ECE 435 – Network Engineering
Lecture 35

Vince Weaver

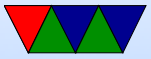
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

24 April 2026

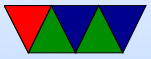
Announcements

- HW#11 due
- Don't forget course reviews (we are at 0% as of yesterday)
- Title II was averted
- Projects next week
- Will grade homeworks. Note I might not grade them in chronological order



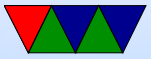
Final Exam Preview

- Final on Monday 4th of May at 8:00am, here (yes, I know)
- Can have one single-side 8.5x11" piece of paper for notes
- Cumulative, but focusing on things after the first midterm
- Know the 7 OSI layers
- Physical layer: know things like the tradeoffs fiber/copper, satellite, fiber
- Link Layer: Ethernet (why it won over token ring),

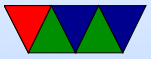


how collision detection works. Wireless ethernet, how collision detection works.

- IPv4 – addresses. traceroute output
- IPv6 – addresses, why necessary
- TCP/UDP – why use one over the other, three-way handshake
- Cellphones, – be aware of these topics but any questions on them will be brief
- Probably no socket programming
- Might show packet dumps, not expect you to memorize all the offsets, will provide the info you need to decode

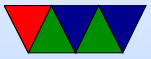


them

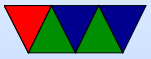


HW#6 Review – TCP Header

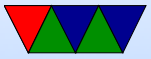
```
0x0022:  bda5 _________ Source port (48549)
0x0024:  0050 _________ Destination port (80)
0x0026:  cdc4 6a49 ____ Sequence Number
0x002a:  3c7b 6ca5 ____ Acknowledgement Number
0x002e:  80 ___________ 0b1000 header length = 8*4=32
0x002f:  18 ___________ 0b11000 ACK+PSH
0x0030:  00e5 _________ Window Size = 229 (likely *128)
0x0032:  79f4 _________ Checksum = 0x79f4
0x0034:  0000 _________ Urgent = ?
0x0036:  01       ____ Option: NOP (padding)
0x0037:  01       ____ Option: NOP (padding)
0x0038:  080a     ____ Option: Timestamp, 10 bytes
0x003a:  0104 3e58 ____ Timstamp TSval
0x003e:  34a8 7bc3 ____ Timestamp TSecr Echo Reply
```



- Header offset/length was the most trouble, top 4 bits of nibble (0x8) multiplied by 32
  can sanity check with size (starts at 0x22 ends 0x42)
- Decode the flags (ACK and PSH)
- Timestamp not necessarily actual times, used for more advanced congestion
- Data is ASCII, handy thing to recognize
- People getting offset, mostly confused by reserved/flags. Count bits. Note things, like checksum is mandatory on TCP so can't be 0.
- It's a web request

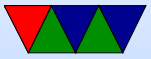


- Size: 0x46 = 70 bytes, 4/70 = 5.7%
  trouble counting bytes vs nybbles
  “useful data” issue this year



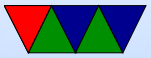
HW#6 Review – TCP Connections

- 3-way handshake SYN/SYN+ACK/ACK
  note also other things in packet, windowscale, sackOK (selective), TS, val, ecr (timestamp: value, echo-reply)
- Sends hi / ack / sends back HI / ack.
  Note PSH sent so that it doesn't wait and piggyback
  Why is PSH sent? Most(?) TCP stacks when you do a write() will set PSH on the last packet containing data from the write.
- Closing connection. FIN/ACK+FIN/ACK



HW#6 Review – Noticing Congestion

- Timeout
- Multiple duplicate ACKs
- Note: not multiple timeouts
- ECN can notice congestion, but in this case it happens before packets start getting lost (otherwise you'd never get the packets with the ECN info)



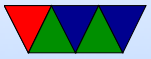
HW#6 Review – Security

- Network connections: Should you worry?
  - CLOSE-WAIT: received a FIN and ACKed it, waiting to close

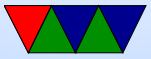
    Only a few, https and imap
  - ESTAB: established, a few ssh, https, imap connections
  - SYN-RECV: way too many, SYN flood

    Could a lot of legitimate ssh connections cause this?

    Unlikely. Have to stop handshake mid-way Why attack

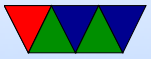


ssh? Have to try a socket someone is listening on
  - TIME-WAIT: connection closed, waiting a bit before re-using port
  - UNCONN – UDP listening. 789? ipp, mdns (multi-cast DNS, bonjour, can find names on network w/o running DNS), `lsof -i udp:789`, rpcbind
  - LISTEN – listening. Can see ipp (CUPS printing), netbios/microsoft, apparently have SAMBA running,
- Synflood, by default Linux uses SYN cookies to defend against this



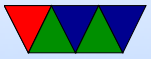
HW#7 Review – IPv4 Header

```
0x000e:  4500 = version(4), header length(5)=20 bytes
                ToS=0
0x0010:  0038 = packet length (56 bytes)
0x0012:  572a = identifier
0x0014:  4000 = fragment 0100 0000 0000 0000 =
                do not fragment, offset 0
0x0016:  40 =   TTL = 64 hops
0x0017:  06 =   Upper layer protocol (6=TCP)
0x0018:  69cc = checksum
0x001a:  c0a80833 = source IP 192.168.8.51
0x001e:  826f2e7f = dest IP 130.111.46.127
```



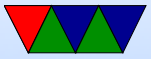
HW#7 Review – IPv4 Addresses

- Valid IPs
  - 1.1.1.1 = Y
  - 123.267.67.44 = N
  - 192.168.8.1 = Y
  - 3232237569 = 192.168.8.1 = Y
  - 0xc0a80801 = 192.168.8.1 = Y
- A class-A allocation is roughly $2^{24}/2^{32}$ which is 0.39%



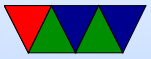
HW#7 Review – Subnetting

- 192.168.13.0/24. subnet 255.255.255.0, lowest ip 192.168.13.1, highest 192.168.13.254 (traditionally can't use the host values with all 0 or 1s (so .0 and .255 on a /24). There's a push to allow .0 on Linux
- First hop not local (how to tell?) goes to router Otherwise go direct (can you go direct? how).



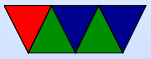
HW#7 Review – IPv4 ping/traceroute

- Ping google. 1e100.net?
- Traceroute. Some routers block?
  Used to pass through Neville hall
- Interesting, people tracerouting umaine from spectrum have packets going via chicago and boston bngrme/sebgme/rochny/chgil



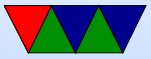
HW#7 Review – NAT

- No 192.168.8.x should not be able to connect to outside directly.
- NAT is happening.
- Why is nat showing UNREPLIED? TCP vs UDP difference. Can you detect when TCP connection is closed? Yes. Can you detect when UDP connection is done? No. Must keep port open a bit in case reply. How long. Forever? What goes wrong with that?



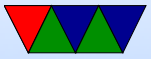
Some Last Notes on HW#7

- People seeing Apogee Telecom in their traceroutes; I hadn't realized campus had outsourced the internet in the dorms
- If you have Spectrum it's possible all your packets to campus go via Chicago
- Note TTL is in hops, not seconds



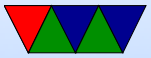
HW#8 Review – IPv6 Addresses

- 2607:f8b0:4009:0801:0000:0000:0000:200e – OK
- 2607:f8b0:4009:801::200e – OK
- 2607:f8b0::4009:801::200e – can you have two colons?
- 123.45.67.18 – ipv4



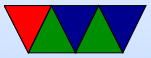
HW#8 Review – IPv6 Packet

```
0x000e:  6002 2618 :
 6 = IPv6
 00 = traffic class
 2618 = flow label
0x0012:  0031 =       payload length, 49
0x0014:  11 =         next header = 0x11, UDP
0x0015:  40 =         hop limit 0x40, 64
0x0016:  2610 0048 0100 08da 0230 18ff feab 1c39
                      source address
0x0026:  2001 4860 4860 0000 0000 0000 0000 8844
                      destination address
```



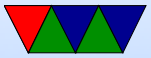
HW#8 Review – Traceroute

- internet2
- bost/hart/newy probably boston, hartford, new york
- lon2.uk London
- janet is british academic network
- 6→7 across ocean
- 80ms = ?? speed of light
- 80e-3s 3e8m/s = 24000km? 5500km = 1/4 speed of light?



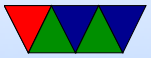
HW#8 Review – Traceroute6

- different hops? IP6 different? random chance
- hop 5→6
- Washington? internet 2?
- Abilene was the predecessor to internet2
- fra.de Frankfurt Germany probably not France
  ams.nl probably Amsterdam in Netherlands
- latency 133ms rather than 106ms



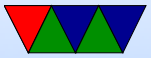
HW#8 Review – Anycast / Multicast

- Anycast: things where can load balance local. DNS. Google / facebook. CDNs
- Multicast: less load on server to just send one packet, instead of millions. Also better for bandwidth/congestion



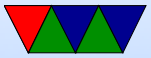
Homework #9 Review – Bandwitdh

- NOTE: be sure you use the proper log (base 10 or base 2) and not the natural log (ln)
- S/N is 25. db=10 log S/N, roughly 14dB
- 100MHz, 20dB bps = Hlog 2 (1 + S/N)
  S/N = 100, bps = 100M*log2(1+100) = 666Mbps

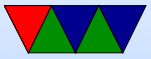


Homework #9 Review – Tradeoffs

- Fiber vs copper
  - Speed? This varies,
  - Electrons in copper 50-90% of speed of light, Light in fiber 70-90%
  - This is why microwaves used for high-speed trading
- Satellite vs fiber:
  - no need to run cables everywhere
  - Can broadcast over greater area
- Fiber vs satellite:

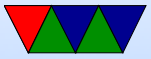


- security (harder to tap?)
- latency
- Cost? Which is more expensive?
- faster?



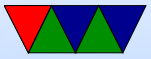
Homework #9 Review – Frequency use

- FCC won't let me be
- Though they only regulate consumer, federal govt (like military, FAA, etc, NTIA National Telecommunications and Information Administration) 4.3GHz airport/radio navigation
- FCC database lists numerous companies, but they don't own freq, just have license to make radio altimeters
- 100W sounds like a lot, but as long as you're not holding it in your hands not really that large for a transmitter.



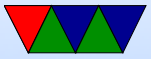
HAM radios, 100W light bulbs.

- This is in the C-band, but C-band as a whole is not reserved, it's just a descriptive name for it.



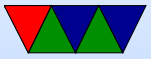
HW#10 Review – Ethernet Frame

- Ethernet header: MAC/MAC/IPv4
  - MAC addresses dest/src. 00:11:22:33:44:55 (they don't look like IP addresses)
  - Note not size, as it's 2048 and size must be smaller than 1500
    0x800 means IPv4
- OUI: Speed Dragon – cheap 2nd Ethernet card in my gateway / Pi Foundation
- MAC address is that of router. Routers strip off Ethernet



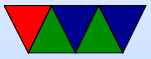
header, maybe add another if outgoing on other network is also Ethernet.

Note: switches and hubs don't have MAC addresses or at least you shouldn't be able to see them.



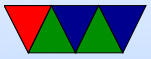
HW#10 Review – ARP

- ARP / maps IP addresses (or other) to MAC.
- Given IP, what's MAC. Not MAC, what's IP (that's reverse-ARP and rarely needed)
- Note ARP is ipv4 only, use neighbor discovery protocol for IPv6

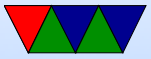


HW#10 Review – Ethernet vs Token Ring

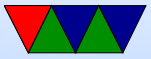
- Ethernet was simpler and cheaper than token ring
  - Cheaper is relative, high-end Ethernet card in 1987 was $800 ($2300 inflation adjusted 2025)
    low-end $400 ($1100 2025)
  - Token ring would have been more
  - By the time I first had one, 1996 or so, more like $50 ($100 today)
- Simplicity
  - Famous Linux rants by Donald Becker who wrote early



Ethernet cards, against 3c501 (only had RAM for one frame, so if trying to set up for send and one came in, would have to drop)
  - Part of this is people using 1980s designs still in 1990s
  - Lots of rants against ubiquitous NE2000 cards
  - Some later analysis shows part of the problem might have been poor code in Linux drivers
- Bandwidth, maybe, depends on year. token ring was 4/16MBps while Ethernet was 10/100MBps. Different behavior under load
- efficient? You'll have to explain that

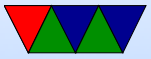


- Twisted pair? While twisted pair is cheaper, Ethernet was co-ax at the time (and even token ring got twisted-pair eventually)



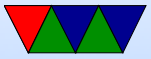
HW#10 Review – Other Ethernet Questions

- 64 bytes ensured a collision could happen
- Maximum size of 1500 was due to cost of RAM, but also the larger it is the more likely an error can happen. Also related to RAM on Alto I think Fragmentation?
- Ethernet drops things on floor if error



HW#10 Review – Investigation

- Collision count low? Most likely you're connected to a switch (full duplex) so there aren't any collisions.
  - Low traffic or low packet size could also help, but that wasn't necessarily the case here
  - Running in a VM can also have no collisions as in theory your OS is faking up an Ethernet card
- Way to tell if switch is notice full-duplex. In theory gigabit usually (but not always) will imply a switch as well



Sample Project Presentation

Applesoft BASIC Webserver on 8-bit Apple II

Posted to the website as we ran out of time due to the fire alarm.