ECE 435 – Network Engineering
Lecture 31

Vince Weaver

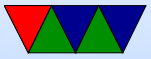
https://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

15 April 2026

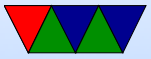
Announcements

- HW#10 due Friday
- Project status reports due Friday (17th)
- 6GHz band being clawed back? https://arstechnica.com/tech-policy/2025/07/trump-and-congress-finalize-law-that-could-hurt-your-wi-fi/
- What's the deal with modern wifi antennas



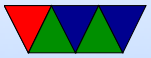
Terminology

- Station = device on wireless network
- Access Point (AP)



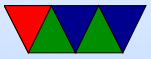
Wireless Network Topology

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



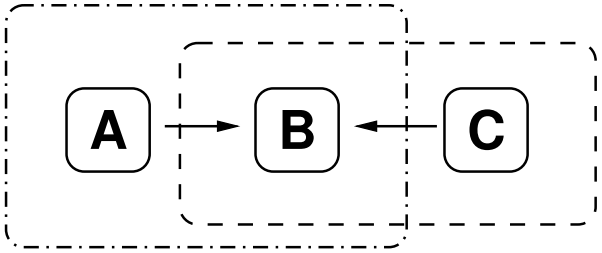
Service Sets

- 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

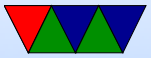


802.11 – Why not just Ethernet over the Air

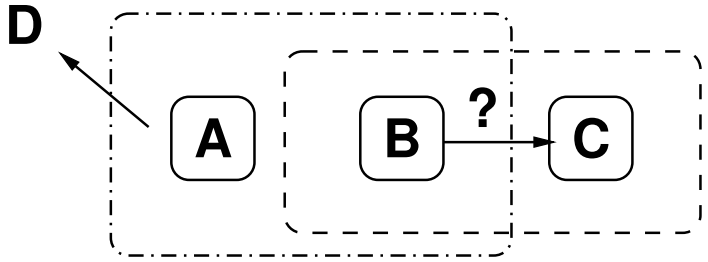
- Hidden station/terminal problem A in range of B, B in range of C, but A cannot see C. If A and C transmit at same time, they'll not get collision, only way of knowing is if not get ACK.



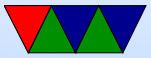
- Exposed station problem. A and C not overlap, but B



does not know this so it sees A transmitted to D and doesn't transmit to B even though it wouldn't cause collision.

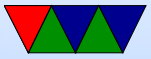


- To deal with this, Distributed Coordination Function (DCF) and point coordination function (PCF)



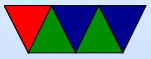
First some Timing Notes

- Network Allocation Vector (NAV), send along estimated time for how long things will take, other stations see this
- Interframe Spacing, 4 types
  - Short (SIFS)
  - PCF (PIFS)
  - DCF (DIFS)
  - EIFS



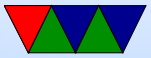
Also Note on Transmitter

- Half-duplex (full more expensive)
- Multiple frequency? Does each need own antenna?



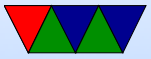
Notes on BSSID

- Each AP can handle more than one network group (i.e. guest, tempest, etc)
- BSSID (basic service set identifier)
- Each BSSID has 48-bit MAC. Randomly generated, with "local" bit set
- AP supposed to filter on this so only frames destined to correct BSS handled properly. Book stresses not everyone does this right.

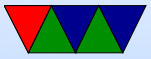


DCF – Distributed Coordination Function

- No central control
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
- Different from Ethernet CSMA/CD (D=detection)
- Every time ready to transmit, looks to see if can transmit (listen to see if channel clear)
- If clear, waits DIFS (inter frame) waits random time (to avoid two waiters starting simultaneously, to try to pre-emptively avoid collisions), then transmits

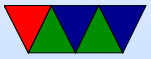


- If busy, waits until clear. Then it will wait a random backoff time before starting. Why? Multiple transmitters might have all been waiting and they would all instantly collide once clear.
- There is a short inter-frame interval (SIFS) which gives time for receiver to transmit an ACK packet.
- If source does not get an ACK, then it backs off and retries
- DCF not optimal, can take 60us to transmit ACK, whereas a 54MB connection could have send 3k of data in same time.



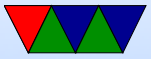
More on ACKs

- ACKs on unicast only, not sent on multicast/broadcast (so those are more unreliable)
- ACK, CTS, and fragments can send during SIFS



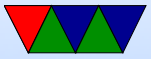
DCF: Fragmentation

- In some situations can fragment frames into smaller parts
- This is completely separate from IP fragmentation
- Why do it? – the longer the frame, the more likely it is to lose bits to interference. So split things up into smaller chunks likely to get through
- Fragment burst



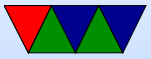
DCF: Error Handling

- Resend if error
- How detect error. No ACK?
- Short retry counter and long retry counter
- Backoff
  - Number of slots, based on how many retries
  - Each station randomly picks one of slots
  - If fails again, backs off and increases the slots

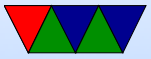


DCF: RTS/CTS Mode (used for "large" frames)

- Optional (rarely used) 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 that hints how long it will take

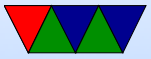


- ACK at end

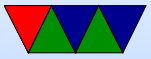


DCF: PCF – Point Coordination Function

- Also rarely used (mostly between infrastructure)
- 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
- Guaranteed a certain fraction of bandwidth
- 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.

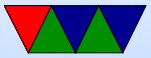


- Problem can happen if two different APs in range, in this case PCF won't be able to help collision problem if it's the other AP causing it



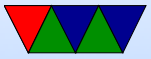
Does my router use PCF or DCF

- It appears that most use DCF, PCF is somewhat uncommon
- There is 802.11e which enhances this to Enhanced distributed channel access (EDCA)
- Introduces HCF (Hybrid Coordination Function)
- Still most are using DCF



Wireless Frames

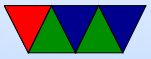
Different types have different layout



Wireless Data Frames

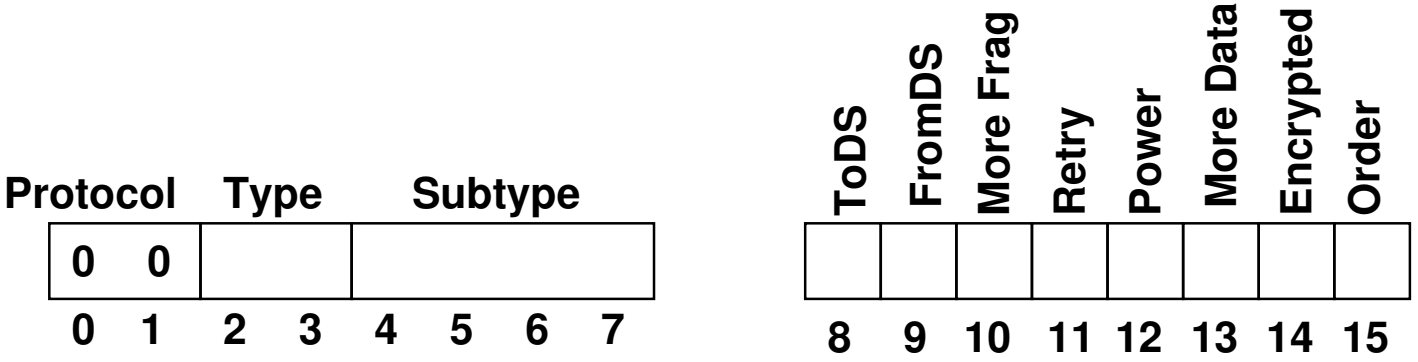
FC	Duration	Addr 1	Addr 2	Addr 3	SEQ	Addr 4	Body	FCS
2	2	6	6	6	2	6	0-2312	4

Note: the IEEE spec lists the fields LSB first. This sort of makes sense as they get transmitted in that order, but we usually write values MSB first so this makes it a huge pain to decode.

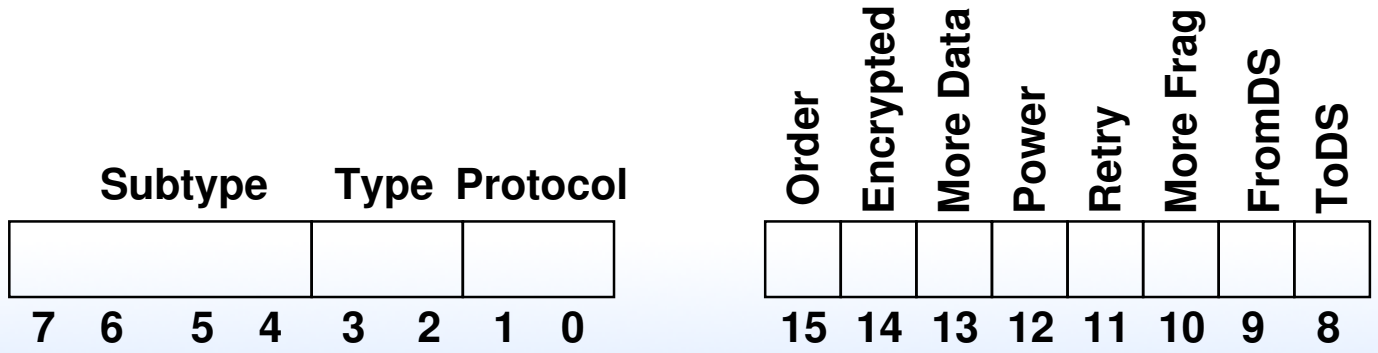


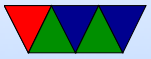
Wireless Frames – Frame Control (FC)

From the specification:



How we'd see the data in a hexdump:

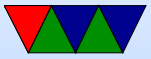




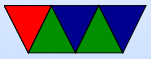
- Protocol Version (2 bits) [only 00 in practice]
- Type (2 bits): note, bit order is 3/2 so flipped depending how you decode
  00=management, 01=control, 10=data, 11=reserved
- Subtype (4 bits): bits 7,6,5,4
  see next slide for expansion
- ToDS/FromDS(1,1) (going to or from the access point)

	ToDS=0	ToDS=1
FromDS=0	mgmt	from station
FromDS=1	to station	bridge

- MF – more fragments to follow

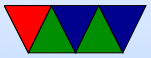


- Retry
- Power Management (into or out of sleep)
- More (more data coming, more than 1 frame being sent)
- W or Protection: WEP (or other encryption enabled)
- O frames must be in-order



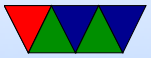
Wireless Frames – Management Frames (00)

- 0000 – Association request
- 0001 – Association response
- 0010 – Reassociation request
- 0011 – Reassociation response
- 0100 – Probe request
- 0101 – Probe response
- 1000 – Beacon
- 1001 – Announcement traddic indication message (ATIM)
- 1010 – Disassociation
- 1011 – Authentication
- 1100 – Deauthentication
- 1101 – Action (spectrum management)



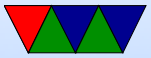
Wireless Frames – Control Frames (01)

- 0000 - 0111 (reserved)
- 1000 – Block Acknowledge Request
- 1001 – Block Acknowledgement
- 1010 – Power Save Poll
- 1011 – RTS
- 1100 – CTS
- 1101 – ACK
- 1110 – Contention-free end
- 1111 – CF-END+CF-Ack



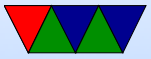
Wireless Frames – Data Frames (10)

- 0000 – Data
- 0001 – Data+CF-Ack
- 0010 – Data+CF-Poll
- 0011 – Data+CF-Ack+CF-Poll
- 0100 – Null data (no data)
- 0101 – CF-ACK (no data)
- 0110 – CF-Poll (no data)
- 0111 – CF-Ack+CF-Poll (no data)
- 1000 - 1111 - same as above but with QoS



Wireless Frames – Duration

- Duration/ID (2 bytes) – how long will occupy channel
- Network Allocation Vector (NAV)
- TODO: this varies based on various things, including fragmentation
- is microseconds?
- Special meaning, top bits 10 = contention free period, max 32k. top bits 11 = poll, for sleeping devices

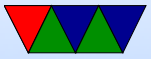


Wireless Frames – Addresses

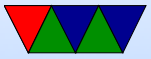
- Note that destination/receiver are not necessarily same
  - Destination: where the bytes will be used
  - Receiver: device that is going to decode the radio waves
- Same with transmitter/sender

  Sender is the device who put together the bytes in the packet

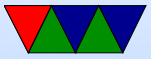
  Transmitter is device that sent it out over the radio waves



- Special case when broadcast/multicast, BSSID also checked
- See table (source IEEE 802-11 2012 Table 8-19)
- How addresses defined depends on tods/fromds fields
- Addr1 (6 bytes) Receiver
  Usually destination, not always
- Addr2 (6 bytes) Transmitter
- Addr3 (6 bytes) Base Station Source? filtering?
- Address4 (6 bytes) Base Station Dest (for wireless bridges, uncommon to use)
- More on addresses

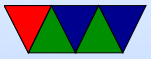


- basic service set identifier (BSSID)
  MAC address of the access point (randomly generated?)
- source address (SA)
- destination address (DA)
- transmitting address (TA) who sent it,
- receiving STA address (RA) destination, this might not be addr1 on CTS/ACK frames.



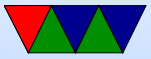
Wireless Frames – Sequence/Fragment

- Sequence control (2 bytes)
- Fragment (4)
- Frame (sequence) (12 bits)
- TODO: book has more on this



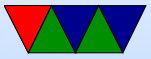
Wireless Frames – Body

- Frame body (0-2312)
- Can actually be 0 (no need to pad for collisions) control frames can be size 0
- Actually can be a bit more
- Why that size? Idea is for about 2k of data, then with the additional frame/packet/encryption overhead
- In practice rarely would see much bigger than 1500 bytes because things would have to be fragmented once they hit wired ethernet



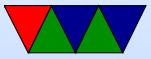
Wireless Frames – Encapsulation

- How can you tell what is in a frame (IPv4, IPv6, ARP, etc?)
- Ethernet has a type field, but we don't
- For wifi we have to encapsulate it
- Two ways to do this
  - RFC 1042 (sometimes called IETF)
  - IEEE 802.1H (tunnel)
  - Due to Microsoft precedent, Appletalk/IPX use 802.1H, IPv4/IPv6/etc use IETF



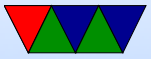
Wireless Frames – RFC1042 Encapsulation

- Start with wifi frame
- Add SNAP field. Various forms but here probably starts 0xAA 0xAA
- Add type
- Then include data
- Double check this
- Relatively straightforward to go ethernet to wifi and wifi to ethernet



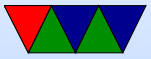
Wireless to Wired

- Validate, discard if not for BSSID
- Decrypt
- Reassemble frame
- Setup ethernet header
- Recalculate FCS
- Transmit



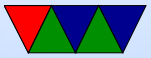
Wired to Wireless

- Setup wifi header
- Encapsulate
- Queue to transmit
- Encrypt
- Recalculate FCS
- Transmit



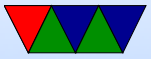
Wireless Frames – CRC

- FCS CRC (4 bytes)
- Same as Ethernet, but has to be recalculated if move from Ethernet to Wifi due to different header
- ACK if correct
- If incorrect, no NACK, just drop it, so wait for timeout



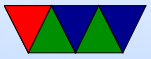
Multi-rate Handling

- Common speeds handled by all devices
- Speeds used by two currently talking (station and AP usually)
- Rate Fallback (slow down if too many errors)

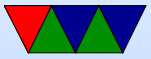


Frames

- Class 1 – send any time
- Class 2 – only if authenticated
- Class 3 – only if associated

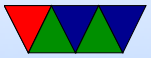


Control Frames



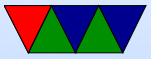
Control Frames – RTS

- Subtype 1011
- Duration
- Addr1: station
- Addr2: transmitter



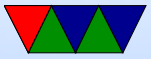
Control Frames – CTS

- Subtype 1100
- Answer RTS
- Used in 802.11g to avoid interference with 802.11b

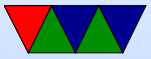


Control Frames – ACK

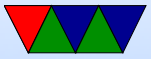
- Subtype 1101
- Addr1: receiver addr



Control Frames – PS-Poll

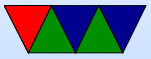


Management Frames – Authentication



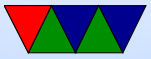
Management Frames – Capabilities / Beacon

- Address of AP
- Listen Interval
- Association ID/Timestamp
- Reach code
- Status code
- SSID – plain text, 32 bytes (usually ASCII), easier than MAC for keeping BSSID separate
- Supported rates, mandatory and optional (originally



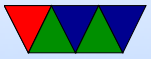
multiple of 500k/s)

- Association ID
- Freq-Hop
- DS (channel)
- Traffic Indication Map
- Country – 3 bytes (country abbreviation plus I/O for indoor/outdoor)



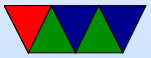
Management Frames – Beacon Interval

- announce existence of 802.11 at regular interval
- time around 1ms, but called kilo-microseconds (kus). kilo is 1024, ms=1000



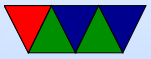
Management Frames – Beacon

- Probe request
- Probe response
- Disassociation
- Deauthentication
- Association Request
- Reassociation Request



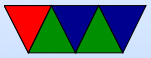
Reliability

- Wireless can be noisy and unreliable
- What do you do if there's packet loss?
  - Send slower
  - Send shorter frames
  - Fragment frames

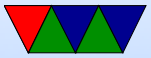


802.11e QoS

- Leaves idle time before sending next frame
- Different sizes for different traffic
- DIFS – DCF inter-frame spacing
  - SIFS – short (control frames)
  - AIFS1 – Arbitrary (high priority)
  - DIFS – regular DIFS
  - AIFS4 – low priority
  - EIFS – extended, for errors
- TXOP – transmission opportunity



- Usually fixed number of frames so faster devices held back
- Instead, provide equal airtime rather than equal frames



Power Saving

- Important for mobile devices
- AP beacon frames from AP every 100ms
- Can indicate you want power saving, then go to sleep, on next beacon wake up and notice from beacon if data available to read (AP will buffer)
- APSD – auto power-save, AP will buffer frames until device sends something, send buffered data knowing it's awake