University of Antwerp
Faculty of Science

Advanced Wireless & 5G Networks

Prof. Dr. Ir. Michael Peeters — 2023–2024

Topics for today

- **What to do with 20/10?**
- **What are your expectations?**
- **1. Introduction (continued)**
  - Recap of last week
- **2. Technology baselining/refresher**
  - Two formulas

Planning

Session	Date	Topic
1	20231006	~~Introduction, history, market, industry, bands, licensed vs. unlicensed, …~~
2	20231013	~~Technology baselining (a.k.a. refreshing what you should have known): 2G, WiFi, …~~
3	20231020	~~Cancelled~~
4	20231027	Shannon/Friis continued. 2G as a ”low-complexity” example
5	20231110	L 3GPP 2G-3G-4G-5G architecture evolution. 5G
6	20231117	L Other licensed and special cases (CBRS, LAA, Public Safety, Loon, V2V, Satellite)
7	20231124	U IEEE Wifi Network Architecture: the 802.11 family
8	20231201	U 802.11 abgn
9	20231208	U QoS, 802.11 ac,ax and 802.11 ad,ay
10	**20231215 – 3h**	U short range 802.15.4: Zigbee, BLE, and UWB
11	**20231222 – 3h**	U Specials: LoRa, Sigfox (perhaps), proprietary, 802.11p
	TBD	Extra: Technology enablers and acronyms you need to be aware of: ADC, FEM, PA, LSA, and other key analog and digital HW blocks, mMIMO, Beam management, 802.11be, AI, 6G, THz and their implications to the network

Your expectations

- How it is possible that, in a world where the number of devices continue to grow, every device can get mobile wireless connectivity with the internet without saturating the network.
- How do 4G/5G/... technologies actually work.
- How do you go about designing a good WiFi network, both on the physical end (devices, access point locations, ...) and on the configuration end.
- What are the technologies behind the current advancement in Cellular and Wi-Fi networks?
- Be able to understand the need for improved and efficient networking technologies, and how to approach solving the drawbacks of current technologies.
- What are the limitations of 5G in regard to the latest trends in Ai, AR/VR and technologies that require very low latency.
- What is next?
- Wifi 6 & 7 – new features.
- Link to cloud.
- How do modern mobile networks work and how have they changed from the previous ones?
- What are the main problems or limitations faced by different types of networks? If it is possible, what are the best ways to solve them?
- How will wireless and mobile networks possibly evolve in the near future?
- ~~To better understand historical challenges in wireless that companies such as blackberry faced.~~
- To better understand wireless technologies such as Zigbee and LoRaWan and their use in IOT projects.
- What role data science could have in this field?
- Can networks be perfected to the point where we don't need to keep on creating new ones or upgrade the existing ones?
- ~~Can governments stop the development of networks?~~
- ~~Will connectivity ever be available underwater or underground?~~
- Security of wireless networks.

2. Baselining

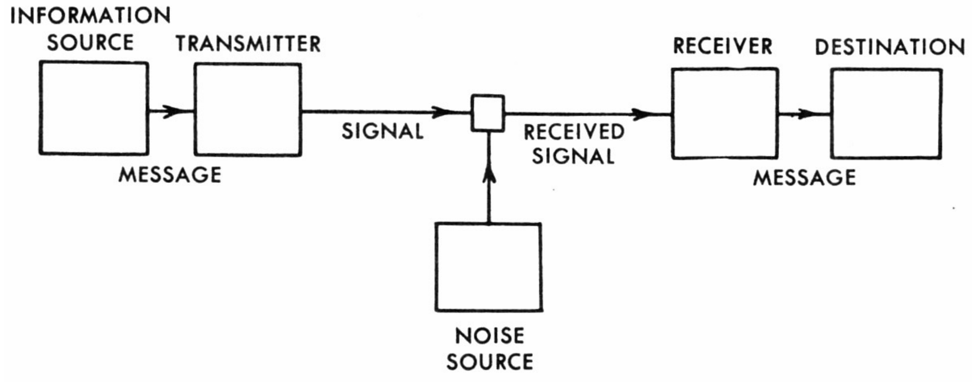
(concepts & toy examples)

What will we cover

- ~~Mobile vs. Wireless vs. Fixed~~
- Shannon’s law, to calculate capacity and compare technologies
- Friis’s equation, to calculate coverage
- Cellular and 2G as a reference system

Shannon’s law – Wireless examples

- **A bunch of assumptions**
  - Wireless, not mobile – movement captured in noise
  - All noise is “white”– not frequency dependent, uncorrelated in time
  - All noise is Gaussian - normally distributed
  - All noise is additive – linear combination of noise and transmission
  - Interference from other users is part of overall Gaussian noise – large numbers
  - Signal and noise are uncorrelated – intersymbol interference is extra noise
  - The environment and the noise are stationary – no blocking or fading
- **This is called the AWGN channel**
  - Additive
  - White
  - Gaussian



Shannon-Hartley for AWGN

$$\underbrace{C}_{\text{bits per second}} = \overset{\text{Hertz}}{W} \log_2\left(1 + \boxed{\frac{\overset{\text{Watt}}{P}}{\underset{\text{Watt}}{N_0 W}}}\right)$$

Signal to noise ratio

$$SNR = \frac{P}{N_0 W}$$

- **Shannon-Hartley = maximum bitrate for error-free transmission** (with assumptions)
- **C = capacity, the problem to which telecommunication technology is a solution**
- **W = bandwidth, expensive because of**
  - scarcity
  - infrastructure
  - technical implementation (higher switching speeds)
- $^{P}/_{N_0 W}$ **=** **received** **signal power vs. noise power, expensive because of**
  - regulation
  - technical implementation (low noise)
  - inside log2, so large changes needed

Key metric:

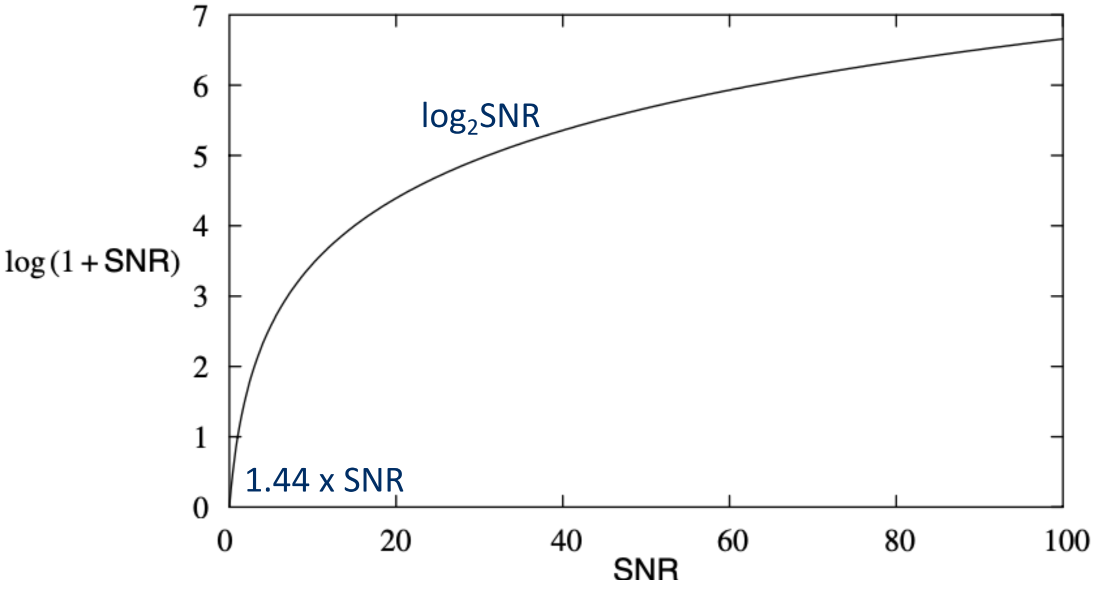
Spectral Efficiency

$$SE = \eta = {}^{C}/_{W}$$

How does this formula behave?

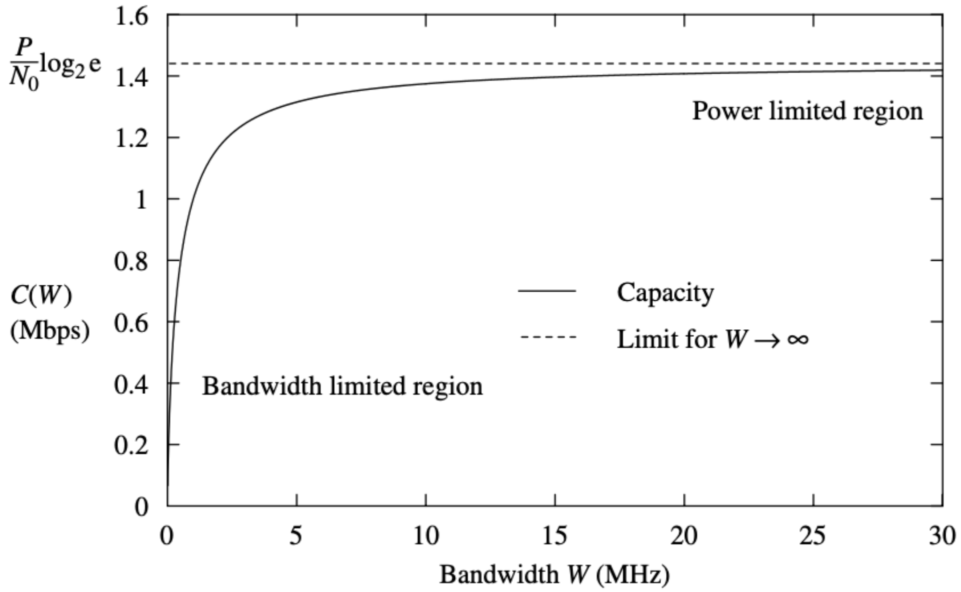
$$C = W \log_2\left(1 + \frac{P}{N_0 W}\right)$$

Dependence on power



$$\log_2(1+x) \approx x \log_2 \mathrm{e} \qquad \text{when} x \approx 0,$$
$$\log_2(1+x) \approx \log_2 x \qquad \text{when} x \gg 1.$$

Dependence on bandwidth



$$W \log\left(1 + \frac{\bar{P}}{N_0 W}\right) \approx W\left(\frac{\bar{P}}{N_0 W}\right)\log_2 \mathrm{e} = \frac{\bar{P}}{N_0}\log_2 \mathrm{e}.$$

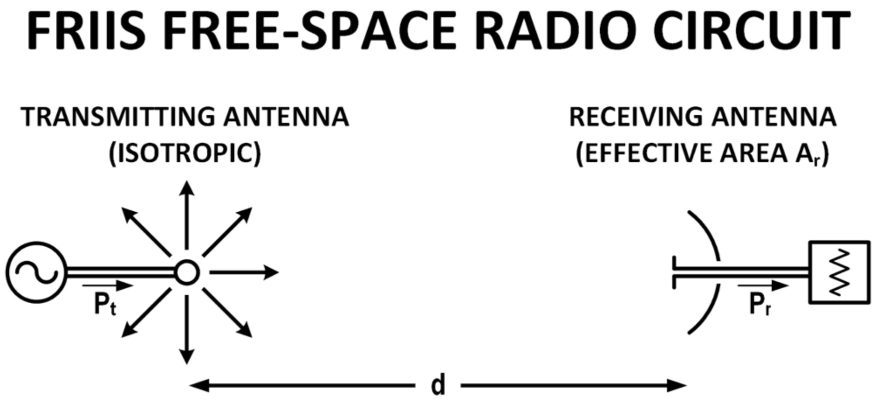
Blackboard to Jupyter

- **Logarithms**
- **dB, dBm, dBW and dBi**
- **Power levels**
  - Wifi Access Point
  - 5G Small Cell
  - 5G Basestation
  - 5G Cell Phone
- **Power spectral density (PSD)**
- **Noise**
  - Johnson-Nyquist PSD=$k_B.T$
  - Wifi 1, Wifi 6, 2G, 5G

Received Power?

- **Friis transmission equation**
- **A bunch of assumptions**
  - Sufficiently large distance between transmit and receive — far field
  - Free space: no absorption or scattering — vacuum (or air)
  - Co-polarized antennas with conjugate matching — good engineering, best case
  - Boresight alignment — antennas are pointed correctly
  - No reflections or multipath — line of sight (LOS)
  - No blocking — clear Fresnel zone

Friis transmission equation



$$P = P_r = \frac{P_t . D_t . D_r}{FSPL}$$

$$FSPL = \left(\frac{4\pi f_c}{c} d\right)^2$$

Driving the techno-economics:

P_r — Received Power; higher is better, more bits/second/hertz

P_t — Transmitted Power; expensive because of regulation and technology

D_t — Transmit antenna directivity; cost, weight and size

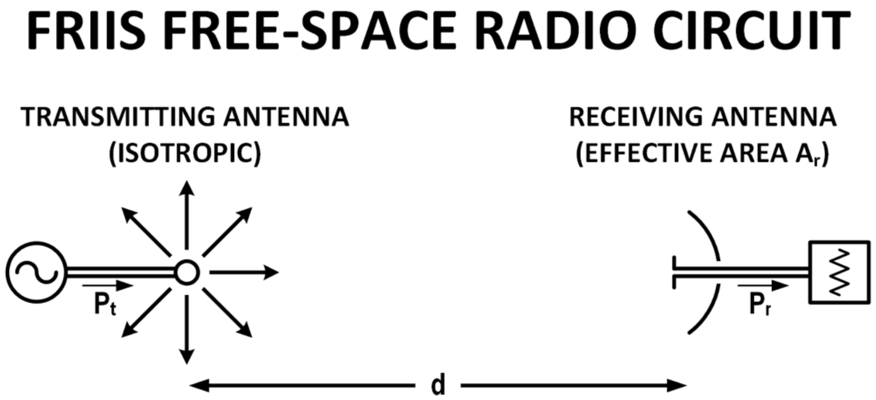
D_r — Receive antenna directivity; cost, weight and size (especially in the phone)

f_c —frequency; spectrum regulation, technical challenge

d — Distance between transmit and receive; amount of infrastructure

FSPL — Free space pathloss

Friis transmission equation in dBx



$$P = P_r = \frac{P_t . D_t . D_r}{FSPL}$$

$$FSPL = \left(\frac{4\pi f_c}{c} d\right)^2$$

$$P_r^{dBm} = P_t^{dBm} + D_r^{dBi} + D_t^{dBi} - 20\log_{10}\left(\frac{4\pi f_c}{c} d\right)$$

Received = Transmitted + Antenna gain + Antenna gain - Free space loss

With f_c in GHz and d in km:

$$P_r^{dBm} = P_t^{dBm} + D_r^{dBi} + D_t^{dBi} - 92.44dB$$
$$-20\log_{10} f_c - 20\log_{10} d$$

e.g. at 1 GHz and 1km, isotropic antennas, P_r=P_t–92.44dB

Blackboard to Jupyter

- **Relationship between frequency, wavelength and the speed of light**
  - $c = {}^{\lambda}/_{f}$ (with c in m/s, λ in meter and f in per second or Hz)
- **Typical pathloss & antenna directivity(gain)**
  - Wifi
  - Satellite
- **Typical capacities (given certain noise temperature)**

A “real” system: 2G

What do you know/remember?

- Requirements
- Specifications

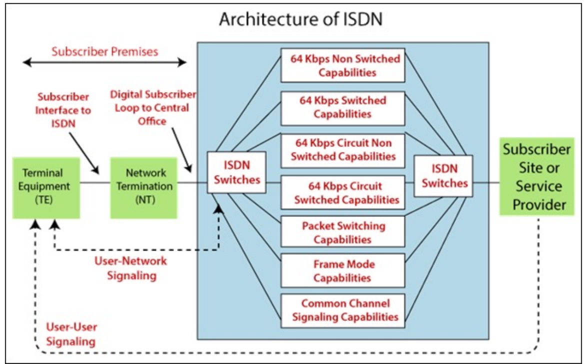
2G a.k.a. GSM

Requirements

- It should offer good subjective speech quality
- It should have a low phone or terminal cost
- Terminals should be able to be handheld
- The system should support international roaming
- It should offer good spectral efficiency
- The system should offer ISDN compatibility

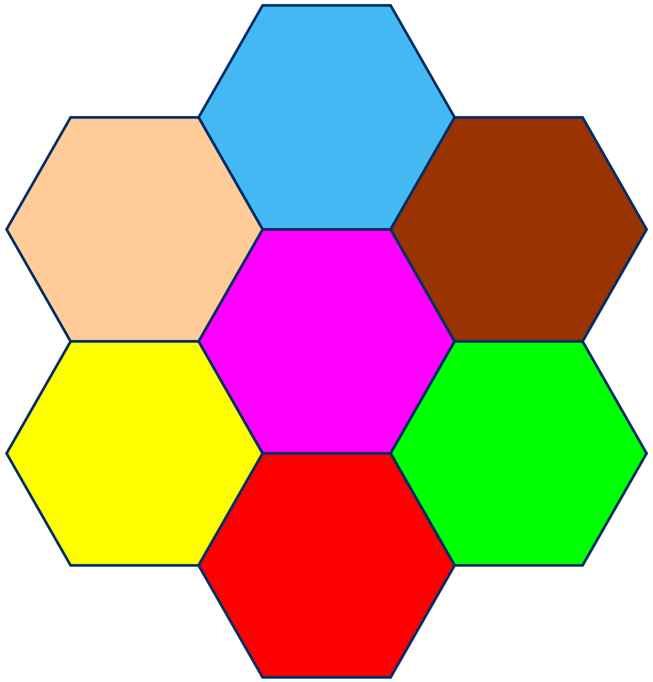
SPECIFICATION SUMMARY FOR GSM CELLULAR SYSTEM

Multiple access technology	FDMA / TDMA
Duplex technique	FDD
Uplink frequency band	890 - 915 MHz (basic 900 MHz band only)
Downlink frequency band	933 -960 MHz (basic 900 MHz band only)
Channel spacing	200 kHz
Modulation	GMSK
Speech coding	Various - original was RPE-LTP/13
Speech channels per RF channel	8
Channel data rate	270.833 kbps
Frame duration	4.615 ms



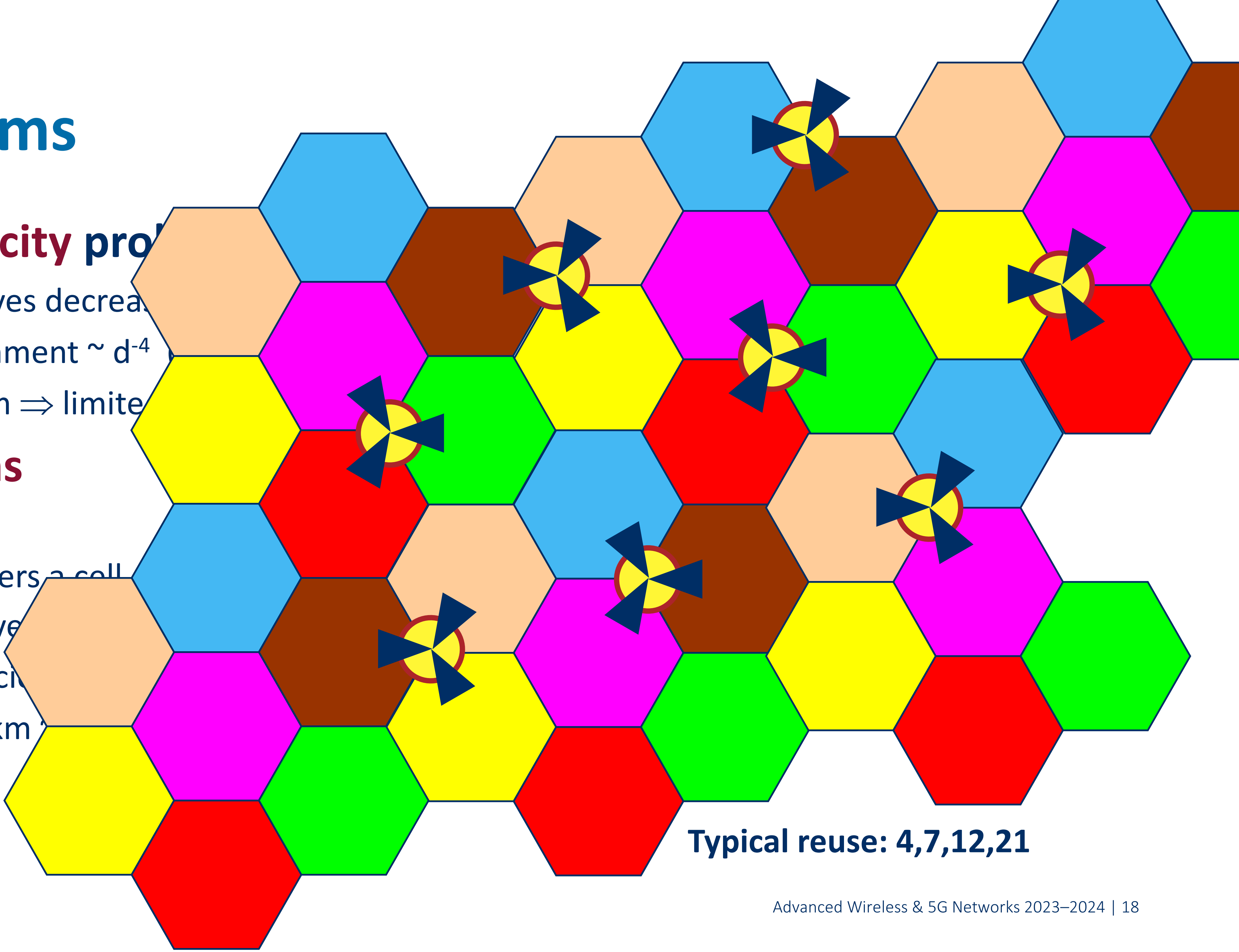
Cellular systems

- **Coverage/capacity problems**
  - power radio waves decreases ~ d^{-2} (Friis)
  - in urban environment ~ d^{-4} (Pathloss models)
  - limited spectrum $\Rightarrow$ limited number of users
- **Cellular systems**
  - Bell Labs, 1971
  - base station covers a cell
  - “small” cells solve power decrease problem
  - reusing frequencies solves capacity problem
  - GSM cell size 1 km ~ 10 km



Cellular systems

- **Coverage/capacity pro**
  - power radio waves decrea
  - in urban environment ~ d^{-4}
  - limited spectrum ⇒ limite
- **Cellular systems**
  - Bell Labs, 1971
  - base station covers a cell
  - "small" cells solve
  - reusing frequenci
  - GSM cell size 1 km



Typical reuse: 4,7,12,21

How does cellular system capacity scale?

- **Single system (a la TV broadcast)**
  - T channels = T users in parallel
- **Cellular system**
  - T = number of channels (frequencies)
  - K cells per cluster (frequency reuse)
  - M clusters
  - Then we have N channels(users) per cell: N = T/K and total system capacity M.T
- **Example**
  - K=7, 490 channels, 9 clusters
  - 70 channels(users) per cell, **4410** total channels

i.s.o 1 huge area with 490 users max.

Ideal: reuse 1 (4G, 5G)

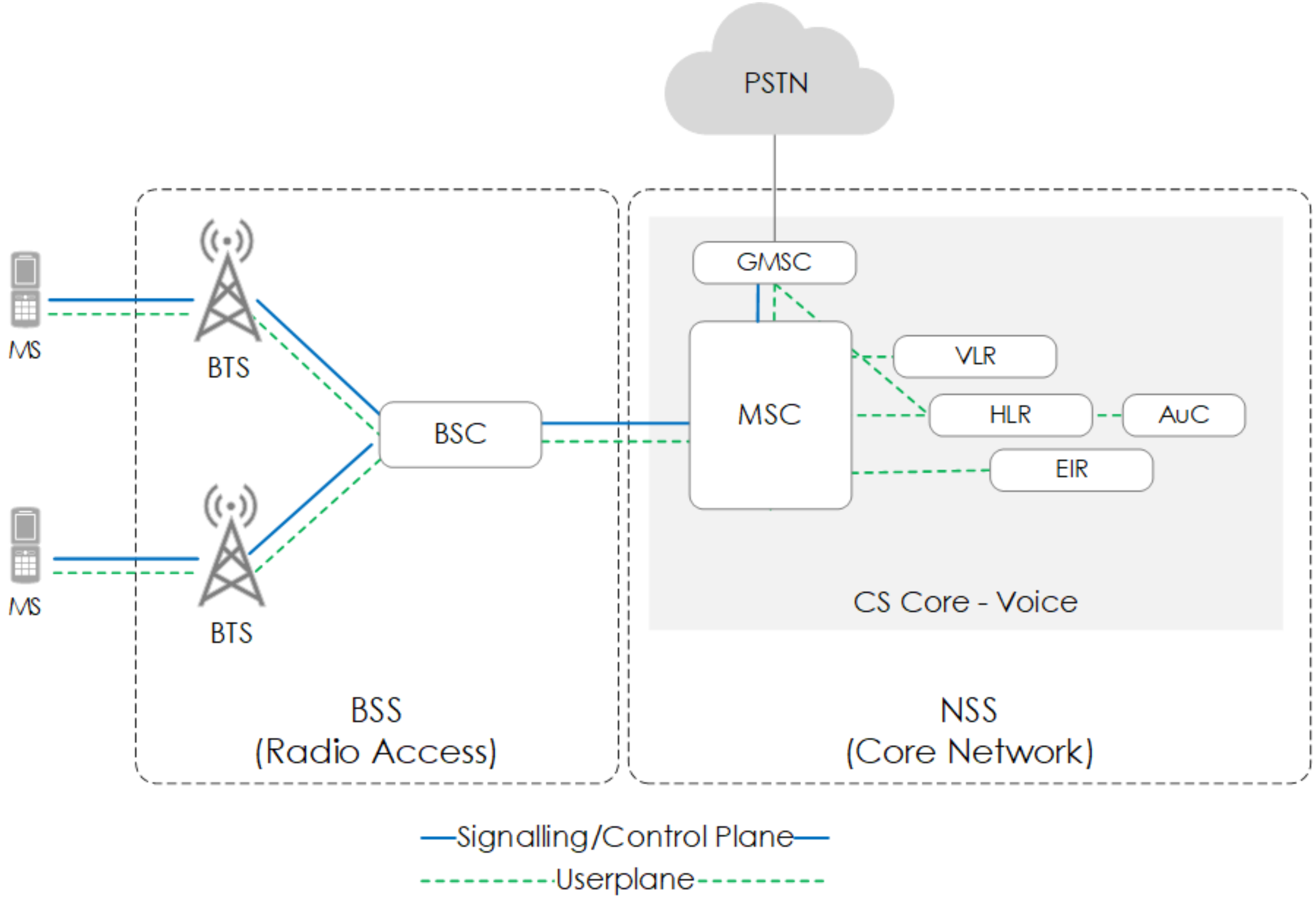
Cellular Systems: Additional complexity

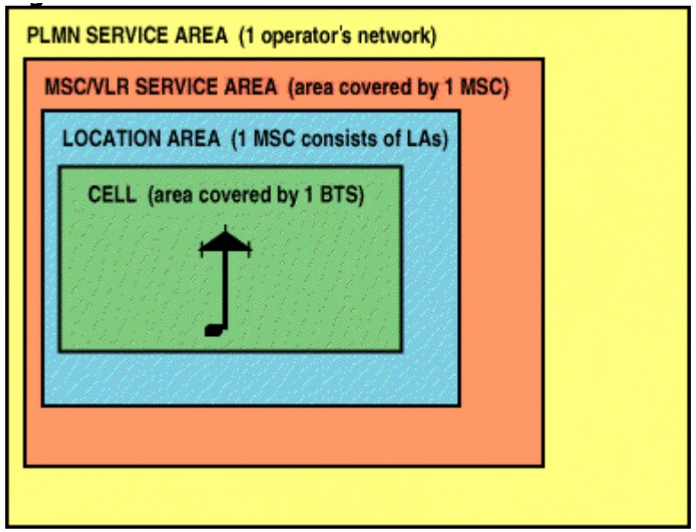
- **Radio Interface Management**
  - # radio channels < # potential users
  - radio channels are allocated/released on call basis
  - states of a mobile station:
    - idle mode : listen to broadcast channel, no dedicated channel
    - dedicated mode : bidirectional channel

Cellular Systems: Mobility

- **Locating a subscriber (mobility aspects for idle terminal)**
  - location updating: each change of cell is indicated to the network
  - ubiquitous updating: no update; paging messages are broadcast to all cells
  - compromise: update between location area, paging within a location area
- **Handover (mobility aspects for terminals in dedicated mode)**
  - detection of cell changes
  - channel switching between cells
- **Roaming**
  - mobile station can use different networks
  - roaming requires administrative and technical agreements
  - advantage of GSM

2G architecture





Mobile Station (MS)

- **Functions:**
  - radio and processing function to access the network through radio interface
  - human user interface (microphone, loudspeaker, display)
  - interface to other equipment
- Subscriber Identity Module (SIM)
  - smart card with subscriber related information
  - PIN code
  - list of phone numbers, settings, etc.

Base Station Subsystem (BSS)

- **Connects MS with NSS controlled by OSS**
- **BSS consists of:**
  - Base Transceiver Station (BTS)
    - BTS contains radio transmission/reception devices
    - connects with MS via radio interface
    - Transcoder/Rate Adaptor Unit (TRAU) contains GSM specific speech codec and data traffic adaptation
  - Base Station Controller (BSC)
    - connects with NSS (A interface) and BTS (Abis)
    - management of radio channels
    - handover
    - 1 BSC controls a number of BTS

Network & Switching Subsystem

- **Mobile Service Switching Center (MSC)**
  - basic switching function (for millions of users)
  - interface to BSS and external network (IWF)
  - one MSC controls a few BSCs
  - databases for mobility management and subscriber data

- **Home Location Register (HLR)**
  - database with subscriber information independently of actual location
  - information related to actual location of subscriber
  - contains Authentication Center

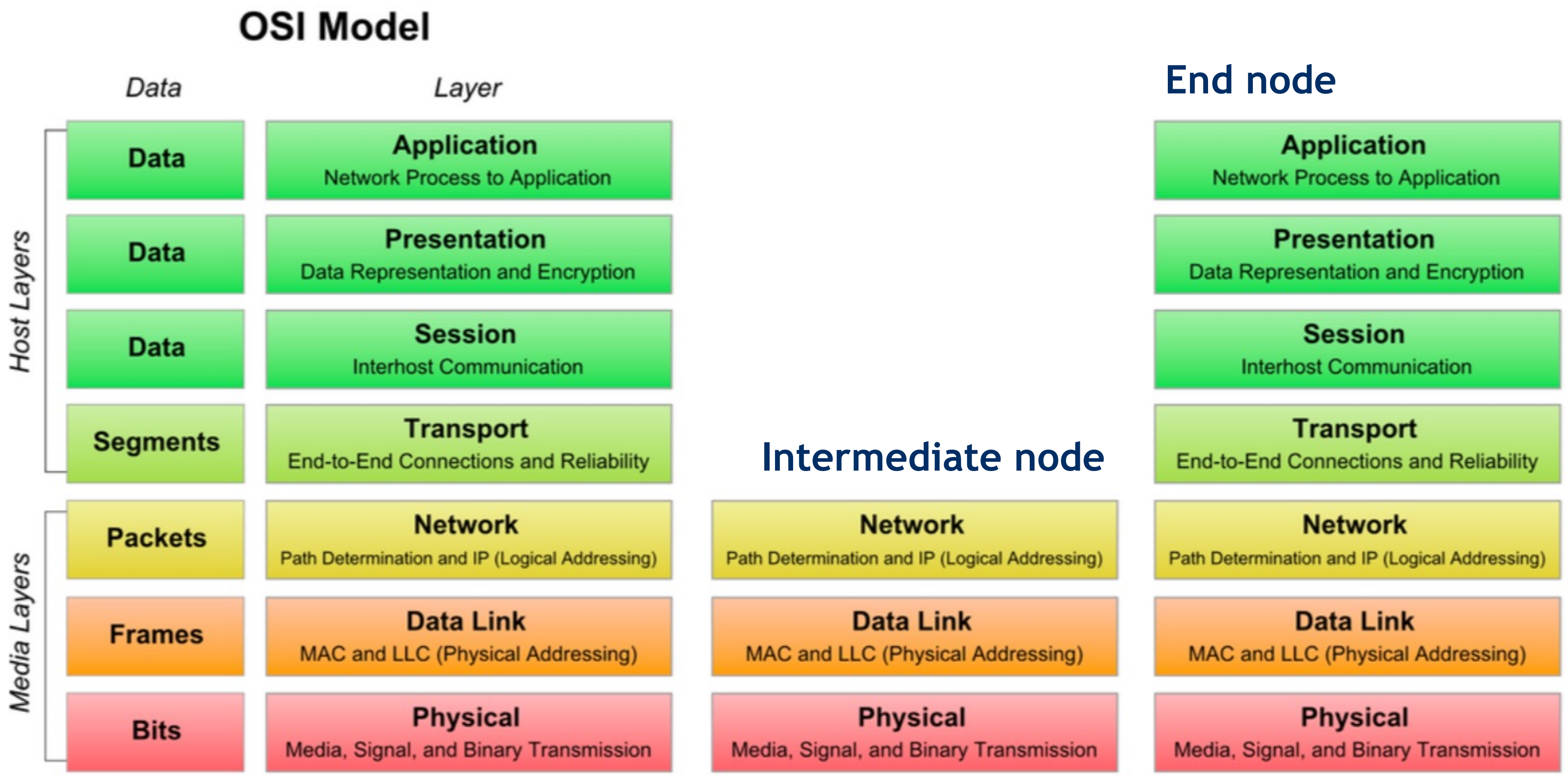
Network & Switching Subsystem

- **Visitor Location Register (VLR)**
  - VLR related to one or more MSC
  - database with information of subscribers currently in these MSCs
- **Gateway Mobile Switching Center (GMSC)**
  - An MSC fetches the location information of a subscriber (using HLR)
  - GMSC routes call to visited MSC
- **Signaling System 7 (SS7)**
  - signalling between NSS machines

Operation Subsystem (OSS)

- **Functions of OSS**
  - Network operation and mainatenance
  - Subscription management (SIM)
    - subscriber data management (HLR)
    - call charging
  - Mobile station management (Terminal equipment)
- **Interface with NSS machines through SS7 signalling**

OSI STACK


OSI Model
Data
Layer
Host Layers
Media Layers
Data
Application
Network Process to Application
Data
Presentation
Data Representation and Encryption
Data
Session
Interhost Communication
Segments
Transport
End-to-End Connections and Reliability
Packets
Network
Path Determination and IP (Logical Addressing)
Frames
Data Link
MAC and LLC (Physical Addressing)
Bits
Physical
Media, Signal, and Binary Transmission
Intermediate node
Network
Path Determination and IP (Logical Addressing)
Data Link
MAC and LLC (Physical Addressing)
Physical
Media, Signal, and Binary Transmission
End node
Application
Network Process to Application
Presentation
Data Representation and Encryption
Session
Interhost Communication
Transport
End-to-End Connections and Reliability
Network
Path Determination and IP (Logical Addressing)
Data Link
MAC and LLC (Physical Addressing)
Physical
Media, Signal, and Binary Transmission

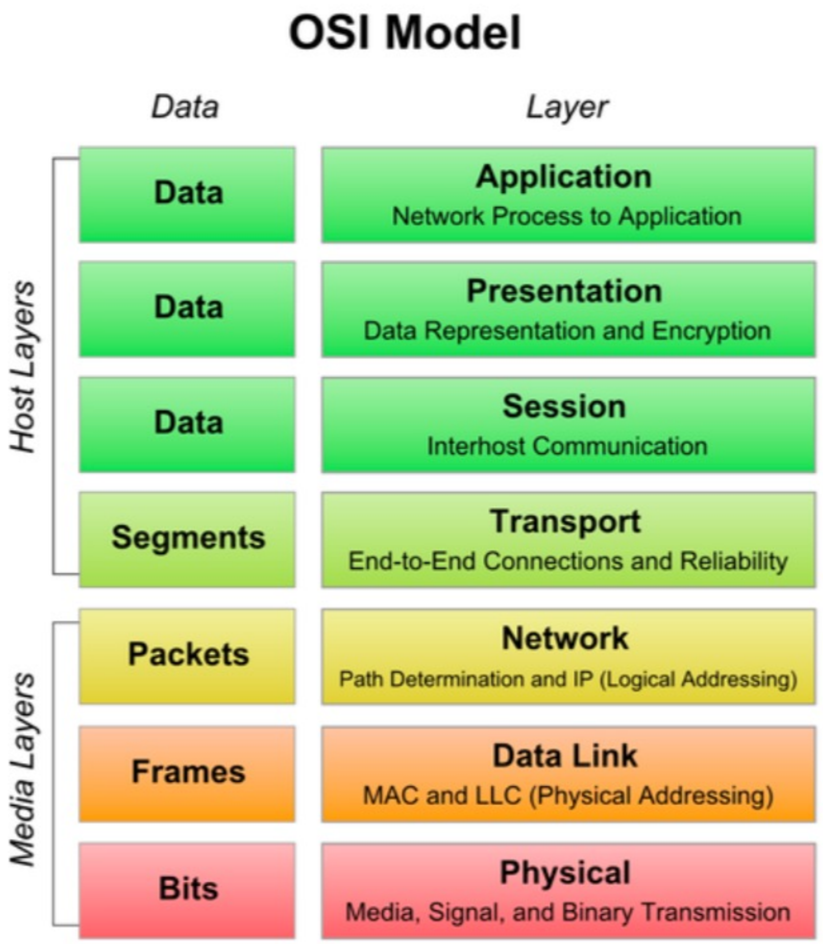
ISO-OSI Layers (1)

- **Physical Layer**
  - rules by which bits are passed (duration of a bit, voltage of a bit, frequency used, …)
- **Data Link Layer**
  - error detection/correction
  - flow control
- **Network Layer (IP)**
  - Addressing
  - Routing (statical/dynamical)
  - IP Protocols: ARP, DHCP, NAT, ICMP
  - Standard protocols: IPv4, IPv6

ISO-OSI Layers (2)

- **Transport Layer**
  - end-to-end protocols (UDP, TCP)
  - data arrives error-free, in sequence, without losses, without duplicates
  - end-to-end flow control, congestion control
- **Session Layer**
  - dialogue between applications (1/2 way, alternate)
- **Presentation Layer**
  - compression, encryption, conversion
- **Application Layer**
  - e-mail , FTP, HTTP,...

OSI STACK



FOCUS OF THIS COURSE

We're making a 2G voice call (simplified)

Now, let's really start from the application

What are the steps?

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.
11.
12.

PROFIT !

What are the steps?

1. Switch on the mobile (& infrastructure)
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits
5. Listen to synchronize and get system information
6. Pick a time to send
7. Wait for a response (try again)
8. Get a control channel assigned
9. Ask to make a call
10. Authenticate
11. Get voice channel and talk
12. … (location update, release call, handover, etc …)