The Link Layer

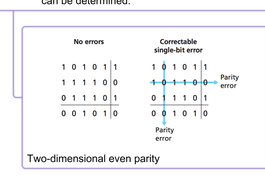
(Possible) Services provided by the Link Layer

- Framing
  - Framing means encapsulating the network diagram with a link-layer frame containg a data field where the network-layer datagram is inserted, and a number of header fields.
- Link access
  - A medium access control (MAC) protocol specifies the rules by which a frame is transmitted onto the link. Basically which link to send the datagram to next.
- Reliable delivery
  - When a link-layer protocol provides reliable delivery service, it guarantees to move each network-layer datagram across the link without error.
- Error detection and correction
  - When this is implemented into a link-layer protocol the link-layer can detect the error an correct it before sending it further.

Where is the Link Layer Implemented

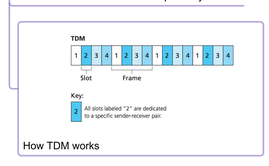
- Hardware
  - Most often it is implemented in a network adapter/network interface card(NIC).

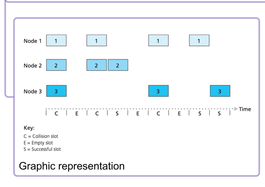
Error-Detection and -Correction Techniques

- Parity Check
  - Suppose the information to be sent consists of d bits.
    This check will den add a new bit at the end called the "Parity bit".
    This will either be 1 or 0 depending on the bits in the package.
    If the original data contains an odd number of 1s the parity bit will be 1. If the data contains an even number of 1s the parity bit will be 0. To summarize, the total bit sequence including the parity bit will have an even number of 1s. If not, an error has occured.
  - This is obviously not good enough. As, if an even number of bit is altered, the error won't be detected.
- Two-dimensional parity
  - The same as parity check, but using two rows instead. This way the exact place of the bit error can be determined.
  - 

    Two-dimensional even parity
- This can also work with odd number of 1s instead of even
- Checksumming Methods
  - Basically the same method as the checksumming method used in the network layer
- Cyclic redundancy Check (CRC)
  - See section 5.2.3 for a deeper explanation about how this works

Multiple Access Links and Protocols

- Point-to-point link
  - Consists of a single sender at one end of the link and a single receiver at the other end of the link
- Broadcast link
  - Can have multiple sending and receiving nodes all connected to the same, single, shared broadcast channel
- Multiple access problem
  - How to coordinate the access of multiple sending and receiving nodes to a shared broadcast channel
- Multiple access protocols
  - Channel partitioning protocols
    - IDEAL protocol should have the following properties
      - When only one node has data to send, that node has a throughput of R bps.
      - When M nodes have data to send, each of these nodes has a throughput of R/M bps. (On average)
      - The protocol is decentralized; that is there is no master node that represent a single point of failure for the network.
      - The protocol is simple, so that is is inexpensive to implement
    - Time-division multiplexing (TDM)
      - Divides time into time frames
      - Divide each time-fram into N time slots
      - Eliminates collisions and is perfectly fair
      - 

        How TDM works
    - Frequency-division multiplexing (FDM)
      - Divides the R bps channel into different frequencies.
      - Each node gets its own frequency
      - Eliminates collisions and is perfectly fair
    - Code division multiple access (CDMA)
      - Assigns a different code to each node
      - Each node uses it's unique code to encode the data bits it sends
      - Different nodes can transmit simultaneously
      - Often used in cellular telphoney
  - Random access protocols
    - Slotted ALOHA
      - Advantages
        - Assume all frames consist of exactly L bits
        - Nodes start to transmit frames only at the beginnings of slots
        - Time is divided into slots of size L/R seconds
          - The time it takes to transmit one frame
        - All nodes are synchronized so that each node knows when the slots begin.
        - If two or more frames collide in a slot, then all the nodes detect the collision event before the slot ends
      - How it works
        - 

          Graphic representation
      - Disadvantages
        - Some math shows that the effective transmission rate (given that the channel has a throughput = R) is only 0.37R bps.
    - (Unslotted) AHOLA
      - Works the same as slotted AHOLA, but instead of given slots, it retransmits when there is a collision after some randomly chosen time period
    - Carrier Sense Multiple Access (CSMA)
      - Two basic principles
        - Listen before speaking
          This is called carrier sensing. If you sense someone else transmitting data, wait for it to stop.
        - If someone else begins talking at the same time, stop talking.
          This is called Collision detection. If you sense someone else transmitting, stop your transmission, and wait a random amount of time before repeating the sense-and-transmit-when-idle cycle
  - Taking-turns protocols
    - Polling protocol
      - One master node
      - Master node polls each of the nodes.
        First tellas node 1 that it can transmit some data.
        After that it tells node 2 this and so on n cycle.
      - Advantages
        - Eliminates collision
        - Eliminates empty slots
      - Disadvantages
        - Polling delay
          - The time required to notify a node that it can transmit
          - If only one node is active, the master node still have to notify every other node that it can transmit, so the rate will be less than R bps
          - If the master node fails, the entire channel becomes inoperative.
    - Token-passing protocol
      - No master node
      - A frame known as a token is exchanged among the nodes in som fixed order.
        Example: Node 1 always sends the token to node 2. Node 2 always sends the token to node 3...Node N always sends the token to node 1.
      - Once a node has a token it holds on to it only if it has some frames to transmit.
        Otherwise it immediately forwards the token to the next node.
      - Advantages
        - Decentralized
      - Disadvantages
        - Failure of one node can crash the entire channel

Switched Local Area Networks

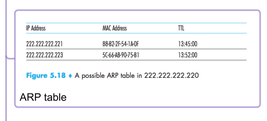
- Link-Layer Addressing and ARP
  - MAC Addresses
    - Addresses used in linka layer
    - Not given to hosts or routers, but their adapter, that is their network interfaces.
    - A host or router with multiple network interfaces will have multiple MAC adresses associated with it.
    - 6 bytes long, giving 2^48 possibilities
    - Every adapter has a unique address (Allocated by IEEE which manages address chunks)
    - Never changes (unlike IP-addresses)
  - When an adapter receives a frame it will check if the MAC-address matches it's own. If not the frame will be discarded. If it indeed is a match it will process it.
  - If a sending adapter wants all of the adapters on the LAN to receive and process the frame it can use the MAC broadcast address. (FF:FF:FF:FF:FF:FF)
  - ARP(Address Resolution Protocol
    - Protocol to translate between IP-adresses and MAC-addresses
    - Only resolves IP-addresses for hosts and router interfaces on on the same subnet. (Unlike, for example, DNS).
    - How does it work
      - Each host and router has an ARP table in its memory.
        This contains mappings of IP addresses to MAC addresses.
      - All addresses will have a TTL. Usually around 20 minutes.
        After this it will be deleted. This causes the table to update at least every 20 minutes.
      - 

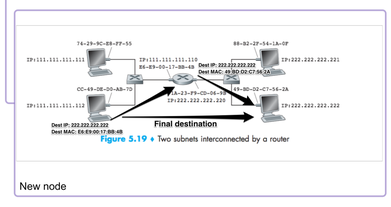
        Figure 5.18 • A possible ARP table in 222.222.222.220
        ARP table
      - If the sender don't have a receiver in its table it will need to resolve the address.
        The sender first construct a special packet called an ARP packet. This includes the sending and receiving IP and MAC addresses.
        The address will here be the MAC broadcast address. All adapters it reaches will then check if the destination IP address in the packet matches. If it does it sends back a response ARP packet, which contain the necessary information (it's MAC address). The sender can now update it's table.
    - Plug-and-play. An ARP table gets built automatically, with no configuration needed from a system administrator.
  - Sending datagrams off the Subnet
    - To do this, the sender can't access the MAC address of the host with the correct IP. Therefore the destination MAC address will not be the MAC address of the destination IP but the MAC address to the router/switch connected to the "outside" Internet.
    - 

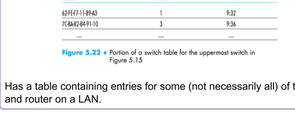
      Figure 5.19 • Two subnets interconnected by a router
      New node
- Switched Local Area Networks
  - Ethernet
    - Link layer interface
    - Header fields
      - Data field. Carries the IP datagram
      - Destination address. MAC address of the destination adapter
      - Source address. MAC address of the source adapter
      - Type field. As ethernet can be use for other things than IP it has the ability to differentiate different type of traffic.
      - Cyclic redundancy check(CRC). Used to detect bit errors.
      - Preamble. Used to synchronize the adapter clocks. (Section 5.4.2 for more on this)
    - When a fram fails the CRC check, adapter B discard the fram. (Lacks reliable transport, this is where something like TCP is useful)
    - Has changed a lot since it was first conceived but the standard today has the following properties:
      - Backward compatible with older Ethernet technologies
      - Allows for both point-to-point links and shared broadcast channels.
        - Broadcast channels uses hubs. A hub is a physical-layer device that acts on individual bits. When a bit arrives it re-creates it and boosts its energy strength. It then gets transmitted into all the other interfaces.
  - Link-Layer Switches
    - Filtering
      - Filtering is the switch function that determines whether a fram should be forwarded to some interface or should just be dropped.
    - Forwarding
      - Forwarding is the switch function that determines the interfaces to which a fram should be directed, and then moves the fram to those interfaces.
      - 

        Figure 5.23 • Portion of a switch table for the uppermost switch in Figure 5.15
        Has a table containing entries for some (not necessarily all) of the hosts and router on a LAN.
    - Differences between routers and switches
      - Switches forward packets based on MAC addresses rather than on IP addresses
      - A large switched network would require large ARP tables in the hosts and routers and would generate substantial ARP traffic and processing.
      - Routers are not plug-and-play
    - Constructing the table (Incoming packet with destination address DD:DD:DD:DD:DD:DD arriving on interface x)
      - There is no entry in the table for DD:DD:DD:DD:DD:DD. In this case the switch simply broadcasts the fram to all it's interfaces except for x
      - There is an entry in the table, associating DD:DD:DD:DD:DD:DD with the interface x. In this case there is no need to forward the frame, the switch then discards the frame.
      - There is an entry in the table, associating DD:DD:DD:DD:DD:DD with interface y != x. In this case the frame gets forwarded to the output buffer that precedes interface y.
    - Plug-and-play. No configuration from system administrator needed (Self-learning)
      - The switch is initially empty
      - For each incoming frame received on an interface, the switch stores in its table the MAC address in the frame's source address field and the current time.
      - The switch deletes an address in the table if no frames are received with that address as the source address after som period of time (the aging time).
    - Properties of Link-Layer Switching
      - Elimination of collisions
      - Heterogeneous links. (In a network the wires doesn't necessarily operate under the same speed)