TÉCNICO LISBOA

Lab 10: Wi-Fi (IEEE 802.11)

Understanding Wi-Fi

Wi-Fi (IEEE 802.11)

- Goals:
  1. Explore the structure of Wi-Fi frames.
  2. Learn the basics about Wi-Fi (dis)association and data transfer.

(Pseudo-)Evaluation

- Where
  - *Lab 10: Wi-Fi* on Moodle (already opened)
- Submission due
  - Friday, February 4, 23h59
- No comments this time

Wi-Fi (IEEE 802.11)

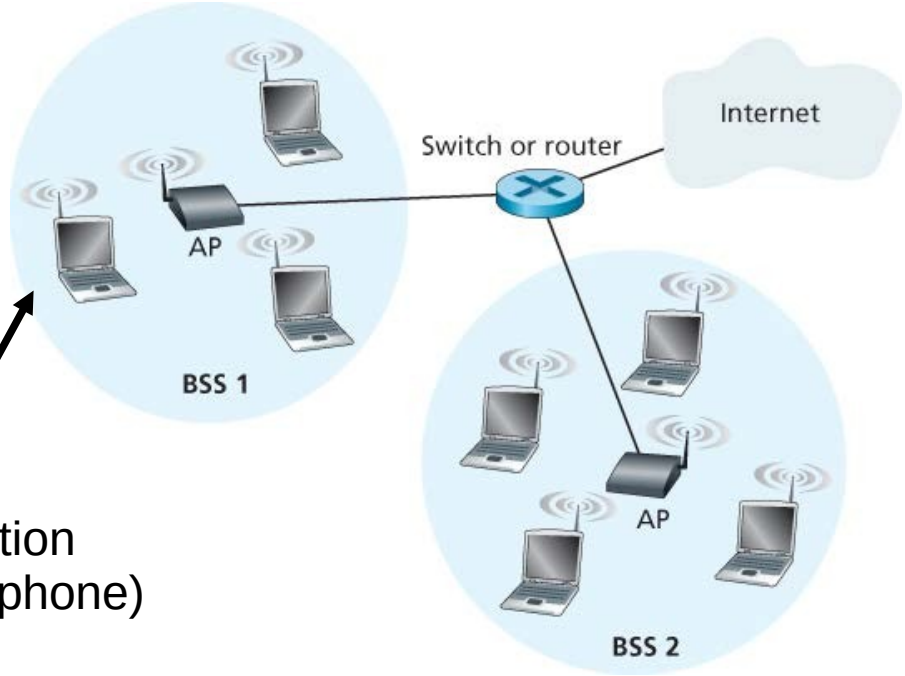
The large family of IEEE 802 standards

- IEEE 802 is a family of standards
  - Applied to local area networks
  - Cover wireless network protocols
  - Divided into different areas of focus

Wi-Fi (IEEE 802.11)

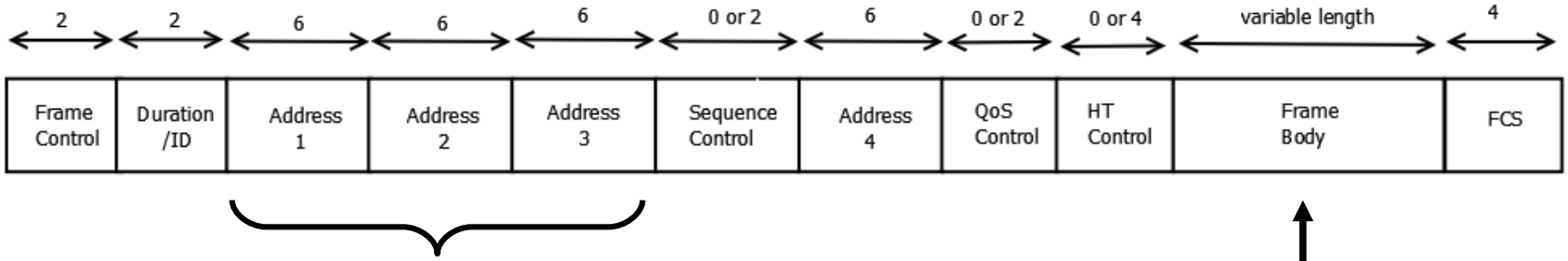
- IEEE 802.11 is also a family of standards
  - Implement wireless LAN (or WLAN) communication
  - Ensures interoperability between different devices connected to the same wireless network (such as laptops, printers, smartphones, or tablets)

Wireless LAN architecture



Wireless station
(like your smartphone)

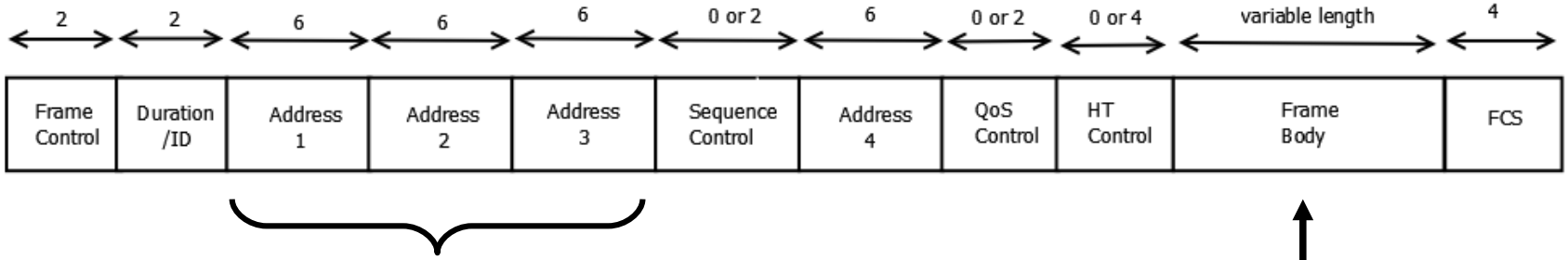
The IEEE 802.11 frame



- 48-bit MAC addresses
- At least, three different addresses are needed

Usually carries IP datagrams

The IEEE 802.11 frame

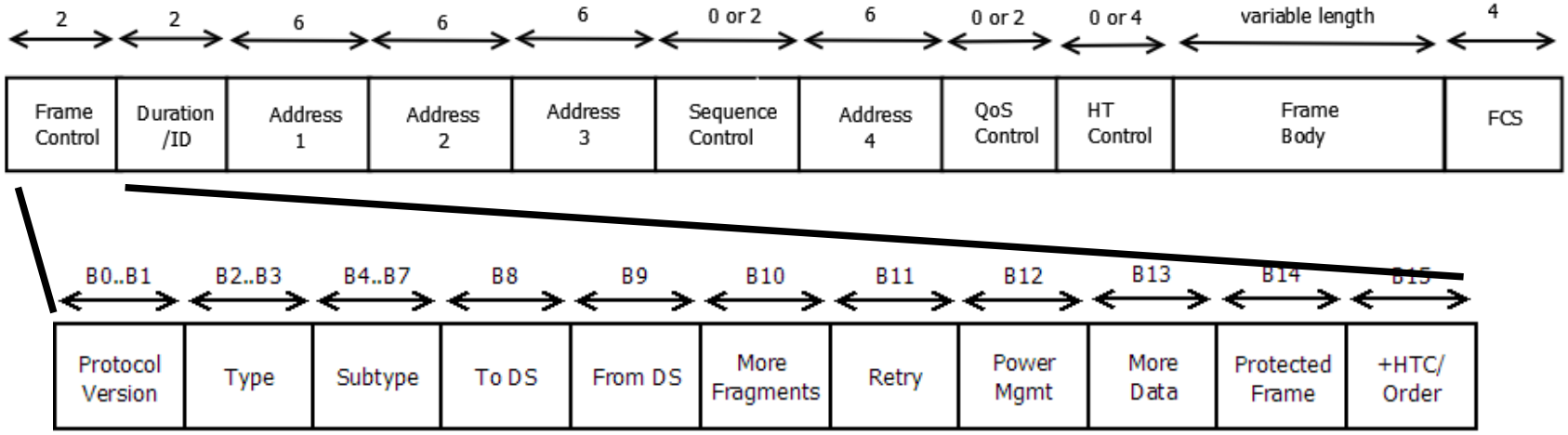


- 48-bit MAC addresses
- At least, three different addresses are needed

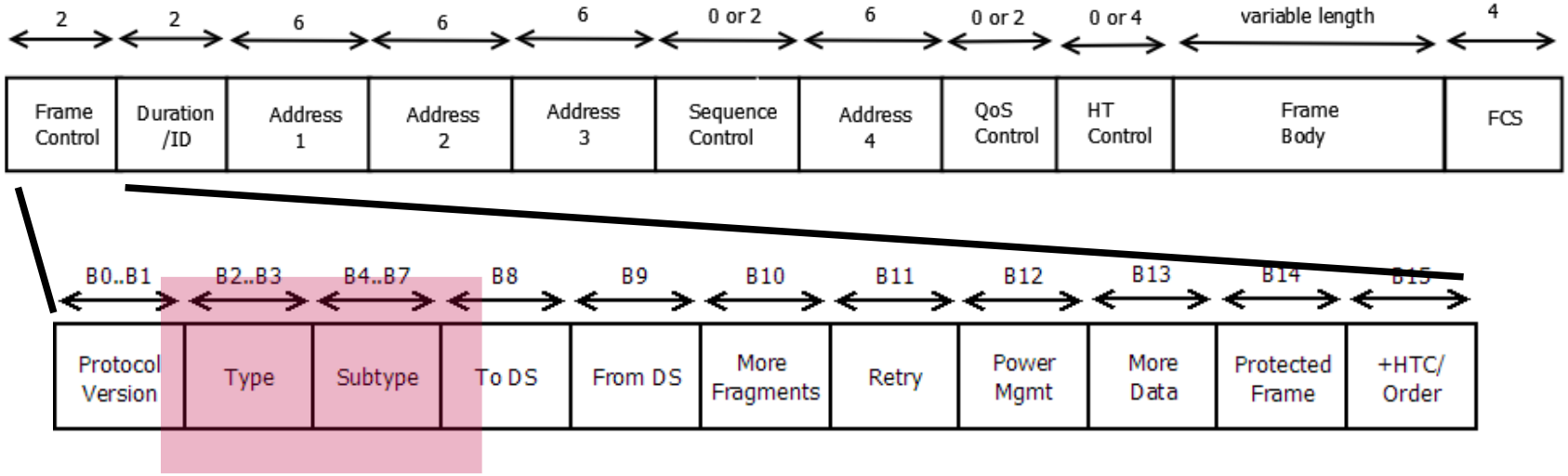
Why?

Usually carries IP datagrams

The IEEE 802.11 frame



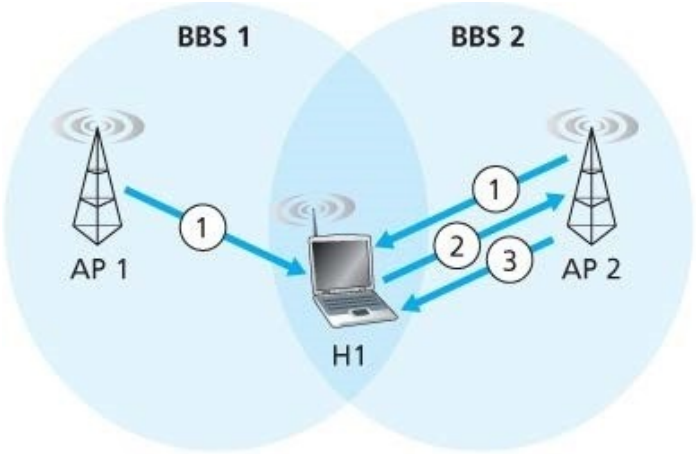
The IEEE 802.11 frame



Determine the type of the frame (e.g.: **beacon**, **association request**, etc.)

Access point association

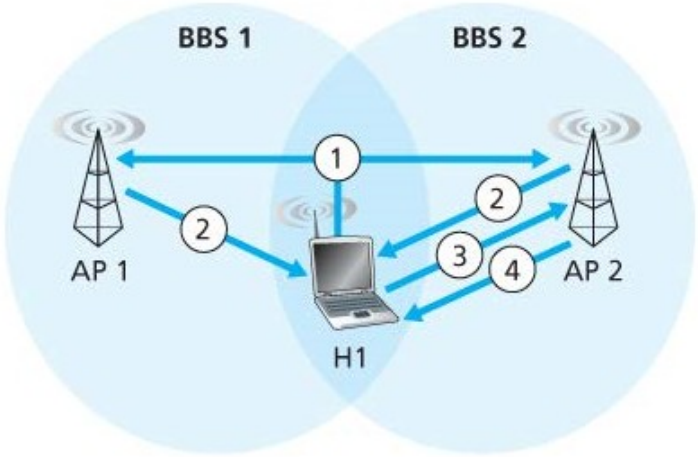
Passive scanning



1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: Selected AP to H1

Access point association

Active scanning



1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent:
   H1 to selected AP
4. Association Response frame sent:
   Selected AP to H1