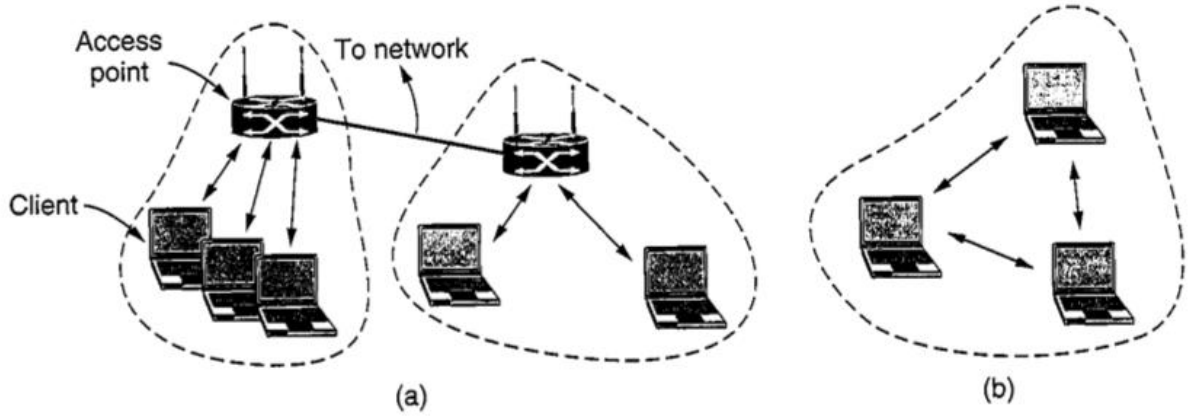
Lecture 15
Plan: Wireless networks and Bluetooth

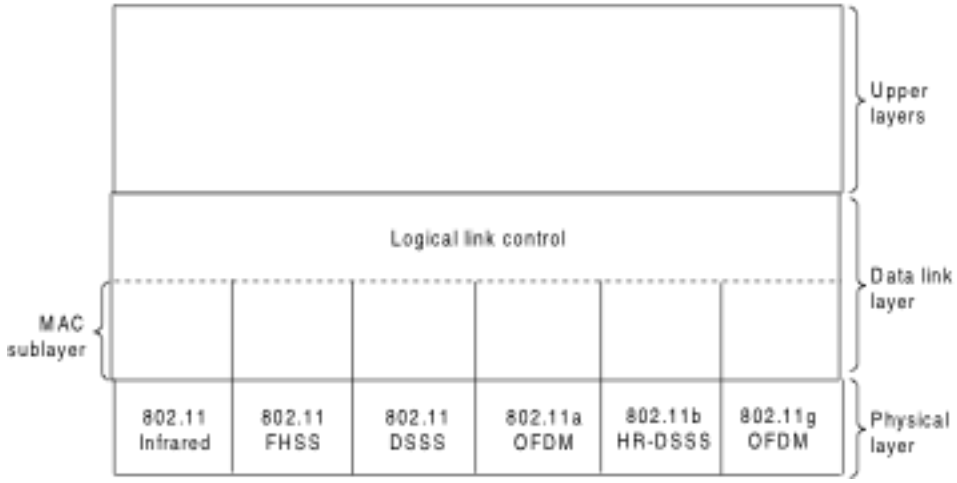
Topic: Wireless Networks (802.11) and Bluetooth (802.15)

1. 802.11
The protocol defines physical and data link layers → upper layers are not confined.

Modes of operations
a. infrastructure mode (with base station or access point)
b. ad hoc mode (without base station (peer to peer))



We will focus on the infrastructure mode. The overall stack of the 802.11 is the following



1. Physical layer
Transmission is by infrared or radio wave (more prevalent)
2.4 GHz ISM band (**I**ndustrial, **S**cientific, and **M**edical)

- Pro: no licensing necessary
- Con: interference with microwave oven, cordless phones,

6 different physical layer protocols (1 infrared and 5 radio) → focus radio wave protocols

Terminology

- spread spectrum: occupy a wider bandwidth without actually using it.
- frequency hopping: use spread spectrum, the base frequency changes at least several times per second
  Q:/ Why?
  A:/ more secure, less interference

FHSS and DSSS were used in 1997 to 1999 (now defunct)

FHSS – Frequency hopping spread spectrum

- 79 channels defined using different frequencies in ISM band with 1MHz per band.
- sender and receiver hop from frequency to frequency at least 2.5 times per second.
- sequence is random→ they must use the same random number generator and stay in sync to make sure they hop to the same band.
- data rate: 1 or 2 Mbps

DSSS – Direct Sequence Spread Spectrum

- 1 wide channel is defined in ISM band
- Each bit is sent as an 11-bit chip sequence → similar to CDMA
- chip sequence is determined by random number generator
- sender sends code = message xor (chip sequence)
- receiver computers code xor (chip sequence)=message
- rate: 1 or 2M bps

802.11b (1999)

- uses HR-DSSS (high rate DSSS) → similar to DSSS but with more complicated coding → higher bps
- rate: up to 11Mbps
- slower than 11a but offers a longer range because the frequency band is 2.4G here compared with 5G for 802.11a.

802.11a (1999)

- uses OFDM (orthogonal frequency division multiplexing)
  - several signals with different frequencies are used to send for a single source
  - orthogonal means that all those signals are orthogonal to each other.
- up to 48 data channels are defined around 5GHz band using FDM
- bit stream is sent in parallel (similar to ADSL)
- data rate: up to 54Mbps

802.11g(2001)

- uses OFDM in 2.4GHz range
- up to 54Mbps

802.11n (2007)

- uses OFDM in 2.4GHz or 5GHz

- at least 100Mbps
- up to four MIMO (multiple input, multiple output) antennas
- overhead reduction
- With the finalization in Oct 2 2009 on 802.11n, the speed can reach 600Mbps with 4 antennas and wider channels.

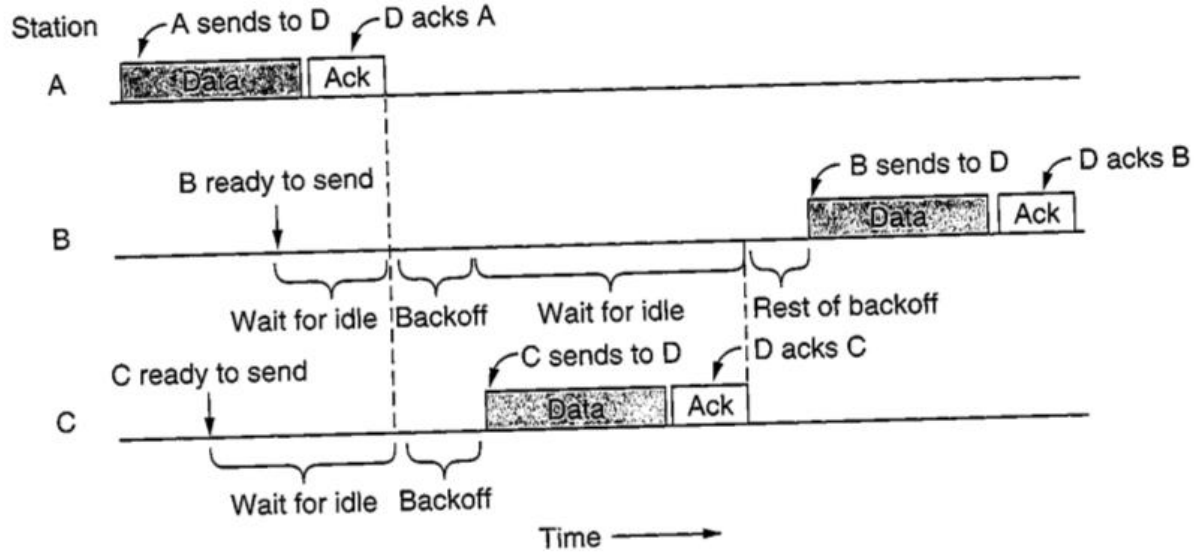
2. MAC Layer

Issues:

- range of radio waves
- a station cannot detect the channel while it is transmitting because its own signal is so much stronger than incoming ones →half duplex

CSMA/CA (collision avoidance) is used to solve medium access problem in wireless →based on MACA

In this protocol, a station that has a frame to send starts with a random backoff. It doesn't wait for a collision. The number of slots to back off is chosen between 0 and 15. It basically counts down on the number and pauses the counting when the channel is used. When the count down is to 0, the frame is sent. The receiver will ack the frame as soon as it is received.
Q:/ Does it eliminate collision?
A:/ No.
Q:/ What if there is no ack from the reciever?
A:/ double the backoff time and try again.



Two versions of multiple access

DCF (distributed coordination function)

- Based on MACA principle (RTS-CTS)
- frames may be broken into fragments to reduce error rate
- Fragments may be sent in bursts, using only one RTS-CTS pair. Each fragment is separately ACKed.

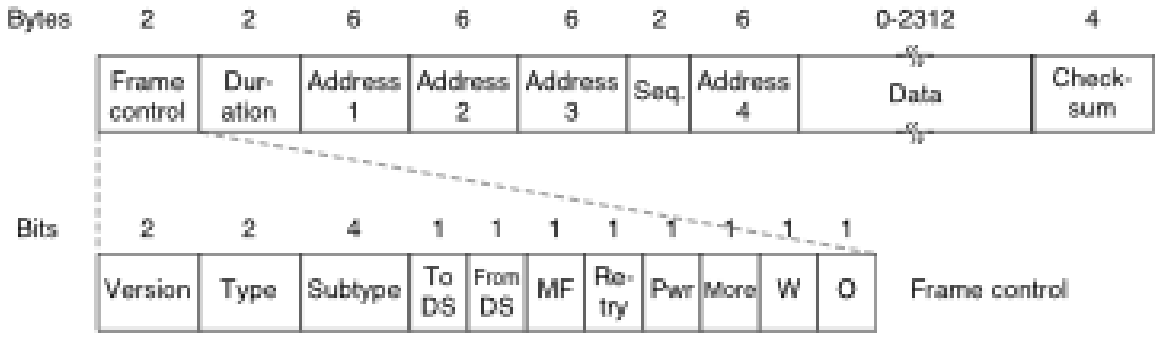
PCF (point coordination function)

- A centralized multiple access control (base station is the arbitrator)
- Base station transmits a beacon frame to poll what wants to send

Both DCF and PCF exist on the same channel
Q:/ How?
A:/ use prioritization based on the wait time after an ACK. → each sender must wait a period of time before sending the next frame.
The highest priority waits the least amount of time, if nothing happens, then the next priority can take pace.

1. The same sender in a single dialog. → facilitate sending fragments in bursts
2. base station beacon frame (PCF)
3. Any sender wishing to claim the channel with RTS message (DCF)
4. A receiver reporting a bad or unknown frame

3. Data Frame Structure
All 802.11 variations use the same frame structure



Frame control: 2 bytes
Version: protocol version (reserve for future 802.11 versions) Right now, it is just 00.
Type: data, control, or management
Subtype: RTS or CTS
To/From DS: whether the frame comes from or goes to the intercell distribution system (Ethernet)
MF: More fragments to come
Re-try: it is a re-transmission
Pwr: active-powerSave or vice versa (put the receiver to sleep or wake it up)
W: WEP (wired equivalent privacy) algorithm encryption
WPA(wifi protected access) and WPA2 are currently used to ensure security.
O: Frame must be processed strictly in order

Duration: time in microseconds (estimate how long the frame will occupy the channel)
Q:/ What is duration used?
A:/ for the purpose of MACA based waiting.
Address: 6-byte MAC address
receiver, sender

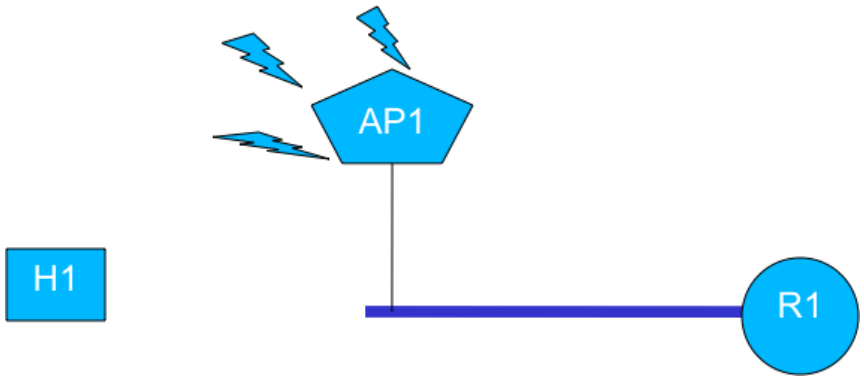
Q:/ Why do we need four addresses?
A:/ The last two are for the source and destination base stations for intercell traffic.

Sequence: sequence number of fragments
Data: 0-2312
Checksum: CRC

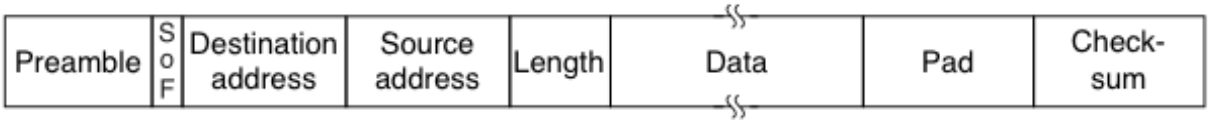
4. Services:

- Association/De-association
  - establish a connection to a base station
  - AP sends out beacon frames periodically, containing name and MAC address
  - host can then request association using 802.11 protocol
  - if all is ok, then host becomes part of the AP's BSS (basic service set)
- Distribution – Internetworking with a wired part of the network
- Authentication
- Privacy/ Encryption (RC4)
- Data Delivery
-

E.g. Suppose that a wireless host H1 is connected to an assess point AP1, which is connected on an Ethernet to an Internet Router R1. An IP datagram is sent to H1 from a host through R1. What happens?



1. The datagram contains the IP address of H1. The router uses ARP to get H1's MAC address.
2. The router puts the datagram in an Ethernet frame and sends it on the Ethernet, with H1's address as the destination address



3. AP1 receives the frame, removes the Ethernet framing and puts the contents in a 802.11 frame with
   * address 1 = H1 (wireless destination)
   * address 2 = AP1 (wireless source)
   * address 3 = R1 (DS source)
   * from DS flag set
   * address 4 will have the mac address of the router sending the frame to R1.
4. When H1 sends a reply, it constructs an 802.11 frame with

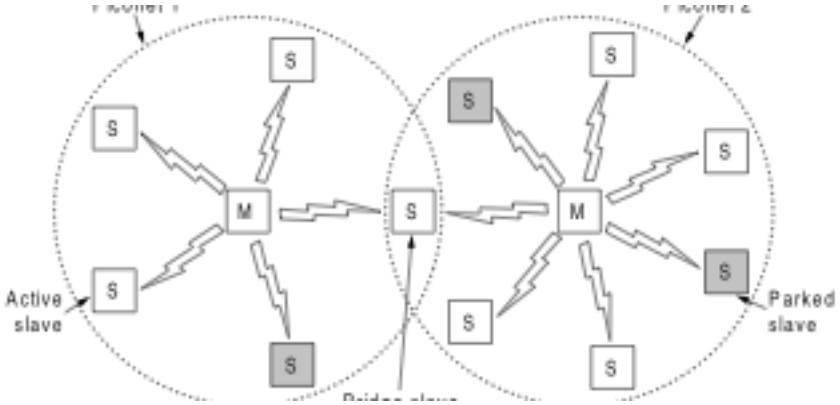
* address 1 = AP1
* address 2 = H1
* address 3 = the mac address of the router sending the frame to R1.
* address 4 = R1
* to DS flag set

5. When AP1 receives the frame, it converts it to an Ethernet frame with source = H1 and destination = R1

Bluetooth (802.15) – WPAN (wireless personal area network)

Purpose: replace cables between computers and peripherals

- uses lower power than 802.11 but shorter range
- Architecture
  - piconet – a master node with up to 7 active slave nodes within 10 meters
  - Use centralized TDM. (master allocates time slots 525 microseconds) to slaves
  - no slave-slave commnication.
  - multiple piconets can connect using bridge slaves (scatternet)



- Physical layer
  - use low power radio waves (2.4GHz)
  - Frequency modulation with FHSS on 79 channels
  - may interfere with 802.11 b/g
  - data rate: up to 721 kbps