Alma Mater Studiorum – University of Bologna
CdS Laurea Magistrale (MSc) in
Computer Science Engineering

Mobile Systems M course (8 ECTS)
II Term – Academic Year 2019/2020

# 01 – Overview on Wireless Communications

Paolo Bellavista
paolo.bellavista@unibo.it

Luca Foschini
luca.foschini@unibo.it

http://lia.disi.unibo.it/Courses/sm1920-info/

# A few elements of Wireless Propagation Models

Exactly to make you worried immediately from the beginning ☺, all and all always comes from Maxwell's equations…

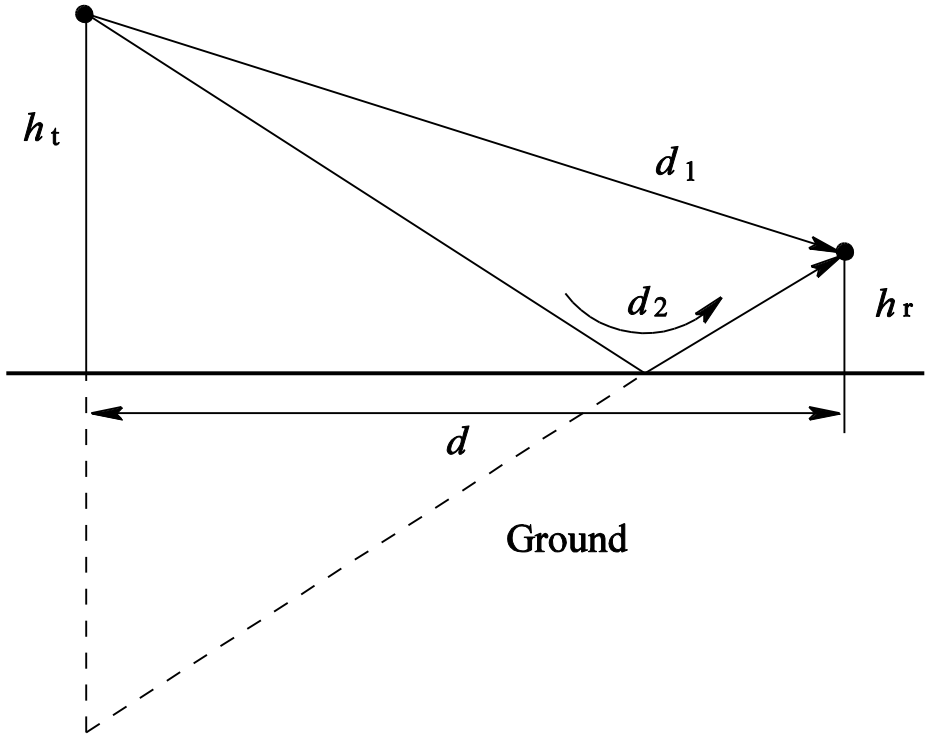
You did discuss a lot about propagation and fading models in the course «Fondamenti Telecomunicazioni T», didn't you?

- Propagation models
  - ***Free-space loss***

    $P_r(d) \sim P_t G_t G_r (\lambda/4\Pi d)^2$

  - ***Plane earth loss***

    $P_r(d) \sim P_t G_t G_r (h_t h_r/d^2)^2$

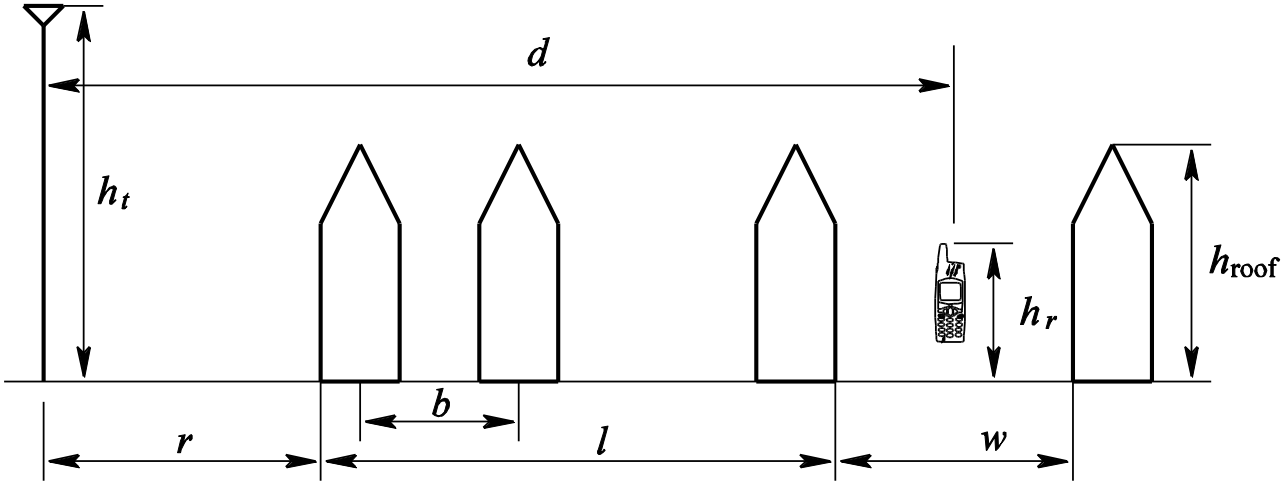


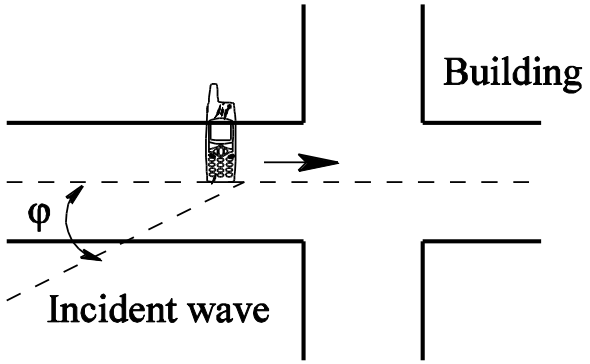
# A few elements of Wireless Propagation Models

In ***real or realistic*** scenarios, actual conditions are far more complex; this pushes, as very frequently occurs in engineering, towards ***approximated empirical models***

- ***Propagation models***
  - ***Plane earth loss***

    $P_r(d) \sim P_t G_t G_r (h_t h_r / d^2)^2$



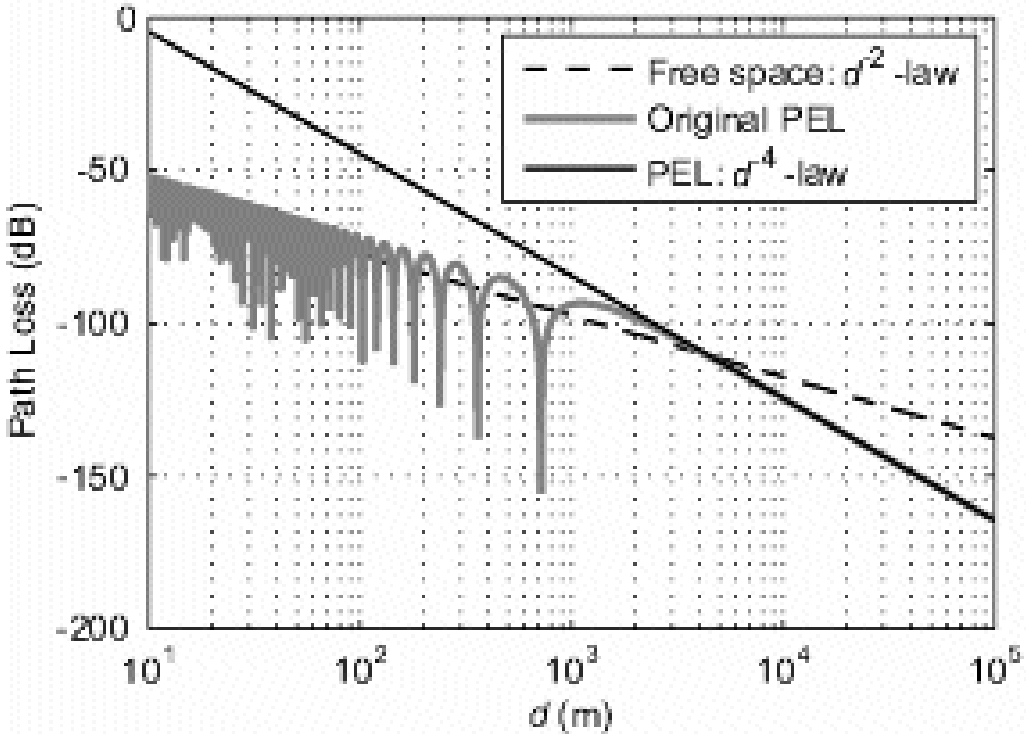
# A few elements of Wireless Propagation Models

In real or realistic scenarios, actual conditions are far more complex; this pushes, as very frequently occurs in engineering, towards ***approximated empirical models***

- ***Propagation models***
  - ***Plane earth loss***

    $P_r(d) \sim P_t G_t G_r (h_t h_r / d^2)^2$

  - ***Okumura-Hata***
  - ***COST-231-Hata***
  - ***COST-231-Walfisch-Ikegami***
  - ***…***
  - ***Indoor propagation models***
  - ***Ray-tracing-based propagation models (geometric optics and diffraction)***



# A few elements of Channel Fading Models

***Three primary types of channel fading*** in mobile communications (physically due to reflection, diffraction, and scattering):

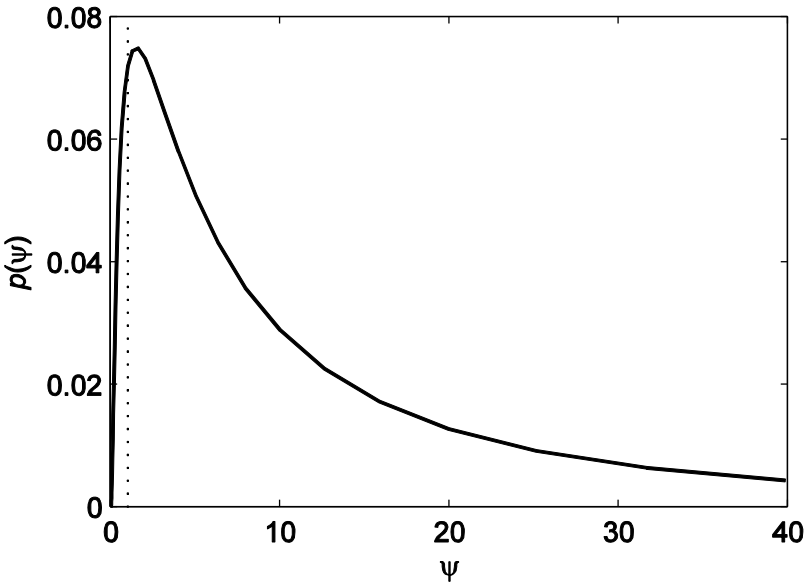
1. ***Shadowing*** (or slow-fading)
2. Multipath ***Rayleigh*** fading
3. ***Frequency-selective*** fading

***Shadowing***: ***total absorption and partial reflection*** by trees, buildings, mobile vehicles, … ➡ ***decrease of received power strength in a wide spectrum of frequencies***

probability distribution function (pdf)

$$\text{pdf} = \frac{1}{r\sigma\sqrt{2\pi}} e^{-\frac{(\ln r - m)^2}{2\sigma^2}}$$

$\Psi = P_r/P_t$



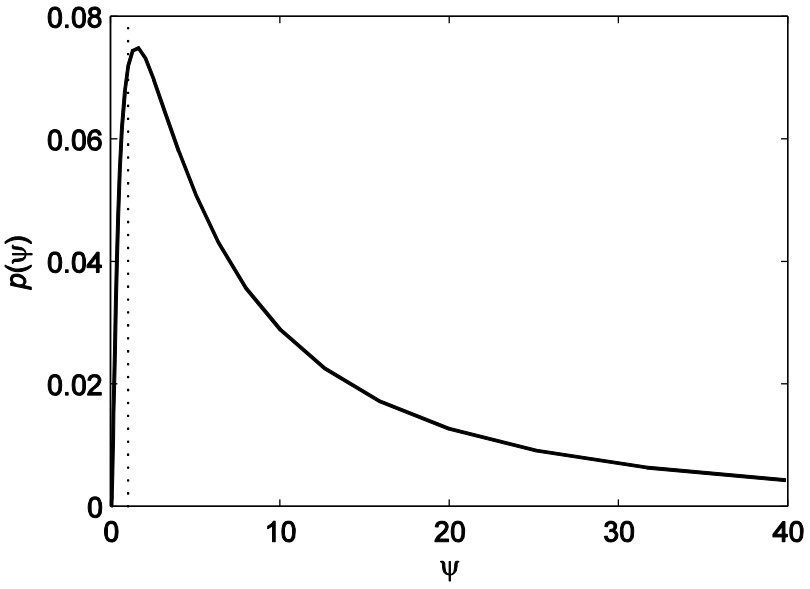
# Shadowing: Probability!

***Shadowing:***

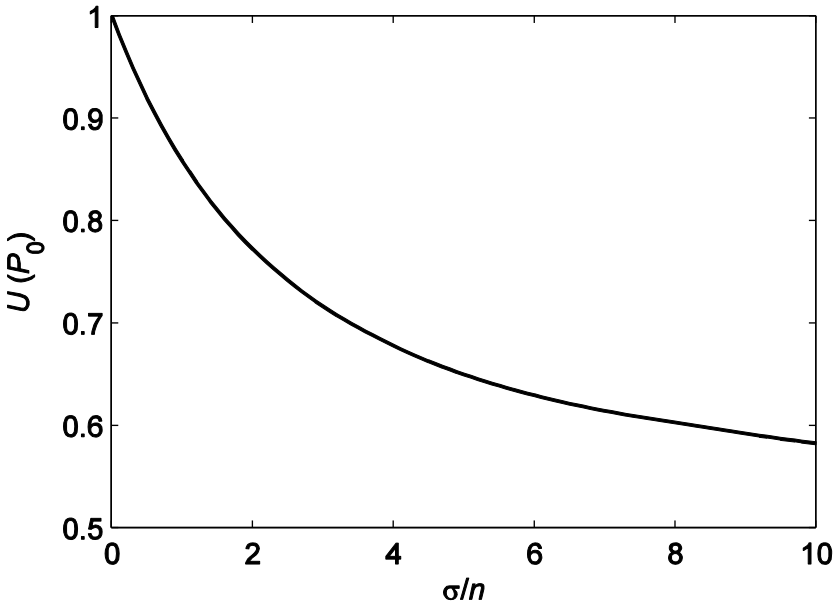
from ***pdf*** to the determination of $U(P_0)$, that is

***probability of being in the coverage area***
(percentage of the coverage area with received signal power strength greater than $P_0$)

pdf

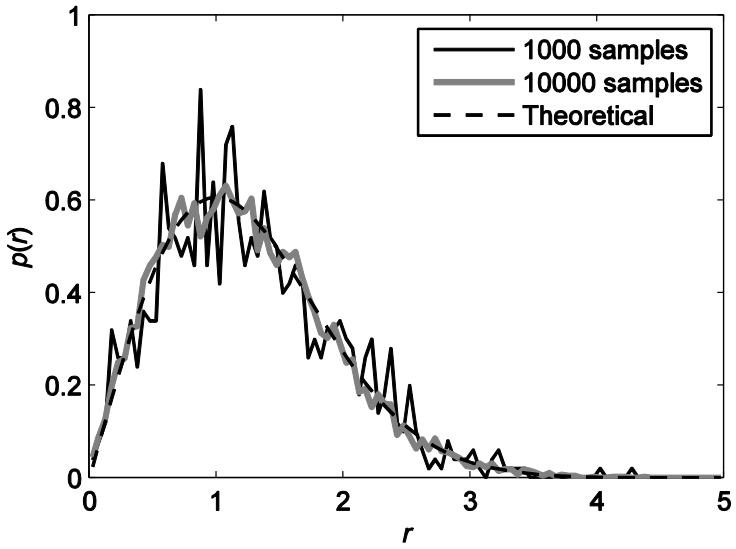


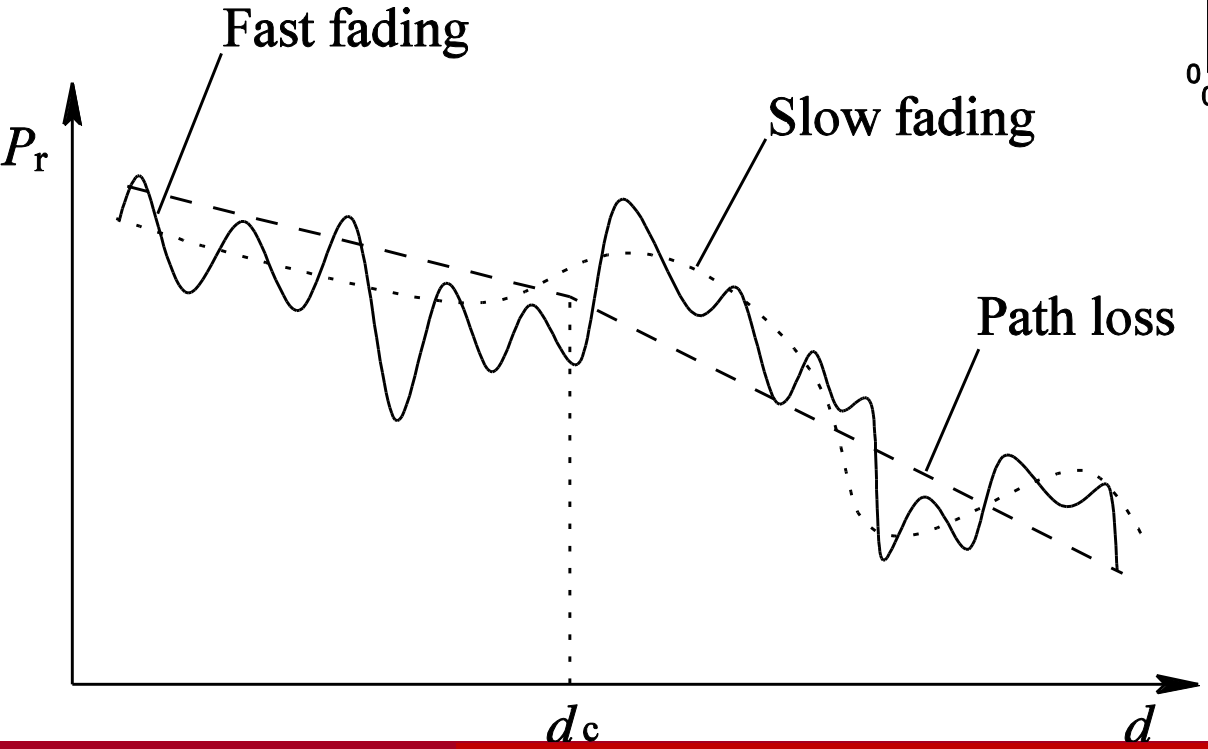

$U(P_0)$



# Rayleigh Fading and Combined Effects

Rayleigh Distribution

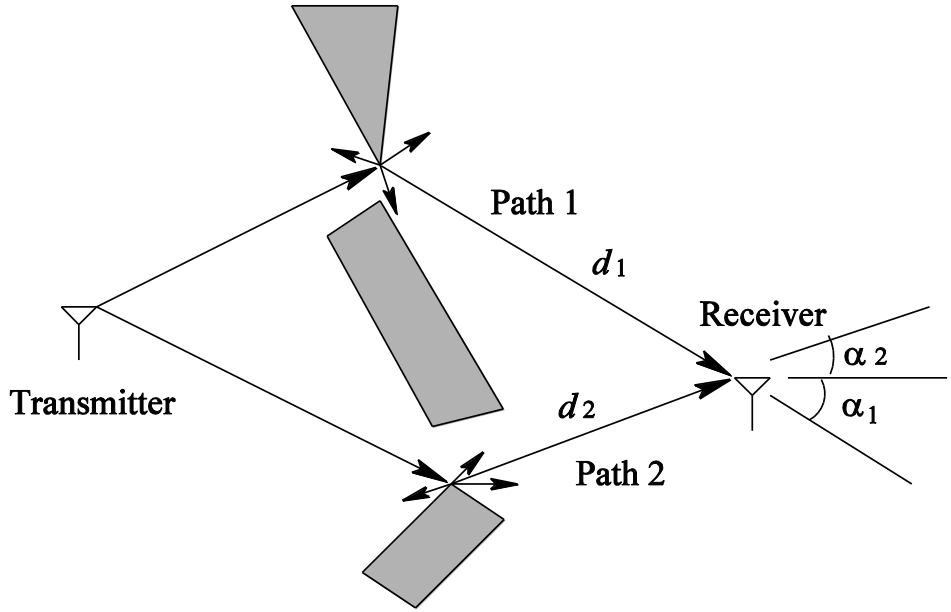



***Signal power fluctuation depending on trasmitter distance*** is motivated by Rayleigh (fast fading), shadowing (slow fading), and multipath delay spread (frequency–selective)

# Rayleigh Fading and Combined Effects

It is possible to demonstrate that Rayleigh fading can be explained as the result, for example, of a simple ***multipath model, with 2 paths***

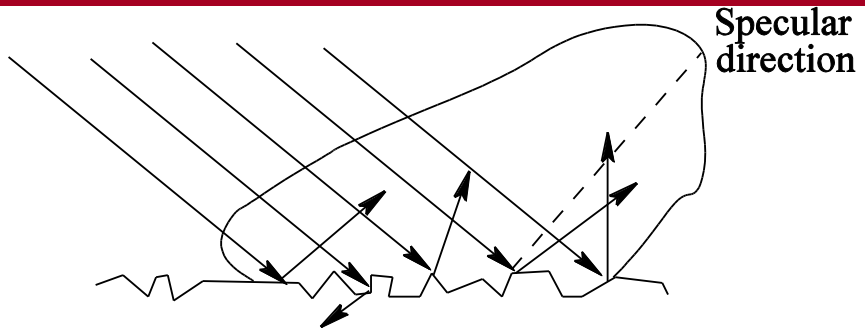



In addition, ***Doppler effect*** and frequency shift (time-selective fading)

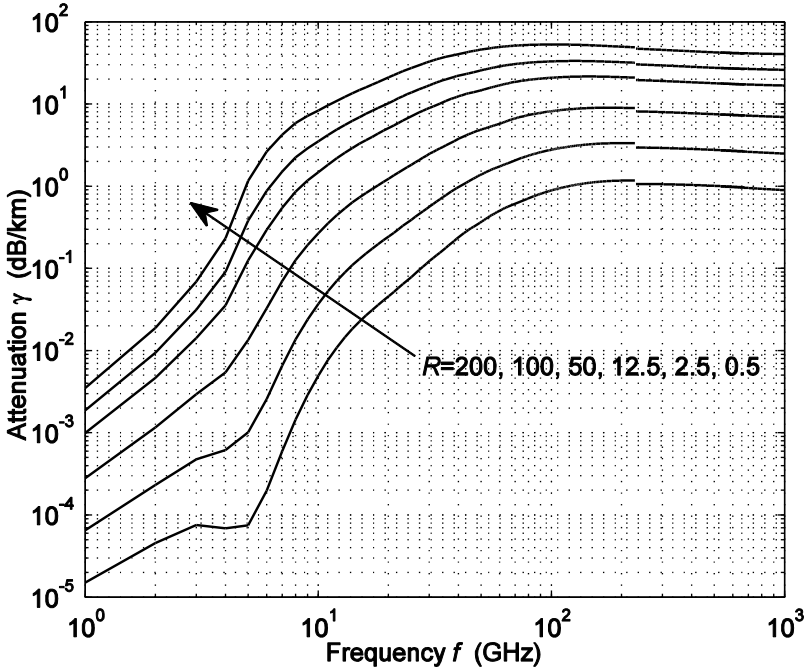
But also Ricean fading, Nagakami fading, Suzuki fading, …

# Additional Effects: Scattering, Athmosperic Absorption, …

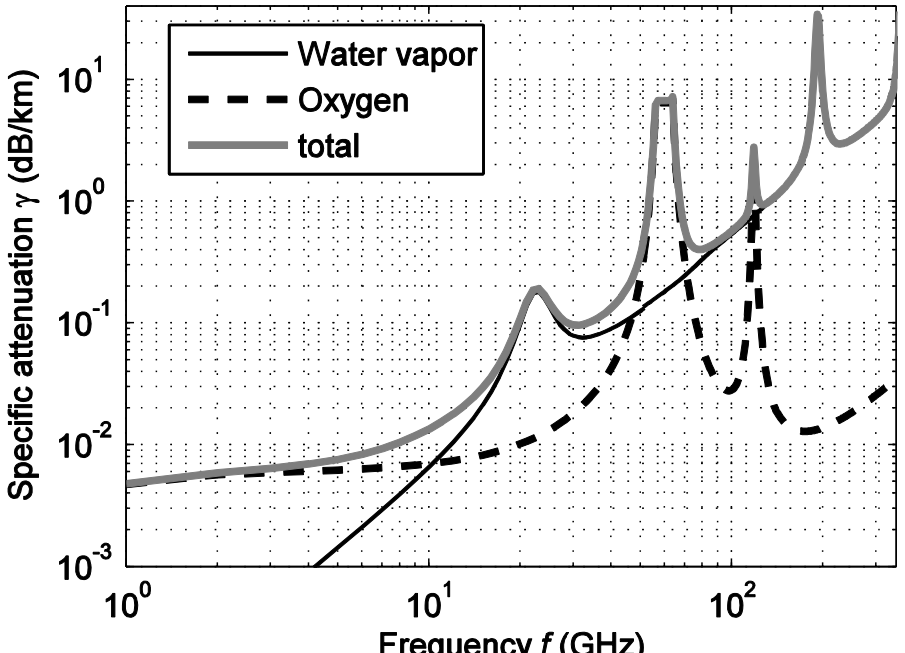
Scattering due to rough surface




Rain-associated attenuation




Gas-associated absorption



# Lessons learnt, at the physical layer

- Complexity of real world
- Probabilistic approaches
- Only partial math/physical models
- Empirical models
- Need for in-the-field measurements

Often, no need to be very sophisticated in these aspects because of the ***many and many simplifying assumptions*** imposed by any model…

Pragmatic approach

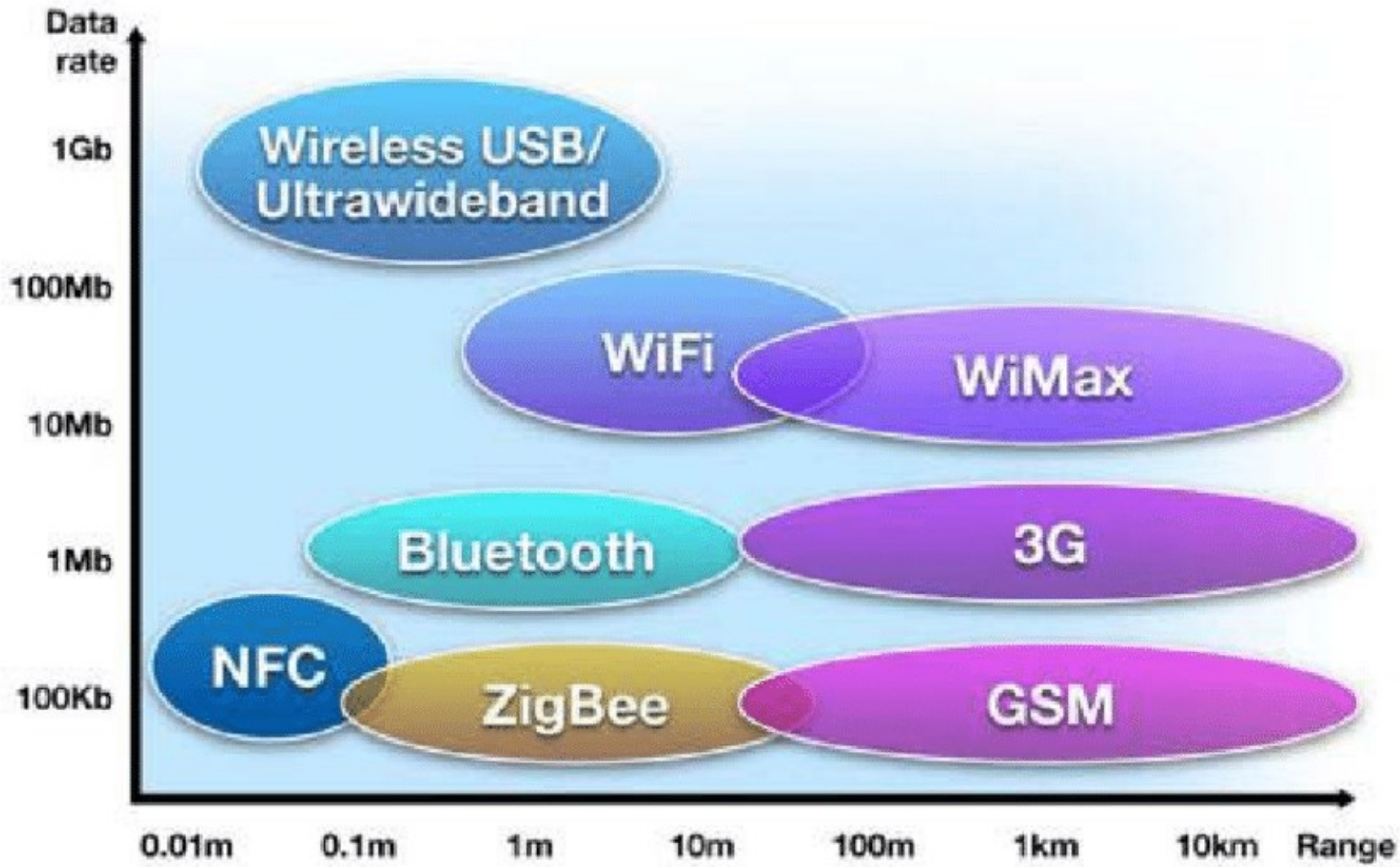
*Anyway, do not worry ☺, this course will not discuss anymore about the physical layer*

# Wireless Communications: Which Connectivity Technologies today?

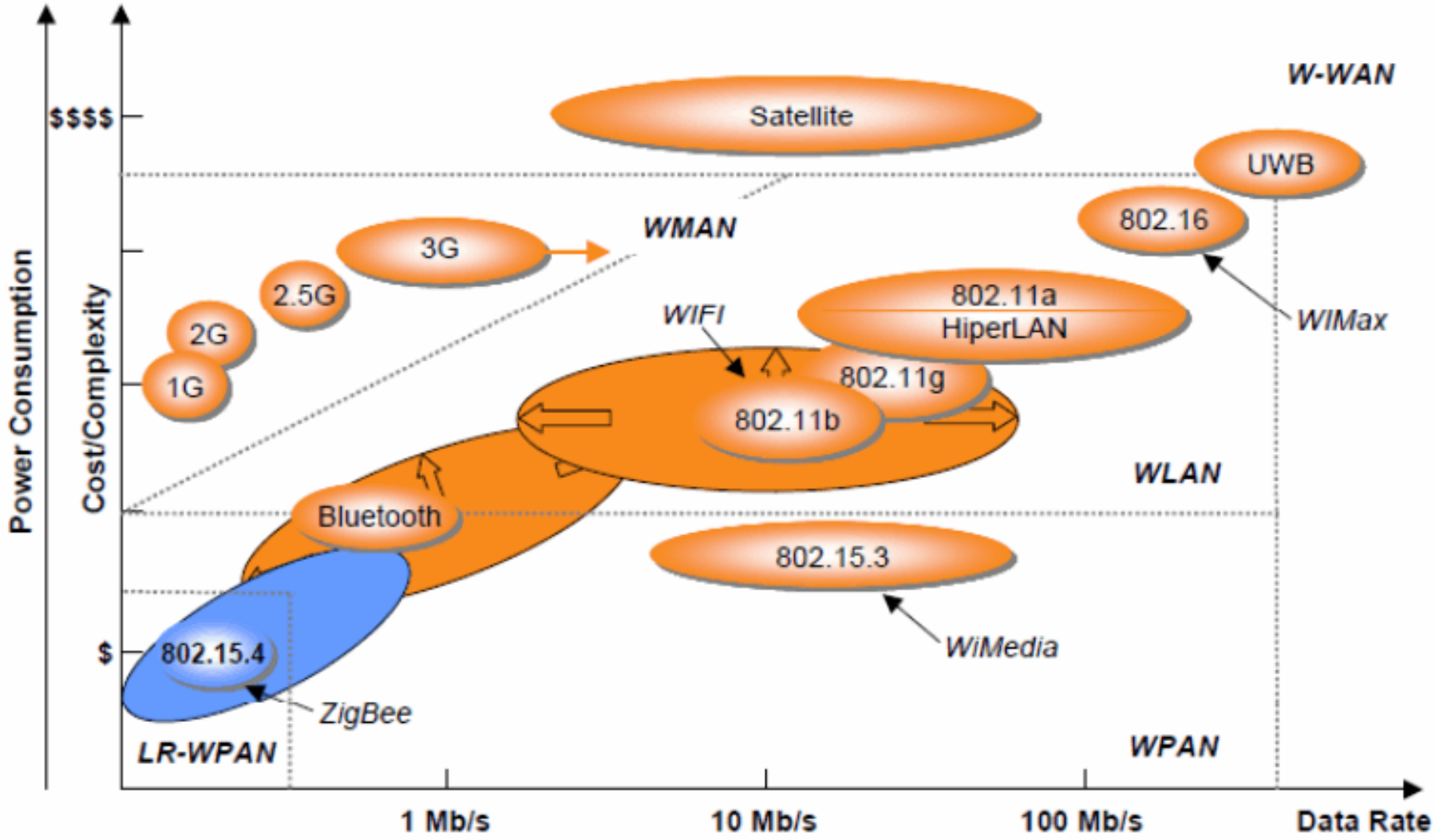
Overview on:

- Wireless LAN – IEEE 802.11
- Wireless MAN
  - IEEE 802.16 – WiMAX/WirelessMAN
  - IEEE 802.20/802.11p – MBWA/Vehicular Mobility
  - IEEE 802.11 - WiFi & Mesh Networking
- Cellular Networks
- Wireless PAN (IEEE 802.15)
  - Bluetooth and Bluetooth Low Energy (BLE)
  - ZigBee, Low rate WPAN, …

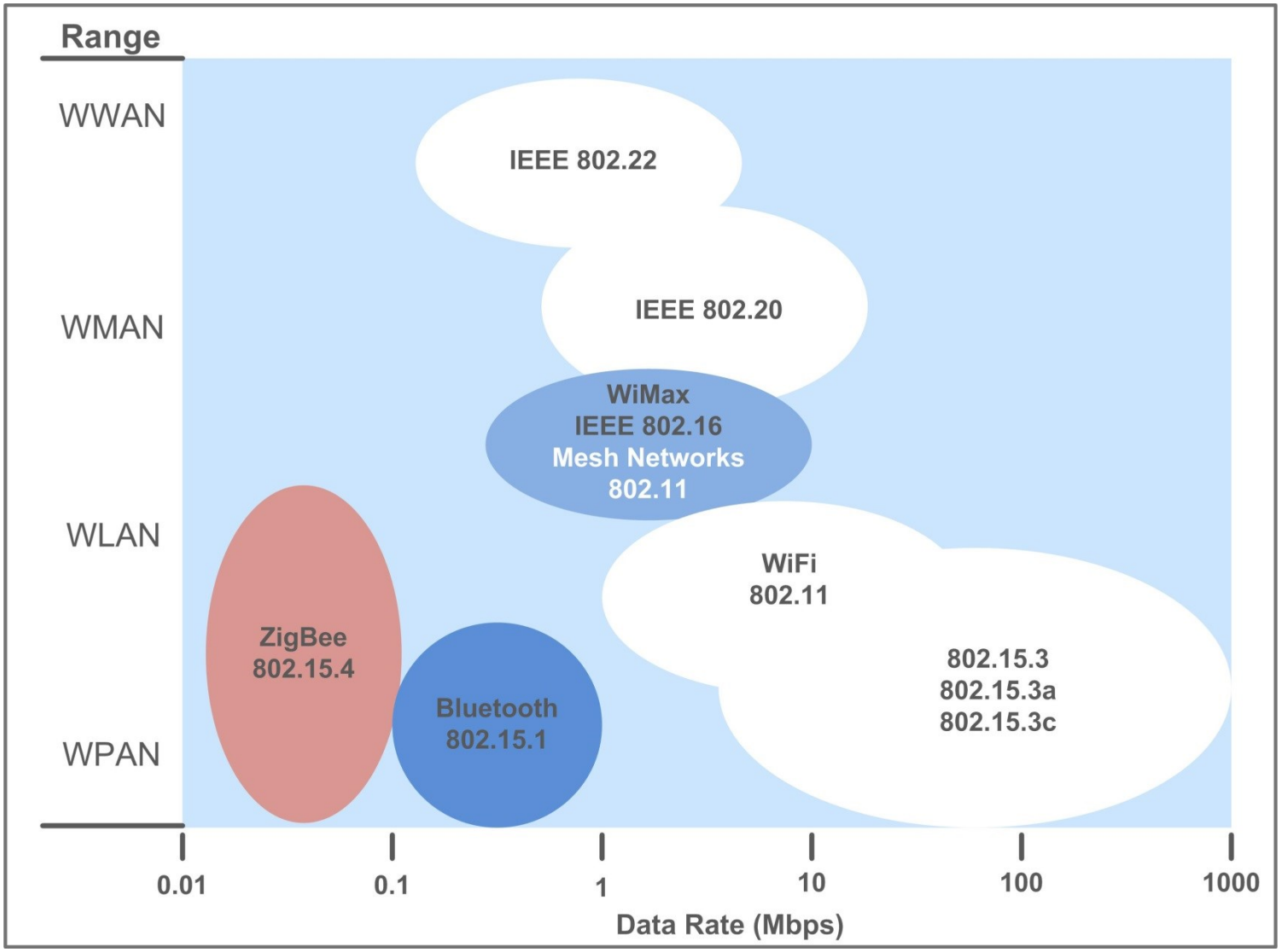
# Wireless Space



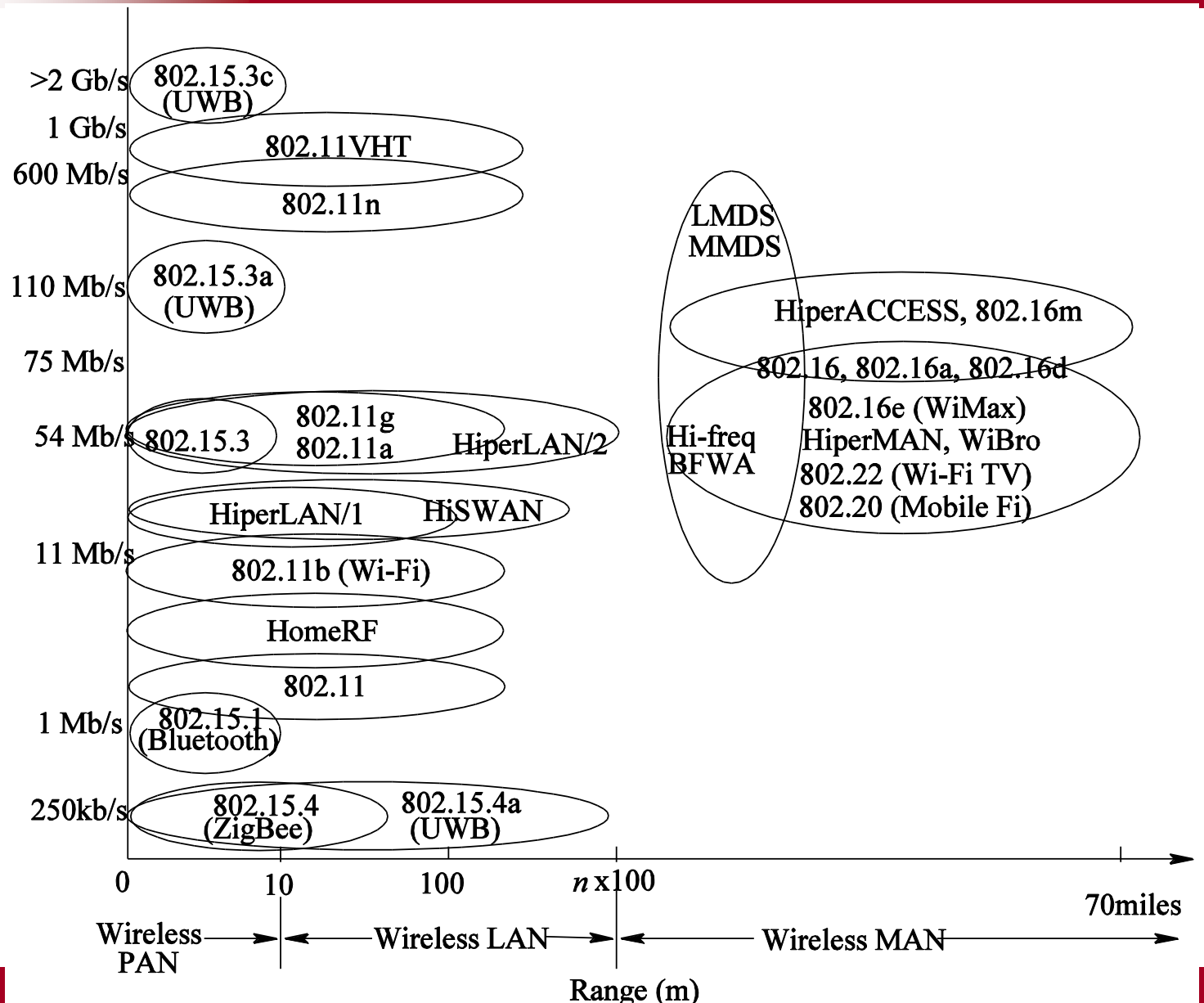
# Wireless Communications Space: with finer Details…



# Wireless Communications Space: with finer Details…



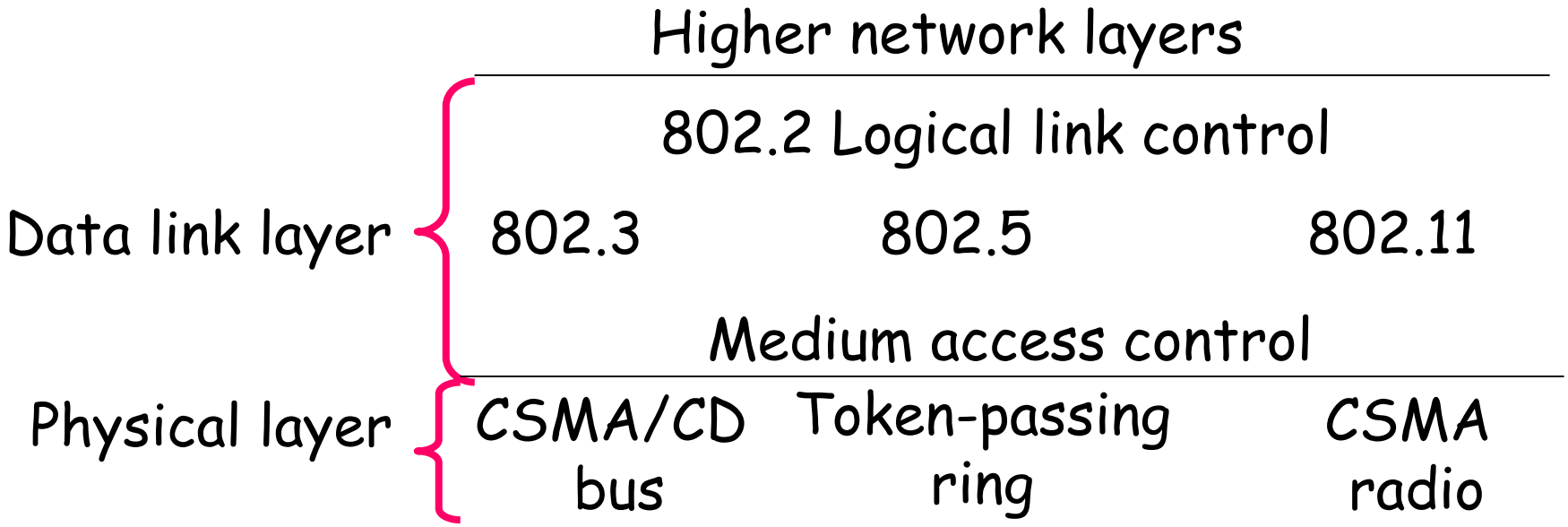
# Wireless Communications Space: with finer Details…



# IEEE 802.x Standard for Local Area Networks (LAN)

The IEEE 802.x standards define:

- Physical layer protocols
- Datalink layer protocols
  - Medium Access Control (MAC) sub-layer
  - Logical Link Control (LLC) sub-layer



# Ethernet/IEEE 802.3 based on CSMA/CD

- ***TRADITIONAL CSMA/CD Algorithm:***
  - To perform channel ***sensing***
    - If idle, immediate transmission
    - If occupied, wait until the channel becomes idle again
  - ***Collision Detection***
    - Immediate abort of a transmission if collision detected
    - Following transmission try after waiting for a ***random time interval***

- Why CSMA/CD?
  - CSMA relevantly reduces the number of collisions
  - CD reduces the negative impact of potential collisions

***OPTIMISTIC APPROACH***

# Exactly the same Ethernet Algorithm

***1-persistent CSMA + binary exponential backoff***

- ***Channel sensing***
- If ***idle***, immediate transmission *(p-persistent, here p=1)*
- Otherwise, wait until the channel is idle and then immediate transmission
- If collision is detected
  - ***Random selection*** of a transmission slot in the range $[0, 2^n)$, where n=min(10,k) and k is the number of collisions already occurred for that frame
    - Slot length = 2 * end-to-end propagation delay
  - Transmission during the selected slot
- Algorithm self-adapts well to the dynamic changes in network load

# Wireless LAN or IEEE 802.11

- Wireless communications for so-called ***short range***
  - Transmission range < 250m
- Bandwidth up to 866Mbps (with many and many variants)
  - ***802.11b*** (many variants, up to 2 and 11Mbps at 2.4GHz)
  - ***802.11a*** (many variants, up to 54Mbps at 5GHz)
  - ***802.11g*** (many variants, up to 54Mbps at 2.4GHz)
  - ***802.11n*** (many variants, up to 150Mbps at 2.4GHz)
  - ***802.11ac*** (many variants, up to 866Mbps at 5GHz)
  - ***802.11ax*** (WiFi-6, 2019, many variants, up to 1201Mbps)
  - ***802.11be*** (under discussion, WiFi-7, 20Gbps?)
- Standardization ***of MAC layer, of physical layer***, and of some security aspects (partial support)
  - Typically ***no Quality of Service***

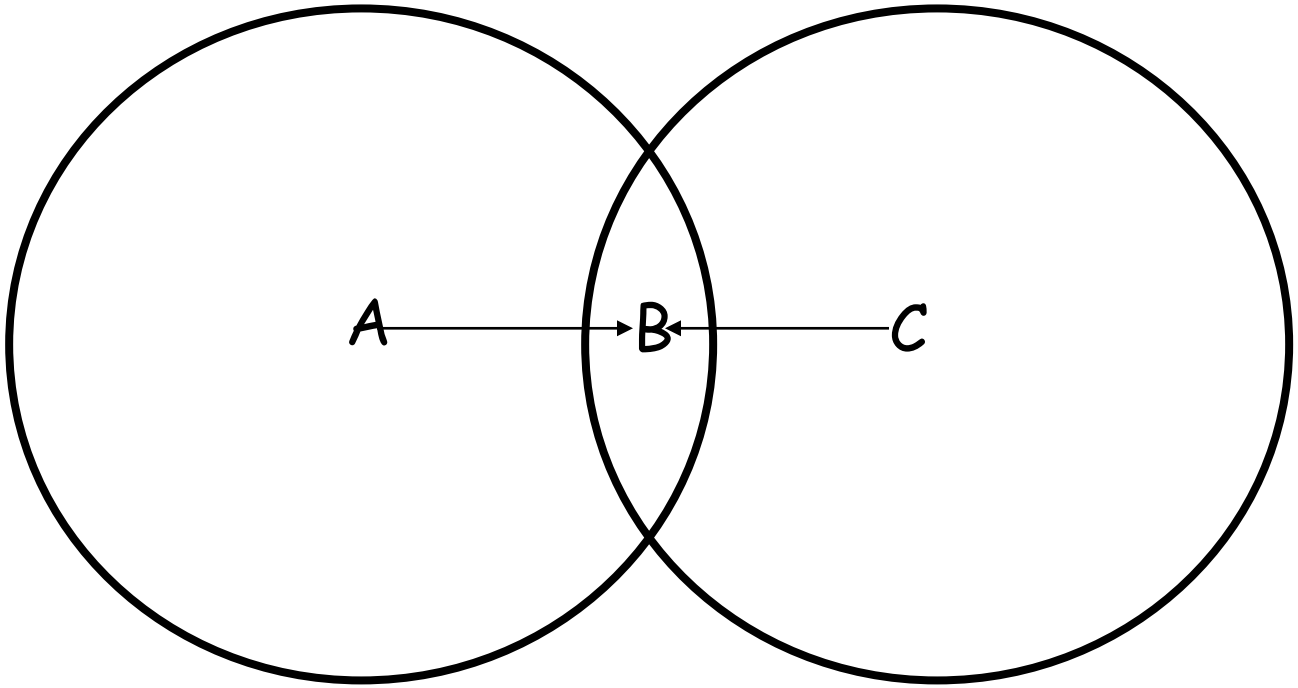
# IEEE 802.11: Primary MAC-layer Issues

From several perspectives, the IEEE 802.11 approach is similar to Ethernet, but:

- Can CSMA/CD work correctly over wireless medium?
- ***Simple forms of CD are NOT possible (may fail) because of attenuation issues***
- Also CS exhibits some issues: not all nodes are in the coverage range of any other node
- What affected by ***mobility***?

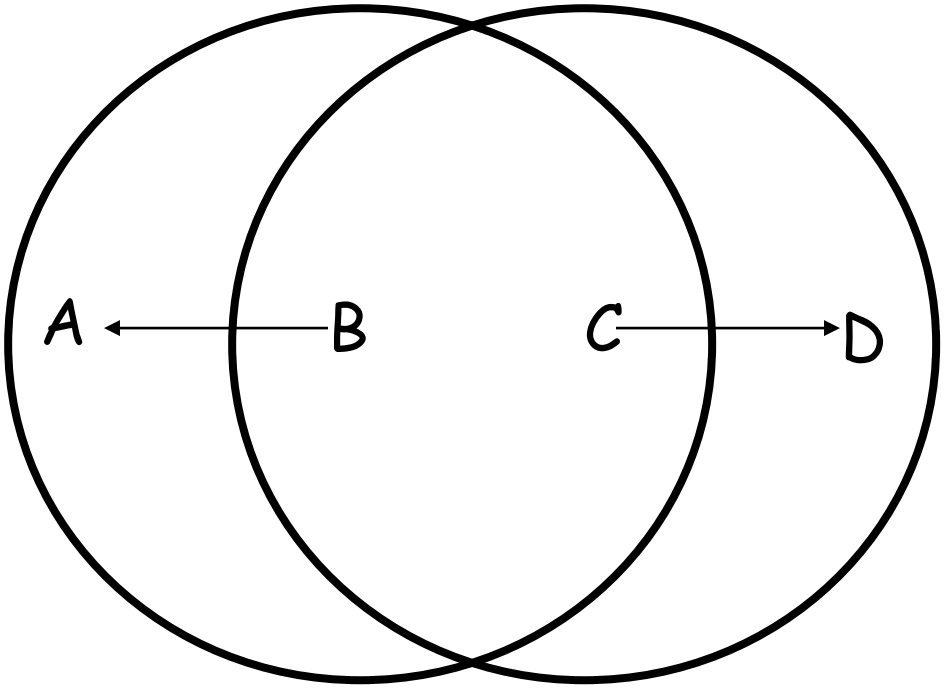
- Let's start with "classical" NEW problems, which are not possible in wired communications:
  - ***Hidden node***
  - ***Exposed node***

# The so-called Hidden Node Issue



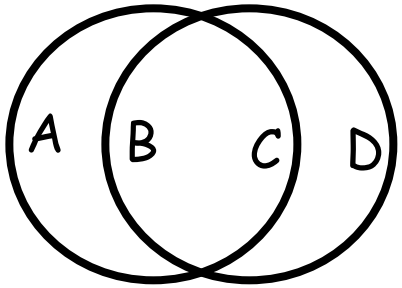

- A starts transmitting to B
- ***C cannot be aware of A's communication (out of range)*** and therefore starts transmitting to B
- ***Collision!***

# The so-called Exposed Node Issue




- B starts transmitting to A
- C detects this transmission and does NOT send any communication towards D
- ***Error***: this communication ***would NOT have interfered*** with A and D

# Multiple Access Collision Avoidance (MACA)




B is willing to transmit to C

- B transmits a first ***Ready To Send*** (RTS) frame towards C. The frame includes the length of data to be transmitted
- C replies with a ***Clear To Send*** (CTS) frame
- Other nodes overhear the RTS frame and HAVE to stay inactive (in silence) for ***sufficient time*** to allow C to reply with its CTS
- Other nodes overhear the CTS frame and HAVE to remain in silence for the whole duration of B's transmission

# MACA: are Collisions still Possible?

- Collisions may occur ANYWAY
  - For instance, simultaneous sending of RTS frames
  - But at least ***data frames CANNOT collide***
  - And because of ***mobility?***

- Solution: ***nodes anyway make re-transmissions by using the "classical" Ethernet algorithm***, i.e., binary exponential backoff

Try to countercheck experimentally how often the RTS/CTS mechanism is really employed in your WiFi networks?

How? For instance, via sniffing of the radio channel…

Ever used *WireShark* or similar?

# IEEE 802.11: Two Primary Configurations

- ***Ad hoc***: all nodes are potentially mobile and communicate directly the ones with the others. We will see in MANETs…
  - How many hops? Which availability and reliability? Which latency is still acceptable? Which trade-offs between those elements?
  - Which issues/challenges if implemented with the MAC/routing/transport mechanisms and algorithms that you already know?

  ***Differences wrt Wi-Fi Direct?***

  Wi-Fi Direct devices host sw-based access points ("Soft APs")…

- ***Base station***:
  - Fixed nodes, equipped also with wired connectivity, serve as ***access points*** (or base stations) for wireless communications
  - Mobile nodes communicate through access points
  - Mobile nodes operate ***occasional scans*** in their locality to find new/other access points by using a simple ***probe/response prot***
  - Which issues/challenges if implemented with the MAC/routing/transport mechanisms and algorithms that you already know? For instance, ***dynamic transfer*** from one access point to one another

# (Brief Note on) WiFi Direct

**Wi-Fi Direct**, or Wi-Fi P2P (initial name),

enabler for ***direct connection*** of off-the-shelf devices, also ***multi-point***, competitor of Bluetooth for applications that do not need low energy consumption

- ***Only one of the Wi-Fi devices HAS to be compliant with Wi-Fi Direct to establish a peer-to-peer connection***
- ***Pairing***
- We'll return to it after Bluetooth and MANET presentations

Wi-Fi Direct essentially FORCES any compliant device to implement a ***software access point (Soft AP)***. Soft AP implements a version of the AP connection mode called ***Wi-Fi Protected Setup*** (*push-button or PIN-based setup*)

- When a device enters the range of a Wi-Fi Direct host, it obtains setup info through Protected Setup in simplified and quasi-automated way

# (Brief Note on) WiFi Direct Soft AP

- A Soft AP may be implemented according to different levels of complexity, depending on the role to be played (standard ***flexibility***)
  For instance, a digital picture frame can provide only very base services for connectivity and upload by cameras; a ***smart phone typically offers more complex data tethering*** with bridge capability towards the Internet

Note that (virtualization vs physical location):

"Pairing" of Wi-Fi Direct devices may be configured to request ***real proximity of devices***, for example, via verification of Near Field Communication (NFC) or Bluetooth signals (and/or explicit button press by the devices' users)



# WiFi Direct Soft AP

Are WiFi Direct nodes
peer-to-peer nodes (no infrastructured) in a cooperative network?

More info in the following parts of the course…

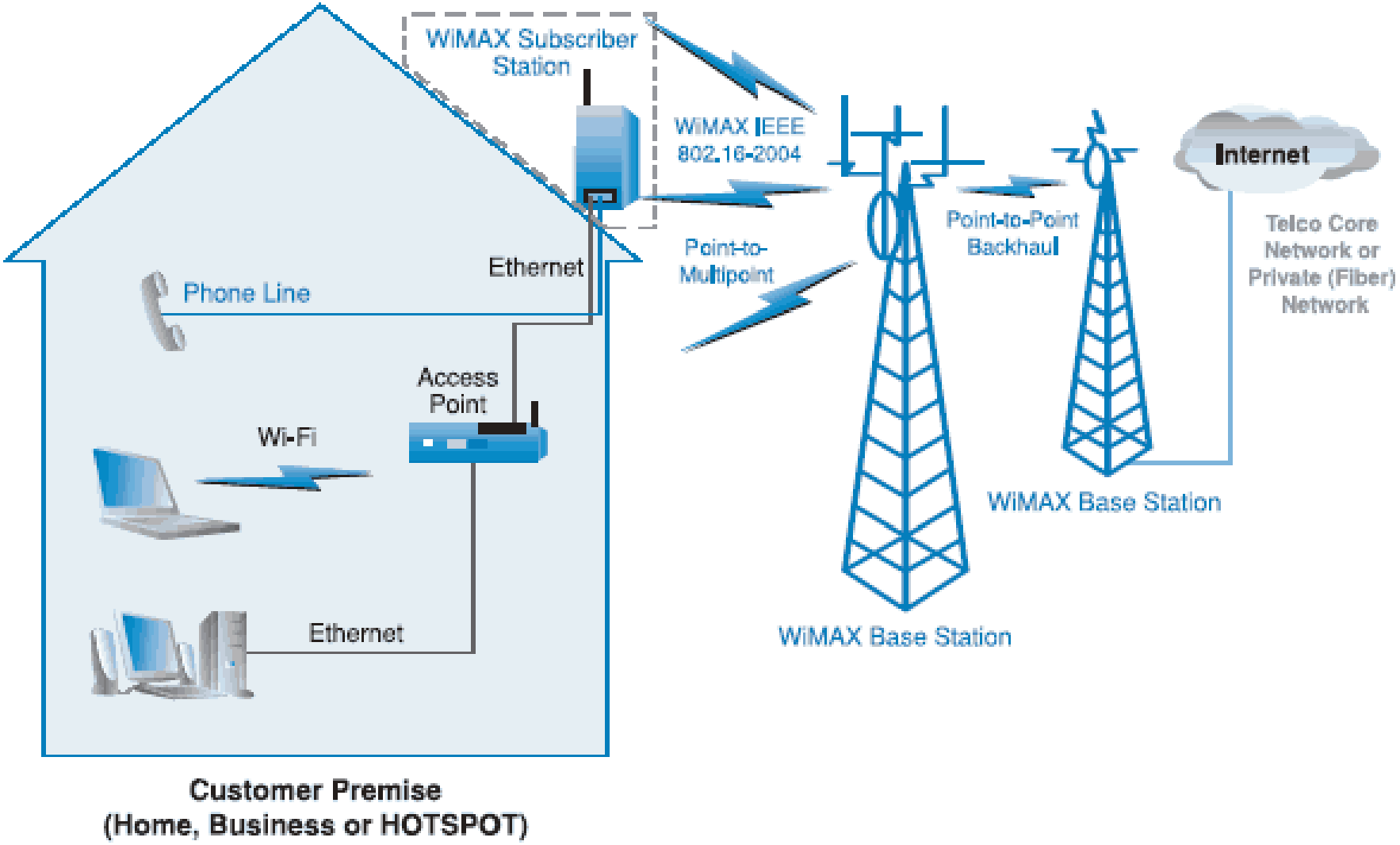
# Wireless MAN: IEEE 802.16 or WiMAX

- Goal: ***broadband access in metropolitan areas***
- Why?
  - Growing demand for ***local network connectivity with high bandwidth***
  - High capacity fiber/cable towards any user is typically ***unsustainable from the economic point of view*** (think to WiMAX in mountain areas or for covering geographic areas with limited population density)
  - IEEE 802.11 is short range (around 250m in optimal conditions)
  - Cellular communications (see next lectures) could be or could be perceived as ***too expensive for the offered datarate***

# Wireless MAN: IEEE 802.16

- IEEE 802.16 standard (WiMAX) ***to cover "last mile"***
  - Maximum datarate = **70Mbps** (in first version; think to current datarates of IEEE 802.11 variants and 5G cellular networking)
- ***Optimized for "fixed stations"***
  - Basic idea: ***every building equipped with an antenna (subscriber station)*** that communicates with central base stations, wired connected to the Internet
  - ***Circuit commutation***, hierarchical architecture
- In your opinion, why ***limited spread***, in particular in some national contexts (e.g., Italy)?

# Wireless MAN: IEEE 802.16



# Mobile Broadband Wireless Access (MBWA): IEEE 802.20 – Vehicular Mobility

IEEE 802.20 - ABANDONED - standardized physical and MAC layers for ***mobile broadband wireless access (MBWA) systems***

- Worked in licensed band under 3.5 GHz
- Optimized for IP-oriented data communications
- Datarate – peek in downlink per user > **1 Mbps**
- Datarate – peek in uplink per user > **300 Kbps**
- ***Number of concurrent active users HIGHER*** than in other mobile wireless solutions

- Supported ***different classes of vehicular mobility***, up to 250 Km/h in MAN environments
- But which other issues ***are present in terms of routing, transport, application-layer, …***?

***NOW IEEE 802.11p? …***

# IEEE 802.11p – Vehicular Mobility

Basically IEEE 802.11 variant ***with no need of long association time to AP*** (basic service set – BSS)

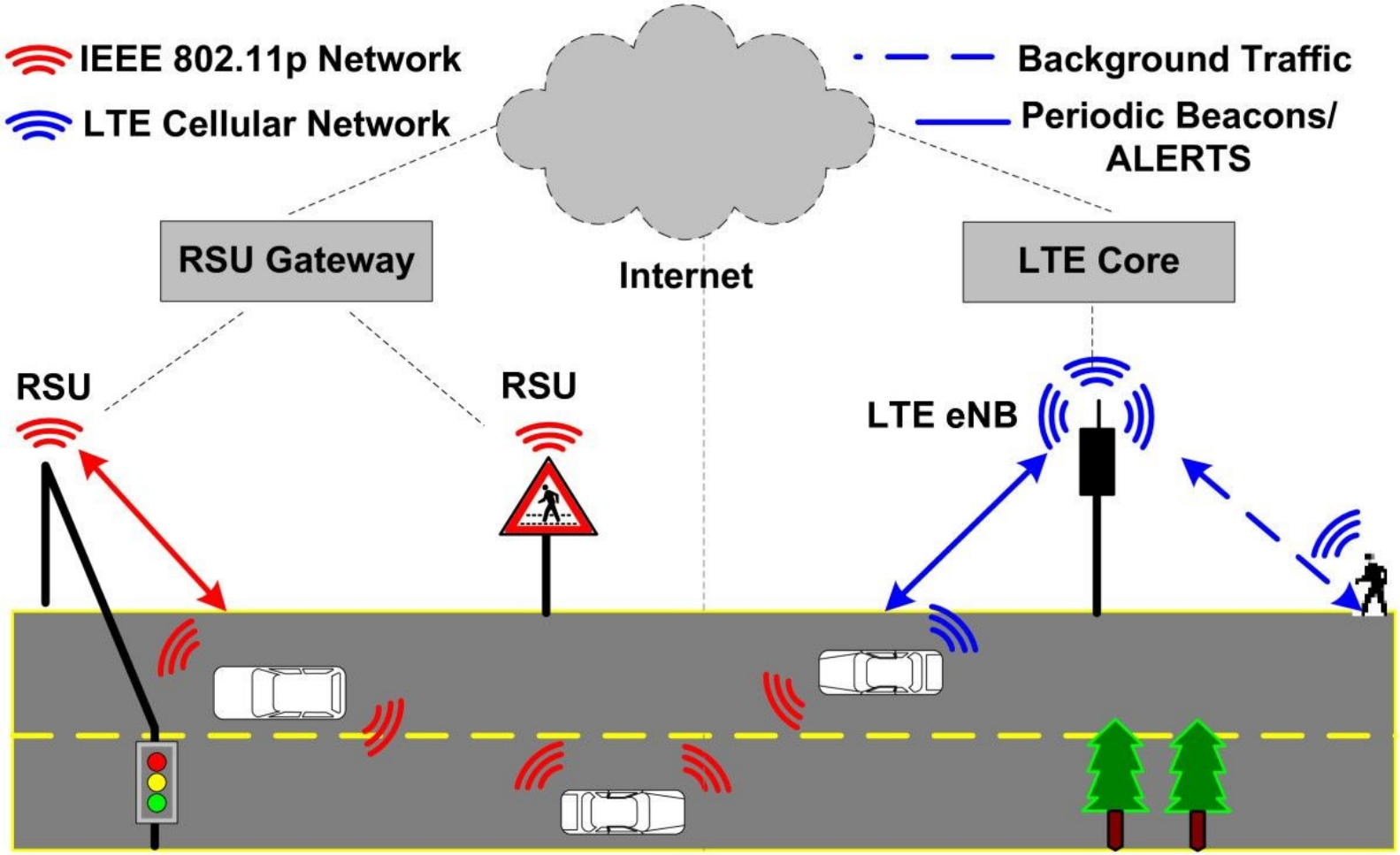
IEEE 802.11p is an approved amendment for ***wireless access in vehicular environments (WAVE)***

Includes data exchange between ***high-speed vehicles*** and between the ***vehicles and the roadside infrastructure***

Licensed ITS band of 5.9 GHz (5.85-5.925 GHz)

***IEEE 1609*** is a higher layer standard based on 802.11p and also the base of a European standard for vehicular communication known as ***ETSI ITS-G5***

# IEEE 802.11p – Vehicular Mobility



# Wireless MAN: WiFi Coverage?

- School of Engineering and Architecture, Viale Risorgimento, relatively well covered ☺ by WiFi APs
- How to properly cover more extensive regions?
  - Already done in several cities, of various sizes

    Brooklin Massachusetts, Rochelle Illinois, Thorold Ontario, Milton Keyens UK, Oulu Finland, Galatsi Greece, and many others are examples of municipalities with the need to provide WiFi access for city internal operations, public safety, meter reading and more, …
  - City-wide WiFi *mesh networks*, IEEE 802.11s, for example

    interested students can see C. Gomez, J. Paradells, "Urban Automation Networks: Current and Emerging Solutions for Sensed Data Collection and Actuation in Smart Cities", ***MDPI Sensors 2015***, doi:10.3390/s150922874

➡ Open question: how to organize and manage a WiFi mesh network? Which technological challenges?

# IEEE 802.11 for Municipal Mesh Network

- IEEE 802.11 base stations compose an infrastructure and can wirelessly communicate the one with the other
  - Compose a ***mesh (mesh networking)***
  - Can manage client connection handoffs between different base stations (***support to mobility***)
  - Which technical differences wrt “regular” IEEE 802.11?
- Why mesh-based solution?
  - Costs, robustness, …
  - Possibility of connecting only a few base stations to the Internet via wired connections
- Ideally any domestic or university campus AP (or even any mobile node) can ***contribute to the mesh infrastructure***
  - Which problems? Which needs?

# IEEE 802.11 for Municipal Mesh Network

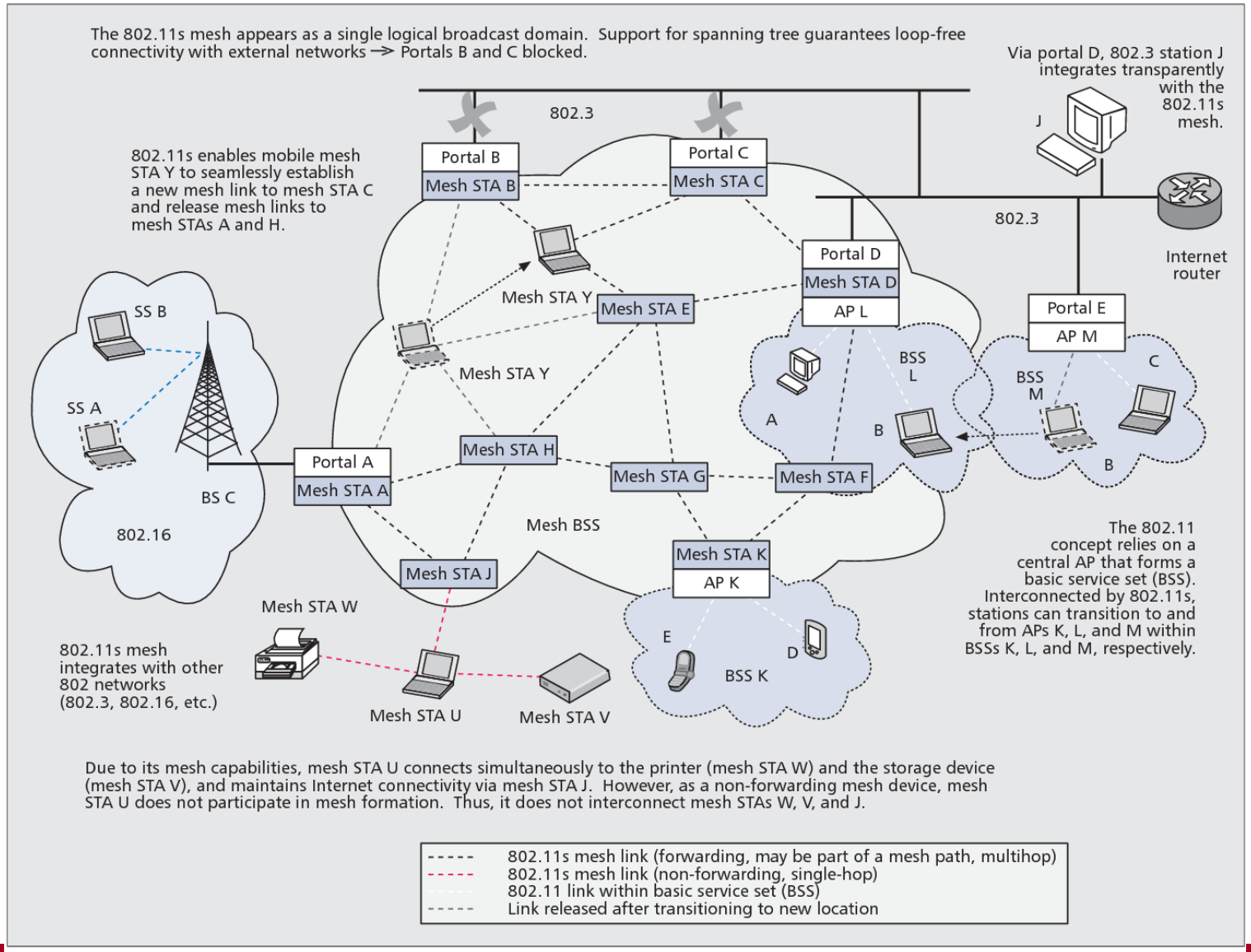
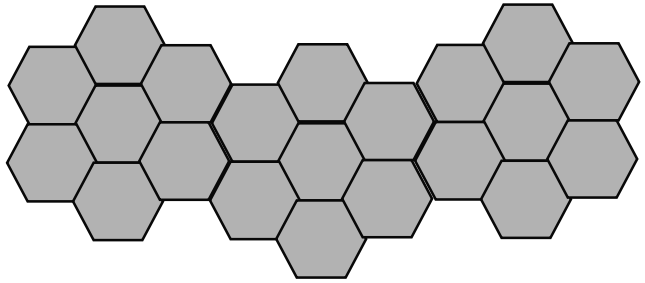



**Figure 1.** *802.11s enables seamless connectivity among dissimilar 802 networks.*

# Cellular Networking: Basic Idea

- Many transmission antennas with low power (800-900MHz)
  - ***Why? Scalability and incremental deployment***
- Geographical area split into ***adjacent cells***



- Any cell is served by one base radio station (Base Station - BS)
  - Analogously to what seen for IEEE 802.11 BS (access point)
- ***Radio frequencies can be re-used in non-adjacent cells***, provided that a proper spatial interval (of non-interference) is respected

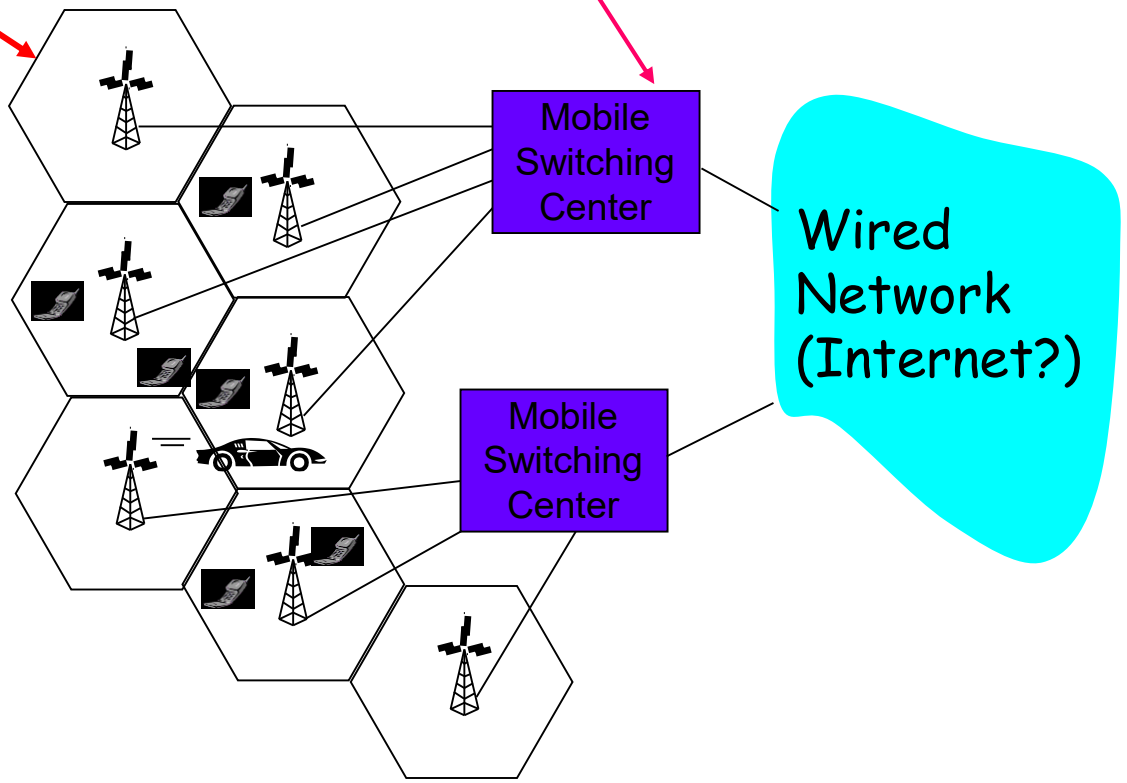
# Cellular Network Architecture

## MSC

- connects cells to WAN
- manages setup of local calls
- manages mobility

## cell

- covers a geographical area
- *base station*
- *mobile users* connect to the network through BS
- *air-interface:* physical/link-layers protocols between mobile devices and BS



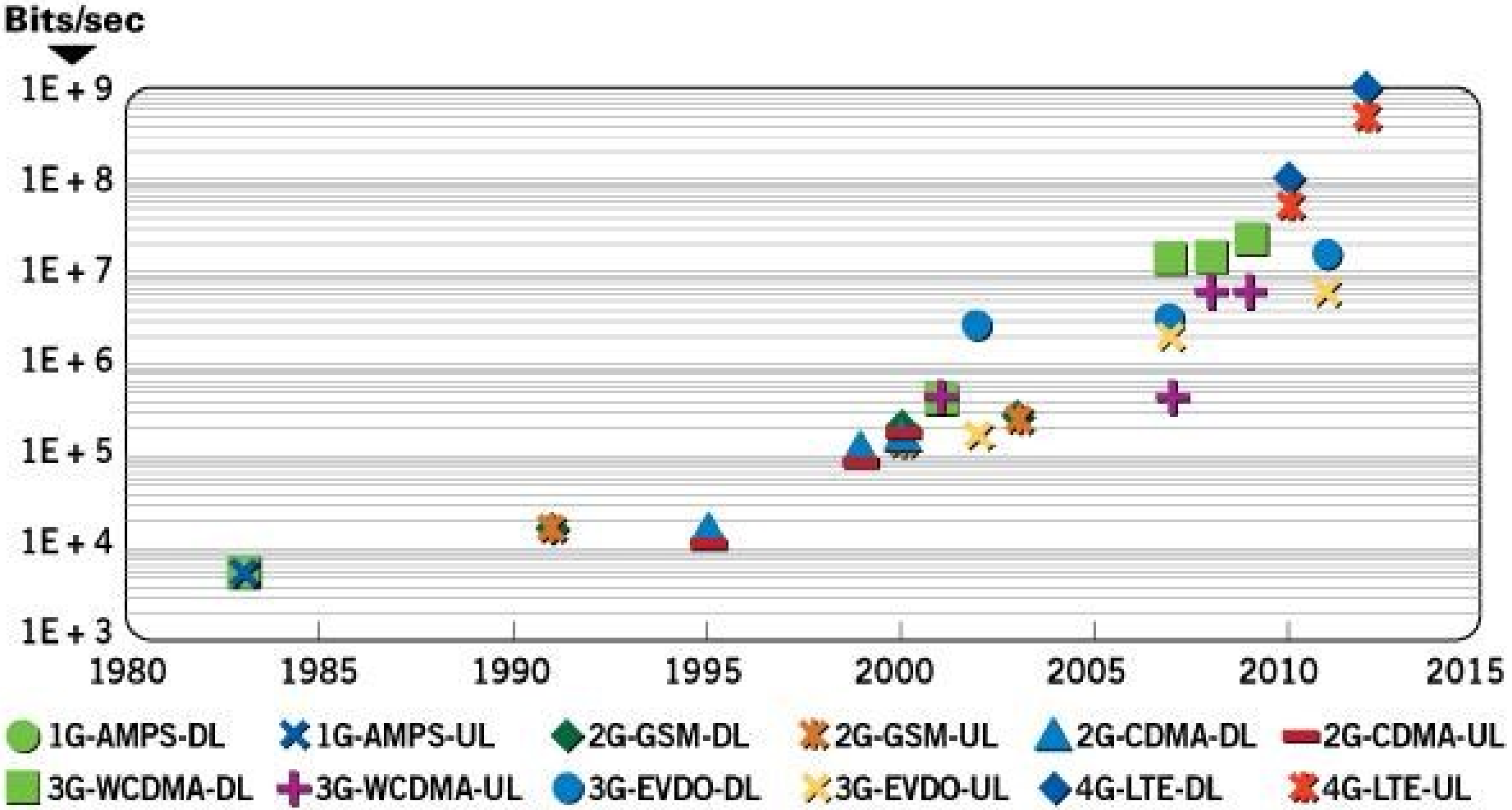
# A Plethora of Different Standards for Cellular Networking (1)

- ***2G systems***: **only voice channels** (but already digital tech in both communication and commutation)
  - IS-136 TDMA: FDMA/TDMA combined (N.America)
  - Global System for Mobile communications (GSM): FDMA/TDMA combined
    - Most widespread and used
  - IS-95 Code Division Multiple Access (CDMA)
- ***2.5G systems***: ***channels for voice and data***
  - Extensions to 2G before the widespread adoption of 3G
  - General Packet Radio Service ***(GPRS)***
    - GSM evolution
    - Data sent over multiple channels, when available

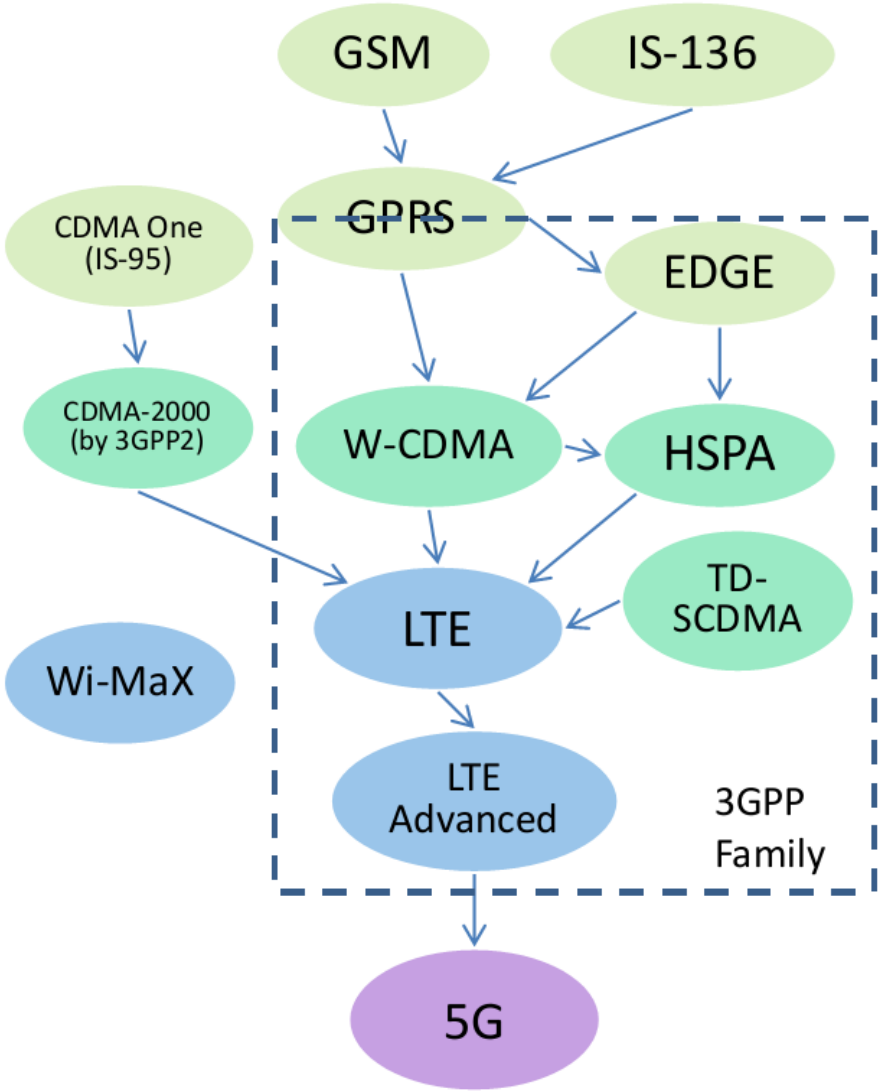
# Cellular Networking Standards (2)

- ***… 2.5G***
  - Enhanced Data rates for Global Evolution ***(EDGE)***
    - Also in this case, GSM evolution; modulation change
    - Datarate up to 384Kbps
- ***3G systems***: voice and data channels, of course
  - Universal Mobile Telecommunications Service (UMTS)
    - Further evolution step of GSM, but with CDMA exploitation
    - CDMA-2000
    - WCDMA
- ***4G systems***: voice and data channels, of course
  - Datarate upto 1000Mbps (download) and 500Mbps (upload)
  - Often indicated as LTE or LTE-Advanced
  - Already available in Japan since 2006

# Cellular Networking Standards: Evolution



# Cellular Networking Standards: Evolution



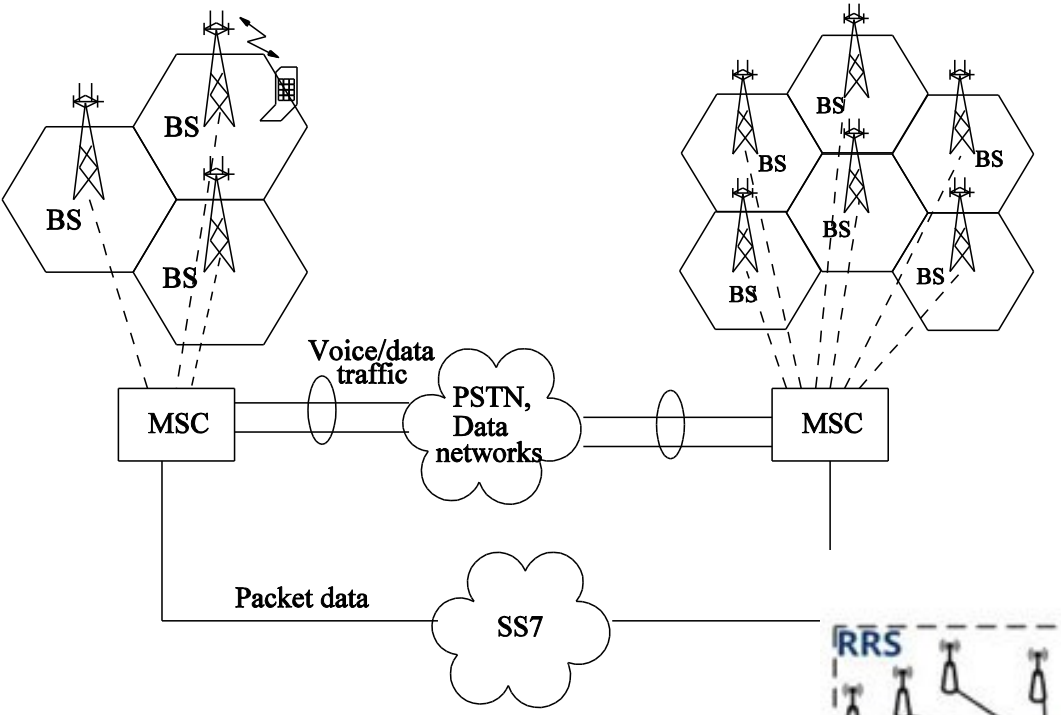

**2G**
- Mainly circuit switched, with packet-switching introduced since GPRS
- Based on TDMA (and CDMA for CDMA One)

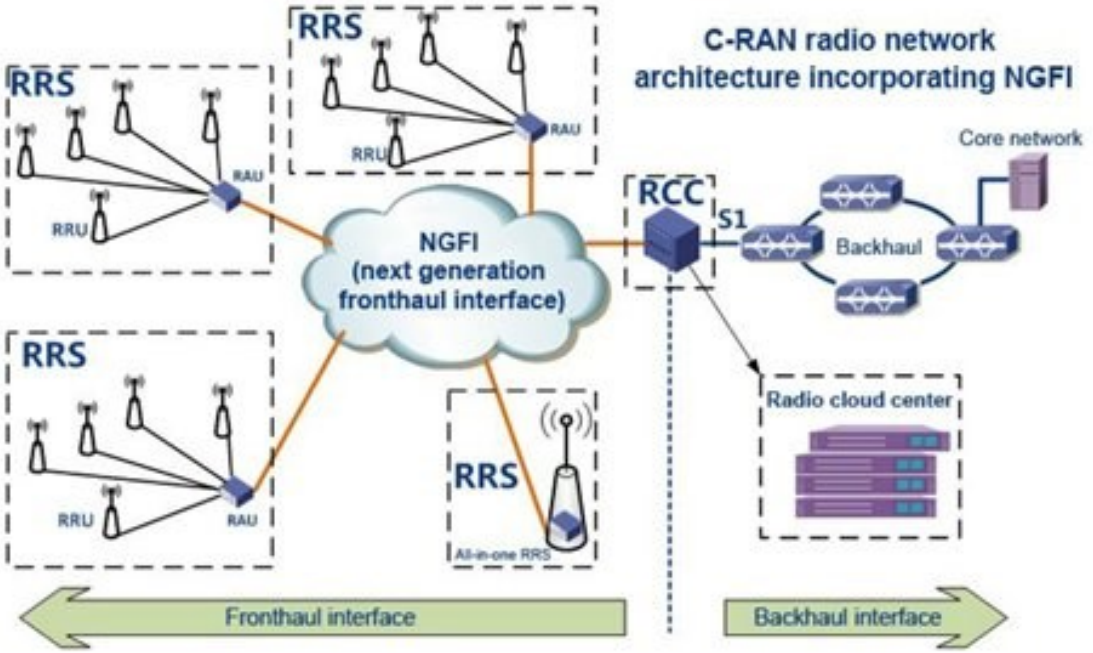
**3G**
- Circuit and Packet-switched
- (Primarily) based on wideband CDMA

**4G**
- All IP flat architecture with evolved packet core.
- Based on OFDM and MIMO
- Cooperative processing

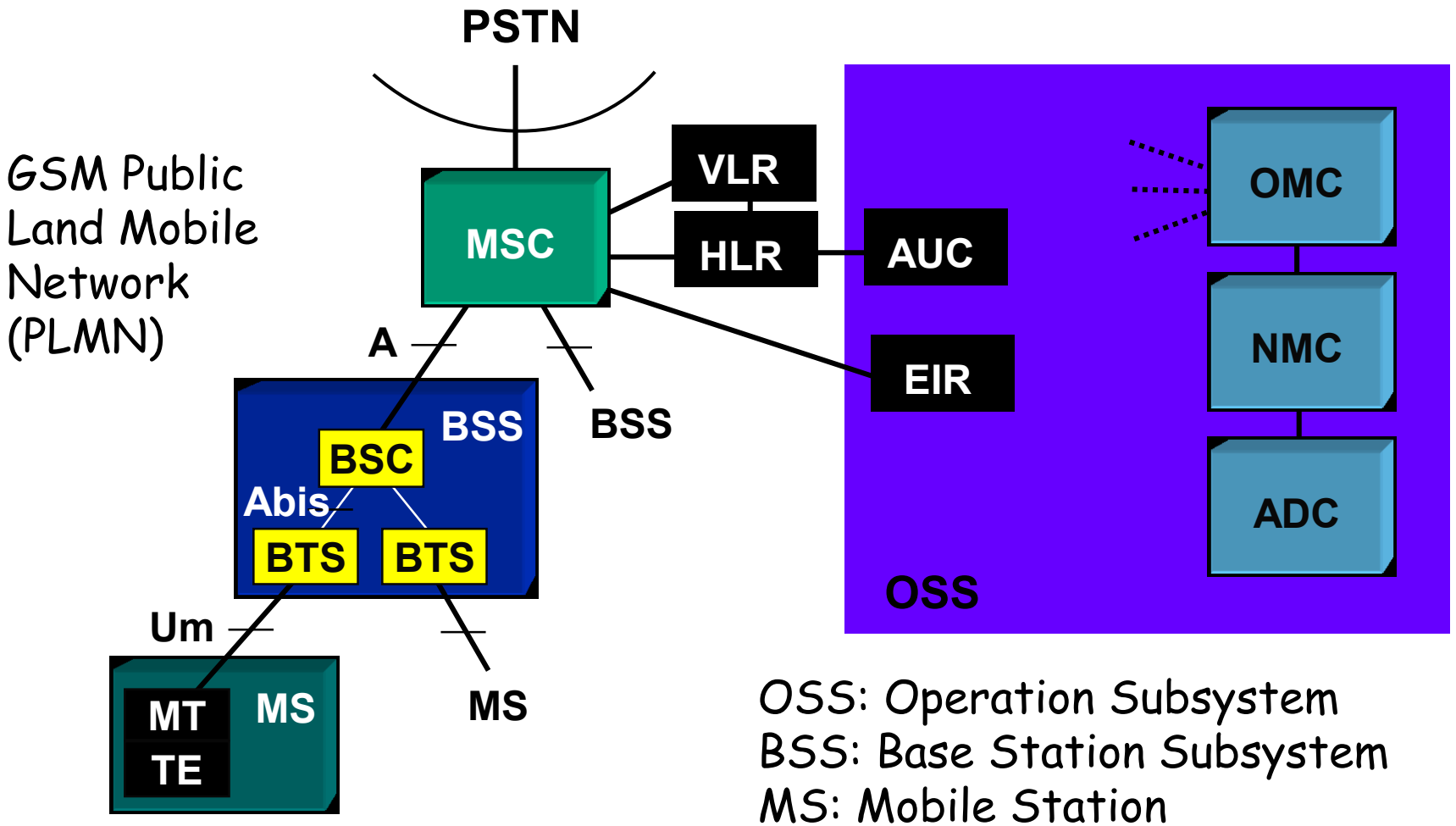
**5G**
- Based on massive MIMO, Small Cell and centralized processing techniques
- Integrated wire and wireless full IP networks

# Cellular Networking: from Circuit to Packet Switching



# GSM: General Architecture (1)




OSS: Operation Subsystem
BSS: Base Station Subsystem
MS: Mobile Station

# GSM: General Architecture (2)

- MS ***communicates with several BSSs*** via its radio interface Um
- Mobile Terminal (MT) ***supports physical channels between MS and BSS*** (radio transmission, channel coding, voice conversation coding, …)
- Terminal Equipment (TE) ***contains terminal/user-specific data*** (also user profiles) and ***smart card data*** (e.g., associated with SIM)
  - Identifies the user towards the network, e.g., when supporting personal mobility (in addition to terminal mobility) and security

By the way, do you know the differences among ***user mobility***, ***terminal mobility***, ***session/resource mobility***?

# GSM: General Architecture (3)

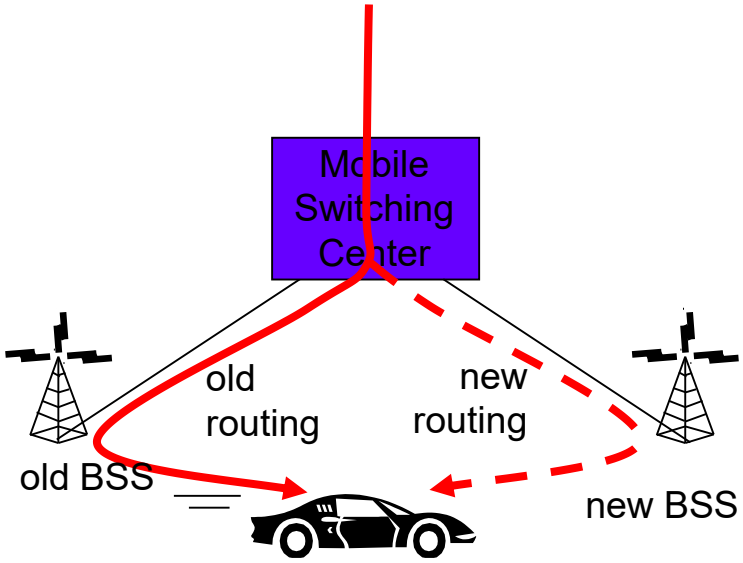
***Hierarchical organization and locality principle***

- BSS communicates with MSC via network interface A
- Base Transceiver Station (BTS) manages ***channel allocation, signaling, frequency hopping, handover triggers***, …
- BTS communicates with Base Station Controller (BSC) by using the Abis interface
- BSC manages radio channels, paging, handoff for different BTS
- MSC plays the role of ***gateway to PSTN and to packet data networks***
  - Works for switching, paging, location updates of MS, handoff control, …
- ***Home Location Register (HLR)*** stores subscribers' info and part of the location data of MS to perform ingress call routing towards the proper ***Visitor Location Register (VLR)***
- ***VLR stores the list of "visiting" users*** in its area and assigns the so-called roaming numbers

# GSM: General Architecture (4)

- ***AUthentication Center (AUC)*** is accessed by HLR for users' authentication before service access
- ***Equipment Identity Register (EIR)*** supports the identification of stolen or fraudolent (stolen identity) MS
- OSS works for network monitoring, control, and management
  - Operations and Maintenance Center (OMC)
  - Network Management Center (NMC)
  - ADministration Center (ADC)

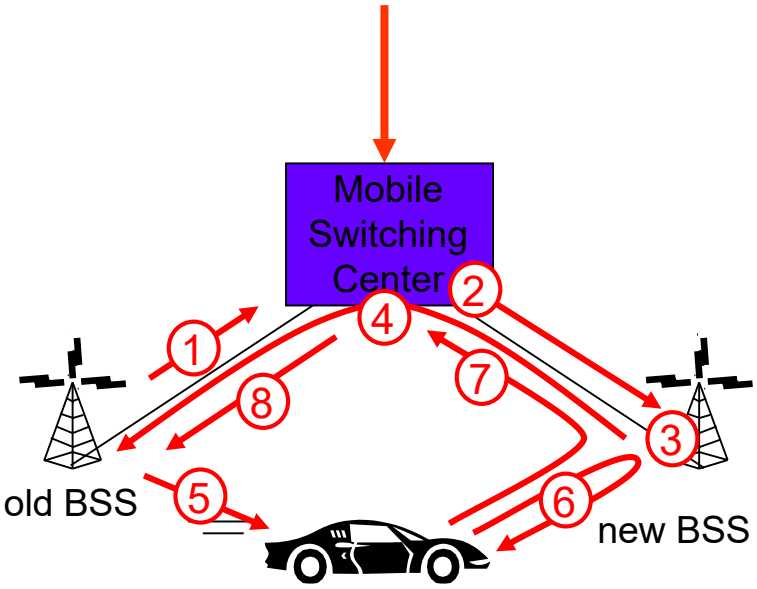
# GSM Handoff (under the same MSC)




- ***Motivations for handoff*** *(or handover)*
  - ***Stronger signal*** from/to new BSS ( "more continuous" connectivity, minor battery consumption, …)
  - ***Load balancing***: it may free channels for the current BSS
  - GSM does NOT specify ***why to*** operate handoff (***policy***), but only ***how*** (***mechanisms***)

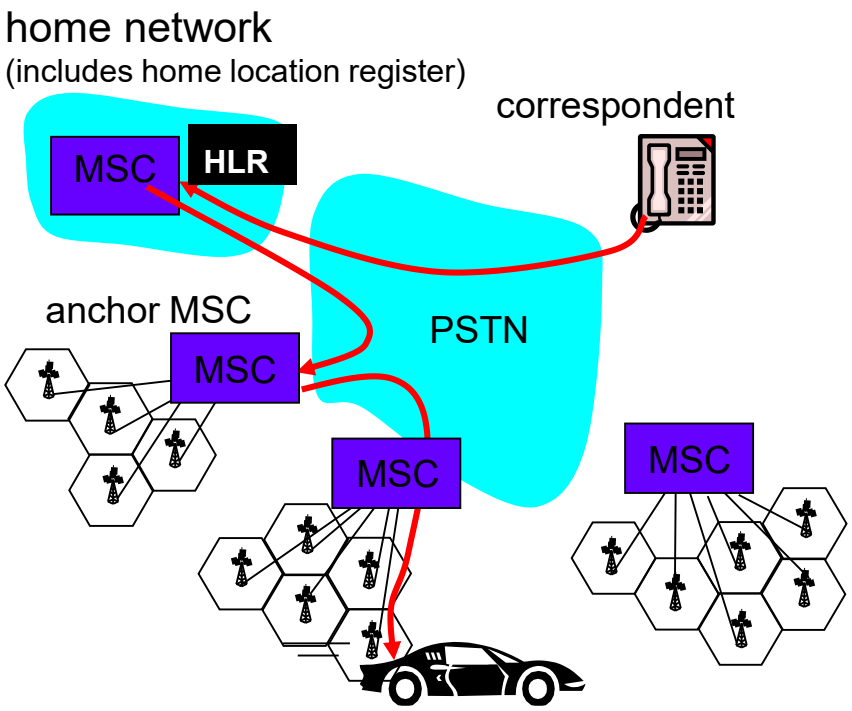
- ***Handoff triggered by the OLD BSS***

# GSM Handoff (under the same MSC)




1. Old BSS informs MSC of the need to perform handoff, by providing it with a ***list of one or more new BSSs***
2. MSC ***configures the new path (resource allocation)*** towards the new BSS
3. New BSS ***allocates the radio channel*** that the mobile "visitor" will have to use
4. New BSS signals to MSC and old BSS signals its ***ready state***
5. Old BSS informs mobile device of ***the need to operate handoff towards the new BSS***
6. It is the mobile device that signals to new BSS to activate the new channel
7. Mobile device signals to MSC, via the new BSS, that the ***handoff has been completed; MSC performs call re-routing***
8. ***Resources are released*** on the MSC-to-OldBSS path

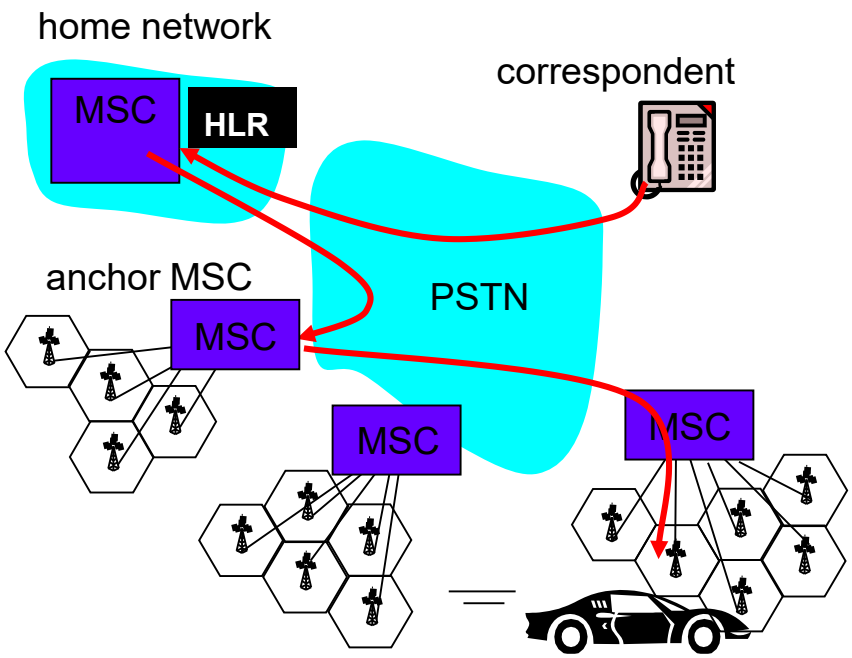
# GSM Handoff (different MSCs)




(a) before the handoff

- ***Anchor MSC***: ***first visited MSC*** during the call
  - Call remains routed through the anchor MSC
- New MSCs ***are appended at the end of the MSC chain***, step by step, as the mobile device is moving
- IS-41 allows ***minimizing the path*** (*optional feature*) in the ***multi-MSC chain***

# GSM Handoff (different MSCs)




(b) after handoff

- ***Anchor MSC***: ***first visited MSC*** during the call
  - Call remains routed through the anchor MSC
- New MSCs ***are appended at the end of the MSC chain***, step by step, as the mobile device is moving
- IS-41 allows ***minimizing the path*** (*optional feature*) in the ***multi-MSC chain***

# Need for Clarifications about 5G?

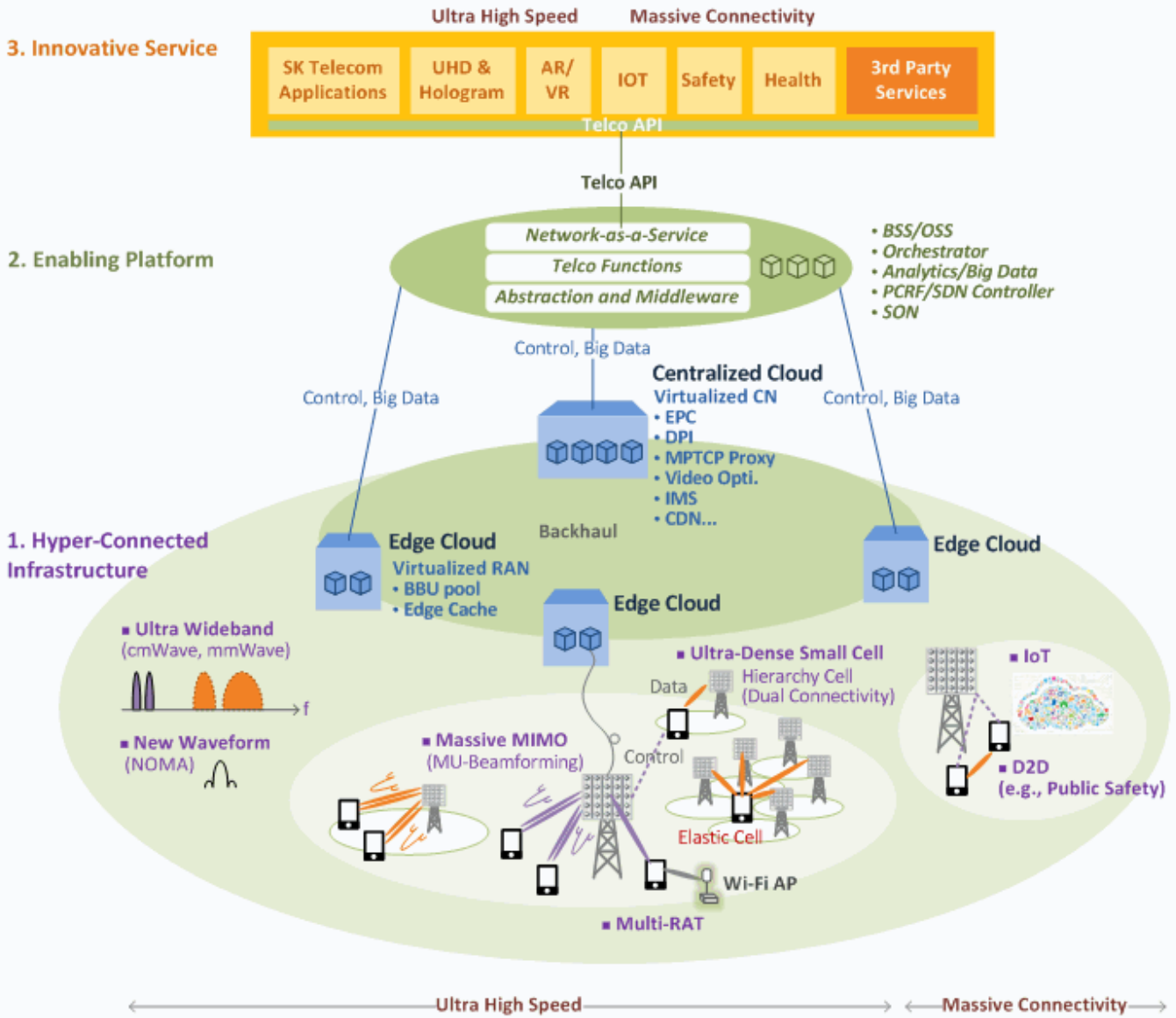



**Figure 3. SK Telecom's 5G architecture** (Source: SK Telecom's 5G whitepaper - Re-illustrated by Netmanias)

As you may see, ALSO:

- ***Virtualization***
- ***Middleware***
- ***Cloud***
- ***Edge cloud***
- ***….***

We'll discuss 5G and mobile edge technologies in the last lectures…

# A Parenthesis about Handoff
## (additional details in future lectures…)

Several taxonomies and classifications are possible (see also the wide literature in the field)

- ***Horizontal*** (homogeneous connectivity) ***or vertical*** (het connectivity) ***handoff***
- ***Mobile-initiated or network-initiated***. In addition, where is the handoff ***decision*** taken?
- ***When*** to trigger the handoff procedure?
  - ***Reactive***
  - ***Proactive***
- How to choose the ***destination network***?
  - Which ***monitoring indicators*** to considerate and with which ***metrics***?

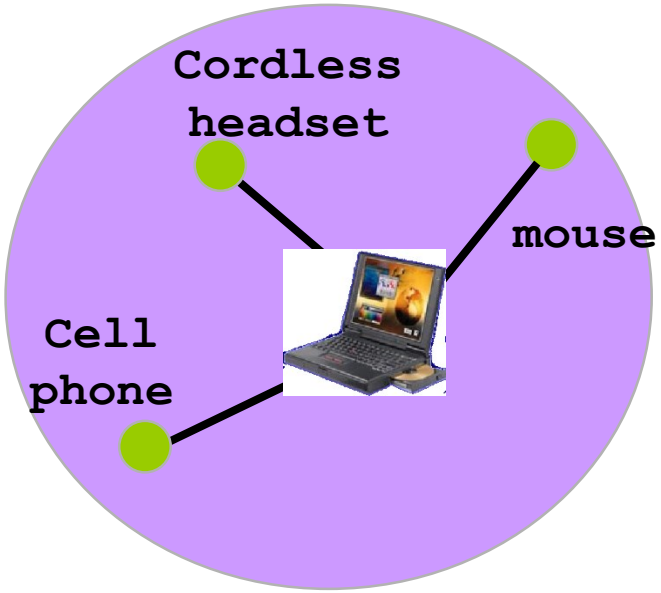
# A Parenthesis about Handoff
## (additional details in future lectures…)

- ***Hard handoff or soft handoff*** management (to concurrently enable ***multiple «virtual» radio interfaces*** or only one?)
  - Which pros and cons?
- Even ***multiple paths,*** also ***heterogeneous***…
  - Which technical challenges? What is currently supported?
- Standardization efforts and ***IEEE 802.21*** – Media Independent Handover Services (for both 802 and non-802 networking solutions)

# Wireless PAN: Bluetooth or IEEE 802.15.1

Radio interface (2.4 GHz band) used for the connection and communications of wireless devices

- Designed as ***technology for cable replacement***
- *It could (?) be* used for ***multi-hop communications in ad hoc networks***
  - Short-range: 10-100 m
  - "Traditional" peek datarate: 1 Mbps
- ***Low cost***: goal was $5-$10 per interface at the proposal (widely achieved and passed nowadays)
- Manages both voice and data



# Bluetooth

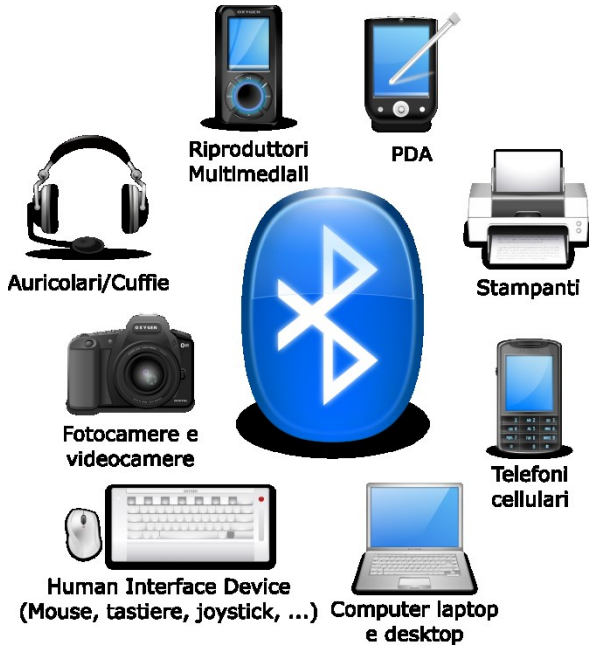
***Bluetooth*** was born in 1998 from the alliance of IBM, Ericsson, Intel, Nokia, and Toshiba (***Bluetooth SIG***)

Objective: to design and implement a short-range radio communication system, based on small-size and low-cost components

- Bluetooth SIG defined the specifications of a set of ***protocols*** for radio communications and the associated ***software stack***
- In addition to basic specifications, also definition of ***profiles that describe how to use the protocols by guaranteeing intercommunication between het devices***

# Bluetooth

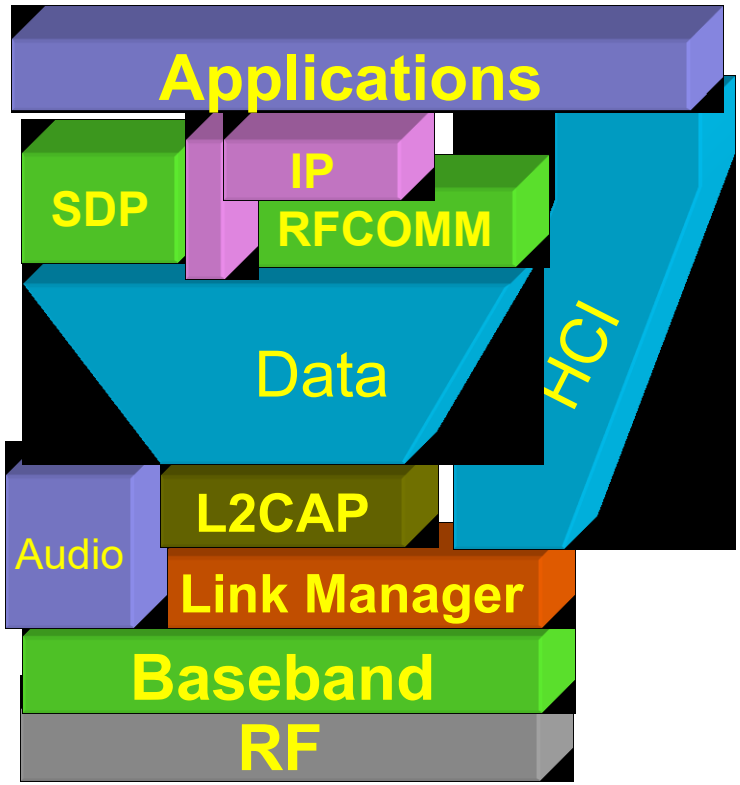
- 2.4 GHz communications (same band of IEEE 802.11) in frequency hopping
- Initial theoretical bandwidth of 1306 kb/s (v2.0 + EDR)
- Consumed power: 1mW–10 mW
- Piconet: network topology with one master and 7 slaves at maximum
- Scatternet




Differences wrt infrastructured IEEE 802.11:

- ***Point-to-point communications*** (between master and slaves)
- Needs ***discovery*** of devices and services
- ***Very limited broadcast mechanism***

# Protocols Stack (articulated…)




- Radio, Baseband, and Link Manager are usually ***implemented in firmware***
  - ***The higher layers usually in software***
  - Which tradeoff between implementations at different layers?
- Applications interact with firmware via ***Host Controller Interface (HCI)***
  - Defined and supported interfaces: RS232, USB, PC Card

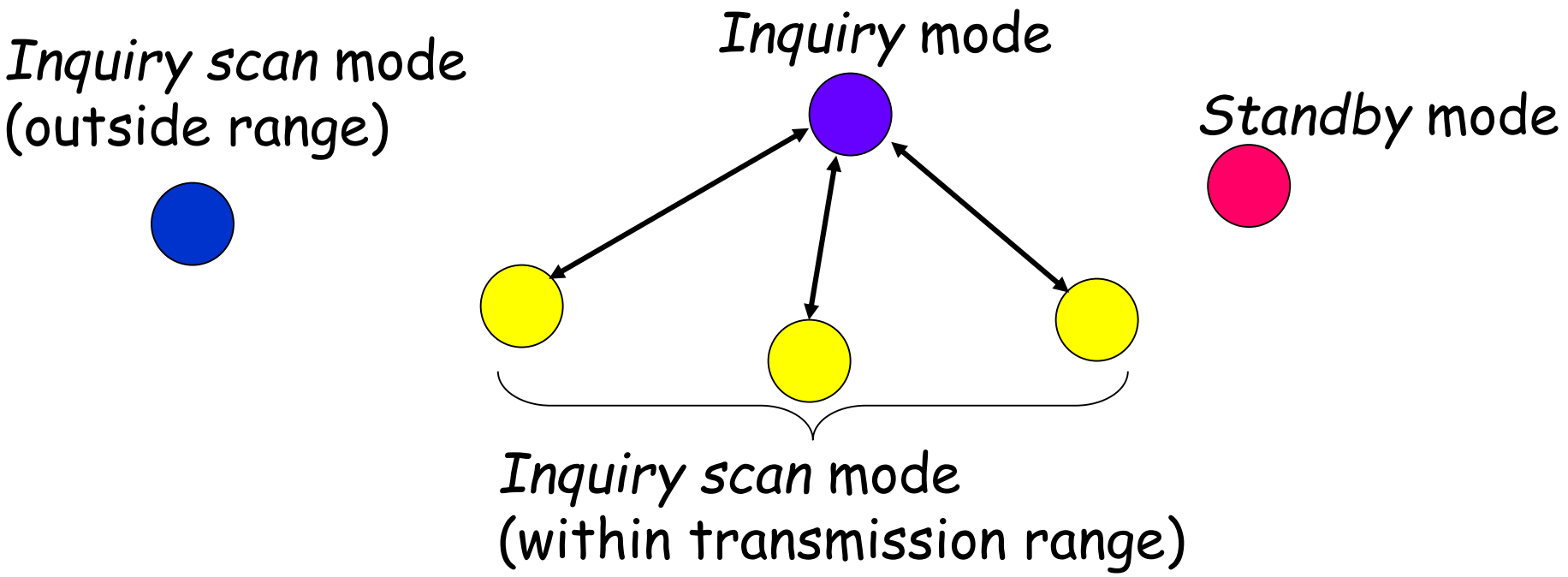
# Topology Formation

- Bluetooth specifies a protocol for the ***construction of the current topology*** implemented at the baseband layer
  1. ***Inquiry phase***: a node in need of communication performs the ***discovery of nearby nodes*** (within its transmission range)
     - ***Who starts the protocol*** becomes the ***master***, discovered nodes play the role of ***slaves***
  2. ***Page/paging phase***: master establishes a ***bidirectional communication channel (frequency hopping)*** with its slaves

- ***Piconet is the base topology unit*** for Bluetooth
  - One master
  - Up to 7 active slaves (up to 256 slaves in parked state)
  - Single channel in frequency hopping

# Inquiry Phase

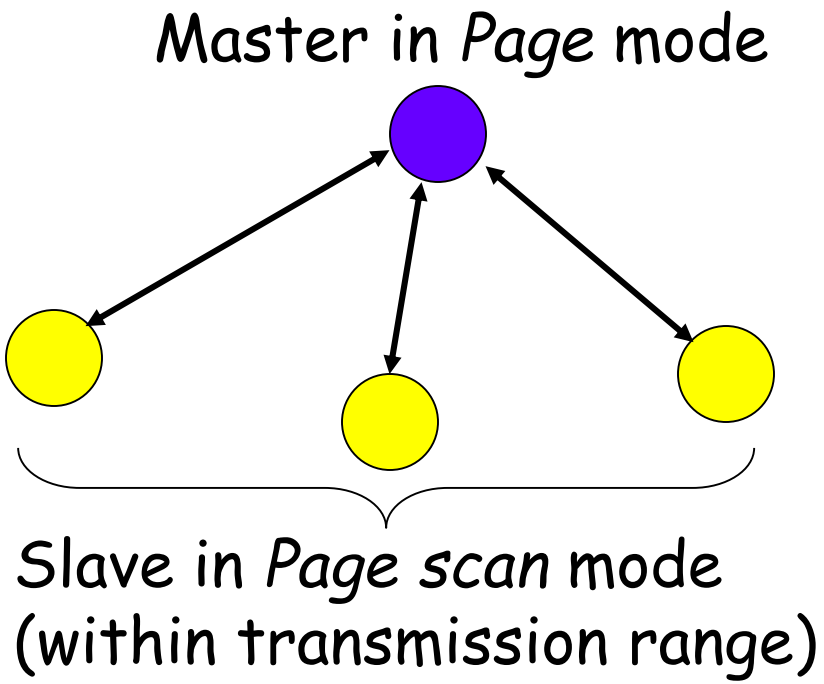
***Goal***: ***to collect sufficient info*** on neighbor nodes in order to ***establish a piconet***



# Inquiry Phase

- Nodes that ***need to communicate*** enter the ***Inquiry mode state***
  - They transmit their short ID (Inquiry Access Code – IAC)
  - They wait for replies from neighbors
- To save energy, ***other devices can alternate Inquiry Scan mode and Standby mode***
  - Inquiry Scan = listening to communication requests
    - Nodes reply when necessary
- After a given time interval, ***master enters the Page phase provided that it has received at least one reply***

# Page Phase

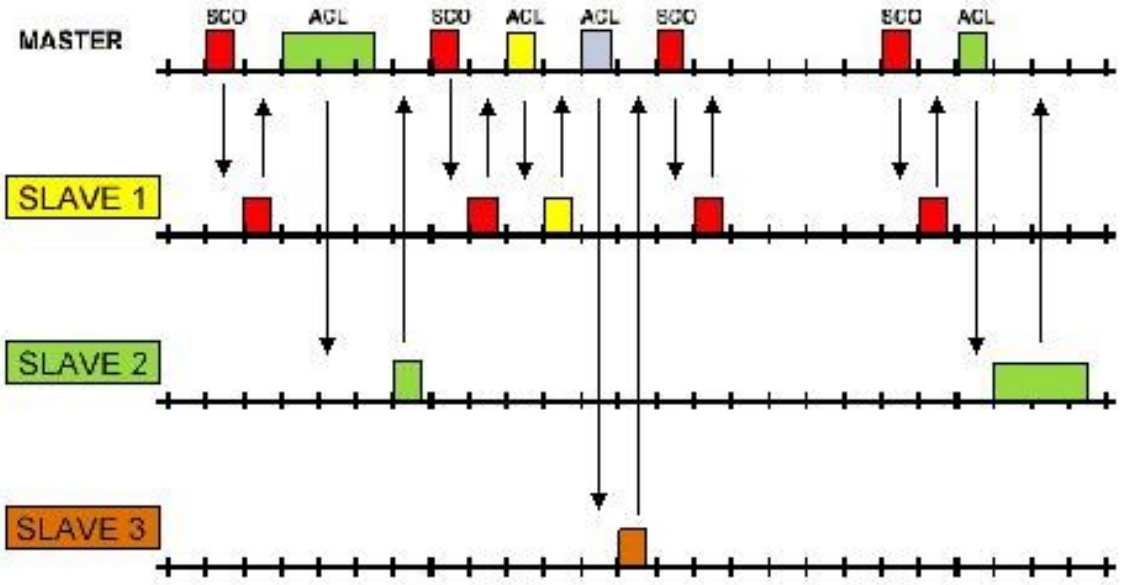



- Master knows the ***value of the estimated clock and BT_ADDR per each slave***
- Master performs ***broadcast of packets with ID***
- When a slave replies, ***master and slave go on with the exchange*** of the info needed to establish connection
- ***Piconet communications are typically connection-oriented***

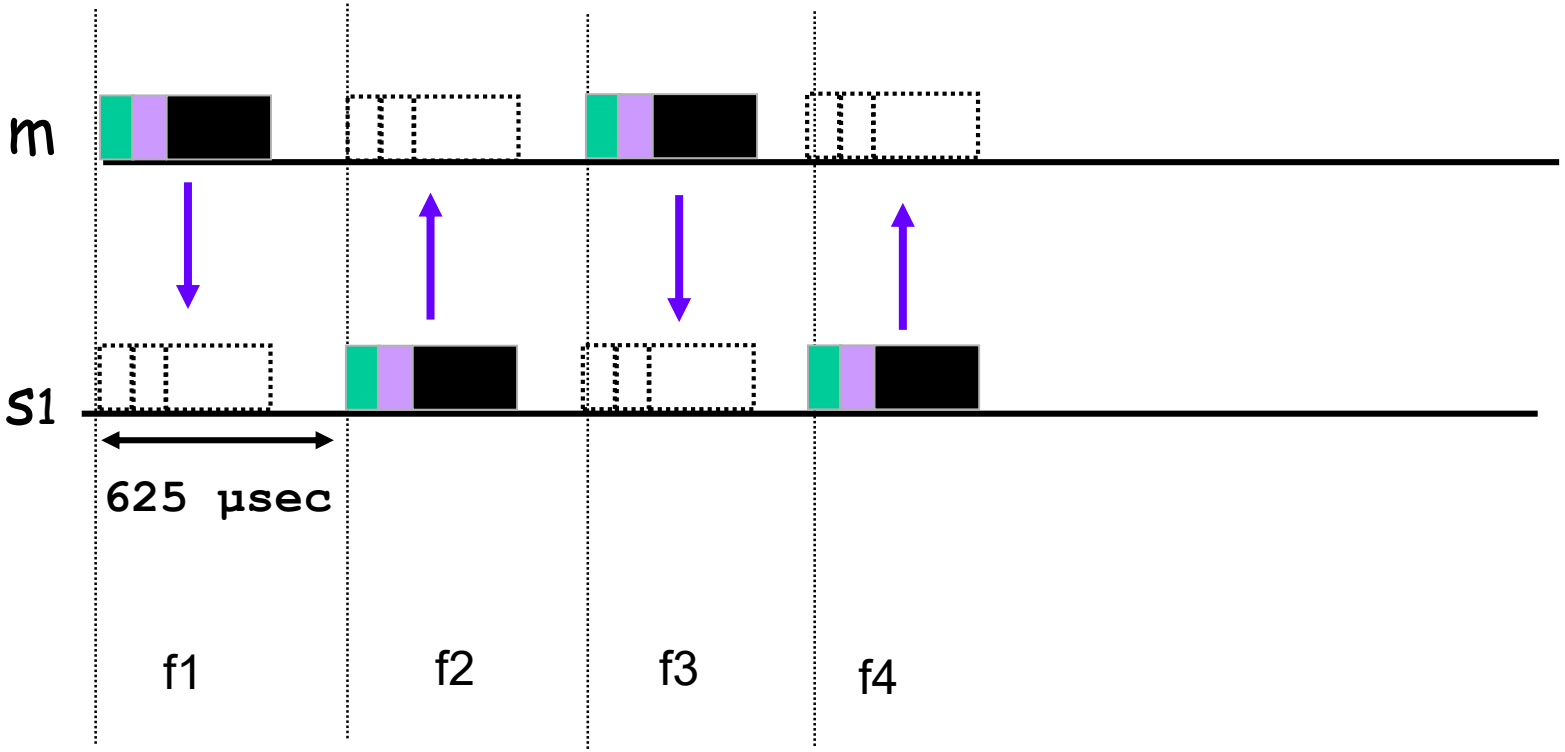
# Bluetooth: Frequency Hopping

***Bluetooth exploits frequency hopping in 2.4 GHz ISM band*** (79 hop frequencies at 1 MHz distance). ***Hopping sequence is determined based on the master address; all devices in the piconet HAVE to follow the same sequence***

- Master ***communicates with each slave (rounds)*** in a periodical way
  Time is split into 625us slots
  Master transmits at the beginning of odd slots, slaves at the beginning of even slots. ***Need for synch at the piconet level***



# Piconet Communications




- ***Channel is split into time slots*** – each one of 625µs
- Time Division Duplex: master and its slaves ***alternate in transmitting/listening***

# Bluetooth: Timing and Clock

Bluetooth synchronizes most of its operations with ***clock signal in real time***. For instance, to synch data exchange between devices, to determine which packets are re-transmitted or lost, to generate a pseudo-random sequence that is predictable and reproducible
Bluetooth clock is implemented via a counter (28 bit) that is set to 0 when switching on the device and that increments every 312.5 μs (half slot)

- Any Bluetooth device has its own native clock (CLKN)
- CLK: ***piconet clock, coincides with the CLKN of the piconet master***. All piconet nodes HAVE to synch their CLKN with CLK
- CLKE: also this clock derives from CLKN through *offset*; it is used by the *master* in the case of creation of a connection to a new slave, before that the *slave* is synch-ed with the *master*

A ***master transmission always start when CLK[1:0] = 00 (odd indexed slots)***, while a slave transmission starts always when CLK[1:0] = 10 (even indexed slot)

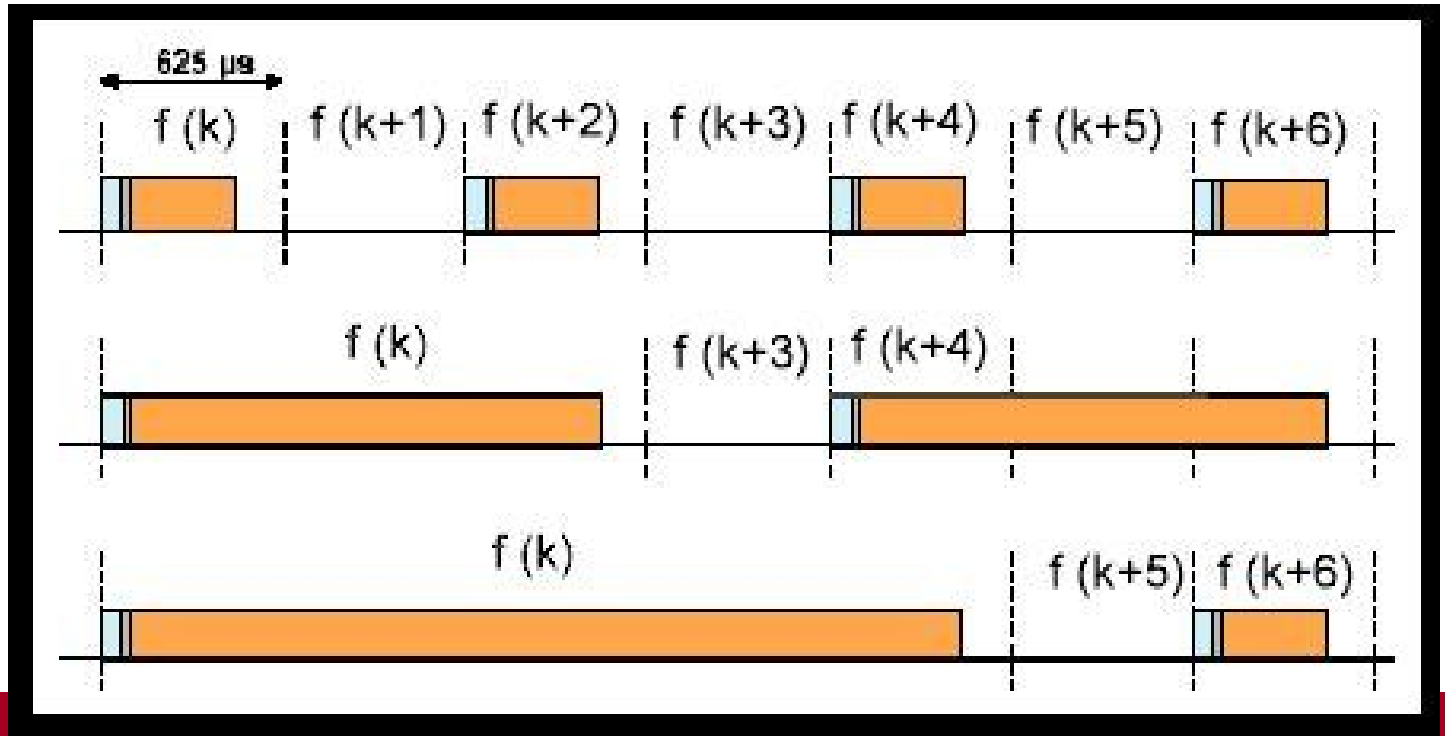
# Bluetooth: Connection Types

Bluetooth connections can be of two types: ***connection-oriented and connectionless***, designed for the support of voice applications and data transfer: asynch service with no connection ***(ACL, Asynchronous ConnectionLess)*** and synch service oriented to connections ***(SCO, Synchronous Connection Oriented)***

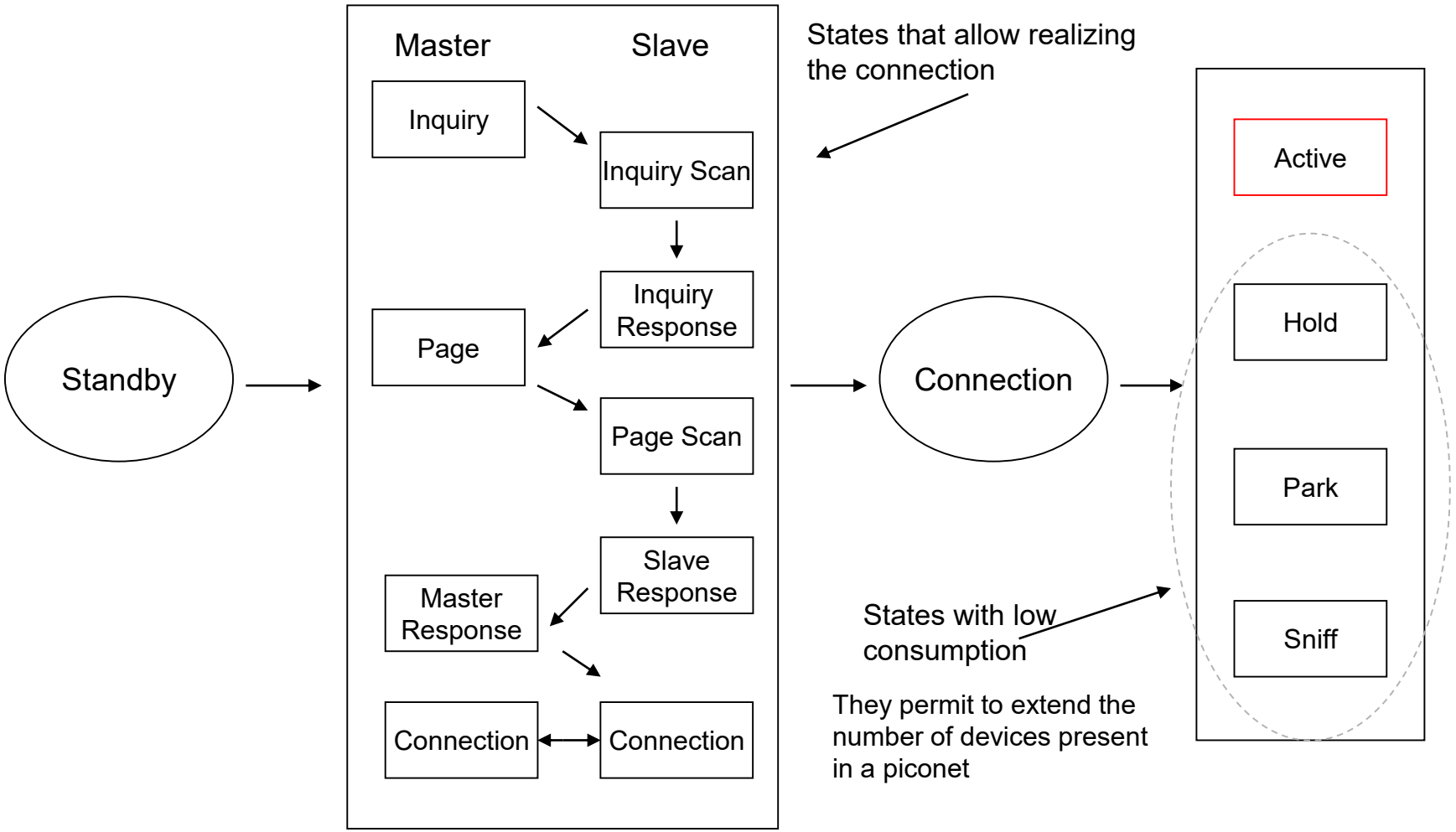
- ***ACL, data traffic and best-effort service***
  ACL supports packet-switched, point-multipoint, and symmetric/asymmetric connections. Symmetric connections with maximum datarate of 433.9 kbit/s, asymmetric connections 723.2/57.6 kbit/s; a ***slave can transmit only if in the previous slot it received a packet by the master***
- ***SCO, connections with real-time and multimedia traffic***
  Circuit-switched, point-point, symmetric connections, voice transportation in 64 kbit/s channels, usually; *master* can support up to 3 SCO connections towards the same *slave* or different *slaves* in the same piconet
  ***no re-transmission in the case of errors or losses (why?)***

# Bluetooth: Frequency Hopping

- In SCO connections, channel “reserved” for 2 time slots for communications between the master and one specific slave ***Slot reservation periodicity is decided by the master (similar to circuit switching)***; time slots are allocated independently by the need of transmission
- ACL transmissions may occur in ***pause intervals between SCO reserved slots***



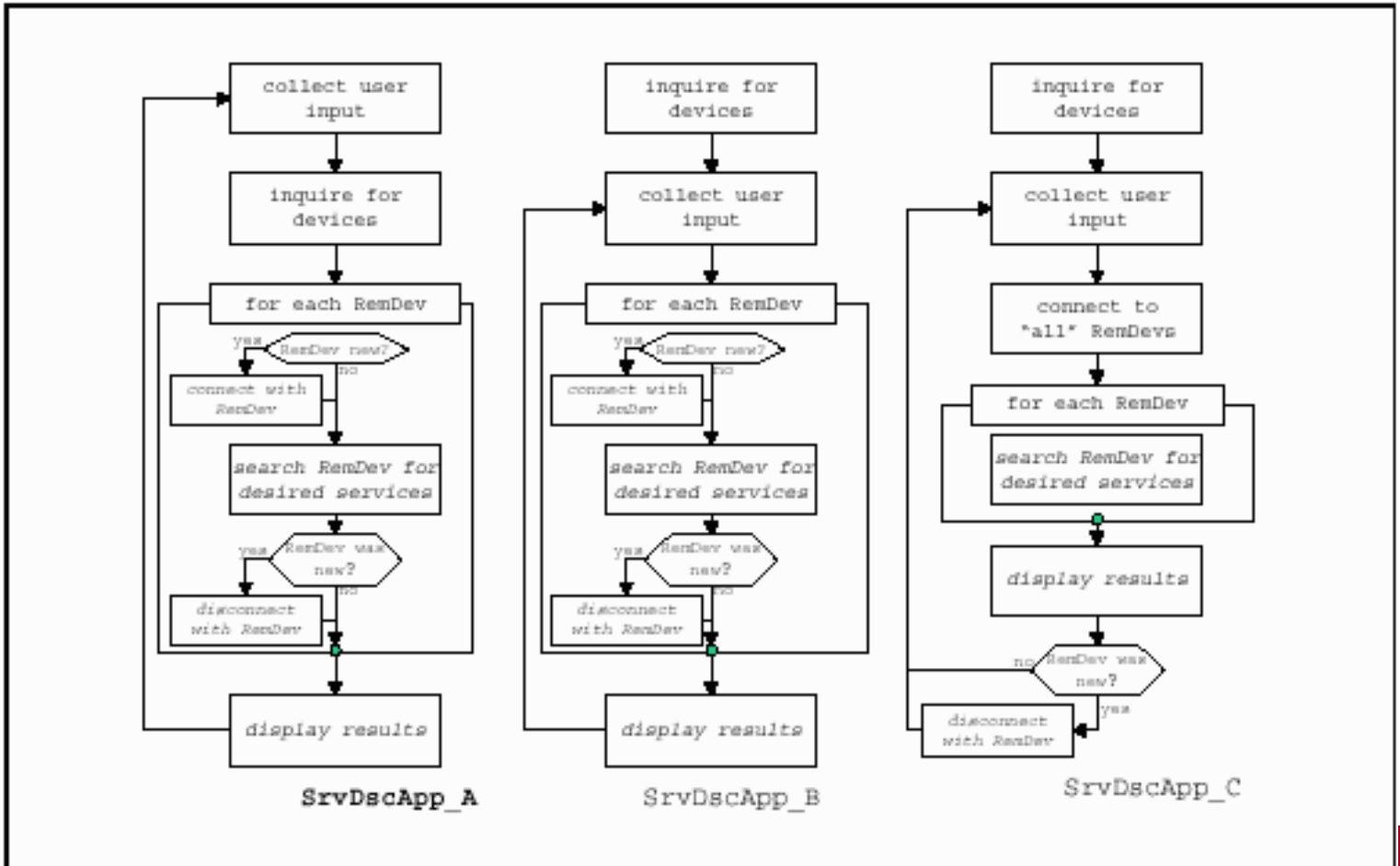
# Device States



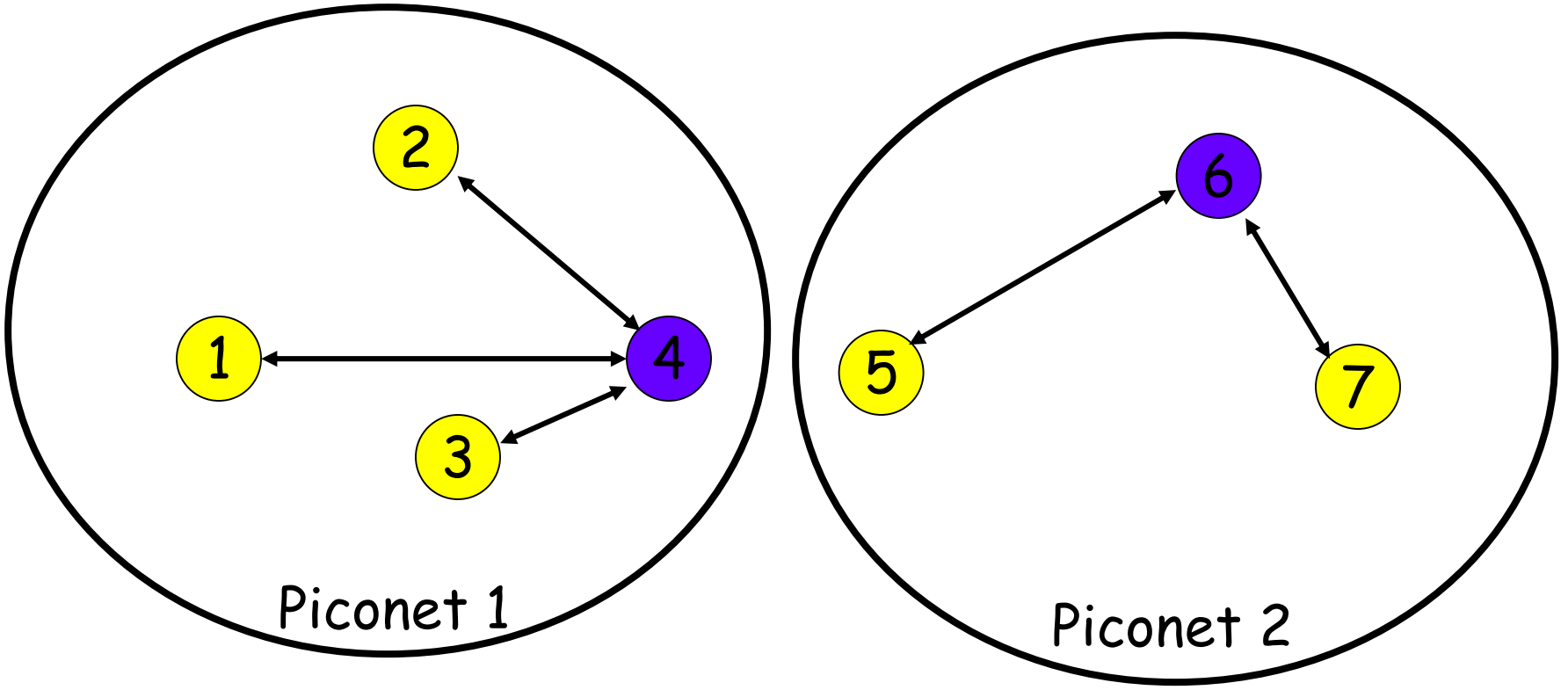
Also need to go up in the abstraction layer:

# Service Discovery Protocol (SDP)

- To discover available devices and services, Bluetooth applications exploit ***Service Discovery Protocol***
- Any server keeps updated its database, available for clients, including the ***service records related to the offered services***



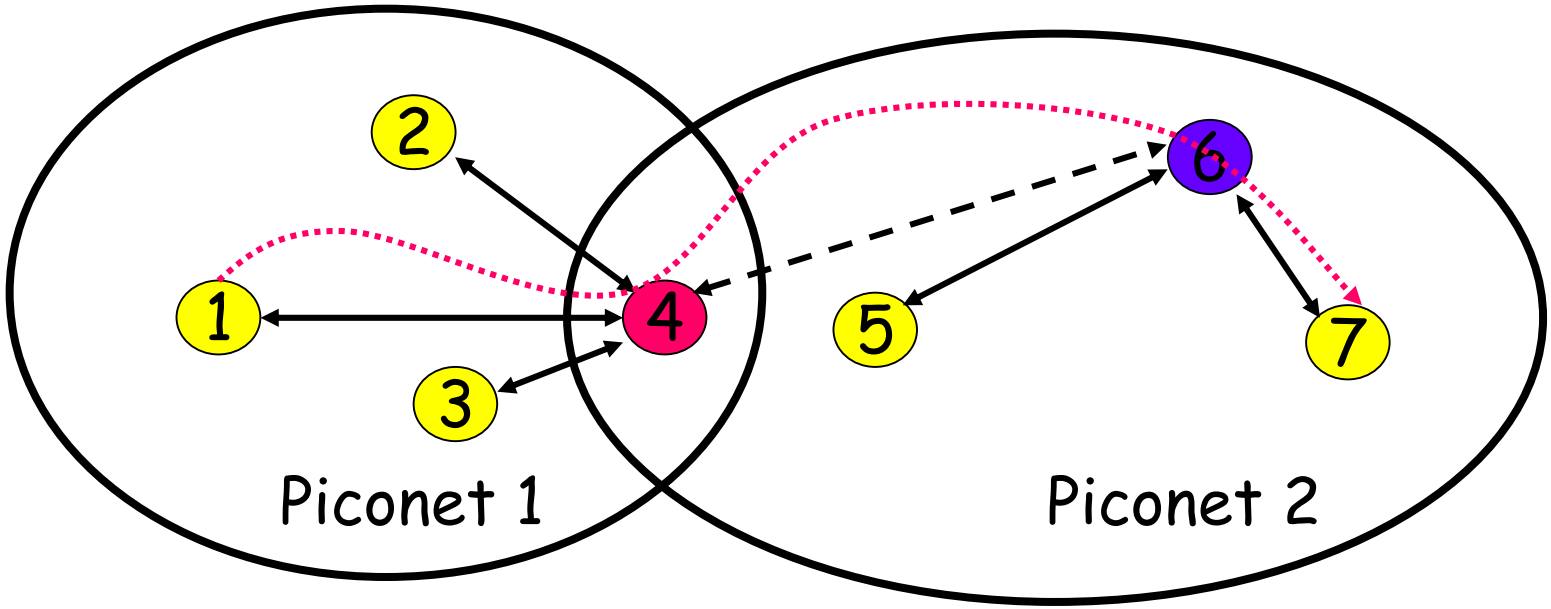
# Does Bluetooth Support Multi-Hop Communications?




For instance, how can node1 communicate with node7 if the node distance is greater than their transmission range?

# Bluetooth Scatternet

- ***Connection of multiple piconets***, in proximity, via the ***sharing of either a common master OR of a common slave***
- A node may be slave in a piconet and master in another one
  - That node can "move" back and forth between the two piconets
- For a long time, ***no commercial implementation*** available (only a few academic experiments)




- Node4 plays the role of master in Piconet1 and of slave in Piconet2
- A path may be created from node1 to node7 via nodes 4 and 6

# Clashing Issues in Inquiry/Paging


| | Inquiry | Paging |
|---|---|---|
| Typical | 5.12 *s* | 0.64 *s* |
| Max | 15.36 *s* | 7.38 *s* |

- The maximum values are measured when ***multiple devices***, within the transmission range of each other, ***enter in Inquiry/Paging mode in the same interval***

# Bluetooth Low Energy (BLE)

Just to complete the overview…

- Compared to Classic Bluetooth, Bluetooth Smart (or BLE) is intended to provide ***considerably reduced power consumption and cost while maintaining a similar communication range***
- Originally introduced under the name Wibree by Nokia in 2006; merged into the main Bluetooth standard in 2010 with the adoption of the Bluetooth Core Specification Version 4.0

The Bluetooth SIG predicts that by 2018 more than 90% Bluetooth-enabled smartphones will support Bluetooth Smart

- BLE operates in the same spectrum range as Classic Bluetooth, but with a different set of channels (40 2-MHz channels). Within a channel, data is transmitted using Gaussian frequency shift modulation. Bitrate is 1 Mbit/s, and the maximum transmit power is 10 mW

# Bluetooth Low Energy (BLE)

- BLE uses ***frequency hopping*** to counteract narrowband interference problems. Classic Bluetooth also uses frequency hopping but the details are different

- ***Advertising and discovery***

  BLE devices are detected through a process based on ***broadcast advertising packets***. This is done using 3 separate channels (frequencies), in order to avoid interference
  Both the advertising devices, and the scanners looking for those devices, step through the three channels in sequence
  only about a 1 in 9 chance of a scanner detecting a particular device's advertisement
  time to discover devices highly variable and long

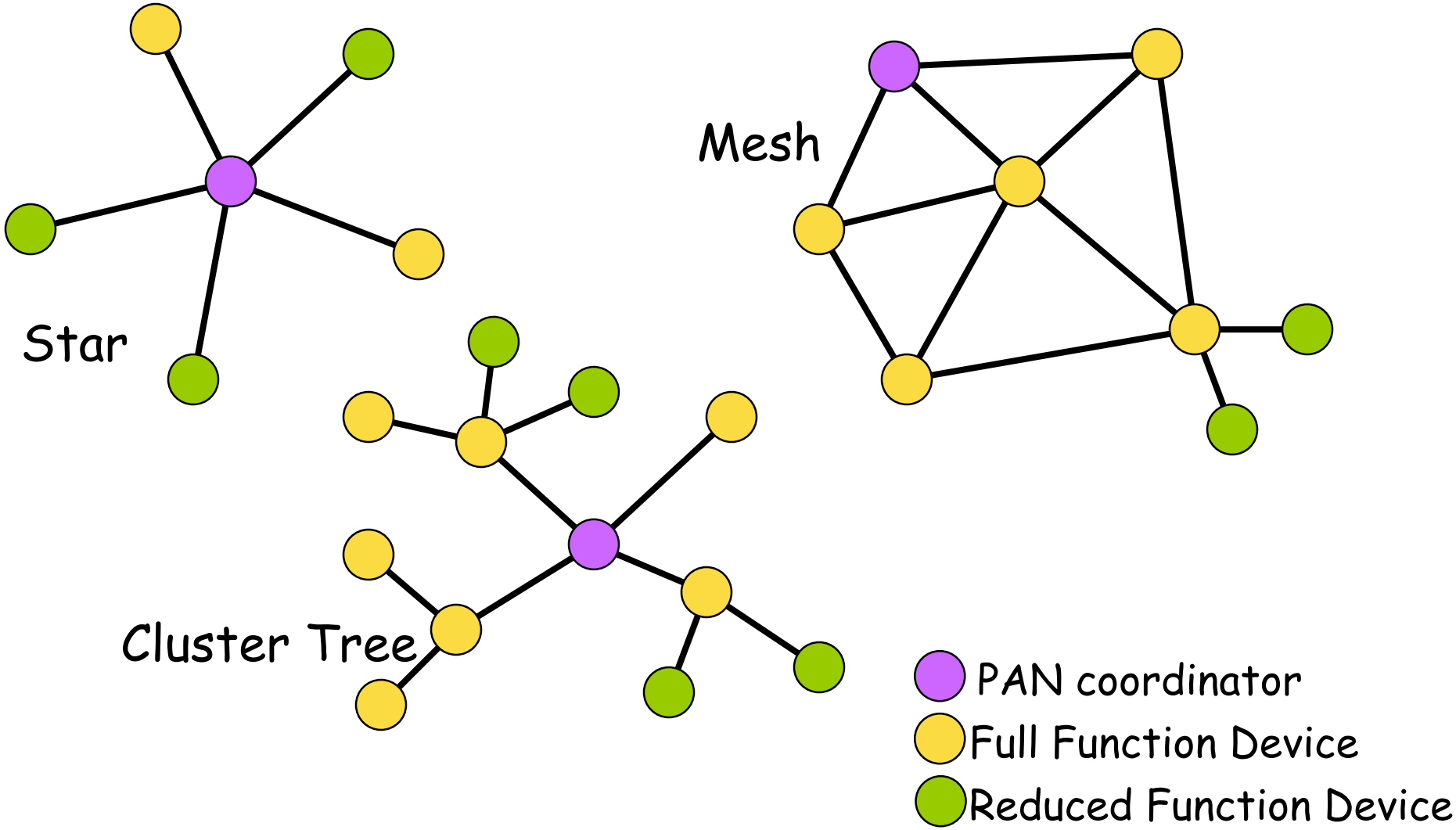
- ***Software model***

  All Bluetooth Smart devices use the Generic Attribute Profile (GATT)

# Wireless PAN: ZigBee or IEEE 802.15.4

- This standard is specifically designed for ***sensors and actuators networks*** with reliability, cost-effectiveness, and ***low power*** requirements
- Applications:
  - Control of home appliances
  - Automation and control of large buildings and industrial plants
  - Monitoring of patients and elders, in particular at homes
  - Environmental monitoring
  - War applications and homeland security
- As Bluetooth, ZigBee provides ***profiles*** for higher layers of the support/application stack
- Up to 65536 nodes (clients) in a network
- Optimized for time-critical apps and for limited power consumption
  - Join < 30ms; state change from sleep to active < 15ms
- Support to ***full mesh networking***

# ZigBee Topologies



# Types of Roles and Channel Access Options

- Different types of roles for ZigBee devices
  - ***Coordinator*** (one and only one for each ZigBee network)
    - Starts ***the network formation***
    - Can serve as ***router*** once the network is operating
  - ***"Full" device***
    - ***Participates to message routing***
  - ***Device with limited features/functions***
    - Only sensing and actuating operations, no routing
- Options for channel access
  - ***Non-beaconed network***
    - Exploits CSMA-CA, almost the same way as already described
    - Positive acks for successful reception of packets
  - ***Beacon-enabled network***
    - Coordinator transmits ***beacons at regular time intervals***
    - Dedicated bandwidth and low latency
    - Low power mode also for the coordinator