Wireless LANs

Slide Set 10

Characteristics of wireless LANs

Advantages

Flexibility and Mobility: very flexible within the reception area

Planning: *Ad-hoc* networks without previous planning possible

Design: (almost) no wiring difficulties (e.g. historic buildings, harzardous media, firewalls)

Robustness: more robust against disasters like, e.g., earthquake, fire or flood...

Cost: Adding additional users to a wireless network will not increase the cost. Cheap Hardware.

Disadvantages

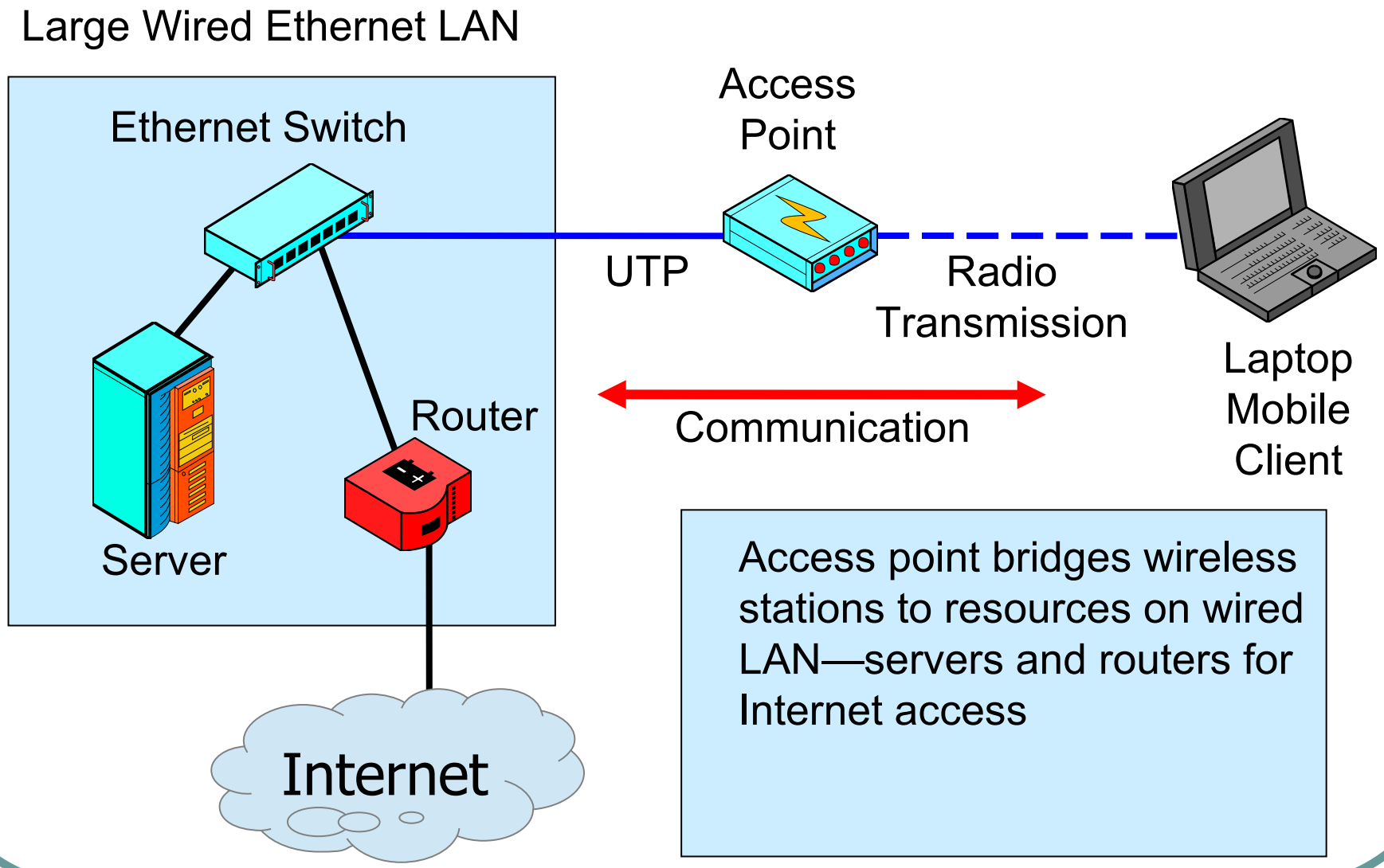
Throughput: typically lower speed compared to wired networks but increasing everyday.

Proprietary solutions: many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11). Now, 802.11n is a popular solution.

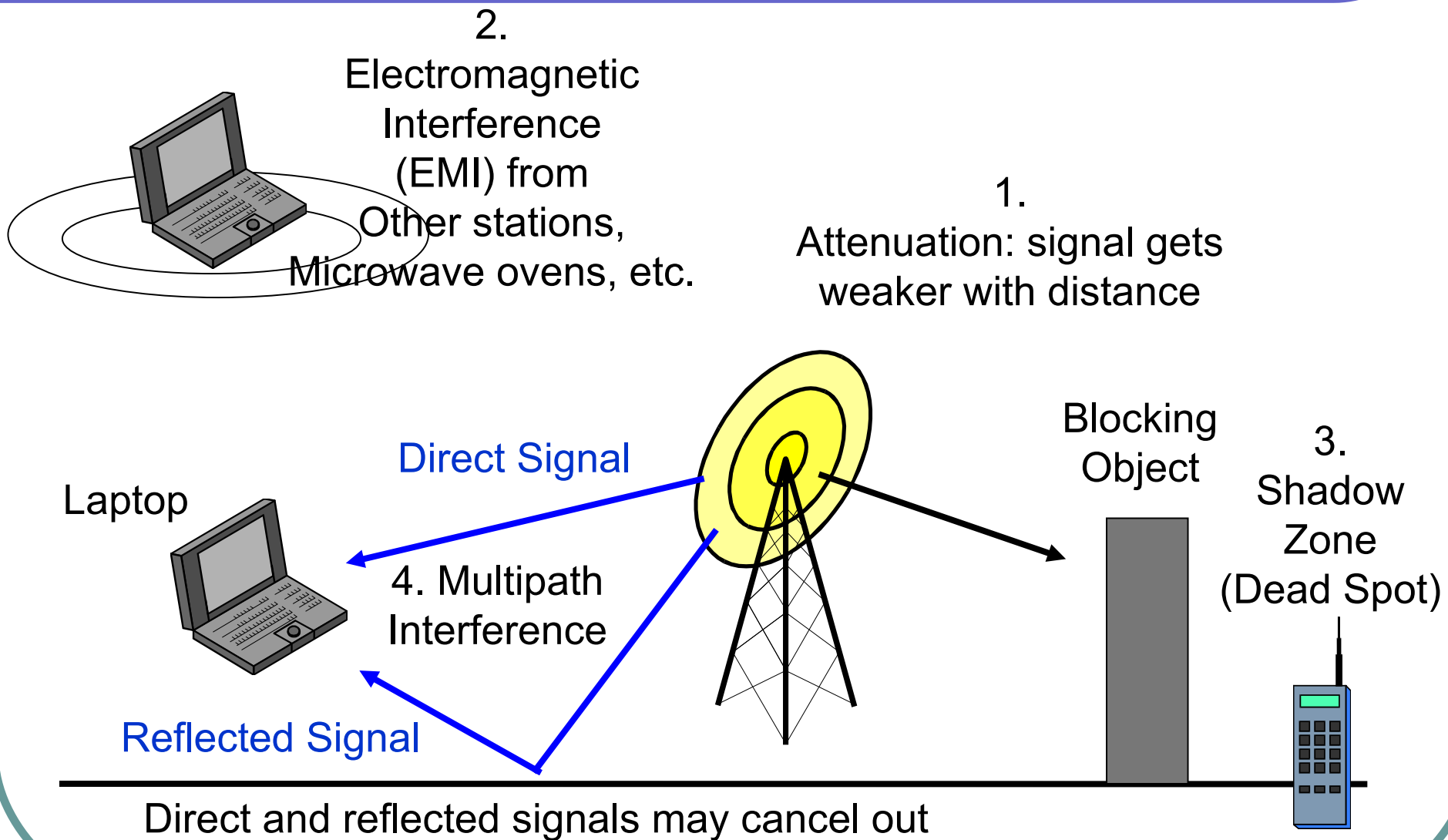
Legal Restrictions: Have to conform to many national restrictions if working with wireless.

Safety and Security: Precautions have to be taken to prevent safety hazards and interference. Confidentiality and integrity must be enforced.

Wireless LAN (WLAN) Access Point



Wireless Propagation Problems

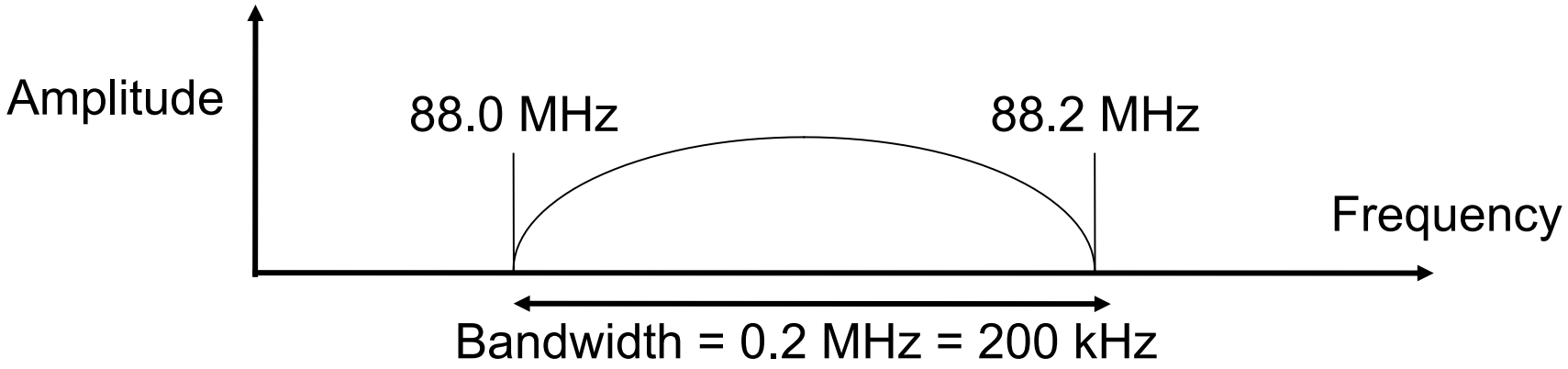


Wireless Propagation Problems

- Some problems are Frequency-Dependent
  - Higher-frequency signals attenuate faster
    - Absorbed more rapidly by moisture in the air
  - Higher-frequency signals blocked more by obstacles
    - At lower frequencies, signal refract (bend) around obstacles like an ocean wave hitting a buoy
    - At higher frequencies, signals do not refract; leave a complete shadow behind obstacles

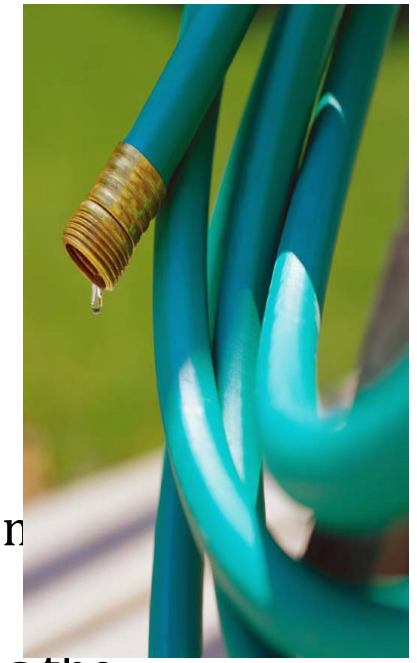
Channel Bandwidth

- Channel Bandwidth
  - An 88.0 MHz to 88.2 MHz channel (FM radio) has a bandwidth of 0.2 MHz (200 kHz)
  - Higher-speed signals need wider bandwidths



Transmission Speed

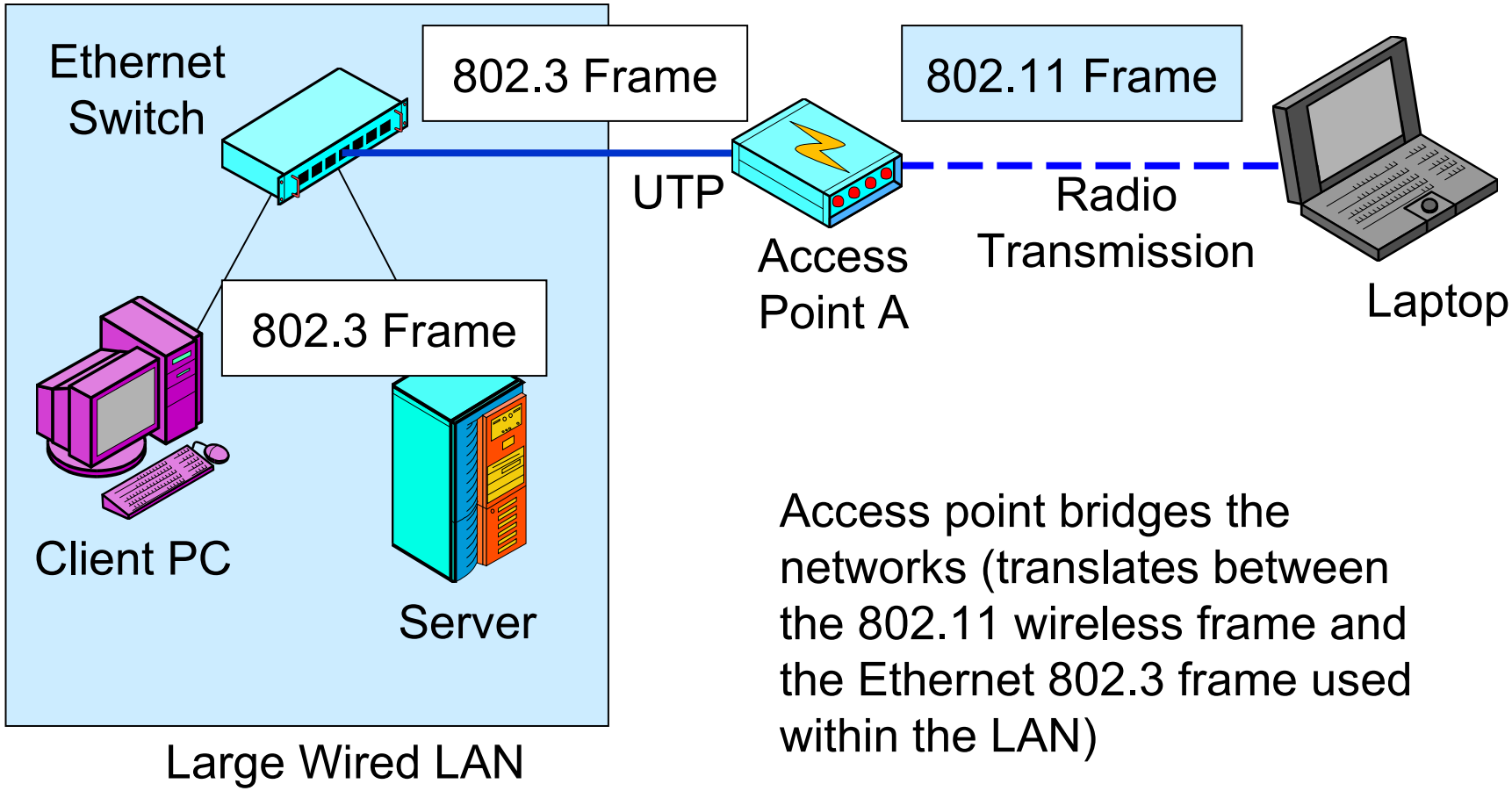
- Shannon Capacity Theorem
  - $C=B \log_2 (1+S/N)$
    - C = Maximum possible transmission speed in the channel (bps)
    - B = Bandwidth (Hz) (Like thickness of a hose)
    - S/N = Signal-to-Noise power
  - Note that doubling the bandwidth (B) doubles the maxin transmission speed
  - More generally, increasing the bandwidth by X increases the maximum possible speed by X
  - Increasing S/N helps slightly but usually cannot be done to any significant extent



The Golden Zone

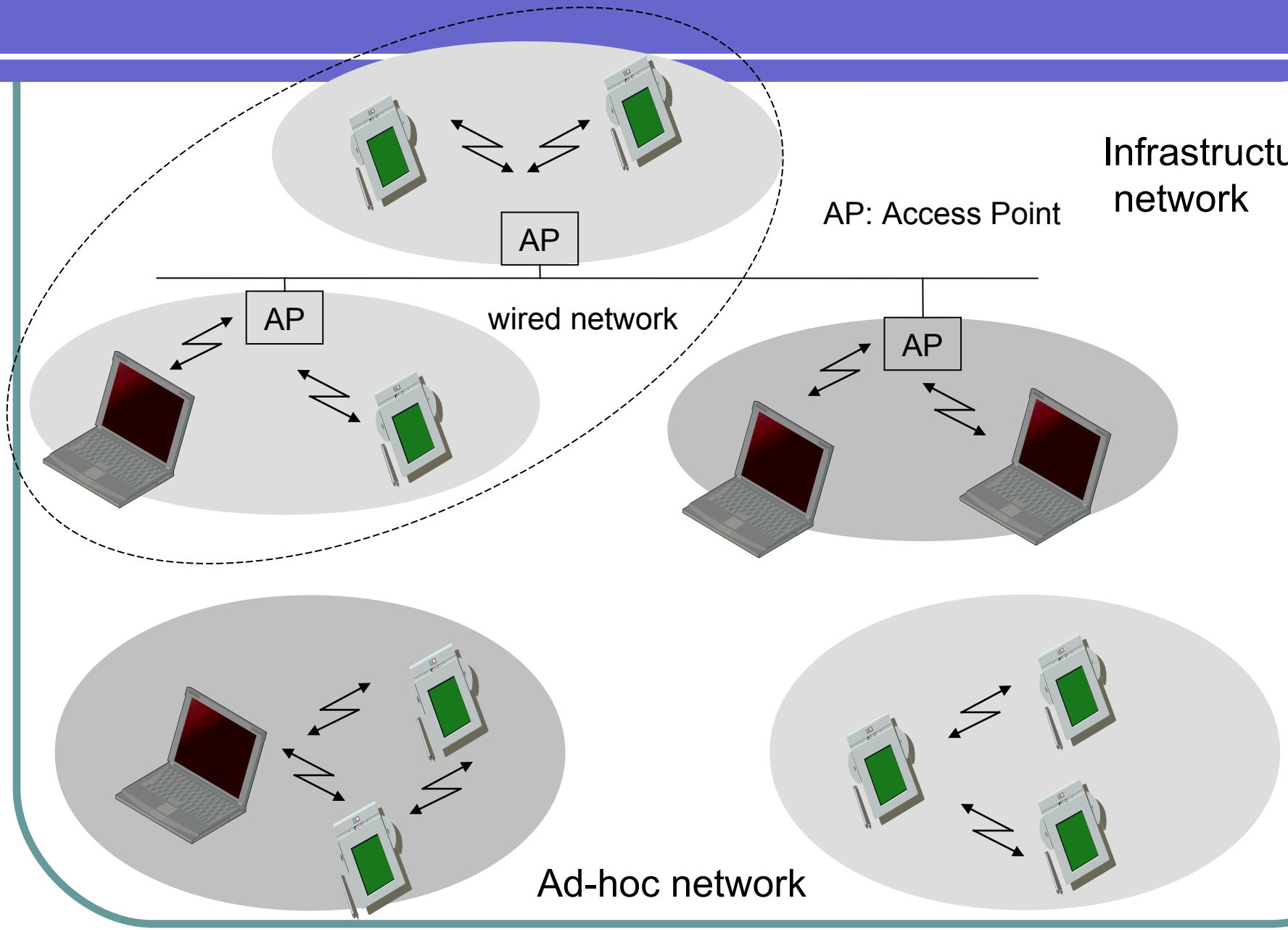
- The Golden Zone
  - Most organizational radio technologies operate in the “golden zone”
  - High megahertz to low gigahertz range
  - At higher frequencies, there is more available bandwidth
  - At lower frequencies, signals propagate better.
  - Frequencies should be high enough for there to be large total bandwidth
  - Frequencies should be low enough to allow fairly good propagation characteristics.

Typical 802.11 Wireless LAN Operation with Access Points

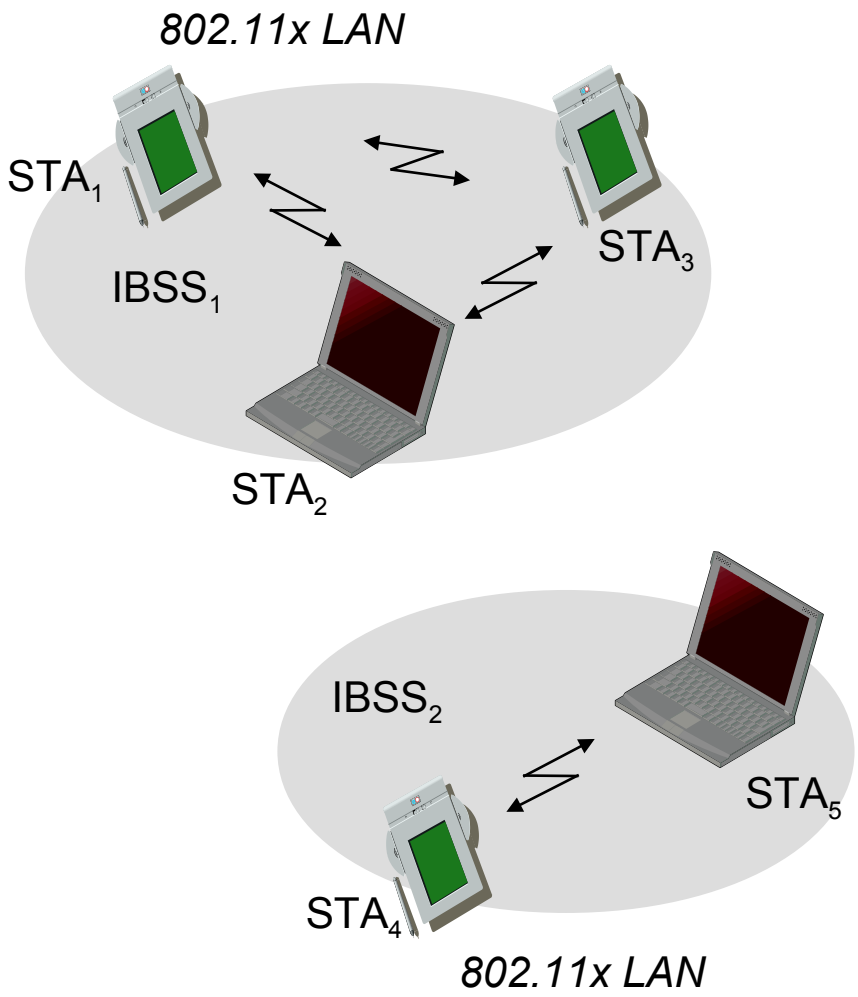


Access point bridges the networks (translates between the 802.11 wireless frame and the Ethernet 802.3 frame used within the LAN)

Infrastructure Mode vs. Ad-hoc Mode



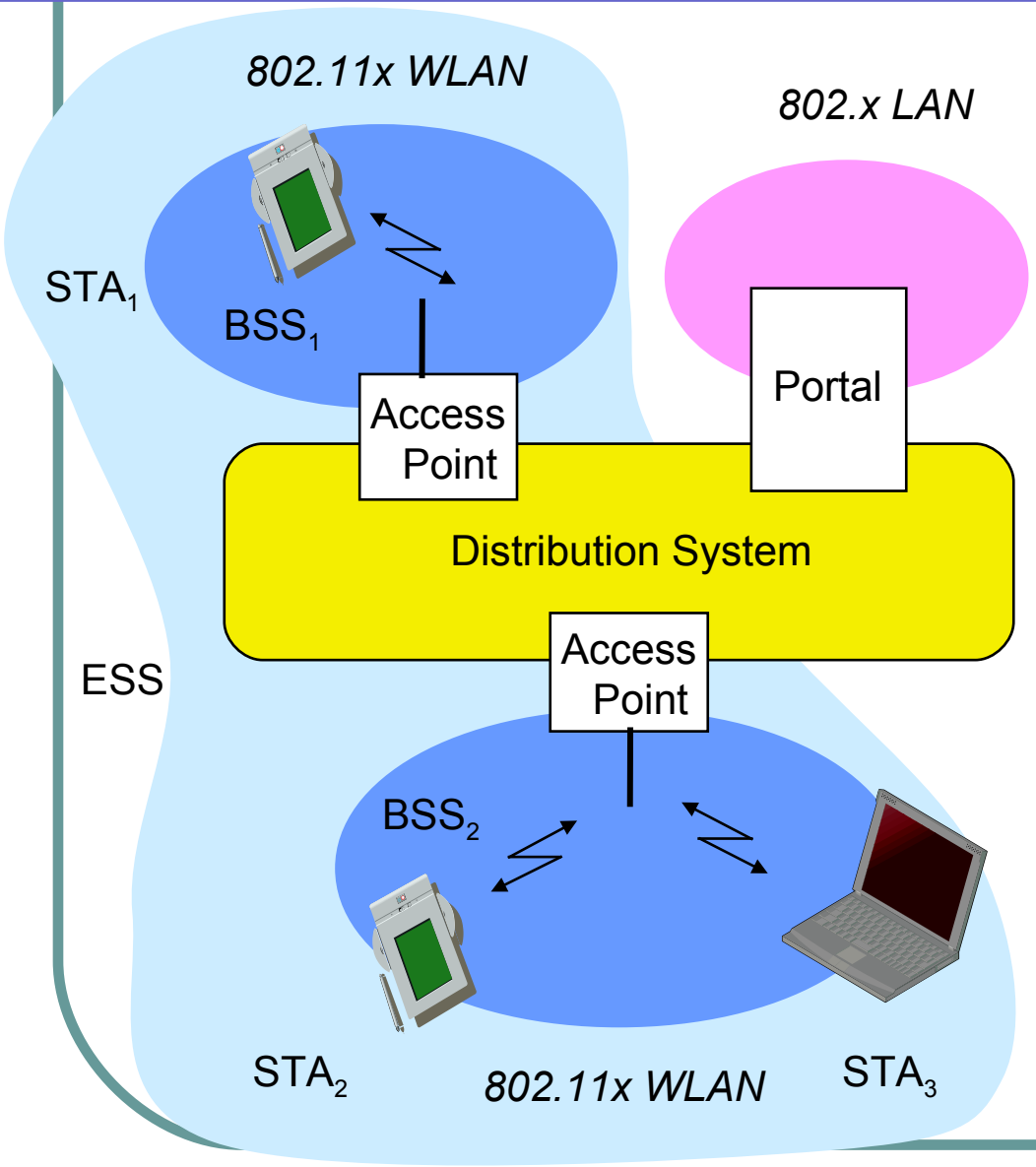
802.11 - Architecture of an *ad-hoc* network



Direct communication within a limited range:

- Station (STA): terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS): group of stations using the same radio frequency

Architecture of an infrastructure network



Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point (AP)

- station integrated into the wireless LAN and the distribution system

Portal

- bridge to other (wired) networks

Distribution System

- interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

802.11x Wireless Access Point and Wireless LAN Adapters (PCMCIA, PCI & USB)

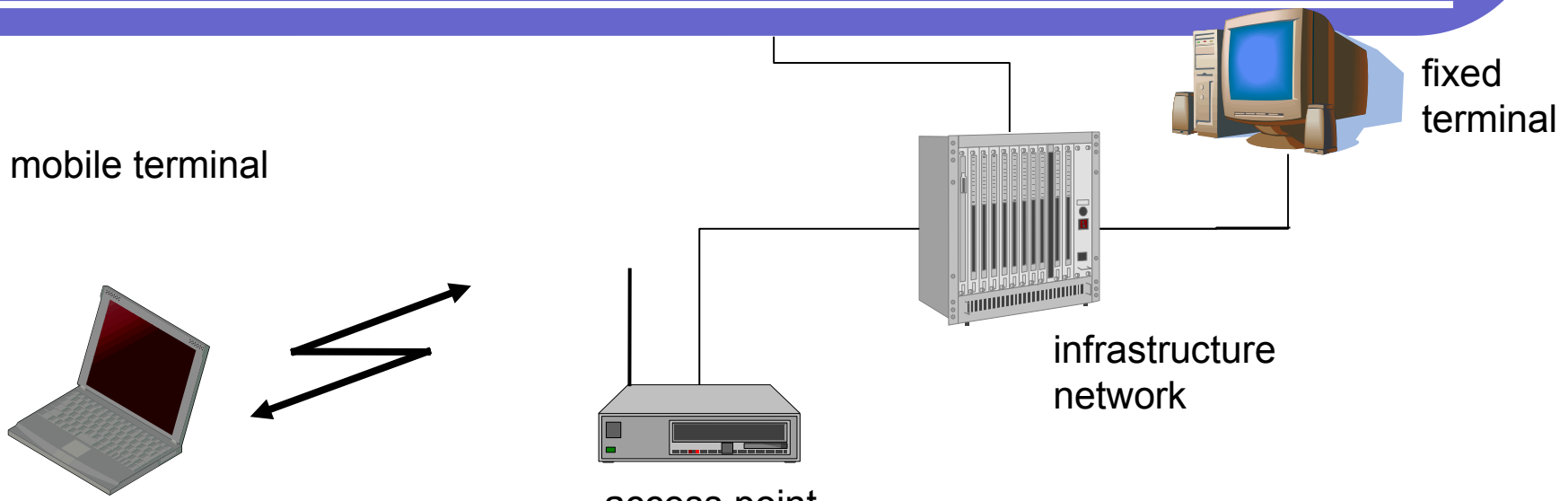
A 802.11g Access Point with two antennas

USB: Most popular and portable. Works with any device with USB ports

PCMCIA: used in
old laptops with no built-in WLAN Adapter

PCI: used in Desktop PCs

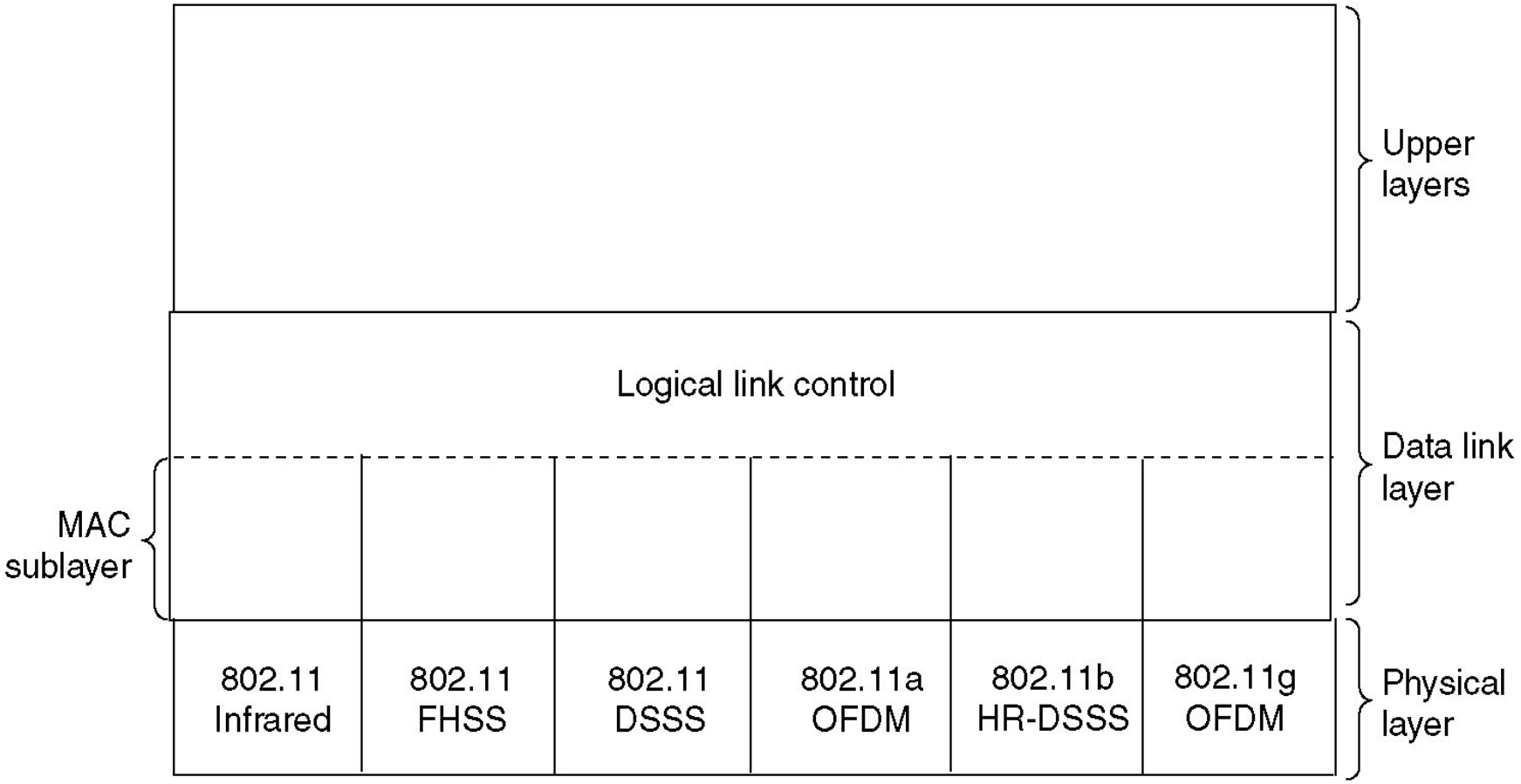
IEEE standard 802.11



application		application
TCP		TCP
IP		IP
LLC	LLC	LLC
802.11 MAC	802.11 MAC / 802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY / 802.3 PHY	802.3 PHY

The 802.11 Protocol Stack

Part of the 802.11 protocol stack.



802.11 - Frame format

Types

- control frames, management frames, data frames

Sequence numbers

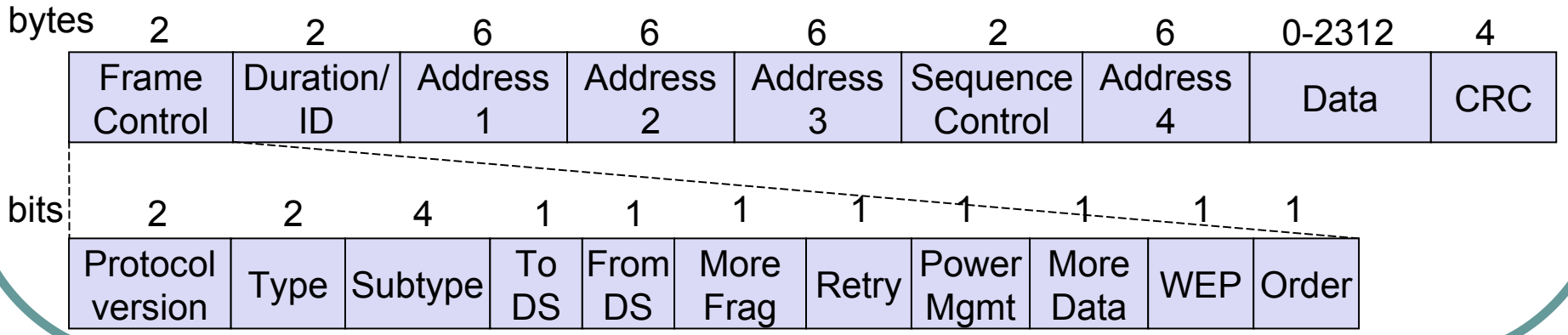
- important against duplicated frames due to lost ACKs

Addresses

- receiver, transmitter (physical), BSSID, sender (logical)

Miscellaneous

- sending time, checksum, frame control, data



MAC address Configurations

scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	DA	SA	BSSID	-
infrastructure network, from AP	0	1	DA	BSSID	SA	-
infrastructure network, to AP	1	0	BSSID	SA	DA	-
infrastructure network, within DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address

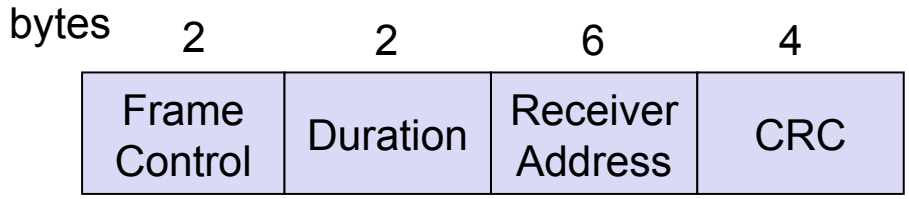
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

- *Ad-hoc* network: packet exchanged between two wireless nodes without a distribution system
- Infrastructure network, from AP: a packet sent to the receiver via the access point
- Infrastructure network, to AP: a station sends a packet to another station via the access point
- Infrastructure network, within DS: packets transmitted between two access points over the distribution system.

Special Frames: ACK, RTS, CTS

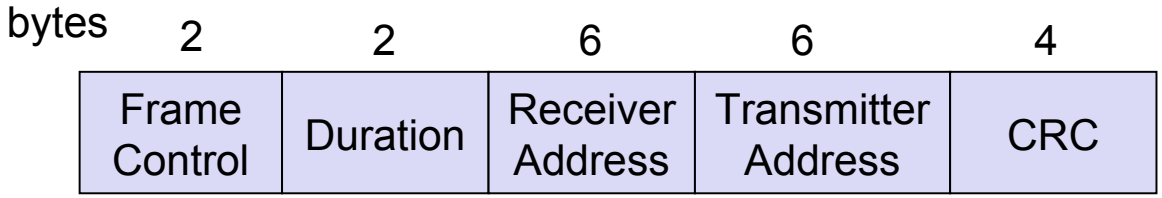
Acknowledgement

ACK



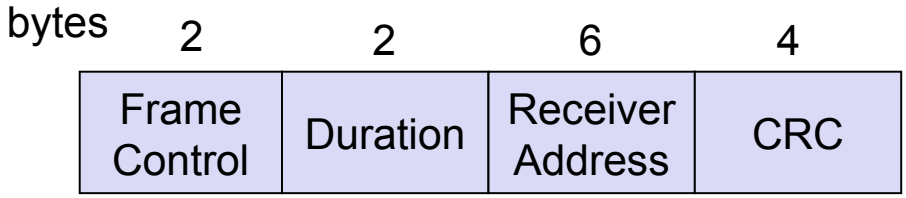
Request To Send

RTS



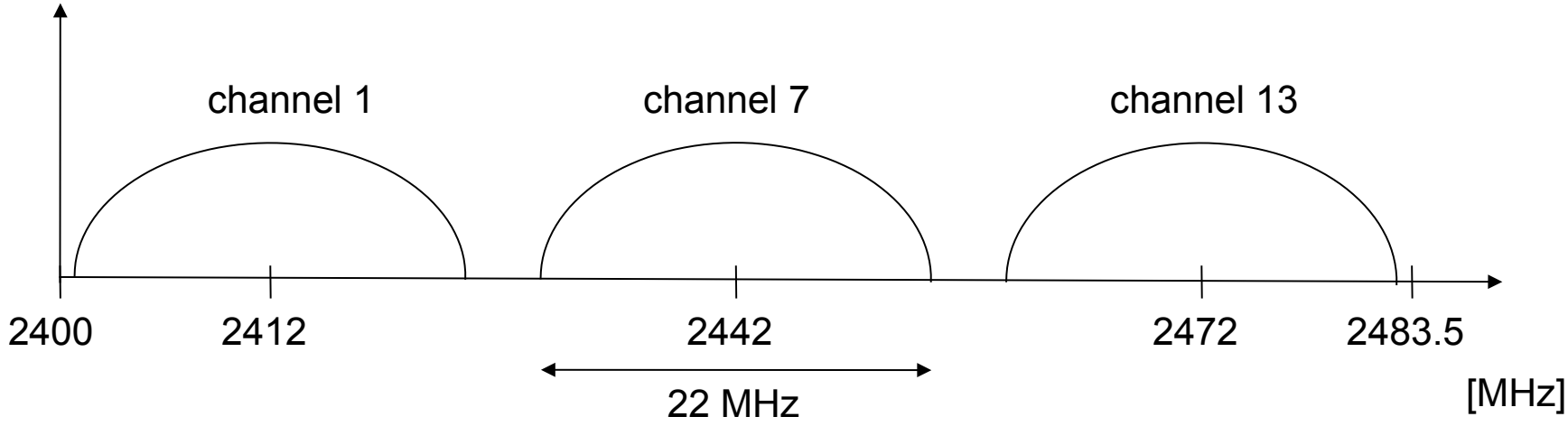
Clear To Send

CTS

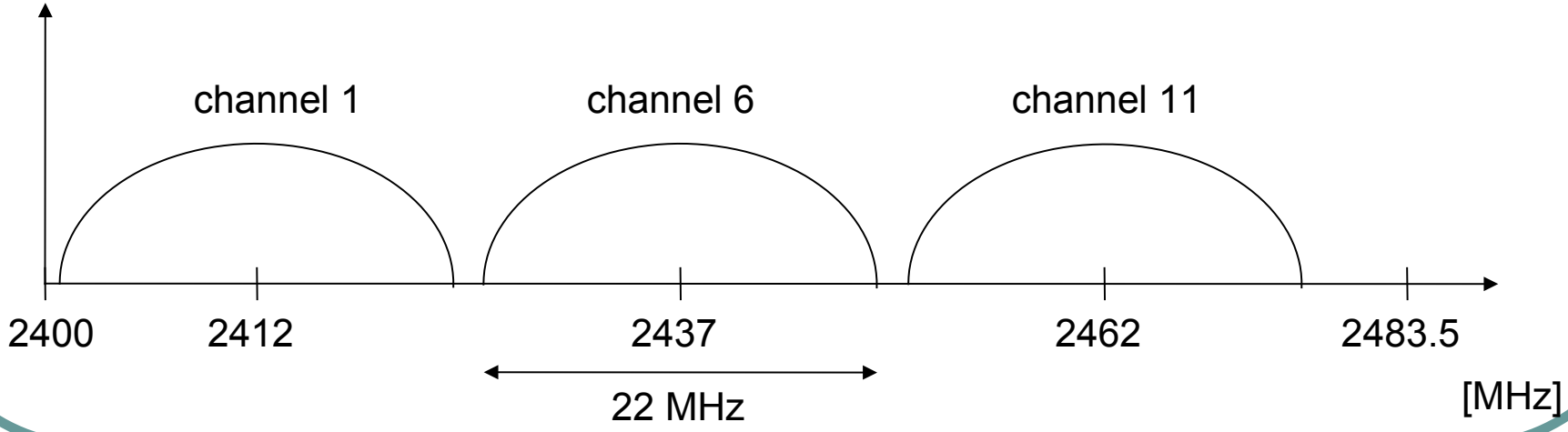


Channel selection (non-overlapping)

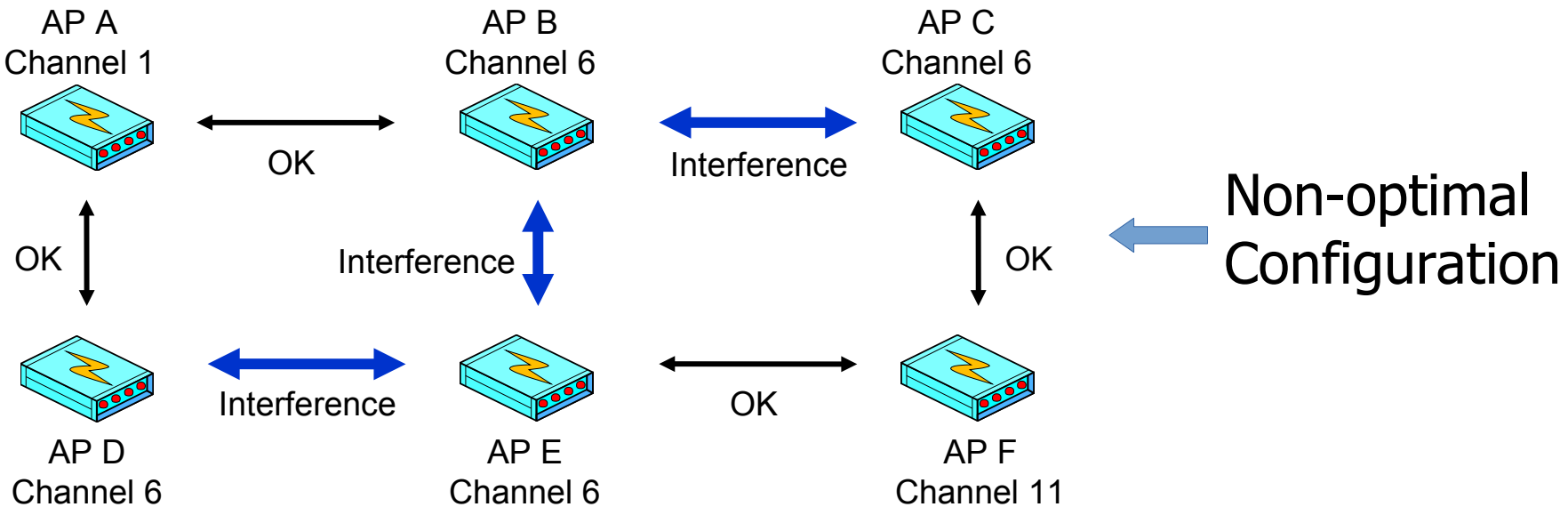
Europe (ETSI)



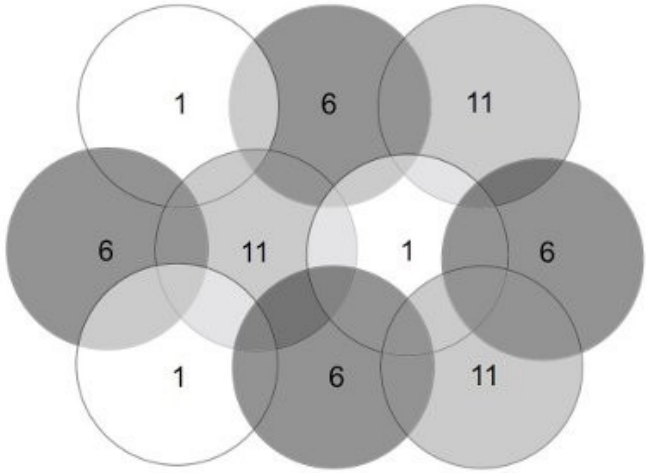
US (FCC)/Canada (IC)



4 or more AP Configuration for minimal Interference in close vicinity



Optimal Configuration



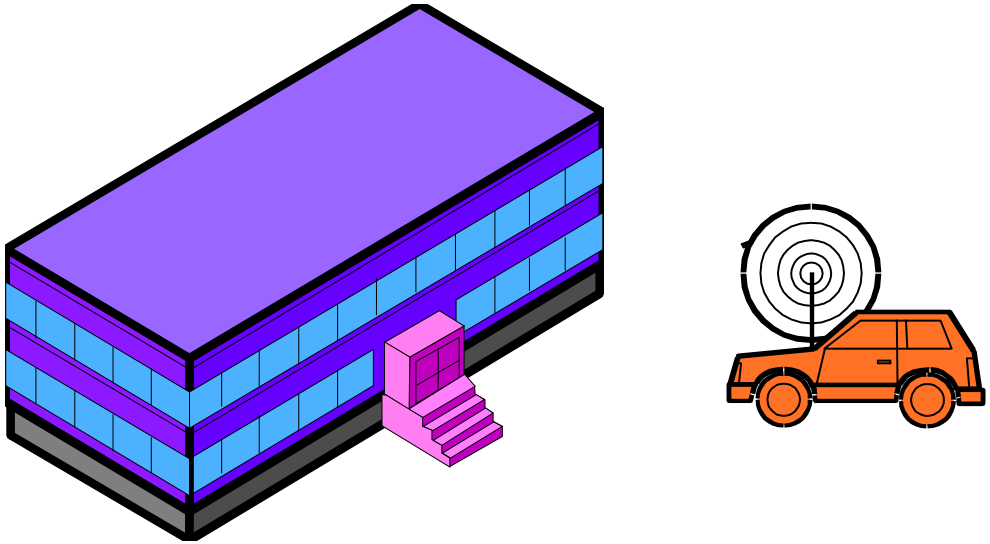
802.11 Wireless LAN Standards

802.11-Standard	Standard Year	Frequency (GHz)	Bandwidth (MHz)	Modulation Type	Max. Data Rate (Mbit/s)
802.11a	1999	5 GHz	20 MHz	OFDM	54 Mbit/s
802.11ac	2013	5 GHz	40/80/160	OFDM	6,93 Gbit/s
802.11ad	2012	60 GHz	2160	SC-OFDM	6,76 Gbit/s
802.11b	1999	2,4 GHz	20	DSSS	11 Mbit/s
802.11g	2003	2,4 GHz	20	DSSS/OFDM	54 Mbit/s
802.11n	2009	2,4/5 GHz	20/40	OFDM	600 Mbit/s

DSSS, direct sequence spread spectrum
FHSS, frequency hopping spread spectrum
OFDM, orthogonal frequency division multiplex
SC-OFDM, single carrier orthogonal frequency division multiplex

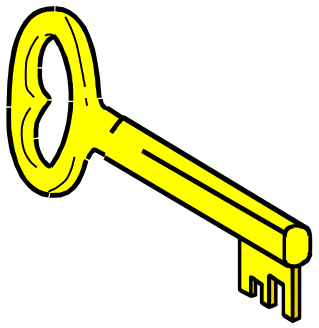
802.11x Security

- Automated Drive-By Hacking (War Driving)
  - Can read traffic from outside the corporate walls
  - Can also send malicious traffic into the network



802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Initial flawed security method developed by the 802.11 Working Group for 802.11 devices
  - All stations share the same encryption key with the access point
  - This key is cannot be changed
  - This is a shared static key

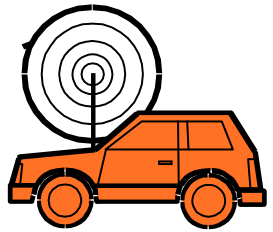


802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Shared static keys means that a large volume of traffic is encrypted with the same key
  - With so much traffic generated with one unchanging key, cryptanalysts (code-breakers) can crack the key by collecting data for a few days
  - Once the key is cracked, the attacker can read all messages and send attack messages into the network without going through a firewall filter

802.11 Security, Continued

- Wired Equivalent Privacy (WEP)
  - Software that automates the hacking process is widely available e.g. AirSnort
    - Locate vulnerable access points by driving around (war driving)
    - Collect traffic and crack the key
    - **No longer recommended to use WEP nowadays**



802.11 Security, Continued

- 802.11i Security
  - Products started becoming available in late 2003
- WiFi Protected Access (WPA)
  - Stopgap security method introduced before full 802.11i security could be developed
  - Introduced some parts of 802.11i in 2002 and 2003
  - It was often possible to upgrade older WEP products to WPA

802.11 Security, Continued

- 802.11i Security (WPA2) (Stronger than WPA)
  - Later, 802.11 Working Group introduced strong security
    - 802.11i
  - 802.11i specifies the Temporal Key Integrity Protocol (TKIP)
    - Each station gets a separate key for confidentiality
    - This key can be changed frequently

802.11 Security, Continued

- Ways to strengthen your Wireless LAN
  - Do not use WEP. Use WPA or WPA2 instead
  - Enforce MAC address Association (i.e only allowed wireless adapters can join your wireless network)
  - Disable BSSID broadcast once all permitted stations have been allowed to join the wireless network.
  - Enable Access Point firewall features to prevent potential attacks.

802.11 Security, Continued

- The Transition to Strong Security
  - We will soon have a mix of no security, WEP, 802.11i, WPA, and other security protocols
  - Only as strong as the weakest link
  - Legacy equipment that cannot be upgraded to 802.11i will have to be discarded
  - (802.11i is sometimes called WPA2)

802.11 Security, Continued

- Rogue Access Points
  - Unauthorized access points set up by department or individual
  - Often have very poor security, leaving a big opening for hackers
  - Often operate at high power, attracting many clients to these access points with weak security