Wireless network technologies: WLAN, WPAN, ad hoc networks

Prof. Fabio Martignon

Summary (1)

- Introduction to wireless networks
  - Main differences with wired networks
  - Radio channel
  - Mobility management
- WLAN
  - 802.11 standards
  - Network architecture
  - MAC (legacy and QoS MAC 802.11e)

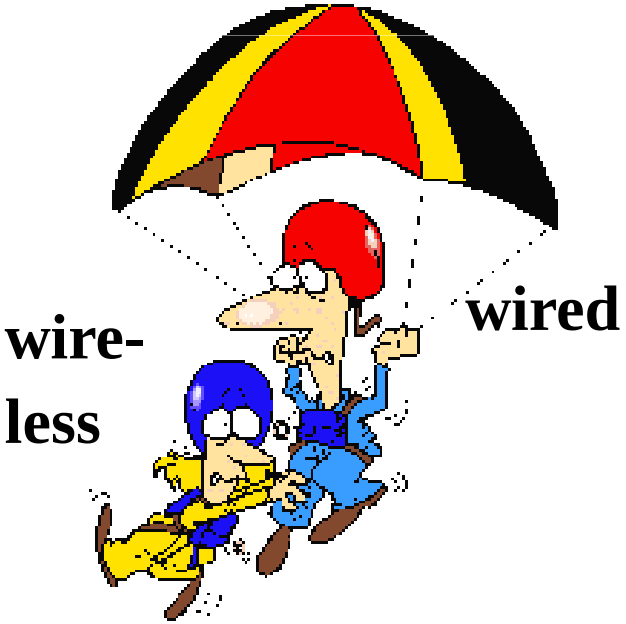
Summary (2)

- WPAN
  - Bluetooth
    - Network architecture
    - Medium access control
    - Network formation
  - ZigBee
    - Network architecture
    - Medium access control
- Ad Hoc
  - Definitions and basic networking issues
  - Routing schemes

Wireless Networks

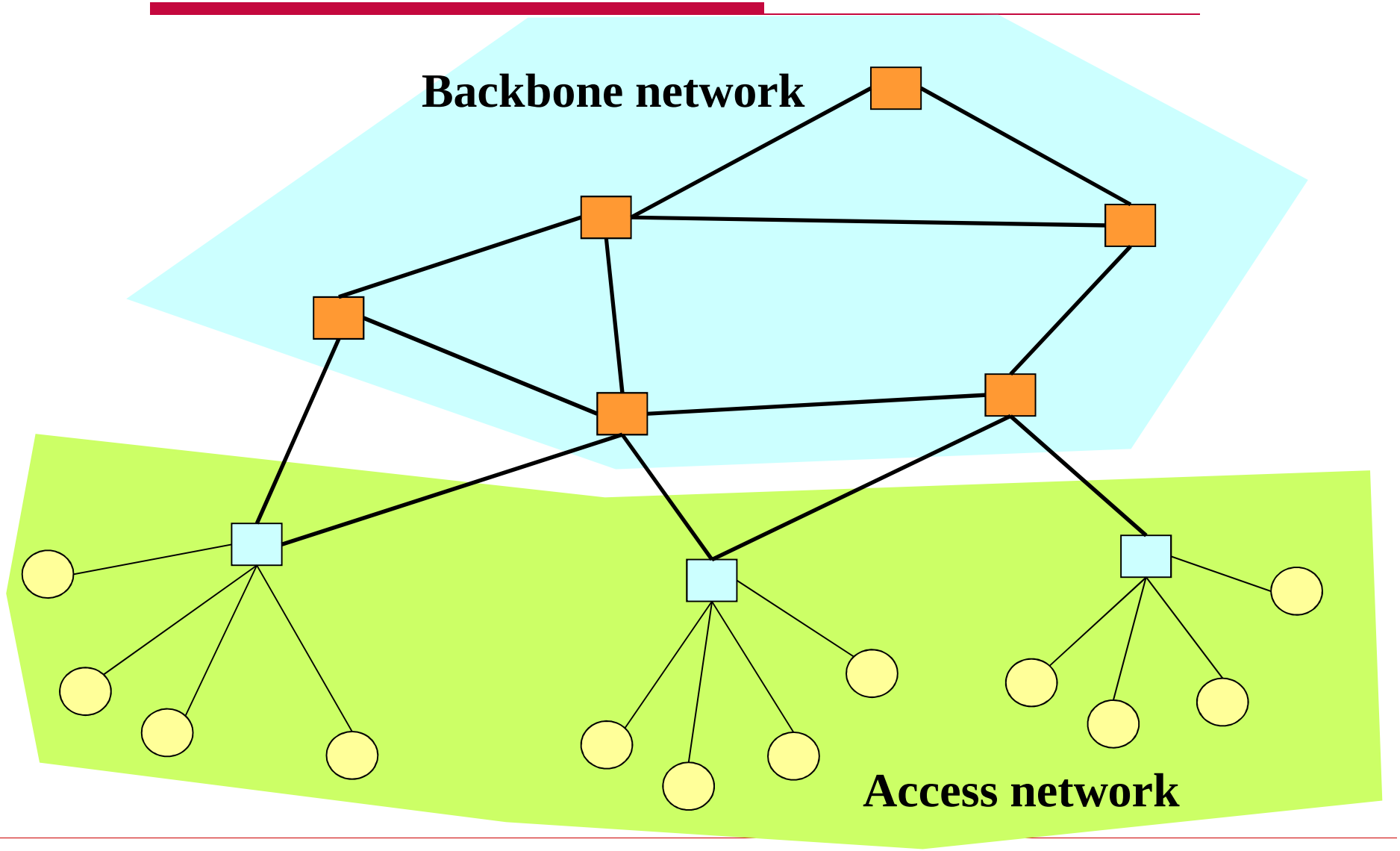
Wireless or wired, which is better?

Well, it depends on the situation!



- Is the transmission medium the only difference?
  - The peculiar medium characteristics have great impact on system characteristics
  - Wireless networks allow users to move and naturally manage mobility

Network architecture

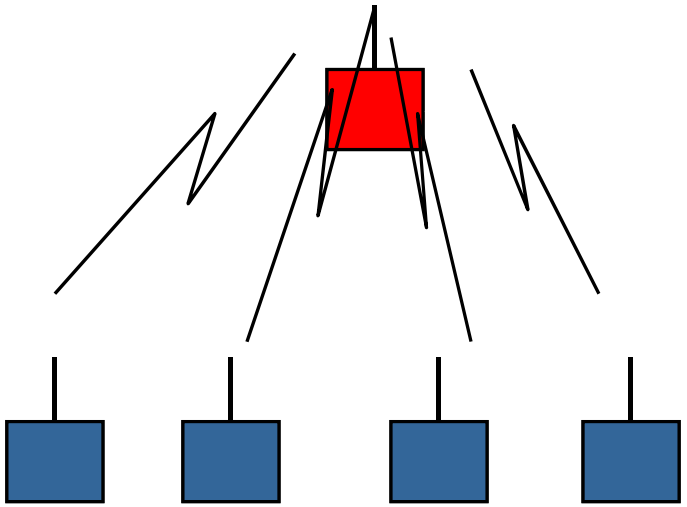


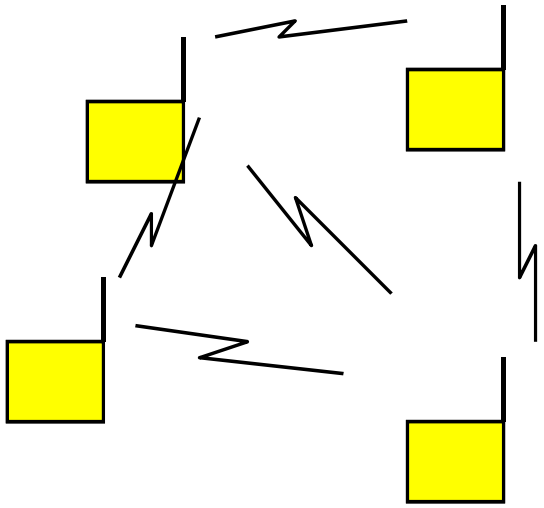
Wireless access networks

- Wireless networks are mainly access networks
- Backbone networks composed of radio point-to-point links are usually not considered wireless networks
- Wireless access networks are more challenging and have many fundamental differences with respect to wired access networks
- The first main difference is that the transmission medium is broadcast

Broadcast channel

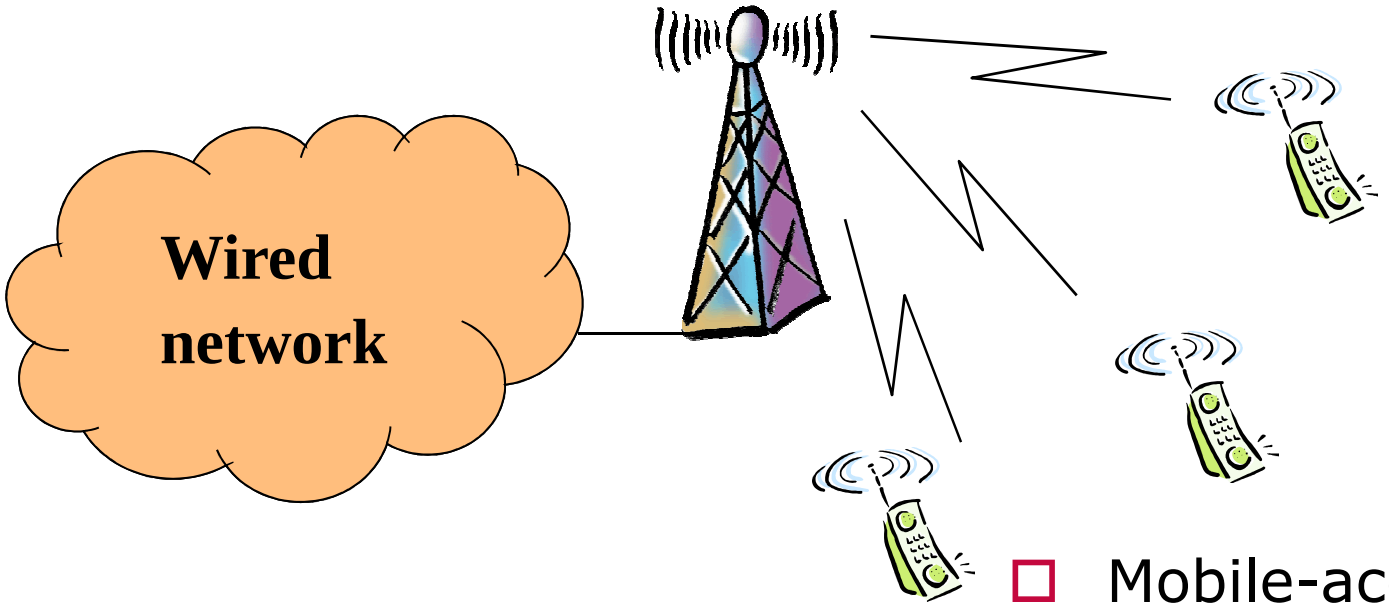
- Centralized broadcast channel
- Distributed broadcast channel





Centralized broadcast channel

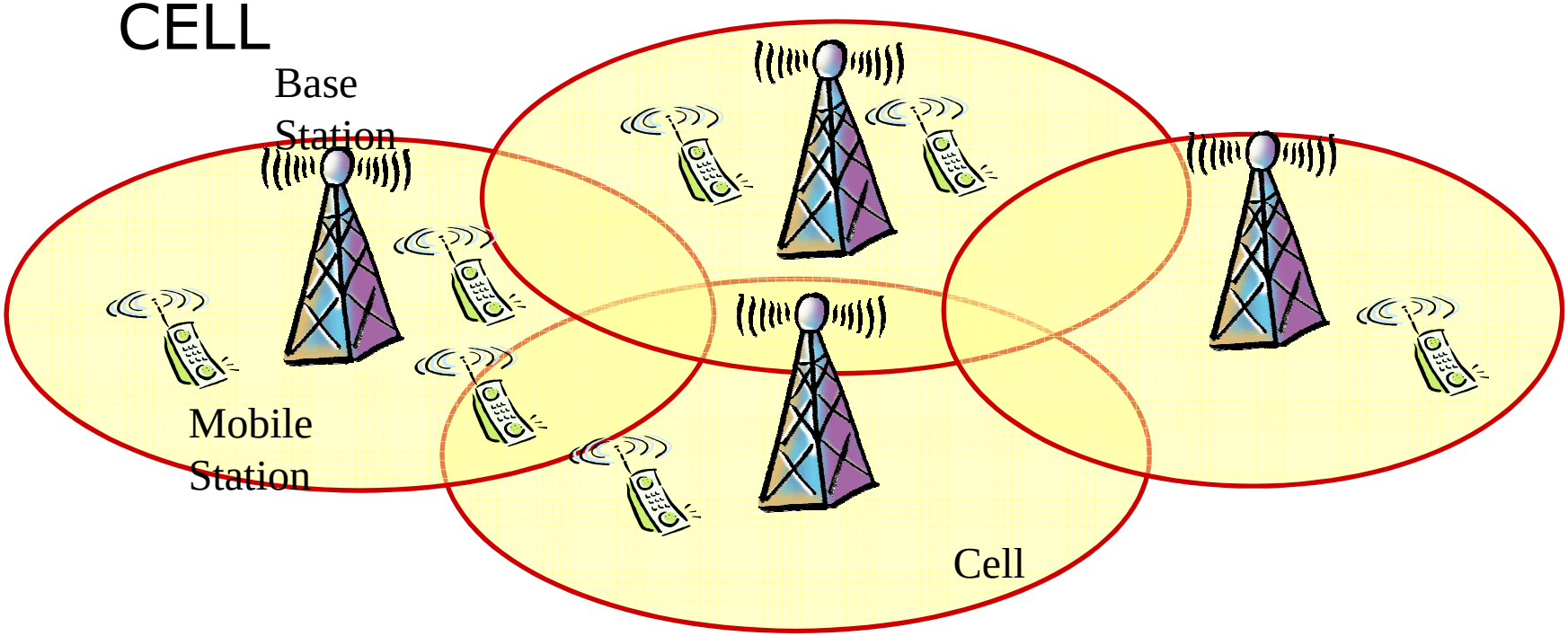
- Fixed access point (cellular systems, WLAN, WMAN)



- Mobile-access point connection

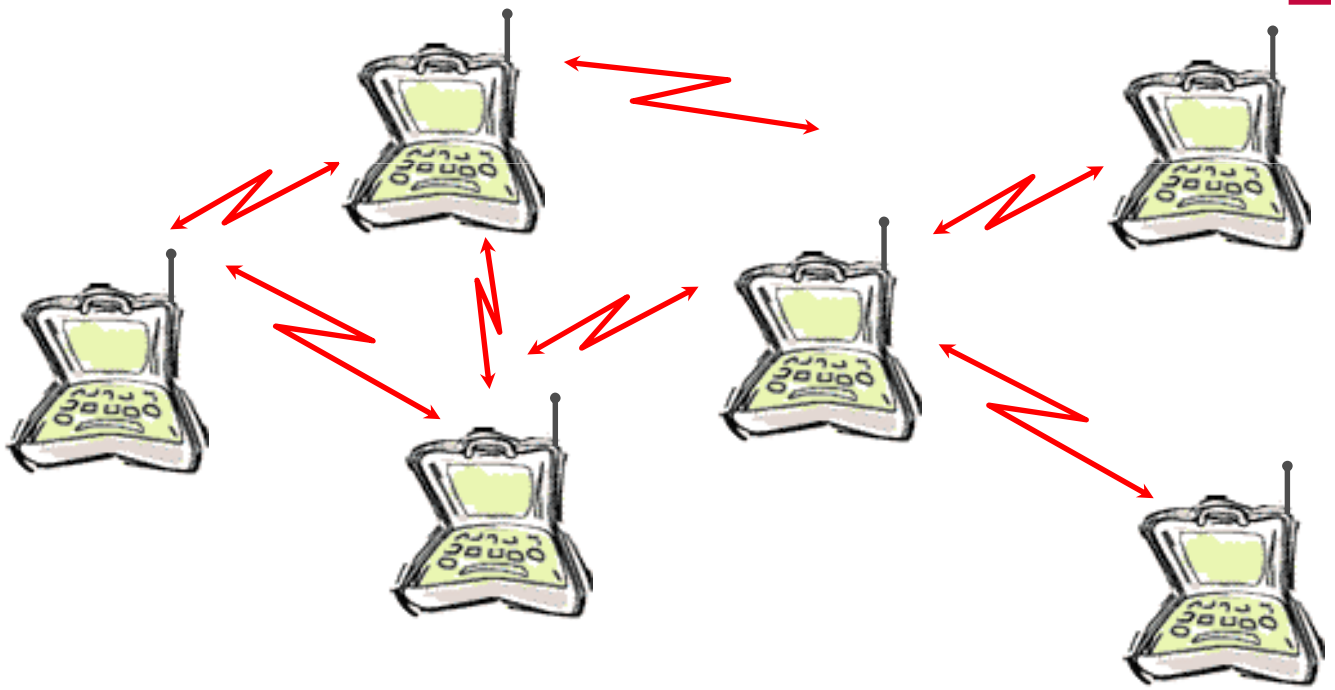
Centralized broadcast channel

- Cellular coverage: The territory coverage is obtained by Base Stations–BS (or Access Points) that provide radio access to Mobile Stations–MS within a service area called CELL



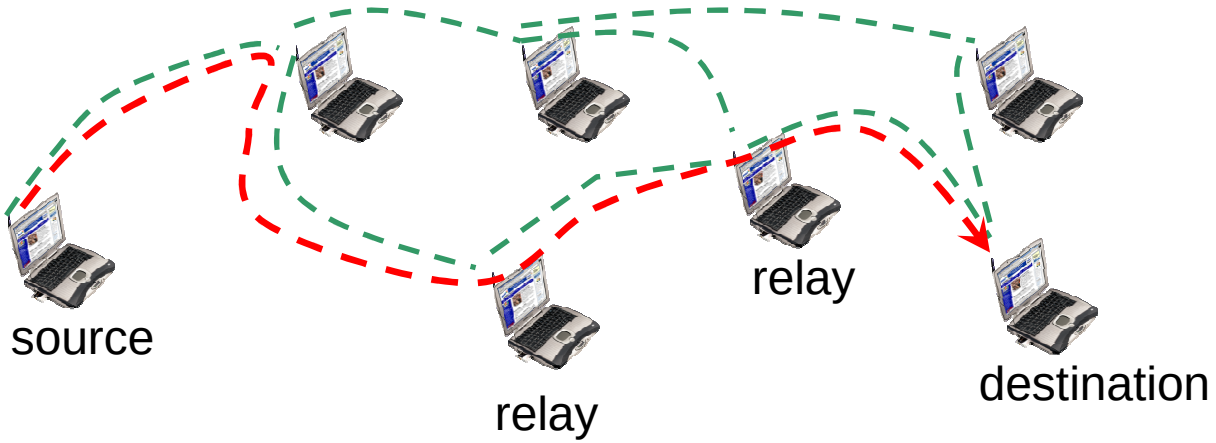
Distributed broadcast channel

- Ad-hoc wireless networks (mesh networks, sensor networks)
  - mobile - mobile connections



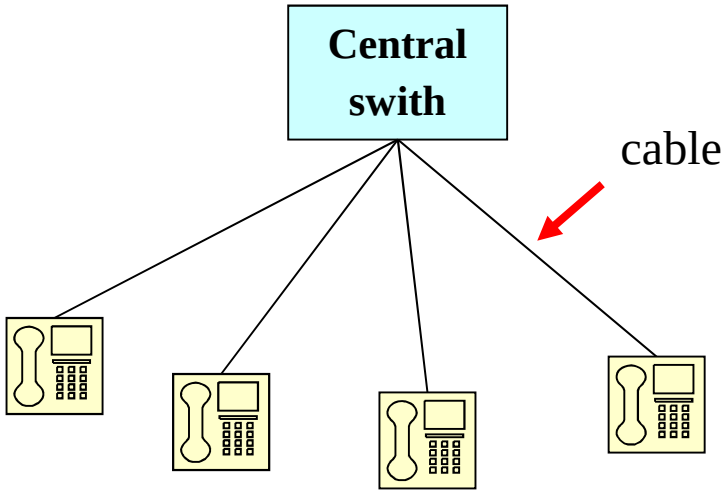
Distributed broadcast channel

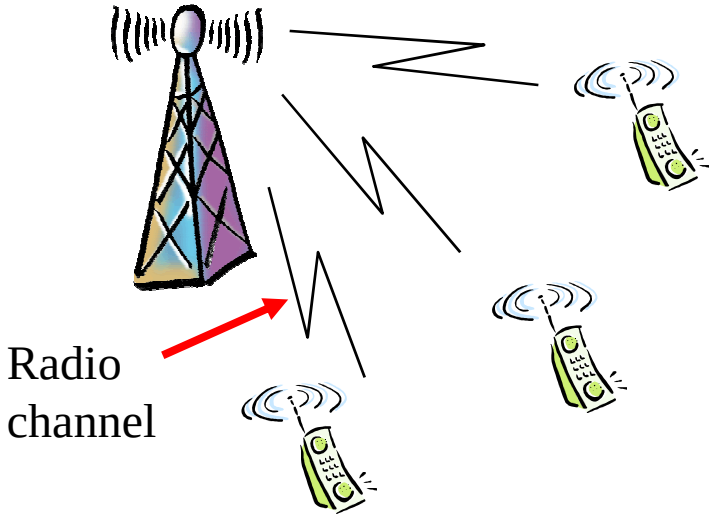
- In multi-hop operation mobile stations can forward information



Wired-Wireless networks: Main differences

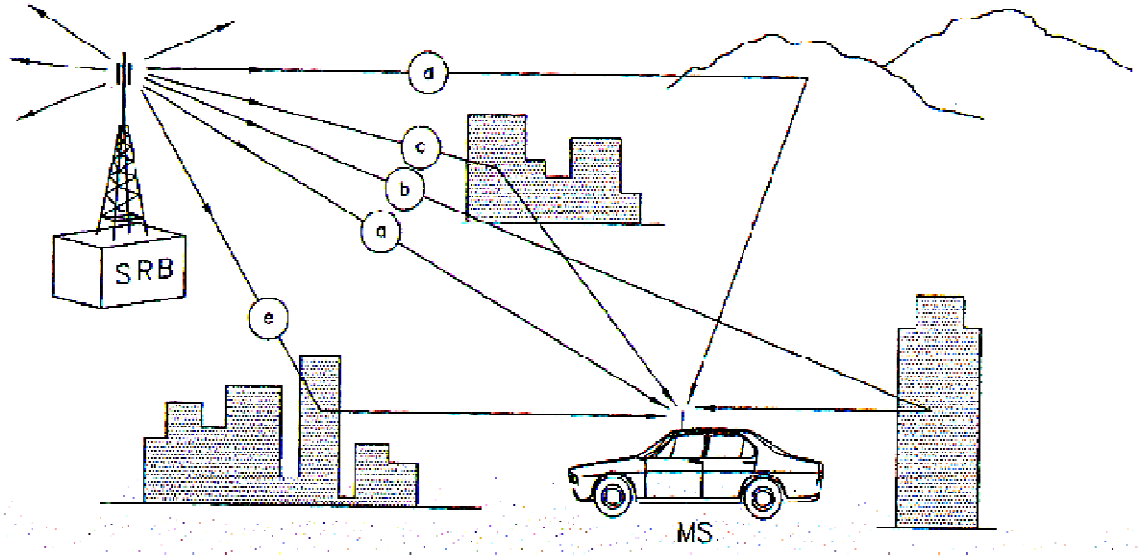
- Shared transmission medium
  - → Multiple access mechanisms
  - → Radio resource reuse





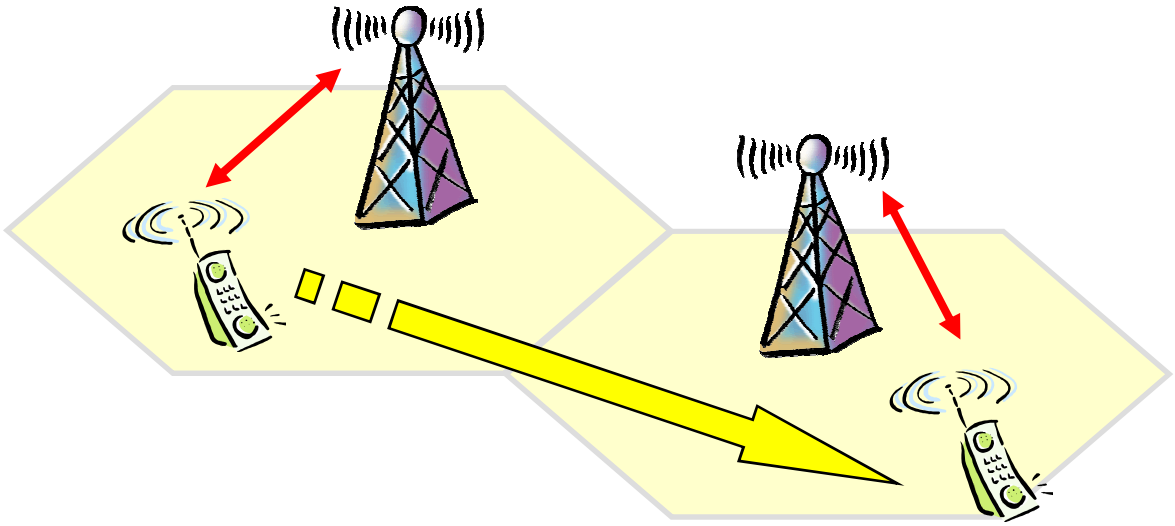
Wired-Wireless networks: Main differences

- Radio channel
  - ➔ Variable channel characteristics
  - ➔ Advanced modulation and coding schemes



Wired-Wireless networks: Main differences

- User mobility
  - ➔ Stand-by mobility
  - ➔ Active session (conversation) mobility



Wired-Wireless networks: Main differences

- In this course we'll focus on wireless technologies (how these problems are solved in practice):
- But first a few comments on:
  - Wireless channels

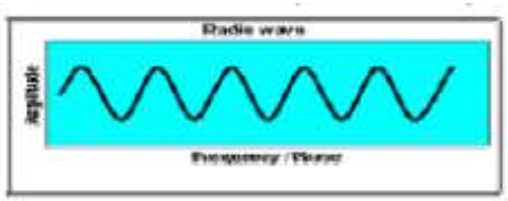
Wireless channel

- *Very bad* channel compared to other wired mediums
- Signals propagation is subject to:
  - High attenuation due to distance
  - Supplementary attenuation due to obstacles
  - Multipath propagation

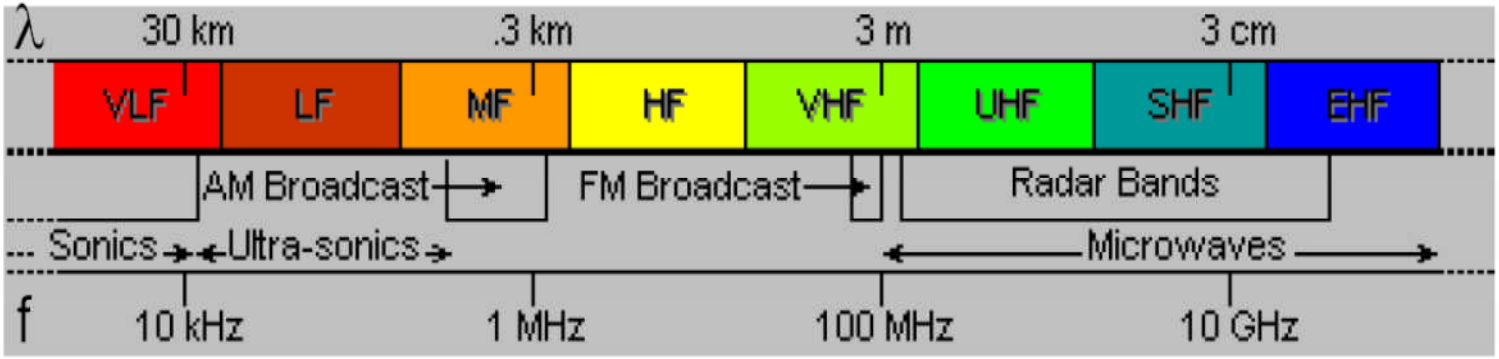
Wireless channel: radio spectrum

- **Radio waves**
  - Wave length $\lambda = \frac{c}{f}$
  - Light speed $c = 3 \cdot 10^8$ m/s
  - Frequency f

$$s(t) = \cos(2\pi f t + \varphi)$$



[V|U|S|E]HF = [Very|Ultra|Super|Extra] High Frequency



Wireless channel: radio spectrum

ELF	<3 KHz	Remote control, Voice, analog phone
VLF	3-30 KHz	Submarine, long-range
LF	30-300 KHz	Long-range, marine beacon
MF	300 KHz –3 MHz	AM radio, marine radio
HF	3-30 MHz	Amateur radio, military, long-distance aircraft/ships
VHF	30-300 MHZ	TV VHF, FM radio, AM x aircraft commun.
UHF	300 MHz - 3 GHz	Cellular, TV UHF, radar
SHF	3-30 GHz	Satellite, radar, terrestrial wireless links, WLL
EHF	30-300 GHz	Experimental, WLL
IR	300 GHz – 400 THz	LAN infrared, consumer electronics
Light	400-900 THz	Optical communications

Wireless channel: radio spectrum

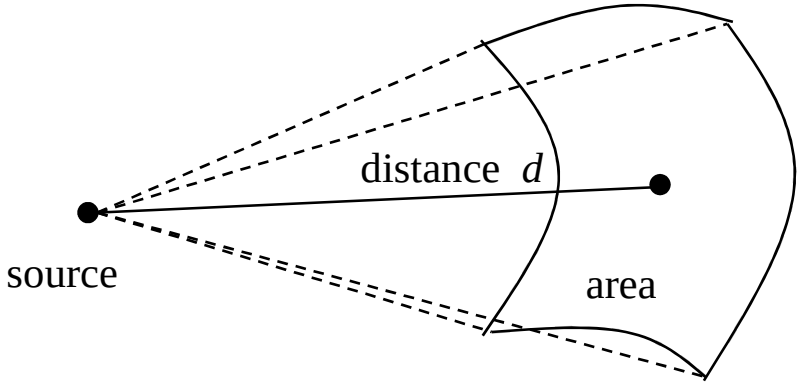
- **Higher frequencies:**
  - more bandwidth
  - less crowded spectrum
  - but greater attenuation through walls
- **Lower frequencies**
  - bandwidth limited
  - longer antennas required
  - greater antenna separation required
  - several sources of man-made noise

Wireless channel: antennas

- Transmission and reception are achieved by means of an **antenna**
- An antenna is an electrical conductor or system of conductors
  - *Transmission* - radiates electromagnetic energy into space
  - *Reception* - collects electromagnetic energy from space
- In two-way communication, the same antenna can be used for transmission and reception
- Isotropic antenna (idealized)
  - Radiates power equally in all directions (3D)
  - Real antennas always have directive effects (vertically and/or horizontally)

Wireless channel: attenuation

- Isotropic radiator transmitting power P_T uniformly in all directions



- Power density F at distance *d* is:

$$F = \frac{P_T}{4\pi d^2} \quad [\mathrm{W/m^2}]$$

Wireless channel: attenuation

- Directive characteristics of real antennas concentrate power in some directions
- This effect can be modeled using the gain $g(\theta)$ in the direction θ

$$g(\theta) = \frac{\text{power at distance } d \text{ in direction } \theta}{P_T / 4\pi d^2}$$

- The maximum gain g_T is conventionally in the direction $\theta = 0$.

Wireless channel: attenuation

- The power density in the maximum gain direction is given by:

$$F(d) = \frac{P_T g_T}{4\pi d^2} \quad [\mathrm{W/m^2}]$$

- The product $P_T\, g_T$ is called EIRP (Effective Isotropically Radiated Power) and it is the power required to reach the same power density with an isotropic radiator

Wireless channel: attenuation

- The *received power* depends on the power density at the receiver antenna and its equivalent area:

$$P_R = F(d)A_e$$

- For an isotropic antenna we have: $A_e = \frac{\lambda^2}{4\pi}$
- While for a directive antenna we can concentrate energy:

$$P_R = F(d)g_R A_e$$

  - where g_R is the receiver antenna gain

- Therefore:

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi d}\right)^2$$

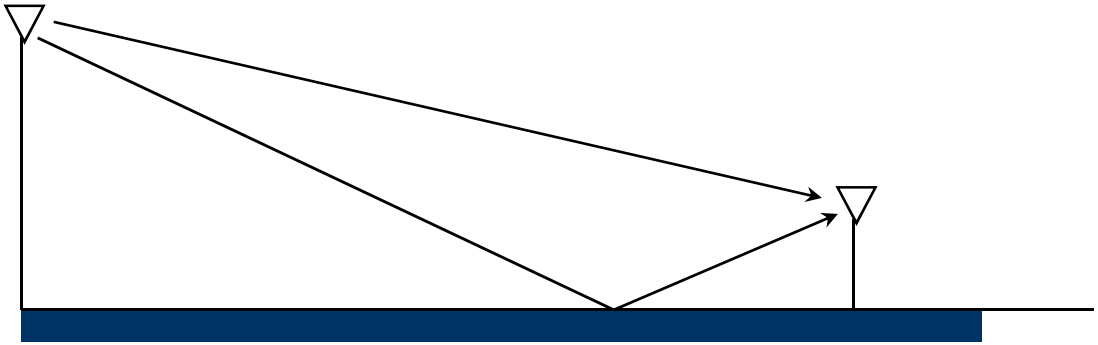
Wireless channel: free space model (Friis)

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi d} \right)^2 = P_T g_T g_R \left(\frac{c}{4\pi f d} \right)^2$$

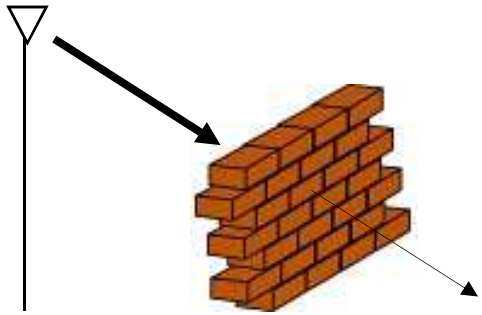
- The received power is $\propto d^{-2}$
- This is known as the *free space* propagation model
- It can be used for example with point-to-point radio links

Wireless channel: propagation impairments

- Unfortunately, in real environments the propagation of electromagnetic waves is more complex than in free space:
  - Reflection



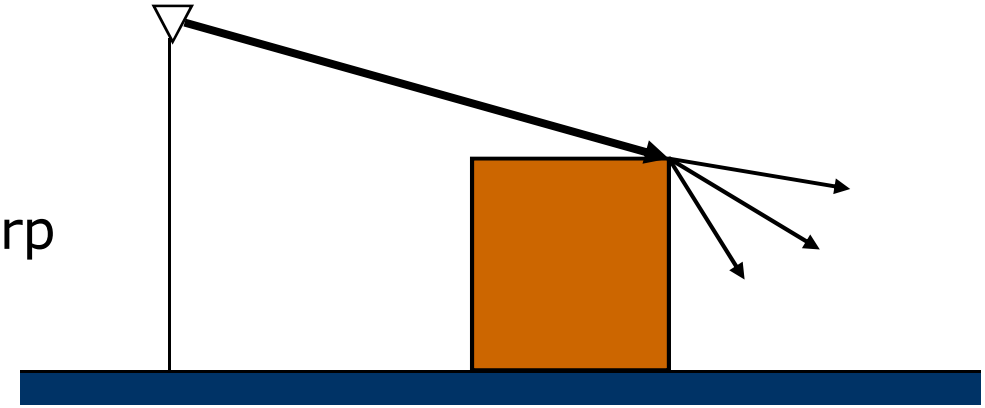
  - Shadowing



Wireless channel: propagation impairments

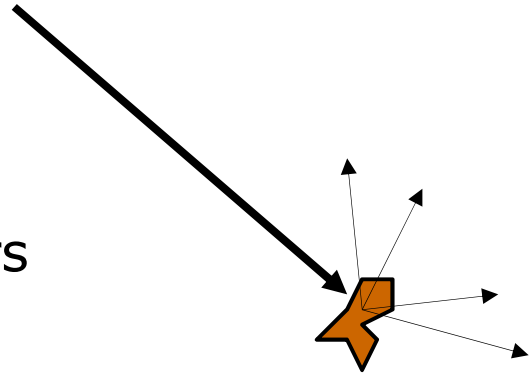
- Diffraction

  When the surface encountered has sharp edges. Bending the wave



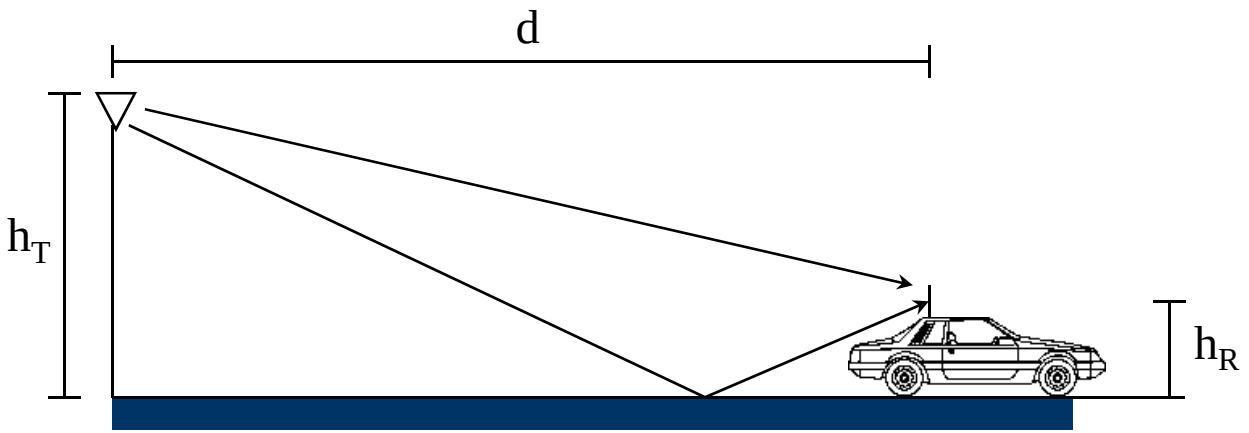
- Scattering

  When the wave encounters objects smaller than the wavelength (vegetation, clouds, street signs)



Wireless channel: two ray model

- Just in the case of reflection with only two rays (a direct ray and a reflected one) the received power is quite different w.r.t. free space
- It can shown that: $$P_R(d) \cong P_T g_T g_R \frac{h_T^2 h_R^2}{d^4}$$



Wireless channel: empirical models

- More complex scenarios can hardly be modeled with closed formulas
- Empirical models are usually adopted where received power is $\propto d^{-\eta}$

$$P_R = P_T g_T g_R \left(\frac{\lambda}{4\pi} \right)^2 \frac{1}{d^\eta}$$

- where η is the *propagation factor* which typically ranges between 2 and 5
- More complex empirical models (e.g. Hata) take into account several parameters including scenario (urban, rural), antenna heights, etc.

Wireless channel: empirical models

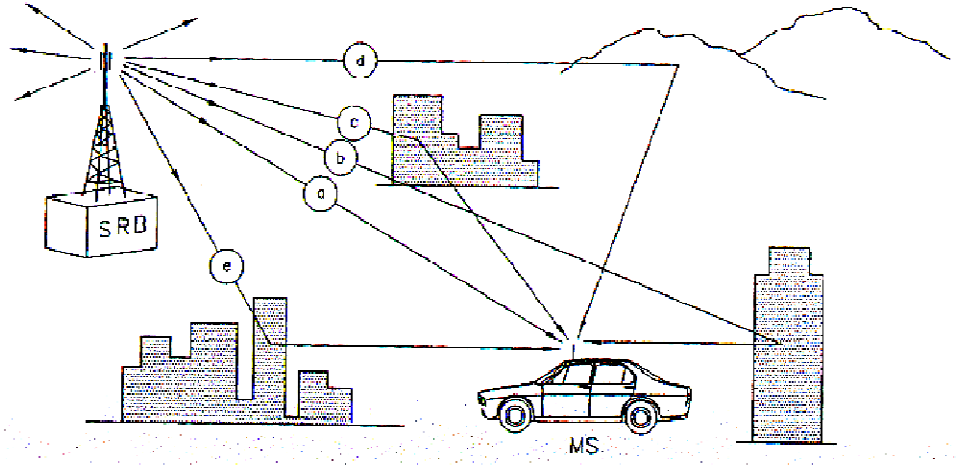
- Okumura/Hata formula:

$$L_P = 69.55 + 26.16 \log f - 13.82 \log h_T - a(h_R) + \\ + \left(44.9 - 6.55 \log h_T\right) \log d \quad [\text{dB}]$$

- where
  - f frequency in MHz (from 150 to 1500 MHz)
  - h_T base station height (in m)
  - h_R mobile station height (in m) – $a(h_R)$ correlation factor depending on area shape
  - d distance (in km)
- For a 900 MHz system, h_T = 30 m, $a(h_R) \approx 0$:

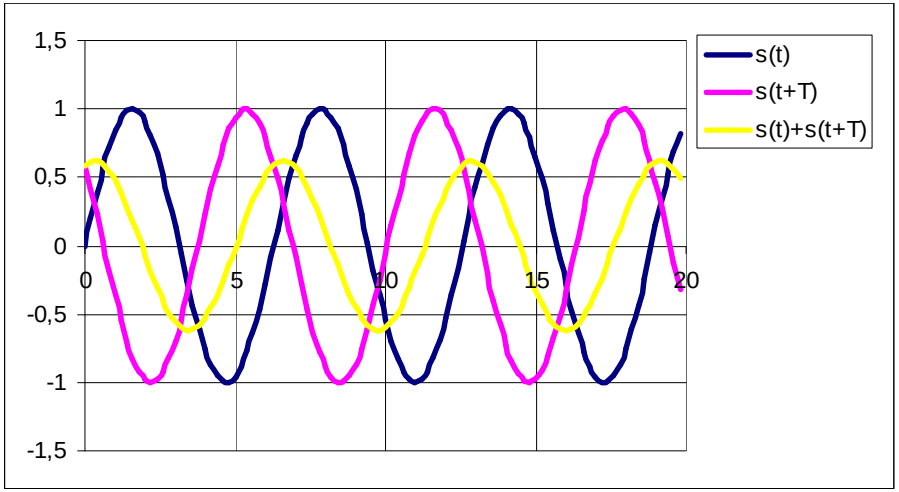
$$L_P = 126.42 + 35.22 \log d$$

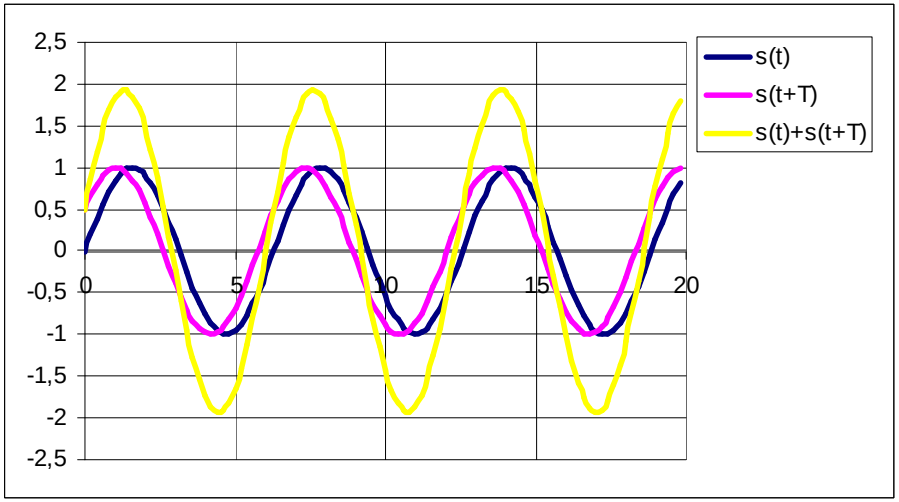
Wireless channel: multipath fading



- Copies of the same signal arrive from different paths
- Their combination at the receiver depends on:
  - Number of copies
  - Relative shift
  - Amplitude
  - Frequency

Wireless channel: multipath fading





- The resulting signal can be attenuated …

$T=4/5\pi$

- … or even amplified !!!

$T=\pi/6$

Wireless channel: shadowing

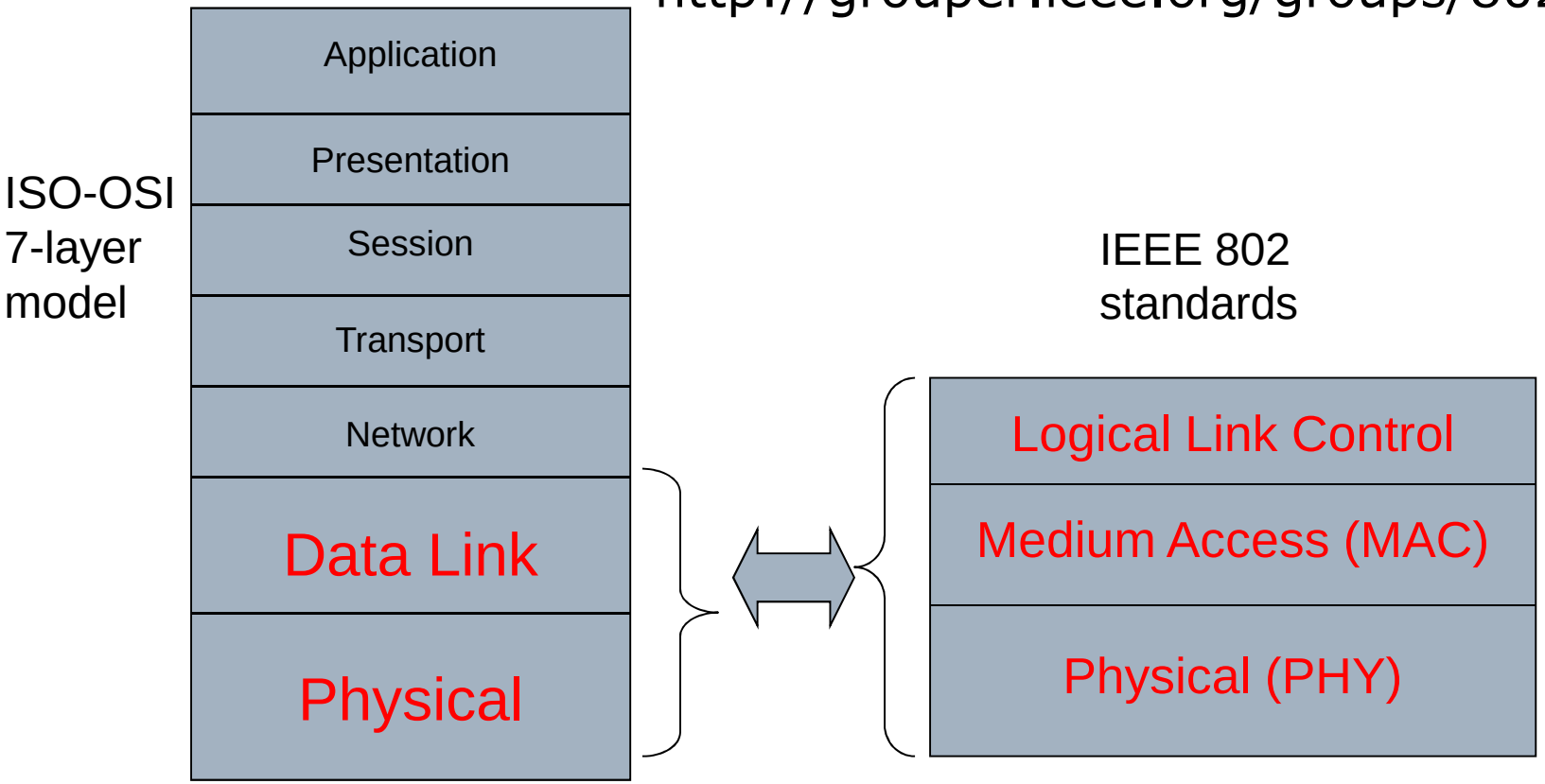
- Signal can be partially absorbed or reflected by obstacles
- Further attenuation called *shadowing*

Part 1
WLAN

Standardization of Wireless Networks

- Wireless networks are standardized by IEEE (Institute of Electrical and Electronics Engineers)
- under 802 LAN/MAN standards committee.

http://grouper.ieee.org/groups/802/11/



802.11 History

Wireless Evolution of LAN

- **802.11-legacy** standard first ratified in July **1997**
  - 802.3 LAN emulation
  - 3 PHY's were specified for 1 & 2 Mbps (FHSS, DSSS, Infrared)
- Two High Rate PHY's ratified in Sep **1999**
  - **802.11a** 6 to 54Mbps in the 5GHz band (OFDM)
  - **802.11b** 5.5 and 11Mbps in the 2.4GHz band
- PHY up to 54 Mbit/s in 2.4 GHz band ratified in **2003**
  - **802.11g**
- 802.11a compatible with European spectrum regulation in 5GHz band ratified in **2004**
  - **802.11h** (Transmit Power control to avoid interference with satellites, radars, etc …)

802.11 History

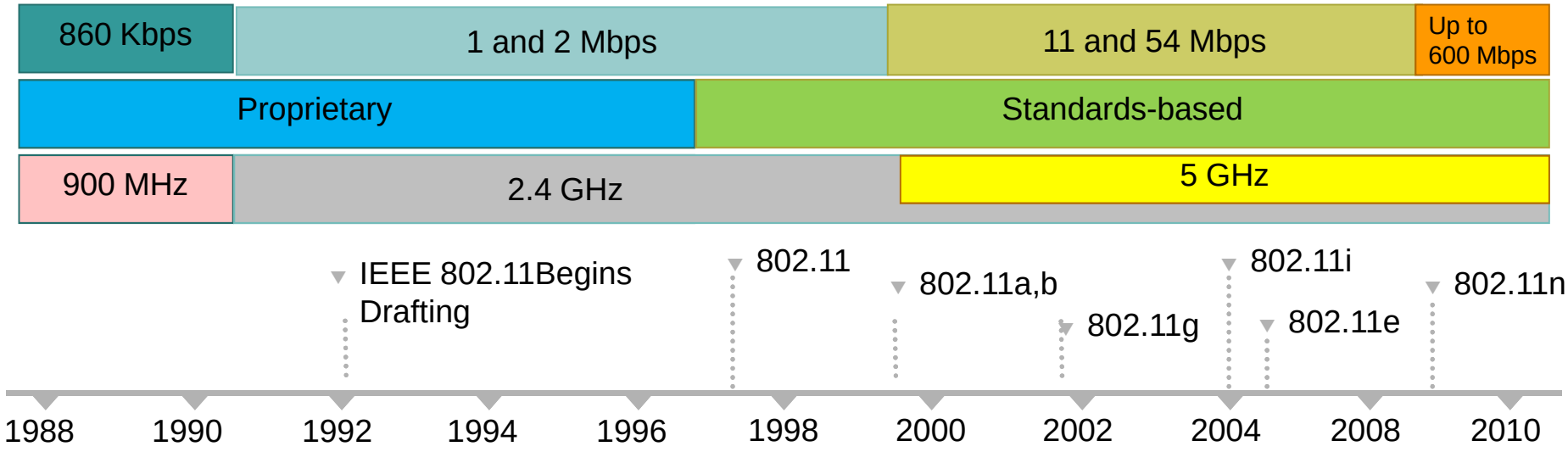
- Enhanced security framework ratified in **2004**
  - **802.11i**
- Enhanced MAC with QoS support ratified in **2005**
  - **802.11e**
- High rate standard (PHY and also MAC) ratified in **2009** (draft 2007 with WiFi pre-standard products)
  - **802.11n**

And more to come:

- **802.11s:** mesh networking
- **802.11p:** WAVE—Wireless Access for the Vehicular Environment
- **802.11v:** Wireless network management
- **802.11ac:** Very High Throughput (0.5 – 1 Gbit/s)
- **802.11af:** White-Fi (CRN, using TV Whitespace …)

802.11 History

- WLAN Timeline

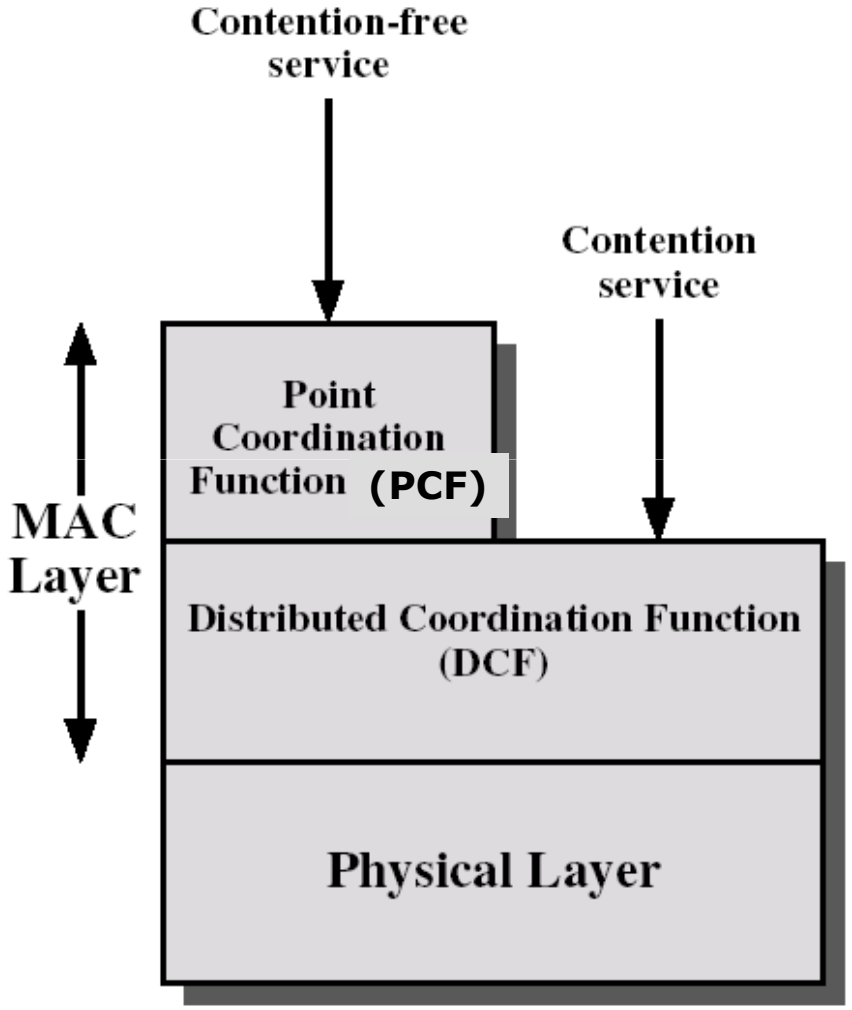


Wi-Fi

- Wi-Fi™ Alliance
  - Wireless Fidelity Alliance
  - 500+ members
  - Over 350 products certified
- Wi-Fi's™ Mission
  - Certify interoperability of WLAN products (802.11)
  - Wi-Fi™ is the "stamp of approval"
  - Promote Wi-Fi™ as the global standard

802.11 Protocol Architecture

- The standard provides two modes of operation which are:
- **DCF** (mandatory) – best effort contention service – uses CSMA with Collision Avoidance (CSMA/CA)
- **PCF** (optional) – base station controls access to the medium – uses a *polling* mechanism with higher priority access to the medium, plus three types of frames: data, control and management



WLAN:
Network architecture

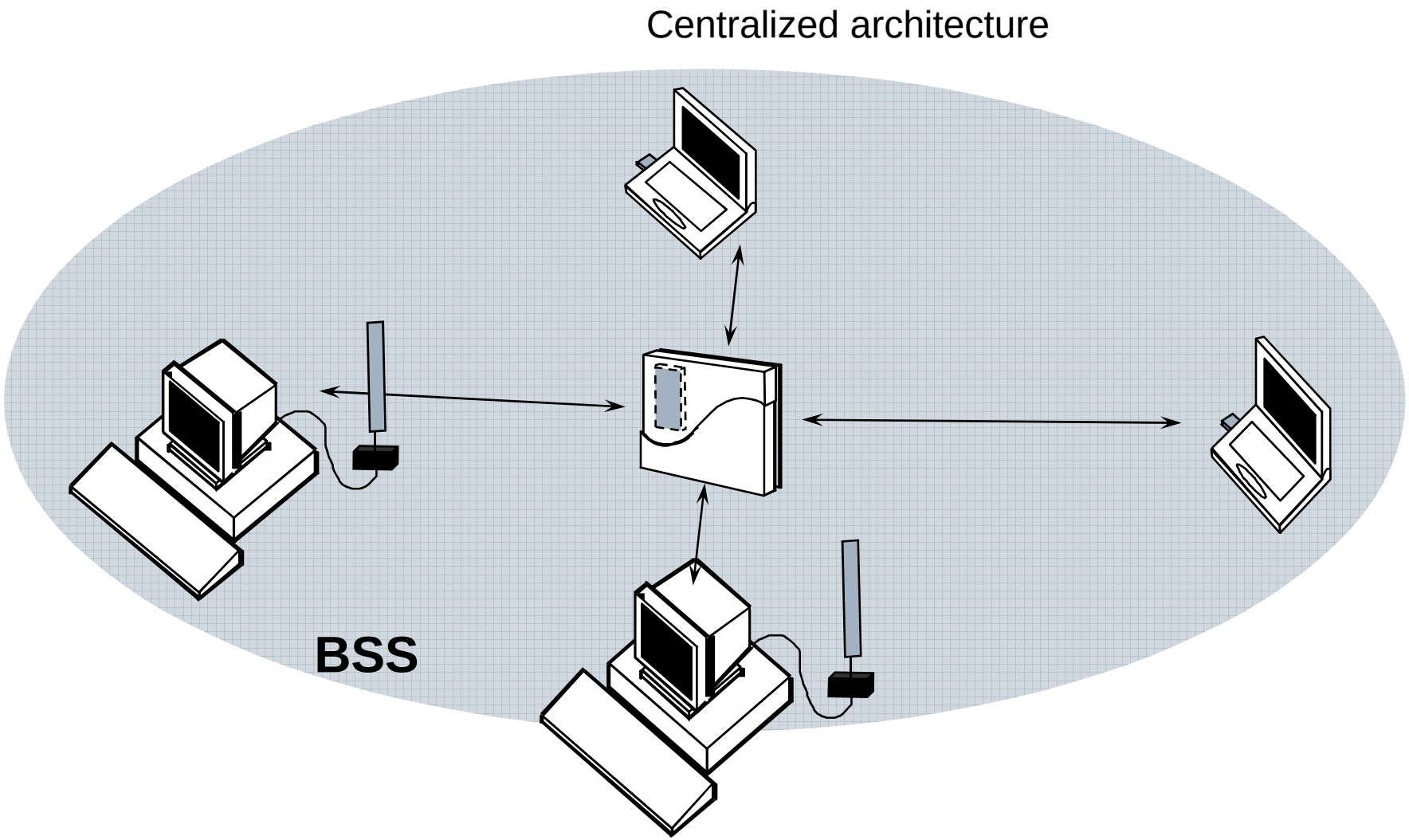
Components

- Station (**STA**)
- *Access Point* (**AP**)
  - *bridging wired/wireless*
- **BSS** - *Basic Service Set*
  - *Infrastructure* BSS: infrastructure based
  - *Independent* BSS (IBSS): *ad hoc*
- **ESS** - *Extended Service Set*
  - Set of *Infrastructure* BSS
  - A set of *access points* connected through a:
- **DS** – *Distribution System* (not directly addressed in the standard)
  - Wired
  - Wireless (WDS)

Basic Service Set (BSS)

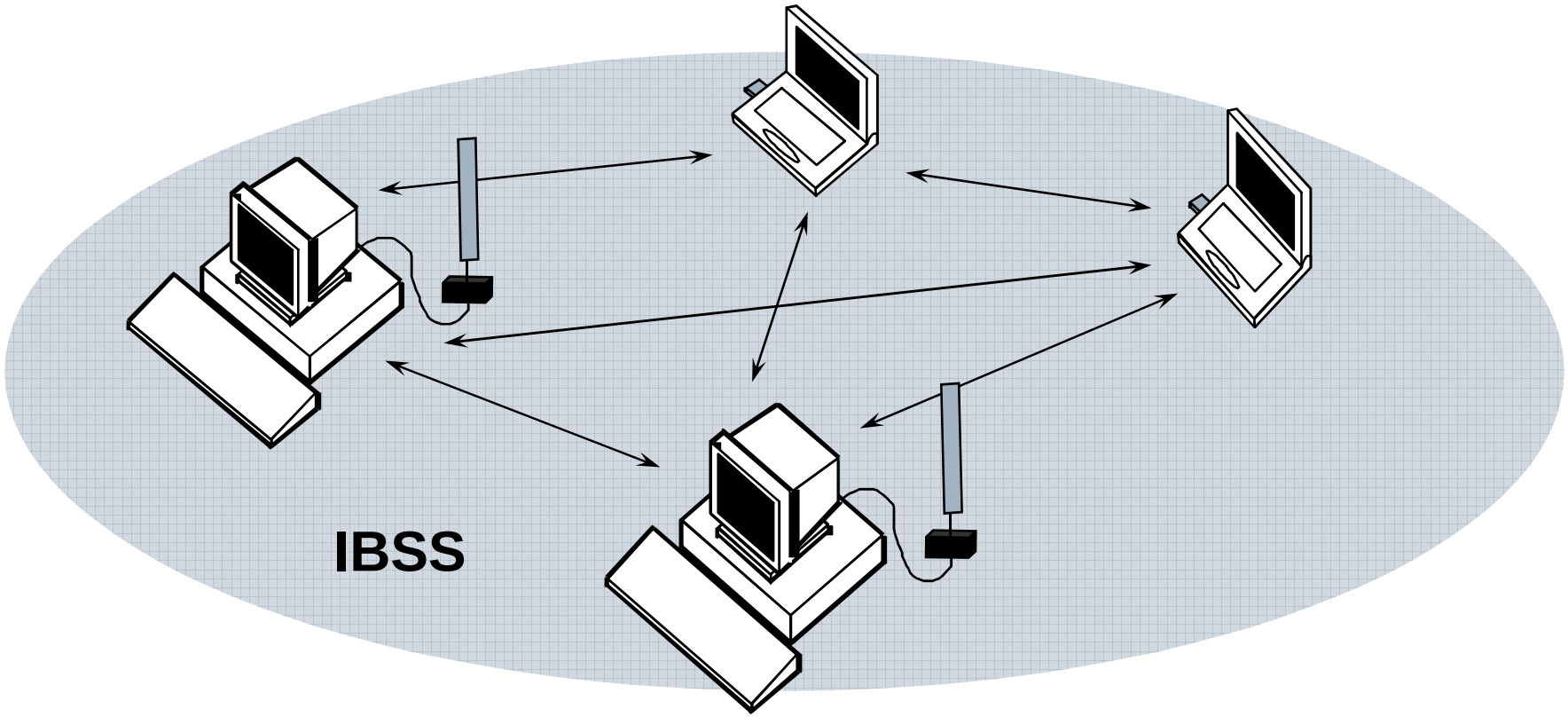
- Set of stations (STAs) controlled by the same "*Coordination Function*" (logic function that manages the access to the shared channel)
- Similar to the concept of "cell" in mobile radio networks
- Two types of BSS:
  - *Infrastructure* BSS
  - *Independent* BSS (IBSS)

Infrastructure BSS

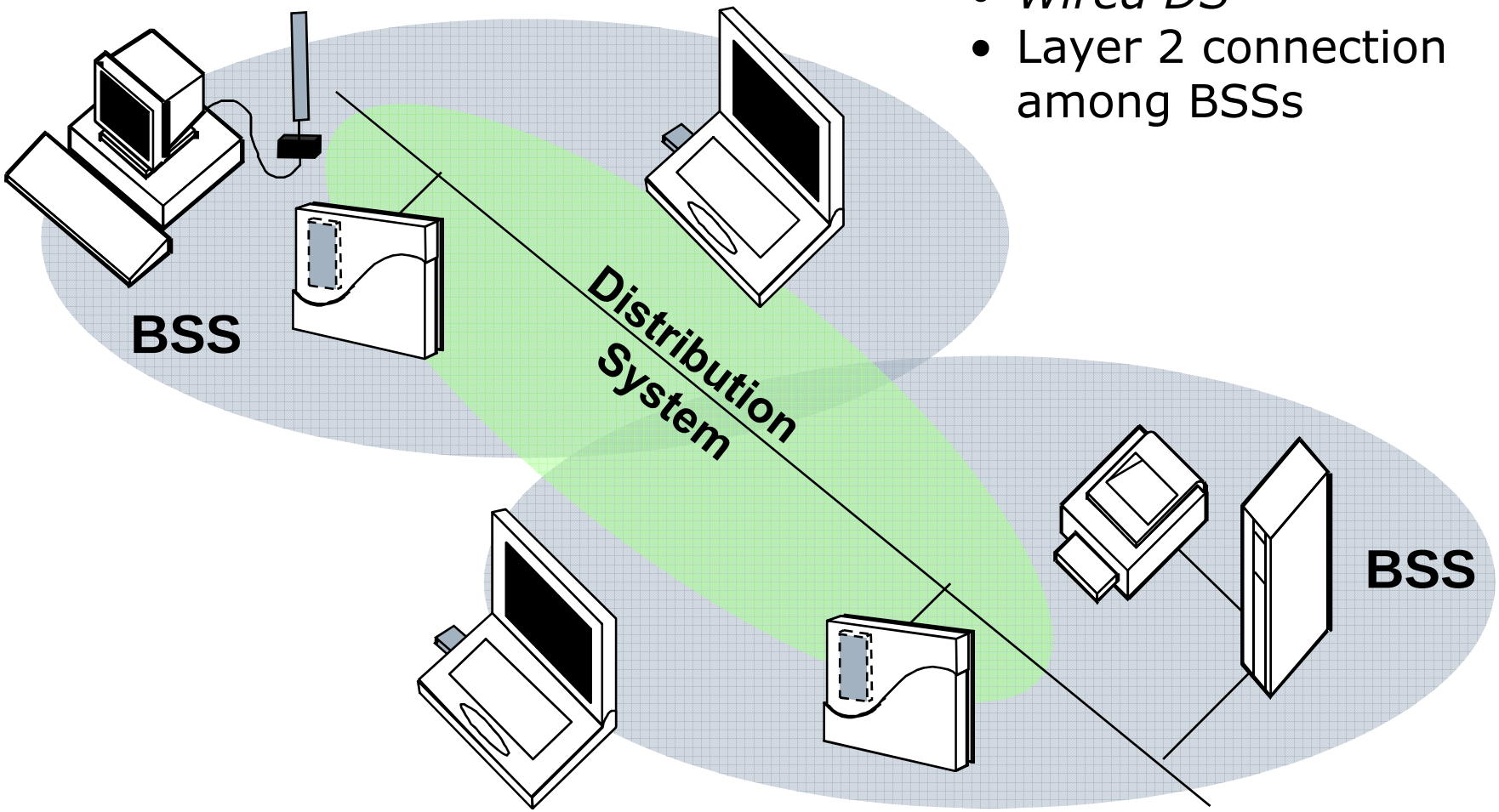


Independent Basic Service Set (IBSS)

Ad hoc architecture

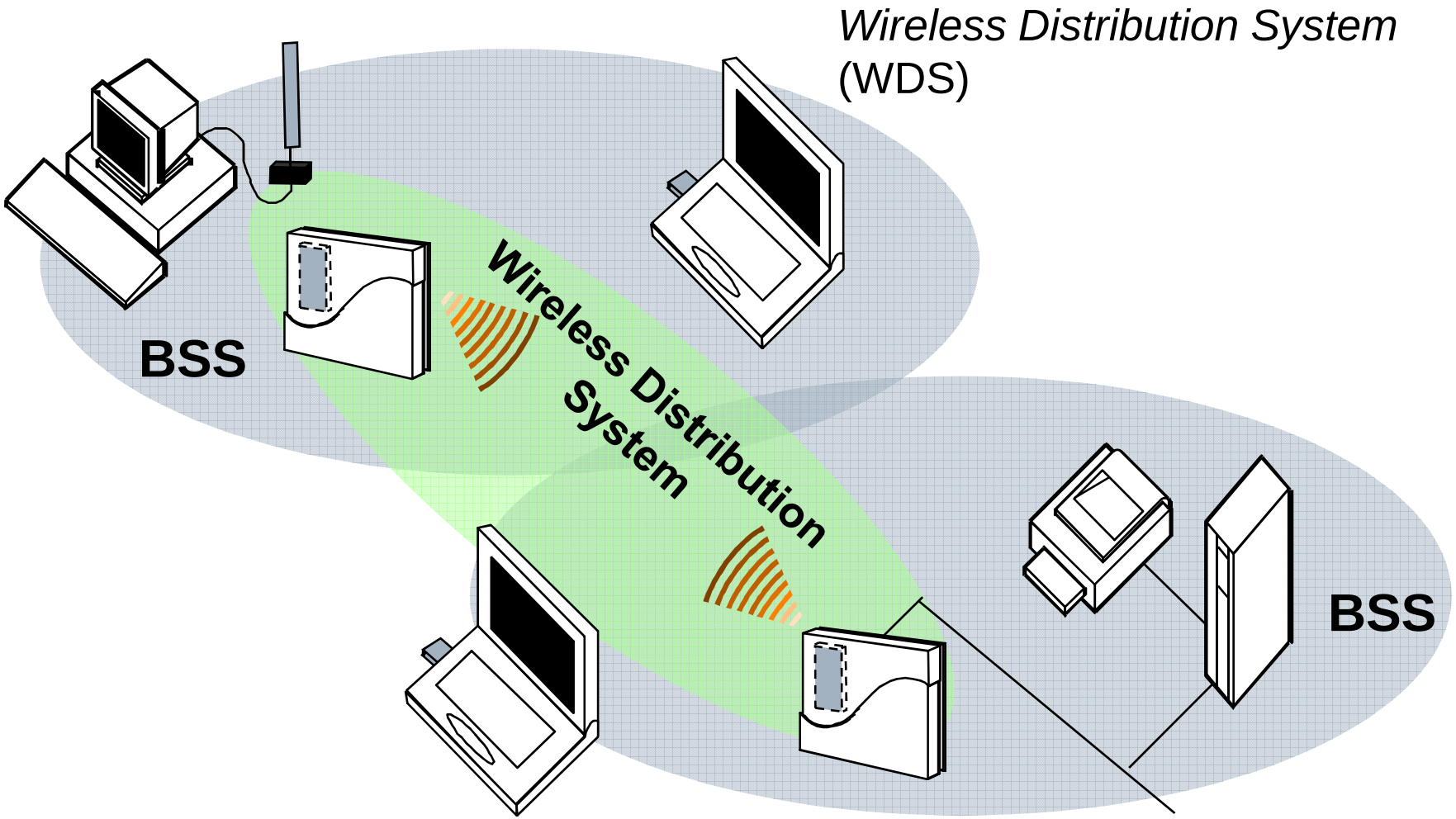


Extended Service Set (ESS)

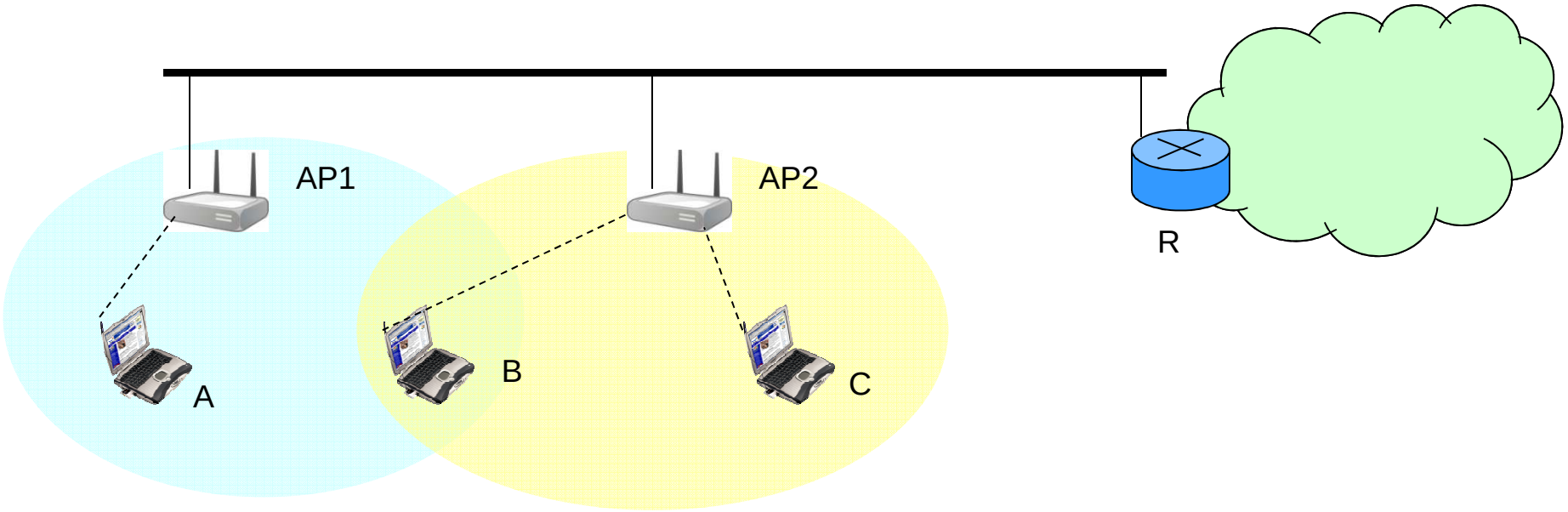


- *Wired DS*
- Layer 2 connection among BSSs

Extended Service Set (ESS)

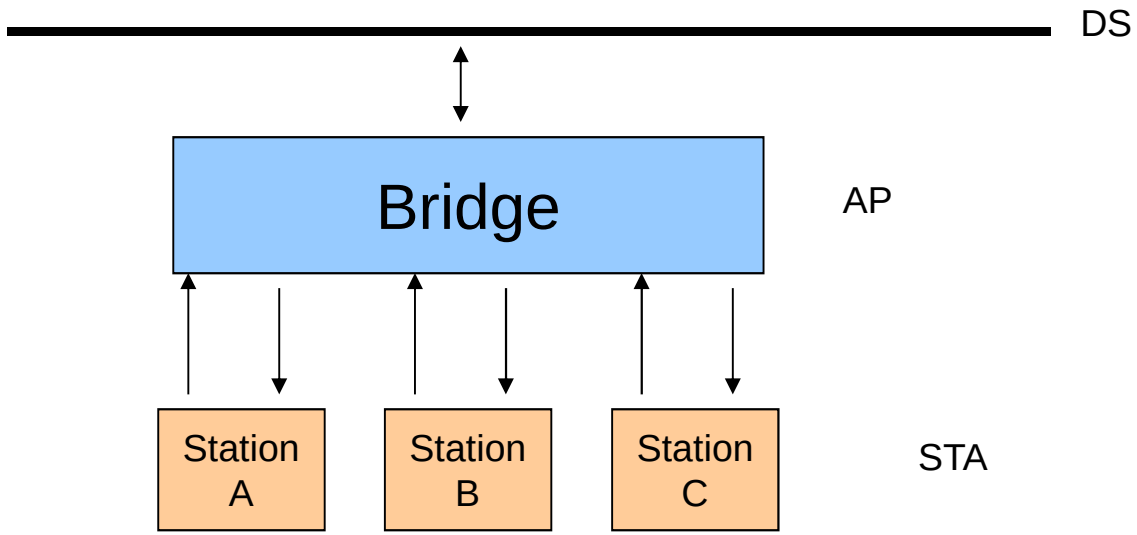


Distribution System



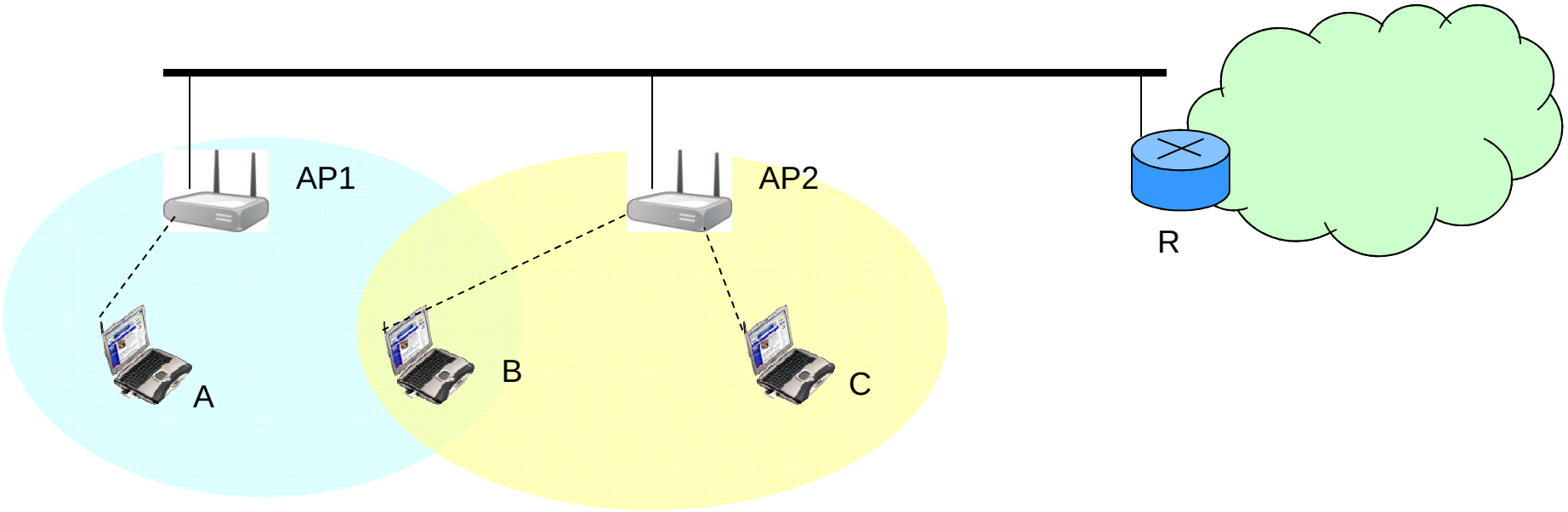
- STA associates to one, and *only one*, AP through an association procedure
- Association procedure is "equivalent" to plugging the ethernet cable
- An ESS is a layer-2 network, and therefore a single IP subnet with its own addressing space

Distribution System



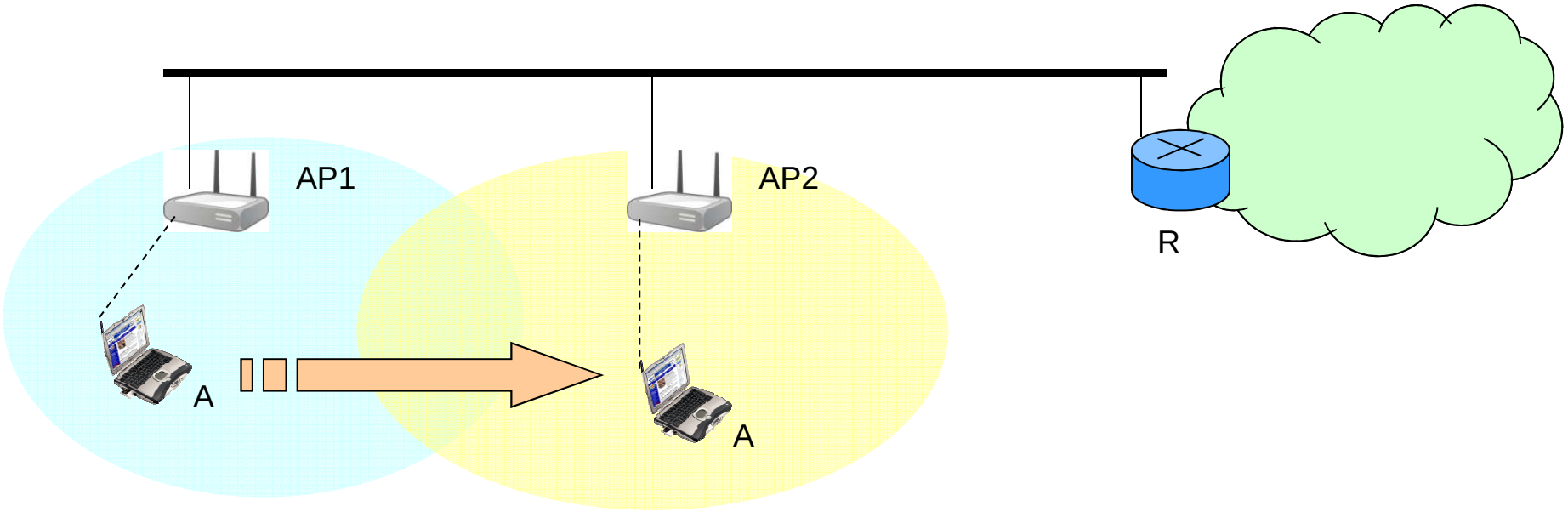
- APs behave like an *Ethernet bridge* (layer-2 switch)
- Association tables are used for the bridging process
- For example, frames received via the DS and indicating as destination a wireless STA are forwarded to the wireless interface once converted to 802.11 format

Distribution System



- **Question**: How exactly can an IP packet go from router R to STA B (assume ARP tables empty)?

Distribution System



- What happens when a station moves from AP1 to AP2? (*handover* or *handoff*)

WLAN:
Medium Access Control

MAC services and functionalities

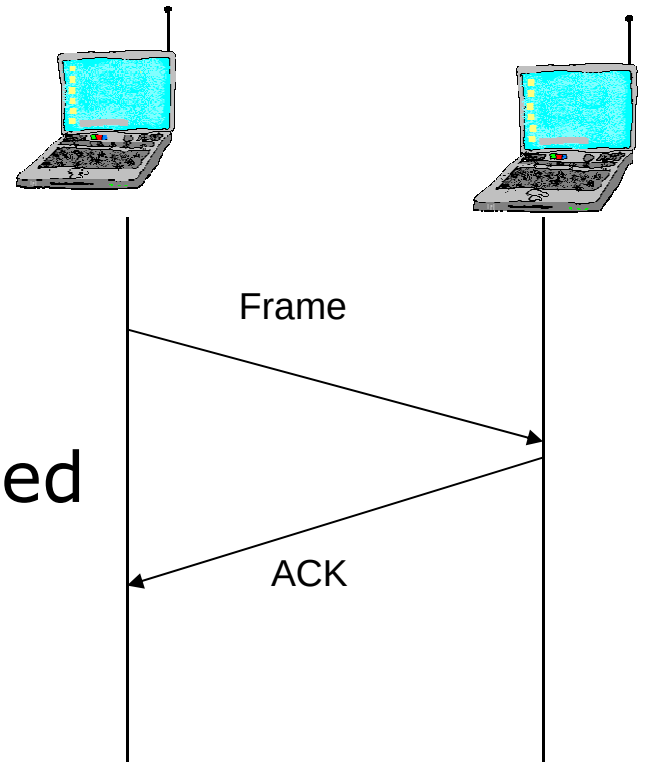
- Channel access
- Error recovery
- Fragmentation and reassembly
- Power saving
- Addressing
- Framing

Channel access

- The access to the transmission medium is regulated by the so called "*coordination functions*"
- Two coordination functions are defined
  - *Distributed Coordination Function* (DCF)
    - Based on CSMA with *backoff*
  - *Point Coordination Function* (PCF)
    - *Collision free* access based on polling
    - Several BUGS in the standard – never implemented in commercial devices

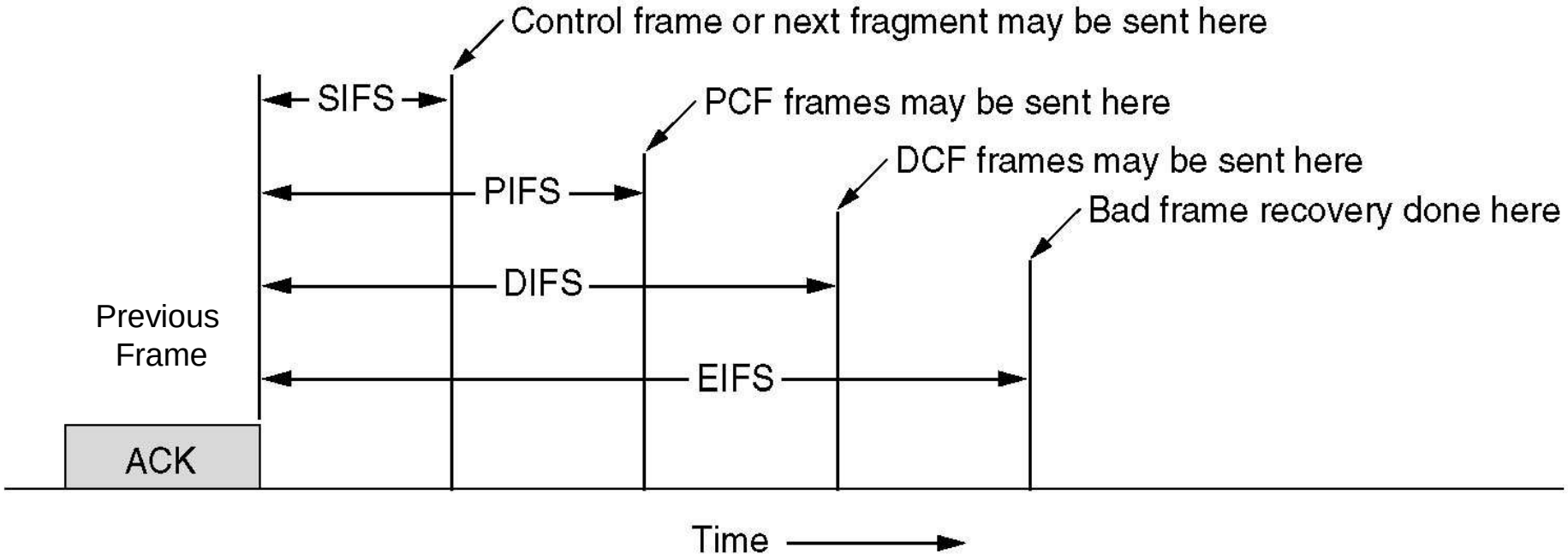
Error recovery

- Absolutely necessary on a "noisy" (wireless) channel
- Only for *unicast transmissions* (broadcast service is *unreliable*)
- Based on a positive acknowledgment per received frame ("*stop & wait*")
- Requires to use retransmission timers



Question: Do we have ACKs in Ethernet? Why?

Interframe spacing



- Several time intervals regulate the channel access
- These are *minimum* waiting intervals after last and are based on the physical *carrier sensing* mechanism

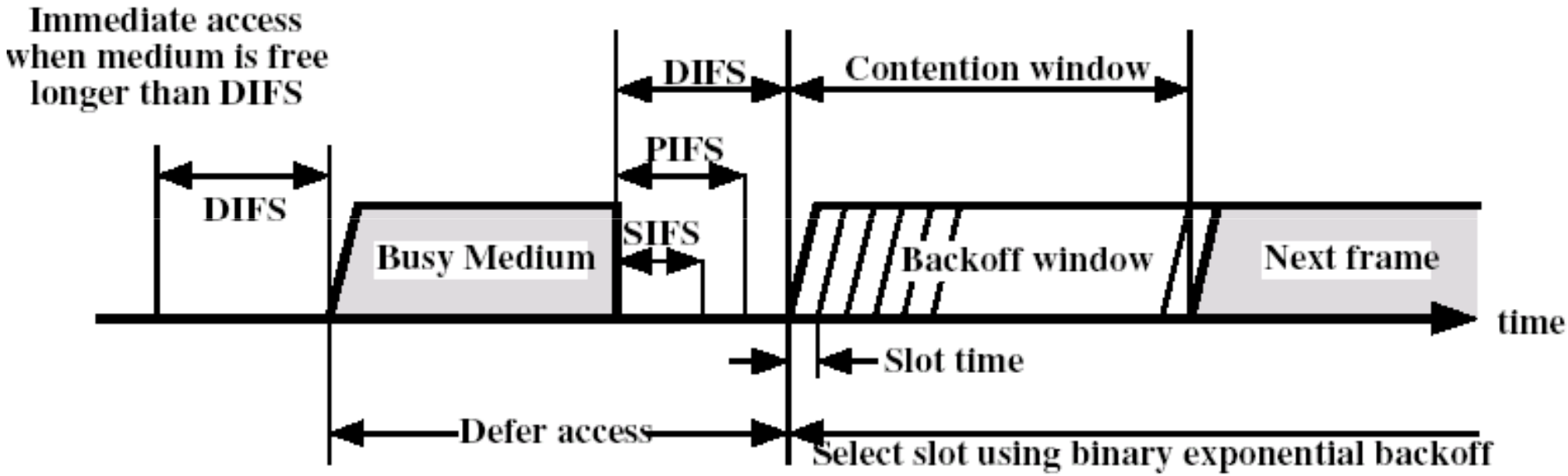
Interframe spacing

- *Short Inter Frame Spacing* (SIFS):
  - High priority transmissions can start after a SIFS after previous transmission
- *PCF Inter Frame Spacing* (PIFS):
  - Interframe space used to issue polling frames in PCF mode
- *DCF Inter Frame Spacing* (DIFS):
  - Regular data transmission in DCF mode can start after a DIFS
- *Extended Inter Frame Spacing (EIFS)*:
  - Used in special cases when previous transmission cannot be decoded

Distributed Coordination Function

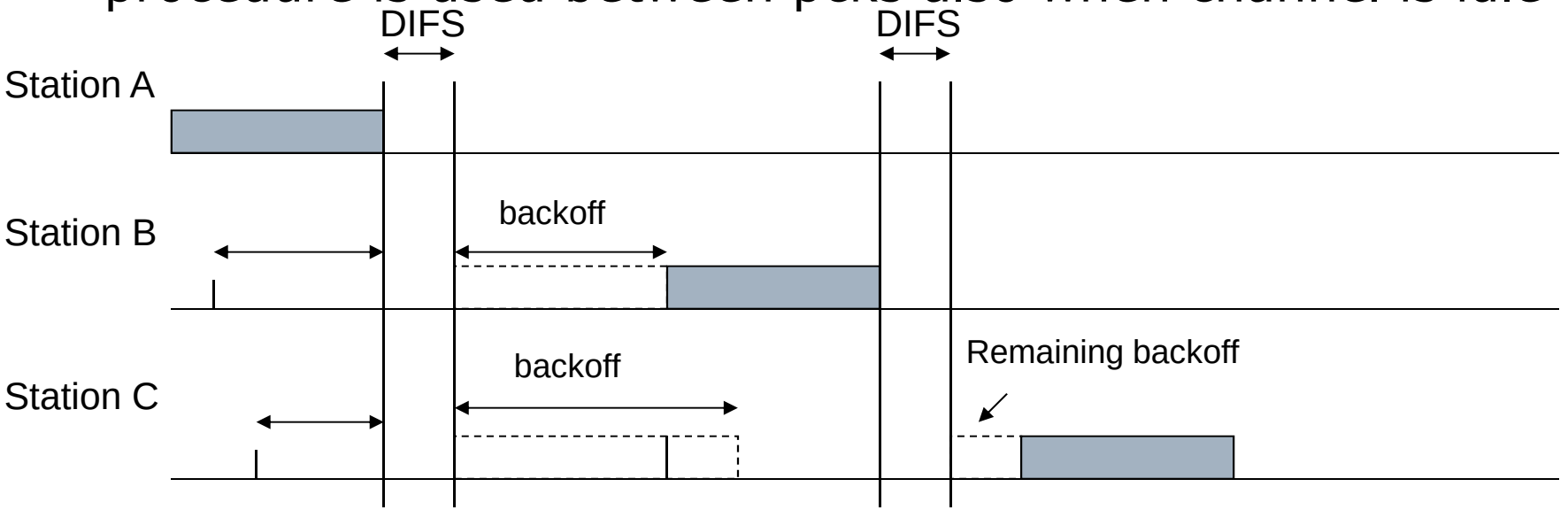
- DCF allows the coordination among stations without the need of a central controlling entity
- It can be used either in a IBSS and in a *infrastructure* BSS
- It is based on *Carrier Sense Multiple Access* with *Collision Avoidance* (CSMA/CA)
  - Before starting a transmission, the station listens to the channel:
    - If the Channel is idle (for *at least* a DIFS): start transmitting
    - If the Channel is busy: wait and start *backoff*

Distributed Coordination Function



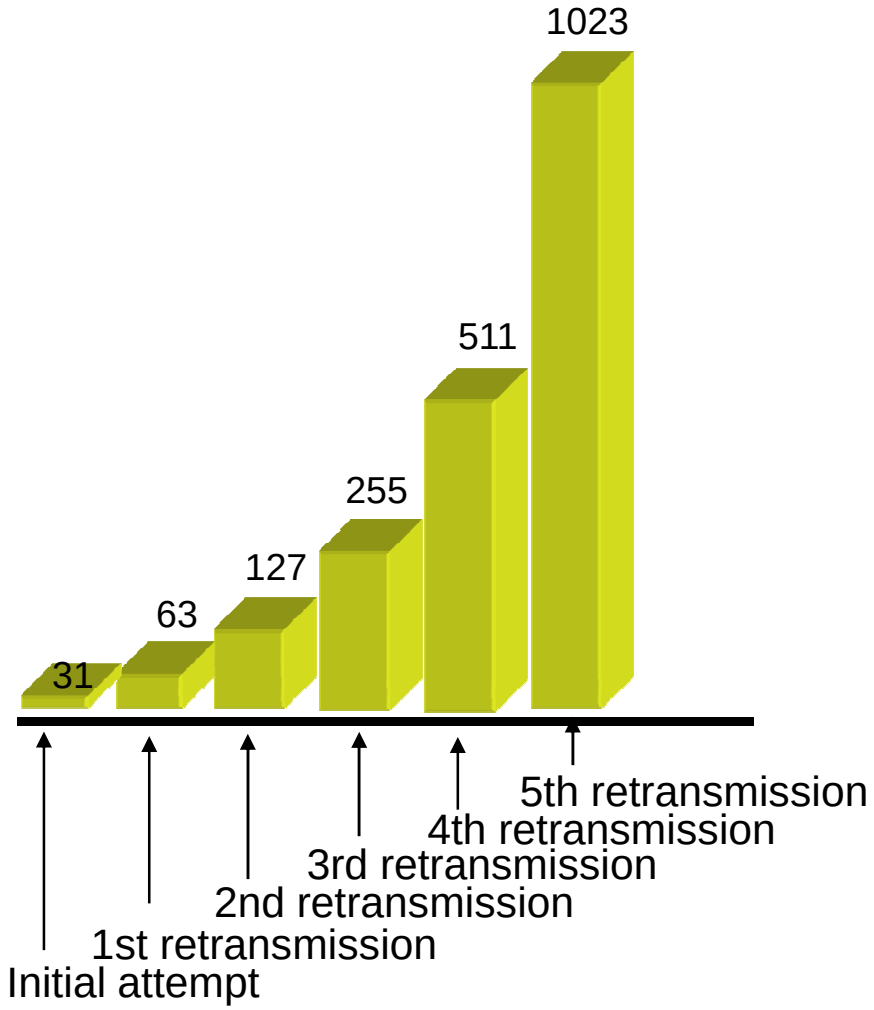
Collision Avoidance through the *Backoff* procedure

- Before transmitting, a station waits for a time period equal to a random number of slots (backoff) + DIFS
- The random number is uniform between 0 and CW (*Contention Window*)
- If during backoff the channel becomes busy, the counting down of slots is *stopped,* and it is then resumed when the channel is idle again
- If consecutive packets need to be transmitted, the backoff procedure is used between pcks also when channel is idle



Backoff Mechanism – the CW parameter

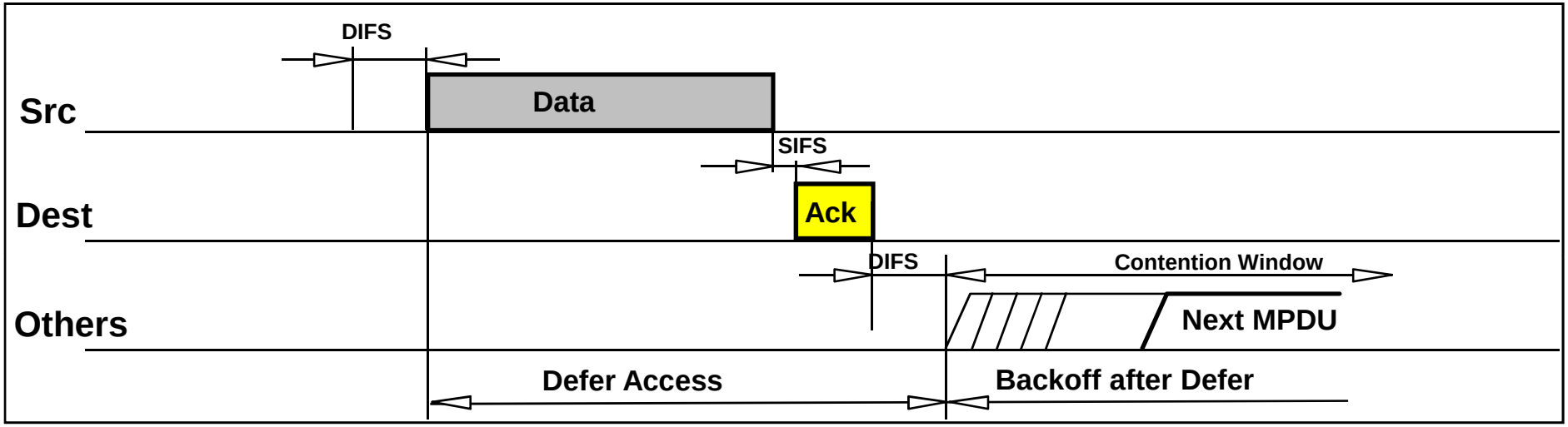
- *backoff* is uniform in [0, CW]
- CW is set dynamically:
  - If an error/collision occurs, (almost) double CW (up to CWmax=1023 slots)
  - If transmission is correct, set CW=CWmin=31



Error recovery in DCF

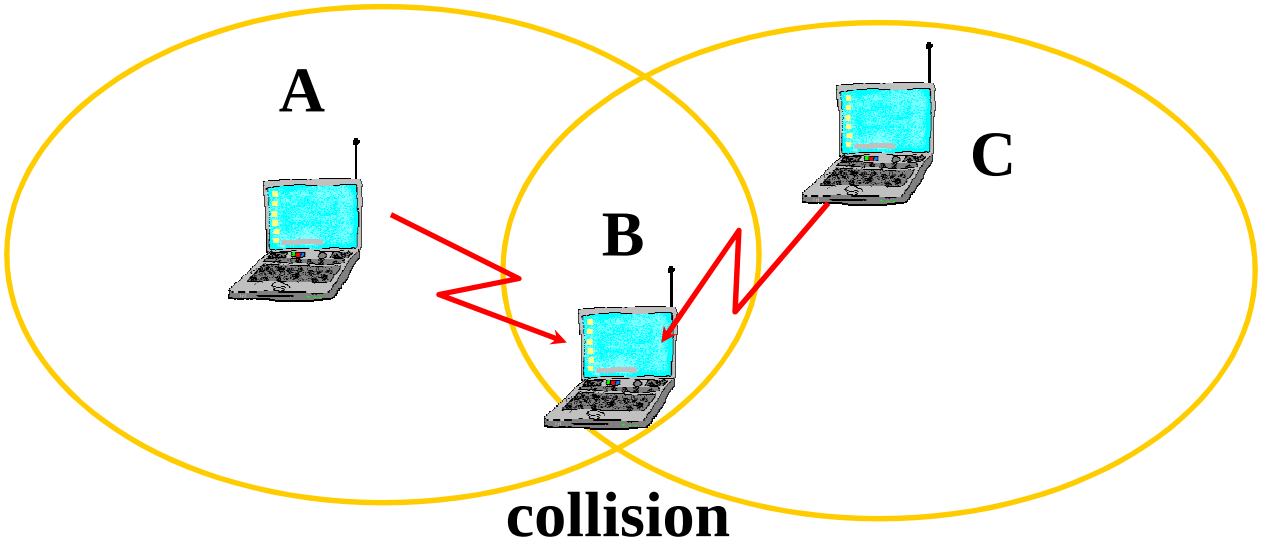
- Transmitting station can recover corrupted frames through retransmission
- Transmission feedback from receiver is based on a "*positive acknowledgement*"
  - Reception of *unicast* frames needs to be acknowledged
  - If acknowledgement is not received, the frame is considered lost and retransmitted
  - There is a maximum number of retransmissions per frame
- Retry Counters
  - *Short Retry counter (for "short" frames)*
  - *Long Retry counter (for "long" frames)*

Transmission example



- SIFS < DIFS, therefore ACKs have priority over data frames

Hidden Terminal

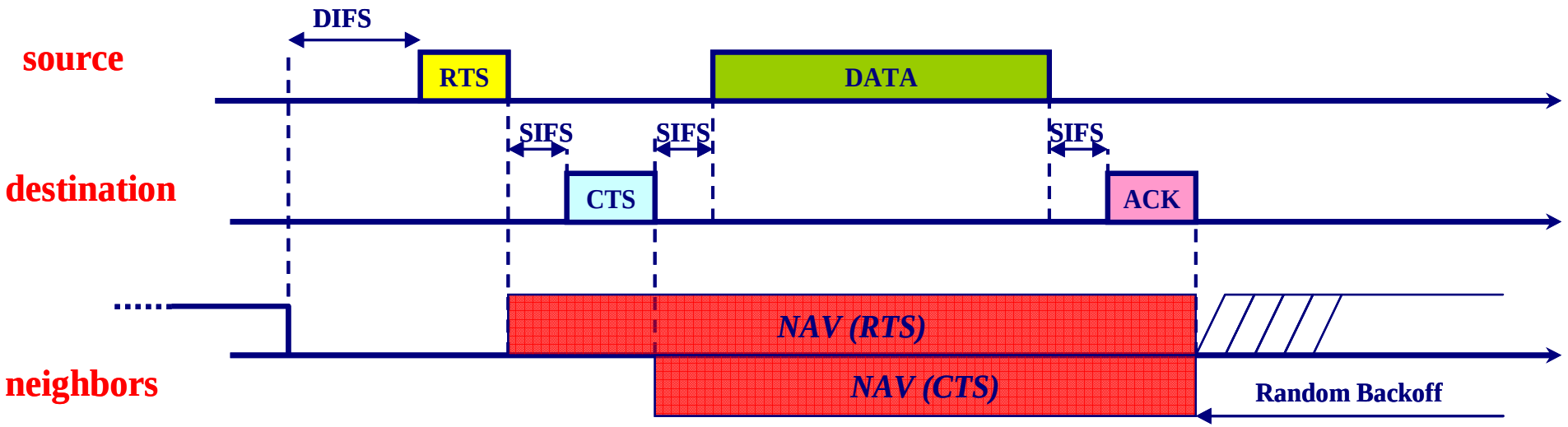


- Station A is "hidden" to station C
- Since B is in range of both A and C, a collision occurs (i.e., two (or more) signals arrive at the same time in the same place, namely station B)

Solution to the *Hidden Terminal*

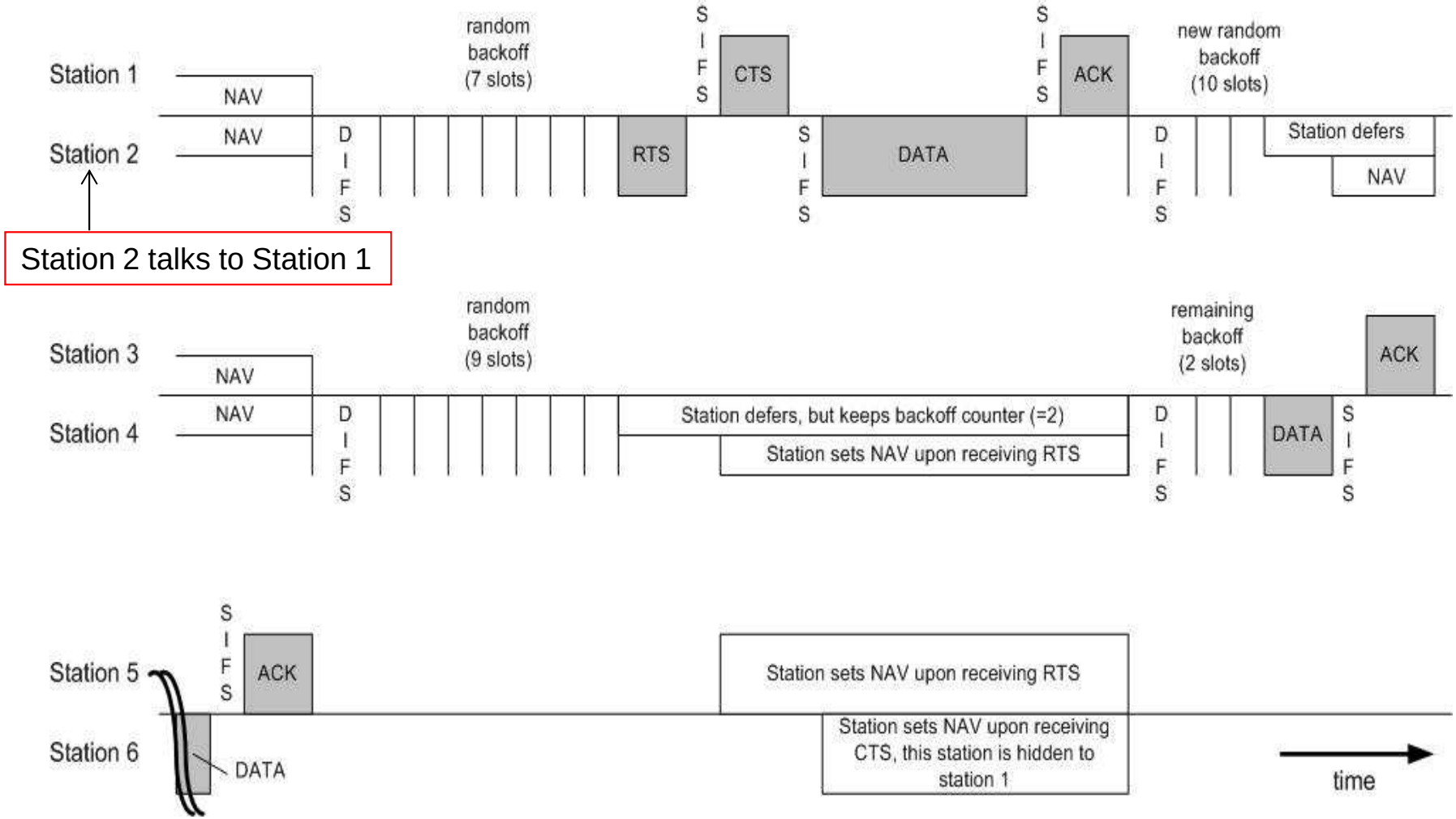
- The standard adds a procedure of logical (virtual) *carrier sensing* to the physical one
- Control frames are used, in which it is coded the so called *Network Allocation Vector (NAV)*
- The NAV contains the *duration* of the communication which is currently occupying the channel
- Mobile stations that receive such control frames do not try to access the channel during the time specified in the NAV

Virtual Carrier Sense

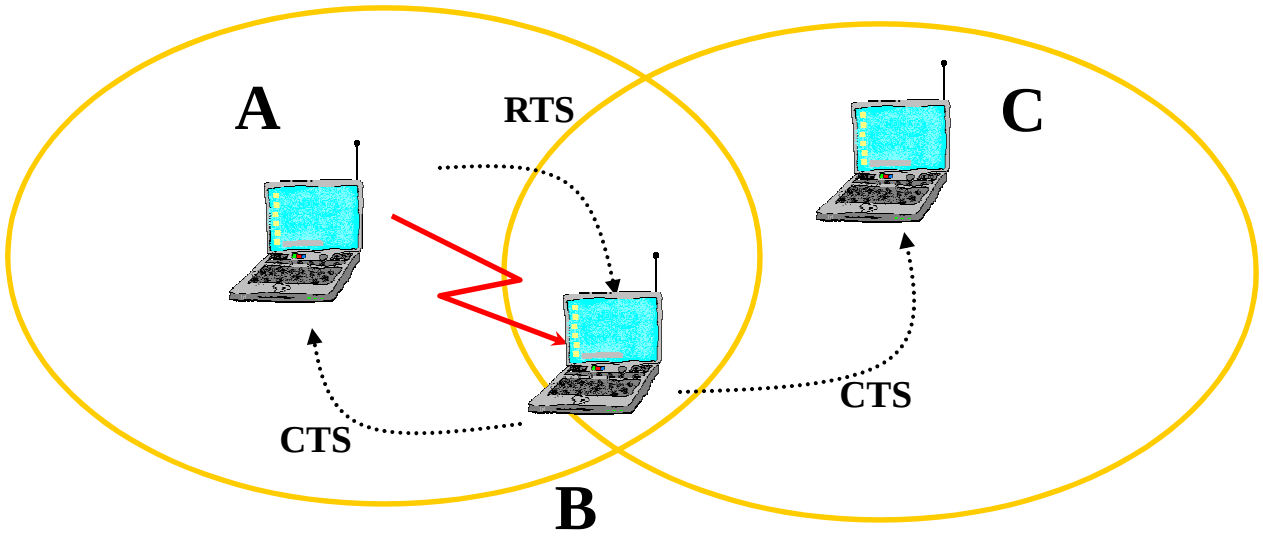


- Ingredients
  - Control frames:
    - *Request To Send (RTS)*
    - *Clear To Send* (CTS)
  - Network Allocation Vector (NAV)

Example

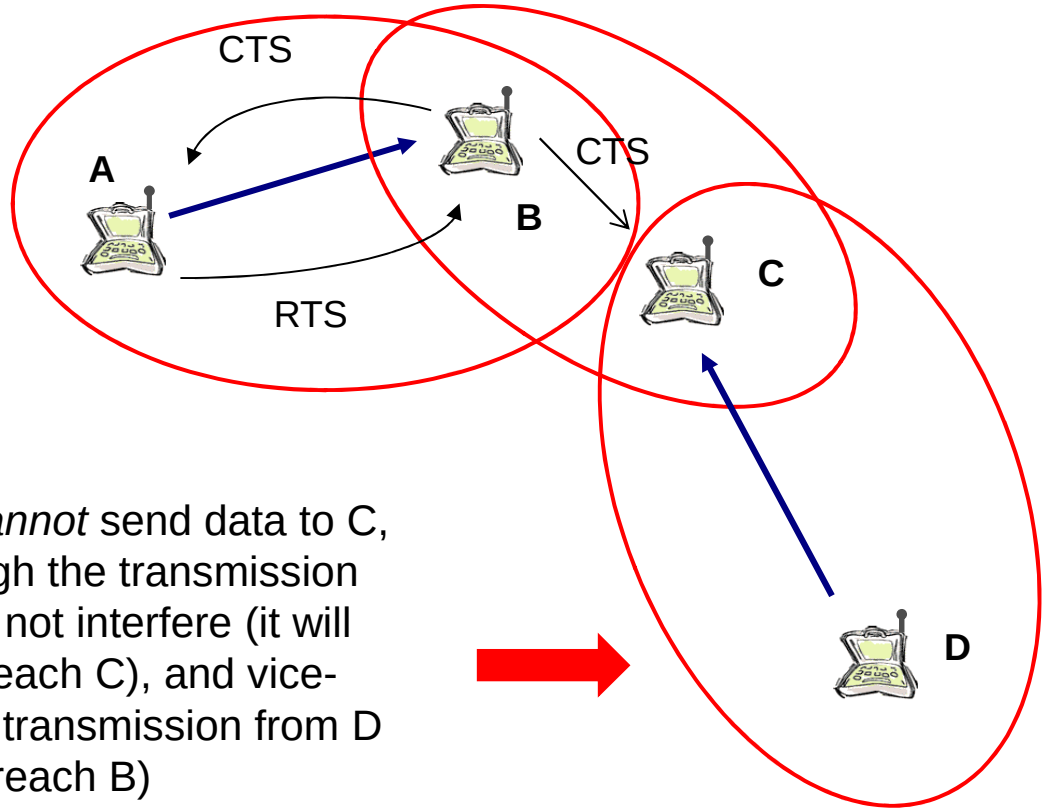

Station 1
Station 2
NAV
NAV
DIFS
random backoff (7 slots)
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
new random backoff (10 slots)
Station defers
NAV
Station 2 talks to Station 1
Station 3
Station 4
NAV
NAV
DIFS
random backoff (9 slots)
Station defers, but keeps backoff counter (=2)
Station sets NAV upon receiving RTS
DIFS
remaining backoff (2 slots)
DATA
SIFS
ACK
Station 5
Station 6
SIFS
ACK
DATA
Station sets NAV upon receiving RTS
Station sets NAV upon receiving CTS, this station is hidden to station 1
time

Hidden terminal solved



Exposed terminal

- … but another problem is created



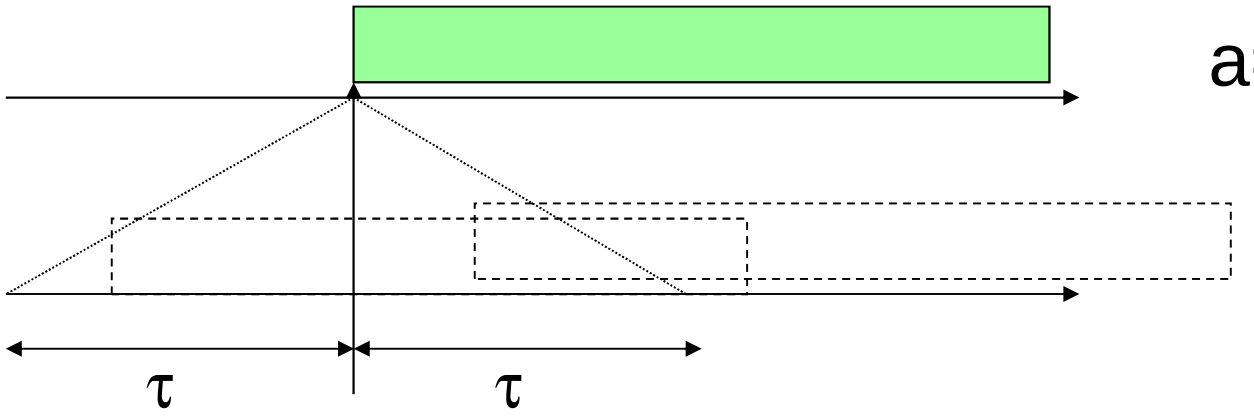
Here, D *cannot* send data to C, even though the transmission from A will not interfere (it will not even reach C), and vice-versa (the transmission from D will never reach B)

Overhead

- The exchange of control frames *reduces* channel capacity
- Transmission efficiency depends on:
  - Channel quality
  - Data frame size
- 802.11 standard defines a threshold (*RTSThreshold*) on the size (D) of data frames:
  - If D < *RTSThreshold,* RTS/CTS exchange is *NOT* used
  - If D > *RTSThreshold*, RTS/CTS exchange is used

Throughput analysis of CSMA

- Simplified model
- No hidden terminals
- CSMA: like Aloha but transmit only when you sense the channel free



Maximum delay (distance) between 2 stations

$a=\tau/T$

Frame duration (supposed fixed)

Throughput analysis of CSMA

- On the channel we have cycles of *Busy* (at least one station senses the channel as busy) and *Idle* (all stations sense the channel free) periods
- The throughput S can be given by:

$$S = \frac{\alpha}{B + I}$$

  - where B and I are the *average busy* and *idle periods,* and α is the probability that there is a successful transmission in a busy period

Throughput analysis of CSMA

- Making the same assumptions of the Aloha infinite population model we have: $\alpha = e^{-aG}$

$$I = \frac{1}{G}$$

$$B = e^{-aG}(1+a) + (1-e^{-aG})(1+a+Z)$$

- where Z is the time when colliding transmissions partially overlap

Throughput analysis of CSMA

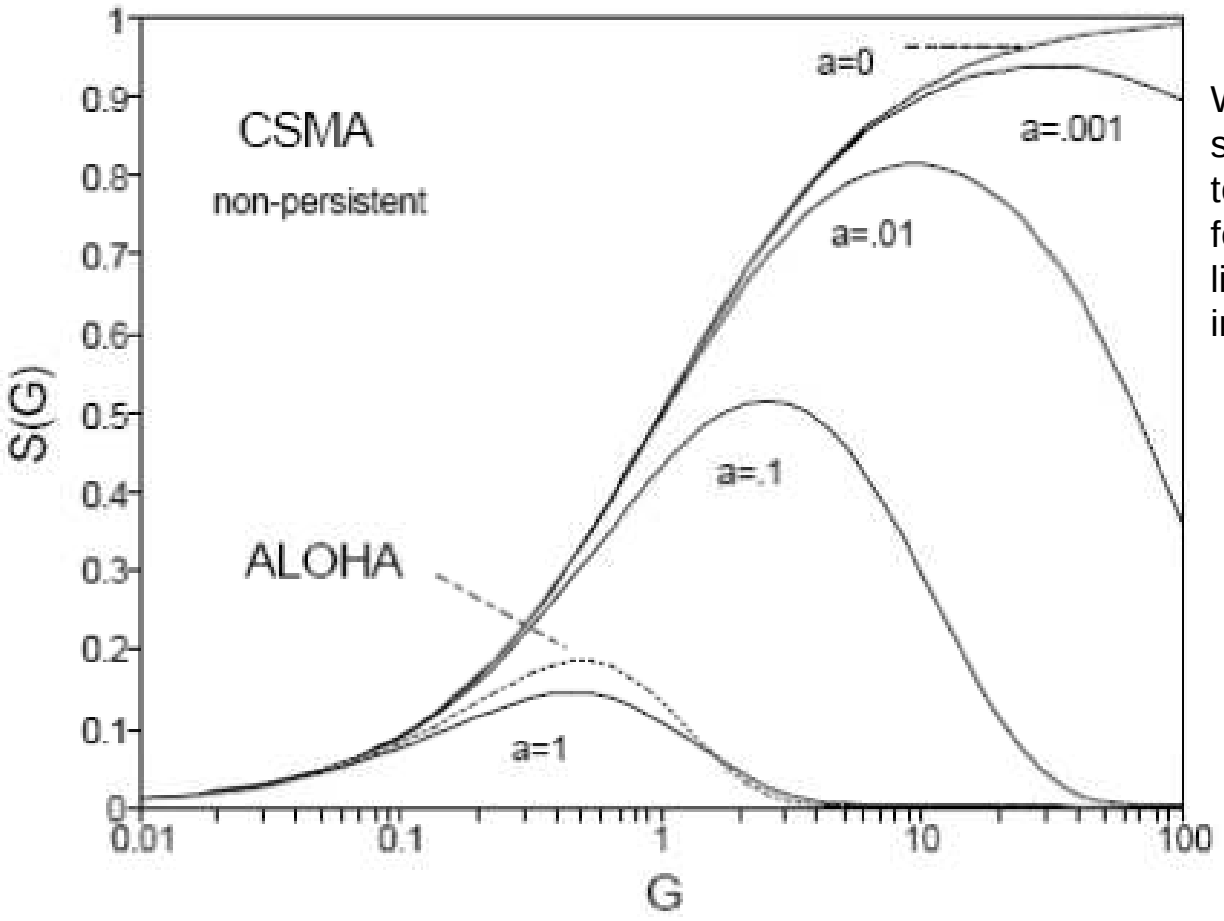
- It can be shown that:

$$Z = a + \frac{ae^{-aG}}{1-e^{-aG}} - \frac{1}{G}$$

- Therefore we get:

$$S = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}}$$

Throughput analysis of CSMA



When a is small, all stations are *very close* to each other (the feedback from channel listening is almost immediate)

Throughput analysis of CSMA/CA

- Similarly to the general model we can derive a model for 802.11 DCF

$$\alpha = e^{-aG}$$

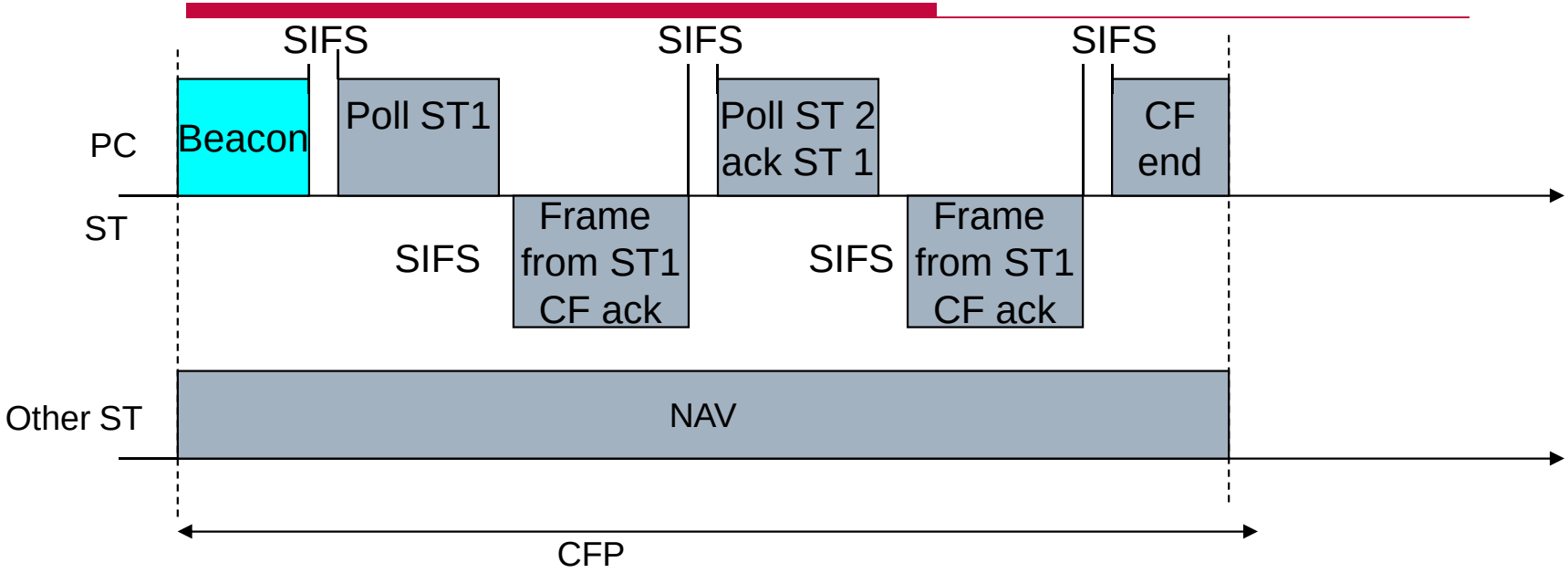
$$I = \frac{1}{G}$$

a = interframe space
b = duration of RTS and CTS

$$B = e^{-aG}(1+3a+2b) + (1-e^{-aG})(b+a+Z)$$

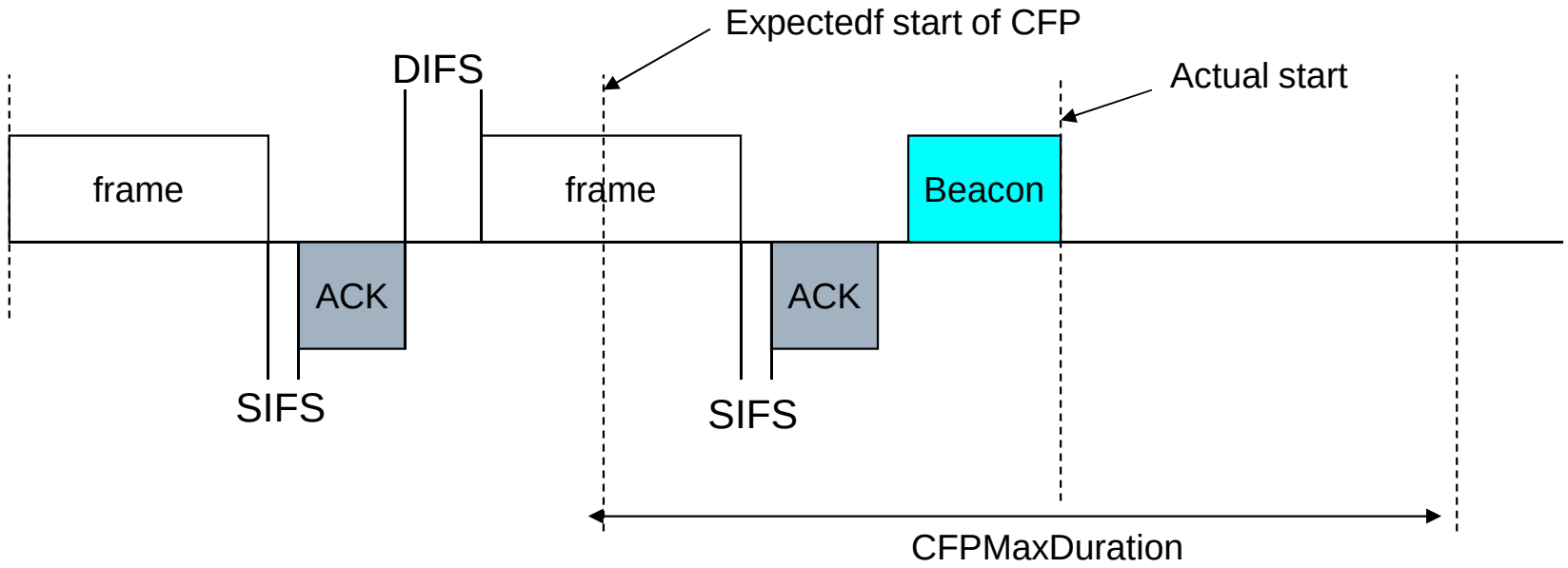
$$S = \frac{Ge^{-aG}}{G(1+2a)+e^{-aG}-G(1-b)(1-e^{-aG})+(2a+2b)Ge^{-aG}}$$

Point Coordination Function (PCF)



- PCF has never been used in commercial devices
- PCF cannot guarantee QoS due to a couple of "mistakes"

Point Coordination Function (PCF)



- Unpredictable inter-beacon interval
- No constraint on frame transmission duration

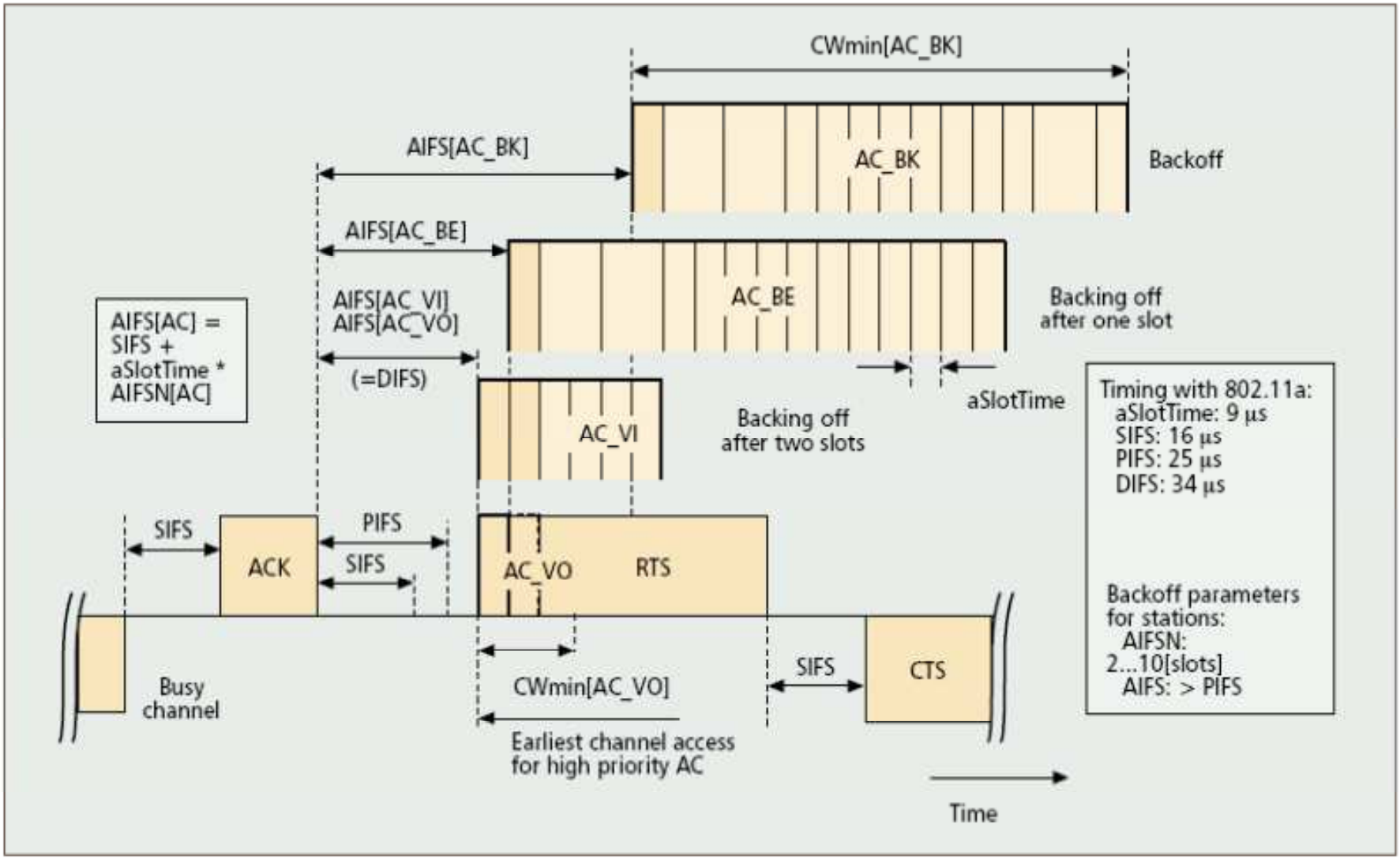
802.11e

- Flow differentiation
  - 4 queues for 4 traffic classes
- *Transmission Opportunities* (TXOP)
  - Defined as the Maximum transmission time per transmission
- Direct transmission
- *Block ACK (*single ACK for a "train" of frames*)*
- *Hybrid Coordination Function (HCF) with two access modes*
  - Contention based (EDCA, *Enhanced Distributed Channel Access*)
  - Contention free (HCCA, *HCF Controlled Channel Access*)

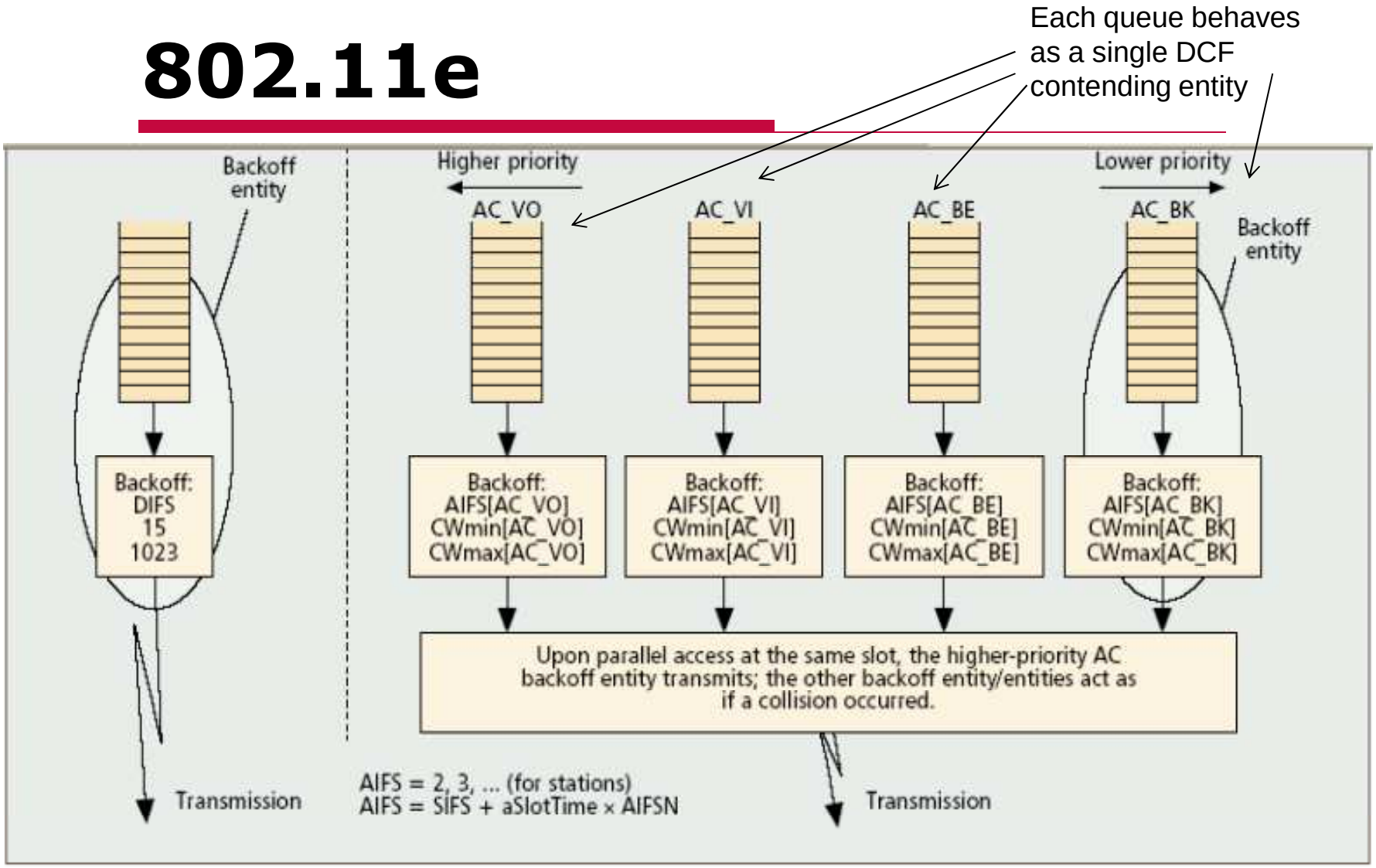
EDCA

- 4 Access Categories (AC)
  - AC_VO: voice
  - AC_VI: video
  - AC_BE: best effort
  - AC_BK: background
- Each AC is characterized by different *backoff* parameters:
  - *AIFS[AC]: inter-frame space*
  - *CWMin[AC]: minimum backoff window*
  - *CWMax[AC]: maximum backoff window*
  - *TXOPlimit[AC]: maximum transmission duration*

Example: access with EDCA

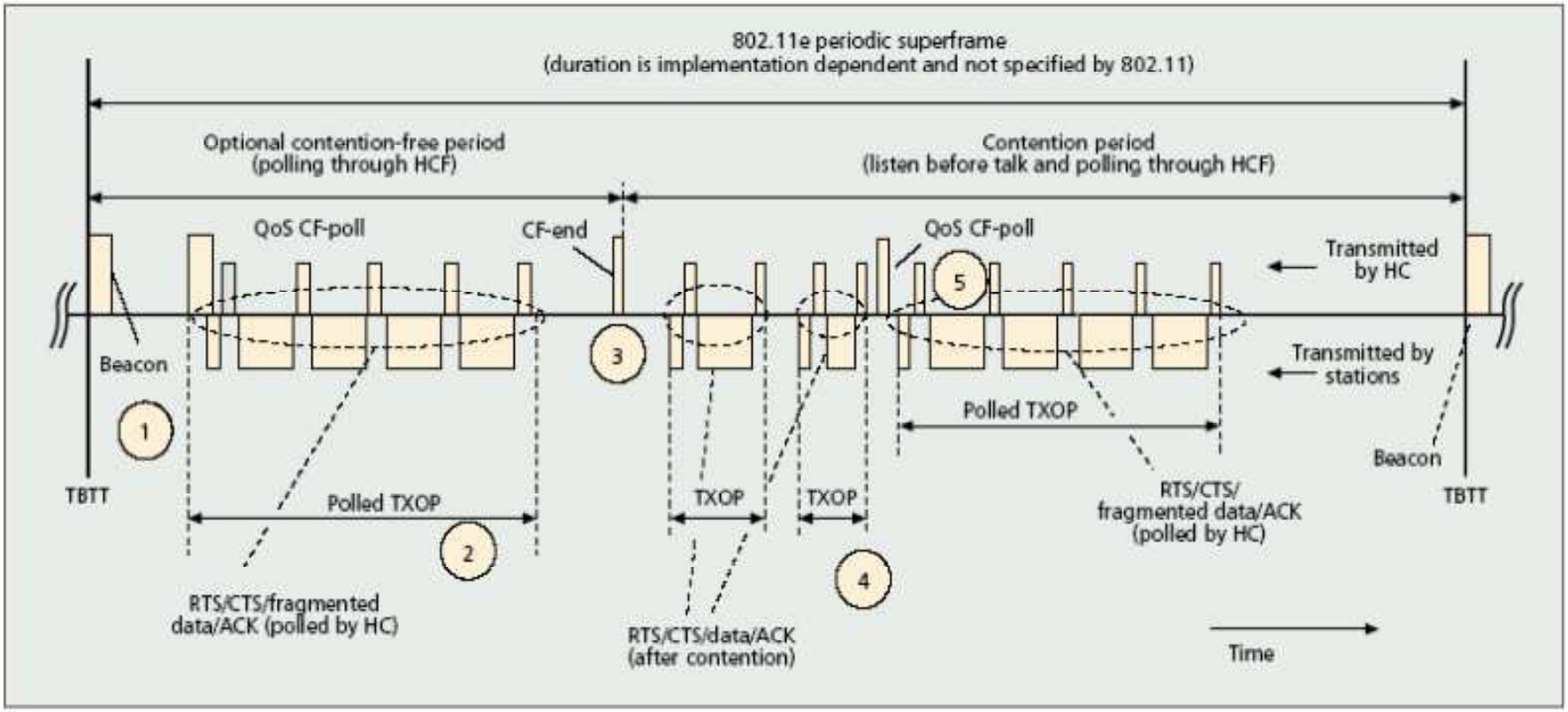


802.11e



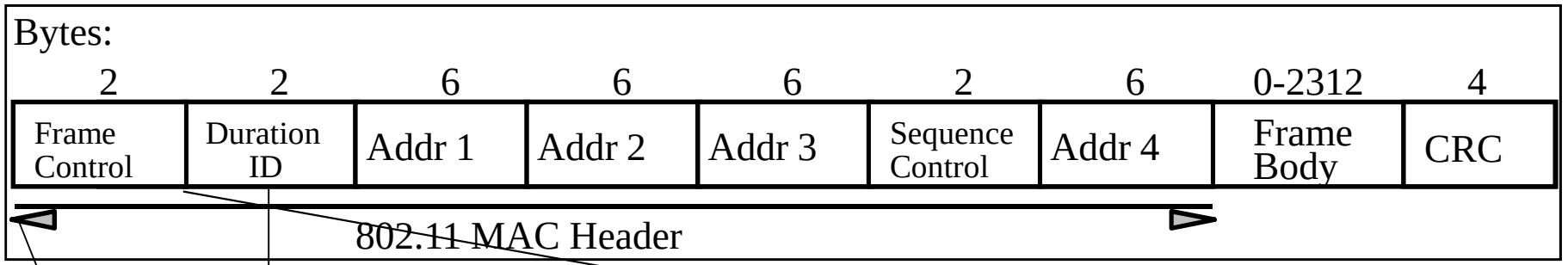
- Several *backoff entities* inside the same station (*Virtual collision* handler)

HCCA

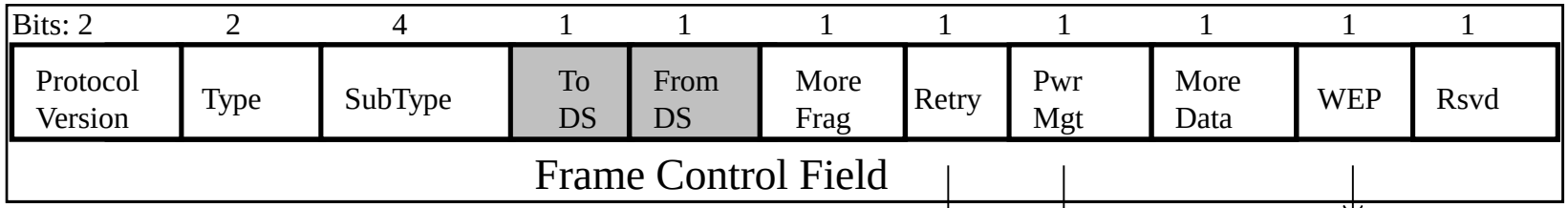


- Contention-free and contention-based transmissions can be mixed together

Frame Format



used to set NAV



set to ”1” when frame encrypted

any retransmitted frame sets the Retry bit to ”1”.

”1” means devices are in power-saving mode, ”0” active. (APs are not allowed to power-save mode because they perform management functions).

Type & Subtype

- Data (type=10)
- Control (type=01)
- Management (type=00)

Management

Subtype bit	**Message**
0000	Association request
1000	Beacon
1011	Authentication

Control

Subtype bit	**Message**
1011	RTS
1100	CTS
1101	ACK

Data

Subtype bit	**Message**
0000	DATA
0001	DATA+CF ack
0010	Data+CF poll

Addresses

- Four address fields: 48 bits long (as in Ethernet). Not always used, and not for all the MAC frames: they depend on frame type
- Different types of addresses:
  - *Destination Address (DA):* final destination
  - *Source Address (SA):* frame source
  - *Receiver Address (RA):* receiving station
  - *Transmitter Address (TA):* transmitting station
  - *Basic Service Set ID (BSSID):* BSS address
    - *Infrastructure* BSS: MAC address of the AP
    - IBSS: random number or address of one station

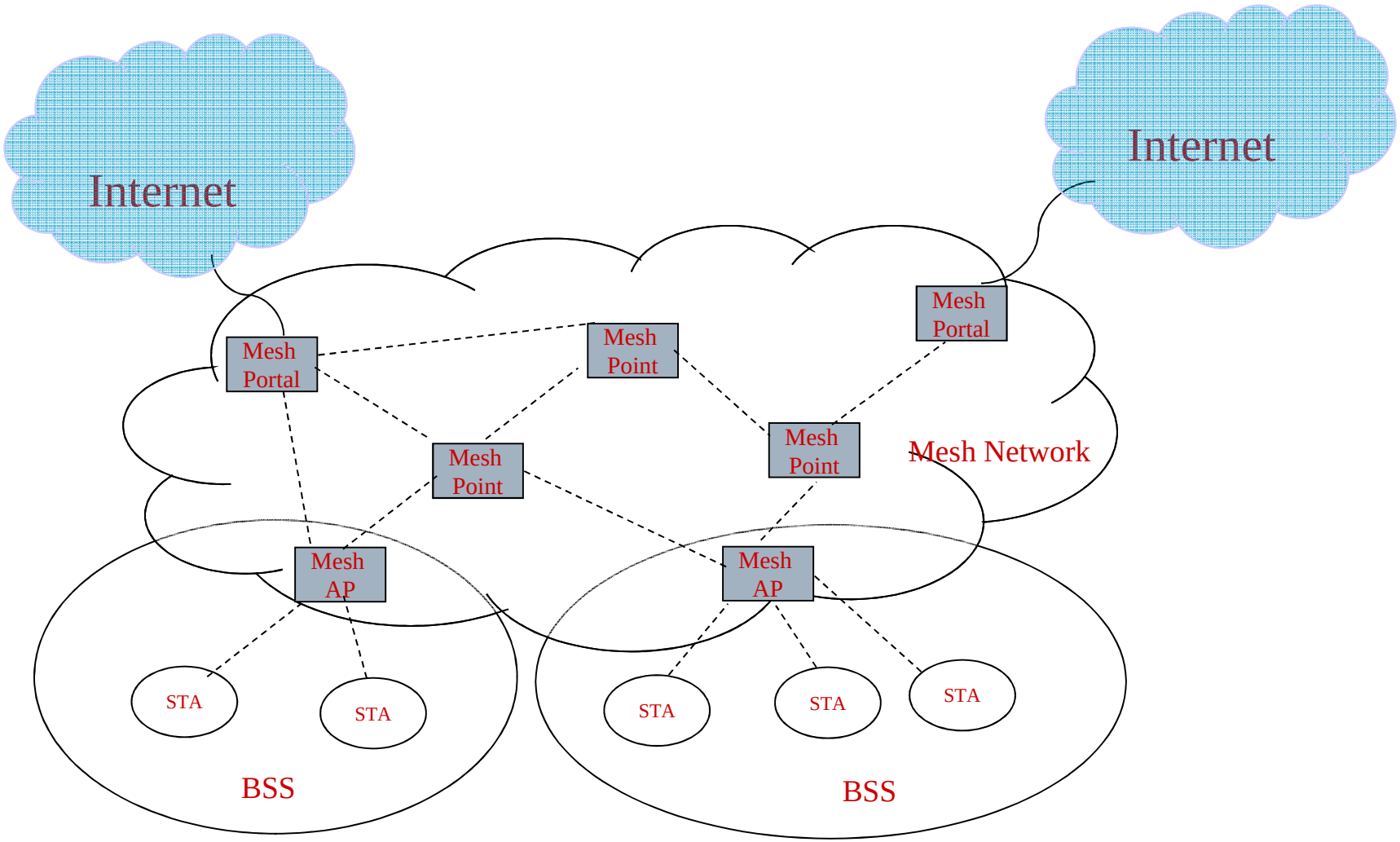
Addresses

- Rule of thumb:
  - address1 used for the receiver;
  - address2 used for the transmitter;
  - address3 used for filtering by the receiver (frames discarded from a BSS other than the associated one).

Network *Management*

- Management frames are used for:
  - *Scanning*
  - *Authentication*
  - *Association*
  - *Power Management*
  - *Synchronization*

Wireless Mesh Networks

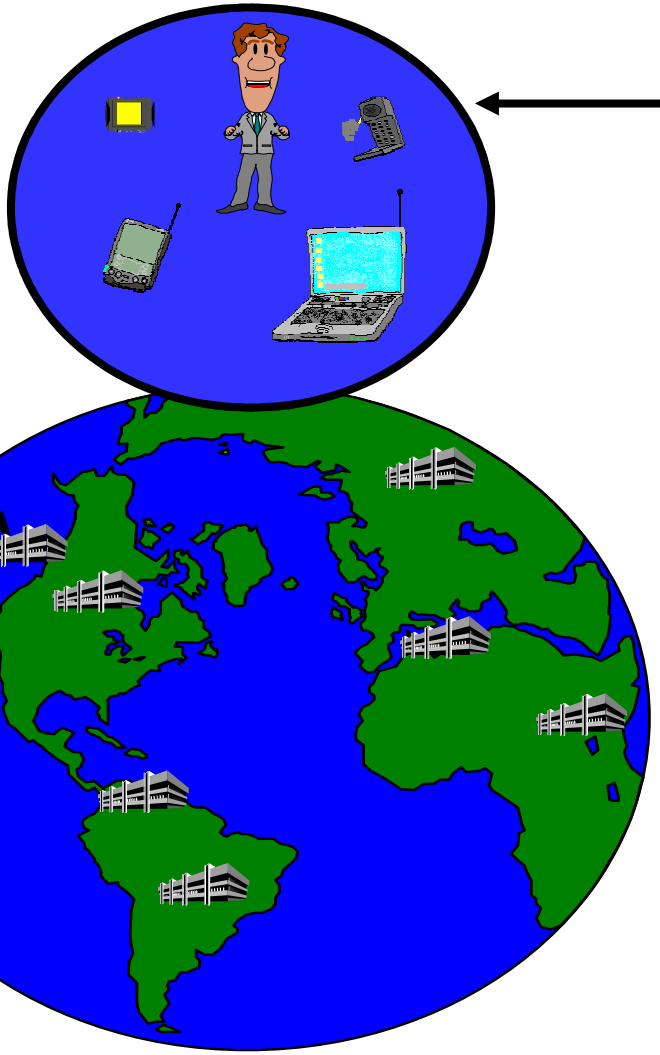


Part B
WPAN

Personal Area

WLAN

On-campus: Office, School, Airport, Hotel, Home



WPAN

Person Space: Office, Room, Briefcase, Pocket, Car

Short Range/Low Power

Voice AND Data

Low-cost

Small form factor

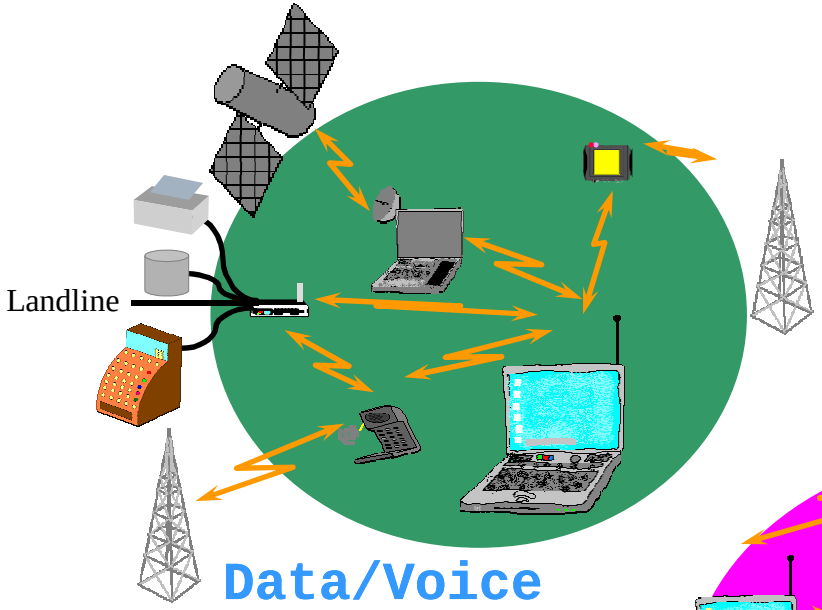
Many Co-located Nets

Universal Bridge

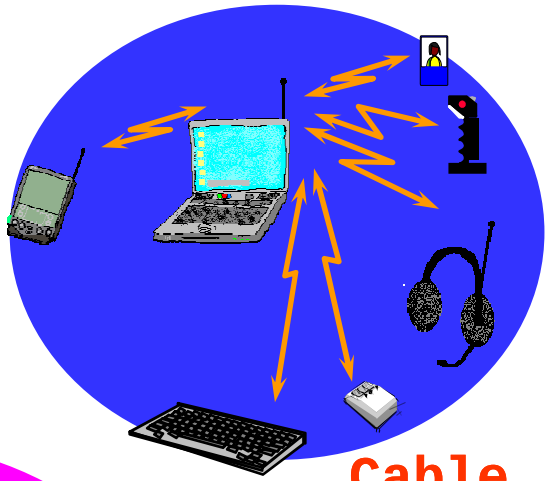
Cellular

Off-Campus Global Coverage

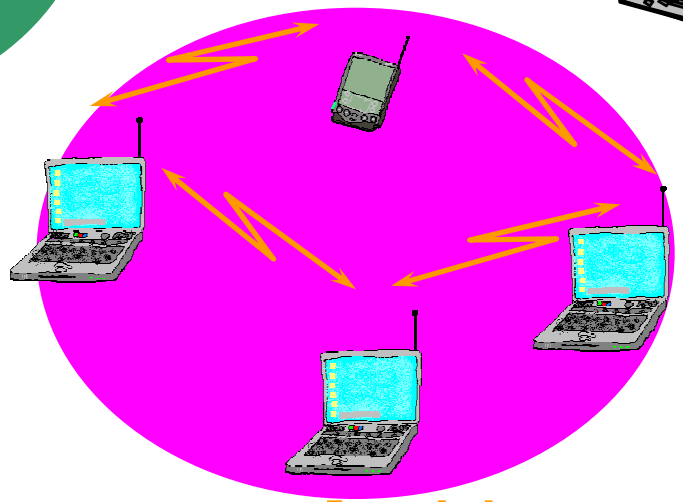
Personal Area



Data/Voice
Access Points



Cable
Replacement



Personal Ad-hoc
Connectivity

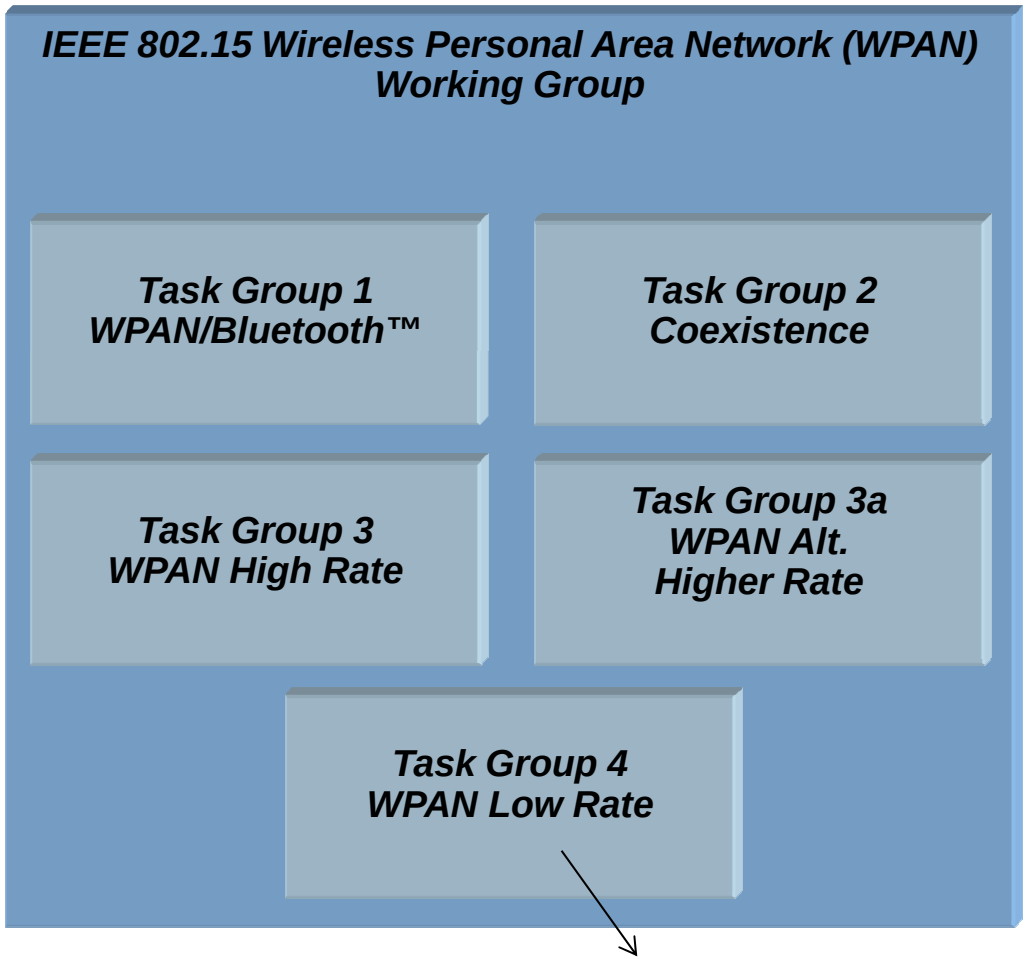
IEEE 802.15

Wireless Personal Area Networks (WPANs™)

- Short range
- Low power
- Low cost
- Small networks (including point-to-point links)
- "Personal Operating Space"

- Working Group (WG) created by IEEE, pushed by Bluetooth success

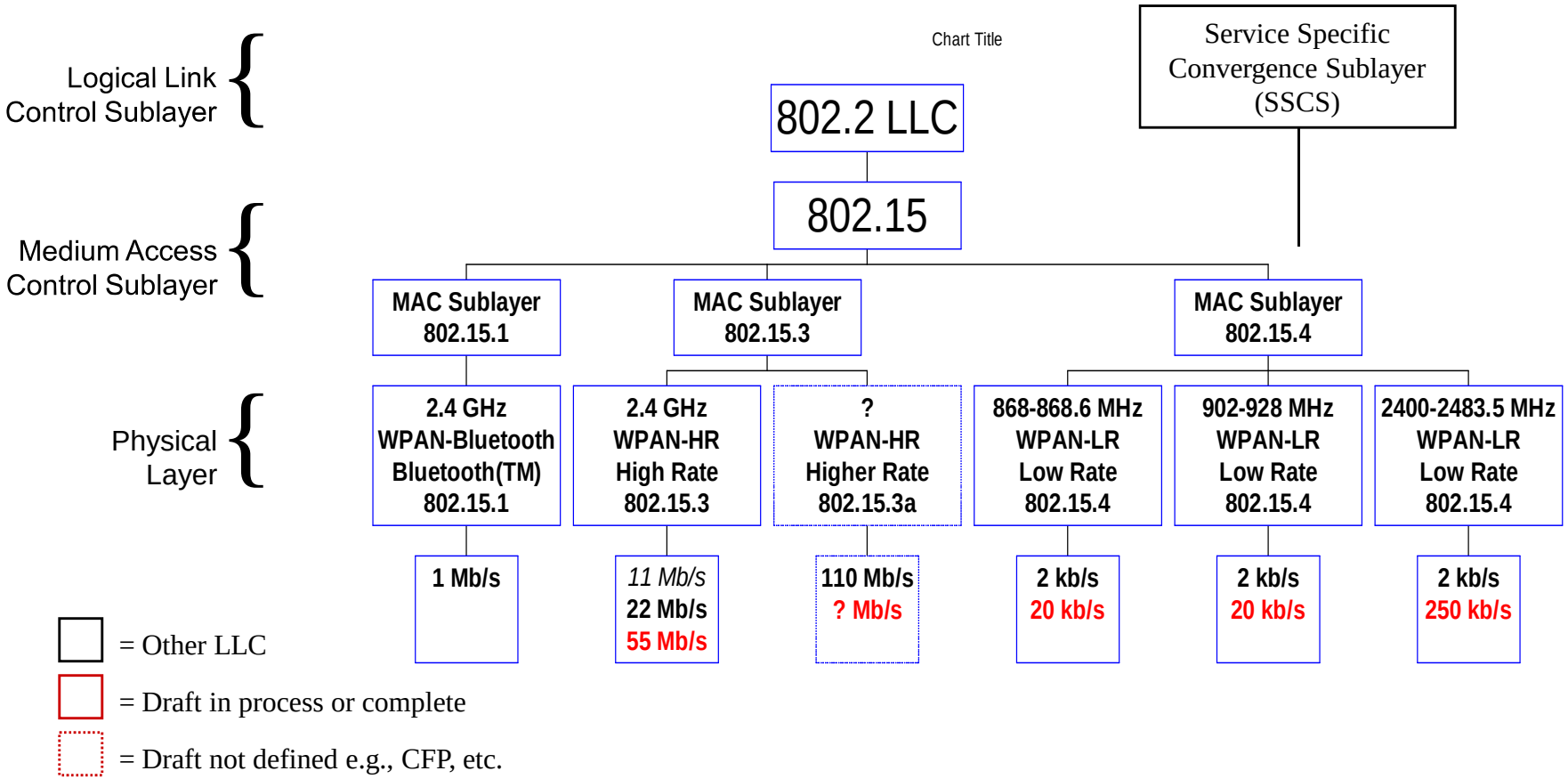
IEEE Wireless Standards



- IEEE 802.11 WLAN Working Group
- IEEE 802.16 WMAN Working Group
- IEEE 802.18 Radio Regulatory TAG
- IEEE 802.19 Coexistence TAG
- IEEE 802.20 Mobile BWA Working Group
- IEEE 802.22 Wireless Regional Area Networks

But very long life battery!

802.15 family

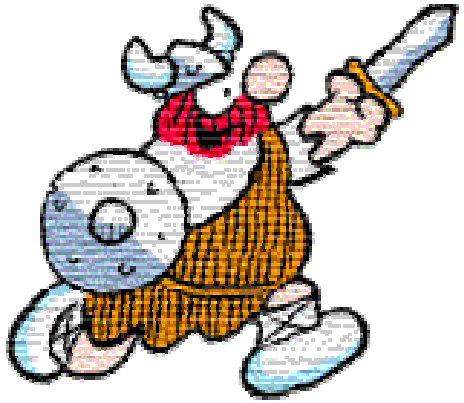


Bluetooth

Bluetooth vs. 802.15.1

- Bluetooth is an *industrial* standard for WPAN
- WG 802.15.1 adopted Bluetooth specifications for levels 1 and 2
- ’96-’97: Ericsson internal project
- ’98: Bluetooth Special Interest Group (SIG) (Ericsson, IBM, Intel, Toshiba, Nokia)
- ’99: Other companies join the SIG (3Com, Lucent Technologies, Microsoft, Motorola)

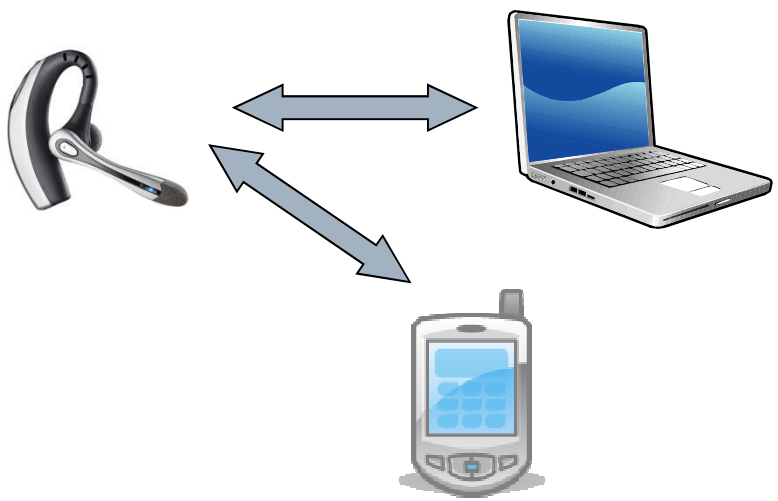
Bluetooth



- Danish king of the middle ages, Harald Blaatand II, alias *Bluetooth* (940-981)
- Unified Denmark and Sweden

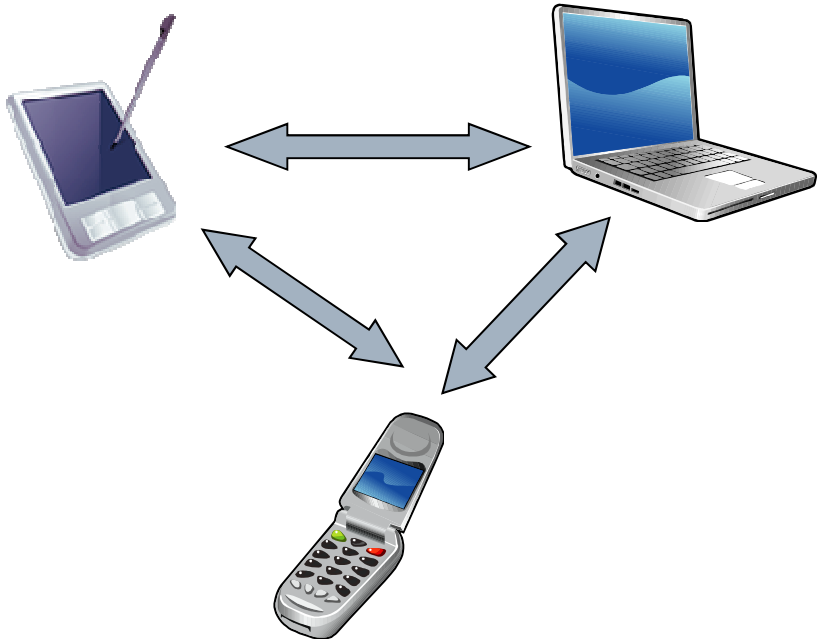
- Radio technology
- Low cost
- Short range (10-20 m)
- Low complexity
- Small size
- Transmission band ISM 2.4 GHz
- Only the first two levels are standardized by IEEE 802.15.1

Application scenarios



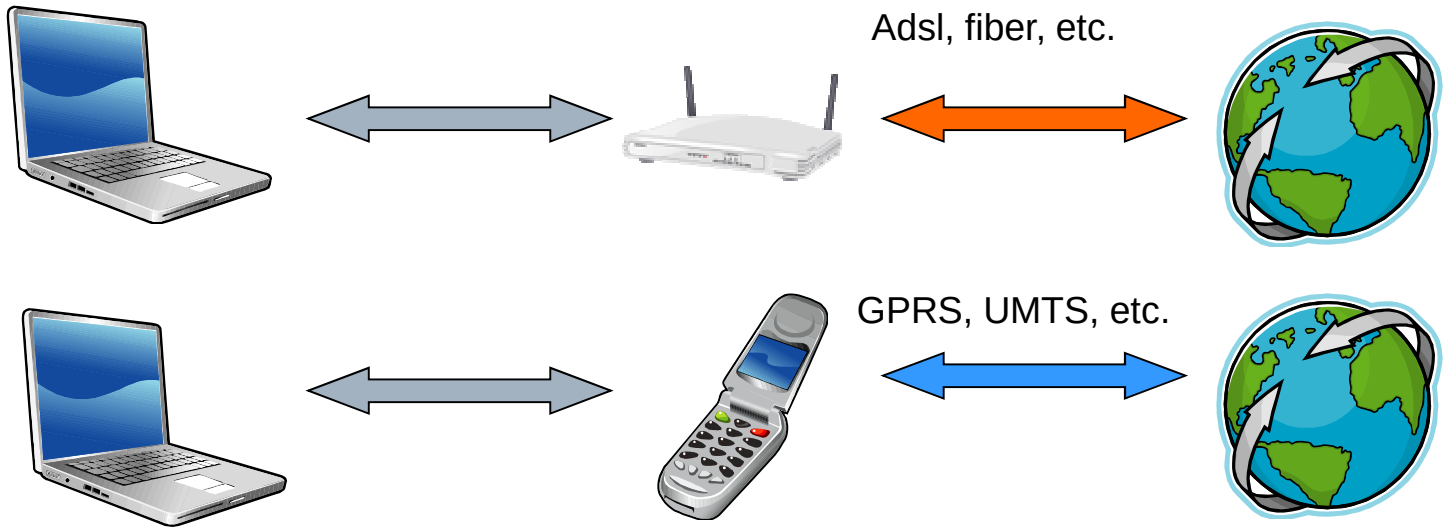
- Headset

Application scenarios



- Data sinchronization

Application scenarios



- Access point

Physical layer

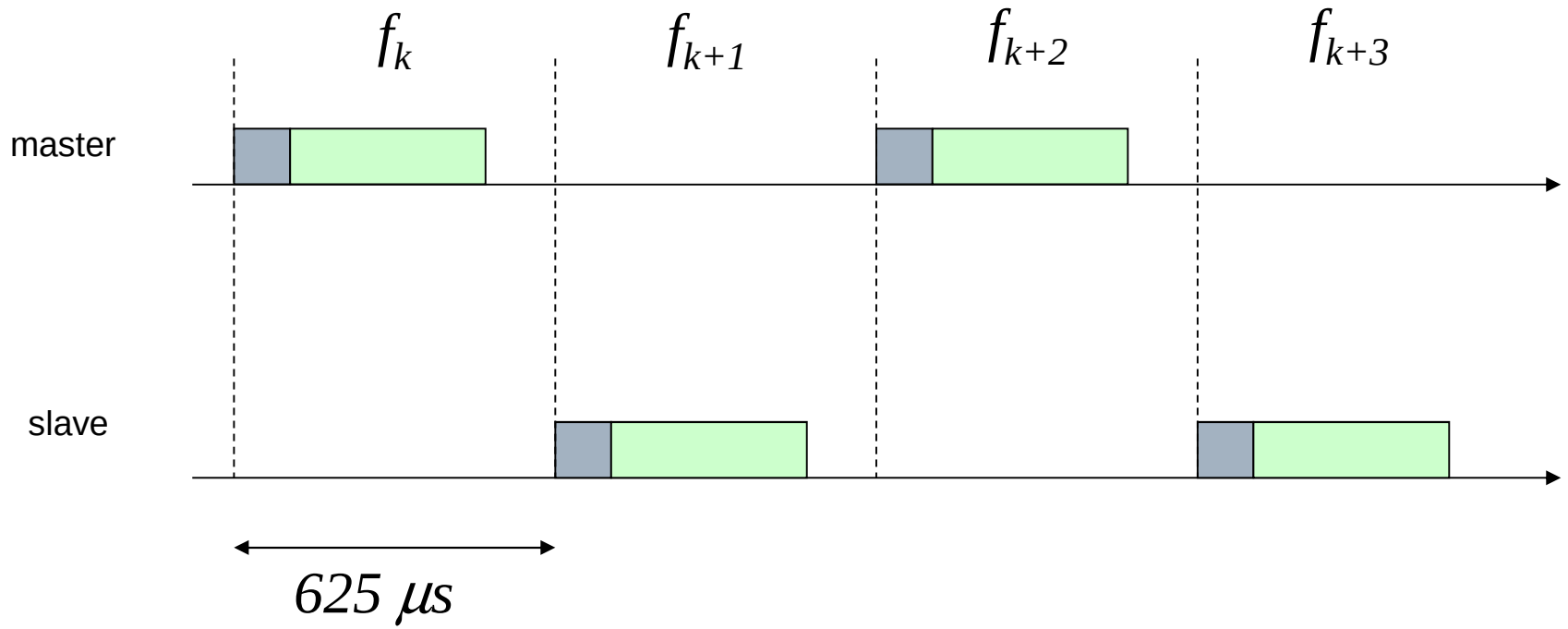
- ISM Band at 2.4 GHz
- 79 (only 23 in France and Japan) channels spaced by 1 MHz (2402-2480 MHz)
- G-FSK (Gaussian FSK) Modulation (1 Mb/s)
  - a binary one is represented by a positive frequency deviation and a binary zero by a negative frequency deviation
- Device classes

Class	**Power (mW)**	**Power (dBm)**	**Range (Approximated)**
Class 1	100 mW	20 dBm	~ 100 meters
Class 2	2,5 mW	4 dBm	~ 10 meters
Class 3	1 mW	0 dBm	~ 1 meter

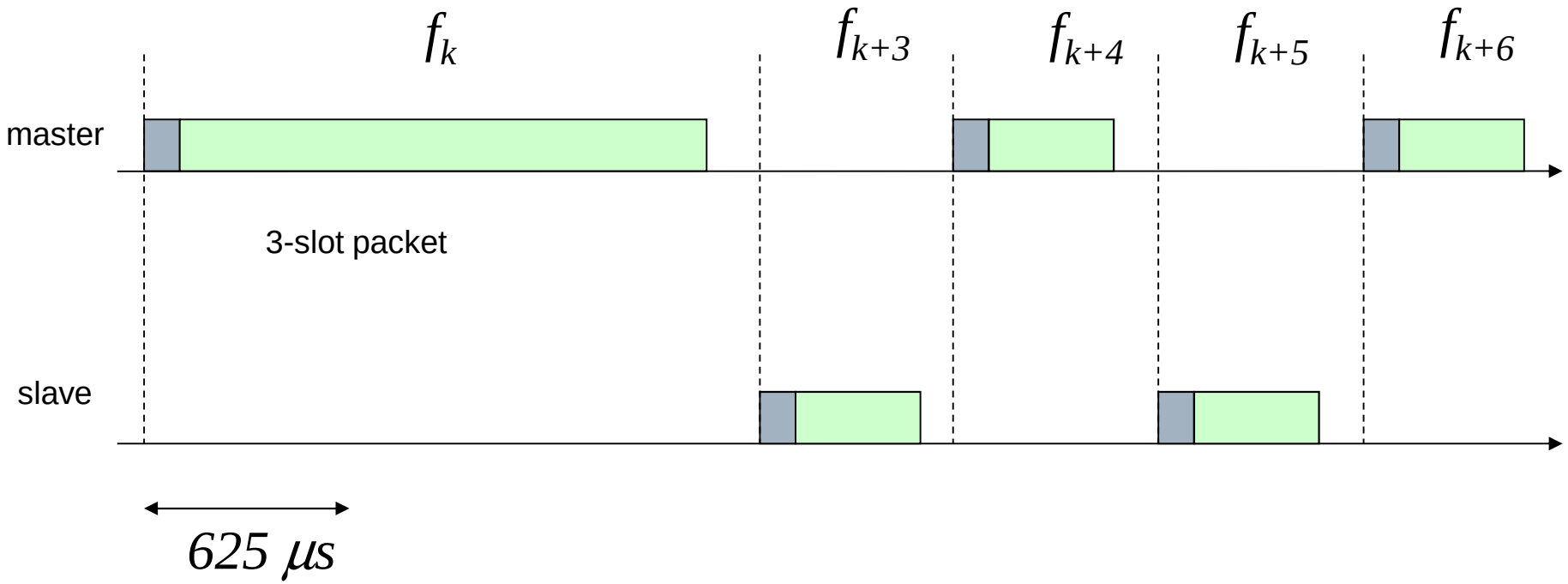
Physical layer

- Frequency Hopping (FH)
- 1600 hops/s (625 μs per hop)
- FH sequence is pseudo random and defined by the clock and the address of the *master* station that regulates channel access
- The other devices are *slave* and follow the sequence f_k defined by the master

Physical layer

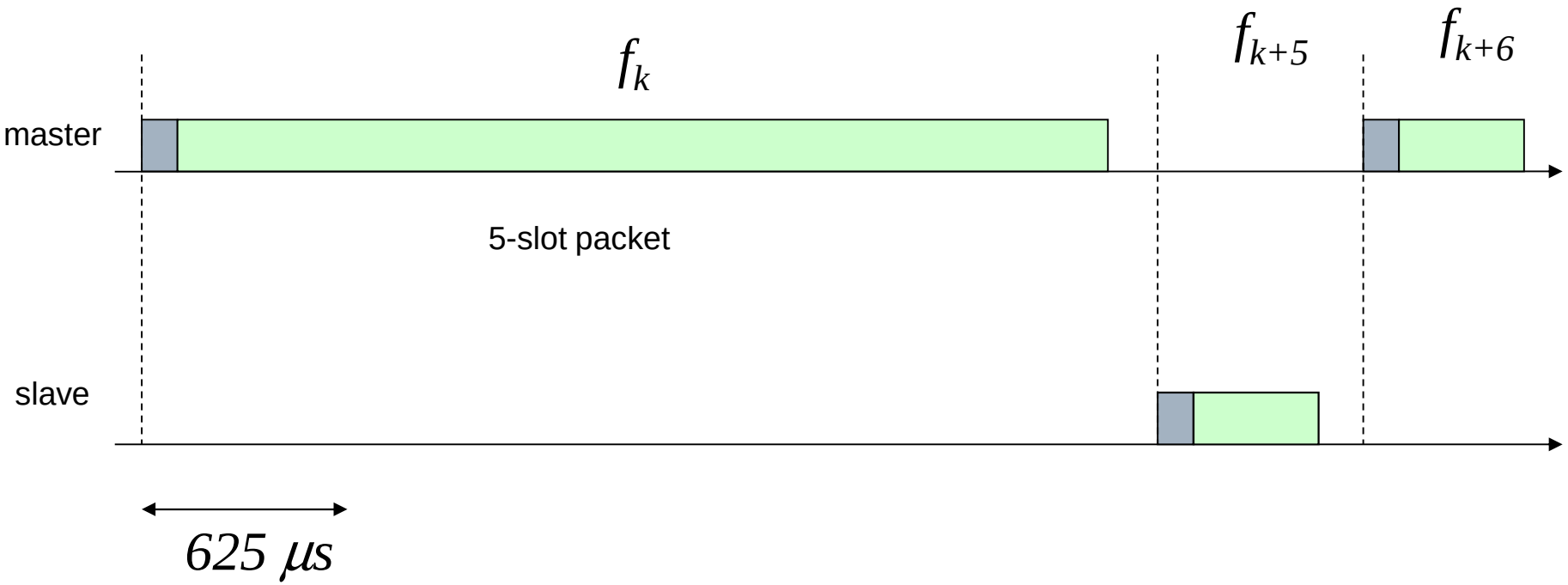


Physical layer



- Packets can span over 1, 3 or 5 slots (625 μs)

Physical layer

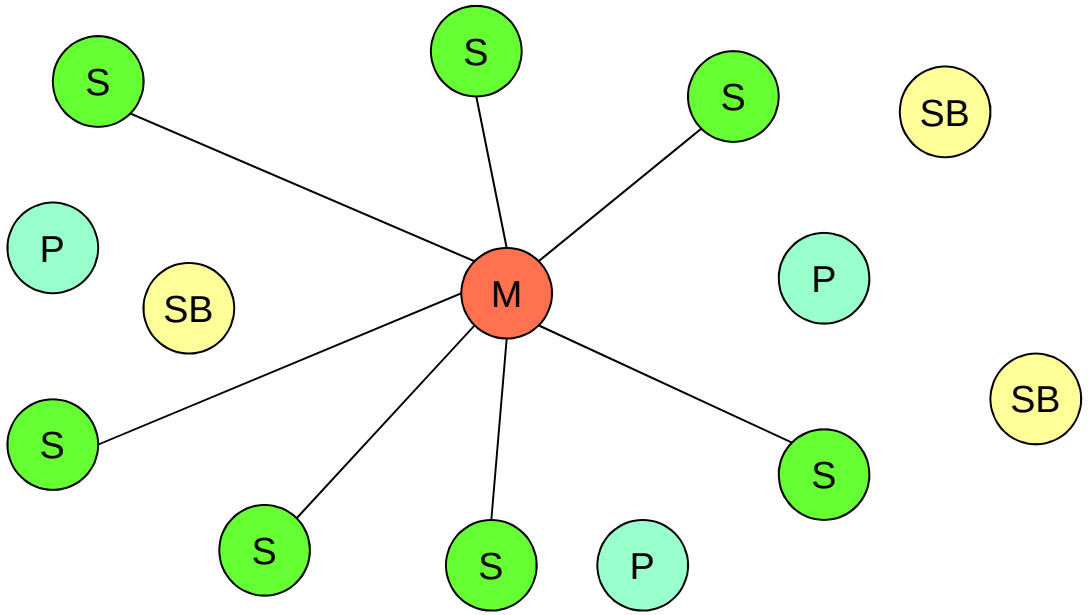


- Packets can span over 1, 3 o 5 slots

Piconet

- Piconet is the simplest architecture of a Bluetooth network
- A Piconet is an **ad hoc network** composed of **2 or more devices**
- One device acts as master, and all the other(s) as slave(s)
- The communication is *only* between master and slaves: slaves *cannot* communicate directly among themselves
- Up to 7 slaves can be activated
- The other nodes can be in:
  - Stand-by (not members of the piconet)
  - *Parked* (still members of the piconet, but not active; up to 256 parked slaves)

Piconet



M= Master
S=Slave

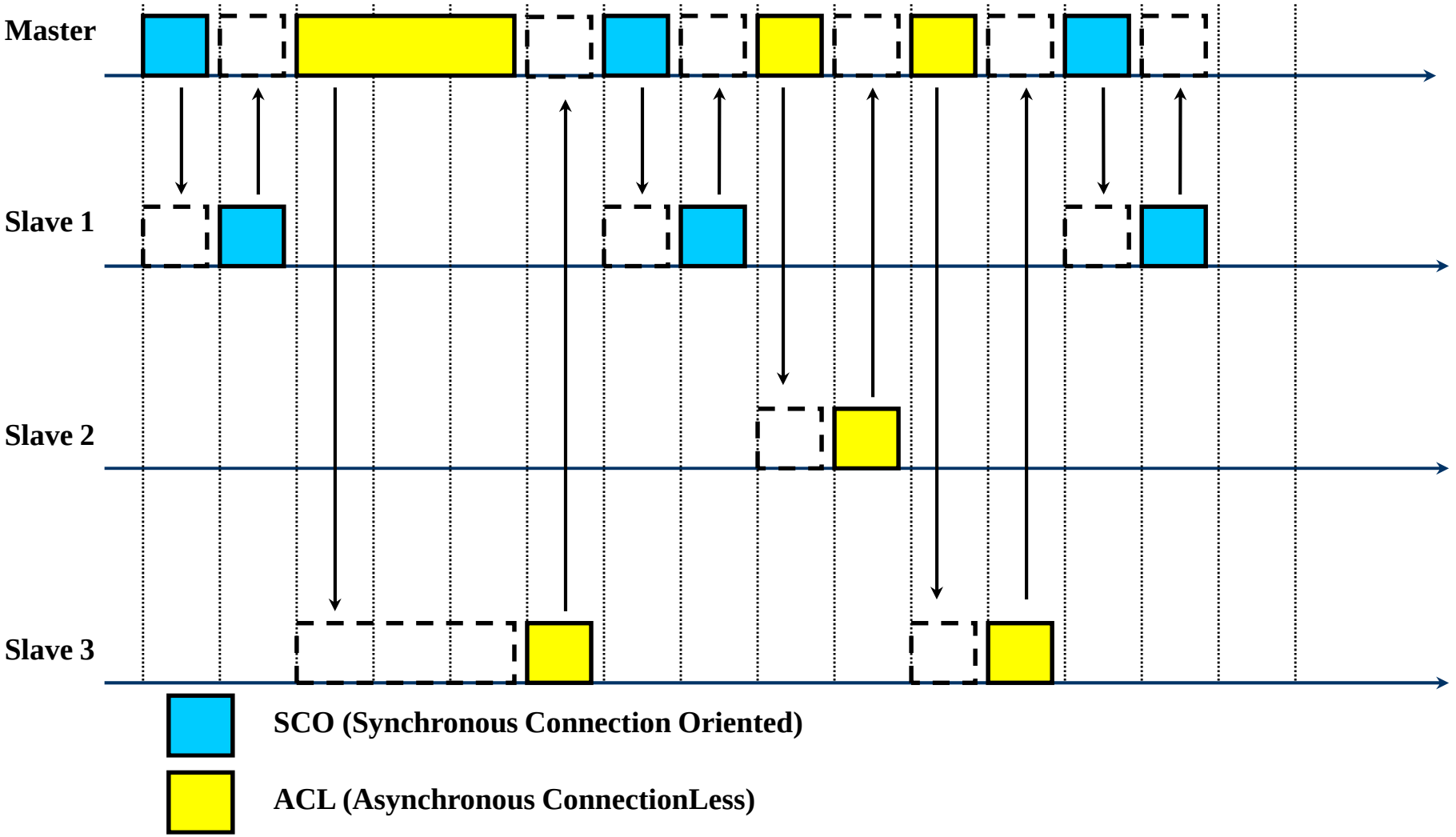
SB=Stand-by
P=Parked

- Addresses
  - MAC address 48 bits
  - AMA (Active Member Address) 3 bits ⟶ Up to 8
  - PMA (Parked Member Address) 8 bits ⟶ Up to 256

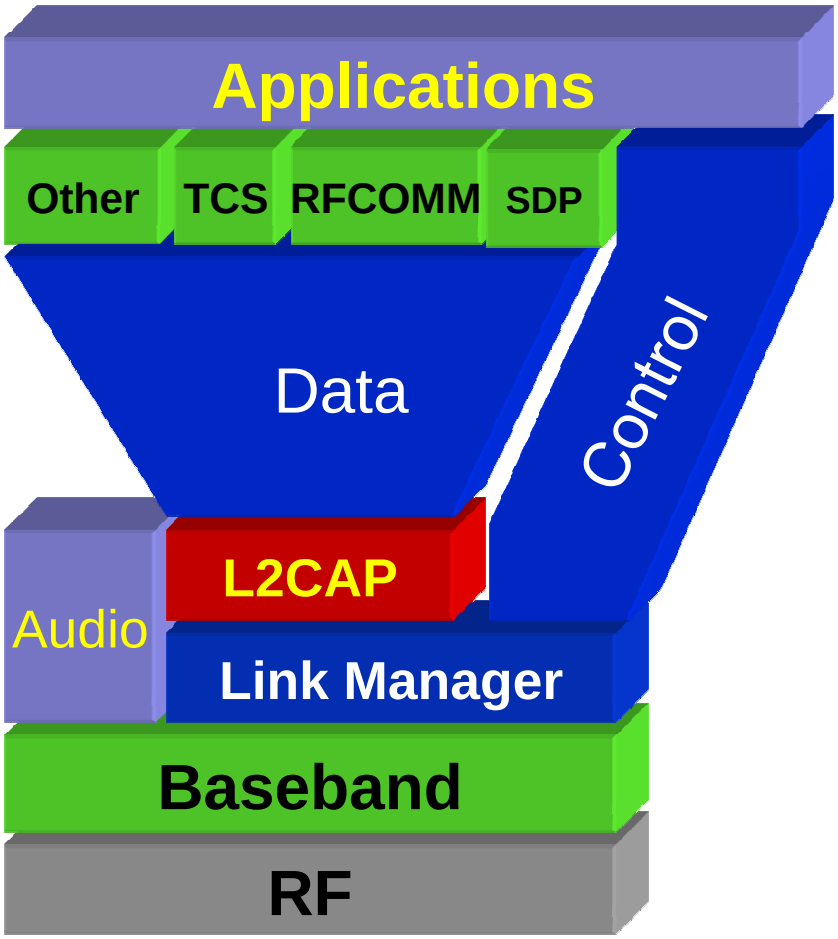
Connection types

- Bluetooth considers two types of connections
- SCO (Synchronous Connection Oriented)
  - Symmetric
  - Bidirectional fixed-capacity connection (“circuit”)
  - Optionally FEC
  - Basic speed 64 kbit/s
- ACL (Asynchronous ConnectionLess)
  - Packet service between master and slaves based on a polling mechanism
  - Several packet formats available
  - Rate up to 433.9 kbit/s symmetric (using 5 slot packets in both directions) and 723.2/57.6 kbit/s asymmetric (using 5 slots in one direction and 1 slot packet in the other)

Multiple access

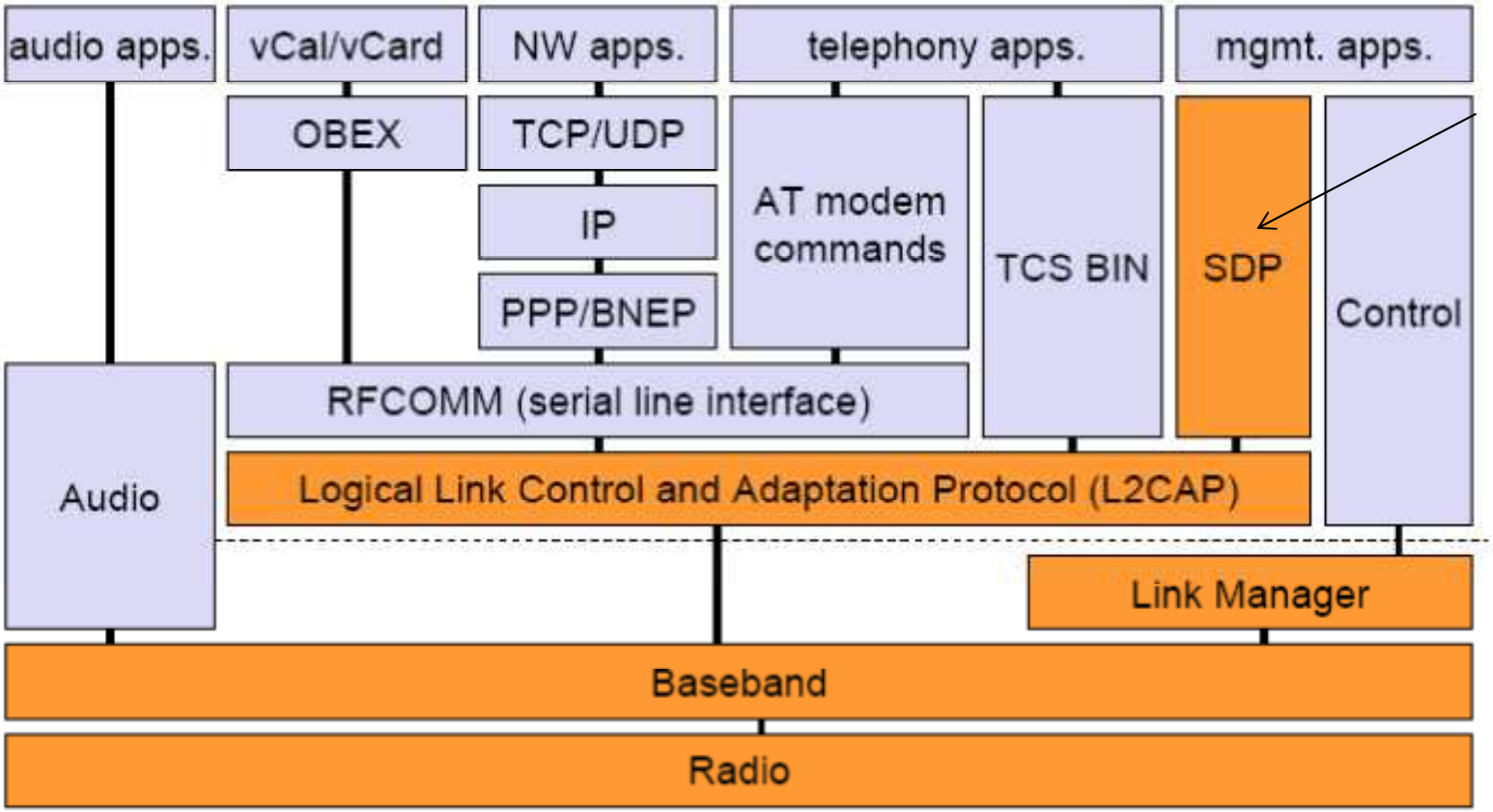


Protocol architecture



- Protocol stack *non compliant* with OSI model (adapted by 802.15.1 specifications with some compromise)
- RF + Baseband equivalent to PHY + MAC
- Control plane for network creation and connection management

Protocol architecture

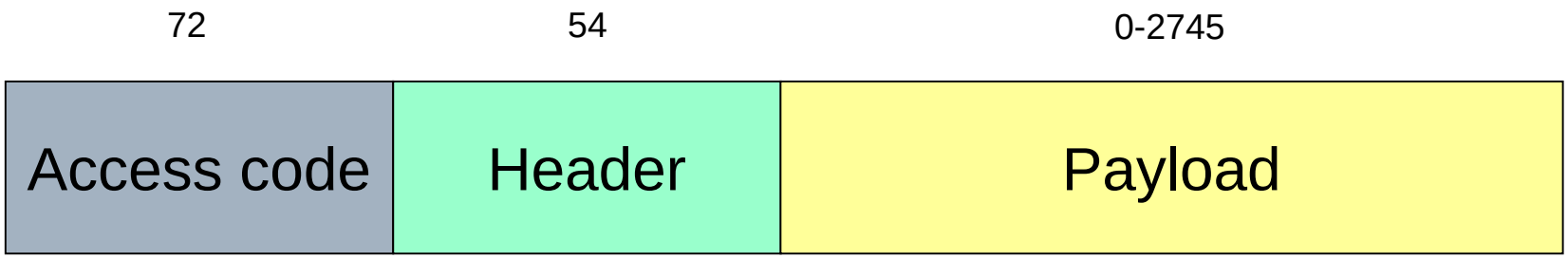


Allows a device to discover services offered by other devices, and their associated parameters

AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

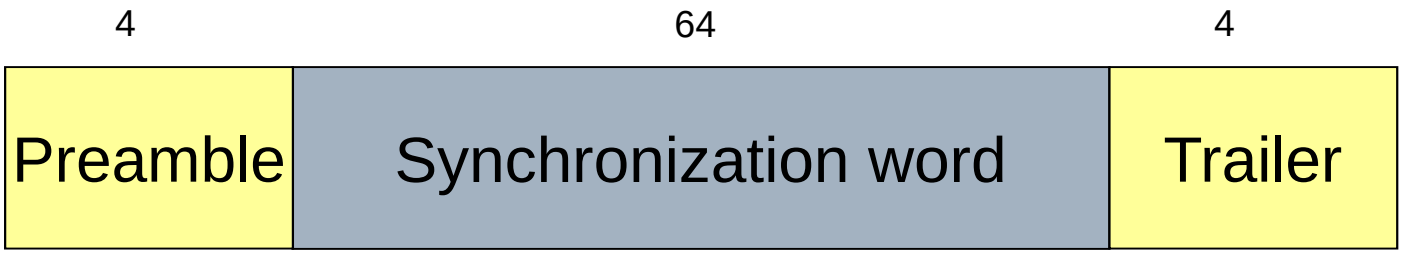
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Packet Format



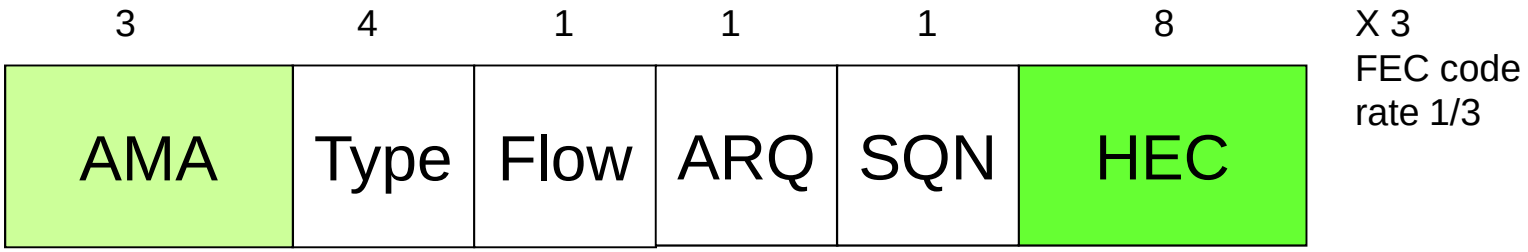
- BT includes three parts:
  - An **Access Code** used for synchronization and piconet identification
  - An **Header** used for Link Control (LC) and ARQ
  - A **Payload** whose format depends on the connection type and packet type (number of slots, FEC, etc.)

Packet Format: Access Code



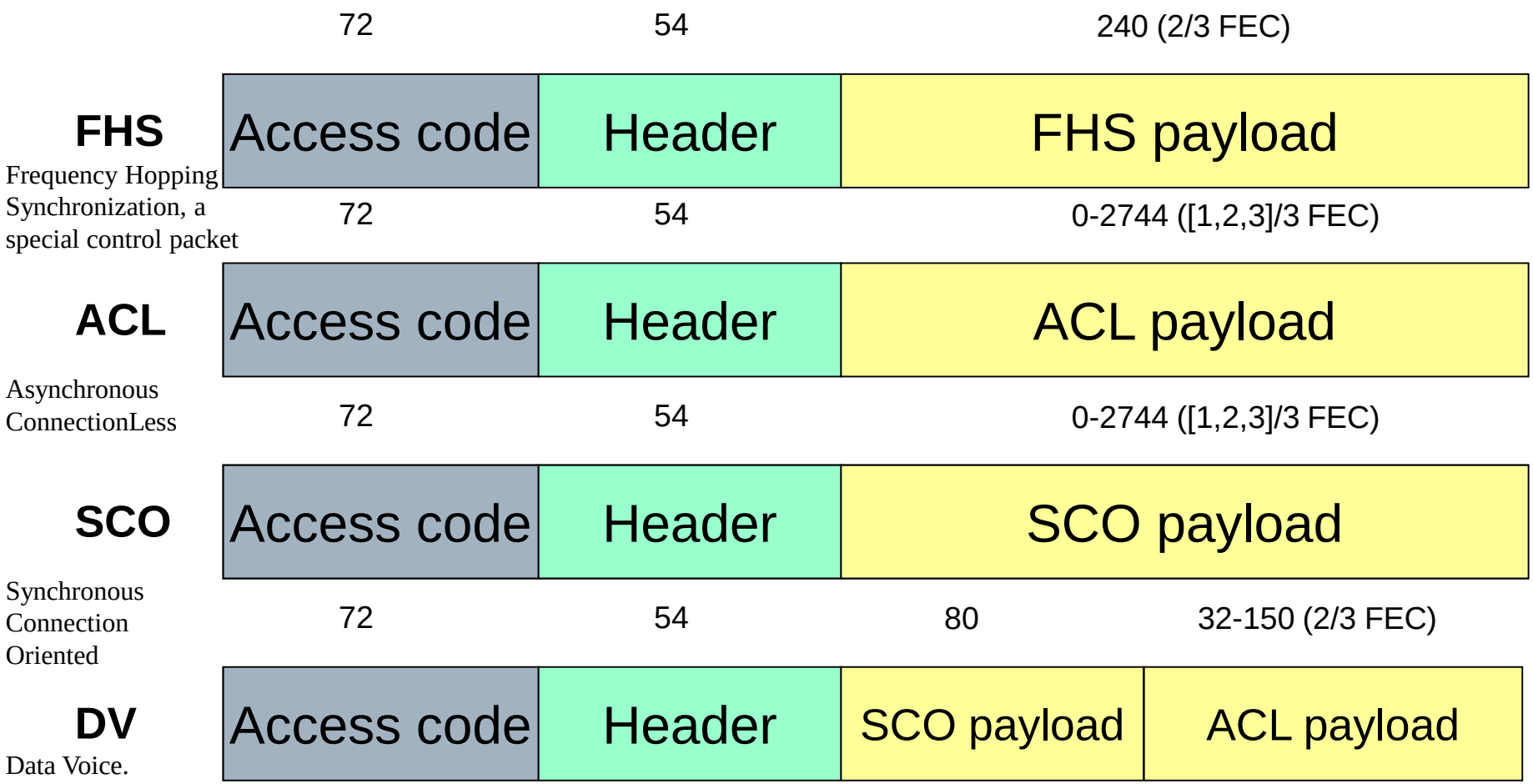
- Access code:
  - There are *three types* of access codes:
  - Channel Access Code (CAC): used to identify the piconet. It defines a piconet and is used in all transmissions; it is based on the *master* MAC address
  - Device Access Code (DAC): used for paging a device before network formation; it is derived directly from the device MAC address
  - Inquiry Access Code (IAC): used to search for all BT devices in range (inquiry)

Packet Format: Header

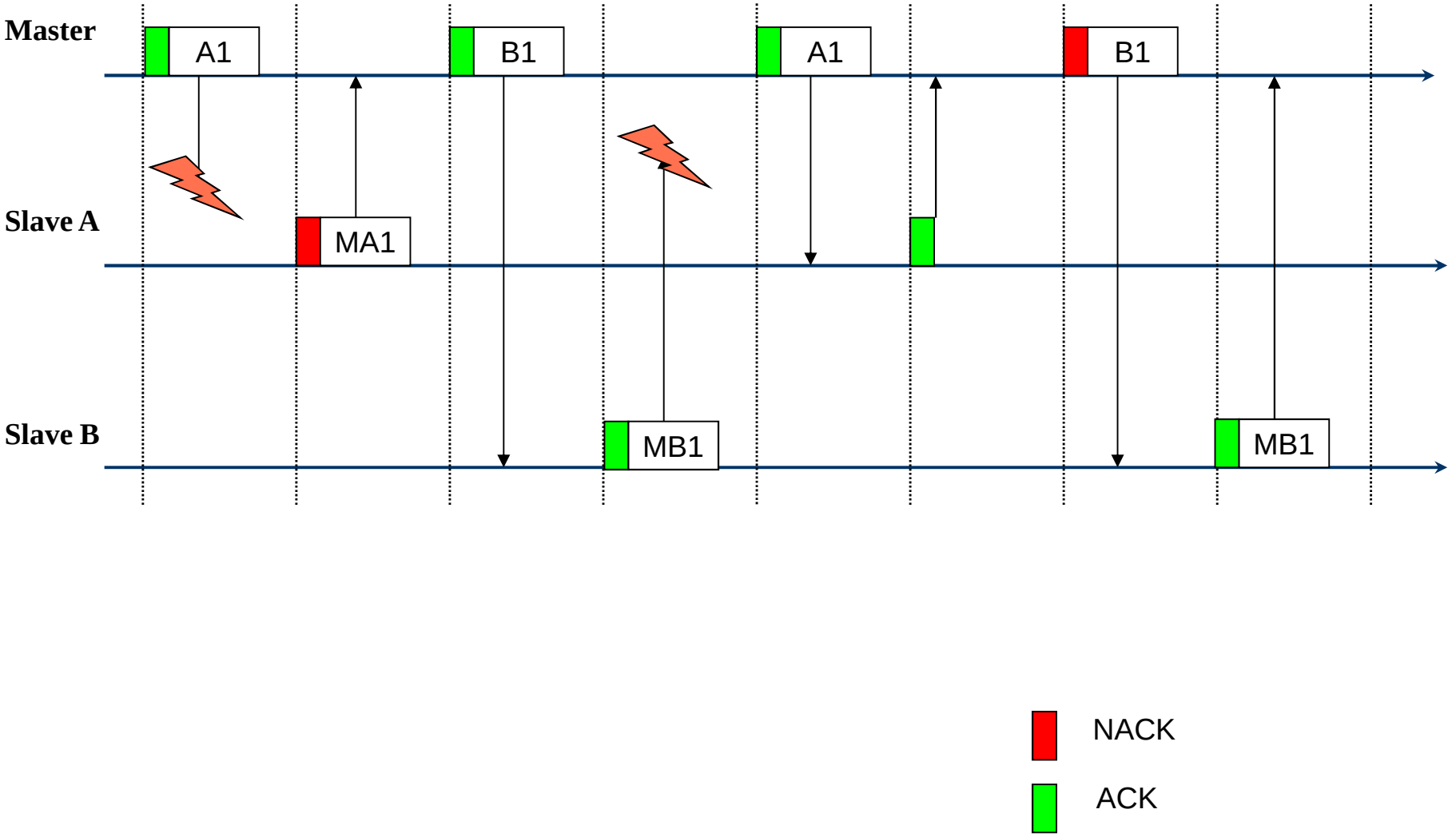


- Header:
  - Active Member Address (AMA)
  - Type: Packet type (there are 16 different types of packets)
  - Flow: Flow control
  - ARQ: Retransmission
  - SQN: Sequence number
  - HEC: checksum

Packet Format



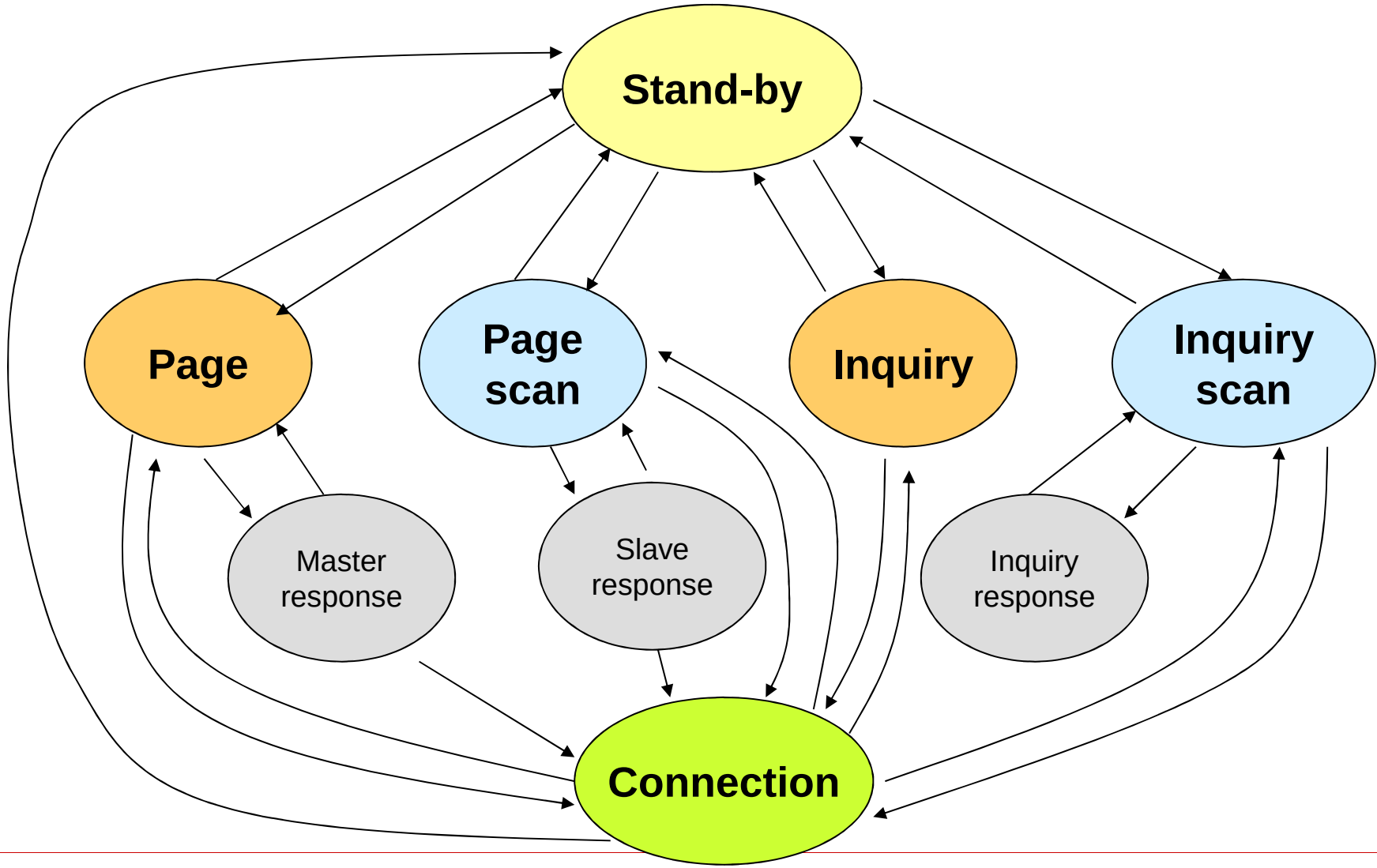
Link controller: ARQ



Link controller: states

- **Stand-by**: device is disconnetted and the radio is off
- **Connection**: device is connected with other devices
- **Inquiry**: device is searching for other devices in range
- **Inquiry Scan**: device is idle, but it listens to possible inquiry messages for short intervals of time (low duty cycle)
- **Page**: device is trying to connect to a specific device
- **Page Scan**: Similar to inquiry scan but for page messages

Link controller: states



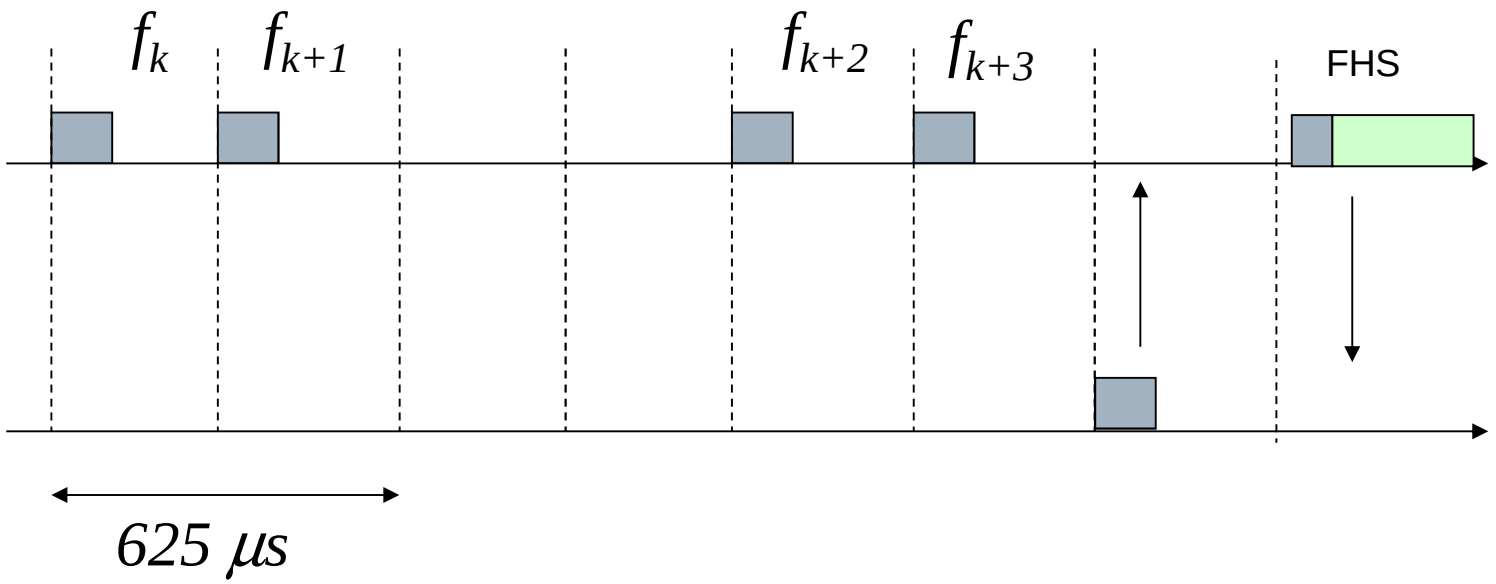
Page procedure

- If a device wants to connect to another device, it needs to know its address and then start the *page* procedure
- From the address, the Device Access Code (DAC) can be derived
- A stand-by device enters periodically in the page scan state and listens to receive its DAC
- Due to ISM band rules, page procedure cannot be performed on a fixed channel
- The device in page scan follows a pseudo random sequence tuning on 32 channels

Page procedure

- In order to limit the *energy consumption*, the device performs the page scan for **10 ms** on a channel and then goes to sleep for a **few seconds** (from 1.28 to 3.85 s)
- At every scan, a different channel is used according to the scanning pseudo-random sequence
- The paging device can calculate the sequence, but usually it doesn’t know the clock (phase)
- So it transmits the DAC on all possible frequencies sequentially

Page procedure



- In 10 ms, the paging device can transmit the DAC on 16 out of 32 channels
- The transmission sequence is repeated until a reply is received
- If after a sleep time no reply is received, the other 16 channels are considered

Page procedure

- The reply message is actually the same DAC
- The connection is established in 2 sleep times in the worst case
- The paging device replies with a FHS packet including all information on the device, including address and clock
- Connection is established
- The paging device becomes the Master, and the scanning device becomes the Slave

Page procedure

- What about energy consumption?
- Why the paging device continues to transmit the DAC, spending a lot of energy, while the scanning device just listen to channels every once and a while?
- Would a more fair approach be preferable?

Inquiry procedure

- The inquiry procedure allows to discover all the other active devices in range
- It is similar to the page procedure, but the Inquiry Access Code (IAC) is adopted instead of the DAC
- Also the inquiry scan sequence is pseudo random
- The reply is a FHS packet
- Collisions may occur due to multiple devices in range
- After an inquiry, the devices switch to scan in order to setup the connection
- However, since it knows the clock of the device, the scan time can be minimized

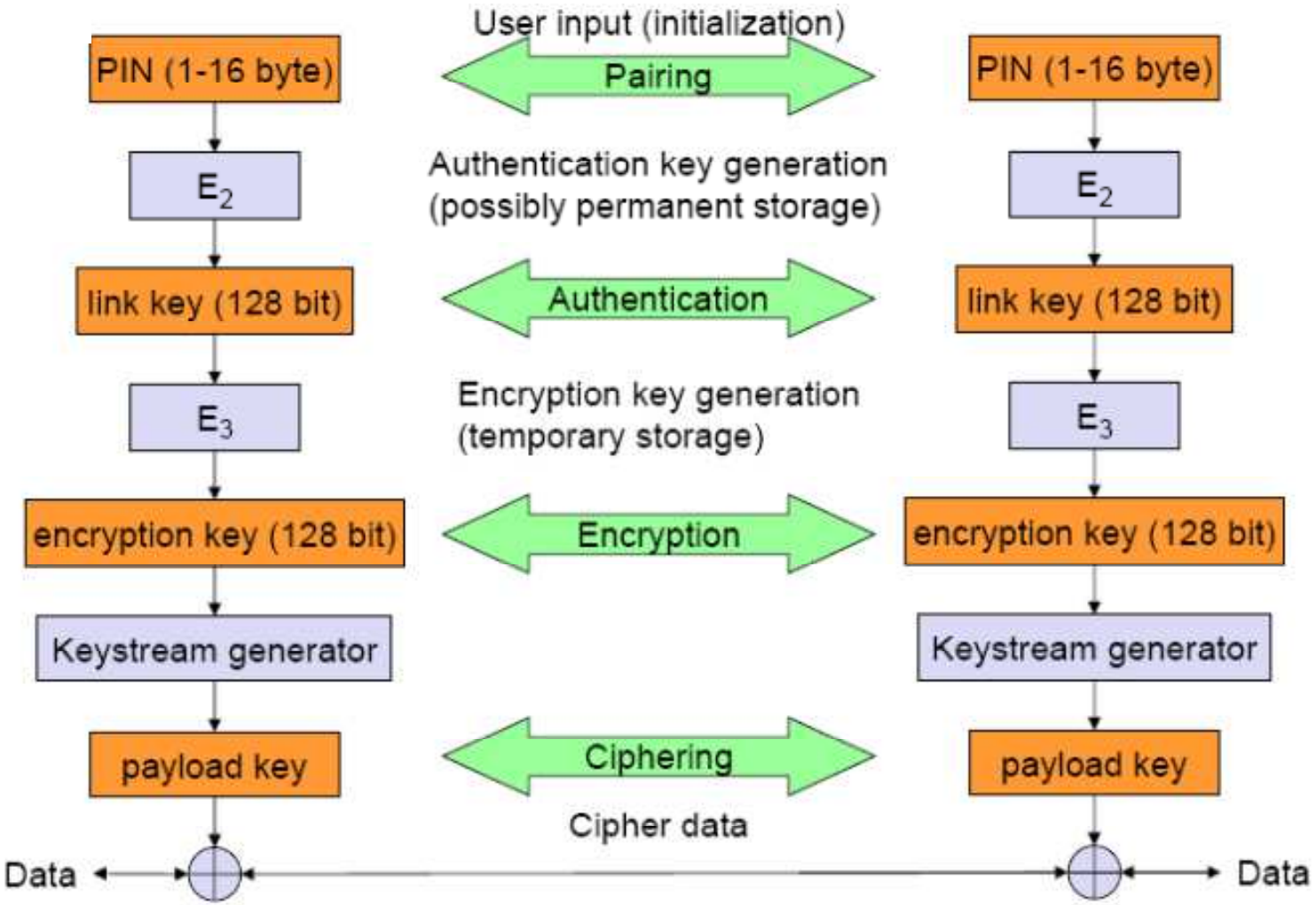
Low power modes

- When connected, the device can optionally enter *low power* modes
- **Hold**: slave stops listening to the channel for a time period agreed with the master (it keeps its AMA, Active Member Address)
- **Sniff**: slave alternates listening and sleep periods according to a cycle agreed with the master (also here it keeps its AMA)
- **Park**: in this state, the slave releases its AMA and gets a PMA (Parked Member Address) from the master. It listens to the channel with a low duty cycle for receiving *unpark* message from the master

Protocols: Link Management

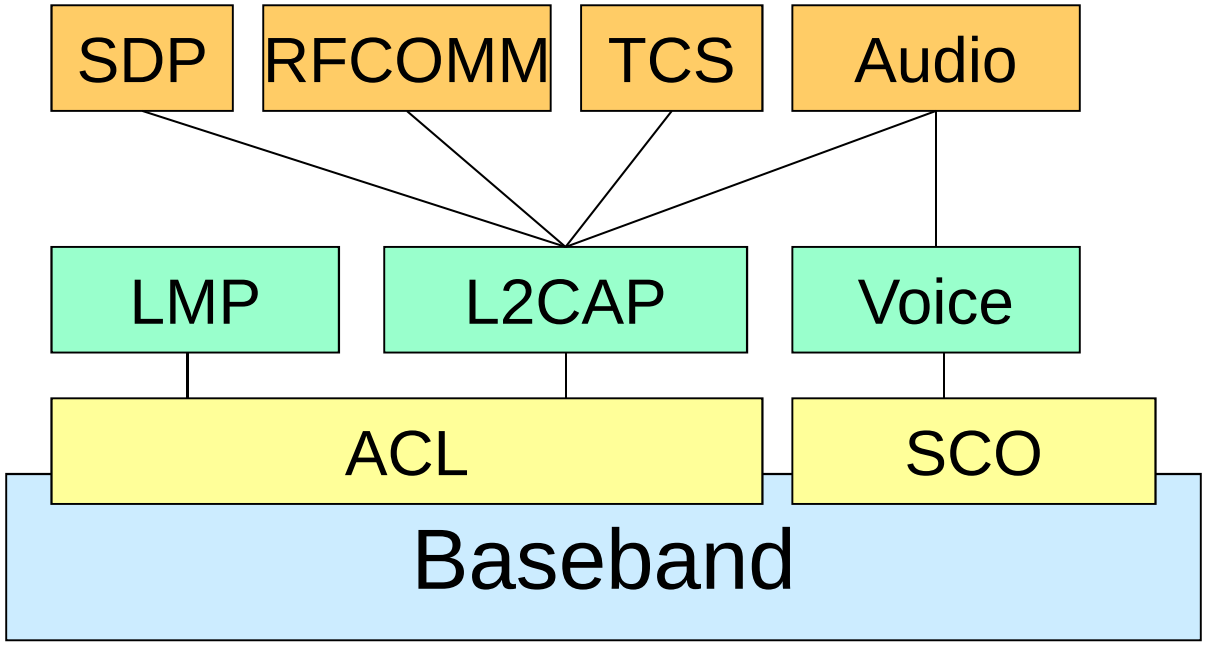
- The link management protocol is in charge of the connection setup, security and control procedures
- Setup of ACL and SCO links
- Management of security procedure
- Add and remove slaves from a piconet
- LMP messages have priority over all the others

Protocols: Security



Protocols: L2CAP

- Logical Link Control and Adaptation Protocol (L2CAP)
- Adaptation functions (segmentation and reassembly) and multiplexing

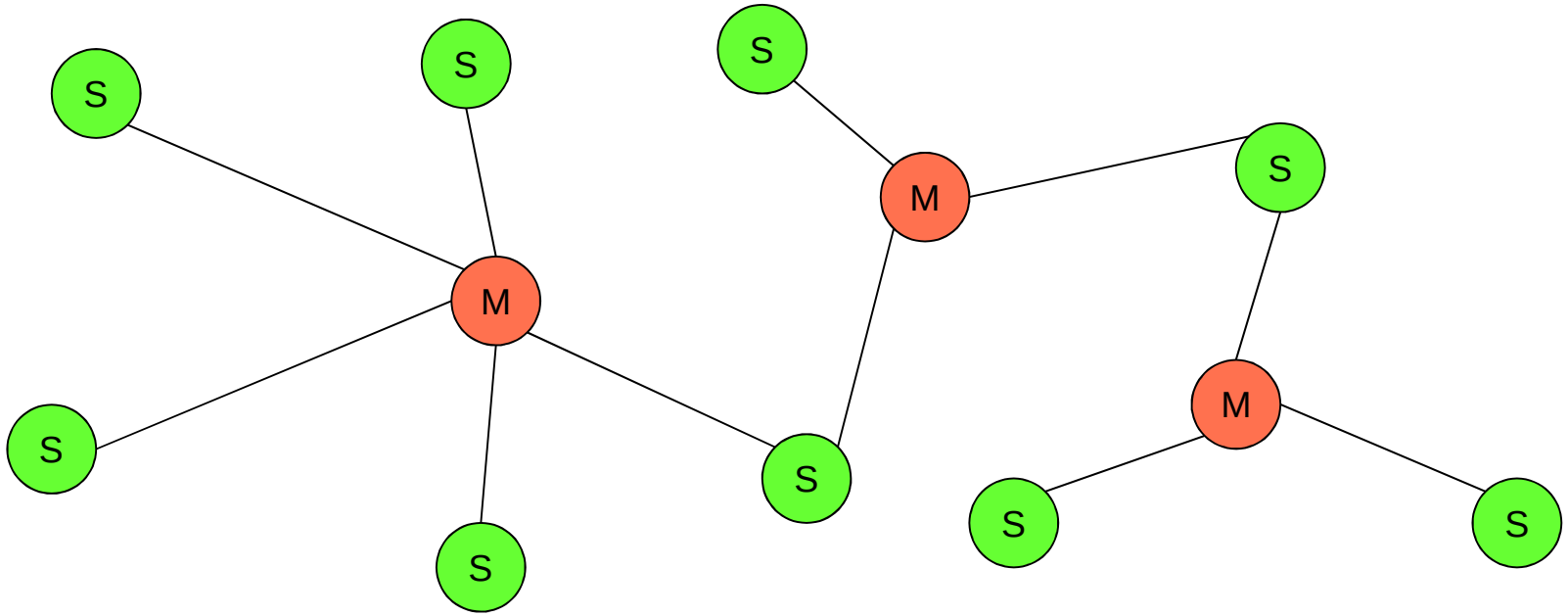


Profiles

- Profiles are sets of standard functions that allow interoperability of devices of different vendors through a standard implementation of specific applications

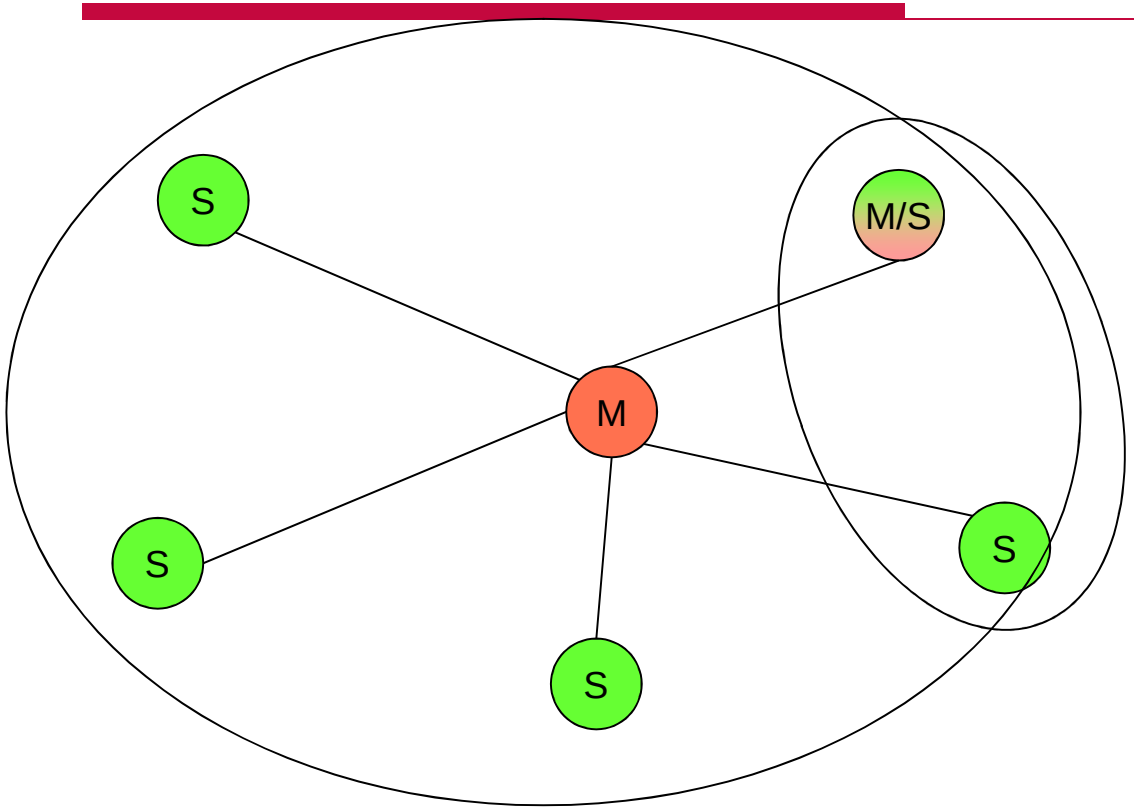
- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile
- Advanced Audio Distribution
- PAN
- Audio Video Remote Control
- Basic Printing
- Basic Imaging
- Extended Service Discovery
- Generic Audio Video Distribution
- Hands Free
- Hardcopy Cable Replacement

Scatternet



- Devices can participate to different picones simultaneously
- A device can be Master only in one piconet (Why?)
- Devices can switch from one piconet to another using the *hold* and *sniff* modes
- Scatternet formation and routing are out of standard specifications

Scatternet (2)



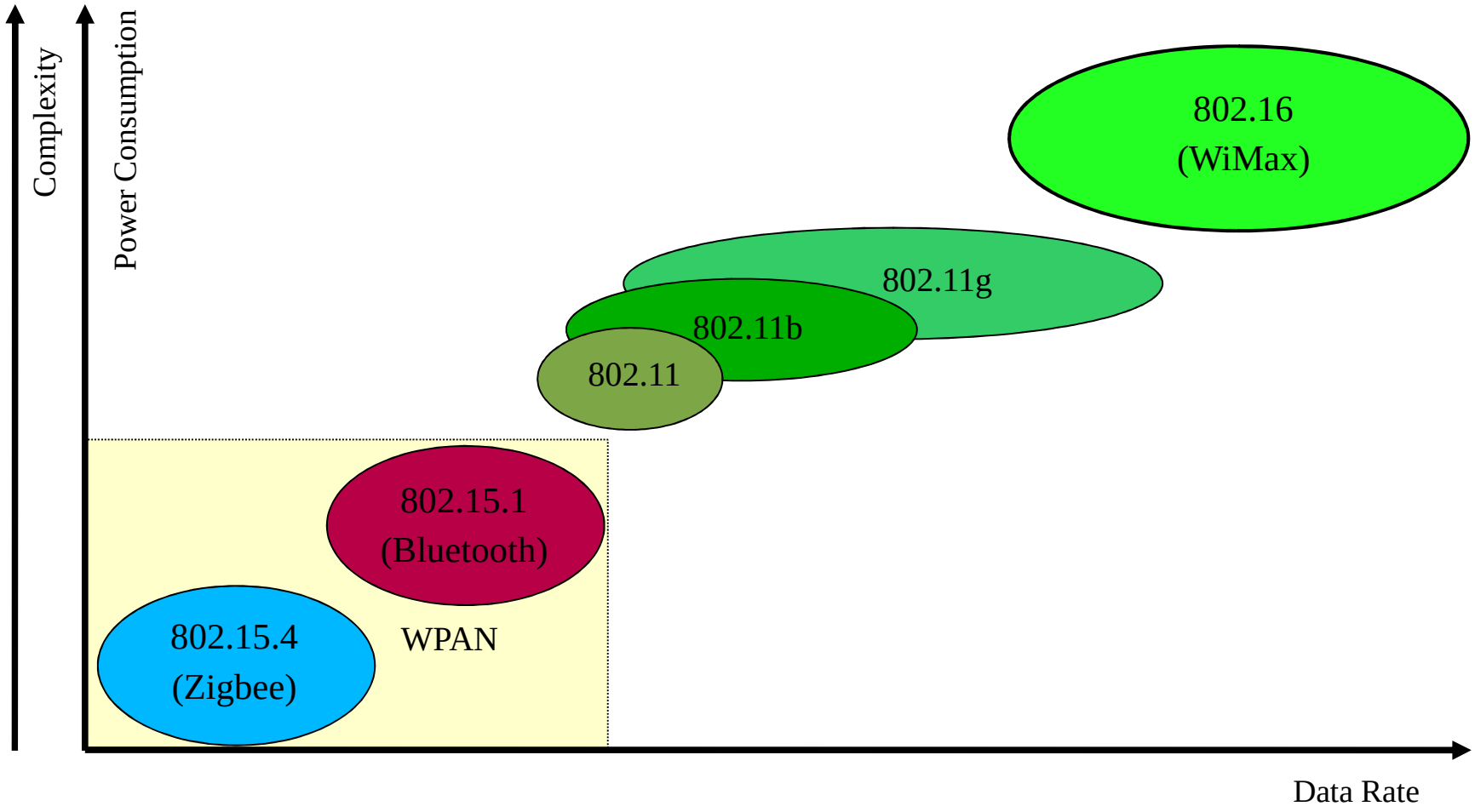
- Scatternet allows, when necessary, to create direct links

Zigbee

Low Rate - WPAN

- Most applications in Wireless Networking require high transmission rates
- Starting in the 90's, a lot of efforts have been devoted to these application and to high rate wireless technologies: WLAN (IEEE 802.11), BlueTooth (IEEE 802.15), WiMax (IEEE 802.16)
- However, there are also several applications that require short range, low energy consumption and low rate
- Low Rate WPAN (LR-WPAN) have been considered for this specific application segment

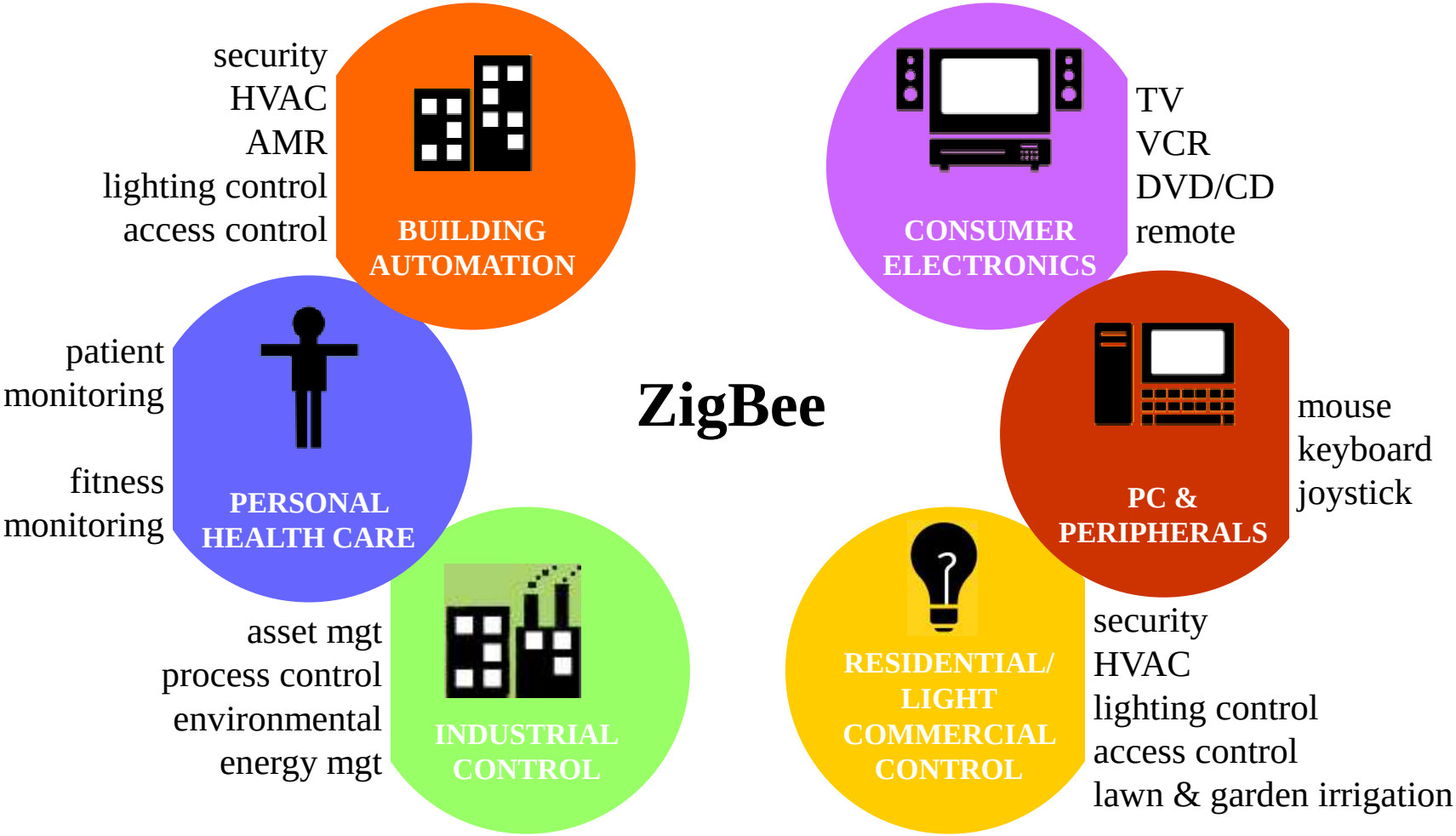
Low Rate - WPAN



Characteristics

- Low cost of the hardware (< 1$) and the software
- Low transmission range (~10-30m)
- Low latency, if necessary
- And, above all, low energy consumption!

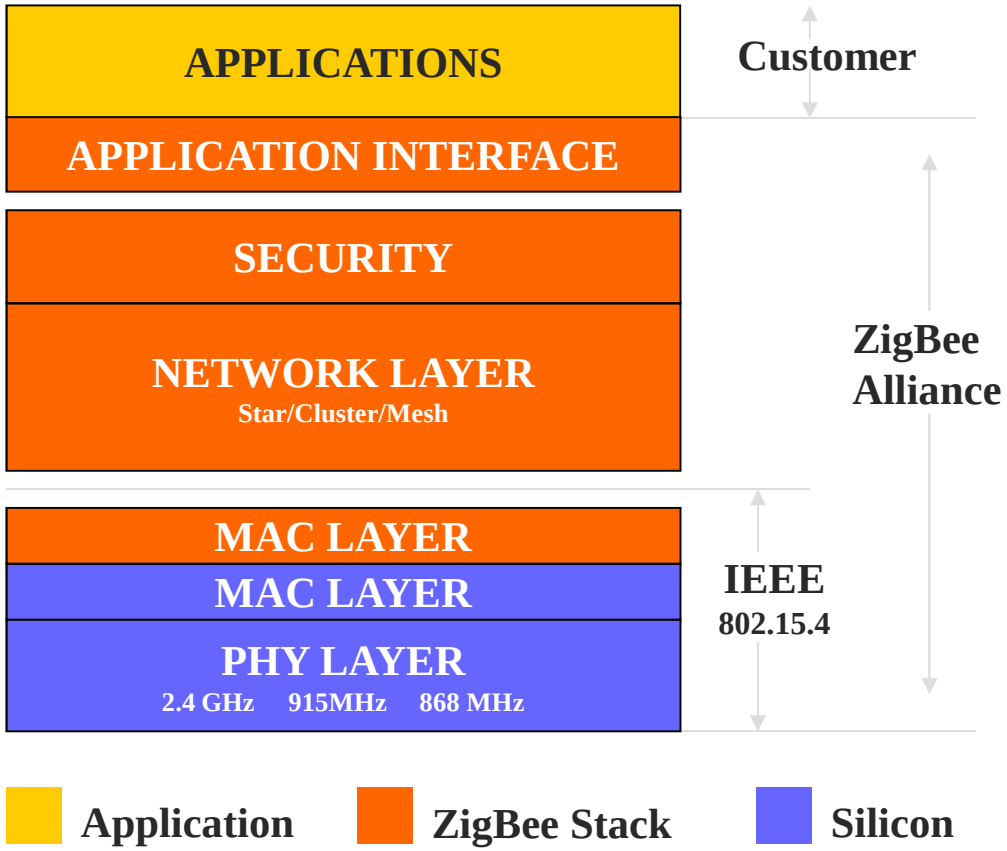
Applications



Toward Zigbee …

- Starting in mid 90s, several manufacturers designed proprietary solutions for *sensor networks* …
- … with obvious compatibility and high cost problems
- A standardization activity was necessary: the Working Group 4 is created within the IEEE 802.15 project (2001)
- IEEE 802.15.4 standard, considering physical and MAC layers, is published in May 2003
- The technology takes the commercial name of

Zigbee: protocol stack



Zigbee: protocol stack

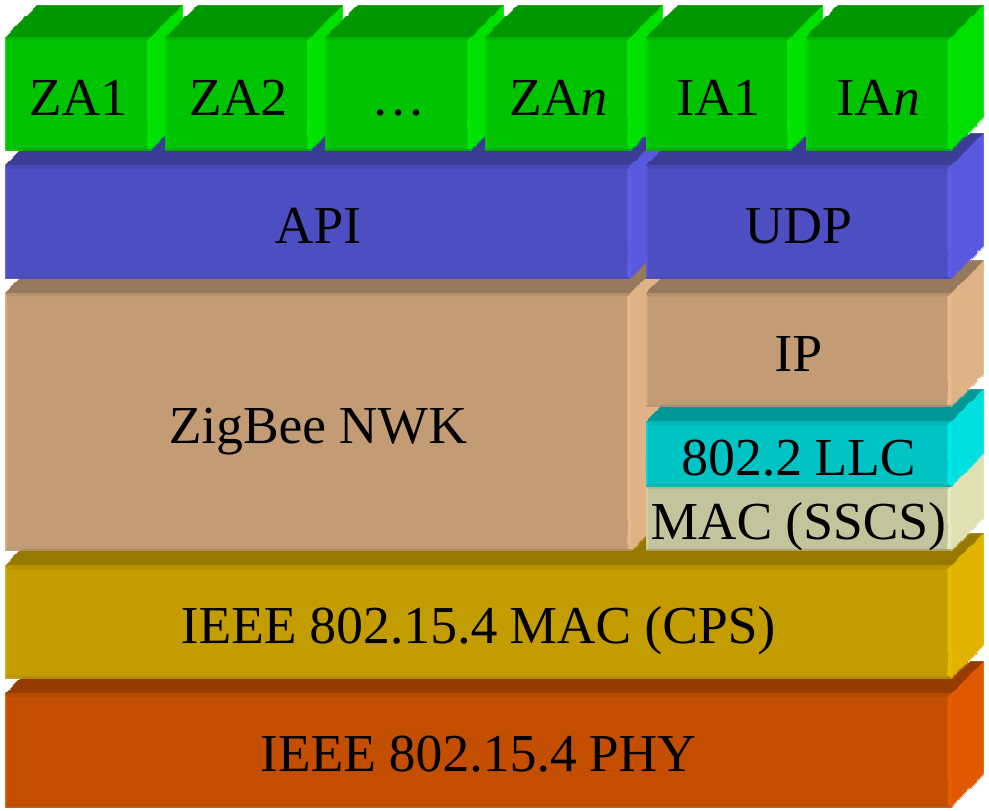
End developer applications, designed using application profiles

Application interface designed using general profile

Topology management, MAC management, routing, discovery protocol, security management

Channel access, PAN maintenance, reliable data transport

Transmission & reception on the physical radio channel



Zigbee: channels and rates

BAND	COVERAGE	DATA RATE	# OF CHANNEL(S)
2.4 GHz	ISM	Worldwide	250 kbps	16
868 MHz		Europe	20 kbps	1
915 MHz	ISM	Americas	40 kbps	10

ZigBee vs. Bluetooth

ZigBee

- DSSS- 11 chips/ symbol
- 62.5 K symbols/s
- 4 Bits/ symbol
- Peak Information Rate ~128 Kbit/second

Bluetooth

- FHSS
- 1 M Symbol / second
- Peak Information Rate ~720 Kbit / second

ZigBee vs. Bluetooth

ZigBee:

- Network join time = 30ms typically
- Sleeping slave changing to active = 15ms typically
- Active slave channel access time = 15ms typically

Bluetooth:

- Network join time = >3s
- Sleeping slave changing to active = 3s typically
- Active slave channel access time = 2ms typically

ZigBee vs. Bluetooth

	Bluetooth	ZigBee
AIR INTERFACE	FHSS	DSSS
PROTOCOL STACK	250 kb	28 kb
BATTERY	rechargeable	non-rechargeable
DEVICES/NETWORK	8	255
LINK RATE	1 Mbps	250 kbps
RANGE	~10 meters (w/o pa)	~30 meters

Zigbee: devices

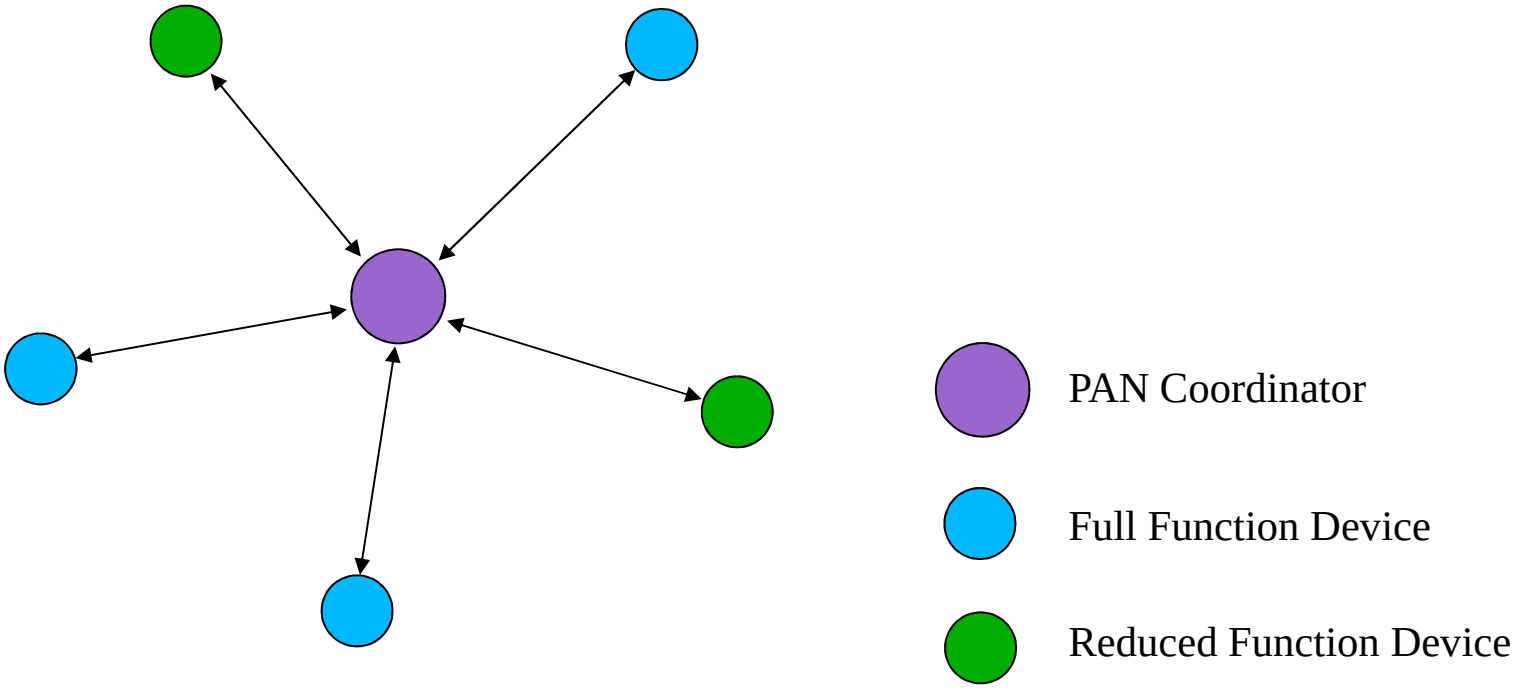
Standard defines tow device types:

- **Full Function Device (FFD):**
  - Can transmit beacon frames
  - Can directly communicate with other FFD
  - Can make routing
  - Can act as PAN coordinator
- **Reduced Function Device (RFD):**
  - Cannot route traffic
  - Cannot communicate directly with other RFD
  - Can only communicate directly with one FFD

Zigbee: topologies

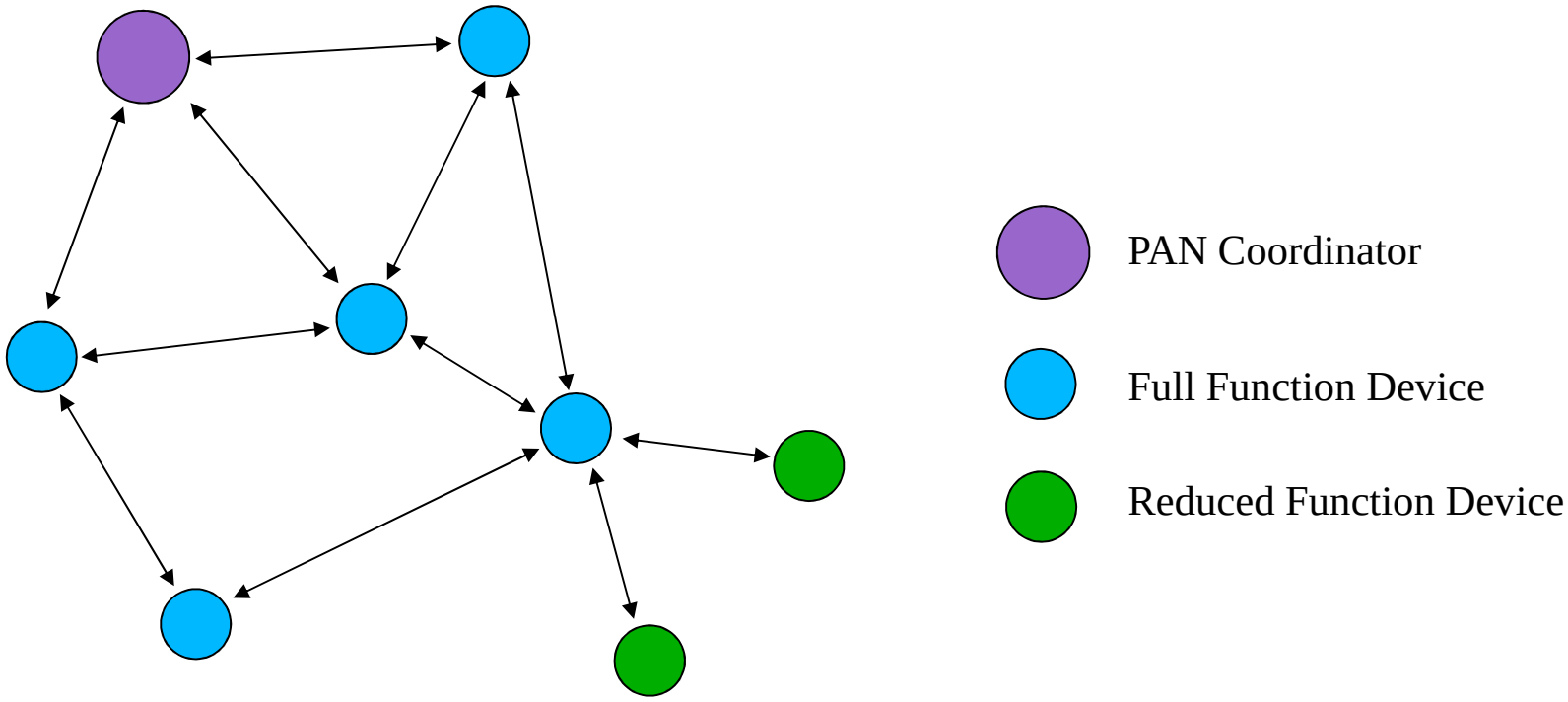
Three topologies are defined:

1 - STAR TOPOLOGY



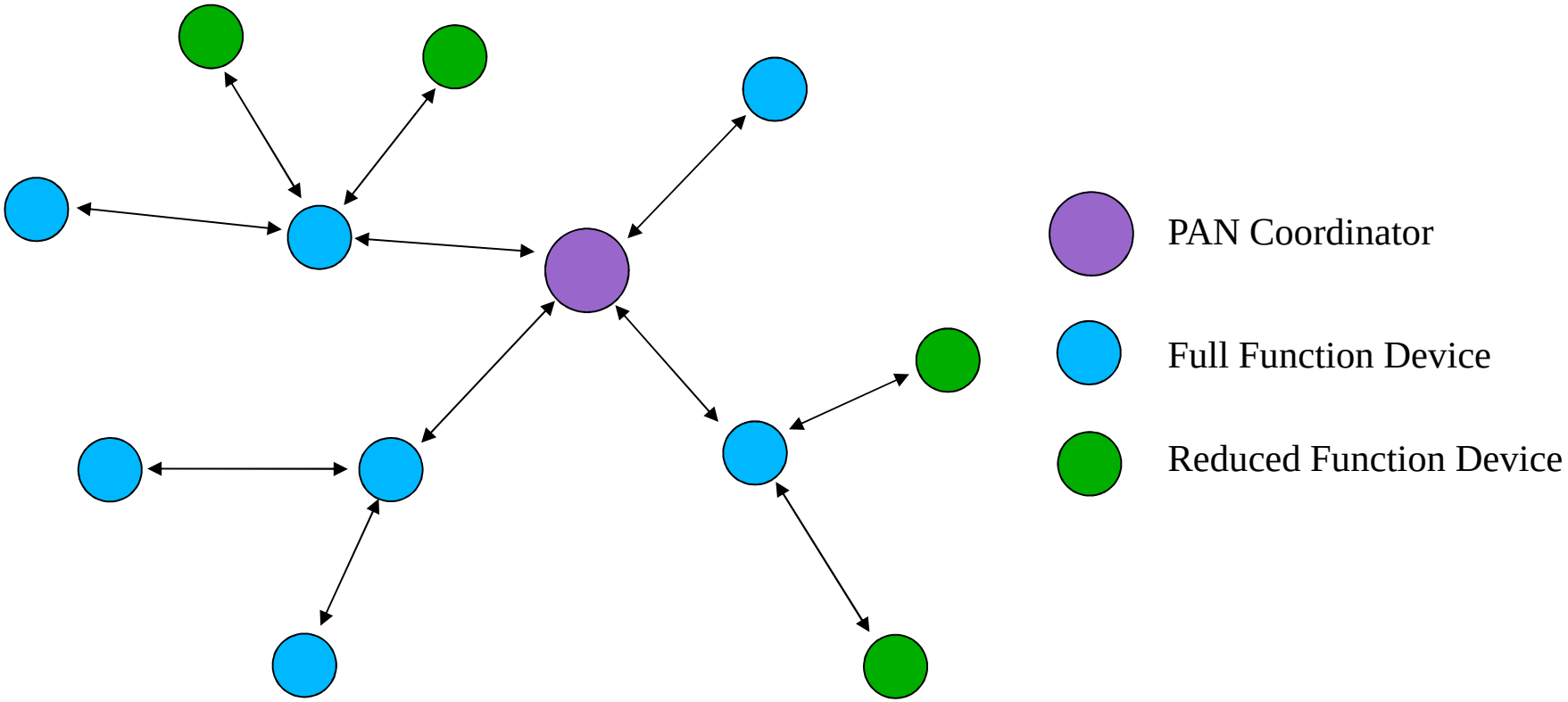
Zigbee: topologies

2 - MESH TOPOLOGY



Zigbee: topologies

3 - CLUSTER TREE



Physical layer

Direct Sequence Spread Spectrum (DSSS)

Frequency	Zone	Modulation	Bit-Rate	Channels
868 Mhz	Europa	BPSK	20 kbit/s	1
915 Mhz	USA	BPSK	40 kbit/s	10
2.45 Ghz	Everywhere	O-QPSK	250 kbit/s	16

Physical layer

- Receiver Energy Detection (Free channels search)
- Scanning (Search for Beacon frames)
- Channel selection
- Clear Channel Assessment (channel busy/available)
- Link Quality Detection (LQI: estimation of channel quality)
- Quality feedbacks to upper layers

Physical layer

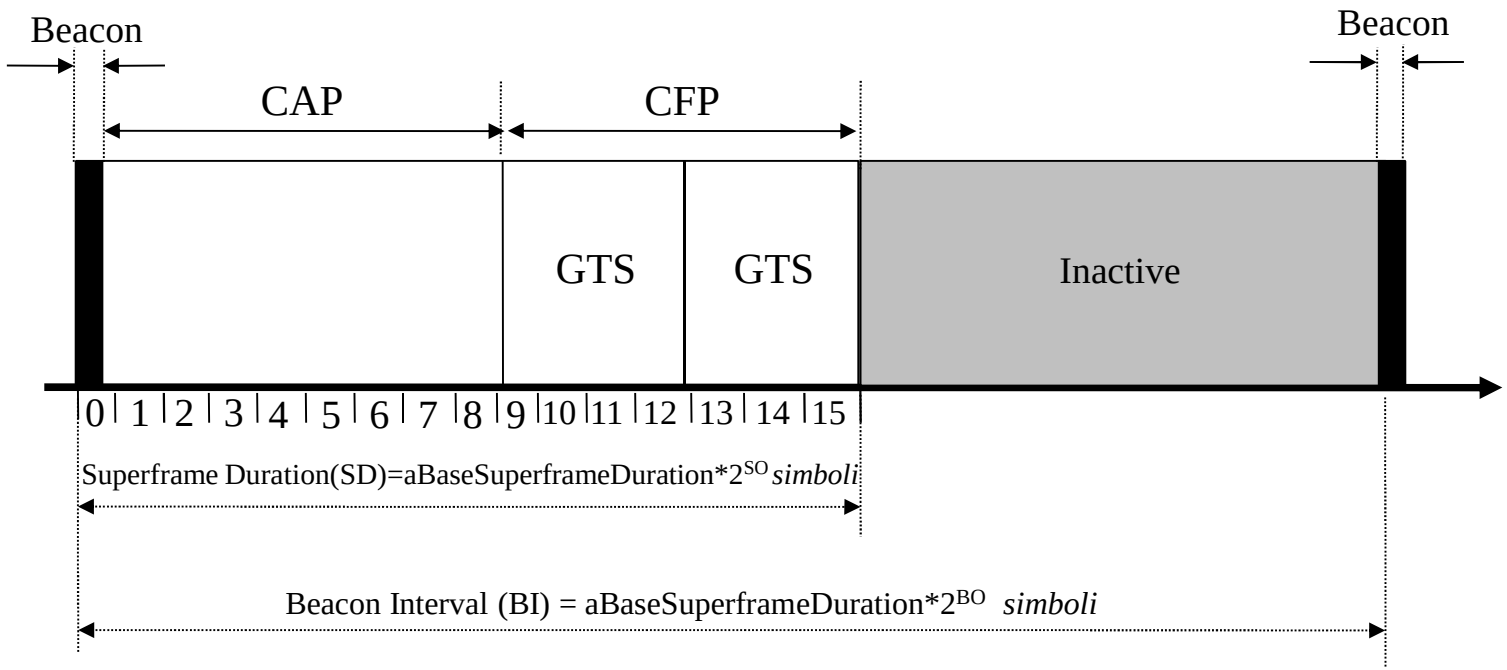
4 Byte	1 Byte	1 Byte		Variabile
PREAMBLE	START of FRAME DELIMITER (SFD)	FRAME LENGHT (7bit)	Reserved (1 bit)	PSDU
Synchronization Header (SHR)		Protocol Header (PHR)		Payload

MAC layer: overview

- Two operation modes are defined:
  - **Beacon Enabled** (slotted CSMA/CA)
  - **Non Beacon Enabled** (unslotted CSMA/CA)

MAC layer: overview

- **Beacon Enabled** (slotted CSMA/CA)



- Frame duration: from 15ms to 252sec (15.38ms*2n where $0 \leq n \leq 14$)
- Guaranteed Time Slots assigned in the beacon frame

Slotted CSMA/CA

- The time unit adopted is the backoff period (BP), usually equal to 20 symbols
- Three variables are adopted:
  - NB, number of access attempts for a packet
  - CW, number of free BPs to wait at the end of the backoff period before starting a transmission
  - BE, exponent that defines the maximum number of BPs required before starting the CCA (Clear Channel Assessment) procedure
- Data transmission (and optionally the ack) must end within the CAP
- In case this is not possible, MAC has to suspend the random backoff and wait for the beginning of next CAP
- If the macBattLifeExt bit is set to 1, countdown of the backoff can be executed onliy during the first 6 BPs following the beacon

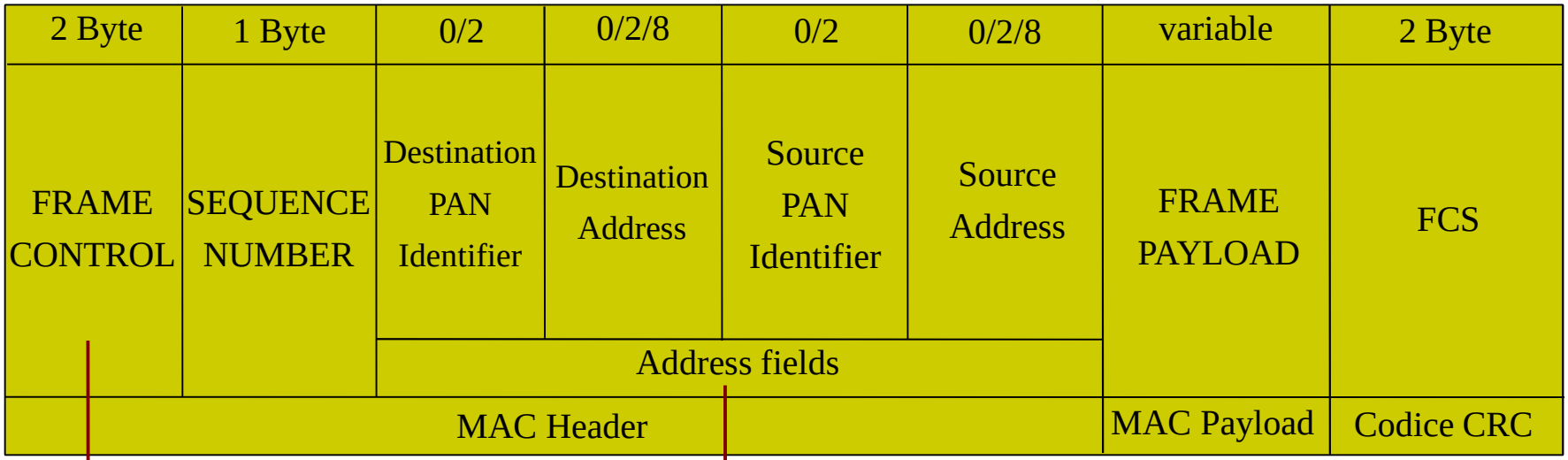
Unslotted CSMA/CA

- Classical access scheme CSMA/CA (data - ACK) without synchronization

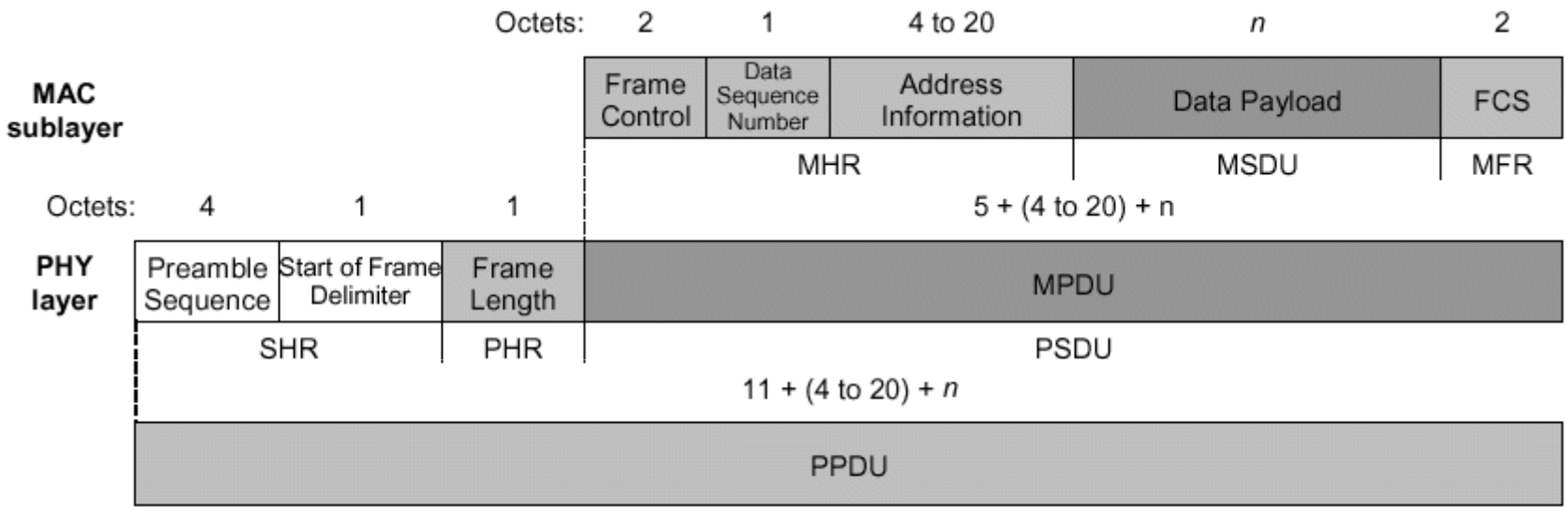
MAC layer: functionalities

- Beacon Management (Synchronization)
- Channel access management
- Guaranteed Time Slot (GTS) Management
- Association and disassociation
- Frame Acknowledgement

MAC layer: frame format

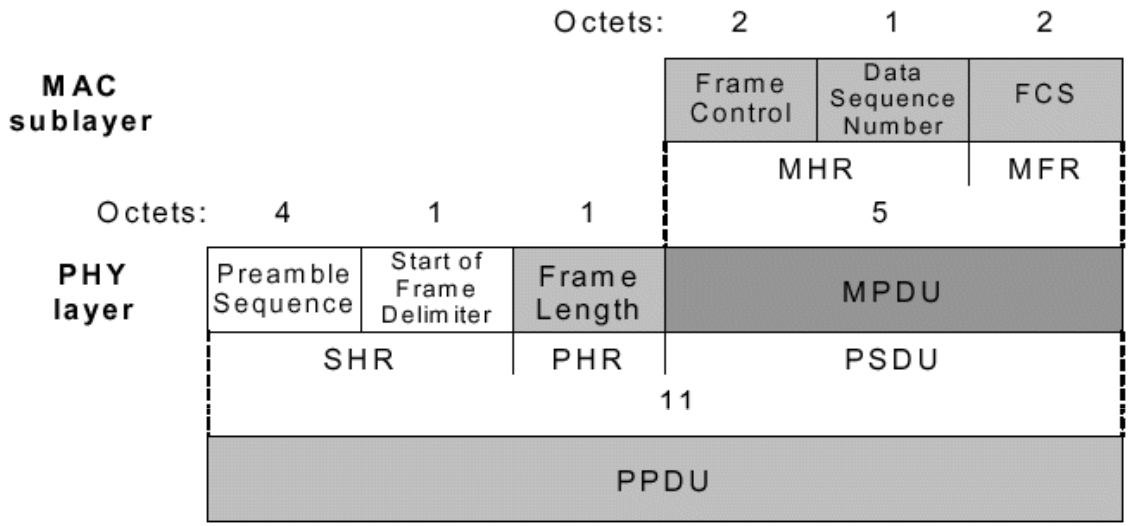


Data Frame



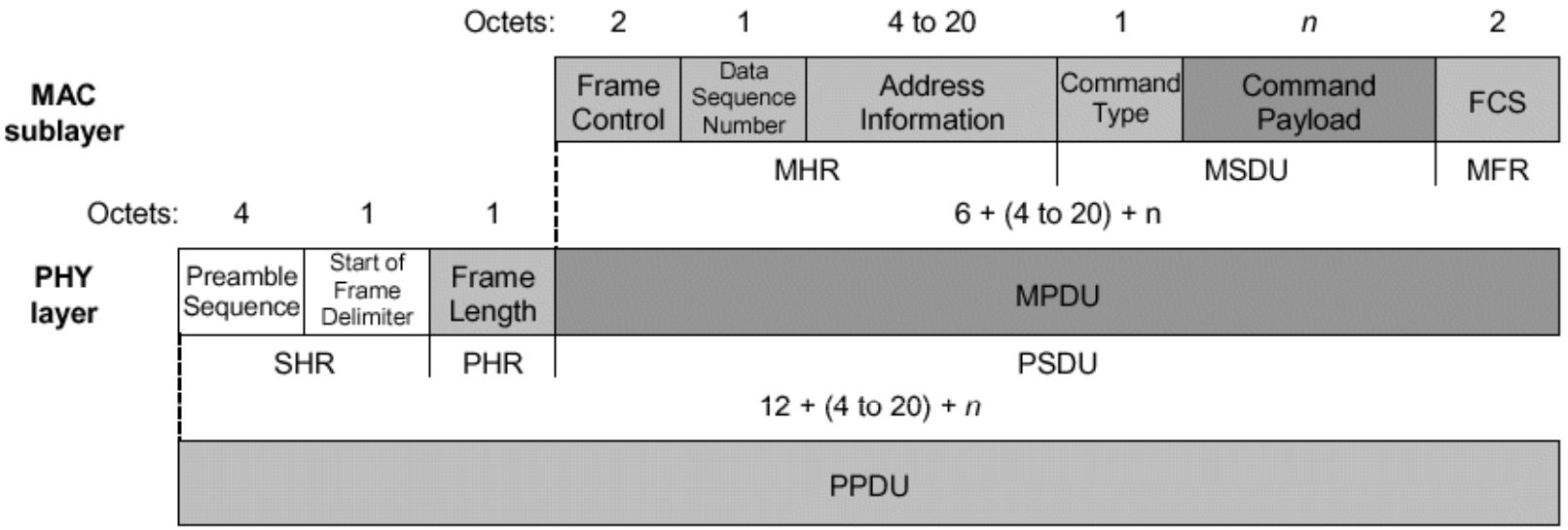
- Up to 104 bytes payload

Ack Frame



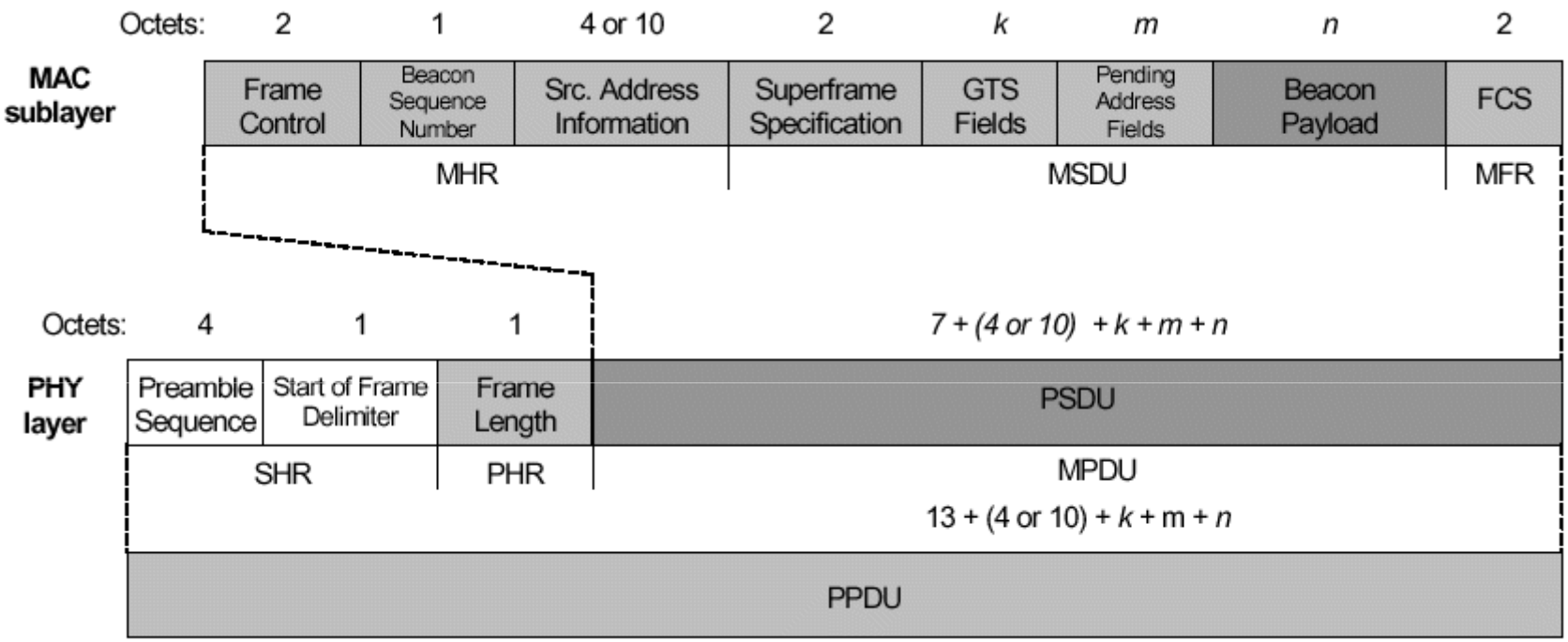
- Transmitted right after data frame

Command Frame



- It allows the remote configuration and control of client devices
- It basically allows the implementation of a centralized network management and control for large size networks

Beacon Frame format

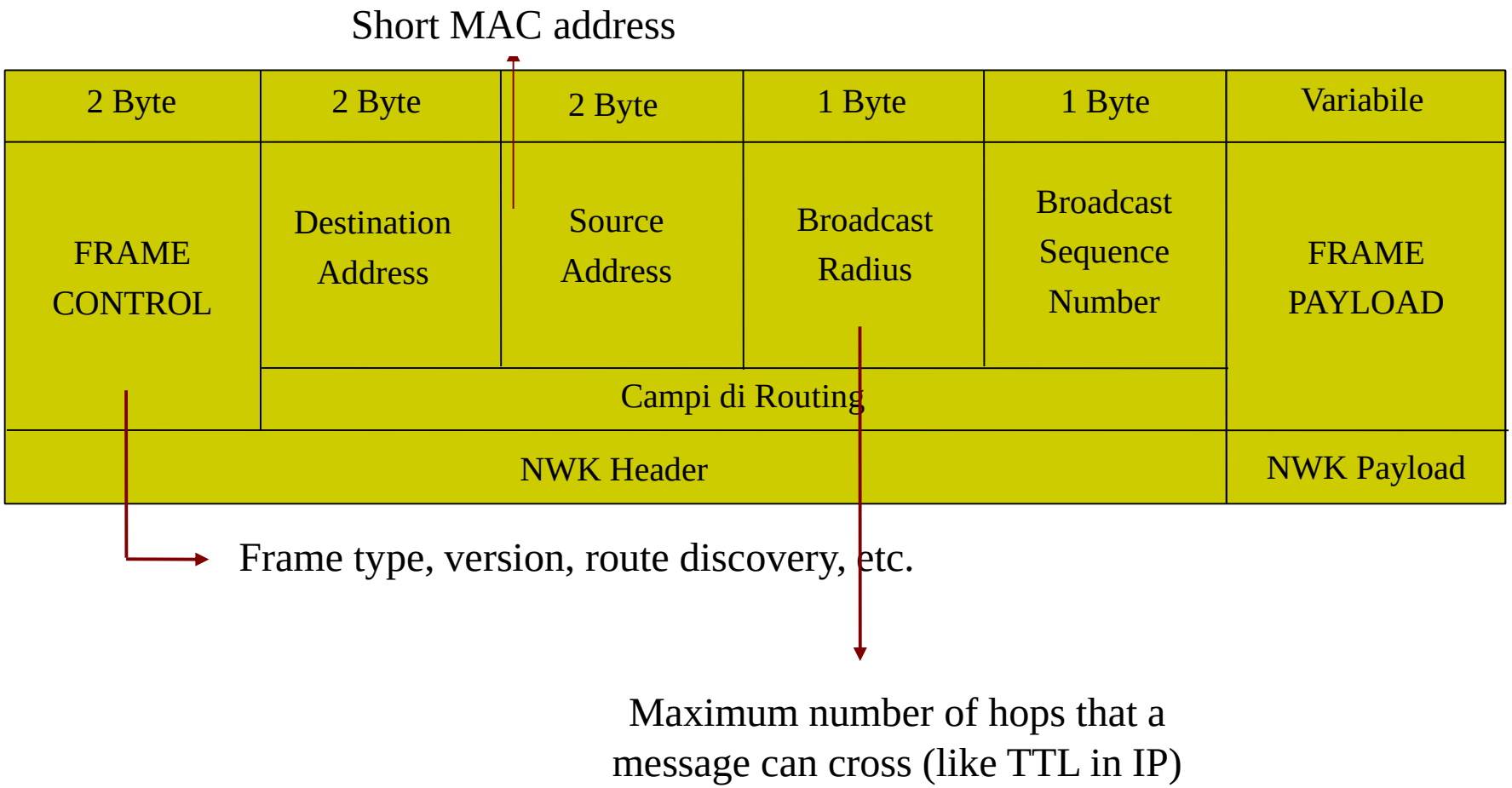


- Frame synchronization and GTS assignment

Network formation

- An FFD device search for a free channel and select a PANid *(Channel Scanning)*. Then it starts transmitting Beacon frames
- A device that want to associate to a network scans channel and listen to Beacon frames
- Once scan is completed, a network is selected setting the access parameters according to the information in the beacon frame
- Association is performed issuing an Associate Request Command to PAN Coordinator
- PAN Coordinator replies with a Association Response Command

Network layer: frame format



Zigbee Routing: overview

- Defined by Zigbee Specification, published by the Zigbee Alliance (7/2005)
- Three types of devices:
  - *ZB Coordinator (FFD)*
  - *ZB Router (FFD)*
  - *ZB End-Device (RFD o FFD)*
- Routing is "zigbee oriented" and considers the two types of physical device (FFD RFD)
- Routing used two algorithms:
  - *Ad-hoc On-demand Distance Vector (AODV)*
  - *Cluster Tree Algorithm*

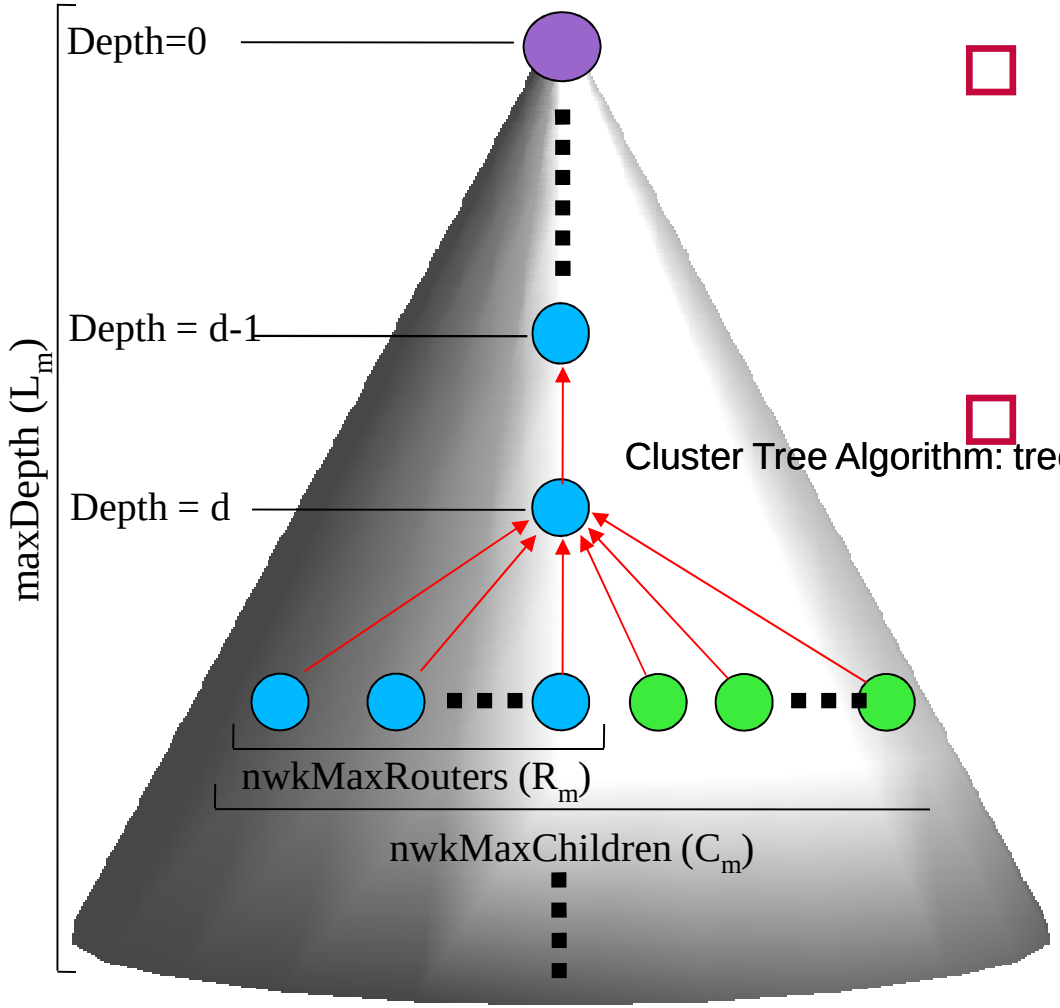
Ad-hoc On-demand Distance Vector

- Simple on-demand routing protocol
- See part on ad hoc networks (…)

Cluster Tree Algorithm: tree creation

- Procedure is started from a FFD that acts as network coordinator
- Network coordinator selects one of the available channels (MAC function)
- It selects a PAN*identifier* to the network and assign to itself the *Network Address* "0" (Coordinator)
- The other devices can now join the network associating with the *Network Coordinator*. They can act as *ZB Router* (FFD) or *ZB End-Device*
- Once connected, *ZB Routers* can then allow other devices to join the network
- Address assignment is completely distributed and hierarchical

Cluster Tree Algorithm: tree creation



- Hierarchical addressing simplifies routing in the tree
- Routes along the tree or along paths created with AODV can be used based on needs