ECE 435 – Network Engineering
Lecture 9

Vince Weaver

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

vincent.weaver@maine.edu

28 September 2016

Announcements

- HW#3 was due
- HW#4 posted?
- Note, midterm next Wednesday! Shortened class on Monday.

Bluetooth Applications

- Headsets
- Wireless controllers (Wii, PS3)

Bluetooth

- 1994 Ericsson. With IBM, Intel, Nokia and Toshiba formed a SIG.
- Named after Harald Blaatand (Bluetooth II (940-981) a Viking kind who “united” (conquered) Denmark and Norway. Unite various standards.
- 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, master node and up to seven *active* slave 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?

- Slaves designed to be cheap, so dumb. Master is smart and runs them. slave/slave communication not possible

- Master broadcasts clock 312.5us. Master transmits in even, slave 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 Layering

- 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 master controlling this

  Interferes with 802.11. Bluetooth hops faster so causes more trouble.

  power output class: 100mW class 1, 2.5mW class 2, 1mW class 3.

- 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 slave. 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 master, as can be in range of multiple)

- 54 bit header (addr(3) frame type(4), flow [buffer full](1), Ack (1) seq(1) checksum. 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

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)

- BR/EDR 2 and 3Mbps

Bluetooth 3.0 (2009)

- 25Mbps
- Alternative MAC, bluetooth set up connection but 802.11 used to transmit data?

Bluetooth 4.0 (Bluetooth Low Energy) (2010)

- 25Mbps/200 feet
- Entirely new stack, designed for low power rapid setup links
- Not backwards compatible, but same frequency range
- New profiles

Bluetooth 5.0 (2017)

- Internet of things
- 50Mbps/800 feet

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 it was a 16-byte pin code

Security

- Prior to 2.1 security can be turned off, and only good for 23.5 hours

Linux Bluetooth

- Competing implementations
- 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:
[bluetooth]# power on
Changing power on succeeded
[bluetooth]# scan on
Failed to start discovery: org.bluez.Error.InPr
[bluetooth]# scan on
Failed to start discovery: org.bluez.Error.InPr
```

```
[NEW] Device 64:8A:44:9D:DC:FD 64-8A-44-9D-DC-F
[NEW] Device D3:E8:9D:CA:71:63 D3-E8-9D-CA-71-6
[CHG] Device D3:E8:9D:CA:71:63 RSSI: -89
```

WiMax

- 802.16
- Worldwide Interoperability for Microwave Access
- Fixed or mobile. Originally designed for “last mile” setup, but used as 4G phone (mobile wi-max)
- Distance of miles
- Base station allocates a time slot, good for VOIP and QoS

- Licenses spectrum from 2-11GHz and 10GHz-66GHz High frequency has more bandwidth, but blocked by obstacles
- can run in mesh mode where nodes can act as relays
- OFDM and OFDMA

WiMax mobile

- 802.16e-2005
- handoffs and roaming up to 75MHz
- Lower freq, 2.3 - 2.5Ghz
- up to 75Mbps, can cover 30 mile radius
- soft and hard handoff

WiMax Scheduling

- Unsolicited Grant Service (UGS) – voip w/o silence suppression
- Real-time Polling Service (rtPS) – video, voip w silence suppression
- Non-real-time Polling (nrtPS) – web browsing
- Best Effort (BE) – e-mail, message based
- Extended Real-Time Polling (ertPS) – video, voip w silence suppression

LtE

- Only real 4G is LTE advanced and mobile WiMaX advanced

Why might you want to split up LANs

- Bandwidth concerns
- Different groups, privacy/security
- Equipment costs
- Distance
- Reliability (equipment failure)

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

- How does bridge learn the MAC addresses? self-learning. 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
- Differences
  - 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

- switch –
- router – actually strips off headers and looks at packets

Spanning Tree Protocol

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

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?

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)
- IEEE 802.1Q
- can have priority

- link aggregation, combine two links for higher bandwidth

- why split up?
  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

- how to bridge VLANs? special VLAN field in Ethernet frame

priority, CDI (makes connectionless interface have some manner of connection)