ECE 435 – Network Engineering
Lecture 23

Vince Weaver

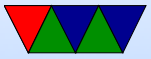
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

14 April 2022

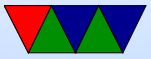
Announcements

- HW#10 will be posted
- HW#9 is due Friday
- Project Status is due Friday
- Security faculty interviews Friday/Monday/Wednesday (note this means office hours rescheduled Monday/Wednesday)



Homework #8 Review

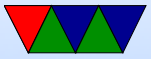
- Questions
  1. Bandwidth
  (a) S/N is 25. db=10 log S/N, roughly 14dB
  (b) 100MHz, 17dB, Shannon? bps = Hlog 2 (1 + S/N)
  S/N = 50, bps = 100M*log2(1+50) = 567Mbps
  2. Tradeoffs
  (a) Fiber over copper
  Speed? This varies, Electrons in copper 50-90% of speed of light, Light in fiber 70-90%



(b) Satellite over fiber:
no need to run cables everywhere
Can broadcast over greater area

(c) Fiber over satellite:
less secure (easier to tap)
longer latency
Cost? Which is more expensive?
faster?

3. FCC won't let me be
Though they only regulate consumer, federal govt (like military, FAA, etc, NTIA National Telecommunications

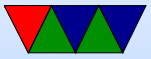


and Information Administration) 4.3GHz airport/radio navigation

FCC database lists numerous companies, but they don't own freq, just have license to make radio altimeters

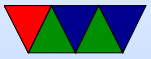
100W sounds like a lot, but as long as you're not holding it in your hands not really that large for a transmitter. HAM radios, 100W light bulbs.

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

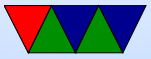


Encryption Issues (from last time)

- News from last year, security issues with WiFI:
- KRACK attack (key reinstallation attack)
  - 4-way WPA2 handshake
  - You can resend 3rd way of handshake with the key, and other side will accept it (in case it was lost) and re-start encryption from beginning
  - This leads to same key being used to encrypt multiple frames
  - That makes reversing the key trivial

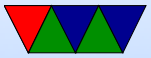


- Frag attack
  - `https://lwn.net/Articles/856044/`
  - (fragmentation bit is outside of the encrypted/protected, so by messing with that you can get rogue chunks of encrypted data inserted into frames)

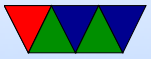


Transmission Power

- 802.11b signal typically around 32mW
- Often use dBmW (often shorted dBm) where 0dBm=1mW
- 1dBm = 0.001258925W
- -50dBm to -60dBm normal signtal strength to receive, -67dBm borderline
- Convert -68 dBm to Watts
  - $P = (1W * 10^{P_{dBm}/10})/1000$
  - -68 dBm = 160pW

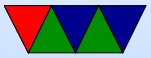


- Convert 1W to dBm
  - $P_{dBm} = 10 * log_{10}(1000 * P_W/1W)$
  - 1W $=$ 30dBm
- Juno space probe (13 Oct 2016)
  - 8.4GHz, received -135.75dBm (2.7e-17W) 18kb/s



Channels

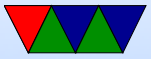
- 802.11b, DSSS 2.4GHz, 2412MHz as first channel, 14 channels 5MHz apart 1-14.
- 802.11g same as 802.11b when talking to b, but a modes when talking to other g
- 802.11a 5GHz band, channels 1-199 starting at 5005MHz 5MHz apart
- CMSA/CA – uses RTS/CTS. 802.11g needs to do this if 802.11b present, slowing things down 20-50%



Linux Interface

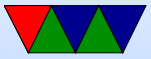
- iwconfig
- iwlist scanning

```
wlan0     IEEE 802.11abg  ESSID:"Whatever"
          Mode:Managed  Frequency:2.452 GHz
                        Access Point: 00:1C:10:11:B4:C6
          Bit Rate=54 Mb/s   Tx-Power=200 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:XXXXX
          Power Management:off
          Link Quality=42/70  Signal level=-68 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

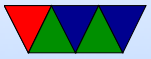


Bridging

- How do you connect together multiple groups of machines into one big LAN?
- An interconnection at the link layer is called a MAC bridge, or bridge. Also a Layer-2 switch
- IEEE 802.1D
- Transparent bridge, as users are not aware of them
- Bridge acts in promiscuous mode (receives every frame

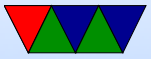


on the LAN) so it can find ones that need to forward on across the bridge



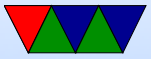
Backward/Self Learning

- How does bridge learn the MAC addresses?
- It watches for frames coming in and their source address. Puts in table.
- How does it learn where destination is? It broadcasts to all. Once the destination also sends a frame (so its source is known) then the switch updates its table and no longer broadcasts.
- How do you handle machines that are moved? Aging



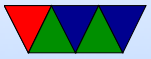
mechanism. If not heard from for a while, expire the table

- Multicast or Broadcast, can follow GMRP or GARP to limit how far it is broadcast



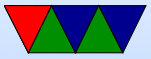
Bridge vs Switch

- Before 1991 a switch was a bridge (in the standard)
- In 1991 Kalpana made a "switch" and differentiated it by cut-through instead of store and forward
- Store and forward – whole frame received before resent larger latency, no problem with broadcast, can check FCS
- cut-through – can start transmitting before receiving completely (destination MAC at beginning). Slightly



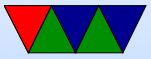
better latency, broadcast not possible, too late to check FCS

- These day most are store and forward



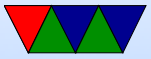
Terminology

- repeater – purely electronic, resends voltages (original Ethernet allowed four)
- hubs – frames coming in one port sent to all others
  creates a collision domain
- bridge – connects two or more LAs. Each line own collision domain
  can maybe bridge different types of networks (Ethernet/token, wired/wireless)
- switch – point-to-point frame routing, sort of like one



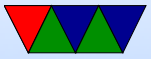
bridge per port

- router – higher layer, actually strips off headers and looks at packets



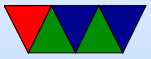
Switch Implementation

- Can implement in software with an OS like Linux
- Multiple ethernet cards
- Use operating system bridge support to bridge the interfaces together



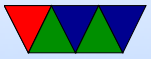
Spanning Tree Protocol

- Invented by Radia Perlman at DEC
- Can have problems if cause a loop in the topology. Frames can circulate loop forever
- Why have a loop then? Redundancy.

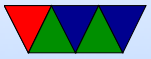


Spanning Tree Protocol – 802.1D

- Each switch and port assigned an ID with priority
- Each link assigned a cost, inversely proportional to link speed
- The lowest ID gets to act as root (there is a protocol on how to elect the root)
- Each LAN connected to upstream port in active topology, called the dedicated port. Receives from root port
- Config info comes from root as bridge protocol data unit (BPDU) on reserved multicast address 01:80:c2:00:00:00

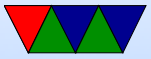


- Switch may configure itself based on BPDU.
- Can take 30-50s to notice failure



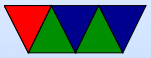
Rapid Spanning Tree Protocol – 802.1w

- Modern replacement
- Can detect failure in milliseconds



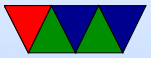
Bridging 802.11 to 802.3

- Need to strip off one header, put new one on
- Need to put fields in as needed, recalc checksum, etc
- What if bridging faster net to slower one
- What if maximum frame size different on different LANs? Can't always fragment
- What if one has encryption and one doesn't
- What of quality of service?

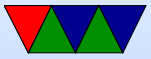


Why might you want to split up LANs

- Bandwidth concerns
- Different groups, privacy/security
- Equipment costs
- Distance
- Reliability (equipment failure)
- Security (someone in promisc mode not see everything)

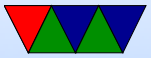


- Load – two groups, one not happy if other group takes up all bandwidth
- Broadcasting – when asks for a connection, broadcasts to all broadcast storms – entire LAN brought down with all machines broadcasting



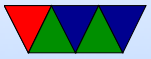
VLAN

- How to switch machines between networks? Request? Someone in wiring closet?
- Physical LAN
- What if want to partition a switch so some nodes are on one and one on another (virtual LANs)



802.1Q

- IEEE 802.1Q
- can have priority
- link aggregation, combine two links for higher bandwidth
- how to bridge VLANs?
  - special VLAN field in Ethernet frame
  - priority, CDI (makes connectionless interface have some manner of connection)



- Changes Ethernet frame, but only between bridges. Endpoints don't see modified frames