Notes for the course Mobile Systems M held by professor Paolo Bellavista, at Alma Mater Studiorum - University of Bologna. Edited by Michele Righi.

Index

Chapter 0 - Introduction

IP addresses assignment: IANA (Internet Assigned Numbers Authority) is responsible for thhe global coordination of IP addresses allocations.

Standard procedure: IANA -> RIRs (Regional Internet Registries) -> ISP (Internet Service Providers) -> my device that needs an IP address.

However, there is the concept of "Non-coordinated IP addressing spaces": IP addresses allocations that are not centrally managed or coordinated by a central standard authority (IANA for the Internet).

Bandwidth (measured in multiple of bps - bits per second): *theoretical* maximum capacity of a network or communication channel;
Throughput (measured in multiple of bps): *actual* amount of data thata can be successfully transmitted over a network or communication channel, in real-world conditions.

Mobile devices are expected to move in most cases, and that has many consequences.

Chapter 1 - Wireless (ISO/OSI Layer 2)

When dealing with mobile systems, the nodes are almost always connected through a wireless connectivity medium.

One of the main differencies from the wired connections, is that in wired ones (e.g. Ethernet) the signal cannot be lost before being received, due to its distance (at least in local networks, it can happen in bigger ones). Generally speaking, that's due to the fact that after X length, there's something that regenerates the signal.

What's for sure, is that in cabled connections, there are NEVER propagation problems.
On the contrary, in wireless communication, you'll always (more or less) have propagation problems: the signal power decreases in space moving further away, at least directly, since you can always repeat the signal.

When you're too far from an AP (Access Point) you'll not be able to associate to it anymore and you have to move near or change it.

Wireless Propagation Models

The signal decreases while traveling along distances, and that physical behaviour is described by Maxwell's laws.

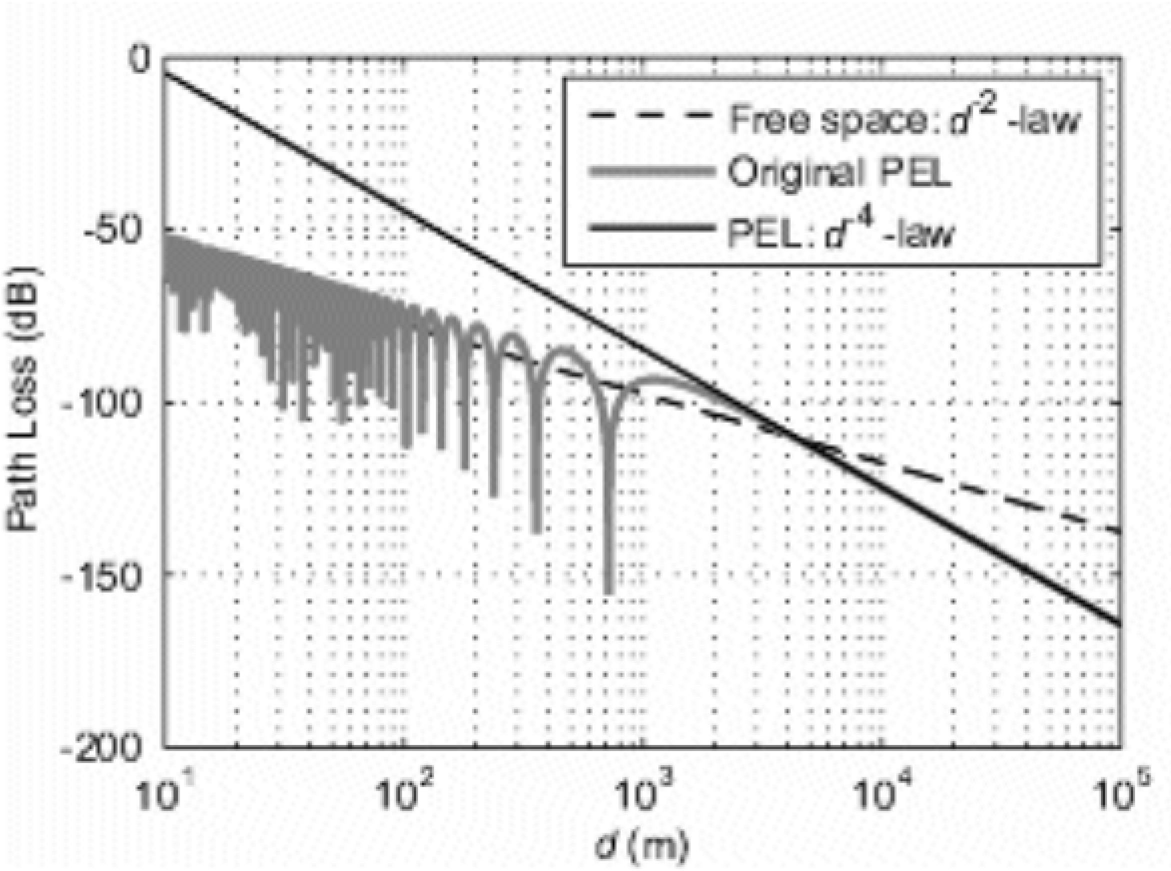
Wireless propagation models are mathematical representations used to describe how radio frequency (RF) signals travel and **attenuate as they propagate** through air and other mediums. Those help researchers and engineers understand and predict the behaviour of wireless communication systems.

Signal Propagation Losses

There are some kind of losses in power received (Pr) by the receiver, from the transmitter. In fact, two important concepts in **wireless propagation** are the following, related to Maxwell's equations:

- **Free-space loss** (~path loss), `Pr(d) ~ Pt * Gt * Gr (λ / 4 Π d)² is the reduction in signal strenght, as a radio wave travels through free space **without any obstacles** or reflections. 2 times inversely proportional to distance (` d^{2}`).
  NB: it increases with distance and frequency
- **Plane earth loss** (~groud reflection loss), `Pr(d) ~ Pt * Gt * Gr (ht * hr / d² )² is **due to Earth's curvature** and affects signals that travel along its surface. Earth is a "curve reflector". 4 times inversely proportional to distance (` d^{4}`).
  NB: it impacts the coverage area of a wireless system, especially when direct line-of-sight communication is not possible.

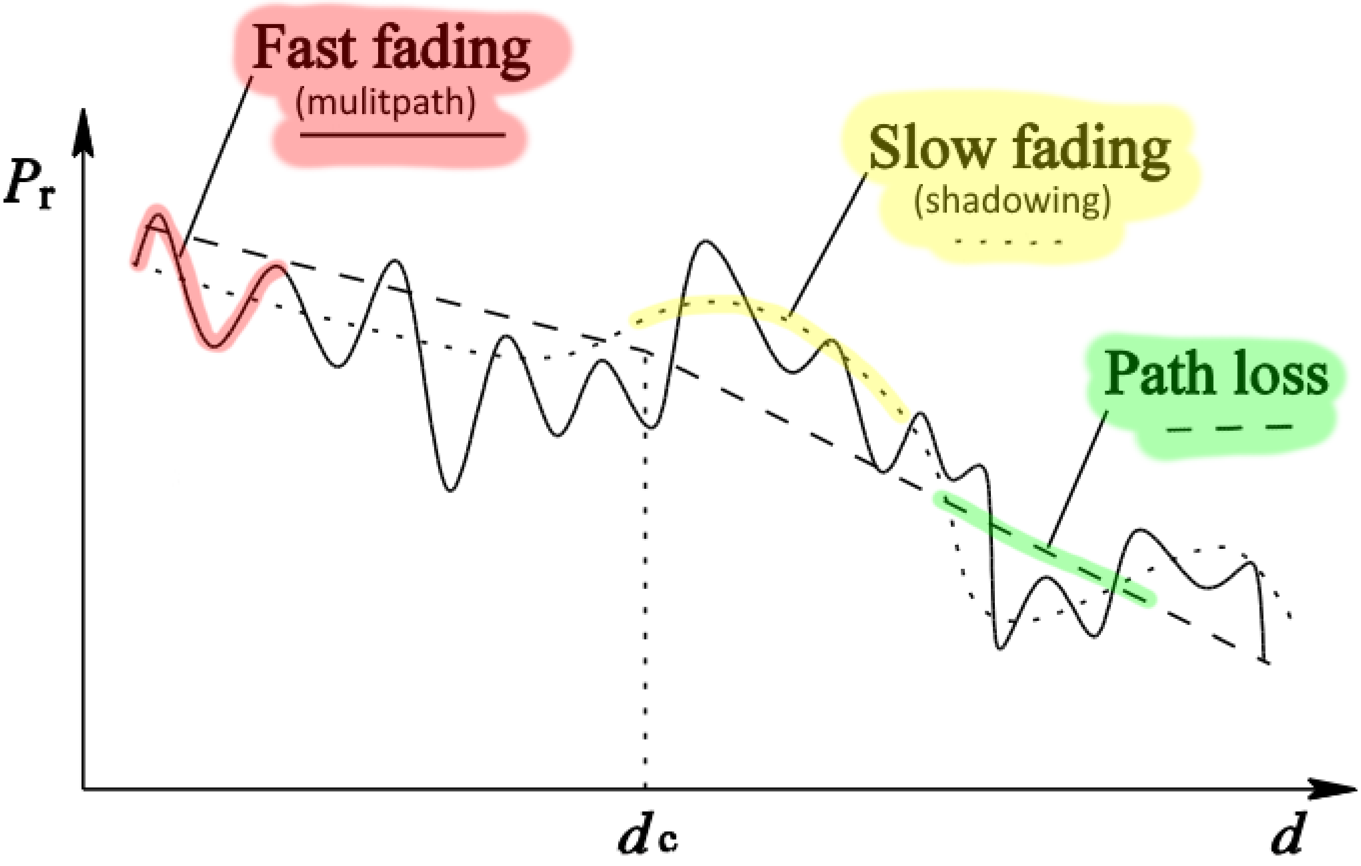
In real life scenarios, the signal tends to be a fluctuation influenced by both of these two laws (which can be thought of as 2 straight lines):



Channel Fading Models

The signal is also influenced by physical phenomena that affects its propagation. The most relevant and dominant ones are shadowing, Raileigh fading, and frequency-selective fading.

NB: large-scale VS small-scale fading. Slow fading implies that the changes in signal strength occur over larger distances or longer periods, making them more predictable and manageable.



The combination of all these effects produces the so called `Pr` which is the Power Received, which usually fluctuates depending on the distance.

Shadowing

Occurs when the signal encounters **obstacles** along its path, causing **long-term strenght variations**.
Also called slow-fading, refers to the long-term variations in signal strenght caused by obstacles and environmental features in the propagation path. It's a type of large-scale or "slow" fading phenomenon that affects the received signal strength, leading to signal fluctuations over distance and time. It's caused by the partial/total absorption and partia/total reflection due to objects (trees, buildings, mobile vehicles, ...) and causes a decrease of the received power strength in a wide spectrum of frequencies. This kind of fading can be calculated for smaller objects, but usually, under a mathematical point of view, we tend to refer to pdf (probability distribution functions): considerations about shadowing usually lead to approximations of the probability of being in the coverage area of the signal.

Multipath Rayleigh Fading

Occurs when the signal reaches the receiver through **multiple paths**, causing **rapid oscillations** in signal strength (constructive/destructive interferences).
It's a type of fast-fading/small-scale fading. When traveling, usually an electromagnetic signal

never go through one single path, but gets scattered many times and what is received is the sum of the "bits" of signal that reaches it, coming from multiple different paths.

Frequency-Selective Fading

Different frequency components of the signal experience varying levels of fading, causing **frequency-dependent strength variations**.
It's a kind of fading similiar to shadowing, that happens when the signal travels through a channel with varying characteristics across its frequency spectrum (for example there could be some obstacles that interfere more at lower frequencies, and cause the signal propagation to fade the most, while at higher frequencies that's not an issue).

Other Effects

Scattering due to rough surfaces; rain-associated attenuation; gas-associated attenuation; ...

Wireless Space

Many heterogeneous wireless connectivity technologies (we'll continue having them in future and the set will expand). They usually classify based on different elements:

- **Coverage rage**, the distance up to which the signal can be transmitted using that kind of technology (the more the better);
- **Data rate**, the largest bandwidth reachable using that technology;
- **Energy consumption**, since battery is also important in mobile devices;
- **Economic cost**;

Typically the variation of one aspect impacts on the others, and that's why the research will keep going on (because it's impossible to reach the perfect value for each parameter). For example, an increase in data rate is obtained through an increase in frequency, but that leads to a physical signal that gets more easily absorbed by surrounding objects and therefore the coverage decreases.

Communication Standards

IEEE 802.x standards defines physical layer and dataling layer protocols.

OSI model	802.3 (Ethernet)	802.5 (Token Ring)	802.11 (Wi-Fi)
Data Link Layer (2)			
Physical Layer (1)	CSMA/CD bus	token-passing ring	CSMA radio

Ethernet (IEEE 802.3)

Ethernet (IEEE 802.3) is based on CSMA/CD (Carrier Sense Multiple Access with Collision Detection ~ *il portatore del segnale percepisce gli accessi multipli con rilevamento delle collisioni*) algorithm. It's an **optimistic approach**, that allows multiple access (MA), i.e. allows multiple devices to share the same communication medium:

- performs **channel sensing** (CS), to detect if someone is already using it:
    - if not (idle), transmit immediately, but keep listening to the channel;
    - otherwise (occupied), wait until the channel becomes idle;
- **collision detection** (CD):
  - immediate abortion of a transmission if collision is detected;
  - the following transmission try will occur after waiting for a **random time interval**.
  - **exponential backoff**: the backoff time is chosen in an interval that grows exponentially over time, to minimize the probability of **repeated collisions**.
  The exponential backoff and randomization prevents the device backoff synchronization (that is when devices keep trying to retransmit at the same interval of time).

NB: That's possible due to the transmission medium characteristics in Ethernet (cable), which doesn't cause signal degradation or propagation problems of any kind! We'll see that in wireless it's not so trivial to detect that (due to signal degradation, but also to other factors).

How ethernet works: How ethernet puts packets at layer 2 on the bus trying to avoid collisions (at layer2 the classical problem is if you're using a shared medium transmission - in case of ethernet is the cable, in wifi is the space/air in which the signal travels - where different nodes can decide to transmit packets at the same time)

Wireless LAN (IEEE 802.11)

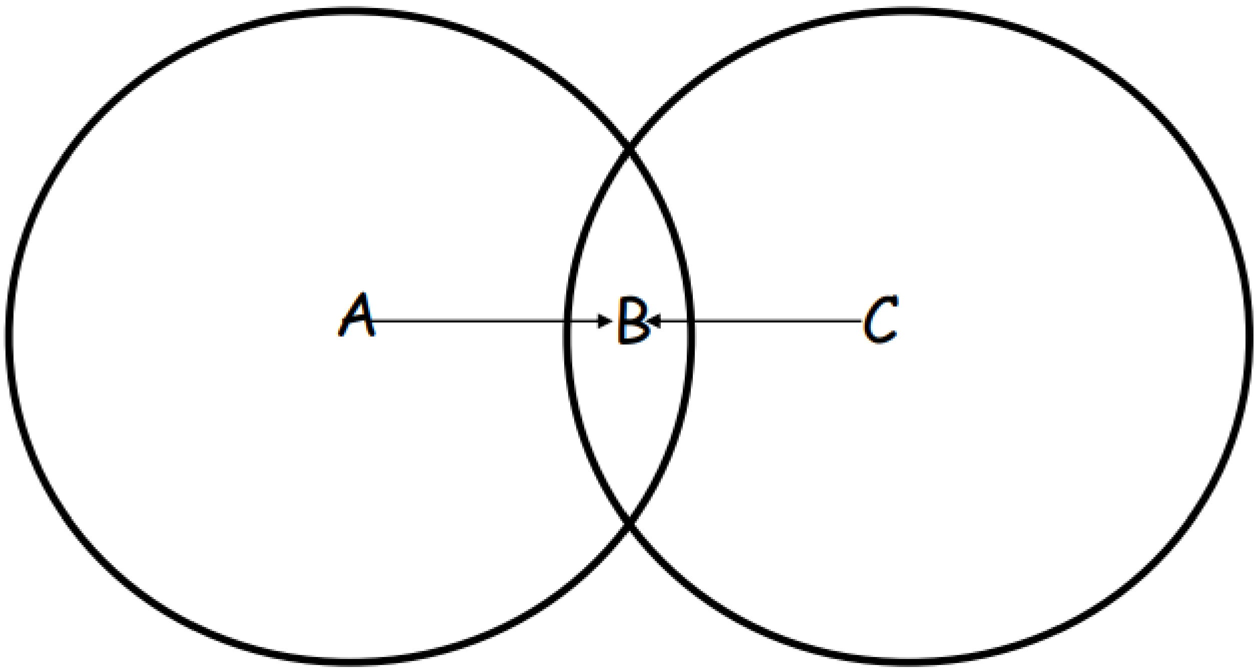
It's the wireless communications for "short-range" (<250m), bandwidth up to 866 Mbps. The standard covers layers 1 and 2, and some security aspects, but doesn't provide any details about Quality of Service.
802.11 is similiar to Ethernet but there are more problems, due to the fact that the cable doesn't degradate the signal, therefore CSMA/CD cannot work correctly:

- collision detection is not always possible nor accurate;
- carrier sensing is not always possible, since not all the nodes are in coverage range;
- mobility considerations;

Wireless LAN Issues

The following problems are 802.11 issues, that doesn't happen in Ethernet.

Hidden Node Issue



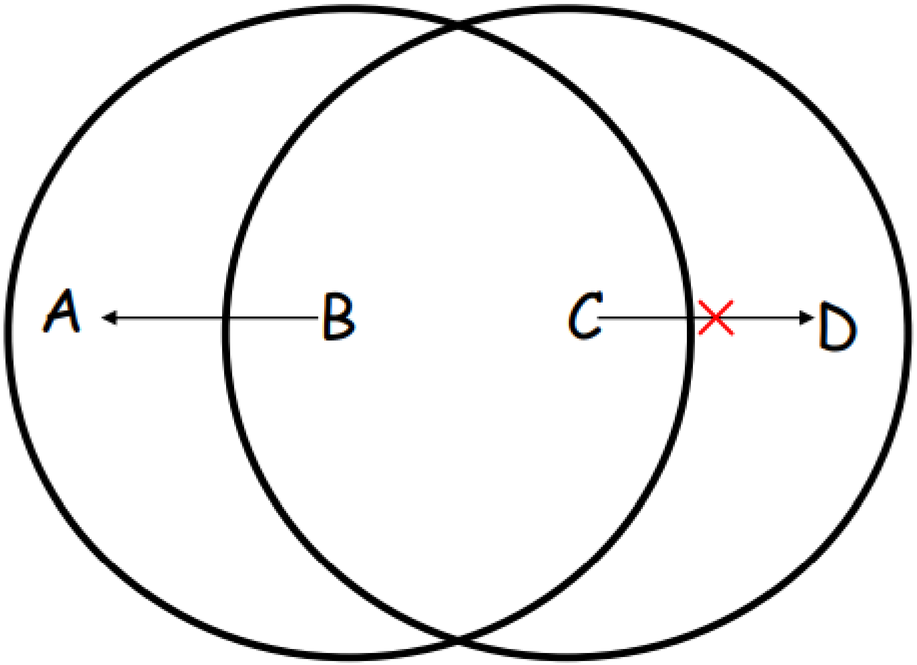
Example:

1. A starts transmittig to B;
2. C cannot be aware of A's communication, because it's out of range, therefore C starts transmitting to B;
3. Collision between the two communication instances;

Occurs when two or more nodes (A and C in the example) are within the range of a central access point AP (B in the example), but they are out of range or unable to sense each other's transmissions.

Is this problem solvable by CSMA? No, but it's not usefull at all.

Exposed Node Issue



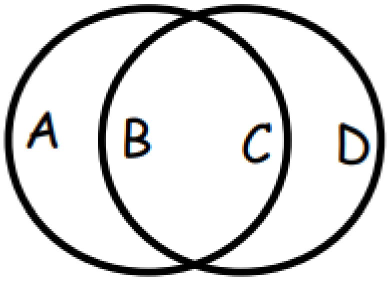
Example:

1. B starts transmitting to A;
2. C detects this transmission and does NOT send any communication towards D;
3. Error: the communication is prevented even if it would not have interfered with A and B.

Occurs when one node refrains from transmitting, even though it could, because it incorrectly believes it might interfere with ongoing communications between other nodes.

Multiple Access Collision Avoidance

To solve hidden node and exposed node issues, CSMA/CD is not suitable. Traditionally it was coupled with an additional algorithm, called **MACA** (Multiple Access with Collision Avoidance).



How does it work? Suppose that B wants to transmit to C;

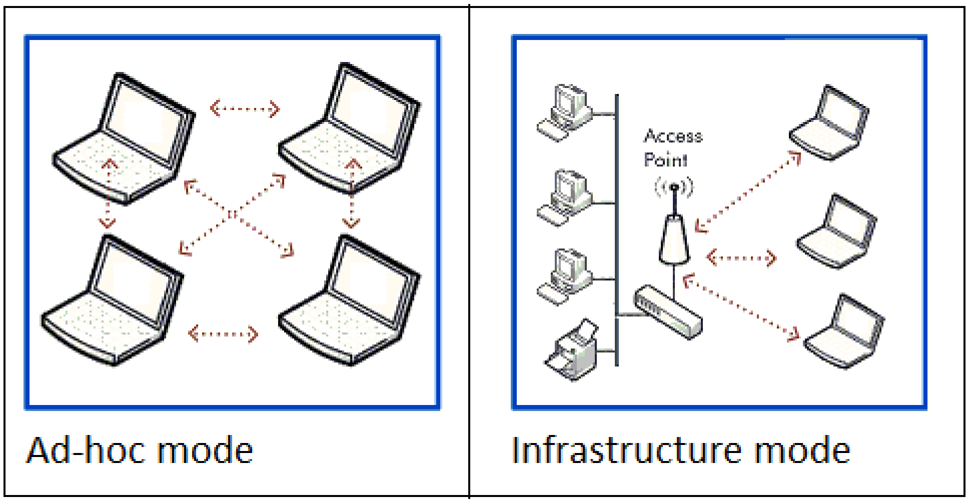
1. B transmits a first RTS (Ready To Send) frame towards C, which includes the length of the message;
2. C replies with a CTS (Clear to Send) frame, that also includes information about the length of the message;

3. other nodes overhear the RTS and have to remain inactive, in silence, for sufficient time to allow C to reply with CTS;
4. other nodes overhear the CTS and remain silent for the whole duration of the transmission.

Collisions may occur anyway (e.g. RTS frame collisions), but at least data frames (which is the important part of the communication) can NOT.

Current situation? WiFi uses CSMA/CA, which basically integrates MACA, but MACA is still left optional. Even if it's not perfect for WiFi, it was adopted because it's simple and therefore allows the usage of more bandwidth.

WiFi (IEEE 802.11) Configurations



There are two primary WiFi configurations:

- **ad-hoc mode**: there are **no access points** between wireless devices and they connect directly;
- **base station** (or infrastructure mode): there is **one AP** that acts like a gateway to reach the Internet and each device connects to it;

In **base station** mode uses the protocol probe/response: a mobile node sends a "probe broadcast message" and Access Points that receive that message respond with a "response message" to signal their presence. Then the mobile node will have a list of available APs to connect to (manually or automatically).
In base station mode, there are no "new" routing problems. Some of the small ones could be:

- what happens if a mobile node moves to another Access Point?
- what happens to our possibility of using the network connection?
  Typically in these 2 scenarios (e.g. when using a service which is continuous in time), the connection must be restarted, because the mobile node changes IP address, when it

connects to a different Access Point. In fact, when changing IP address, in a client/server model, the TCP connection breaks, and it has to be re-enstablished, by building a new one. Sometimes there are middlewares that handle this to improve the user experience, for example Unibo Almawifi automatically detects when a user disconnects from an Access Point and connects to another, and the framework automatically handles this situation.

In **ad-hoc** mode, there is a routing problem that was not present in infrastructure mode (base station): trying to use traditional IP routing (i.e. the one for fixed nodes, often based on Dijkstra's algorithm), it may not always work, but most certainly it's not efficient. A path that might be optimal at a certain time interval t1, might not be optimal anymore at a t2.
Considerations:

- a "scarsly mobile" node could be better to be used as part of the path;
- if a node has low battery probably is not so good to be used, since it might go offline.

WiFi Direct

WiFi Direct (or WiFi P2P) is a sort of **masked "infrastructure mode"**, since it allows 2 nodes to connect directly. However, what actually happens is that one node acts as an Access Point for the other, but it's a **software** implementation.
The interesting aspect is that only one of the two nodes participating in the communication has to be compliant with WiFi Direct standard to enstablish a peer-to-peer connection.

WiMAX (IEEE 802.16)

To cover big areas, WiFi
Goal: grant access to high bandwidth (70Mbps) in metropolitan areas, covering the last mile, since WiFi didn't have enough coverage range (at most 250m). 2 types of stations:

- base stations, installed by Internet Service Providers, and connected via cable to the Internet;
- subscriber stations, installed by users, which acts like modem.

WiFi Mesh (IEEE 802.11s)

WiFi alone cannot be used to cover metropolitan areas. Therefore a variant specific for this task was introduced: IEEE 802.11s, WiFi Mesh, is a WiFi variant that exploits access points (base stations) to create a mesh network. In WiFi mesh, connections can be transfered from one base station to another, granting mobility support.
Pros:

- reduced costs;

- robustness;
  Cons:
- routing complexity;
- implementation difficulties;
- introduced overhead.
  WiFi Mesh didn't have much success, due to the fact that, in order to reach robustness, there was the need to check APs (if one broke for some reason, it would have been necessary to change all the routing paths utilizing the node),

MBWA (IEEE 802.11p)

Mobile Broadband Wireless Access (MBWA) is a standard, which was abandoned quite early, that allowed connections of devices moving at over 250 km/h. WiFi wouldn't allow this, since the association time is too long (several hundreds of ms, compared to 5ms of MBWA).
MBWA didn't have much success, because of WiFi variant IEEE 802.11p.

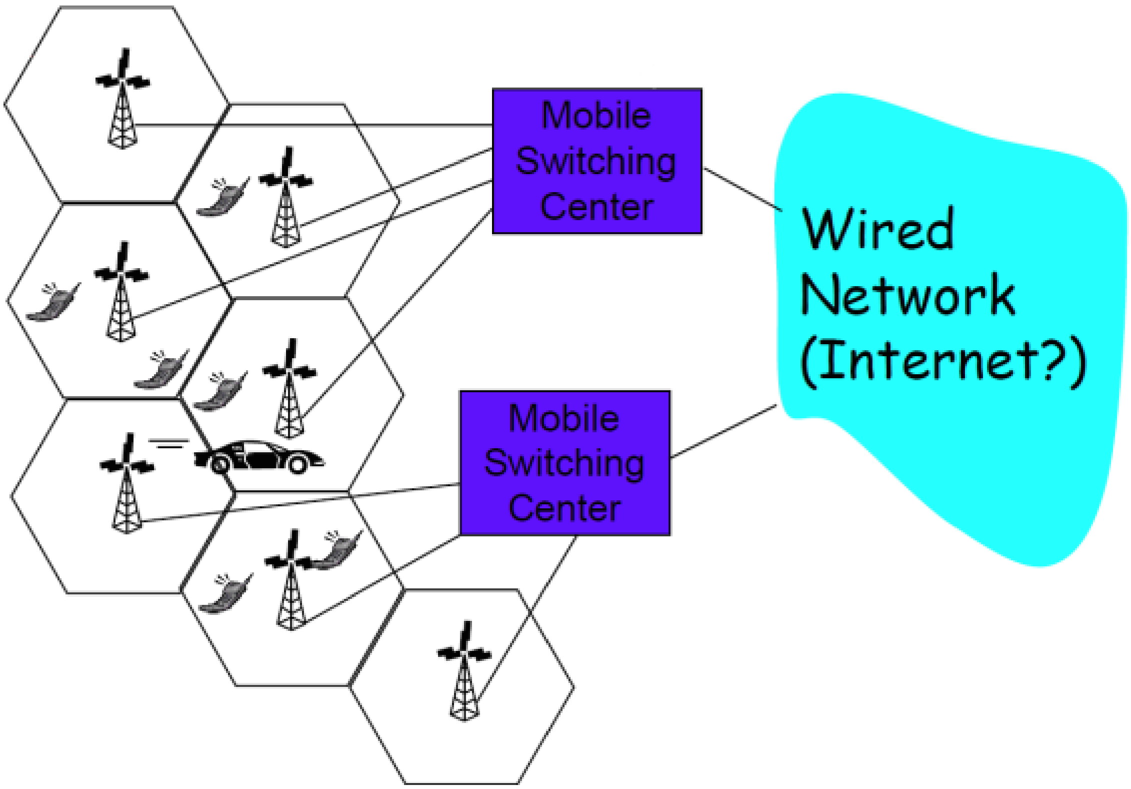
Vehicular Mobility (IEEE 802.11p)

WiFi standard variant proper for vehicular mobility. Includes the exchange of data between vehicles at high velocity and road infrastructures (connected to Internet). This technology is used by some car models.

Cellular Networks

Cellular networks are called this way, due to the implementation concept: geographical areas are divided in adjacent **cells**. Each cell is coveder by an antenna called **Base Station** (BS), as Access Points in base mode.
Each BS is connected to a **Mobile Switching Center** (MSC), that is a fixed station connected

to Internet via cable, that connects cells to the Wide Area Network (WAN).



Suppose we have two nodes A and B, each one referencing a different BSs (BSa and BSb) both belonging to different MSCs (MSCa and MSCb).
A wants to communicate with B, therefore:

1. Node A sends a request to BSa;
2. BSa forwards the message to MSCa;
3. MSCa, passing through Internet, locates MSCb and sends it the message;
4. MSCb forwards the message to BSb;
5. BSb sends the message to node B.

MSCs task is to handle mobility of cellular devices, so that the final user doesn't even notice the cell switching.
Initially it wasn't used Internet, but a proprietary cabled network belonging to telecom companies.

Standard Generations

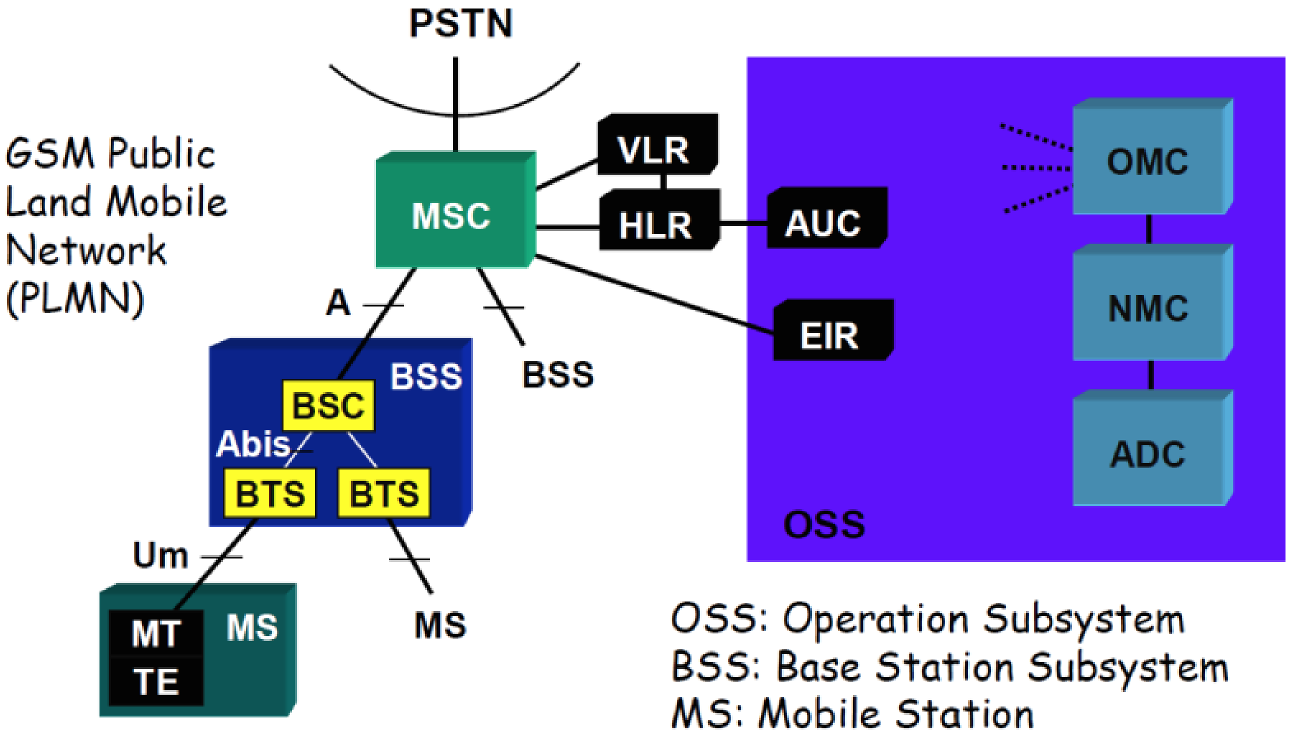
- **1G**, full **analogic** communication (circuit switching);
- **2G**, only **voice channels**, with communication implemented through **digital** circuit switching (NB: before it was analogic). Example: Global System for Mobile

communications (GSM) standard. 2G is the generation where GSM started to gain popularity;

- **2.5G**, channels for **voice and data**. Still relatively ridiculous datarate (384Kbps). Examples:
    - General Packet Radio Service (GPRS) standard, which is an evolution of GSM;
    - Enhanced Data rates for Global Evolution (EDGE), also an evolution of GSM;
- **3G**, channels for **voice and data**. Basically the same as 2.5G but with increased datarate. Reduction of cells size. Example: Universal Mobile Telecommunications Service (UMTS);
- **4G**, channels for **voice and data**. Increased datarate (up to 1000Mbps download, 500Mbps upload). NB: it's interesting noting that typically in wired connections download and upload datarate are the same, but it's up to the protocol designer to specify it (maybe have greater download, since it is the mostly used);
- **5G**

GSM (Global System for Mobile communications)

Global System for Mobile communications (GSM) is a standard developed for mobile communication systems. It's the most widely used standard for mobile phones globally and serves as the foundaton for 2G mobile networks.
GSM architecture is hierarchical and follows locality principle.



A Mobile Station (mobile node, e.g. a smartphone) is composed by:

- one **Terminal Equipment (TE)**, containing terminal/user-specific data (associated with SIM card)
- one **Mobile Terminal (MT)**, that allows to communicate with the BSS.
  A Base Subsystem Station (BSS) is composed by:
- one **Base Station Controller (BSC)**, that manages radio channels, paging and handoff for different BTSs;
- many **Base Transceiver Station (BTS)**, that manages channel allocation, signaling, frequency hopping, handover triggers. BTS contains transceiver that enable them to communicate with MS.

BTS (Base Transceiver Station)

BTS are distributed accross the country and provide coverage to mobile devices.

BSC (Base Station Controller)

BSC are located in centralized sites and manages many BTS.

MSC (Mobile Switching Center)

MSC is used to setup and clear calls and deliver text messages. It also tracks the location of mobile devices under its management.

MSC acts like a **gateway** to:

- **Public Switching Telephone Network (PSTN)**, which is the traditional and circuit-switched network used prior to Internet;
- **packet data networks** (like Internet) which are more recent.

MSC contains 2 registries:

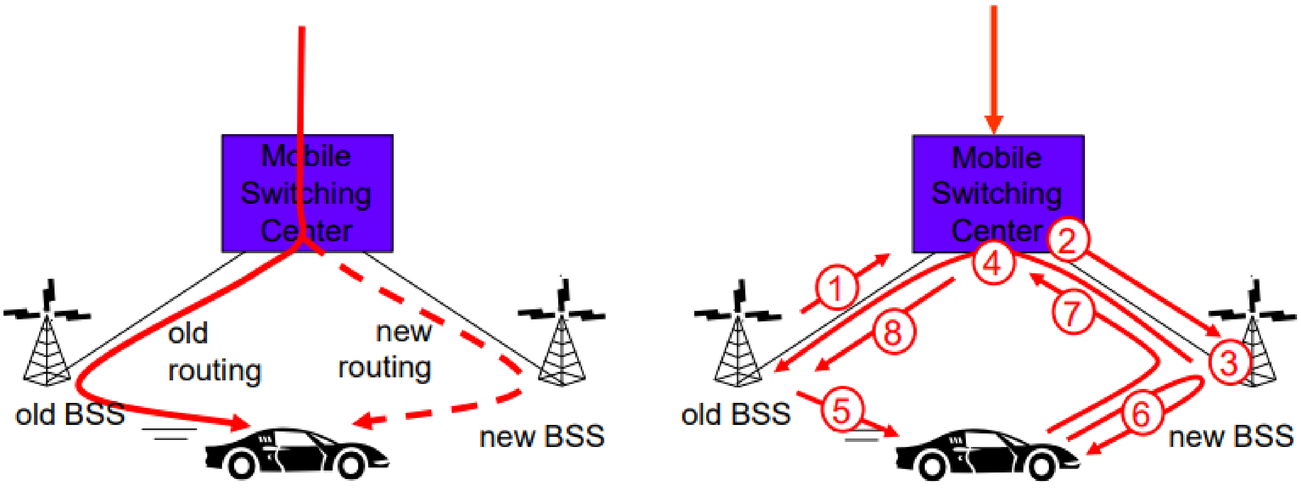
- **Home Location Register (HLR)** is a centralized database that stores permanent info about subscribed (literally "abbonati", via a telephonic/Internet contract) mobile devices. These info includes and identifier, some location data, service that the user activated, etc. When a mobile node - subscribed to that HLR - starts a call or data session, the MSC queries the HLR to get the needed info.
- **Visitor Location Register (VLR)** is a temporary database associated with each MSC and stores info about mobile devices currently within the coverage range of that MSC (i.e. under one or more of the BSS referencing that MSC). When a mobile device enters the coverage area of a MSC, its VLR is updated. It also help in load balancing, since it reduces the overall query load to the centralized HLR.
  MSC, HLR and VLR serve to provide seamless mobile communication services, ensuring that subscriber information is efficiently managed, and calls can be set up regardless of the mobile device's current location, within the network.

GSM Handoff (or Handover)

Motivations:

- stronger signal
- load balancing

- GSM only specifies how (mechanisms) to operate handoff, not why



Handoff steps (same MSC):

1. Old BSS decides to perform the handoff process, and send a message to the MSC, providing a list of possible desinations (one or more new BSSs).
2. MSC notifies the new BSS, because it needs to allocate resources.
3. (If there is enough space) the new BSS alloactes the radio channel that the mobile visitor will use. If it doens't arrive in a given time interval, the radio channel is deallocated. NB: that's proactive, because the channel is allocated before receiving the actual connection.
4. New BSS signals the MSC and old BSS it's readiness.
5. Old BSS informs the mobile device the need to operate handover towards the new BSS.
6. The mobile deevice signals to the new BSS to activate the new channel.
7. Mobile device signals to MSC (through the new BSS) that the handoff has been completed, and MSC performs a re-routing.
8. MSC deallocates resources of the old routing path and notify the old BSS that deallocates the old radio channel associated with the mobile node.

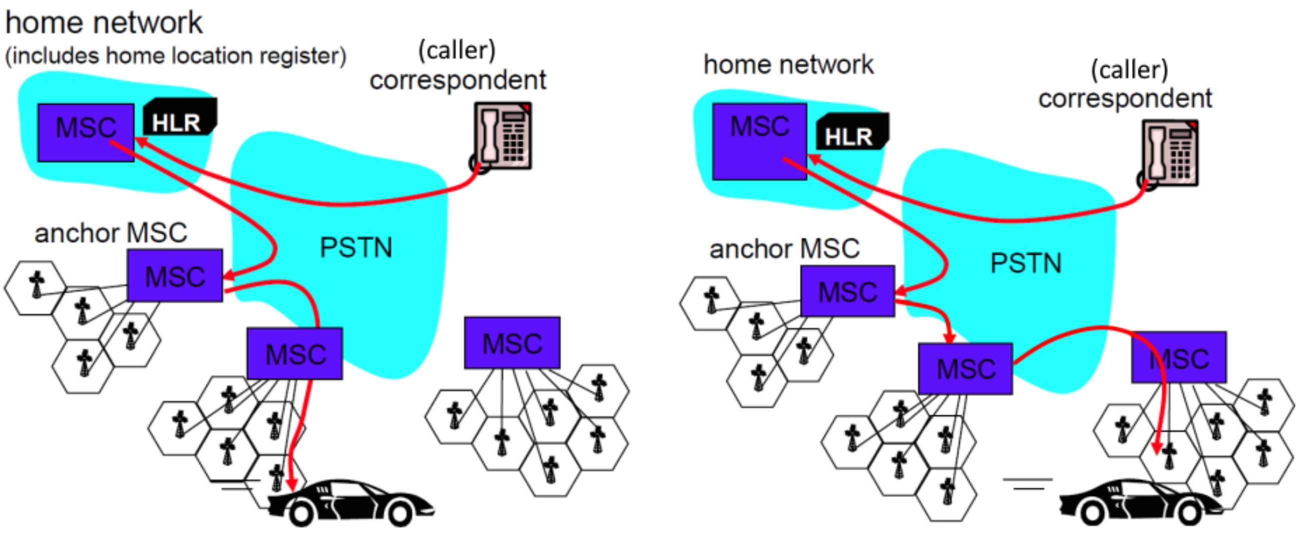
> That's how handoff works in cellular networks. These terms refer to 2G, but the concepts are valid for any later generation).

In crowded areas, typically you can still get connected, due to the fact that an area can be covered by multiple antennas.

One BSS has N radio channel slots to be allocated for N different users (different frequencies, each for a different visitor).
Among these, a quota is always maintained for moving users. The actual amount is not defined in the standard, but usually around 25%.
That's a static reservation, which has a cost and is not optimal, but cannot be predicted apriori.
In fact, when a BSS predicts the new BSS the mobile node can connect to, the prediction MAY

be wrong. Therefore resources need to be allocated, even if not always used.
Common goal: achieve service continuity at max at any time. Target is to perform handoff in less than 30ms (main supported service was voice, and it's proven that humans do not notice delays under 30ms).

Handoff (different MSC):



(a) prima dell'handoff (b) dopo l'handoff

1. The correspondent mobile node starts a call (or data session) towards another mobile node.
2. The request passes through the PSTN that identifies, given the number of the receiver, the corresponding HLR (of the receiver).
3. From the receiver HLR it's possible to obtain the current location of the receiver node and its MSC (the MSC that it's currently connected to).
4. The connection is enstablished.

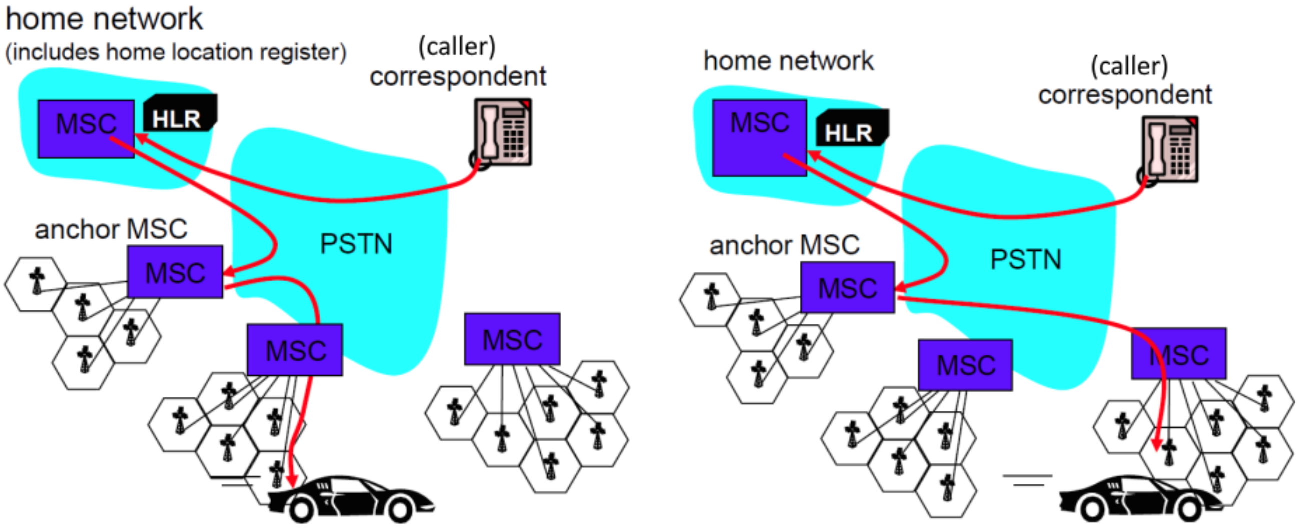
If the receiver moves, the new MSCs are appended at the end of the chain, but the anchor will always be present.

Anchor MSC is important because in case the mobile phone changes, at runtime, the cell to other MSC, it's the anchor that maintains the link with the currently visited MSC. Independently from your position, you have an anchor MSC (the point where the conversation started), if you or the receiver change position, there's still a link to it. The anchor MSC also keeps information about the call (duration and cost, for example).

Obviously it's possible to have a "direct link" or a chain of links for all the visited MSC during the service. Both options are possible according to the standard.

There's an optional feature (IS-41) that optimize the path, by minimizing it. However, what's not changed is the anchor MSC.

IS-41 example:



(a) prima dell'handoff (b) dopo l'handoff

Handoff classification:

- connectivity:
  - **horizontal**, if the connectivity is homogeneous (e.g. handoff between two GSM BSS);
  - **vertical**, if the connectivity is heterogeneous (e.g. handoff passing from 4G connectivity to WiFi);
- node that initiate the procedure:
  - **mobile-initiated** (e.g. WiFi);
  - **network-initiated** (e.g. GSM);
- when it's triggered:
  - **reactive**, if the handoff is triggered only after (as a consequence, as a reaction) a node loses connectivy to the previous AP (e.g. WiFi);
  - **proactive**, if the handoff is triggered before that happens (e.g. GSM);
- management:
  - **hard**, if the mobile device disconnects from the old BSS (e.g. GSM, WiFi);
  - **soft**, if during time interval of the handoff the mobile device stays connected both to the old BSS and the new one (not possible in GSM, nor WiFi, but one could have 2 WiFi cards);

Bluetooth (IEEE 802.15)

Bluetooth belongs to wireless Personal Area Network (PAN) family, with relatively small range: ~10-100m, low cost (~5/10$ per interface) and that manages both voice and data. It was designed as a technology for cable replacement.

Bluetooth standard defines specs of protocols for wireless communication, how to use them, and the corresponding software stack.

Main characteristics:

- works in 2.4GHz frequencies (same as WiFi), exploiting ***frequency hopping***;
- initial bandwidth of ~1Mbps;
- low consumption: 1mW-10mW;
- **piconet**, network "star" topology with a master and 7 slaves at most;

Main differences with WiFi:

- In Bluetooth the communication always passes through the master, while in WiFi there is a point-to-point communication between master (AP) and slave (MN).
- Bluetooth needs a preliminar discovery phase, while in WiFi a mobile node simply sends a probe message to all near APs.
- Very limited broadcast mechanism.

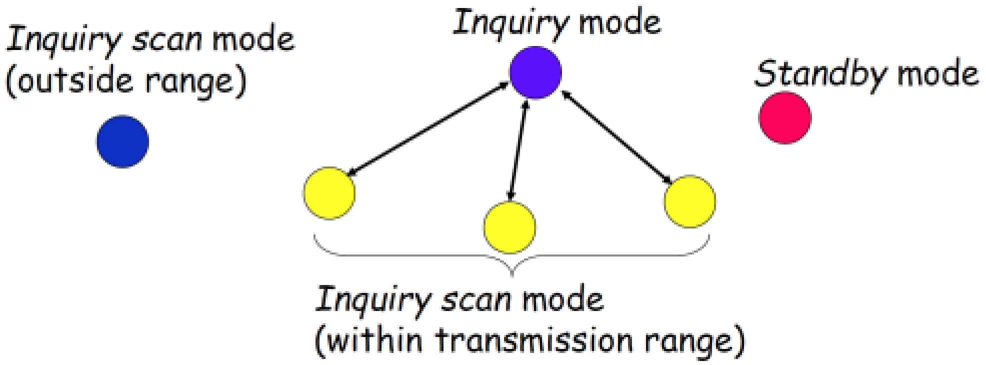
Bluetooth Topology Formation

Bluetooth topology is the piconet, that consists of a star network formed by a master and up to 7 slaves. Actually nodes can be up to 256 if set to "parked"/"standby" state, i.e. they're part of the network but they're inactive and cannot communicate. Each slave communicate through a single channel in frequency hopping.
The piconet formation occurs in 2 phases:

1. Inquiry phase, to discover the participant and who'll be the master (stupidly/simple enough, the one who started this phase).
2. Page phase, where the master enstablish a bidirectional channel to the slaves.

Inquiry Phase

Goal: collect sufficient info and nodes to enstablish a piconet.
A node that wants to communicate enters the "inquiry mode": it sends its ID and waits for an answer from its neighbours (containing their IDs). At the end, the node will have a list of the IDs that participate to the piconet. To save energy, other nodes can switch between "inquiry scan mode" and "standby mode".
The node that starts the inquiry becomes the master, and the other will be the slaves. After a time interval, if it received at least one answer, the master enters the page mode.

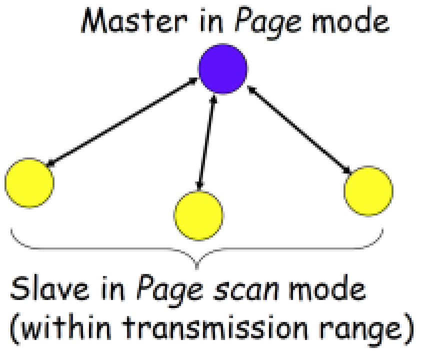


Example:

- purple starts inquiry mode;
- blue is outsite, therefore doesn't receive the inquiry message (and won't be able to join further on);
- red is in range but doesn't respond because it's in standby mode;
- yellows respond because are in "inquiry scan mode" and the connection with them is enstablished.

Page Phase

The master enstablish a bidirectional communication channel with its slaves.
Then it sends the value of its logical clock to the slaves, in order to make them synchronize with it, and requires the slaves to send their estimated clocks and their bluetooth addresses. Another info that is exchanged is the frequency sequence.
The clock synchronization is necessary because in Bluetooth, contrary to WiFi, the communication is split in time slots to prevent collisions *by design*.
One piconet disadvantage is that it requires some time to be built (in seconds). That's tollerable for the devices that Bluetooth is thought for (printers, headphones, etc.).
Once the connection is enstablished, it remains so until the end of the usage.



Frequency hopping

Bluetooth exploits frequency hopping in 2.4GHz band (79 hop frequencies, at 1 MHz distance). Since piconet members have successfully passed the page phase, we know their clocks are synchronized.
The hopping sequence is determined based on the master address. Each piconet member has to follow the same sequence.
Master and slaves communicate alternating in periodic slots (called rounds). In each slot only a device can communicate: master can communicate using odd slots, while slaves even ones. That prevents collisions.
Pros:

- tends to be more robust to distrubs;
- harder to attack a node if it continuously changes frequency;
  Cons:
- the slot usage is not optimized, since not always a device has something to send/receive.

NB: the master can use its slot to send messages but also

Timing and clock

Any bluetooth device has its own native logical clock CLKN. The piconet has a clock, that coincides with the CLKN of the master.

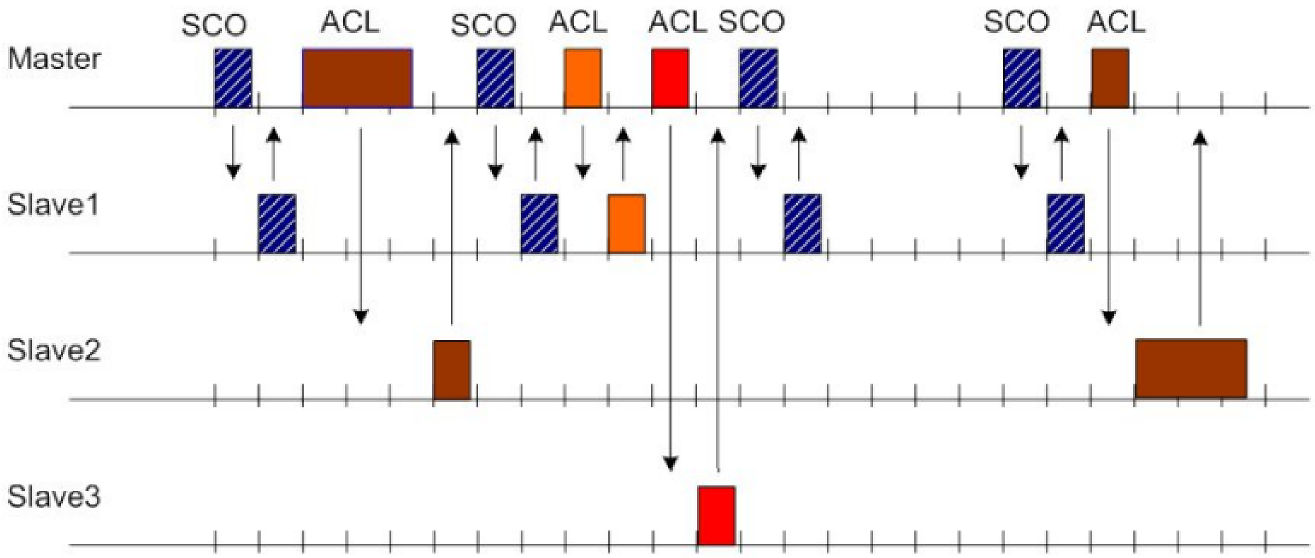
Connections

There are 2 types of connections:

- **Asynchronous Connection-Less (ACL)**: used for **data** traffic (not voice or multimedia) and best-effort service (simplicity over guarantees). Supports:
  - packet-switch connections;
  - point-multipoint connections;
  - symmetric (max ~400Kbit/s)/asymmetric (max ~700Kbit/s downlink and ~60Kbit/s uplink) connections.
    NB: a slave can transmit only if it received the permission from the master in the previous slot.
- **Synchronous Connection-Oriented (SCO)**: used for real-time and **multimedia** traffic. Guaranteed bandwidth (64Kbit/s). Support:
  - circuit-switched connections;
  - point-point connections;
  - symmetric connections;
    Max 3 connections SCO towards the same or different slaves, to avoid consume the already little bandwidth for BT. There is no retransmission of packets if they're lost.

Why? Because in real-time communication the user just wants a low latency, it doesn't care about the multimedial content to be completely intact. A potential retransmission would do more damage than otherwise (think of it as for UDP).

In SCO connections, a channel is reserved for 2 time slots for communication between master and one specific slave. The reservation periodicity is decided by the master, independently by the need of transmission. ACL communication can only occur in pause intervals between SCO reserved slots. That's also why there is a limit to 3 SCO connections, otherwise every slot could be reserved, not leaving any space for ACLs.

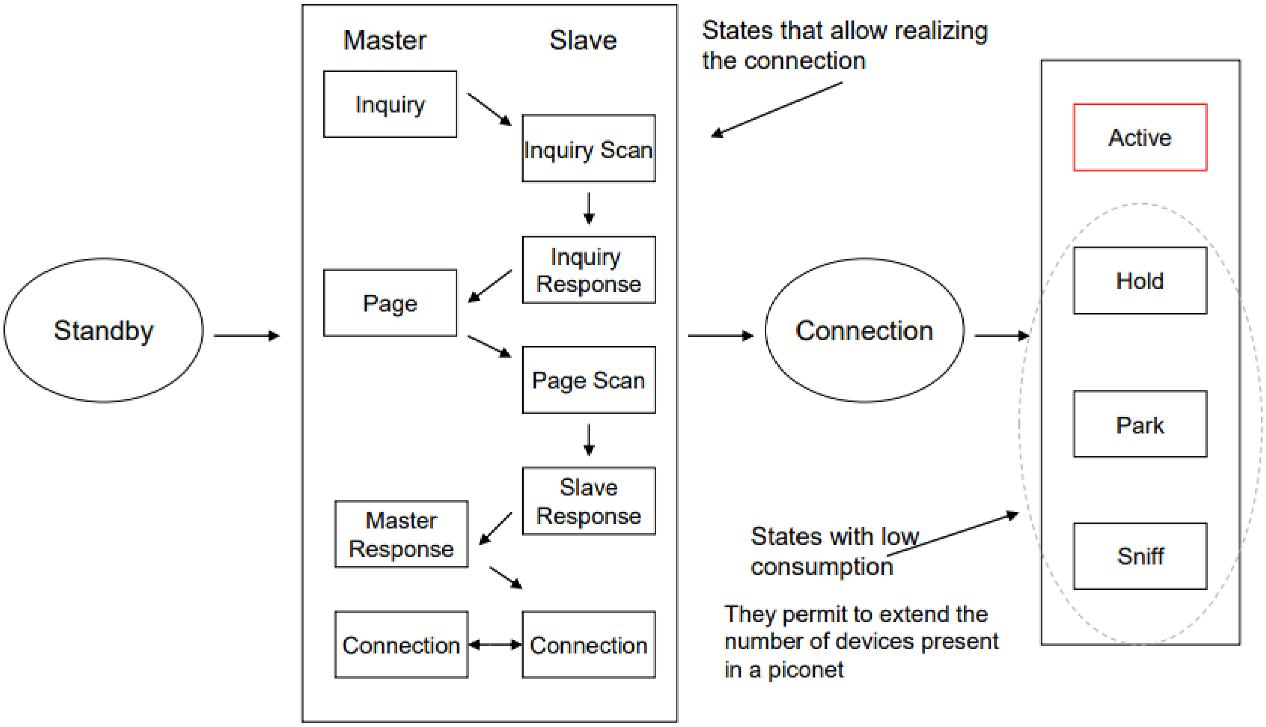


Device States

Bluetooth is not only a 2 layers protocol, but much more (e.g. how devices communicate). Different states:

- active
- hold (low consumption)
- park (low consumption)

- sniff (low consumption)

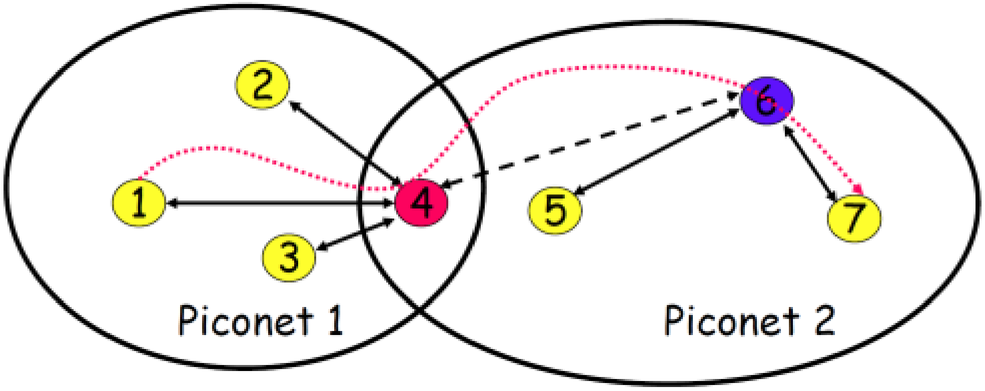


Service Discovery Protocol

Since it was created to replace cables, a user would also need to discover what service a particular node offers.

Scatternet

Piconets are the classical way to use Bluetooth, but it's not the only topology available.
A scatternet is a combination of more piconets where at least one node participate in both of 2 of the piconets (that for 2 piconets forming a scatternet): they can have a common master but also a common slave.



Performance in a scatternet is absolutely not optimal, since the communication becomes multihop and the cost of creating a connection increases. Moreover to coordinate all these nodes become much complex, with inquiry and page phases requiring a lot more time.

Bluetooth Low Energy (BLE)

Bluetooth variant that allows to significantly reduce battery consumption, by keeping a great communication range. It was included in Bluetooth 4.0.
The main difference with classic Bluetooth is that BLE has a different set of frequencies (40 instead of 79), but wider (2MHz instead of 1MHz).
To avoid interferences and reduce power consumption, BLE uses 3 channels.
Nodes can send advertising packets (advertising node) in broadcast or listen for offered services (scanner node). But since any node (both advertising and scanner) can use all the channels indiscriminately, there's only 1 probability on 9 that a scanner will detect an advertising packet. Therefore BLE has the disadvantage of having a long and variable discovery time.

ZigBee (IEEE 802.15.4)

Another wireless PAN standard, but specifically designed for sensors and actuators networks, with the following requirements:

- reliability;
- cost-effectiveness;
- low power;
  While Bluetooth is designed for domestic environments (replace cables at home), ZigBee is designed for industrial ones (monitoring).
  Bluetooth was not suitable for industrial environments, due to its topologies beeing too complex to manage with increasing sizes.
  ZigBee supports up to 64k nodes. As BT, ZigBee provides profiles for higher layers of the support/application stack.
  It's optimized for topology formation time, especially for when a new node connects (<30ms compared to BT's several seconds).
  Support to full mesh networking.

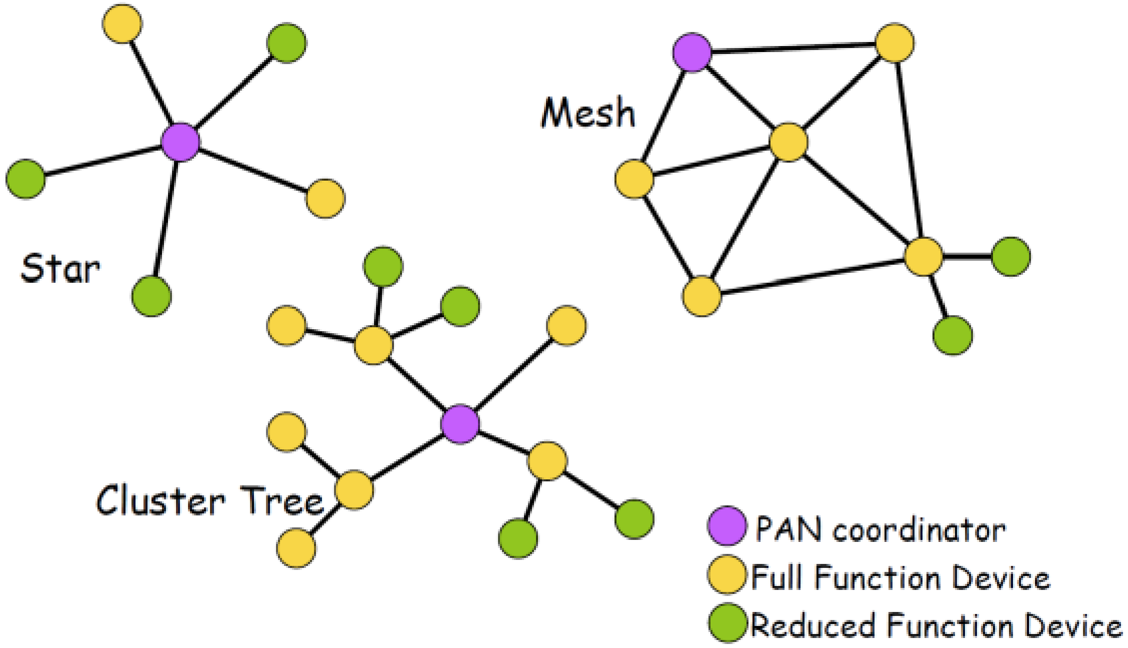
  > NB: in ZigBee there's nothing that automatically decides a network topology or how to access a channel. Those choices must be done by the network administrator that programs the PAM coordinator.

Topologies

3 different topologies:

- **star**, same as piconet, is the simplest one;

- **mesh**, similiar to WiFi mesh. Each node can have an arbitrary number of connections towards other nodes in its neighborhood. It's very resilient, since each node can have multiple connections. Disadvantage: Overhead;
- **cluster tree**, tree hierarchical topology, with PAN coordinator as the root node. RFD can only be the leaves. The root node has global visibility. Great for scalability and low coordination costs but it's not robust to failures.



Devices Different Roles

There are different roles for ZigBee devices:

- **PAN coordinator** (~master), one for each ZigBee network. It activates the network formation and acts like a router once the network is functioning. The PAN coordinator must be a reliable node (high battery level, possibly fixed or with limited mobility, etc.);
- **Full Function Device (FFD)**, participates in messages routing;
- **Reduced Function Device (RFD)**, executes only sensing and actuating operations, no routing.

Channel Access Options

To access the channel, the nodes can choose between 2 networks types:

- **non-beaconed network**, the nodes will start communicating by basically exploiting MACA and sending positive ACKs for successful reception of packets;
- **beacon-enabled network**, similiar to SCO channels in Bluetooth, the PAN coordinator transmits the permission to transmit (as beacons) at regular time intervals.

Summary on ZigBee: is a sort of combination of the previously seen protocols. It's pretty much domain-specific and it's rare to see (even more rare on a smartphone).

Chapter 2 - MANET and Routing (ISO/OSI Layer 3)

Chapter 3 - Mobile IP and Positioning

2.1 MANET and Routing

2.2 Mobile IP and Positioning

Chapter 3 - IoT and Related Applications

Chapter 4 - Android

Chapter 5 - Discovery

Chapter 6 -