ECE 435 – Network Engineering
Lecture 27

Vince Weaver

https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

4 April 2025

Announcements

- HW#9 due today
- We'll have to see if we cover enough for HW#10
- If you're looking for a CE focused tech elective for next year, you can consider ECE531 Advanced OS

Ethernet Frame layout

This is Ethernet II/DIX standard, the most common

```
 ---------- ----- ---- ---- ----- ----------- -----
| Preamble | SFD | DA | SA | T/L |    Data     | FCS |
 ---------- ----- ---- ---- ----- ----------- -----
   7 bytes    1     6    6     2    46-1500      4
```

Frame size is variable. Often first two fields are excluded and said that Ethernet frames are between 64 and 1518 bytes long

Ethernet Frame Preamble

- Fixed 1010...1010 in transmission order (LSB, least significant bit first)
- On original Ethernet this was 10MHz 6.4us pulse used to synch clocks
- PHY might do other things (100BASE-X uses 4B/5B stuff, so different pattern)

Ethernet Start Frame Delimiter (SFD)

- SFD - indicates the start of the frame
- value 10101011 in transmission order
- Original Ethernet declared 8 bytes of same pattern, but on modern first 7 bytes might be different

Ethernet MAC addresses

- DA = 48 bit destination MAC address
- SA = 48 bit source MAC address
  - First 3 bytes the OUI (organization unique identifier)
  - Next 3 bytes supposed to be a unique ID
- Ethernet packets put on the wire least-significant bit first (as if shifted right out of a shift register)
- Multicast if the "first" bit (meaning 0x1, not 0x80) is set in the first octet (e.g. 01-80-C2-00-00-00)
- Broadcast if all bits set ff:ff:ff:ff:ff:ff

Ethernet Type/Length Field

- Originally type field
- 802.3 makes it length of *data* (not length of frame)
- In 1997 802.3 approved as type too, so dual meaning
- How tell difference?
  - Max len 1500, value bigger than 0x600 (1536) is type
  - 0x0800 = IPv4, 0x86dd = IPv6, 0x0806 = ARP
  - How tell length if type? Detect end of signal or inter-frame gap, or valid checksum (this is most common)
  - How tell type if length? Will have 802.2 header?

Ethernet Frame – Data

- Data – data from 46 to 1500 bytes
- Why limit 1500B? because RAM was expensive in 1978.
- If smaller than 46 bytes padded. Makes sure checksum works.
- Also if too short, could be done transmitting before a collision can be detected (light travel to furthest node and back)

Ethernet Frame Check Sequence (FCS)

- FCS – a 32-bit CRC code.
- To avoid problems with all-zeros, bits are complemented when running. These means a ‘good’ result isn’t 0 but 0xc704dd7b
- Somewhat complicated to calculate, a bit beyond this class
  - Hard to get a clear description of what it looks like w/o a lot of math
  - You can implement with linear feedback shift register

(shift register with xors)

  - Possibly CRC calculated MSB first rather than LSB

- If incorrect FCS, silently drops

End of Frame / Inter Packet Gap

- At end of frame, drop carrier
- More modern Ethernet might signal this with a symbol
- Inter-packet gap, 96 bits (12 bytes) of idle before sending next frame
- Gives receiver time to handle frame before next starts

ARP – address resolution protocol

- On local network, how do we find MAC address if we know IP?
- Hard-code mapping `/etc/ethers`?
- Can it be automatically determined somehow?
- ARP – address resolution protocol (IPv4)
- ND – Neighborhood Discovery (IPv6)

ARP (RFC826)

- Device first checks ARP cache to see if already knows
- Otherwise, broadcasts to ff:ff:ff:ff:ff:ff "who has this IP"
- Device reply with its IP and MAC (unicast)
- These are cached
- Timeout in case you reassign
- ARP announcement: can broadcast when your address changes so they can update (gratuitous ARP)
- Other optimizations(?)

ARP Security

- Can you spoof ARP responses to get frames meant for a different device?

IPV6: Neighborhood Discovery Protocol

- Uses ICMPv6 message format
  - Router Solicitation (Type 133) – used to find router for local network
  - Router Advertisement (Type 134) – routers periodically also send their router info to whole local network
  - Neighbor Solicitation (Type 135) – can request MAC address from IPv6 address of neighbors
  - Neighbor Advertisement (Type 136) – response to a

solicitation, or can just send it to everyone if something changed

- Redirect (Type 137)

- To do request, must create two multicast addresses. Less overhead than ARP as in this case only a small number of hosts will share the multicast address
  - solicited-node multicast address least-significant 24 bits of the number looking up and appending to prefix ff02::1:ff00:0/104
  - solicited-node multicast MAC address least-significant 24 bits of the previous solicited-node multicast address

and appending to prefix 33:33:FF:xx:xx:xx

- Secure Neighbor Discovery Protocol (SEND) – uses certificates and stuff to avoid ARP spoofing

RARP/BOOTP

- Some cases need to do RARP (Reverse ARP) (RFC 903) have own MAC, find IP (netbooting is common reason)
- ARP packets not forwarded, so extension called BOOTP that allowed network booting.
- BOOTP automated by DHCP.
- IPv6 has IND (Inverse Neighborhood Discovery Protocol)

Classic Ethernet Transmission (Review)

- Break data into frame
- In half-duplex CSMDA/CD senses carrier. Waits until channel clear
- Wait for an inter-frame-gap (IFG) 96 bit times. Allows time for receiver to finish processing
- Start transmitting frame
- In half-duplex, transmitter should check for collision.
  Co-ax, higher voltage than normal
  For twisted pair, noticing signal on the receive while

transmitting

- If no collision, then done
- If collision detected, a *jam* signal is sent for 32-bits to ensure everyone knows. Pattern is unspecified (can continue w data, or send alternating 1s and 0s)
- Abort the transmission
- Try 16 times. If can't, give up
- Exponential backoff. Randomly choose time from 0 to $2^k - 1$ where k is number of tries (capping at 10). Time slot is 512 bits for 10/100, 4096 for 1Gbs
- Wait the backoff time then retry

Classic Ethernet Receiving (Review)

- Physical layer receives it, recording bits until signal done. Truncated to nearest byte.
- If too short (less than 512 bits) treated as collision
- If destination is not the receiver, drop it
- If frame too long, dropped and error recorded
- If incorrect FCS, dropped and error recorded
- If frame not an integer number of octets dropped and error recorded
- If everything OK, de-capsulated and passed up

- Frame passed up (minus preamble, SFD, and often crc)
- Promiscuous mode?

Maximum Frame Rate

- 7+1 byte preamble 64-byte frame, IFG of 12 bytes between transmissions. equals 672 bits. In 100Mbps system 148,800 frames/second

Ethernet Flow Control

- Flow control is optional
- In half duplex a receiver can transmit a "false carrier" of 1010..10 until it can take more.
- Congested receiver can also force a collision, causing a backoff and resend. Sometimes called force collision
- Above schemes called "back pressure"
- For full duplex can send a PAUSE frame that specifies how much time to wait.

Full Duplex MAC (requires switch)

- Early Ethernet was coaxial in a bus
- Twisted pair has replaced this, usually in a hub/or switch star topology
- 10BASE-T and 100BASE-TX pair for transmit or receive
- inefficient. Since point to point, why do you need arbitration?
- Full-duplex introduced in 1997. Must be able to transmit/receive w/o interference, and be point to point.
- Full duplex effectively doubles how much bandwidth

between. Also it lifts the distance limit imposed by collision detection

Hub vs Switch vs Router

- Hub
  - One collision domain
  - All frames are broadcast to all others
  - Virtual old co-ax wire shared by all
  - Bandwidth is shared (only say 100MB for all)
  - No smarts in hub, mostly electronic connection
- Switch
  - Direct connection provided between source and destination (unless it's a broadcast frame)

- Full-duplex. No collisions
- Each point-to-point connection full bandwidth
- Generally has some sort of microcontroller/embedded system to control the connections

- Router
  - Can be on multiple networks and move frames from one to another
  - Usually moving packets at the network layer, not just link layer
  - Can be confusing as routers can be built into switches

Multi-Speed Hubs

- When 10/100MB first came out, cheap hubs could only run at 10MB or 100MB
- But switches *really* expensive.
- They had a compromise 10/100MB hub that internally had a hub for both then a mini-switch to bridge the gap.

Magnetics

- With long runs of twisted pair cables, can have issues with noise/surging
- Will need some way to isolate signals
- Often use some sort of transformer / BALUN which provide magnetic decoupling
- This can act to block DC or low-frequencies, so higher speed protocols have to be designed with that in mind