CS 456 Hao Pan
Salahuddin, Mohammad
Spring 2018

Chapter 6.3 LANs

6.3.1 MAC Addresses and ARP

- A **MAC address** is a 32-bit IP address.
- The MAC address is a network-layer address (layer 3) used for forwarding.
- Formally, it functions to locally get frames from one interface to another interface that is physically connected (same network or in IP-addressing state).
- 48-bit MAC addresses, which are burned into the Network Interface Controller ROM (NIC ROM), are also sometimes used for the software settable.
- An example of a MAC address is *1A-2F-BB-76-09-AD*. The numbers are in hexadecimal, meaning they each represent 4 bits.

6.3.2 LAN Address and ARP

- Each adapter on LAN has a unique LAN address.
- MAC address allocation is administered by IEEE.
- Manufacturers buy a portion of available MAC address space in order to assure uniqueness.
- As an analogy, compare a MAC address to a Social Security Number - and compare an IP address to a postal code.
- A MAC address is portable since the LAN card can move from one LAN to another. IP addresses are not portable, though, since they depend on the IP subnet that the node is attached to.

6.3.3 Address Resolution Protocol (ARP)

- Every IP node (host, router...) on LAN has an ARP table.
- The **ARP table** contain IP/MAC address mappings for some LAN nodes in the form of: *¡IP address; MAC address; TTL¿*. The *Time to Live (TTL)* represents the time after which the address mapping will be forgotten. It is typically set to 20 minutes.
- Over the same LAN, if one host wants to send a datagram to another:
  - If it doesn't have the target's MAC address in its ARP table, it will broadcast an ARP query packet containing the target's IP address.
  - The target will, after receiving the ARP packet, reply to the sender with its own MAC address.
  - A cache will save the IP-to-MAC address mapping until it times out.
- Over another LAN:
  - Note that the sender will have the IP address of its first hop router, and it will know the router's MAC address (because of OSPF?).
  - It will create an IP datagram marking itself as the source and the target as the destination.

- It will create a link-layer frame with the router's MAC address as the destination. The frame contains the datagram.
- Once the router receives the frame, the datagram is removed and passed up to IP.
- The router will create a link-layer frame with the destination's MAC address as the destination. The frame contains the datagram.
- The frame will be forwarded to the destination MAC address after that.

6.3.4 Ethernet

- **Ethernet** is the dominant wired LAN technology.
- Ethernet is cheap ($20 for NIC), the first widely used LAN technology, simpler and cheaper than token LANs and ATM, and kept up with the speed race (10Mbps - 10Gbps).
- Two Ethernet physical topologys are widely used:
  - **Bus** was popular through the mid 90s. All nodes are in the same collision domain, meaning they can all collide with each other.
  - **Star** is widely used today. An active switch is placed in the center of the topology, and each "spoke" runs on a separate Ethernet protocol which connects to the switch. Thus, nodes will not collide with one another.
- Ethernet is **connectionless**. There is no handshaking between the sending and receiving NICs.
- It is *unreliable*. The receiving NIC doesn't send acks nor nacks back to the sending NIC. Thus, data in dropped frames can only be recovered if the sender uses a higher layer rdt, like TCP. Otherwise, the dropped data is lost.
- Ethernet's MAC protocol uses unslotted *CSMA/CD with binary backoff*.

6.3.5 Ethernet Frame Structure

- The sending adapter encapsulates an IP datagram (or any other network layer protocol packet) in an *Ethernet frame*.
- If the adapter receives a frame with matching destination address or with a broadcast address (such as ARP packets), it will pass the data in the frame to the network layer protocol. Otherwise, the frame is discarded.
- The **type** indicates higher layer protocol. It's mostly IP, but others are also possible.
- A *cyclic redundancy check (CRC)* is done at the receiver. The frame is dropped if an error is detected.

6.3.6 Ethernet Standards

- Many different Ethernet standards exist.
- A common MAC protocol and frame format should be used for consistency.
- Different speeds can be used.
- Different physical layer media exist, such as *fiber* and *cable*.

6.3.7 Ethernet Switch

- The **Ethernet switch** is a link-layer device. It takes an active role in storing and forwarding Ethernet frames.
- Incoming frames are examined, and based on their MAC address, the frames are selectively forwarded to one or more outgoing links when they are about to be forwarded on segments. CSMA/CD is used to access segments.

- Hosts are unaware that swiches exist.
- Switches are self-learning. They do not need to be configured.
- Hosts have a dedicated and direct connection to the switch.
- Ethernet protocol is used on each incoming link, but there is no collisions since full duplex is used. Thus, each link has its own collision domain.
- See an example of simultaneous transmissions over a switch on **slide 5-50**.
- Switches contain a switch table. Each entry maps a host's MAC address to the interface required to reach that host *(host MAC address, interface used, time stamp)*. It looks very similar to a routing table.
- A switch is *self-learning* in that they learn which host can be reached through which interfaces. Whenever a frame is received, the switch learns the location of the sender and records that information in the switch table.
- When a frame is sent through a switch, the switch will index its switch table using the MAC destination address. If an entry is found, then it will check if the destination is on the segment from which the frame arrived. It will drop the frame if it is, and forward the frame on the entry it found if it's not. If the entry could not be found in the switch table, every interface except for the sending one will be flooded. See a more clear representation of this process on **slide 5-53**.
- Switches can be connected together, like in the diagram on **slide 5-55**. Switches do self-learning exactly as they do in a single-switch case.

6.3.7.1 Switches vs. Routers

- Both routers and switches are store-and-forward applications; however, routers are *network-layer* devices while switches are *link-layer* devices.
- Both also have forwarding tables. A router computes tables using routing algorithms. Routers rely on IP addresses. Switches, on the other hand, learn forwarding tables by flooding and self-learning. Switches rely on MAC addresses.