Data Link Layer (Layer 2): Router

- This layer must control how data is transmitted over a specific mediums and over single link/segment, and must make accommodations for the medium
- This link layer can be divided into two sub layers – **Logical Link Control and Media Access Control**

Data Link Layer Addressing:

- Previously in above layers Ip address and ports doesn't change but in link layer headers and trailers are rewritten in each hop

Data Link Protocol/Types:

- **Point to Point:** Involves two host. A frame has only one possible destination making addressing redundant (Think two host connecting (they are devices not router or switches) to each other and transmitting stuff between each other). Mac Addressing less important since one host

- **Multi-access:** such as Ethernet multiple host connecting to same network segment
    - Uses mac addressing to determine which frames (relates to packets which are now frames) go to which host. Since with multi-access we have lots of host
    - Must be careful about how and when they can transmit to avoiding ***collisions*** which makes transmitted data unusable
        - *Collision:* Two devices/host transmitting at same time can cause collision requiring message to be resent. So must take turns **via Media ACCESS CONTROL**

Logical Link Control sublayer: Wireshark Type: IPV4

- Layer that interacts with network layer and tells the receiver which network protocol is encapsulated (usually Ipv4 or Ipv6)
- Encapsulates network layer data (Normally packets but now frames) into frames

Media Access Control (MAC. Relates to multi-access) sublayer: Wireshark – Destination and Source

- Does most of the link layer functions such as:
- Describe how frames should be formatted for transmission
- Governs Media access and *addressing* to ***reduce collision***

Media Access Control Addressing:

- Mac addressing to determine which frames (relates to packets which are now frames) go to which host.

Media Access Control address vs IP:

- Used by Multi access networks, since a frame can have multiple destination so we need an addressing scheme to tell which goes to which host/physical address of computer or hardware

- Mac addresses: uses **Hop to hop** when packet arrives at destination the destination Mac address is changed from what was first determined at the start (If routers are involved).
    - So the MAC address of destination host should = Mac address of the interface facing the original sender.
- Ip address uses: end to end so packets should arrive at destination with same source and destination IP that was determined at the start.

- They are hardware address and will never change and they identify the exact device on network

- Mac addresses commonly have 48 bits and use hexadecimals
    - Used by Ethernet and Wi-Fi
- Assigned by network interfaces by manufacturer and shouldn't be changed.
- Unique to every network but within the local area network the mac address has to be unique to make sure frames go in right destination.
- Split into →
    - Organisation Unique Identifier- An identifier specifies to manufacture and vendor
    - Nic specific: assigned by manufacturer vendor

- EG: 12:34:56:78:9a:BC (column)
- 12-34-56-78-9a-BC
- 1234.5678.9abc

Ip address are 32 bits (IPV4) or 128 bits (IPV6). They are address bound to device on network configured through operating system. They can change so they identify where you are connected in terms of location on the internet
Mac address are made up of 48 bits and are made out of hexadecimals. They are hardware address and will never change and they identify the exact device on network

Media Access Control approaches: Controlling transmission over multi access network to: **<u>reduce Collison</u>**-

- Controlled access (wireless): (not used anymore) Device can transmit at a **given time**. Avoids collision.
  - ***Token Based/Ring****:* Devices are given a token and then they can transmit. They then pass the token when they have nothing to transmit. Responding devices must have token to respond.
  - ***Time division multiple access:*** Transmission time is divided into slots controlled by a node (mobile tower). Devices can transmit in each of the divided transmitted slots. Based by polices and demand
    - 3G uses this since geographic distance
    - Use Time division when devices are further away from each other as token passing takes a long time
  - ***Frequency division multiple access:***
    - Available spectrum is sub dived among all devices in range
    - Each device may only transmit on its allocated frequency, if frequencies are not spaced than they can interfere and collide with one another.
    - For: satellite communication or full duplex communication
  - ***Frequency hopping spread spectrum:***
    - Divides usable frequency space into multiple channels
    - Communicating devices establish random hopping pattern between channels different devices share medium using different patterns
    - For: Bluetooth

- Contention based access: *Most common compared to controlled access. Devices can transmit at **any time** but usually devices must listen for other transmission before transmitting. This is done by
  - ***Carrier sense multiple access:***
    - Carrier Sense Multiple Access/Collusion Detection: Ethernet – when two packets collide a jamming signal will be transmitted forcing a back out period where devices stop transmitting
    - Carrier sense Multiple access/Collusion Avoidance:
      - Wireless devices are unable to reliably detect collisions because there may be a hidden node problem where not all devices are within range to hear transmission from each other
      - Idea is a random amount of time before sending the process is:
        - Device send a request to send which signifies start of transmission
        - This prevents other devices from transmitting packets until transmission is complete
        - Devices await clear to send which signifies permission to transmit packets and also acknowledgement that the receiver has frame

Duplexing:

- Half-Duplex: host can only send or receive packets at a given time
  - EG: Wireless radio and WIFI and fibre

- Full Duplex: supports host transmission in both directions at same time
    - EG: modern Ethernet (think xbox set up)

Physical Layer (Layer 1):

- Encodes binary bits (0s and 1s) into signals that can be carried across the physical medium (communication medium) by amplitude, frequency or phase. Techniques/Methods
    - Manchester Encoding: bits encoded in middle of each period
    - Demarcating Frames: uses specific signal patterns to identify the start and end of a frame
- Specifies the physical connectors and cables (communication medium) can be used

Communication Medium:

Copper Medium: uses electronic signals. Types-

- Coaxial Cable: (not used much compared to alternative)
    - Copper cable used for TV networks but can deliver broadband
    - Performs poorly compared to twisted pair cabling since very thick and not bendable + expensive
    - 10Base2 and 10Base5 Ethernet.
- Twisted Pair: (more common than above)
    - Twists colour coded pair of copper wire to reduce the impact of *interference*
    - Different categories such as:
        - Cat5e/6/6a: Used for modern Ethernet
        - Cat3: for telephone services
- Serial Cables: (think raspberry Pi pin cable)
    - Used between a router and ISP as wan link
    - Can be break easily due to small pins
- Rollover Cable: console cables
    - Used for configuring network equipment (doesn't twist copper)
    - One end has serial and other Ethernet

Fibre Medium: Use light/laser for transmission of data along strand

- Single Mode Fibre:
    - Core is small that light goes through in straight path. Laser as light
    - More expensive then multi-mode
    - Uses wave length division frequencies
- Multi-Mode Fibre:
    - Larger cores allow multiple paths for light typical led as light sources
    - Cheaper then single mode

Wireless Medium: Digital signals are used

Factors which will make signal less strong

Attenuation:

- Signals in all medium will attenuate/reduce in strength with more distance
    - Lan speed (Ethernet) always going to be faster wan speed (adsl)
    - Ethernet max distance of 100meter must use cat5
- Depends on medium: highest is wireless → copper → Fibre
- Depends on frequencies

Interference:

- Is noise introduced into signal on medium by external factors that can signal strength to decrease
- May cause errors in transmission such as render data unreadable
- EG: microwave frequencies effect wifi/radio waves → Why cables may shielded to reduce

* ***The logical topology*** is the schema of the actual path the data follows within the physical topology. It differs from the **physical topology** in that not only does **it show the location of network components**, ***it also shows the path the data follows*** through these components as well as the ***direction of travel***

Network Topologies (Layout of networks):

- **Physical Bus Topology**: Has a single main cable and each devices can be connected to it with short cables. EG
    - 10base2/5 Ethernet network:
        - Uses coaxial cable as single main cable
        - Requires less cables to support this type of bus topology and new devices and new devices can join
        - Requires CSMA/collusion detection
    - Data over cable service interface specification (docsis or HFC)
        - Uses single coaxial cable and all houses will share bandwidth in street (at same time) So HFC uses part fibre and part coaxial cable
        - Basically uses cable tv to deliver internet
- **Physical Star Topology**: Has multiple cables one for each device and they all connect to a single node
    - 10BaseT Ethernet network:
        - Uses twisted pair cables as the multiple cables
        - Requires hubs and switches to connect to devices
        - Switches forward transmission to destination no collision
    - 802.11 (WIFI): Network:
        - Uses radio frequency for devices with a wireless access point to connect to (node)
        - Supports of 11MBps -2167Mbps
        - Popular due to convince
    - ADSL (asymmetric digital subscriber line) Network:
        - Common internet connection that can use existing telephone cables and connects to ISP dslam (so think our home internet used to connect to exchange)

        - Upload speed slower + Supports 1.6mbps to 24mbps (depends on DSlam distance)
        - If DSlam is closer then obviously faster. The dslam (exchange) connect to isp using fibre
        - Can use phone and internet because of different frequencies
    - Very High Bit-rate DSL (VDSL or FTTN):
        - Move DSLM (Exchange) closer to house through a node. Therefore less than 1 km of copper
    - Direct/Point-to-point fibre
        - Fibre is connected directly into premise all the way from main exchange (DSLM) more for business
        - Costly and connection is one to one with two fibres to every site since duplex (upload and download)
    - Gigabit Passive Optical Network (FTTP)
        - Connect a single fibre to small single street unit, which then splits light out to a single fibres connected to homes
        - Passive no need for node
- **Logical Ring Topology:**
    - Token Ring network:
        - Host will pass token allowing transmission
        - Cabled using star topology but uses logical ring topology
        - Early version used coaxial but twisted pair become available
        - Support 4mbps -16mbps