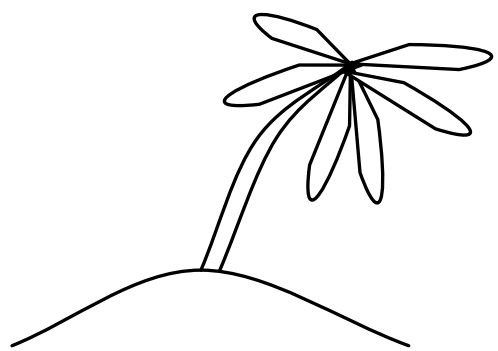
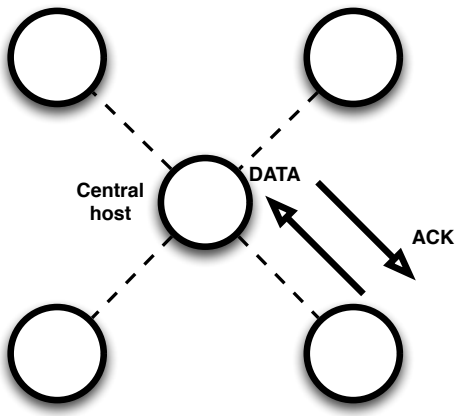
Wireless data networks

Martin Heusse



Aloha (1972)




```
i = 1
while (i <= maxAttempts) do
  send packet
 wait for acknowledgement or timeout
  if ack received then
    leave
  wait for random time
increment i
end do
```

```
t = 1
while (t <= maxAttempts) do
  send packet
  wait for acknowledgement or timeout
  if ack received then
    leave
  wait for random time
  increment t
end do
```

1. AlohaNet is a wireless network with a central host that sends or receives all frames (much like access points in 802.11 networks in fact!)
2. AlohaNet used 2 channels: 1 for sending to the central host, 1 for broadcasting from it — so access contention was, in effect, limited to the "uplink"
3. Hosts can not check if the medium is idle before transmitting! (it's the same for RACH of GSM…)
4. ARQ ensures retransmissions after transmission errors or collisions…

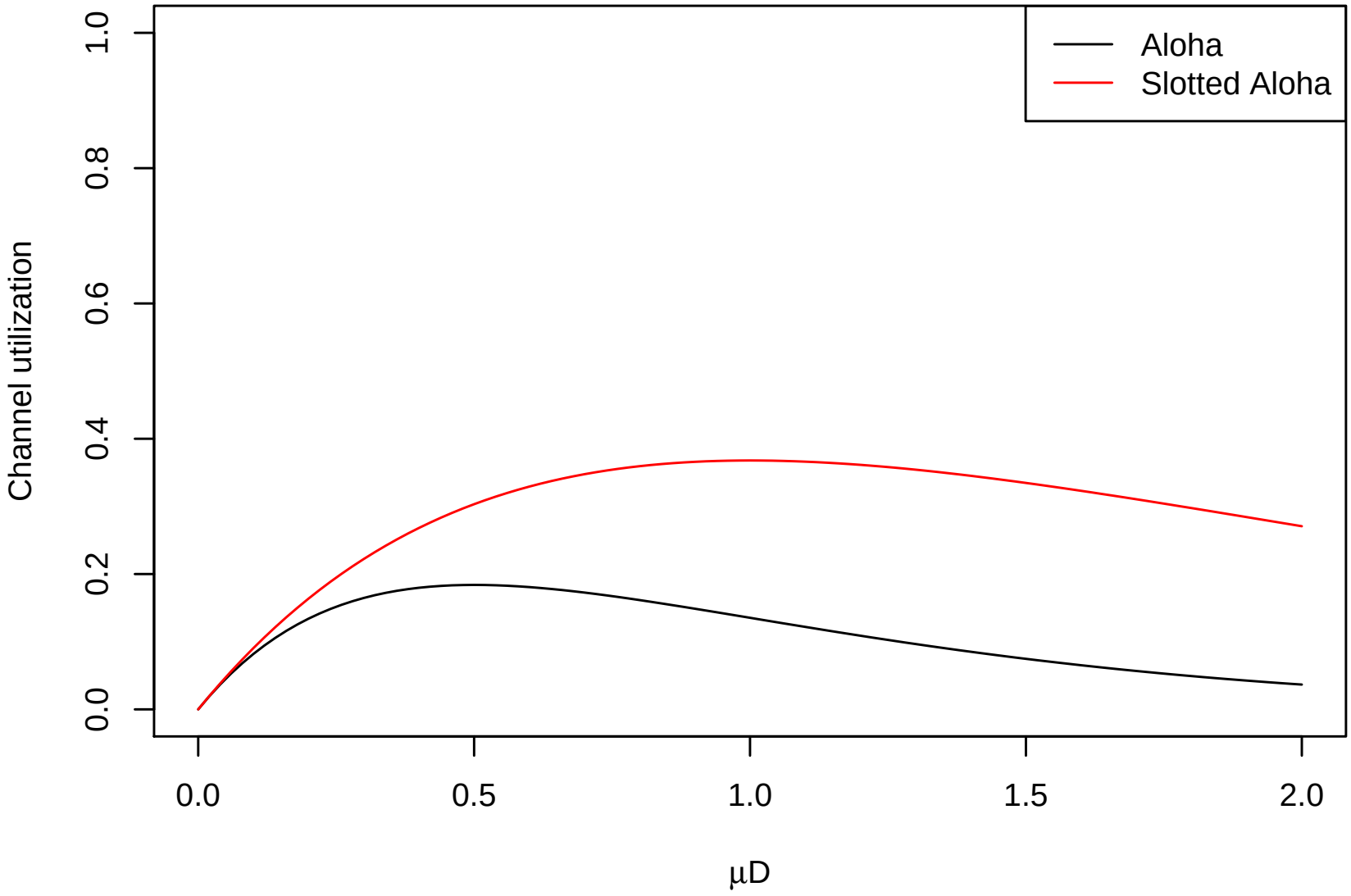
Aloha performance with Poisson traffic

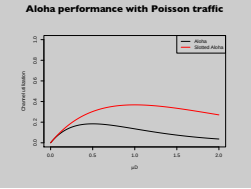
- A transmission is successful only if a frame does not interfere with an earlier of later transmission
- $\Rightarrow$ For every transmission attempt (which occupy the channel for a fraction $\mu \times$ `frame_duration` of the time) There should be **no other transmission** during $2 \times$ `frame_duration` (*fd*)

$$P[N(t) = n] = \frac{(\mu\ t)^n}{n!} \exp(-\mu\ t) \quad \text{(Poisson process)}$$

$$P[N(2\ fd) = 0] = \exp(-2\mu\ fd)$$

Aloha performance with Poisson traffic





1. Even with *backlogged traffic*, the random wait randomizes transmissions
2. μ *fd* is the important parameter to measure channel load: it is the channel occupancy, regardless of collisions *etc.*
3. $\exp(-2\mu$ *fd*$)$ is the probability that a given transmission is not a collision
4. μ *fd* $\exp(-2\mu$ *fd*$)$ is the fraction of time the channel is used by successful transmissions!
5. Rather disappointing performance… less then 1/5 of capacity utilization! Unless you are alone! Slotted aloha brings a major improvement.
6. To the left of the maximum, the channel is empty; to the right, there are more and more collisions. The tradeoff is the same for CSMA/CA, although with much better utilization…

Slotted Aloha

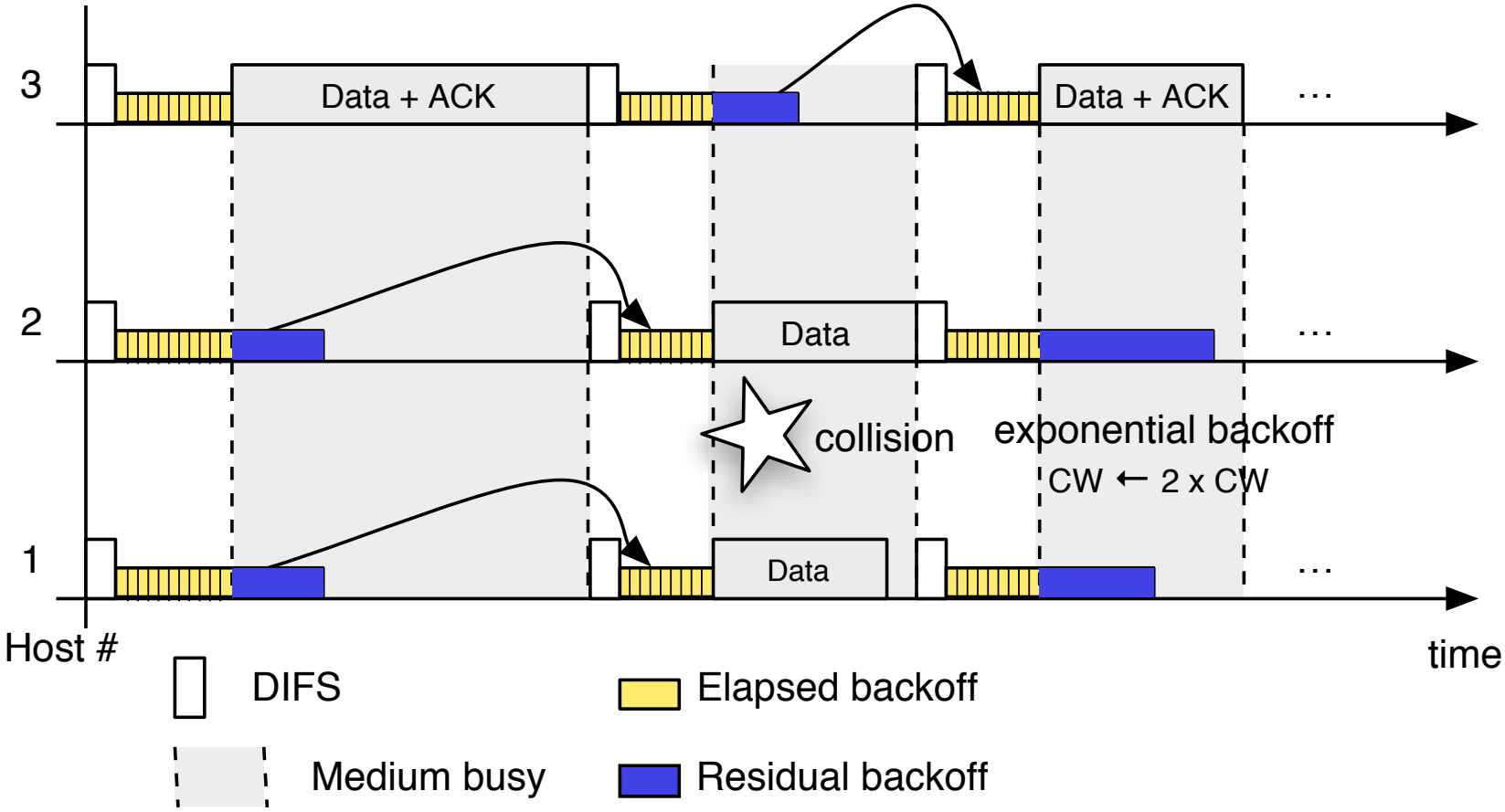
- Access takes place on discrete time "slots"
  (D, 2 $\times$ D , 3$\times$ D… after the end of the previous transmission)
- Number of transmissions during a slot of size D (Poisson traffic):
  $P[N(D) = n] = \frac{(\mu D)^n}{n!} \exp(-\mu D)$
- The probability of transmission without collision becomes simply: $P[N(D) = 1] = \mu D \exp(-\mu D)$
  Max for $\mu D = 1$
- Used for initial access in GSM…

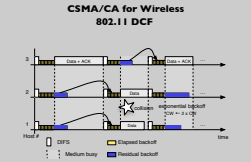
Slotted Aloha

- Access takes place on discrete time "slots" (D, 2 × D, 3× D… after the end of the previous transmission)
- Number of transmissions during a slot of size D (Poisson traffic): $P[N(D) = n] = \frac{(\mu D)^n}{n!} \exp(-\mu D)$
- The probability of transmission without collision becomes simply: $P[N(D) = 1] = \mu D \exp(-\mu D)$
  Max for $\mu D = 1$
- Used for initial access in GSM…

1. The maximum utilization improves significantly, and the system is much less sensitive to overload
2. Need a clock! Readily available on a system that uses TDMA (propagation times need to be compensated for or made harmless, though)…

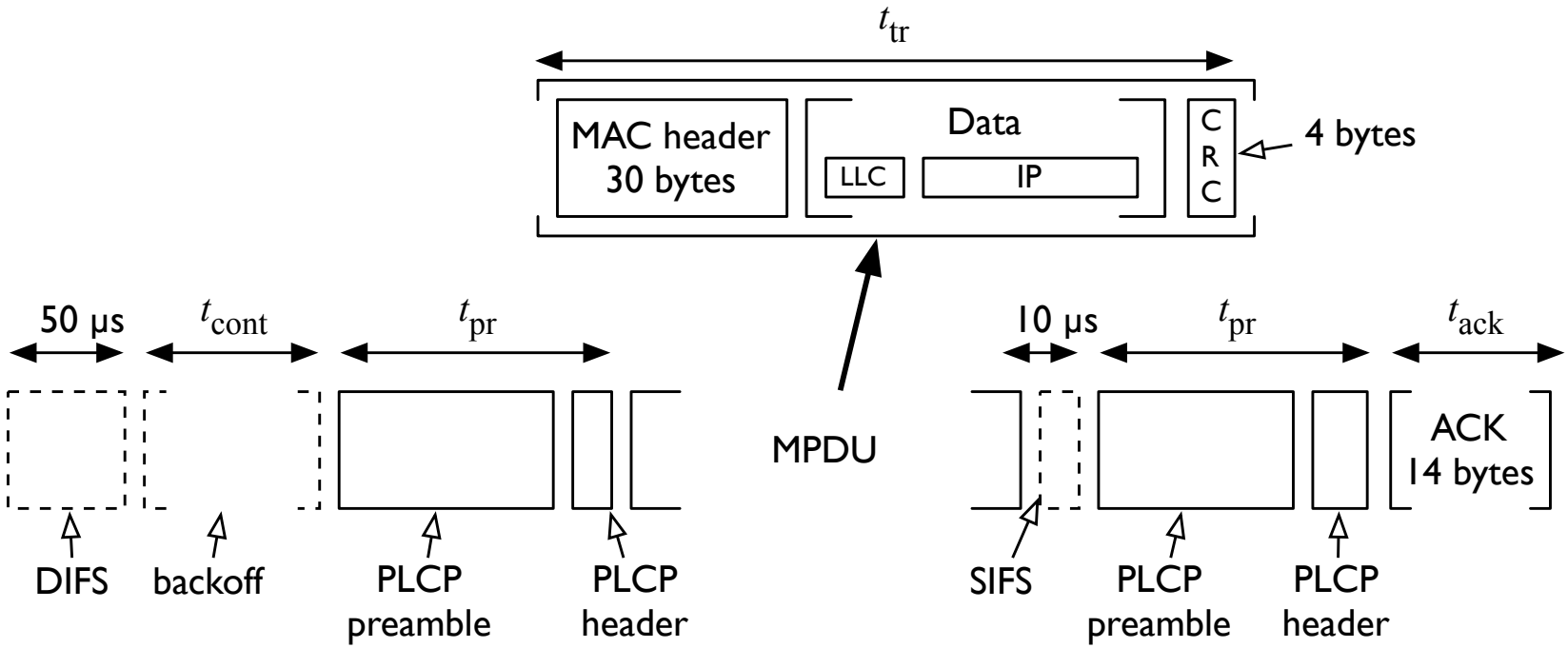
CSMA/CA for Wireless
802.11 DCF



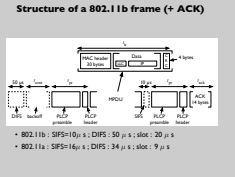


1. CA is for Collision Avoidance
   we saw in the introduction lectures that there is no way you can assess someone else is transmitting if you are!
   So we avoid collisions by randomizing the accesses after the natural synchronizing events (= channel release)
2. In 802.11 CSMA/CA, the residual backoff when an another host starts sending is kept for the next contention cycle $\rightarrow$ really good short term fairness
   - as long as the channel is similar for all hosts (no asymmetric collisions)
   - many people still (or used to) think short term fairness is bad in 802.11. They are (were) wrong
3. It is possible to signal the transmission… before the transmission, using an RTS/CTS handshake. This is to avoid collisions with hidden hosts (that are "within reach" of the receiver but who can not hear the sender)

Structure of a 802.11b frame (+ ACK)



- 802.11b : SIFS=10μ s ; DIFS : 50 μ s ; slot : 20 μ s
- 802.11a : SIFS=16μ s ; DIFS : 34 μ s ; slot : 9 μ s



1. Now you understand what is the PLCP layer in the OSI layers slide in the introduction
2. The PLCP **header** is for
   - Telling the receiver what modulation is going to be used for the payload
   - Signaling how long the transmission will last

802.11b PHYs
2.4GHz band

- 1Mb/s: DSSS 11Mchip/s 1Mbit/s DBPSK
  Chip sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, –1, -1
- 2Mb/s: DSSS 11Mchip/s, DQPSK (the chips are complex symbols)
- 5.5Mb/s and 11Mb/s : complementary code keying / DQPSK still 11Mchips/s

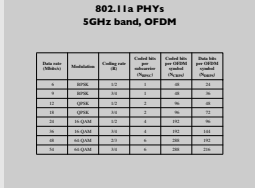
802.11b PHYs
2.4GHz band

- 1Mb/s: DSSS 11Mchip/s 1Mbit/s DBPSK
  Chip sequence: +1, -1, +1, +1, -1, -1, +1, +1, +1, -1, +1, -1
- 2Mb/s: DSSS 11Mchip/s, DQPSK (the chips are complex symbols)
- 5.5Mb/s and 11Mb/s : complementary code keying / DQPSK still 11Mchips/s

1. DSSS is for Direct Sequence Spread Spectrum. Send 11 chips (=symbols) per bit of actual information. Take a decision after reception of the entire sequence. Chip rate is higher than the bit rate, so we use more spectrum. See the slides on spread spectrum for more details.
2. N.B.: at 11Mb/s, there are **still 2 chips/bit**…

802.11a PHYs
5GHz band, OFDM

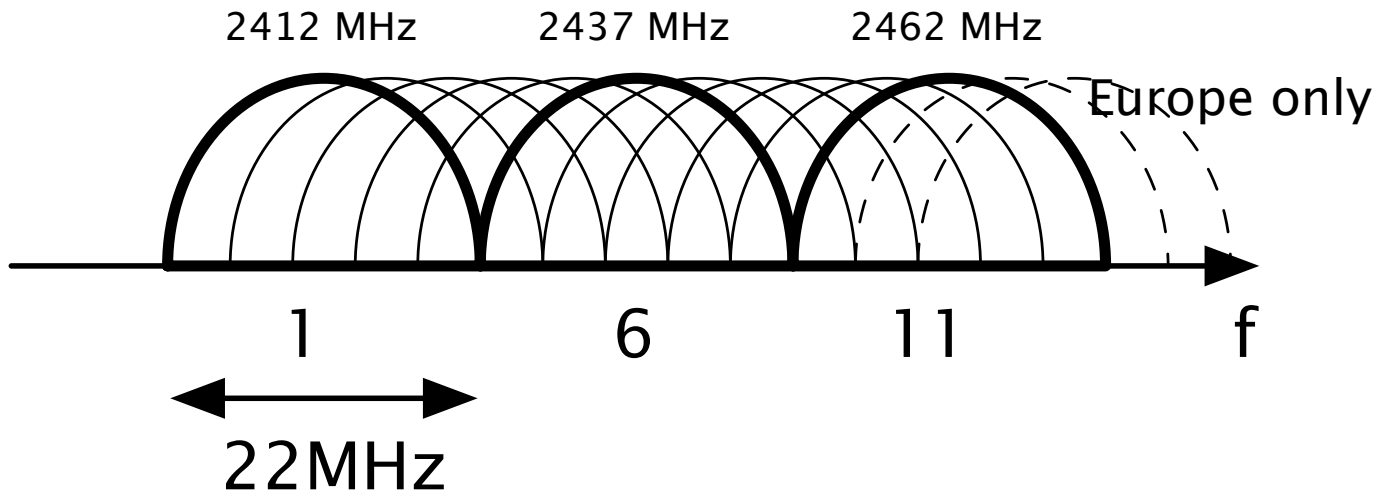
Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216


802.11a PHYs
5GHz band, OFDM

Data rate (Mbits/s)	Modulation	Coding rate (R)	Coded bits per subcarrier (N_{BPSC})	Coded bits per OFDM symbol (N_{CBPS})	Data bits per OFDM symbol (N_{DBPS})
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

1. 802.11 uses OFDM modulation over 48 carriers (plus 4 pilot carriers)

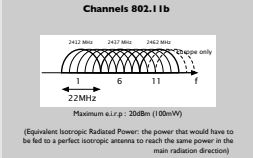
Channels 802.11b



Maximum e.i.r.p : 20dBm (100mW)

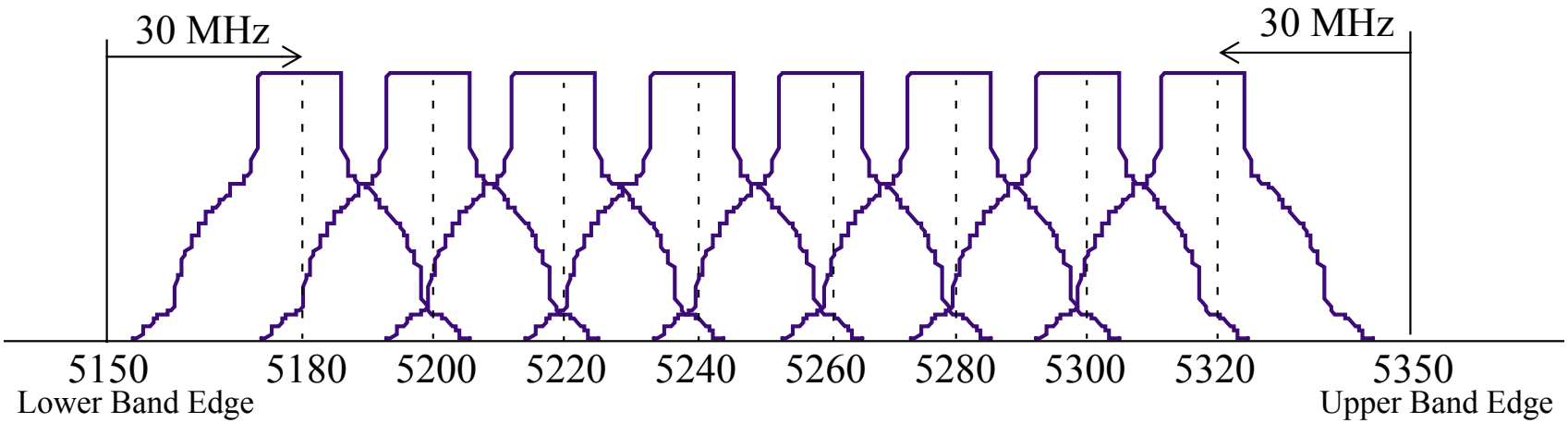
(Equivalent Isotropic Radiated Power: the power that would have to be fed to a perfect isotropic antenna to reach the same power in the main radiation direction)

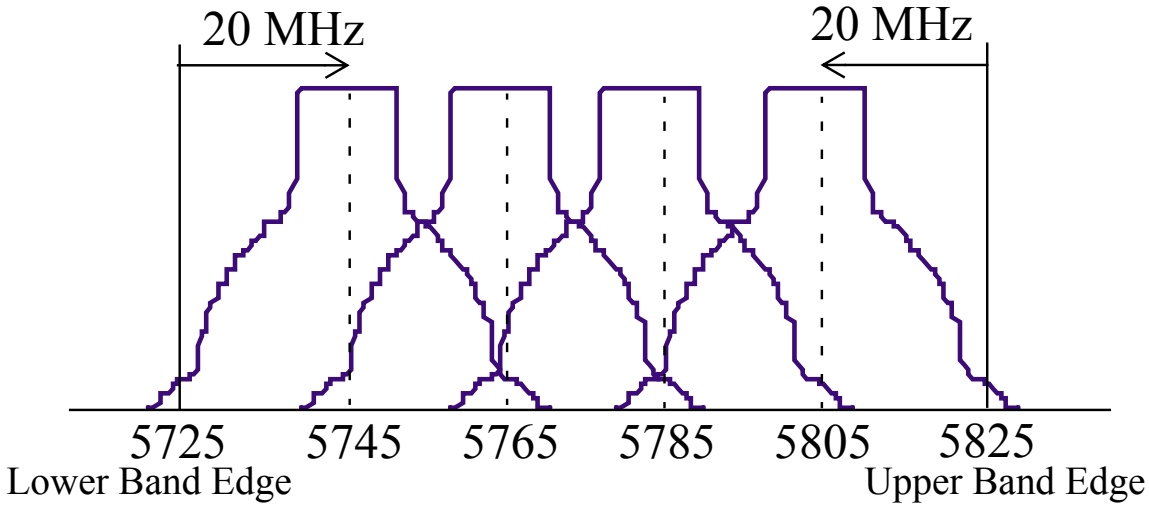
Channels 802.11b



1. 802.11b channels **are not** disjoint!
2. Please use only channels 1, 6 and 11 (or 12, 13 in Europe)

802.11a


30 MHz
30 MHz
5150
Lower Band Edge
5180
5200
5220
5240
5260
5280
5300
5320
5350
Upper Band Edge


20 MHz
20 MHz
5725
Lower Band Edge
5745
5765
5785
5805
5825
Upper Band Edge

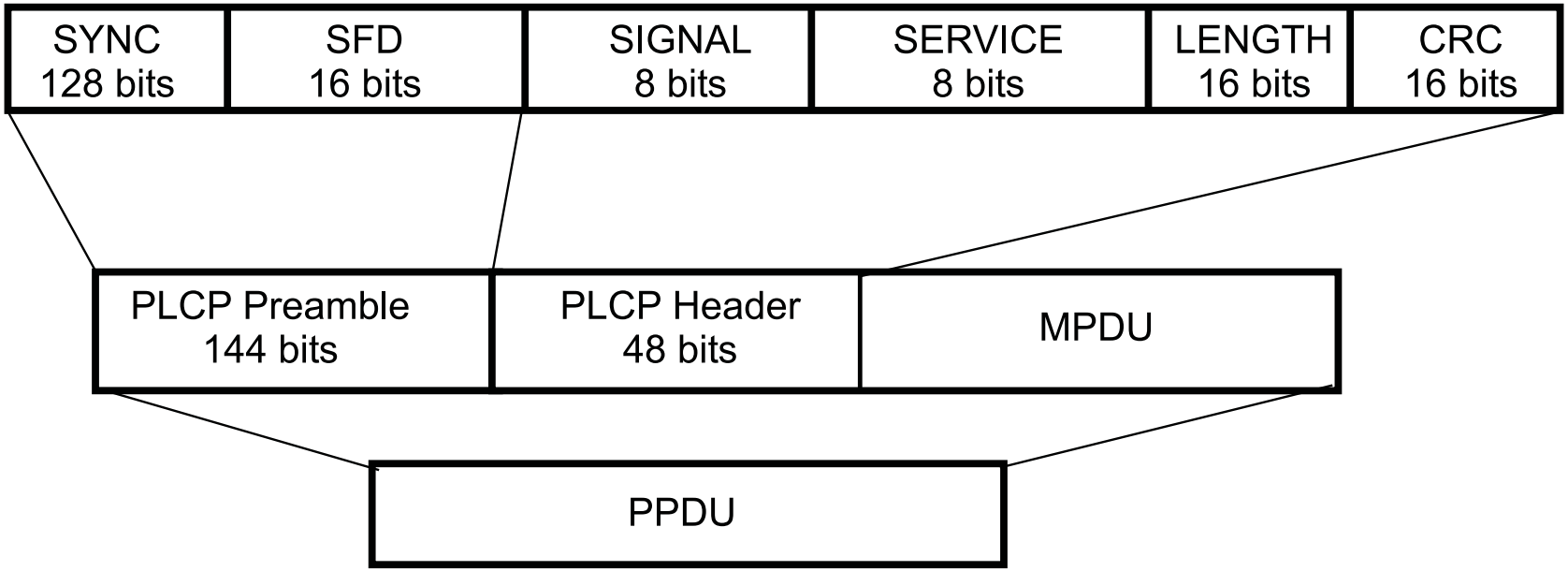
802.11a (cont.)

Regulatory domain	Band (GHz)	Operating channel numbers	Channel center frequencies (MHz)
United States	U-NII lower band (5.15–5.25)	36 40 44 48	5180 5200 5220 5240
United States	U-NII middle band (5.25–5.35)	52 56 60 64	5260 5280 5300 5320
United States	U-NII upper band (5.725–5.825)	149 153 157 161	5745 5765 5785 5805

Maximum e.i.r.p : 30dBm (for devices with a Radar Interference Detection function)

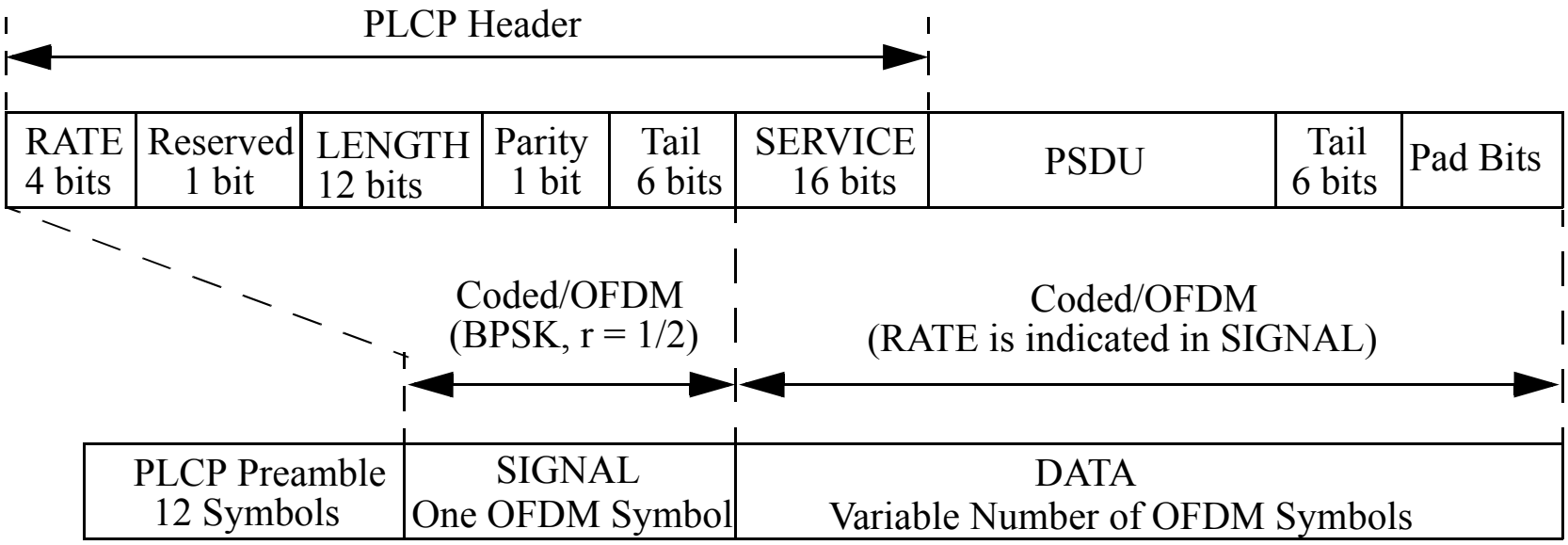
(Outdoor range $\sim$ 2.2km @ 6Mb/s with L.O.S.)

PLCP 802.11b
Phy. Layer Convergence Proto.



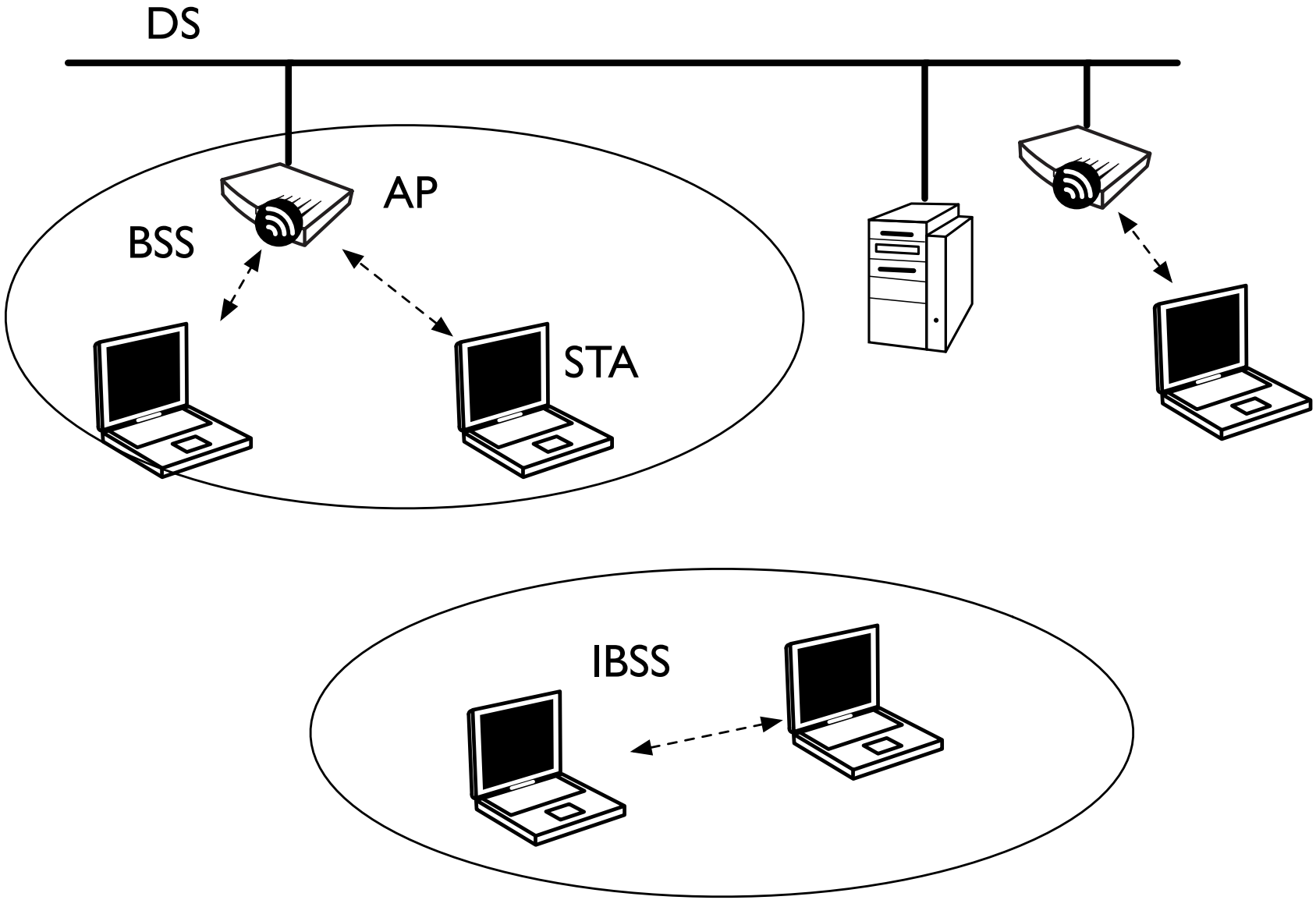
- Duration: 802.11b: 192µs @ 1Mb/s
  (Short preamble option: 72 bits preamble @ 1Mb/s, PLCP head. @ 2Mb/s $\rightarrow$ 92µs)
- Signal: data transmission bit rate
- Length: tells when reception should stop (framing)

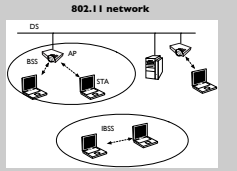
PLCP OFDM (11a, 11g)



Duration: ≈22µs

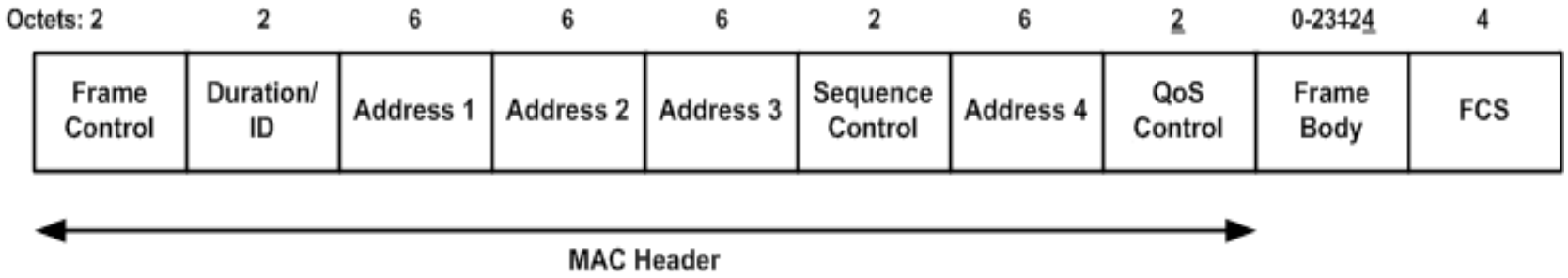
802.11 network





1. IBSS: "*ad hoc*" network, no AP. Stations still beacon
2. BSS: Basic Service Set. BSSID is the AP MAC address. SSID is the network "name", mentioned in the beacons sent by all the beacons of the SS. (Think Eduroam, WIFI campus…)
3. DS: Distribution system: the backhaul network. Generally a simple Ethernet switch, or a fancier box

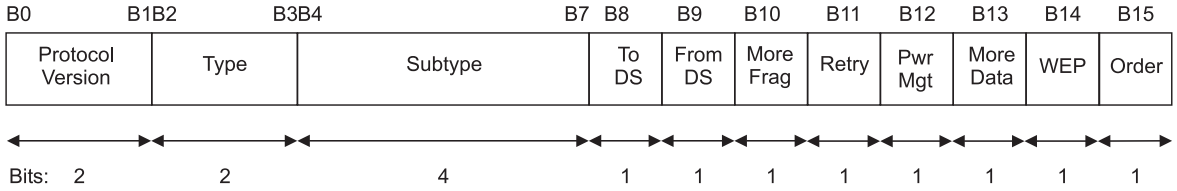
802.11 Data frame



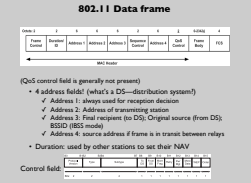
(QoS control field is generally not present)

- 4 address fields! (what's a DS—distribution system?)
  - ✓ Address 1: always used for reception decision
  - ✓ Address 2: Address of transmitting station
  - ✓ Address 3: Final recipient (to DS); Original source (from DS); BSSID (IBSS mode)
  - ✓ Address 4: source address if frame is in transit between relays
- Duration: used by other stations to set their NAV

Control field:



802.11 Data frame



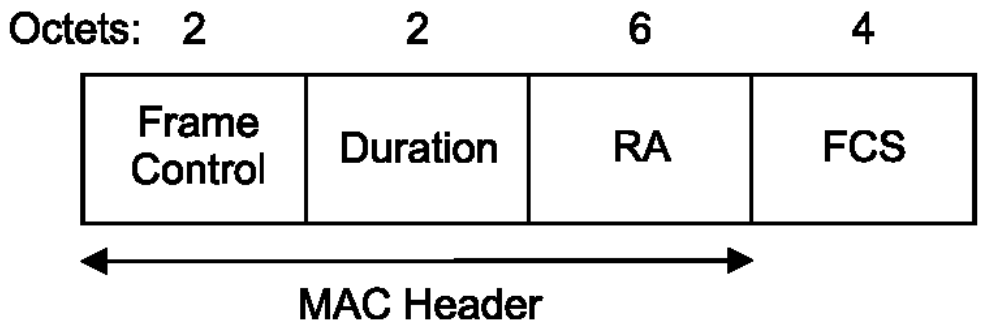
1. The length of the header changes depending on the information is needs to carry. The control field specifies is entirely
2. In general, there are 3 MAC addresses in the frames, two for the first hop, and another one to reach the destination (or specify the source) in the DS – see next slide for more details

Address fields content

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

N/A means field is not present in header

ACK frame format



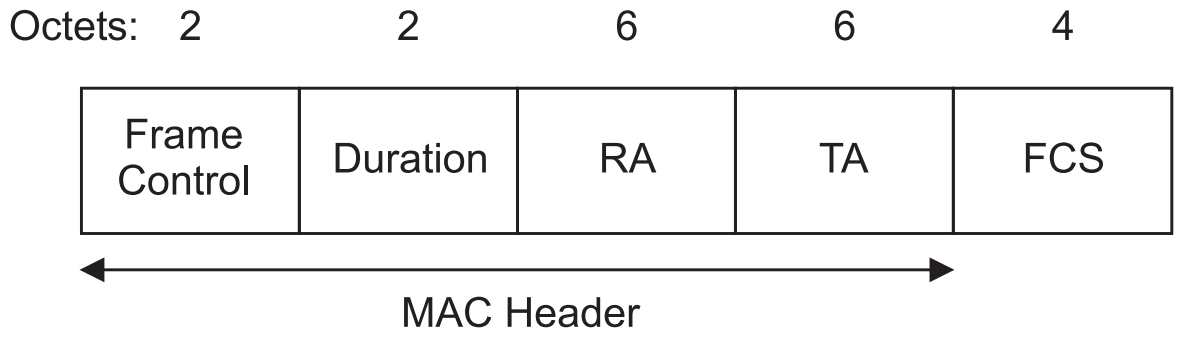
RA: address of sender of data frame

Number of retries: 7 for short frames (RTS or frames below RTS/CTS threshold)

4 for long frames (Above RTS/CTS threshold)

The counter are incremented only after a failure, so one transmission can fail 7 times at the RTS CTS handshake and 4 times after the data frame transmission

RTS frame format



- Duration: RTS+SIFS+CTS+SIFS+DATA+SIFS+ACK

Management frames

- Beacons:
  - ✓ Timestamp
  - ✓ Beacon interval
  - ✓ Capability (PCF available? Encryption required?)
  - ✓ SSID (up to 32 bytes)
  - ✓ Required rates
- Probe requests, response
- Association requests/responses

Management frames

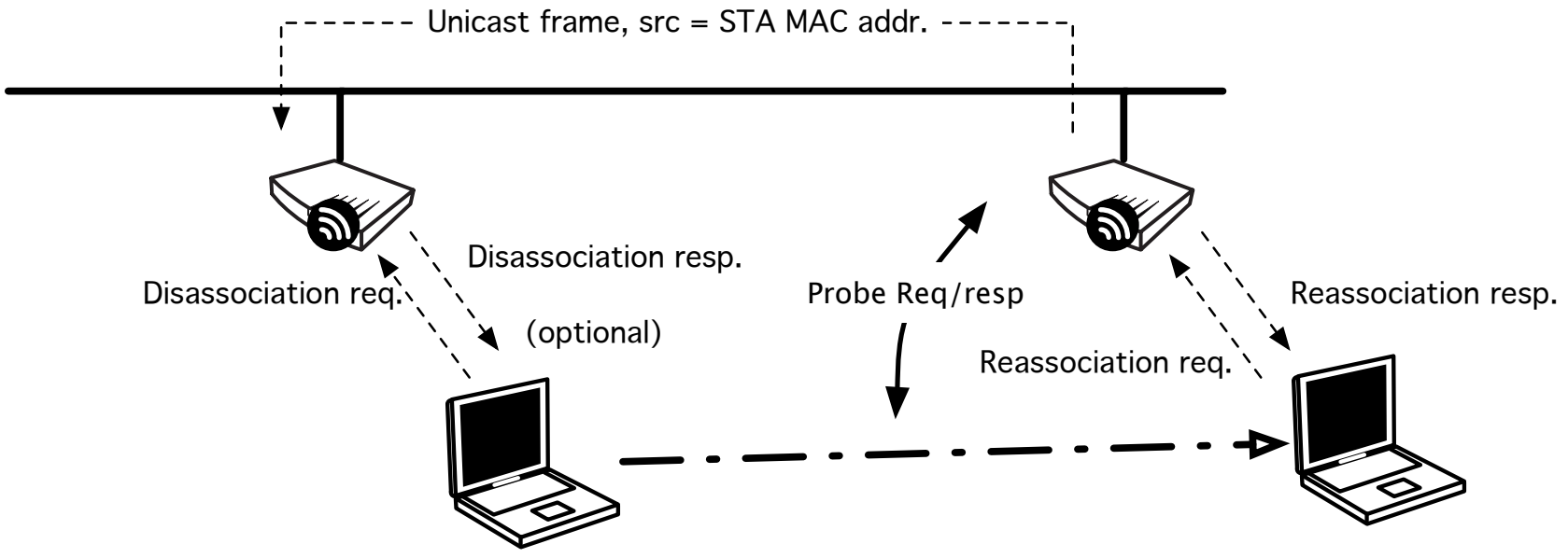
- Beacons:
  - ✓ Timestamp
  - ✓ Beacon interval
  - ✓ Capability (PCF available? Encryption required?)
  - ✓ SSID (up to 32 bytes)
  - ✓ Required rates
- Probe requests, response
- Association requests/responses

1. On top of the "usual" IP-world management frames (ICMP, ARP), there is quite a bit of 802.11 frame exchanges to allow
   - hosts to learn what networks are available, and if they have a chance to enter it (if they match the requirements)(Probes, beacons)
   - The APs to learn who they should relay frames for (that's the associated hosts)! (Association frames)

Roaming

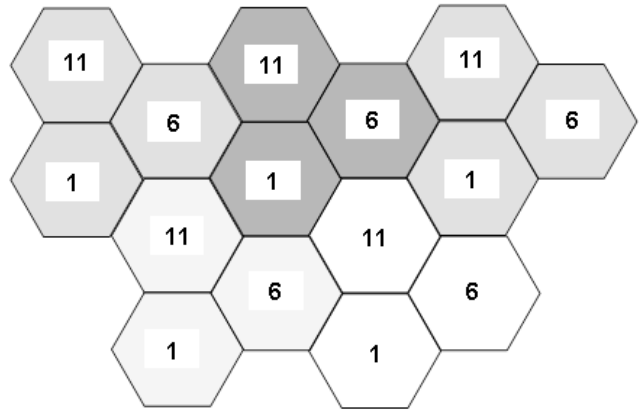
- Clients need to scan other channels (maybe helped by current AP) ← they have to leave the channel for some time. (Can also leave for good and then scan)
  - ✓ The client can declare that it's going into power save mode…
- Active (probe request) or passive scanning
- Reassociation handshake (contains address of former AP)
- Frame sent on the DS to update switch tables

Roaming (cont.)

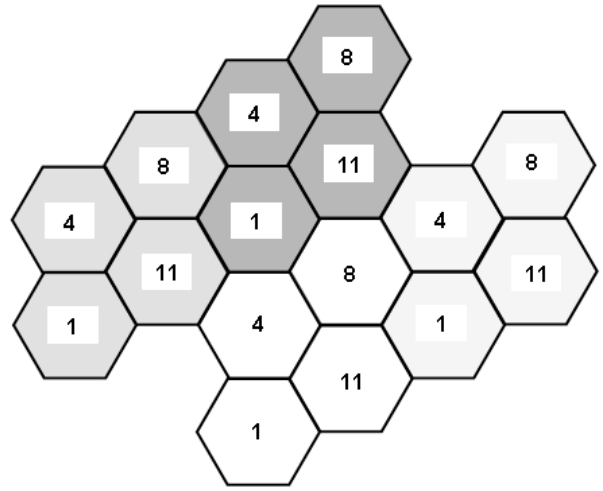


Infrastructure network planning

- If the access points do not hear each other, it does not mean the cells are disjoint!
- Paving with 3 channels:



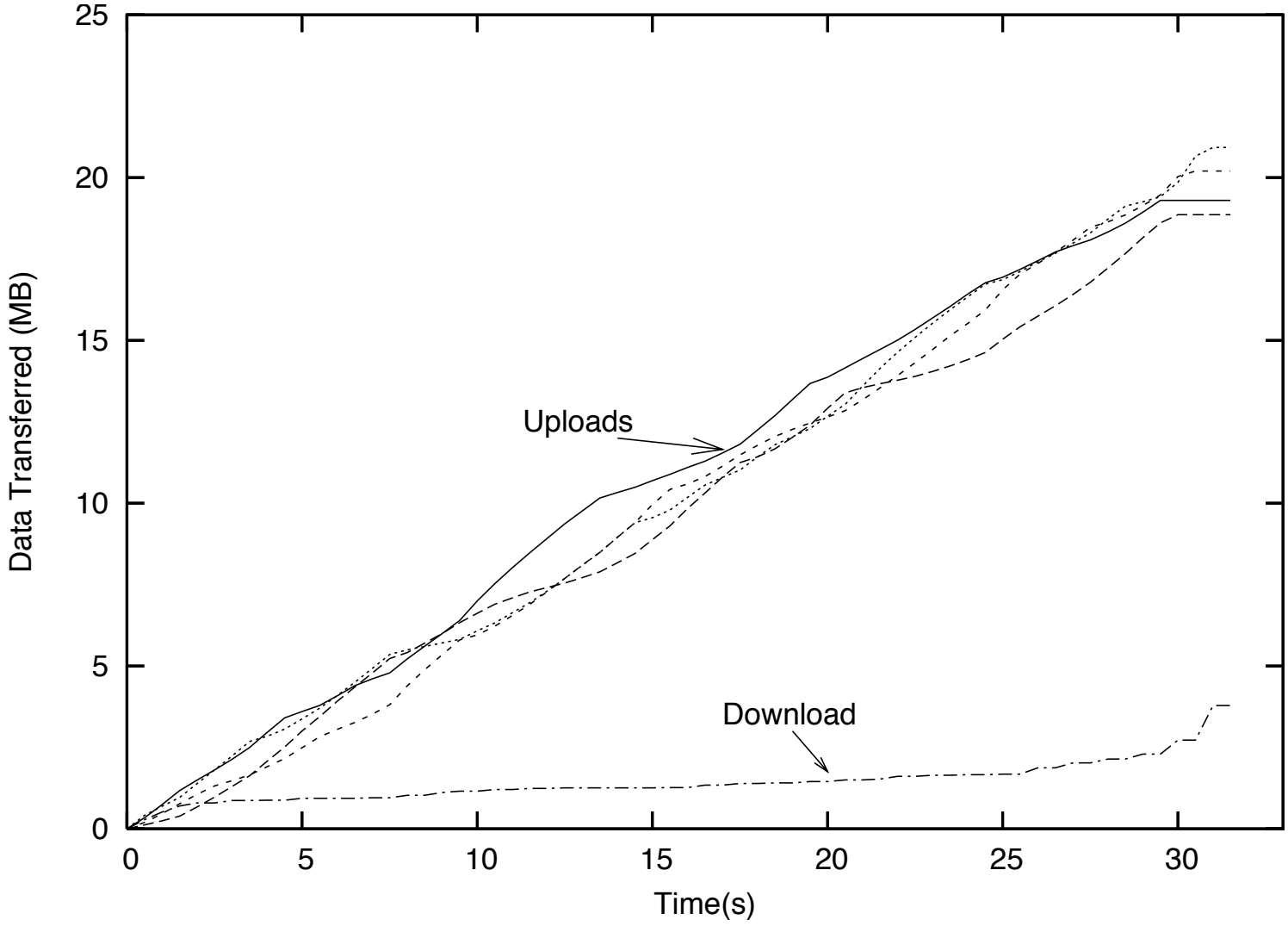
- Paving with 4 channels:



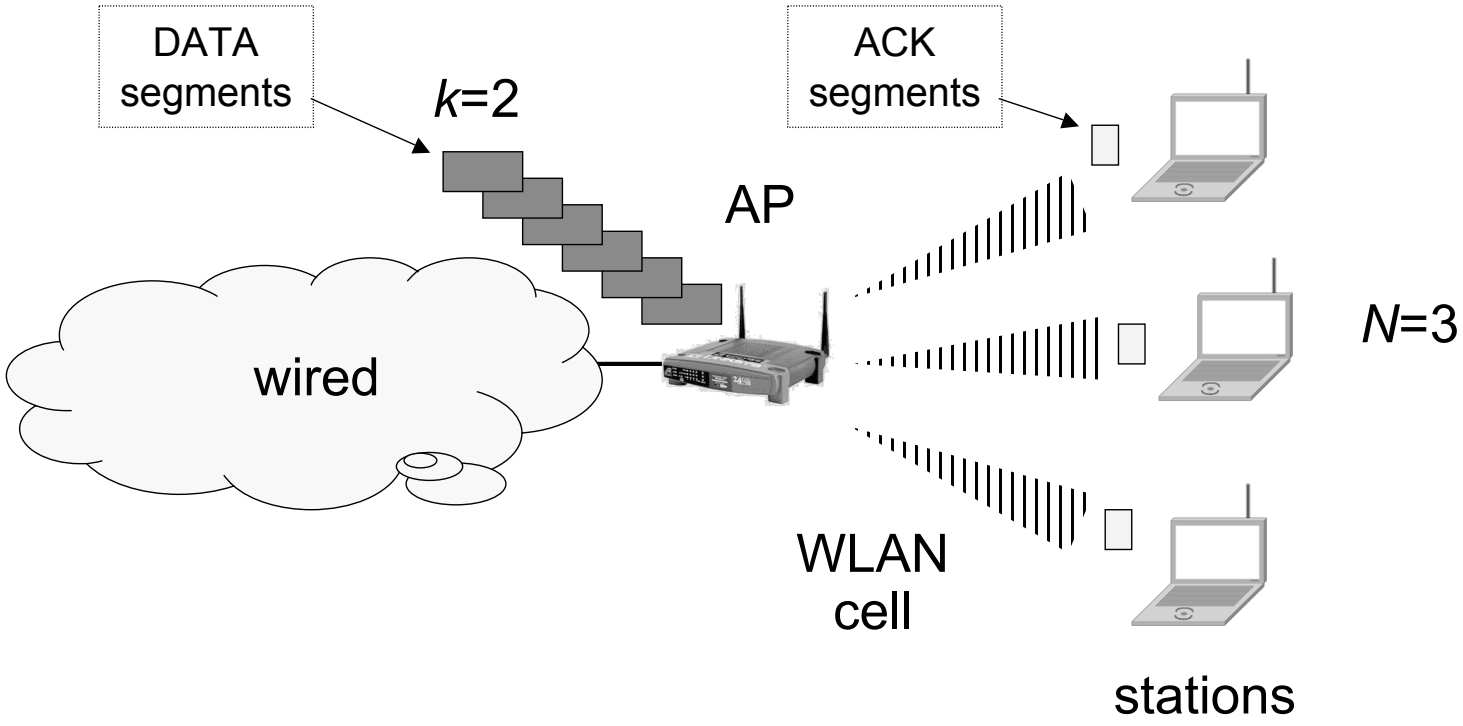
One problem in a multirate cell ("Performance anomaly")

- All stations access the network with same probability
- So in time T, they will all send approx. the same number of frames
- If one of them transmit at 1Mb/s, everybody gets only a fraction of this

Another problem: TCP over WLAN



Another problem: TCP over WLAN (cont.)

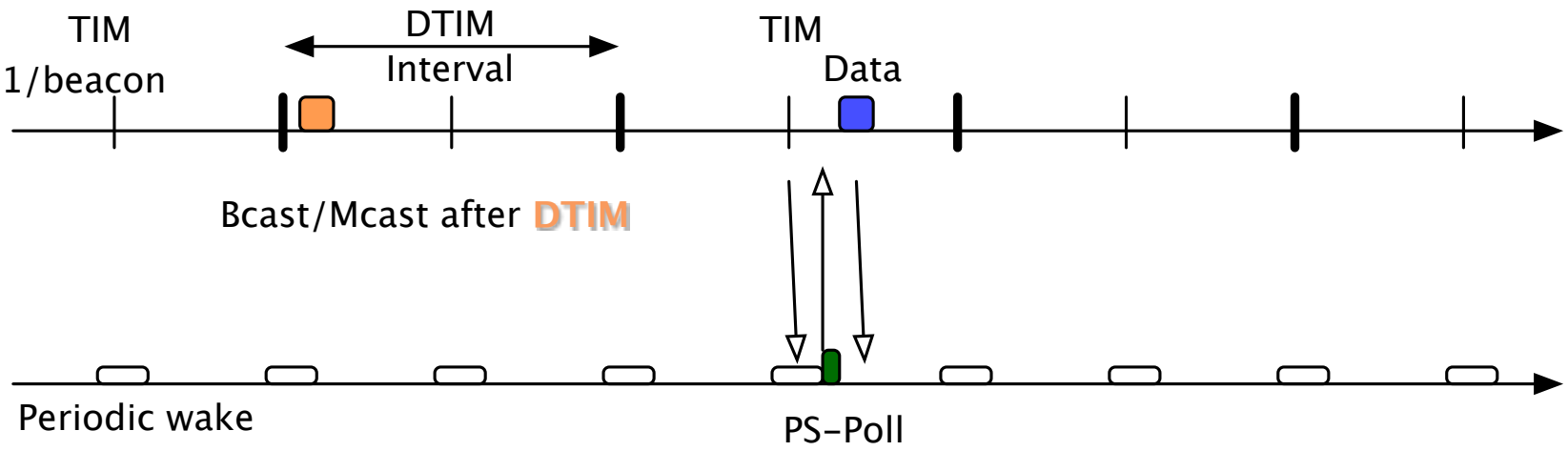


Solutions?

- PCF
- 802.11e
- Another access method?
- Uplink-aware queueing

Power save

- TIM: Traffic Indication Message
  - ✓ TIM is in the beacon
  - ✓ TIM period > beacon period
    (Otherwise STAs have to wake up for each beacon)
- AP buffers **broadcast** frames until next DTIM



Power save (cont.)