Justin Ciocoi

Dec. 16, 2023

CSCI 379 Textbook Notes

Chapter 6.4: Switched Local Area Networks

6.4.1: Link-Layer Addressing and ARP

- **MAC Addresses**
    - Hosts and routers themselves do not have link-layer addresses, but it is rather their adapters, or network interfaces, which do
    - Link layer addresses are also referred to as LAN addresses, physical addresses, or MAC addresses
    - A MAC address is meant to be permanent, and although it can be changed using software, we will assume for the remainder of this section that an adapter's MAC address will remain fixed
    - The IEEE manages the MAC address space such that no two adapters have the same MAC address, meaning MAC addresses are completely unique
    - When an adapter wants to send a frame to some destination adapter, the sending adapter inserts the destination adapter's MAC address into the frame and then sends the frame into the LAN
    - When an adapter receives a frame, it will check whether the destination MAC address matches its own MAC address
- **Address Resolution Protocol (ARP)**
    - Because there are both IP addresses and MAC addresses, there exists a need to translate between them
    - In the case of the internet, this is the job of the *Address Resolution Protocol (ARP)*
    - The ARP module on a sending host will take a destination IP address for a link-layer frame and return the corresponding MAC address such that the frame could be sent over the LAN

- Each host and router on a LAN have an ARP table in memory which contains various mappings of IP addresses to MAC addresses
- What happens when the ARP table does not have the necessary corresponding MAC address?
  - The sender constructs a special packet called an *ARP packet*
  - This packet's purpose is to query all other hosts and routers on the subnet to determine the correct corresponding MAC address
  - The query is broadcast to all hosts on the subnet, whereas the response is simply directed back to the sending host
- In order to send a frame into a different subnet, a similar protocol is followed where ARP first relays a router MAC address in order to cross subnets, followed by ARP on the receiving subnet in order to obtain the ultimate destination MAC address

6.4.2: Ethernet

- Ethernet has largely taken over the wired LAN market, as it is the most prevalent wired LAN technology and is likely to remain so for the foreseeable future
- We can learn much about ethernet through examining the ethernet frame, which we can consider in the context of sending an IP datagram from one host to another host on the same ethernet LAN

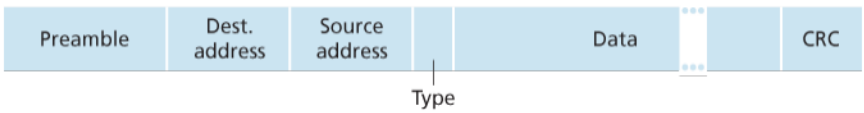

Figure 6.20 Ethernet frame structure

6.4.3: Link-Layer Switches

- **Forwarding and Filtering**
  - Filtering is the switch function which determines whether a frame should be forwarded to some interface or should just be dropped
  - Forwarding is the switch function that determines the interfaces to which a frame should be directed, and then moves the frame to the appropriate interfaces
  - These functions are achieved using a *switch table*
- **Self-Learning**

- A switch has the useful property that its table is built automatically, dynamically, and autonomously, and is accomplished as follows

    1. The switch table is initially empty
    2. For each incoming frame received on an interface, the switch stores in its table:
        - The MAC address in the frame's *source address field*
        - The interface from which the frame arrived
        - The current time

        This allows the switch to record in its table the LAN segment on which the sender resides
    3. The switch deletes an address in the table if no frames are received with that address as the source address after some period of time

- **Properties of Link-Layer Switching**
    - *Elimination of Collisions*
        - In a LAN built from switches, there is no wasted bandwidth due to collisions
        - The switches buffer frames and never transmit more than one frame on a segment at any one time
        - As with a router, the maximum aggregate throughput of a switch is the sum of all the switch interface rates
    - *Heterogeneous Links*
        - Since a switch isolates one link for another, it allows links in the LAN to operate at different speeds and run over different media
        - This is especially useful for a LAN in which both legacy and newer technologies are used
    - *Management*
        - A switch eases network management tasks in various ways by automating and detecting various occurrences
- **Switches vs. Routers**

- Routers are store and forward packet switches which forward packets using network layer addresses
- A switch is fundamentally different in that it uses MAC addresses rather than network layer-addresses
- Since both can be used to create interconnected networks, we must consider the pros and cons for both switches and routers
- *Pros and Cons of Switches*
    - Switches are plug-and-play, which is a cherished property by any network administrator
    - Switches also have relatively fast filtering and forwarding rates since they process frames only through 2 layers instead of 3
    - The active topology of a switched network is restricted to a spanning tree
    - A large switched network also requires large ARP tables and will generate substantial ARP traffic and processing
- *Pros and Cons of Routers*
    - Since network addressing is hierarchical, packets do not normally cycle through routers even when the network has redundant paths
    - This means there is no restriction on active network topology and instead the network can use the best path between source and destination
    - The most significant drawback is that routers are not plug-and-play, meaning that they must be configured manually