Wireless

Wireless

- Wireless networking evolved dramatically over the last 15 years. We have:
  - Mobile telephony (W-CDMA, GSM, LTE (Long Term Evolution Standard, 3GPP (3th Generation Partnership Project) Release 10)
  - WiFi (wireless fidelity)
  - Bluetooth
  - etc (infrared devices, remote control)

Wireless

- **Characteristic problem**: How can the different stations which are transmitting be differentiated, and how can they together share a communication medium?
- The problem is even harder when stations move in or out a certain region (mobile). Think of:
  - Using the internet on the auto-bahn
  - Using the internet at a hotspot

Wireless

- Hotspots in cities in the US are partly created by using “old fashioned” telephone booths!
  - Have coverage and already connected to a network.
- Characteristic problem solved by several techniques.

1 CDMA

- Code Division Multiple Access
- Used in cellular networks (mobile phone) and hotspots.
- Assumption: The transmitting frequency is much higher than the bit rate.
- The quotient of "transmitting freq" over "bit rate" is called the "chip rate".

(Synchronous) CDMA

- Each bit can therefore be represented by a <u>sequence</u> of signals, say M.
- PSK (phase shift keying) followed by PM (phase modulation)
- E.g. M = 8

1	1	1	1		1			
				-1		-1	-1	-1
(0) -1				1		1	1	1
	-1	-1	-1		-1			

the code $C_1 \ldots C_M$

(Synchronous) CDMA

Now, each bit to be transmitted is encoded by:

For $1 \leq m \leq M$: $Z_{i,m} = d_i \, c_m$

So, if $d_1 \, d_2 \, d_3 = 1 \; 0 \; 1$ $(1 \; -1 \; 1)$, then the transmitted signal is:

1	1	1		1							1		1	1	1	1	1	1		1			
			-1		-1	-1	-1	-1	-1	-1		-1							-1		-1	-1	-1

(Synchronous) CDMA

The receiving station performs:

$$d_i = \frac{1}{M}\sum_{m=1}^{M} Z_{i,m} \cdot c_m$$

Thereby recovering the original signals (d_i)

Example:

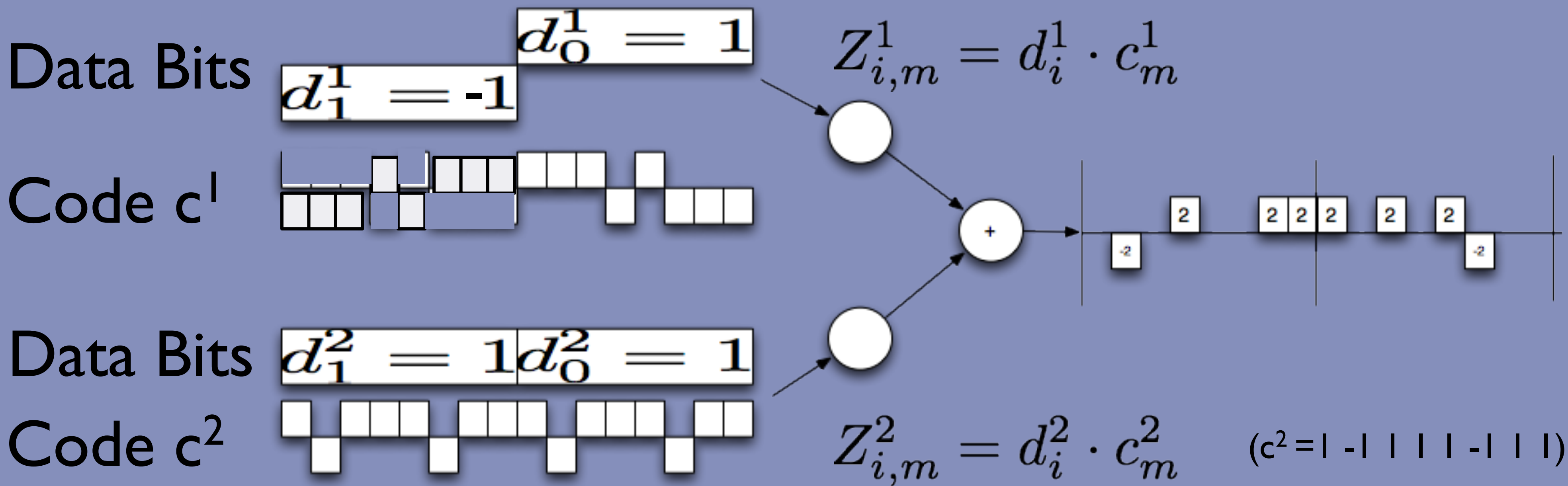
$$d_2 = \frac{1}{8}\sum_{m=1}^{8} Z_{2,m} \cdot c_m$$

$$d_2 = \frac{1}{8}(Z_{2,1} \cdot c_1 + Z_{2,2} \cdot c_2 + \ldots + Z_{2,8} \cdot c_8)$$

$$d_2 = \frac{1}{8}(-1 \cdot 1 + -1 \cdot 1 + -1 \cdot 1 + 1 \cdot -1 + -1 \cdot 1 + 1 \cdot -1 + 1 \cdot -1 + 1 \cdot -1) = \frac{1}{8}(-8) = -1$$

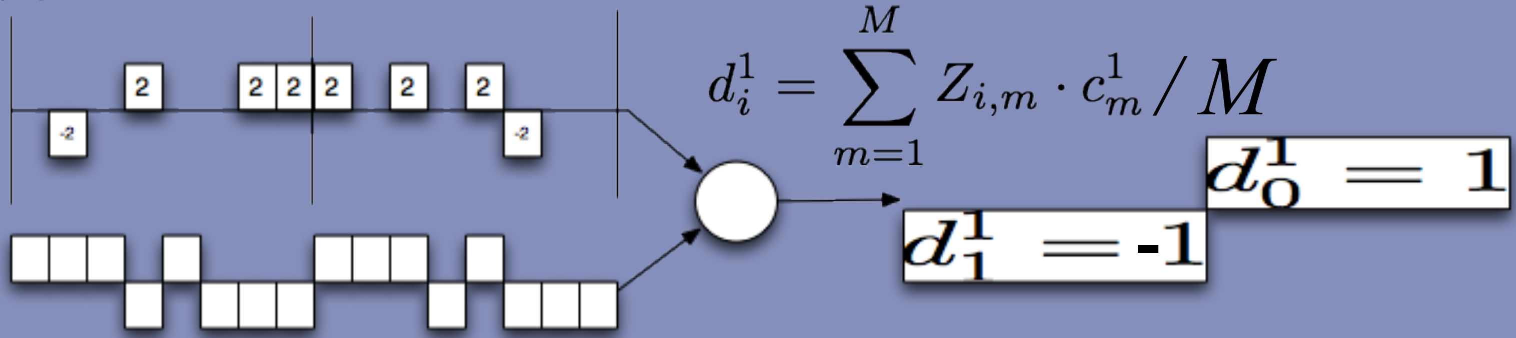
(Synchronous) CDMA

For just one transmitter this seems very stupid. However, when there are several stations transmitting, who move in and out of an area. Then each station is assigned its own code:



(Synchronous) CDMA

Receiver 1



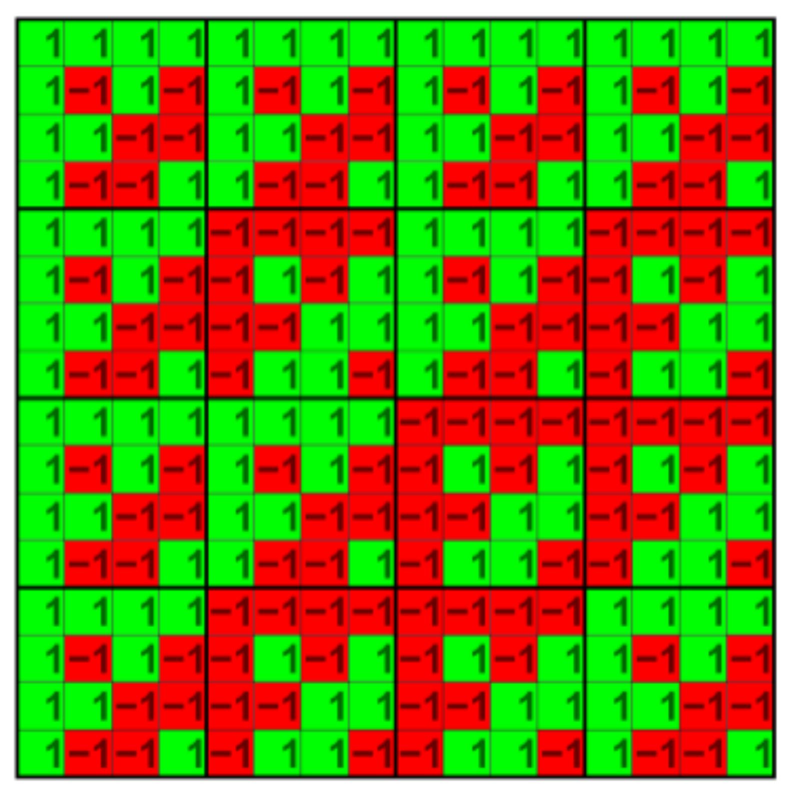
$$\frac{1\cdot 0 + 1\cdot -2 + 1\cdot 0 + -1\cdot 2 + 1\cdot 0 + -1\cdot 0 + -1\cdot 2 + -1\cdot 2}{8} = \frac{-8}{8} = -1$$

Receiver 2 is similar, but then code c^2 is used.

So, the trick is to find the right code so that this works!!!

Orthogonal Basis

In general **Walsh/Hadamar Matrices** are used for constructing the chip Codes M:



- **square matrices with dimensions of some power of 2,**
- **entries of ±1, and**
- **the dot product of any two distinct rows (or columns) is 0.**

https://en.wikipedia.org/wiki/Walsh_matrix

Recursive Definition

$$H(2^1) = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

$$H(2^2) = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix},$$

and in general

$$H(2^k) = \begin{bmatrix} H(2^{k-1}) & H(2^{k-1}) \\ H(2^{k-1}) & -H(2^{k-1}) \end{bmatrix} = H(2) \otimes H(2^{k-1}),$$

for $2 \leq k \in N$, where $\otimes$ denotes the Kronecker product.

CDMA, CDM, TDMA, FDMA

- **CDMA** can be both **synchronous** as well as **asynchronous**. Asynchronous CDMA is more flexible than synchronous CDMA.
- **CDM** is used to refer to synchronous CDMA
- **TDMA** (Time Division Multiple Access). Similar to Time Division Multiplexing. **GSM** relied on TDMA (CDMA was not available yet). In the US, where mobile telephony was commercially available at a later time CDMA was adopted (more flexible).
- **FDMA** (Frequency Division Multiple Access). Used commonly in Satellite Communication.

GSM: Global System for Mobile Communications

Spread Spectrum characteristics of (Asynchronous) CDMA

Asynchronous and synchronous CDMA both used chip codes. Asynchronous uses **pseudorandom** sequences of chips, which are **not synchronized** and spread over a **range of (changing) frequencies**. The receiver perceives the signals of other codes as a noise signal which can be filtered out.

Asynchronous CDMA is ideally suited to a mobile network where large numbers of transmitters each generate a relatively small amount of traffic at irregular intervals.

Overview of the different mobile phone standards

Feature	NMT	GSM	UMTS (3GSM)	IS-95 (CDMA one)	IS-2000 (CDMA 2000)	LTE
Technology	FDMA	TDMA and FDMA	W-CDMA	CDMA	CDMA	OFDMA
Generation	1G	2G	3G	2G	3G	4G
Encoding	Analog	Digital	Digital	Digital	Digital	Digital
Year of First Use	1981	1991	2001	1995	2000 / 2002	2009
Roaming	Nordics and several other European countries	Worldwide, all countries except Japan and South Korea	Worldwide	Limited	Limited	Limited
Handset interoperability	None	SIM card	SIM card	None	RUIM (rarely used)	SIM card
Common Interference	None	Some electronics, e.g. amplifiers	None	None	None	None
Signal quality/coverage area	Good coverage due to low frequencies	Good coverage indoors on 850/900 MHz. Repeaters possible. 35 km hard limit.	Smaller cells and lower indoors coverage on 2100 MHz; equivalent coverage indoors and superior range to GSM on 850/900 MHz.	Unlimited cell size, low transmitter power permits large cells	Unlimited cell size, low transmitter power permits large cells	
Frequency utilization/Call density	Very low density	0.2 MHz = 8 timeslots. Each timeslot can hold up to 2 calls (4 calls with VAMOS) through interleaving.	5 MHz = 2 Mbit/s. 42Mbit/s for HSPA+. Each call uses 1.8-12 kbit/s depending on chosen quality and audio complexity.	Lower than CDMA-2000?	1.228 MHz = 3Mbit/s	
Handoff	Hard	Hard	Soft	Soft	Soft	Hard
Voice and Data at the same time	No	Yes GPRS Class A	Yes[2]	No	No EVDO / Yes SVDO[3]	No (data only) Voice possible through VoLTE or fallback to 2G/3G

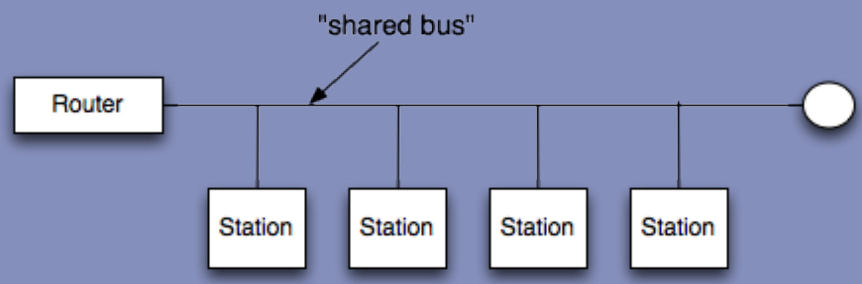
https://en.wikipedia.org/wiki/Comparison_of_mobile_phone_standards

II. CSMA/CD

Carrier Sensed Multiple Access / Collision Detection

Developed as part of the IEEE 802 standard for Ethernet & Fast Ethernet LANs (802.3).

The shared medium in the early versions of the Internet were the COAX cable.



CSMA/CD

- Random Access: each station can send arbitrarily (However, the configuration is much more stationary in contrast to CDMA)
- Based on ALOHA technique for radio transmission:
  - Station sends a frame, then waits for acknowledgement (round trip propagation delay + fix time increment)
  - If multiple senders are active at the same time, then collision & receiver discards frames.
    - Leads to 17-37% efficiency rate of the medium.

CSMA/CD

1. If medium is idle ("carrier sensed"), then transmit. (CSMA)
2. If medium is busy, then listen until medium is idle, then retransmit. (CSMA)
3. If collision is detected <u>during</u> transmission, then send jamming signal to all stations and stop transmission. (CSMA/CD)
4. Wait random amount of time and go to 1. (CSMA/CD)

CSMA/CD **Randomisation**

After a collision, the time is divided in a number of **time slots**, based on the length of the worst case round trip propagation time.

Binary Exponential Backoff

- After first collision (jamming), each station waits **0** or **1** time slot.
- After **2** collisions, each station waits 0,1,2 or 3 time slots.
- After **3** collisions, each station waits, 0,1,2,3,4,...,7 time slots, etc ($0,1,\ldots,2^i-1$).
- After **10** collisions randomisation is frozen on 1024 slots
- After **16** collisions, failure reported.

IEEE 802.3 Ethernet LAN standard

- Differentiates between:
  - Physical layer
  - Medium Access Control
  - Logical Link Control
    - Unacknowledged connection less service
    - Connection mode services
    - Acknowledged connection less services

Frame Format

The frame format of IEEE 802 is based on the MAC (Media Access Control) format

7	1	2/6	2/6	2	>0	>0	4
Preamble	SFD	DA	SA	length	LLC data	pad	FCS

- Preamble: 010101... meant for syncing of clocks
- SFD: Start Frame Delimiter: 10101011
- DA/SA: Destination/Source address (the MAC address)
- length: length of the LLC field
- LLC: Logic Link Control data.
- pad: padding
- FCS: CRC-32 of all fields except preamble, SFD & FCS

III. CSMA/CA

CA: **Collision Avoidance**

IEEE	Freq Range	Data Rate
802.11b	2.4-2.485 GHz	≤11 Mbps
802.11a	5.1-5.8 GHz	≤54 Mbps
802.11g	2.4-2.485 GHz	≤54 Mbps

WiFi is based on CSMA/CA

Main difference with, say Ethernet is Collision **Avoidance** vs Collision **Detection**.

CSMA/CA

- Tradeoffs between **CA** and **CD**
  - In order to detect collisions, senders must also be able to **send and receive at the same time**. Because of signal weakness, it is very **costly** to build hardware.
  - Because senders can be shielded off, **not all collisions** can be detected.

CSMA/CA

WiFi

- As soon as a sender starts transmitting a frame, it will send the whole frame.
- So, collisions will have to be avoided at all costs.

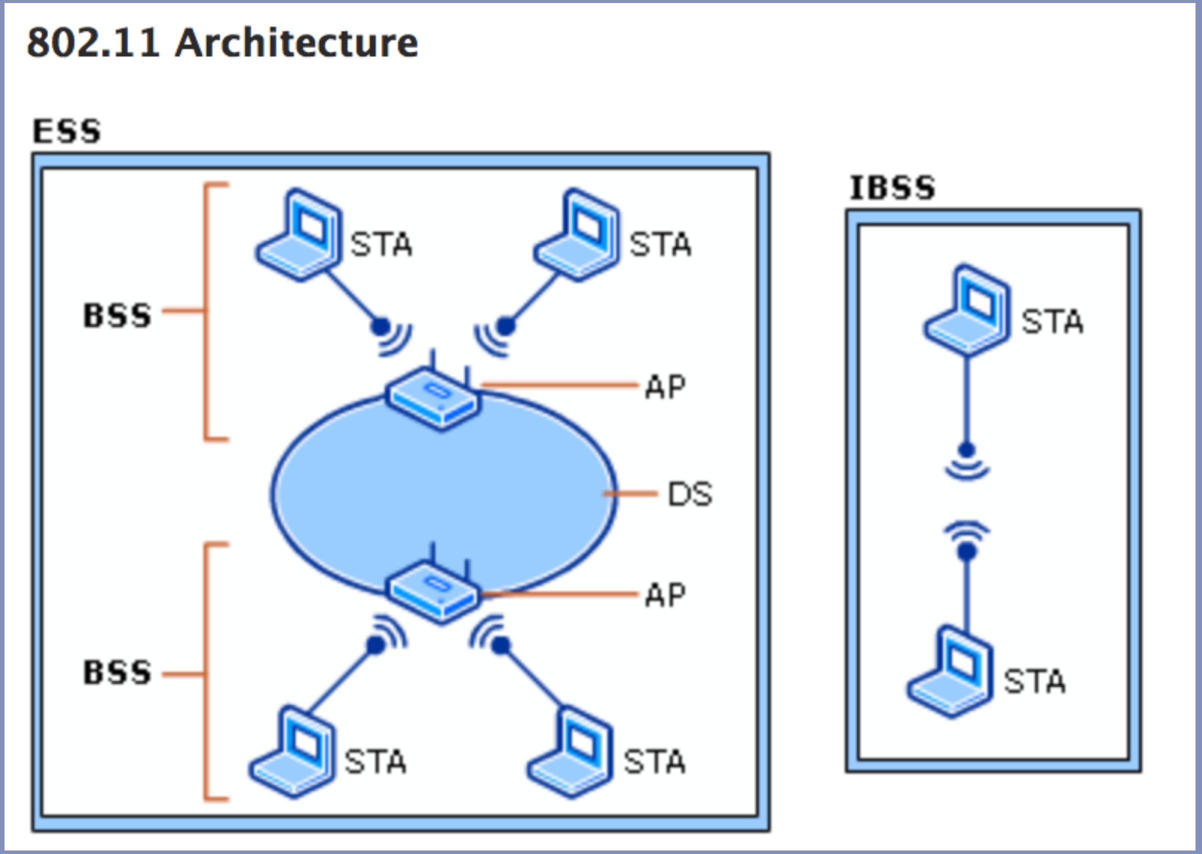
CSMA/CA

- Based on: Short Inter Frame Spacing (**SIFS**)
- Stop and Wait ARQ
  - When the destination station receives a frame & it passes CRC, then it waits a short time (**SIFS**), before it sends an **ACK** frame.
  - If sender does not receive **ACK**, then it will do a retransmit.

CSMA/CA

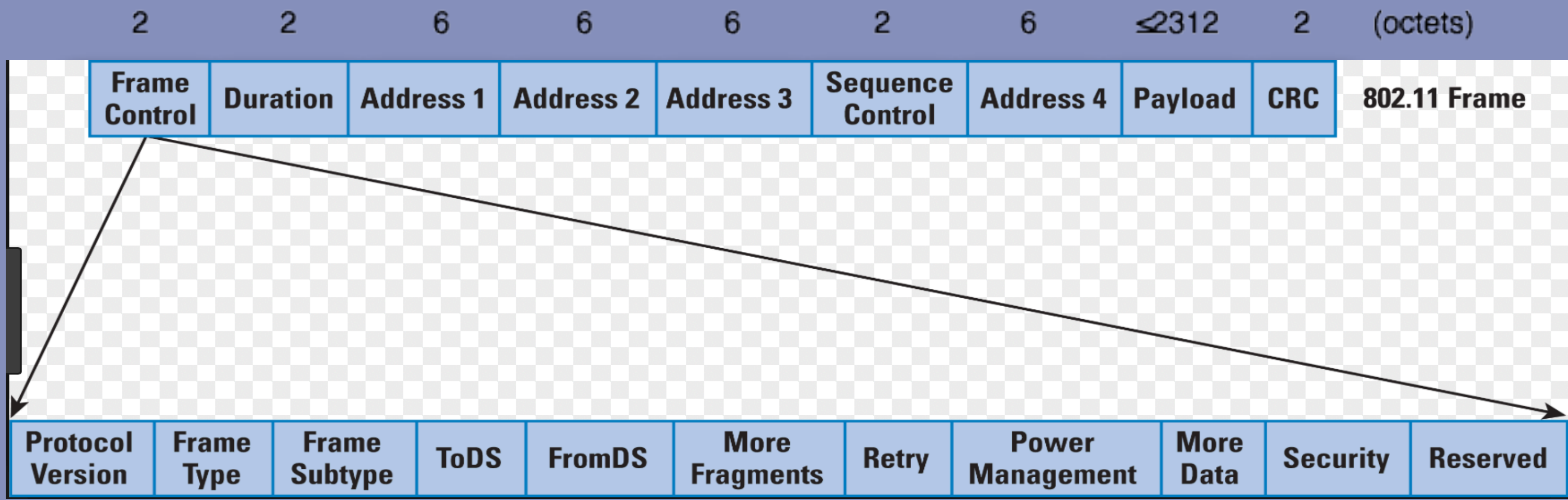
1. If station senses channel to be **idle** then:
   1. Wait a short period of time: **Distributed Inter Frame Space** (**DIFS**)
   2. Transmit frame
2. If channel is **not idle**:
   1. Choose a **random back off value.** Count down this value.
   2. If counter reaches 0, then transmit & wait for **ACK**.
3. If **ACK** is received, then **goto 1**, otherwise **goto 2** (with larger count down value)

IEEE 802.11 WiFi Standard



station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS)

IEEE 802.11 WiFi Frame Format



DS = Distribution System,
WEP = Wired Equivalent Privacy (obsolete, replaced by WPA(2))

Based on 802, but clearly different in number of addresses.

- **Protocol Version** provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported.
- **Type and Subtype** determines the function of the frame. There are three different frame type fields: control, data, and management. There are multiple subtype fields for each frame type . Each subtype determines the specific function to perform for its associated frame type.
- **To DS and From DS** indicates whether the frame is going to or exiting from the DS (distributed system), and is only used in data type frames of STAs associated with an AP.
- **More Fragments** indicates whether more fragments of the frame, either data or management type, are to follow.
- **Retry** indicates whether or not the frame, for either data or management frame types, is being retransmitted.
- **Power Management** indicates whether the sending STA is in active mode or power-save mode.
- **More Data** indicates to a STA in power-save mode that the AP has more frames to send. It is also used for APs to indicate that additional broadcast/multicast frames are to follow.
- **WEP** indicates whether or not encryption and authentication are used in the frame. It can be set for all data frames and management frames, which have the subtype set to authentication.
- **Order** indicates that all received data frames must be processed in order.

Duration/Connection ID: If used as a duration field, indicates the time (in microseconds) the channel will be allocated for successful transmission of a MAC frame. In some control frames, this field contains an association, or connection, identifier.

HEX Dump of a captured WiFi Frame

Frame Control: Data frame, from STA to DS (to AP)

Duration

Receiver address (MAC of AP)

Transmitter address (MAC of source STA)

Destination address (MAC of dest. STA)

Sequence control

```
08 01 30 00 e4 ce 8f 66 b2 42 e4 ce 8f 5b a1 f6
e4 ce 8f 5a 0c 5e f0 00 aa aa 03 00 00 00 08 00
45 00 00 37 59 33 40 00 40 06 60 1a c0 a8 00 10
c0 a8 00 13 e0 1c 11 5c f4 6d 68 b2 cf a7 ee 49
80 18 00 e5 2d eb 00 00 01 01 08 0a 00 00 33 f5
00 00 33 85 48 69 0a
```

Frame body

bijbehorende ACK

Frame Control: Control frame type, ACK subtype

Duration

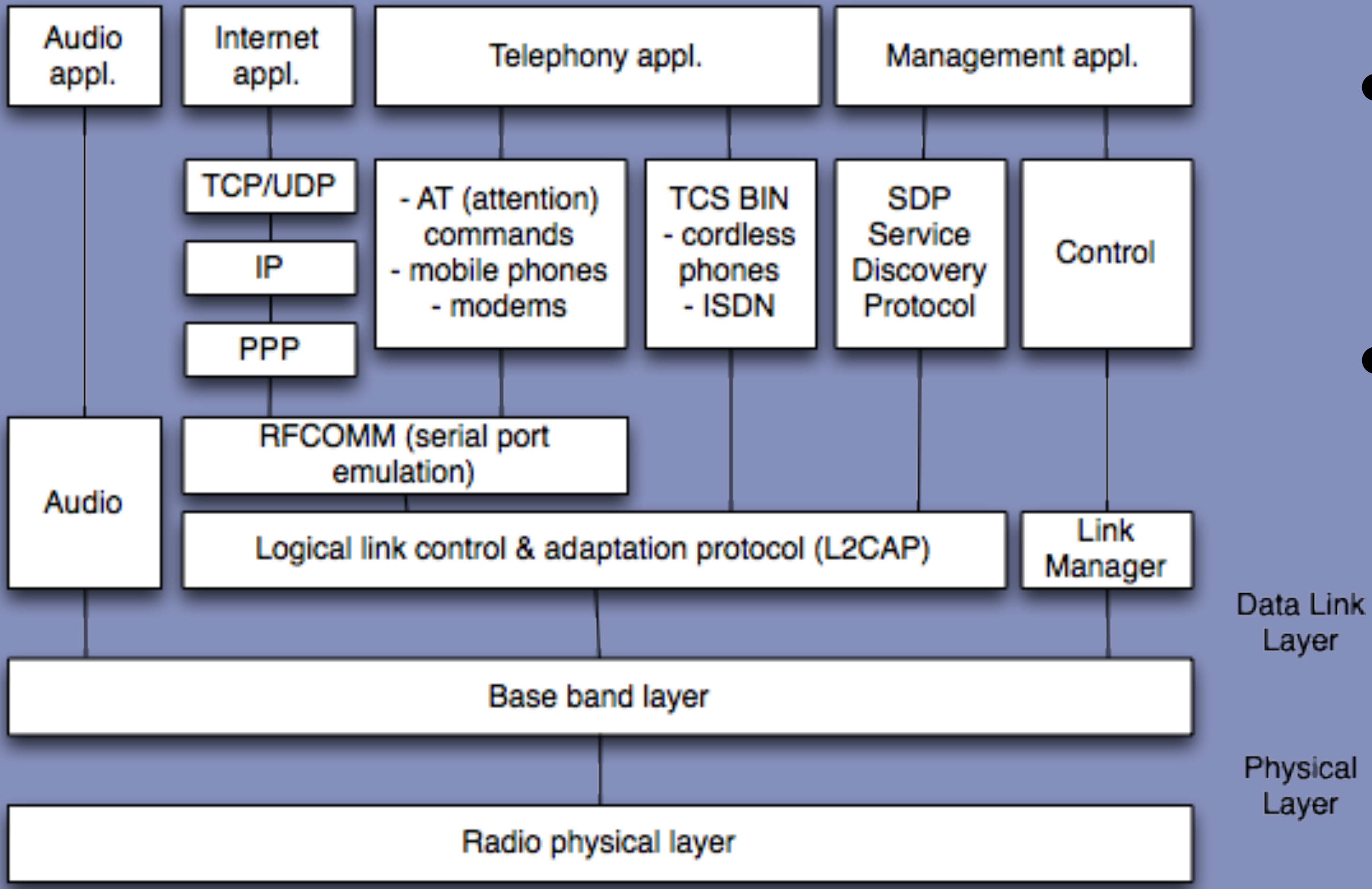
Receiver address (TX MAC of frame that is being acknowledged)

```
d4 00 00 00 e4 ce 8f 5b a1 f6
```

WiFi Address Fields

- Address 1: **MAC** address of **receiving** station.
- Address 2: **MAC** address of **transmitting** station.
- Address 3: **MAC** address of **router interface** to other subnets.
- Address 4: For ***ad hoc*** networks.

IV. Bluetooth



- RFCOMM: Radio freq communication
- TCS BIN: Telephony control protocol specification (binary)

Bluetooth

- Industrial standard!! So a whole range of application profiles are also part of the standard.
- Based on short range radio transmission arranged in WPAN (Wireless Personal Area Networks)