ECE 435 – Network Engineering
Lecture 32

Vince Weaver

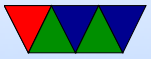
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

16 April 2025

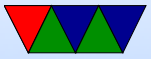
Announcements

- HW#10 was graded
- HW#11 will be posted
- Don't forget status updates
- TODO: Look up DECT-2020 NR+ protocol 1.9GHz? Possible bluetooth competitor?



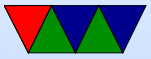
HW#10 Review – Ethernet Frame

- 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



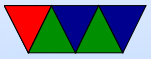
header, maybe add another if outgoing on other network is also Ethernet.

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



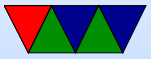
HW#10 Review – ARP

- 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

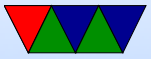
- Ethernet was simpler and cheaper than token ring
  - Cheaper is relative, high-end Ethernet card in 1987 was $800 ($2300 inflation adjusted 2025)
    low-end $400 ($1100 2025)
  - Token ring would have been more
  - By the time I first had one, 1996 or so, more like $50 ($100 today)
- Simplicity
 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



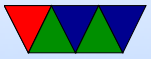
Ethernet cards, against 3c501 (only had RAM for one frame, so if trying to set up for send and one came in, would have to drop)

  - 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

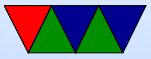


- Twisted pair? While twisted pair is cheaper, Ethernet was co-ax at the time (and even token ring got twisted-pair eventually)



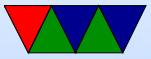
HW#10 Review – Other Ethernet Questions

- 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



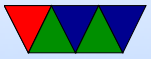
HW#10 Review – Investigation

- 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



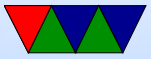
Bluetooth

- Personal Area Network (PAN)
- Short-range wireless, replace need for cables
- Power limited, often 2.5mW for range of 10m (33 feet)
- In 2.4GHz ISM band



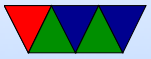
Bluetooth Applications

- Headsets
- Wireless controllers (Wii, PS3)
- Wireless keyboards, mice
- Earbuds
- Cell phone, file transfers

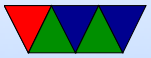


Bluetooth

- Late80s/Early90s Ericsson. With IBM, Intel, Nokia and Toshiba formed a SIG.
- Named after Harald Blaatand (Bluetooth II (940-981) a Viking king who "united" (conquered) Denmark and Norway. Unite various standards.
- Symbol is runes for HB.
- Get rid of cables, specifically serial cables
- Interferes with 802.11
- IEEE came in an decided to take standard and make it

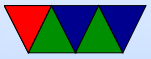


802.15.1 but no longer maintains it



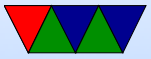
Bluetooth Architecture

- Basic unit: piconet, controller node and up to seven *active* device nodes within 10m
- Many can exist in an area, and can be connected by a bridge. Connected piconets are called a scatternet
- There can also be up to 255 “parked” nodes in a picnoet
- When parked, can only respond to activation on beacon
- Hold and siff?
- Devices designed to be cheap, so dumb. Controller is smart and runs them. device/device communication not



possible

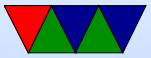
- Controller broadcasts clock 312.5us. Controller transmits in even, device in odd.



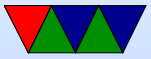
Bluetooth Applications – Profiles

Bluetooth V1.1 has 13 different application protocols.

- Required
  - generic access – link management
  - service discovery – discovering services
- Serial port
  - Object exchange
- Networking
  - LAN access
  - Dial-up

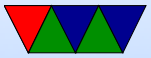


  - Fax
- Telephony
  - Cordless phone
  - Intercom
  - Headset
- File exchange
  - Object push
  - File transfer
  - Synchronization

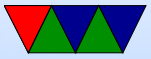


Bluetooth Radio Layer

- 2.4GHz, 10 meters. 79 channels of 1MHz.
- Frequency shift keying, 1 Mbps but consumed by overhead
- Frequency hopping spread spectrum, 1600 hops/sec dwell of 625 usec. All nodes in piconet hop at once, with controller controlling this (PRNG) 1,3, or 5 slots/packet
- Interferes with 802.11. Bluetooth hops faster so causes more trouble.
- power output class: 100mW class 1, 2.5mW class 2,

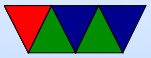


1mW class 3.



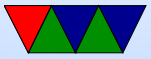
Bluetooth Baseband Layer

- Asynchronous Connection-less link (ACL) packet-switch data at irregular info, no guarantees. one per slice
- Synchronous Connection Oriented (SCO) – for real time data.
- Three per device. Error correction. Each can send 64kpbs PCM audio



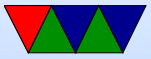
L2CAP layer

- accept packets of 64kB and break into frames.
- Handles multiplexing.



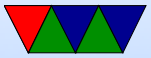
Bluetooth Frames

- Several different formats
- 72 bits access (identify controller, as can be in range of multiple)
- 54 bit header
  - (addr(3) frame type(4), flow [buffer full](1), Ack (1) seq(1) checksum(8)
  - This is repeated 3 times.
  - Majority wins (redundancy, cheap small protocol)
- Data 0-2744 bits. SCO always 240 bits.



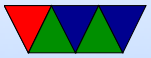
Bluetooth 1.1 (2002)

- First stable version
- Basic Rate (BR)
- Gaussian Freq-shift Keying (GFSK). Smooths signal instead of abrupt 1/0 transition
- 1Mbps peak in theory



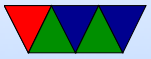
Bluetooth 1.2

- Adaptive frequency hopping, skip busy frequencies
- Up to 721kbps
- eSCO allow retransmitting corrupted packets, at expense of audio latency
- HCI host controller interface, three wire



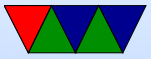
Bluetooth 2.0 (2004)

- 2.0
  - EDR = Enhanced Data Rate
  - BR/EDR 2 and 3Mbps
  - Pi/4 DQPSK – differential quadrature phase-shift keying
- 2.1
  - Secure simple pairing
  - Extended inquiry response



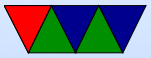
Bluetooth 3.0 (2009)

- Up to 25Mbps "HS" (high speed)
- Alternative MAC, bluetooth set up connection but 802.11 used to transmit data?



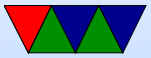
Bluetooth 4.0 (2010)

- Splits things in three, Classic, High-speed (wifi related), and the new Bluetooth Low Energy (BLE)
- BLE
  - Entirely new stack, designed for low power rapid setup links
  - 40 2MHz channels, 1Mbit/s
  - Max power 10mW
  - Not backwards compatible, but same frequency range
  - New profiles



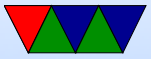
Bluetooth 5 (2017)

- Internet of things
- Can get 2MBit/s with shorter range, longer 240m at slower speed
- 5.1 (2019) various things including angle of arrival
- 5.2 (2019) – Low Energy Audio
- 5.3 (2021) – alt mac removed
- 5.4 (2023)



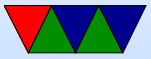
Bluetooth 6.0 (202?)

-



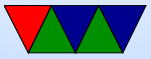
Setting up Connections

- In discoverable mode, will transmit name, class, services, etc on demand
- Has unique 48 bit number but that's rarely seen

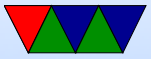


Bonding / Pairing

- To avoid people stealing info from your device, require some sort of user interaction to connect for the first time.
- Before 2.1 (Legacy) it was a 16-byte pin code
  - Some just fixed value, 1234
  - Some have you enter number
- Secure simple pairing, pub key crypto
  - “Just Works” – can prompt
  - Numeric compare, see if same on both, click OK

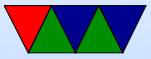


- Passkey – shows 6 digit number, enter on other
- Out of Band – QR, NFC, or some other way



Security

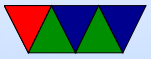
- Prior to 2.1 security can be turned off, and only good for 23.5 hours
- Exploits
  - "Bluejacking" – people walk around sending unwanted pictures/text to unsecured devices
  - Lots of issues over the years do to pairing
  - With proper antenna can attack from afar (1 mile away?)



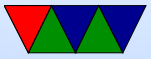
Linux Bluetooth

- Competing implementations (bluez, Affix)
- Install bluez
- bluetoothctl

```
[NEW] Controller B8:27:EB:05:9D:BB pi3 [default]
[bluetooth]# exit
[DEL] Controller B8:27:EB:05:9D:BB pi3 [default]
root@pi3:/home/vince# bluetoothctl
[NEW] Controller B8:27:EB:05:9D:BB pi3 [default]
[bluetooth]# scan on
Discovery started
[CHG] Controller B8:27:EB:05:9D:BB Discovering: yes
[bluetooth]# power on
```



```
Changing power on succeeded
[bluetooth]# scan on
Failed to start discovery: org.bluez.Error.InProgress
[bluetooth]# scan on
Failed to start discovery: org.bluez.Error.InProgress
[NEW] Device 64:8A:44:9D:DC:FD 64-8A-44-9D-DC-FD
[NEW] Device D3:E8:9D:CA:71:63 D3-E8-9D-CA-71-63
[CHG] Device D3:E8:9D:CA:71:63 RSSI: -89
```



Linux Bluetooth Investigation

- Can use tcpdump on it