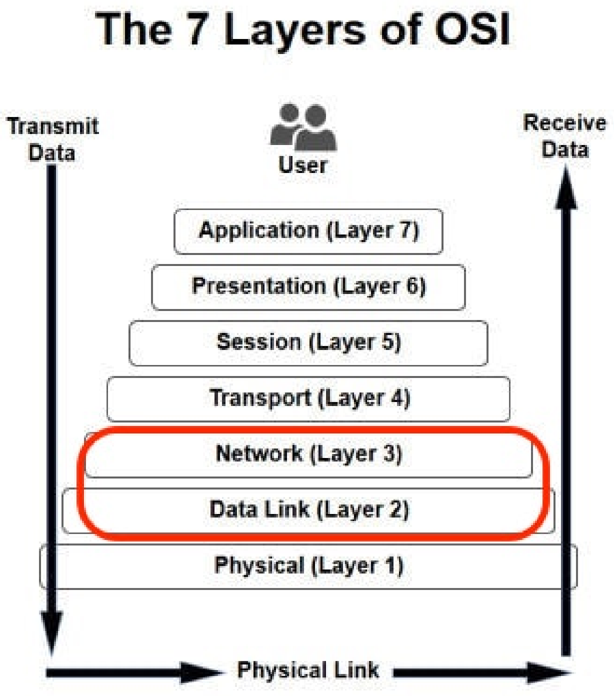
jy2gm
sg4fz

Lecture 5

CS 4457
January 28, 2020



1 Review of MAC Protocols

Last lecture we discussed the MAC protocols and these were some of the most important points to remember:

1. the protocols allow for channel partitioning, which uses concepts of time, frequency, or code division
2. it also allows for random access (dynamic)
   - i ALOHA, S-ALOHA, CSMA, CSMA/CD
   - ii carrier sensing: easy in wired technologies, and harder for wireless ones
   - iii CSMA/CD used in Ethernet
   - iv CSMA/CA used in 802.11
3. lastly, MAC protocols allow taking turns, which considers polling from a centralized source and/or token passing, which allows only the host with the token to broadcast. Furthermore, this is how bluetooth, FDDI, and token ring works

2 LANs

2.0.1 Definitions

LAN (Local Area Network). Used to connect an end system to the edge router

MAC (or LAN or physical) address A *link-layer* address. For most LANs, the MAC address is 6 bytes long, giving 2^{48} possible MAC addresses. MAC address allocation administered by the IEEE. Designed to be permanent, but possible to be changed via software. Analogous to a social security number

IP address 32-bit *network-layer* address. Analogous to a postal address

2.1 Addressing, ARP

The **Address Resolution Protocol (ARP)** translates between IP addresses and MAC addresses. Each host and router has an **ARP table** in memory which contains these mappings along with a time-to-live (TTL) value which indicates when each mapping will be deleted from the table.

2.1.1 Sending a Datagram on the Same Subnet

1. A wants to send datagram to B (B's MAC address not in A's ARP table)
2. A broadcasts ARP query packet, containing B's IP address received by all nodes on the LAN
3. B receives ARP packet, replies to A with its (B's) MAC address
4. A caches (saves) IP-to-MAC address pair in its ARP table until TTL

2.1.2 Sending a Datagram off the Subnet

1. A creates IP datagram with IP source A, destination B
2. A creates link-layer frame with R's MAC address as dest, frame contains A-to-B IP datagram
3. Frame sent from A to R
4. Frame received at R, datagram removed, passed up to IP
5. R forwards datagram with IP source A, destination B
6. R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram

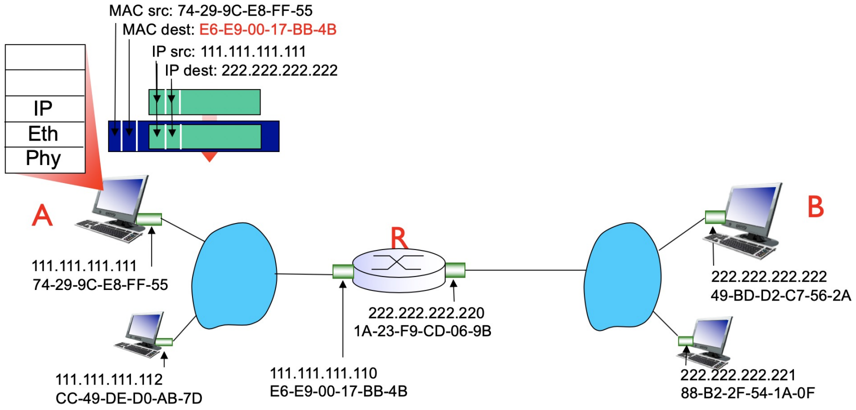


Figure 1: ARP Protocol

2.2 Ethernet

Ethernet is the dominant form of wired LAN technology. First proposed by Metcalfe using the sketch below, Ethernet took over the wired market due to its cheap and reproduceable NIC design which was able to keep up with the speed race as the rest of the network stack improved.

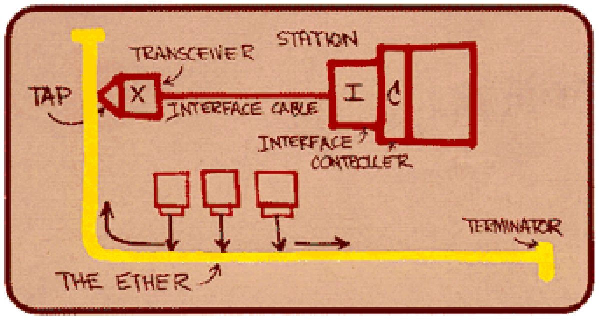


Figure 2: Metcalfe's Ethernet sketch

The physical topology of Ethernet had two prevailing models throughout its lifetime:

Bus This method was popular through the mid 90s and used the idea of all nodes in the same collision domain. This meant that collisions were inevitable

Star This is the most popular method today and is based off of a centralized active switch which directs datagrams. Each spoke coming out of the center runs a separate Ethernet protocol, which prevents collisions from every happening

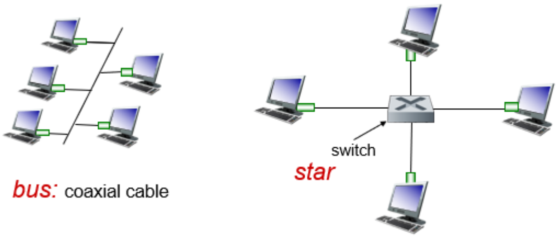


Figure 3: Diagram showing how bus and star methodoligies differ

2.2.1 Ethernet Frame Structure

The frame structure of Ethernet includes the following:

Preamble These first eight bytes of the frame allows the receiver to sync the local clock with the sender's in order to decode the Manchester encoding and receive the intended payload

Destination Address This is a six byte MAC address of the receiver which lets the network know where to send the frame

Source Address This is a six byte MAC address of the sender, which lets the switch know which interface the source maps to

Type Indicates higher later protocol, mostly in terms of IP

Data (Payload) The datagram that is being communicated by the source to the destination

CRC The error detection bits that the receiver must use to know the validity of the message (See lecture 3 notes)

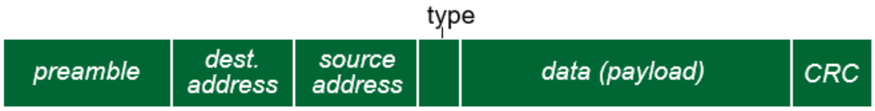


Figure 4: The split of the Ethernet frame

2.2.2 Ethernet Features

Connectionless This means that there is not handshaking between sending and receving NICs

Unreliable Receiving NIC does not send acknowledgements to the sending NIC, meaning any dropped data is forever lost, as no request is made to resend

There are many different Ethernet standards, between these protocols we have the following variables differing:

i speeds such as 2 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps

ii physical later media such as fiber versus cable

While these differ, MAC protocol and frame format are often the same among all the different Ethernet standards.

2.3 Switches

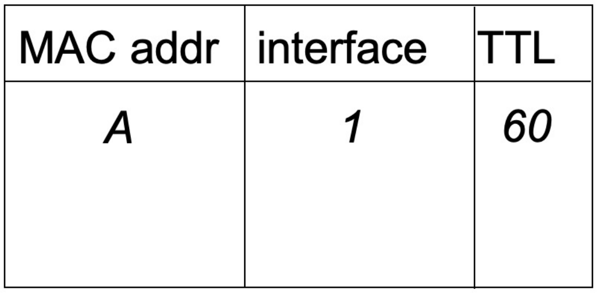
Ethernet installations used a star topology with a **switch** in the middle. A switch is not only collision-less, but is also a store-and-forward packet switch. Unlike routers which operate up through the *network layer*, a switch operates only up through the *link layer*.

2.3.1 Definitions

Filtering The switch function that determines whether a frame should be dropped or forwarded to some interface

Forwarding The switch function that determines the interfaces to which a frame should be directed, then moves the frame to those switches

Switch table Contains a MAC address, the switch interface that leads toward that MAC address, and the time at which the entry was placed in the table



MAC addr	interface	TTL
A	*1*	*60*

Figure 5: Switch Frame

2.3.2 Self-Learning

Switches are programmed to learn which interfaces match with which host. This is done upon *receiving* a frame from the host (to be sent to some other destination), at which time a **Switch Table** is populated, with the fields MAC address of the host, the interface it connects to, and its TTL (time to live). The last field is a safety measure, accounting for hosts switching interfaces and not breaking the system.

In the case where a receiving host's connecting interface is known by the switch, the frame is sent directly to that host through the corresponding frame recorded in the switch table. However, when no such knowledge exists and the switch is unaware of which interface the receiver is connected to, the frame is **flooded** to all interfaces, less the sending one. The intended receiver can simply scan the frame for the destination address and if it matches its own MAC address, then it will go on to the rest of the steps, otherwise the frame can be dropped. The right side of *Figure 3* displaying the star method of Ethernet topology shows us this setup where the middle device is the switch housing the switch table, and the lines connecting the devices is the interface each host connects to the switch through.

2.3.3 Interconnecting Switches

Switches are not only limited to connecting its interfaces to host computers, it can also connect to other switches. This allows the network to form bidirectional graphs which the frames can traverse.

The introduction of cycles into this graph can cause the looping of the same frame upon a host or switch, to combat this problem, the time to live of a given frame decreases by one upon each broadcast, when this reaches zero, the frame is dropped from the network. In a real network, this happens very often and it is the job of an efficient routing algorithm to the figure out the shortest path a frame can take from any given source to any given destination.

Professor Graham proposed the class with the challenge of figuring out how a network can solve such a problem or at least approximate a shortest path from a source to destination, give it a try!

2.3.4 Switches vs. Routers

- Both are store-and-forward:
  - Switches: link-layer devices (examine link-layer headers)
  - Routers: network-layer devices (examine network-layer headers)
- Both have forwarding tables:
  - Switches: learn forwarding table using flooding, learning, MAC addresses
  - Routers: compute tables using routing algorithms, IP addresses

2.4 VLANs

Let us first consider the motivation behind VLANs. Let there be a partitioning of offices which the networks wants to identify, like Computer Science and Electrical Engineering offices all inside a single LAN network. To properly divide these up and allow for easy access across the switches between the department networks, we consider VLANs, which stands for *Virtual Local Area Network*. Let us consider the concrete definitions of VLAN concepts:

VLAN allows for switches to be configured to define multiple virtual LANs over a single physical LAN infrastructure

Port-based VLAN switch ports grouped (by switch management software) such that a single physical switch operates as multiple virtual switches. The figure below illustrates an example of port-based VLAN using our example from the introduction to VLANs

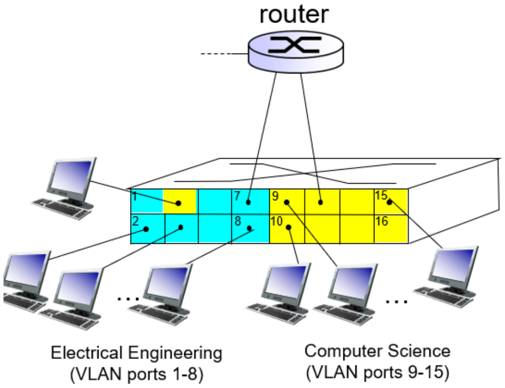


Figure 6: Port-based VLAN analogy put to a figure

Now let us consider port-based VLANs in depth. These allow for *traffic isolation*, meaning ports from a certain group can only reach other ports within that group. It is important to notice that VLAN can also be defined based on MAC addresses of endpoints, rather than switch ports.

Furthermore, port-based VLANs allow *dynamic memberships*, which allows ports to be dynamically assigned among VLANs. In our simple case above, this means a port can shift from the Computer Science group to the Electrical Engineering group dynamically and without issue.

Lastly, port-based VLANs allow *forwarding between VLANs*. This is done via routing, just as is done with separate switches.

Next, we consider VLANs spanning multiple switches. The main concept here is a *trunk port*, which carries frames between VLANs define over multiple physical switches. The frame format for these include a preamble that syncs the clocks for Manchester encoding and much more as shown in *Figure 4*.