ECE 435 – Network Engineering
Lecture 8

Vince Weaver

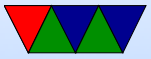
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

26 September 2016

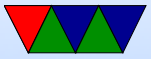
Announcements

- HW#3 was posted
- note – the warnings you were getting on toupper() was because you need to include ctype.h
- tempest – was NSA standards for keeping from being wirelessly spied on



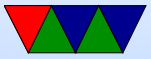
Wireless Frames

- Diagram?
- Frame format frame Control (2) Duration/ID (2) Addr1 (6) Addr2 (6) Addr3 (6) Sequence control(2) Address4 (6) Frame body (0-2312) FCS (4)
- Control: Version (2) Type (2) [data, ctonrol, management], subtype(4) [rts,cts],ToDS/FromDS(1,1), MF (1) more fragments to follow, Retry(1)



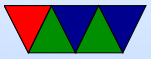
powermanagement(1), More(1) [more coming], W(1) WEP [encryption], O(1) frames must be in-order

- Duration says how long will occupy channel
- Addresses source, destination transmitter address , receiver addr. Last two optional, usually if bridge.
- Sequence: 12 for frame, 4 for fragment
- Up to 2312 byte of Data
- Checksum

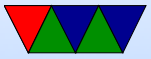


802.11 – Why not just Ethernet over the Air

- Hidden station/terminal problem A in range of B, B in range of C, but A cannot see C. If A and C transmit at same time, they'll not get collision, only way of knowing is if not get ACK.
- Exposed station problem. A and C not overlap, but B does not know this so holds out
- To deal with this, Distributed Coordination Function

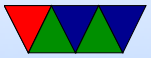


(DCF) and point coordination function (PCF)

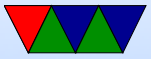


DCF – Distributed Coordination Function

- Basic DCF
  - No central control
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Different from Ethernet CSMA/CD.
  - Every time ready to transmit, looks to see if can transmit (listen to see if channel clear)
  - If clear, waits DIFS (inter frame) time and transmits
  - If busy, waits until clear and then also a random backoff

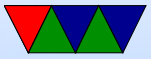


time before starting
  - There is a short inter-frame interval (SIFS) which gives time for receiver to transmit an ACK packet.
  - If source does not get an ACK, then it backs off and retries
- Optional RTS/CTS mode
  - Before sending data, sends short RTS (request to send) packet
  - Receiver responds with short CTS (clear to send)
  - Data only sent if CTS sent properly
  - All stations can see both CTS *and* RTS, this and



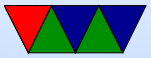
hopefully avoids collisions.

- There's a duration field too to hint how long it will take



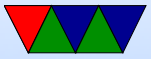
Wireless Networks

- Ad-hoc mode – peer to peer
- Infrastructure mode – many to access point (AP) which has a wired connection
- In infrastructure mode all access goes through the AP



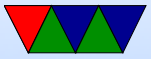
Service Sets

- A basic service set (BSS) is a group of nodes that all recognize each other
- An extended service set (ESS) is a group of overlapping BSSes with APs that are connected together
- An AP keeps the BSSes in line by periodically transmitting beacon frames



PCF – Point Coordination Function

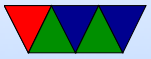
- PCF provides central control. A point coordinator in the AP periodically transmits a beacon to announce a contention-free period (CFP). Stations keep quiet.
- Sort of like time-division multiplexing
- For power saving, base station can tell receiver to go to sleep, and buffer packets for it until wakes up
- Can combine PCF and DCF in same cell.



Wireless Services

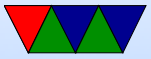
Must provide 9 services

- intracell for dealing with things outside of a cell
  - Association – allow stations to connect to base stations. When arriving announce its identity and capability
  - Disassociation – either side may break the association, should do it before shutting down
  - Reassociation – can change preferred base station, useful for handover (but best-effort)



- Distribution – determines best way to route frames
- Integration – in case frame needs to be sent through a non-802.11 network

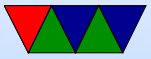
- Intercell
  - Authentication – check password
  - Deauthentication – to leave network
  - Privacy – encryption
  - Data delivery – modeled on Ethernet, no guarantees frames will get in



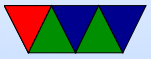
Encryption

- WEP – Wired Equivalent Privacy
  Used RC4 and CRC32
  Deprecated 2004
  Meant to be 64 bit, originally 40 but due to export limitations
  Later 128-bit. Can enter in hex or ASCII chars
  Can be cracked fairly quickly these days

- WPA – Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) 64 or 128 bit encryption key

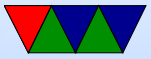


- WPA2



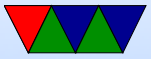
Authenticated

- Three states: not authenticated, authenticated but not associated, authenticated and associated
- device sends probe requests. Advertise data rates and what version of 802.11 supported. BSSID of ff:ff:ff:ff:ff:ff so all access points that hear it will respond
- if an access point (AP) supports a common data rate, it will respond with SSID, data rate, encryption mode, etc
- device chooses an access point and authenticates.

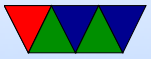


Originally this would have been WEP, but deprecated so often happens in open and usually succeeds. Device sends a 802.11 open authentication frame, seq 0x01

- AP responds saying open with seq 0x02
- if AP receives frames other than auth or probe from device, responds with a deauth to make it start over
- A device can be authenticated to multiple APs but only associated with one
- device determines who to associate with and requests



- AP responds and creates association ID
- once associated then WPA/WPA2 has to happen still before data can flow

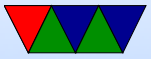


More

- 802.11b signal typically around 32mW
  Often use dBmW where 0dBm=1mW
  1dBm = 0.001258925W
  $P = 1W * 10^{P_{dBm}/10}/1000$ 200??? -68 dBm = 160pW
  $P_{dBm} = 10 * log_{10}(1000 * P_W/1W)$

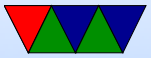
- 802.11b, DSSS 2.4GHz, 2412MHz as first channel, 14 channels 5MHz apart 1-14.

- 802.11g same as 802.11b when talking to b, but a modes



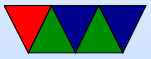
when talking to other g

- 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%



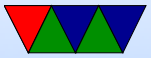
Linux Interface

```
wlan0     IEEE 802.11abg  ESSID:"Whatever"
          Mode:Managed  Frequency:2.452 GHz  Acce
          Bit Rate=54 Mb/s   Tx-Power=200 dBm
          Retry short limit:7   RTS thr:off   Fra
          Encryption key:XXXXX
          Power Management:off
          Link Quality=42/70  Signal level=-68 dB
          Rx invalid nwid:0  Rx invalid crypt:0
          Tx excessive retries:0  Invalid misc:0
```



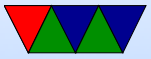
Bluetooth Applications

- Headsets
- Wireless controllers (Wii, PS3)

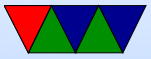


Bluetooth

- 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

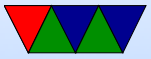


- IEEE came in an decided to take standard and make it 802.15.1 but no longer maintains it



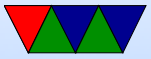
Bluetooth Architecture

- 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

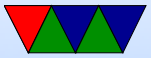
- Master broadcasts clock 312.5us. Master transmits in even, slave in odd.



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