sure that the minimum frame size requirement is met
- The purpose of sending a jamming signal is to ensure that every station in the medium is notified that a collision has occurred.
- To summarize:
  - Latency depends on the physical length of the link
    - This is the time to propagate a packet from one end to the other end
  - Latency has implications on minimum frame size
- i.e. Figure of Stations Communicating

  ```
  |---|       latency d       |---|
  | A |=======================| B |
  |---|                       |---|
  ```

  - Suppose station/host `A` sends a packet at time `t`
    - Station/host `B` senses an idle medium just before time `t + d`. So, `B` starts transmitting its frames/packets
      - Station/host `B` detects a collision, and sends a jamming signal. However, station/host `A` cannot see the collision until time `t + 2d`
  - This figure demonstrates the reason why there needs to be a minimum frame size

- Switched Ethernet
  - Currently, switches are the most prevalent ethernet topology or configuration scheme in local area networks
    - Compared to shared medium ethernet, ethernet switches have many advantages
  - Switched ethernet is mostly comprised of switches, apart from the transmission medium, which can be a twisted wire, fiber optics, copper cable, etc.
    - Unlike hubs, switches are link layer devices that have the ability to store and forward ethernet frames
  - In order to determine what outgoing port an ethernet frame needs to be forwarded to, the switch needs to examine the frame header field, and selectively forward the frame/packet based on the destination MAC address
  - From the point-of-view of hosts, they do not see the presence of switches, nor are they aware of the existence of switches

- From the perspective of hosts, it is as if they are directly connected to one another. Hosts do not realize that they are connected to different ports on a switch

- Switches operate at layer-2 in an obstructive manner
  - This style of operation is very different from routers
    - In routers, the sender has to configure the routing table to send data directly to the destination host within the local area network. However, if the destination is outside, then the packet is forwarded to the router, by utilizing the IP address of the router
      - ARP is used to determine the MAC address of the router, and then the host will be able to send link layer frames to the router
    - In comparison, switches are transparent to hosts, while a router's information needs to be configured at the host
- Switches are very convenient to use, because the entire operation is done via plug and play, and without needing to explicitly configure the topology or provide information about how many hosts are present, and how many hosts are connected to a particlar port
  - Switches can learn the connectivity, and utilize this information to make accurate forwarding decisions for link layer frames

- Forwarding
  - i.e. Diagram of a LAN Connected Via Switches

```
                        |---|
                        | S |
                        |---|
                       /  |  \
                      /   |   \
                     /    |    \
                    /     |     \
                   /      |      \
                1 /     2 |     3 \
                 /        |        \
                /         |         \
               /          |          \
|---|  1  |---|         |---|         |---|  3  |---|
| H |-----| S |     |---| S |---|     | S |-----| H |
|---|     |---|     |   |---|   |     |---|     |---|
         /  |       |     |     |       |  \
        /   | 3     | 1   |     | 3   1 |   \
     2 /    |       |     |     |       |    \ 2
      /   |---|     |     |     |     |---|   \
     /    | H |     |     |     |     | H |    \
|---|     |---|     |     | 2   |     |---|     |---|
| H |               |     |     |               | H |
|---|             |---|   |   |---|             |---|
| H |   |   | H |
|---|   |   |---|
        |
      |---|
      | H |
      |---|
```

- Question: When sending a packet/frame, how to determine which LAN segment to forward a frame to?
  - This looks like a routing problem
- The diagram above is a hierarchical local area network (LAN) that consists of multiple switches, and contains several hosts
  - The network has switches at the lower tier, and these switches connect directly to hosts
  - The top layer switch is connected to the lower tier switches
    - The ports on the switches are connected (via Ethernet)
  - From an individual host's point-of-view, the hosts are within the same local area network (LAN) and have direct connectivity
- For a particular packet that arrives at a switch, the switch needs to figure out which particular destination address should the packet be forwarded to?
  - Should the packet be forwarded to another host connected to one of its own ports, or should it be forwarded to another switch, which will ultimately connect to the destination MAC address?
    - This decision is automatically learned by switches without any explicit configuration
  - The answer to this problem is similar to network routing protocols. However, routing protocols have several different algorithms such as distance vector algorithms, Dijkstra's algorithm, etc. These algorithms require knowledge of the topology, or a store of local information and exchange of information among neighbouring routers, such as distance vectors
    - Switches operate on much simpler principles and dynamics than routers

- Self Learning
  - Switches utilize a mechanism called 'self learning'
    - This enables switches to learn which hosts can be reached through which interface
  - How self learning works:
    - Firstly, all switches store some kind of local table
      - Local tables are also referred to as switch tables
      - A local/switch table on a switch is similar to a routing/forwarding table on a router
        - However, they store different information

          - i.e. Routers store destination IP addresses, and network interfaces
      - Switch tables consist of multiple entries of 3-tuples, where each tuple contains the destination MAC address, the interface/port of the switch, and the time to live (TTL) field
        - The 'TTL' field indicates the validity of the switch. It is imperative, because local area neworks tend to be dynamic. Devices can be easily added to, or removed from, a LAN. They can also switch interfaces/ports. Therefore, a 'TTL' field is needed to indicate when the informtion will expire, so the self learning algorithm can kick in, and populate the switch table or make adjustments/updates to it
          - Stale entries in the switch table are dropped after a certain period of time
            - i.e. 'TTL' can be 60 minutes
    - To learn which host can be reached through which interface, learning is done in an on-demand manner
      - Switches do not run an algorithm, or a protocol, to actively exchange information. Instead, the switch will wait until it receives a link layer frame. Then, it will utilize the information in the frame to learn the mapping between MAC addresses and interfaces/ports. Upon reception of a link layer frame, the switch will look at the source MAC address of the frame.
        - This is very different from routing protocols
    - When a host sends a message to another host, or a broadcast message, upon reception of a message from a host, the switch will look at the source MAC address contained in the link layer frame, and the port it arrived at. By observing the frame, the switch is able to learn that host 'X', with a MAC address of 'XXX' is on interface 'Y'. A 'TTL' field can now be added in the local/switch table
  - Self learning works by observing the frame that arrives at different interfaces/ports
    - However, this does not solve the entire problem
- Filtering/Forwarding
  - If the local/switch table is initially empty, and the switches do not have any information, then all switch table queries are answered
    - This is because the link layer frame is dropped
  - When switches receive a frame, through self learning they can populate their switch table with information from the frame, such as source MAC address and the interface/port that the frame arrives on
    - However, at this time it is unknown how to forward the

frame to the destination MAC address

- Upon receiving a frame, and in addition to self learning, switches also look at the destination MAC address in the frame
    - Switches can look inside their tables, and determine if the destination address has been previously learned
        - In other words, if the switch has seen another frame originate from the destination MAC address of the current frame, then it knows where to forward the current frame too
    - Two situations can occur:
        1. The destination address is already in the switch's local table
            - In this case, the switch knows which interface/ port the frame needs to be forwarded to
            - This situation (#1) can be further divided into 2 cases:
                1. The incoming frame is on the same port as the destination frame
                    - This could happen in a hierarchical network topology
                    - The frame would be received by the destination through the downstream switch
                2. The destination host is on a switch that is different from the switch that the frame arrived at
                    - The frame is forwarded to the interface that is stored in the forwarding table
                    - The switch forwards the message to the destination through another port
        2. The switch's local table contains very little information because it just started its operations
            - In this situation, the ethernet switch will flood the entire local area network with the incoming frame
                - The switch will forward the frame to all ports, except for the port that the frame arrived from
                    - The incoming interface is not flooded, because any station on the incoming interface would have that frame already
                - Flooding is the only valid option, because the switch does not know which port corresponds to the destination address in the frame. Thus, the network needs to be flooded for discoverability reasons
            - Flooding is (sort of) a last resort
                - It allows ethernet switches to bootstrap
                - In absence of any knowledge of the outgoing

                      interface of a particular destination MAC address, switches will flood the message throughout the entire network
                        - This allows switches to bootstrap
                      - Flooding allows communication between any pair(s) of source and destination host, via flooding their frames through the entire local area network (LAN)
  - To summarize, when a switch receives a frame:

```
index switch table using MAC destination address
if (entry found for destination)
then:
    if (destination on segment from which frame arrived)
    then:
        drop the frame
    else:
        forward the frame on interface indicated
else:
    flood
```

  - Flooding forwards the message on all other interfaces/ports, except for the interface on which the frame arrived
  - The self learning and flooding mechanisms allow ethernet switches to continuously learn the connectivity between hosts and ports.
    - Based on this information, switches can update their local tables
    - As time goes on, and more information is learned, then fewer floods are required to learn connectivities in the local area network (LAN)
      - In other words, flooding becomes unnecessary to reach a particular destination host
- Switch Example
  - i.e. Diagram of a LAN Connected Via Switches

```
                        |-----|
                        |  S  |
                        |-----|
                       /   |   \
                      /    |    \
                     /     |     \
                  1 /      |      \ 3
                   /     2 |       \
                  /        |        \
                 /         |         \
|---|     |-----|       |-----|       |-----|     |---|
| A |-----| hub |   |---| hub |---|   | hub |-----| I |
|---|     |-----|   |   |-----|   |   |-----|     |---|
         /   |      |      |      |      |   \
        /    |      |      |      |      |    \
       /     |      |      |      |      |     \
      /    |---|    |      |      |    |---|    \
     /     | C |    |      |      |    | G |     \
|---|      |---|    |      |      |    |---|      |---|
| B |               |      |      |               | H |
|---|             |---|    |    |---|             |---|
                  | D |    |    | F |
                  |---|    |    |---|
                           |
                         |---|
                         | E |
                         |---|
```

  - 'S' corresponds to an ethernet switch
    - The switch is at the very top, connects all hubs and their respective hosts together
  - 'hub' corresponds to an ethernet hub
    - It connects all hosts that are connected to it
  - The hosts are: 'A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I'
- The diagram above is a hierarchical network that is configured with hubs; which are utilized to connect several hosts together in the local area network (LAN)
- Hubs are link-layer-1 devices that tend to be very cheap, because they are not intelligent
  - Any message/frame that arrives at a hub's port/ interface, the message is replicated and sent to all other ports/interface on the hub
    - i.e. If station `A` sends a message, then the hub will replicate the signal, and send it to station `B`, station `C`, and port/ interface #1 that corresponds to switch `S`
- The current information in the switch table, `S`, is:

Local Table For Switch `S`	
Address	Interface
A	1
B	1
E	2
G	3

  - The switch's local table starts off empty, and over time through self learning the switch learns connectivity information, such as:
    - Host `A` is attached to Interface #1
    - Host `B` is attached to Interface #1
    - Host `E` is attached to Interface #2
    - Host `G` is attached to Interface #3

- Since hubs are a layer-1 device, from a switch point of view, it does not know that hosts `A`, `B`, and `C` are connected via a hub
  - From the switch's point of view, the hosts are directly connected to port #1 on the switch
- Assume that switch `S` receives a frame that is destined to host `D`, and is sent from host `C`
  - When the frame, from host `C`, arrives at port #1 on switch `S`, the switch will update its local table by adding an entry corresponding to the frame sent by host `C`. The self learning mechanism is activated, because there is no entry in the table that corresponds to the incoming packet from `C`
    - The frame has a source MAC address of `C`, and a destination MAC address of `D`. The switch adds an entry to its local table, which corresponds to the source address, `C`, and the port number the frame arrived at, number one.
      - This entry is added to the switch's local table for station `C`. The switch is now aware of the location of host `C`, via its self learning behavior
      - Now, all subsequent frames that are destined to `C` can be properly forwarded to `C`, without needing to flood the LAN
  - After the frame is received, the updated switch table is:

Local Table For Switch 'S'	
Address	Interface
A	1
B	1
E	2
G	3
C	1

  - Now, the received frame needs to be forwarded to the correct port/interface on the switch. However, the MAC address of `D` is not (yet) available in the switch's local table. The switch has no idea which port/interface that host 'D' is attached to
    - The switch's only option is to flood the frame/ message throughout the entire local area network (LAN), except for the port/interface

that the frame came from. The switch will forward the frame/packet to the other ports; port #2 and #3

    - The hubs that receive the frame/packet will replicate the signal, and forward it to all hosts that are attached to its ports
    - Since the frame is flooded throughout the LAN, host `D` will receive the frame, and so will the other hosts, but their network interface card will look at the destination MAC address and drop the frame, because it is not destined for them
    - By the end of the flood, host `D` will receive the frame, but the switch has still not learned anything about host `D`
        - The switch can only learn about host `D`, if it sends a message. The moment the switch receives something that originates from `D`, through self learning the switch will learn which interface host `D` is connected to

- Suppose that host `D` replies/responds to the initial frame sent by host `C`
    - Once the frame arrives at the switch, it will know that host `D` is attached to port #2, and it will update its local table
        - The new local table looks like:

Local Table For Switch 'S'	
Address	Interface
A	1
B	1
E	2
G	3
C	1
D	2

    - Since the switch learned about `C` from its previous message, it already contains information about which interface `C` is connected to. By performing a lookup in the local table, the switch knows that `C` is connected to interface #1. Thus, the switch can

        directly forward the frame toward host `C`, without having to resort to flooding
        - Note: There is no acknowledgement mechanism in Ethernet. Host `D` is under no obligation to respond to host `C`. It is possible that host `C` sends a message to host `D`, and that is it; host `D` does not respond
            - Acknowledgements are handled by the upper layer protocols, like TCP. If host `C` establishes a connection to host `D` via TCP, then host `D` must send a response
- Assume that host `C` sends a frame to host `B`
    - In this scenario, host `B` and `C` are connected via a hub. So, the moment `C` sends a message, it will be received by `B`, because the signal is replicated by the hub, and immediately sent to all other hosts that are connected to the hub
    - Communication between host `B` and `C` has nothing to do with switch `S` and its local table. Whether `S` has an entry for `B` in its table or not, host `B` and `C` are directly connected at the physical layer, via the hub
        - The hub forwards any message from `C` to all other devices that are connected to it. The message is forwarded to host 'A' and 'B', and port #1 on switch `S`.
            - In essence, the hub is a repeater, and it repeats messages it receives, and sends it to all other ports that are connected to it
    - When the frame/packet arrives at the switch table, there 2 things that can happen:
        1. The switch will perform a lookup, and discover that host `B` is on the same interface as host `C`. The switch will drop the message, because there is no need to further send the message back or forward to other interfaces. The switch is intelligent enough to know that the frame sent by `C` has already been received by `B`
        2. If there is no entry for host `B` in the switch's local table, because the switch has not yet learned that station `B` is attached to interface #1. Thus, the switch does not know that the frame has already been received by `B`. As a result, the switch will flood and forward the frame to interface #2 and #3, but not interface #1. Since the frame arrived from interface #1, interface #1 is not flooded
            - The flooded messages are wasted because none of them will be able to reach host `B`, because `B` is not attached to interface/

port #2 or #3

        - As frames are sent back and forth between hosts, the switch will continue to learn about which interface each host is connected to. Through self learning the switch will update its local table, and at one point it won't have to flood the network to send a frame
    - Question: Can the self learning and forwarding/flooding mechanism be used for IP routing?
        - Answer: NO! These mechanisms are only valid on a small scale, like local area networks. Implementing this in the Internet would not work because there would be too much congestion and wasted traffic. This mechanism does not scale for billions of hosts. Each host will flood the network, and cause congestion
            - From a theoretical standpoint, the algorithm is correct, but it is not scalable, because it relies on flooding at the very beginning and to discover new hosts. Even with IP aggregation, this approach will not scale to billions of network hosts
                - This showcases the difference between an idea being correct from a theoretical point-of-view, and what is efficient in practice
                - Realistically, large Ethernet networks should adopt a better, more intelligent, mechanism to determine/establish the switch's local table
- Switch: Traffic Isolation
    - The advantage ethernet switches have over ethernet hubs is traffic isolation
        - Hubs are simple devices that replicate signals. All stations/hosts that are connected to the same hub will contend each other other when they transmit information at the same time
        - Switches can isolate the transmission of stations/hosts that are connected through different ports/interfaces
            - The hosts do not share a common medium, and concurrent transmissions are allowed
    - To summarize:
        - Switches break subnets into LAN segments, which helps in filtering/forwarding packets
            - Frames that originate from a particular LAN are not usually forwarded to other LAN segments
            - Segments become separate collision domains
    - i.e. Diagram of Switch & Collision Domains

```
                   |---|
|------------------| S |------------------|
|                  |---|                  |
|                    |                    |
|                    |                    |
|       * * * * * *  |  * * * * * *       |
|       *            |           *        |
              |       *  |---|   |---|   |---|  *       |
              |       *  | D |---| H |---| D |  *       |
              |       *  |---|   |---|   |---|  *       |
              |       *            |            *       |
              |       *            |            *       |
              |       *          |---|          *       |
              |       *          | D |          *       |
              |       *          |---|          *       |
              |       *                         *       |
              |       * * * * * * * * * * * * * *       |
              |                                         |
              |                                         |
        * * * | * * * * * * * * *     * * * * * * * * * | * * *
        *     |                 *     *                 |     *
        *   |---|       |---|   *     *   |---|       |---|   *
        *   | H |-------| D |   *     *   | D |-------| H |   *
        *   |---|       |---|   *     *   |---|       |---|   *
        *     |  \              *     *              /  |     *
        *     |   \             *     *             /   |     *
        *     |    \            *     *            /    |     *
        *   |---|   \           *     *           /   |---|   *
        *   | D |    \          *     *          /    | D |   *
        *   |---|     \         *     *         /     |---|   *
        *              |---|    *     *    |---|              *
        *              | D |    *     *    | D |              *
        *              |---|    *     *    |---|              *
        * * * * * * * * * * * * *     * * * * * * * * * * * * *
```

  - 'S' represents an ethernet switch
  - 'H' represents ethernet hubs
  - 'D' represents connected hosts/devices

- In the diagram above, there are 3 ports/interfaces on switch `S`, and each of them can be viewed as a local area network segment, or collision domain
- Transmissions from different segments are allowed at the same time
  - However, transmissions within each segment are subject to the media access control, and contention of the medium
- Switches can isolate collision domains
  - Each collision domain corresponds to a segment
  - All hosts within the same switch are part of the same broadcast domain
    - Broadcast messages on a local area network are disseminated to all other hosts, whether they are connected by ethernet hubs or switches

- Institutional Network
  - i.e. Diagram of a Potential Institutional Network

```
        |----------|
        | External |
        | Network  |
        |-----|----|
              |
              |
              |
        * * * | * * * * * * * * * * * * * * * * * * * * * * * * *
        *     |                                                 *
        *   |---|                  |--------|                   *
        *   | R |                  | Mail   |                   *
        *   |---|                  | Server |                   *
        *        \                 |--------|                   *
        *         \                    |                        *
        *          \                   |                        *
        *           \                  |           |--------|   *
        *            \___________      |      _____| Web    |   *
        *                        \     |     /     | Server |   *
        *                         \    |    /      |--------|   *
        *                          \   |   /                    *
        *                           \  |  /                     *
        *                            |---|                      *
        *             |--------------| S |----------|           *
        *             |              |---|          |           *
        *             |                |            |           *
        *             |                |          |---|         *
        *             |                |      |---| S |---|     *
        *             |                |      |   |---|   |     *
        *             |                |      |     |     |     *
        *           |---|              |      |     |     |     *
        *       |---| S |---|          |    |---|   |   |---|   *
        *       |   |---|   |          |    | H |   |   | H |   *
        *       |     |     |          |    |---|   |   |---|   *
        *       |     |     |          |            |           *
        *     |---|   |   |---|        |            |           *
        *     | H |   |   | H |        |          |---|         *
        *     |---|   |   |---|        |          | H |         *
        *             |                |          |---|         *
        *             |                |                        *
        *           |---|            |---|                      *
        *           | H |       |----| S |----|                 *
        *           |---|       |    |---|    |                 *
        *                       |      |      |                 *
        *                       |      |      |                 *
        *                       |      |      |                 *
        *                       |    |---|    |                 *
        *                       |    | H |    |                 *
        *                       |    |---|    |                 *
        *                       |             |                 *
        *                     |---|         |---|               *
        *                     | H |         | H |               *
        *                     |---|         |---|               *
        *                                                       *
        *                                           * * * * * * *
        *                                           * IP SUBNET *
        * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
```

    - 'S' represents ethernet switches
    - 'R' represents a router
    - 'H' represents hosts/devices connected to the network
  - The diagram above is an example of a potential institutional network
    - It is possible to have different hierarchies
    - An external network can be connected through a router
  - In the network:
    - Routers are not aware of the existence of switches
      - This is because switches are a layer-2 device, and they don't even have an IP address
    - Routers only see end-hosts and servers
    - Routers need to populate their tables based on the IP addresses of the hosts
    - From the router's point-of-view, every device is directly connected to the router
      - Routers don't see switches
- Summary: Comparison of Hubs, Switches & Routers
  - i.e. Diagram of Relationship Between Hosts, Hubs, Switches, & Routers

```
|-------|                                               |-------|
|   5   |                                               |   5   |
|-------|                                               |-------|
|   4   |                                               |   4   |
|-------|                                   |-------|   |-------|
|   3   |                                   |   3   |   |   3   |
|-------|                       |-------|   |-------|   |-------|
|   2   |                       |   2   |   |   2   |   |   2   |
|-------|   |-------|           |-------|   |-------|   |-------|
|   1   |   |   1   |           |   1   |   |   1   |   |   1   |
|-------|   |-------|           |-------|   |-------|   |-------|
 host A      hub                 switch      router      host B
```

    - A packet sent from host 'A' will travel to an ethernet hub, then an ethernet switch, then a router, and finally destination host 'B'
      - The end-host devices operate on 5 network layers
      - Routers operate on 3 network layers
        - Implement all layers from the bottom, up to and including the network layer
          - Network layer, data link layer, and physical layer
      - Switches operate on 2 network layers
        - Data link layer, and physical layer
      - Hubs only operate on the (bottom) physical layer
  - i.e. Table Comparing Hubs, Switches & Routers

	Hubs	Routers	Switches

Traffic Isolation	No	Yes	Yes
Plug & Play	Yes	No*	Yes
Optimal Routing	No	Yes	No
Cut Through	Yes	No	Yes*

  - This table summarizes the key differences between switches, routers, and hubs
  - The asterisk ('*') implies that the answer is not a simple 'yes/no'. It all depends on implementation
- Ethernet Hubs are layer-1 devices that only implement the physical layer
- Ethernet Switches are layer-2 devices that implement the physical layer and data link layer
- Routers are layer-3 devices that implement all layers up to the network layer
- Hubs do not provide any traffic isolation
- All hosts connected to a hub are in the same contention domain
- Routers and switches DO provide traffic isolation
- All switches and hubs are 'plug and play'
  - Meaning, they can be connected to a host, or hosts, without setting anything up
- Routers are not 'plug and play', because configuration regarding routing protocols/metrics need to be setup by the network administrator
  - Information like 'RIP' is based on hop count, and 'OSPF' associates the links with certain costs, needs to be configured
    - If this information is pre-configured, then the router can be used without manual configuration
    - Typically, routing metrics are automatically setup through message exchanges
- Routers can figure out the optimal route, or the least cost path
  - This is accomplished utilizing Dijkstra's algorithm, or a distance vector algorithm like 'RIP'
- Hubs and switches do not calculate the optimal route
  - The self learning algorithm found in switches learns the connectivity between hosts, and does not nescessarily figure out the least cost path from one host to another
  - Hubs replicate and forward messages to all connected

devices
        - The notion of optimal routing does not exist, and is not possible, in hubs
    - Hubs and switches support an operation called 'cut through' transmission
        - 'Cut through' means that a partially received frame can be forwarded without the complete reception of the frame
            - In other words, some switches can start forwarding the frame to the corresponding port/interface by looking at the address field of the frame, and make a decision before it receives the entire frame
            - Routers can only forward full frames
                - This is because the entire packet needs to be received, the checksum needs to be calculated and compared so the router can decide whether it should drop the packet or forward it to a particular destination port

- March 19th, 2021
    - Recap
        - Ethernet switches learn to find the pass from one device to another device via self learning and a combination of forwarding based on the information that's already stored in the switch's local table
            - If the switch has no information in its local table, then it resorts to flooding
        - Routers VS. Switches VS. Hubs
            - Switches have the ability to isolate different local area network segments
                - This allows concurrent transmissions among machines/devices that belong to different segments
            - Hubs are a layer-1 device that repeat whatever signal it receives
                - All devices connected to a hub have to contend one another for access to the shared medium
        - Ethernet is a combination of the physical layer and data link layer
            - The data link layer is divided into 2 sub-layers:
                1. Logical Link Control (LLC)
                2. Media Access Control (MAC)
                    - MAC is the center of most discussions
    - WLANs
        - WLAN is a (very important) local area network technology
        - Compared to Ethernet, WLAN is used more often by consumers
        - Note: WLAN = Wireless Local Area Network
    - Elements Of A Wireless Network (1)
        - For this course, discussions regarding element of wireless networks refers to an enterprise network that tends to be

more complicated than an average home Wi-Fi setup

- Typically, in an enterprise Wi-Fi network, there are many-many access points and devices that need to connect with the wired network infrastructure

- i.e. Diagram of Enterprise Network Infrastructure

```
* * * * * * * * * * *           * * * * * * * * * * * * *
*                   *           *                       *
*   ((H))   ((H))   *        |-------/\       ((H))     *
*                   *        |  *   /__\                *
*        /\         *        |  *                       *
*       /__\-----------|     |  *            ((H))      *
*                   *  |     |  *                       *
*   ((H))           *  |     |  *     ((H))        (H)) *
*                   *  |     |  *                       *
* * * * * * * * * * *  |     |  * * * * * * * * * * * * *
                       |     |
                       |     |
                       |     |
                # # # # # # # # # #
                #     NETWORK     #
                # INFRASTRUCTURE  #-----------|
                # # # # # # # # # #           |
                |                             |
                |                             |
                |                             |
* * * * * * * * | * * * * * *           * * * | * * * * *
*               |           *           *     |         *
*   ((H))       |           *           *     |         *
*               |           *           *    /\         *
*       ((H))   |   ((H))------------------>/__\        *
*               |           *           *               *
*               |           *           *               *
*   ((H))      /\           *           *        ((H))  *
*             /__\          *           *               *
*                           *           *               *
*       ((H))               *           *               *
* * * * * * * * * * * * * * *           * * * * * * * * *
```

  - 'H' represents wireless hosts/devices
  - Base stations, also called access points, are represented by triangle shaped entities
    - They are connected, via wire, to the network infrastructure
- In the network infrastructure, above, there are several components
  - i.e. Wireless hosts, base stations, wireless links, etc.
- A major part of networks are connected hosts/devices
  - Hosts can be connected via wire or wireless
  - In the diagram above, hosts are connected wirelessly
  - Hosts run applications

  - The applications communicate with other applications over the Internet
- Example of hosts include, but not limited to:
  - Laptops, smartphones, tablets, and even some Desktops utilize wireless connectivity
- Hosts can be mobile, like a mobile device, or they can be stationary
  - Note: Stationary means non-mobile
  - Wireless does not always mean mobility
    - i.e. Desktops connected via wireless

- Elements Of A Wireless Network (2)
  - i.e. Diagram of Enterprise Network Infrastructure

```
* * * * * * * * * * *           * * * * * * * * * * * * *
*                   *           *                       *
*   ((H))   ((H))   *        |-------/\       ((H))     *
*                   *        |  *   /__\                *
*        /\         *        |  *                       *
*       /__\-----------|     |  *            ((H))      *
*                   *  |     |  *                       *
*   ((H))           *  |     |  *     ((H))        (H)) *
*                   *  |     |  *                       *
* * * * * * * * * * *  |     |  * * * * * * * * * * * * *
                       |     |
                       |     |
                       |     |
                # # # # # # # # # #
                #     NETWORK     #
                # INFRASTRUCTURE  #-----------|
                # # # # # # # # # #           |
                |                             |
                |                             |
                |                             |
* * * * * * * * | * * * * * *           * * * | * * * * *
*               |           *           *     |         *
*   ((H))       |           *           *     |         *
*               |           *           *    /\         *
*       ((H))   |   ((H))------------------>/__\        *
*               |           *           *               *
*               |           *           *               *
*   ((H))      /\           *           *        ((H))  *
*             /__\          *           *               *
*                           *           *               *
*       ((H))               *           *               *
* * * * * * * * * * * * * * *           * * * * * * * * *
```

  - 'H' represents wireless hosts/devices
  - Base stations, also called access points, are represented by triangle shaped entities
    - They are connected, via wire, to the network infrastructure
- Base stations are the second most important element

which provide physical layer connectivity with the network infrastructure/host

    - Typically, access points have 2 interfaces:
      1. Wireless Interface
         - Provide connectivity to wireless hosts/devices
      2. Wired Interface
         - Allows the access point, or base station, to connect to the network infrastructure, or the backbone of the local area network
           - Typically, access points are connected to a wired network via ethernet
    - The main role of base stations is to relay packets from the wired network to the wireless network, and vice versa, in its "area"
      - Examples of base stations include, but not limited to: Cell towers, 802.11 access points, etc.
    - Wireless networks are not limited to Wi-Fi networks; they can also be cellular networks
      - Cellular data networks are another type of wireless networks. Instead of having wireless access points, like Wi-Fi, cellular networks have cellular towers
        - Typically, cellular towers are connected via wired backbone
- Elements Of A Wireless Network (3)
  - The 3rd element of wireless networks are the wireless links that allow connectivity between (mobile) devices and base stations
  - In some networks, it is possible to use the wireless link as the backbone link, and connect to the backbone network
    - i.e. In remote areas, a satellite may be the backbone that interconnects multiple cellular towers. Alternatively, there may be some kind of wireless mesh network built on top of Wi-Max or some other technology. It also possible to use minimal wave technology that allows the transmission of data at high speed, among backbone devices. Then, the backbone devices interface with the customer
  - In order to access the wireless link for connectivity between wireless base stations and mobile devices, the network needs to utilize some kind of medium access control to coordinate access between stations and devices
    - Medium access control (MAC) is required due to the nature of wireless technologies
    - For devices that are within the same proximity, the MAC protocol needs to determine which device gets to transmit, and at what time
      - Wireless technologies have many different ways to arbitrate access
      - In wireless LAN (WLAN), a medium access control (MAC) protocol called CSMA/CA is used to facilitate

access for different wireless devices

-
  -
    - Wireless technologies such as cellular may use different MAC protocols to coordinate access between stations and devices
      - i.e. Divide the wireless spectrum into different frequency bands, and allocate different frequency bands to different customers
      - Access can be facilitated based on codes, time, etc.
        - There are many different mechanisms that allow sharing of wireless mediums
- Different physical layer technologies can support different data rates, and have different transmission radiuses
  - i.e. Typical indoor Wi-Fi is on the order of 100 meters
    - Outdoor coverage ranges from 50 - 100 meters
  - i.e. Cellular towers have a coverage of 200 meters
    - 2G/3G towers may have a coverage of several kilometers
  - i.e. 5G has a much shorter coverage than its predecessor cellular technologies
    - 5G cell towers tend to be much smaller
    - 5G uses linear waves
- Cellular towers are like bridges between wireless clients, and the wired backbone of the network
  - Depending on the generation of the cellular network, cellular towers follow different physical layer technology, and different link layer technology
- Packet corruption is typically caused by a very poor radio channel, but this assumes that there are no other concurrent transmissions
  - Poor radio signal can be the result of going through a tunnel, or cruising on a high speed train
  - In cellular contexts, the signal strength tends to be very weak if the device is moving around, or if there are lots of obstructions between the device and the cellular tower.
    - As a result, the throughput, or data rate, will be very low
      - In some cases, the device will not be able to connect to the cellular tower at all
    - In this situation, the bit error rate tends to be high in cellular connections
  - In a home Wi-Fi setting, the primary source for packet corruption are contention stations
    - i.e. Neighbor's Wi-Fi network interferring with your local network
      - This kind of interference leads to bit error rate in Wi-Fi connections
- Generally, the further a device is from an access point, the higher the corruption rate

- The signal power that arrives at the access point is inversely proportional to the distance raised to a certain exponent
  - i.e. P_rx ~ d^(-x)
    - 'P_rx' = Received power level
    - 'd' = Distance between transmitter and receiver
    - 'x' = Exponent that models the environment
      - In free space, or a vacuum, 'x' typically equals 2
      - In an indoor environment with lots of walls, and furniture, 'x' is typically greater than 2, it can be 3 or 4
        - As `x` increases, the signal attenuates faster, or the distance is longer, and the received signal power is smaller
          - As a result, the link quality is worse, and there are likely to be more bit errors in the received frames. Thus, more packet corruption

- Elements Of A Wireless Network (4)
  - Base stations connect (mobile) devices to the wired network
  - In Wi-Fi networks, there are 2 modes to operate the network
    1. Infrastructure mode
    2. Ad-hoc mode
  - Cellular networks only have one option; it is infrastructure mode
  - In infrastructure mode, base stations connect mobile devices to the wired network
    - Since every base station has limited coverage, because it operates on wireless technology
      - i.e. Wi-Fi access point, cellular tower, etc.
      - If the base station is too far, then the signal is so low/weak that the data cannot be recoded
    - Each base station has its own coverage radius
    - When a mobile device moves from one base station's covered area to another base station's covered area, an operation called 'handoff' needs to be performed
      - Typically, handoff is done at the physical layer, and in some cases it may involve the data link layer
      - Generally, handoff is made transparent, or aware, to upper layer protocols
        - From a user point-of-view, it seems as if your device is always connected to the wireless infrastructure
          - Although, as a device moves around, it will connect to different base stations
- Elements Of A Wireless Network (5)
  - Ad-hoc mode does not have dedicated devices, or always-on devices such as base stations that are always connected, via wire, to a backbone

    - Put simply, ad-hoc mode does not have any base stations
  - In ad-hoc mode, wireless (mobile) devices serve themselves; both as a client, as well as (kind of) part of the infrastructure that interconnects devices
    - A mesh can be formed on top of it
      - i.e. Wi-Fi Direct
        - This allows 2 wireless devices to communicate with one another without the presence of an access point, or base station
      - A mesh network can be built by utilizing wireless hosts/devices as relays, or "routers"
        - This will form some kind of multi-hop wireless network
    - Nodes/devices can only transmit to other nodes within link coverage
    - Nodes/devices organize themselves into a network, and they route among themselves
  - Generally, ad-hoc is not utilized; primarily because of its power consumption
    - Since mobile devices are battery powered, operating its wireless interface in ad-hoc mode, and allowing traffic to relay from other wireless devices, can drain battery power very quickly
      - Even though most (mobile) devices support ad-hoc mode, it is not utilized, and turned off
  - Ad-hoc is a latin term which roughly translates to, "something that can be formed spontaneously, or on demand; it is not planned"
    - In contrast, infrastructure mode requires building the infrastructure before the network can operate, and (mobile) devices can communicate with one another
    - In ad-hoc mode, if 2 or more people can meet each other in person, then they can continuously form an ad-hoc network
- 802.11 LAN Architecture
  - i.e. Diagram of LAN Architecture

```
# # # # # # # # # # # # # # # # # # # # # # # # # # # # #
#                                                       #
#   * * * * * * * * * *           * * * * * * * * * *   #
#   *                 *   |---|   *                 *   #
#   *   ((H))    /\_______| S |   *     ((H))       *   #
#   *           /__\      | / |   *                 *   #
#   *  ((H))          *   | H |______/\      ((H))  *   #
#   *                 *   |---|     /__\            *   #
#   *      ((H))      *     |     *       ((H))     *   #
#   *                 *     |     *                 *   #
#   *         * * * * *     |     *         * * * * *   #
#   *         * BSS 1 *     |     *         * BSS 2 *   #
#   * * * * * * * * * *     |     * * * * * * * * * *   #
#                           |                           #
#                           |                     # # # #
#                           |                     # ESS #
# # # # # # # # # # # # # # | # # # # # # # # # # # # # #
                            |
                            |
                            |
# # # # # # # # # # # # # # | # # # # # # # # # # # # # #
#                           |                           #
#                     //--------\\                      #
#                     || Router ||                      #
#                     \\--------//                      #
#                           |                           #
#                           |                           #
#                           |                           #
#               |-----------------------|               #
#               |                       |               #
#               |                       |               #
#               |       Internet        |               #
#               |                       |               #
#               |                       |               #
#               |-----------------------|               #
#                                                       #
# # # # # # # # # # # # # # # # # # # # # # # # # # # # #
```

- This diagram is an example of a LAN architecture
- There are 2 basic service sets that are connected by a switch or hub
    - The access point from each basic service set (BSS) is connected to the switch/hub
- The joined basic service sets form an extended service set (ESS)
- The switch/hub connects the extended service set (ESS) to a wide area network (WAN), known as the Internet

- In wireless LAN, the infrastructure consists of base stations as well as the wired infrastructure that connects the base stations, or access points, through hubs or switches
    - Note: The terminology of base stations and access points are used interchangeably
    - At some point, the hubs/switches may be connected to a router that interfaces with a wide area network, such as the Internet
- In a Wi-Fi network, the "cell" that corresponds to each access point is referred to as a basic service set (BSS)
    - A basic service set (BSS) contains a wireless host, or hosts, and a single access point
    - Infrastructure mode contains wireless hosts, and an access point (AP)
    - Ad-hoc mode only contains hosts
        - Known as 'IBSS'

- With the help of wired technology, multiple basic service sets can be connected utilizing a distributed system (DS)
  - This is called an extended service set (ESS)
  - Put simply, an extended service set (ESS) is the combination of two or more basic service sets
    - Distributed systems (DS) are used to connect multiple access points
  - i.e. McMaster's campus Wi-Fi network can be viewed as an extended service set (ESS) that utilizes a backbone to connect different access points at different locations of the same building, or across multiple buildings

- IEEE 802.11 Specs
  - An extensive table of IEEE 802.11 specs can be found at: https://en.wikipedia.org/wiki/IEEE_802.11#Protocol
  - In the last few decades, wireless Wi-Fi networks are among one of the most dynamic and fast evolving technologies
    - In 1997, when 802.11 was first ratified, the data rate that could be supported was 1-2 Mbit/s (megabit/second)
    - Currently, Wi-Fi 6 is the new standard - the protocol is 802.11ax - and it supports a data rate up to 10.53 Gbit/s (gigabit/second)
    - In (roughly) 2 decades, the throughput of 802.11 has multiplied by a factor of 10,000; this is a big increase
      - The primary driver of this gigantic improvement in 802.11 is due to the physical layer; in terms of the radio bandwidth that can be utilized
        - i.e. Wi-Fi 6 can use 5 GHz, and 6 GHz
        - i.e. 802.11ad, which operates on millimeter waves, operates on a frequency of 60 GHz
      - Another reason for this big improvement is the utilization of more advanced radio technologies that employ ODFM technology
        - ODFM allows the utilization of multiple channels on the access point side, infrastructure side, and (mobile) device side
          - By having more antennas that can transmit/ receive, multiple streams and multiple users can be concurrently supported
          - Combining all these advancements allows devices to reach a peak data of 10 Gbit/s, with the newest LAN technology

- 5GHz (802.11a/h/j/n/ac)
  - The following examples about channels are old, but the basic concepts still apply
  - i.e. Diagram of Non-Overlapping Channels For 2.4 GHz WLAN: 802.11b (DSSS) Channel Width 22 MHz

```
                                                 2.4835
                                                  GHz
2.4 GHz                                            |   2.5
```

```
       |                                             |   GHz
       |                                             |    |
       |                                             |    |
       | |-----------| |-----------| |------------|  |    |
       | | Channel 1 | | Channel 6 | | Channel 11 |  |    |
       | | 2412 MHz  | | 2437 MHz  | | 2462 MHz   |  |    |
    ---|-|-----------|-|-----------|-|------------|--|----|--
       |                                             |    |
```

  - This diagram is the radio channel for 802.11b
- 802.11b is (pretty much) the first generation of wireless technology
  - The radio channel that 802.11b utilizes is 2.4 GHz
  - In total, there are 4 orthogonal channels that can be utilized for transmissions
    - The channels are:
      - Channel 01 @ 2412 MHz
      - Channel 06 @ 2437 MHz
      - Channel 11 @ 2462 MHz
      - Channel 14 @ 2484 MHz
        - Not shown in diagram above, due to space constraints
    - Each channel corresponds to a frequency range around the 2.4 GHz
      - A central frequency is allowed
      - Frequency ranges of channels do not overlap
        - Hence, they are called orthogonal channels
  - Access points can operate in different channels
    - However, the diagram above only shows a few orthogonal channels
    - Devices can also operate at different channels
  - The benefit of using orthogonal channels for access points and devices is to allow concurrent transmissions of multiple devices
    - As long as devices operate at different orthogonal channels, then concurrent transmissions are allowed
    - If the the channels overlap with one another, then there may be interference during transmission
- i.e. Diagram of Non-Overlapping Channels For 2.4 GHz WLAN:
  802.11g/n (ODFM) Channel Width 20 MHz

```
                                                        2.4835
                                                           GHz
    2.4 GHz                                                 |
       |                                                    |
       |                                                    |
       |      /|-----------|\          /|-----------|\      |
       |     / | Channel 1 | \        / | Channel 6 | \     |
       |    /  | 2412 MHz  |  \      /  | 2437 Mhz  |  \    |
       |   /   |           |   \    /   |           |   \   |
    ---|--/----|-----------|----\--/----|-----------|----\--|
       |                                                    |
       |                                                    |
```

  - This diagram is the radio channel for 802.11g/n
  - 16.25 MHz is used by sub-carriers
  - In total there are 3 orthogonal channels that can be utilized for transmissions
    - The channels are:
      - Channel 01 @ 2412 MHz
      - Channel 06 @ 2437 MHz
      - Channel 11 @ 2462 MHz
- i.e. Diagram of Non-Overlapping Channels For 2.4 GHz WLAN:
  802.11n (ODFM) Channel Width 40 MHz

```
                                                  2.4835
                                                   GHz
    2.4 GHz                                         |      2.5
       |                                            |      GHz
       |                                            |       |
       |        /|----------------|\                |       |
       |       / |                | \               |       |
       |      /  |    Channel 3   |  \              |       |
       |     /   |                |   \             |       |
       |    /    |    2422 MHz    |    \            |       |
       |   /     |                |     \           |       |
    ---|--/------|----------------|------\----------|-------|-
       |                                            |       |
       |                                            |       |
```

  - This diagram is the radio channel for 802.11n
  - 33.75 MHz used by sub-carriers
- It is (relatively) easy to tell if a radio is operating on 2.4 GHz
  - Chances are it is either 802.11g or 802.11b
- A common problem with operating on 2.4 GHz channels is network congestion
  - i.e. Typically happens when everyone comes home from work/school, turn on the Wi-Fi, and start generating traffic
    - Multiple people generating traffic at the same time can congest the network
      - As a result, the throughput, or data rate, slows down to a crawl
  - One potential solution to this problem is to change the channel, via the administration menu, that the Wi-Fi access point communicates on, to a channel that is not utilized
    - The purpose of doing this is to operate on a channel that is far away from everyone else
      - Unfortunately, 2.4 GHz Wi-Fi has too few options
        - i.e. Only 3-4 orthogonal channels
  - This issue has been improved in 802.11a, 802.11ac, etc.
    - Since radios operate in 5 GHz with 20 MHz channel

bandwidth, there are many more orthogonal channels that can be utilized

- Simply put, more channels equals less congestion
- 5 GHz Wi-Fi is less problematic in residential neighbourhoods and apartment buildings that contain a lot of (home) Wi-Fi networks

- Now, orthogonal channels are even less of an issue, because access points can automatically configure the channel(s) that connected devices operate on
  - This optimizes, and reduces channel congestion

- i.e. Table of Channel Width & Numbers For 5GHz Wi-Fi

Channel Width	Valid Channel Numbers
20 MHz	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 161, 165, 169
40 MHz	38, 46, 54, 62, 102, 110, 118, 126, 134, 142, 151, 159
80 MHz	42, 58, 106, 122, 138, 155
160 MHz	50, 114

- 802.11 Frame: Addressing (1)
  - i.e. Format of an 802.11 Frame

```
    2          2          6         6         6
|---------|----------|---------|---------|---------|
| Frame   | Duration | Address | Address | Address | * * *
| Control |          |    1    |    2    |    3    | * * *
|---------|----------|---------|---------|---------|
                                                         |
                                                         |
                                                         |
      |--------------------------------------------------|
      |
      V        2          6        2304     4
          |----------|---------|---------|-----|
    * * * | Sequence | Address | Payload | CRC |
    * * * | Control  |    4    |         |     |
          |----------|---------|---------|-----|
```

    - This diagram is the format of an 802.11 frame
      - The format is the same regardless of which type of 802.11 implementation is used
        - The format is the same for 'a', 'g', 'h', etc.
    - The size is measured in bytes
      - i.e. The size of 'CRC' is 4 bytes
    - Address 1: MAC address of wireless host or access point

to receive this frame

  - Address 2: MAC address of wireless host or access point transmitting this frame
  - Address 3: MAC address of router interface to which access point is attached
  - Address 4: Used only in ad-hoc mode
  - In WLAN, there is no maximum limit on how large the payload can be
- 802.11 frames have a number of fields, such as:
  - Frame control
    - Indicates the type of the frame
  - Duration
    - Is immediately after frame control
    - Specifies how much transmission time the frame will occupy the medium
  - Address(es)
    - In an 802.11 frame, there are 4 address fields in total
      - In contrast, an Ethernet frame only consists of the source and destination MAC address field
    - The 1st address field indicates the receiver, or the destination MAC address, in terms of the wireless host or access point
      - If a (mobile) device transmits a frame to the access point (AP), then the 1st address field will be set as the MAC address of the access point (AP)
      - Basically, this field is the destination MAC address
    - The 2nd address field corresponds to the source MAC address
      - If a particular (mobile) device transmits something to an access point, then this field will be set as the MAC address of the particular (mobile) device
    - The 3rd address field corresponds to the MAC address of the router interface, to which the access point (AP) is attached to
      - This field differs from Ethernet frames
      - In a Wi-Fi network, the access point is connected through the local area network (LAN), and eventually it connects to a router
      - In a home network it is possible for the 3rd address field to be the same as the 2nd address field
      - Generally, the 3rd address field corresponds to the MAC address of the router interface
    - The 4th address field is not typically used in infrastructure mode
      - It is only utilized in ad-hoc mode, when a mesh

```
                  network needs to be constructed
- 802.11 Frame: Addressing (2)
    - i.e. Diagram of WLAN Network Connecting to The Internet
           Through a Router
                                    |---------------------------|
                                    |                           |
                                    |                           |
                                    |                           |
                                    |          INTERNET         |
                                    |                           |
                                    |                           |
                                    |                           |
                                    |---------------------|-----|
                                                          |
                                                          |
                                                          |
        * * * * * * * * * * * * * * * *                   |
        *                             *                   /
        *  ((H))                      *                  /
        *                             *                 /
        *      ((H1)) ======> /\      *                /
        *               |    /  \     *          |----|
        *  ((H))        |   / AP \  ===========> | R1 |
        *               |  /______\   *    |     |----|
        *      ((H))    |             *    |
        *               |             *    |
        * * * * * * * * | * * * * * * *    |
                        |                  |------------|
                        |                               |
                        |                               |
                        V                               |
        |---------------------------------------|       |
        | 802.11 Frame                          |       |
        |----|---------|---------|---------|----|       |
        | ~~ | AP MAC  | H1 MAC  | R1 MAC  | ~~ |       |
        | ~~ | Address | Address | Address | ~~ |       |
        |----|----|----|----|----|----|----|----|       |
                  |         |         |                 |
                  V         V         V                 |
               Address   Address   Address              |
                  1         2         3                 |
                                                        |
                                                        |
                                                        V
                                |-----------------------------|
                                | 802.3 Frame                 |
                                |----|---------|---------|----|
                                | ~~ | R1 MAC  | H1 MAC  | ~~ |
                                | ~~ | Address | Address | ~~ |
                                |----|----|----|----|----|----|
                                          |         |
                                          V         V
                                       Dest.     Source
                                       Address   Address
```

    - 'AP' is the access point
    - 'H1' is the host/device that connects to the 'AP'
      - 'H' corresponds to other hosts/devices connected to the 'AP'
    - 'R1' corresponds to the router that connects the 'AP' to the Internet
    - The frame sent from 'H1' to the 'AP' is 802.11
      - 802.11 corresponds to wireless
    - The frame sent from the 'AP' to 'R1' is 802.3
      - 802.3 corresponds to ethernet
  - This diagram above illustrates how a wireless LAN (WLAN) network connects to the Internet through a router, and how frames are received by the access point, which forwards the frames to the router. The router is like a bridge that connects the local area network (LAN) to a wide area network (WAN), like the Internet
  - Assume that a host 'H1' wants to access `google.com`. 'H1' sends a link layer frame to the access point. The frame sent by 'H1' is 802.11, and contains 4 address fields. However, in this situation only 3 are relevant: destination MAC address, source MAC address, and the MAC address of the router
    - Once the access point (AP) receives this frame, it will send it to the router 'R1'. But, before it sends it to 'R1' the access point (AP) will replace the destination MAC address
      - It will change the destination MAC address from the MAC address of the access point to the MAC address of router 'R1'
        - The access point does this, because it has another interface; the ethernet interface that is connected to the router
        - This process converts the 802.11 (wireless) frame into an 802.3 (ethernet) frame
          - The 802.11 frame is sent by 'H1' to 'AP'
          - The 802.3 frame is sent by 'AP' to 'R1'
      - Similarly, upon reception of a frame from the router, the access point (AP) will need to construct an 802.11 (wireless) frame from the received 802.3 (ethernet) frame, before sending it to 'H1'
- 802.11 Frame: More
  - i.e. Format of an 802.11 Frame

```
                                          |----------------------|
                                          | Duration of reserved |
                          |-------------> | transmission time    |
                          |               | RTS/CTS              |
                          |               |----------------------|
                          |
             2         2  |       6         6         6
        |---------|-------|--|---------|---------|---------|
        | Frame   | Duration | Address | Address | Address | * * *
        | Control |          |    1    |    2    |    3    | * * *
        |---------|----------|---------|---------|---------|
        <-------------------- MAC Header ------------------  * * *

                        2         6        2304      4
                  |----------|---------|---------|-----|
            * * * | Sequence | Address | Payload | CRC |
            * * * | Control  |    4    |         |     |
                  |-----|----|---------|---------|-----|
            * * *  -----|---->
                        |               |-----------------------|
                        |               | Frame Sequence Number |
                        |-------------> | For reliable ARQ      |
                                        |-----------------------|
```

  - Measured in bytes
- The duration field is utilized to indicate the overall time that the transmission, or frame, will take
  - This can be utilized to reserve the medium to avoid excessive contention
    - i.e. No other devices can transmit for X seconds
- Ethernet is connectionless, and is unreliable at the data link layer
- Wireless LAN (WLAN) has some mechanisms to realize reliable data transfer
  - However, there is no guarantee that a frame will be delivered
  - Wireless LAN (WLAN) utilizes acknowledgements to determine whether a frame has been successfully received or not
    - It utilizes the 'sequence control' field in the ethernet frame
- The 'sequence control' field includes the sequence number of the frame
  - WLAN combines this with acknowledgements to do its best effort at delivering frames successfully to the destination host
  - The data link layer has some similarities with the transport layer
    - The data link layer uses sequence numbers, and it can use acknowledgements. Similarly, TCP also uses sequence numbers and acknowledgements for reliable data transfer. However, in this scenario the transmission is between neighbouring devices, so there is no need to use acknowledgement numbers from the receiver, because sequence numbers will suffice

  - Simply put, the sequence control number is utilized for reliable data transfer
- After the 4th address field is the payload
  - Unlike ethernet, there are no restrictions on the size of the payload for WLAN frames
    - In contrast, an entire ethernet frame is limited to 1500 bytes. The payload for Wi-Fi networks is unlimited
- The last field in an 802.11 frame is 'CRC'
  - It is similar to the CRC field in ethernet frames
  - CRC is utilized for error detection, via circular redundancy checks
- i.e. Options For The Frame Control Field

```
                                    |----------------------|
                    |-------------> | Frame type           |
                    |               | (i.e. RTS, CTS, ACK, |
                    |               |      data)           |
                    |               |----------------------|
                    |
                    |
          2       2 |      4      1      1     1
    |----------|----|-|---------|----|------|------|
    | Protocol | Type | Subtype | To | From | More | * * *
    | version  |      |         | AP | AP   | Frag | * * *
    |----------|------|---------|----|------|------|

                  1       1      1      1     1
              |-------|-------|------|-----|------|
        * * * | Retry | Power | More | WEP | Rsvd |
        * * * |       | Mgt   | Data |     |      |
              |-------|-------|------|-----|------|
```

  - Measured in bits
- The frame control field can be further expanded to consist of several different fields, such as:
  - Protocol version
  - Frame type
  - Frame subtype
  - Which direction a particular frame is heading to
    - i.e. Is the frame going to an 'AP' or coming from an 'AP'
  - Is there any fragmentation
    - i.e. Are there subsequent parts to this frame?
  - Is this a good transmission?
  - Power management state of the device
    - A (mobile) device can be operated in a power management mode, such as power saver
      - In this mode, if the device does not have any data to transmit, then the Wi-Fi interface can be put to standby mode, but the device will still need to wakeup and listen to the beacon

transmissions coming from the access point (AP)

          - If the access point has any data to send, it can indicate in the frame control field which station should remain ON for the rest of the beacon interval, to receive data from the access point (AP)
    - Etc.
      - In addition to the fields listed above, there are other flags in the frame control field
- Frame Types
  - There are many types of frames in Wi-Fi, such as:
    - Management Frames
      - Beacon
        - Are sent periodically
        - Contain important information such as E-SSID, B-SSID, etc.
          - E-SSID is the SSID of the extended service set (ESS)
          - B-SSID is the SSID of the basic service set (BSS)
        - Are important, because when a new device comes to a network it needs to learn what wireless networks are available
          - When a device scans different channels, upon decoding the beacon messages, it can see what wireless local area networks are available to connect to
            - i.e. McMaster campus has Mac Wireless
              - This information is sent through beacon messages
      - (De)Association request/respond
        - Allows a host to connect and establish layer-2 connectivity with an access point (AP)
      - Announcement traffic indication message
        - Allows the access point (AP) to tell the (mobile) device that there is some pending data to be sent
      - Authentication/Deauthentication
        - Allows a device to be able to connect to a secured wireless network
    - Control Frames
      - Poll frame
      - Poll response frame
      - RTS/CTS
        - Used for reserving the medium to reduce the amount of contention
      - ACK
        - Acknowledgement frame
        - Used to indicate to the transmitter whether a frame has been successfully received or not

      - Power save (PS-poll)
    - Data Frames
      - Limitation on payload size
      - Can be extended to 7395 (with multiple fragments)
  - Control and management frames are utilized to ensure smooth operation and control in wireless local area networks
    - However, data frames are utilized to transmit real data
- Association
  - In order to connect to the Internet, via home Wi-Fi (WLAN), a device needs to have layer-2 connectivity with the access point (AP). Without this, nothing can happen. This situation is similar to connecting a device to an access point (AP) via ethernet. The ethernet cable connects to the device on one end, and on the other end it connects to a port of an ethernet switch or directly to the access point (AP)
    - Connecting an ethernet cable to a device requires both the device and access point (AP) to have the cable plugged in to their respective ports; the user needs to perform this physical action of plugging in the cable
      - In wireless connections, this process is called 'Association', and is done through an exchange of messages. A host will need to scan several channels - like 802.11g, 802.11n, and 802.11a - find an access point (AP) operating and broadcasting beacon frames on a specific channel
        - Beacon frames contain information about the extended service set (ESS), basic service set (BSS), and other information that is related to the service provided by the access point (AP)
          - But, the most important information in the beacon frame(s) is the SSID. The SSID contains the ID of the basic service set
            - This identifier is used to distinguish one basic service set within another
      - Utilizing SSID information, from the BSS, the user identifies which access point (AP) he wants to associate with. Then, the (mobile) device can select which access point to be associated with, and it can initiate the Association protocol.
        - Depending on what type of network the device is connecting to, whether it is open, closed, or secured, additional authentication steps may be required to obtain connectivity
      - After passing authentication, and the association protocol, the device now has physical and link layer connectivity. The device can now exchange information with the access point (AP). The next step is to obtain an IP address via DHCP. Once a local IP address is acquired, the device can officially online and can access the Internet

    - To summarize:
        - If a host/device wants to connect to an access point (AP), then it must perform the following steps:
            1. Scan channels, listen for beacon frames containing service set identifier, and the access point's MAC address
                - The SSID is 32 octets long
                - Each network, BSS or IBSS, has 1 SSID
            2. Select access point to associate with, and initiate association protocol
            3. Maybe: Perform authentication
                - This depends on the type of network the host is connecting to, and whether it is secured or not
            4. Run DHCP, or some other protocol, so the host can get an IP address in the access point's subnet
- 802.11 Association
    - There are 2 ways for a device to be associated with, or connect to, a wireless network
        1. Passive Scanning
        2. Active Scanning
    - i.e. Diagram of Passive Scanning

```
* * * * * * * * *                     * * * * * * * * *
*               *  (1)   |---|   (1)  *               *
*   (((AP-1)))==========>| H |<==========(((AP-2)))   *
*               *        |-|-|        *      |        *
*               *          |     (2)  *      |        *
*               *          |------------->   |        *
*               *                     *      |        *
*               *                (3)  *      |        *
*               *          <-----------------|        *
*               *                     *               *
*       * * * * *                     *       * * * * *
*       * BSS 1 *                     *       * BSS 2 *
* * * * * * * * *                     * * * * * * * * *
```

        - This diagram depicts passive scanning:
            1. Beacon frames are sent from the access points
            2. An association request frame from host `H` is sent to the selected access point
            3. An association response frame is sent from the selected access point to Host `H`
    - In the example above, there are 2 basic service sets
        - Each basic service set (BSS) corresponds to one access point, and the area it covers
    - Host `H` is in the intersection of both access points' coverage area
        - Meaning, host `H` can connect to either basic service sets
        - Access points periodically send beacon messages. These messages announce the SSID, contain the identifier of the basic service set (BSS), and the MAC address of the

access point (AP)

- Host `H` will listen to the beacon frames that are in its vicinity/area
  - Since host `H` is at the intersection of the coverage area of 2 basic service sets, it can hear beacon messages from both basic service sets
- Upon reception of beacon frames, indicated by (1) in the diagram above, the host can send an association request to the access point it wants to connect/associate too
  - Host `H` can connect to either `AP-1` or `AP-2`
    - There are many mechanisms that a device can use to select which access point it wants to connect to

      i.e. The host can associate with the access point (AP) that has a stronger signal, which may indicate that the access point (AP) is closer to the host. Potentially, this can yield higher throughput, or data rate
  - A device can only be associated with one basic service set (BSS) at a time
    - Meaning, a device cannot connect to multiple basic service sets, or access points
- If host `H` decides to connect/associate with BSS 2, then:
  - It will send an association request to `AP-2`
    - This is possible because host `H` already learned the MAC address of both access points from the beacon frames
  - Upon reception of the association request message from host `H`, `AP-2` will send a response message
    - In the diagram above, the response message is (3)
- i.e. Diagram of Active Scanning

  ```
  * * * * * * * *                     * * * * * * * *
  *             *   (1)         (1)   *             *
  *  ((AP-1))<-------------|------------->((AP-2))  *
  *      |      *          |          *      |      *
  *      |      *          |          *      |      *
  *      |      *   (2)  |-|-|  (2)   *      |      *
  *      |-------------->| H |<--------------|      *
  *             *        |---|        *             *
  *             *          |          *             *
  *             *          |    (3)   *             *
  *             *          |------------------>     *
  *             *                     *             *
  *             *                     *             *
  *             *               (4)   *             *
  *             *          <-------------------     *
  *     * * * * *                     *     * * * * *
  *     * BSS 1 *                     *     * BSS 2 *
  * * * * * * * *                     * * * * * * * *
  ```
  - This diagram depicts active scanning:
    1. A probe request frame is broadcasted from host `H`,

to all access points in range

      2. Probe response frames are sent from the access points to host `H`
      3. Host `H` sends an association request frame to the selected access point
      4. An association response frame is sent from the selected access point to host `H`
  - Another approach to establishing an association is via active scanning; the previous approach is passive scanning
  - In active scanning, hosts do not wait and listen for beacon messages. Instead, they send broadcast messages, called a probe request, and they ping access points to see what basic service sets are available to connect/associate to
    - Upon reception of this broadcast/probe message, access points (can) send a response called probe response. This allows the access point (AP) to convey to the host what is the B-SSID and MAC address of the access point (AP)
      - Upon reception of the probe response, the remaining steps are similar to passive scanning. The host can decide which access point it wants to connect/ associate with, and it will send an associated request. Then, the corresponding access point sends an associated response frame. Now, the physical link layer connectivity has been established, and the next step may involve authentication. Finally, the DHCP protocol is executed to assign the newly connected host an IP address
- Q/A
  - Q: How does a website determine if a connected device is a phone or a laptop?
    - A: Typically, the website learns this information through metadata that is sent through the HTTP request. The HTTP request can include signature/ identifying information such as browser type, browser version, operating system, etc.
      - This is how companies fingerprint users, and track them
  - Q: How is location determined on a laptop? (i.e. When you connect to a website for the first time, your browser will display a pop-up that says, "Website wants to know your location")
    - A: First of all, phones use triangulation via cell towers to determine your GPS location. On a laptop, IP address aggregation is used. IP addresses contain some information about (general) location, but nothing too specific like postal code. IP addresses are allocated based on organizations. ISPs are assigned a block of addresses, and then they assign those addresses to specific regions. For instance, a block of addresses may correspond to the Hamilton

area, while another block may correspond to Toronto, and Mississauga will have its own block of IP addresses. By looking at the IP address, and determining which block it falls into, then the website can get rough information about your location

- This information is cost granular. Meaning, it is very rough, and cannot be used to pinpoint exact GPS coordinates.
- If you go to Amazon.ca, then Amazon will notice that you are coming from Canada, and offer you the chance to switch to '.ca'. This is possible because your IP address falls into the block of addresses that are allocated to Canadian hosts.
- If you wanted to watch an exclusive TV series that is available in USA, but not Canada, then you would need to get a VPN, and change your IP address to pretend that you are in USA.

- Q: If IP addresses are aggregated, does that imply that my neighbours have a similar IP address to mine?
  - A: If both parties are in the same area, and have the same provider, then Yes. For instance, if you and your neighbour are customers of Rogers, then chances are that your IP addresses are within a subnet from Rogers. Thus, your IP address will be close to your neighbours. However, if you are on different service providers, then the IP addresses can be different