Computer Networking

More on Wi-Fi & Wi-Fi as a sensor

Lecturers: Antonio Carzaniga
Silvia Santini

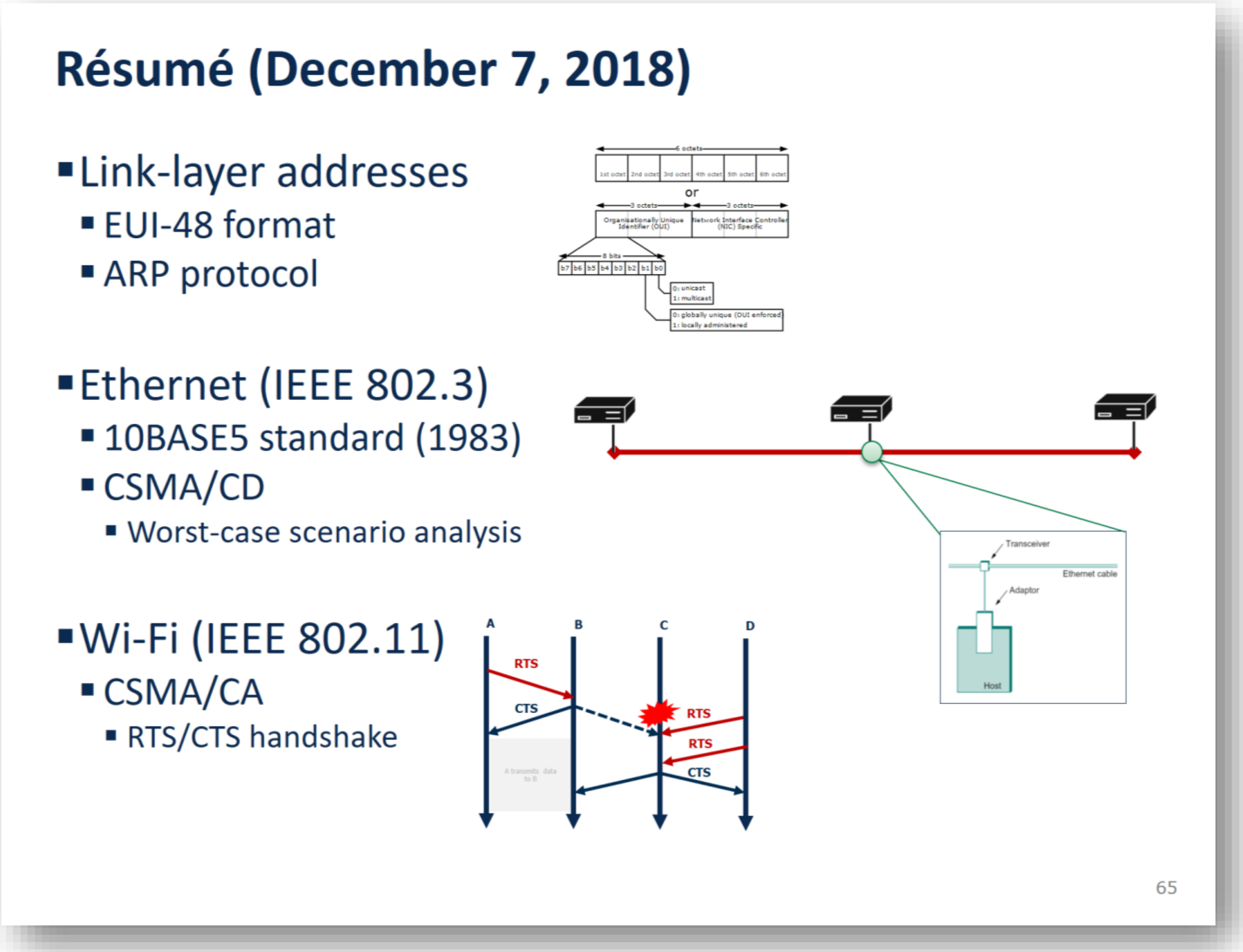
Assistants: Ali Fattaholmanan
Theodore Jepsen

USI Lugano, December 12, 2018

Changelog

- V1: December 12, 2018

Last time, on December 7, 2018…



Résumé (December 7, 2018)

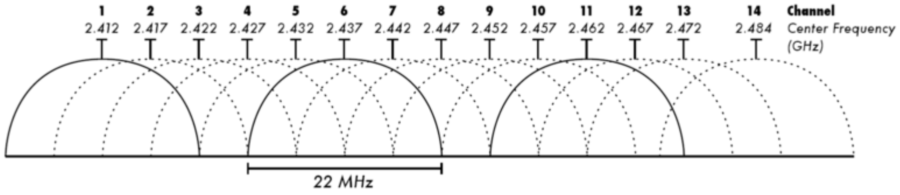
- Link-layer addresses
  - EUI-48 format
  - ARP protocol
- Ethernet (IEEE 802.3)
  - 10BASE5 standard (1983)
  - CSMA/CD
    - Worst-case scenario analysis
- Wi-Fi (IEEE 802.11)
  - CSMA/CA
    - RTS/CTS handshake

65

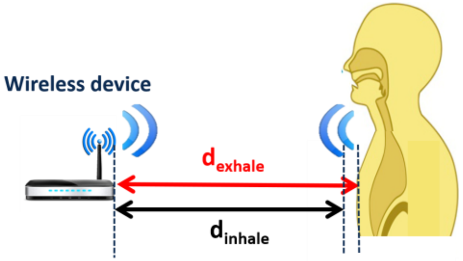
What about today?

- More on Wi-Fi
  - Wi-Fi beaconing
  - Wi-Fi frame format

- Wi-Fi as a sensor
  - Localization
  - Vital signs sensing



6
15
5
4
3
4
11
9
12
10
Real position

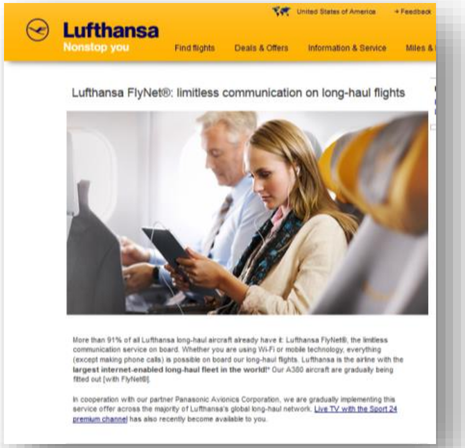


Wi-Fi beaconing

Image source: https://economictimes.indiatimes.com/magazines/panache/struggling-with-poor-wifi-signal-here-are-simple-ways-to-improve-coverage/articleshow/58822296.cms

Wi-Fi access point

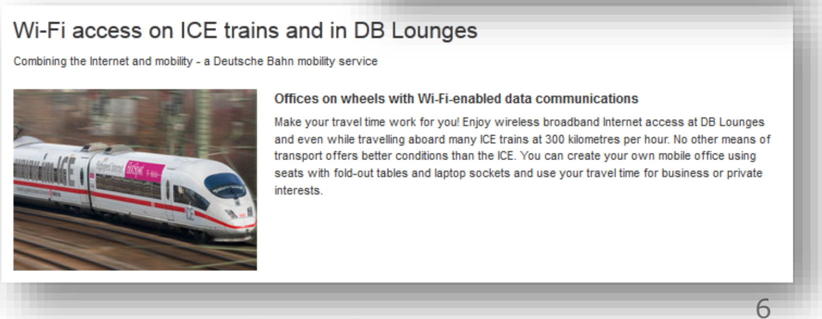
- A Wi-Fi access point is a Wi-Fi certified device that provides wireless connectivity
- A Wi-Fi access point acts as a gateway to other (wireless or wired) networks
  - Typically provides access to the Internet
- Most Wi-Fi access points are still static (fixed to the walls at home or in a bar)
  - But they can also be mobile



Lufthansa FlyNet®: limitless communication on long-haul flights

More than 91% of all Lufthansa long-haul aircraft already have it: Lufthansa FlyNet®, the limitless communication service on board. Whether you are using Wi-Fi or mobile technology, everything (except making phone calls) is possible on board our long-haul flights. Lufthansa is the airline with the **largest internet-enabled long-haul fleet in the world!*** Our A380 aircraft are gradually being fitted out [with FlyNet®].

In cooperation with our partner Panasonic Avionics Corporation, we are gradually implementing this service offer across the majority of Lufthansa's global long-haul network. Live TV with the Sport 24 premium channel has also recently become available to you.



Wi-Fi access on ICE trains and in DB Lounges

Combining the Internet and mobility - a Deutsche Bahn mobility service

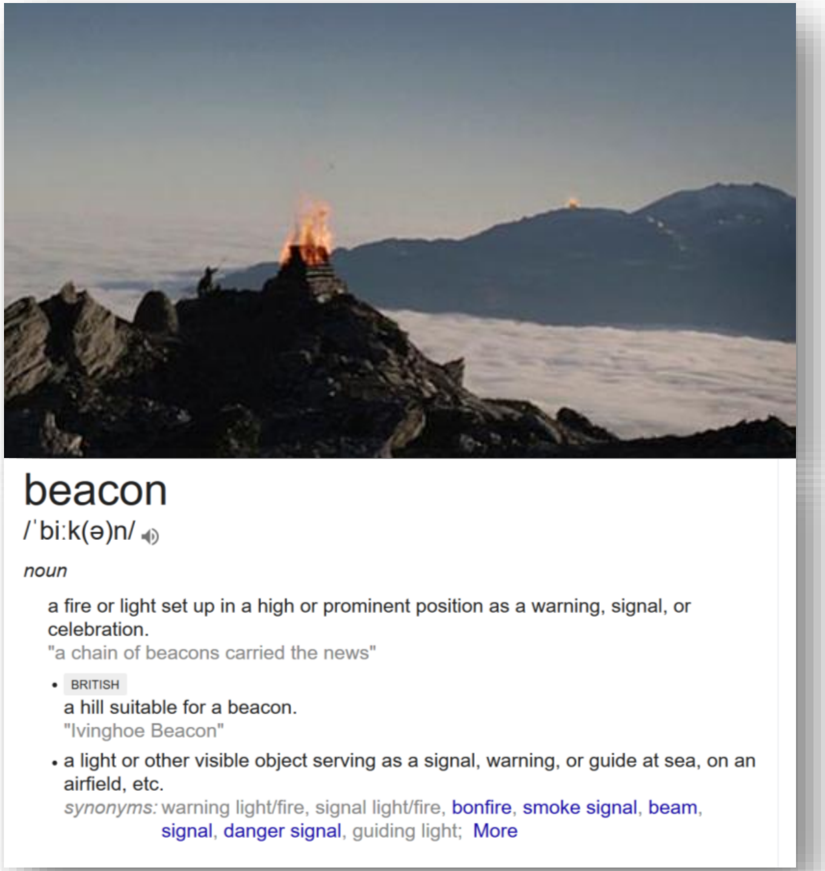
Offices on wheels with Wi-Fi-enabled data communications

Make your travel time work for you! Enjoy wireless broadband Internet access at DB Lounges and even while travelling aboard many ICE trains at 300 kilometres per hour. No other means of transport offers better conditions than the ICE. You can create your own mobile office using seats with fold-out tables and laptop sockets and use your travel time for business or private interests.

Image sources: http://www.bahn.com/i/view/GBR/en/trains/overview/wi-fi-access.shtml, http://goo.gl/jh1DLn.

IEEE 802.11: Beaconing

- **Beacons** are broadcast messages that contain information about a Wi-Fi access point
  - MAC address
  - Service Set Identifier (SSID)
  - Operation mode
  - Active channel
  - Type of encryption
  - Timestamp
  - …



beacon

/ˈbiːk(ə)n/

noun

a fire or light set up in a high or prominent position as a warning, signal, or celebration.
"a chain of beacons carried the news"

- BRITISH
  a hill suitable for a beacon.
  "Ivinghoe Beacon"
- a light or other visible object serving as a signal, warning, or guide at sea, on an airfield, etc.
  synonyms: warning light/fire, signal light/fire, bonfire, smoke signal, beam, signal, danger signal, guiding light; More

Image source: https://tobyelwin.com/this-social-media-fad-will-ruin-organization-development/

IEEE 802.11: Beaconing / Interval and channel

- Access point sends beacons at regular time intervals
  - Default: 100 time units (TU)
  - 1 TU = 1024 µs

- Each access point transmits on a specific **channel**

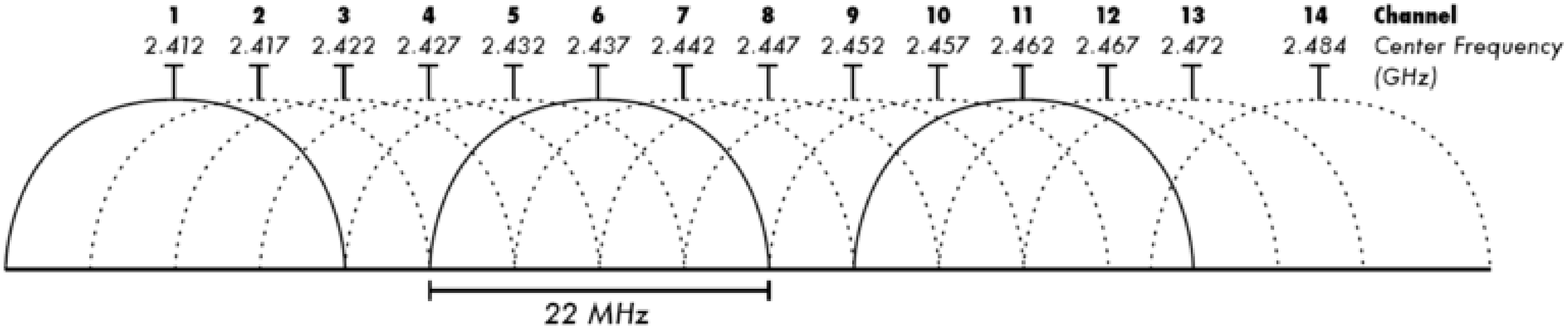
IEEE 802.11: Beaconing / Active probing

- Stations can actively probe for active access point
  - Probe Request
  - Probe Response

- Undirected probe
  - Directed to all access points

- Directed probes
  - Directed to an access point with a specific SSID
  - SSID from the local cache or entered by the user
    - Useful to, e.g., discover invisible access points
    - There are some privacy issues here (see [Pang 2007] and [Rose 2010])

IEEE 802.11: Channels (2.4 GHz, 802.11b,g)

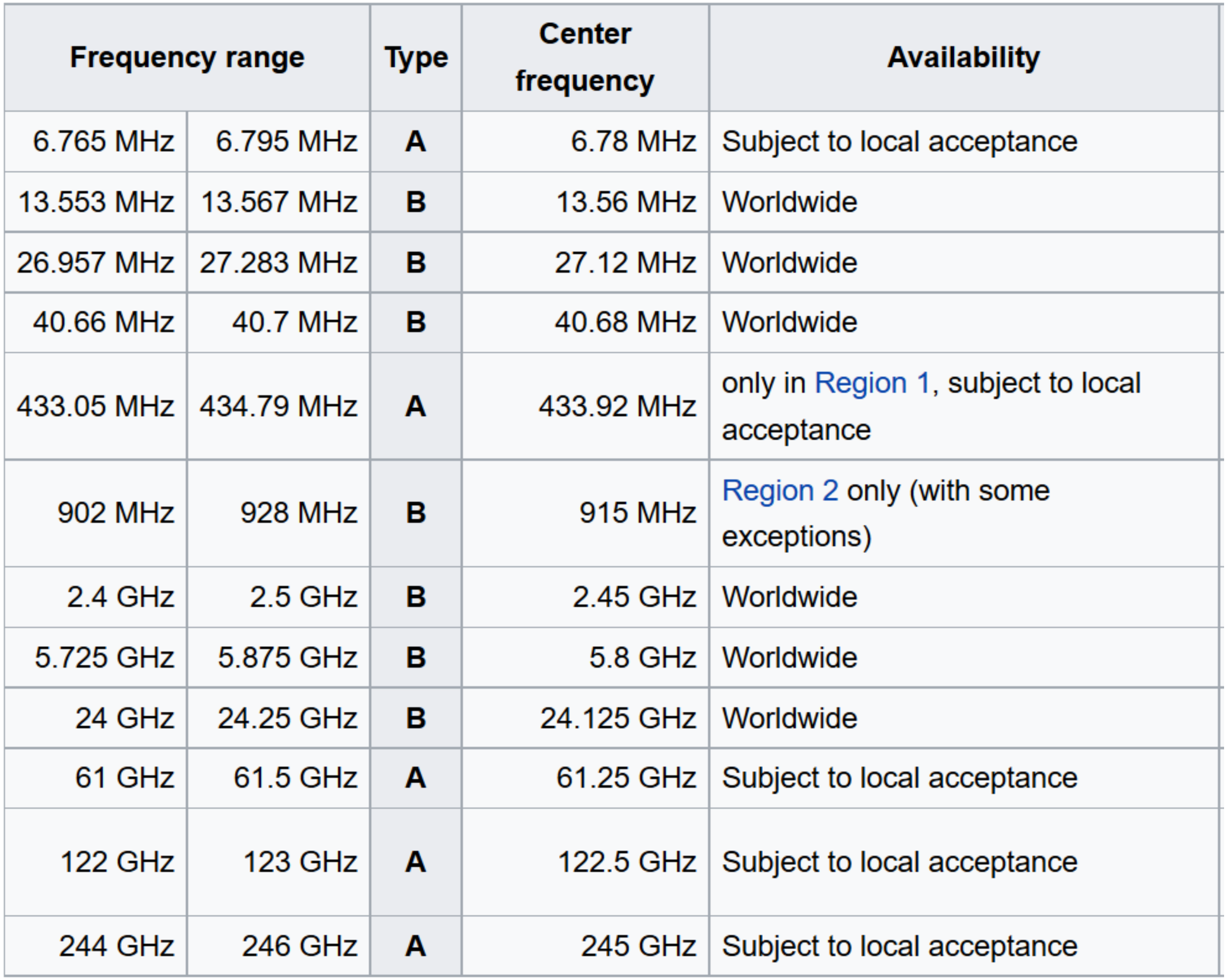


- Depending on the specific standard, IEEE 802.11 transmits in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands

- IEEE 802.11 operates in ISM bands
  - Industrial, scientific and medical (ISM) radio bands

Image source: http://en.wikipedia.org

ISM bands



Frequency range		Type	Center frequency	Availability
6.765 MHz	6.795 MHz	A	6.78 MHz	Subject to local acceptance
13.553 MHz	13.567 MHz	B	13.56 MHz	Worldwide
26.957 MHz	27.283 MHz	B	27.12 MHz	Worldwide
40.66 MHz	40.7 MHz	B	40.68 MHz	Worldwide
433.05 MHz	434.79 MHz	A	433.92 MHz	only in Region 1, subject to local acceptance
902 MHz	928 MHz	B	915 MHz	Region 2 only (with some exceptions)
2.4 GHz	2.5 GHz	B	2.45 GHz	Worldwide
5.725 GHz	5.875 GHz	B	5.8 GHz	Worldwide
24 GHz	24.25 GHz	B	24.125 GHz	Worldwide
61 GHz	61.5 GHz	A	61.25 GHz	Subject to local acceptance
122 GHz	123 GHz	A	122.5 GHz	Subject to local acceptance
244 GHz	246 GHz	A	245 GHz	Subject to local acceptance

Type A = frequency bands are designated for *ISM applications*. The use of these frequency bands for ISM applications shall be subject to special authorization by the administration concerned, in agreement with other administrations whose radio communication services might be affected. In applying this provision, administrations shall have due regard to the latest relevant ITU-R recommendations.

Type B = frequency bands are also designated for ISM applications. Radio communication services operating within these bands must accept harmful interference which may be caused by these applications.

Image source: https://en.wikipedia.org/wiki/ISM_band

The electromagnetic spectrum

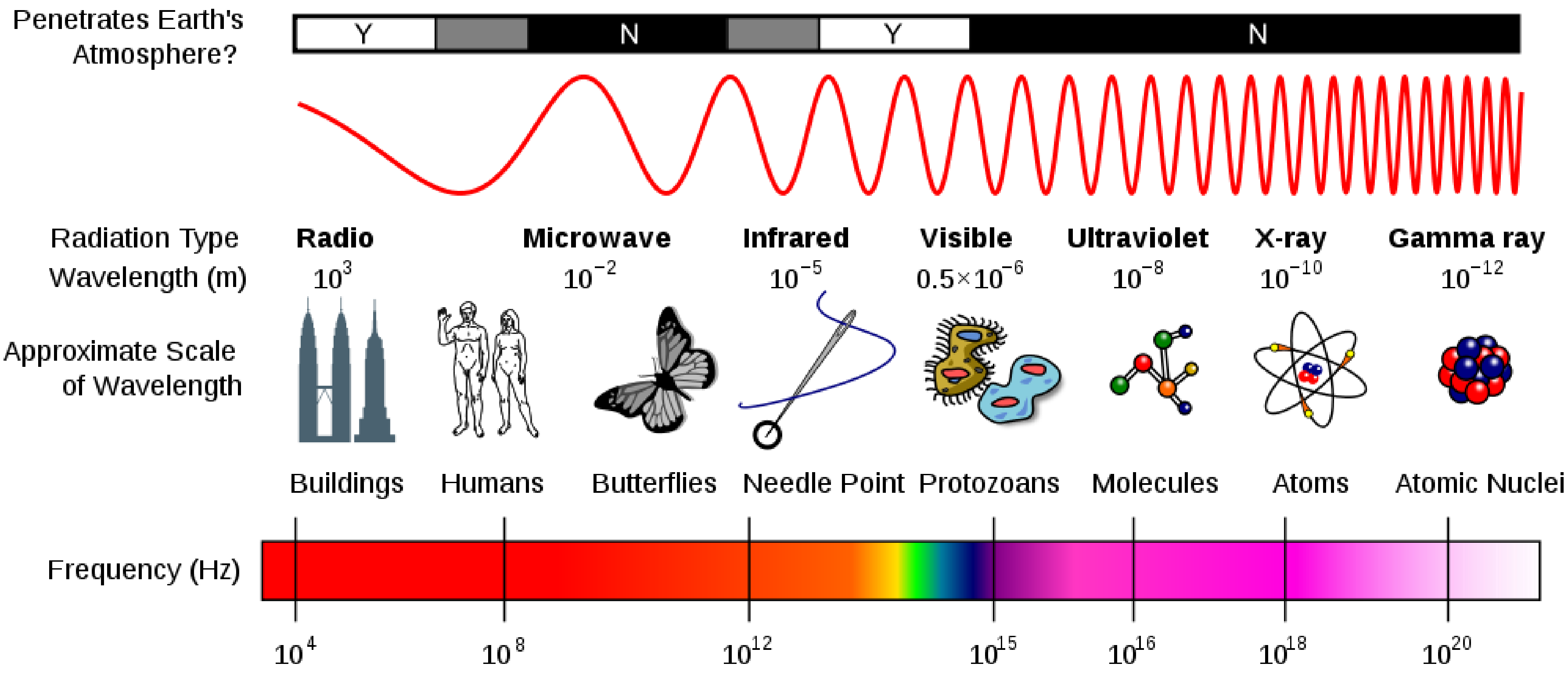
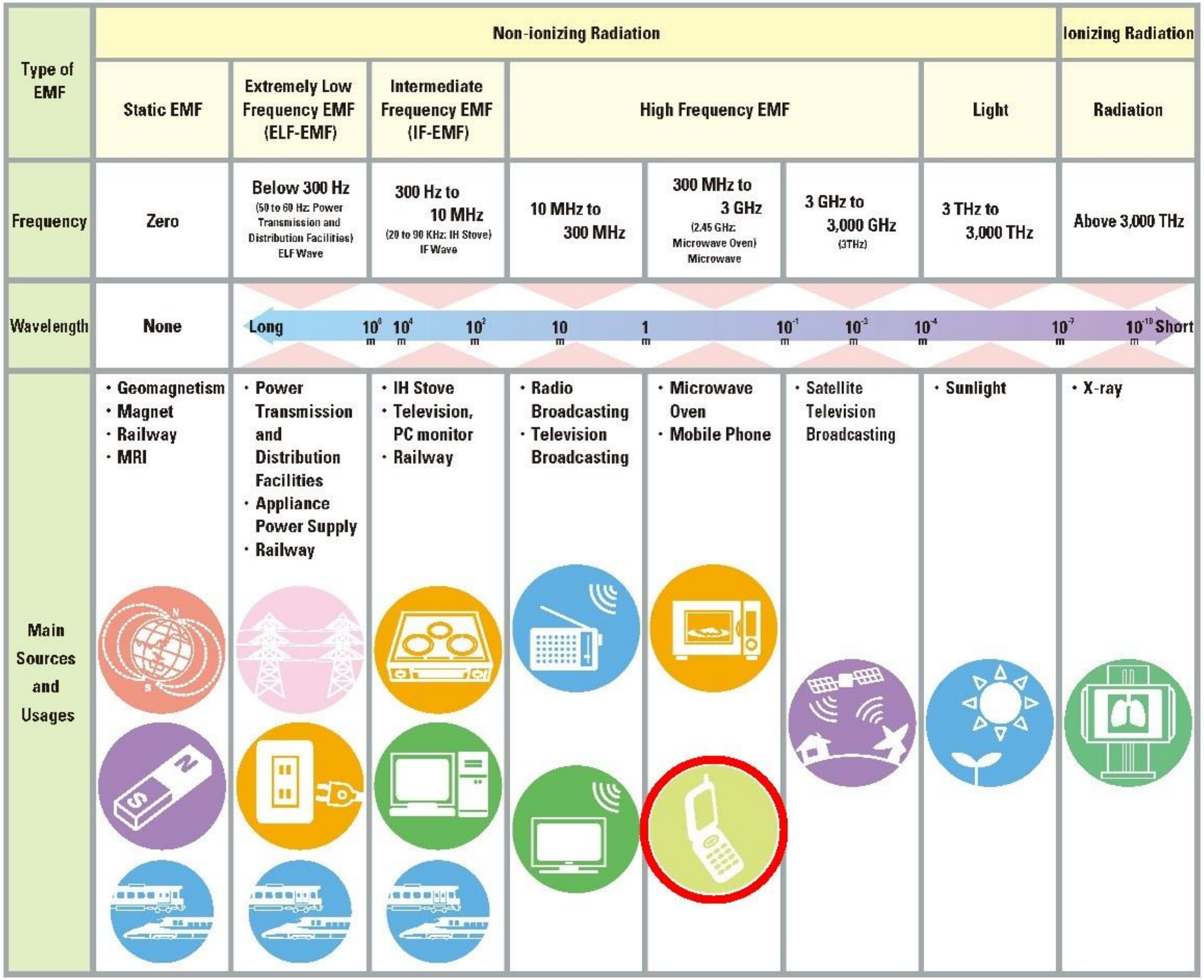


Image source: http://en.es-static.us/upl/2012/05/em_spectrum.png

The electromagnetic spectrum: Allocation

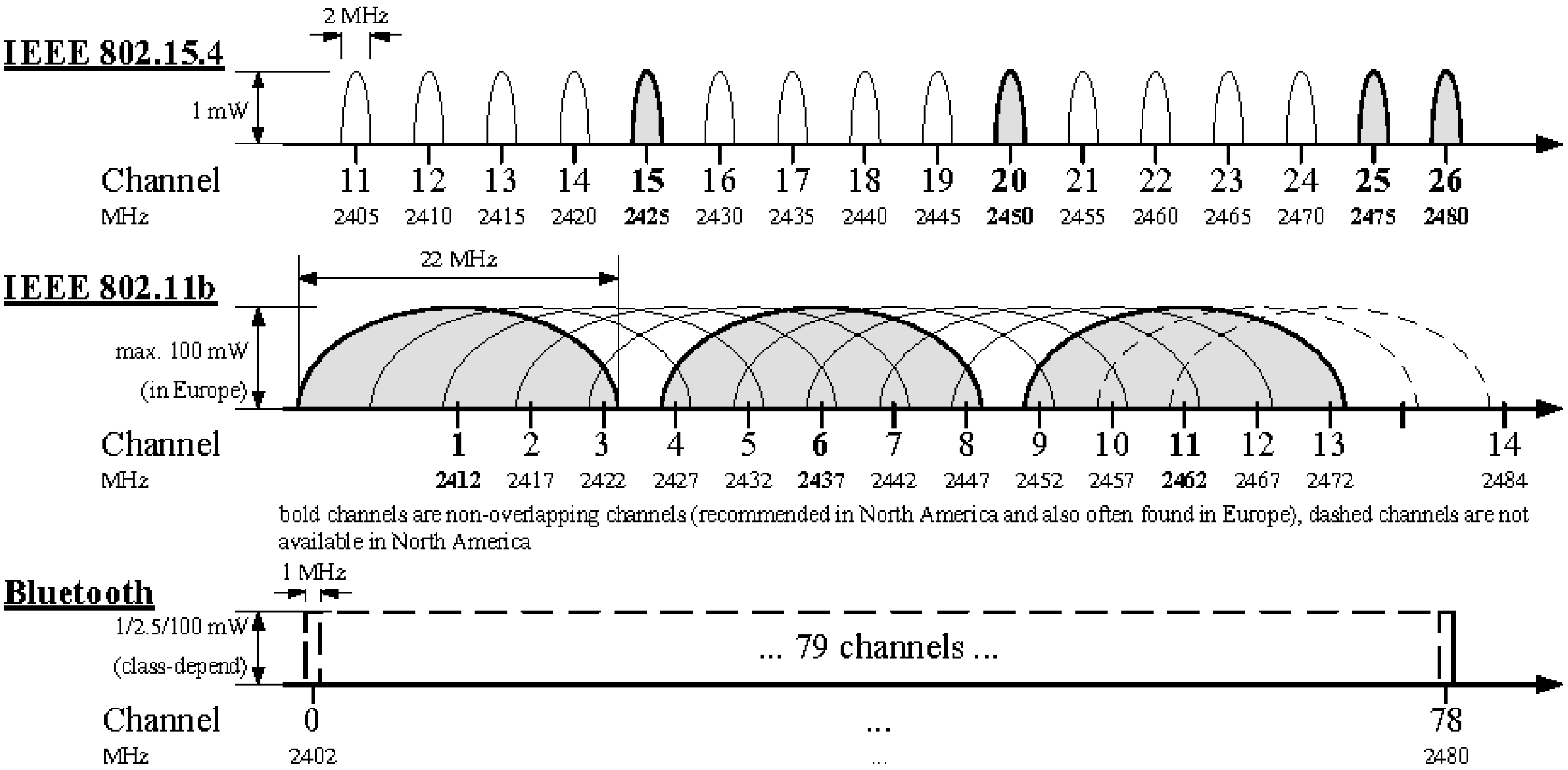


Type of EMF	Non-ionizing Radiation							Ionizing Radiation
	Static EMF	Extremely Low Frequency EMF (ELF-EMF)	Intermediate Frequency EMF (IF-EMF)	High Frequency EMF			Light	Radiation
Frequency	Zero	Below 300 Hz (50 to 60 Hz: Power Transmission and Distribution Facilities) ELF Wave	300 Hz to 10 MHz (20 to 90 KHz: IH Stove) IF Wave	10 MHz to 300 MHz	300 MHz to 3 GHz (2.45 GHz: Microwave Oven) Microwave	3 GHz to 3,000 GHz (3THz)	3 THz to 3,000 THz	Above 3,000 THz
Wavelength	None	Long 10^8 m	10^4 m 10^2 m	10 m	1 m	10^{-1} m 10^{-3} m	10^{-4} m 10^{-7} m	10^{-10} m Short
Main Sources and Usages	• Geomagnetism • Magnet • Railway • MRI	• Power Transmission and Distribution Facilities • Appliance Power Supply • Railway	• IH Stove • Television, PC monitor • Railway	• Radio Broadcasting • Television Broadcasting	• Microwave Oven • Mobile Phone	• Satellite Television Broadcasting	• Sunlight	• X-ray

Note: The frequency unit "hertz (Hz)" represents the number of oscillations in a second, equal to the result obtained by dividing by the wavelength the speed, 300,000 kilometers per second (km/s) at which an electromagnetic wave propagates.
kilo- (k) = 10^3, mega- (M) = 10^6, giga- (G) = 10^9, tera- (T) = 10^{12}

Image source: http://www.jeic-emf.jp/assets/images/home/Electromagnetic_frequency_en_Mo.jpg

Interferences in the ISM 2.4 – 2.5 GHz band



bold channels are non-overlapping channels (recommended in North America and also often found in Europe), dashed channels are not available in North America

- Interesting reading:
  - 20 Myths of Wi-Fi Interference (Cisco) https://www.bradley.edu/dotAsset/887599c0-26bf-4be4-a5b9-3c0843b65d74.pdf

Image source: https://www.semanticscholar.org/paper/Coexistence-measurements-and-analysis-of-IEEE-with-Zacharias-Newe/6077884473f6e82467a28be075e8207eeb720d59/figure/0

What about transmitted power?

- Depends on local regulations

- The EU limits the EIRP of Wi-Fi devices to 100mW
  - Corresponds to 20dBm

dBm -> Decibels referred to milliwatt

20dBm = 100mW
10dBm = 10 mW
0 dBm = 1mW
-10 dBm = 0.1 mW
-20 dBm = 0.01 mW
-30 dBm = 0.001 mW
-40 dBm = 0.0001 mW

What about the received power?

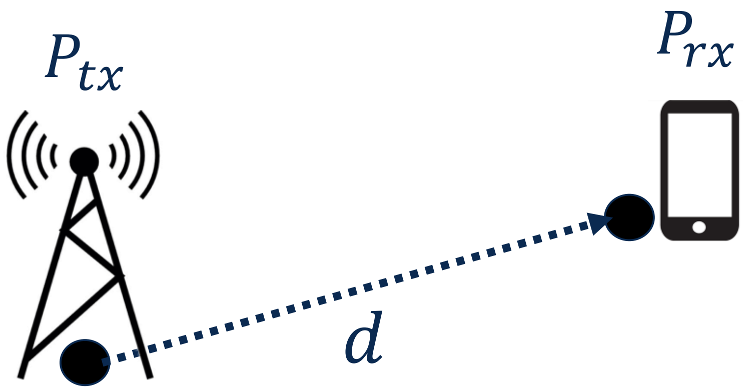
- Mobile phone receives radio signal from access point

- Power of the signal received by the phone:

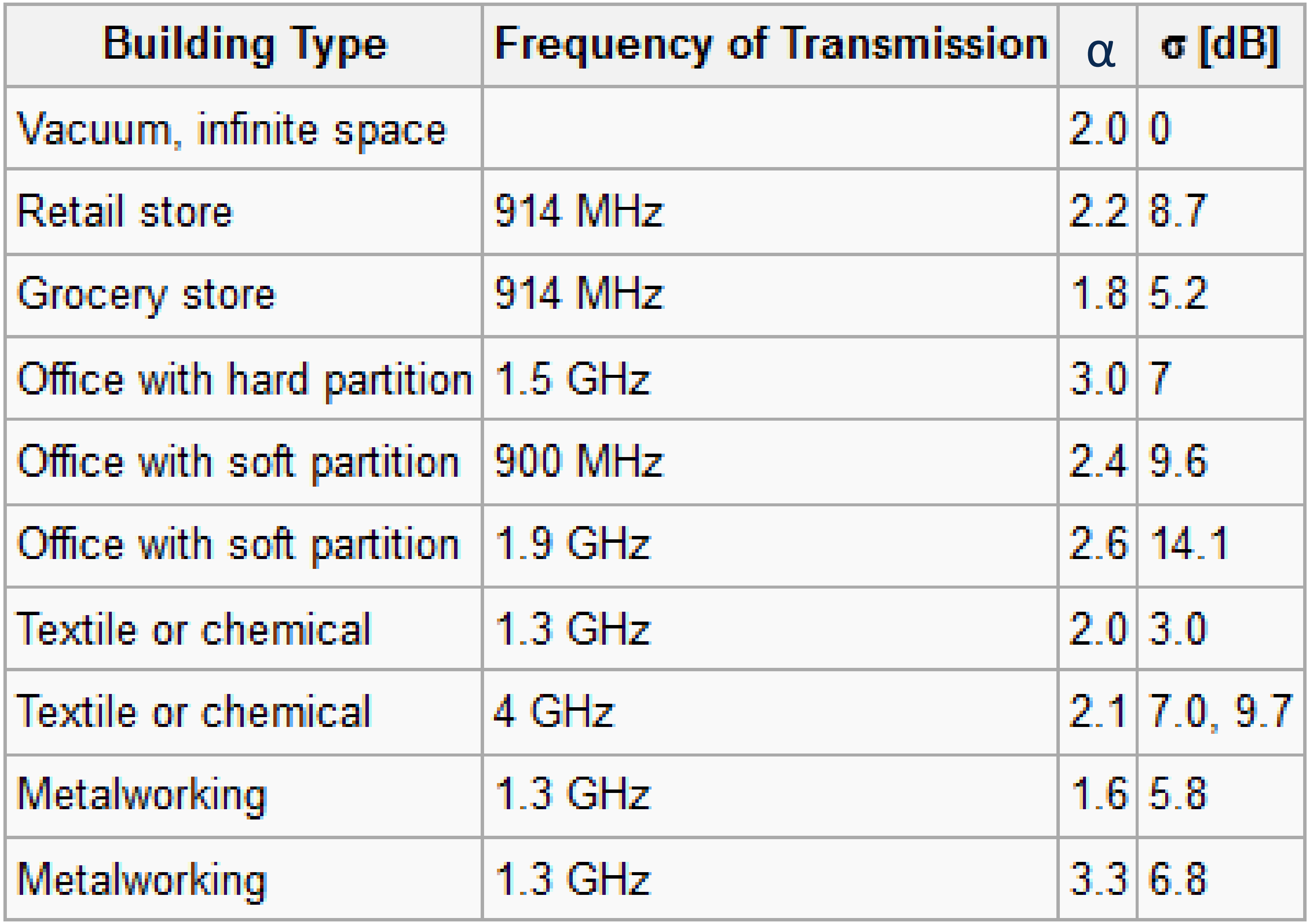
$$\boxed{P_{rx}(d) \approx \beta \cdot P_{tx} \cdot \frac{1}{d^{\alpha}}}$$

Received power depends on distance! The higher the distance, the lower the power!

  - α is the *path loss exponent*
    - Value of α depends on the medium in which the signal propagates
  - β is a multiplicative factor that captures different attenuation effects (e.g, multipath)



Path loss exponent: Typical values



Building Type	Frequency of Transmission	α	σ [dB]
Vacuum, infinite space		2.0	0
Retail store	914 MHz	2.2	8.7
Grocery store	914 MHz	1.8	5.2
Office with hard partition	1.5 GHz	3.0	7
Office with soft partition	900 MHz	2.4	9.6
Office with soft partition	1.9 GHz	2.6	14.1
Textile or chemical	1.3 GHz	2.0	3.0
Textile or chemical	4 GHz	2.1	7.0, 9.7
Metalworking	1.3 GHz	1.6	5.8
Metalworking	1.3 GHz	3.3	6.8

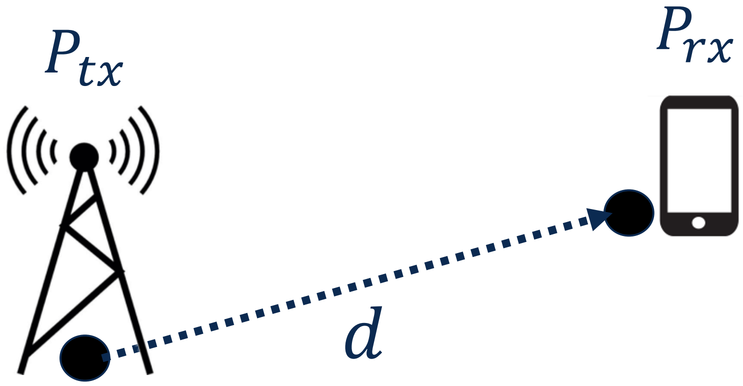
Source: Wikipedia

Image source: https://en.wikipedia.org/wiki/Log-distance_path_loss_model

Received Signal Strength Indicator (RSSI)

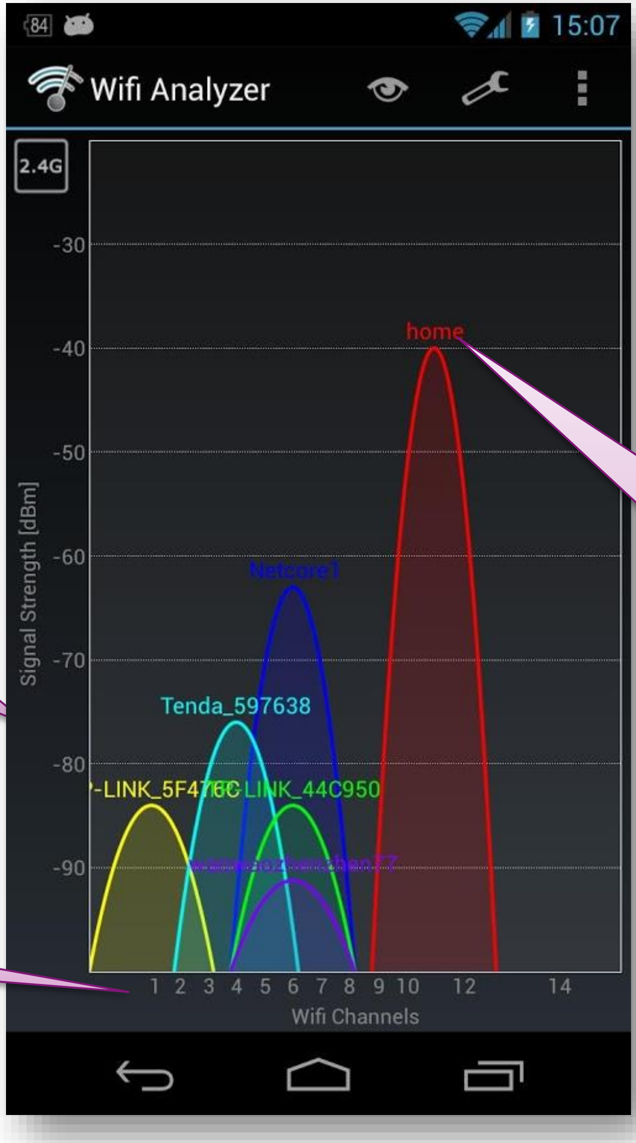
- RSSI measures the strength of the signal that arrives at the receiver
  - $RSSI = 10\log_{10}\frac{P_{rx}}{1mW}$
  - $P_{rx}(d) \approx \beta P_{tx}\frac{1}{d^{\alpha}}$
  - $RSSI = 10\log_{10}\frac{P_{rx}}{1mW} \sim \frac{1}{d^{\alpha}}$

Rule of thumb
The closer the transmitter, the higher the RSSI measured at the phone; The further away the transmitter, the lower the RSSI.



Channel received power in practice: Wi-Fi Analyzer

- Wi-Fi Analyzer (Android application)
  - https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer&hl=en



Received Signal Strength Indicator (RSSI)

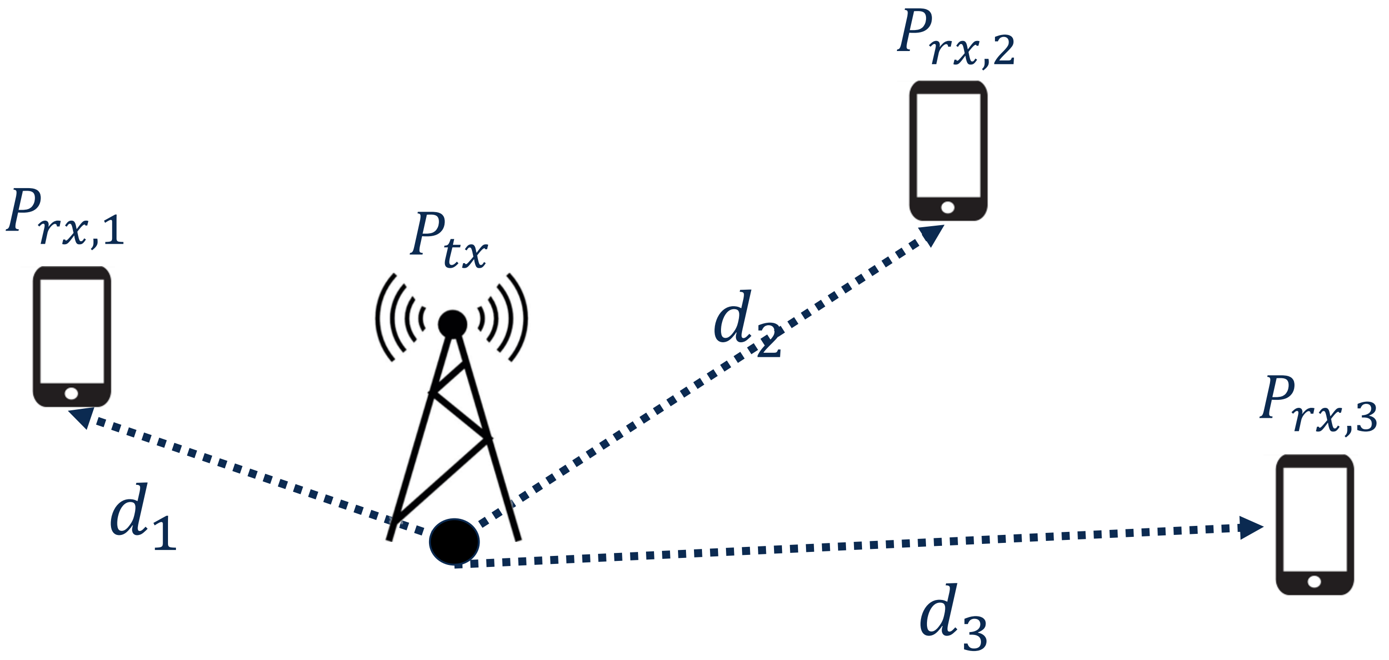
Service Set Identifier (SSID)

Wi-Fi channel

Image source: https://play.google.com/store/apps/details?id=com.farproc.wifi.analyzer

Ranging using RSSI: Theory

- If three mobile devices are at distances d_1, d_2, and d_3 from the same transmitter and $d_1 < d_2 < d_3$, one would expect: $RSSI_1 > RSSI_2 > RSSI_3$
  - **In real settings, however, this is often not the case!**

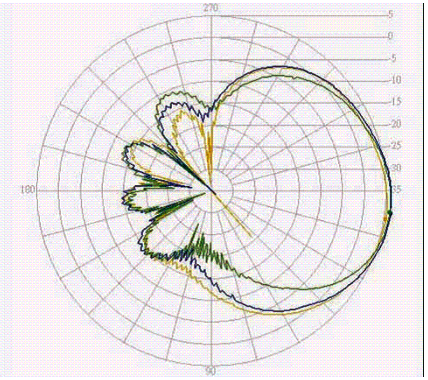


FREE EXTRA

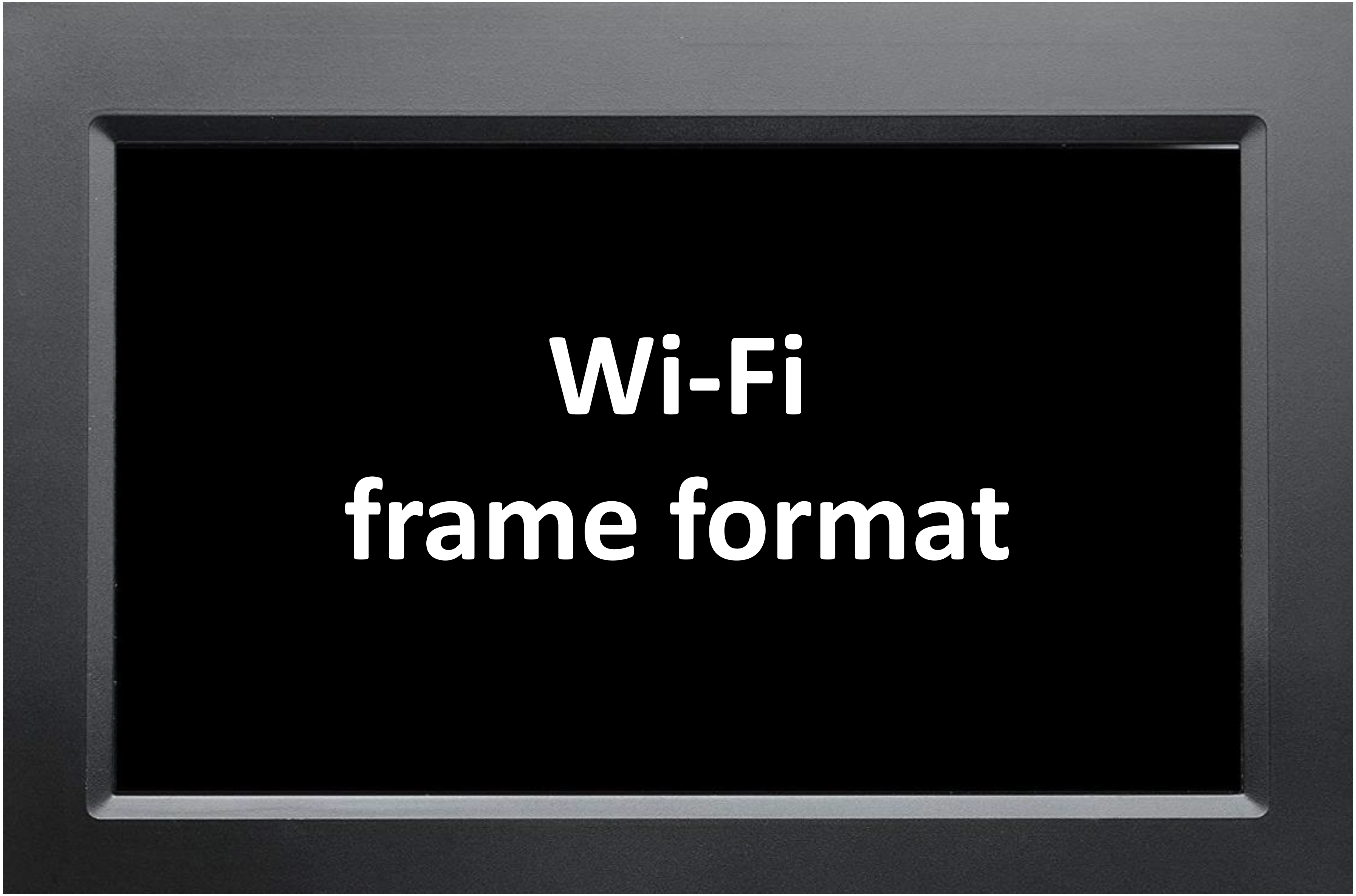
Ranging using RSSI: Practice

- The value of the RSSI may vary depending on several factors
  - Transmission power P_{tx} (may vary over time)
  - Multipath effects
  - Presence of obstacles (e.g., people)

- Also: Antenna pattern is not isotropic!
  - RSSI measured at same distance but different angle may vary significantly!

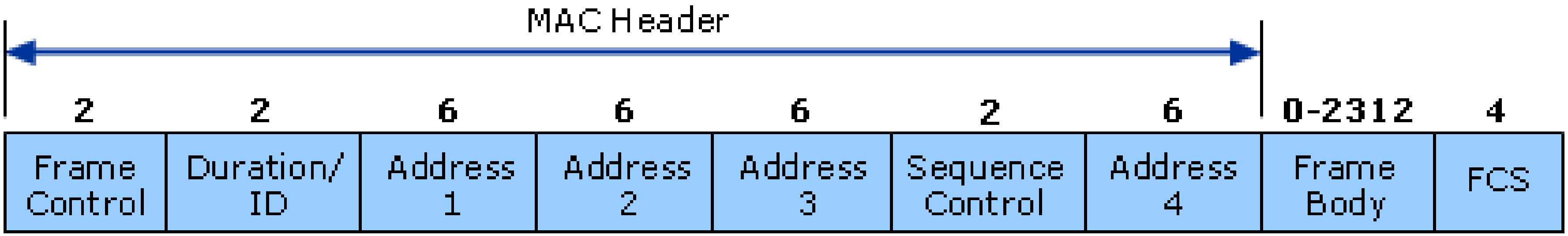


Isotropic: having a physical property which has the same value when measured in different directions.



Wi-Fi
frame format

IEEE 802.11: MAC Frame Format



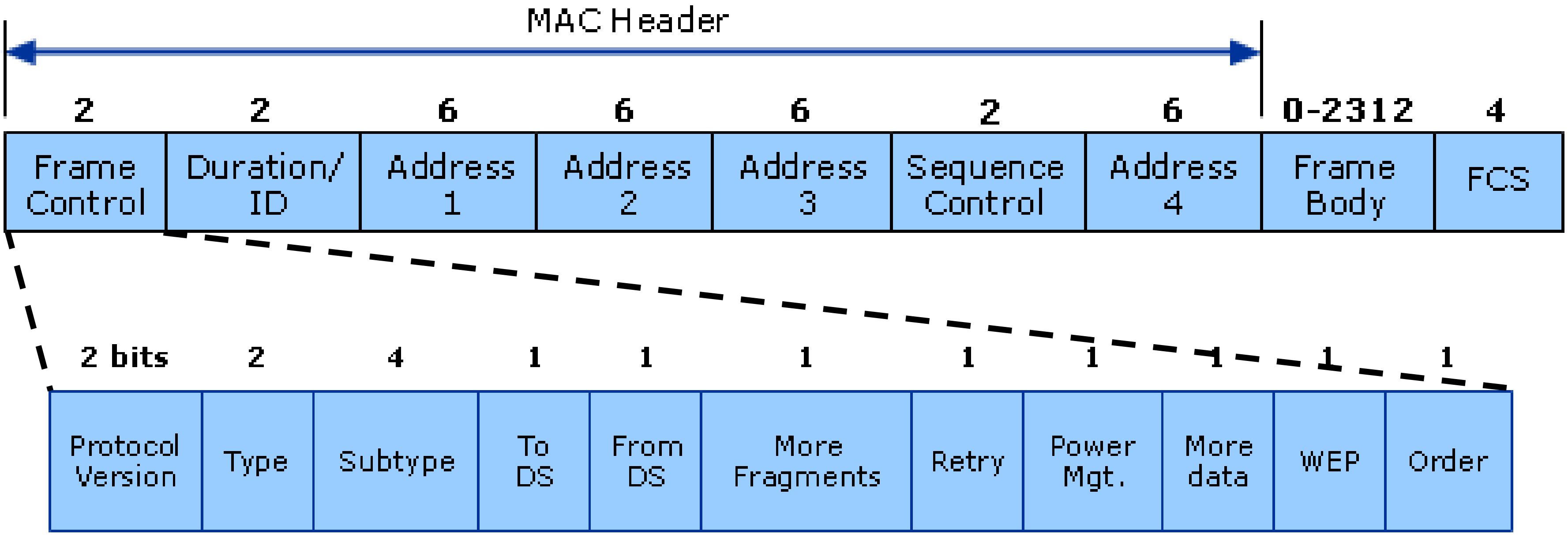
MAC Header

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Fields
  - Frame Control
  - Duration/ID
  - Address 1
  - Address 2
  - Address 3
  - Sequence control
  - Address 4
  - Frame body
  - Frame Check Sequence (FCS)

Image source: [Microsoft 802.11]

IEEE 802.11: Frame Control field



MAC Header

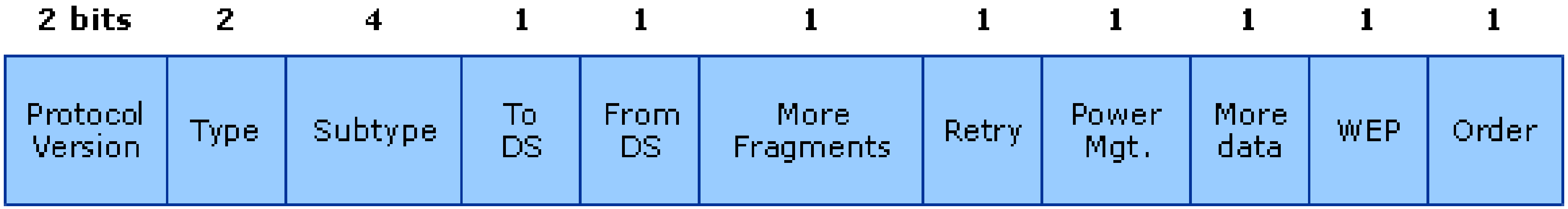
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

- The Frame Control field "*contains control information used for defining the type of 802.11 MAC frame and providing information necessary for the following fields to understand how to process the MAC frame.*" [Microsoft 802.11]

Image source: [Microsoft 802.11]

IEEE 802.11: Frame Control field

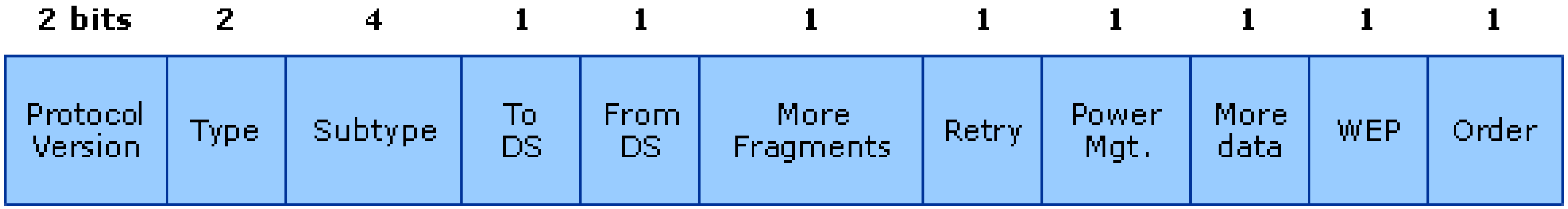


2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

- Protocol Version
  - Provides the current version of the 802.11 protocol used (current version is 00)
  - Receiving STAs use this value to determine if the version of the protocol of the received frame is supported

Image source: [Microsoft 802.11]

IEEE 802.11: Frame Control field

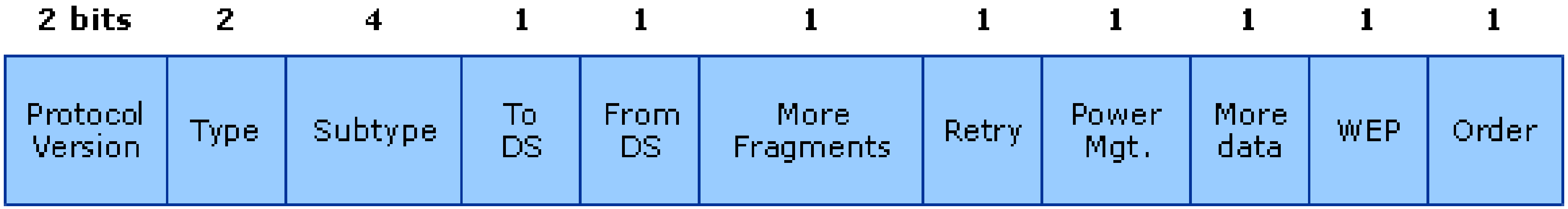


2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

- Type
  - Determines the function of the frame
  - There are three different frame type fields
    - Management (00)
      - Management frames allow for the maintenance of communication
    - Control (01)
      - Control frames facilitate in the exchange of data frames between stations
    - Data (10)

Image source: [Microsoft 802.11]

IEEE 802.11: Frame Control field

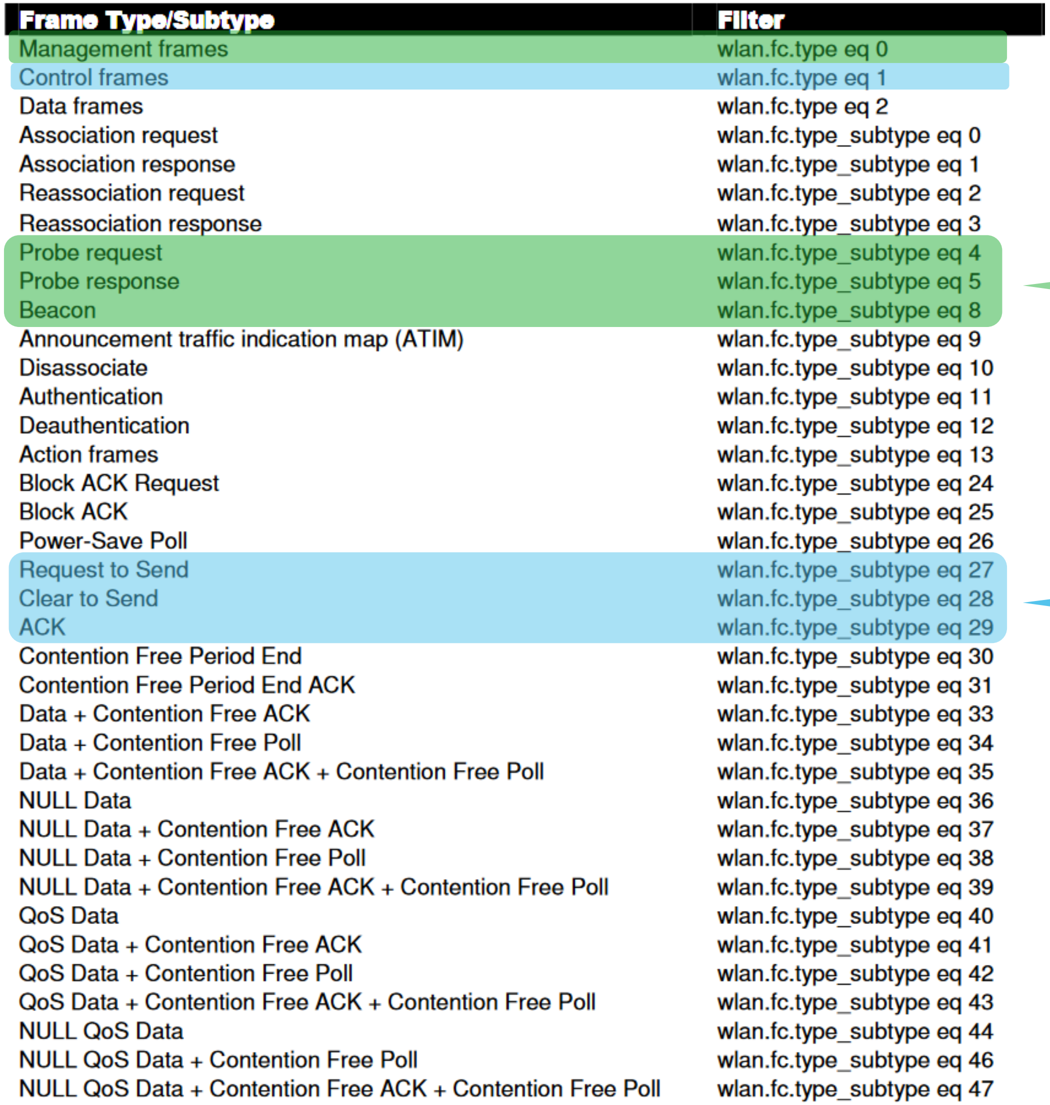


2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

- Subtype
  - There are multiple subtype fields for each frame type
  - Each subtype determines the specific function to perform for its associated frame type

Image source: [Microsoft 802.11]

IEEE 802.11: Frame Control field, Type/Subtype fields



Frame Type/Subtype	Filter
Management frames	wlan.fc.type eq 0
Control frames	wlan.fc.type eq 1
Data frames	wlan.fc.type eq 2
Association request	wlan.fc.type_subtype eq 0
Association response	wlan.fc.type_subtype eq 1
Reassociation request	wlan.fc.type_subtype eq 2
Reassociation response	wlan.fc.type_subtype eq 3
Probe request	wlan.fc.type_subtype eq 4
Probe response	wlan.fc.type_subtype eq 5
Beacon	wlan.fc.type_subtype eq 8
Announcement traffic indication map (ATIM)	wlan.fc.type_subtype eq 9
Disassociate	wlan.fc.type_subtype eq 10
Authentication	wlan.fc.type_subtype eq 11
Deauthentication	wlan.fc.type_subtype eq 12
Action frames	wlan.fc.type_subtype eq 13
Block ACK Request	wlan.fc.type_subtype eq 24
Block ACK	wlan.fc.type_subtype eq 25
Power-Save Poll	wlan.fc.type_subtype eq 26
Request to Send	wlan.fc.type_subtype eq 27
Clear to Send	wlan.fc.type_subtype eq 28
ACK	wlan.fc.type_subtype eq 29
Contention Free Period End	wlan.fc.type_subtype eq 30
Contention Free Period End ACK	wlan.fc.type_subtype eq 31
Data + Contention Free ACK	wlan.fc.type_subtype eq 33
Data + Contention Free Poll	wlan.fc.type_subtype eq 34
Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 35
NULL Data	wlan.fc.type_subtype eq 36
NULL Data + Contention Free ACK	wlan.fc.type_subtype eq 37
NULL Data + Contention Free Poll	wlan.fc.type_subtype eq 38
NULL Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 39
QoS Data	wlan.fc.type_subtype eq 40
QoS Data + Contention Free ACK	wlan.fc.type_subtype eq 41
QoS Data + Contention Free Poll	wlan.fc.type_subtype eq 42
QoS Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 43
NULL QoS Data	wlan.fc.type_subtype eq 44
NULL QoS Data + Contention Free Poll	wlan.fc.type_subtype eq 46
NULL QoS Data + Contention Free ACK + Contention Free Poll	wlan.fc.type_subtype eq 47

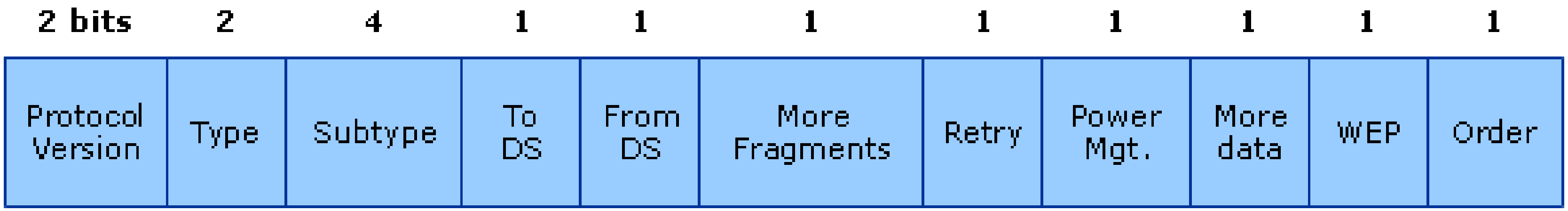
Common management frame subtypes

Common control frame subtypes

Image source: http://www.willhackforsushi.com/papers/80211_Pocket_Reference_Guide.pdf

FREE EXTRA

IEEE 802.11: Frame Control field



2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

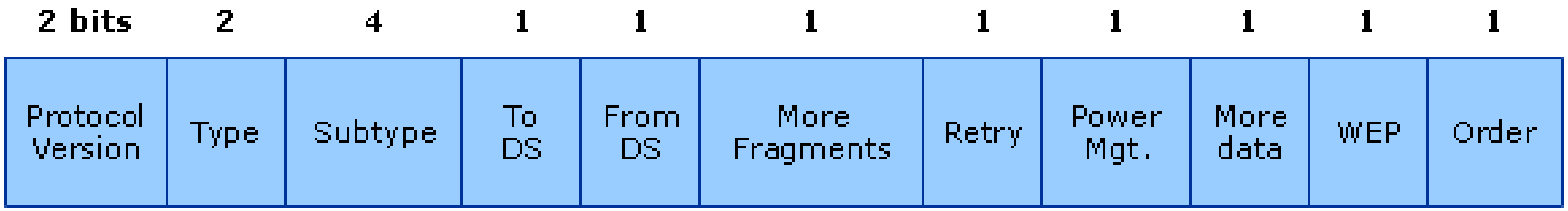
- To DS and From DS
  - Indicates whether the frame is going to or exiting from the DS (distributed system)
  - Only used in data type frames of STAs associated with an AP

- More Fragments
  - Indicates whether more fragments of the frame, either data or management type, are to follow

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: Frame Control field



2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

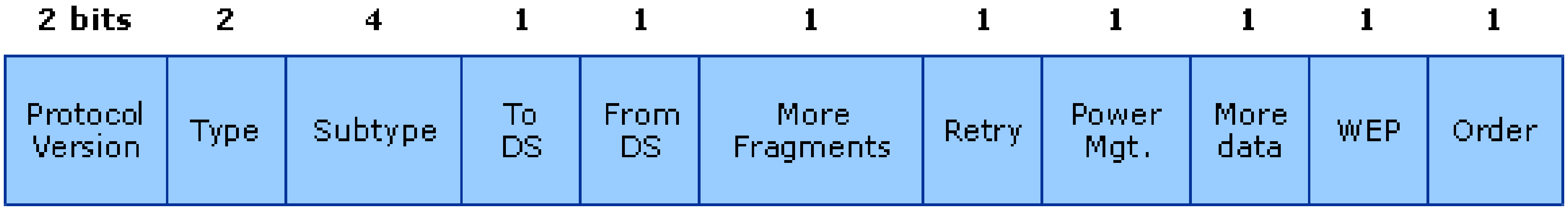
- Retry
  - Indicates whether or not the frame, for either data or management frame types, is being retransmitted

- Power Management
  - Indicates whether the sending STA is in active mode or power-save mode

Image source: [Microsoft 802.11]

IEEE 802.11: Frame Control field

FREE EXTRA



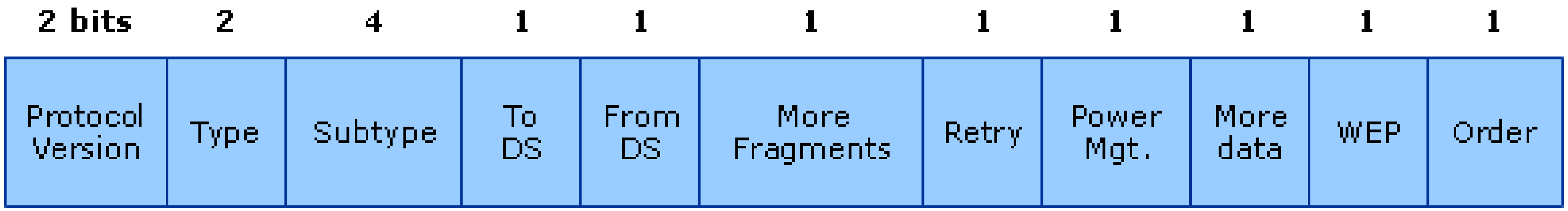
2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

- 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

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: Frame Control field



2 bits	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Fragments	Retry	Power Mgt.	More data	WEP	Order

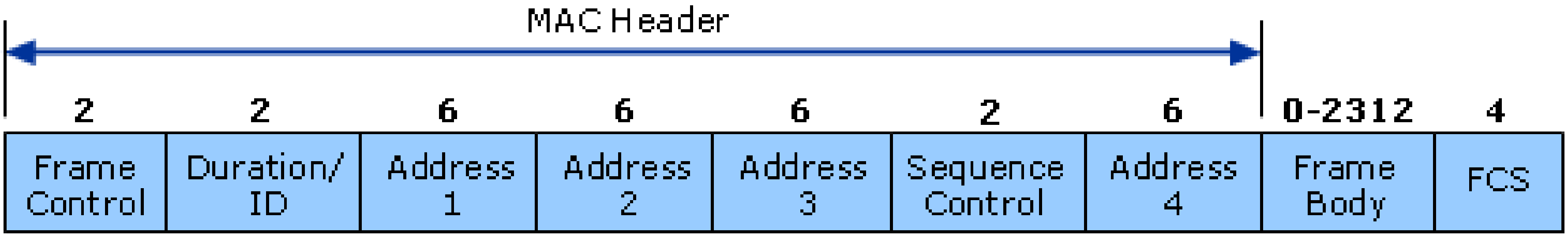
- WEP
  - Indicates whether or not encryption and authentication are used in the frame
  - It can be set for all data frames and management frames, which have the subtype set to authentication

- Order
  - Indicates that all received data frames must be processed in order

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: MAC Frame Format



MAC Header

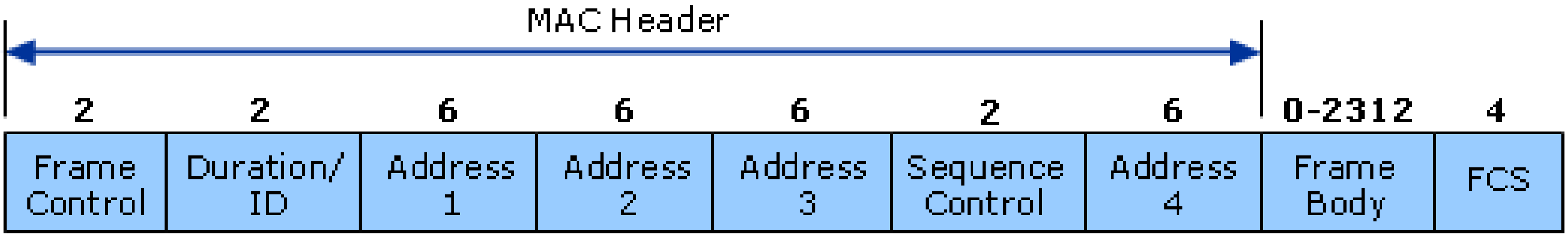
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Fields
  - Frame Control (see previous slides)
  - Duration/ID
  - Address 1
  - Address 2
  - Address 3
  - Sequence control
  - Address 4
  - Frame body
  - Frame Check Sequence (FCS)

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: MAC Frame Format, Duration/ID field



MAC Header

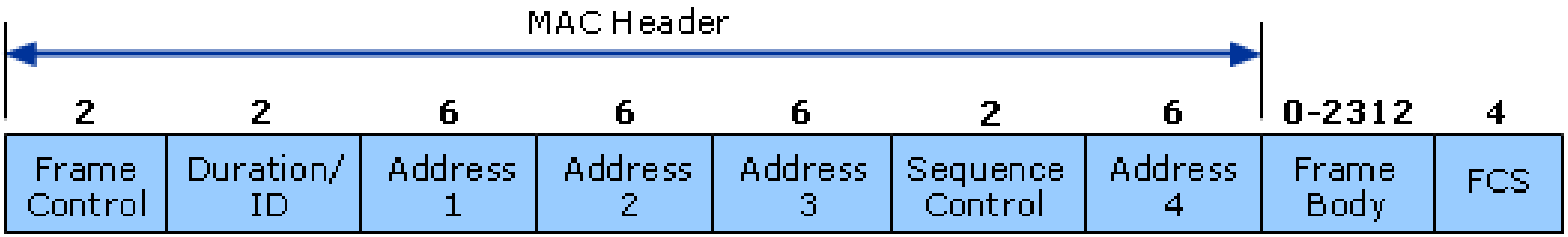
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Duration/ID
  - This field is used for all control type frames to indicate the remaining duration needed to receive the next frame transmission
  - Exception: When the sub-type is PS Poll, the field contains the association identity (AID) of the transmitting STA

Image source: [Microsoft 802.11]

IEEE 802.11: MAC Frame Format, Address fields

FREE EXTRA



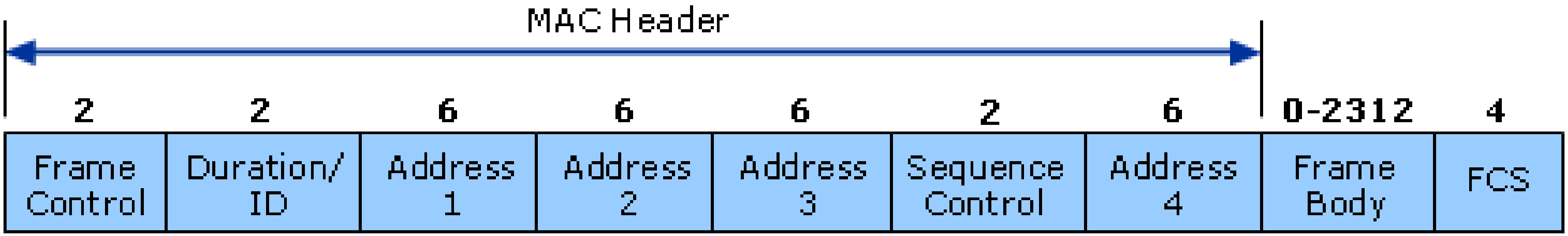
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Address Fields: Depending upon the frame type, the four address fields will contain a combination of the following address types
  - BSS Identifier (BSSID)
  - Destination Address (DA)
  - Source Address (SA)
  - Receiver Address (RA)
  - Transmitter Address (TA)

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: MAC Frame Format, Address fields


MAC Header

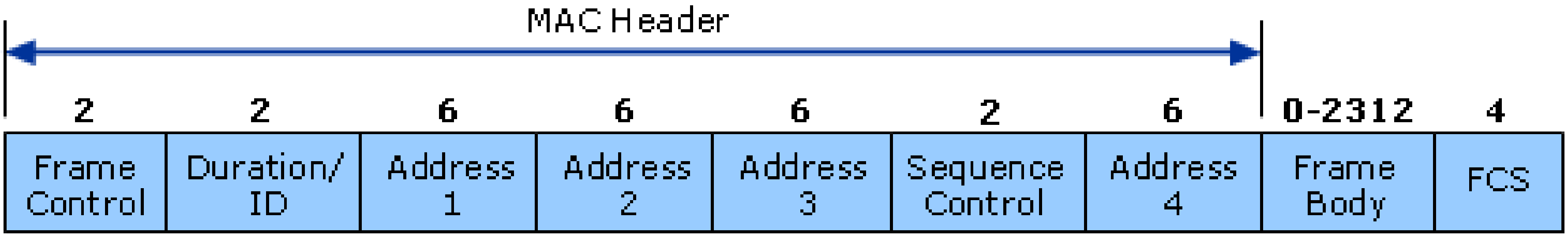
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- BSS Identifier (BSSID)
    - BSSID uniquely identifies each BSS. When the frame is from an STA in an infrastructure BSS, the BSSID is the MAC address of the AP. When the frame is from a STA in an IBSS, the BSSID is the randomly generated, locally administered MAC address of the STA that initiated the IBSS.

Image source: [Microsoft 802.11]

IEEE 802.11: MAC Frame Format, Address fields

FREE EXTRA



MAC Header

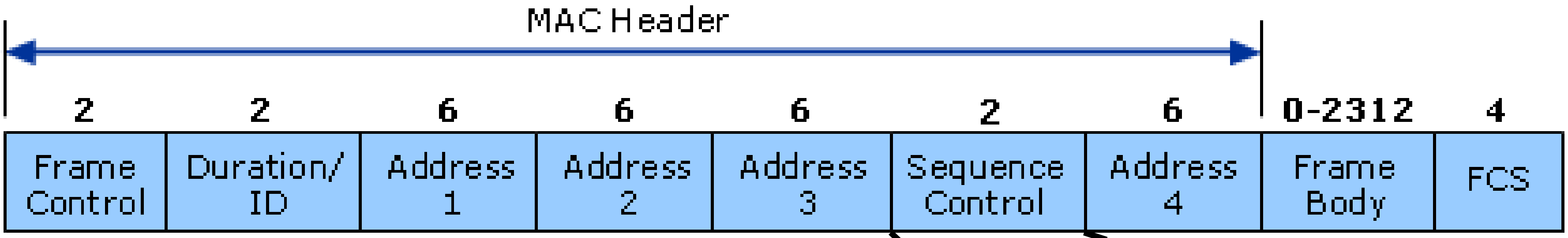
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Destination Address (DA)
  - DA indicates the MAC address of the final destination to receive the frame
- Source Address (SA)
  - SA indicates the MAC address of the original source that initially created and transmitted the frame
- Receiver Address (RA)
  - RA indicates the MAC address of the next immediate STA on the wireless medium to receive the frame
- Transmitter Address (TA)
  - TA indicates the MAC address of the STA that transmitted the frame onto the wireless medium

Image source: [Microsoft 802.11]

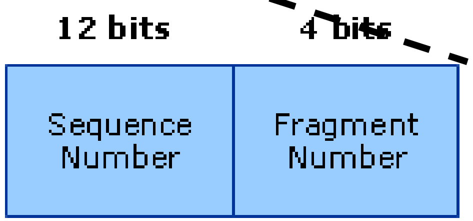
FREE EXTRA

IEEE 802.11: MAC Frame Format



MAC Header

2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS



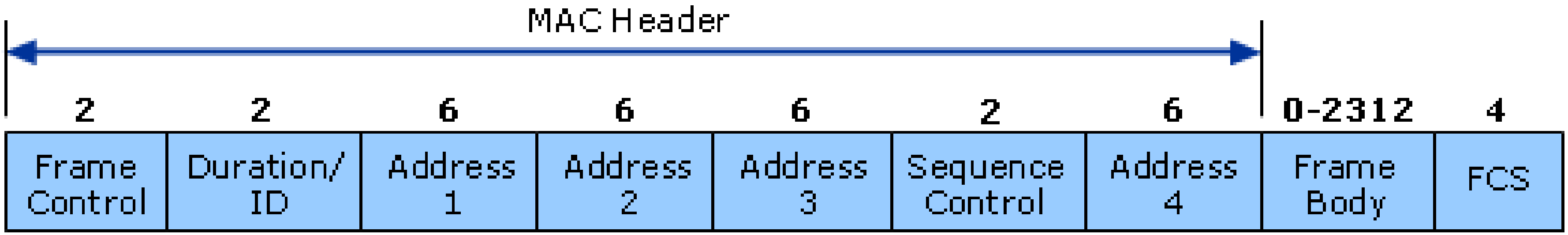
12 bits	4 bits
Sequence Number	Fragment Number

- Sequence control
  - Sequence Number
    - Indicates the sequence number of each frame
    - The sequence number is the same for each frame sent for a fragmented frame; otherwise, the number is incremented by one until reaching 4095, when it then begins at zero again
  - Fragment Number
    - Indicates the number of each frame sent of a fragmented frame
    - The initial value is set to 0 and then incremented by one for each subsequent frame sent of the fragmented frame

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: MAC Frame Format



MAC Header

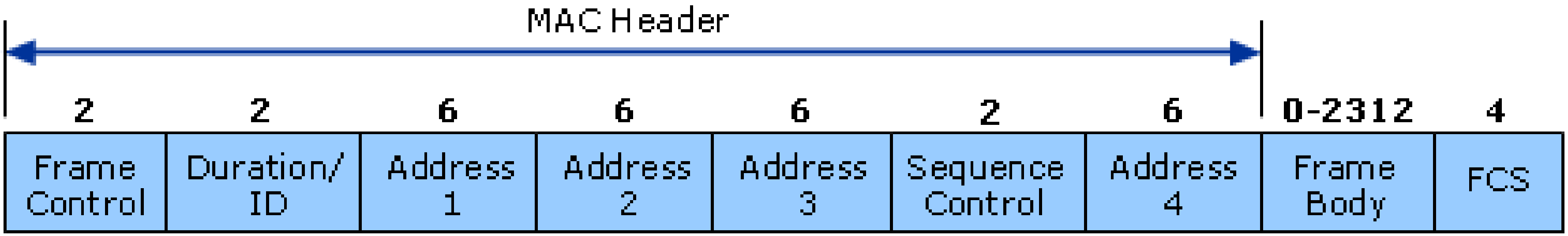
2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Frame body
  - Variable in size, from 0 to 2304 bytes plus any overhead from security encapsulation
  - Contains information from higher layers (the payload)

Image source: [Microsoft 802.11]

FREE EXTRA

IEEE 802.11: MAC Frame Format



2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

- Frame Check Sequence (FCS)
  - It allows for integrity check of frames
  - As frames are about to be sent, the FCS is calculated and appended
  - When a station receives a frame, it can calculate the FCS of the frame and compare it to the one received
  - If they match, it is assumed that the frame was not distorted during transmission

Image source: [Microsoft 802.11]

Wi-Fi Standards and amendments

WF-01

WF-02

WF-03

WF-04

WF-05

WF-06

WF-07

WF-08

WF-09

WF-10

WF-11

WF-12

WF-13

WF-14

WF-15

WF-16

WF-17

WF-18

WF-19

WF-20

WF-21

WF-22

WF-23

WF-24

IEEE 802.11: Standards and amendments

Name	Year	Description
IEEE 802.11-1997	1997	The WLAN standard was originally 1 Mbit/s and 2 Mbit/s, 2.4 GHz RF and infrared (IR) standard (1997), all the others listed below are Amendments to this standard, except for Recommended Practices 802.11F and 802.11T.
IEEE 802.11a	1999	54 Mbit/s, 5 GHz standard
IEEE 802.11b	1999	Enhancements to 802.11 to support 5.5 Mbit/s and 11 Mbit/s
IEEE 802.11c	2001	Bridge operation procedures; included in the IEEE 802.1D standard
IEEE 802.11d	2001	International (country-to-country) roaming extensions
IEEE 802.11e	2005	Enhancements: QoS, including packet bursting
IEEE 802.11F	2003	Inter-Access Point Protocol (Withdrawn February 2006)
IEEE 802.11g	2003	54 Mbit/s, 2.4 GHz standard (backwards compatible with b)
IEEE 802.11h	2004	Spectrum Managed 802.11a (5 GHz) for European compatibility
IEEE 802.11i	2004	Enhanced security
IEEE 802.11j	2004	Extensions for Japan

IEEE 802.11: Standards and amendments

Name	Year	Description
IEEE 802.11-2007	2007	A new release of the standard that includes amendments a, b, d, e, g, h, i, and j.
IEEE 802.11k	2008	Radio resource measurement enhancements
IEEE 802.11n	2009	Higher-throughput improvements using MIMO (multiple-input, multiple-output antennas)
IEEE 802.11p	2010	WAVE—Wireless Access for the Vehicular Environment (such as ambulances and passenger cars)
IEEE 802.11r	2008	Fast BSS transition (FT)
IEEE 802.11s	2011	Mesh Networking, Extended Service Set (ESS)
IEEE 802.11T	2011	Wireless Performance Prediction (WPP)—test methods and metrics Recommendation (CANCELLED)
IEEE 802.11u	2011	Improvements related to HotSpots and 3rd-party authorization of clients, e.g., cellular network offload
IEEE 802.11v	2011	Wireless network management
IEEE 802.11w	2009	Protected Management Frames

IEEE 802.11: Standards and amendments

Name	Year	Description
IEEE 802.11y	2008	3650–3700 MHz Operation in the U.S.
IEEE 802.11z	2010	Extensions to Direct Link Setup (DLS)
IEEE 802.11-2012	2012	A new release of the standard that includes amendments k, n, p, r, s, u, v, w, y, and z
IEEE 802.11aa	2012	Robust streaming of Audio Video Transport Streams
IEEE 802.11ac	2013	Very High Throughput <6 GHz;[50] potential improvements over 802.11n: better modulation scheme (expected ~10% throughput increase), wider channels (estimate in future time 80 to 160 MHz), multi user MIMO
IEEE 802.11ad	2012	Very High Throughput 60 GHz — see WiGig
IEEE 802.11ae	2012	Prioritization of Management Frames
IEEE 802.11af	2014	TV Whitespace
IEEE 802.11-2016	2016	A new release of the standard that includes amendments ae, aa, ad, ac, and af

IEEE 802.11: Standards and amendments

Name	Year	Description
IEEE.11ah	2016	Sub-1 GHz license exempt operation (e.g., sensor network, smart metering)
IEEE 802.11ai	2016	Fast Initial Link Setup
IEEE 802.11aj	2018	China Millimeter Wave
IEEE 802.11ak	2018	General Links
IEEE 802.11aq	2018	Pre-association Discovery

Wi-Fi-based localization

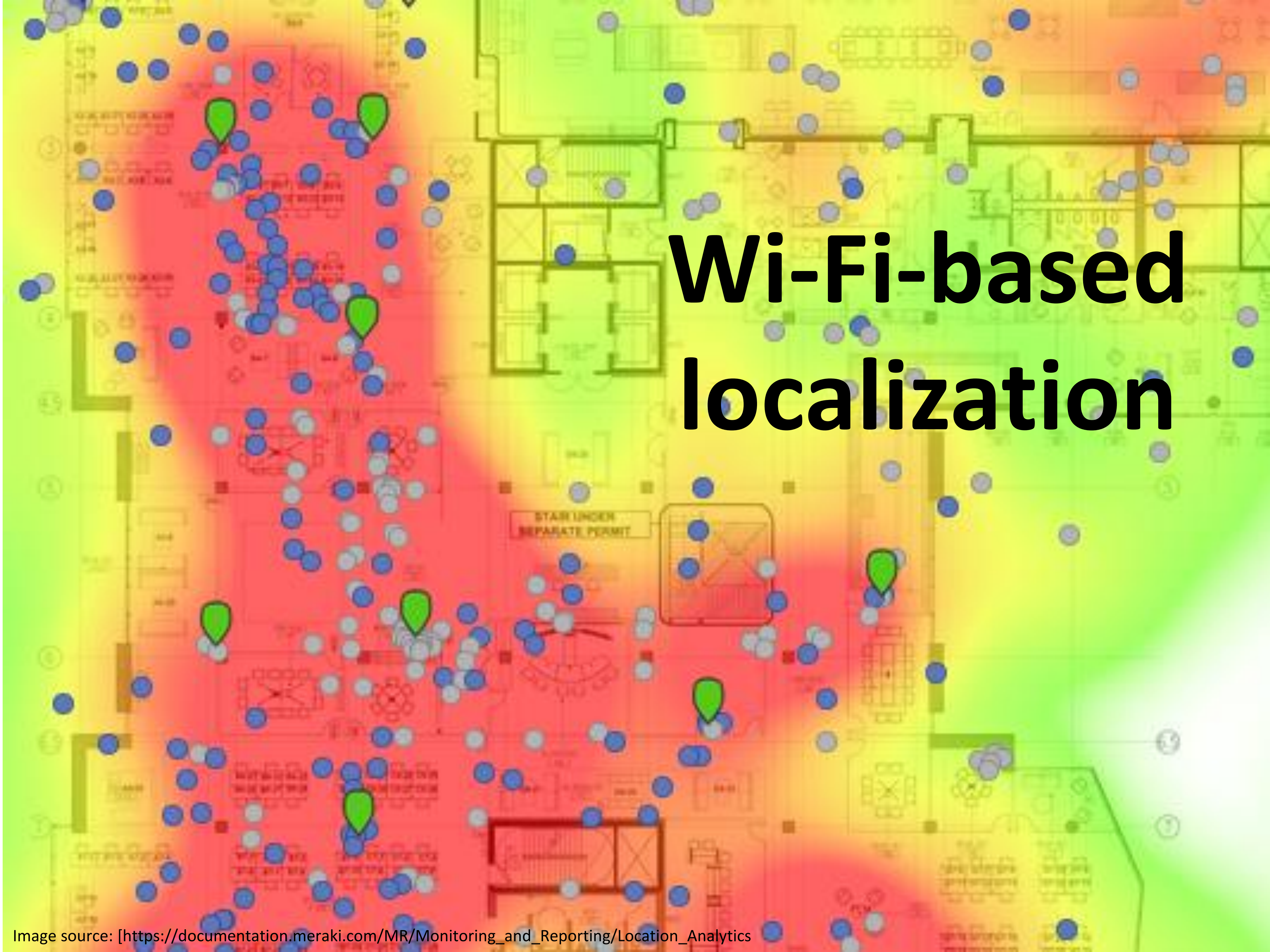


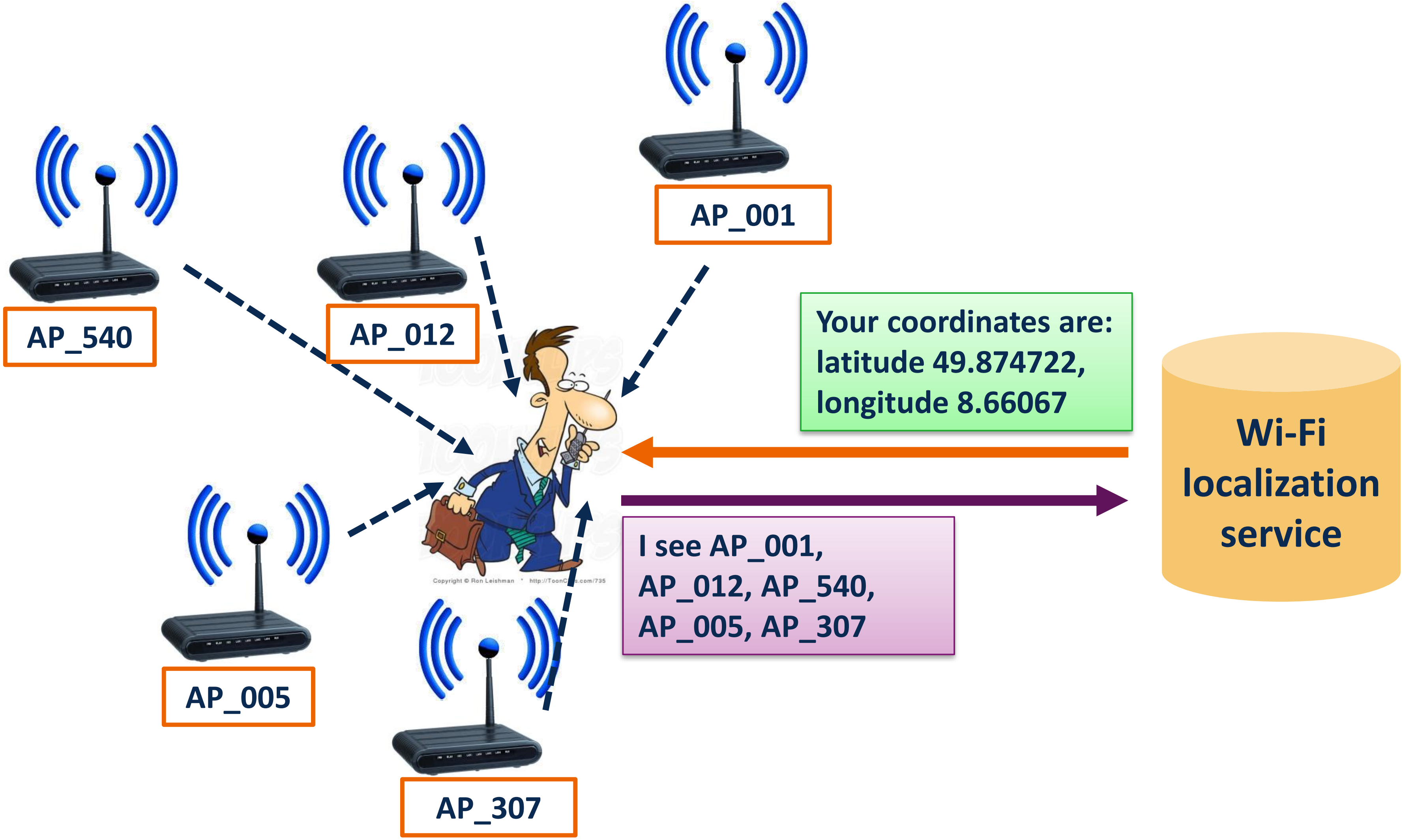
Image source: [https://documentation.meraki.com/MR/Monitoring_and_Reporting/Location_Analytics

Wi-Fi-based localization

- Exploit the ubiquitous presence of Wi-Fi access points (AP) to locate mobile phones
  - Or to locate anything else that has a Wi-Fi receiver

- Main steps (simplified)
  1) A mobile phone records information about visible Wi-Fi APs
  2) The mobile phone sends these identifiers to the server of a Wi-Fi-based localization service
  3) Records sent by the phone are processed on the server
  4) The server returns location data (typically as position expressed in longitude and latitude coordinates) to the mobile phone

As simple as this?Almost ☺


AP_001
AP_540
AP_012
AP_005
AP_307
Copyright © Ron Leishman * http://ToonClips.com/735
Wi-Fi localization service

Your coordinates are:
latitude 49.874722,
longitude 8.66067

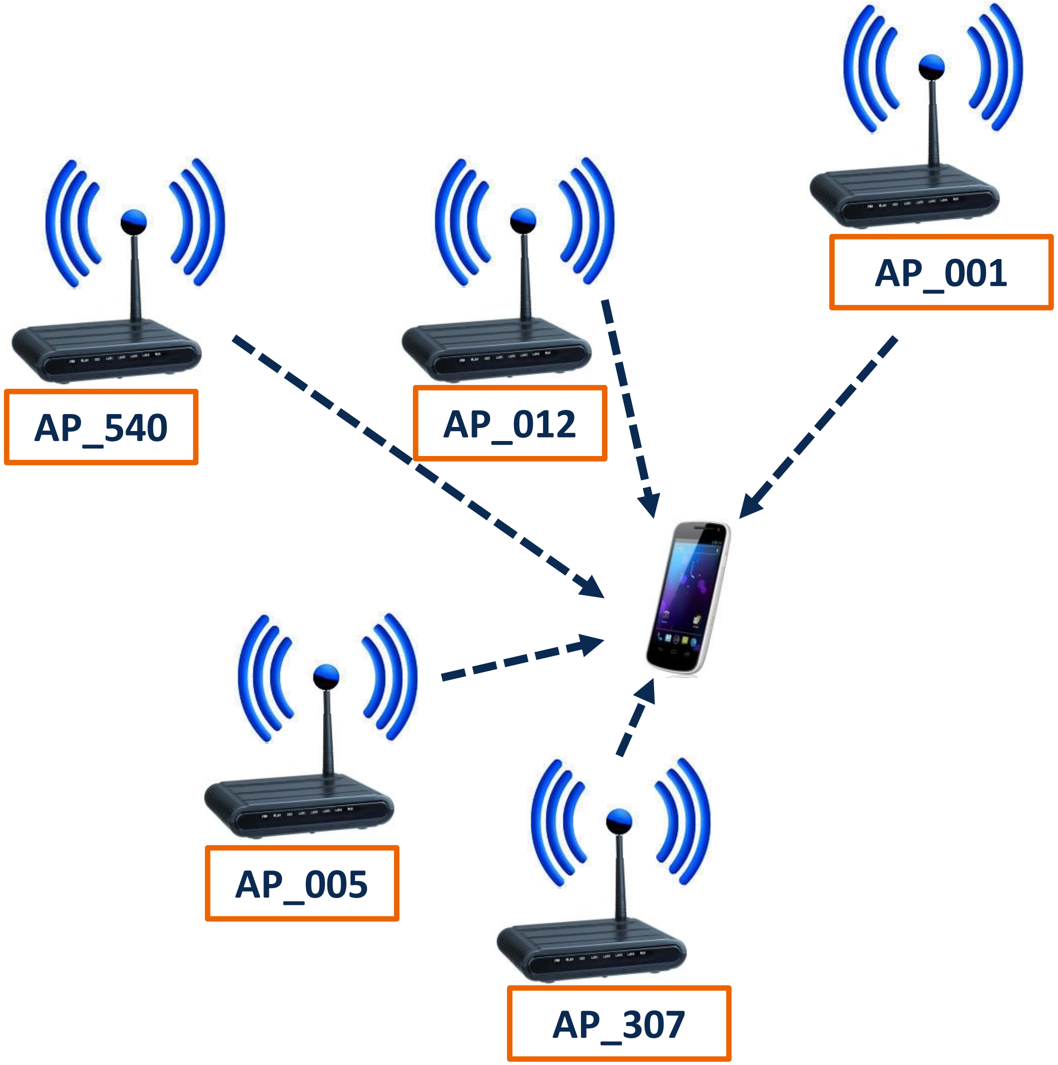
I see AP_001,
AP_012, AP_540,
AP_005, AP_307

Images sources: http://toonclips.com/600/735.jpg

Let's look at some details

- What is a Wi-Fi access point?
  - What is Wi-Fi, by the way?
- How can Wi-Fi access points be discovered?
- How does the “identifier” of a Wi-Fi AP look like?
- How does the location service compute a position using the APs’ identifiers sent by a mobile phone?

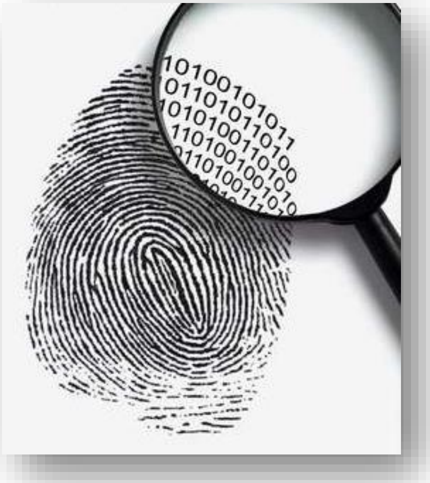
Discovering Wi-Fi access points



- If a mobile device can receive a radio signal from the access point, the access point is **visible** to the device

- Wi-Fi access points advertise their presence through beacons

Fingerprint



- A Wi-Fi access point produces an imaginary „fingerprint“ on each specific location at which the access point is visible

- How is this fingerprint „detected“?
  - By recording information about the access point

- Information included in the fingerprint
  - Typically: MAC address of the Wi-Fi device, SSID of the network, RSSI
  - Possibly: Encryption type, channel, etc.

Image source: http://ozgunt.files.wordpress.com/2010/08/biometrics-1.jpg

Providers of Wi-Fi based localization services

- Several different providers
  - Google, Apple, Navizon, Skyhook Wireless, …
- Proprietary databases
  - Fingerprints of hundreds of millions of access points
- How are fingerprints collected?

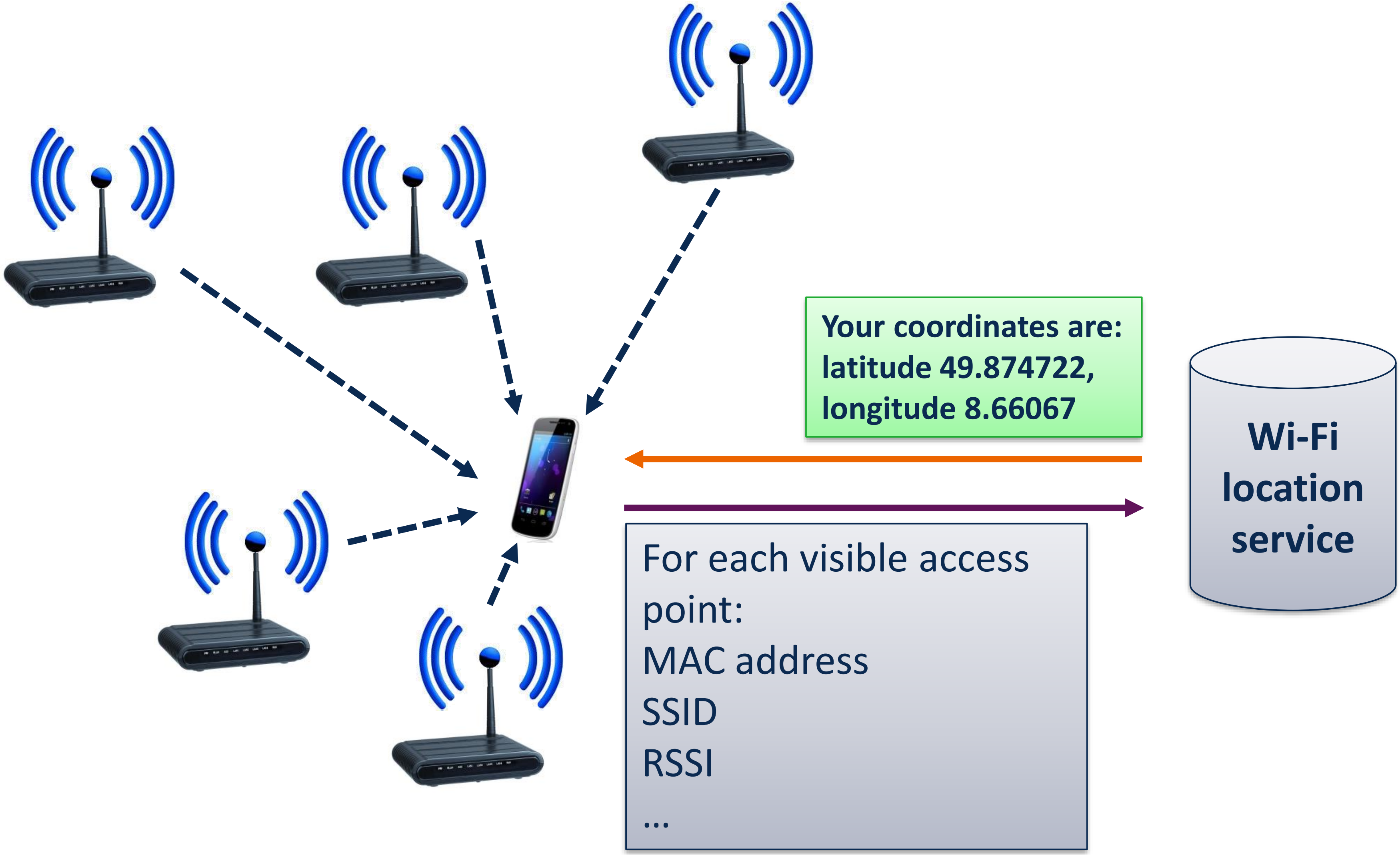
Wardriving (good old days…)

- Vehicle-based signal scanning
  - A car or similar vehicle that travels roads and highways
  - Special equipment to capture information about access points (date, time, location stamp, RSSI, …)
  - High-frequency sampling (e.g., 1 sample every second)

- Wardriving determines the *fingerprint* of an AP and records the position at which the fingerprint has been recorded

Image sources: http://josh.st/2006/11/27/wardriving-in-style/, http://revolutionof1.files.wordpress.com/2010/05/wardriving1.jpg, http://www.hackerstickers.com

From visible access points to positioning



Your coordinates are:
latitude 49.874722,
longitude 8.66067

For each visible access point:
MAC address
SSID
RSSI
…

Wi-Fi location service

One more thing: The privacy issue

- Can my mobile phone (and thus, me!) be localized without explicit consent?

- If I give my consent (as we usually do), what happens with the data (fingerprints) that I give for free to the location service?

- Can I avoid my private access point to be included in the database of companies that provide Wi-Fi-based localization?

The _nomap option

- In November 2011, Google announced that it would do more to address user privacy concerns
  - http://googleblog.blogspot.com/2011/11/greater-choice-for-wireless-access.html

- Prevent access point to be included in the Google Location Server by adding the string _nomap to the SSID of the access point
  - Before: MyCoolNetworkName
  - After   : MyCoolNetworkName_nomap

- Similar to the robots.txt protocol for web crawling robots

Indoor localization using Wi-Fi

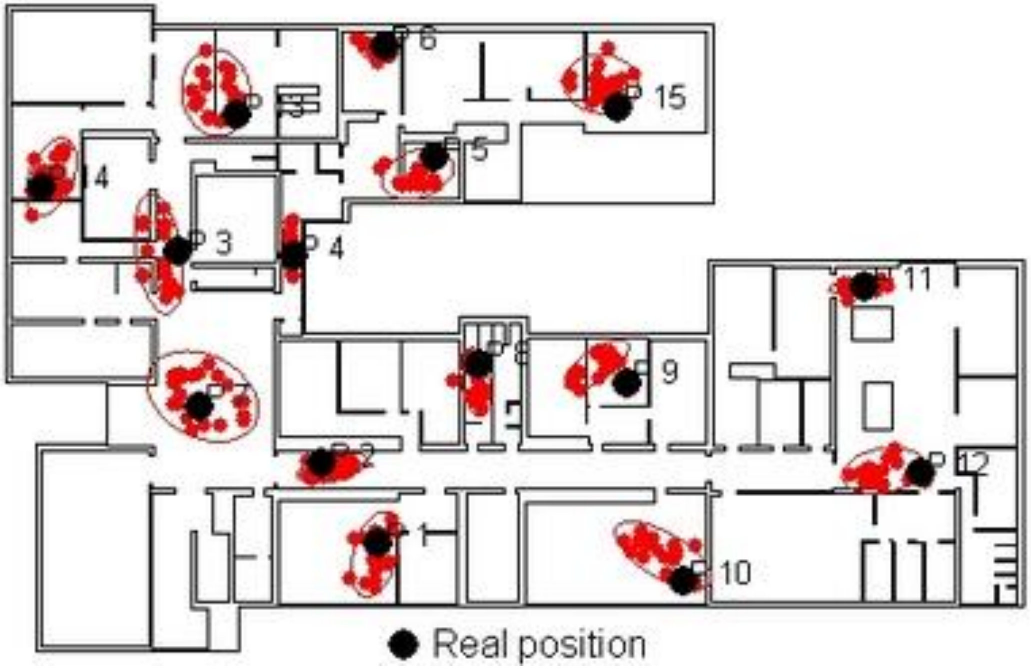


Image source: https://lopsi.weebly.com/personal-indoor-localization.html

Indoor localization using Wi-Fi

- Wi-Fi initially envisioned to be used where GPS does not work
  - Indoor
  - Specific outdoor scenarios, e.g., urban canyons
- Widespread of Wi-Fi made Wi-Fi-based localization now complements other outdoor localization technologies (GPS, cell-based localization)
- Example of Wi-Fi-based indoor localization system: RedPin project

The Redpin project

- http://redpin.org/
  - "*Redpin is an open source indoor positioning system that was developed with the goal of providing at least room-level accuracy. Moreover, it avoids the time-consuming training and setup phase known from other systems and instead relies on the user community.*"

Scanning radios

Image source: http://redpin.org/

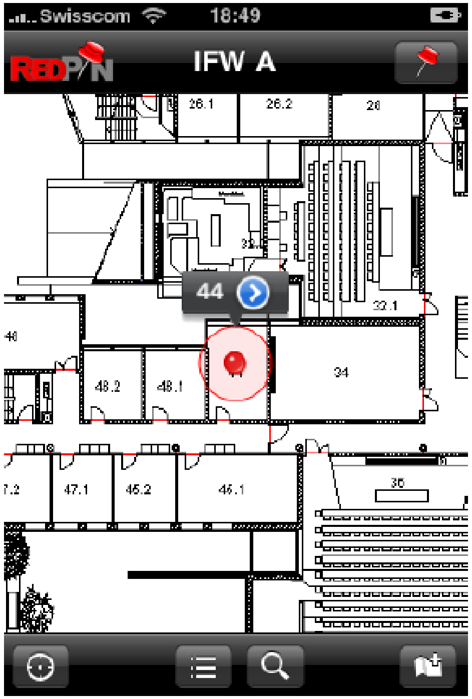
The Redpin project (II)

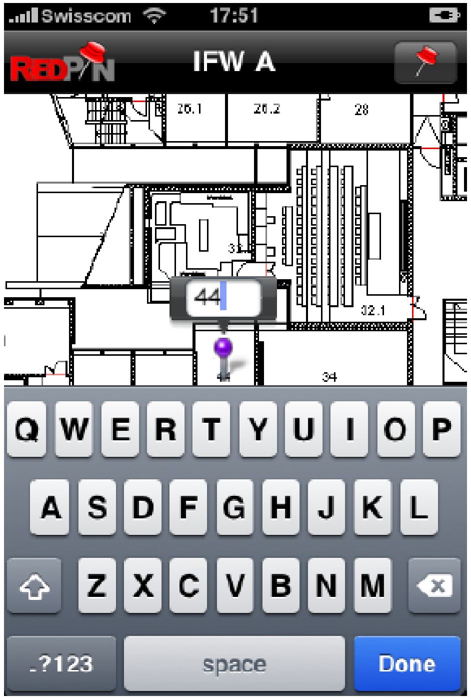
- Indoor localization based on Wi-Fi signatures
  - Scan for nearby access points only when phone is not moving
  - Detect movement using the phone's in-built accelerometer

- Problem: how to "label" places?
  - E.g., I am in room S3|06 052 now and this is the Wi-Fi signature that I am observing

- Solution: Rely on users to label places for you

The Redpin project: User-driven labeling

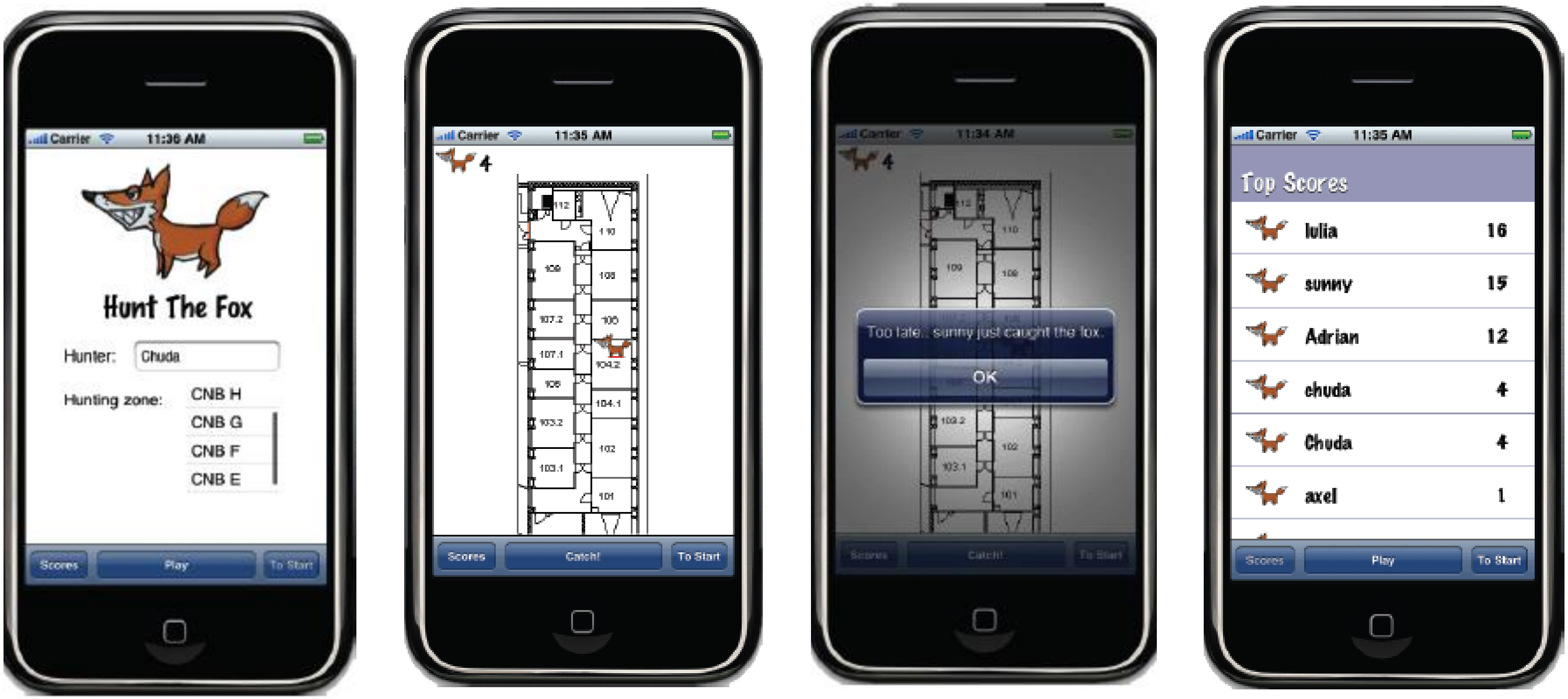




- Using a mobile client, users can collaborate in labeling places
- BUT: How to motivate users to participate?
  - In Fun We Trust ☺

Images sources: http://redpin.org/, [Bolliger 2009]

The Redpin project: "Hunt the fox"



Hunt The Fox

Hunter: Chuda

Hunting zone: CNB H, CNB G, CNB F, CNB E

Too late.. sunny just caught the fox.

Top Scores

Iulia	16
sunny	15
Adrian	12
chuda	4
Chuda	4
axel	1

- Users can play with friends and colleagues, hunt the foxs and collect Wi-Fi signatures!

This is a game with a purpose! (GWAP)

Images sources: http://redpin.org/, [Bolliger 2009]

Monitoring vital signs using Wi-Fi

Image source: http://witrack.csail.mit.edu/vitalradio/

How does it work?

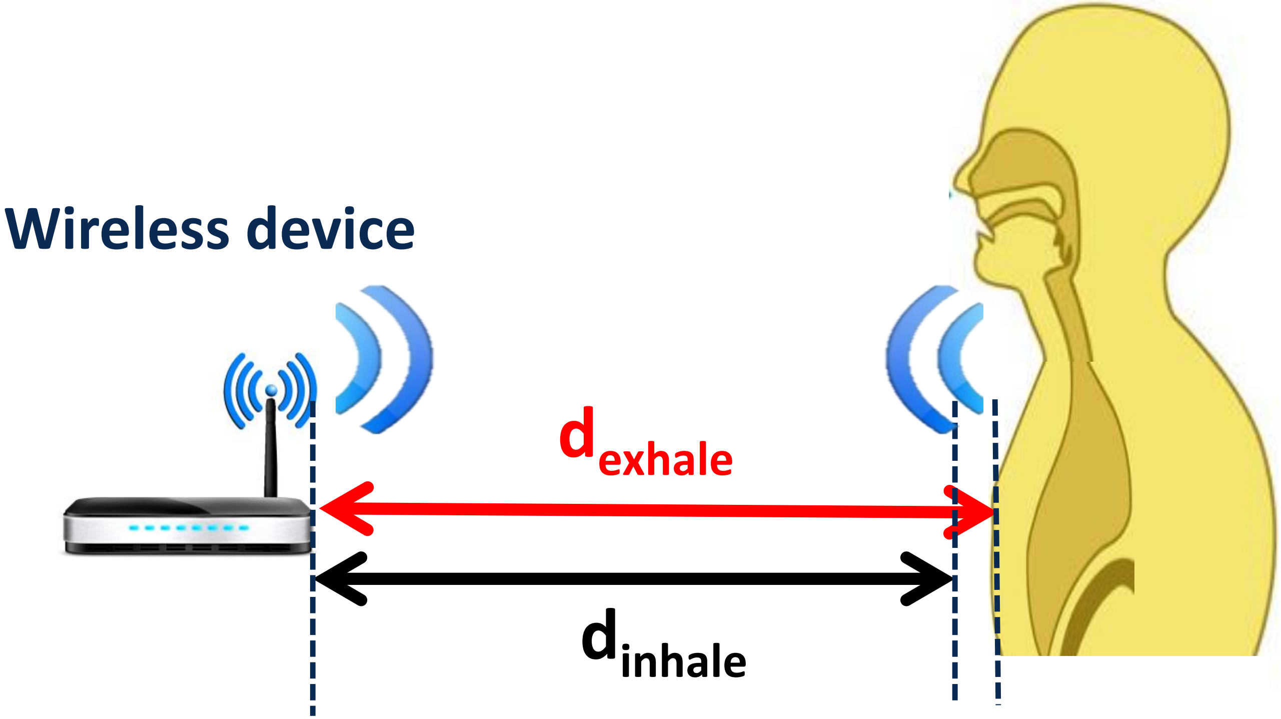


Image source: witrack.csail.mit.edu/vitalradio/content/VitalRadio-slides.pptx

How does it work?

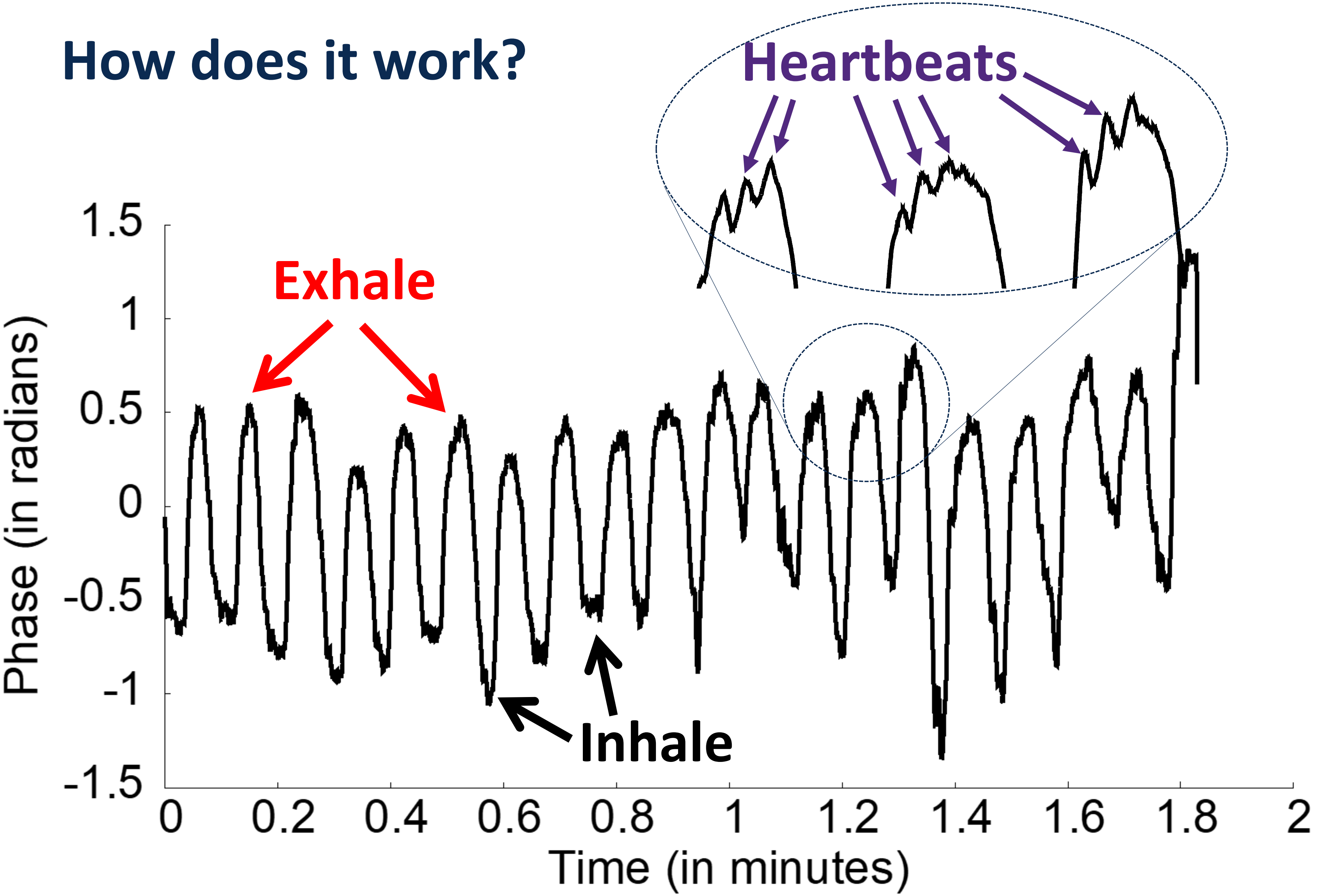
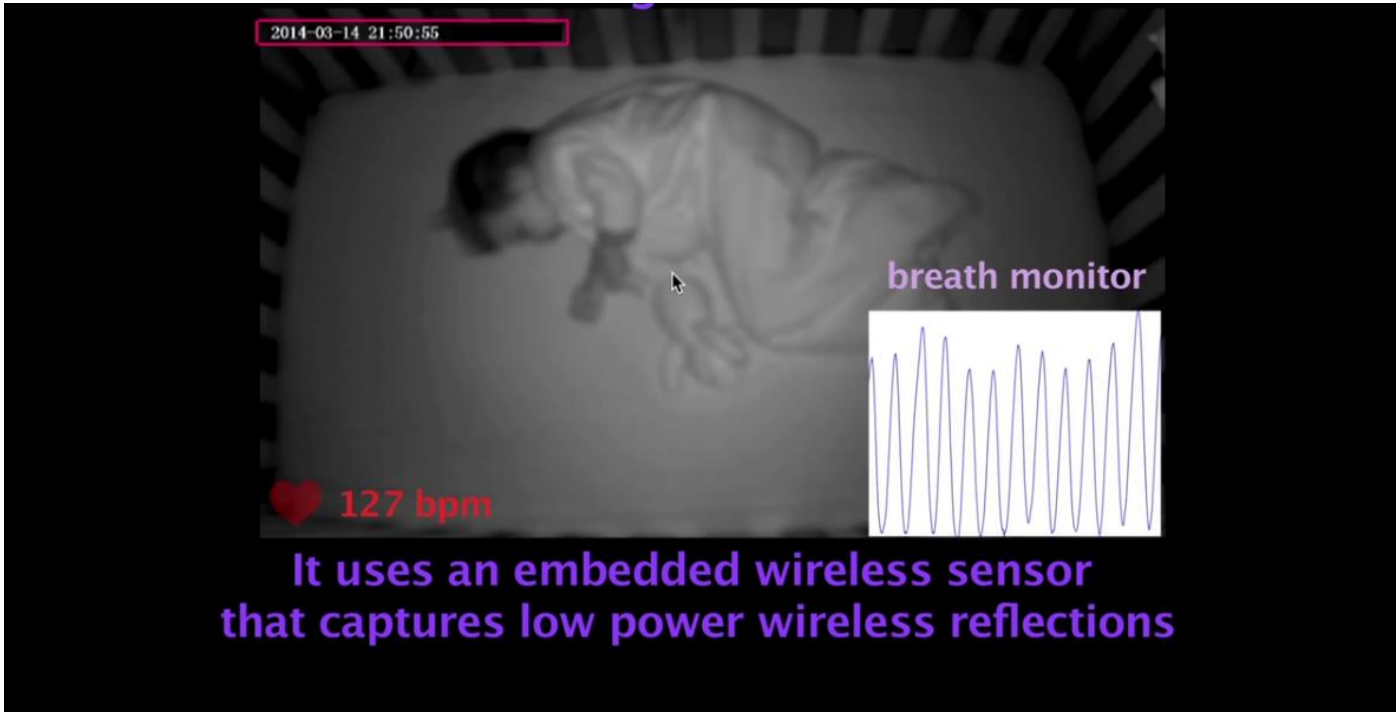


Image source: witrack.csail.mit.edu/vitalradio/content/VitalRadio-slides.pptx

What can we do with it?

- Just one of many examples:



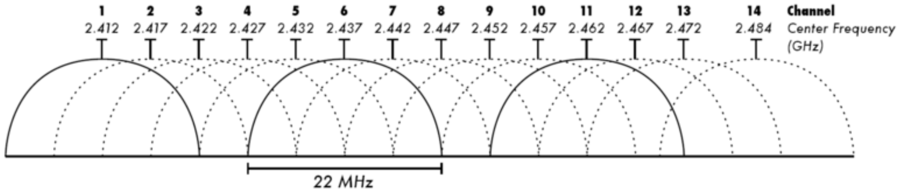
It uses an embedded wireless sensor
that captures low power wireless reflections

Image source: witrack.csail.mit.edu/vitalradio/content/VitalRadio-slides.pptx

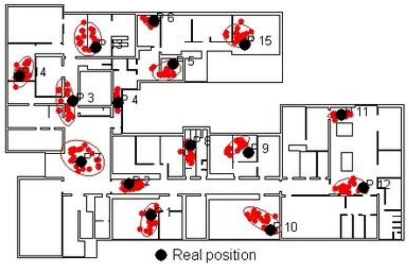
CONCLUSIONS

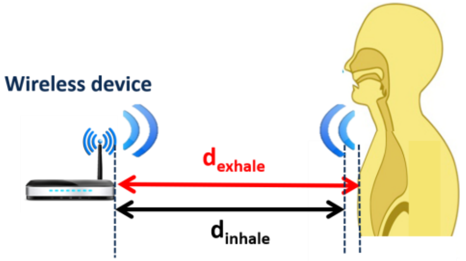
Résumé (December 12, 2018)

- More on Wi-Fi
  - Wi-Fi beaconing
  - Wi-Fi frame format



- Wi-Fi as a sensor
  - Localization
  - Vital signs sensing





Required readings

[Kurose 2013] James F. Kurose and Keith W. Ross. Computer Networking: A Top-Down Approach. Pearson, 6th Edition 2013. **[Section 6.1, 6.2 (excl. 6.2.1), 6.3 (excl. 6.3.4, 6.3.5, and 6.3.6)]**

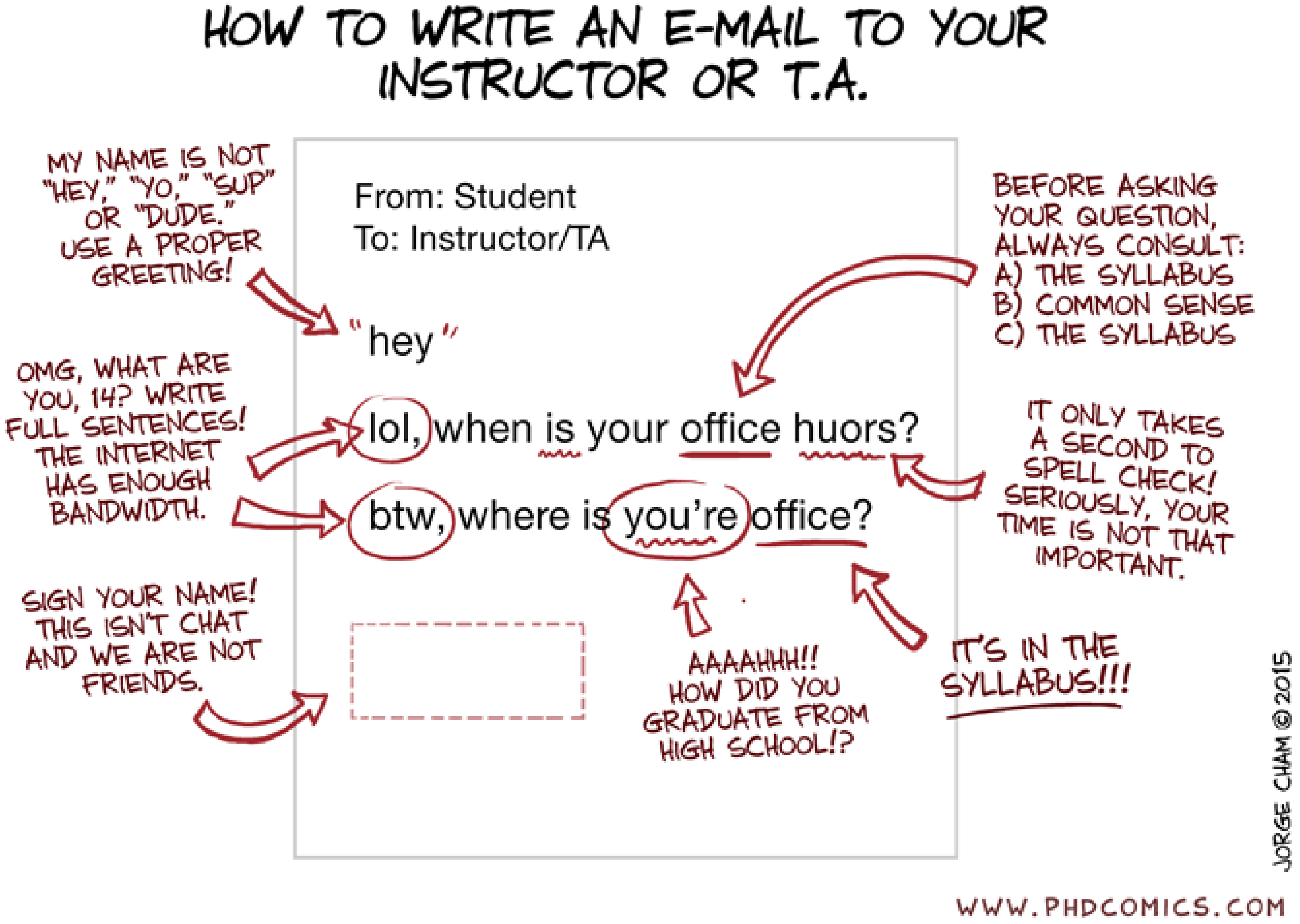
Additional references

[Bolliger 2009] Philipp Bolliger, Kurt Partridge, Maurice Chu, Marc Langheinrich. Improving Location Fingerprinting through Motion Detection and Asynchronous Interval Labeling. Proceedings of the 4th International Symposium Location and Context Awareness (LoCA 2009), Tokyo, Japan, May 7-8, 2009.

Acknowledgments

- The following sources or authors have directly or indirectly contributed (through their ideas, papers, presentations, and more) to the realization of these slides:
  - Philipp Bolliger, Dina Katabi and her research group,
  - and others that might have been omitted unintentionally.

Comic of the day


HOW TO WRITE AN E-MAIL TO YOUR INSTRUCTOR OR T.A.
From: Student
To: Instructor/TA
"hey"
lol, when is your office huors?
btw, where is you're office?
MY NAME IS NOT "HEY," "YO," "SUP" OR "DUDE." USE A PROPER GREETING!
OMG, WHAT ARE YOU, 14? WRITE FULL SENTENCES! THE INTERNET HAS ENOUGH BANDWIDTH.
SIGN YOUR NAME! THIS ISN'T CHAT AND WE ARE NOT FRIENDS.
BEFORE ASKING YOUR QUESTION, ALWAYS CONSULT: A) THE SYLLABUS B) COMMON SENSE C) THE SYLLABUS
IT ONLY TAKES A SECOND TO SPELL CHECK! SERIOUSLY, YOUR TIME IS NOT THAT IMPORTANT.
AAAAHHH!! HOW DID YOU GRADUATE FROM HIGH SCHOOL!?
IT'S IN THE SYLLABUS!!!
JORGE CHAM © 2015
WWW.PHDCOMICS.COM

Source: http://phdcomics.com/comics/archive.php?comicid=1795