Topic 5: Physical Layer

Ross Emile Aparece

Class 8
02/25/2025

- Physical layer is the lowest level:
  - Understanding that the physical properties of various transition mediums define the proctocls we use
  - Bit by bit encoding of information into physical signal
- Ethernet (copper) cables:
  - Encoded as pulses of electricity
- Fiber cables:
  - Encoded as pulses of light
- Different physical properties so they may have different protocols
- Cabled connections
  - DLL protocol = 802.3 Ethernet
  - Point to point connections (exactly two devices)
    - Fiber
      - Full enclosed glass tubes with mirrored shielding
      - Photons bounce along the cable until it reaches a detecor
      - Needs to be as straight as possible
    - Copper / Twisted Pair
      - Pair needed to complete the circuit
      - Two electrical magnetic field generated positive and negatively charged respectively
      - Field is powerful enough to corrupt data
      - Electomagnetic inteference cancel each other out if they are close enough hence twisted
- Wireless connections

  - DLL protocol = 802.11 WiFi
  - Non-directional
    * All wireless devices go in every direction
    * Only matters if the device is within the range
    * Everyone in the recipient range of the device recieves the data
  - Encryption by default
    * Encryption by default has speed cost
  - Encoded as radiowaves
- Channel Types
  - Simplex (unidirectionality)
  - Duplex (biderectionality)
    * Full Duplex (send and receive at the same time)
    * Half Duplex (send or receive at any time only one receiver)
  - All cables can full duplex only restriction is cost
  - All wireless operate at half duplex
  - Modern devices operate at half duplex but extremely highspeed
    * Operates on the scale of picoseconds
  - Feels like full duplex
- Hardware
  - Each layer has a specific hardware devices
  - Network Hub (Physical Layer, Historical)
    * Solve the limitation of the cable
    * Central hub that ideally connects all devices
    * Act as an n-dimensional cables
    * No CPU or memory, just a bunch of logic gates (reducing cost)
    * Duplicates signal and sends the signal to all ports
    * Problem arises when two or more devices send at the same time data easily corrupted
      · This is called a collision domain
      · If there is more than one sender none of the messages get through
    * Cannot update the hub so you have to update all the devices connected
    * Carrier Sense Multiple Access
      · Solves collission domain problem by sharing the network

```
function CSMA(message){
    while(receiving){
        wait();
    }
    send(message);
}
```

- Downgrades connection to half duplex
- Limitation is assuming everyone upgrading at the same time
- Devices with CSMA and devices with no CSMA do not play well together
- Device without CSMA can still corrupt transmitted data

* CSMA With Collision Dection

```
function CSMACD (message){
    for(i = 0; i < message.length; i++){
        while(receiving){
            wait();;
        }
        send(messaage[i]);
    }
}
```

– Network Switch

*

Class 9
02/27/2025

- Topic 6: Data Link Layer
  - Translation from digital bits into physical bits
  - Hop to hop delivery between two directly connect adjacent nodes over a single transmission medium (can be wireless)
  - Addressing:
    * How to distinguish between different devices
    * DLL (Data Link Layer): MAC Address
      - A globally unique hardware identifier assigned to every network card
      - No two MAC addresses should be the same
      - 48 bits 2^{48} = 281 trillion
      - ex. 6E-3F-BB-22-A0-0F (6 pairs of hexadecimal numbers)

        - First 3 pairs = Organizational Unique Identifier
        - Last 3 pairs = Network Interface Component/Card
        - MAC addresses managed by IEEE
        - First 3 pairs are assigned to a company
    * You can change the MAC address but in 99% it doesn't make sense
    * MAC address survive a single hop and only used to bring you one hop closer
    * Cannot fool anyone more than 1 hop away from you
- Protocols
    * 802.3 Ethernet (wired connections): simple header and data protocol
    * 802.11 WiFi (wireless): complex protocol
        - Many (100s) of different types of messages
    * Underlying physical properties between the two are so different they need different protocols
    * Ex. ethernet cable you just need to plug in but for wireless you need to select the correct device and put in a password
    * Wireless needs a more complex protocol to accomodate its physical properties
    * Ethernet has a faster protocol focused on throughput
- What is provided by the header?
    * Preamble = alternating set of 0 and 1 used to provide synchronization between sender and receiver
        - Devices operate at different speeds but need to communicate
        - SFD last byte of preamble contains a bunch of 1's to signal that the preamble is over
    * Destination MAC and Source MAC
        - Lets us know who the sender is and who the receiver is
        - Each number = number of bytes
    * EtherType
        - Tells us the network protocol used in the payload, most common:
        - 0x0800 = IPv4
        - 0x86DD = IPv6
        - 0x0806 = ARP
        - 0x8100 = IPv4 and 802.1Q
    * IPv4: mainly used in the US, we didn't make the IP address field large enough
    * IPv6: used in addition, used in the rest of the world
    * ARP: used to translate IP to MAC address

* IPv4 + 802.1Q: 802.1Q provides VLAN support
* Provides logical seperation of networks where you are phsyically conencted to other devices
* Provides quality of service, refers to priority
* Allows us to assign higher priority to different devices
* Can make a difference in real time applications
* CRC/FCS
    - Frame Check Sequence
    - Algorithm provides data integrity
    - Ability to detect when data is corrupted while in transit
    - Internally uses CRC32 hash algorithm to provide the property
    - Takes variable sized input, fed into hash algorithm, received fixed length digest
* Interframe = ensures messages dont collide
* Data Integrity vs Reliable delivery
    - Data Integrity = Ability to detect when data is corrupted
    - Reliable delivery = Constantly redeliver message until it is delivered
* Ethernet itself does not provide reliable delivery
* Reliable delivery is not free, data integrity is more important