



Comunicações Móveis

Mestrado em Engenharia de Computadores e Telemática
MIECT
1º Semestre, 2022/2023

Daniel Corujo, UA/IT

Mobile Networks

- Professors
 - Daniel Corujo (dcorujo@ua.pt) – DETI (UA)/IT
 - Francisco Fontes (fontes@alticelabs.pt) – ALB/IT

	Segunda	Terça	Quarta	Quinta
9:00				
9:30				
10:00				
10:30				
11:00				
11:30				
12:00				
12:30				
13:00				
13:30				
14:00				
14:30				
15:00				
15:30				
16:00				
16:30				
17:00				
17:30				
18:00				
18:30				
19:00				

Planning

- 13 weeks scheduled for theoretical and practical classes
 - Information in elearning...
 - English language in slides

Objectives

- Develop concepts associated to different types of mobile networks
 - Overall perspective of different wireless networks
 - Integration into a future vision, with heterogeneous environments.
 - “5G”-alike world.
 - Focus on networking, system and protocol aspects
 - IT-integration aspects mostly in other subject
 - Students should be able to:
 - understand future mobile network integrated systems;
 - understand new technologies and concepts of wireless communications;
 - be able to use their knowledge to react to the current changes in wireless networks

Program

Class #	Date	Topic
1	22/sep	Introduction Mobile Communications Multicast/Broadcast: Radio vs IP
2	29/sep	Mobile Networks models: the 802.x architecture. WSN, PAN, LAN, WAN, BAN
3	06/out	Wireless Local Networks: Wi-Fi and its evolving nature
4	13/out	Buletooth architecture: BT 3-4, and BLE. Overview of sensor networks and the ZigBee technology
5	20/out	Practical Work: Wi-Fi
6	27/out	Practical Work: Wi-Fi (part 2) + Bluetooth
7	03/nov	Cellular networks: from 1G to 4G
8	10/nov	Cellular networks: 5G Technological revolution (SDN, NFV, MANO, EDGE, ML/IA)
9	17/nov	Practical Work: Software Defined Networking
10	24/nov	WWSD: LoRa, SigFox, ...
	01/dez	Pratical Test (written) + Choice of Pratical Project
	08/dez	
11	15/dez	Project Work
12	22/dez	Project Work - Preliminary demo
13	05/jan	Demo and evaluation (full-day)

- The Lab will be used both for Theoretical and Practical classes

Evaluation criteria

- Theory: 50%
 - Exam at the normal season
 - Final exame (a.k.a. exame de recurso) will contain all subjects as well
- Practical: 50%
 - 15%: Written mini-test about the practical works (24/11)
 - 35%: Project Work
 - 10%: Preliminary Demo of on-going work (22/12)
 - 20%: Final Demo (5/1)
 - 10% for the demo itself
 - 5% for the overall joint presentation
 - 5% for students' individual answers to questions
 - 5% for the written report

Organization

- All information to be displayed in e-learning
 - Announcements
 - Classes handout
 - Practical works
 - Evaluation and grades
- Summaries in paco.



Mobile Networks Introduction

Aula da Cadeira Comunicações Móveis

Daniel Corujo

dcorujo@ua.pt

2022/2023

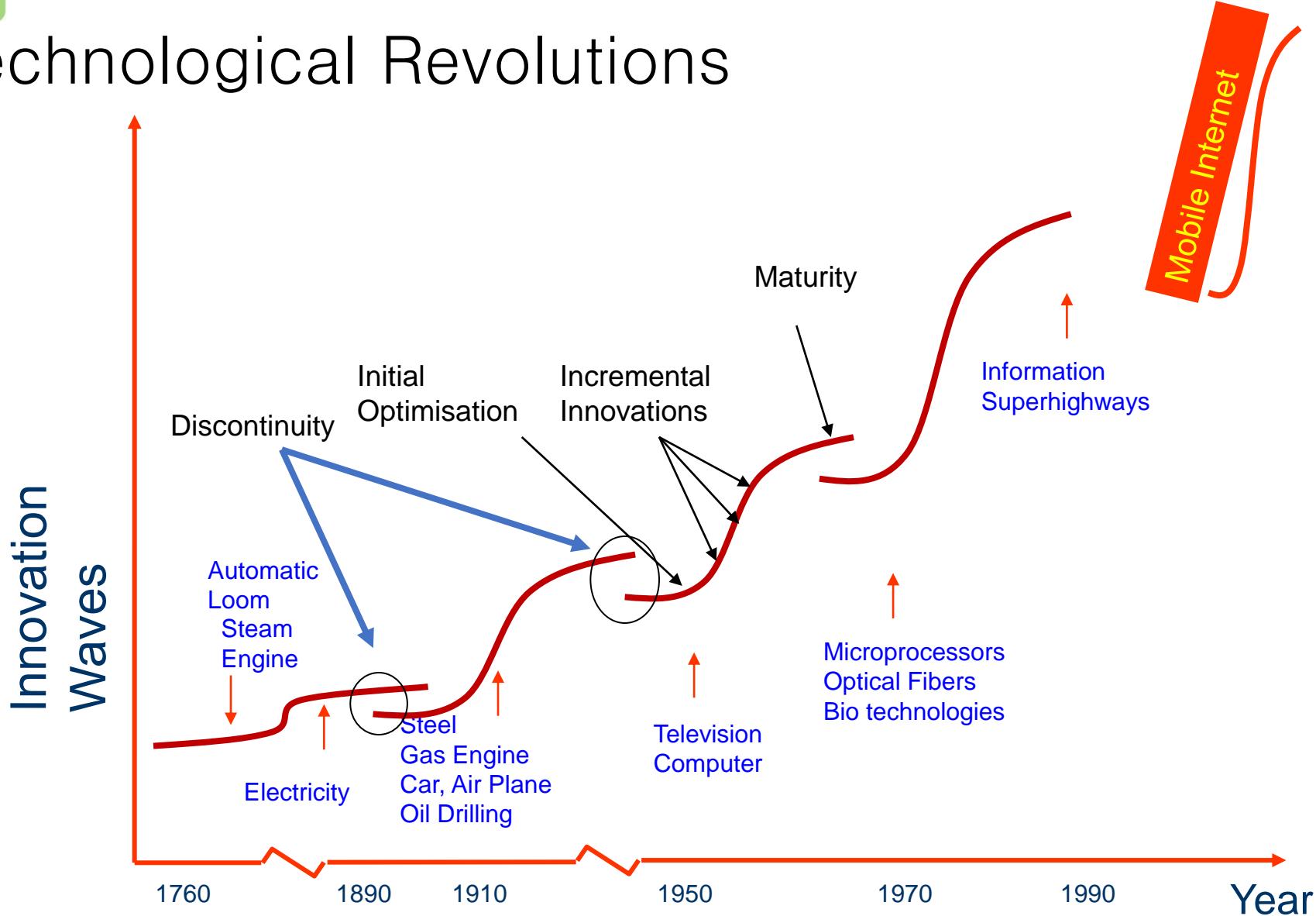


The communication network

Trends and history



Technological Revolutions





The weight of time

The beauty of networking effects

Everybody uses it

The ugliness of networking effects

Now everybody uses it...

Society takes time

- Business
- People habits
- Technology interoperation



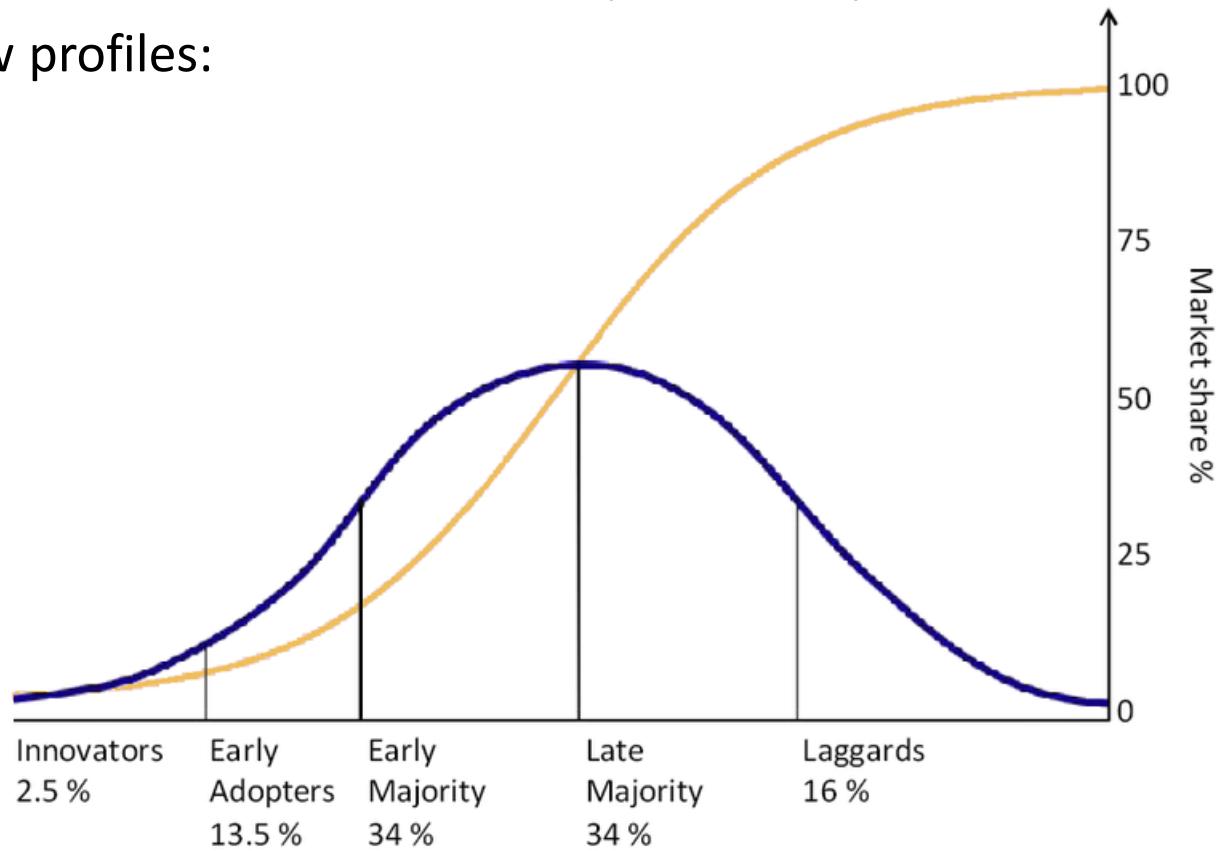
How networks evolve?

- Real life evolution is complicated
 - Depends on real life – technologies, business, society, relationships, laws, ...
- Users are shaping communication networks
 - Networks are no longer a business/technology binomial, but strongly depend on users acceptance of (or requirements for) change
 - “Killer ideas” are often unpredictable
- Legacy is a major issue
 - Large networks cannot be changed instantaneously
 - Mobile is particularly lenient in this aspect (why?)



The user

- Internet is being challenged by its own success
 - Internet initially designed for expert users
 - Now more than 63% of the world online (statista.com)
- Users follow profiles:
 - Techs
 - Business
 - Teens
 - “World”
 - “Oldies”





Trends in communications

- Current telecommunication industry has been the result of different trends in the last 40 years:
 - The saturation of the telephone market, at the end of the 80's
 - The coming of age of the data world, in the early 90's
 - The pervasiveness of mobility, in the mid 90's.

Note: many upcoming slides with statistics are dated around 2010, when 3G was established in Western Europe, and we were moving to 4G.

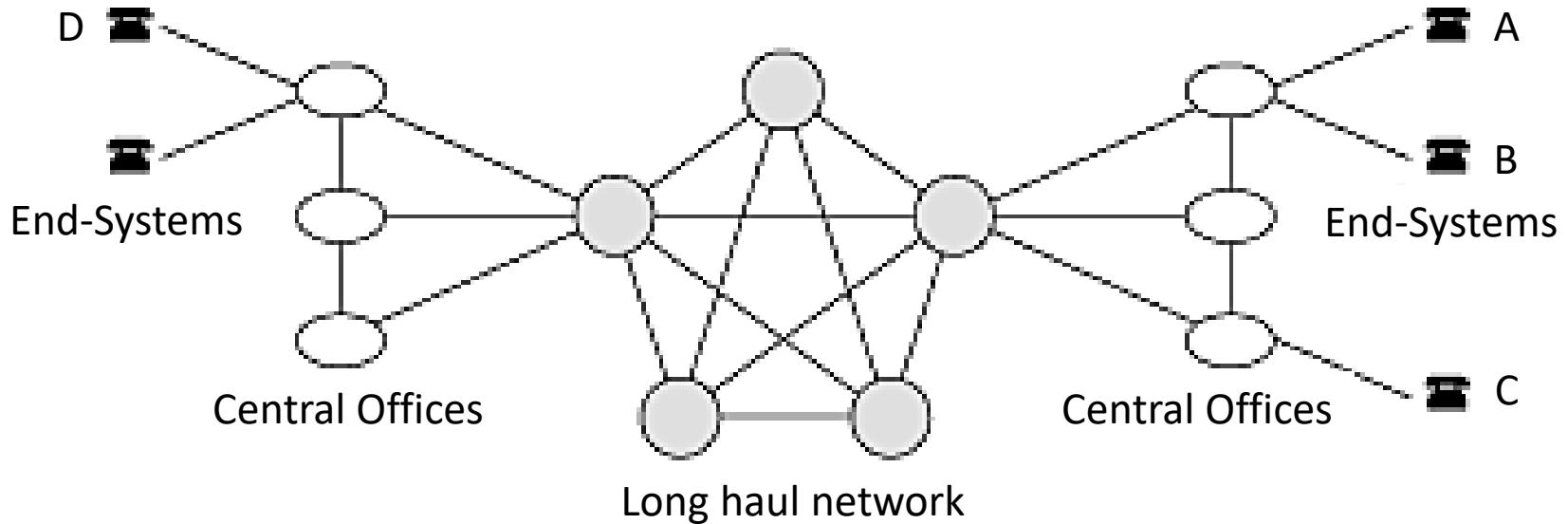


The communication network

The phone network



Telephone System



- Uses switched circuits (virtuals...)
- Access via low bandwidth circuits
- “out-of-band” call establishment using signaling system based in packets (SS7)
- Channels between switching exchanges carry multiple calls
 - Multiplexing (analogue or digital)

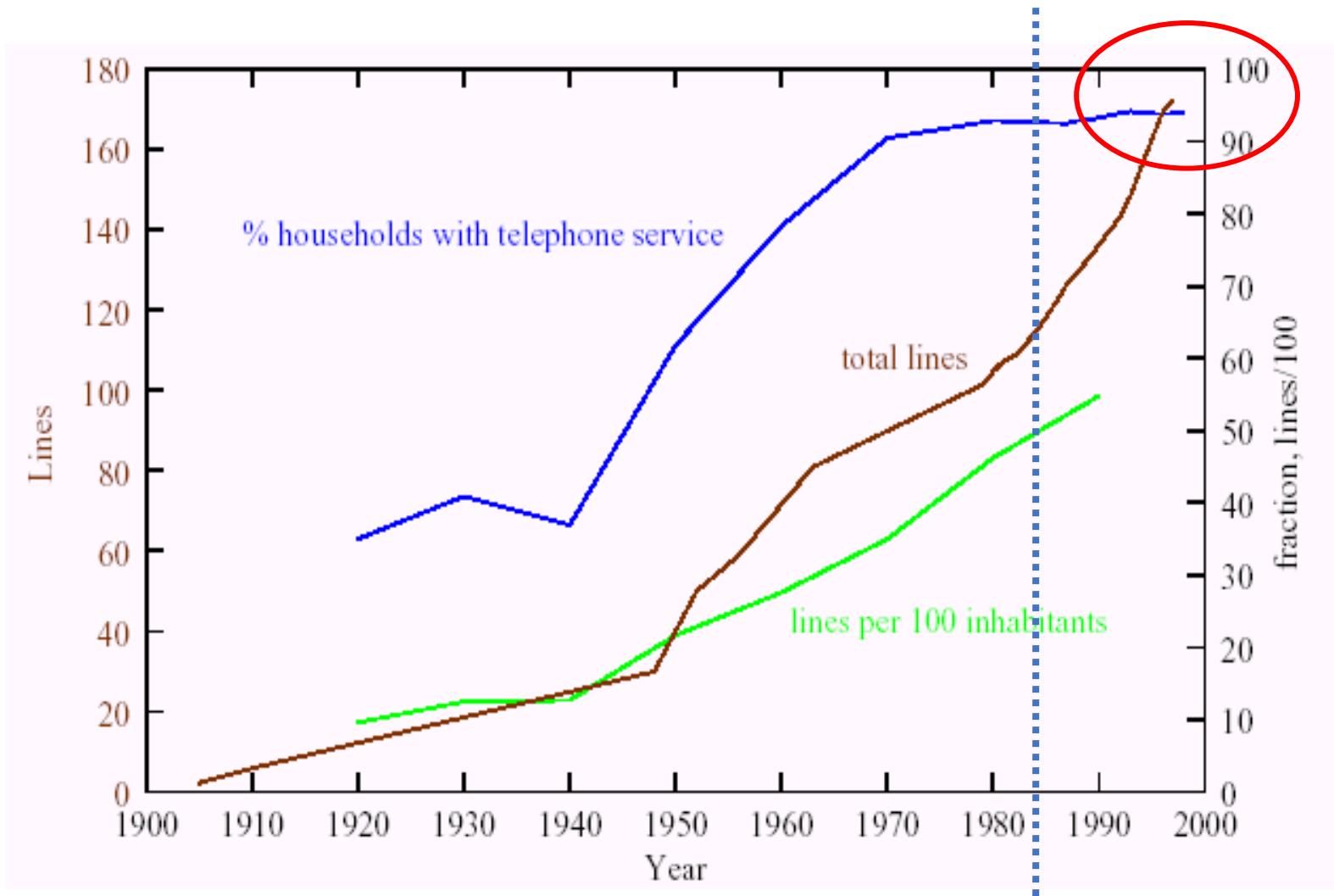


Public telephony (PSTN): history

- 1876 invention of the phone
- 1915 first transcontinental connection (NY–SF)
- 1920's first automatic switching exchanges
- 1956 transatlantic cable TAT-1 (35 linhas)
- 1962 digital transmission (T1)
- 1974 Internet: voice over packets
- 1977 digital switching exchange
- 1980s Signaling System #7 (out-of-band)
- 1988 RDIS (ISDN Blue Book)
- 1990s Intelligent Networks
- (1990s ATM)
- 2000 local bundle liberalization (Europe)



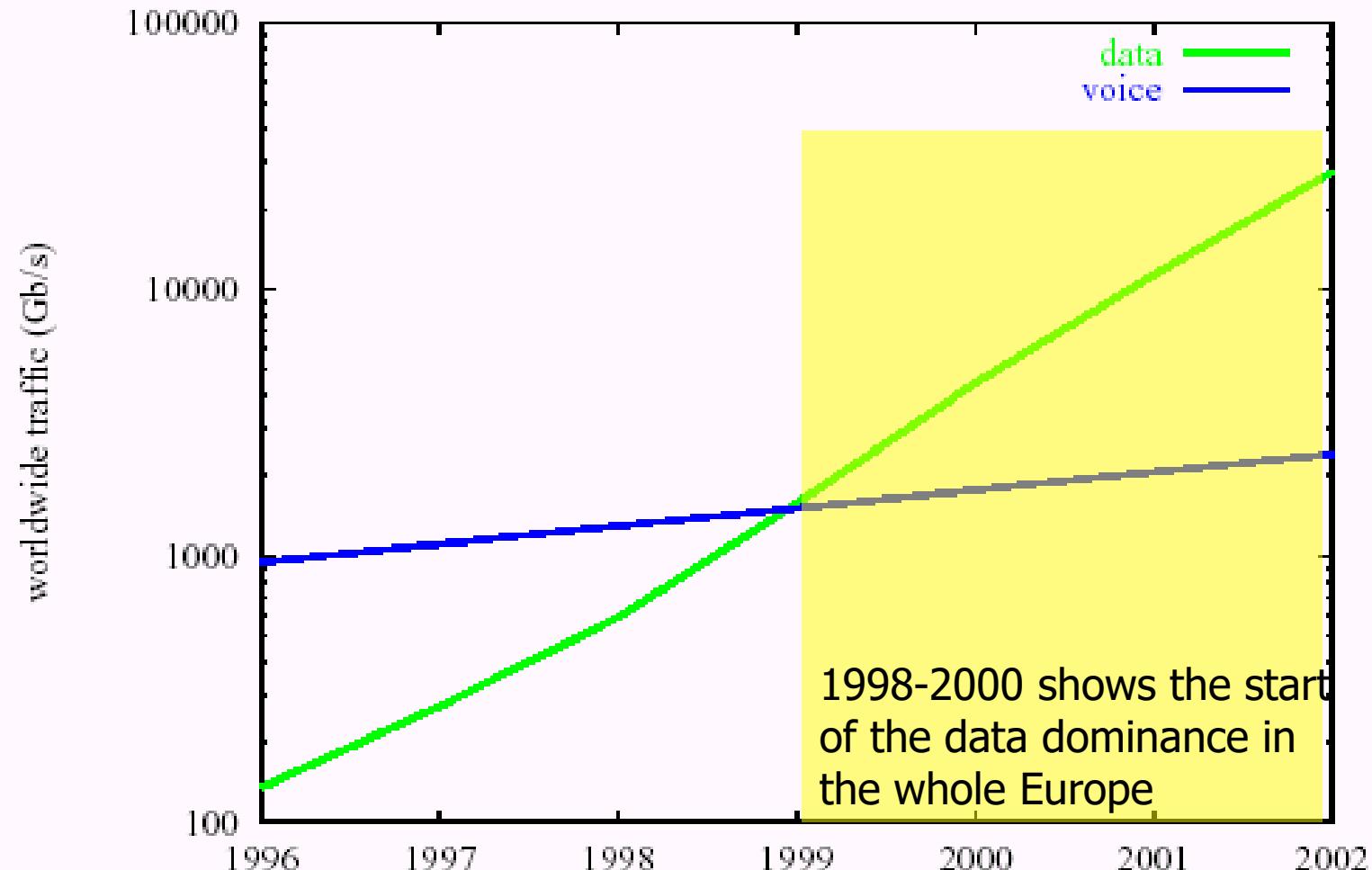
11 Phone service in US



AT&T Divestiture



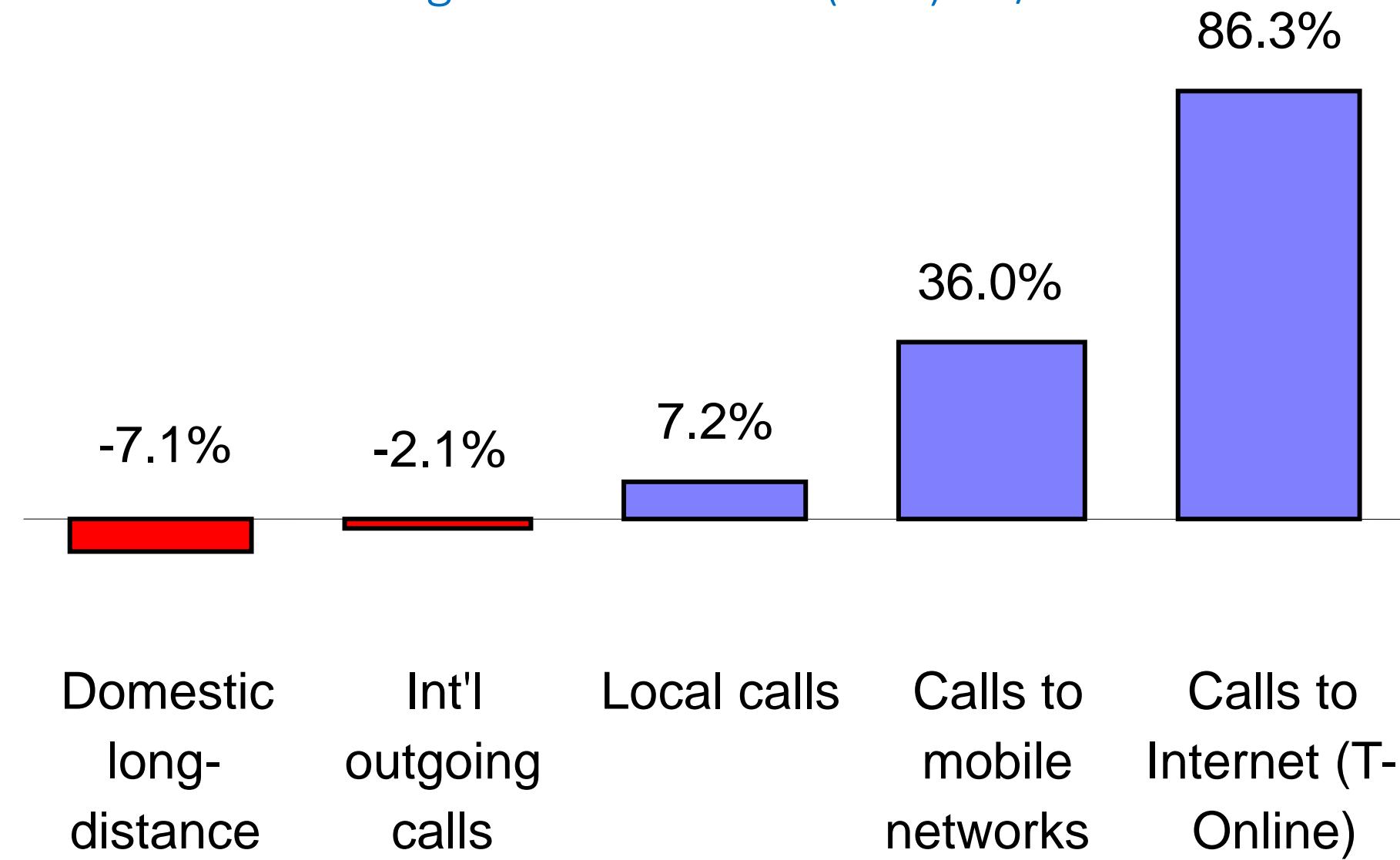
Evolution: Voice vs Data





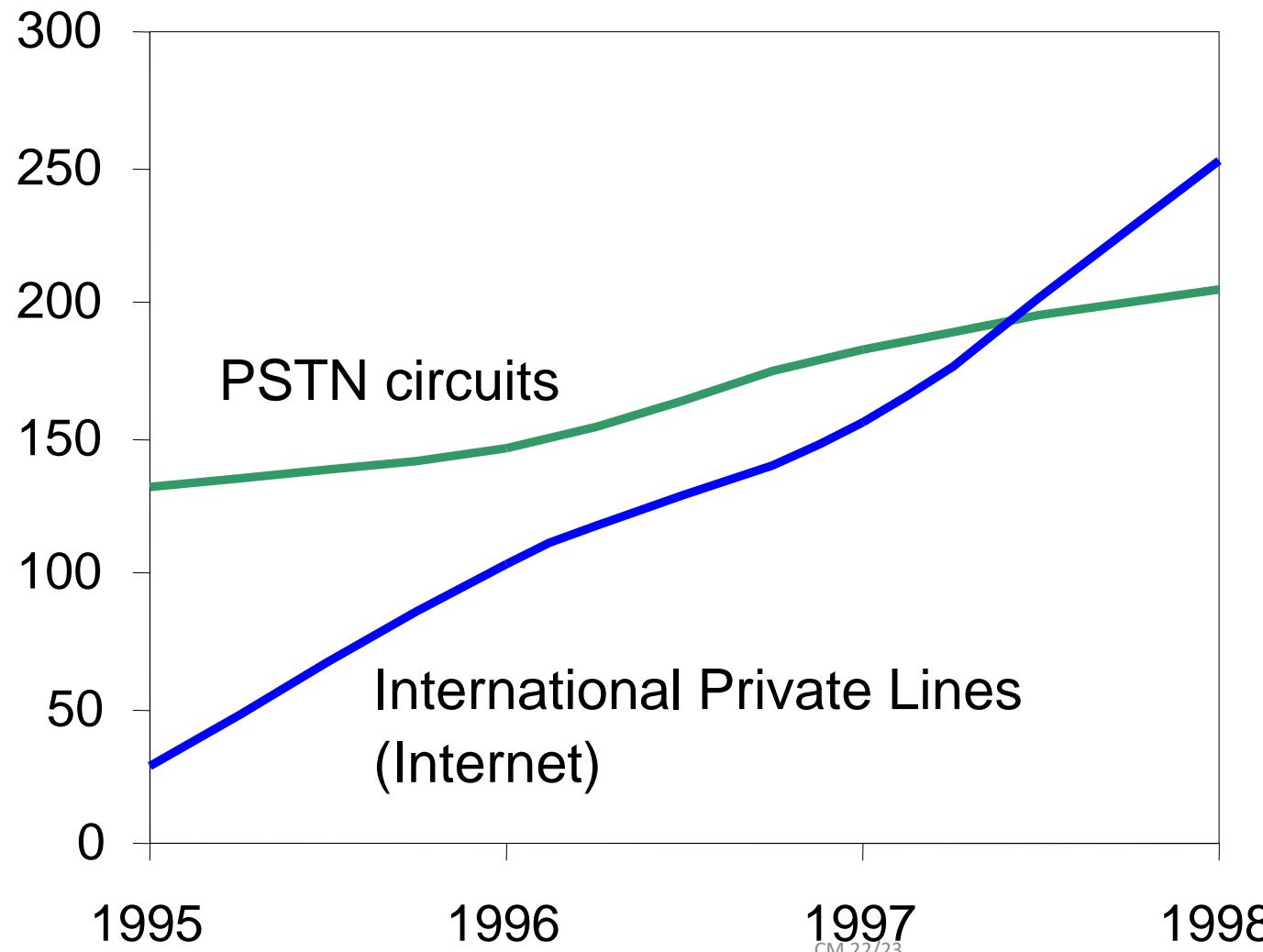
Deutsche Telekom

% change in call volume (min) 98/99

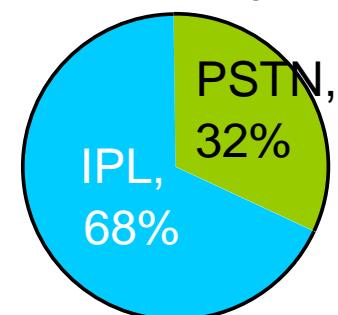




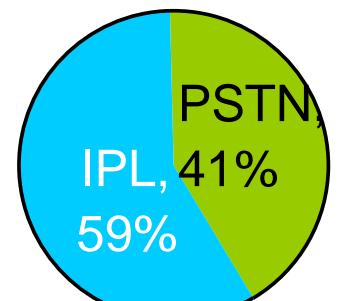
Number of int'l circuits in use, worldwide, and by region 1998
(in thousands)



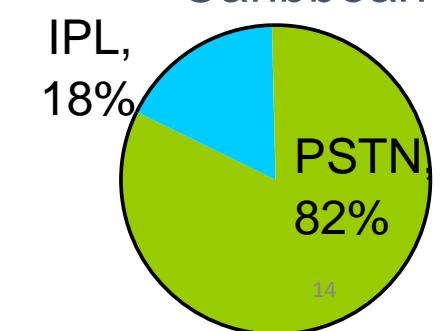
Western Europe



Asia



Caribbean



Source: FCC. Applies to US carriers only.



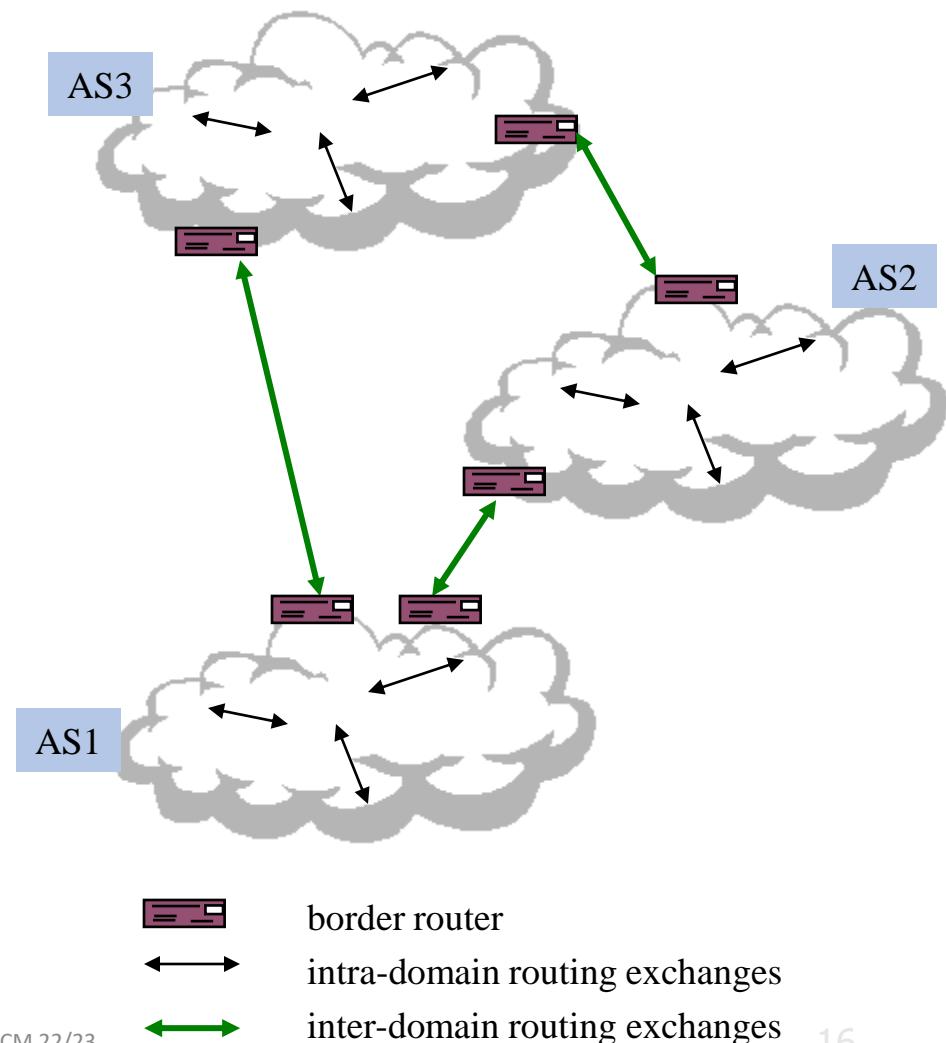
The communication network

The Internet



Internet structure

- Administrative borders define
 - Autonomous Systems (AS)
 - **Intra-domain routing**
 - Individual internal policies
 - May use different metrics between domains
 - protocols: RIPv2, OSPFv2
- AS interconnections
 - **Inter-domain routing**
 - Connectivity information
 - protocols: BGP



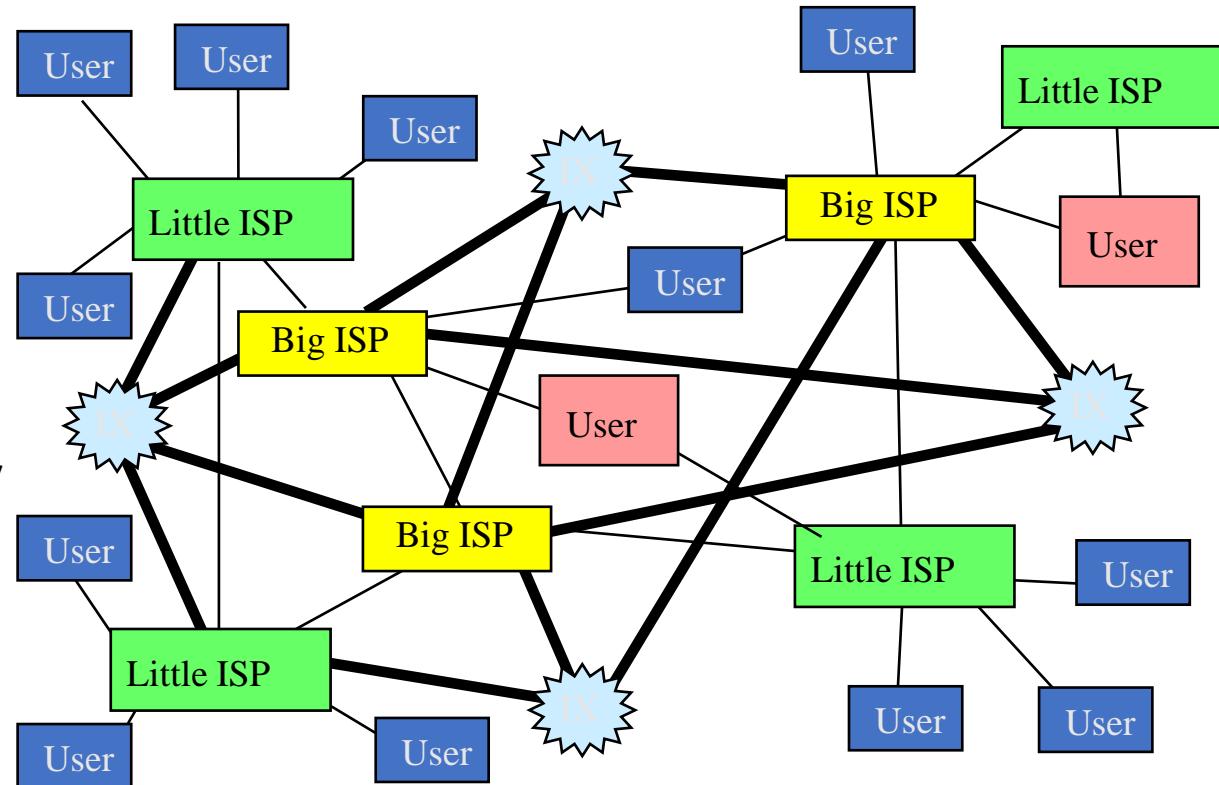


Internet: currently

- Self-organized set of interconnected autonomous components
 - More than 60.000 autonomous domains (with more than 100K numbers allocated)
 - Single guarantee is running TCP-IP
 - Works by packet switching
 - More than 340 millions of registered domains (URL)!
- Commercial traffic larger than non-commercial
 - Exponential growth in all numbers (number of users, traffic)
- Different machines (networks) can offer different services
 - Each user can select what it uses
- Only bi-directional media that support communications
 - One to one (unicast, e.g. email); one to many (multi-cast, e.g., electronic news)
- NB: Internet networks are operated AUTONOMOUSLY
 - After connecting to the Internet, the network **becomes PART of the Internet**



Real structure



- Apparently hierarchical
 - Backbone ISP provides service to increasingly smaller ISPs
 - Smaller ISPs eventually providing service end users.
- But hierarchy is not respected
 - Private connection agreements
 - Mechanisms for improvement of the network
 - All companies provide service to (some) users
 - Service providers connect to multiple connection provider
 - Users connect to multiple ISPs



“Data vs voice”: packet switching vs circuit switching

Packet switching solves everything?

- Great for burst information
 - Resource sharing
 - No call setup time
- When excessive congestion: delays and losses
 - Needs reliable data transfer protocols
- Providing circuit switching services?
 - For multimedia applications we need bandwidth and delay
 - Problem not yet completely solved

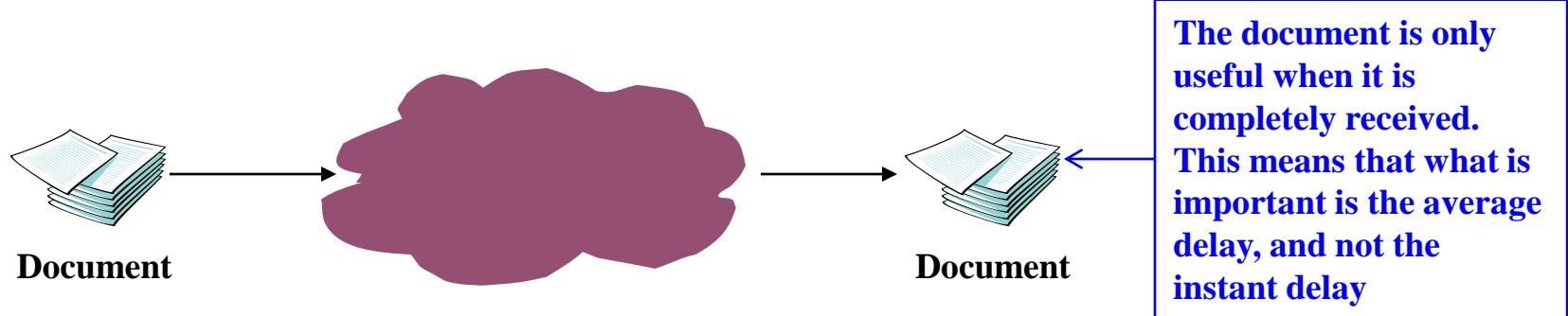


Transport service (operador/ISP) vs applications

- Packet loss
 - Some apps (audio/video real time) handle losses
 - Other applications (file transfer, telnet) require 100% of success in transmission
- Bandwidth
 - Some applications (multimedia) need a minimum bandwidth to be effective
 - Other applications (“elastic applications”, ex. email, file transfer) use the bandwidth available
- Timing
 - Some applications (Internet voice, multiuser games) require low delays to be effective
 - Other applications (without real time requirements) do not have strict delays end-to-end.



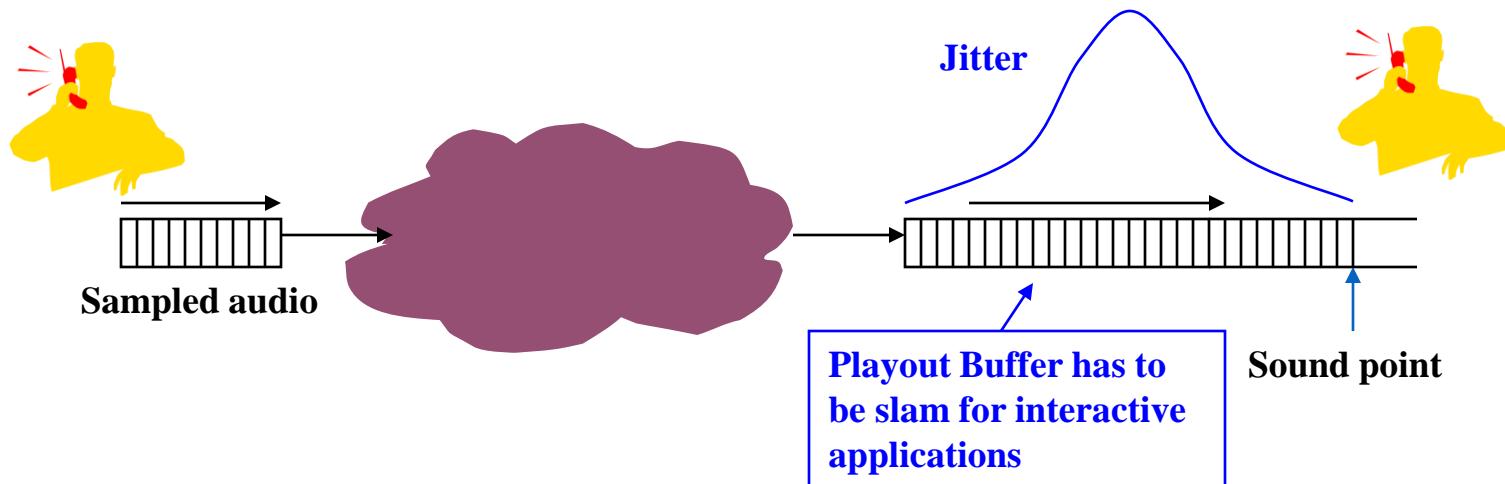
Elastic operations



- Elastic applications
 - Interactive data transfer (e.g. HTTP, FTP)
 - Sensitive to the medium delay, not to rare occurrences
 - Bulk data transfer (e.g. mail, news)
 - Not sensitive to delay
 - Best effort works...



Inelastic applications



- Interactive applications
 - Sensitive to packet delay (telephony, gaming)
 - Maximum delay may be limited
- Non-interactive applications
 - Adapt to larger ranges of delays (streaming audio, video)



Application requirements

Applications	Losses	BW	Timing
File transfer	lossless	elastic	no
e-mail	lossless	elastic	no
Web documents	lossless	elastic	no
Real time audio/video	supports	audio: 5K-1Mbps video:10K-5Mbps	yes, 100's ms
Streamed audio/video	supports	See above	yes, few secs
Interactive gaming	supports	Some Kbps	yes, 100's ms
Finance applications	lossless	elastic	Yes and no



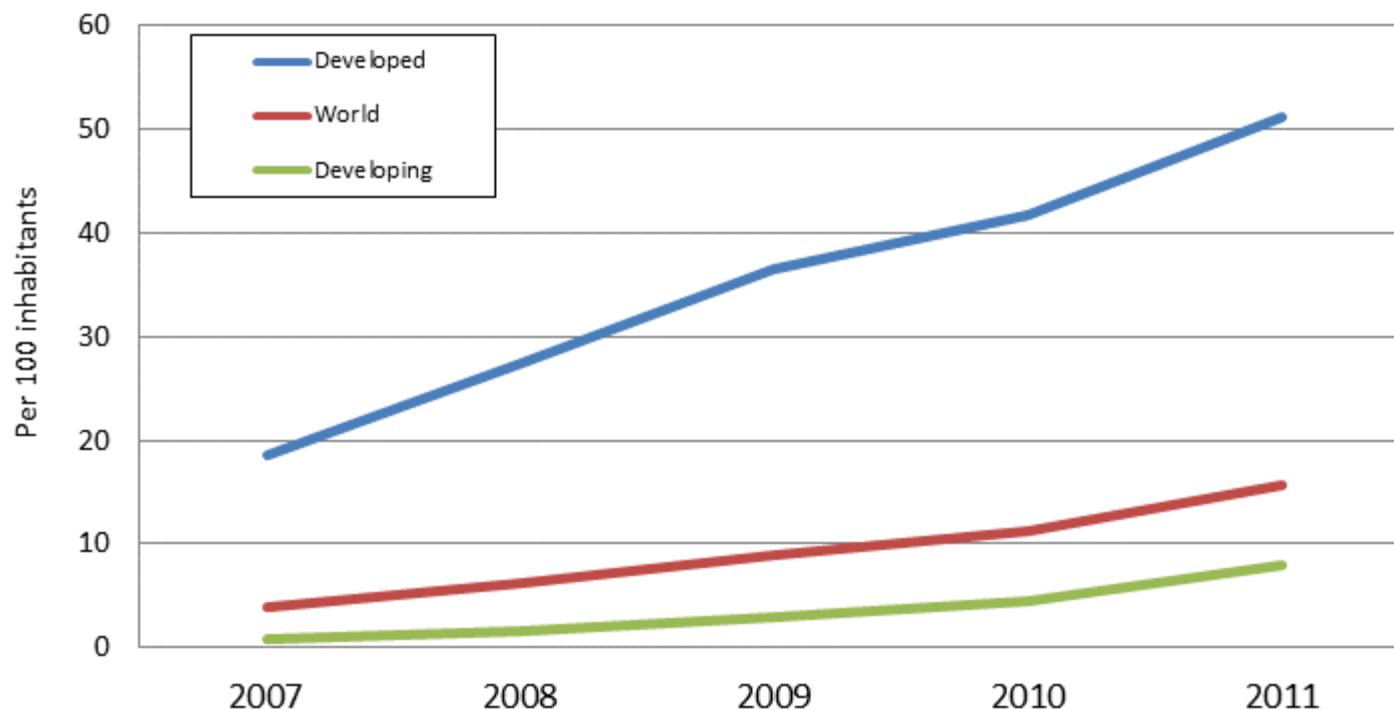
The communication network

The Mobile network



Data vs voice traffic

**Active mobile-broadband subscriptions per 100 inhabitants,
2007-2011**



The developed/developing country classifications are based on the UN M49, see:

<http://www.itu.int/ITU-D/ict/definitions/regions/index.html>

Source: ITU World Telecommunication/ICT Indicators database

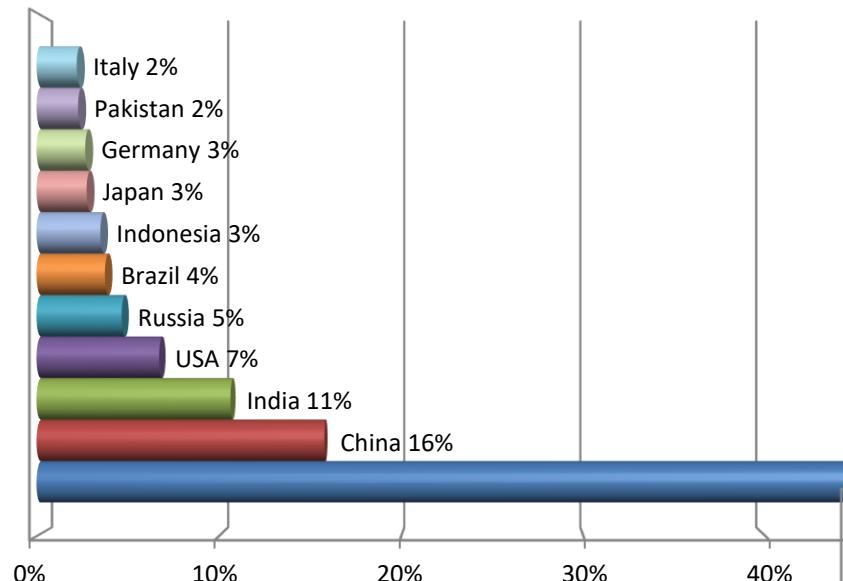


Dec/2004 → Sep/2014

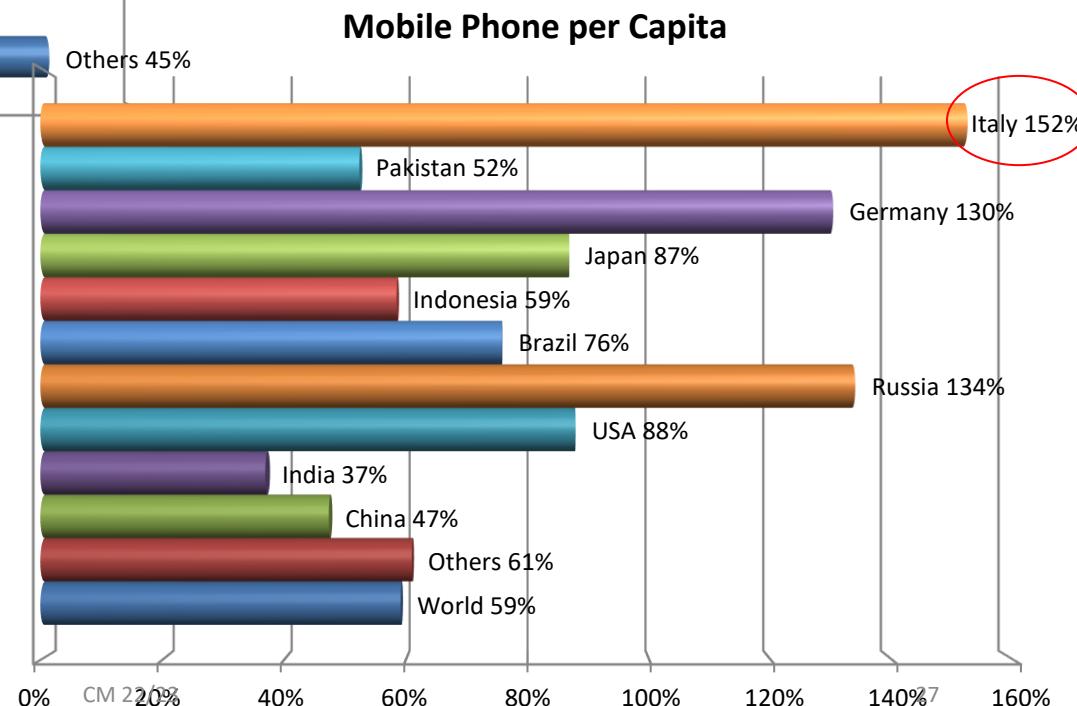
- Global Mobile Users 1.52/6.91 billion (Analogue Users 34/0?m)
- Global GSM users 1.25/4.4 billion
- Global CDMA Users 202/701m Global TDMA users 120/0?m
- US Mobile users 140/ 335.6m
- Total European users 342.43/780m
- Total African users 53/629.7m
- Total 3G users 130m/ 1880m
- #1 Mobile Country China (300/1273m) (GSM 282/582m)
- #1 Network In Europe T-Mobile (28m)
- #1 In Infrastructure Ericsson
- Global monthly SMS 36/400 per user
- SMS Sent Global 135 billion/10000 billion
- SMS sent in UK 3/2004 2.1 billion

Mobile Market

Mobile Phone World Distribution



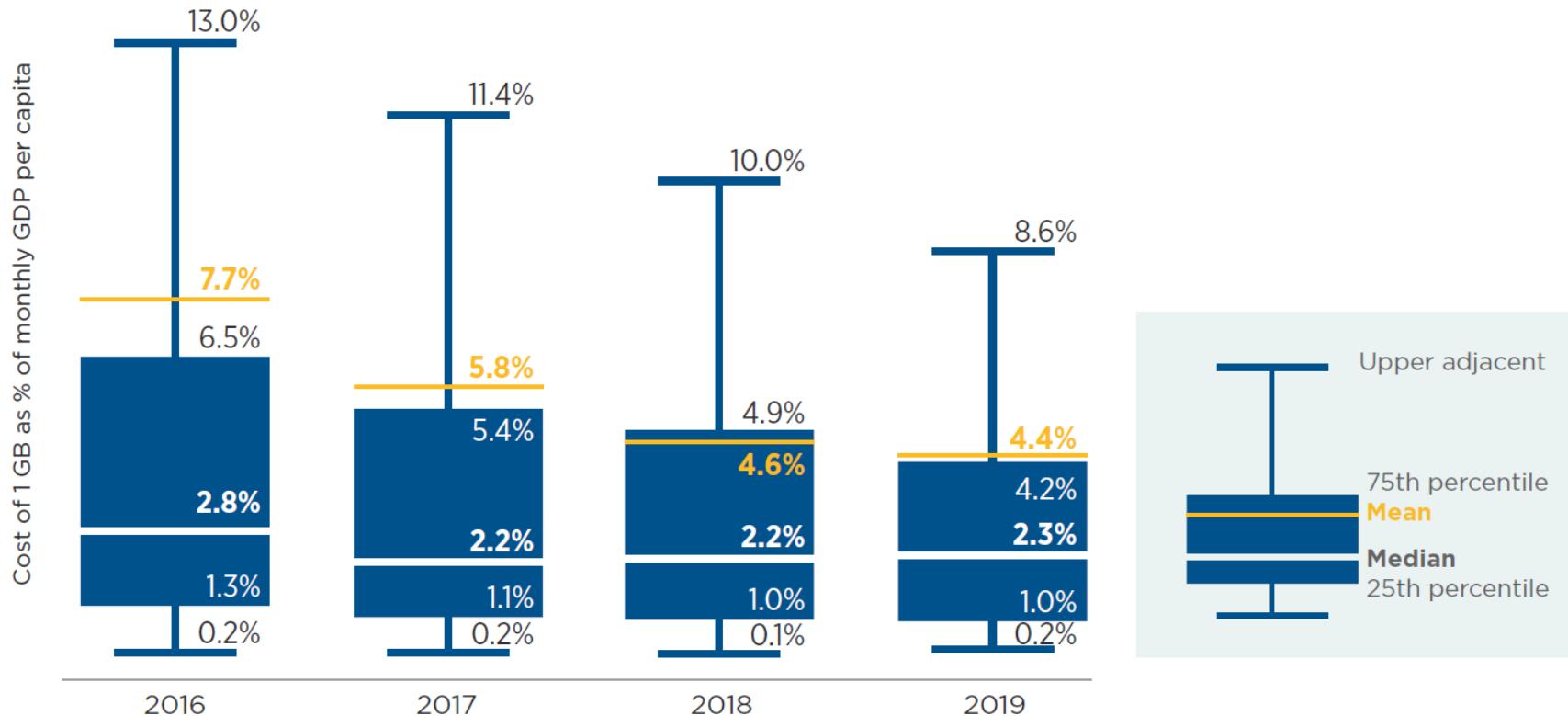
Mobile Phone per Capita



Source: Frost and Sullivan

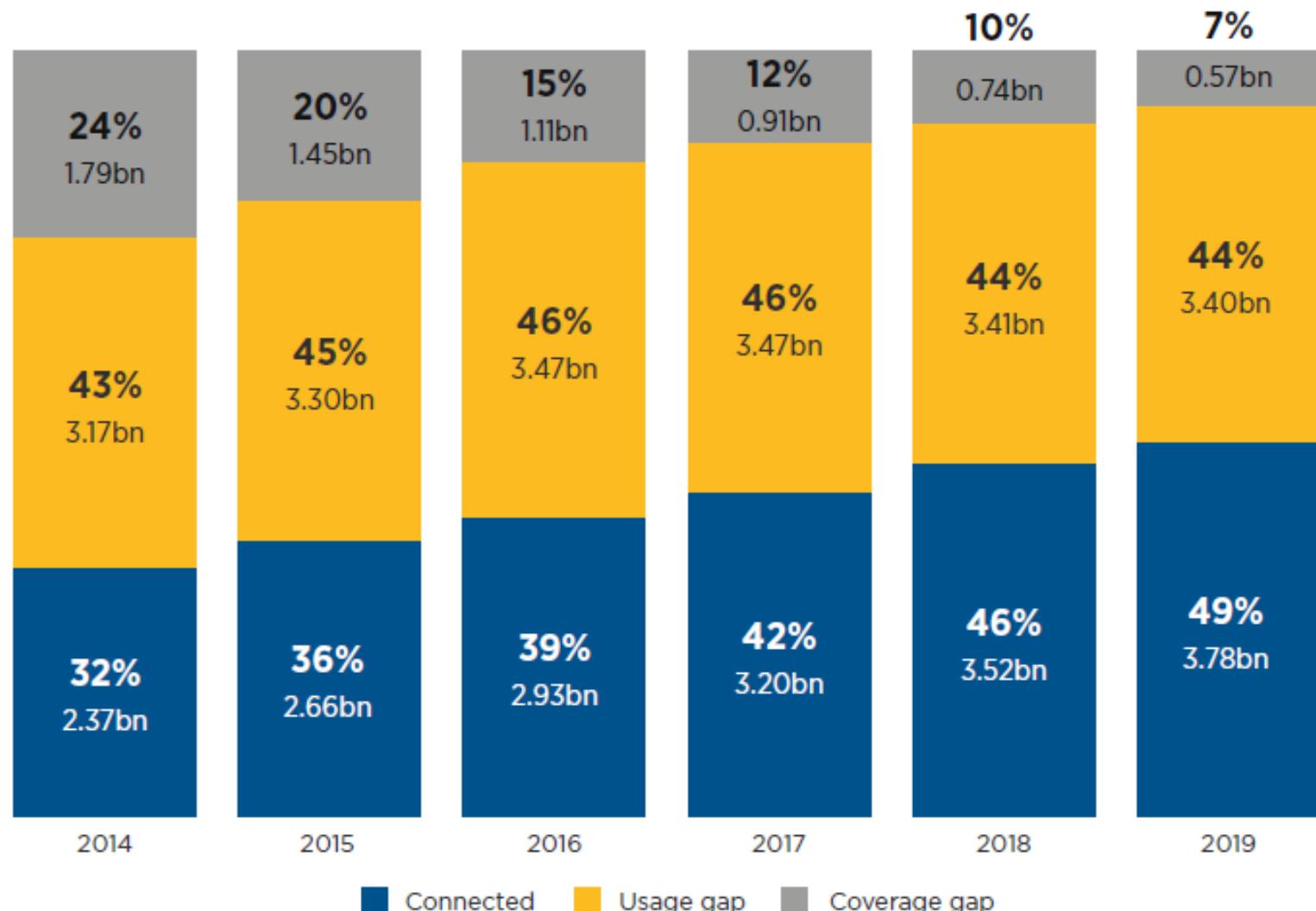


Affordability of 1 GB of data in LMICs, 2016–2019





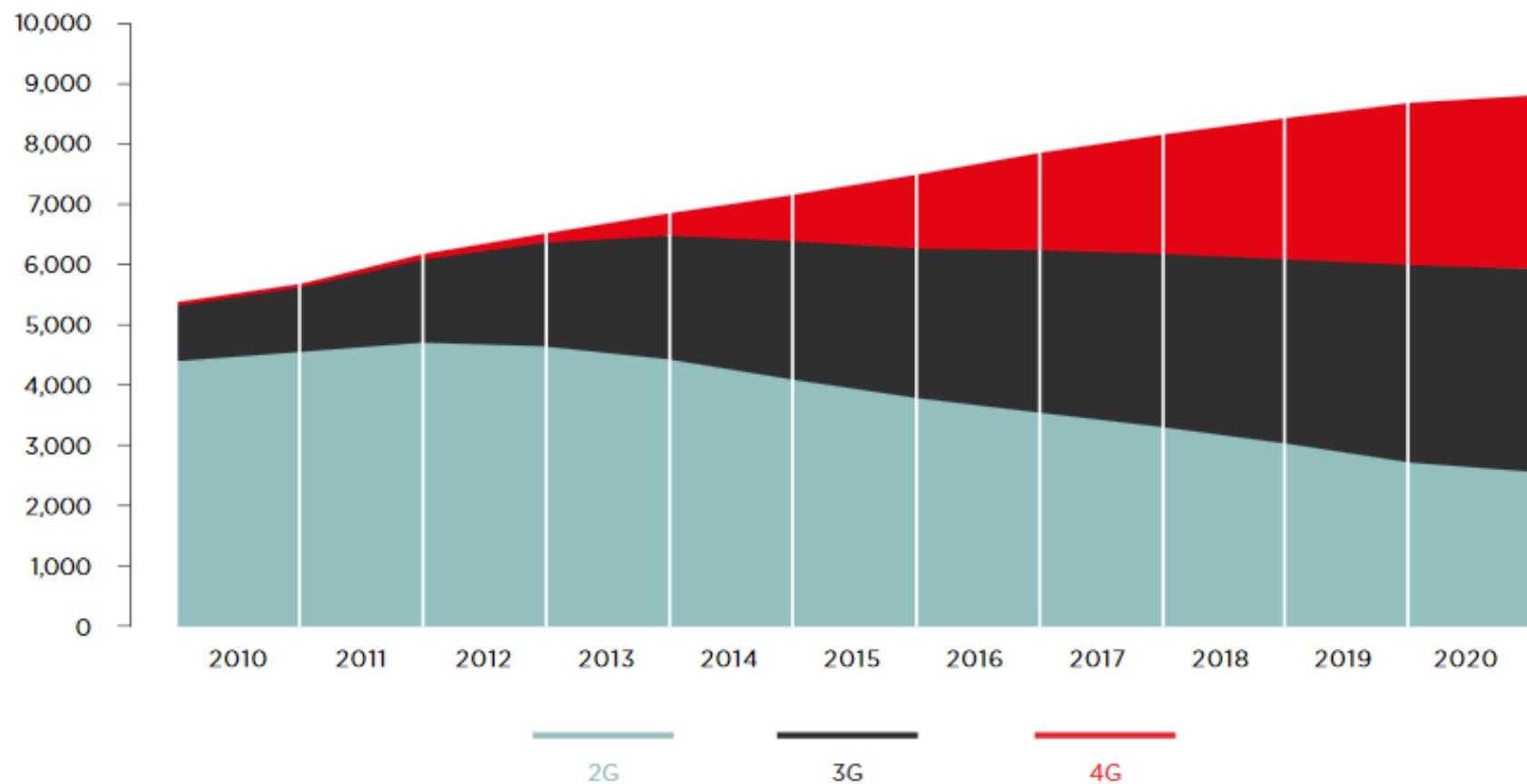
Evolution of global mobile internet connectivity, 2014–2019





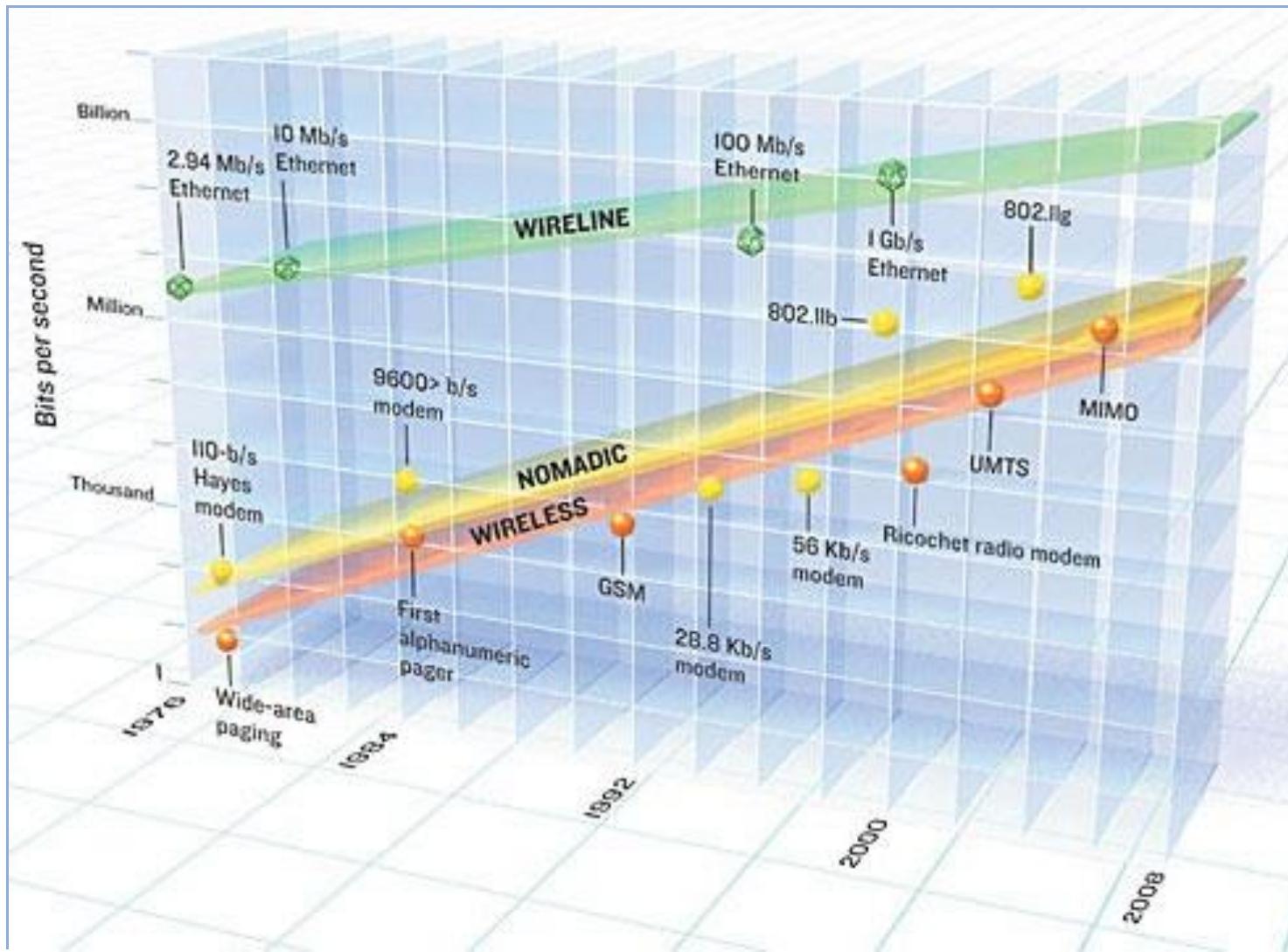
Global connections by technology

(millions, excluding M2M)



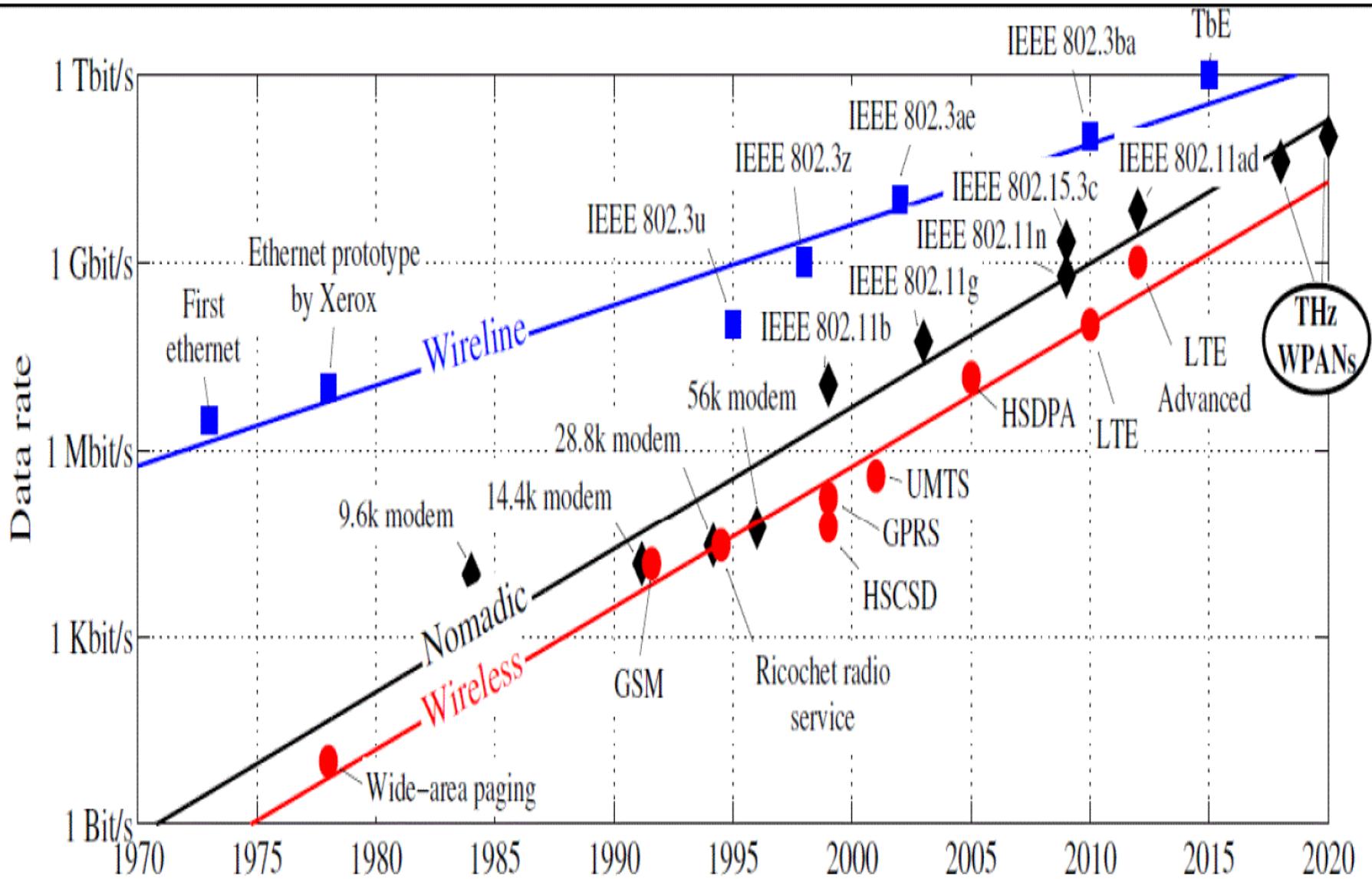


Edholm's Law





Fedholm's Law

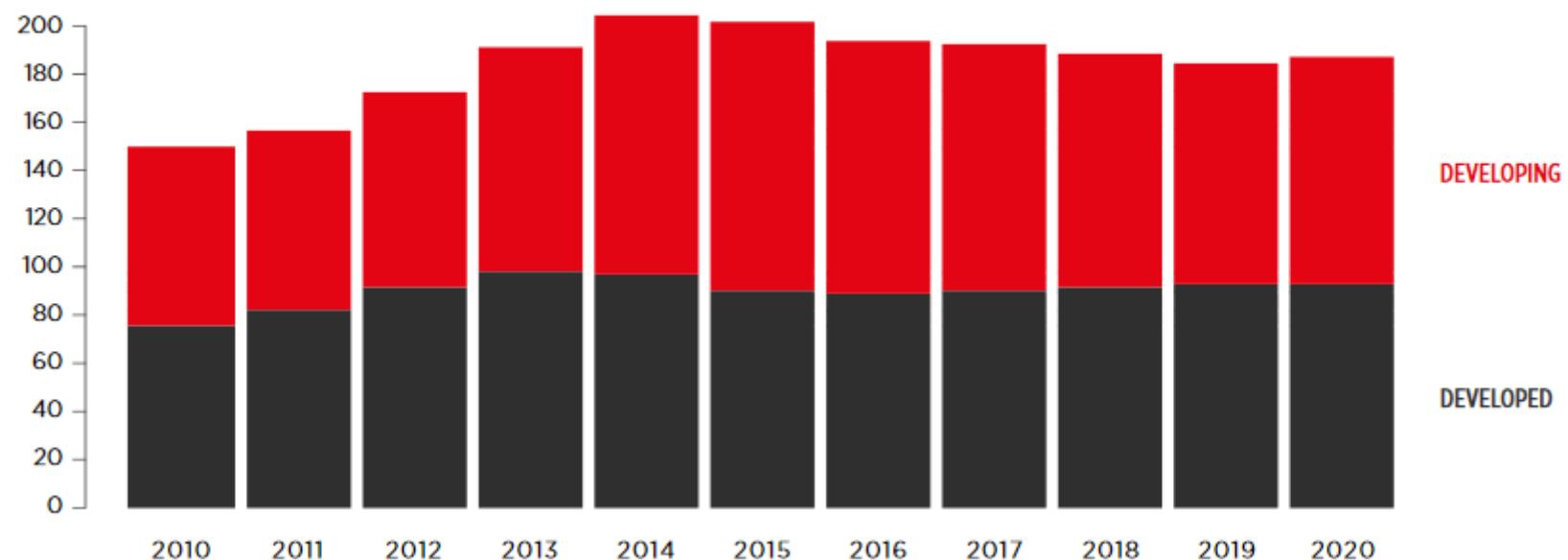




Cost of investment in telecom

Global mobile operator capex

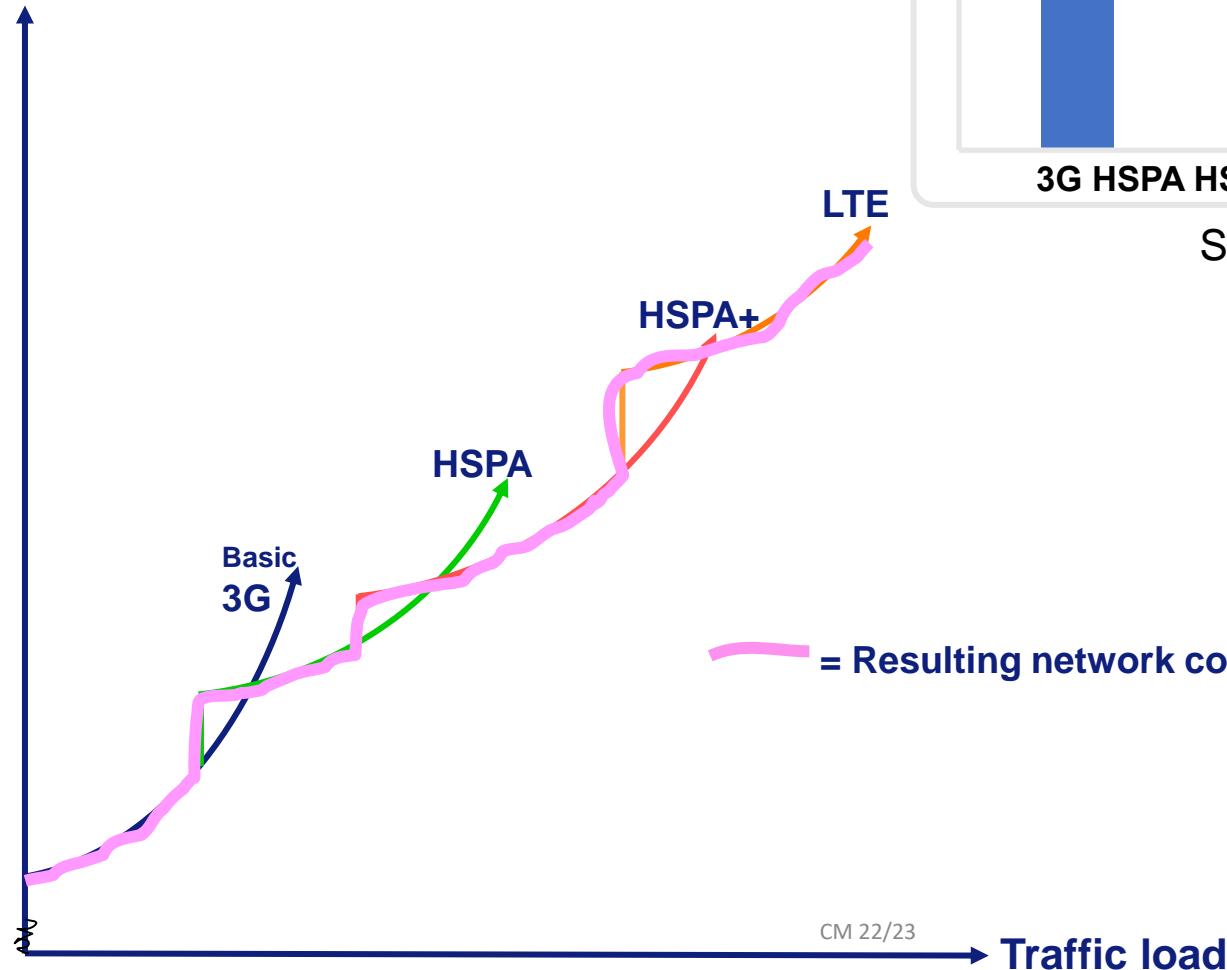
(\$ billion)





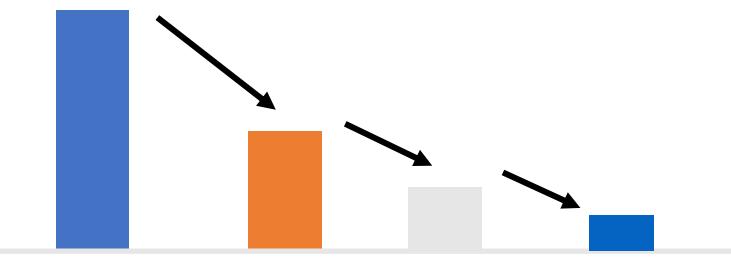
Motivations for technologies

Network cost

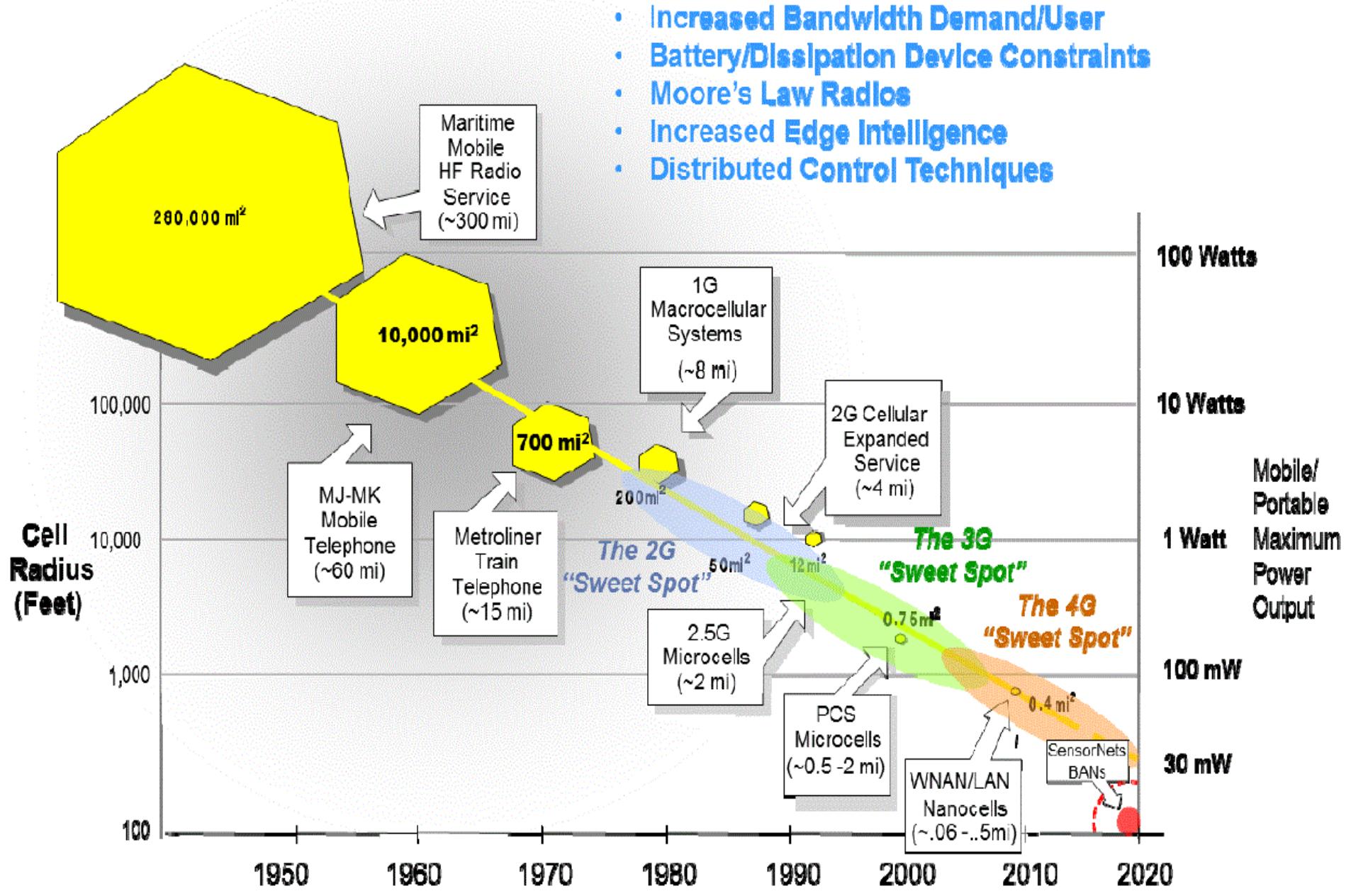


Lower production cost per bit

Cost per Mbyte

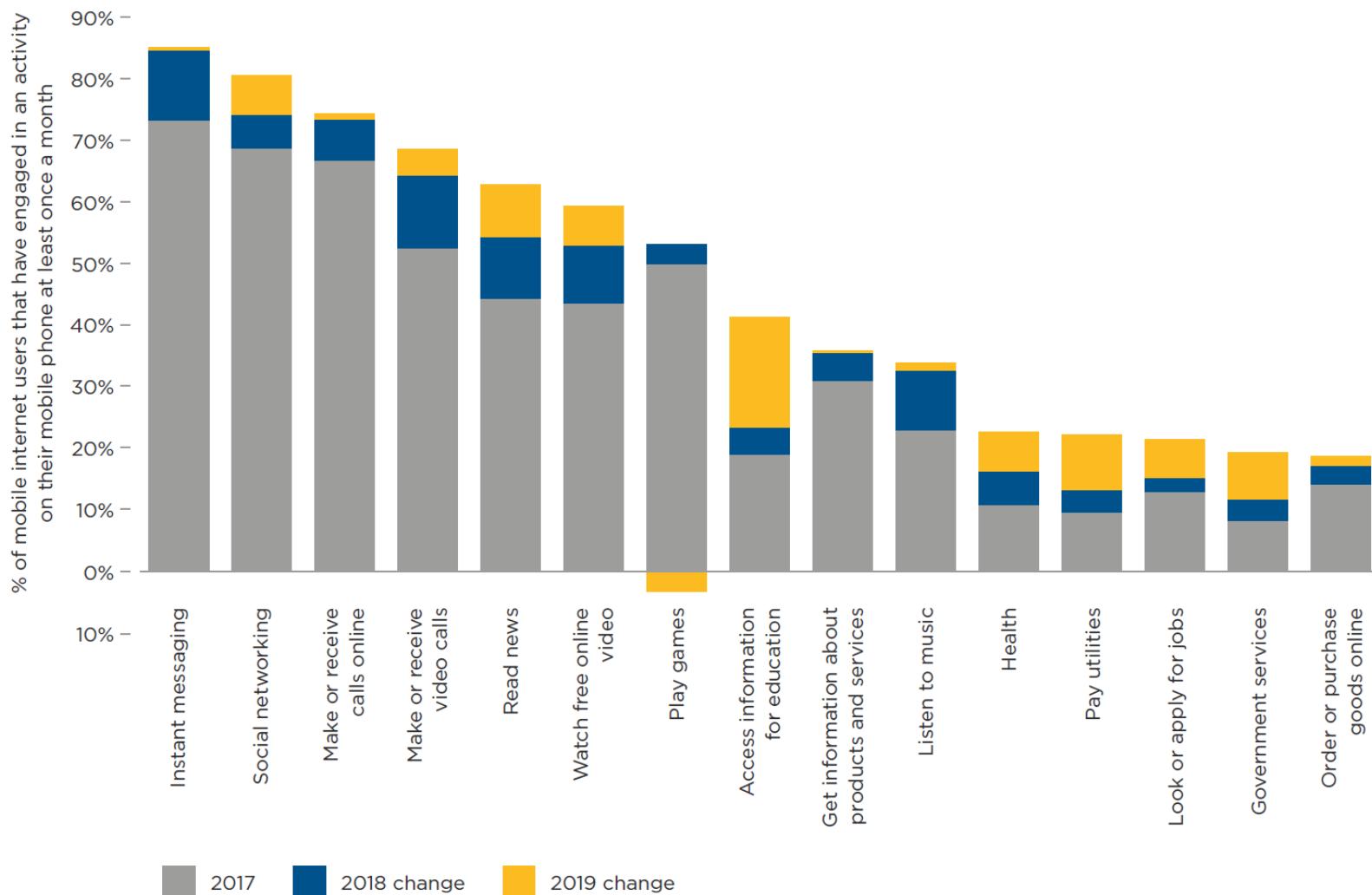


Source: NSN



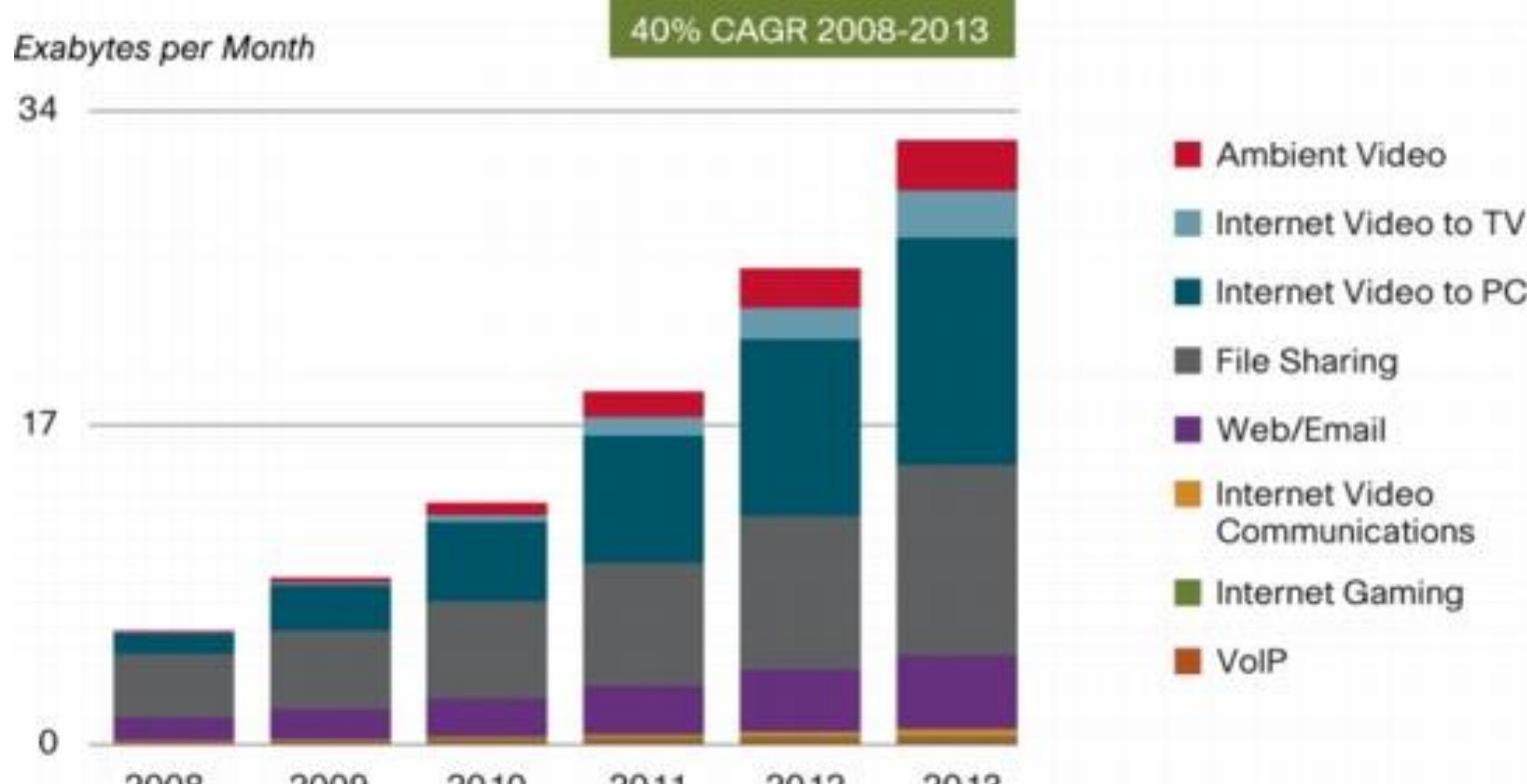


Activities undertaken on mobile internet based on usage in surveyed LMICs, 2017-2019





Consumer Traffic, VNI

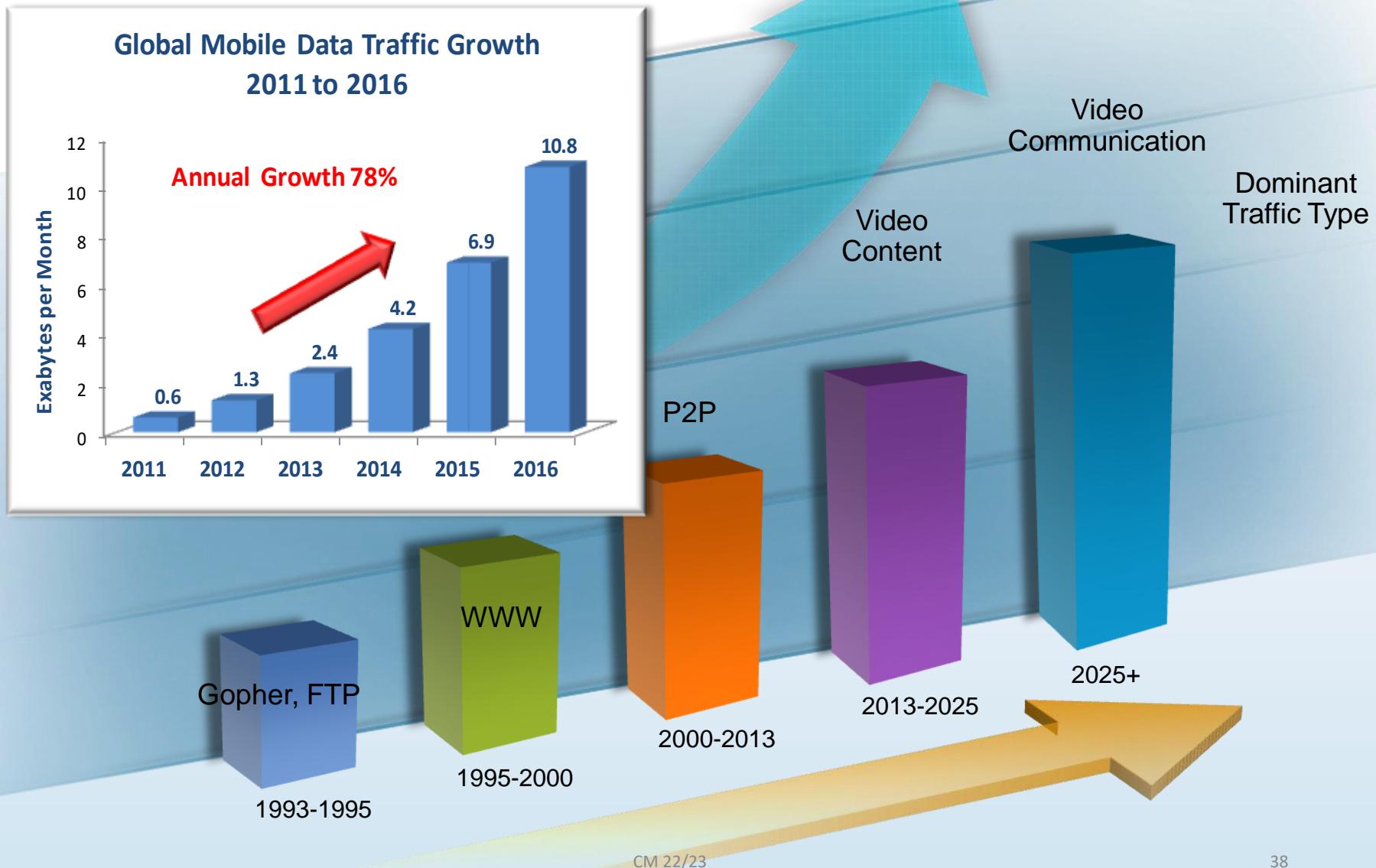


Source: Cisco VNI, 2009

- http://newsroom.cisco.com/dlls/2009/prod_060909.html
- 1 Exabyte is appr. 250 mill. DVD's



Dramatic Traffic Growth Fueled by Video





The things that surround us





Network is now more than bits and bytes – it adapt to users





GIGAOM

THE APP STORE ECONOMY

THE APP STORE CONTAINS
133,979 APPS 

AVAILABLE FOR 

MADE BY OVER
28,000 DEVELOPERS

WHO WAIT AN AVERAGE OF

4.78 DAYS 

FOR THEIR APP'S APPROVAL

APP STORE **USERS**

DOWNLOADED AN AVERAGE OF

3.7 APPS EACH IN DECEMBER

Service market (2016)

Mobile Services are now a major contention between operators and manufacturers (AppleStore, OviStore, Android Market, Palm App Catalog)

Source: GigaOM

ONE QUARTER OF WHICH WERE PAID

TOP 50 PAID APP PRICES

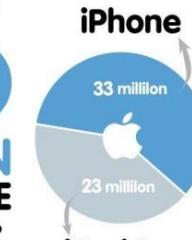
99¢	25
\$1.99	6
\$2.99	8
\$3.99	1
\$4.99	3
\$5.99	2
\$6.99	4
\$7.99	0
\$8.99	0
\$9.99	1

AT AN AVERAGE COST OF **\$2.59**

EACH iPhone USER SPENDS AN AVERAGE OF **\$10** ON APPS EVERY MONTH.

WITH OVER

56 MILLION APP STORE USERS,



200 MILLION APPS ARE BEING DOWNLOADED

MONTHLY, 

GENERATING MORE THAN

\$500 MILLION IN REVENUES

OF WHICH 30% GOES TO **APPLE & 70% TO DEVELOPERS** ...EACH MONTH.

For more information, visit [GigaOM.com](#), [AdMob.com](#), [Apple.com](#)

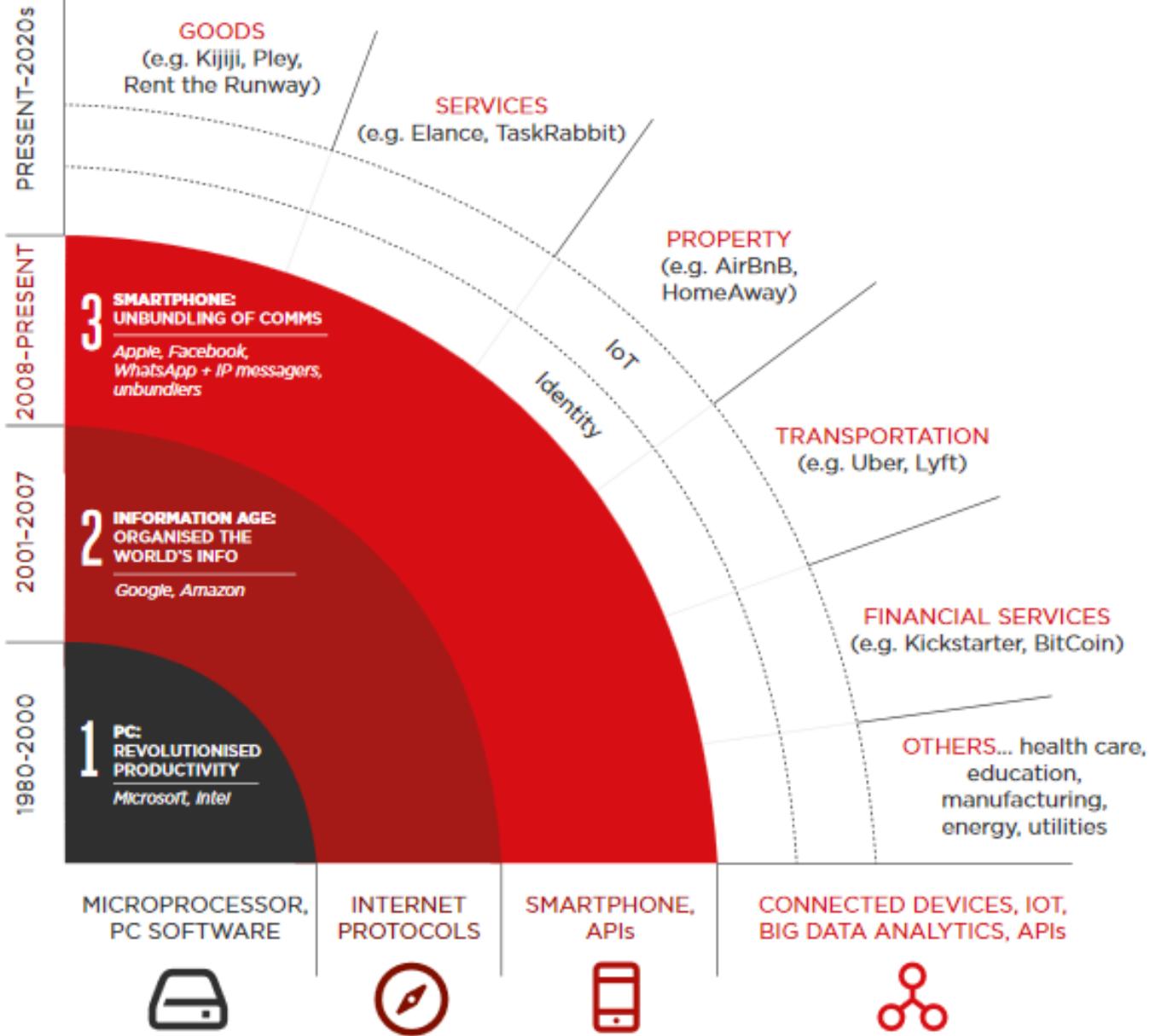


The (mobile) Internet economy (2016)

Rank	Company	Region	Current Market Value (\$B)	Q1:16 Cash (\$B)	2015 Revenue (\$B)
1	Apple	USA	\$547	\$233	\$235
2	Google / Alphabet	USA	510	79	75
3	Amazon	USA	341	16	107
4	Facebook	USA	340	21	18
5	Tencent	China	206	14	16
6	Alibaba	China	205	18	15
7	Priceline	USA	63	11	9
8	Uber	USA	63	--	--
9	Baidu	China	62	11	10
10	Ant Financial	China	60	--	--
11	Salesforce.com	USA	57	4	7
12	Xiaomi	China	46	--	--
13	Paypal	USA	46	6	9
14	Netflix	USA	44	2	7
15	Yahoo!	USA	36	10	5
16	JD.com	China	34	5	28
17	eBay	USA	28	11	9
18	Airbnb	USA	26	--	--
19	Yahoo! Japan	Japan	26	5	5
20	Didi Kuaidi	China	25	--	--
Total			\$2,752	\$447*	\$554*



4 DIGITISATION: FROM WEB PHENOMENON TO WHOLE SECTORS OF ECONOMIES

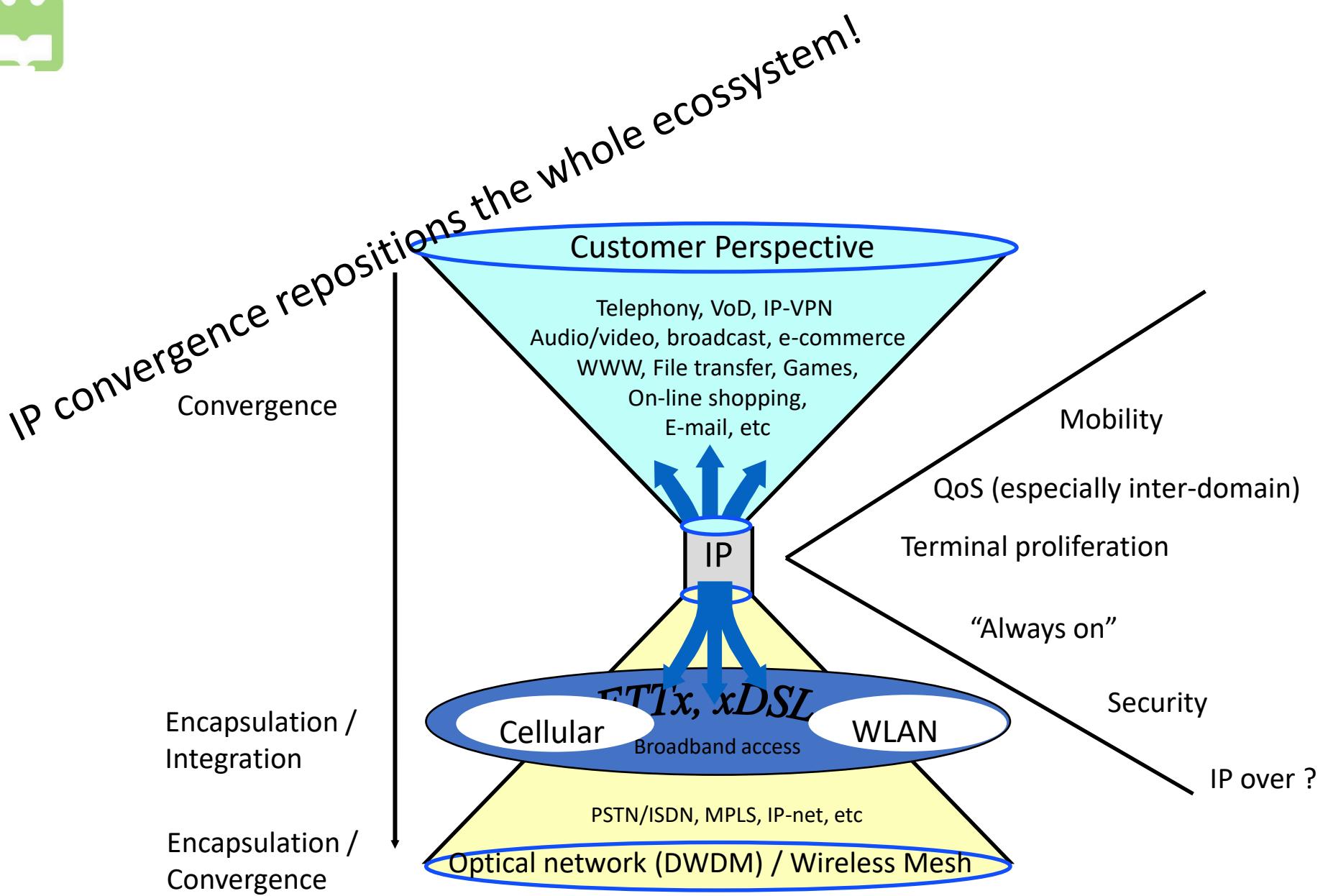


INNOVATION CATALYST FOR EACH WAVE



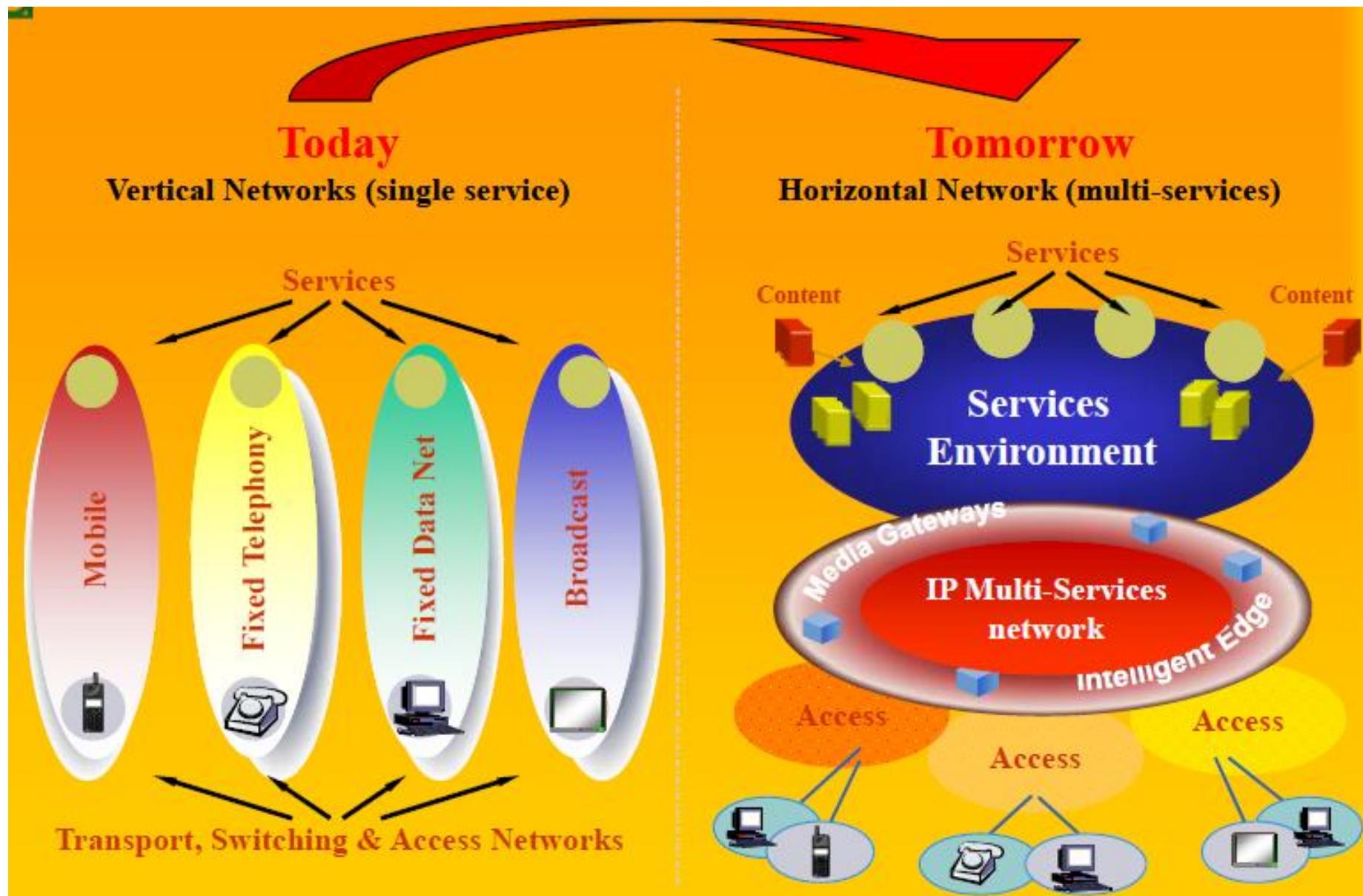
User behaviour and trends

- Increased Internet—based services
 - Phone market is now saturated
 - “Everything” came to “data communications”
- Increased broadband requirements
 - P2P being replaced by service-based
 - Internet access 2x every 2 years – fiber access now blooming
 - 70% broadband penetration
- Increased mobility and roaming
 - Always on and session continuity
 - Increased end-user content
 - Both WLAN and 4G
 - Increased context information
 - Increased personalization
 - Increased machine/vehicle/object communications



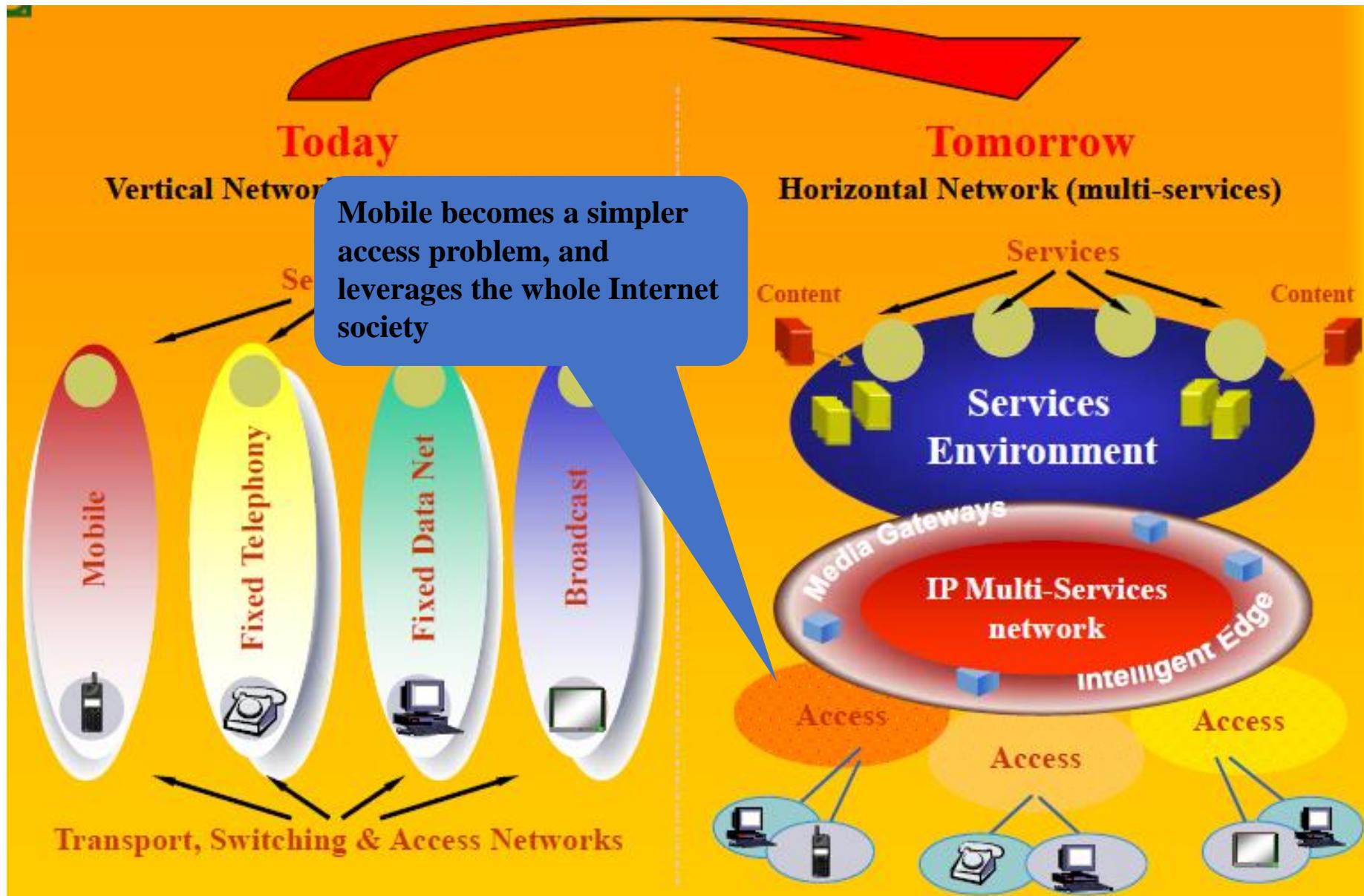


The opportunity provided by network heterogeneity





The opportunity provided by network heterogeneity





A Mobile Storage Revolution



Embedded Flash
128MB >>> 64GB



- Small size to minimise handset cost
- Used for storing system data: applications, messages, contacts, ring-tones



Embedded
(SD/H)DD
2GB >>> 256GB

- Large storage for user content
- But high impact on terminal cost



Memory Card
128MB >>> 1TB

- Large and removable storage for easy transfer of user content
- Interoperable with other consumer electronic devices
- Provides a distribution channel for selling content



... and a Multiplicity of Local Connectivity...



Today

- Bluetooth
- WiFi
- Memory cards
- USB
- Near Field Communications
 - device pairing & local network configuration
 - service discovery/initiation

Tomorrow

All of the above with the addition of:

- WLAN+ (802.11g++)
 - home and office connectivity
 - wireless extension of DSL in the home
- UWB
 - wireless USB
- TV/DVB



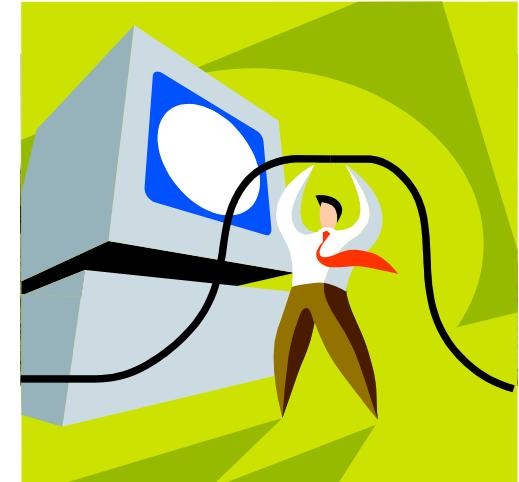
The wireless framework

- Mobile systems is THE major business
- Operators are becoming increasingly focused on mobile customers
 - Most of market will be wireless anyway on the access
- Services are now a dominant aspect in this arena
 - Large economic fights ongoing
- Mobility brought a novel importance to Location-based Services (LBS)
 - Now proximity is a dynamic variable for the user



What's going on here?

But what is all the tech fuss about?

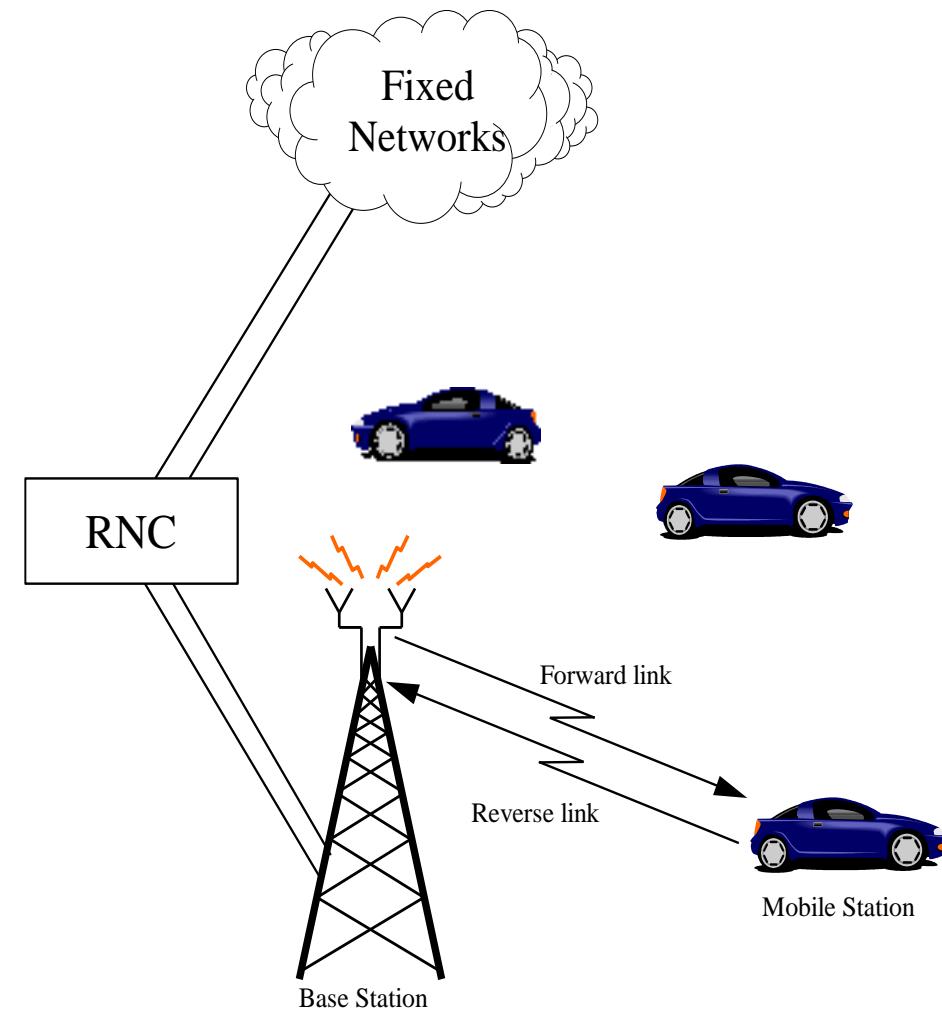




Wireless Systems

CM 22/23

- Mobile users communicate through fixed points (Base Stations/Access Points)
- Rely on radio transmission - final link between terminals and network
 - Finite resource, spectrum available is strictly limited
 - Multipath propagation, fading & interference
 - Terminal mobility complicates the system





Mobile hassles

1. Wireless connections limitations

- Multiple independent access networks and technologies
- (frequent) connection dropouts
- (More) limited bandwidth
- Lacking of mobility awareness by system/applications

2. Spectrum limitations

- Bandwidth cannot be improved just by adding parallel connections
- Spectrum is highly regulated

3. Mobile device limitations

- Battery lifetime
- Limited capabilities

4. Scaling considerations

- Mobile devices counted by the 1.000 millions
- Cost(s) needs to be low
- Energy is becoming a problem



Device Issues

- By their own nature:

**SMALL!
LOW POWER!**

- Potentially Low Power devices
 - Limited computing performance
 - Low quality displays
- Potential Loss of Data
 - Easily lost
 - Must be conceived as being “network-integrated”
- Potentially small and limited User Interface
 - Limited real estate for keyboards
 - Icon intensive/handwriting/speech
- Potentially Small Local Storage
 - Flash memory rather than disk drive



Scaling: You mean *Everywhere*?!?

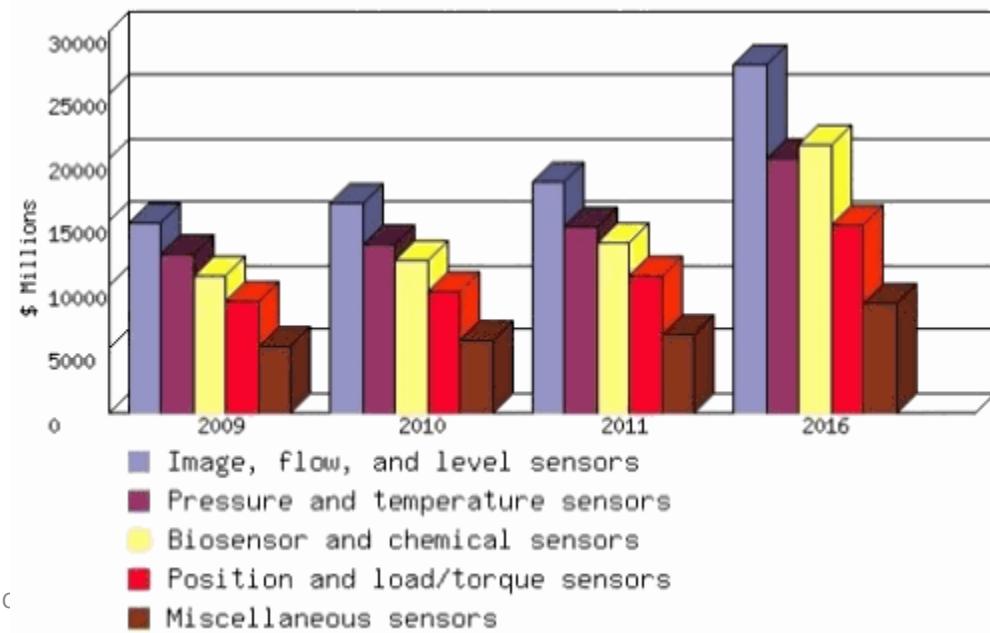
6.000 million users





Scaling: You mean *Everywhere*?!?

- 6.000 million users
- x10 sensors
- x2 general purpose computers
- x5 special purpose devices





Remember!

- Addressing
 - Total number of IPv4 addresses is ~4 200 millions
- Routing
 - Routing tables are already quite large
- Security
 - Securing everything? With certificates?
- Multimedia bandwidths
 - In wireless?!?
- Sensors and actuators
 - Electric grid on the net?!?!



Why is mobile hard?

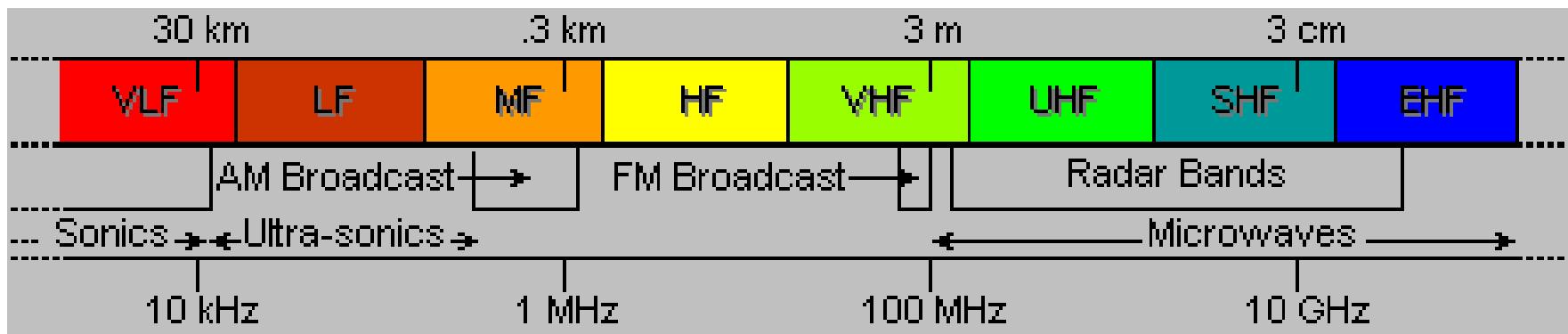
- Mobile communications are hard to handle, specially because spectrum is a scarce good
 - One critical economic issue from the governments point of view
- Also the whole nature of mobile systems is problematic – including the device specific issues
 - Although it is improving, power is still a problem
- As mobile systems became dominant (even into broadband!), scaling is a problem
 - We never dreamed with such a large success



It gets worse than this: RF Spectrum

- RF Spectrum = Radio Frequency allocation
 - Electromagnetic signal that propagates through “ether” at the speed of light
 - Ranges 3 KHz .. 300 GHz
 - Omnidirectional applications
 - Directional applications (above 5/10 GHz)
 - Or 100 km .. 0.1 cm (wavelength)

CM 22/23





Spectrum (only) looks like a lot!

- 300 GHz is huge amount of spectrum!
 - Spectrum can also be reused in space
- Not quite that much:
 - Most of it is hard or expensive to use!
 - Noise and interference limits efficiency
 - Most of the spectrum is allocated by Regulators
 - ISM bands unlicensed – but subject to multiple constraints
- Governments control who can use the spectrum and how it can be used.
 - (ITU-T WRC. Anacom, Oftel, FCC...)
 - Need a license for most of the spectrum
 - Limits on power, placement of transmitters, coding, ..
 - Need rules to optimize benefit: guarantee emergency services, simplify communication, return on capital investment, ...



UNITED STATES FREQUENCY ALLOCATIONS THE RADIO SPECTRUM

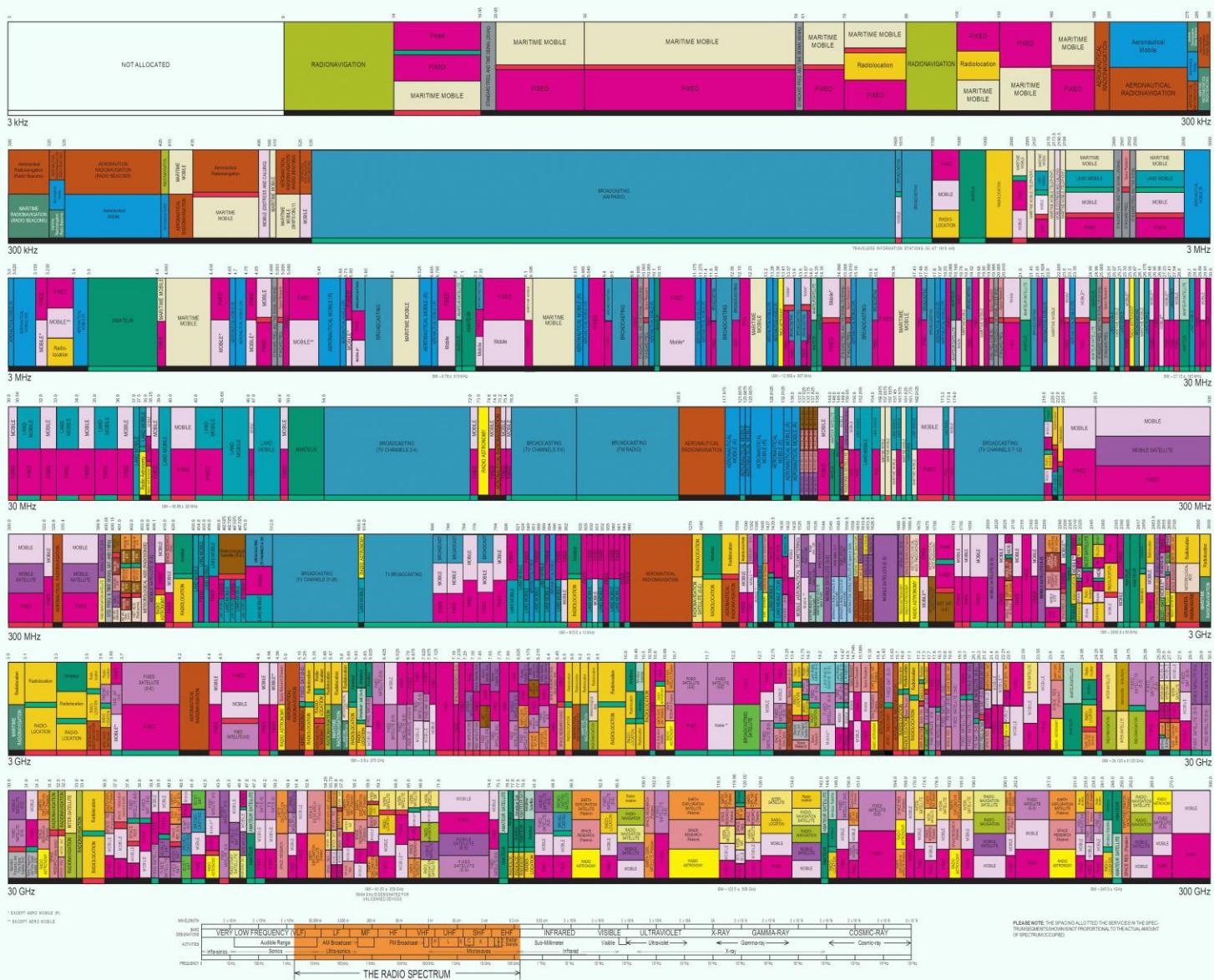


ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

The U.S. Laws and Regulations open-time portion of the Table of Frequency Allocations used by the Federal Government and the National Telecommunications and Information Administration are available in the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the correct details of the allocation.

U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
October 2000



* EXCEPT AERO. VISIBLE (P)

* EXCEPT AERO. VISIBLE

** EXCEPT AERO. SATELLITE

*** EXCEPT AERO. SATELLITE

**** EXCEPT AERO. SATELLITE

***** EXCEPT AERO. SATELLITE



General Frequency Ranges

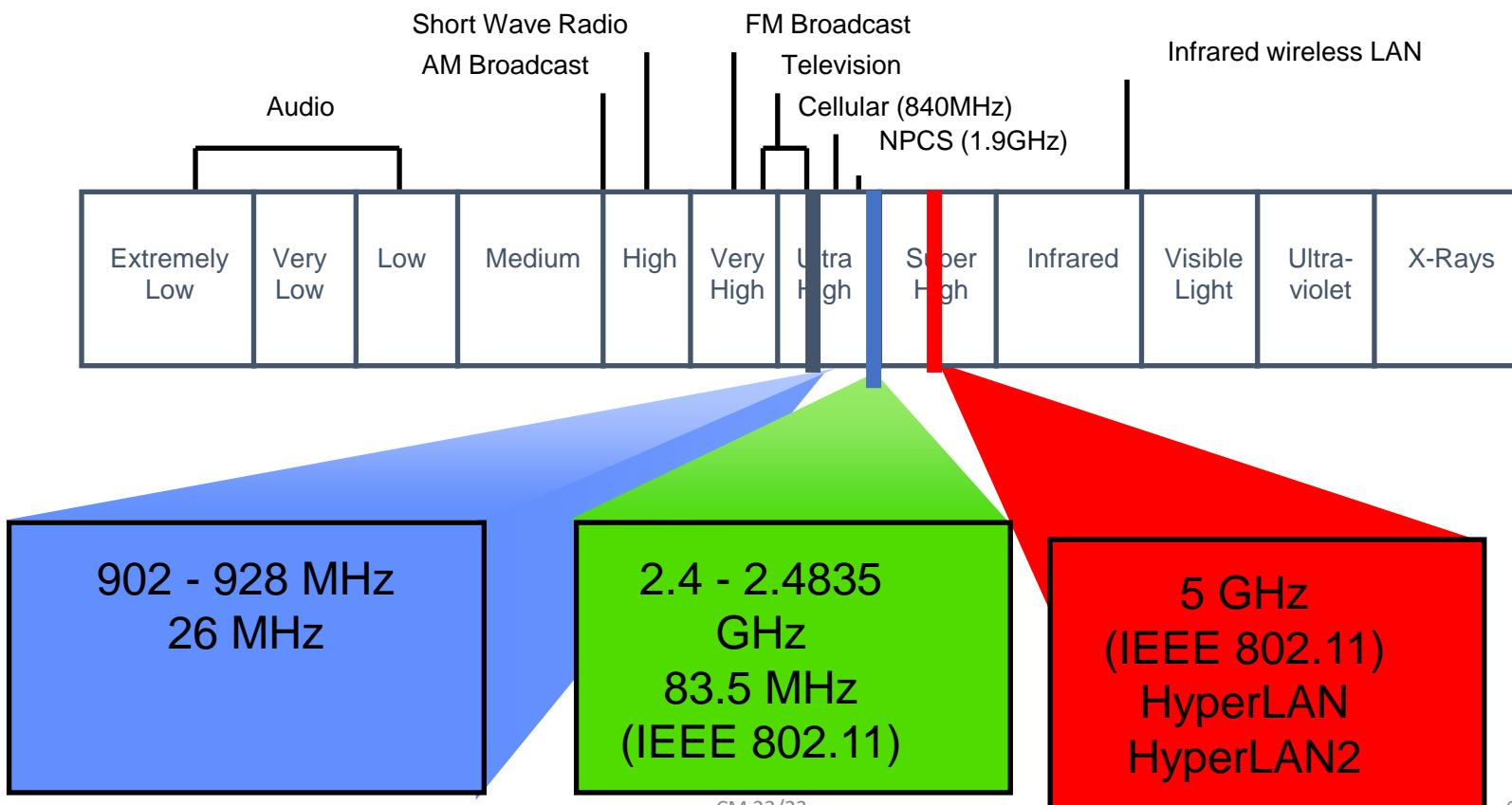
CM 22/23

- Microwave frequency range
 - 1 GHz to 40 GHz and higher
 - Directional beams possible
 - Suitable for point-to-point transmission
 - Used for satellite communications
- Radio frequency range
 - 30 MHz to 1 GHz
 - Suitable for omnidirectional applications
- Infrared frequency range
 - Roughly, 3×10^{11} to 2×10^{14} Hz
 - Useful in local point-to-point multipoint applications within confined areas



Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed, 22 MHz channel bandwidth





Portugal

http://www.anacom.pt/streaming/qnafuk.pdf?contentId=29658&field=ATTACHED_FILE

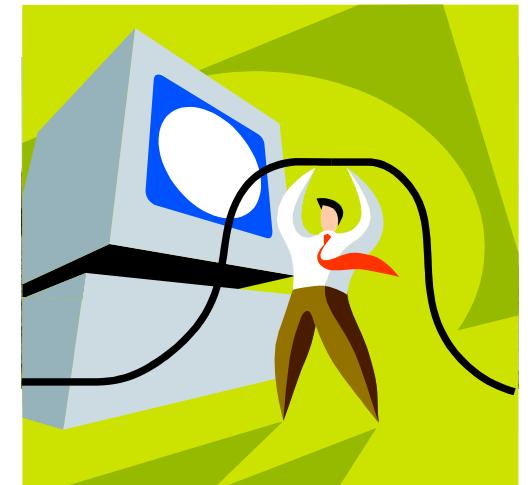
CM 22/23

http://www.anacom.pt/streaming/qnaf0506_integral_uk.pdf?contentId=354390&field=ATTACHED_FILE



Physical Layer

Problems we face





Classifications of Transmission Media

- Copper: twisted pair versus coax cable
 - Variety of modulation techniques are used
- Fiber: modulate an optical signal
 - Lots of capacity available!
 - Typically uses simple modulation schemes
- Wireless: no solid medium to guided signal
 - Wide variety of distances: frequencies, distances, ...
 - Often uses very aggressive modulation techniques (later)



Why Use Wireless?

There are no wires!

Has several significant advantages:

- No need to install and maintain wires
 - Reduces cost – important in offices, hotels, ...
 - Simplifies deployment – important in homes, hotspots, ...
- Supports mobile users
 - Move around office, campus, city, ... - users get hooked
 - Remote control devices (TV, garage door, ..)
 - Cordless phones, cell phones, ..
 - WiFi, GPRS, WiMax, ...



What is Hard about Wireless?

There are no wires!

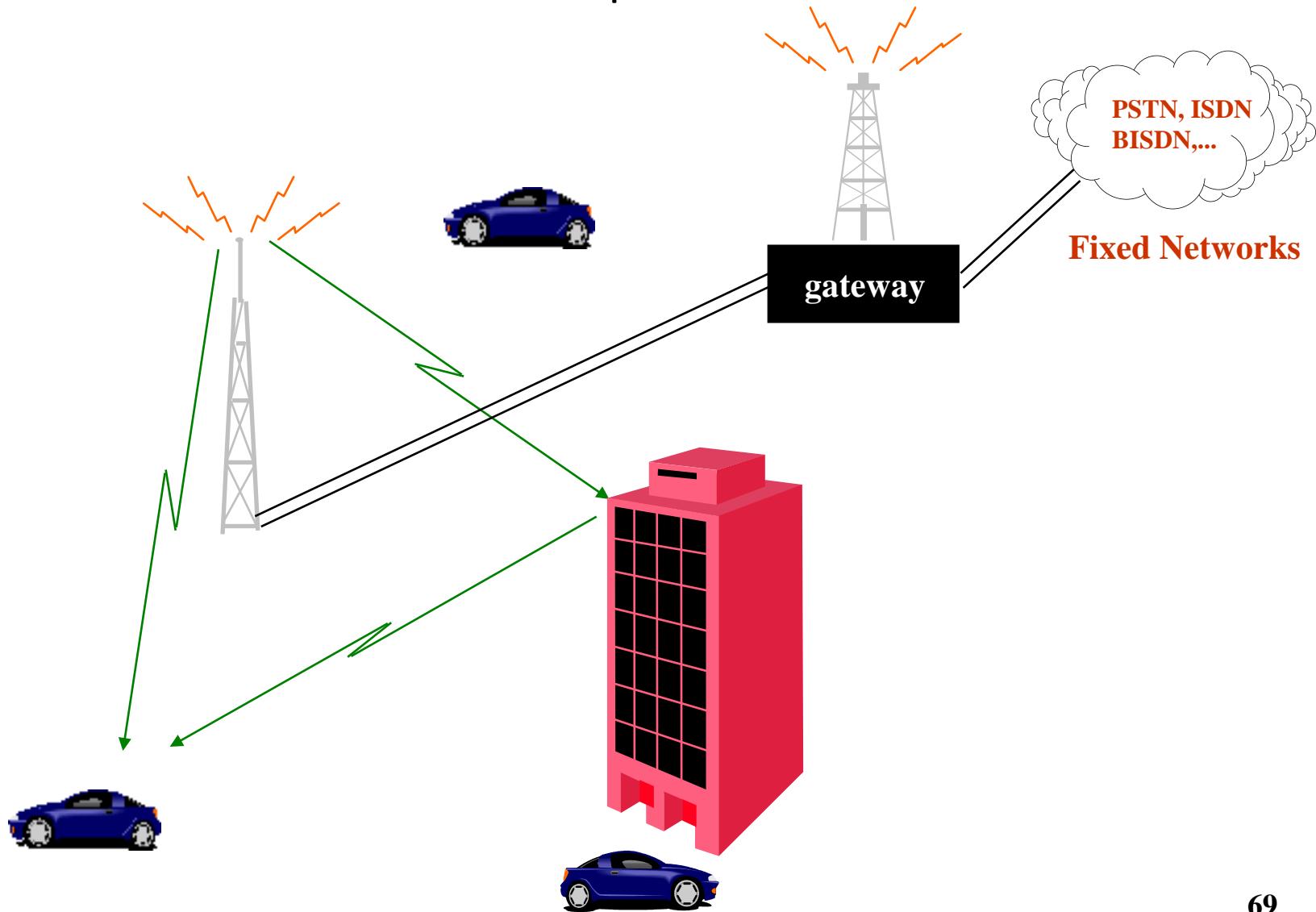
Causes problems in many areas:

- Quality of transmission
- Interference and noise
- Capacity of the network
- Effects of mobility



CM 22/23

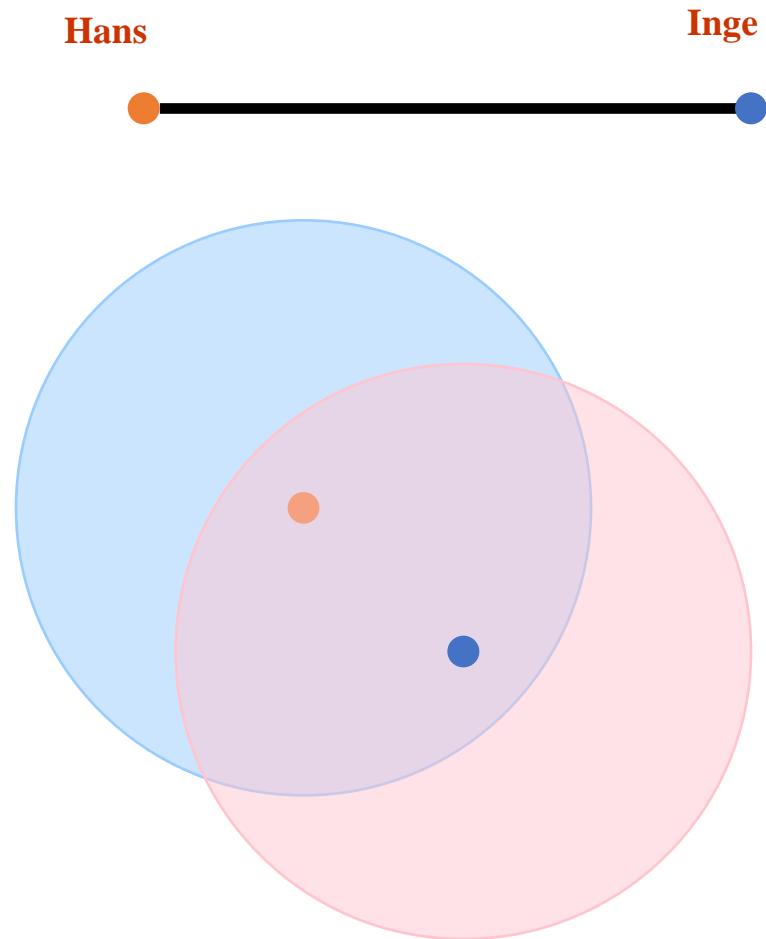
Radio Transmission Impairments





Communication based on Broadcasting

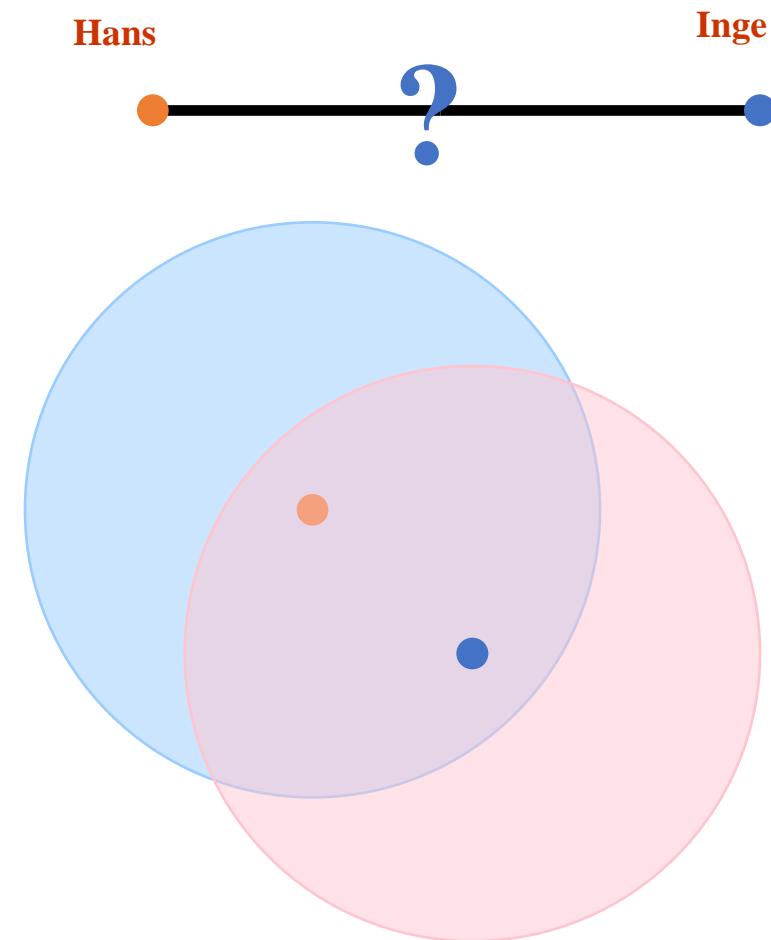
- Wired communication is usually point-to-point.
 - Broadcast is hard to scale
- Wireless communication is inherently broadcast.
 - Well, usually
- Of course: it does allow nodes to move





Mobility

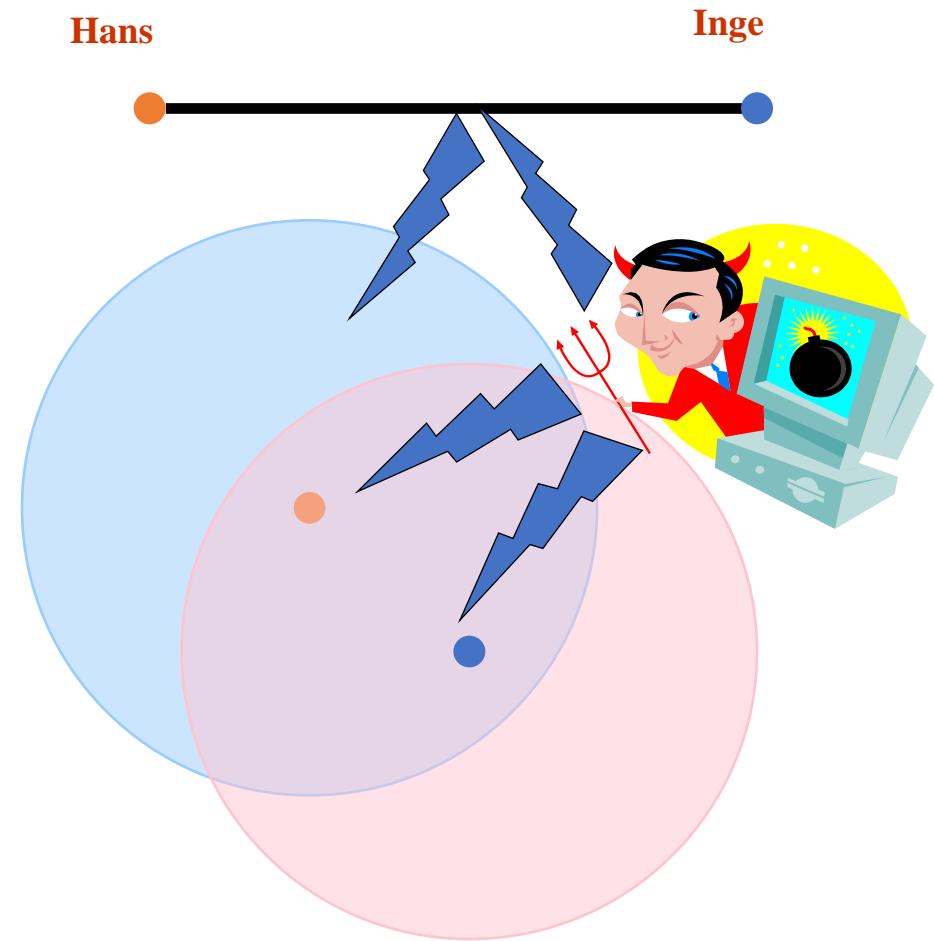
- Wired communication is usually point-to-point.
 - Broadcast is hard to scale
- Wireless communication is inherently broadcast.
 - Well, usually
- Of course: it does allow nodes to move





Wireless is very Sensitive to Noise ...

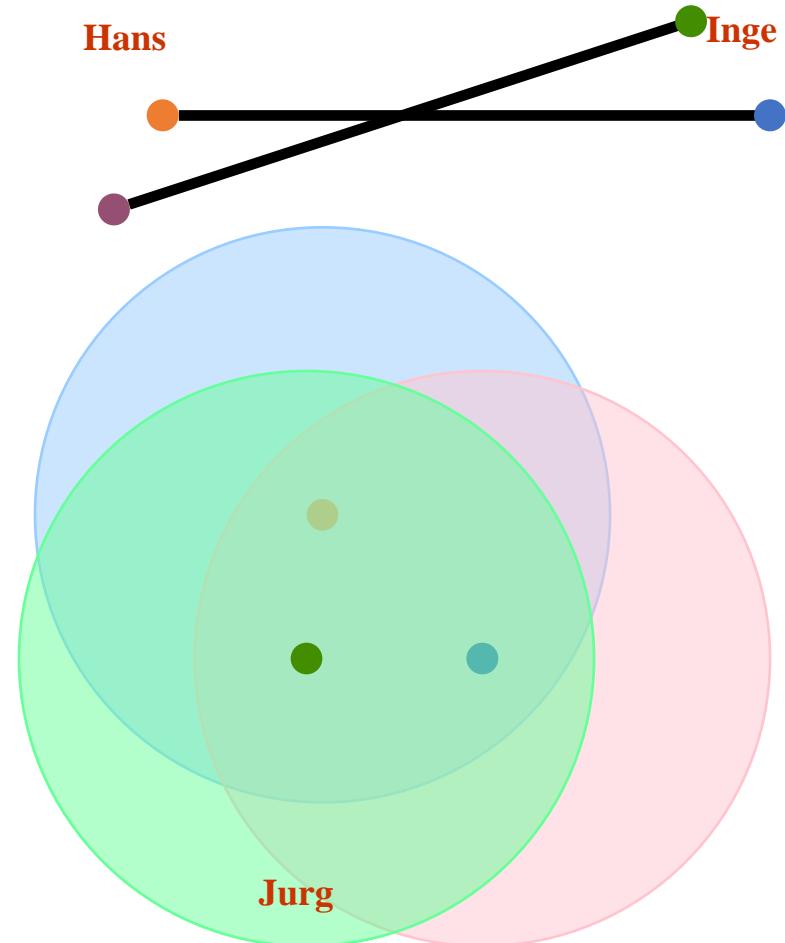
- Noise is naturally present in the environment from many sources.
- Interference can be from other users or from malicious sources.
- Impacts the throughput users can achieve.





... and Interference

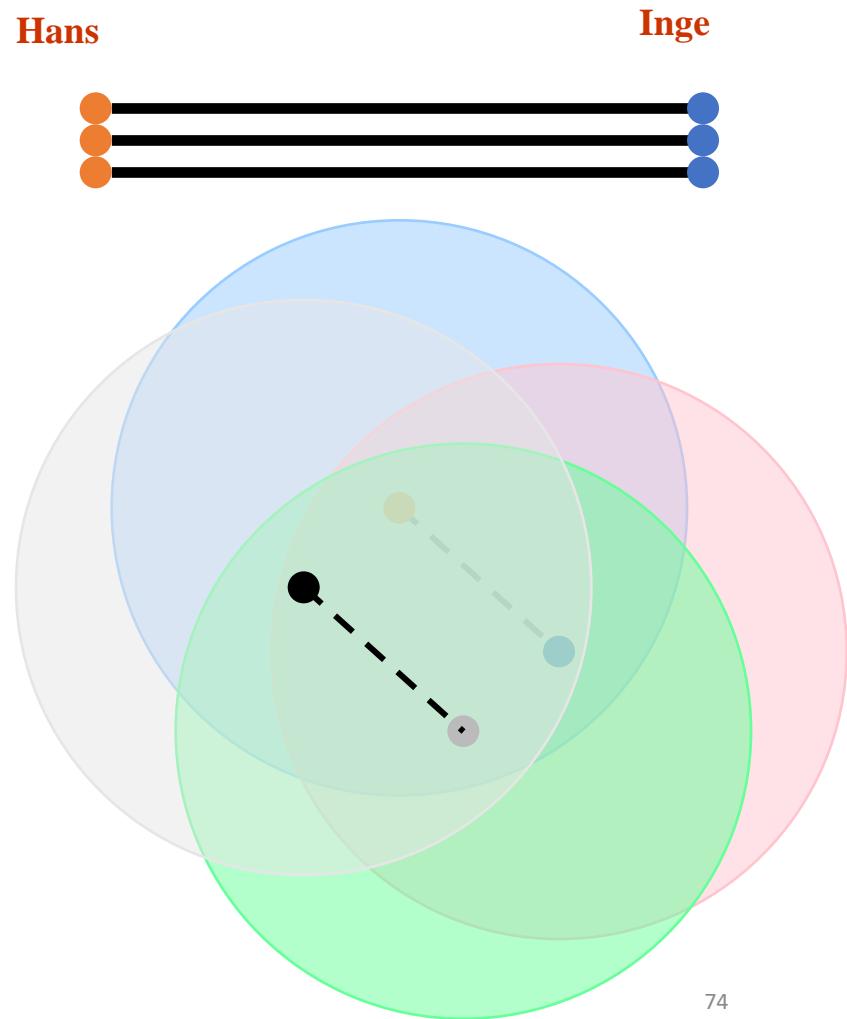
- Noise is naturally present in the environment from many sources.
- Interference can be from other users or from malicious sources.
- Impacts the throughput users can achieve.





How Do We Increase Network Capacity?

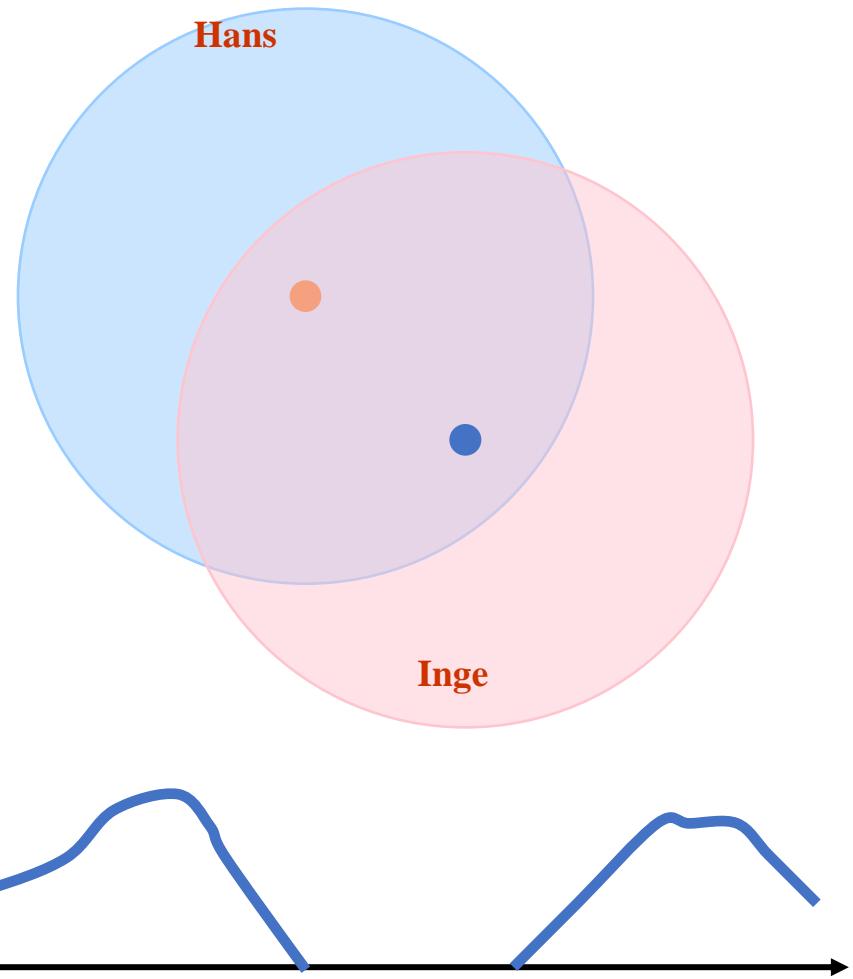
- Easy to do in wired networks: simply add wires.
 - Fiber is especially attractive
- Adding wireless “links” increases interference.
 - Frequency reuse can help ... subject to spatial limitations
 - Or use different spaces ... subject to frequency limitations
- The capacity of the wireless network is fundamentally limited.





Mobility Affects the Link Throughput

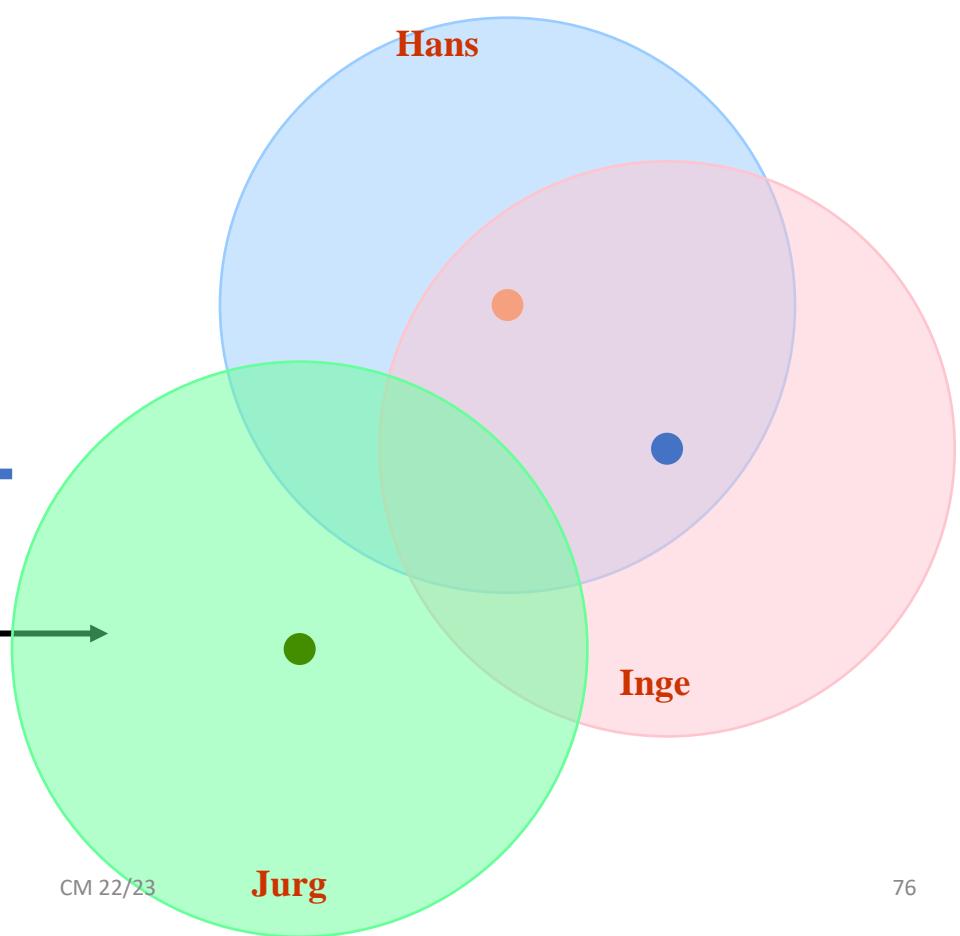
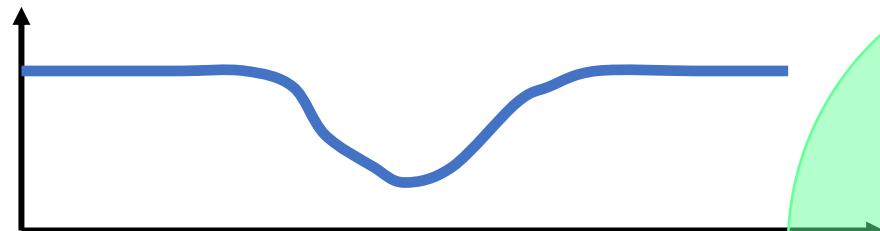
- Quality of the transmission depends on distance and other factors.
- Affects the throughput mobile users achieve.
- Worst case is periods with no connectivity!





Mobility is an Issue even for Stationary Users

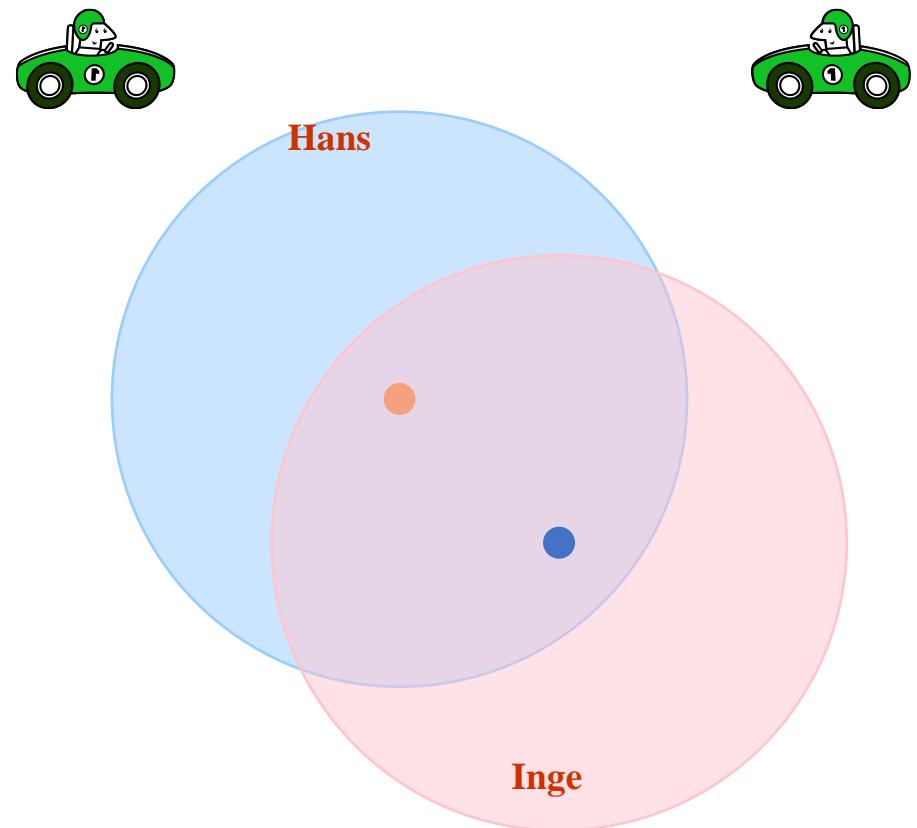
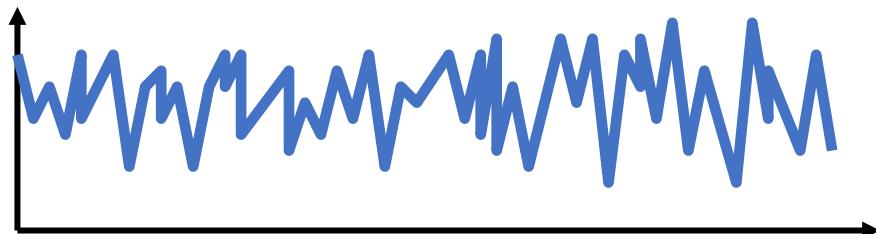
- Mobile people and devices affect the transmission channel of stationary nodes.





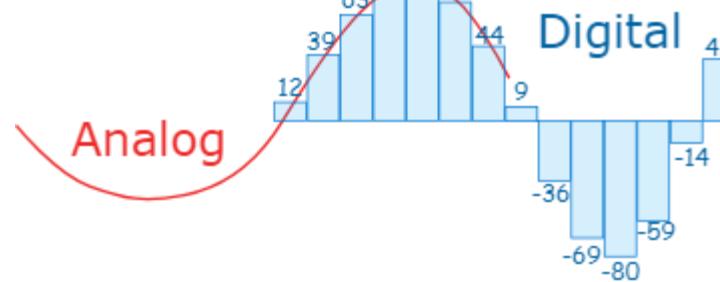
And It Gets Worse ...

- The impact of mobility on transmission can be complex.
- Mobility also affects addressing and routing.





Time-Domain View



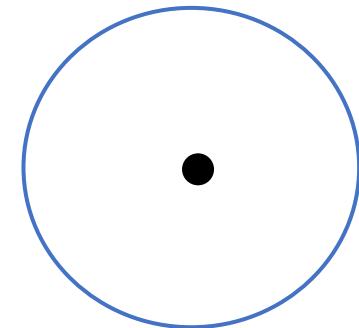
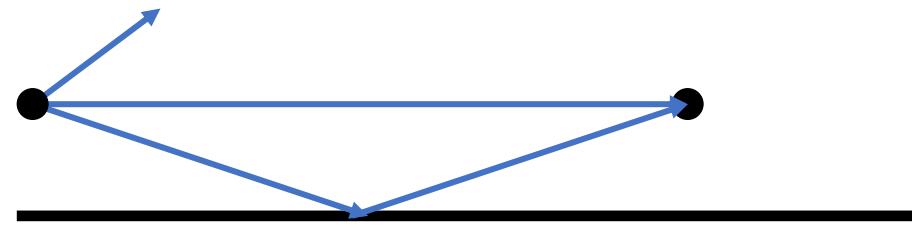
- Can be used to represent both an analog and a digital signal.
- Analog signal - signal intensity varies in a smooth fashion over time
 - No breaks or discontinuities in the signal
 - E.g. voice signal traveling over traditional phone line
- Digital signal - signal intensity maintains a constant level for some period of time and then changes to another constant level.
 - E.g. stream of 1 and 0 values represented as “low” and “high” signal



Two Graphical Views of an Electromagnetic Signal

CM 22/23

- Both are real in some way
- Think of it as energy that radiates from an antenna and is picked up by another antenna.
 - Helps explain properties such as attenuation
- Can also view it as a “ray” that propagates between two points.
 - Helps explain properties such as reflection and multipath

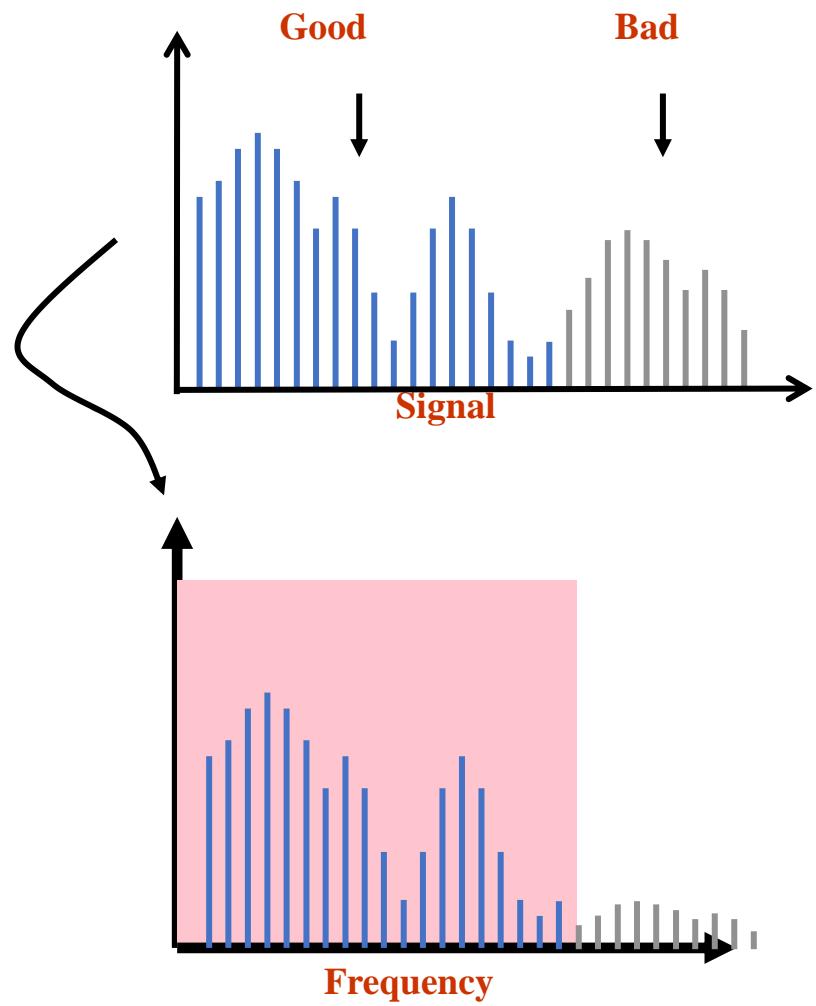




Transmission Channel Considerations

CM 22/23

- Example: green frequencies get attenuated significantly
- For wired networks, channel limits are an inherent property of the channel
 - Different types of fiber and copper have different properties
- As technology improves, these parameters change, even for the same wire
 - Electronics rule
- For wireless networks, limits are often imposed by policy
 - Can only use certain part of the spectrum
 - Regulatory/business considerations





Channel Capacity

- Data rate - rate at which data can be communicated (bps)
 - Channel Capacity – the maximum rate at which data can be transmitted over a given channel, under given conditions
- Bandwidth (signal theory)- the bandwidth of the transmitted signal as constrained by the transmitter and the nature of the transmission medium (Hertz)
- Noise - average level of noise over the communications path
- Error rate - rate at which errors occur
 - Error = transmit 1 and receive 0; transmit 0 and receive 1



Propagation Modes

CM 22/23

- Line-of-sight (LOS) propagation.
 - Most common form of propagation
 - Happens above ~ 30 MHz
 - Subject to many forms of degradation (next set of slides)
- Ground-wave propagation.
 - More or less follows the contour of the earth
 - For frequencies up to about 2 MHz, e.g. AM radio
- Sky wave propagation.
 - Signal “bounces” off the ionosphere back to earth – can go multiple hops
 - Used for amateur radio and international broadcasts



Propagation Degrades RF Signals

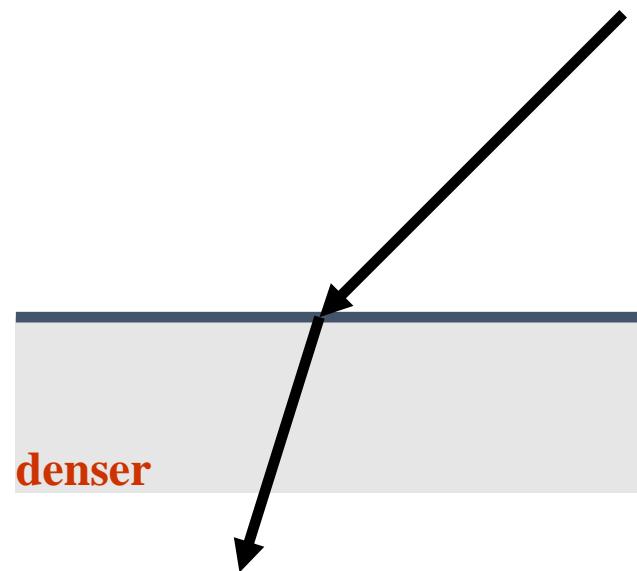
- Attenuation in free space: signal gets weaker as it travels over longer distances
 - Radio signal spreads out – free space loss
 - Refraction and absorption in the atmosphere
 - Frequency dependent!
- Obstacles can weaken signal through absorption or reflection.
 - Part of the signal is redirected
- Multi-path effects: multiple copies of the signal interfere with each other.
- Mobility: moving receiver causes another form of self interference.
 - Big change in signal strength



Refraction

CM 22/23

- Speed of EM signals depends on the density of the material
 - Vacuum: 3×10^8 m/sec
 - Denser: slower
- Density is captured by refractive index
- Explains “bending” of signals in some environments
 - E.g. sky wave propagation
 - But also local, small scale differences in the air





Noise Sources

CM 22/23

- Thermal noise: caused by agitation of the electrons
 - Function of temperature
 - Affects electronic devices and transmission media
- Intermodulation noise: result of mixing signals
- Cross talk: picking up other signals
 - E.g. from other source-destination pairs)
- Impulse noise: irregular pulses of high amplitude and short duration
 - Harder to deal with

Fairly
Predictable
➤Can be
planned for
or avoided



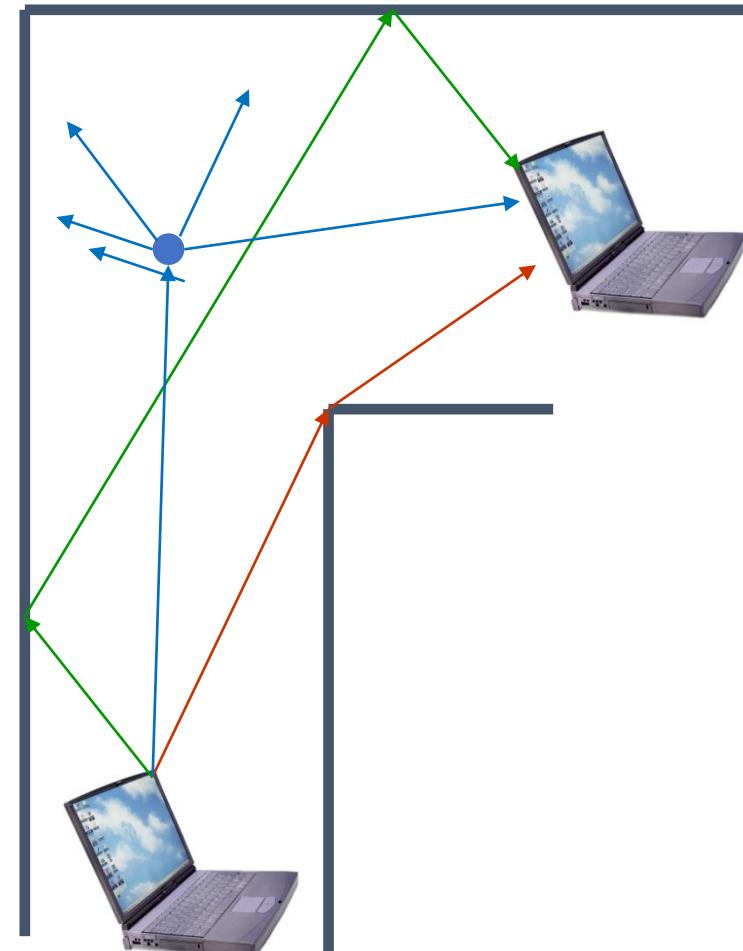
Other LOS Factors

- Absorption of energy in the atmosphere.
 - Very serious at specific frequencies, e.g. water vapor (22 GHz) and oxygen (60 GHz)
 - Obviously objects also absorb energy



Propagation Mechanisms

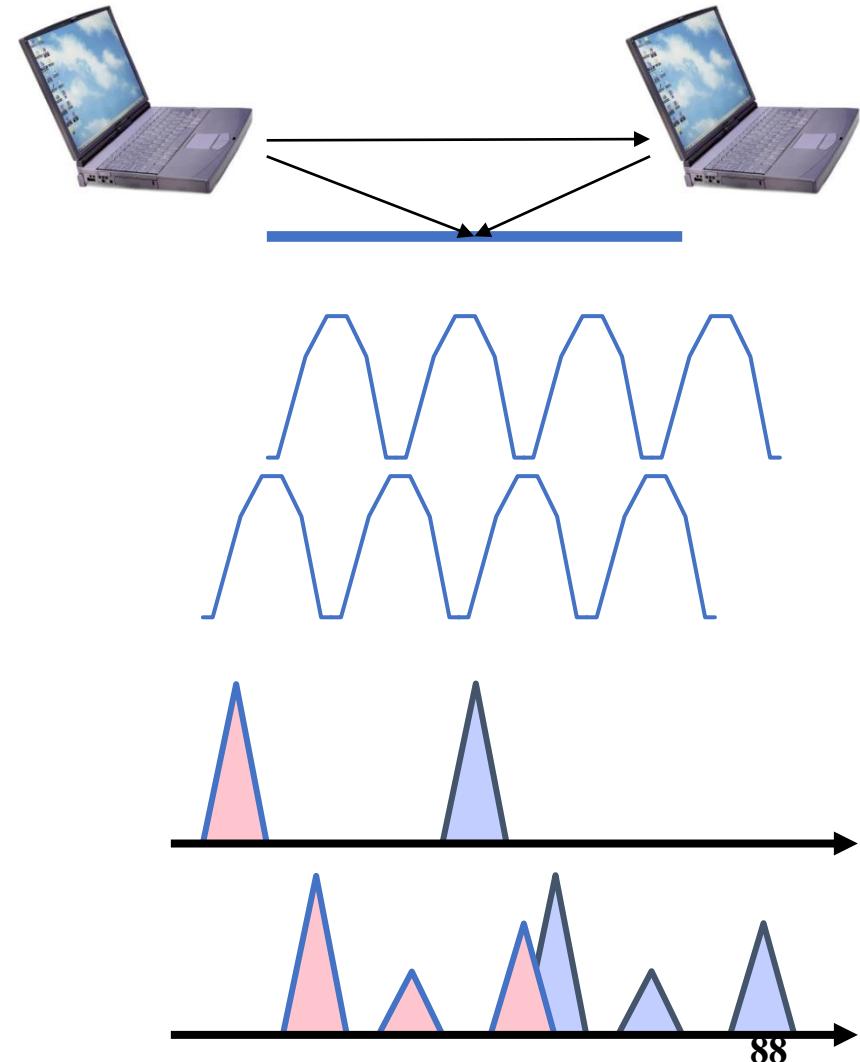
- Besides line of sight, signal can reach receiver in three other “indirect” ways.
- **Reflection**: signal is reflected from a large object.
- **Diffraction**: signal is scattered by the edge of a large object – “bends”.
- **Scattering**: signal is scattered by an object that is small relative to the wavelength.





Multipath Effects

- Receiver receives multiple copies of the signal, each following a different path.
- Copies can either strengthen or weaken each other.
- Small changes in location can result in big changes in signal strength.
- Difference in path length can cause intersymbol interference (ISI).





Introducing Redundancy

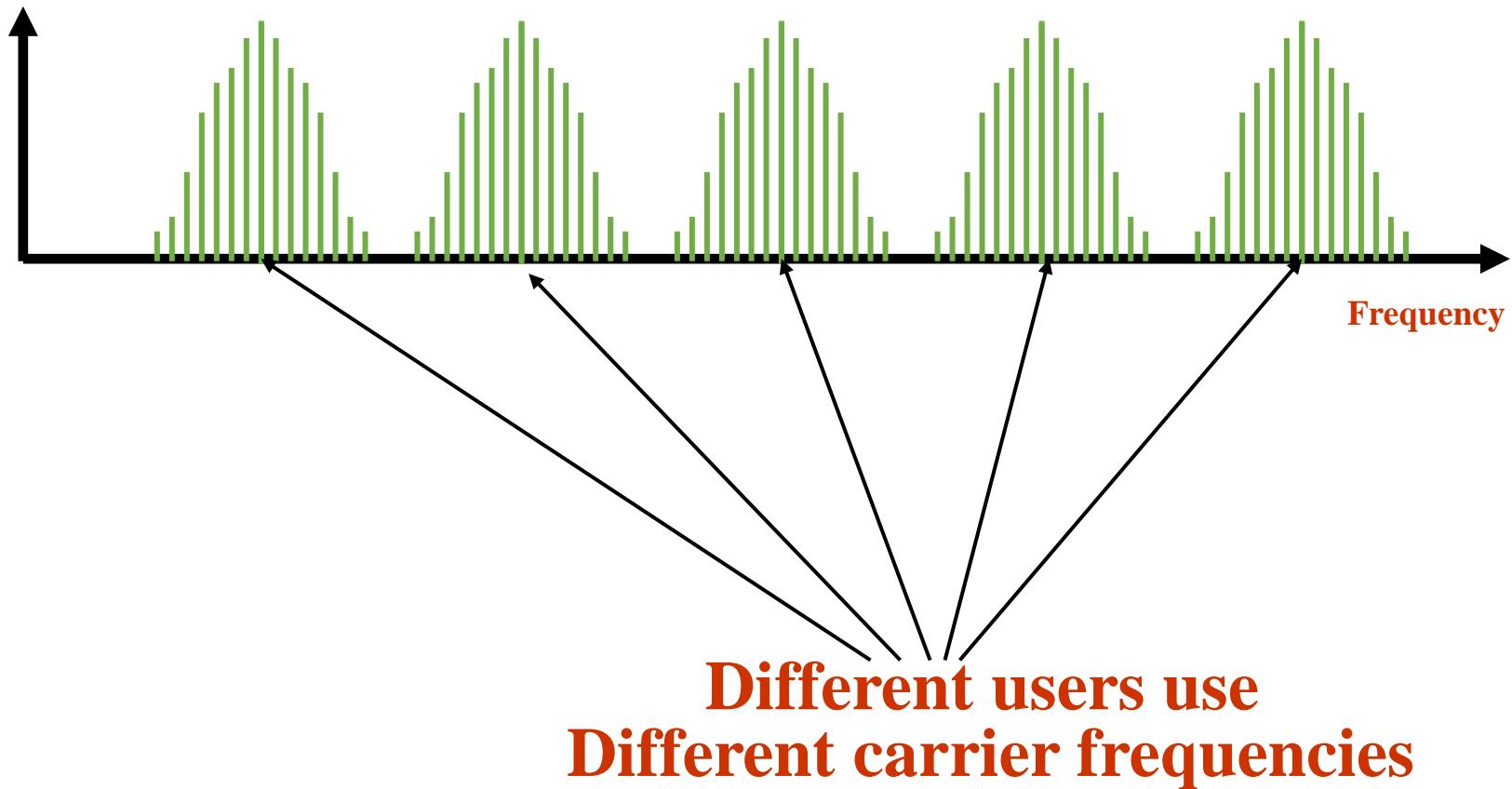
CM 22/23

- Protects digital data by introducing redundancy in the transmitted data.
 - Error detection codes: can identify certain types of errors
 - Error correction codes: can fix certain types of errors
- **Block codes** provide Forward Error Correction (FEC) for blocks of data.
 - (n, k) code: n bits are transmitted for k information bits
 - Simplest example: parity codes
 - Many different codes exist: Hamming, cyclic, Reed-Solomon, ...
- **Convolutional codes** provide protection for a continuous stream of bits.
 - Coding gain is n/k
 - Turbo codes: convolutional code with channel estimation



Multiple Users Can Share the Spectrum

CM 22/23





So Why Don't we Always Send a High Bandwidth Signal?

CM 22/23

- Channels have a limit on the type of signals it can carry
 - Good transmission of signals only in certain frequency range
 - Signals outside of that range get distorted, e.g. attenuated
- Distortion can make it hard for receiver to extract the information
 - It is beneficial to match the signal to the channel
 - Limits the throughput of the channel





Spread Spectrum

CM 22/23

- Spread transmission over a wider bandwidth
 - Don't put all your eggs in one basket!
- Good for military: jamming and interception becomes harder
- Also useful to minimize impact of a “bad” frequency in regular environments
- What can be gained from this apparent waste of spectrum?
 - Immunity from various kinds of noise and multipath distortion
 - Including jamming
 - Can be used for hiding/encrypting signals
 - Only receiver who knows SS code can retrieve signal
 - Several users can independently share the same higher bandwidth with very little interference (later)
 - Code division multiple access (CDMA)



Spread Spectrum Concept

CM 22/23

- Input fed into channel encoder
 - Produces narrow bandwidth analog signal around central frequency
- Signal modulated using sequence of digits
 - Spreading code/sequence
 - Typically generated by pseudonoise/pseudorandom number generator
 - Not actually random
 - If algorithm good, results pass reasonable tests of randomness
 - Need to know algorithm and seed to predict sequence
- Increases bandwidth significantly
 - Spreads spectrum
- Receiver uses same sequence to demodulate signal
- Demodulated signal fed into channel decoder



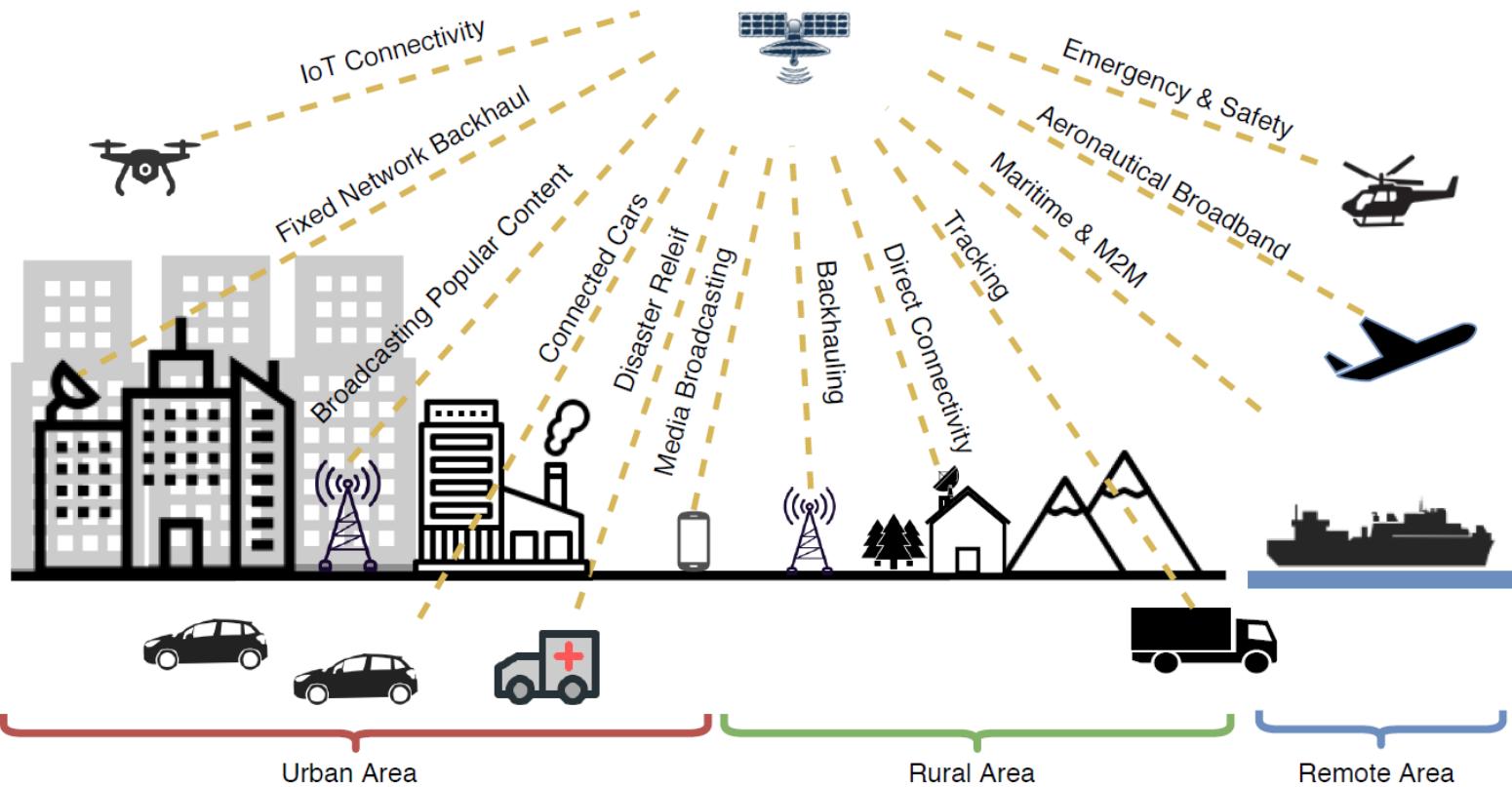
Satellite networks



SATELLITES

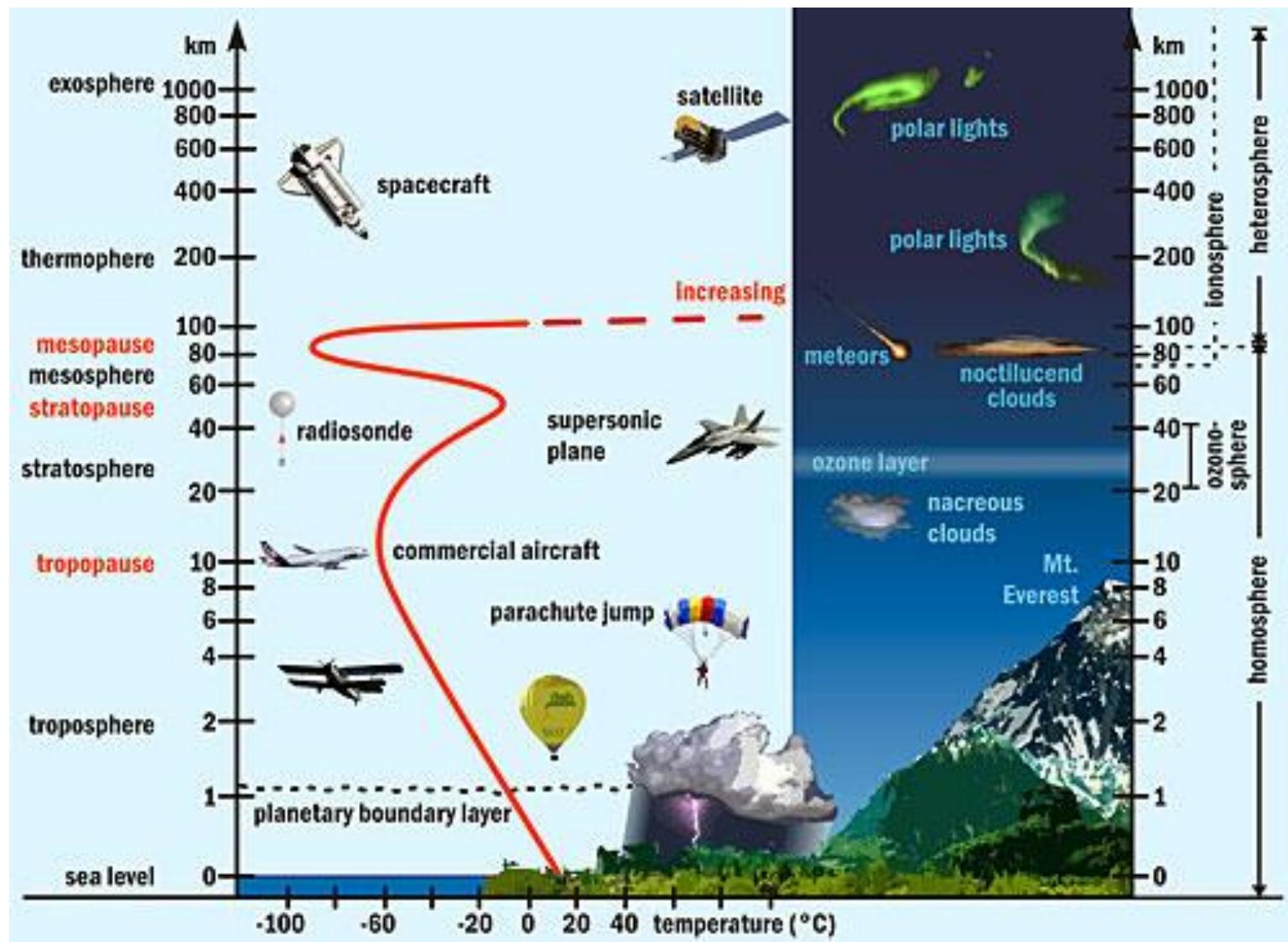


Distance: 378.000 km
Period: 27.3 days





Earth's atmosphere





Basics

- ❑ elliptical or circular orbits
- ❑ complete rotation time depends on distance satellite-earth
- ❑ inclination: angle between orbit and equator
- ❑ elevation: angle between satellite and horizon
- ❑ LOS (Line of Sight) to the satellite necessary for connection
 - ➔ high elevation needed, less absorption due to e.g. buildings
- ❑ Uplink: connection base station - satellite
- ❑ Downlink: connection satellite - base station
- ❑ typically separated frequencies for uplink and downlink
 - transponder used for sending/receiving and shifting of frequencies
 - transparent transponder: only shift of frequencies
 - regenerative transponder: additionally signal regeneration



Features of Satellite Networks

- **Effects of satellite mobility**

- Topology is dynamic.
- Topology changes are predictable and periodic.
- Traffic is very dynamic and non-homogeneous.
- Handovers are necessary.

- **Limitations and capabilities of satellites**

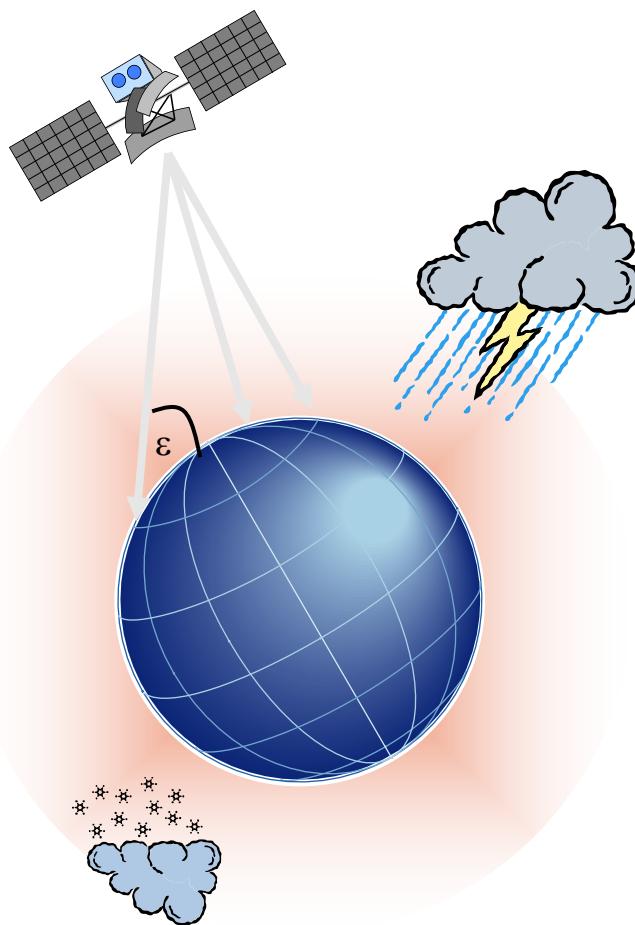
- Power and onboard processing capability are limited.
- Implementing the state-of-the-art technology is difficult.
- Satellites have a broadcast nature.

- **Nature of satellite constellations**

- Higher propagation delays.
- Fixed number of nodes.
- Highly symmetric and uniform structure.

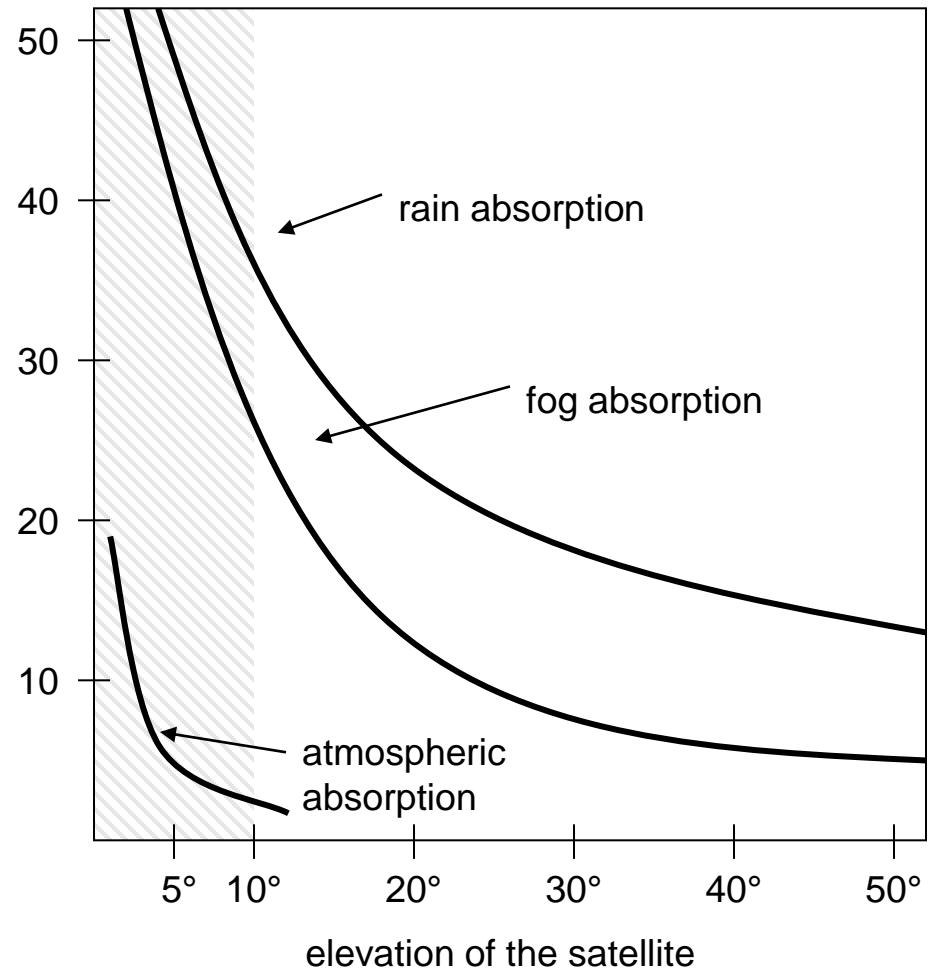


Atmospheric attenuation



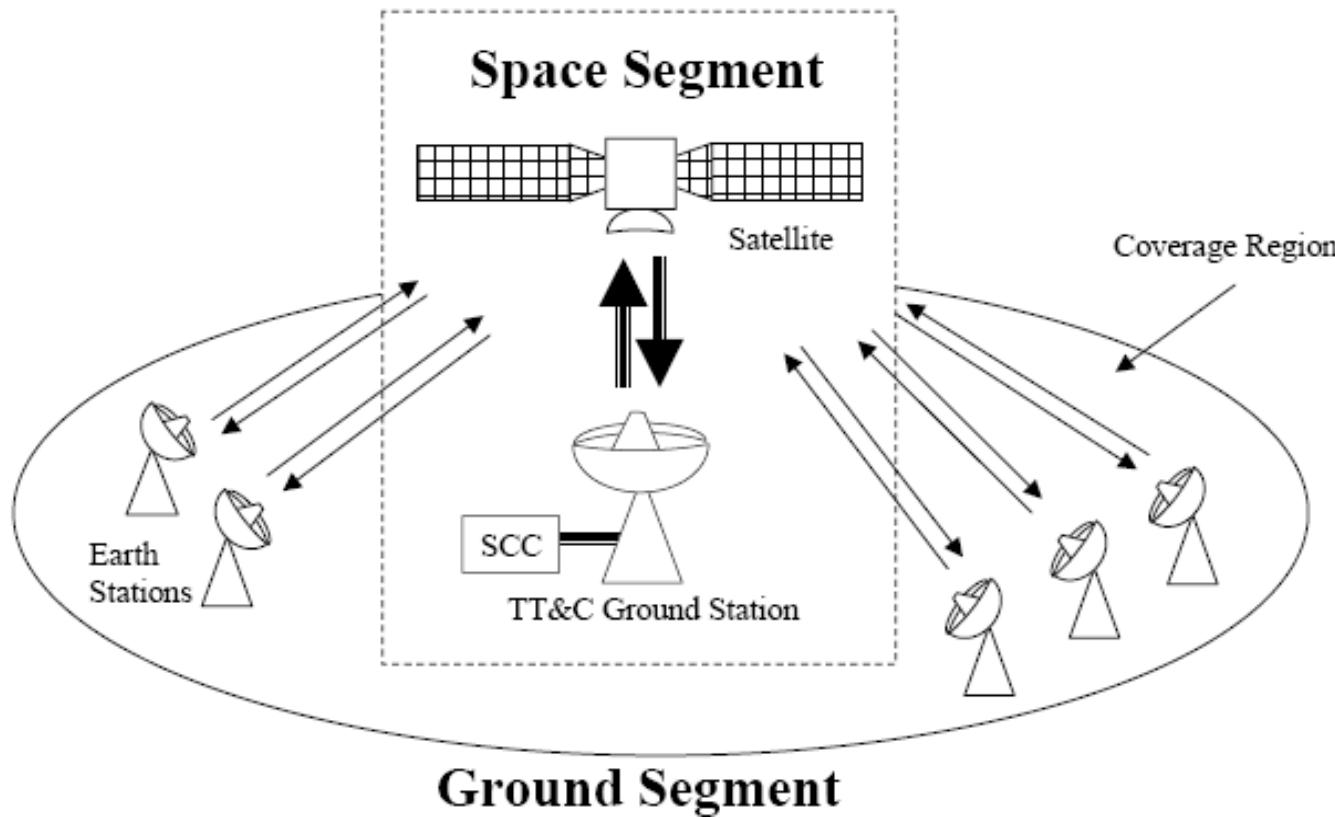
Attenuation of
the signal in %

Example: satellite systems at 4-6 GHz





Satellite System Elements



SCC- Satellite Control Center
TTC – Telemetry, Tracking and Command



Satellite Transmission Links

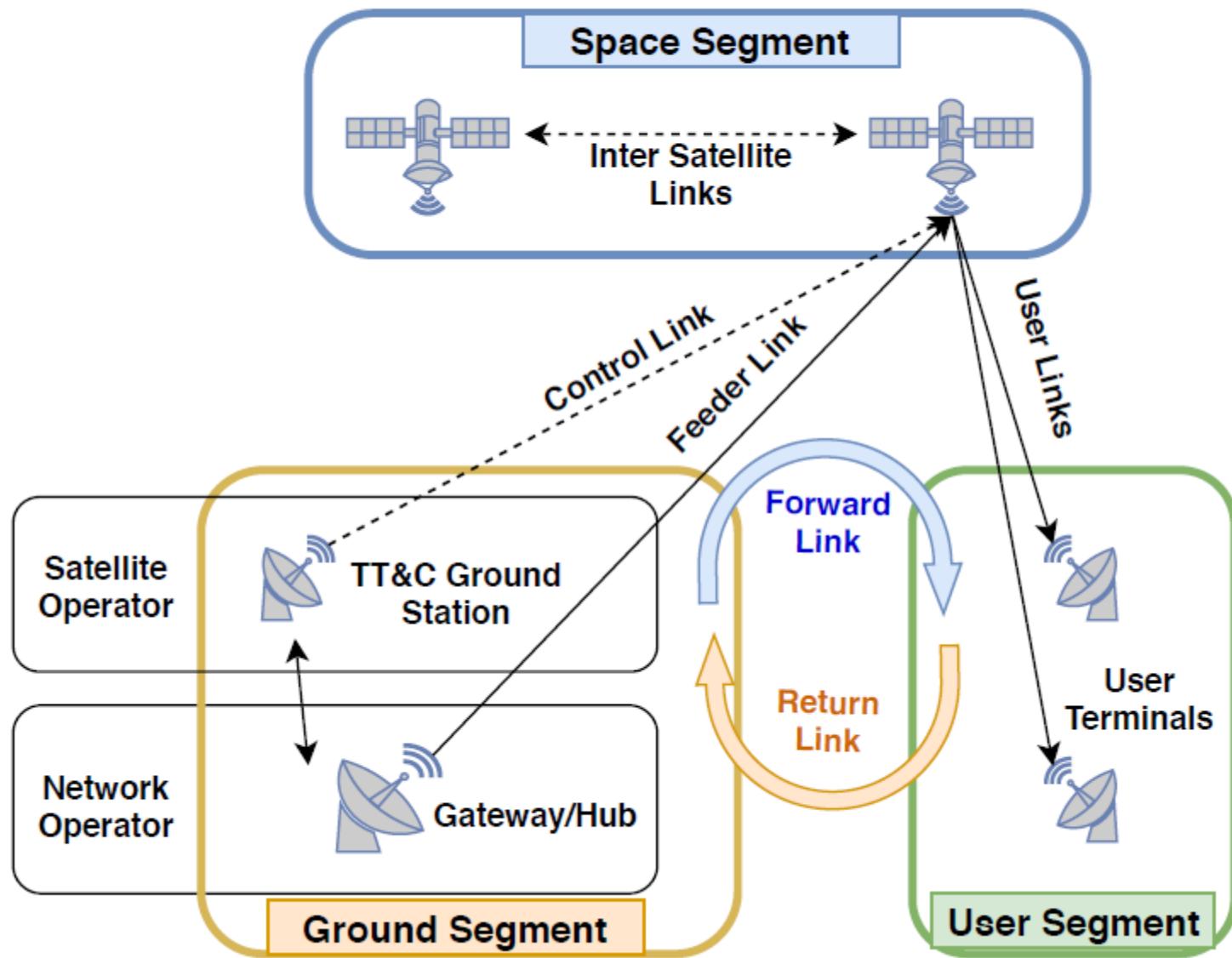
- Earth stations communicate by sending signals to the satellite on an uplink
- The satellite then repeats those signals on a downlink
- The broadcast nature of downlink makes it attractive for services such as the distribution of TV programs



- Satellite up links and down links can operate in different frequency bands:

Band	Up-Link (Ghz)	Down-link (Ghz)	ISSUES
C	3,700-4,200 MHz	5,925-6,425 MHz	Interference with ground links.
Ku	11.7-12.2 GHz	14.0-14.5 GHz	Attenuation due to rain
Ka	17.7-21.2 GHz	27.5-31.0 GHz	High Equipment cost

- The up-link is a highly directional, point to point link
- The down-link can have a footprint providing coverage for a substantial area "spot beam".





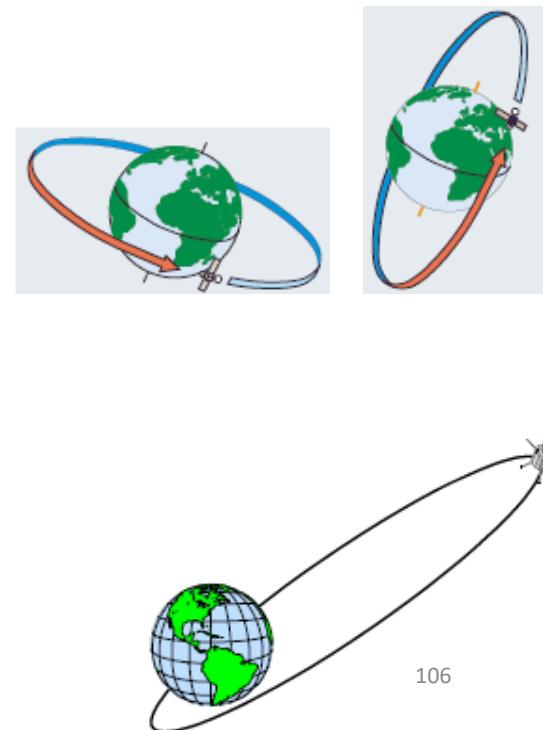
Satellite Uplink and Downlink

- ▶ **Downlink**
 - ▶ The link from a satellite down to one or more ground stations or receivers
- ▶ **Uplink**
 - ▶ The link from a ground station up to a satellite.
- ▶ Some companies sell uplink and downlink services to
 - ▶ television stations, corporations, and to other telecommunication carriers.
 - ▶ A company can specialize in providing uplinks, downlinks, or both.



Types of Satellite Orbits

- Based on the inclination, “ i ”, over the equatorial plane:
 - Equatorial Orbits above Earth’s equator ($i=0^\circ$)
 - Polar Orbits pass over both poles ($i=90^\circ$)
 - Other orbits called inclined orbits ($0^\circ < i < 90^\circ$)
- Based on Eccentricity
 - Circular with centre at the earth’s centre
 - Elliptical with one foci at earth’s centre



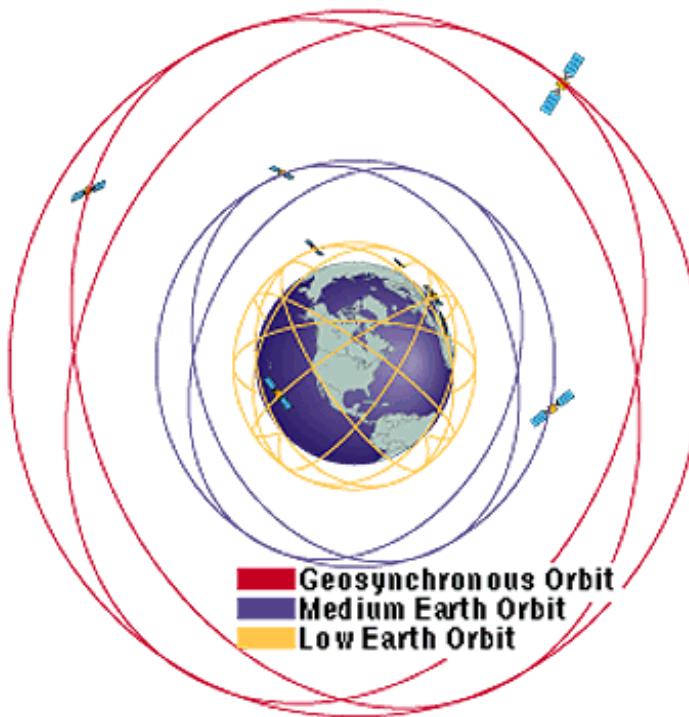


Types of Satellite based Networks

- Based on the Satellite Altitude
 - GEO – Geostationary Orbits
 - 36000 Km = 22300 Miles, equatorial, High latency
 - MEO – Medium Earth Orbits
 - High bandwidth, High power, High latency
 - LEO – Low Earth Orbits
 - Low power, Low latency, More Satellites, Small Footprint
- VSAT
 - Very Small Aperture Satellites
 - Private WANs



Satellite Orbits

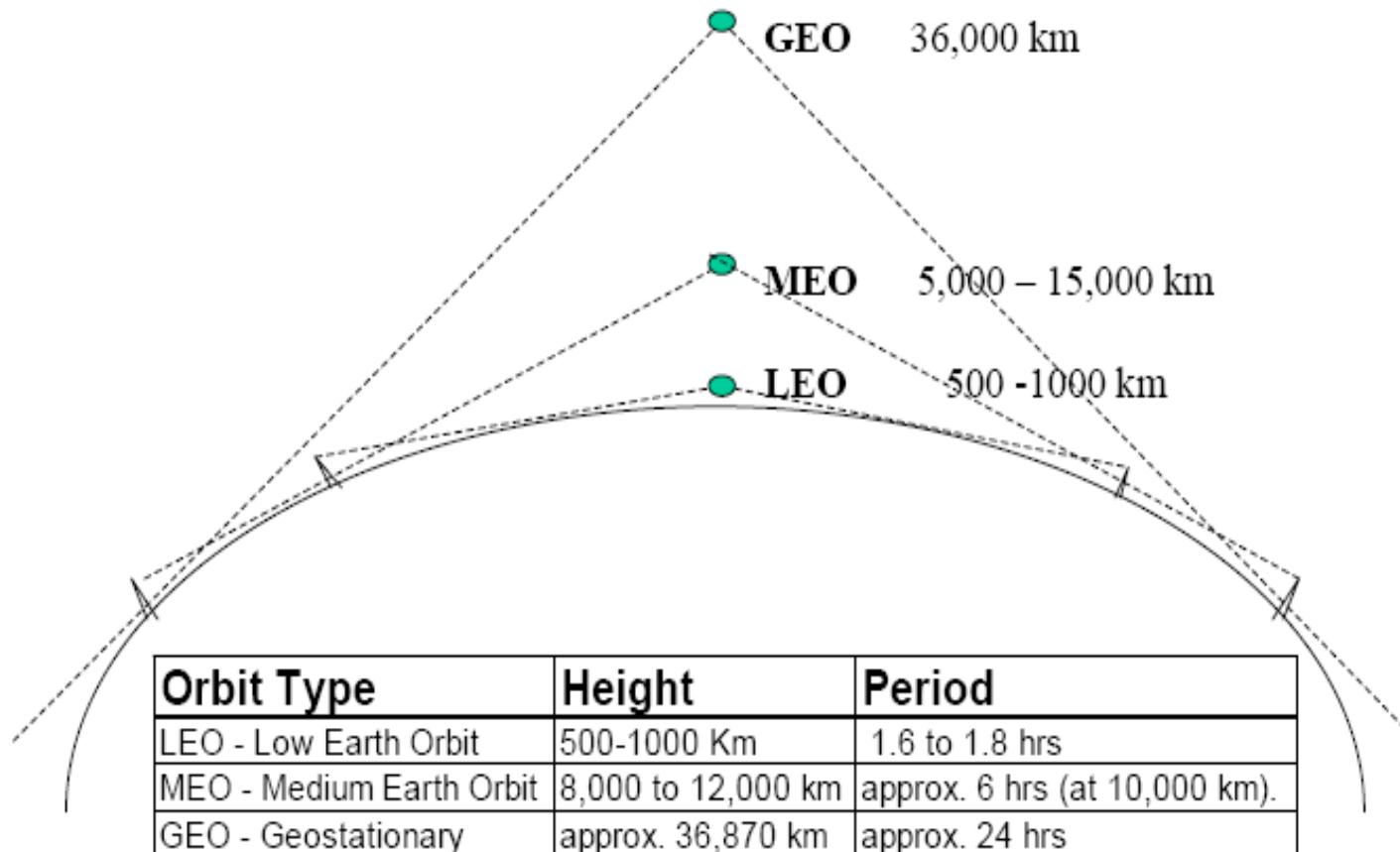


- **Geosynchronous Orbit (GEO):** 36,000 km above Earth, includes commercial and military communications satellites, satellites providing early warning of ballistic missile launch.
- **Medium Earth Orbit (MEO):** from 5000 to 15000 km, they include navigation satellites (GPS, Galileo, Glonass).
- **Low Earth Orbit (LEO):** from 500 to 1000 km above Earth, includes military intelligence satellites, weather satellites.

Source: Federation of American Scientists [www.fas.org]



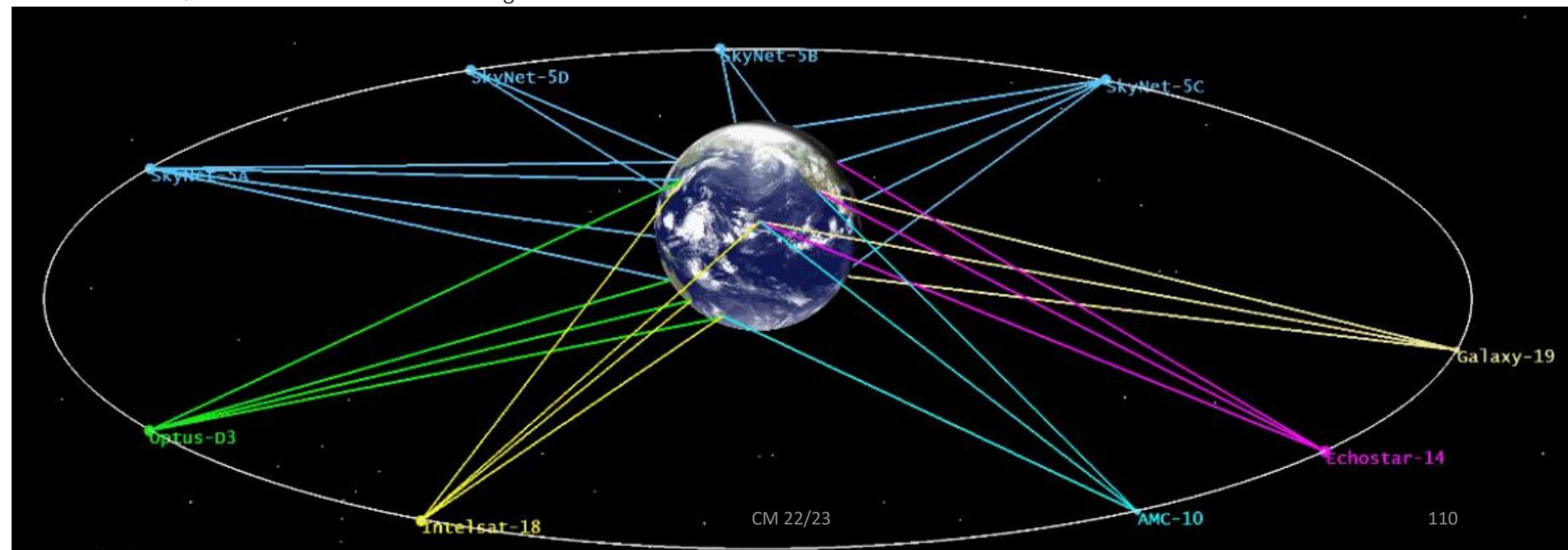
Satellite Orbits





GEO - Geostationary Orbit

- ▶ In the equatorial plane
- ▶ Orbital Period = 23 h 56 m 4.091 s
 - = 1 sidereal day*
- ▶ Satellite appears to be stationary over any point on equator:
 - ▶ Earth Rotates at same speed as Satellite
 - ▶ Radius of Orbit r = Orbital Height + Radius of Earth





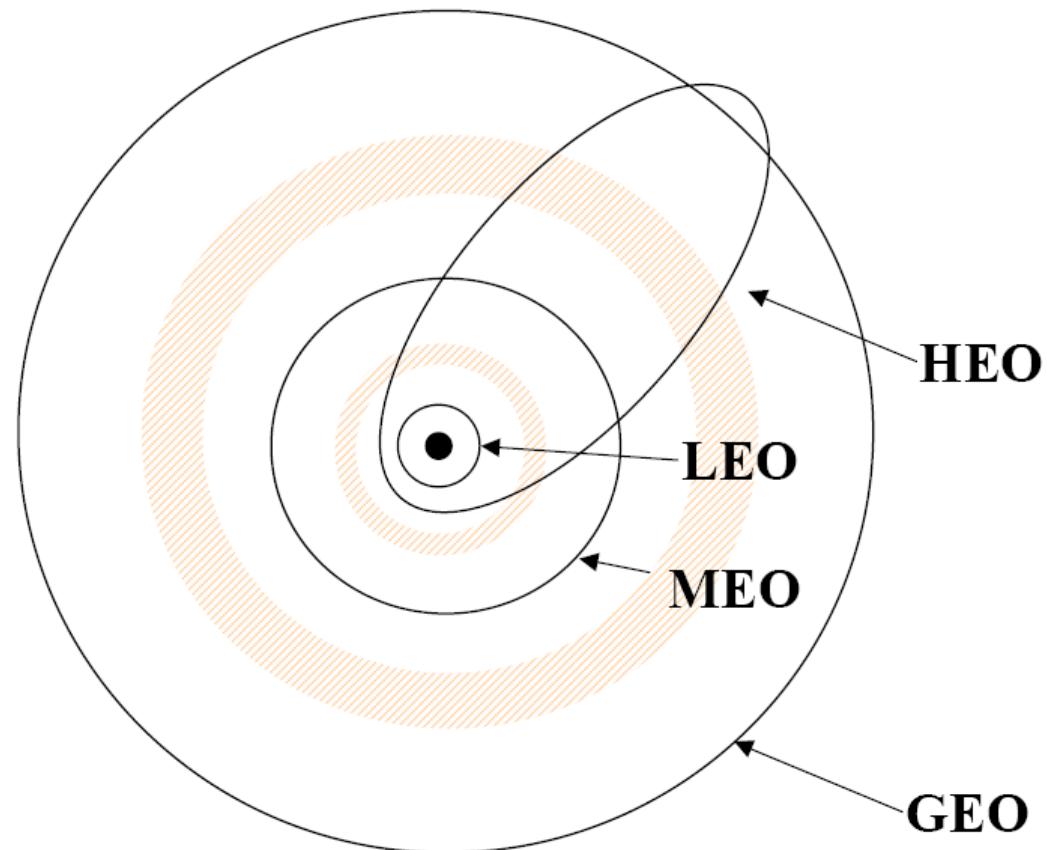
GEO Satellites

- No handover
- Altitude: ~35.786 km.
- One-way propagation delay: 250-280 ms
- 3 to 4 satellites for global coverage
- Mostly used in video broadcasting
- Another applications:
 - Weather forecast, global communications, military applications
- Advantage: well-suited for broadcast services
- Disadvantages: Long delay, high free-space attenuation



NGSO - Non Geostationary Orbits

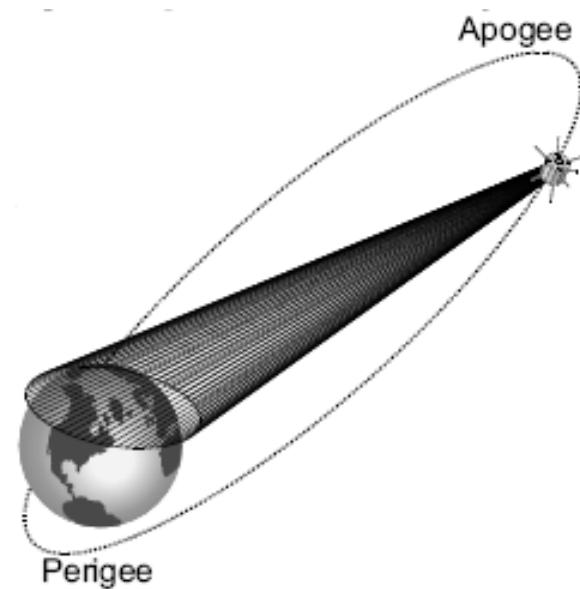
- Orbit should avoid Van Allen radiation belts:
 - Region of charged particles that can cause damage to satellite
 - Occur at
 - $\sim 2000\text{-}4000 \text{ km}$ and
 - $\sim 13000\text{-}25000 \text{ km}$





HEO - Highly Elliptical Orbits

- HEOs ($i = 63.4^\circ$) are suitable to provide coverage at high latitudes (including North Pole in the northern hemisphere)
- Depending on selected orbit (e.g. Molniya, Tundra, etc.) two or three satellites are sufficient for continuous time coverage of the service area.
- All traffic must be periodically transferred from the “setting” satellite to the “rising” satellite (Satellite Handover)





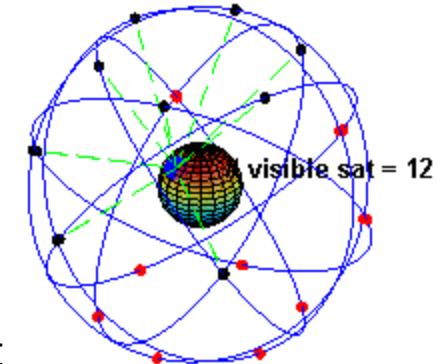
MEO Satellites

- Altitude: 10.000 – 15.000 km
- One-way propagation delay: 100 – 130 ms
- 10 to 15 satellites for global coverage
- Infrequent handover
- Orbit period: ~6 hr
- Mostly used in navigation
 - GPS, Galileo, Glonass
- Communications: Inmarsat, ICO



MEO Example: GPS

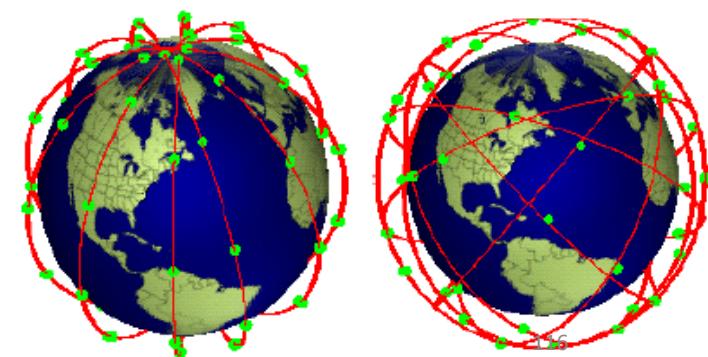
- Global Positioning System
 - Developed by US Dept. Of Defence
 - Became fully operational in 1993
 - Currently 31 satellites at 20.200 km.
 - Last lunch: March 2008
- It works based on a geometric principle
 - “Position of a point can be calculated if the distances between three objects with known positions can be measured”
- Four satellites are needed to calculate the position
 - Fourth satellite is needed to correct the receiver’s clock.
- Selective Availability
- Glonass (Russian): 24 satellites, 19.100 km
- Galileo (EU): 30 satellites, 23.222 km, under development (expected date: 2013)
- Beidou (China): Currently experimental & limited.





LEO - Low Earth Orbits

- Circular or inclined orbit with < 1400 km altitude
 - Satellite travels across sky from horizon to horizon in 5 - 15 minutes => needs handoff
 - Earth stations must track satellite or have Omni directional antennas
 - Large constellation of satellites is needed for continuous communication (66 satellites needed to cover earth)
 - Requires complex architecture
 - Requires tracking at ground





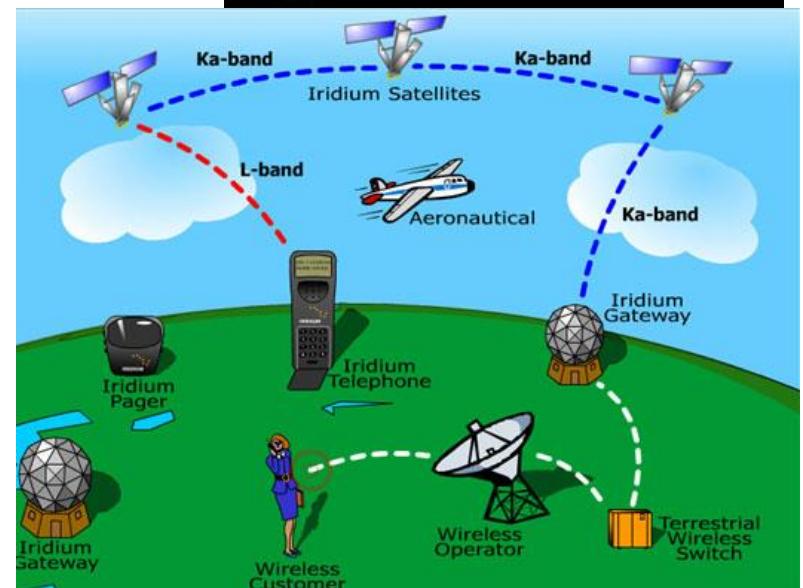
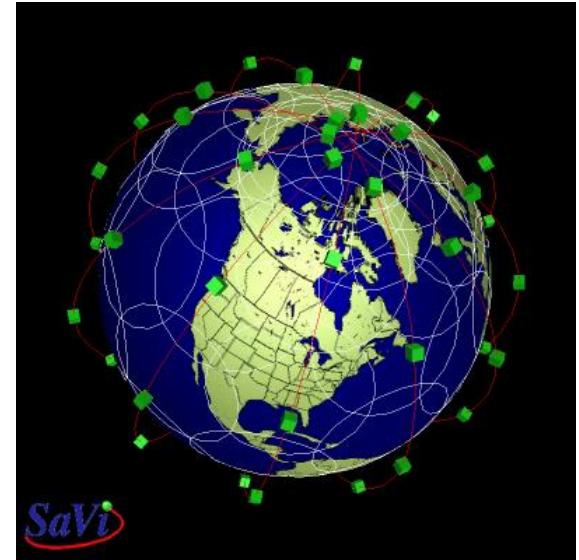
LEO Satellites

- Altitude: 700 – 2.000 km
- One-way propagation delay: 5 – 20 ms
- More than 32 satellites for global coverage
- Frequent handover
- Orbit period: ~2 hr
- Applications:
 - Earth Observation
 - GoogleEarth image providers (DigitalGlobe, etc.)
 - RASAT (First satellite to be produced solely in Turkey)
 - Communications
 - Globalstar, Iridium
 - Search and Rescue (SAR)
 - COSPAS-SARSAT



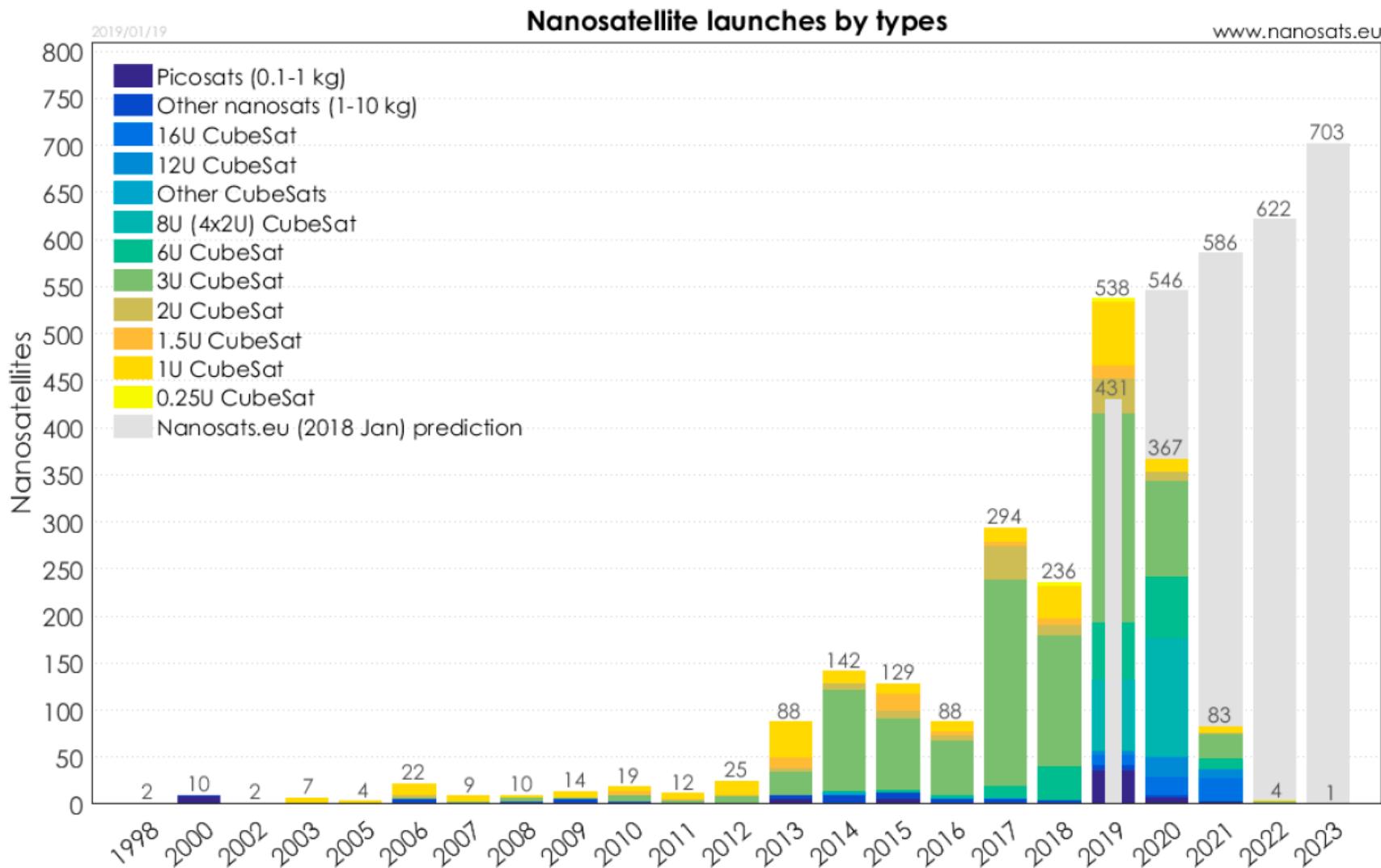
Iridium

- 66 satellites (6 planes, 11 sat per plane) and 10 spares.
- 86.4° inclination: full coverage
- Altitude: 780 km
- Intersatellite links, onboard processing
- Satellite visibility time: 11.1 min
- Satellites launched in 1997-98.
- Initial company went into bankruptcy
 - Technologically flawless, however:
 - Very expensive; Awful business plan
 - Cannot compete with GSM
- Now, owned by Iridium satellite LLC.
- 280.000 subscribers (as of Aug. 2008)
- Multi-year contract with US DoD.
- Satellite collision (February 10, 2009).



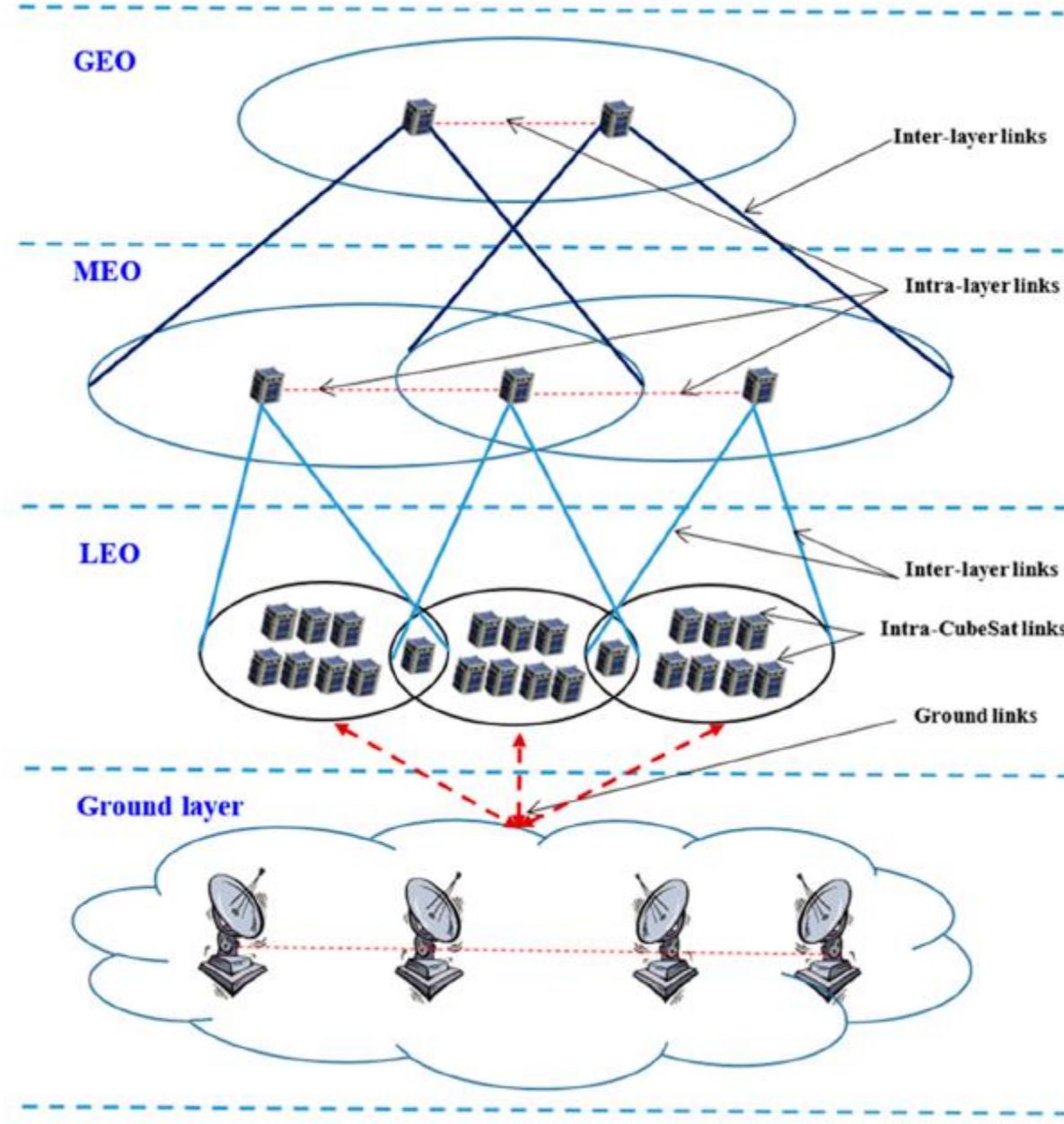


The cubesat explosion





Challenges	Implications
Intermittent connectivity	<ul style="list-style-type: none">- Satellites on this orbit are characterized by scheduled predictable/semi-predictable intermittent connectivity, whether for a satellite to ground links or inter-satellite links.- There are no contemporary paths present for satellite and ground station communication or cross-link communication.
Orbital period	<ul style="list-style-type: none">- LEO satellite orbital velocity ≈ 7800 m/s, based on the satellite altitude orbital period of about 90–110 minu for 160–1200 km altitudes respectively.- Limited encounter time between satellites which in turns bounds data transfer rate.
Inter-CubeSat links	<ul style="list-style-type: none">- Transmission range between two satellites, approximately 5–200 km.- The transmission range of inter-CubeSats is bound by cross-link antenna transmission power.- Limited antenna size and capability compared with the conventional satellites.- Limited antenna coverage compared with the conventional satellites.
Up/Downlinks with the ground station	<ul style="list-style-type: none">- Transmission range between satellite and ground station, approximately 200–1200 km- The transmission range of CubeSats is bounded by the downlink antenna transmit power.- Satellite revisit time Limited antenna size and capability
Altitude and inclination ranges	<ul style="list-style-type: none">- Orbit altitude rang is 200–1200 km above the Earth and orbit inclination ranges 0°–180°.
Natural drag	<ul style="list-style-type: none">- Common de-orbiting behaviour leads to changes in orbital height and hence meeting time between CubeSats will also change over time.- Orbiting at lower altitudes increases the drag process.- The drag upsurges with increasing solar activity (sunspots).
High failure rate	<ul style="list-style-type: none">- Space radiation effects on electronic components, particularly Commercial-off-the Shelf (COTS) components.- Impossibility of recovery under failure.
Energy	<ul style="list-style-type: none">- Solar cells limited space available on the small size of the CubeSat body.- Small storage batteries.- High power consumption of up/downlinks and cross-links.
Topology density	<ul style="list-style-type: none">- Satellite dissemination and encounter times.
CubeSat stability on orbit	<ul style="list-style-type: none">- There is no space on the CubeSats for advanced stability control devices.- Antenna directionality and steering ability.
Data rate	<ul style="list-style-type: none">- A single CubeSat has limited data rate- CubeSat swarms and constellations can provide a higher overall system data rate, however, networking CubeSats in these systems is challenging and requires advanced routing protocols.





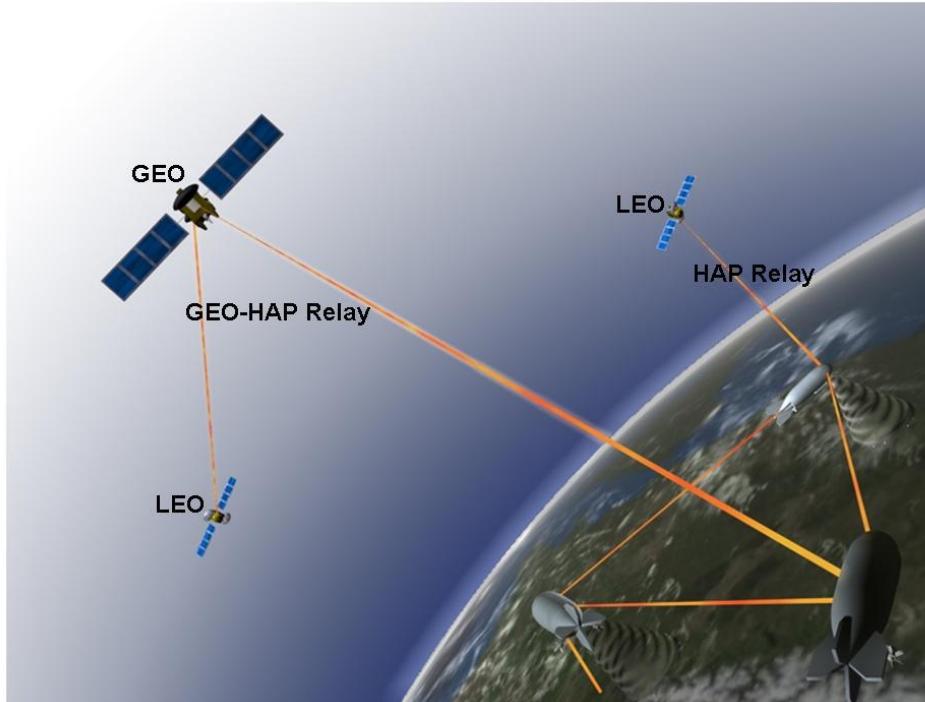
High Altitude Platforms (HAPs)

- Aerial unmanned platforms
- Quasi-stationary position (at 17-22 km)
- Telecommunications & surveillance
- Advantages:
 - Cover larger areas than terrestrial base stations
 - No mobility problems like LEOs
 - Low propagation delay
 - Smaller and cheaper user terminals
 - Easy and incremental deployment
- Disadvantages:
 - Immature airship technology
 - Monitoring of the platform's movement

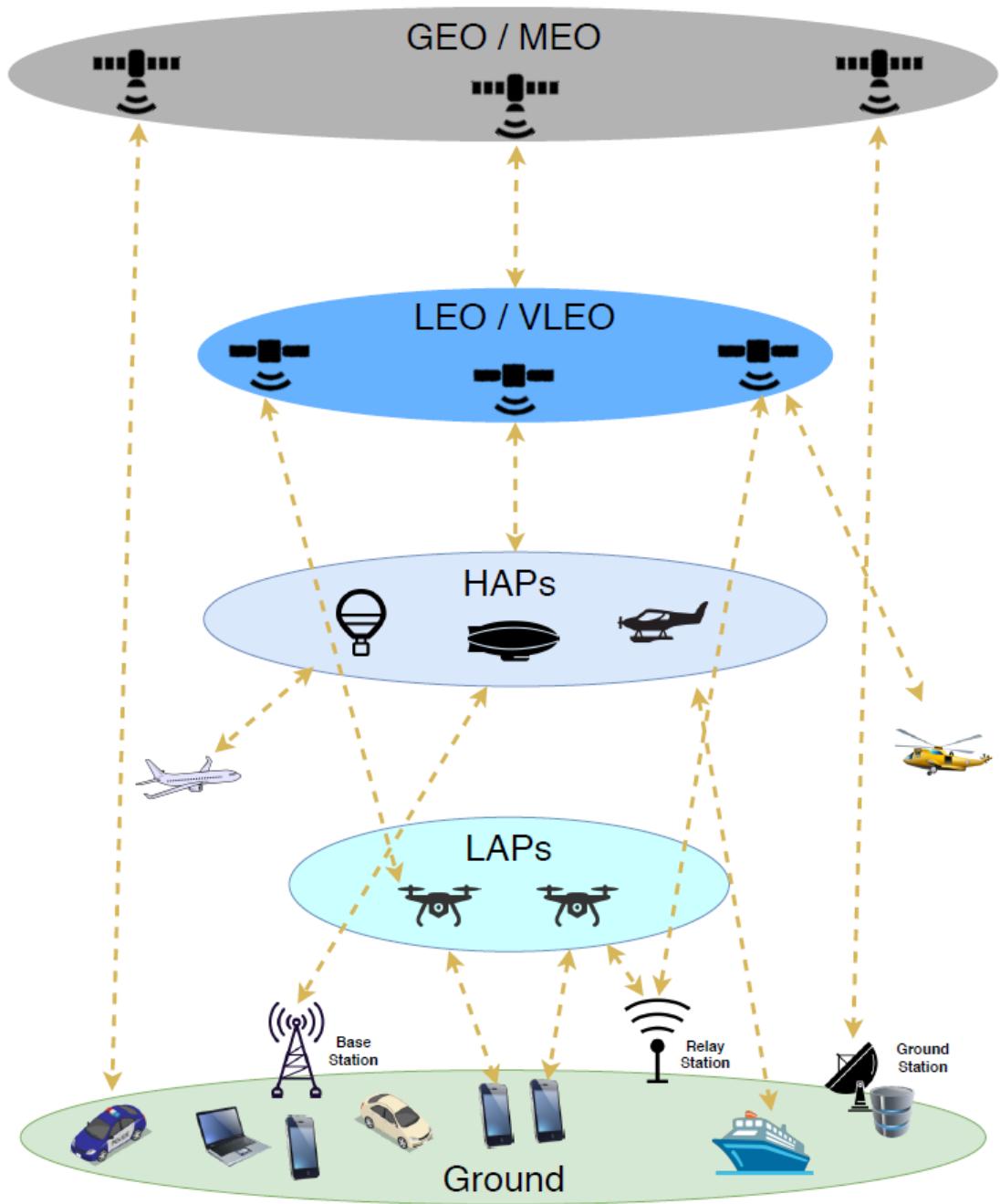




HAP-Satellite Integration



- HAPs have significant advantages.
- Satellites still represent the most attractive solution for broadcast and multicast services
- Should be considered as complementary technologies.



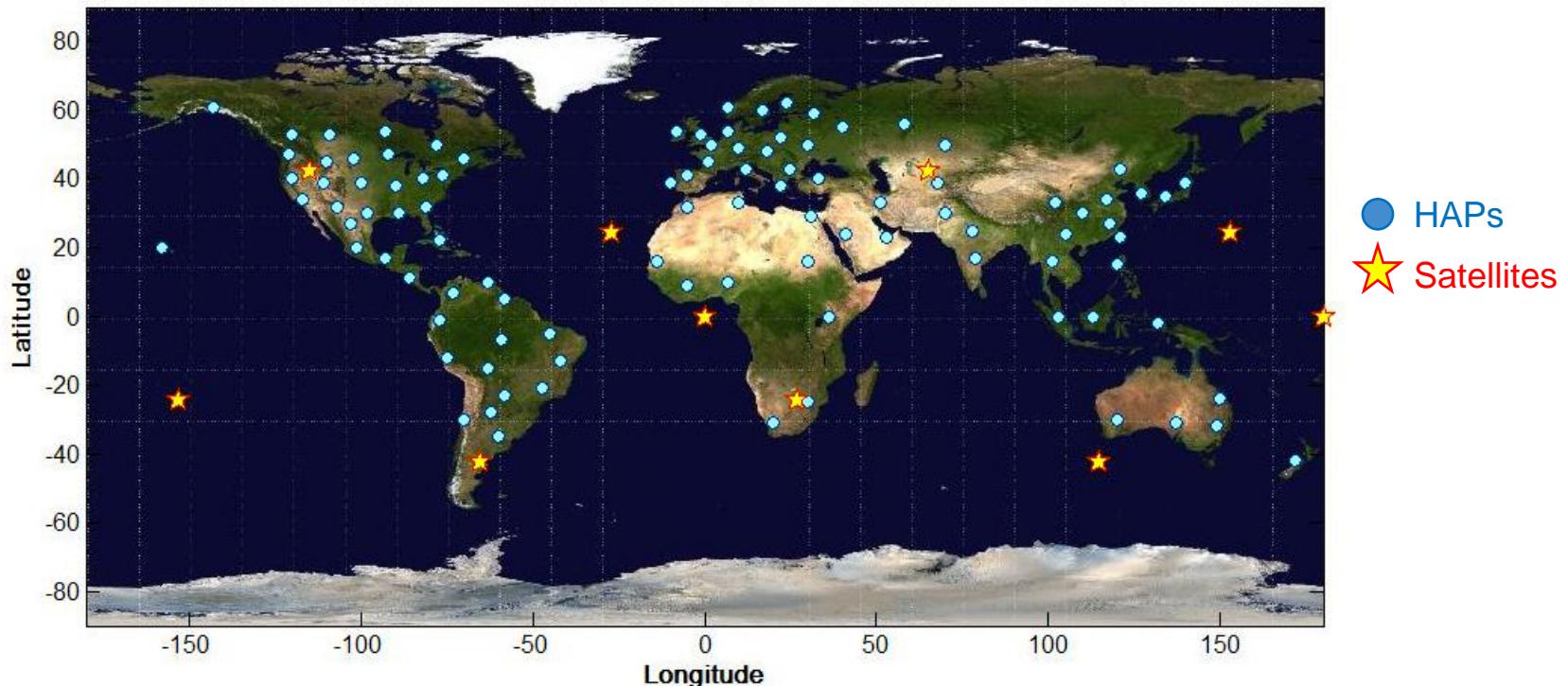


Satellites - Overview

- GEOs have good broadcasting capability, but long propagation delay.
- LEOs offer low latency, low terminal power requirements.
- Inter-satellite links and on-board processing for increased performance and better utilization of satellites
 - From flying mirrors to intelligent routers on sky.
- Major problem with LEOs: Mobility of satellites
 - Frequent hand-over
- Another important problem with satellites:
 - Infeasible to upgrade the technology, after the satellite is launched



An Integration Scenario

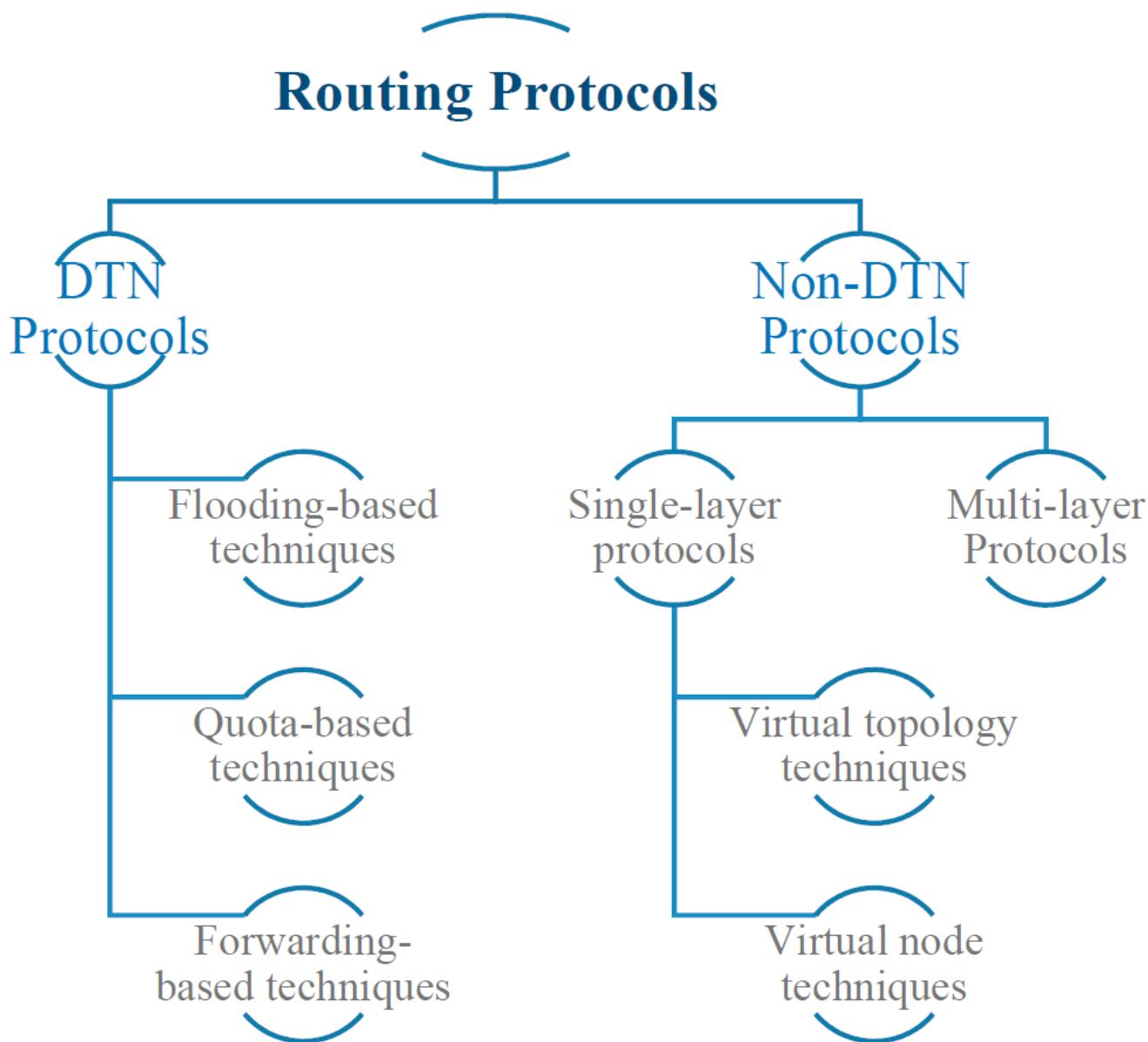


- Integration of HAPs and mobile satellites
- Establishment of optical links



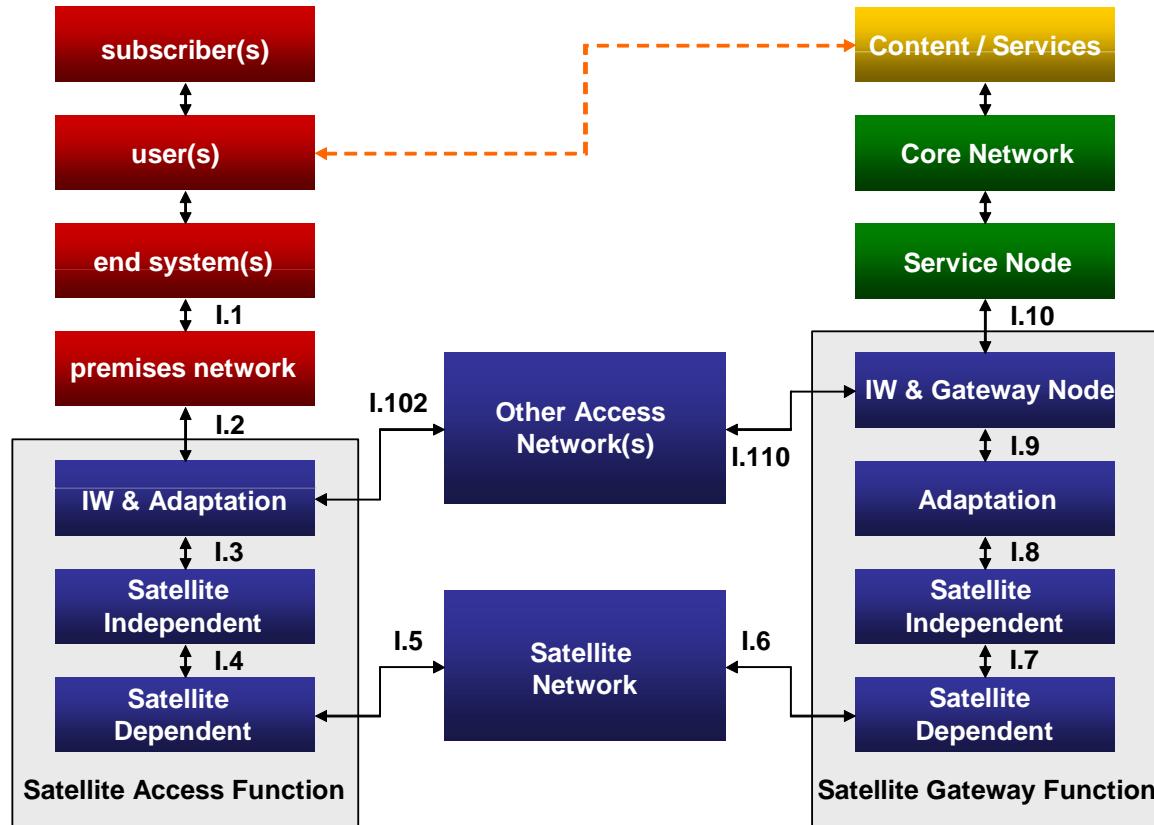
Routing

- One solution: inter satellite links (ISL)
 - ❑ reduced number of gateways needed
 - ❑ forward connections or data packets within the satellite network as long as possible
 - ❑ only one uplink and one downlink per direction needed for the connection of two mobile phones
- Problems:
 - ❑ more complex focusing of antennas between satellites
 - ❑ high system complexity due to moving routers
 - ❑ higher fuel consumption
 - ❑ thus shorter lifetime
- Iridium and Teledesic planned with ISL
- Other systems use gateways and additionally terrestrial networks



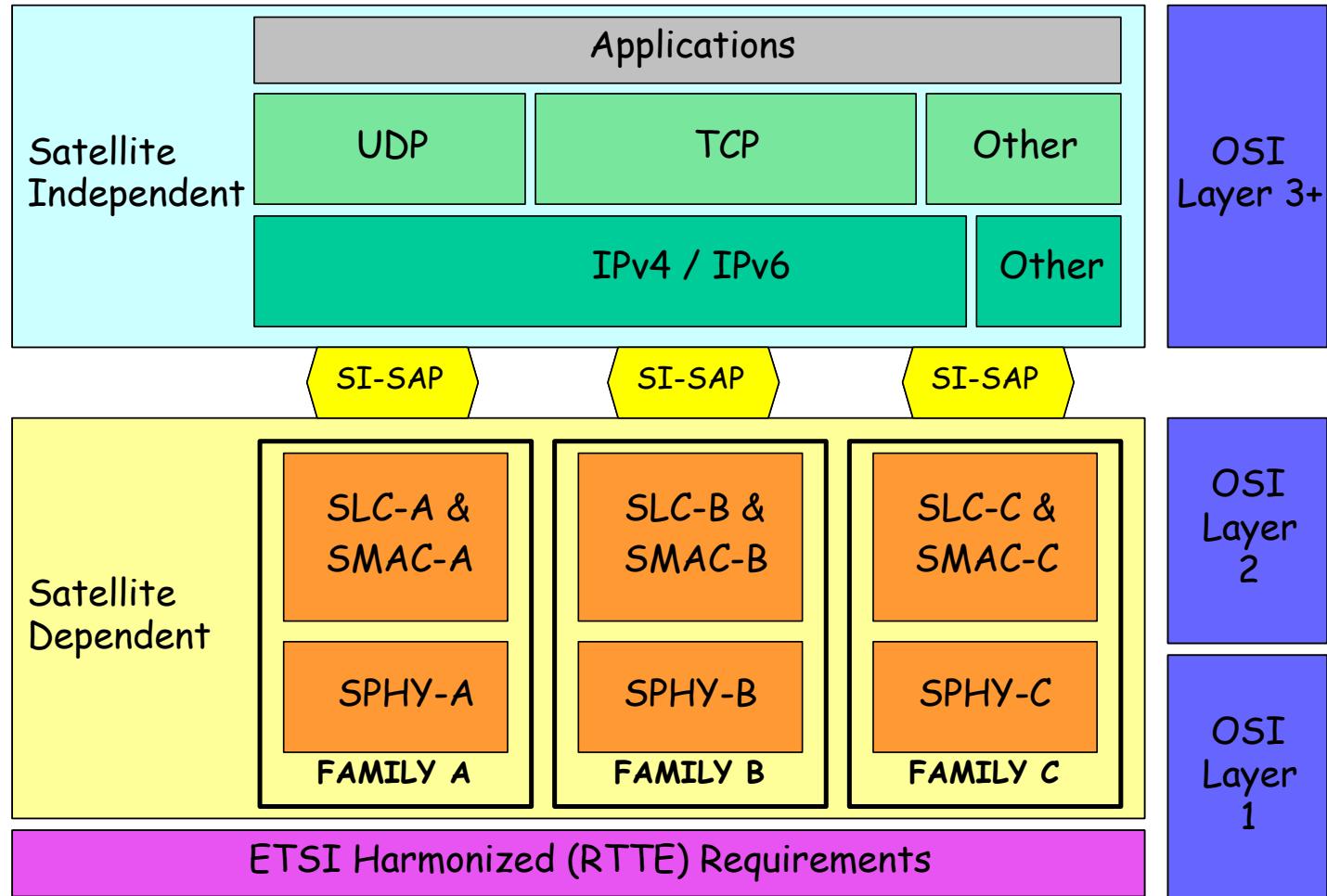


Reference model for satellite access



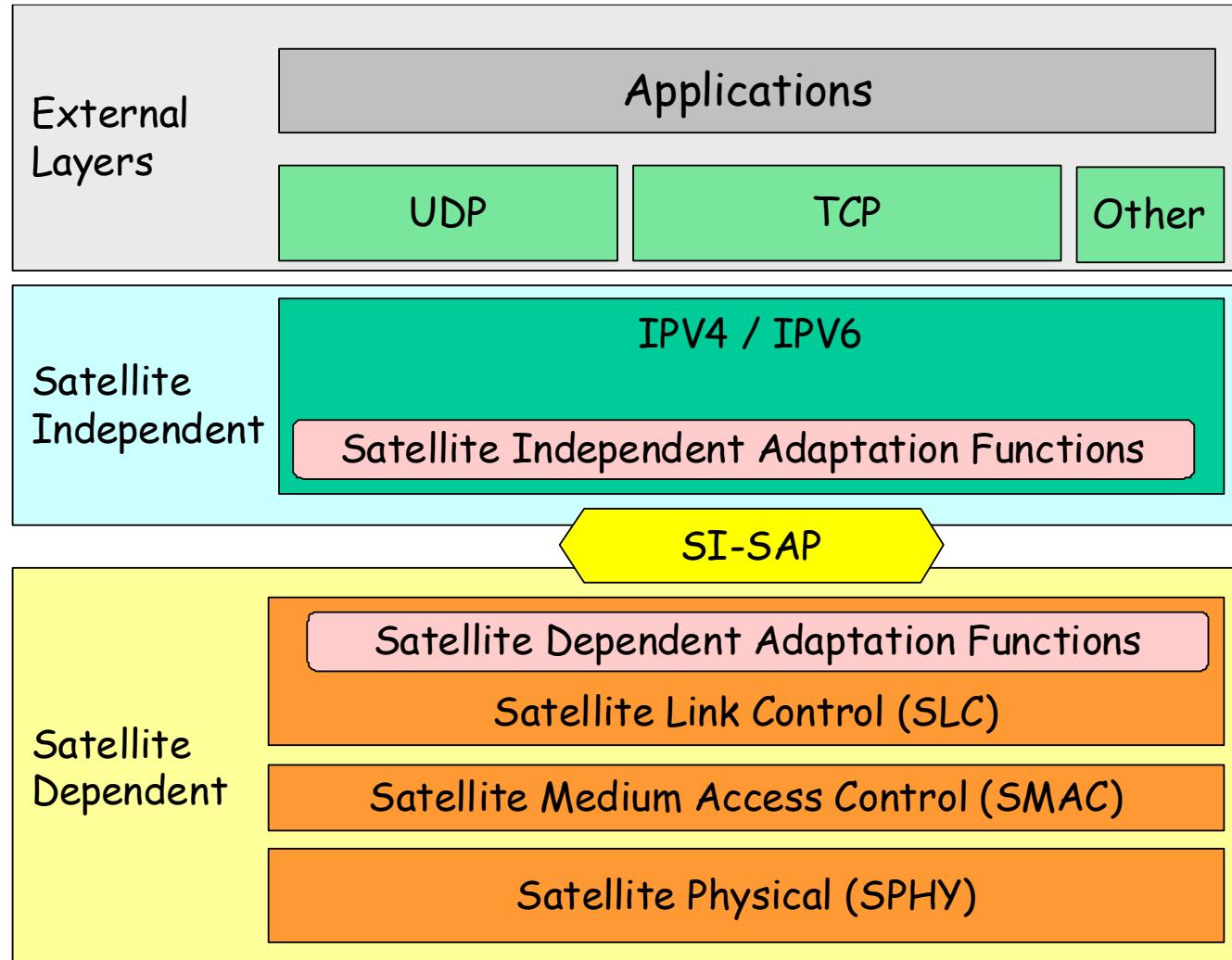


Protocol architecture



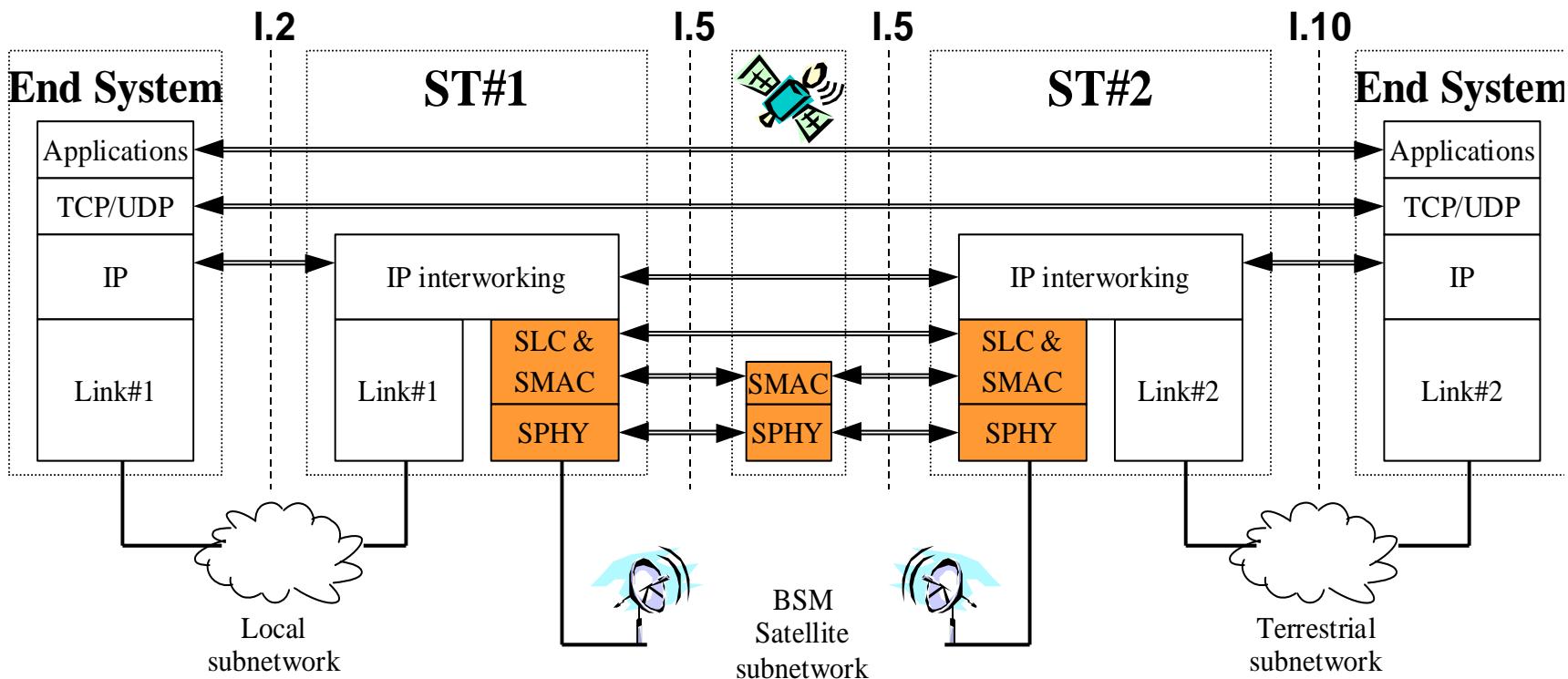


Protocol architecture





IP interworking





Some recent papers

- Satellite Communications in the New Space Era: A Survey and Future Challenges

IEEE COMMUNICATIONS SURVEYS & TUTORIALS

Oltjon Kodheli, Eva Lagunas, Nicola Maturo, Shree Krishna Sharma, Bhavani Shankar, Jesus Fabian Mendoza Montoya, Juan Carlos Merlano Duncan, Danilo Spano, Symeon Chatzinotas, Steven Kisseleff, Jorge Querol, Lei Lei, Thang X. Vu, George Goussetis

- DTN and Non-DTN Routing Protocols for Inter-CubeSat Communications: A comprehensive survey

Electronics,

Mohamed Atef Ali Madni, Saeid Iranmanesh and Raad Raad



Communication Satellites

- A Communication Satellite can be looked upon as a large microwave repeater
- It contains several transponders which listens to some portion of spectrum, amplifies the incoming signal and broadcasts it in another frequency to avoid interference with incoming signals.



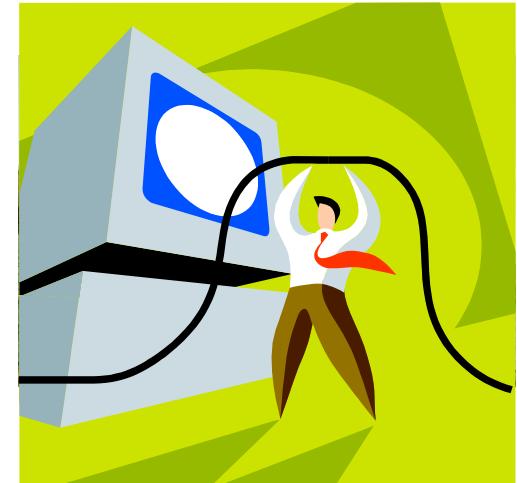
Satellite Signals

- Used to transmit signals and data over long distances
 - Weather forecasting
 - Television broadcasting
 - Internet communication
 - Global Positioning Systems



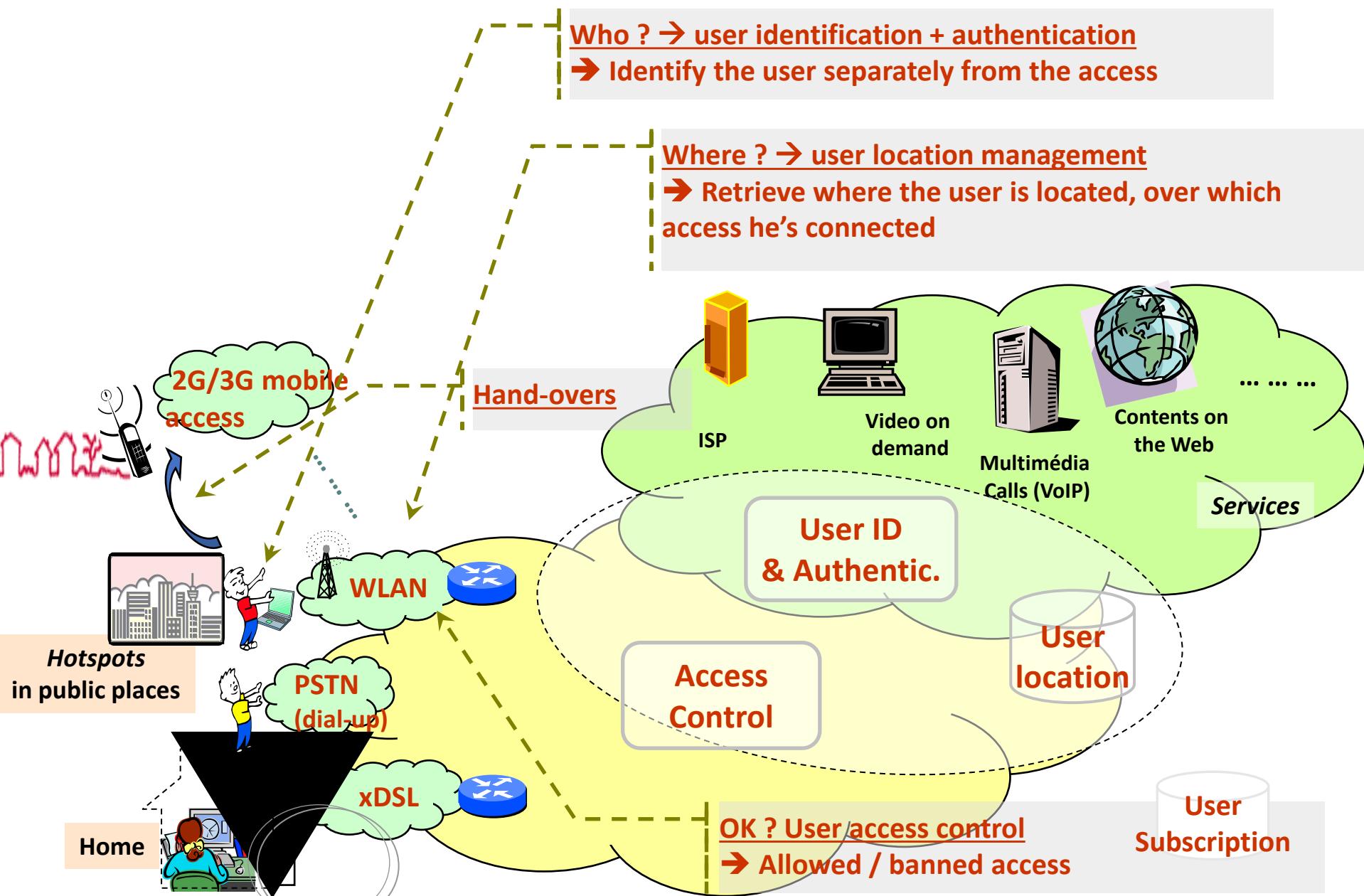
Mobile Networks

Connections and structures





Requirements in a mobile network





Types of connections

- Point-to-point networks
 - Communication points need to be in line of sight (LoS) (e.g. satellite).
- Diffusion networks
 - There is no specific physical relationship between the two communication points (e.g. 802.11)
- Semi-diffusion networks
 - Require some limitations in the relative positioning of the communication points (e.g. Infrared)



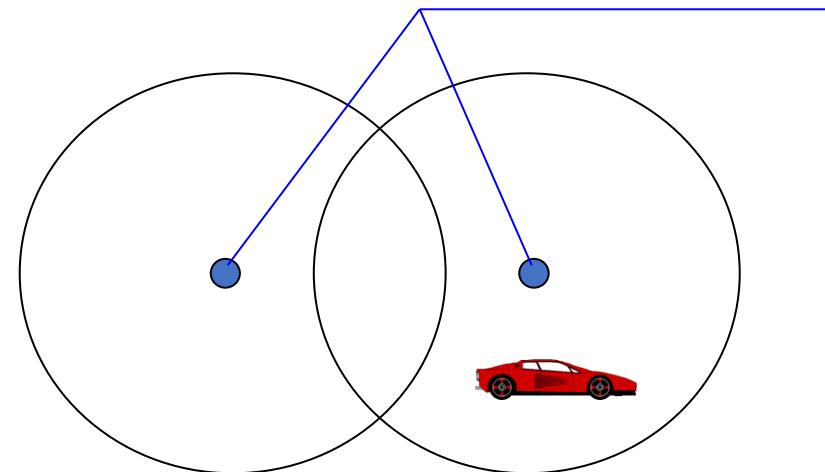
Cell

- Smallest physical entity that allows the access to mobile entities
- Cell ≠ point-to-point connection
- Associated to the physical mechanism of information transfer (radio technologies or infrared)
- Cell
 - Terminal oriented or
 - Defined by a base station
- There is overlapping of different cells in a wireless network



Public cellular network

- Access network with radio link
 - Space is divided in cells with a base station
 - Mobile Node (MN) can work when changing between cells



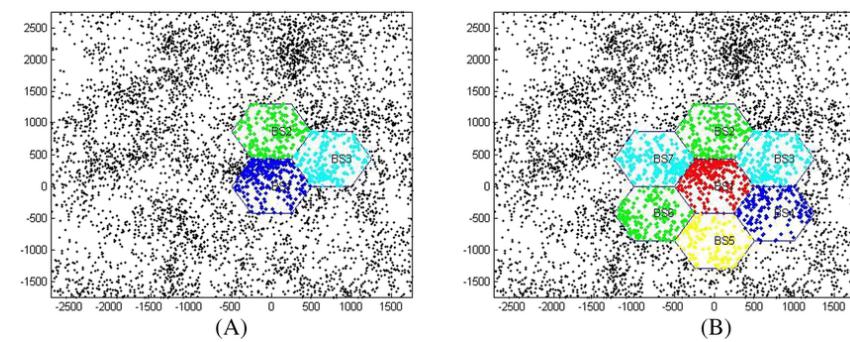
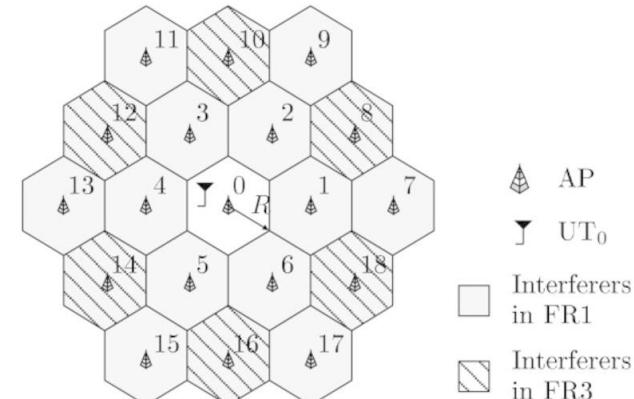
Cell coverage size is

- Highly variable
- Depends on the technology
- Depends on the number of users



Cells

- Coverage size:
 - 100m to 35 km (GSM)
 - Microcells: closed spaces
 - Hat cell: set of cells
 - Avoid frequent handoffs in critical places
- Format:
 - Theoretically analyzed as a hexagon
 - Reality: it depends on the place
- BS positioning:
 - Cell centrally excited
 - BS in the center of the cell, with omni-directional antenna
 - Cell side excited
 - BSs in the vertices (in three)
 - Directional antennas





Cells

Advantages:

- > capacity
- > # users
- < power
- > robustness (distributed system)

Each cell locally takes care of interference, coverage area, etc...

- **Disadvantages**
 - Uses cabled network between cells
 - Many handovers
 - Interference between cells
- **Fundamental:**
 - Cell dimensioning
 - Length of the cell
 - Frequency re-utilization
 - Channel reservation



Wireless networks

- Networks are designed according to the **number of users** and **coverage area**
- In wireless networks there are several scales on number of users and coverage area
 - Personal: PANs → Bluetooth
 - Local: LANs → IEEE 802.11
 - Regional: WANs → GSM, UMTS
 - Worldwide : Sattelite → Iridium

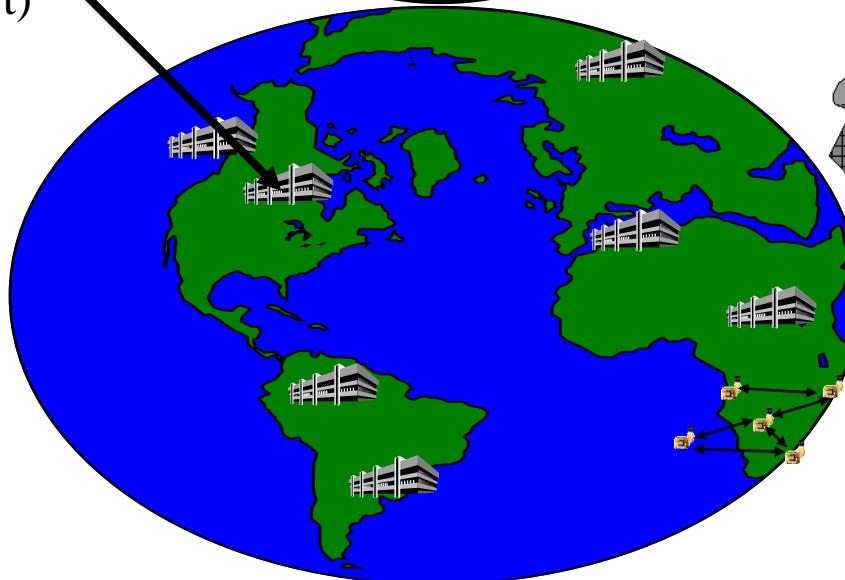




Types of Wireless networks

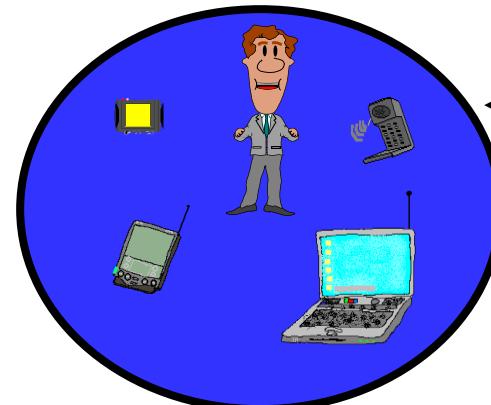
Wireless LAN

Campus (school, company, airport)



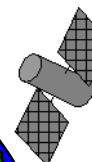
PANs

Personal networks, very limited range
Voice and data with low cost



Satellite

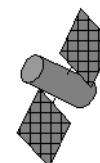
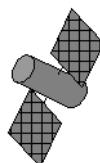
Worldwide networks
High cost



Cellular

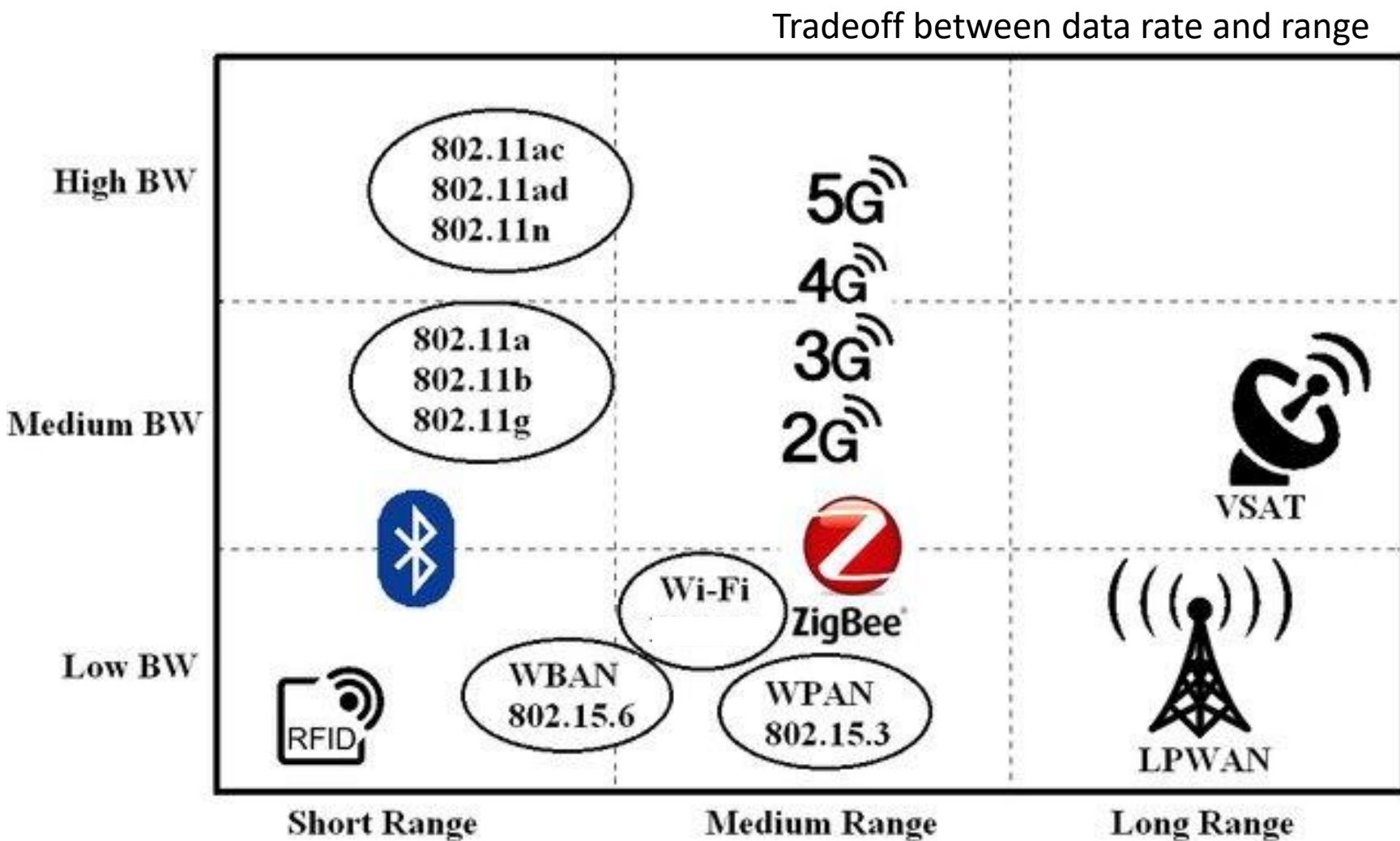
Large geographic coverage

WSN
Multi-dimensional
Variable (low) cost
Usually low bitrate





Comparison Between Wireless Technologies





Wireless Technologies (@~2000)

Metro AreaNetwork

	PAN	LAN	MAN	MAN
Access speed	1-2Mb	11Mb	Mbs	>56kb
Range	10m	100-400m	kms	global
Standard	IEEE 802.15	IEEE 802.11	IEEE 802.16	GPRS 1xRTT
Scalability	Low device specific	Medium ethernet	Infra structure	High regional Infrastructure
Architecture	FHSS	DSSS	cellular	cellular

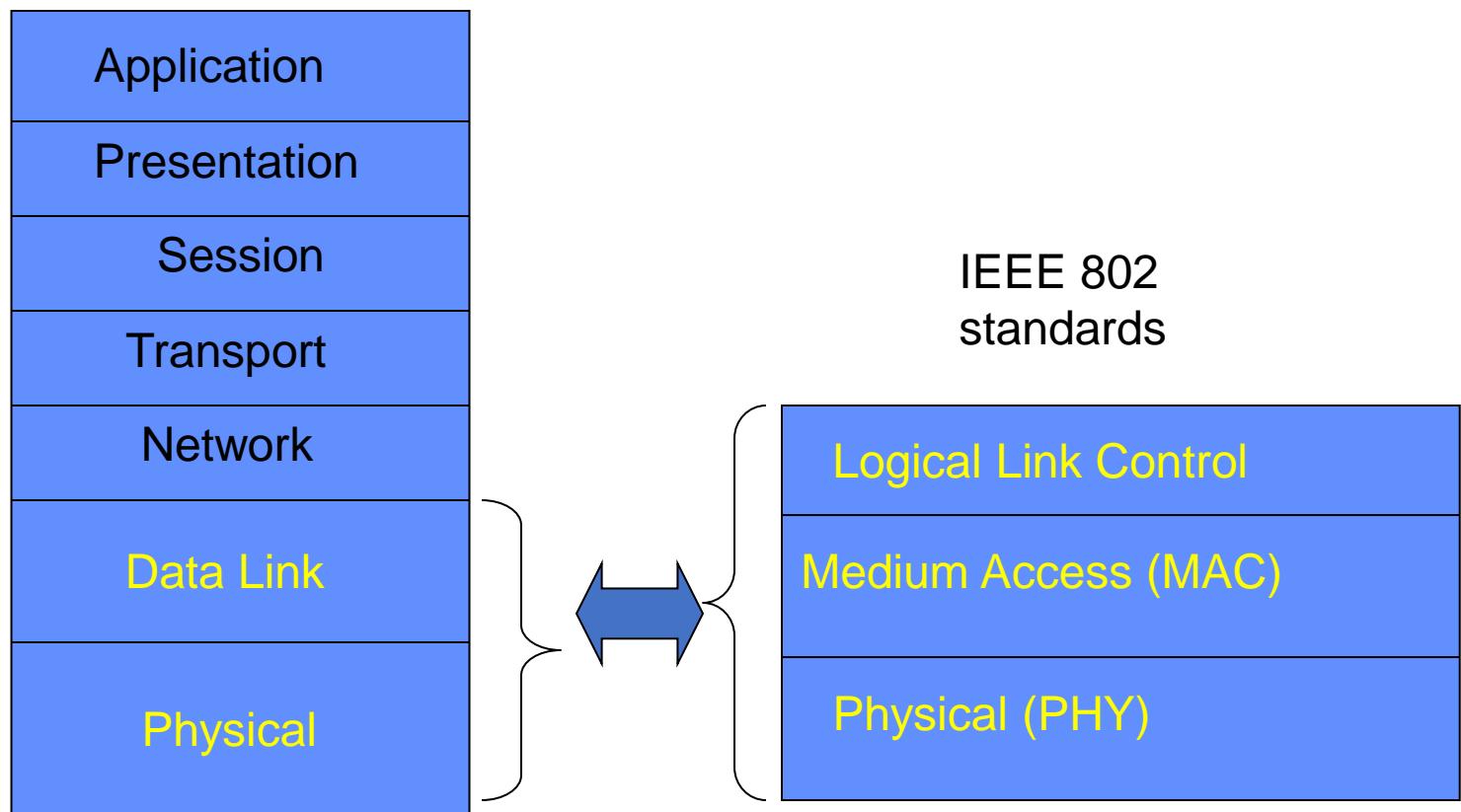


Standardization of Wireless Networks

- Wireless networks are standardized by IEEE.
- Under 802 LAN MAN standards committee.

LAN – Local Area Network
MAN – Metro Area Network

ISO
OSI
7-layer
model





The 802 Class of Standards

- Early list on next slide
- Some standards apply to all 802 technologies
 - E.g. 802.2 is LLC
 - Important for inter operability
- Some standards are for technologies that are outdated
 - Not actively deployed anymore
 - E.g. 802.6

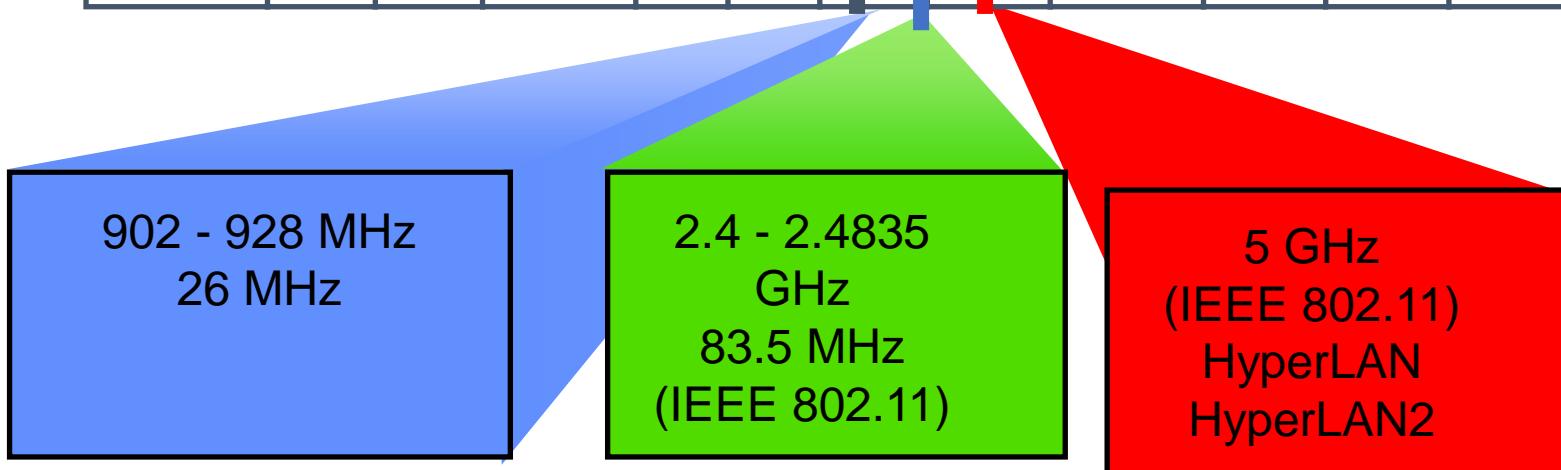
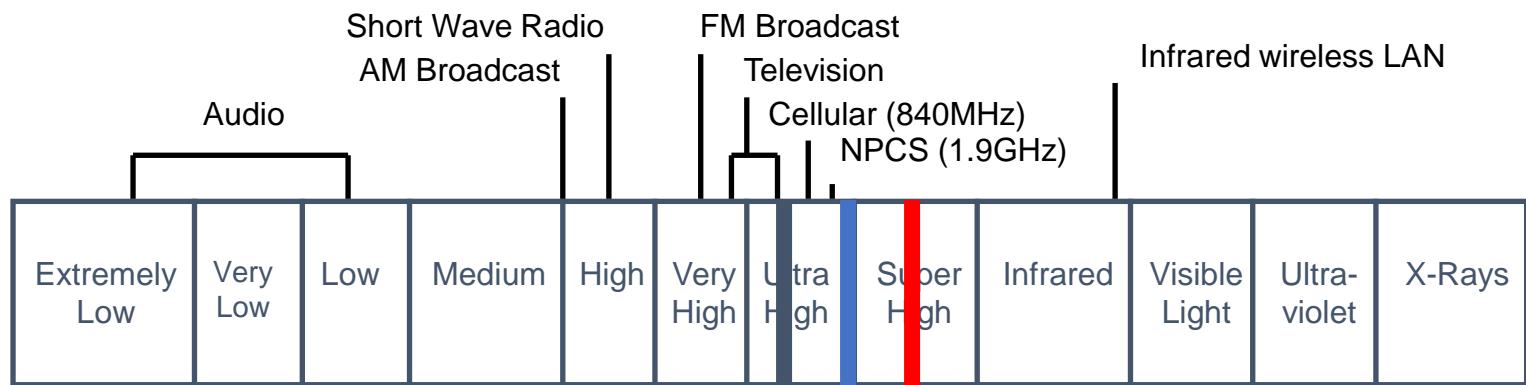


- 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
- 802.1 b Specification for LAN Traffic Prioritization
- 802.1 q Virtual Bridged LANs
- 802.2 Logical Link Control
- 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
 - 802.3a Contention Bus Standard 10base 2 (Thin Net)
 - 802.3b Broadband Contention Bus Standard 10broad 36
 - 802.3d Fiber-Optic InterRepeater Link (FOIRL)
 - 802.3e Contention Bus Standard 1 base 5 (Starlan)
 - 802.3i Twisted-Pair Standard 10base T
 - 802.3j Contention Bus Standard for Fiber Optics 10base F
 - 802.3u 100-Mb/s Contention Bus Standard 100base T
 - 802.3x Full-Duplex Ethernet
 - 802.3z Gigabit Ethernet
 - 802.3ab Gigabit Ethernet over Category 5 UTP
- 802.4 Token Bus Standard
- 802.5 Token Ring Standard
 - 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
 - 802.5f Token Ring Standard 16-Mb/s Operation
- 802.6 Metropolitan Area Network DQDB
- 802.7 Broadband LAN Recommended Practices
- 802.8 Fiber-Optic Contention Network Practices
- 802.9a Integrated Voice and Data LAN
- 802.10 Interoperable LAN Security
- 802.11 Wireless LAN Standard
- 802.12 Contention Bus Standard 1 OOVG AnyLAN
- 802.15 Wireless Personal Area Network
- 802.16 Wireless MAN Standard



Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed, 22 MHz channel bandwidth



NPCS – Narrow Personal Communication Service



802.11



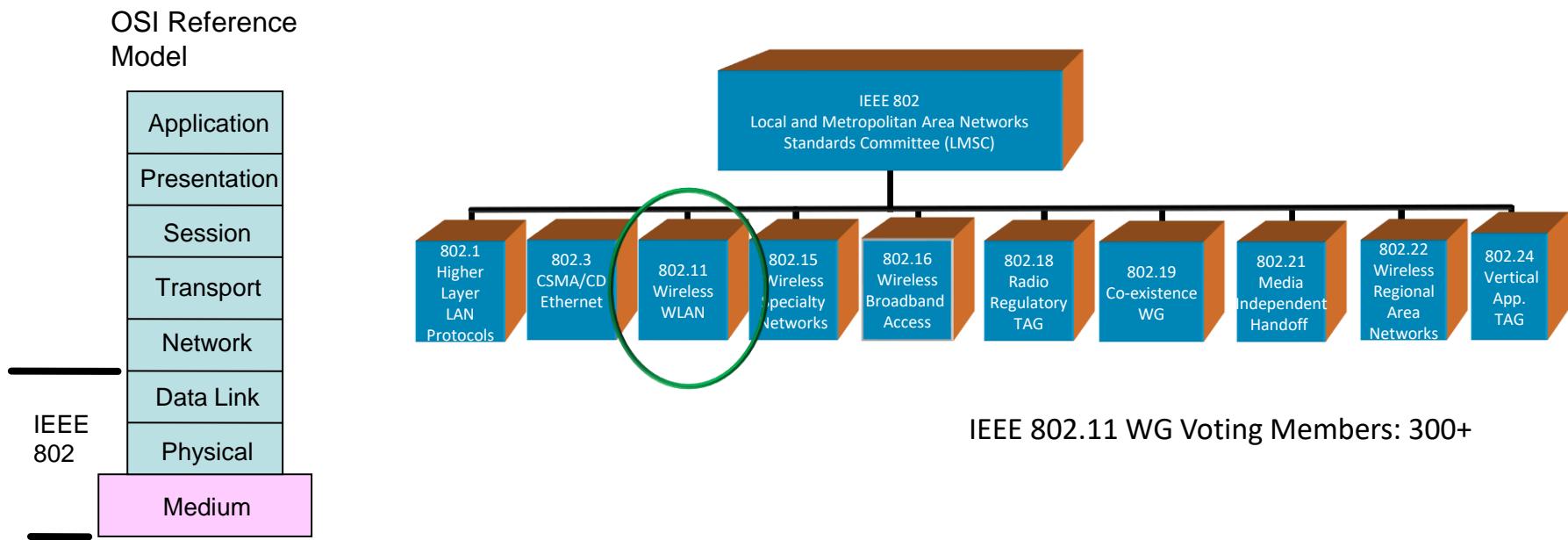
Outline

- 802.11 standard
 - Physical layer
- MAC
 - DCF – Distributed Coordination Function
 - PCF – Point Coordination Function
- Advanced MAC functions



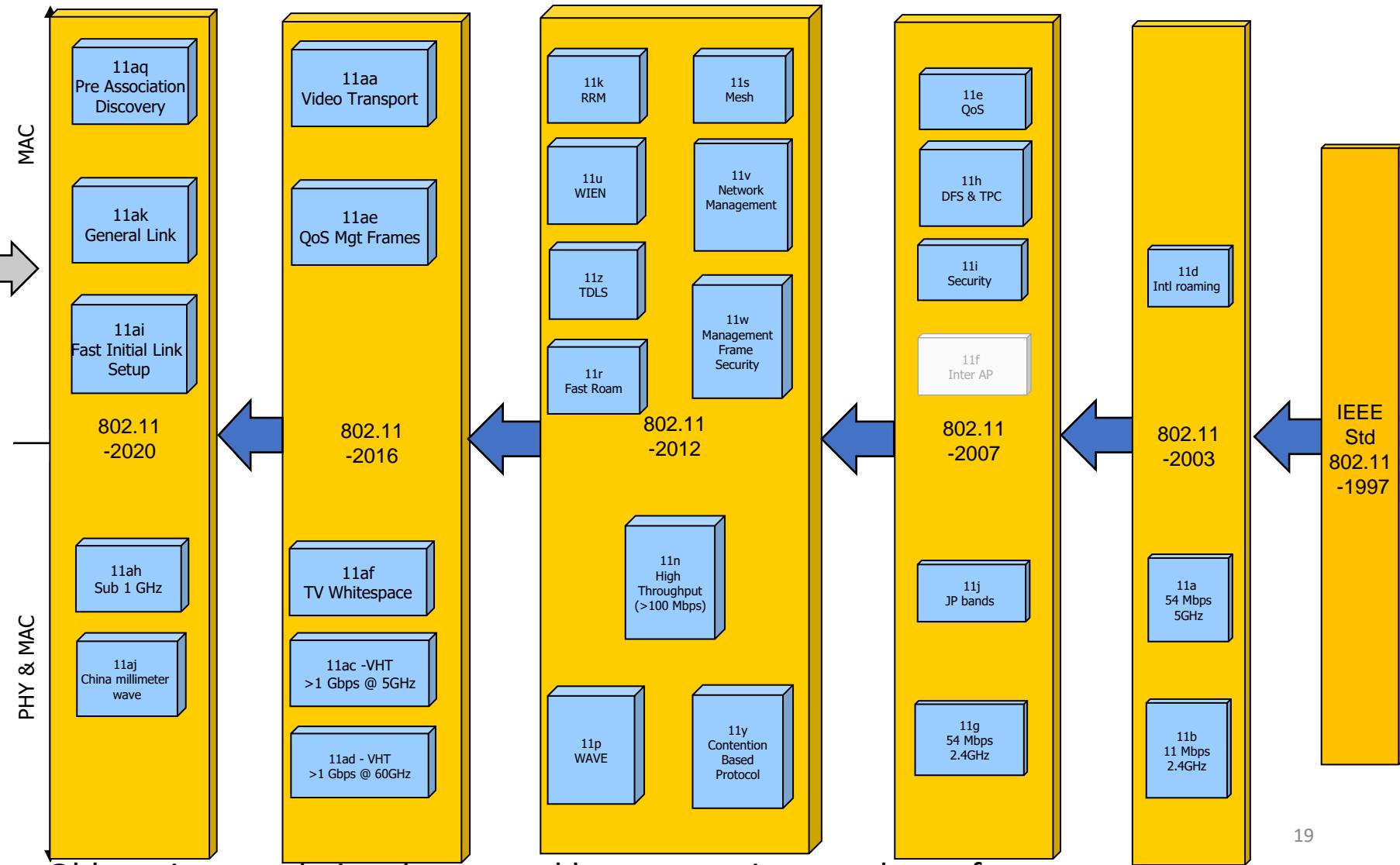
The IEEE 802.11 Working Group

- Standard: Focus on link and physical layers of the network stack
- Leverage IETF protocols for upper layers





Development of the IEEE 802.11 Standard is ongoing since 1997



Old versions are being deprecated by new versions, and new features are added as time goes by.



Historic IEEE 802.11 standard

- Local Wireless Network (WLAN)
- Includes Medium Access Control (MAC)
- Includes(d) five physical layers (PHY)
 - Frequency Hopping Spread Spectrum
 - Direct Sequence Spread Spectrum
 - infrared
 - 11 Mbps - 2.4 GHz
 - 54 Mbps - 5 GHz
 - Early efforts divided in three standards:
 - 802.11
 - 802.11a
 - 802.11b



Historic IEEE 802.11 Family

Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	600 Mbps	~50 m
802.11ac	2014	5 GHz	600Mbps	3.5 Gbps	~35m
802.11ax (Wi-Fi 6)	2021	2.4/5 GHz	130 (2.4 GHz) 400-800Mbps (5GHz)	10 Gbps	~30m
802.11be (Wi-Fi 7)	TBD	2.4/5/6 GHz	?	40 Gbps	?
802.11ay	2021	60 GHz	20 Gbps	20-40 Gbps	300-500m



802.11 Radio technologies evolution

802.11az – 2nd generation positioning features

802.11bb – Light Communications

802.11bc – Enhanced Broadcast Service

802.11bd – Enhancements for Next Generation V2X

802.11be – Extremely High Throughput

802.11bf – WLAN Sensing

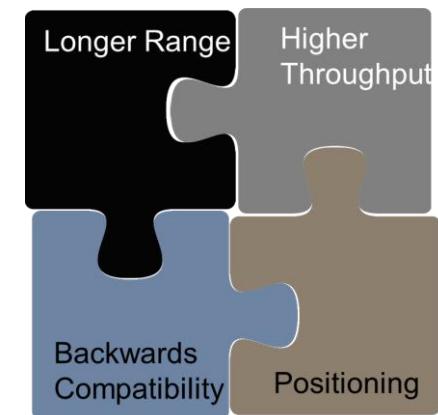
802.11bi – Randomized MAC Addresses

802.11bh – Enhanced Data Privacy

Ultra High Reliability Study Group

AI/ML Topic Interest Group

Ambient Power for IOT Topic Interest Group



<https://www.ieee802.org/11/IEEE%20802-11-Overview-and-Amendments-Under-Development.pptx>



IEEE 802.11 innovation

- Market demands and new technology push for new 802.11 standards
- Demand for throughput
 - Continuing exponential demand for throughput ([802.11ax](#) and [802.11ay](#), [802.11be](#))
 - Most (50-80%, depending on the country) of the world's mobile data is carried on 802.11 (Wi-Fi) devices
- New usage models / features
 - Dense deployments ([802.11ax](#)), Indoor Location ([802.11az](#)),
 - Automotive (IEEE Std 802.11p, Next Gen V2X), Internet of Things ([802.11ah](#))
 - Low Power applications ([802.11ba](#))
 - WLAN Sensing ([802.11bf](#) – pending approval)
- Technical capabilities
 - MIMO (IEEE Std 802.11n, 802.11ac, [802.11ay](#)) and OFDMA ([802.11ax](#))
 - 60 GHz radios ([802.11ay](#))
- Changes to regulation
 - TV whitespaces (IEEE Std 802.11af), Radar detection (IEEE Std 802.11h), 6GHz ([802.11ax](#), [802.11be](#))
 - Coexistence and radio performance rules (e.g., ETSI BRAN, ITU-R)



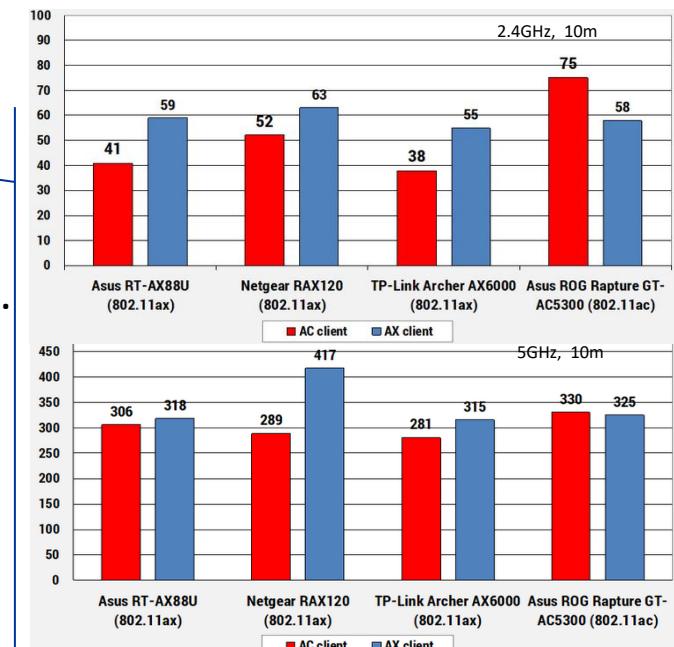
New 802.11 Radio technologies

Current recent innovations being deployed:

- 802.11ax – Increased throughput in 2.4, 5 (and 6) GHz bands. Increased efficiency.

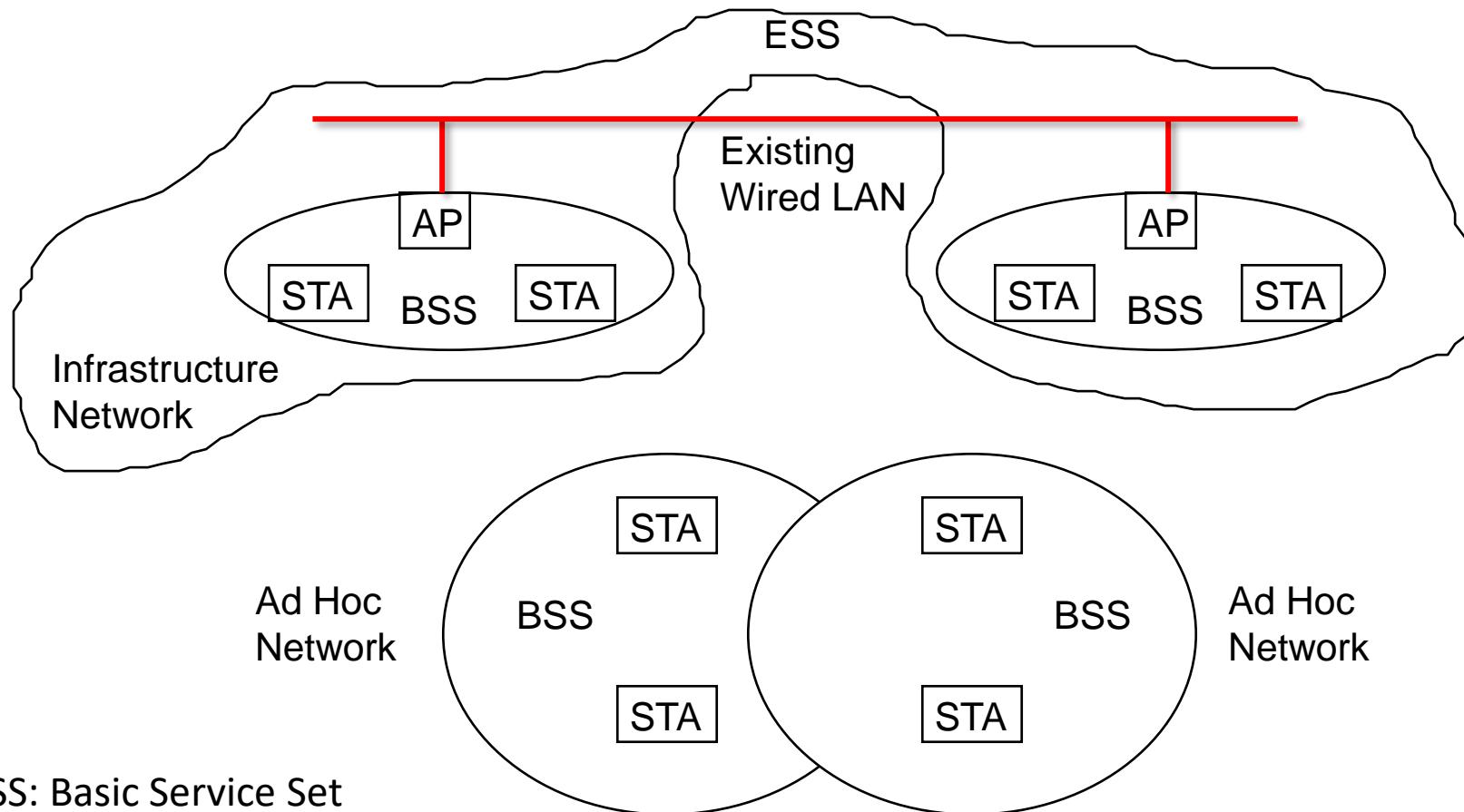
WiFi6

- 802.11ay – Support for 20 Gbps in 60 GHz band.
- 802.11az – 2nd generation positioning features.
- 802.11ba – Wake up radio. Low power IoT applications.
- 802.11bb – Light Communications
- 802.11bc – Enhanced Broadcast Service
- 802.11bd – Enhancements for Next Generation V2X
- 802.11be – Extremely High Throughput
- 802.11bf – WLAN Sensing [pending approval]





802.11 Architecture



BSS: Basic Service Set

ESS: Extended Service Set

DS: Distribution System _____



Components

- Station (STA) — Mobile Terminal
- Access Point (AP) - STA are connected to Access Points (infrastructured networks)
- Basic Service Set (BSS) — STA and AP with the same coverage and connectivity area create a BSS.
- Extended Service Set (ESS) — Multiple BSSs connected via the APs create an ESS.
- Distribution System (DS) - Contains the entity that interconnects APs



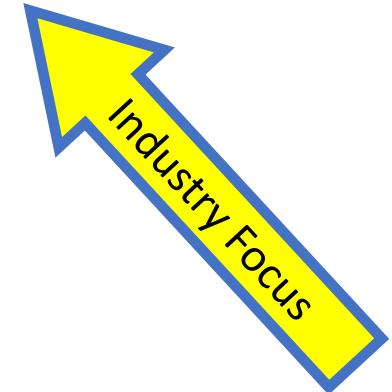
Distribution System (DS)

- The Distribution system interconnects multiple BSSs
- 802.11 standard **logically separates** the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the **Extended Service Set** network (ESS)



Infrastructure vs Ad Hoc Mode

- Infrastructure mode: stations communicate with one or more access points which are connected to the wired infrastructure
 - What is deployed in practice
- Two modes of operation:
 - Distributed Control Functions - DCF
 - Point Control Functions – PCF
 - PCF is rarely used - inefficient
- Alternative is “ad hoc” mode: multi-hop, assumes no infrastructure
 - Rarely used, e.g. military
 - Hot research topic!





What about Ad Hoc?

- Ad-hoc mode: no fixed network infrastructure
 - Based on an Independent BSS
 - A wireless endpoint sends and all nodes within range can pick up signal
 - Each packet carries destination and source address
 - Effectively need to implement a “network layer”
 - How do know who is in the network?
 - Routing?
 - Security?



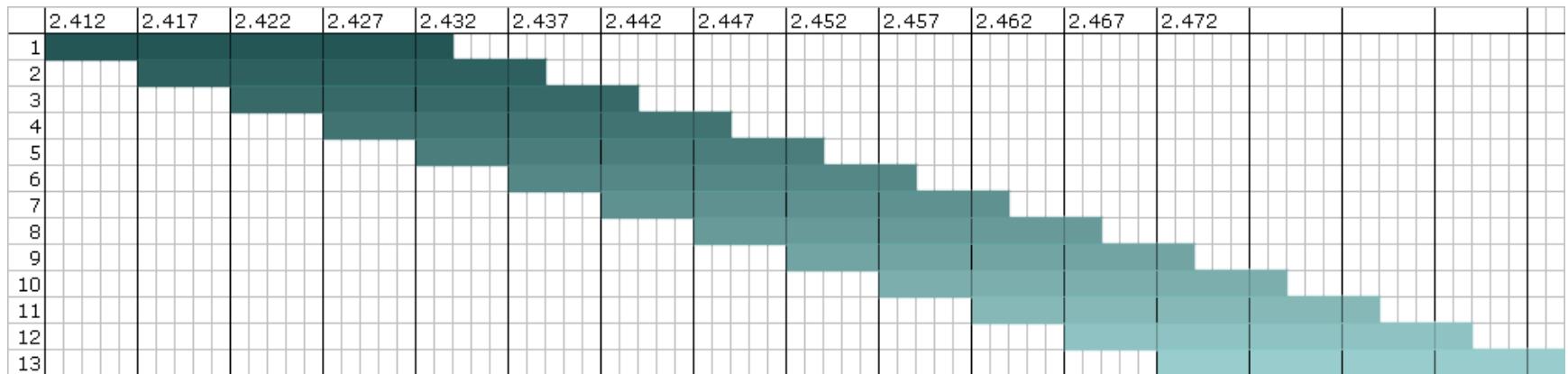
Outline

- 802.11 standard
 - Physical layer
- MAC
 - DCF
 - PCF
- Advanced MAC functions



802.11 Channels (2.4GHz)

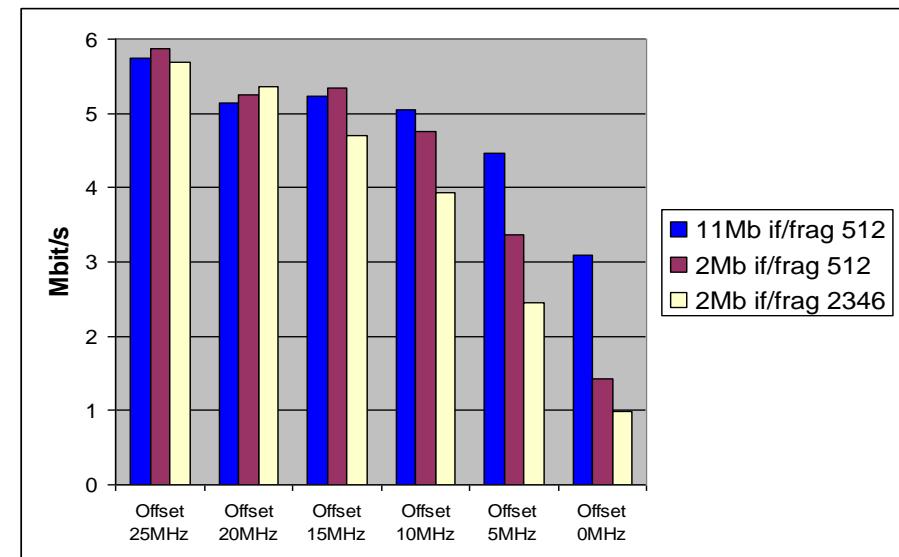
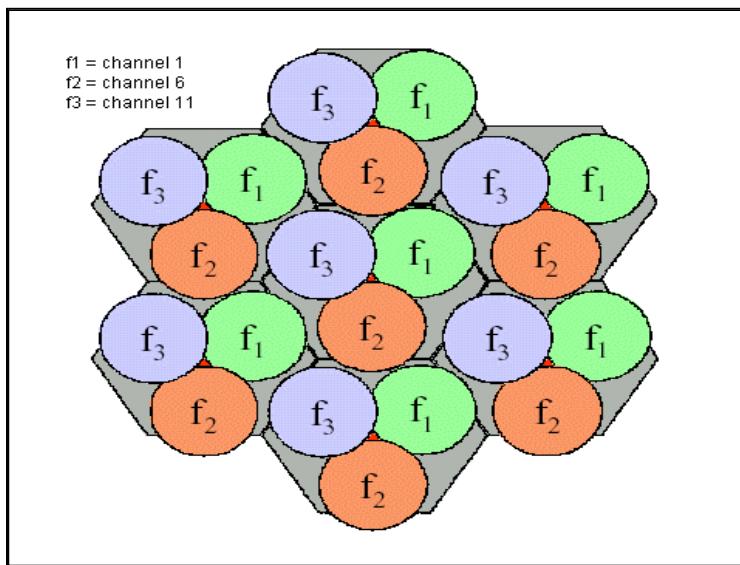
- The frequency is divided in channels
- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22 MHz
- Significant overlap
- Best channels are 1, 6 and 11





Frequency planning

- Interference from other WLAN systems or cells
- IEEE 802.11 operates at uncontrolled ISM band
- 14 channels of 802.11 are overlapping, only 3 channels are disjointed.
For example Ch1, 6, 11
- Throughput decreases with less channel spacing
- A example of frequency allocation in multi-cell network



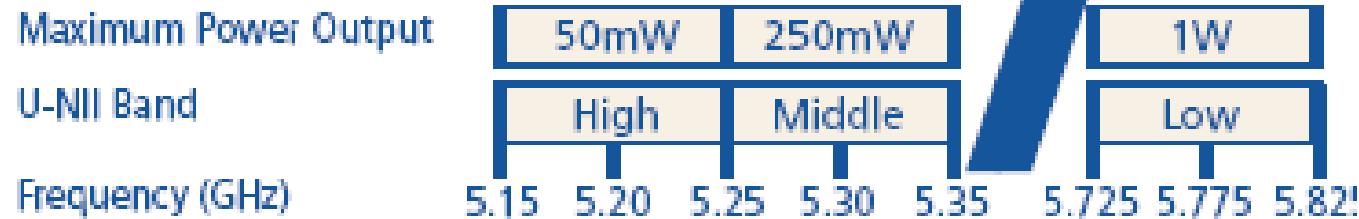
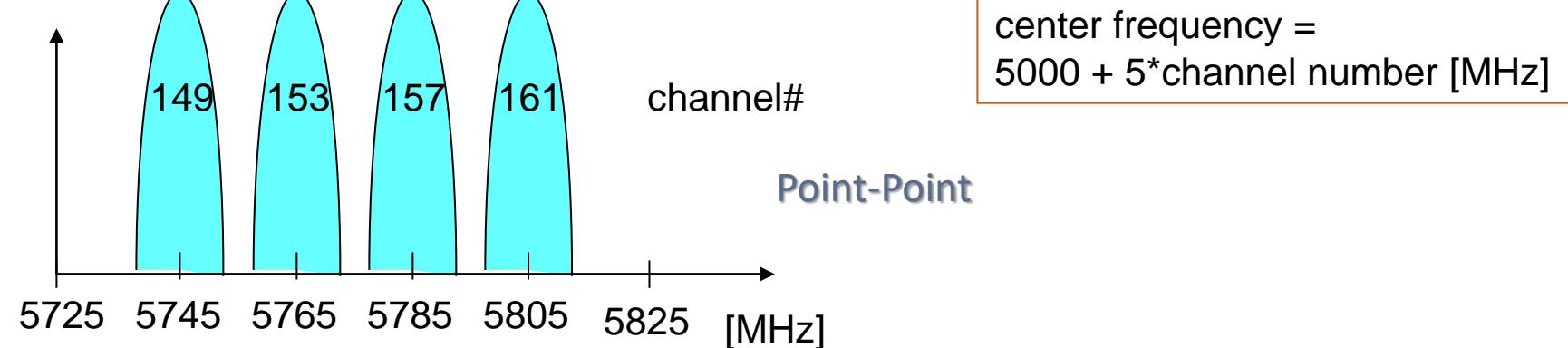
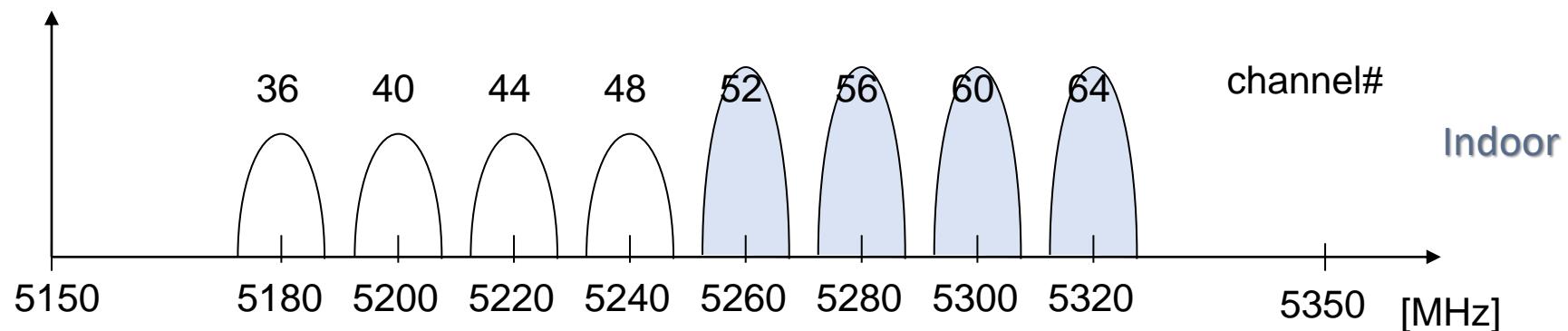


802.11 (5GHz)

- Uses frequency division in the 5.2 and 5.7 GHz bands
- What are the benefits?
 - Greater bandwidth
 - Less potential interference (5GHz)
 - More non-overlapping channels
- But does not provide interoperability
 - Interoperability at chipset level

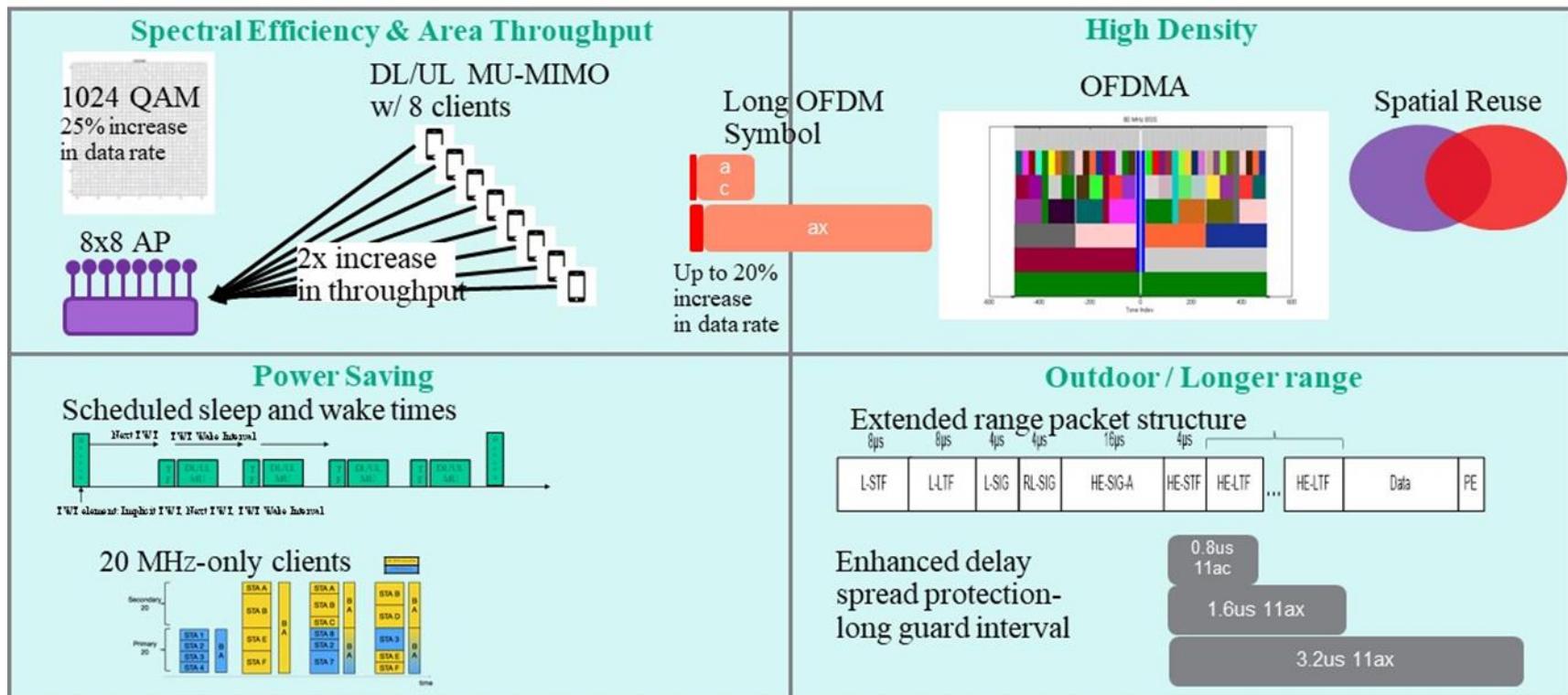


Example: 802.11a Physical Channels





WiFi 6 radio layer enhancements



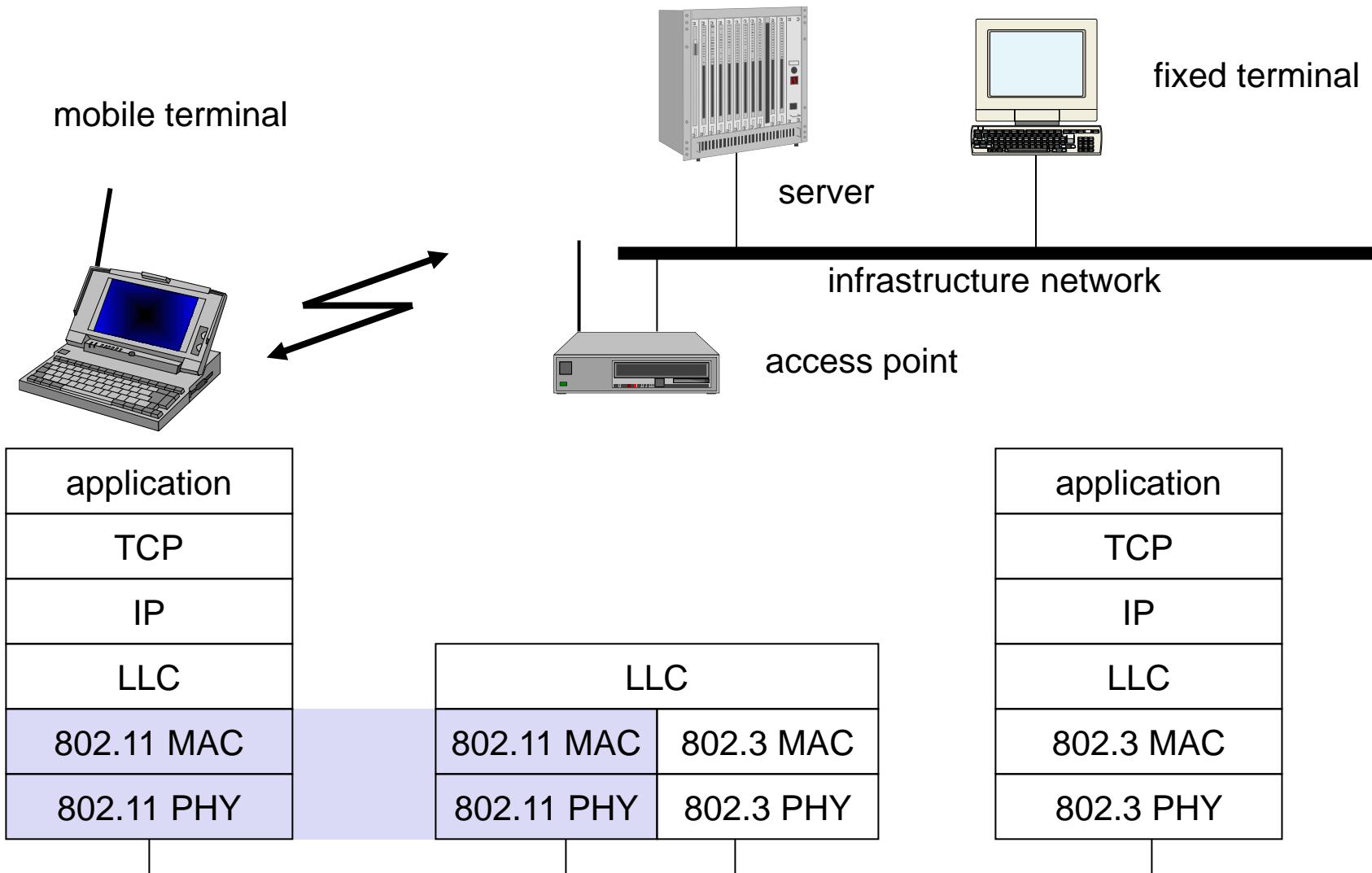


Outline

- 802.11 standard
 - Physical layer
- MAC
 - DCF
 - PCF
- Advanced MAC functions



802.11- in the TCP/IP stack





802.11 MAC Overview

- Uses variant of Carrier Sense Multiple Access with Collision Avoidance (CS/MACA)
 - RTS/CTS used for addressing hidden-nodes
- Automatic Repeat Request (ARQ)
 - Error control method for reliability
 - All frames have to be properly ACK, or timeout occurs
- Two operating modes:
 - Infra-structured network (Access point)
 - Ad-Hoc networks (without access point)
- Power saving support
- Wired Equivalent Privacy (WEP)
- MAC management
- Independent of the physical layer or of operating mode

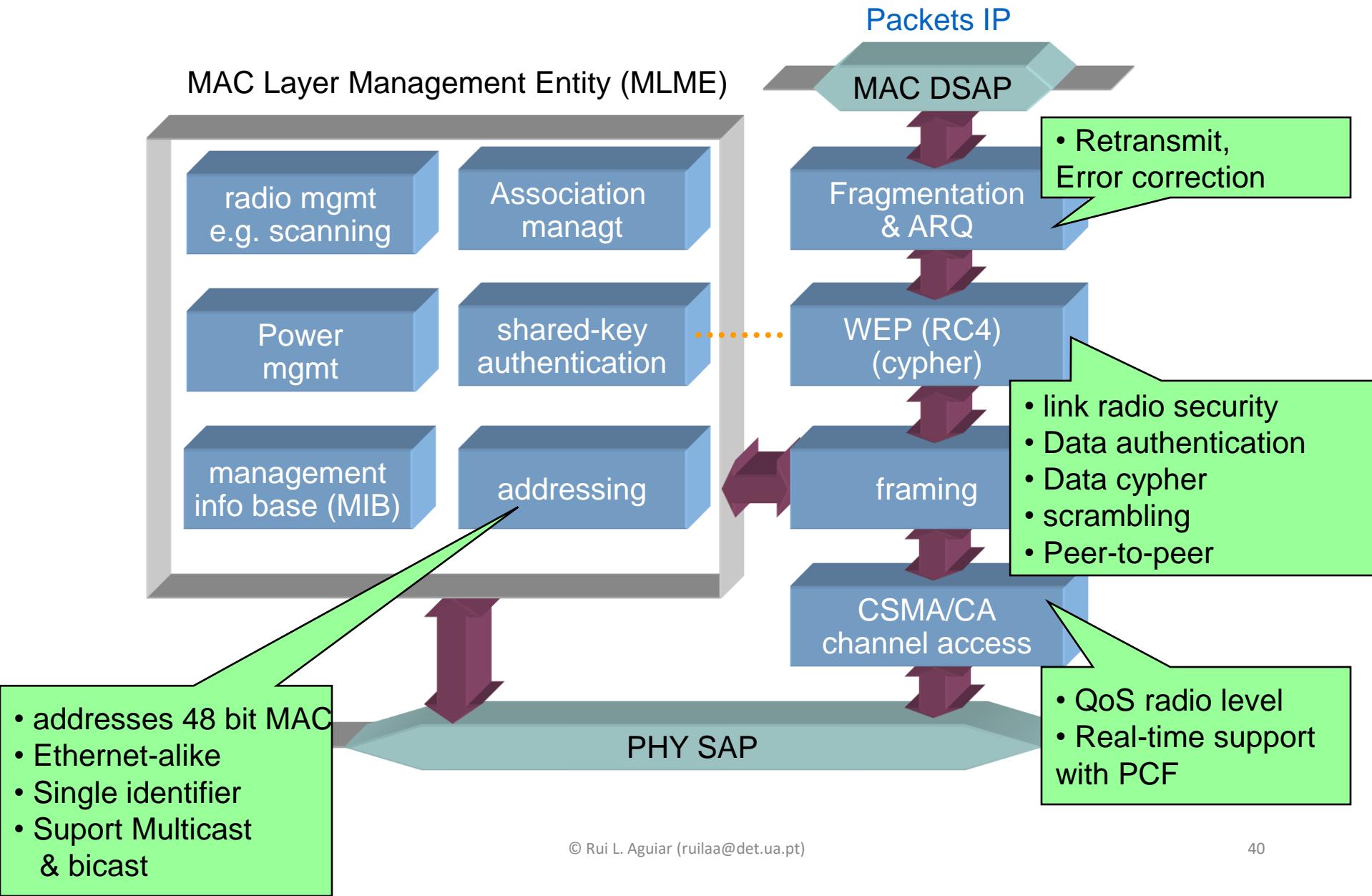


Features of 802.11 MAC protocol

- Fair control access
 - Supports Media Access Control functionalities
 - Addressing
 - CSMA/CA
- Protection of date
 - Error detection (FCS – Frame Check Sequence)
 - Compares number with received values
 - Error correction (ACK frame)
- Reliable data delivery
 - Fragmentation
 - Flow control: stop-and-wait (the next frame is only sent after an ACK from the previous one is received)

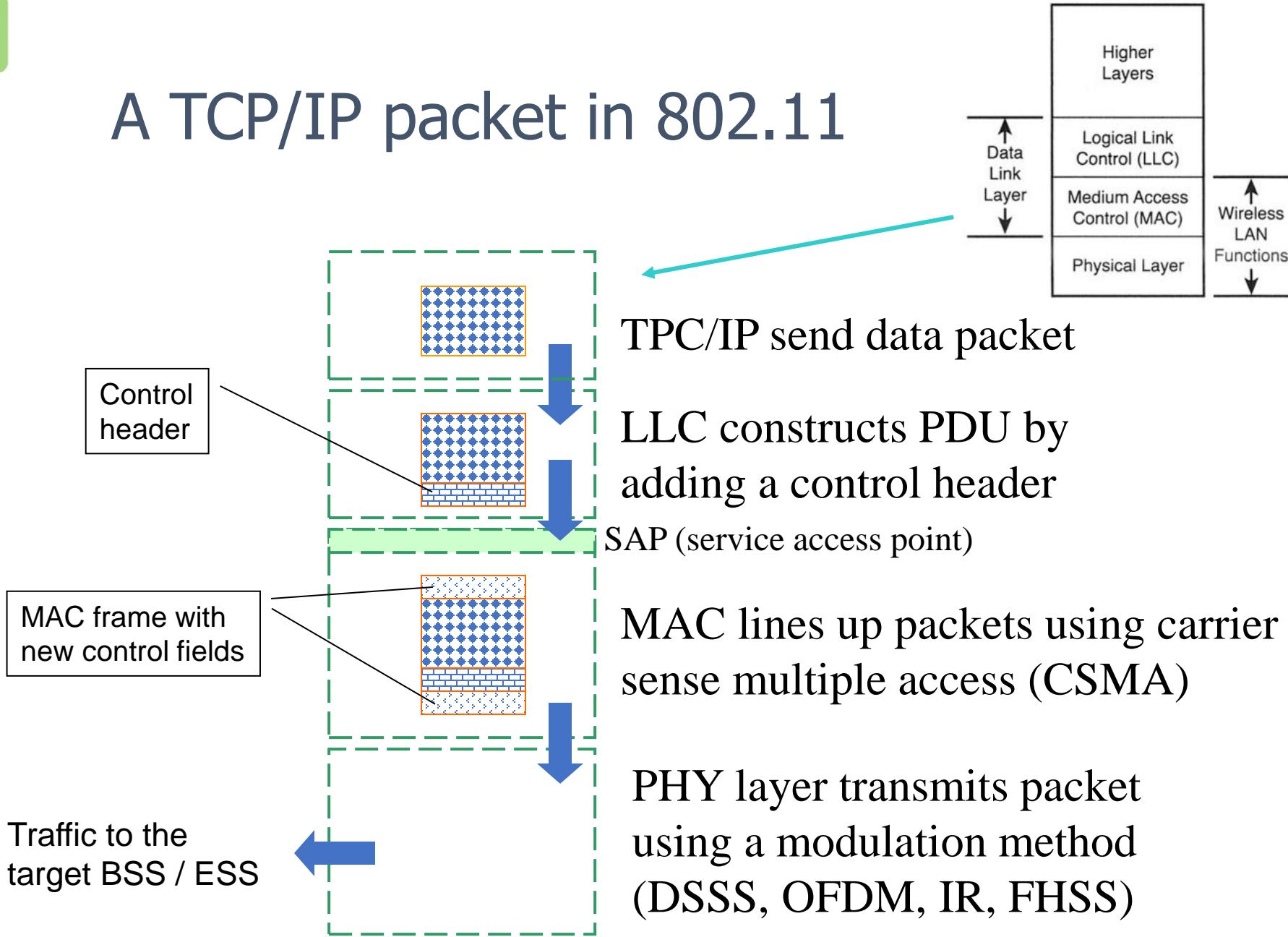


MAC IEEE802.11





A TCP/IP packet in 802.11

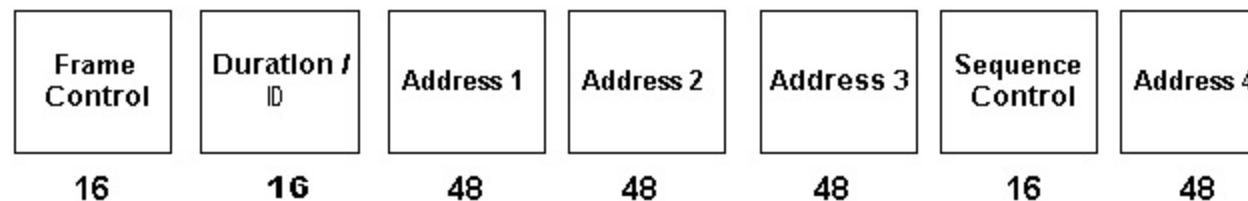


**BDU: protocol data unit*

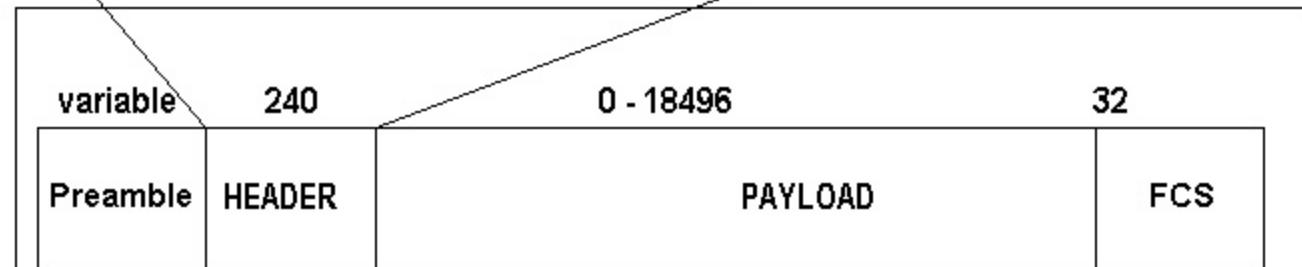


802.11 Frames

- Three types of frames
 - control: RTS, CTS, ACK
 - Management
 - Data
- Header depends on the frame type

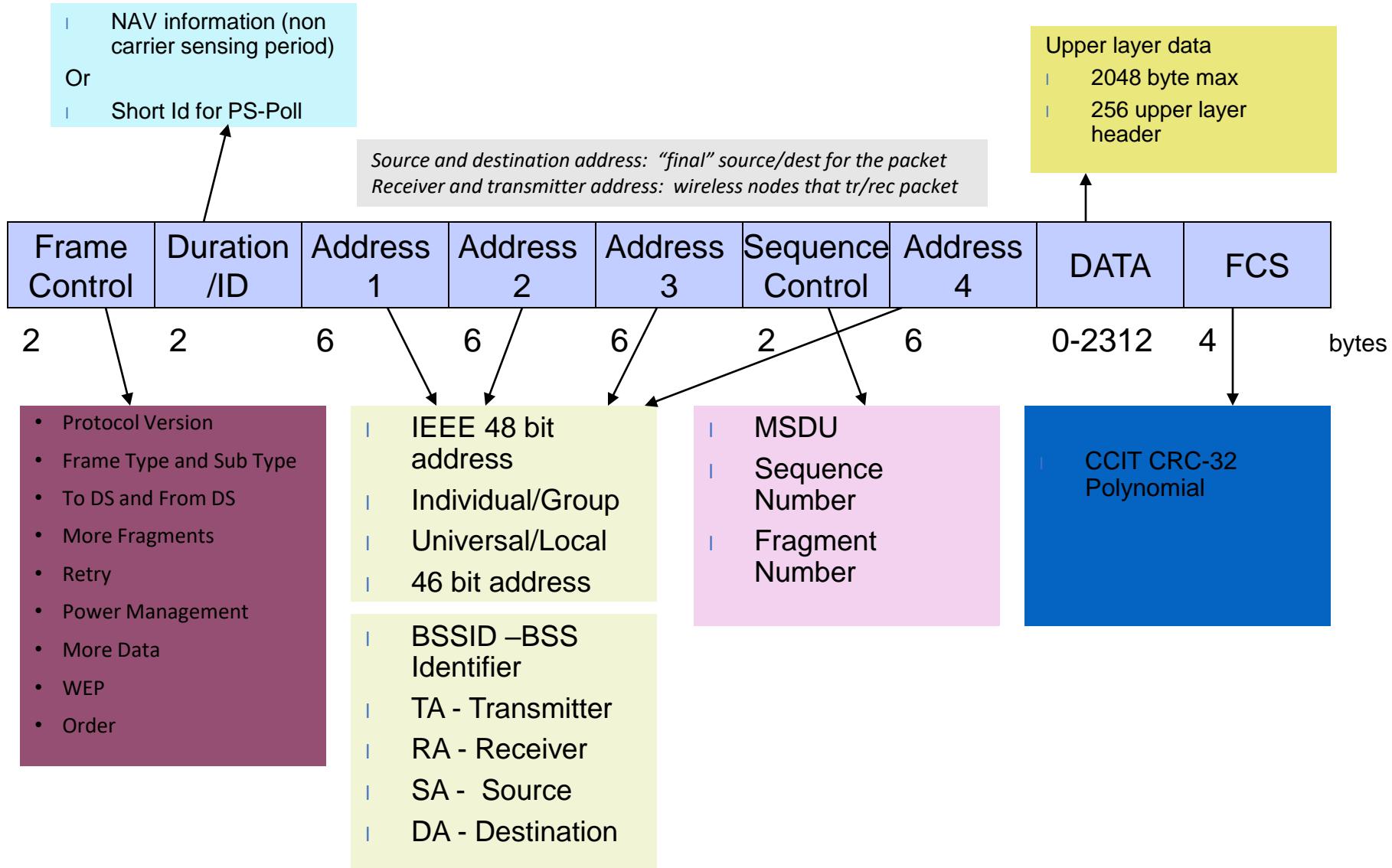


The 240 bit header may be truncated, based on specific frame type





Frame Format





Packet Types

- Type/sub-type field is used to indicate the type of the frame
- Management:
 - Association/Authentication/Beacon
- Control
 - RTS, CTS, CF-end, ACK
- Data
 - Data only, or Data + CF-ACK, or Data + CF-Poll or Data + CF-Poll + CF-ACK

CF → Contention Free



Some More Fields

- Duration/ID: Duration in DCF mode/ID is used in PCF mode
- More Frag: 802.11 supports fragmentation of data
- More Data: In polling mode, station indicates it has more data to send when replying to CF-POLL
- RETRY is 1 if frame is a retransmission;
- WEP (Wired Equivalent Privacy) is 1 if frame is WEP coded
- Power Mgmt is 1 if in Power Save Mode;
- Order = 1 for strictly ordered service



Multi-bit Rate

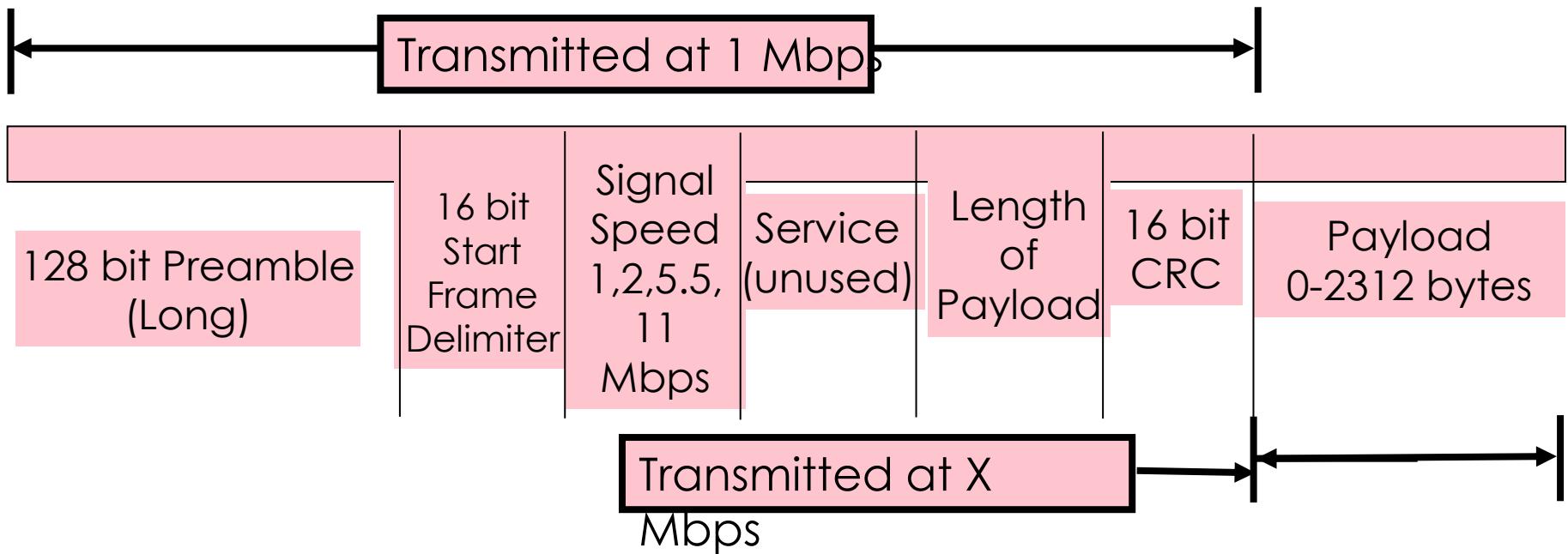
- 802.11 allows for multiple bit rates
 - Allows for adaptation to channel conditions
 - Specific rates dependent on the version
- Algorithm for selecting the rate is not defined by the standard – left to vendors
- Packets have multi-rate format
 - Different parts of the packet are sent at different rates
- Short vs Long preamble
 - Preamble allows the receiver to synchronize with the transmitter
 - Additional data is added to the header to help check for transmission errors
 - Long
 - Older, requires more data to help check for transmission errors (does it better)
 - Short
 - Less data = faster



802.11b: Long Preamble

Long Preamble = 144 bits

- Interoperable with older 802.11 devices
- Entire Preamble and 48 bit PLCP Header sent at *1 Mbps*

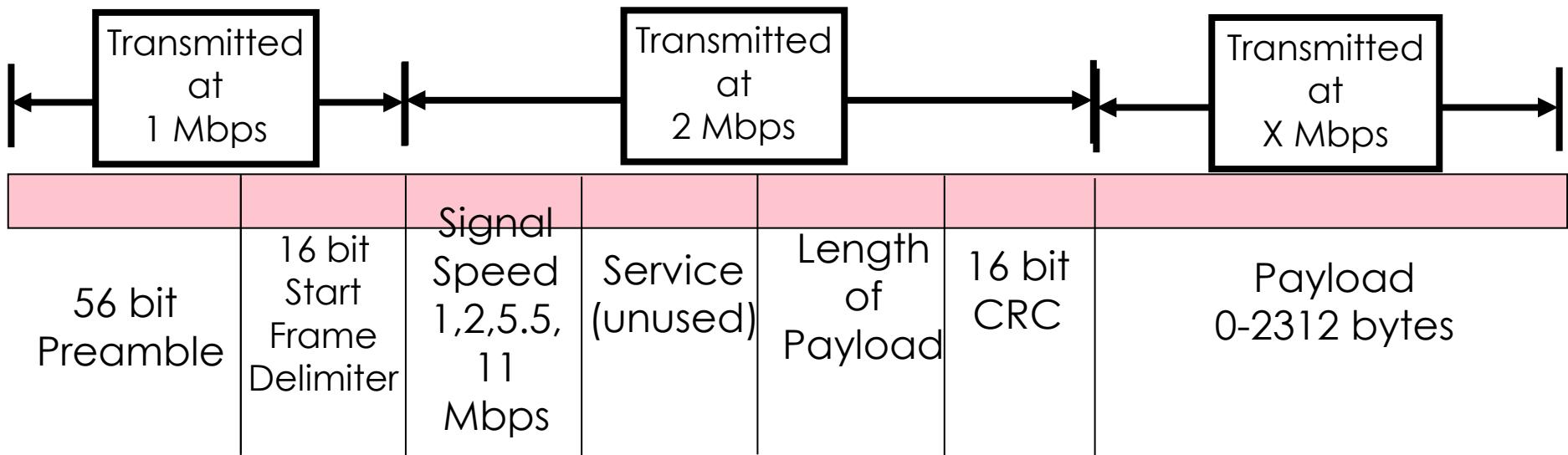




802.11b: Short Preamble

Short Preamble = 72 bits

- Preamble transmitted at 1 Mbps
- PLCP Header transmitted at 2 Mbps
- more efficient than long preamble





Addressing Fields

To DS	From DS	Message	Address 1	Address 2	Address 3	Address 4
0	0	station-to-station frames in an IBSS; all mgmt/control frames	DA	SA	BSSID	N/A
0	1	From AP to station	DA	BSSID	SA	N/A
1	0	From station to AP	BSSID	SA	DA	N/A
1	1	From one AP to another in same DS	RA	TA	DA	SA

RA: Receiver Address

TA: Transmitter Address

DA: Destination Address

SA: Source Address

BSSID: MAC address of AP in an infrastructure BSS

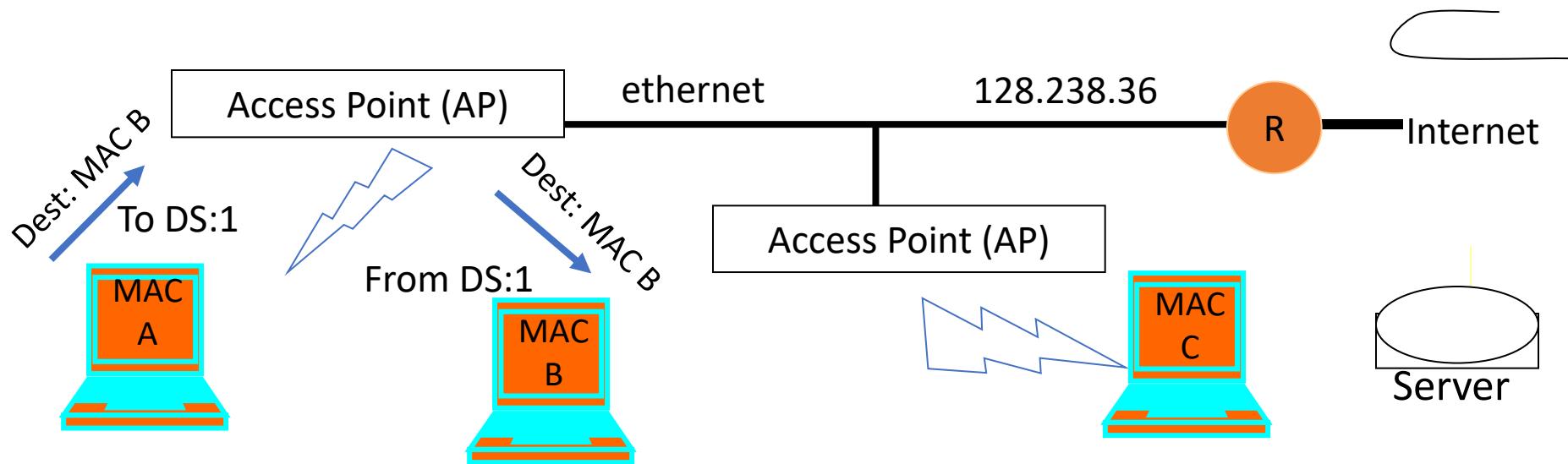


Data Flow Examples

- Case 1: Packet from a station under one AP to another in same AP's coverage area
- Case 2: Packet between stations in an IBSS
- Case 3: Packet from an 802.11 station to a wired server on the Internet
- Case 4: Packet from an Internet server to an 802.11 station



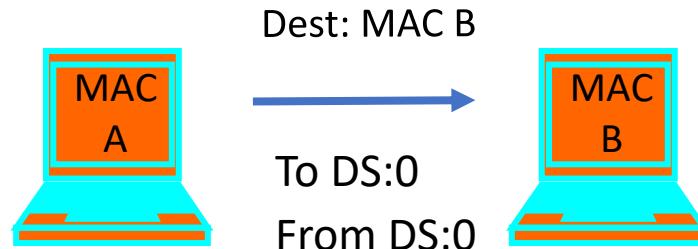
Case 1: Communication Inside BSS



- AP knows which stations are registered with it so it knows when it can send frame directly to the destination



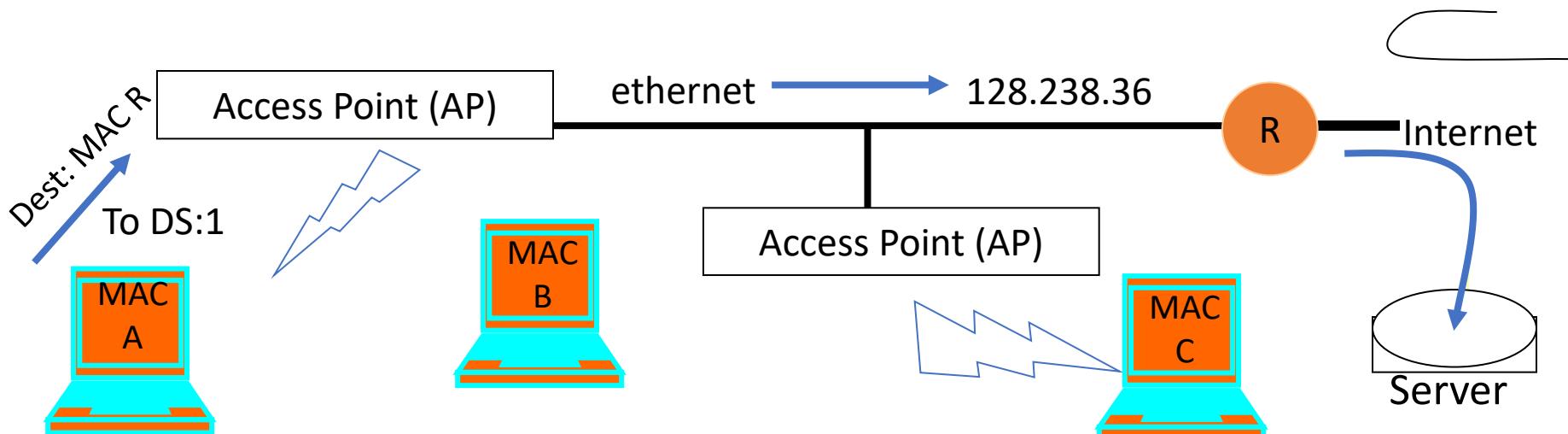
Case 2: Ad Hoc



- Direct transmit only in IBSS (Independent BSS), i.e., without AP
- Note:
 - in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B



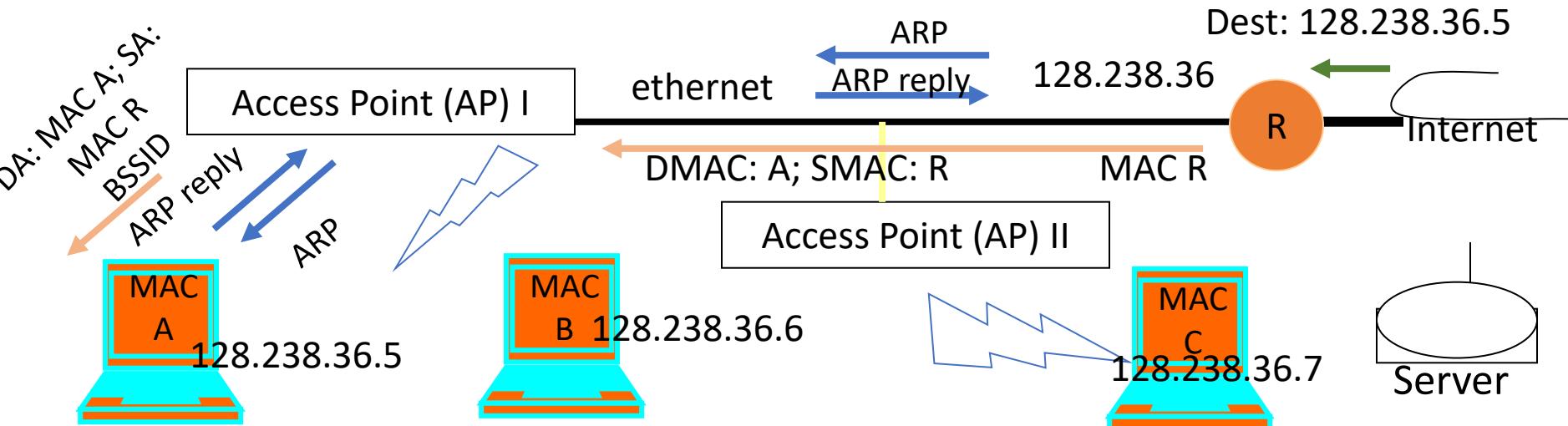
Case 3: To the Internet



- MAC A determines IP address of the server (using DNS)
- From the IP address, it determines that server is in a different subnet
- Hence it sets MAC R as DA;
 - Address 1: BSSID, Address 2: MAC A; Address 3: DA
- AP will look at the DA address and send it on the ethernet
 - AP is an 802.11 to ethernet bridge
- Router R will relay it to server



Case 4: From Internet to Station



- Packet arrives at router R – uses ARP to resolve destination IP address
 - AP knows nothing about IP addresses, so it will simply broadcast ARP on its wireless link
 - DA = all ones – broadcast address on the ARP
- MAC A host replies with its MAC address (ARP reply)
 - AP passes on reply to router
- Router sends data packet, which the AP simply forwards because it knows that MAC A is registered



Outline

- 802.11 standard
- Physical layer
- MAC
 - DCF
 - PCF
- Advanced MAC functions



MAC Layer

- Asynchronous Data Service (DCF)

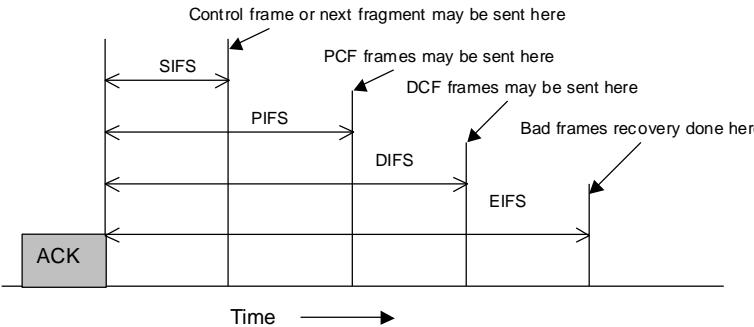
- CSMA/CA
- RTS/CTS

- Timing-controlled service (PCF)

- Polling

- Inter-frame spacing (IFS)

- DIFS (distributed), for the node to start transmitting
- PIFS (point), used by PCF for network access
- SIFS (short), between packets of the same flow



DCF: Distribution Coordination Function

PCF: Point Coordination Function

DIFS: DCF Inter Frame Spacing

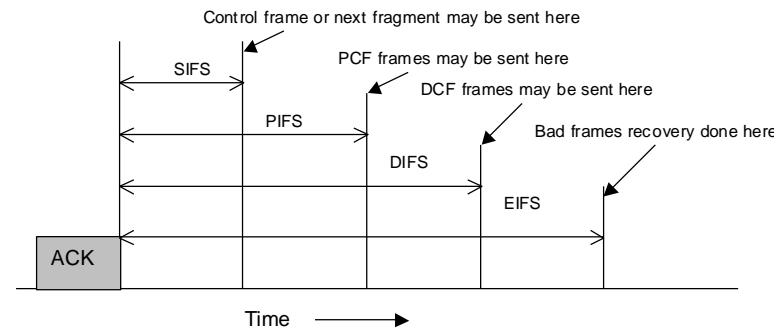
PIFS: PCF Inter Frame Spacing

SIFS: Short Interframe Spacing



Carrier Sense Multiple Access

- Before transmitting a packet, sense carrier
- If it is idle, send
 - After waiting for one DCF inter frame spacing (DIFS)
- If it is busy, then
 - Wait for medium to be idle for a DIFS (DCF IFS) period
 - Go through exponential backoff, then send
 - Want to avoid that several stations waiting to transmit automatically collide
- Wait for ACK
 - If there is one, you are done
 - If there isn't one, assume there was a collision, retransmit using exponential backoff



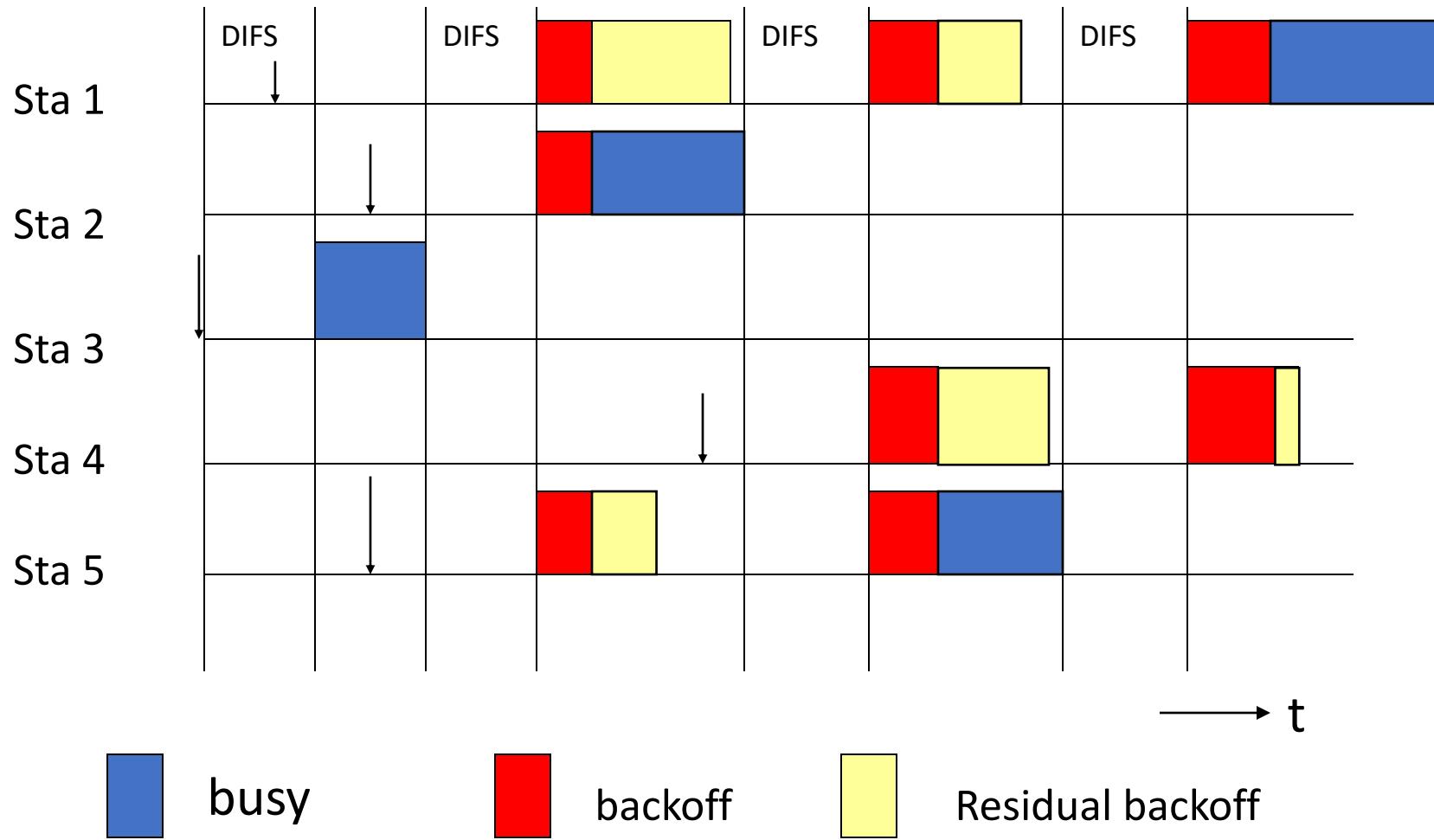


Exponential Backoff

- Force stations to wait for random amount of time to reduce the chance of collision
 - Backoff period increases exponential after each collision
 - Similar to Ethernet
- If the medium is sensed busy:
 - Wait for medium to be idle for a DIFS (DCF IFS) period
 - Pick random number in contention window (CW) = backoff counter
 - Decrement backoff timer until it reaches 0
 - But freeze counter whenever medium becomes busy
 - When counter reaches 0, transmit frame
 - If two stations have their timers reach 0; collision will occur;
- After every failed retransmission attempt:
 - increase the contention window exponentially
 - $2^i - 1$ starting with CW_{min} up to CW_{max} e.g., 7, 15, 31, ...



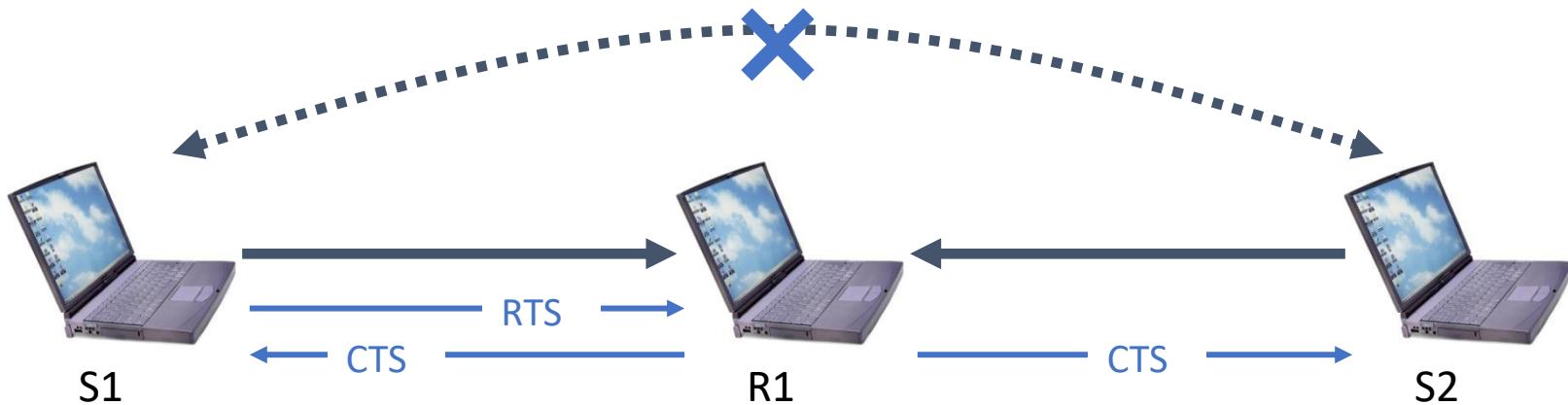
CSMA/CA





Collision Avoidance

- Difficult to detect collisions in a radio environment
 - While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong
- Why do collisions happen?
 - Near simultaneous transmissions
 - Period of vulnerability: propagation delay
 - Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver





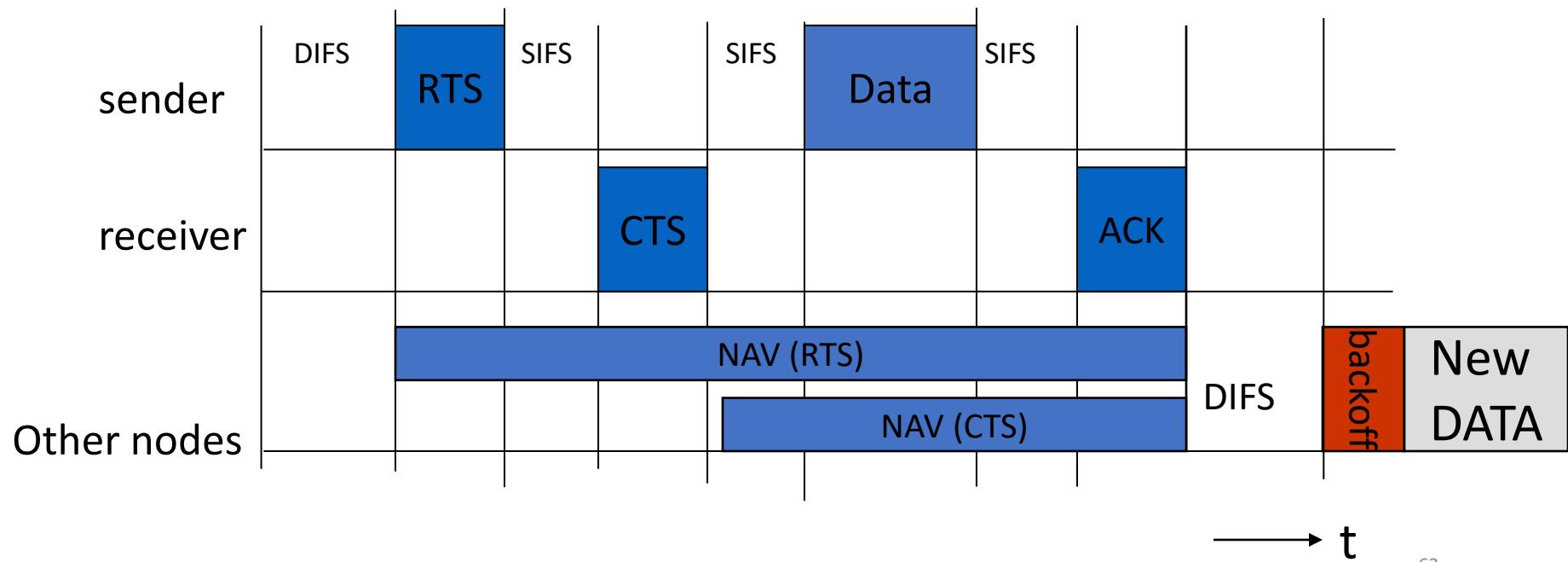
Request-to-Send and Clear-to-Send

- Before sending a packet, a station first sends a RTS.
- The receiving station responds with a CTS.
 - RTS and CTS are smaller than data packets
 - RTS and CTS use shorter IFS to guarantee access
- Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission
 - Based on a Duration ID in the RTS and CTS
- Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)
 - Time that must elapse before a station can sample channel for idle status



RTS/CTS: NAV

- NAV: Network Allocation Vector
- NAV acts as a distributed (in each node) resource allocation register
- RTS/CTS
 - Not a “major” concern





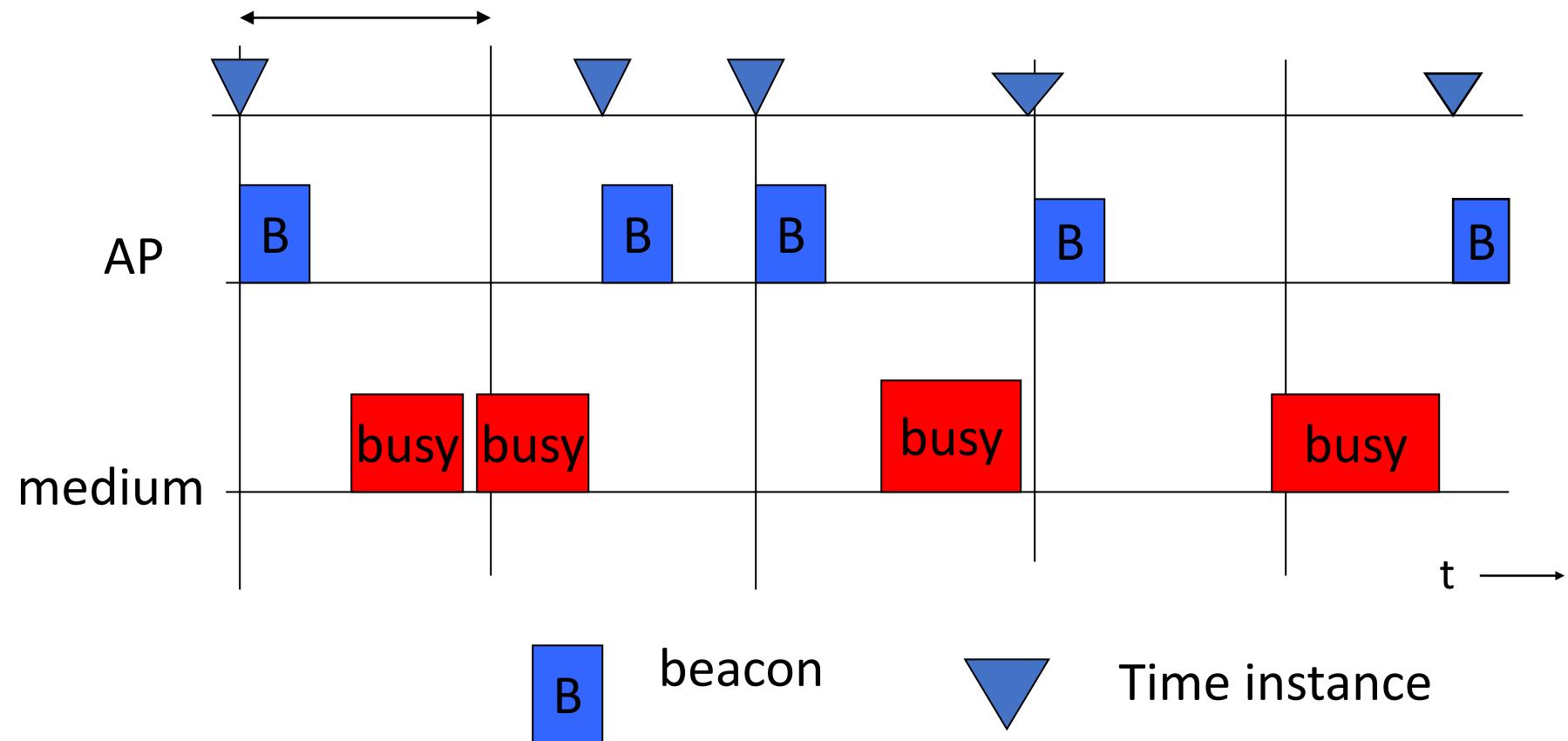
Synchronization

- Timing synchronization function (TSF)
 - Beacons of the AP are sent in well-defined instants.
 - Content of packet is the exact instant when it goes to the network.
- Used also for power management
 - All clocks of all stations ins the BSS are synchronized
 - This allows STA to wake-up to check if packets exist.



Synchronization

Delay between beacons





Outline

- 802.11 standard
- Physical layer
- MAC
 - DCF
 - PCF
- Advanced MAC functions

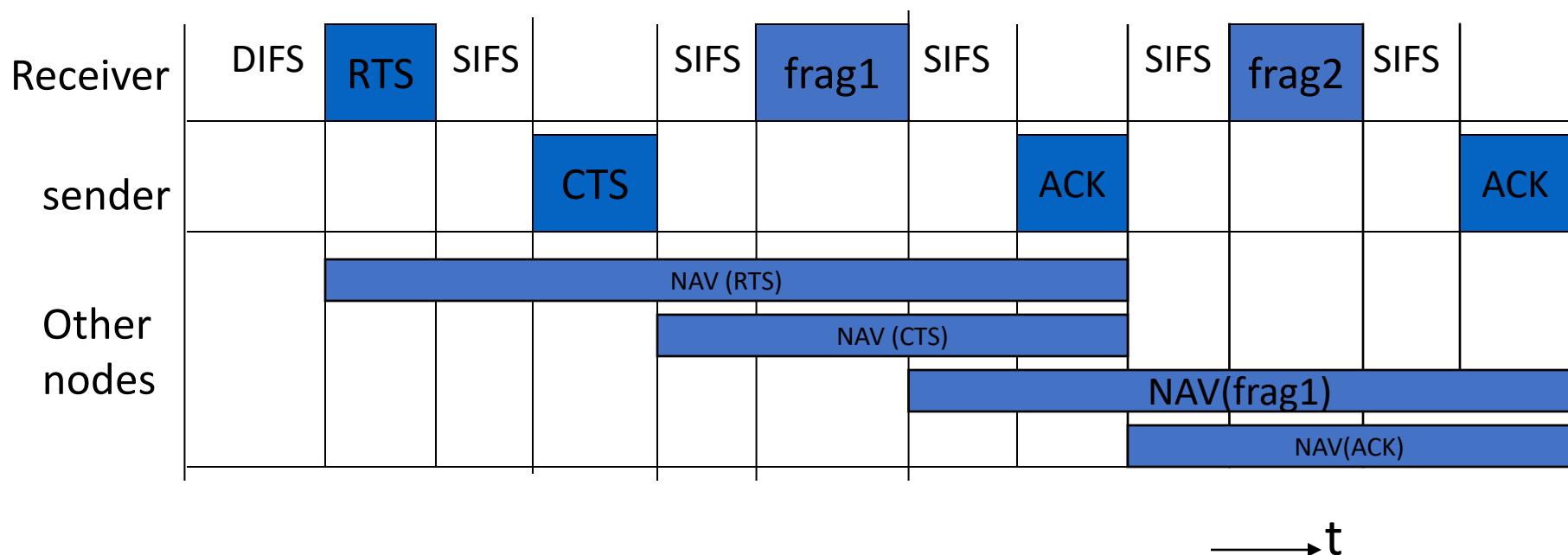


Some More MAC Features

- Use of RTS/CTS is controlled by an RTS threshold
 - RTS/CTS is only used for data packets longer than the RTS threshold
 - Pointless to use RTS/CTS for short data packets – high overhead!
- Number of retries is limited by a Retry Counter
 - Short retry counter: for packets shorter than RTS threshold
 - Long retry counter: for packets longer than RTS threshold
- Packets can be fragmented.
 - Each fragment is acknowledged
 - But all fragments are sent in one sequence
 - Sending shorter frames can reduce impact of bit errors
 - Lifetime timer: maximum time for all fragments of frame



Fragmentation



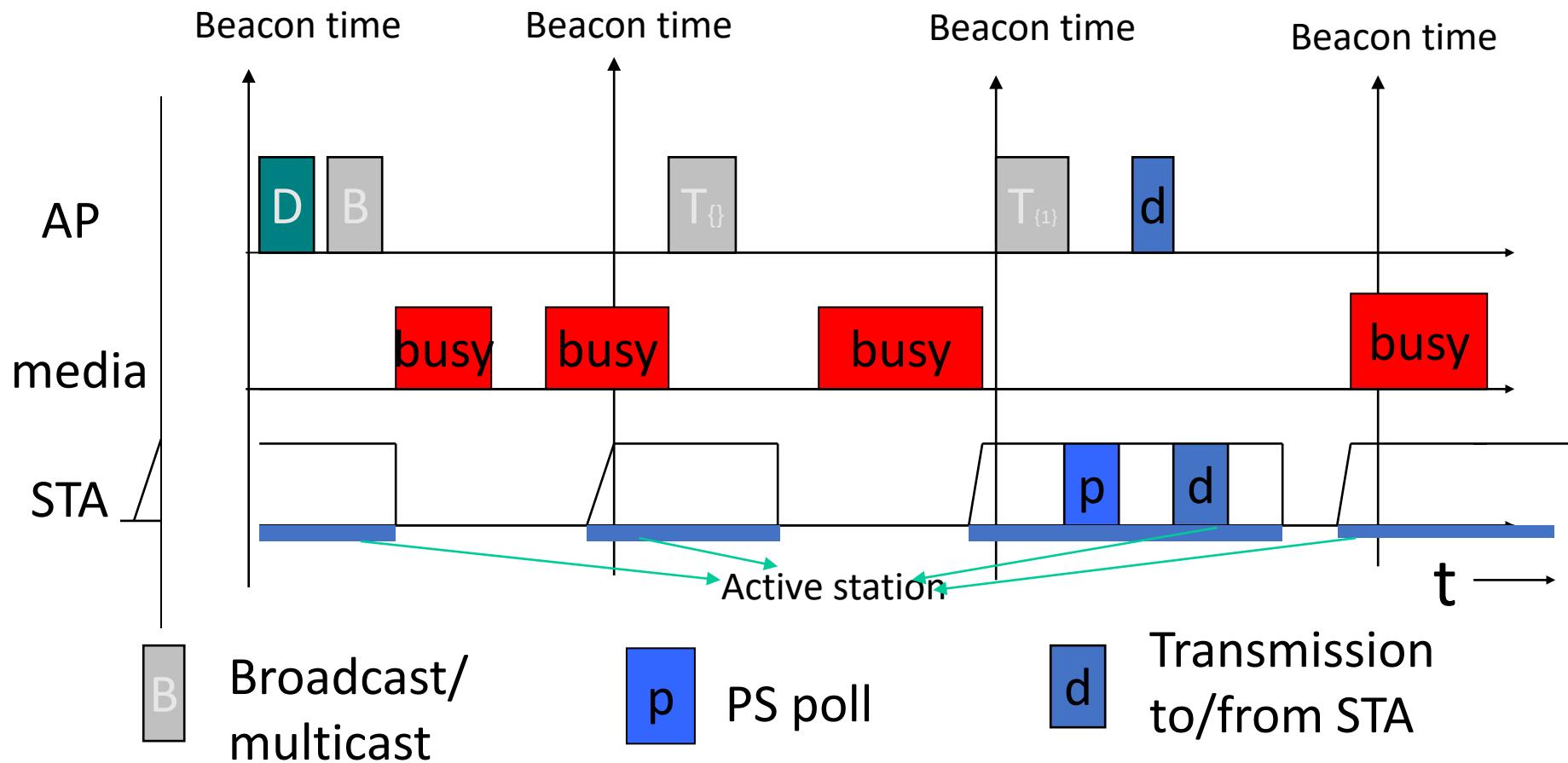


Power management (infrastructure)

- APs buffer packets to stations in power saving mode
 - APs announce in beacons which packets are waiting with the TIM (traffic indication Map)
 - Broadcast/multicast frames are also buffered at AP
 - Sent after beacons, same common timing period.
 - Uses Delivery Traffic Indication Map (DTIM)
 - AP controls DTIM interval
- STA in power save wake periodically to listen for beacons
 - If it has data pending, send a PS-Poll
 - AP sends buffered data to this PS-poll
- TSF (Timing Synchronization Function) assures AP and stations are synchronized
 - Synchronizes clocks of the nodes in the BSS



Power management





How does a station connect to an Access Point?



Control services at MAC

- Synchronization, Roaming and Association
 - Functions to find a network
 - Change APs
 - Search APs.
- Power Management
 - sleep mode without losing packets
 - Power management functions
- MIB: Management information base
- Security: authentication and cypher



SSID

- Mechanism used to segment wireless networks
 - Multiple independent wireless networks can coexist in the same location
- Each AP is programmed with a SSID that corresponds to its network
- Client computer presents correct SSID to access AP
- Security Compromises
 - AP can be configured to “broadcast” its SSID
 - Broadcasting can be disabled to improve security
 - SSID may be shared among users of the wireless segment



Association Management: Scanning

- Scanning is needed to:
 - Find and connect to a networks
 - Find a new AP during roaming
- Passive Scanning:
 - Station simply listens for Beacon and get info of the BSS. Power is saved.
- Active Scanning:
 - Station transmits Probe Request; elicits Probe Response from AP. Saves time.



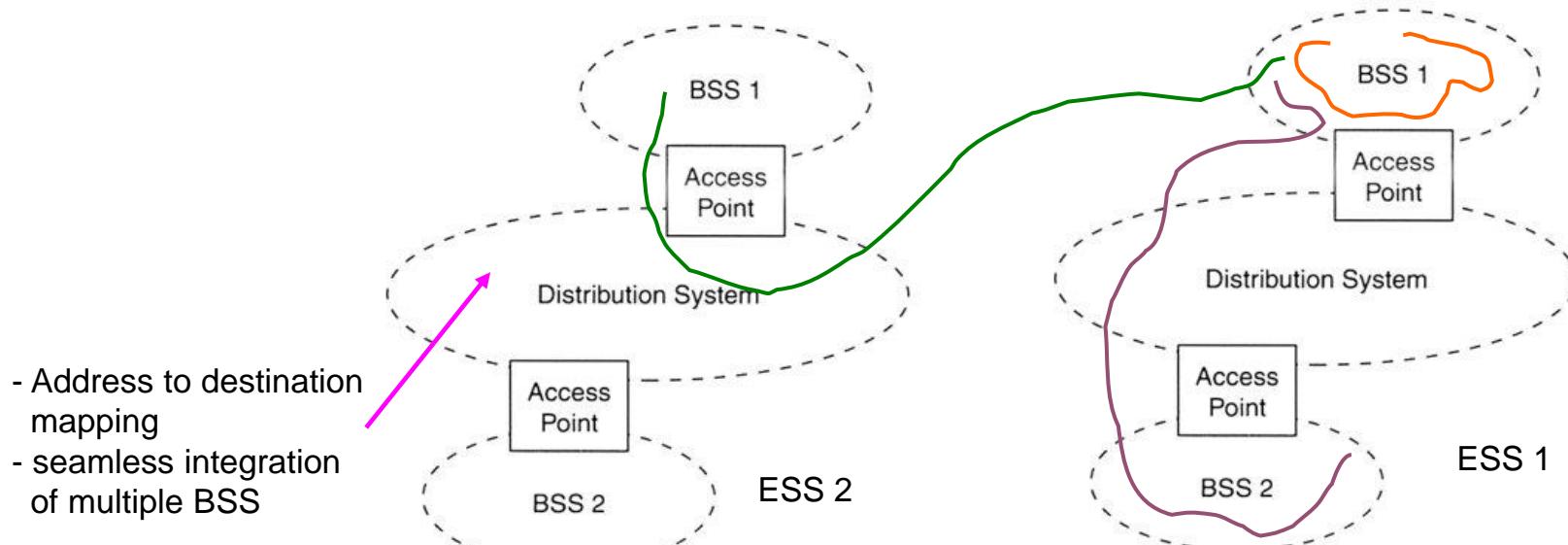
Association Management: Scanning, and Joining

- Station must associate with an AP before they can use the network
 - AP must know about them so it can forward packets
- Re-association (roaming): association is transferred
 - Supports mobility in the same ESS
- Disassociation: station or AP can terminate association
- Stations can detect AP based on scanning
- Joining a BSS
 - Synchronization in Timestamp Field and frequency (i.e., channel) :
 - Adopt PHY parameters
 - Other parameters: BSSID, WEP, Beacon Period, etc.



IEEE 802.11 Mobility

- Standard defines the following mobility types:
 - No-transition: no movement or moving within a local BSS
 - BSS-transition: station moves from one BSS in one ESS to another BSS within the same ESS
 - ESS-transition: station moves from a BSS in one ESS to a BSS in a different ESS (continuous roaming not supported)





Roaming

- Roaming: station changes network (BSS)
- STA may go:
 - Outside the coverage area of their AP
 - But still under the coverage area of another AP
- Reassociate the STA with the new AP allows the communication to continue



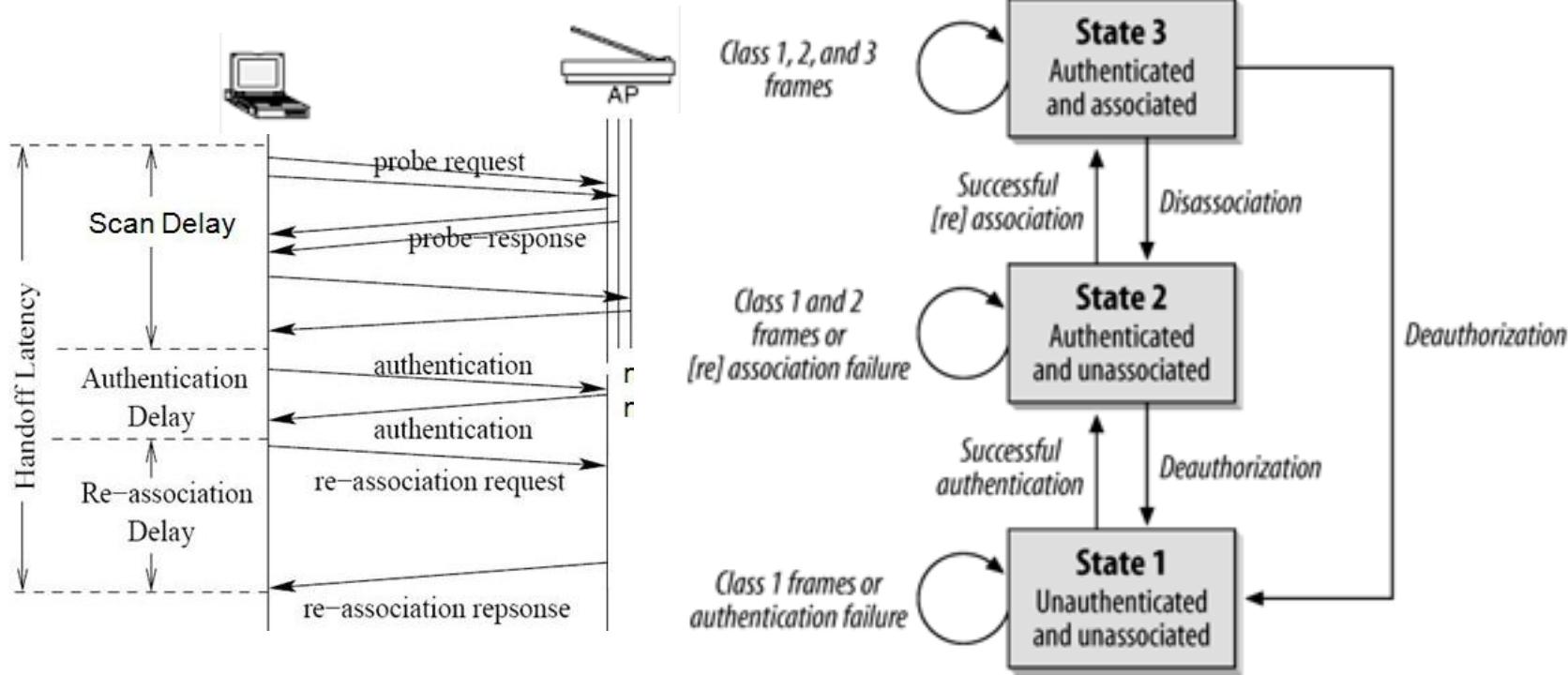
Roaming

- STA decides that the signal with the current AP is bad.
- STA does scanning (act/pas) to find new AP
- STA reassociates with the New AP (NAP)
 - Includes authorization.
- Without positive answer
 - STA does new scan
- With positive answer:
 - STA changed network to the new NAP
 - AP informs the ESS of the new association
 - Information in the distributed system is always updated.



Attachment to a BSS

- The STA finds a BSS/AP through **Scanning/Probing**
- Both **Authentication** as well as **Association** are necessary to enter a BSS





Phase 1: Scanning

- The STA searches for APs
 - **Passive Scanning**
 - STA analyzes channels looking for **Beacon** packets, which are periodically sent by the AP, announcing its presence and SSID
 - **Active Scanning**
 - STA sends **Probe Request** packets to all channels in sequence
 - AP's listening in these different channels respond with a **Probe Response**



Phase 2: Authentication

- After finding and selecting an AP, the STA has to authenticate with it.
Two main methods:
- **Method 1: Open System Authentication**
 - Default procedure, executed in 2 steps:
 - 1 - STA sends an authentication frame including its identity
 - 2 - AP responds with a frame as a Ack/NAck
- **Method 2: Shared Key Authentication**
 - STA and AP have a shared secret, obtained in some other way
 - 1 – STA sends an initial authentication request
 - 2 – AP replies to the STA with a challenge
 - 3 – STA deciphers the challenge with its own key and sends it to the AP
 - 4 – AP uses its own key to decipher the challenge and compares results



Phase 3: Association

- After authenticated, the STA begins the **association** process, i.e., Exchange roaming and capacity information between STA and AP
- Procedure:
 - 1 – STA sends a **Associate Request** to AP, indicating supported transmission rates and intended association SSID
 - 2 – AP allocates resources and decides if it accepts or rejects the STA
 - 3 – AP sends an **Association Response**, indicating the association identifying and supported transmission rates, in case the association is accepted
 - 4 (optional) – In case of a handover (transition of the STA between two different APs), the new AP informs the old AP
- Only after associating to the AP, can the STA start to send and receive data



MESH (TODO)



How to extend range in Wi-Fi?



Wi-Fi “extenders”.

- Inexpensive
- They set up a new SSID, and forward all traffic to the original SSID
- Multi-hop configurations are possible
 - Require manual configuration
- Because the original access point and the extender have different SSIDs
 - Many devices will not automatically connect to whichever is closer
 - They prefer to maintain connection with the original SSID until that signal disappears
 - This is, for many mobile users, reason enough to give up on this strategy.



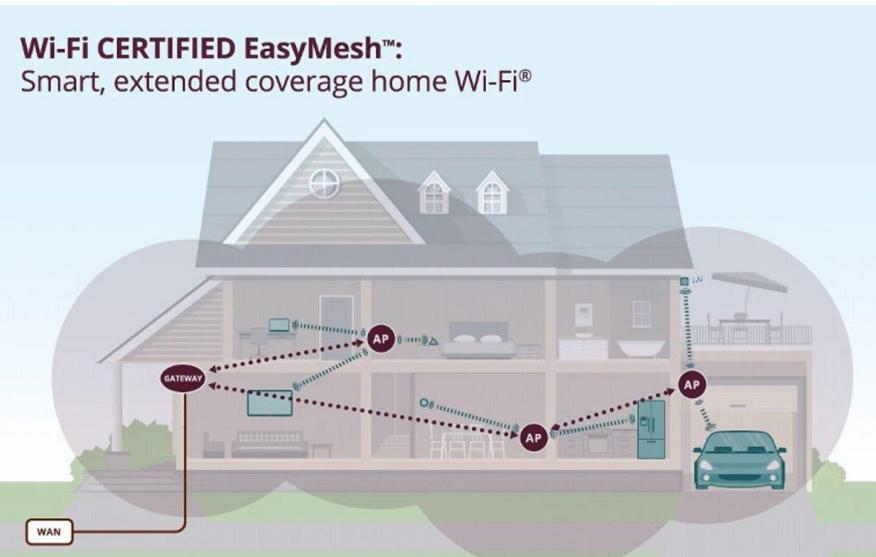
Mesh

- Different standards
 - IEEE 802.11s standard
 - Focuses on the setup of the mesh networks
 - Uses a mandatory routing protocol – Hybrid Wireless Mesh Protocol
 - Mesh Stations can collocate 802.11 AP's and provide access to the mesh network for 802.11 devices
 - A Mesh Gateway interconnects the mesh to other non-802 networks
 - Wi-Fi Alliance standard (a.k.a., "EasyMesh")
 - Focuses on more "easy" setup of mesh WiFi networks
 - incorporates parts of the [IEEE 1905.1](#) standard for home networks, which simplifies initial configuration.
 - Specifies that one access point – the one connected to the Internet – will be a "Multi-AP" Controller
 - the other access points are called Agents.
 - The EasyMesh standard also



Wi-Fi EasyMesh

- WiFi Alliance Certification program that defines multiple access point home and small office Wi-Fi networks that are easy to install and use, self-adapting, and add multi-vendor interoperability.
- This technology brings both consumers and service providers additional flexibility in choosing Wi-Fi EasyMesh devices for home deployment.
- Wi-Fi EasyMesh uses a controller to manage the network, which consists of the controller, plus additional APs, called agents.
- Establishing controllers to manage and coordinate activity among the agents ensures that each AP does not interfere with the other, bringing both expanded, uniform coverage and more efficient service.





EasyMesh specification relies on other standards / specification, either by extending them or simply referencing them.

This includes, most notably:

- Building on and extending IEEE Standard 1905.1 to configure Wi-Fi access point interfaces
 - **Discovery**: how nodes are finding each other and identifying the controller
 - **Push-Button Configuration**: to initialize "onboarding" of access points-the process commonly referred to as "meshing"
 - **Backhaul communication**: Communication between the nodes / access points in the mesh network

[IEEE 1905.1 standard, Convergent Digital Home Network for Heterogeneous Technologies.](#)



IEEE 1905.1 standard, Convergent Digital Home Network for Heterogeneous Technologies.

- This technology enables networked devices connected by different network media--say Gigabit Ethernet 2.4Ghz, and 5Ghz Wi-Fi, to operate as if they were connected across a single network. In EasyMesh, the controllers use data from it to configure each agent's AP radios. It also includes mechanisms to configure control-related policies on agents, such as metrics and steering. Additionally, the controller determines the topology of the network of agents, so it can adapt to changing network conditions.
- also utilize mechanisms from the new Wi-Fi Alliance Agile Multiband standard. New Agile Multiband certified devices will work better as they're moved from spot to spot with intelligent steering and faster network transitions.

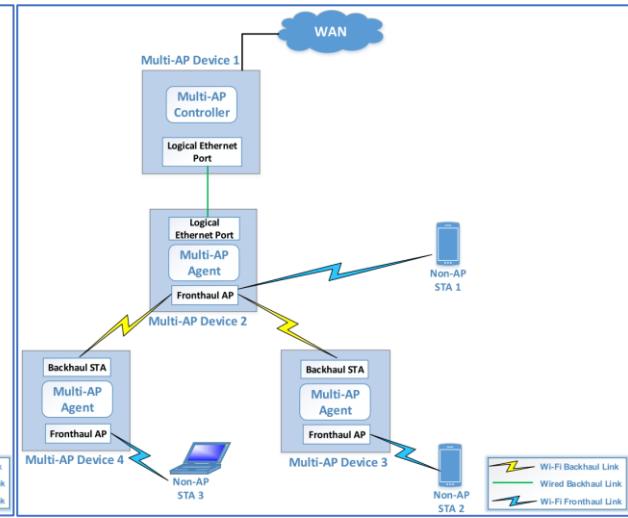
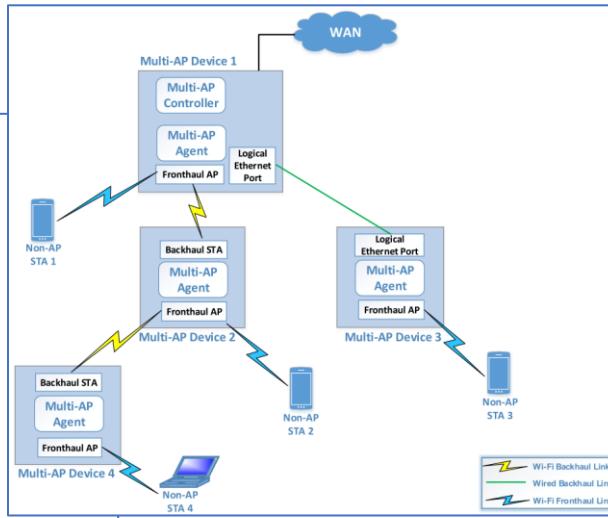
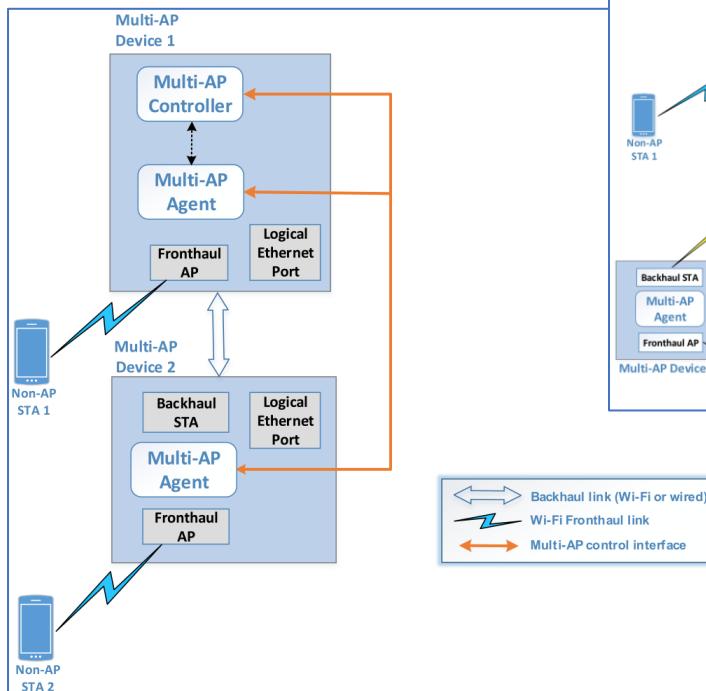


Architecture and components

- **Controller** - every EasyMesh network must have one. The controller can be a unique device or embedded in a device that also has other functionality
- **Agent** - in order for a mesh network to exist, at least two agents must be connected to the controller
- **Device** - any component of a mesh network, whether it contains a controller, an agent, or both



Example deployments



Wi-Fi EasyMesh™ Specification v4.0
Wi-Fi Alliance



- the specification does *not* standardize algorithms or decision-making
- How to do client steering makes up a significant part of the specification, telling manufacturers how to direct a client from one access point to another.
- When a client should be steered is not covered. Therefore, algorithms will still vary (and client roaming mechanisms may of course still interfere).



NETWORK OPERATION MECHANISMS

VELUP
WHOLE HOME WI-FI

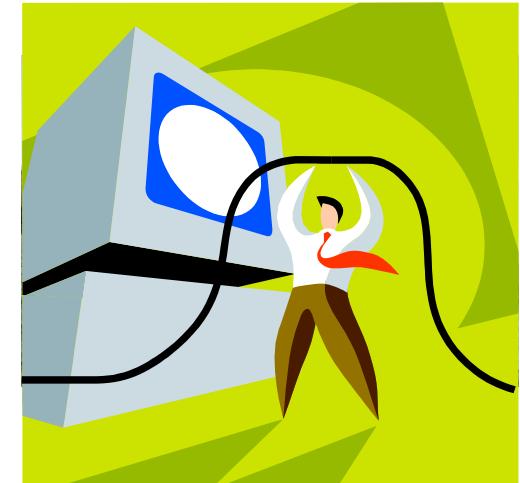
Network operation mechanisms are needed to create and maintain a self-optimizing network that maximizes performance and improves client roaming

- **Capability reporting** - The master node uses the information sent by other nodes to maintain optimal network performance. Based on network conditions reported by the nodes in the network, the master node could send control commands to one or more nodes to move to a different channel, decrease transmit power, or report bandwidth utilization
 - **Channel selection** - The Wi-Fi EasyMesh controller obtains preferred operating channels for the nodes and sets the operating configuration(such as channels, transmit power, etc.) including preferences and restrictions for each radio in the nodes
 - **Link metric collection** - Defines the protocol for network devices to convey link metric information associated with the network
 - **Client steering** - Master Node may choose to send control messages to "steer", or suggest, a client move its connection from one node to another
-  **Optimizing connection between agents** - Manage the connections between nodes by selecting the best path (wired, wireless, or mixed) between nodes to optimize the network



Mobile Networks

Connections and structures





Bluetooth

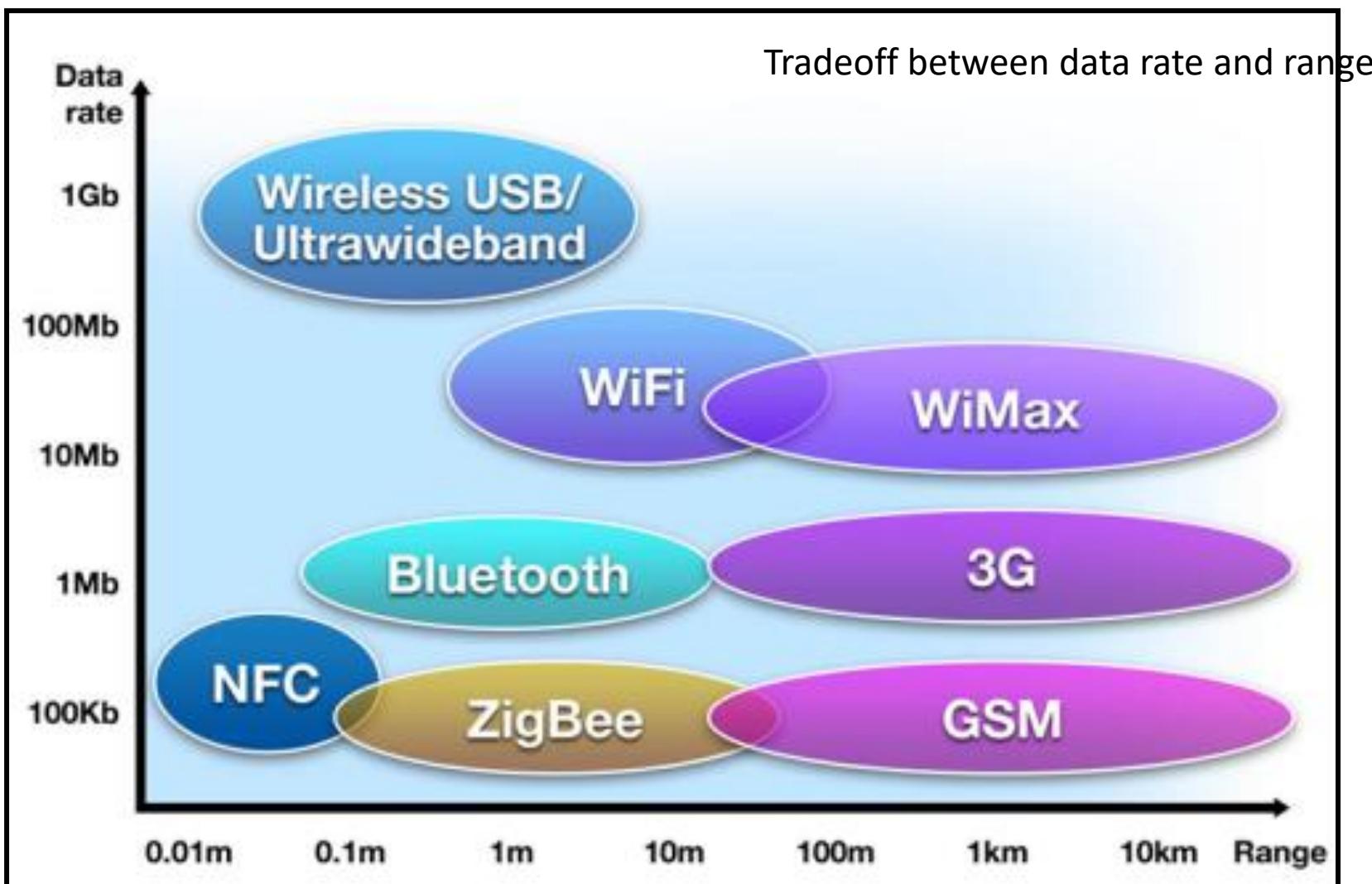
WPAN



Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE

Comparison Between Wireless Technologies





Personal networks: when?

- Access mostly to “transported devices”
- No dominant need for Information Technologies
- No physical access to cabled networks
- No need for large communication rates
- Very low cost system required
- Consumer electronics integration is mandatory



Personal Area Networks

- Target deployment environment: communication of personal devices working together
 - Short-range
 - Low Power
 - Low Cost
 - Small numbers of devices
 - Sometimes have more “bus-like” characteristics
- PAN Standards
 - Bluetooth – Industry consortia
 - IEEE 802.15.1 – “Bluetooth” based
 - IEEE 802.15.2 – Interoperability and coexistence
 - IEEE 802.15.3 – High data rate WPAN (UWB)
 - IEEE 802.15.4 – Low data rate WPAN (Zigbee,...)
 - IEEE 802.15.5 – Mesh Networks
 - IEEE 802.15.6 – Body Area Network



Bluetooth

- Originally for replacing “USB”, not “Ethernet”
 - Cable replacement technology
 - Later also used as Internet connection, phone, or headset
- Created by Ericsson
- PAN - Personal Area Network
 - Up to 1 Mbps connections
 - Includes synchronous, asynchronous, voice connections
 - Piconet routing
- Small, low-power, short-range, cheap, versatile radios
- Master/slave configuration and scheduling



History

1998 - Bluetooth technology is officially introduced and the BLUETOOTH SIG is formed. 1999 - Bluetooth 1.0 Specification is introduced.

2003 - The BLUETOOTH SIG overhauls the Bluetooth Core Specification with the announcement of Version 2.1.

2004 - Bluetooth Version 2.0 + EDR (Enhanced Data Rate) is introduced.

2005 - Devices using Version 2.0 + EDR begin to hit the market in late 2005.

2007 - Bluetooth Core Specification Version 2.1 + EDR is adopted by the BLUETOOTH SIG.

2009 - Bluetooth Core Specification Version 3.0 + HS (High Speed) is adopted by the BLUETOOTH SIG.

2010 - Bluetooth Core Specification Version 4.0 is adopted by the BLUETOOTH SIG.

2013 – Bluetooth 4.1

2014 – Bluetooth 4.2

2016 – Bluetooth 5

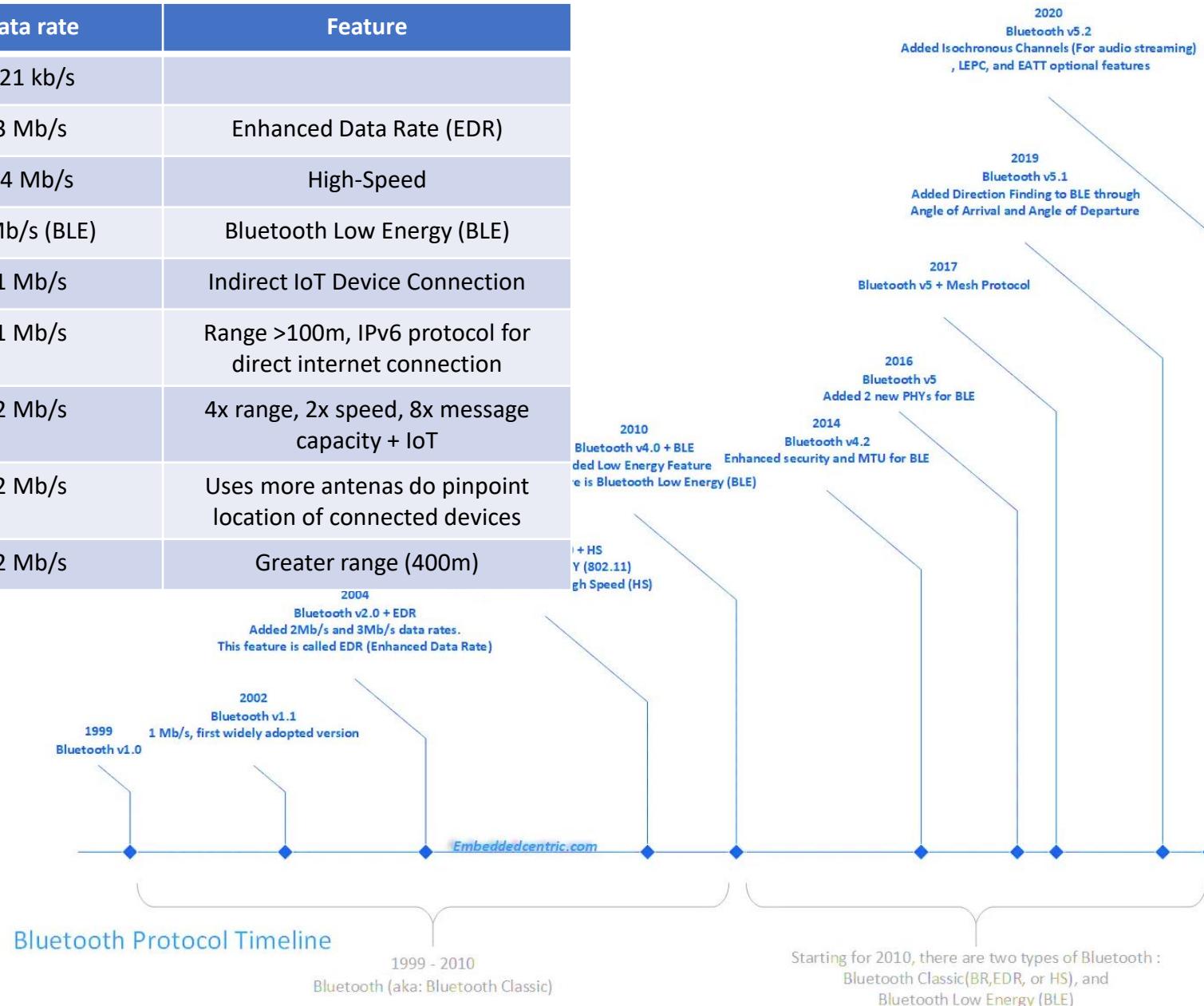
2019 – Bluetooth 5.1, 5.2

2021 – Bluetooth 5.3



Bluetooth Versions

Version	Data rate	Feature
1.2	721 kb/s	
2.0 + EDR	3 Mb/s	Enhanced Data Rate (EDR)
3.0 + HS	24 Mb/s	High-Speed
4.0	1 Mb/s (BLE)	Bluetooth Low Energy (BLE)
4.1	1 Mb/s	Indirect IoT Device Connection
4.2	1 Mb/s	Range >100m, IPv6 protocol for direct internet connection
5.0	2 Mb/s	4x range, 2x speed, 8x message capacity + IoT
5.1	2 Mb/s	Uses more antennas do pinpoint location of connected devices
5.2	2 Mb/s	Greater range (400m)





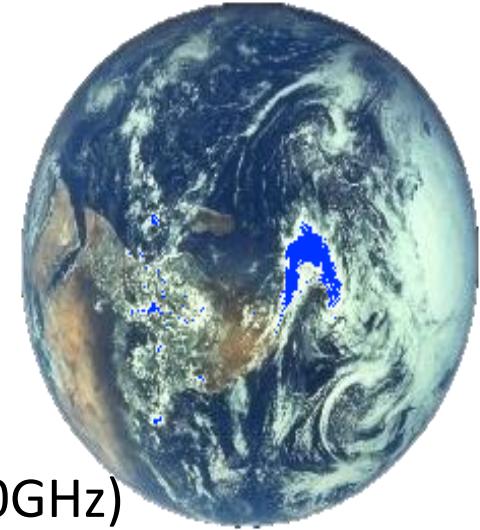
Bluetooth higher speeds (in BT classic)

- Enhanced Data Rate (EDR)
 - Introduced in Bluetooth v2.0 to support faster data transfer
 - Supports a data rate up to **3 Mbps**
 - Using reduced duty cycle control (time radio is ON), EDR can provide lower power consumption
- High Speed (HS)
 - BT HS released in April 2009 (in Bluetooth version 3.0+HS)
 - Bluetooth 3.0+HS provides data transfer speeds of up to **24 Mbps**, though not over the Bluetooth link itself:
 - BT link is used for negotiation and establishment, and the high data rate traffic is carried over a collocated 802.11 link
 - HS part of the specification is not mandatory in BT 3.0
 - Only devices that display the "+HS" logo actually support Bluetooth over 802.11 high-speed data transfer



Bluetooth features

- Radio network, on the 2.4 GHz, **world-wide!**
- Airplane friendly!
- FH (Frequency Hopping) spread spectrum:
79 (**23 - .jp .es .fr**) channels (de 2.402GHz - 2.480GHz)
(We'll see how this works in the next slide!)
- Defines a master that synchronizes everyone to his hop-pattern.
- Defines two types of networks:
 - **piconets**
 - **scatternets**
- Maximum 8 devices per piconet (1 master + 7 slaves)
- Transmission rate: 720 Kb/s (max), assymetrical variable





Frequency Hopping Spread Spectrum (FHSS)

- Signal broadcast over seemingly random series of frequencies
- Receiver hops between frequencies in sync with transmitter
 - Each frequency has the bandwidth of the original signal
 - Dwell time is the time spent using one frequency
- Spreading code determines the hopping sequence
 - Must be shared by sender and receiver (e.g. standardized)
- Eavesdroppers hear unintelligible blips
- Jamming on one frequency affects only a few bits
 - Typically large number of frequencies used
 - Improved resistance to jamming



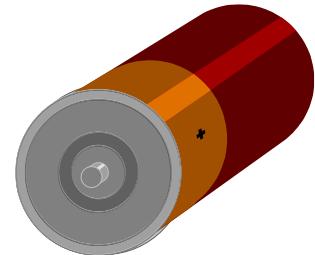
Bluetooth classic vs. cable

Topology	Max. 7 simultaneous lines	1 line = 1 cable
Flexibility	Crosses walls, bodies, etc.	Line-of-sight, physical path
Transmission rate	1 MSPS, 720 Kbps	115Kbps - 400Mbps
Power	0.1 watts active power	0.05 watts or more
Dimensions	25 mm x 13 mm x 2 mm, several grams	Typical 1-2 metros. Weight varies with size
Cost	ci. 5 €/access	~ €4-€100/meter
Range	~ 10 meters	Typical 1-2 metros. Size = range.
Geographic coverage	~similar everywhere.	Cables and connections vary along the world.
Security	Link layer, SS radio. Very safe.	Ideal.



Low power

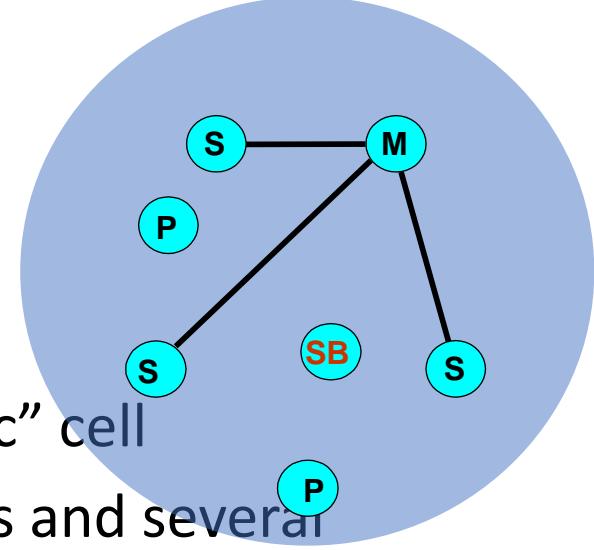
- Global architecture for low power
 - Hold and Park mode: $60 \mu\text{A}$ current
 - Connected device, but not operating
 - Device operates after a 2 ms wait process.
 - In Hold: keeps its AMA (**Active Member Address**); in Park has to free AMA, and later has to claim it back
- Transmission power $\sim 1\text{mW}$
 - 100mW classes also exist
- Standby Current $< 0.3 \text{ mA}$
 \Rightarrow 3 months
- Voice mode: 8-30 mA
 \Rightarrow 75 hours
- Data mode (medium): 5 mA (0.3-30mA, 20 kbit/s, 25%)
 \Rightarrow 120 hours





Piconets

- Bluetooth devices connected in an “ad-hoc” cell
- There is a **master** with up to 7 active slaves and several hundreds parked.
 - Slaves only communicate with master
 - Slaves must wait for permission from master
- Master defines radio parameters (“clock” and “deviceID”)
 - Channel, hopping sequence, timing, ...
- Each piconet has an unique FH pattern (e and a single ID)
- Each piconet has a maximum bandwidth (1MSPS)
- A slave in one piconet can also be part of another piconet
 - Either as a master or as a slave
 - If master, it can create scatternets



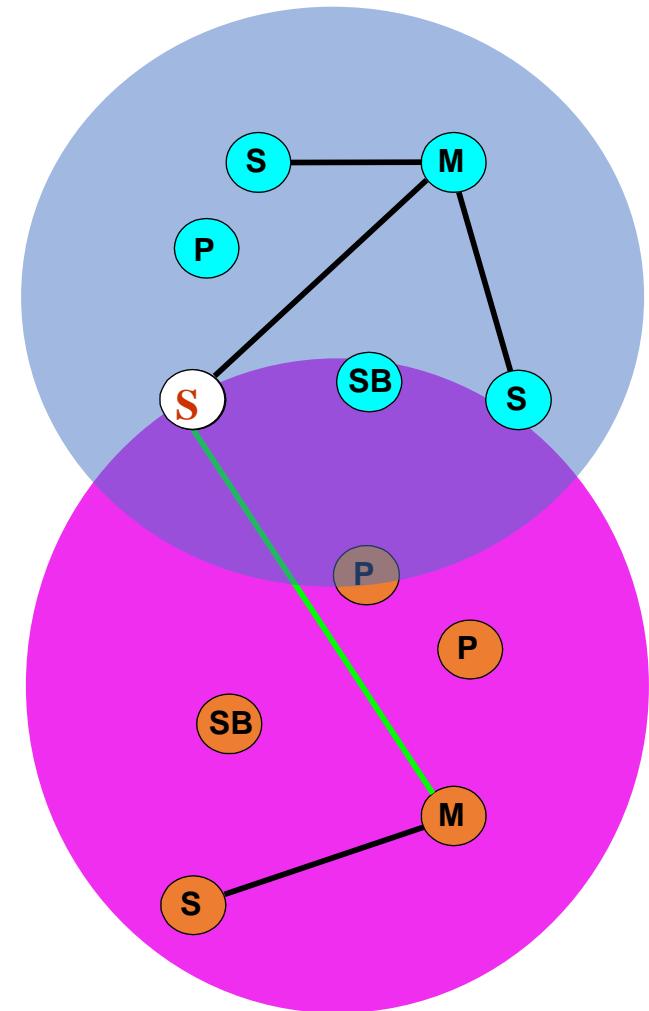
P=**Parked**
SB=**Standby**

M=**Master**
S=**Slave**



Scatternet

- Connection of several piconets
- Through a common device (bridge) (M/S)
- One device can be M/S at the same time
 - Or at least Slave in two piconets
 - Bridge node “stay” in a piconet for some time, then switch to another piconet by changing hop sequence.
- Global system BW unlimited, but piconet BW always <1Mbps
- Impact on piconets is minimal for < 10 piconets.
- Potentially any device can share piconets
 - Reality: limitations on commercial stacks



M=Master P=Parked
S=Slave SB=Standby



Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- Profiles and security
- 802.15.x



Piconet operation

- FH-SS: all devices must share the same hopping pattern:
 - Master provides clock and deviceID such that:
 - deviceID (48-bits) defines hopping pattern
 - Clock defines phase inside the pattern.
- If a device is inside a piconet, and is not connected, it must be in *standby*
- There are two types of piconet addresses (7+200...)
 - *Active Member Address* (AMA, 3-bits)
 - *Parked Member Address* (PMA, 8-bits)

IDa

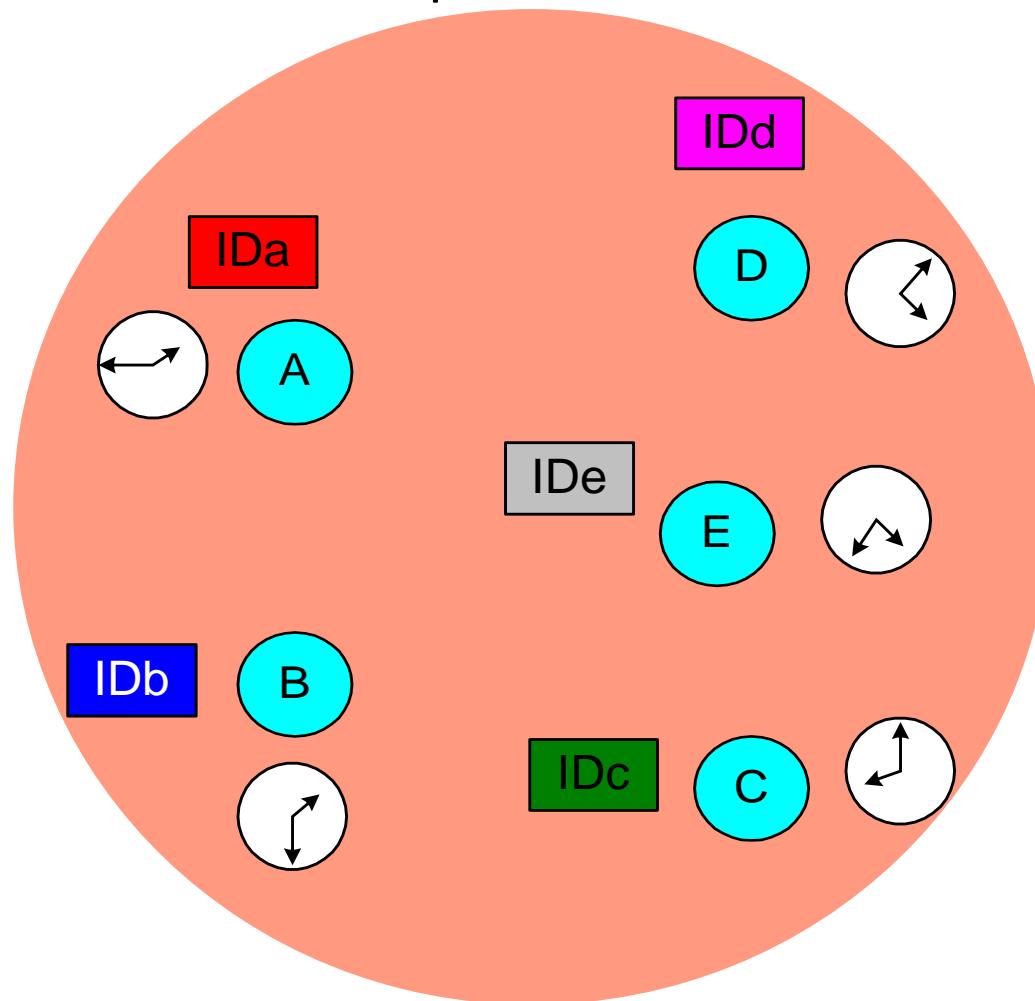


sb



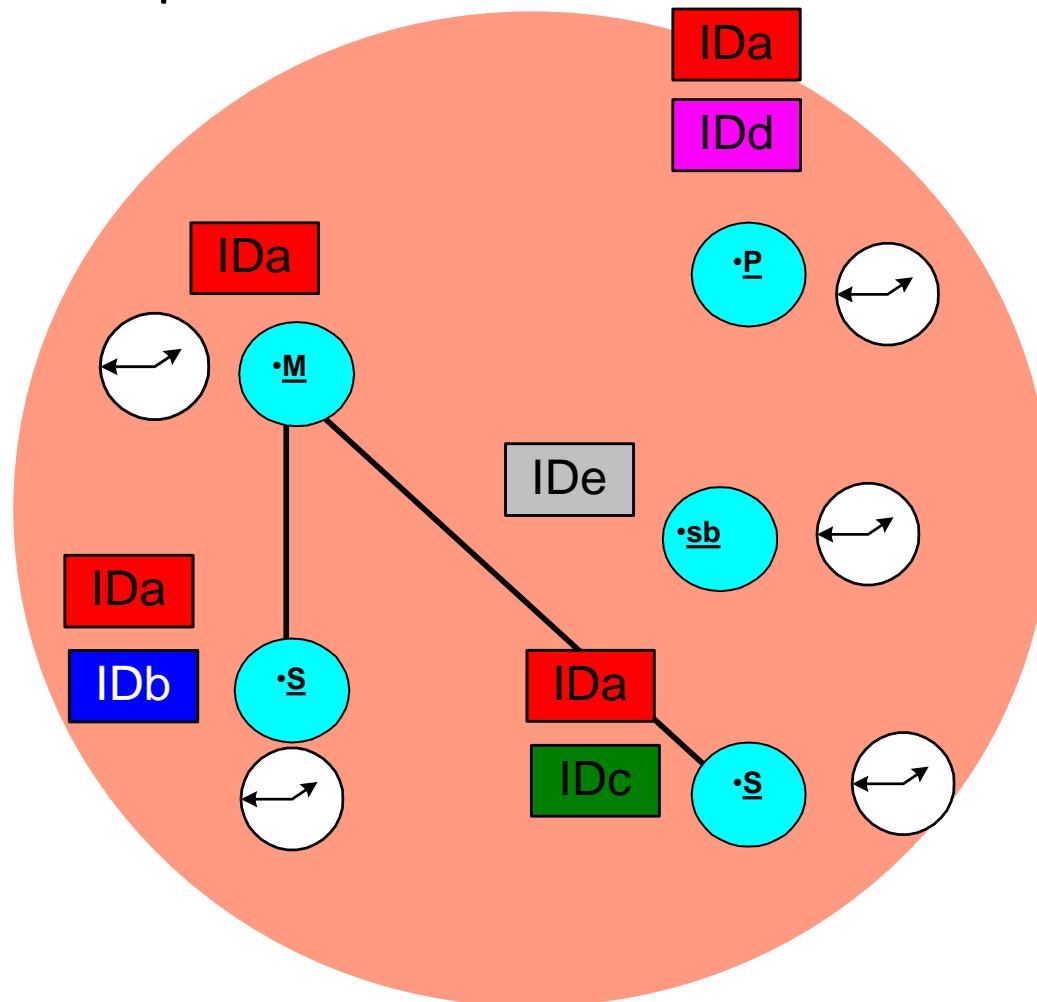


Piconet before setup





Piconet in operation

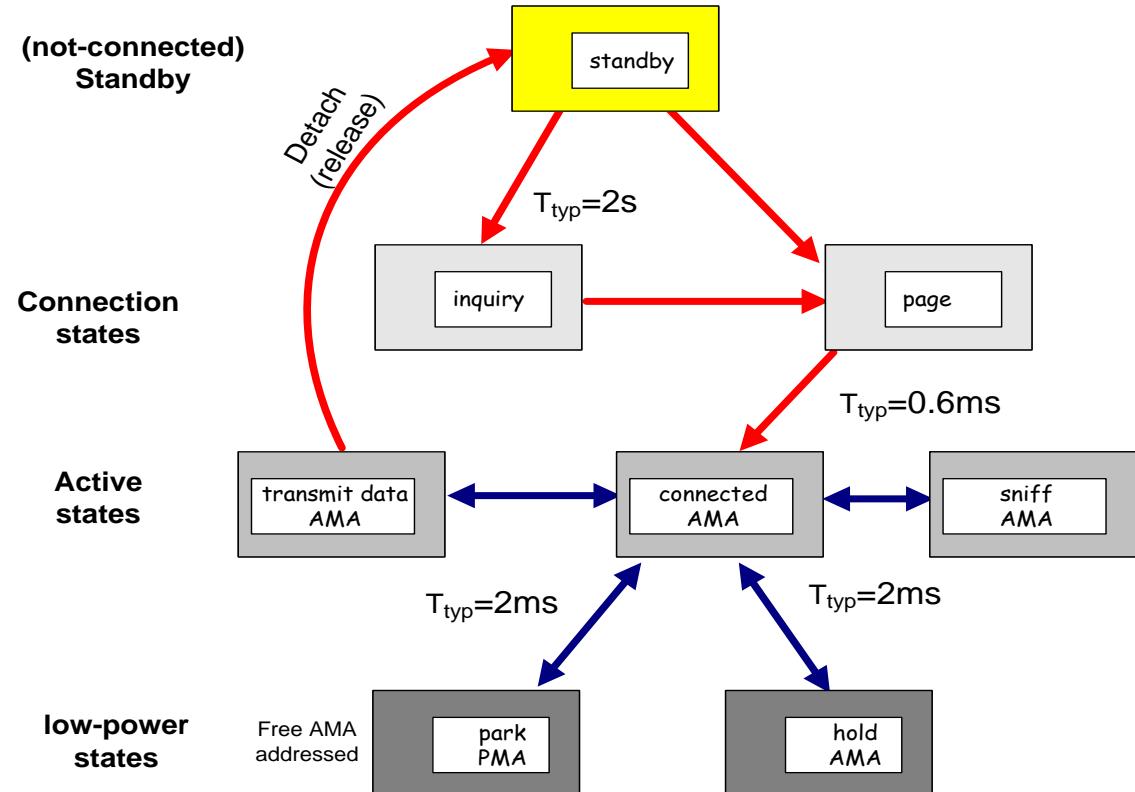


Piconet built!



Device states

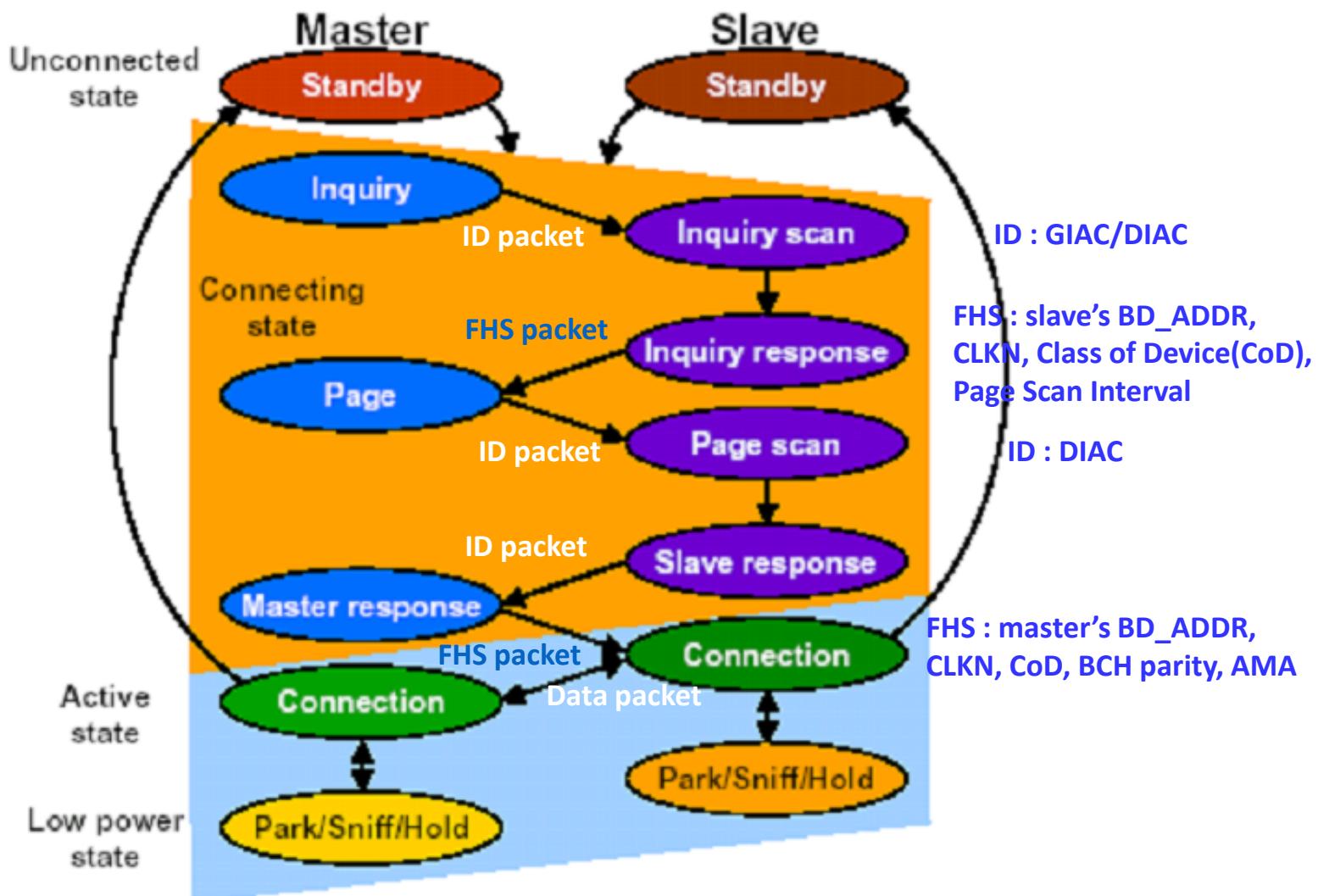
- **Standby**
 - Waiting to join a piconet
- **Inquire**
 - Ask about radios to connect to (discover nodes)
- **Page**
 - Connect to a specific radio
- **Connected**
 - Actively on a piconet (master or slave)
- **Park/Sniff/Hold**
 - Low Power connected states





Connection Procedure

General Inquiry Access Code (GIAC)
Dedicated Inquiry Access Code (DIAC)



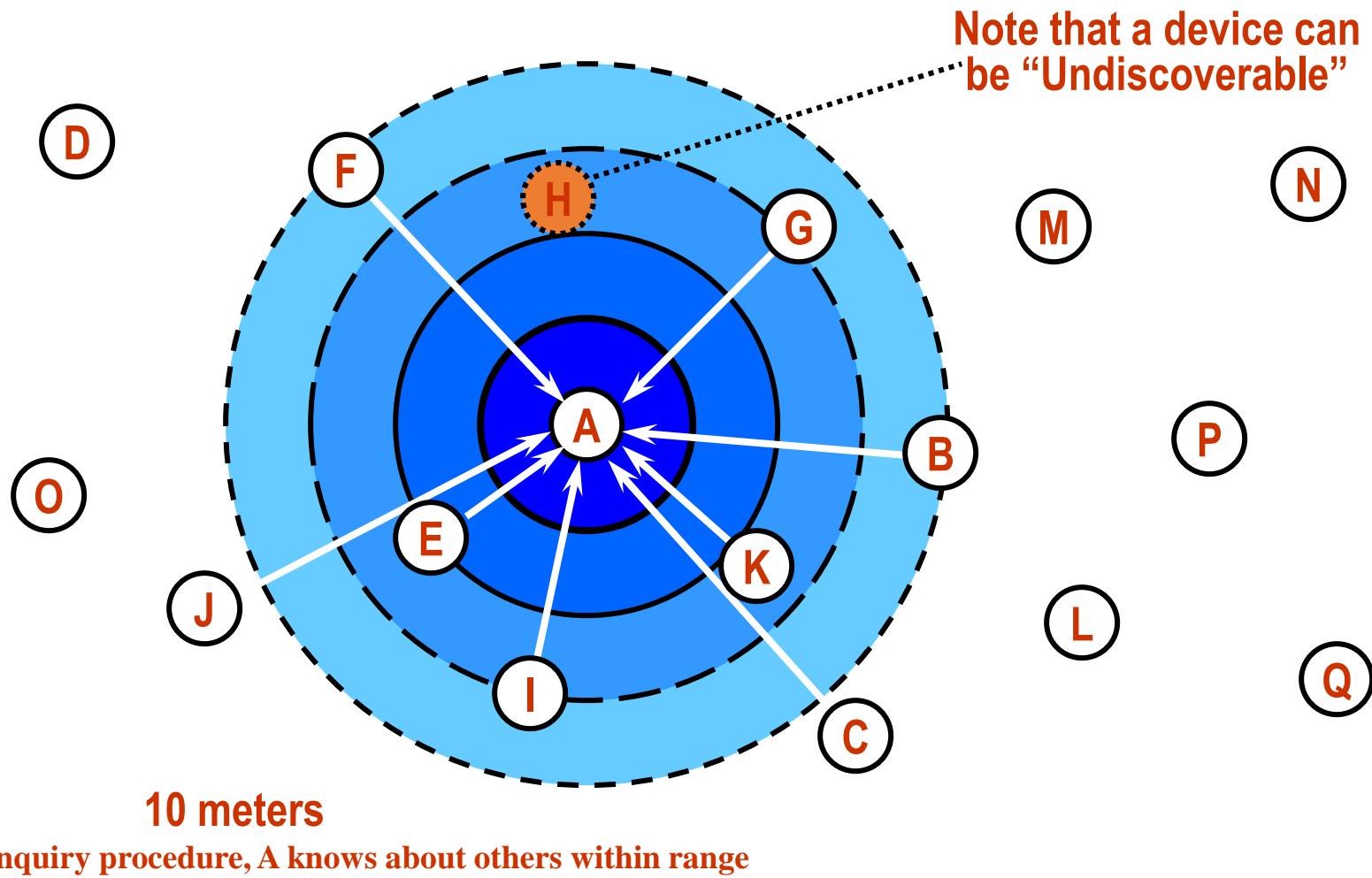


Low-Power Operation in BT classic

- 3 modes:
 - Hold: node sleeps for specified interval.
 - Master can put slaves in hold while searching for new members, attending another piconet, etc.
 - No ACL packets (Asynchronous Connection-Less) → general data packets
 - (there is also Synchronous Connection Oriented → Audio)
 - Sniff: slave low-duty cycle mode.
 - Slave wakes up periodically to talk to master.
 - Fixed “sniff” intervals.
 - Park:
 - Very low power state.
 - Used to admit more than 7 slaves in piconet.
 - Slave gives up its active member address.
 - Receives “parked” member address.
 - Wakes up periodically listening for broadcasts which can be used to “unpark” node.

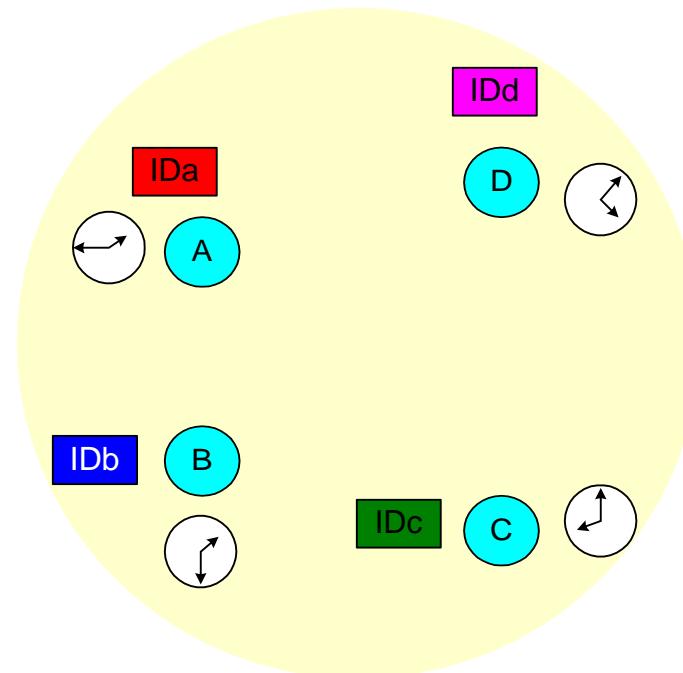


Device Discovery Illustrated





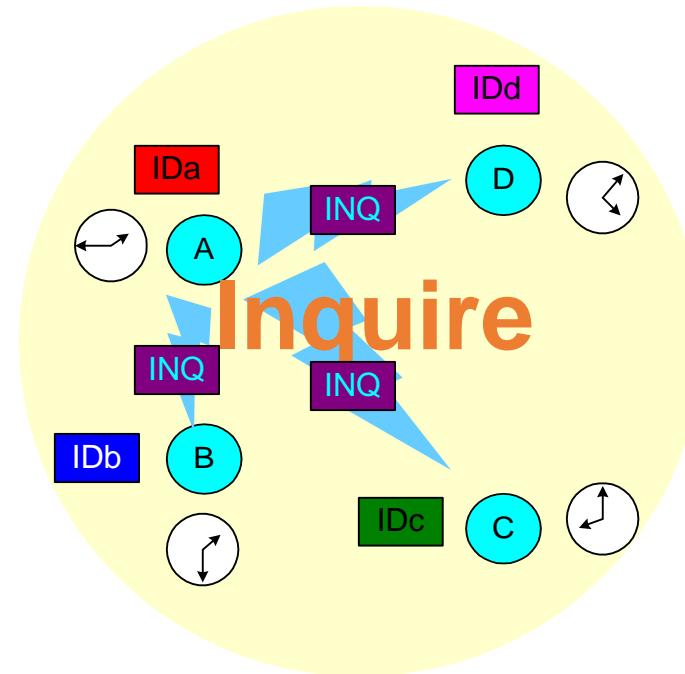
Scanning units



Device A wants to search for stations



Scanning units

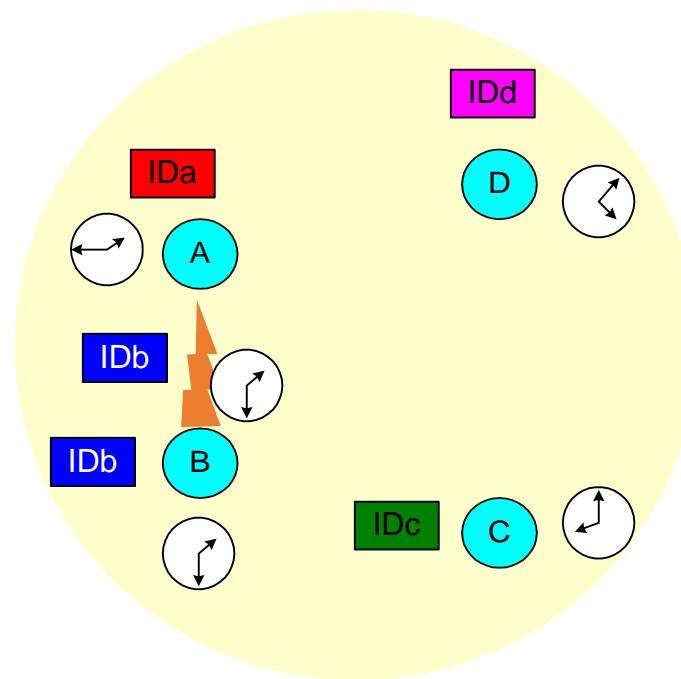


Device A wants to search for stations
A does an inquire (page with ID 000)

Devices B,C,D are doing an inquire scan



Scanning units



Device A wants to search for stations

A does an inquire (page with ID 000)

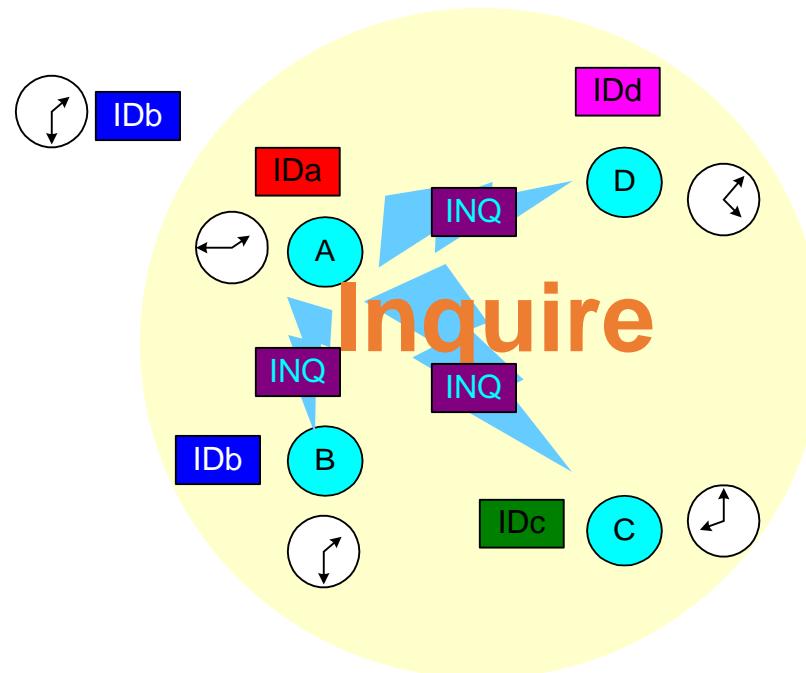
Devices B,C,D are doing na inquire scan

B answers with FHS packet

Contains *DeviceID* and *Clock*



Scanning units



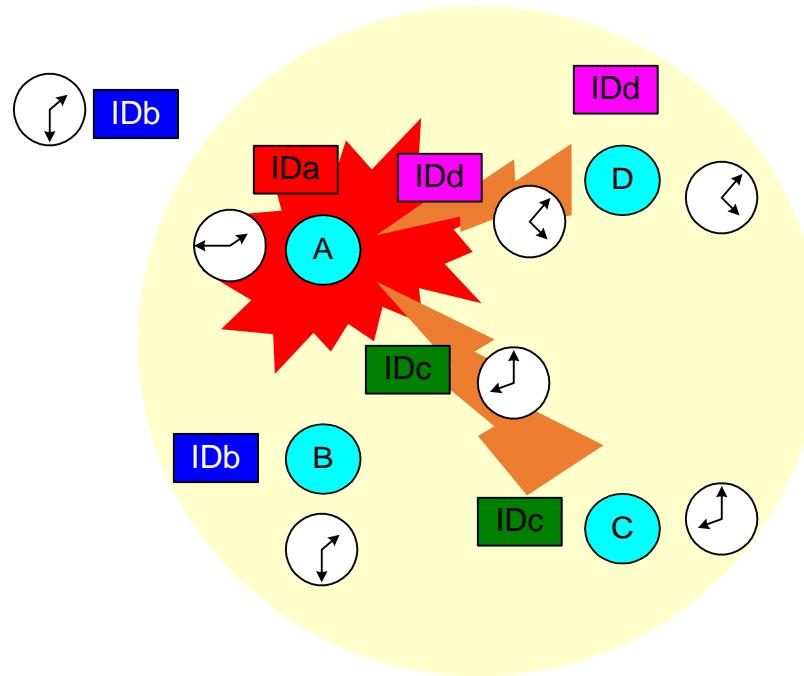
Device A wants to search for stations

- A does an inquire (page with ID 000)
 - Devices B,C,D are doing an inquire scan
- B answers with FHS packet
 - Contains *DeviceID* and *Clock*

A does an inquire again



Scanning units



A wants to search for stations

A does an inquire again

C e D answer at the same time with FHS packet

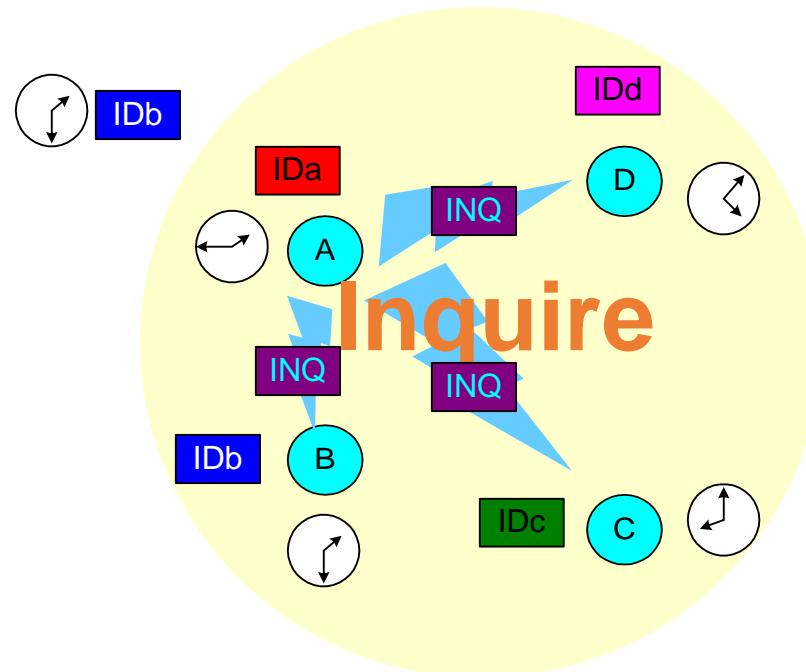
Packets are corrupted

A does not answer

C and D will wait an random number of slots



Scanning units

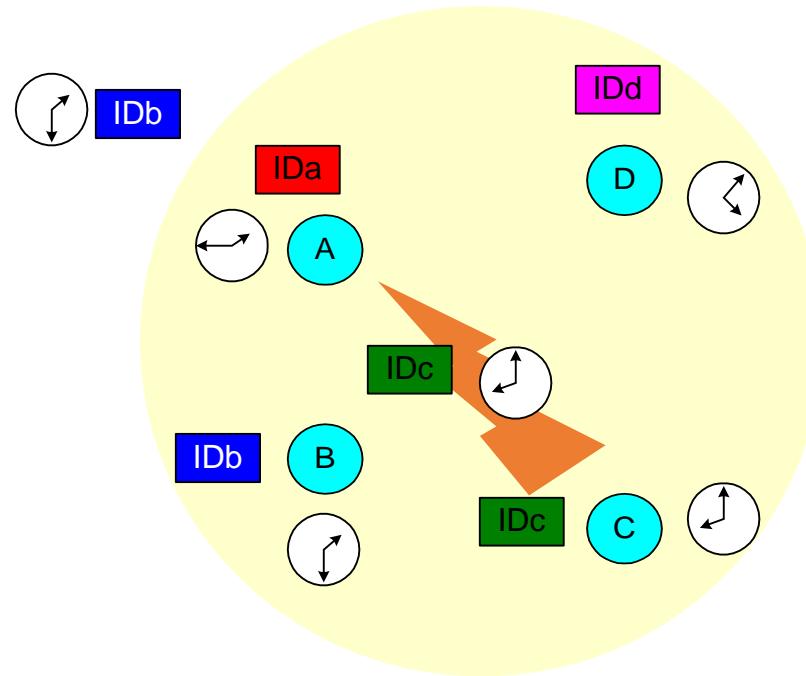


A wants to search for stations

A does an inquire again



Scanning units



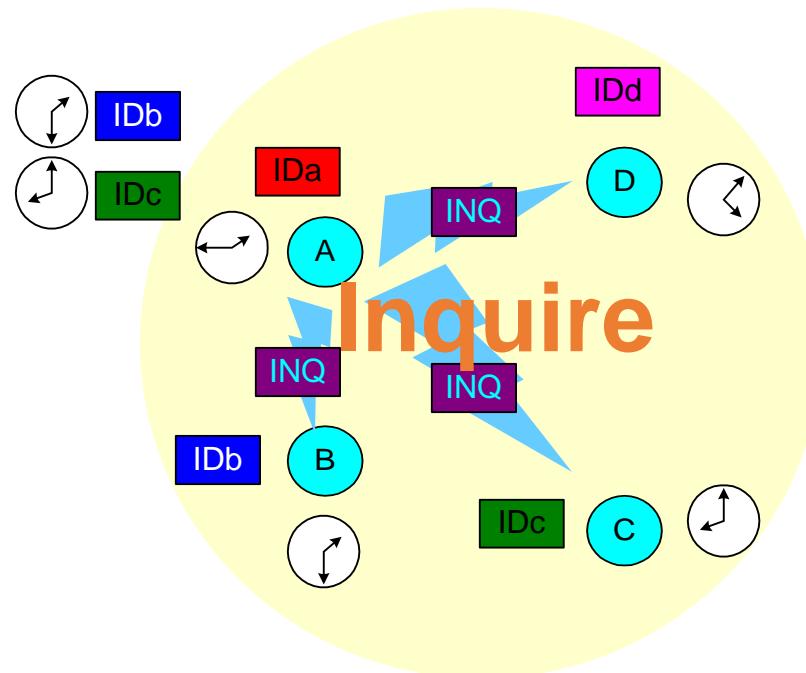
A wants to search for stations

A does an inquire again

C answers with FHS packet



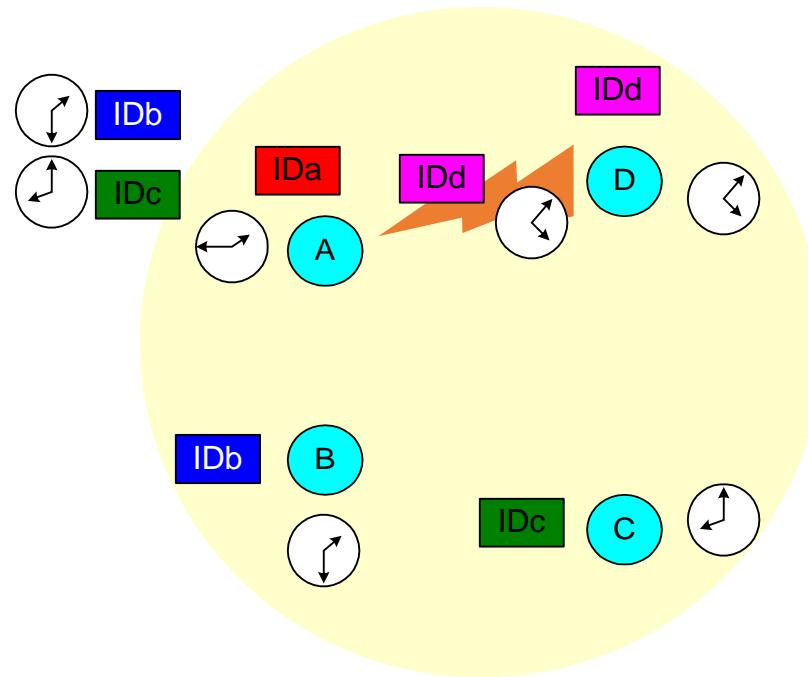
Scanning units



A wants to search for stations
A does an inquire again



Scanning units



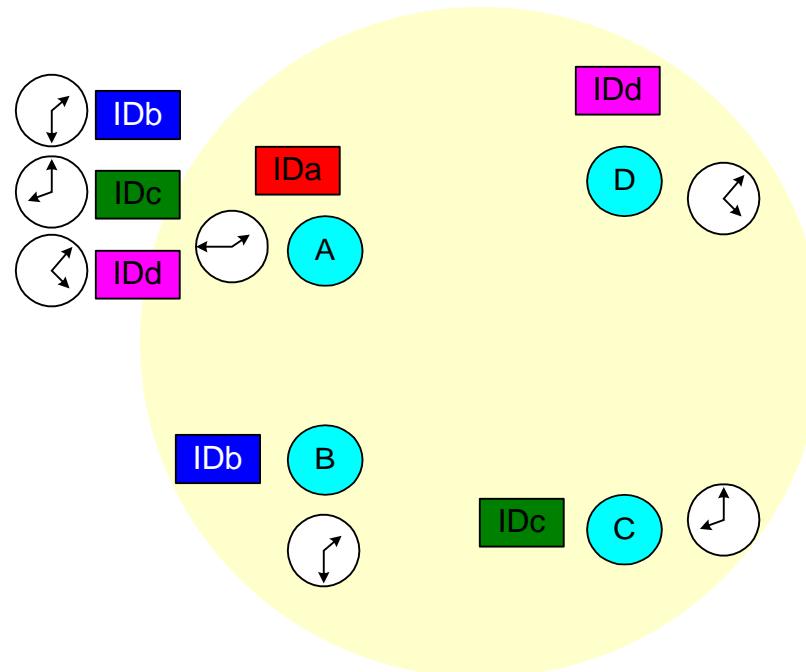
A wants to search for stations

A does an inquire again

D answers with FHS packet



Scanning units



A has all the information it needs about the units in the cell.

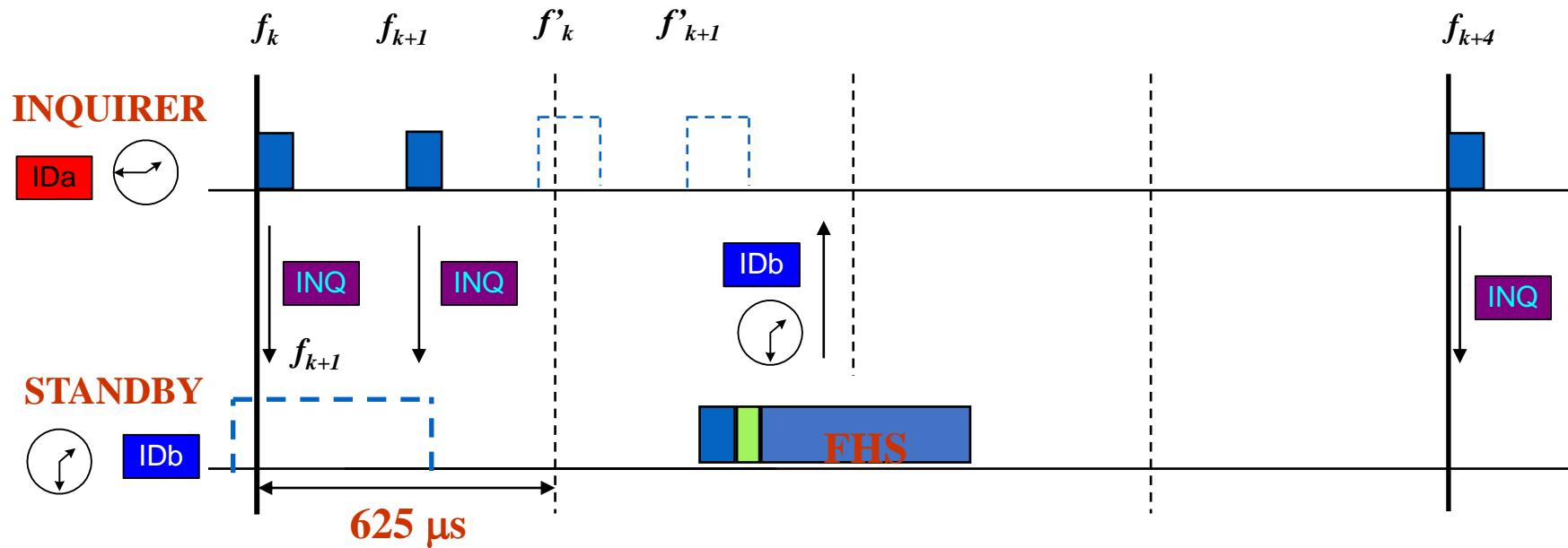


Inquiry scanning: summary

- Inquiry scanning has a common address
 - and a common frequency pattern (from 32 frequencies)
- All devices can page this address (and become masters)
- All machines hearing an inquiry will answer the inquiry request
- There is a detector (*correlator hit*) in the slaves, that detects inquiries, before answering with a FHS providing:
Device ID and Clock
- A machine in low power waits a random time before answering again to a scan
- If there is a collision on answering to a scan, they also wait a random period before answering again.



Timing: Inquiry



Inquiry requires two packets before the slave answers.



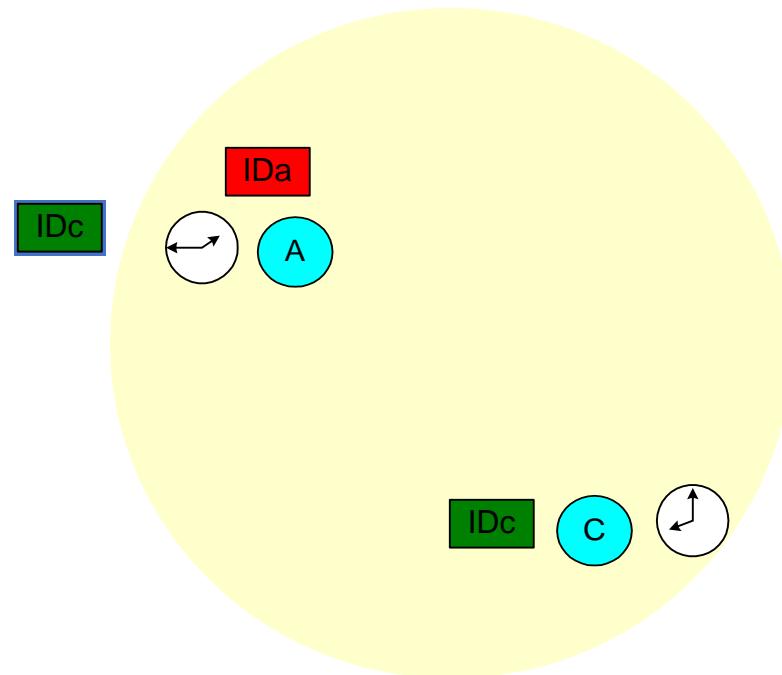
Paging: Will you connect to me?

- Very similar to inquire
- Still have not synchronized clocks or frequencies
- Establishes actual Piconet connection with a device that it knows about
- Connection process involves a 6 steps of communication between the master and the slave

Step	Message	Direction	Hopping Pattern	Pattern Source and Clock
1	Slave ID	Master to Slave	Page	Slave
2	Slave ID	Slave to Master	Page Response	Slave
3	FHS	Master to Slave	Page	Slave
4	Slave ID	Slave to Master	Page Response	Slave
5	1st Master Packet	Master to Slave	Channel	Master
6	1st Slave Packet	Slave to Master	Channel	Master



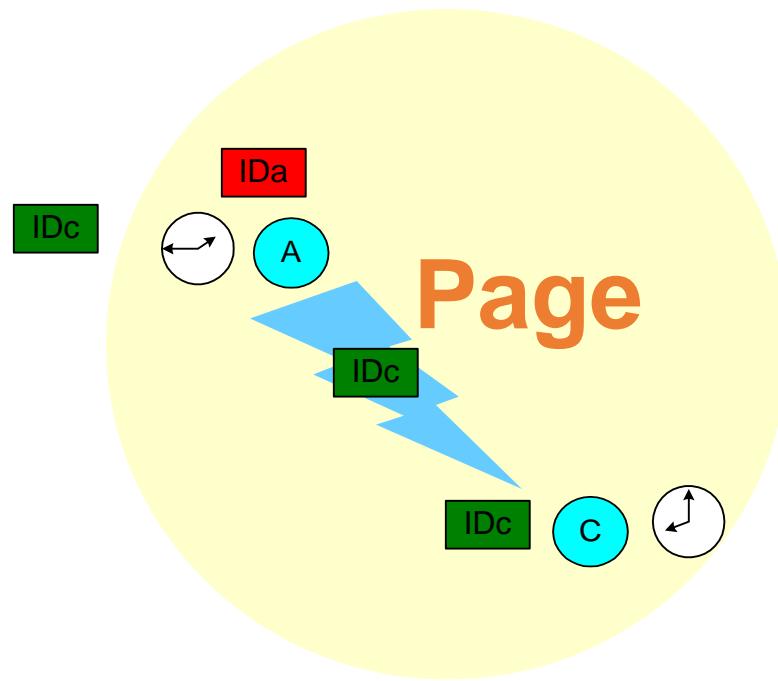
Master Paging Slave



- Paging:
 - Assumes that the master has the *Device ID* and *Clock*



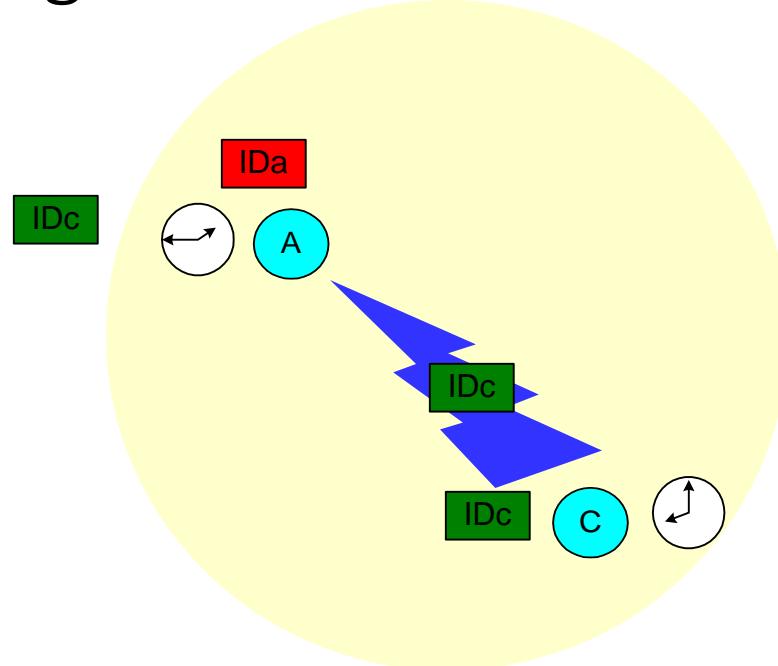
Master Paging Slave



- **Paging:**
Assumes that the master has the *Device ID* and *Clock*
 - *A* pages *C* with the *deviceID* of *C*



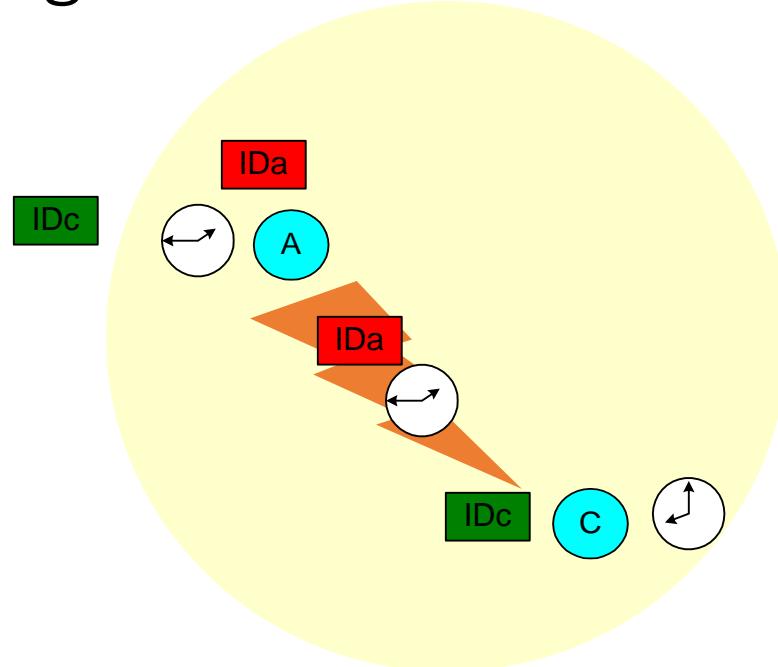
Master Paging Slave



- Paging: master has the *Device ID* and *Clock*
 - A pages C with the *deviceID* of C
 - C answers A with his *deviceID*



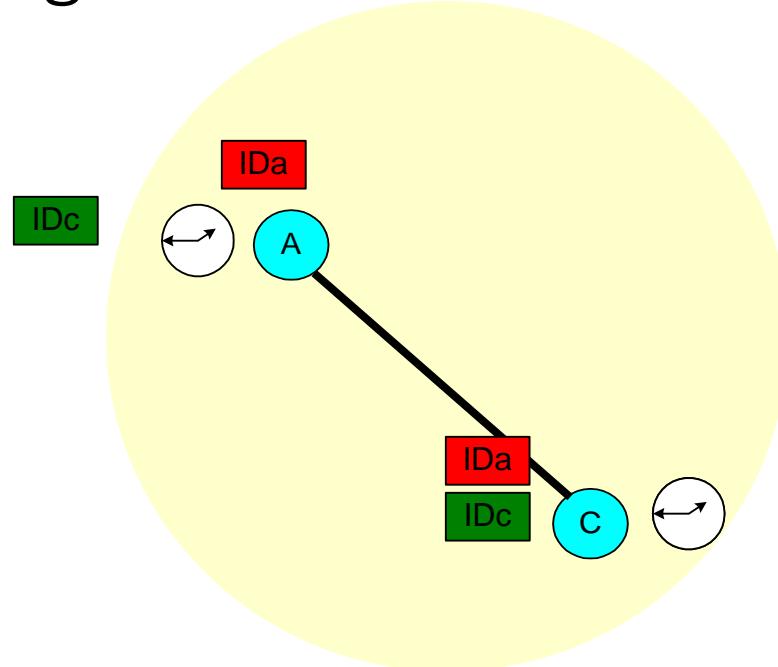
Master Paging Slave



- Paging: master has the *Device ID* and *Clock*
 - A pages C with the *deviceID* of C
 - C answers A with his *deviceID*
 - A send C his *deviceID* and *Clock* (FHS packet)



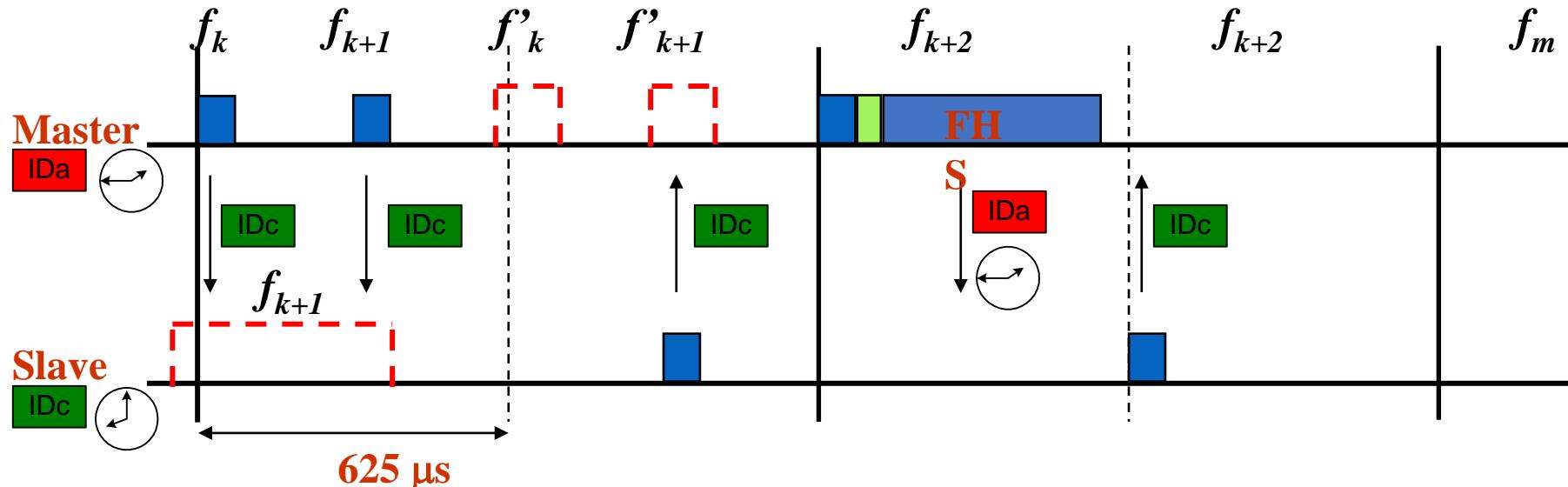
Master Paging Slave



- Paging: master has the *Device ID* and *Clock*
 - A pages C with the *deviceID* of C
 - C answers A with his *deviceID*
 - A send C his *deviceID* and *Clock* (FHS packet)
 - A becomes master of C



Time: Master Paging Slave



- Master pages slave (packet has slave's ID) at the paging frequency of the slave (1 of 32)
 - Master send a train of 16 fqs in the slave hop set.
 - Slave ID sent twice in the slave frequency
 - Master waits for two answers in the slave frequency
 - If it does not work, master will send
- Slave listens for 11 ms (page scan)
 - If it identifies packets, slave wakes up and sends packets in that frequency.
 - Master answers with FHS (*Device ID e Clock*)
 - Slave joins piconet.

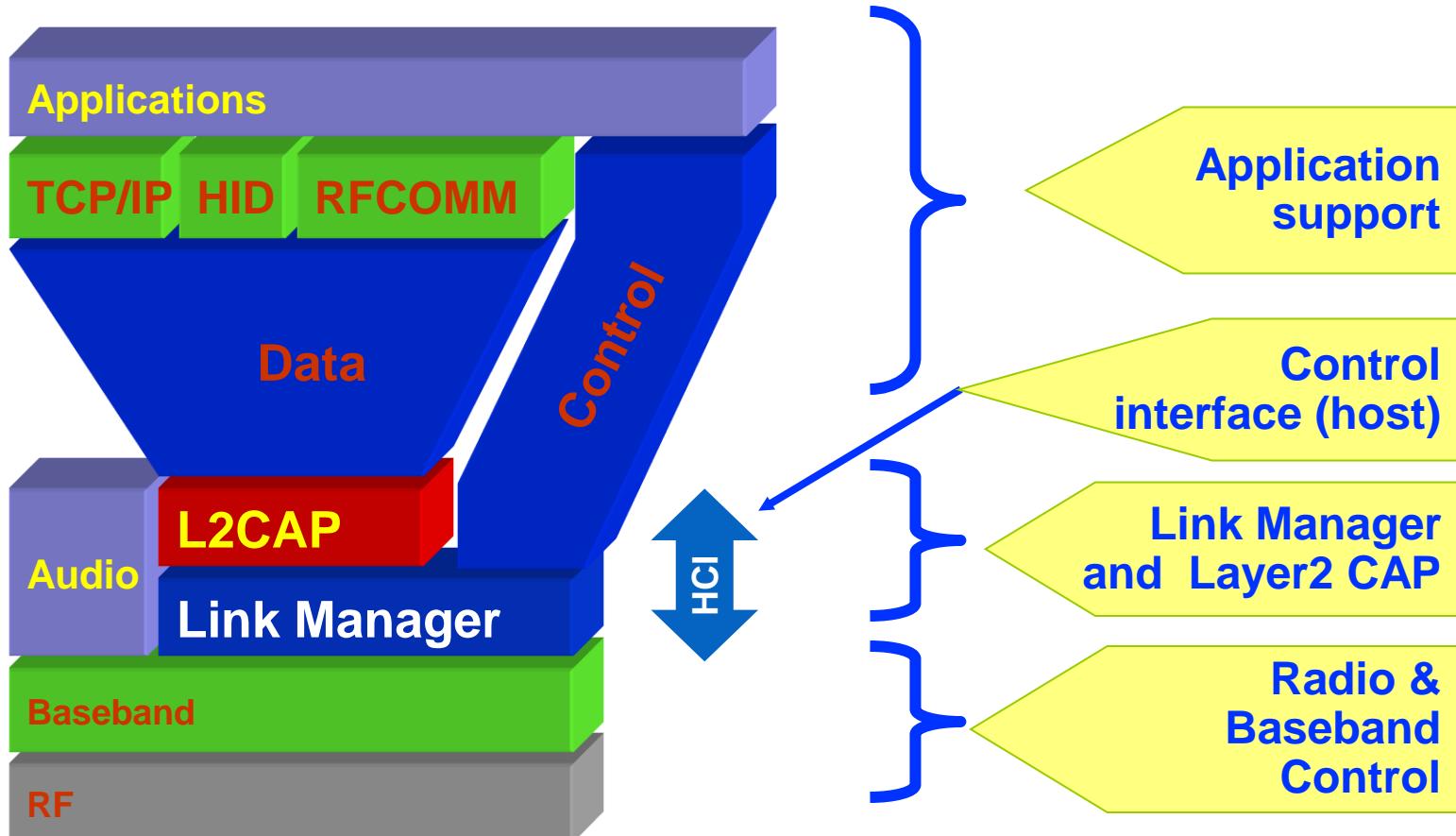


Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- Profiles and security
- 802.15.x



stack Bluetooth



Bluetooth includes:

- A HW description
- an environment for applications

L2CAP – Logical Link Control and Adaptation Protocol

LMP – Link Manager Protocol

HID – Human Interface Device

RFCOMM – serial cable emulation (ETSI)



Bluetooth Protocol

- Radio layer
 - Defines requirements for a Bluetooth radio transceiver
 - Handles conformity to 2.4GHz band
 - Establishes specifications for using Spread-Spectrum Frequency Hopping
 - Classifies device into one of three power classes:
 - long range; (Class 1 - 100mW, 100m)
 - normal/standard range; (Class 2 - 2.5mW, 10m)
 - short range; (Class 3 - 1 mW, 1m)



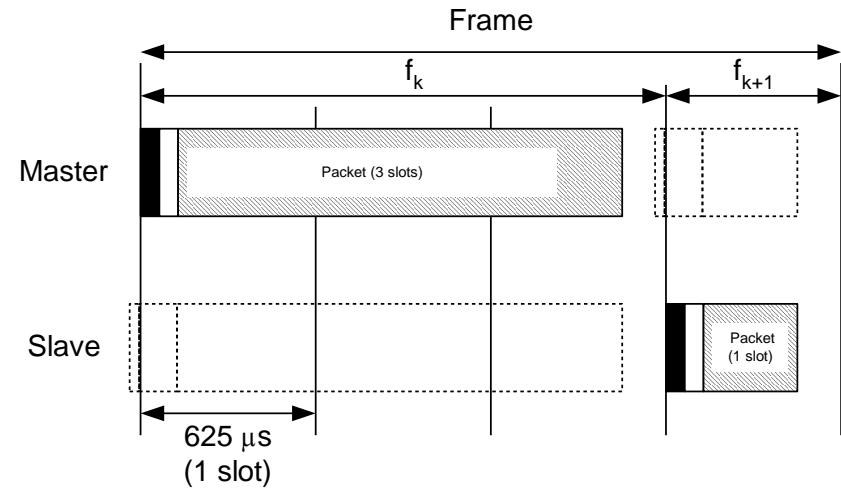
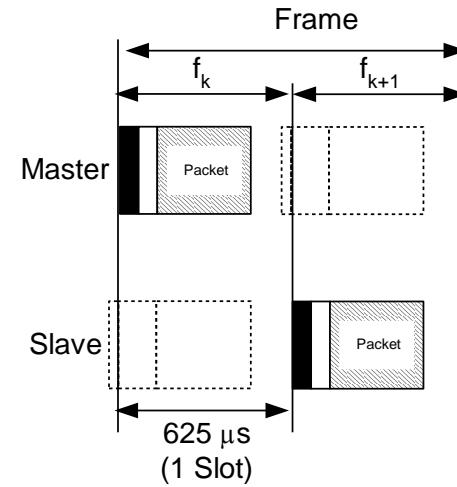
RF: international 2.4Ghz band

- 2.4GHz issues
- Channel BW limited to 1MHz
- Spread spectrum must be used
- Multiple independent networks can interfere
- Microwave ovens also use these frequencies.
- ICs at 2.4 GHz need huge current levels.
- Bluetooth remedies
 - 1 Mb/s baud taxes exploit BW at maximum.
 - Voice coding (CVSDM) allow high speed operation.
 - Fast “frequency hoping” and small packets to avoid interference.
- Interface with the channel minimizes power consumption.
- Interface specifications are relaxed enough to allow its integration in low power chipsets.



Radio Layer

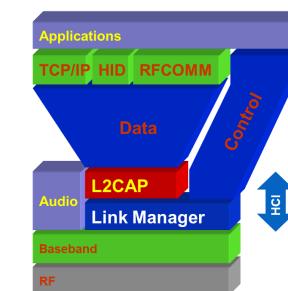
- Radio: FH SS
 - 79/23 channels of 1 Mb/s
 - Hoping: per slot
 - Packets have 1, 3, or 5 slots of 625 μ s.
 - Hoping (nominal) 1600 times per second
 - Frame includes two packets
 - Transmission followed by reception
 - Radio designed to low cost and universal usage
 - (noise, synchronous action technology 2.4GHz, etc...)





Baseband in Bluetooth

- Manages physical channels and logical lines
 - Controls device addressing, channel control, power-saving operations, and flow control and synchronization among devices
 - Implements TDD aspects: master and slave switch in communications
- Works closely with Link controller:
 - Manages link (a)synchronism
 - Controls paging and inquiries
 - Controls power save modes

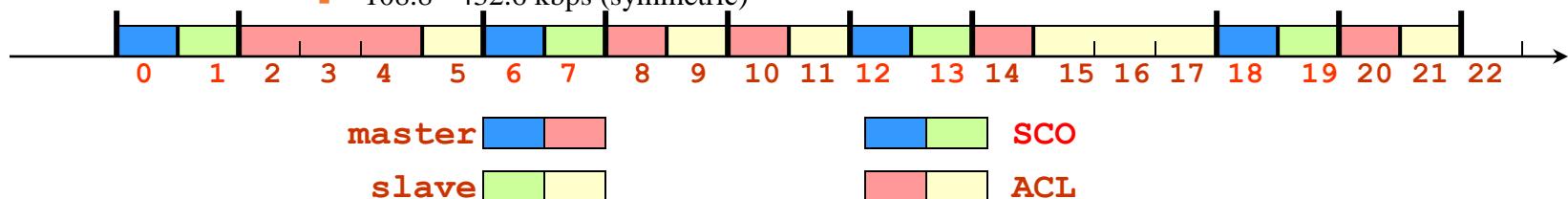




Baseband link types

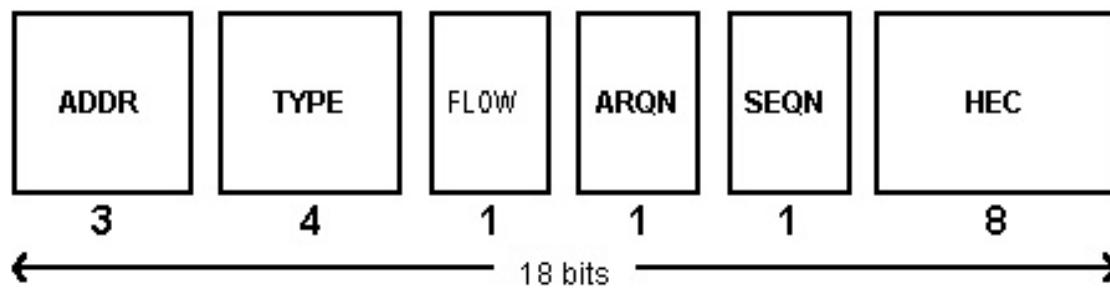
- **Polling-based (TDD) frame transmissions**
 - 1 slot: 0.625msec (max 1600 slots/sec)
 - master/slave slots (even-/odd-numbered slots)
 - polling: master always “polls” slaves
- **Synchronous connection-oriented (SCO) link**
 - “circuit-switched”
 - periodic single-slot frame assignment
 - symmetric 64Kbps full-duplex
- **Asynchronous connection-less (ACL) link**
 - Frame switching
 - asymmetric bandwidth
 - variable frame size (1-5 slots)
 - max. 721 kbps (57.6 kbps return channel)
 - 108.8 - 432.6 kbps (symmetric)

50

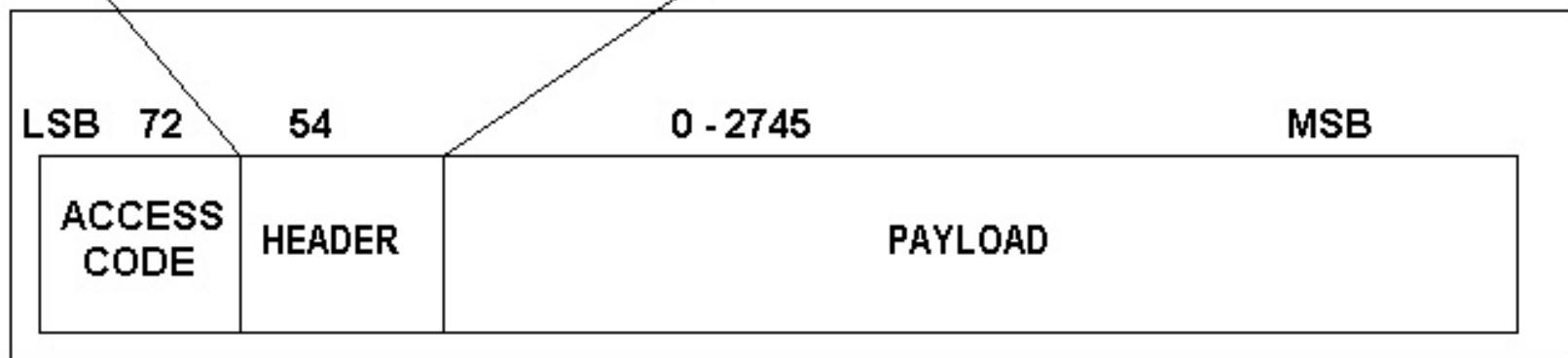




Baseband Packet

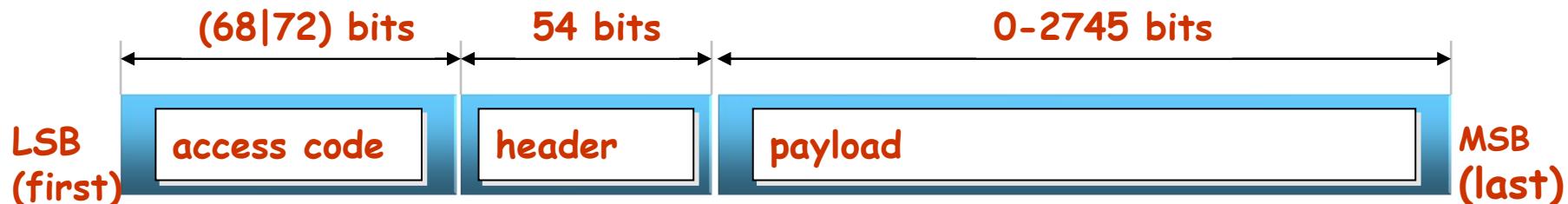


The 18 bit header is encoded with a rate 1/3 FEC resulting in a 54 bit header.





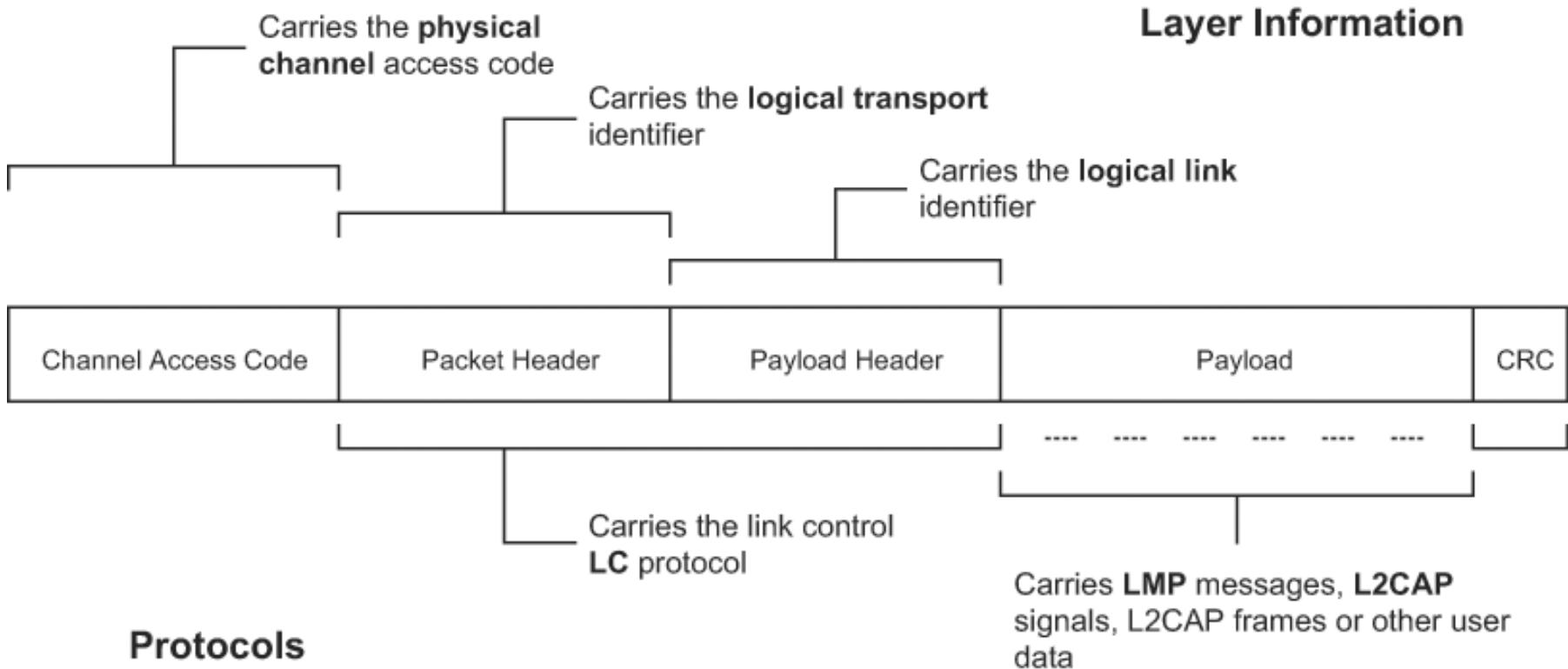
Baseband Frame



- **Access Code:** time synchronization, offset, paging, inquiry.
 - Channel Access Code (CAC), piconet identification, synchronization, DC offset.
 - Device Access Code (DAC), paging and replies.
 - Inquiry Access Code (IAC), inquiries (GIAC, general; DIAC, dedicated)
- **Header:** packet acknowledgement and numbering, flow control, slave address, error checking
- **Payload:** voice, data or both (DV packets).
 - When data, the payload has additional internal header



Bluetooth Frame : Role of fields



ACCESS CODE - based on identity and system clock of Master

Provides means for synchronization; Unique for channel;

Used by all frames on the channel



Packets (common)

TYPE	NAME	#	DESCRIPTION
Common	ID	1	Carries device access code (DAC) or inquiry access code (IAC).
	NULL	1	NULL packet has no payload. Used to get link information and flow control. Not acknowledged.
	POLL	1	No payload. Acknowledged. Used by master to poll the slaves to know whether they are up or not.
	<u>FHS</u>	1	A special control packet for revealing Bluetooth device address and the clock of the sender. Used in page master response, inquiry response and frequency hop synchronization. 2/3 FEC encoded.
	DM1	1	To support control messages in any link type. can also carry regular user data. Occupies one slot.



packets: Synchronous Connection-oriented

SCO	HV1	1	Carries 10 information bytes. Typically used for voice transmission. 1/3 FEC encoded.
	HV2	1	Carries 20 information bytes. Typically used for voice transmission. 2/3 FEC encoded.
	HV3	1	Carries 30 information bytes. Typically used for voice transmission. Not FEC encoded.
	DV	1	Combined data-voice packet. Voice field not protected by FEC. Data field 2/3 FEC encoded. Voice field is never retransmitted but data field can be.



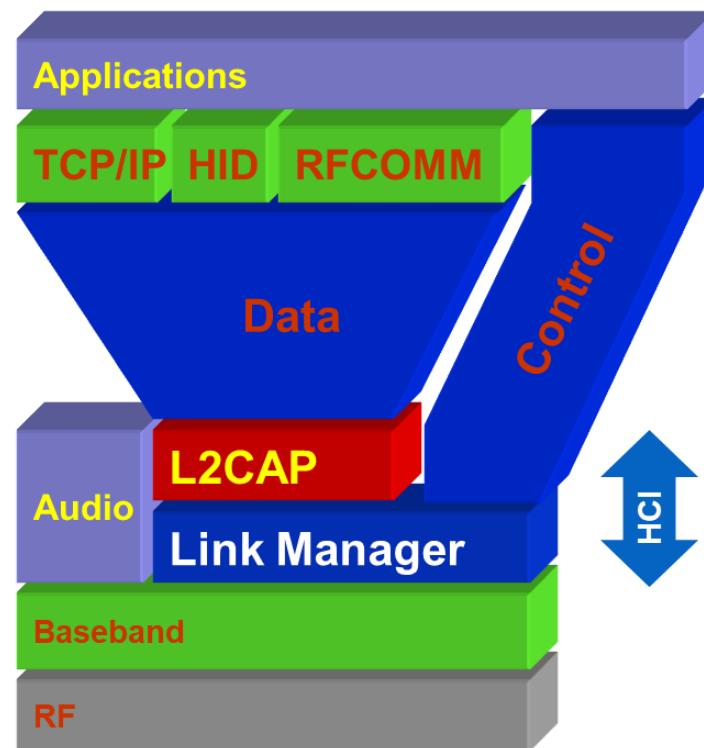
Packets : Asynchronous Connection-Less

ACL	DM1	1	Carries 18 information bytes. 2/3 FEC encoded.
	DH1	1	Carries 28 information bytes. Not FEC encoded.
	DM3	3	Carries 123 information bytes. 2/3 FEC encoded.
	DH3	3	Carries 185 information bytes. Not FEC encoded.
	DM5	5	Carries 226 information bytes. 2/3 FEC encoded.
	DH5	5	Carries 341 information bytes. Not FEC encoded.
	AUX1	1	Carries 30 information bytes. Resembles DH1 but no CRC code.



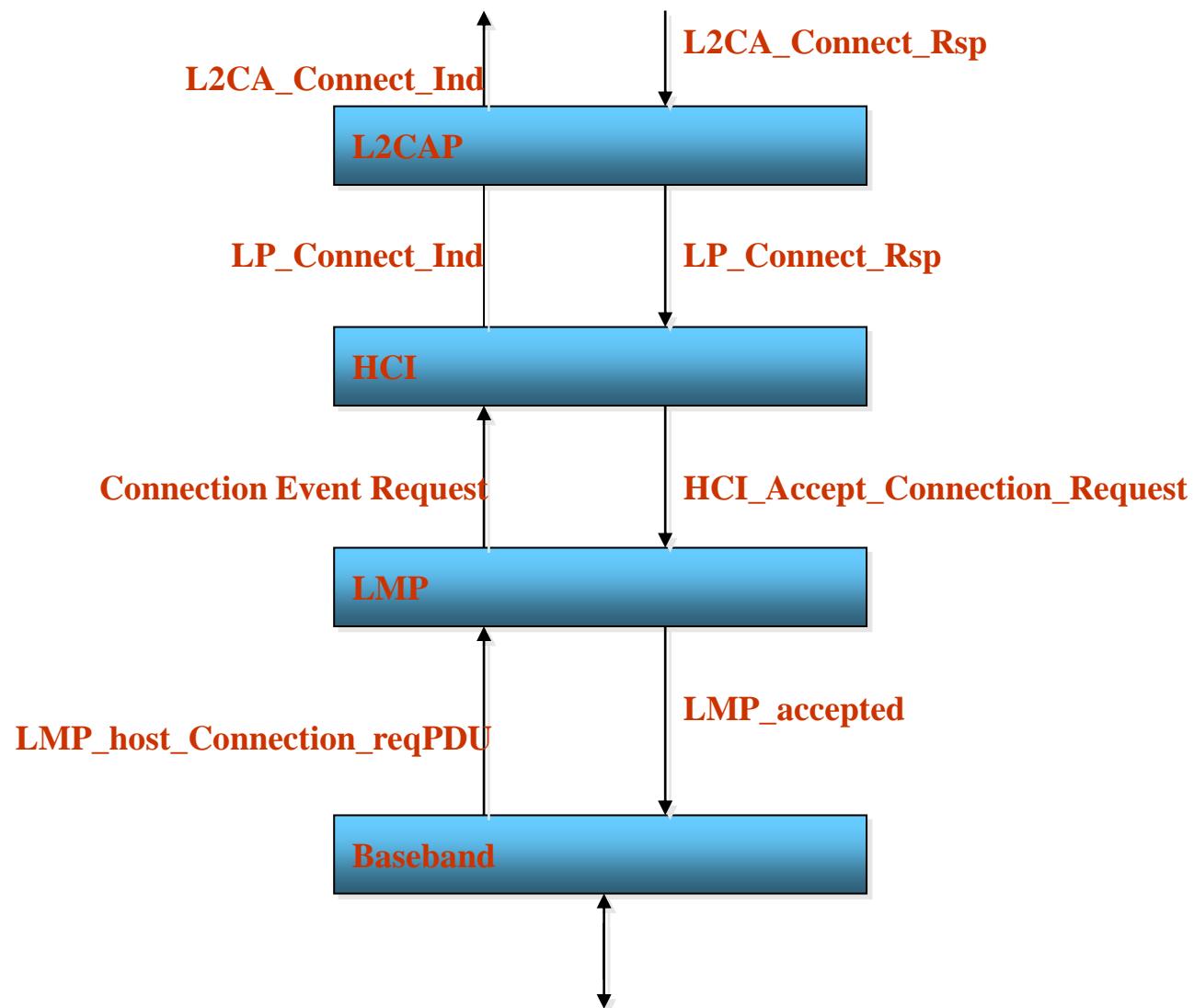
Adaptation protocols

- Link Manager
 - carries out link setup, above baseband, with authentication, link configuration and other protocols
 - Support protocol multiplexing
 - BT may support other protocols besides IP
 - Segmenting and reassembly
- Link Layer Control & Adaptation (L2CAP)
 - Link control protocol, provides connection-oriented and connectionless data services to upper layer protocols
 - Handles ACL and SCO connections
 - Handle QoS specifications per connection (logical channel)
 - Manages concepts as “group of connections”
- Host Controller Interface (HCI)
 - Allows command line access to the baseband layer and LM for control and status information
 - Current interfaces: USB; UART; RS-232
 - Made up of three parts:
 - HCI firmware, HCI driver, Host Controller Transport Layer



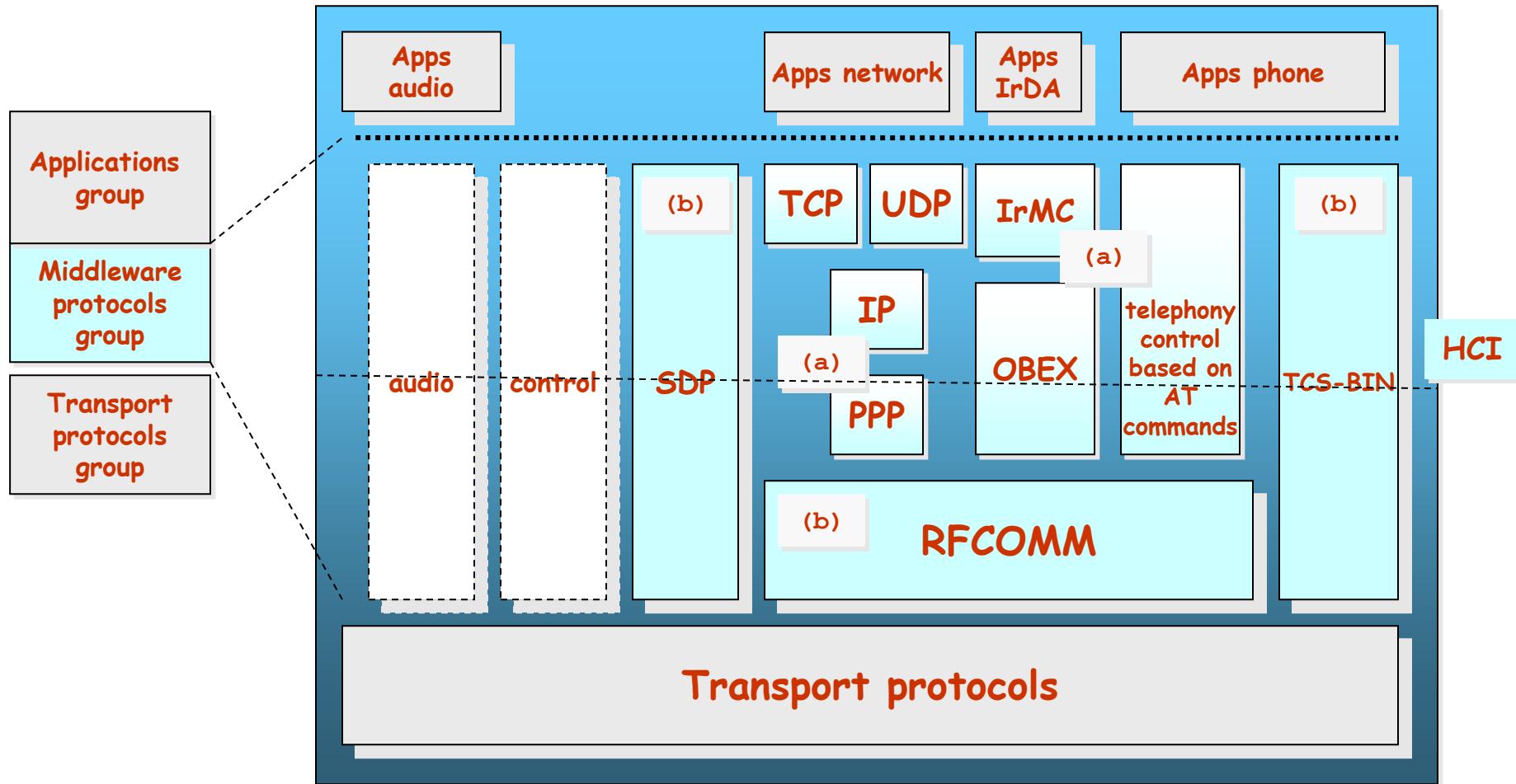


Interlayer communication





Protocols (middleware)



a: common protocol
b: Bluetooth dedicated protocol

SDP: Service Discovery Protocol
OBEX: Facilitates binary transfers between BT devices
TCP-BIN: Telephony-control protocol binary (call control)



Middleware

- Service Discovery Protocol (SDP)
 - Provides a way for applications to detect which services are available and their characteristics
 - Protocol question ↘ answer
 - (search and browsing of services)
 - Defines a format for service registry
 - Information provided by the service *attributes*, a name (ID) + value
 - IDs can be universal (UUID)
- Protocol reusage
 - BT aims to reuse older protocols (e.g. WAP, OBEX-IrDA)
 - Interaction with applications and phones, as commonly done before



Middleware

- RFCOMM
 - Based on GSM TS07.10
 - Emulates a serial port, supporting all traditional applications that were able to use a serial port.
 - Supports multiple ports over a single physical channel between two devices.
- Telephony Control Protocol Spec (TCS)
 - Handles call control (setup, release)
 - Group management for gateways, serving multiple devices
 - Audioconference, e.g.



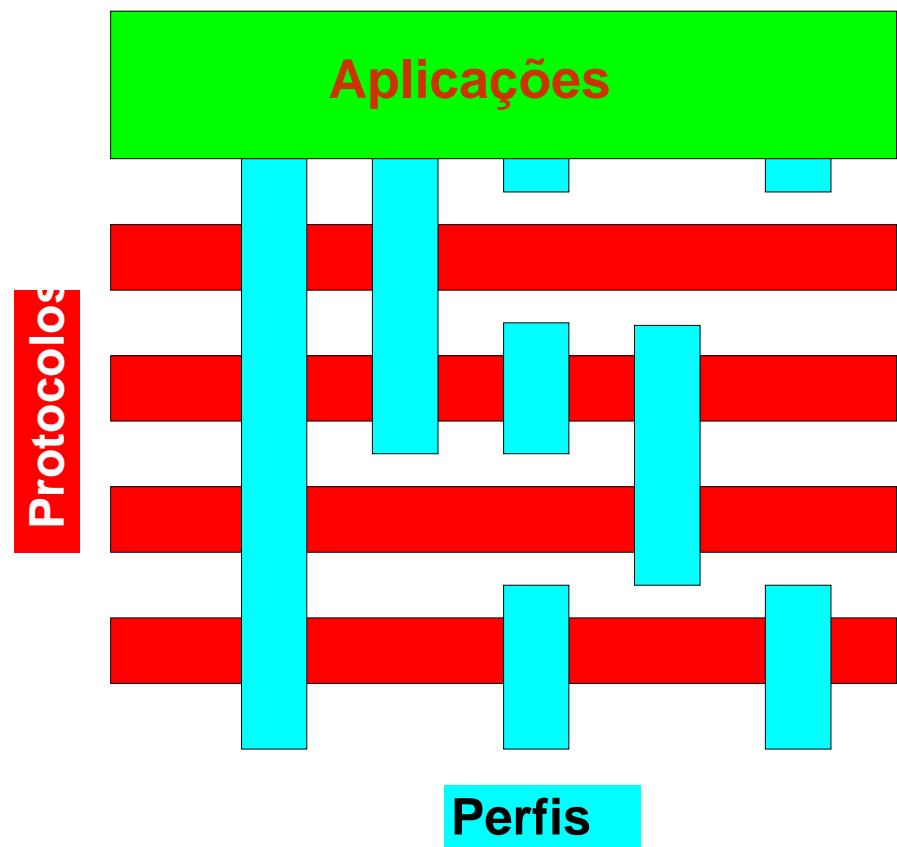
Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- **Profiles and security**
- 802.15.x



Interoperability: Profiles

- Profile: base for BT interoperability (BT too much flexible!)
- “vertical cut” in Bluetooth stack
- A given usage model (typical solution)
- Each BT device supports one or more profiles





Profiles (v.1)

- Generic Access

- Profile SDA
(service discovery application)
- Profiles for serial port, including:
 - Profile Dial-up
 - Profile Fax
 - Profile headset
 - LAN Access (uses PPP)
 - Profile for generic object exchange (OBEX)
 - File transfer
 - Data synchronization
 - Push-pull

- Profile of cordless phone(TCS_BIN)

- Profile interphone
- Profile Cordless Telephony



Profiles (v.2)

- Radio 2 (next generation radio)
 Compatible with existing systems
- Car Profile
- PAN Profile
- GPS Profile
- Printing Profile
- Still image Profile

(globally better facilities in audio/voice/video)

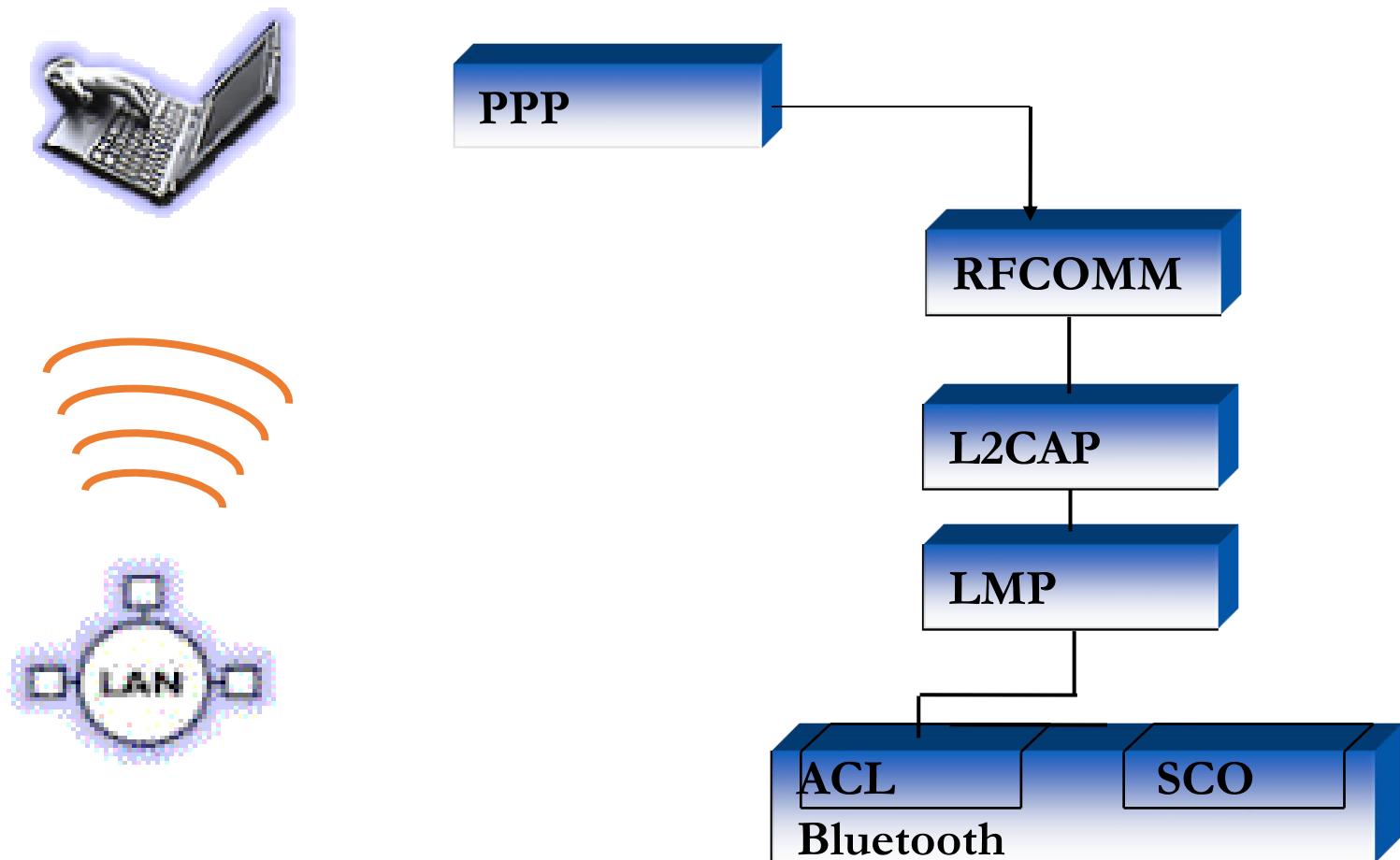
(better service discovery)

(improved human interfaces)

(improved interoperation with other devices at the 2.4GHz ISM)



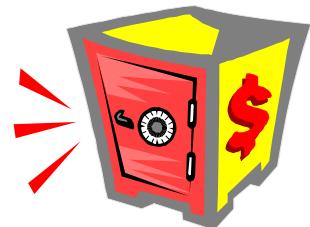
Example: LAN Access Point





Bluetooth: security

- Devices can be:
 - “Trusted”
 - “Untrusted”
 - Also “unknown” devices
- Services security types:
 - Open services – cypher only
 - Authentication only – machine ID
 - Authentication and authorization (ID+explicit service grant)
- Levels of security:
 - Mode 1
 - No security
 - Mode 2
 - Security guaranteed at service level
 - Mode 3
 - Security guaranteed at link level





Bluetooth: security features

- Mechanisms used in BT for security
 - Fast frequency hopping
 - Low range
 - Authentication
 - Two way challenge/response mechanism
 - Cypher (to ensure privacy)
 - Data between two devices can be encrypted
 - Keys used
 - Cypher size configurable (0-16bytes) by the devices, but there are security constraints (goverment)
 - Keys using standard well-known algorithms
 - Security initialization – device pairing
 - PIN (user input)
 - Shared key

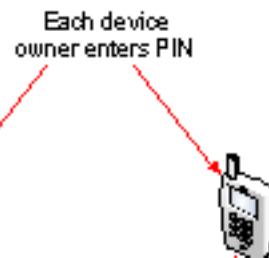


Bluetooth Pairing

Mode 1 – not secure



**Mode 2 – encryption at
the application/service
layer**



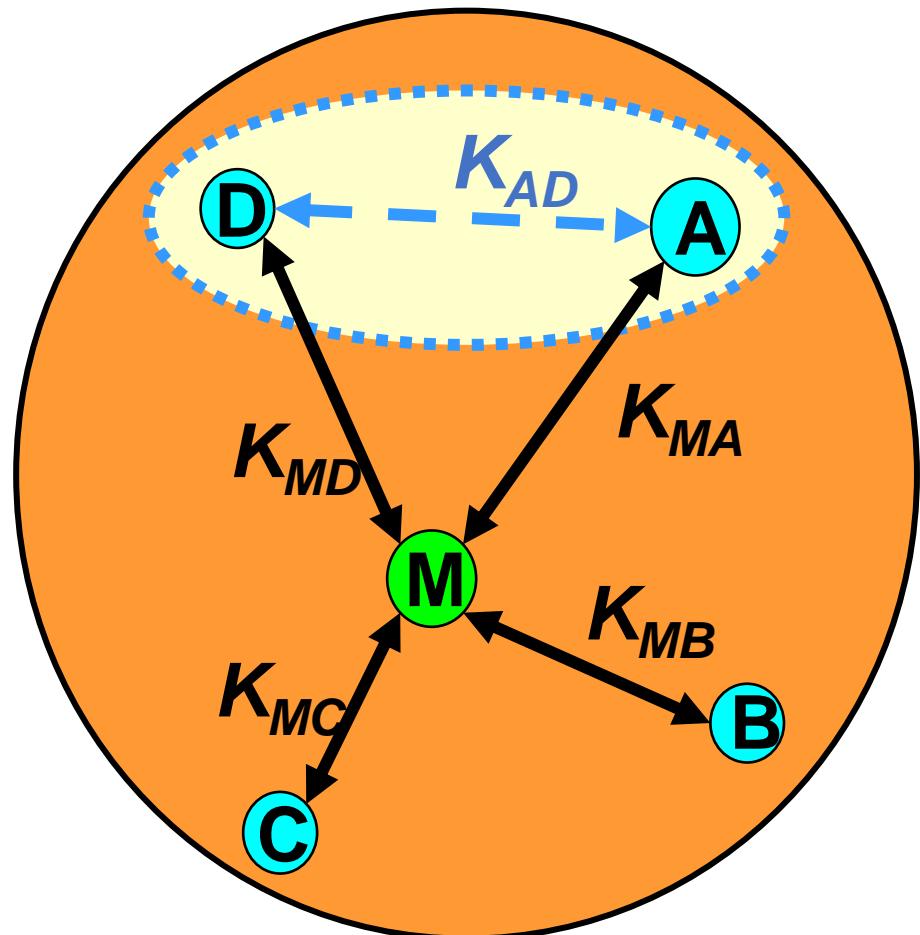
**Pin is used when devices pair.
Size: 1 to 8 bytes**

**Mode 3 – encryption at
the link layer**



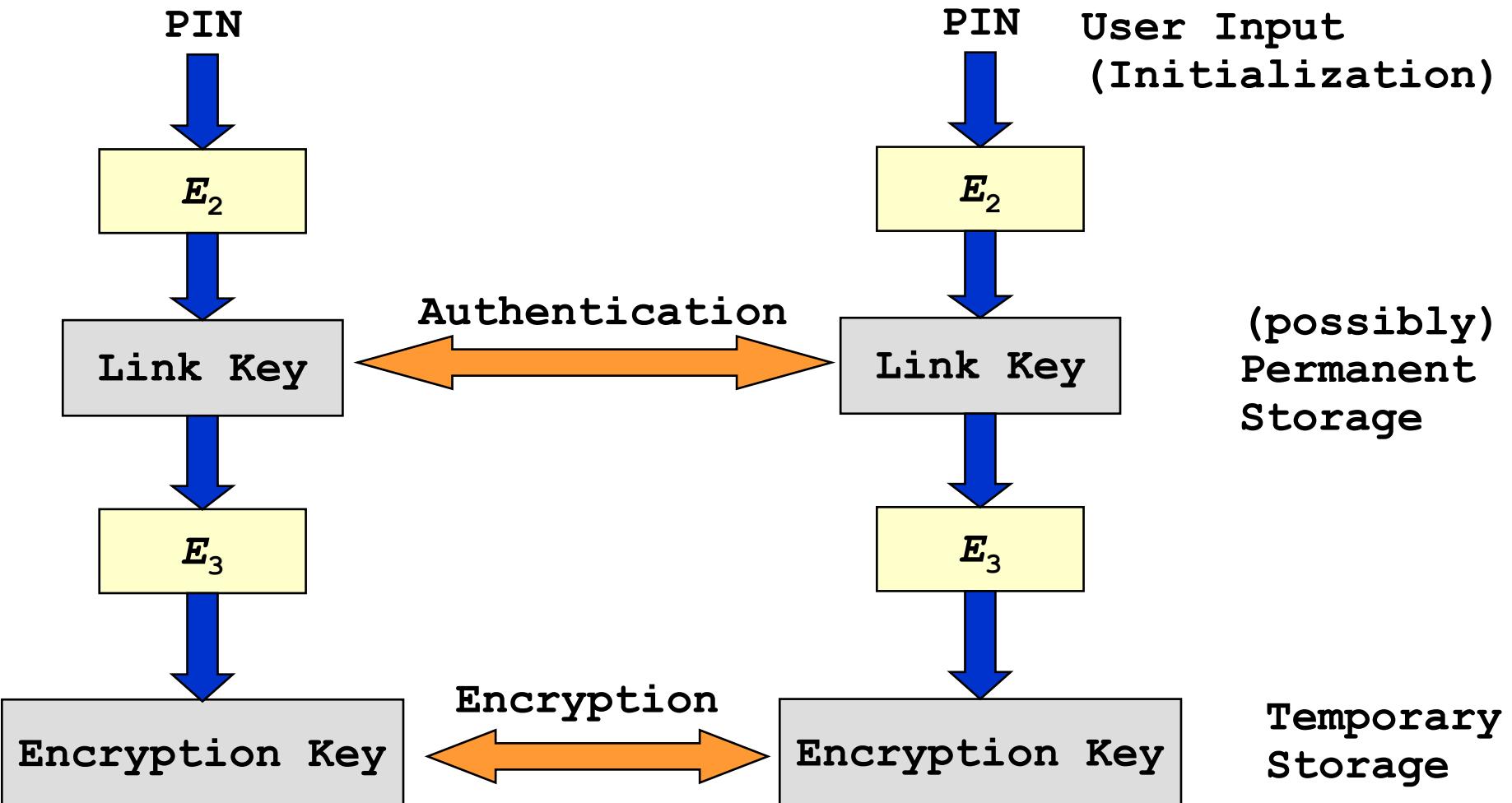
Link keys in a piconet

- Link keys are generated via a PIN entry
- A different link key for each pair of devices is allowed
- Authentication:
 - Challenge-Response Scheme
- Permanent storage of link keys





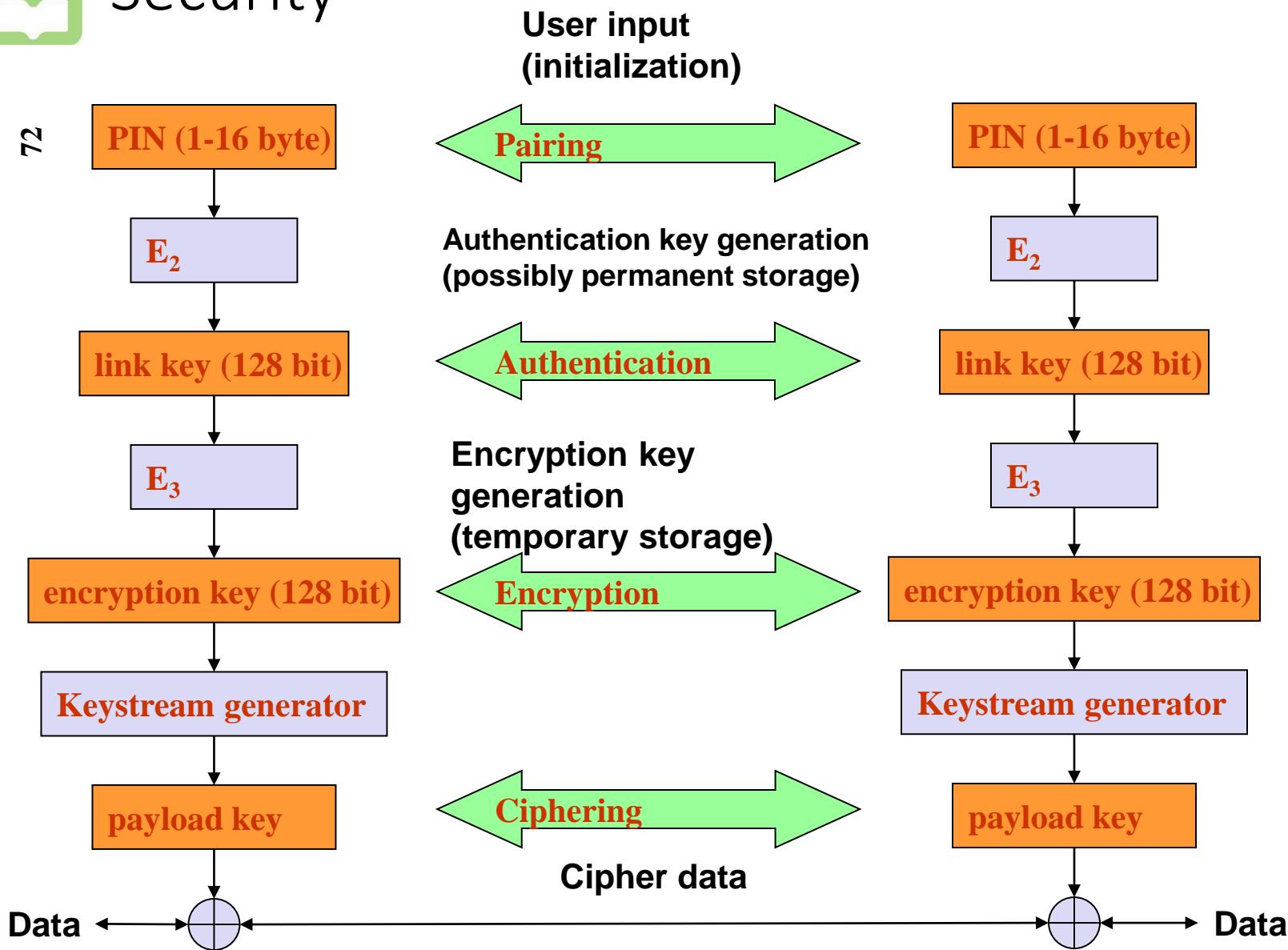
Key generation and usage





Security

72





Outline

- Bluetooth networks
- Piconet operation
 - Inquiry
 - Paging
- Bluetooth stack
- Profiles and security
- **802.15.x**



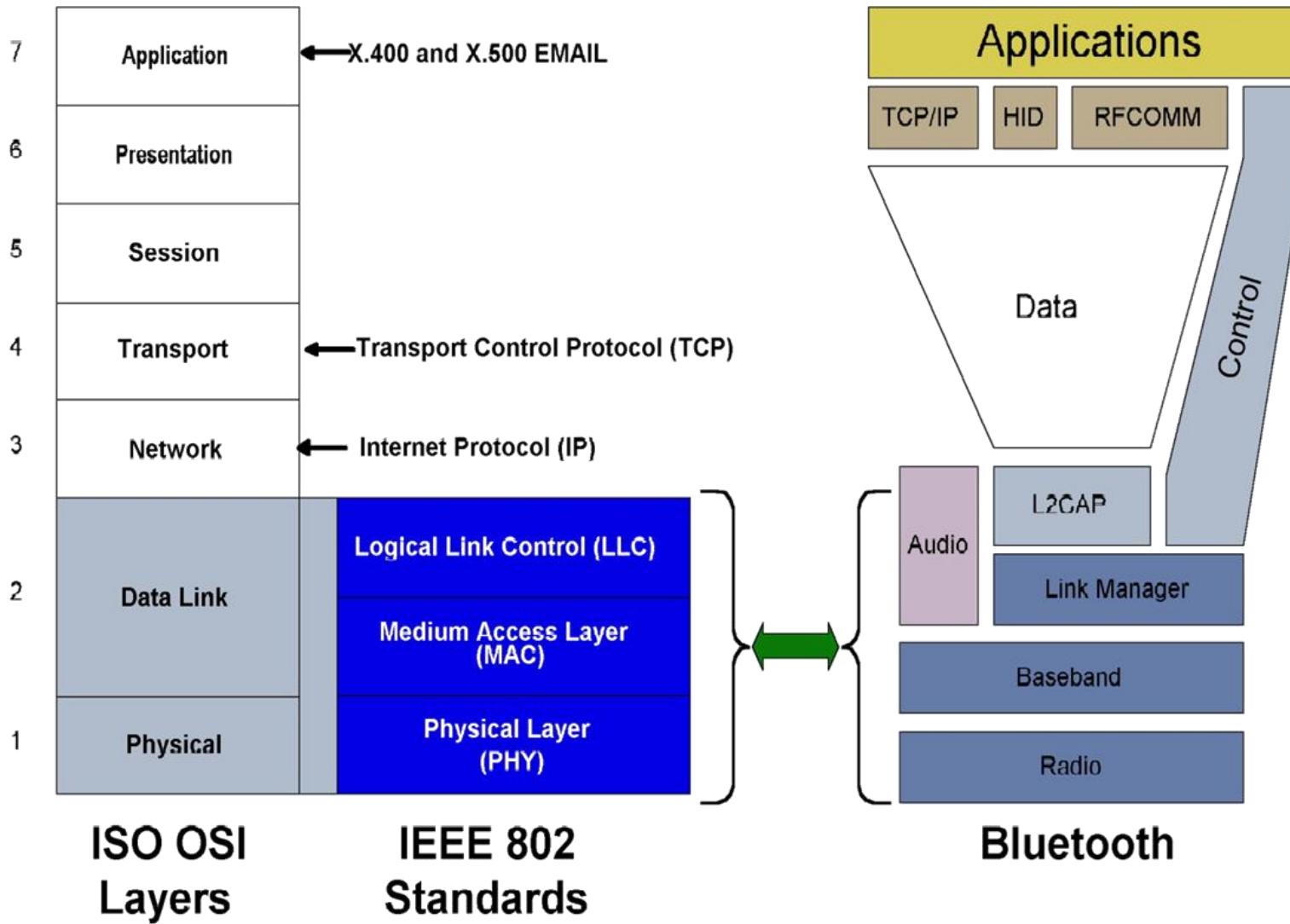
IEEE 802.15.1

- Adopted the Bluetooth MAC and PHY specifications
 - IEEE 802.15.1 and Bluetooth are almost identical regarding physical layer, baseband, link manager, logical link control and adaption protocol, and host control interface
- Range of up to 10 meters, uses FH-SS
- Data transfer rates of up to 1 Mbps
 - And higher for newer versions
- Not designed to carry heavy traffic loads
- Defines:
 - PAN Profile
 - PAN Testing profile
 - New stack layer

Bluetooth Network Encapsulation Protocol (BNEP)



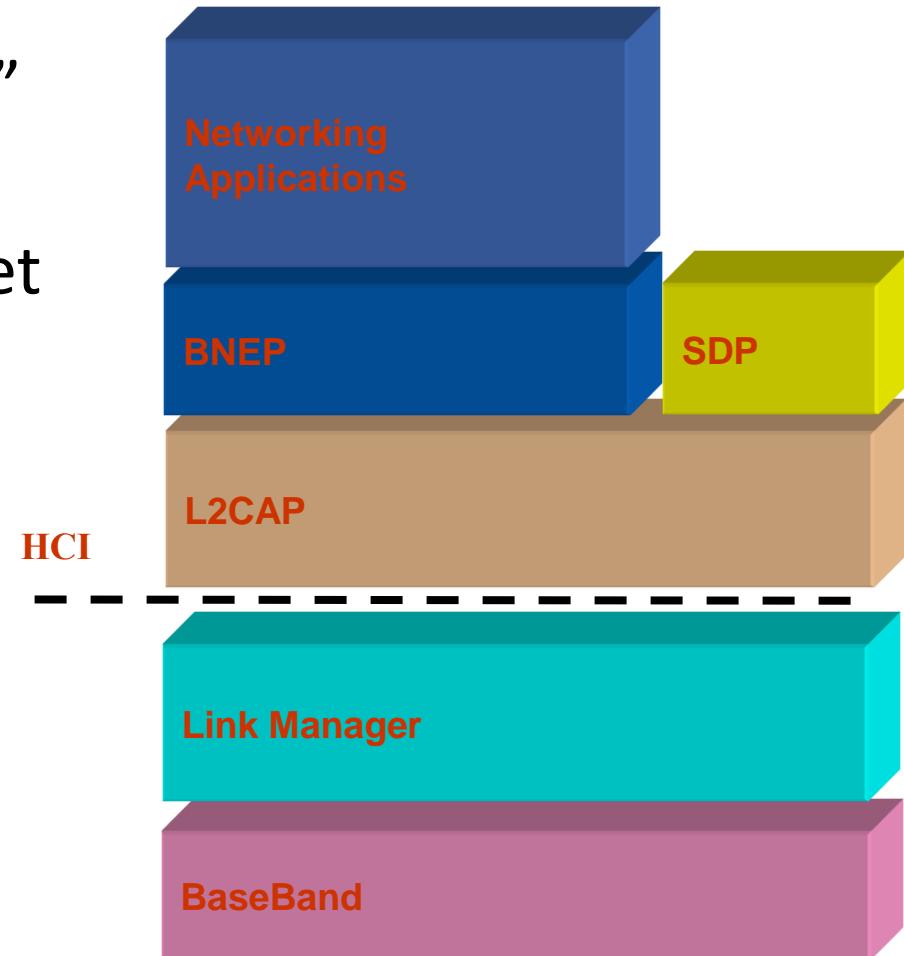
IEEE 802.15 and Bluetooth SIG





Bluetooth Networking Encapsulation Protocol

- Provides an “Ethernet alike” environment
- Supports all type of Ethernet communications
- Deployes header compressions
- Implements packet filtering
- Implements an extension header





BNEP – Why?

- Supports all network protocols (IPV4, v6, e.g.)
 - LAN access from SIG (PPP) does not scale...
- Allows establishment of peer-to-peer, hiding the notion Master-Slave of Bluetooth
- All IETF protocols should work with 802.15.1 with BNEP
- Re-use all existing network applications
- Solution similar to those in other networks (802.11)
- Keep uniform bridge support inside IEEE
- **Cost:**
 - Small overhead, balanced by header compression



WiFi vs. Bluetooth

	Bluetooth	Wifi
Specifications authority	Bluetooth SIG	IEEE, WECA
Year of development	1994	1991
Bandwidth	Low (800 Kbps)	High (11 Mbps)
Hardware requirement	Bluetooth adaptor on all the devices connecting with each other	Wireless adaptors on all the devices of the network, a wireless router and/or wireless access points
Cost	Low	High
Power Consumption	Low	High
Frequency	2.4 GHz	2.4 GHz
Security	It is less secure	It is more secure
Range	10 meters	100 meters
Primary Devices	Mobile phones, mouse, keyboards, office and industrial automation devices	Notebook computers, desktop computers, servers
Ease of Use	Fairly simple to use. Can be used to connect upto seven devices at a time. It is easy to switch between devices or find and connect to any device.	It is more complex and requires configuration of hardware and software.



Bluetooth Spec Evolution (BT classic)

Specifications	1.1	1.2	2.0 + EDR	2.1 + EDR	3.0 +HS	4.0
Adopted	2002	2005	2004	2007	2009	2010
Transmission Rate	723.1 kbps	723.1 kbps	2.1 Mbps	3 Mbps	24 Mbps	25 Mbps
Standard PAN Range	10 m	10 m	10 m	10 m	10 m	50 m
Improved Pairing (without a PIN)				Yes	Yes	Yes
Improved Security		Yes	Yes	Yes	Yes	Yes
NFC Support			Yes	Yes	Yes	Yes
Voice Dialing	Yes	Yes	Yes	Yes	Yes	Yes
Call Mute	Yes	Yes	Yes	Yes	Yes	Yes
Last-Number Redial	Yes	Yes	Yes	Yes	Yes	Yes
Fast Transmission Speeds			Yes	Yes	Yes	Yes
Lower Power Consumption			Yes	Yes	Yes	Yes
Bluetooth Low Energy						Yes



Bluetooth 4.0: Low Energy





What are the USE CASES for BT 4.0?

- Proximity
- Time
- Emergency
- Network availability
- Personal User Interface
- Simple remote control
- Browse over Bluetooth
- Temperature Sensor
- Humidity Sensor
- HVAC
- Generic I/O (automation)
- Battery status
- Heart rate monitor
- Physical activity monitor
- Blood glucose monitor
- Cycling sensors
- Pulse Oximeter
- Body thermometer



Short range wireless application areas

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS	x	y	y	x	x
Bluetooth SCO/esCO	y	x	x	x	x
Bluetooth low energy (BLE)	x	x	x	x	y
Wi-Fi	(VoIP)	y	y	y	x
Wi-Fi Direct	y	y	y	x	x
ZigBee	x	x	x	x	y

State =
low bandwidth, average/low latency data

Low Power



How much energy does traditional Bluetooth use?

- Traditional Bluetooth is *connection oriented*. When a device is connected, a link is maintained, even if there is no data flowing.
- Sniff modes allow devices to sleep, reducing power consumption to give months of battery life
- Peak transmit current is typically around 25mA
- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for **coin cells** and energy harvesting applications



What is Bluetooth Low Energy?

- Bluetooth low energy is a open, short range radio technology
 - Blank sheet of paper design
 - Different to Bluetooth classic (BR/EDR)
 - Optimized for ultra low power
 - Enable coin cell battery use cases
 - < 20mA peak current
 - < 5 uA average current





Basic Concepts of Bluetooth 4.0

- Everything is optimized for lowest power consumption
 - Short packets reduce TX peak current
 - Short packets reduce RX time
 - Less RF channels to improve discovery and connection time
 - Simple state machine
 - Single protocol
 - Etc.



Bluetooth low energy factsheet

Range:	~ 150 meters open field
Output Power:	~ 10 mW (10dBm)
Max Current:	~ 15 mA
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current:	~ 1µA
Modes:	Broadcast, Connection, Event Data Models, Reads, Writes



Designed for exposing state

23.2°C

3.2 kWh

12:23 pm

PLAY >>

Gate 10
BOARDING

- **Data Throughput**

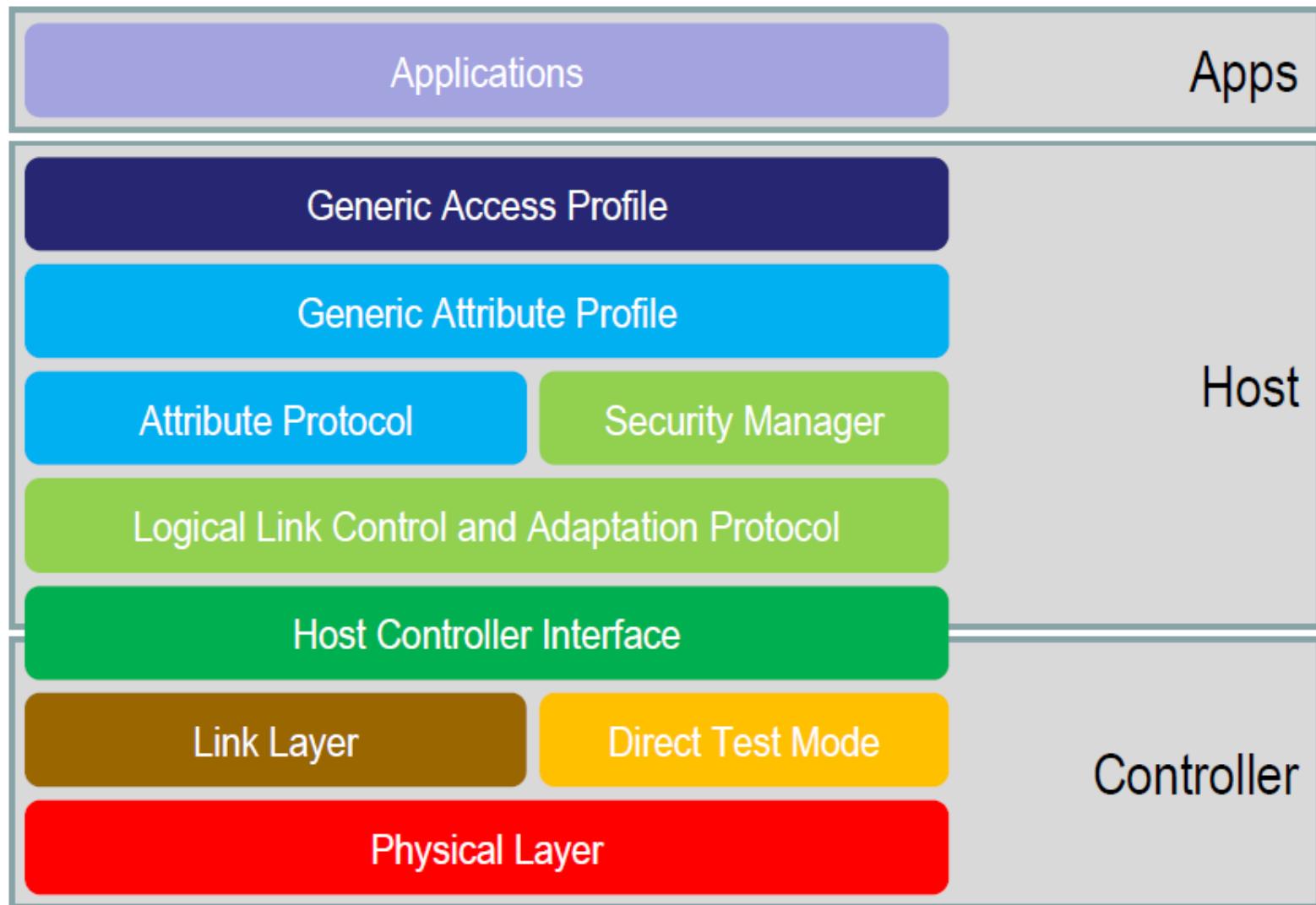
- Data throughput is not a meaningful parameter. It does not support streaming.
- Data rate (typical) = 1Mbps, but is not optimized for file transfer.
- Designed for **sending small chunks of data** (exposing state)
 - It's good at small, discrete data transfers.
 - Data can triggered by local events.
 - Data can be read at any time by a client.
 - Interface model is very simple (GATT)

60.5 km/h

Network
Available



Bluetooth Low Energy Architecture





Device Modes

- Dual Mode
 - Bluetooth BR/EDR and LE
 - BR – Basic Rate
 - EDR – Enhanced Data Rate
 - Used anywhere that BR/EDR is used today



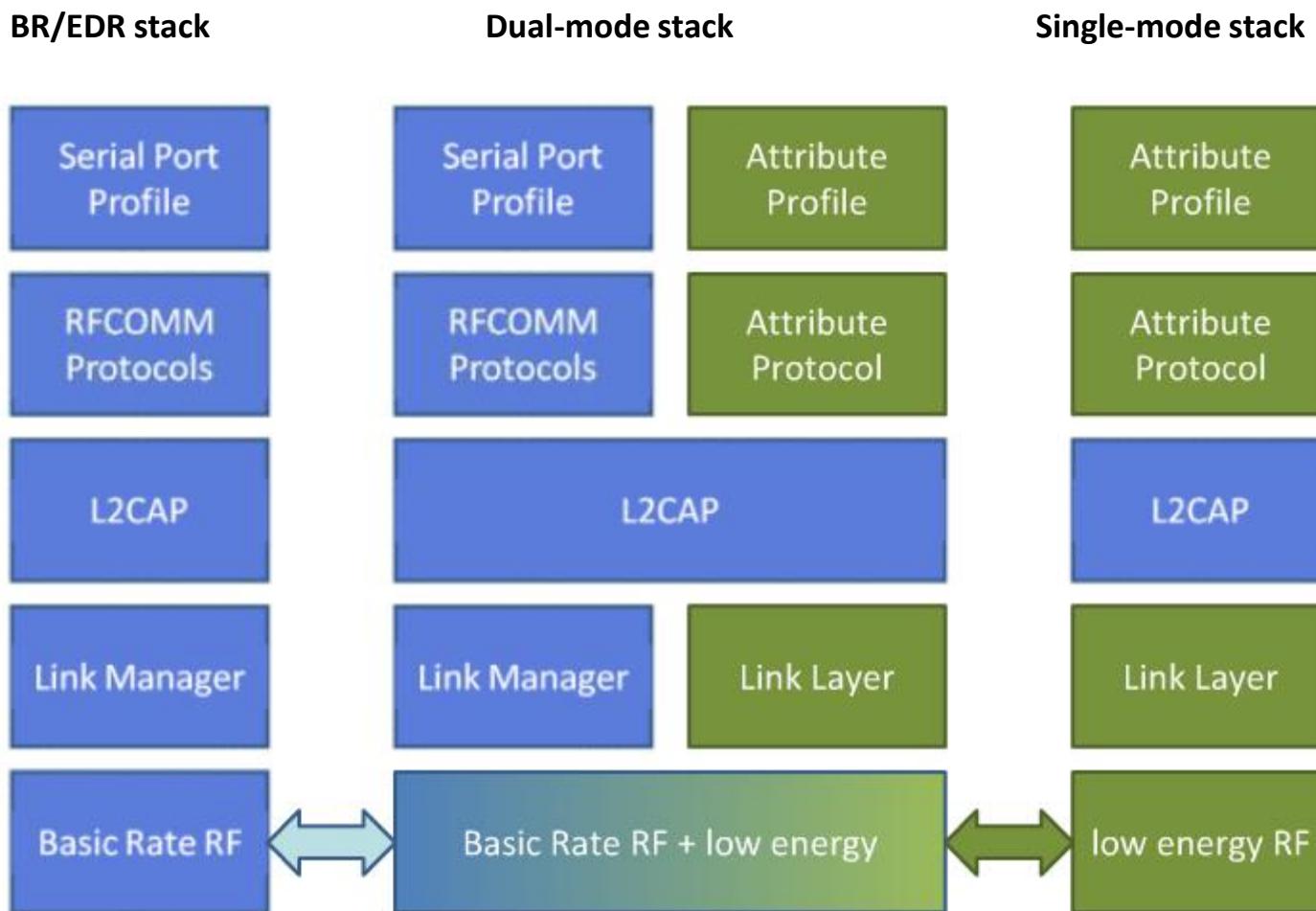
- Single Mode
 - Implements only Bluetooth low energy
 - Will be used in new devices / applications





Device Modes

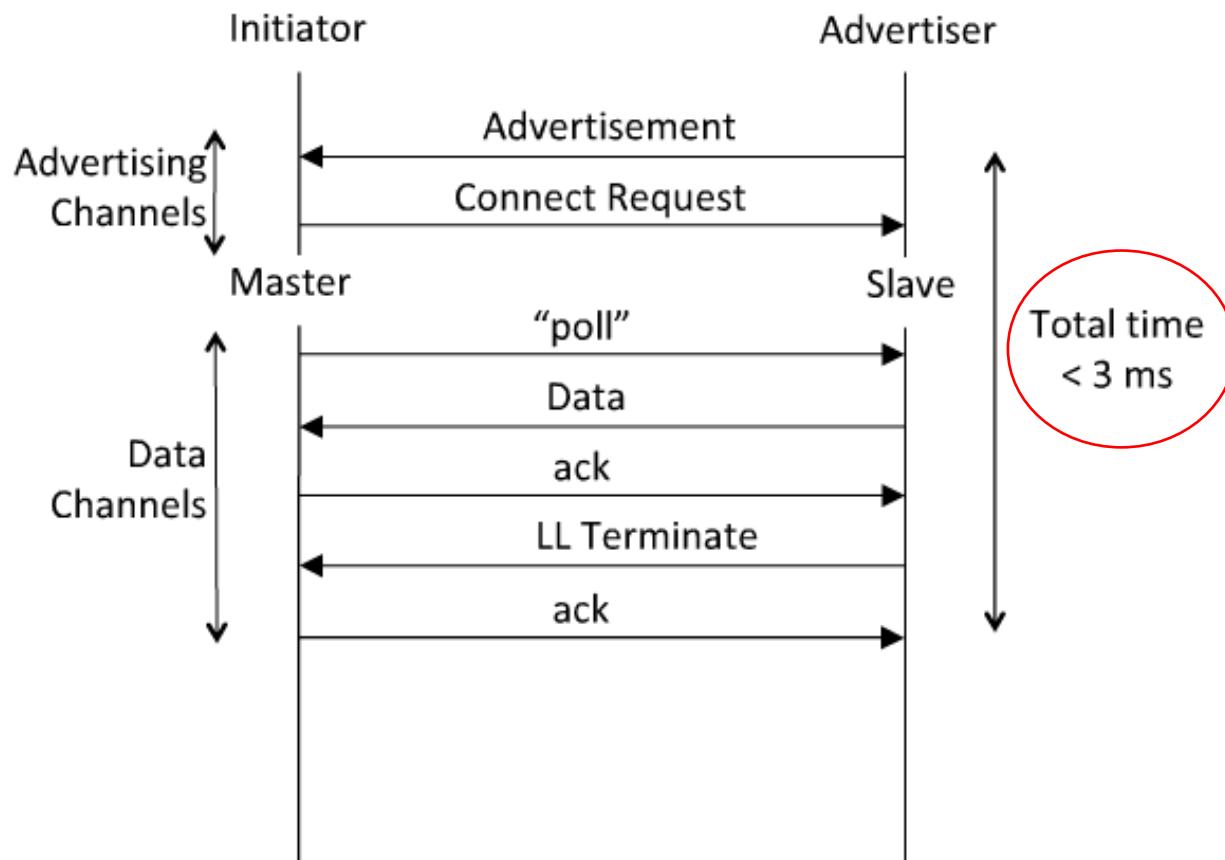
- Dual mode + single modes





Link Layer Connection

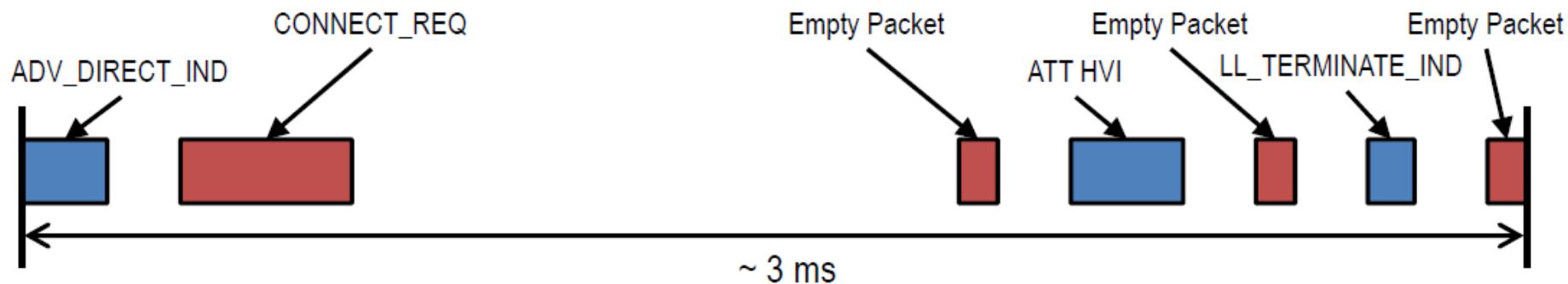
- Very low latency connection





Time From Disconnected to Data ~ 3ms

Time (us)	Master Tx	Radio Active (us)	Slave Tx
0		176	ADV_DIRECT_IND
326	CONNECT_REQ	352	
1928	Empty Packet	80	
2158		144	Attribute Protocol Handle Value Indication
2452	Empty Packet (Acknowledgement)	80	
2682		96	LL_TERMINATE_IND
2928	Empty Packet (Acknowledgement)	80	





How low can the energy get?

- From the previous slide, calculate energy per transaction
 - Assume an upper bound of 3ms per minimal transaction
 - Estimated TX power is 15mW (mostly TX power amp for 65nm chips)
 - For 1.5v battery, this is 10mA. $0.015\text{W} * 0.003\text{ sec} = 45\text{ micro Joule}$
- How long could a sensor last on a battery?
 - An example battery: Lenmar WC357, 1.55v, 180mAh, \$2-5
 - $180\text{mAh}/10\text{mA} = 18\text{Hr} = 64,800\text{ seconds} = 21.6\text{M transactions}$
 - Suppose this sensor sends a report every minute = 1440/day
 - For just the BT LE transactions, this is 15,000 days, or > 40 years
 - This far exceeds the life of the battery and/or the product
- This means that battery will cost more than the electronics
 - This sensor could run on scavenged power, e.g. ambient light



BLE and GAP

- Generic Access Profile (GAP)
 - GAP defines a base profile which all Bluetooth devices implement, which ties all the various layers together to form the basic requirements for a Bluetooth device
 - GAP also defines generic procedures for connection-related services:
 - Device Discovery
 - Link Establishment
 - Link Management
 - Link Termination
 - Initiation of security features



BLE and GAP

- The GAP layer works in one of four profile roles:
 - **Broadcaster:** an advertiser that is non-connectable
 - **Observer:** scans for advertisements, but cannot initiate connections
 - **Peripheral:** an advertiser that is connectable and can operate as a slave in a single link layer connection
 - **Central:** scans for advertisements and initiates connections; operates as a master in a single or multiple link layer connections



BLE and GAP

Temperature Sensor (Broadcaster)



Figure 1 – Temperature Sensor
(Broadcaster)



Temperature Display (Observer)

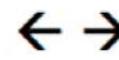


Figure 2 – Temperature Display
(Observer)

Watch (Peripheral)



Figure 3 - Watch
(Peripheral)



Mobile Phone (Central)



Figure 4 – Mobile Phone
(Central)



BLE and GAP – Discoverable Modes

- GAP supports **three** different discoverable modes:
 - **Non-discoverable Mode:** No advertisements
 - **Limited Discoverable Mode:** Device advertises for a limited amount of time before returning to the standby state
 - **General Discoverable Mode:** Devices advertises continuously
- GAP manages the data that is sent out in advertisement and scan response packets



BLE and GAP - Pairing

- Pairing can be initiated by either the central or peripheral device
- The two devices generate and exchange short-term keys (STK) which can be used to decrypt data packets
- Either device can request to enable “bonding” to create a long-term relationship between the two devices
 - A long-term key (LTK) is generated, exchanged, and stored allowing device to re-encrypt the link quickly upon re-connection, **without going through the complete pairing process once again**
 - Profile / Service configuration data is remembered, so that the user does not need to re-configure the device every time they re-connect



BLE and GAP - Pairing

- Each device also states its input/output capabilities from among these options:
 - **DisplayOnly** – no way user can input anything into device, but it can output data
 - **DisplayYesNo** – user can input “yes” or “no” but nothing else; can also display data
 - **KeyboardOnly** – user can input a password or PIN, but no display
 - **NoInputNoOutput** – device has no means for user input, and has no display
 - **KeyboardDisplay** – device has a means for display as well as for input

Wireless Sensor Networks

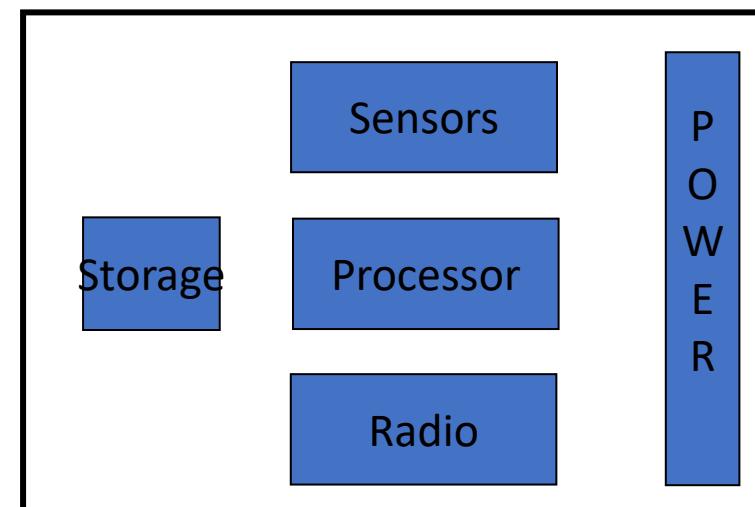
What are wireless sensor networks (WSNs)?

- A wireless sensor network (WSN) is a wireless network using sensors to cooperatively monitor physical or environmental conditions
- Networks of typically small, battery-powered, wireless devices (often MANY, sometimes heterogeneous)
 - On-board processing,
 - Communication, and
 - Sensing capabilities.

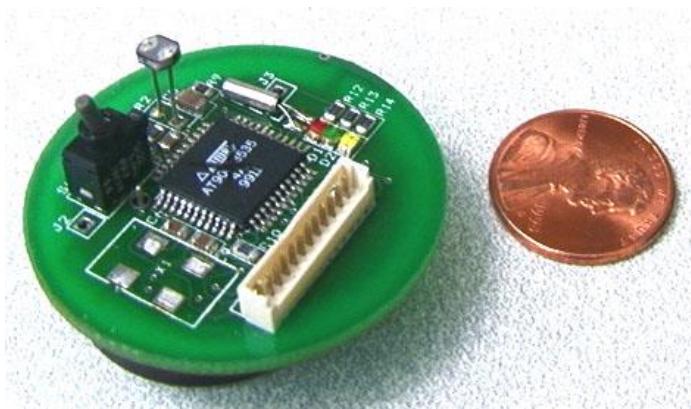
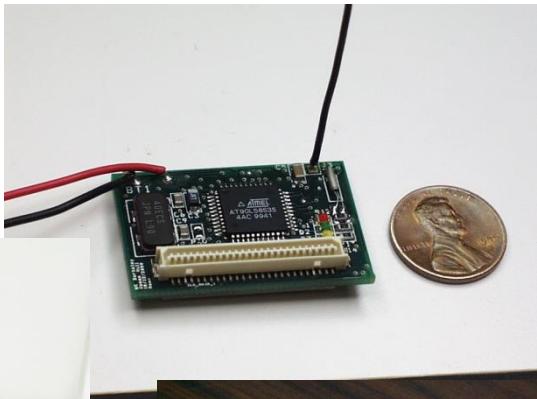
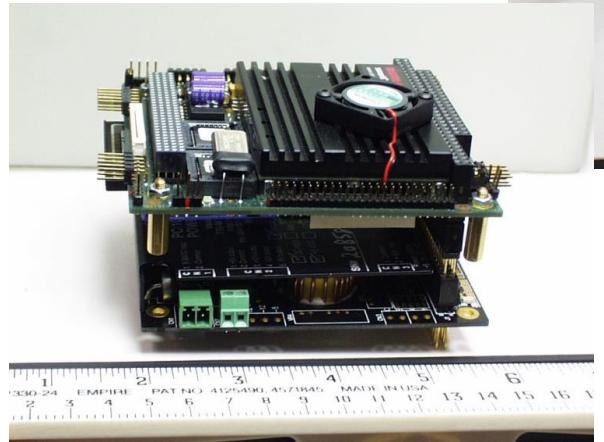
Or...

➤ Wireless sensing + Data Networking!

➤ Group of sensors linked by wireless media to perform distributed sensing tasks



Sensor Nodes and platforms



CM 22/23

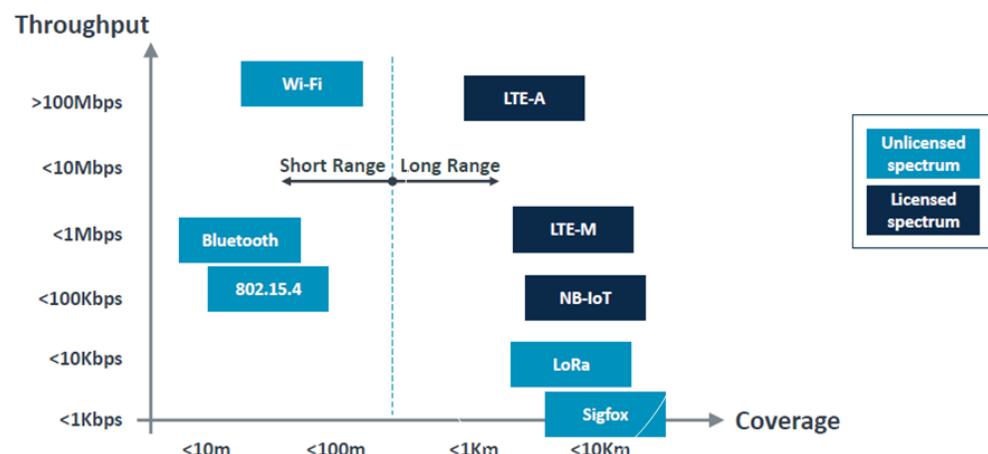


IoT Wireless Connectivity

As with wireless in general, multiple standards with different properties

IoT Wireless Connectivity Technology

Multiple standards, different attributes

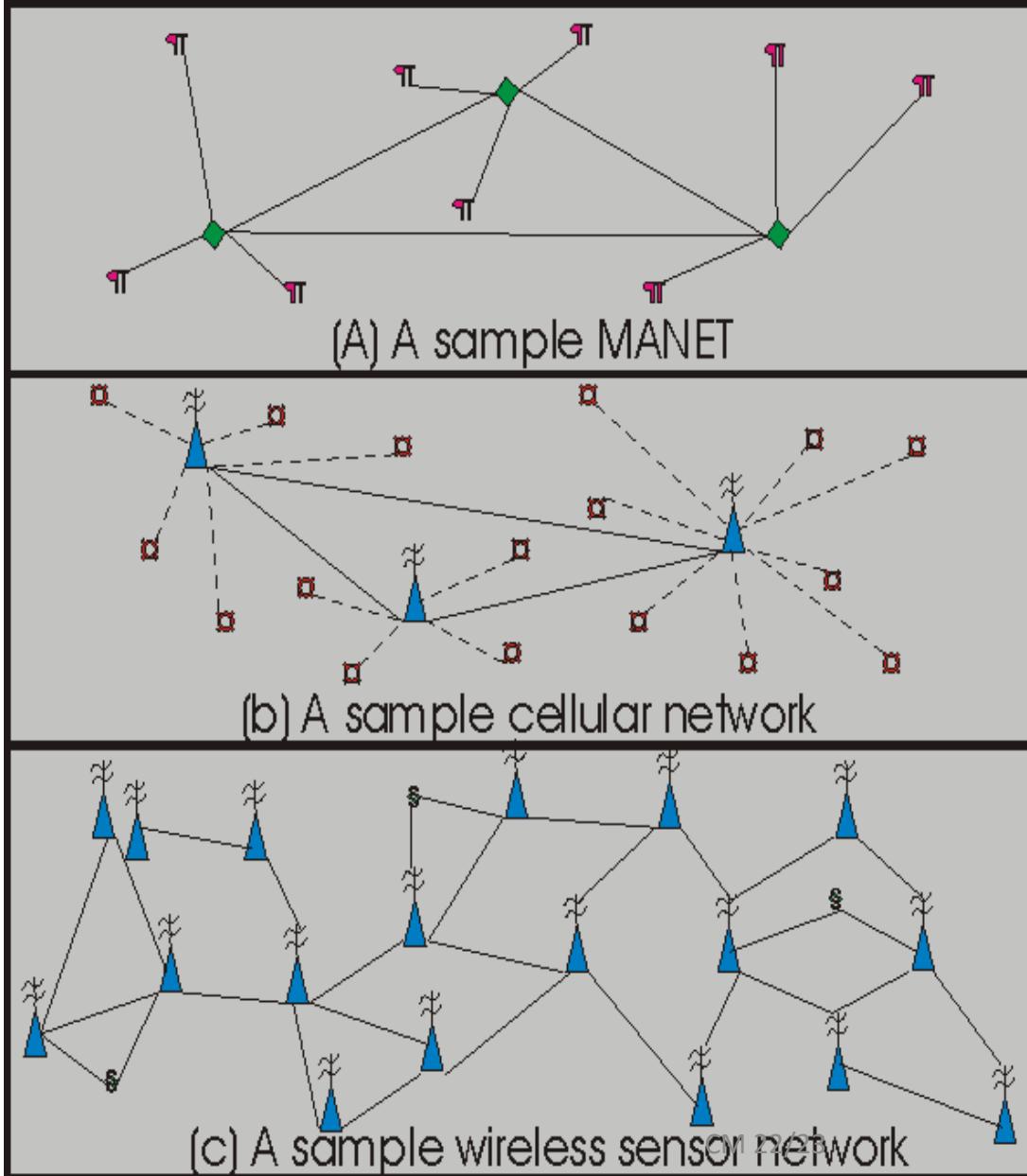


MIoT and HIoT are different

- IoT has multiple scenarios, from human-oriented to machine-oriented, and from industrial to forest environments
- WSN need to adapt to these environments.

	Manufacturing IoT	Consumer IoT
Goal	Manufacturing-industry Centric	Consumer Centric
Devices	Machines, Sensors, Controllers, Actuators, Smart meters	Consumer devices and Smart appliances
Working Environment	Harsh (vibration, noisy, extremely high/low temperature)	Moderate
Data rate	High (usually)	Low or average
Delay	Delay sensitive	Delay tolerant
Mission	Mission-critical	Non-mission-critical

Types of wireless Networks

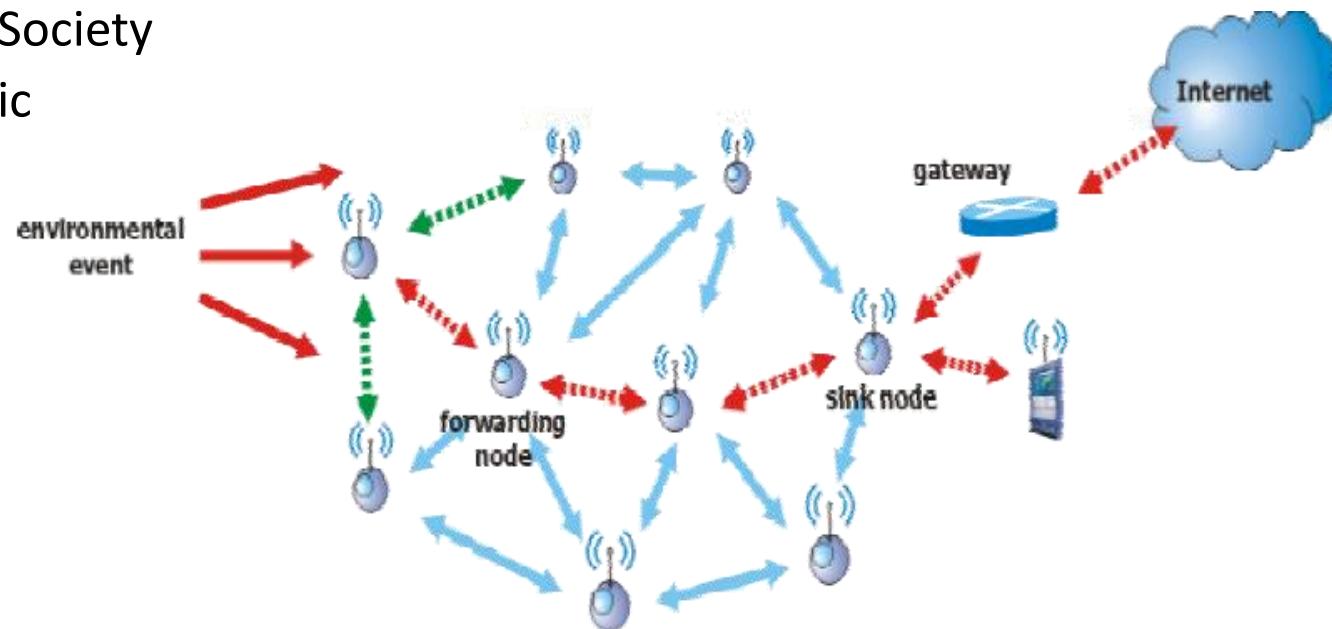


MANET – Mobile Ad-hoc network

WSN can explore the architecture and protocol concepts both of MANETs (mobile ad-hoc networks) and of cellular networks.

Wireless Sensor Network

- Focus on:
 - Ubiquitous Computing
 - Ubiquitous Network Society
 - (often) Human-centric
- **Ubiquitous**
 - Anytime
 - Anyone
 - Anywhere
 - Any Device
 - Affordable
 - All Security
 - Any Information/Service



MAC: challenges for wireless networking

- MAC is a critical layer for networking
- Traditional problems
 - Fairness
 - Latency
 - Throughput
- For Sensor Networks, more problems are added
 - Power efficiency
 - Scalability

MAC challenges for WSN

- Sensor networks are deployed in an ad hoc fashion, with individual nodes remaining largely **inactive for long periods of time**, but then becoming **suddenly active** when something is detected.
- These characteristics of sensor networks and applications motivate a MAC that is different from traditional wireless MACs :
 - **Energy conservation** and **self-configuration** are primary goals.
 - Per-node fairness and latency are less important.

Challenges in WSN's

- Energy and Power Consumption
- Self-organization
- Communication Heterogeneity
- Adaptability
- Security
- Scalability

Design Challenges

Why are WSNs challenging/unique?

- Typically, severely energy constrained.
 - Limited energy sources (e.g., batteries).
 - Trade-off between performance and lifetime.
- Self-organizing and self-healing.
 - Remote deployments.
- Scalable.
 - Arbitrarily large number of nodes.

Design Challenges

- Heterogeneity.
 - Devices with varied capabilities.
 - Different sensors.
 - Hierarchical deployments.
- Adaptability.
 - Adjust to operating conditions and changes in application requirements.
- Security and privacy.
 - Potentially sensitive information.
 - Hostile environments.

Sensor Network MAC Protocols

- The major sources of energy wastage are:

- Collisions – *interfering packets*
- Overhearing – *hearing more than required from a packet*
- Control packet overhead – *control versus data*
- Idle listening – *hearing for nothing*

Typical solutions in wireless MACs ([Homework: compare with WiFi](#))

- Carrier Sensing
 - Only during low traffic load.
- Contention
 - RTS-CTS only during high traffic load.
- Backoff
 - Backoff in application layer is desired other than in MAC layer.

Achieving good scalability and collision avoidance capability is necessary.

Challenges

1. Energy Efficiency:

- Sensor nodes are not connected to any energy source.
- Energy efficiency is a dominant consideration no matter what the problem is.
- Many solutions, both hardware and software related, have been proposed to optimize energy usage.

2. Ad hoc deployment (adaptability):

- Most sensor nodes are deployed in regions which have no infrastructure.
- We must cope with the changes of connectivity and distribution.

Challenges

3. Unattended operation:

- Generally, once sensors are deployed, there is no human intervention for a long time.
- Sensor network must reconfigure by itself when certain errors occur.

4. Dynamic changes (self-healing and scalability)

- As changes of connectivity due to addition of more nodes or failure of nodes, Sensor network must be able to adapt itself to changing connectivity, to arbitrary large numbers of nodes

5. Security

- Both Sensors and Actuators carry sensitive information in an hostile environment

Sensor-MAC (S-MAC)

- S-MAC is a medium-access control (MAC) protocol designed for wireless sensor networks.
 - Explores typical solutions also found in many other sensor MACs.
 - **Nodes periodically sleep, and sleep during other nodes' transmissions**
 - Nearby nodes form virtual clusters to synchronize their wake-up and sleep periods
 - Trades **energy efficiency for lower throughput and higher latency**
 - Message passing is used to reduce the contention latency and control overhead



802.15.4 and Zigbee

What is ZigBee?

- Technological Standard Created for Control and Sensor Networks
 - Based on the IEEE 802.15.4 Standard
 - Centered in small radios
- Created by the ZigBee Alliance
 - 200+ members
- History
 - *May 2003: IEEE 802.15.4 completed*
 - December 2004: ZigBee specification ratified
 - June 2005: public availability

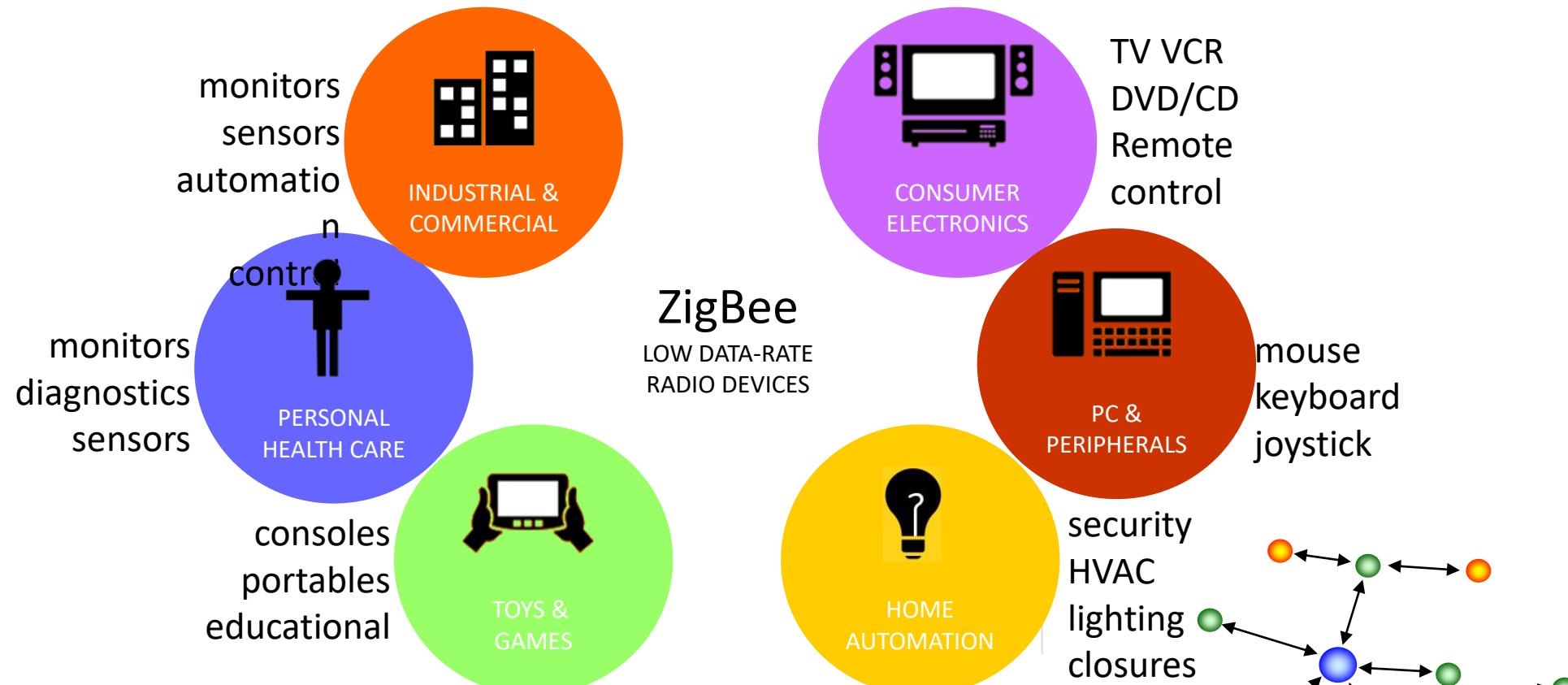
What Does ZigBee Do?

- Designed for wireless controls and sensors
 - Operates in Personal Area Networks (PAN's) and device-to-device networks
 - Connectivity between small packet devices
 - Examples: control of lights, switches, thermostats, appliances, etc.

Zigbee?

- Named for erratic, zig-zagging patterns of bees between flowers
- Symbolizes communication between nodes in a mesh network
- Network components “seen as analogous” to queen bee, drones, worker bees

ZigBee network applications



- Just everything you can imagine for wireless sensor nodes or in general short range communications

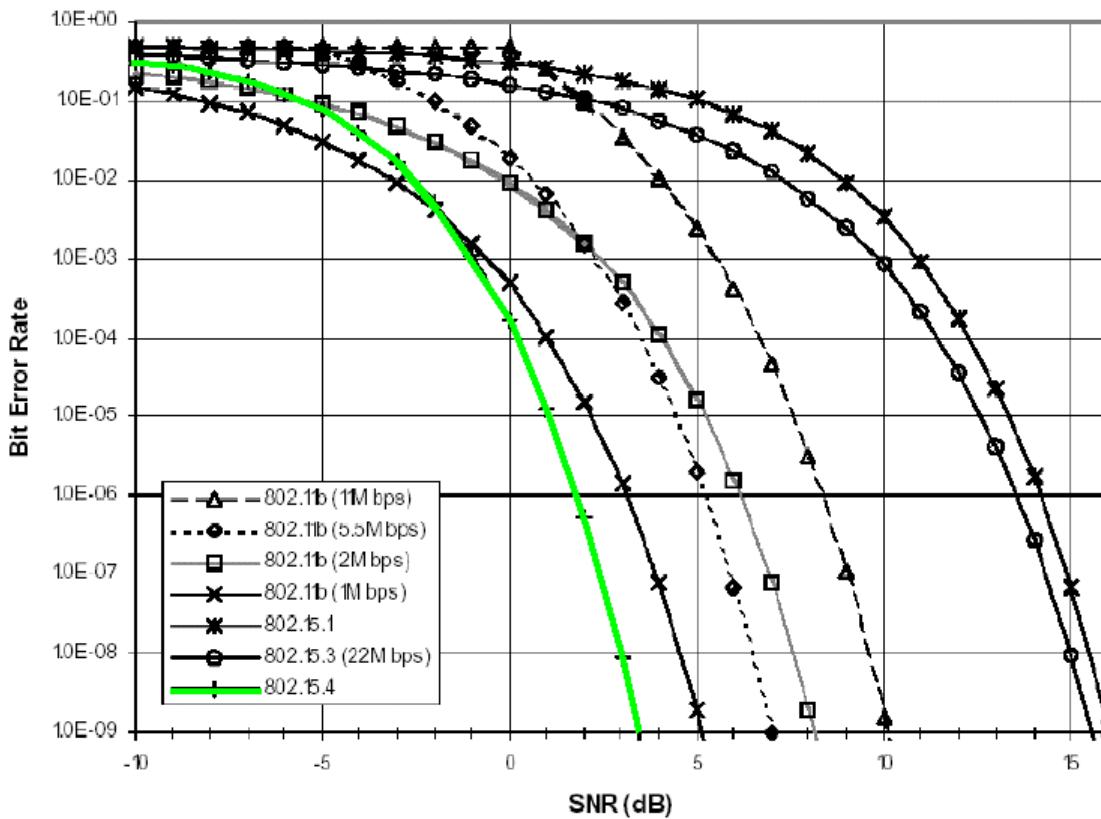
ZigBee and Other Wireless Technologies

Market Name	ZigBee™	---	Wi-Fi™	Bluetooth™
Standard	802.15.4	GSM/GPRS CDMA1xRTT	802.11b	802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - .5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

Why do we need another “WPAN” standard?

- Power consumption
 - ZigBee: 10mA <==> BT: 100mA
- Production costs
 - ZigBee: 1.1 \$ <==> BT: 3 \$
- Development costs
 - Codesize ZB/codesize BT = $\frac{1}{2}$
- Bit-error-rate (BER)
- Sensitivity
- flexibility
 - No. of supported nodes
 - ZigBee: 65536 (in a mesh) <==> BT: 7
- Security
- Latency requirements
- Range
 - ZigBee: up to 75 m in LOS condition <==> BT: 10 m

802.11b, 802.15.x BER Comparison

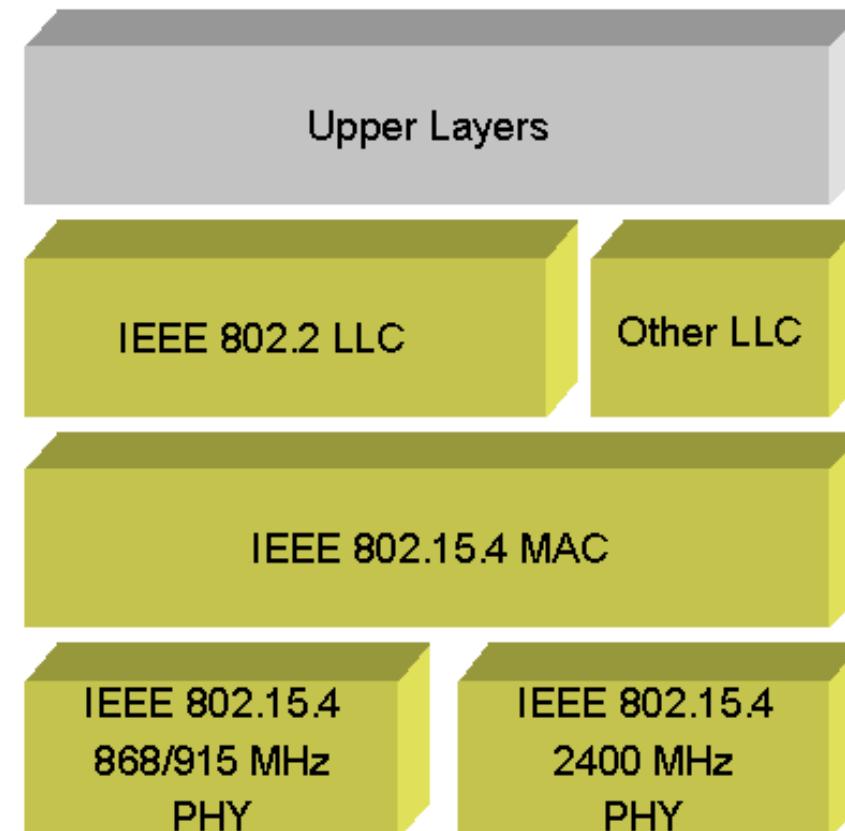


ZigBee/IEEE 802.15.4 features

- Low power consumption
- Low cost
- Small packet
- Low offered message throughput
- Supports large network orders ($\leq 65k$ nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications

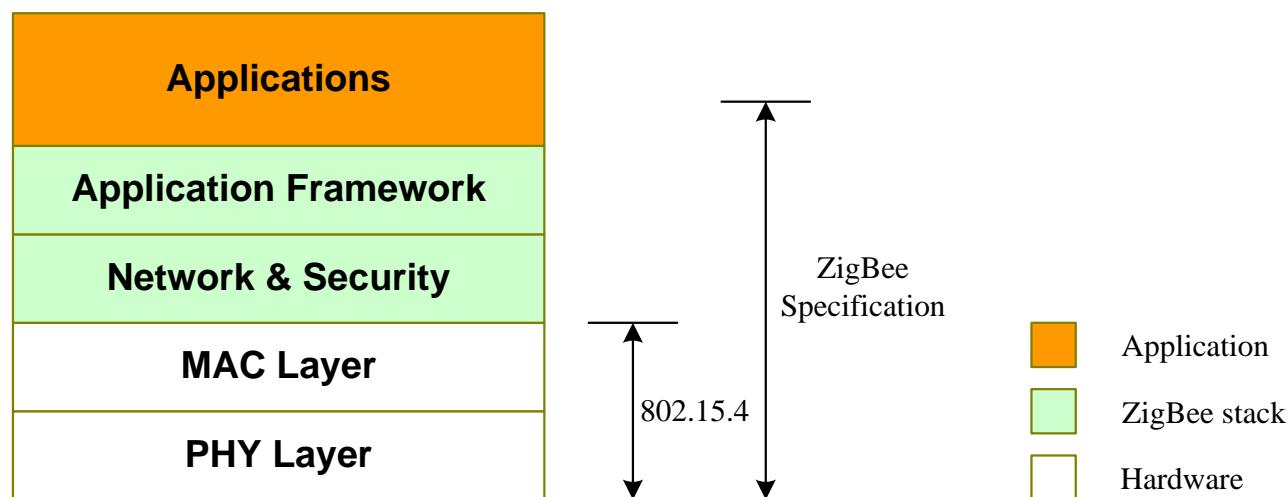
IEEE 802.15.4 - Overview

- Low Rate WPAN (LR-WPAN)
 - E.g. Sensor networks
- Simple and low cost
 - Fully handshake protocol
- Low power consumption
 - Years on lifetime using standard batteries
- Different topologies
 - Star, peer-to-peer, combined
- Data rates: 20-250 kbps
 - Low latency support
- Operates at different frequencies
 - 868 Mhz, 915 Mhz, 2.4 GHz

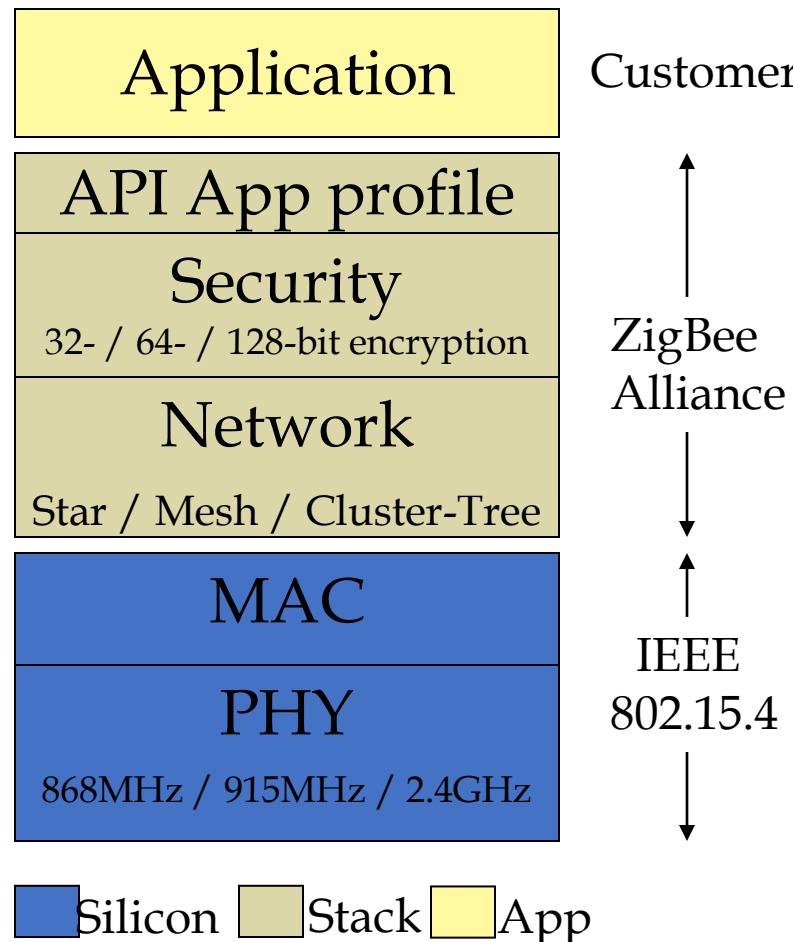


ZigBee/802.15.4 architecture

- ZigBee Alliance
 - Companies: semiconductor manufacturers, IP providers, OEMs, etc.
 - Defining upper layers of protocol stack: from network to application, including application profiles
 - First profiles published mid 2003
- IEEE 802.15.4 Working Group
 - Defining lower layers of protocol stack: MAC and PHY



IEEE 802.15.4 & ZigBee In Context



ZigBee Alliance

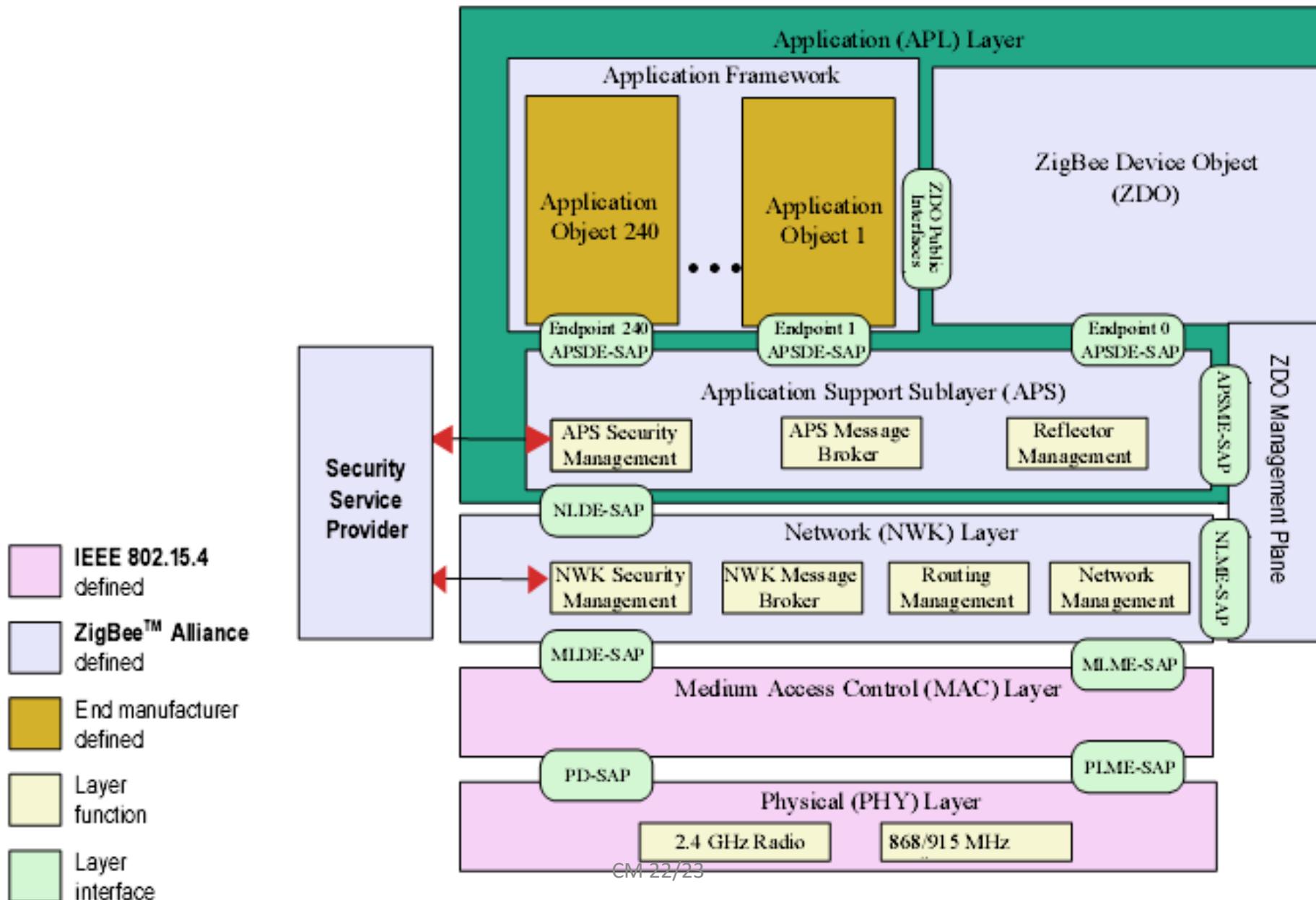
- “the software”
- Network, Security & Application layers
- Brand management

IEEE 802.15.4

- “the hardware”
- Physical & Media Access Control layers

Source: http://www.zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt

Protocol Stack



How ZigBee Works

- Topology
 - Star
 - Cluster Tree
 - Mesh
- Network coordinator, routers, end devices
- 2 or more devices form a PAN/WSN

How ZigBee Works

- States of operation
 - Active
 - Sleep
- Devices
 - Full Function Devices (FFD's)
 - Reduced Function Devices (RFD's)
- Modes of operation
 - Beacon
 - Non-beacon
- Traffic types
 - Intermittent
 - Repetitive
 - Periodic

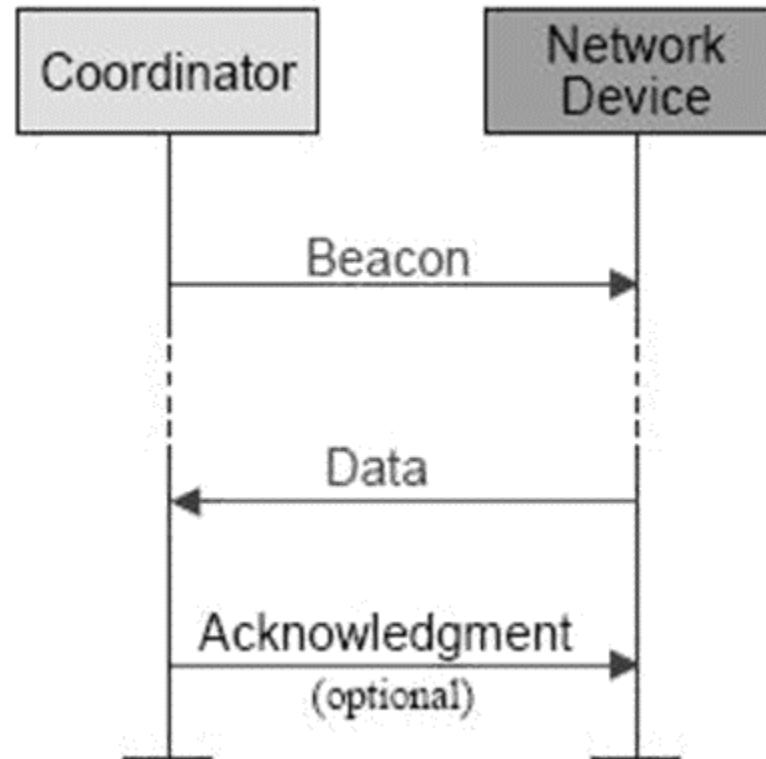
Traffic-Types

- Data is periodic
 - application dictates rate (e.g. sensors)
- Data is intermittent
 - application or stimulus dictates rate (optimum power savings), e.g. light switch
- Data is repetitive (fixed rate a priori)
 - device gets guaranteed time slot (e.g. heart monitor)

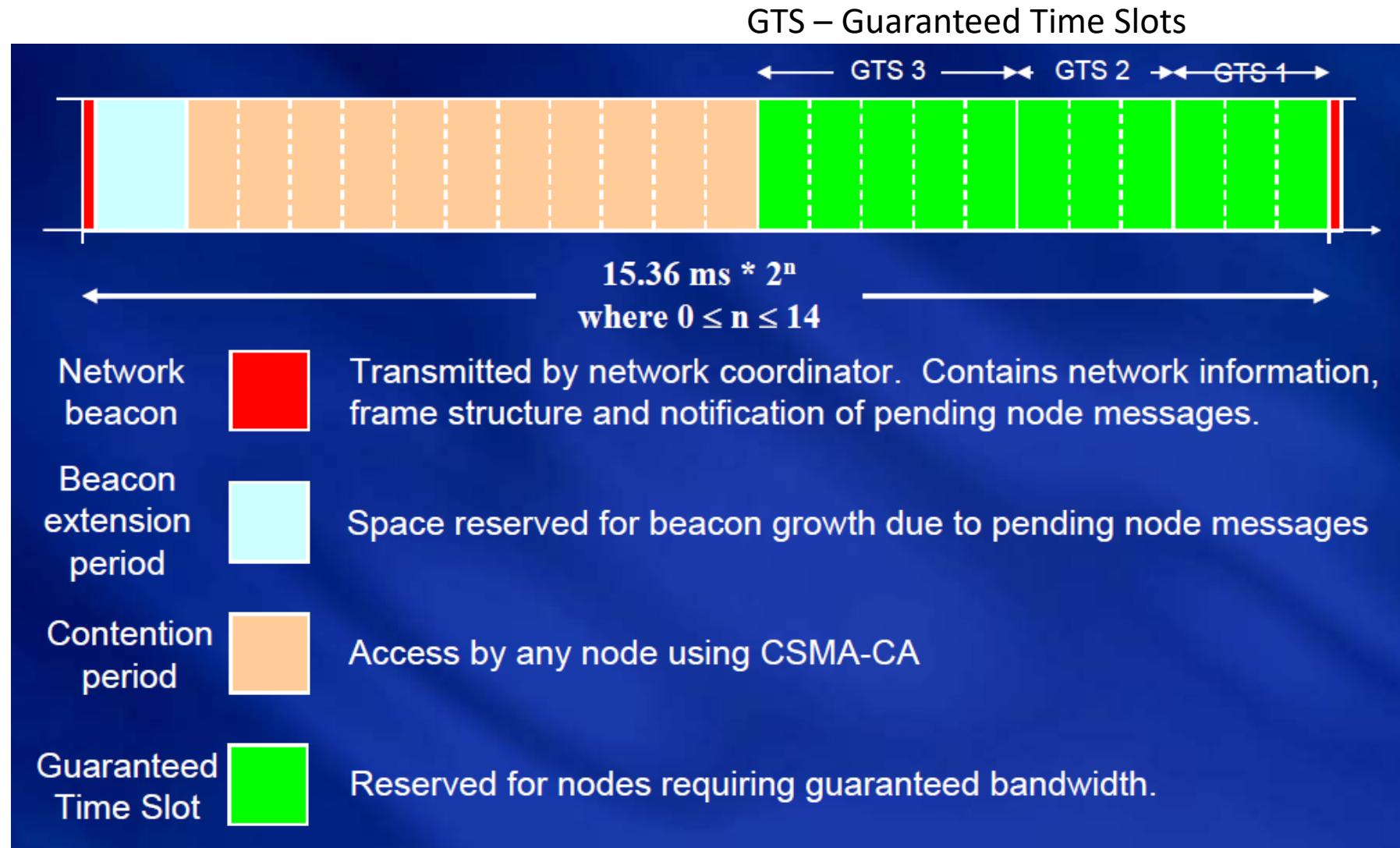
Traffic-Modes

Beacon mode:

- beacon sent periodically
- Coordinator and end device can go to power save
- Lowest energy consumption
- Precise timing needed
- Beacon period (ms-m)



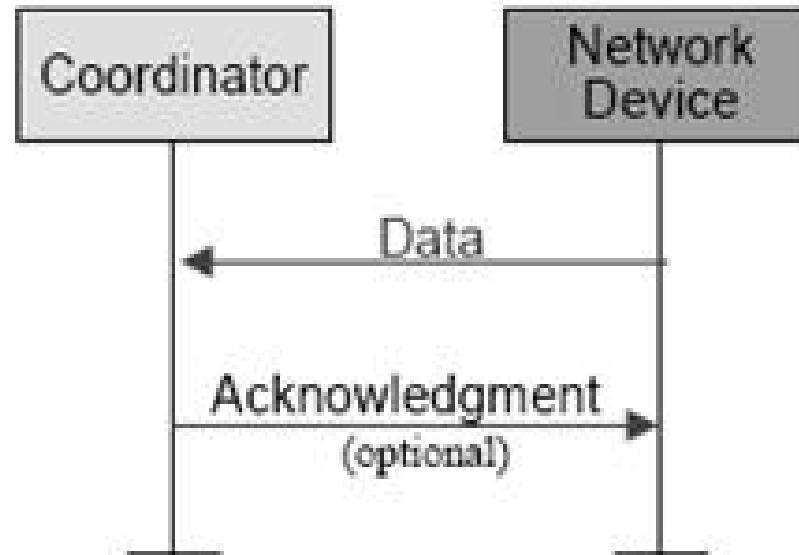
Beacon Mode



Traffic-Modes

Non-Beacon mode:

- coordinator/routers have to stay awake
(robust power supply needed)
- heterogeneous network
- asymmetric power



ZigBee Node-Types

ZigBee Coordinator (ZBC) (IEEE 802.15.4 FFD)

- only one in a network
- initiates network
- stores information about the network
- all devices communicate with the ZBC
- routing functionality
- bridge to other networks

ZigBee Router (ZBR) (IEEE 802.15.4 FFD)

- optional component
- routes between nodes, network backbone
- extends network coverage
- manages local address allocation/de-allocation

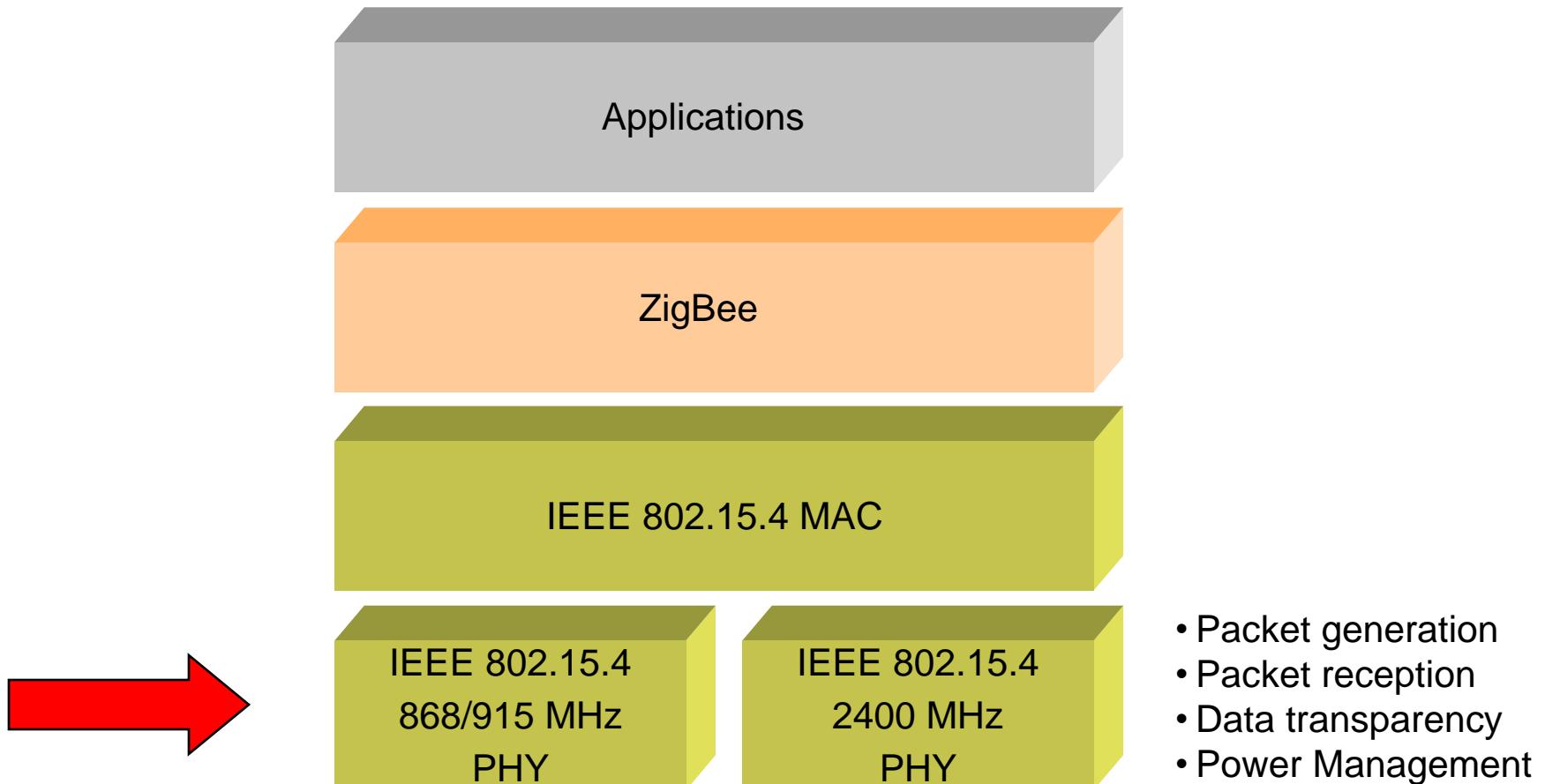
ZigBee End Device (ZBE) (IEEE 802.15.4 RFD)

- optimized for low power consumption
- cheapest device type
 - sensor would be deployed here



Remember:
FFD – Full Function Device
RFD – Reduced Function Device

802.15.4 / ZigBee Architecture



IEEE 802.15.4 basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
 - Channel Access is via **Carrier Sense Multiple Access with collision avoidance** and optional time slotting
 - Message acknowledgement and an optional beacon structure
 - Multi-level security
 - Works well for
 - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
 - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries

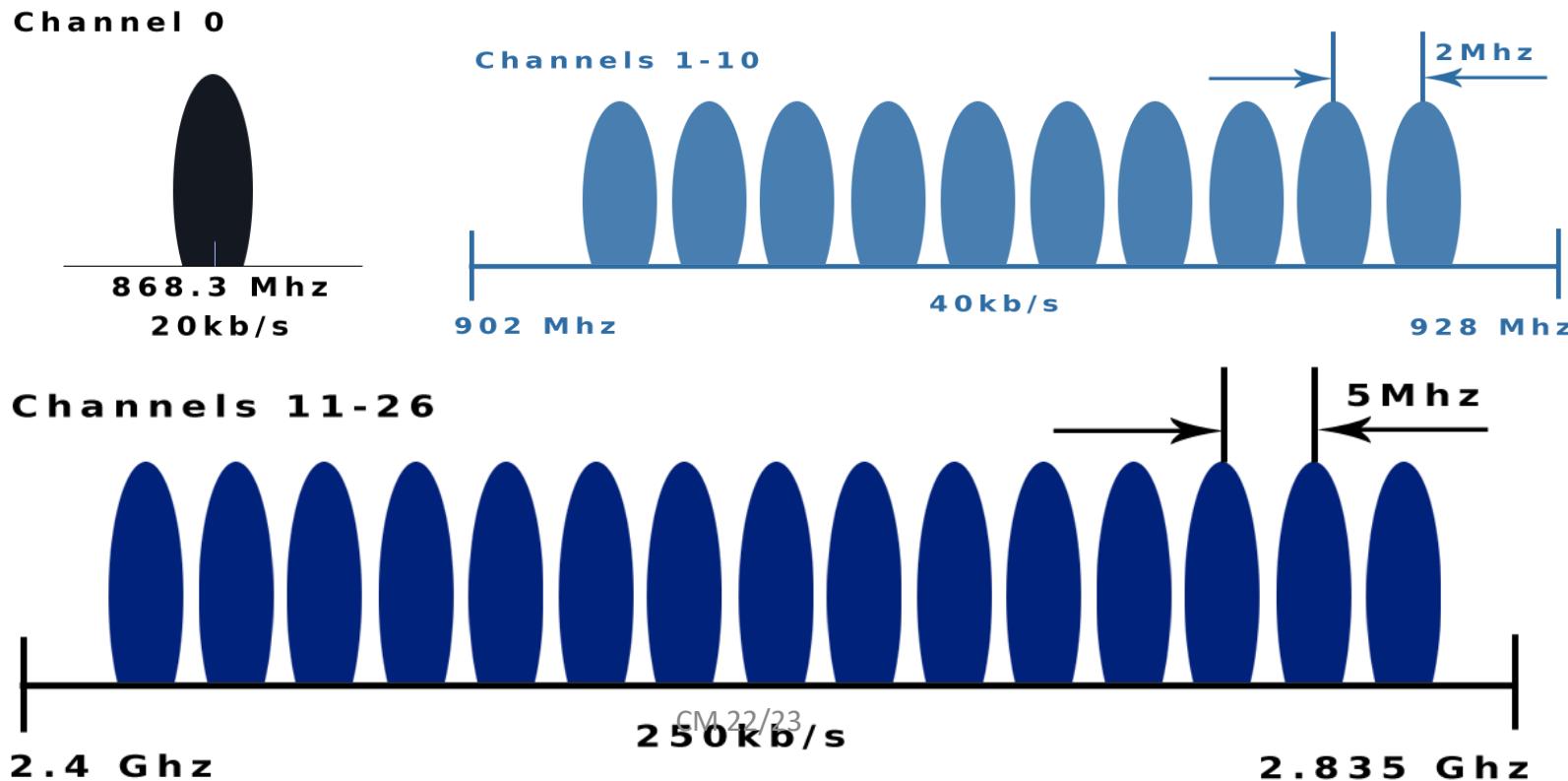
802.15.4 General characteristics

- Data rates of 250 kbps , 20 kbps and 40kbps.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access, with CCA detection
 - Clear Channel Assessment
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- 16 channels in the 2.4GHz ISM band
- 10 channels in the 915MHz ISM band
- one channel in the European 868MHz band.
- Extremely low duty-cycle (<0.1%)

802.15.4 frequency bands

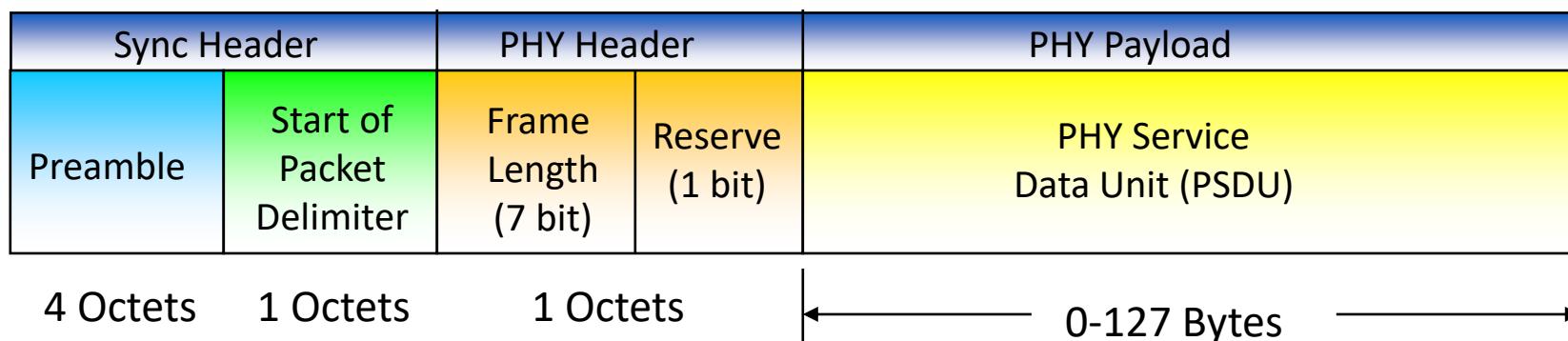
Operates in Unlicensed Bands

- ISM 2.4 GHz Global Band at 250kbps
- 868 MHz European Band at 20kbps
- 915 MHz North American Band at 40kbps

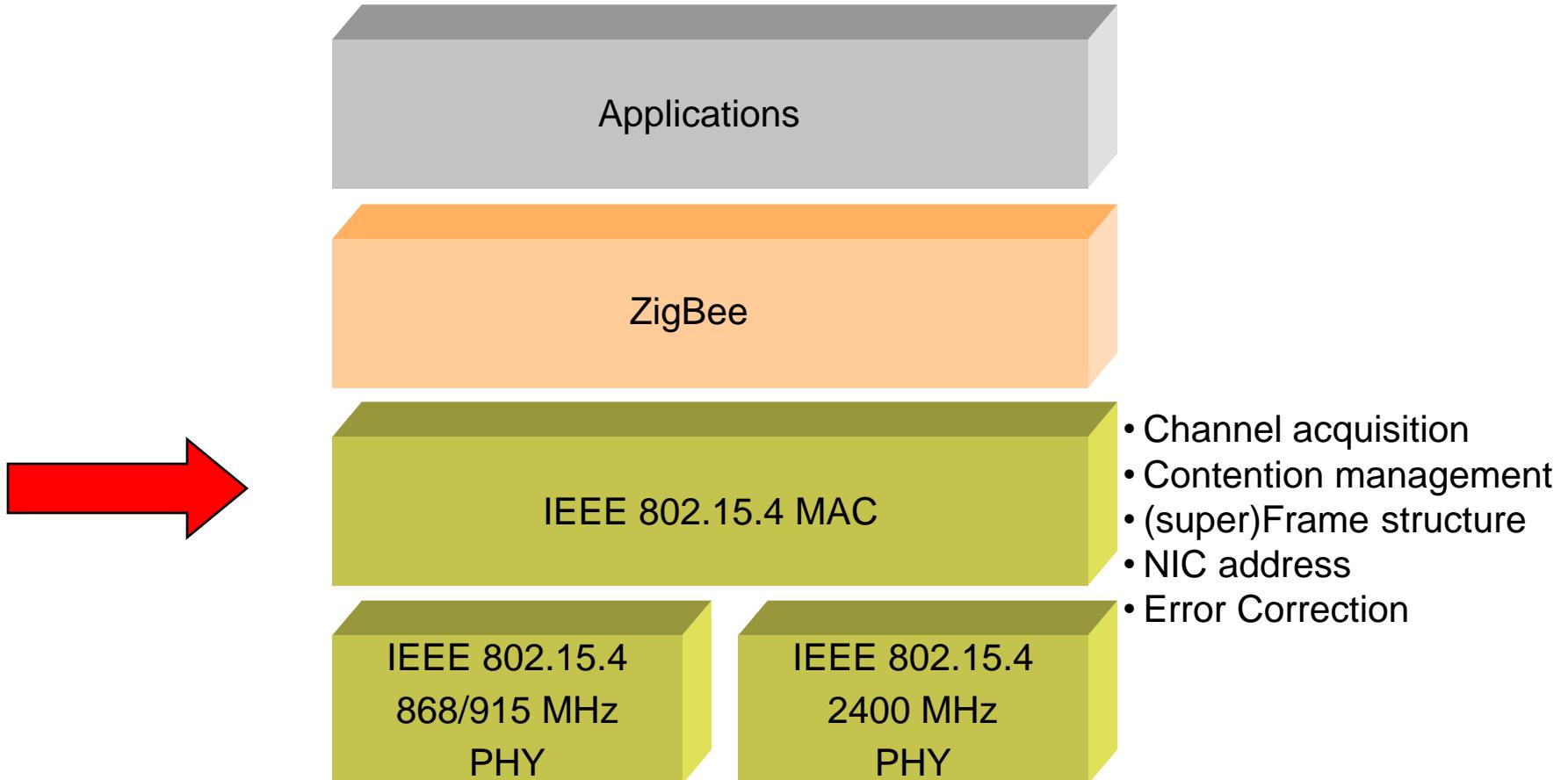


PHY frame structure

- PHY packet fields
 - Preamble (32 bits) – synchronization
 - Start of packet delimiter (8 bits) – shall be formatted as “11100101”
 - PHY header (8 bits) –PSDU length
 - PSDU (0 to 127 bytes) – data field



802.15.4 Architecture (MAC)



IEEE 802.15.4 MAC Design Drivers

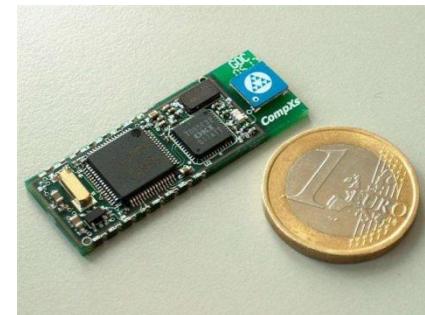
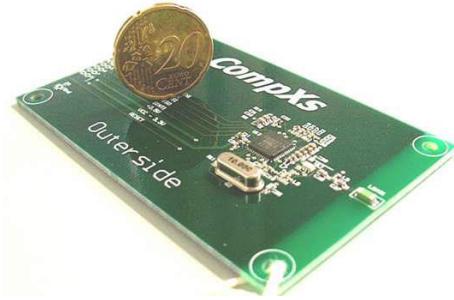
- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol

IEEE 802.15.4 MAC Overview

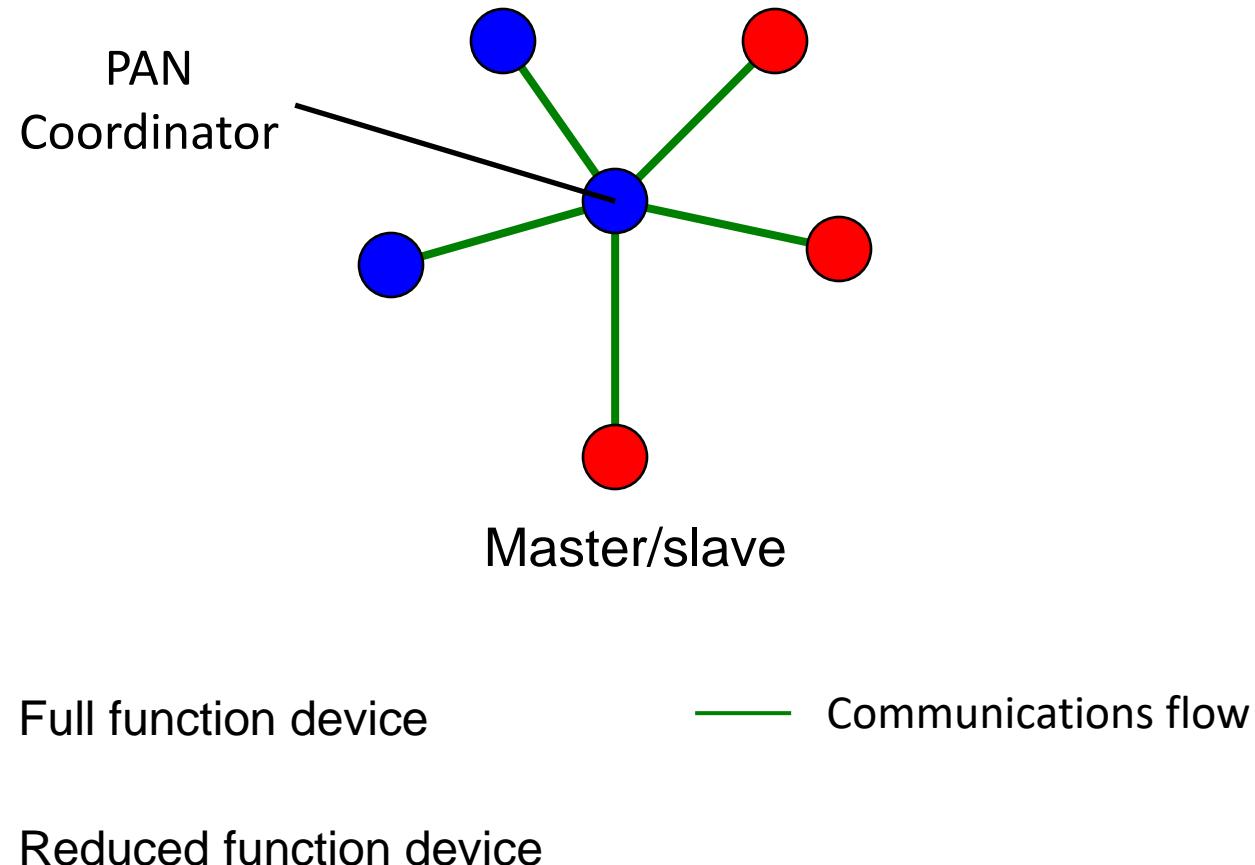
Device Classes

- Full function device (**FFD**)
 - Any topology
 - Network coordinator capable
 - Talks to any other device
 - The FFD can operate in three modes serving
 - Device
 - Coordinator
 - PAN coordinator
- Reduced function device (**RFD**)
 - Limited to star topology
 - Talks only to a network coordinator
 - Cannot become a network coordinator
 - Very simple implementation



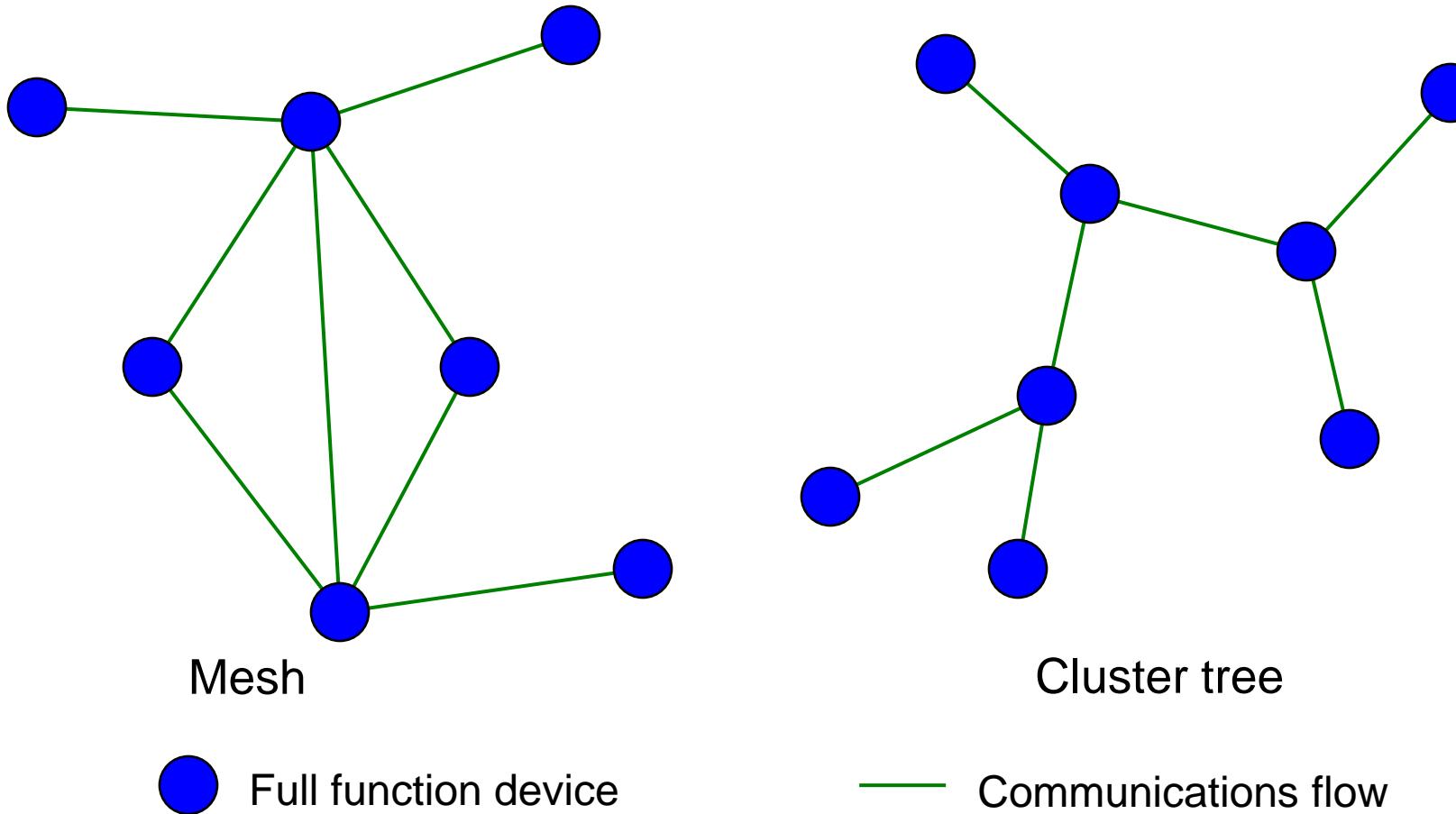
IEEE 802.15.4 MAC Overview

Star Topology



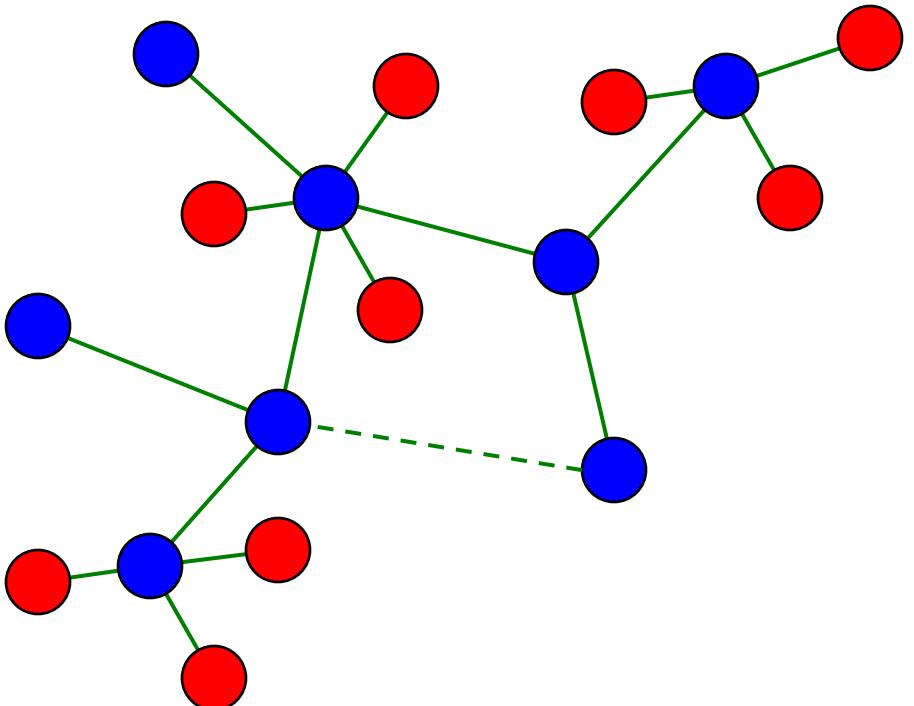
IEEE 802.15.4 MAC Overview

Mesh (Peer-Peer) and cluster tree topologies



IEEE 802.15.4 MAC Overview

Combined Topology



Full function device



Reduced function device



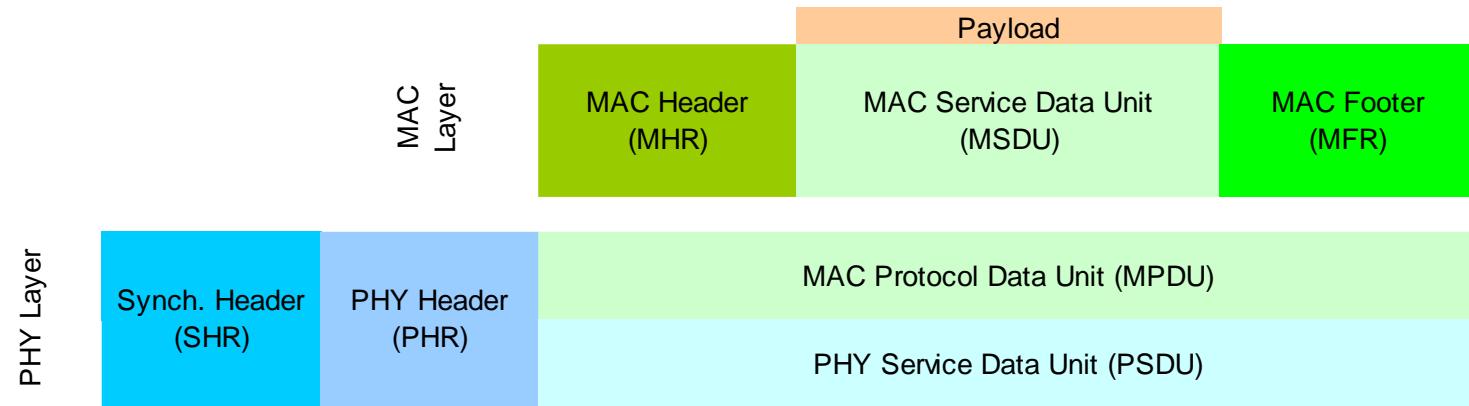
Communications flow

Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

May have a mesh structure in some cases as well

IEEE 802.15.4 MAC Overview

General Frame Structure



4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

MAC layer

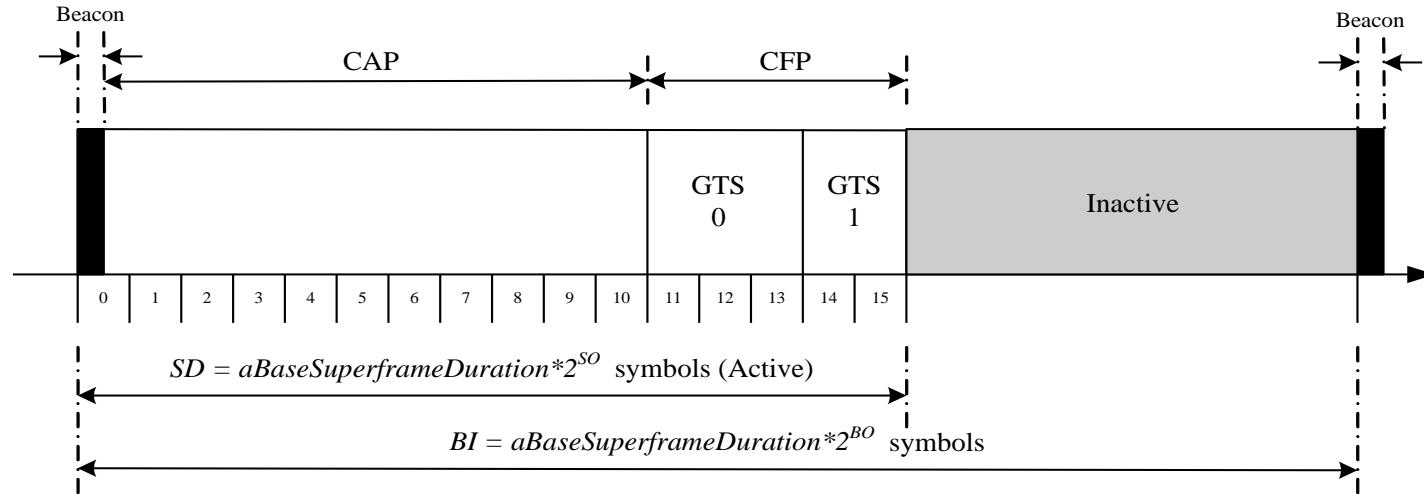
Managing PANs

- Channel scanning (Energy Detection, active, passive, orphan – verifies if it still has a parent)
- PAN ID conflict detection and resolution
- Starting a PAN
- Sending beacons
- Device discovery, association/disassociation
- Synchronization (beacon/nonbeacon)
- Orphaned device realignment

Transfer handling

- Transaction based (indirect transmission)
 - Beacon indication
 - Polling
- Transmission, Reception, Rejection, Retransmission
 - Acknowledged / Not acknowledged
- GTS management
 - Allocation/deallocation/Reallocation
 - Usage

Superframe



- A coordinator in a PAN can optionally bound channel time using a SuperFrame structure
 - bound by beacon frames
- A superframe is divided into two parts
 - Inactive: all devices sleep (including the coordinator)
 - Active:
 - Active period will be divided into 16 slots
 - 16 slots can further be divided into two parts
 - Contention access period
 - Contention free period

CAP – Contention Access Period

CFP – Contention Free Period

SD – Superframe Duration

BI – Beacon Interval

Superframe

- Beacons are used for
 - starting superframes
 - synchronizing with associated devices
 - announcing the existence of a PAN
 - informing pending data in coordinators
- In a beacon enabled network,
 - Devices use the **slotted CSMA/CA** mechanism to contend for the usage of channels
 - FFDs which require fixed rates of transmissions can ask for ***guarantee time slots (GTS)*** from the coordinator

Superframe

- The structure of superframes is controlled by two parameters: *beacon order (BO)* and *superframe order (SO)*
 - BO decides the length of a superframe
 - SO decides the length of the active portion in a superframe
- For channels 11 to 26, the length of a superframe can range from 15.36 msec to 215.7 sec.
 - which means very low duty cycle
- Remember: Duty Cycle
 - Duty Cycle indicates the fraction of time a resource is busy.
 - When a single device transmits on a channel for 2 time units every 10 time units, this device has a duty cycle of 20%.

Superframe

- Each device will be active for $2^{-(BO-SO)}$ portion of the time, and sleep for $1-2^{-(BO-SO)}$ portion of the time
- In IEEE 802.15.4, devices' duty cycle follow the specification

BO-SO	0	1	2	3	4	5	6	7	8	9	≥ 10
Duty cycle (%)	100	50	25	12	6.25	3.125	1.56	0.78	0.39	0.195	< 0.1

BO – Beacon Order

SO – Superframe Order

GTS concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe
- A GTS shall only be allocated by the PAN coordinator
- The PAN coordinator can allocate up to seven GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on:
 - Requirements of the GTS request
 - The current available capacity in the superframe

GTS concepts

- A GTS can be **deallocated**
 - At any time at the discretion of the PAN coordinator or
 - By the device that originally requested the GTS
- A data frame transmitted in an allocated GTS shall use only short addressing
- The PAN coordinator shall be able to store the info of devices that are necessary for GTS, including starting slot, length, direction and associated device address

GTS concepts

- Before GTS starts, the GTS direction shall be specified as either transmit or receive
- Each device may request one **transmit** GTS and/or one **receive** GTS
- A device shall only attempt to allocate and use a GTS if it is currently tracking the beacon
- If a device loses synchronization with the PAN coordinator, all its GTS allocations shall be lost
- The use of GTSs be an RFD is optional

Channel access mechanism

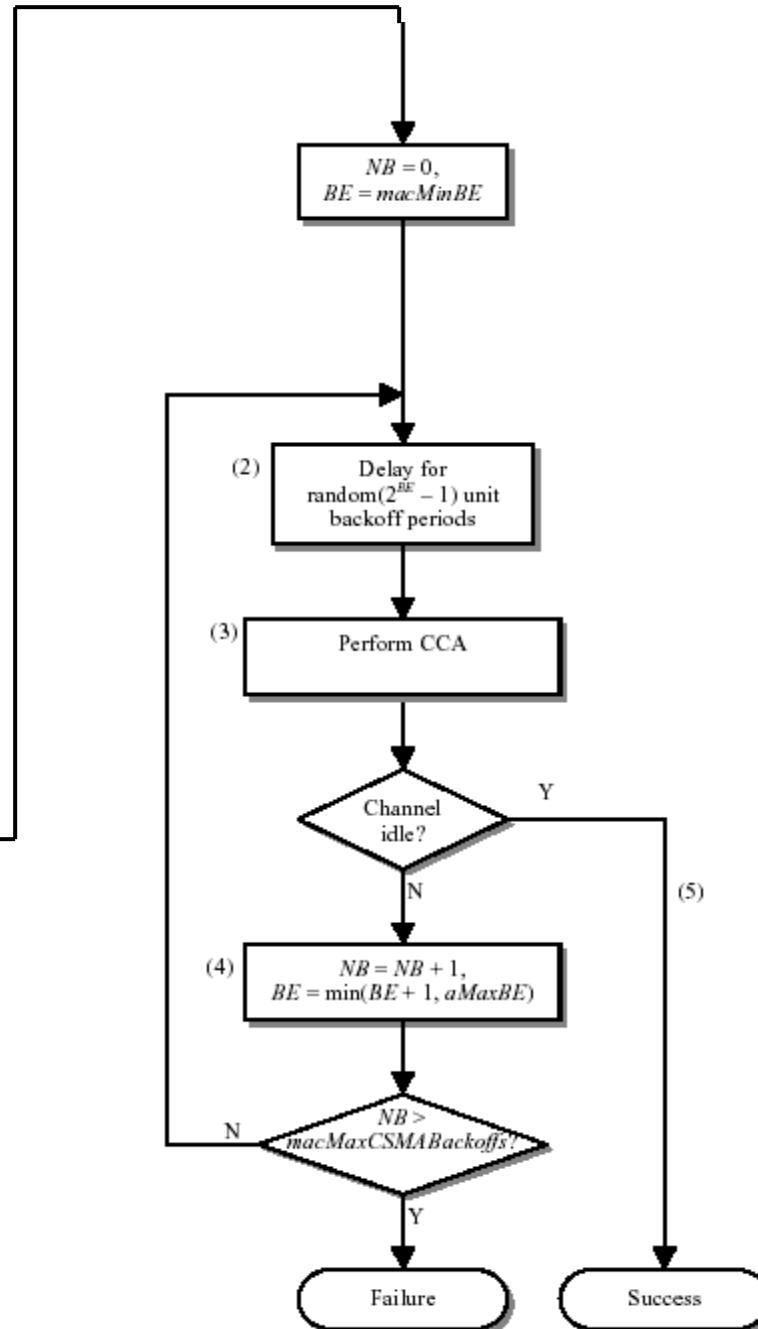
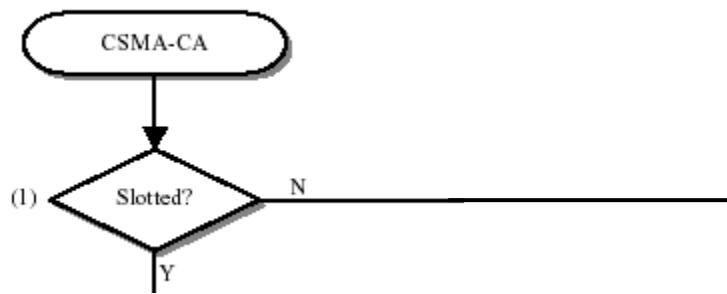
- Two type channel access mechanism:
 - In non-beacon-enabled networks → **unslotted** CSMA/CA channel access mechanism
 - In beacon-enabled networks → **slotted** CSMA/CA channel access mechanism

Unslotted CSMA/CA

NB is the number of times the CSMA-CA algorithm was required to backoff while attempting the current transmission

BE is the backoff exponent, which defines the number of backoff periods a node should wait before attempting **Clear Channel Assessment (CCA)**

MacMinBE constant defined in the standard.



CSMA/CA algorithm

- In slotted CSMA/CA
 - The **backoff period boundaries** of every device in the PAN shall be **aligned with the superframe slot boundaries** of the PAN coordinator
 - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
 - The MAC sublayer shall ensure that the PHY layer commences **all of its transmissions on the boundary of a backoff period**

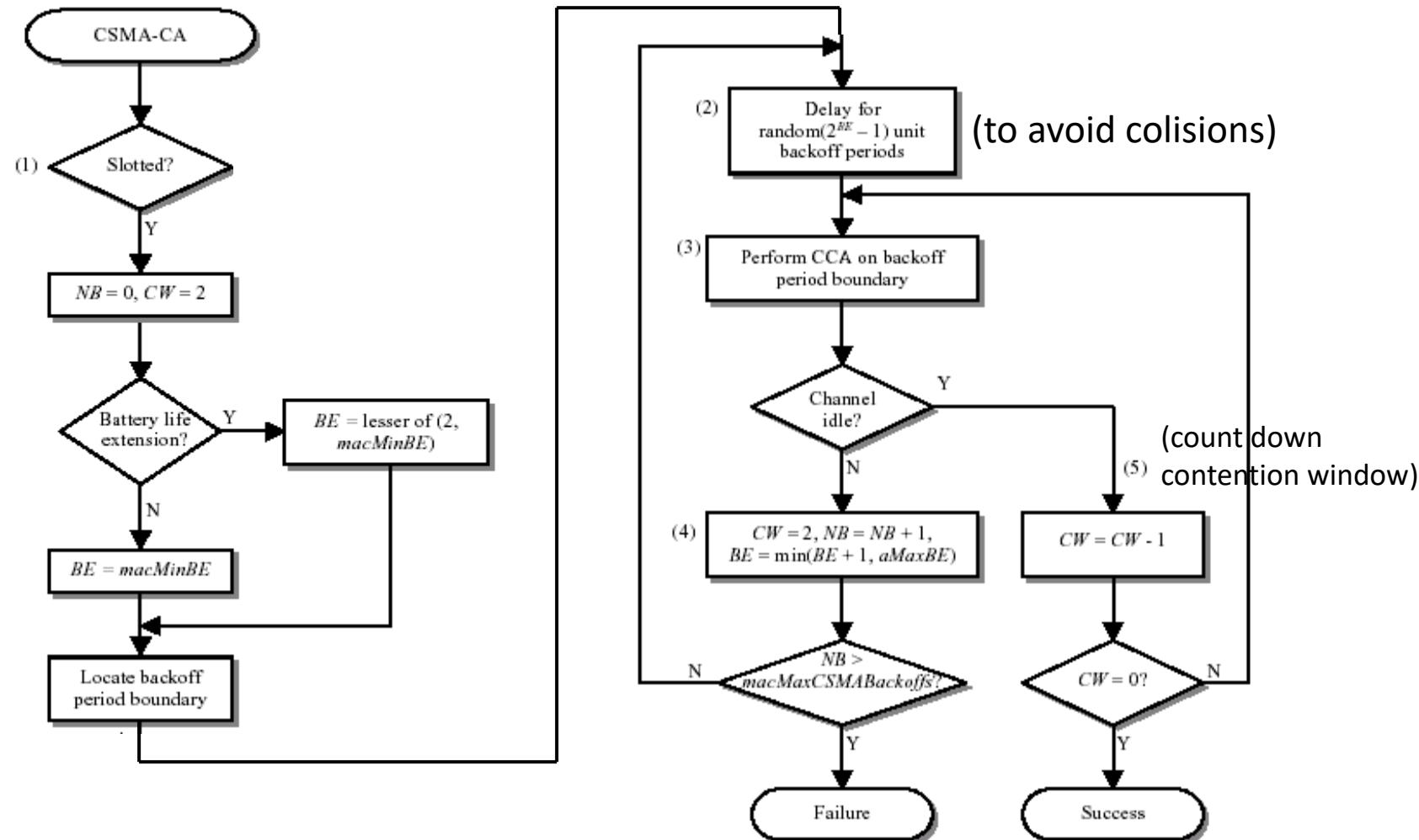
CSMA/CA algorithm

- Each device shall maintain three variables for each transmission attempt
 - NB: number of time the CSMA/CA algorithm was required to backoff while attempting the current transmission
 - CW: contention window length, the number of backoff periods that needs to be clear of channel activity before transmission can commence (initial to 2 and reset to 2 if sensed channel to be busy)
 - BE: the backoff exponent which is related to how many backoff periods a device shall wait before attempting to assess a channel

Slotted CSMA/CA

NB is the number of times the CSMA-CA algorithm was required to backoff while attempting the current transmission

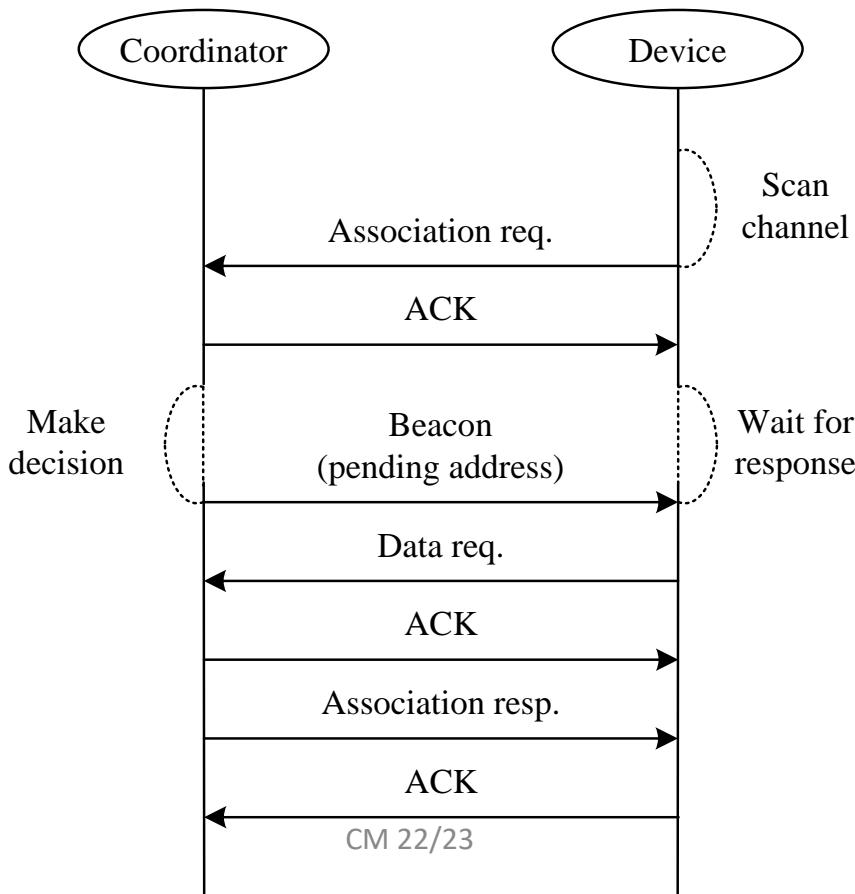
BE is the backoff exponent, which defines the number of backoff periods a node should wait before attempting **Clear Channel Assessment (CCA)**



This ensures performing two CCA operations to prevent potential collisions of acknowledgement frames. If the channel is again sensed as idle (CW = 0), the node attempts to transmit.

Association procedures

- A device becomes a member of a PAN by associating with its coordinator
- Procedures

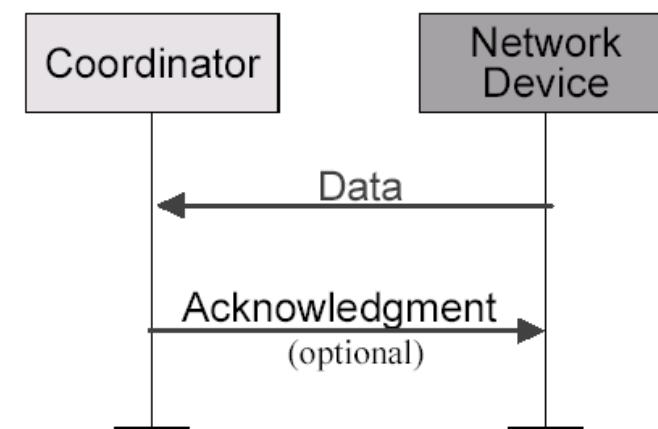
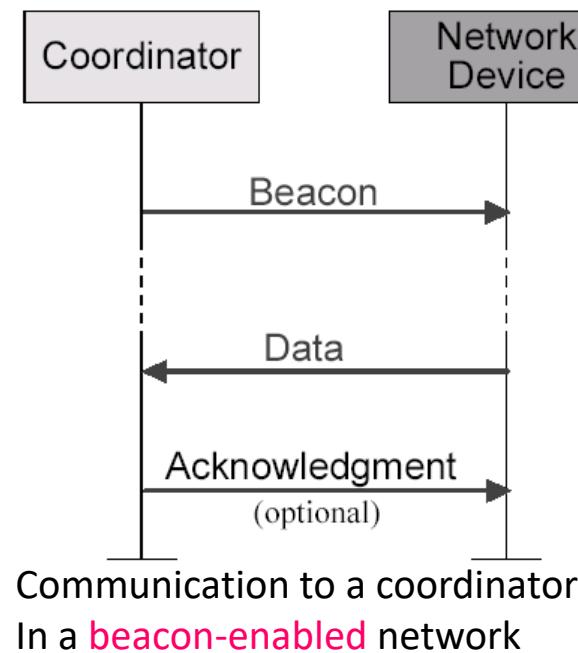


Association procedures

- In IEEE 802.15.4, **association results** are announced in an indirect fashion
- A coordinator responds to association requests by appending devices' long addresses (64 bit) in beacon frames
- Devices need to send a data request to the coordinator to acquire the association result
- After associating to a coordinator, a device will be assigned a 16-bit *short address*.

Data transfer model (device to coordinator)

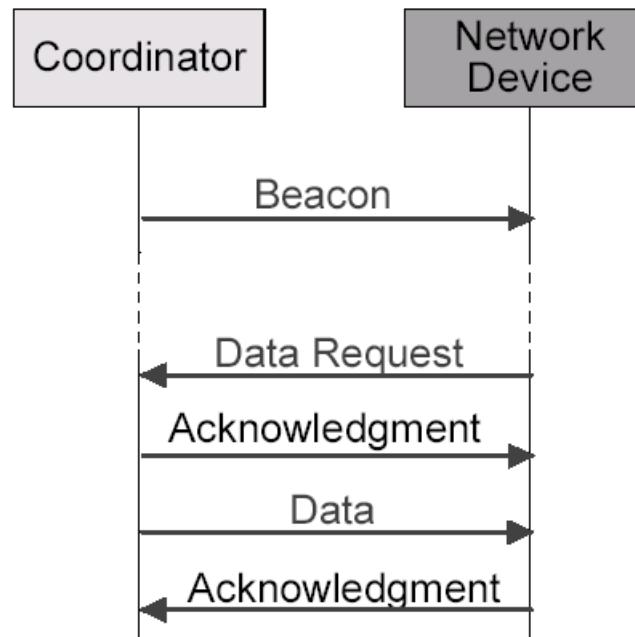
- Data transferred from device to coordinator
 - In a beacon-enable network, the device finds the beacon to synchronize to the superframe structure. Then uses slotted CSMA/CA to transmit its data.
 - In a non beacon-enable network, device simply transmits its data using unslotted CSMA/CA



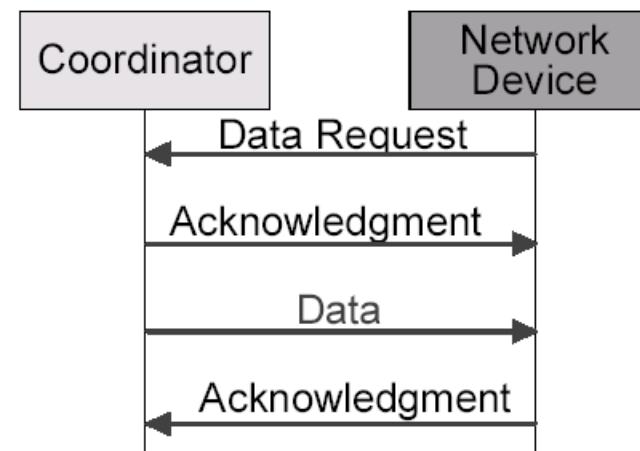
Communication to a coordinator
In a **non beacon-enabled** network

Data transfer model (coordinator to device)

- Data transferred from coordinator to device
 - In a **beacon-enable network**, the coordinator indicates in the beacon that the data is pending. Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary.
 - In a **non-beacon-enable network**, a device transmits a MAC command request using unslotted CSMA/CA. If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA. Otherwise, coordinator transmits a data frame with zero length payload.

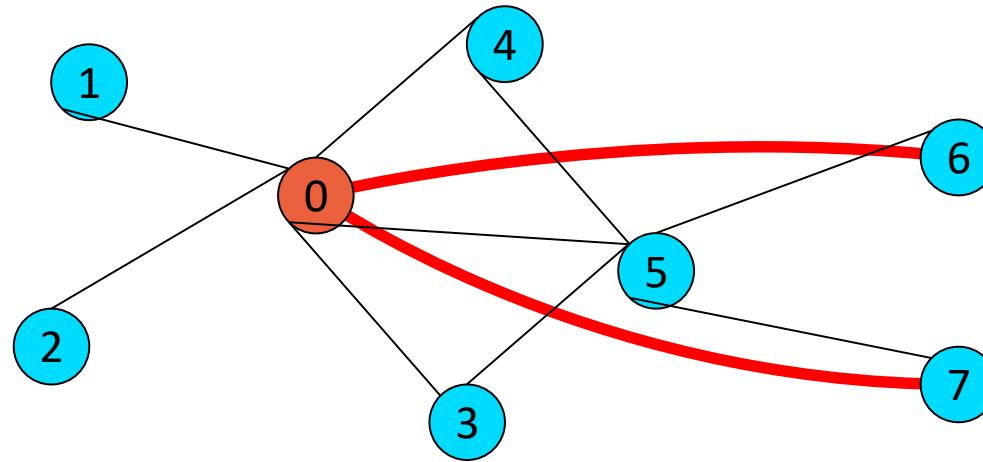


Communication from a coordinator
In a **beacon-enabled** network



Communication from a coordinator
in a **non beacon-enabled** network

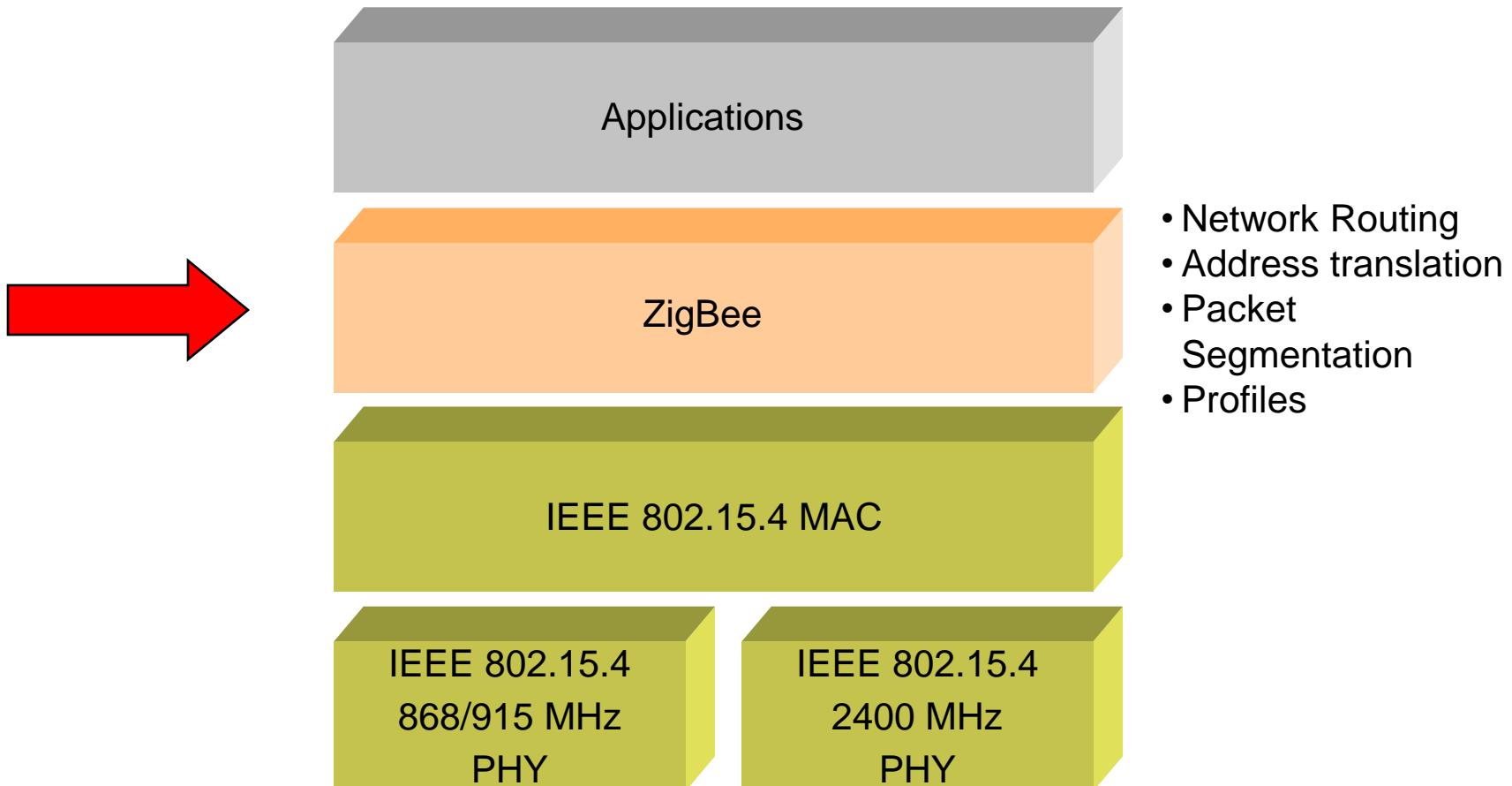
MAC layer



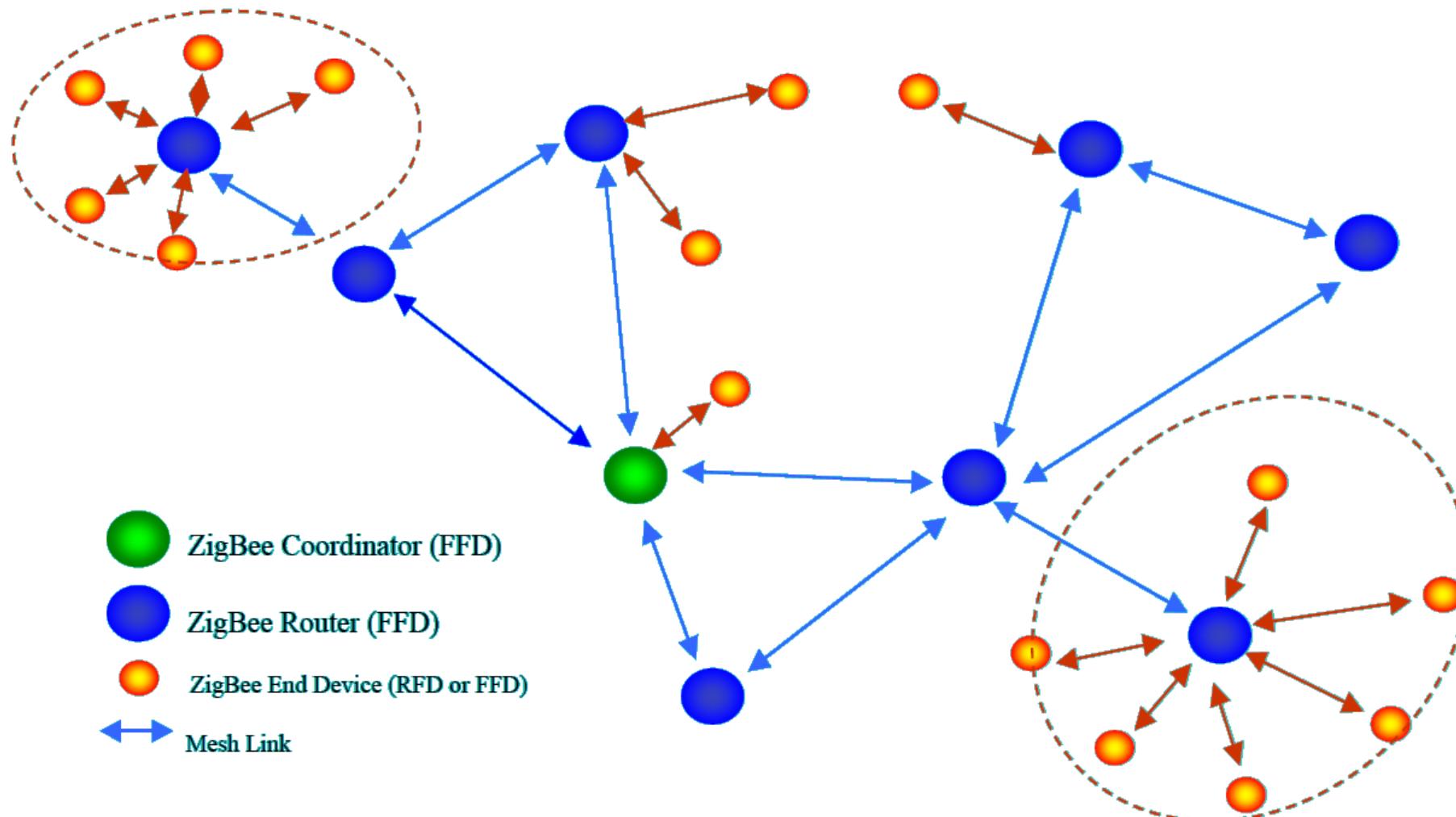
How 6 and 7 connect to coordinator 0?

Routing (NWK Layer)

802.15.4 Architecture



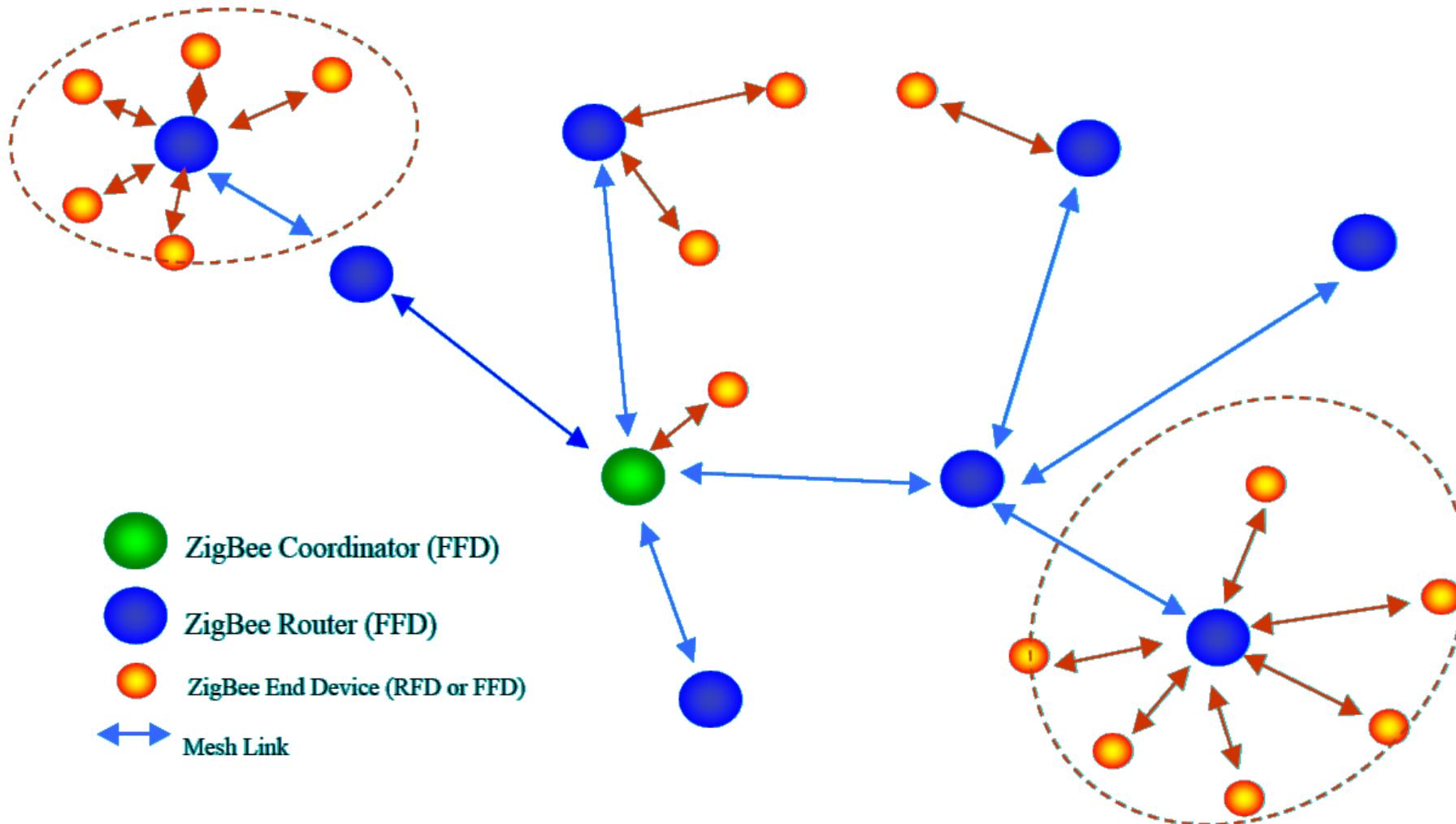
Combined topologies: Mesh Topologies



In a mesh network, regular beacons are not allowed.

Devices in a mesh network can only communicate with each other by peer-to-peer transmissions

Combined Topologies: Tree



In a tree network, the coordinator and routers can announce beacons.

Device addressing

- Two or more devices communicating on the same physical channel constitute a WPAN which includes at least one FFD (PAN coordinator)
- Each independent PAN will select a unique PAN identifier
- All devices operating on a network shall have unique 64-bit extended address (IEEE 802.15.4). This address can be used for direct communication in the PAN
- The network address can use a 16-bit short address, which is allocated to the child routers by the PAN coordinator when the device associates
- 256 sub addresses may be allocated for subunits

Address assignment in a ZigBee network

- In ZigBee, network addresses are assigned to devices by a **distributed address assignment scheme**
 - The ZigBee coordinator determines three network parameters to set the allocations
 - the maximum number of children (C_m) of a ZigBee router
 - the maximum number of child routers (R_m) of a parent node
 - the depth of the network (L_m)
 - A parent device utilizes C_m , R_m , and L_m to compute a parameter called C_{skip}
 - which is used to compute the size of its children's address pools

$$Cskip(d) = \begin{cases} 1 + Cm \cdot (Lm - d - 1), & \text{if } Rm = 1 \\ \frac{1 + Cm - Rm - Cm \cdot Rm^{Lm-d-1}}{1 - Rm}, & \text{Otherwise} \end{cases} \quad \dots \dots \dots$$

- If a parent node at depth d has an address A_{parent} ,
 - the n th child router is assigned to address $A_{parent} + (n-1) \times C_{skip}(d) + 1$
 - n th child end device is assigned to address $A_{parent} + R_m \times C_{skip}(d) + n$

For node C

$C_{skip}=31$

Total:127

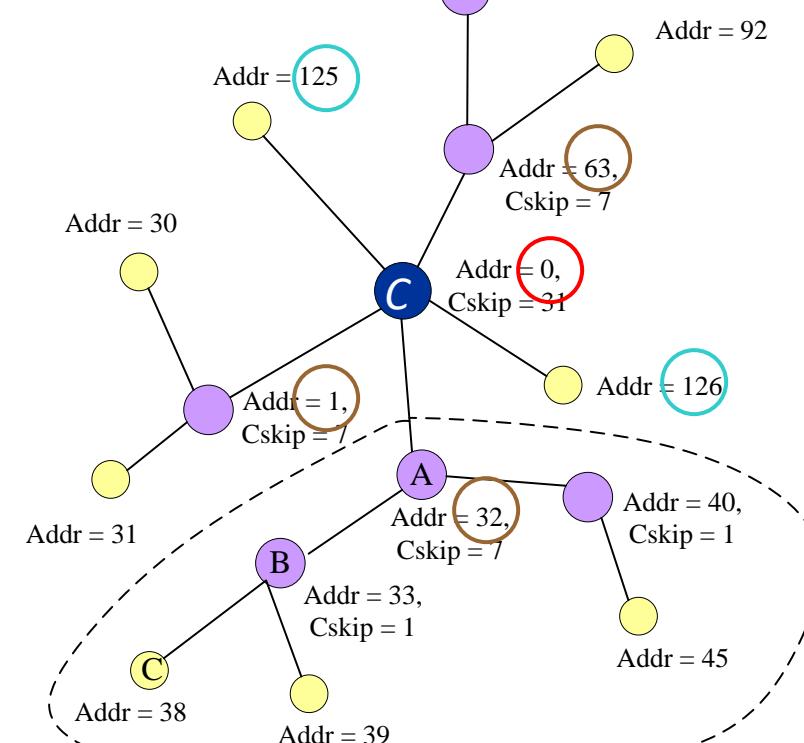


node A

125,126

Cm=6
Rm=4
Lm=3

Addr = 64,
Cskip = 1



ZigBee routing protocols

- In a tree network
 - Utilize the address assignment to obtain the routing paths
- In a mesh network
 - Two options
 - Reactive routing: if having routing capacity
 - Use tree routing: if do not have routing capacity
- Note:
 - ZigBee coordinators and routers are said to have *routing capacity* if they have **routing table capacities** and **route discovery table capacities**

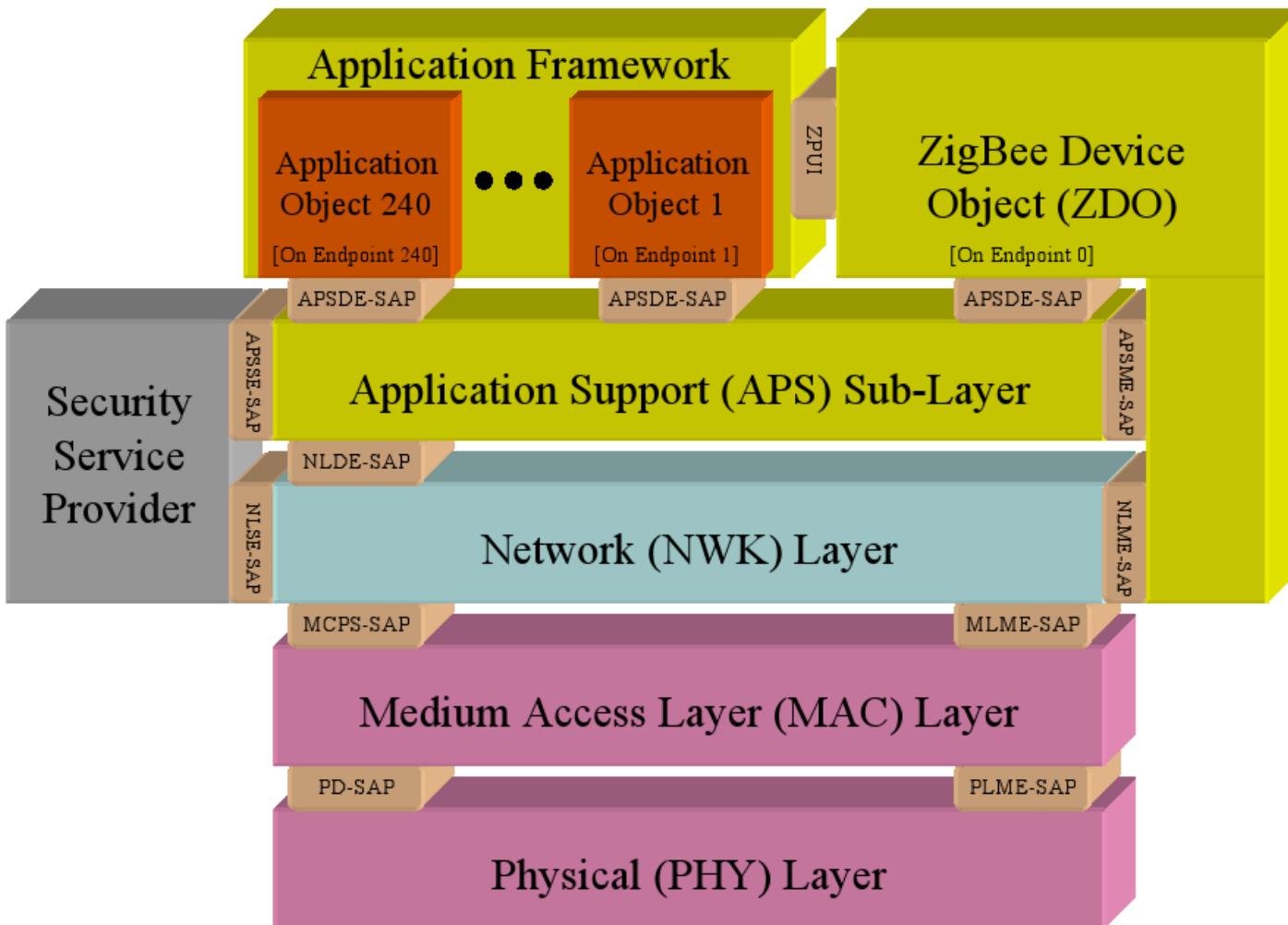
Summary of ZigBee network layer

- Pros and cons of different kinds of ZigBee network topologies

	Pros	Cons
Star	<ol style="list-style-type: none">1. Easy to synchronize2. Support low power operation3. Low latency	<ol style="list-style-type: none">1. Small scale
Tree	<ol style="list-style-type: none">1. Low routing cost2. Can form superframes to support sleep mode3. Allow multihop communication	<ol style="list-style-type: none">1. Route reconstruction is costly2. Latency may be quite long
Mesh	<ol style="list-style-type: none">1. Robust multihop communication2. Network is more flexible3. Lower latency	<ol style="list-style-type: none">1. Cannot form superframes (and thus cannot support sleep mode)2. Route discovery is costly3. Needs storage for routing table

Application Level

CM 22/23



ZigBee defined Objects (ZDO):

- provides common function for applications
- Initializes APS, NWK-Layer and Security Service Specification
- offers services like device-/service-discovery, binding and security management
- assembles information about the network
- for ZBC/ZBR -> e.g. binding table

CM 22/23

Command	Addressing	
	Request	Response
End device bind	Unicast to ZC	Unicast
Bind	Unicast to ZC or Src	Unicast
Unbind	Unicast to ZC or Src	Unicast

Profiles:

Definition of ZigBee-Profiles

- describes a common language for exchanging data
- defines the offered services
- device interoperability across different manufacturers
- Standard profiles available from the ZigBee Alliance
- **profiles contain device descriptions**
- unique identifier (licensed by the ZigBee Alliance)

ZigBee and BLE

- Business comparison:
 - ZigBee is older. It has gone through some iterations
 - ZigBee has market mindshare, but not a lot of shipments yet.
 - Market barriers: connectivity – ZigBee is not in PCs or mobile phones yet.
- Technical comparison:
 - Zigbee is low power; Bluetooth LE is even lower. Detailed analysis depends on specific applications and design detail, no to mention chip geometry.
 - ZigBee stack is light; the Bluetooth LE/GATT stack is even simpler
 - Remember: GATT – Generic ATtribute profile
- Going forward:
 - ZigBee has a lead on developing applications and presence
 - Bluetooth low energy has improved technology, and a commanding presence in several existing markets: mobile phones, automobiles, consumer electronics, PC industry
 - Replacing “classic Bluetooth” with “dual mode” devices will bootstrap this market quickly

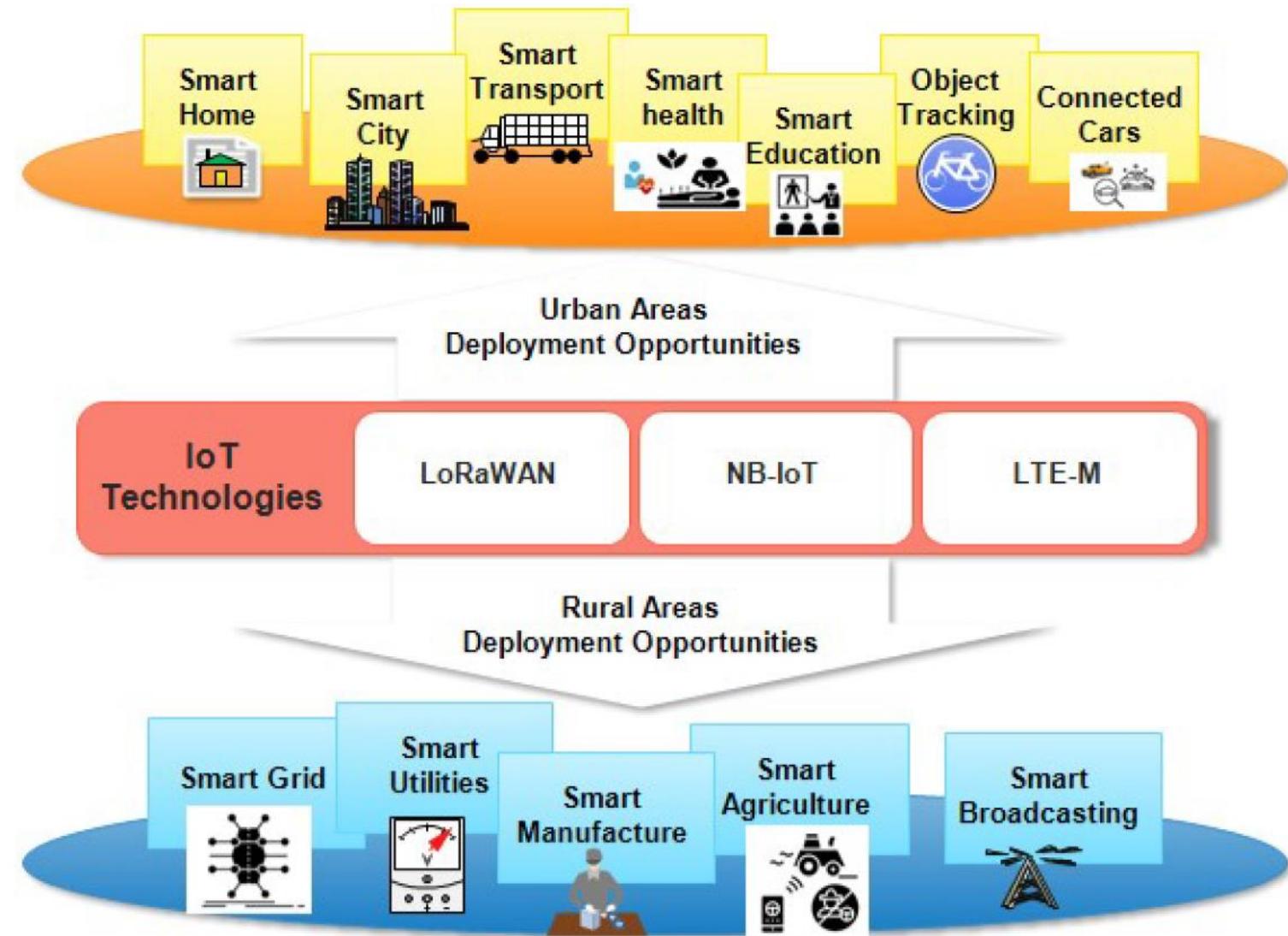
Wide Area Wireless Sensor Networks

WWSN

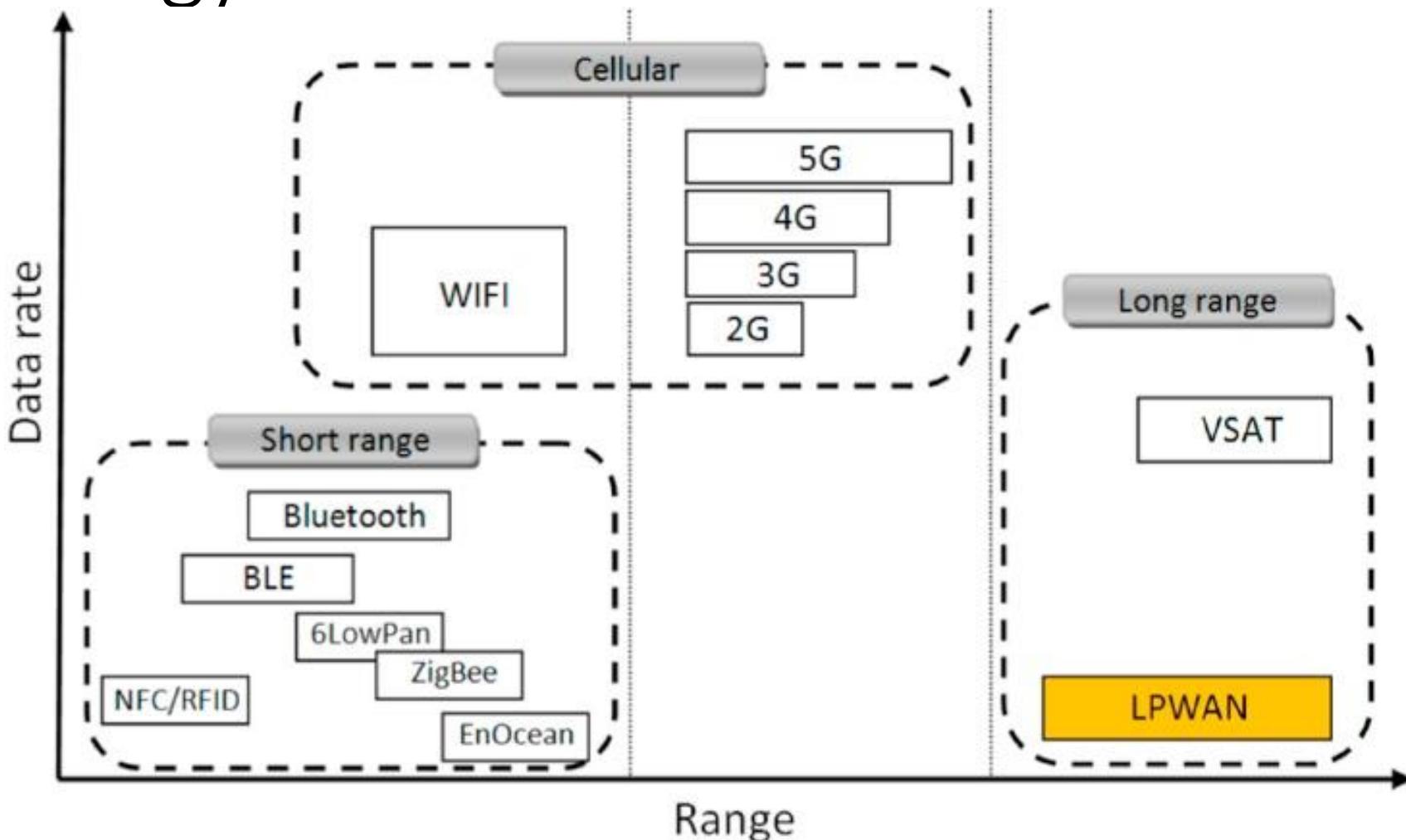
What is this?

- WWSN – wide area wireless sensor networks
- LPWSN – low power wireless sensor networks
- Technologies for sensor networks in wide areas
 - either for low power, or for geography
 - Typically: Sigfox, LoRa, cellular (LTE-M, NB-IoT)

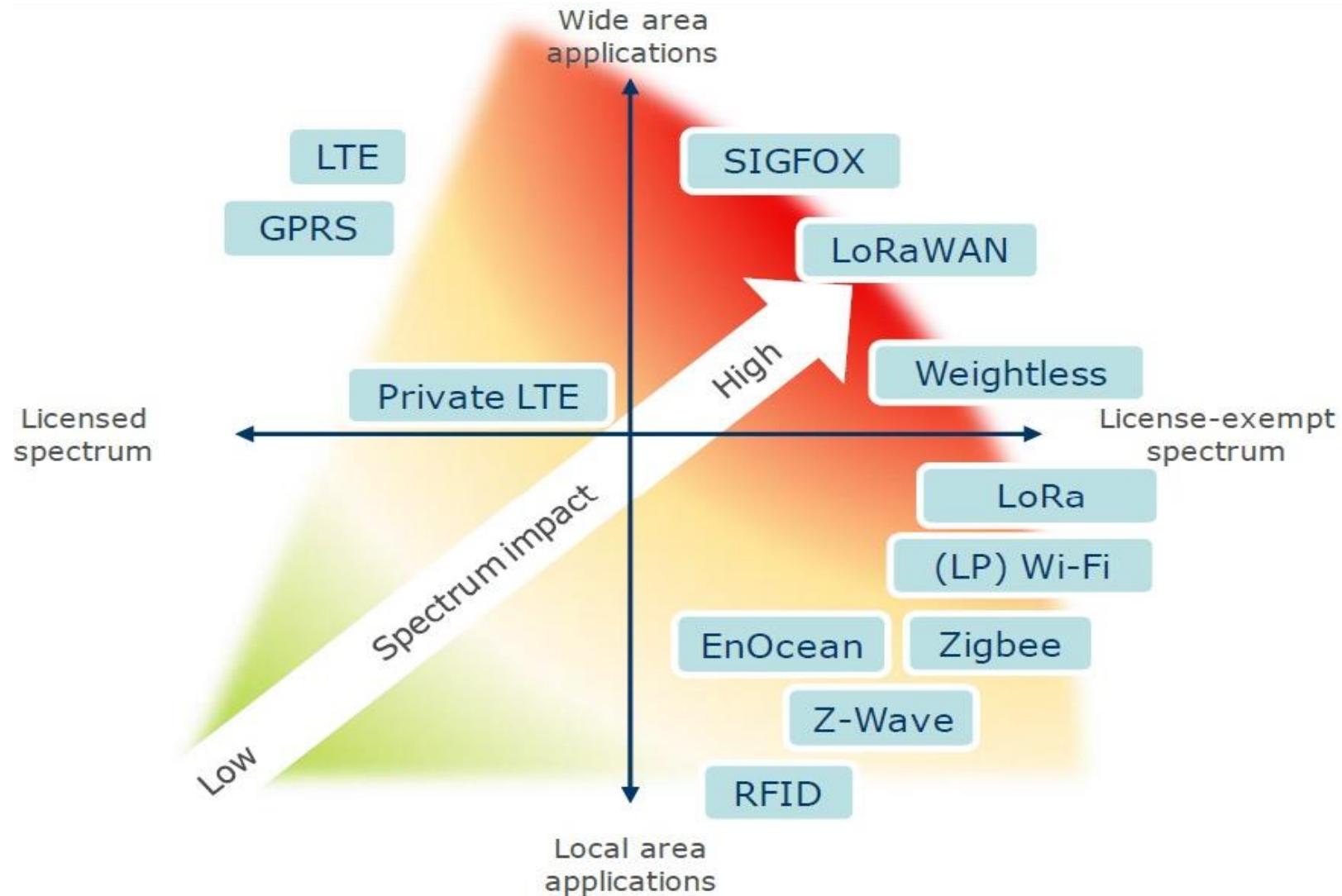
LPWSN



Technology review



Licensed vs licensed-exempt



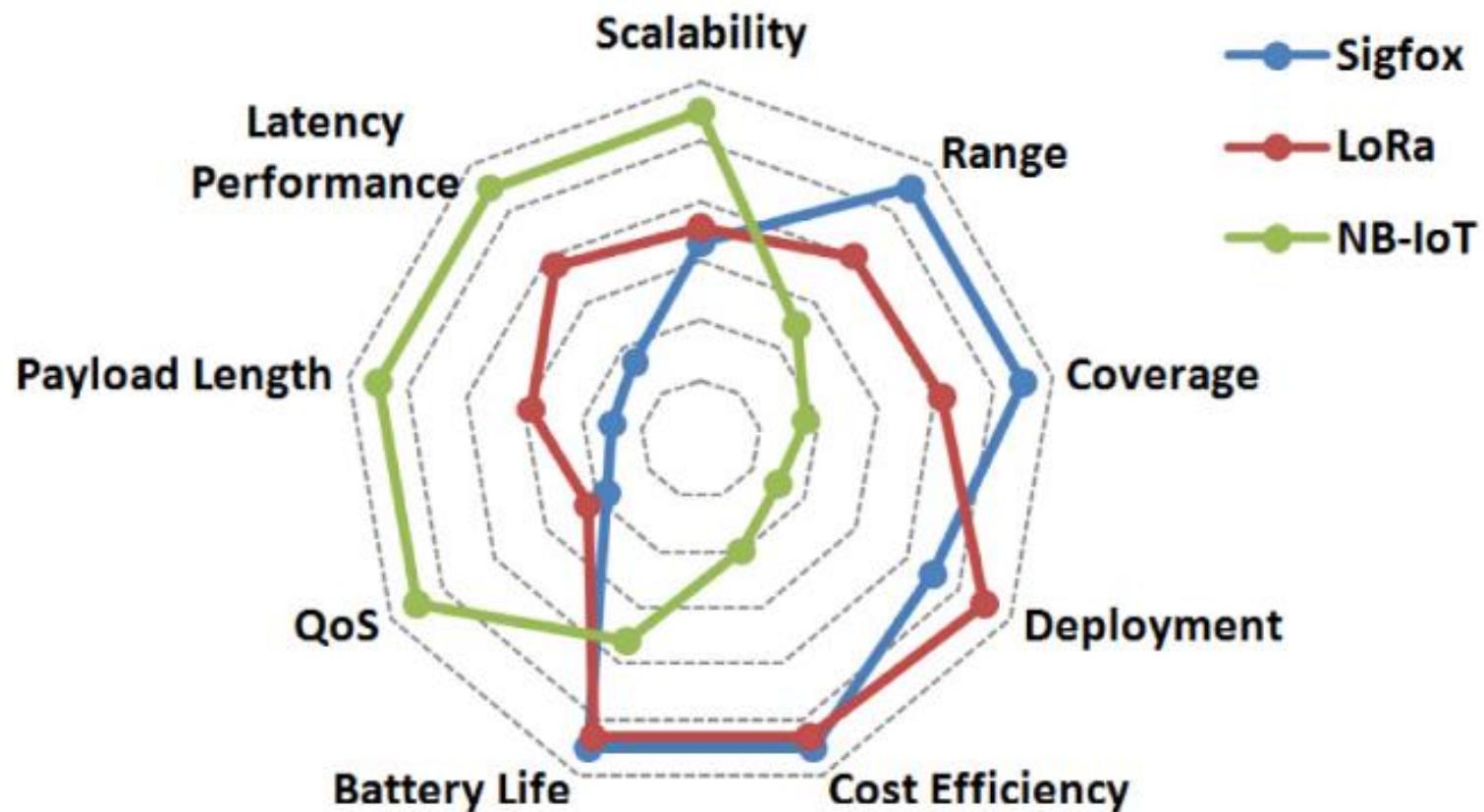
Overview of LPWAN

Overview of LPWAN technologies: Sigfox, LoRa, and NB-IoT.

	Sigfox	LoRaWAN	NB-IoT
Modulation	BPSK	CSS	QPSK
Frequency	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Unlicensed ISM bands (868 MHz in Europe, 915 MHz in North America, and 433 MHz in Asia)	Licensed LTE frequency bands
Bandwidth	100 Hz	250 kHz and 125 kHz	200 kHz
Maximum data rate	100 bps	50 kbps	200 kbps
Bidirectional	Limited / Half-duplex	Yes / Half-duplex	Yes / Half-duplex
Maximum messages/day	140 (UL), 4 (DL)	Unlimited	Unlimited
Maximum payload length	12 bytes (UL), 8 bytes (DL)	243 bytes	1600 bytes
Range	10 km (urban), 40 km (rural)	5 km (urban), 20 km (rural)	1 km (urban), 10 km (rural)
Interference immunity	Very high	Very high	Low
Authentication & encryption	Not supported	Yes (AES 128b)	Yes (LTE encryption)
Adaptive data rate	No	Yes	No
Handover	End-devices do not join a single base station	End-devices do not join a single base station	End-devices join a single base station
Localization	Yes (RSSI)	Yes (TDOA)	No (under specification)
Allow private network	No	Yes	No
Standardization	Sigfox company is collaborating with ETSI on the standardization of Sigfox-based network	LoRa-Alliance	3GPP

	Spectrum cost	Deployment cost	End-device cost
Sigfox	Free	>4000€/base station	<2€
LoRa	Free	>100€/gateway > 1000€/base station	3–5€
NB-IoT	>500 M€ /MHz	>15 000€/base station	>20€

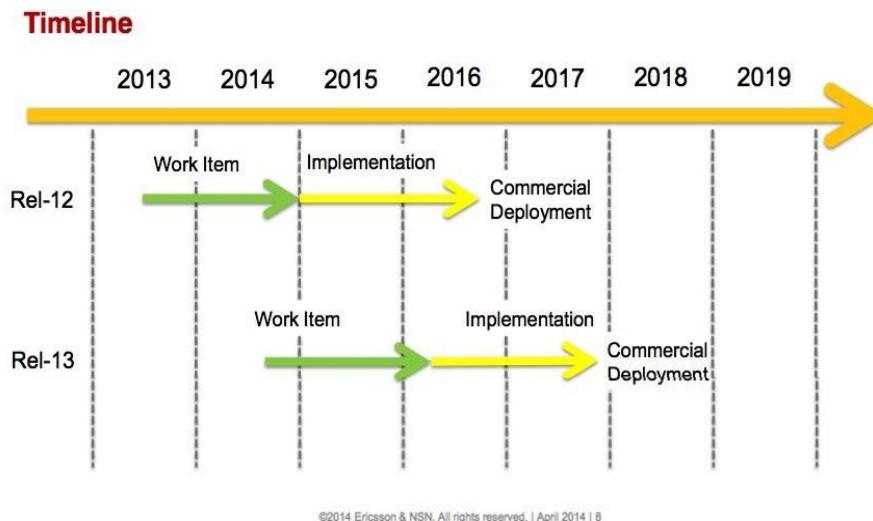
Comparison Radar



LTE-M - Overview



- Evolution of LTE optimized for IoT
- Low power consumption and autonomous
- Easy Deployment
- Interoperability with existing LTE networks
- Coverage up to 11 Km
- Max Throughput \leq 1 Mbps



- ✓ First released in Rel.12 in 2 Q4 2014
- ✓ Optimization in Rel.13
- ✓ Specifications completed in Q1 2016
- ✓ Available since 2017

Evolution from LTE to LTE-M

3GPP Releases	8 (Cat.4)	8 (Cat. 1)	12 (Cat.0) LTE-	13 (Cat. 1,4 MHz) LTE-
Downlink peak rate (Mbps)	150	10	1	1
Uplink peak rate (Mbps)	50	5	1	1
Number of antennas (MIMO)	2	2	1	1
Duplex Mode	Full	Full	Half	Half
UE receive bandwidth (MHz)	20	20	20	1.4
UE Transmit power (dBm)	23	23	23	20

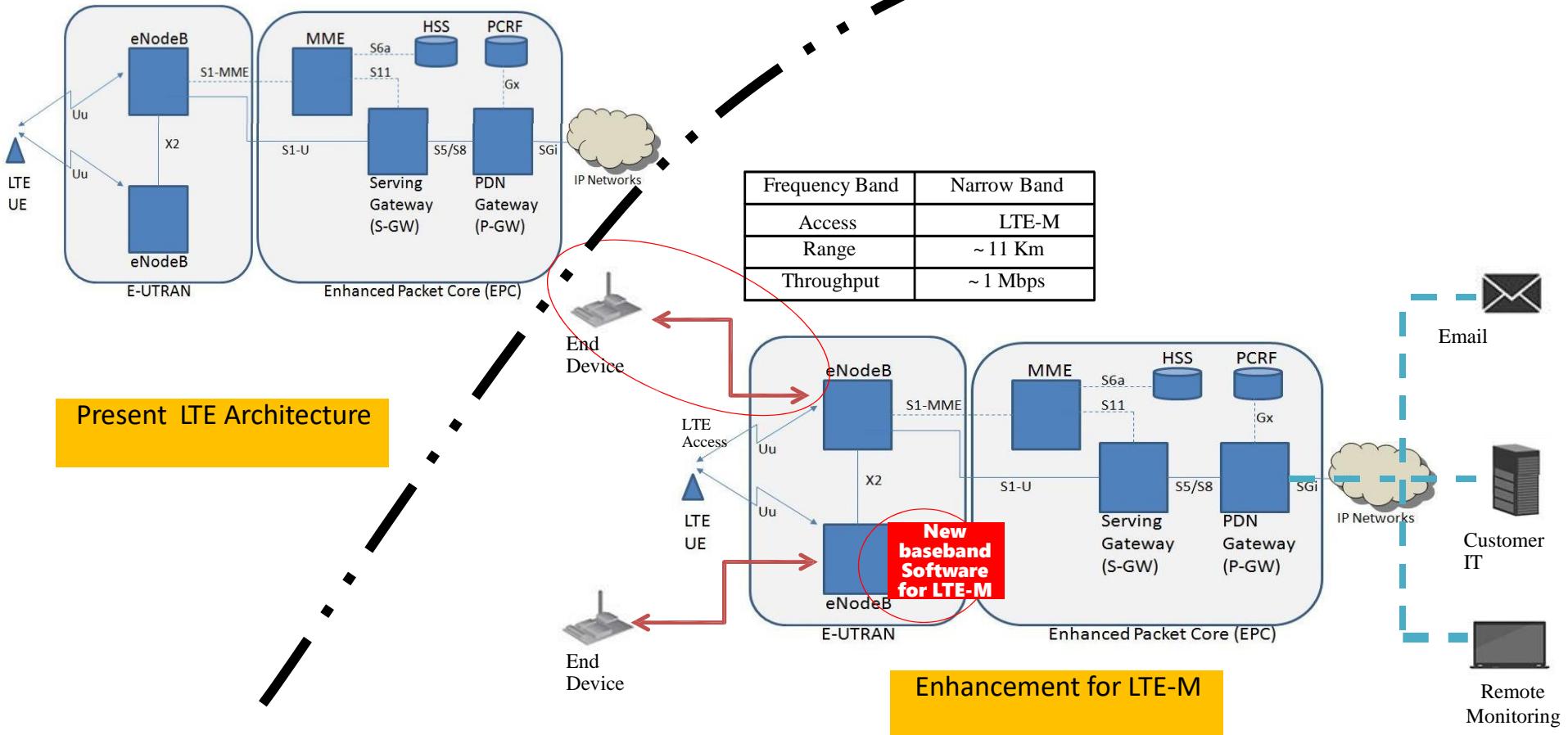
Release 12

- New category of UE (“Cat-0”): lower complexity and low cost devices
- Half duplex FDD operation allowed
- Single receiver
- Lower data rate requirement (Max: 1 Mbps)

Release 13

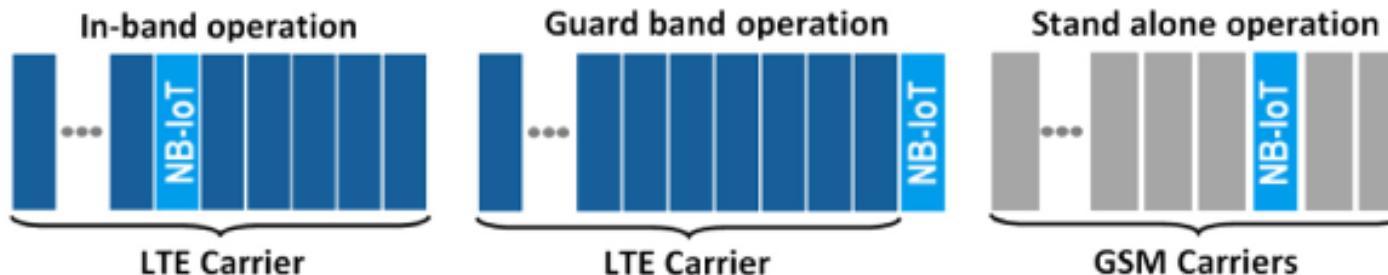
- Reduced receive bandwidth to 1.4 MHz
- Lower device power class of 20 dBm
- 15dB additional link budget: better coverage
- More energy efficient because of its extended discontinuous repetition cycle (eDRX)

LTE to LTE-M - Architecture



NB-IoT

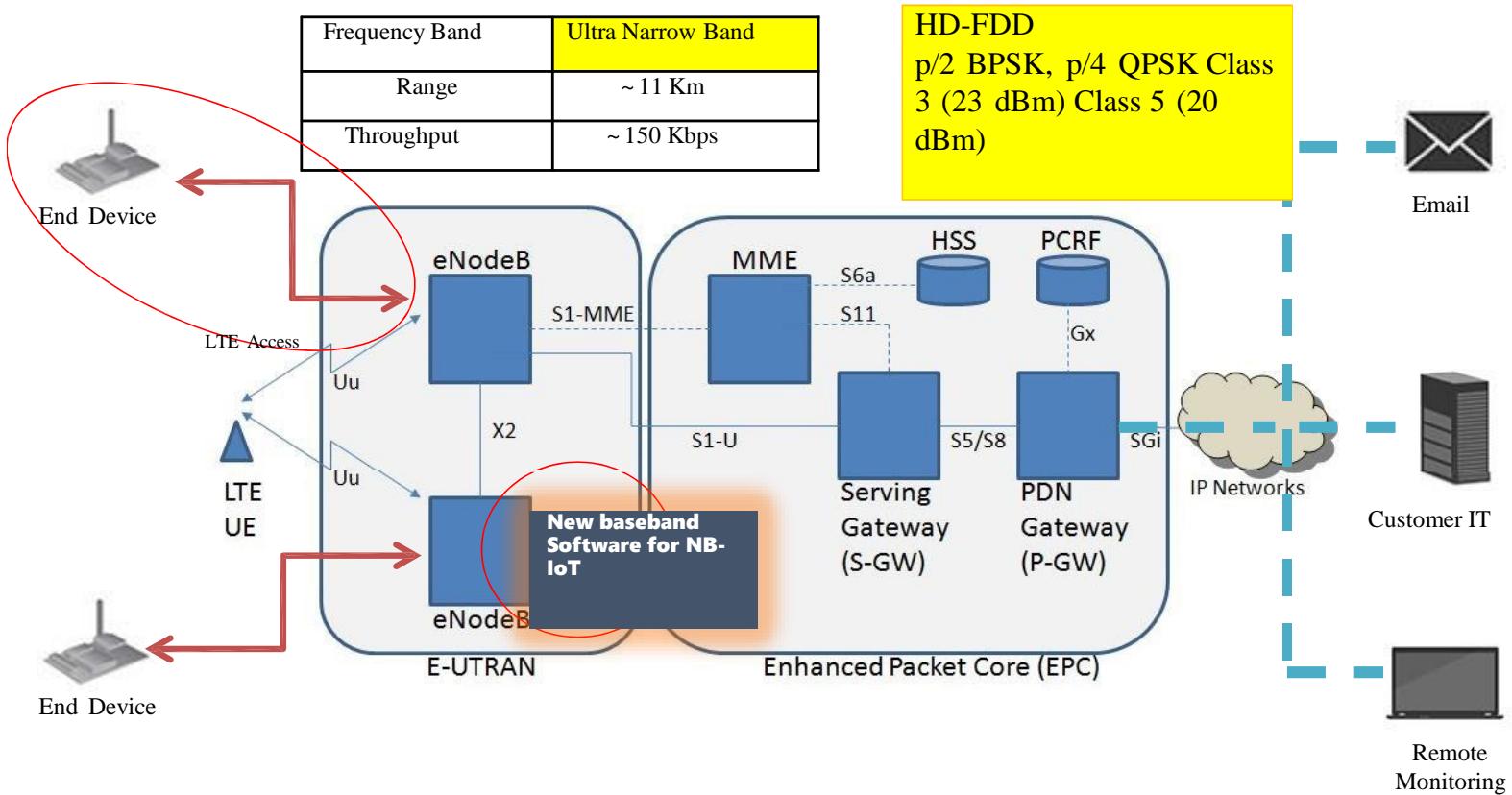
- Defined in R13, another mode instead of LTE-M
- Bandwidth – 200KHz
 - One resource block in GSM/LTE
- Based in LTE protocol, stripped down
 - OFDMA(down)/FDMA(up), QPSK
 - 200kbps (down)/20kbps(up)
- Three modes of operation



NB-IoT

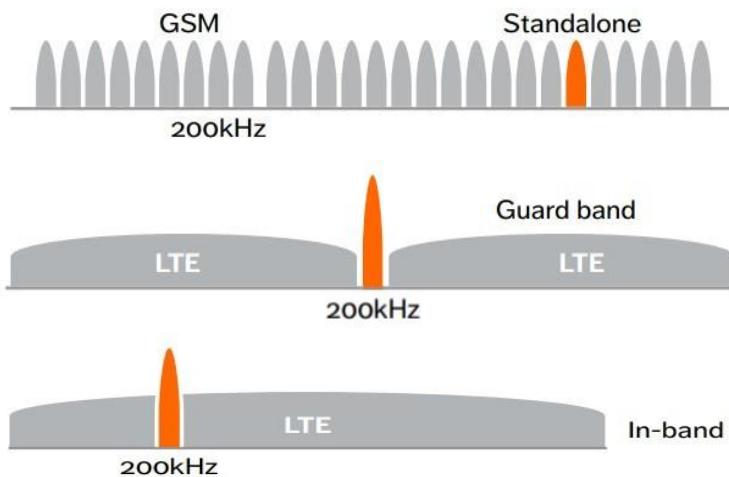
- Uses LTE design extensively
- Lower cost in terms of channel utilization
- Extended coverage
- Low Receiver sensitivity = -141 dBm
- Long battery life: 10 years with 5 Watt Hour battery (depending on traffic and coverage needs)
- Support for massive number of devices: at least 50.000 per cell
- 3 modes of operation:
 - Stand-alone: *stand-alone carrier, e.g. spectrum currently used by GERAN (GSM Edge Radio Access Network) systems as a replacement of one or more GSM carriers*
 - Guard band: *unused resource blocks within a LTE carrier's guard-band*
 - In-band: *resource blocks within a normal LTE carrier*

NB-IoT - Architecture



NB-IoT – Spectrum & Access

Designed with a number of deployment options for licensed GSM ,
WCDMA or LTE spectrum to achieve efficiency



Stand-alone operation

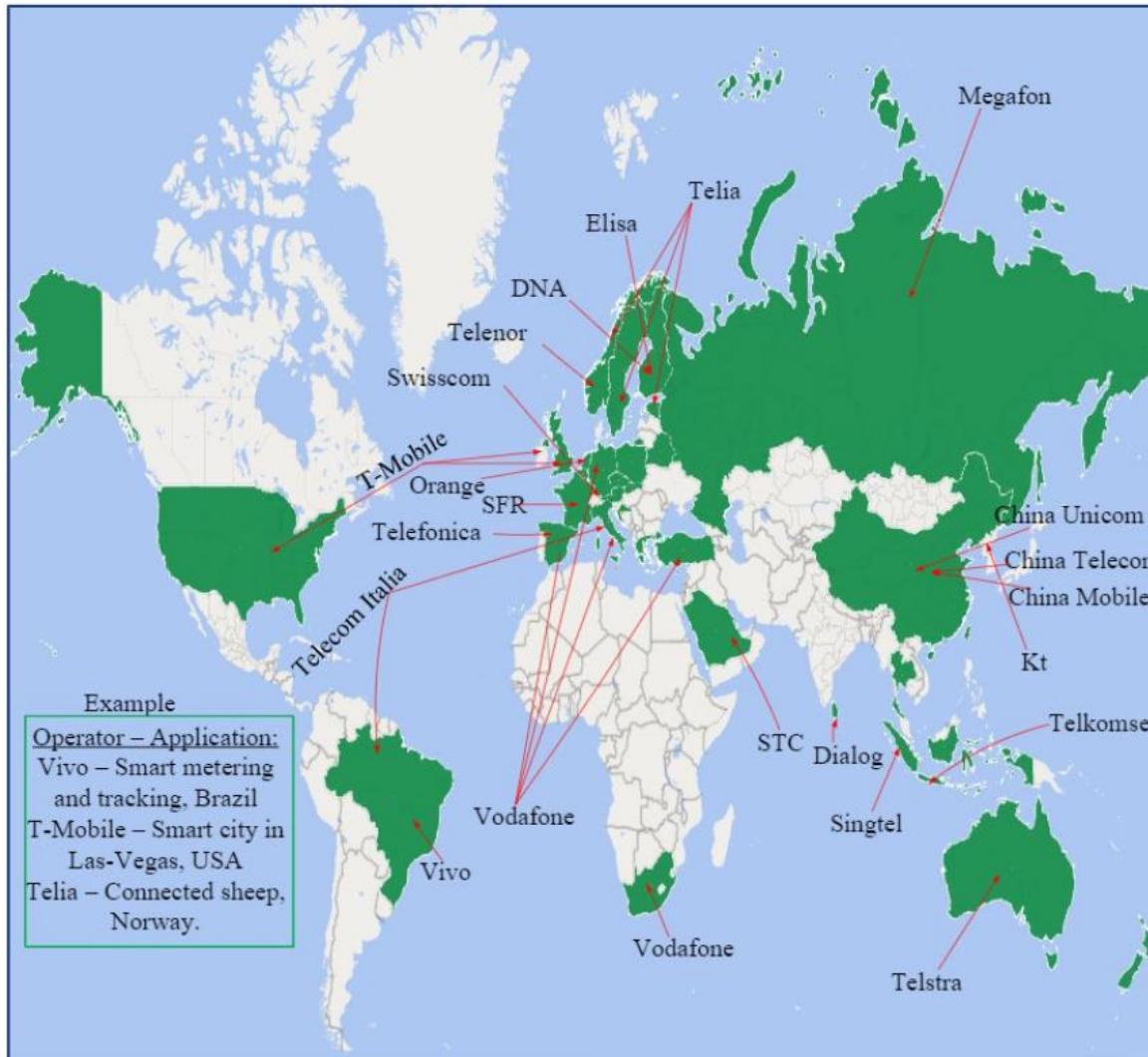
Dedicated spectrum.

Ex.: By **re-farming GSM channels**

Guard band Operation:
Based on the unused RB within a LTE carrier's **guard-band**

In-band operation
Using **resource blocks** within a normal LTE carrier

NB-IoT (@2019)



Cellular technologies

- Two strategies, for different scenarios
 - No MIMO for lower end device energy.

	LTE-M	NB-IoT
Peak data rate	384 kbps	<100 kbps
Latency	50-100 ms	1.5-10 seconds
Power consumption	Best at medium data rates	Best at very low data rates
Mobility	Yes	No, stationary only
Voice	Yes	No
Antennas	1	1

SigFox



- Provide and maintain a PAID connectivity platform
 - Ultra Narrow Band: 100Hz per message
 - Ultra Low Bit rate: 12 byte messages, 140 messages per day (max!)
 - Long Range: ~50KM
 - Sensors lasting 10 years
 - Only provides connectivity, access control and a broker
- Business Model: connectivity service for alarms, smart meters, etc..

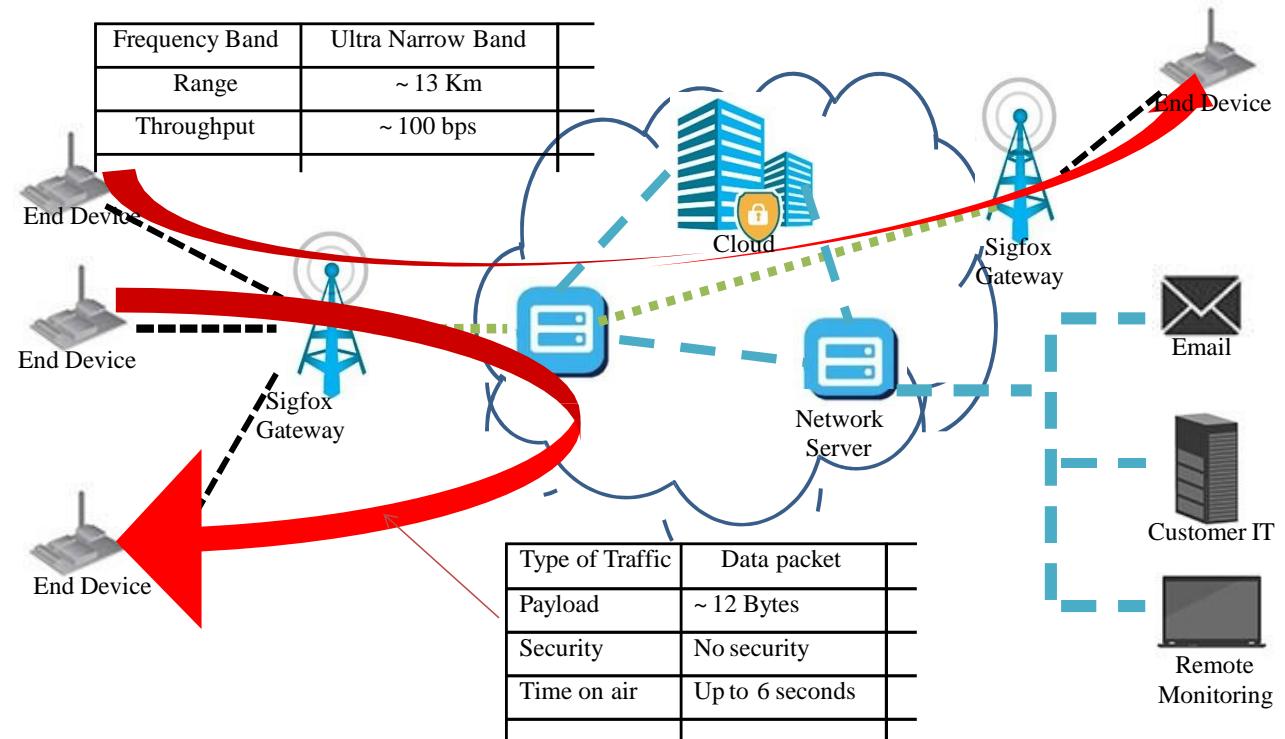
SigFox

- Low Power Wide Area Sensor Network (LPWASN)
- Thousands of millions ☺
 - A million per access point ;)
- Proprietary 😞 commercial
 - You have to use its access infrastructure (built with operators) and software
 - Open market for the endpoints
- 30-50km range in rural areas, and 3-10km range in urban
- Ultra narrow band, 868 (EU) or 902 (US) frequency (MHz)
- Low energy consumption
- Dedicated network

SigFox

- Each device can send up to 140 messages per day
 - Payload: 12 octets (~96 bytes)
 - Datarate: up to 100bps
- **(Duty cycle:** the time occupied by the operation of a device, which operates intermittently)
 - Common in the IoT
- Sigfox exploits this:
 - When a device has a message to be sent, the Sigfox interface wakes up, and the message is transmitted uplink
 - Then, the device listens for a short duration, if there is data to be sent to it
 - This is good for data acquisition scenarios
 - But not so good for command-and-control situations
- Use cases:
 - Smart meters, smoke detectors

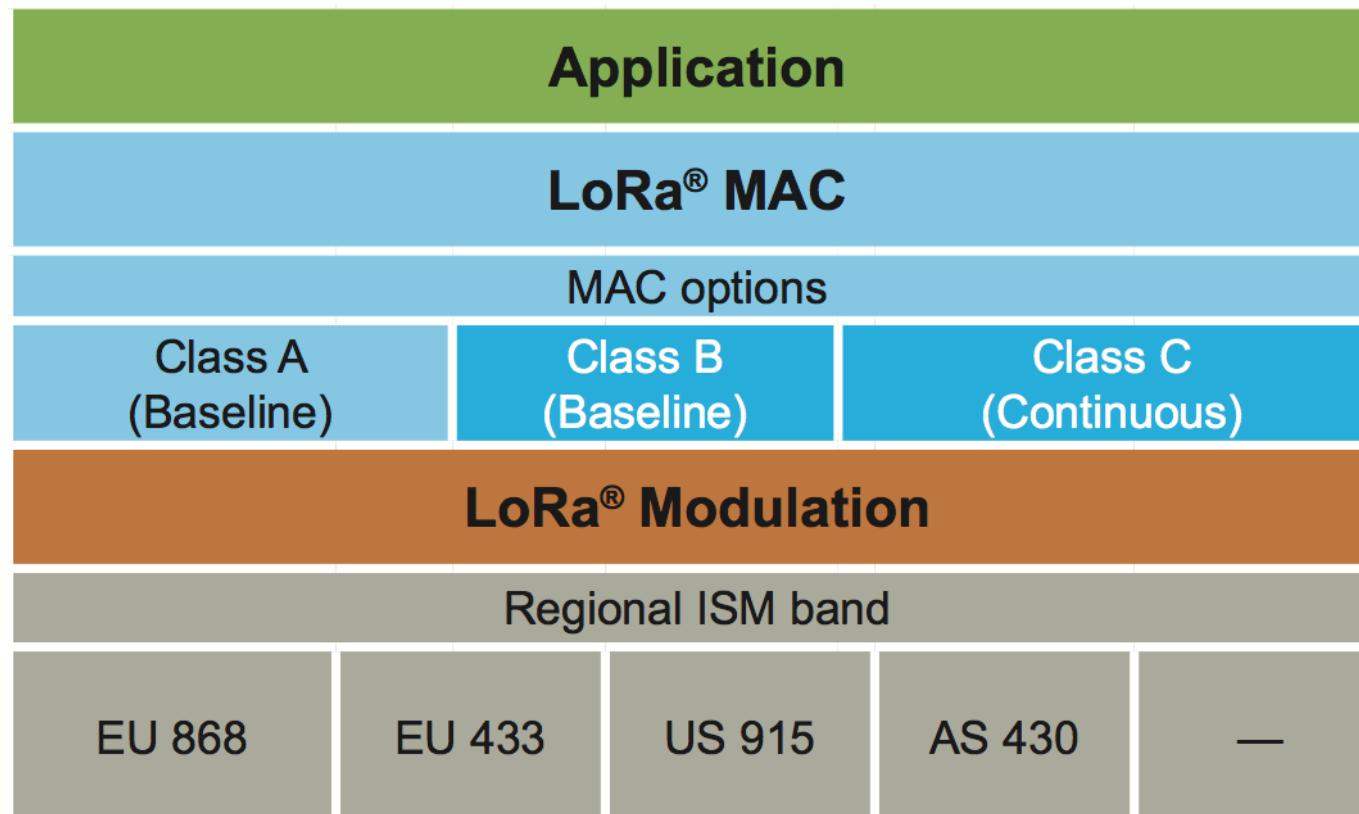
Sigfox - Architecture



LoRa

- Stands for “Long Range”
- To be used in long-lived battery-powered devices scenarios
- Semi-proprietary
 - Parts of the protocol are well documented, others not
 - They own the radio part (but sub-licensing is on the way)
 - You can install your own gateways
- LoRa usually means two different things:
 - LoRa: a physical layer that uses Chirp Spread Spectrum (CSS) modulation
 - LoRaWAN: a MAC layer protocol

LoRa Stack

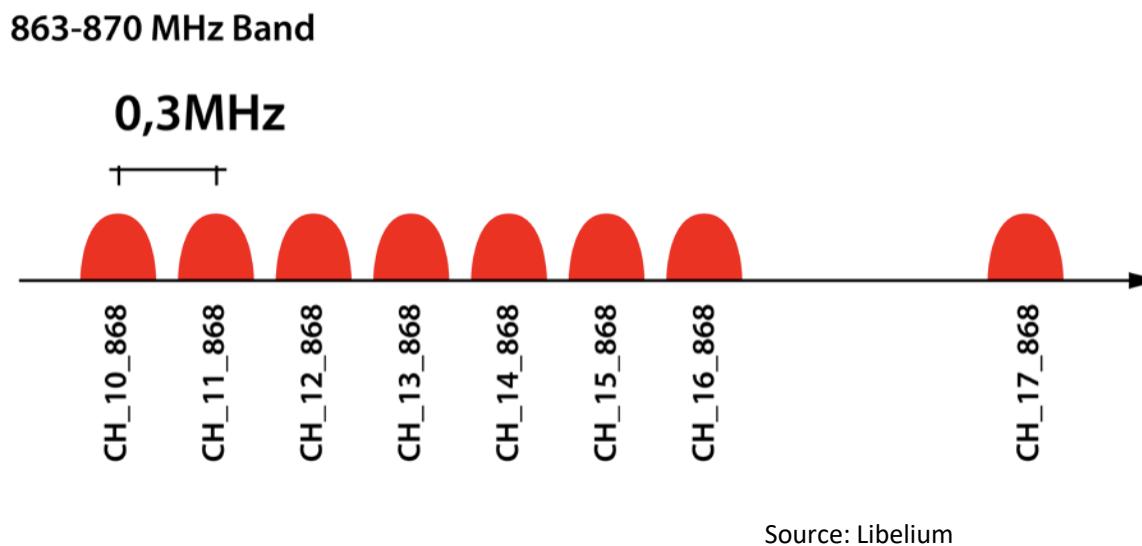


LoRa (the physical layer ☺)

- Developed by Semtech
- Low-range, low-power and low-throughput
- Operates on 433-, 868- (EU) or 915 (US) MHz bands
- Payload from 2 to 255 octets (2Kb)
 - Depends on configuration parameters
- Datarate: up to 50Kbps

LoRa (the physical layer ☺)

- In Europe, 8 channels with a bandwidth of 0.3MHz are used

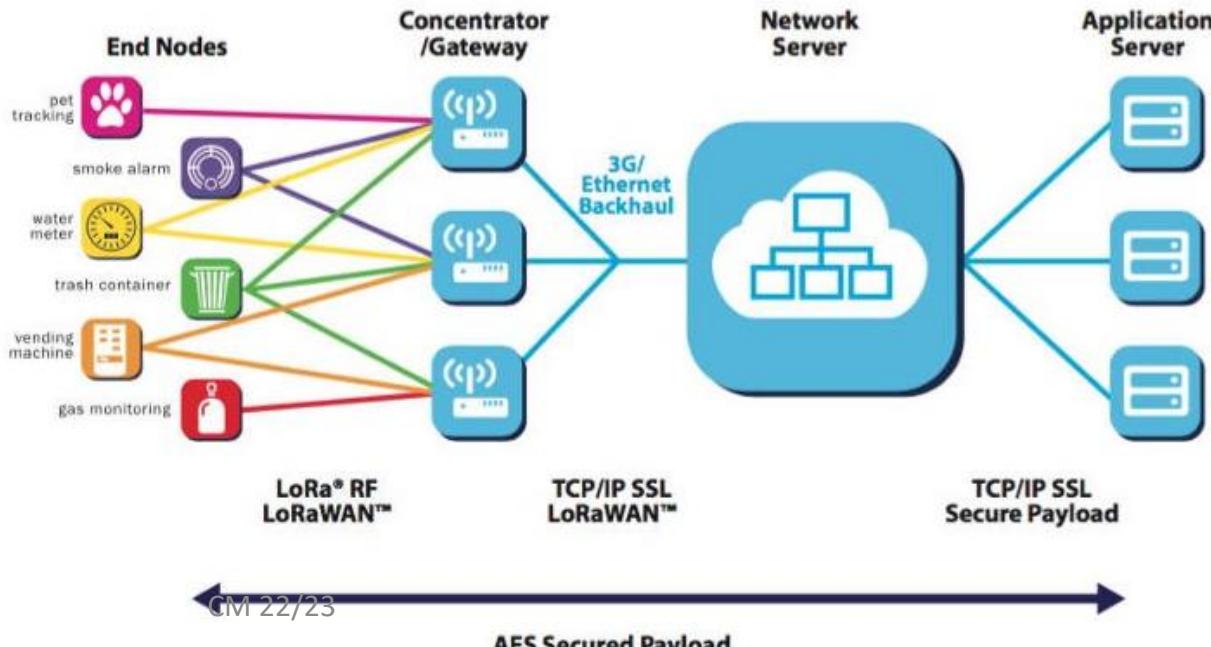


LoRaWAN

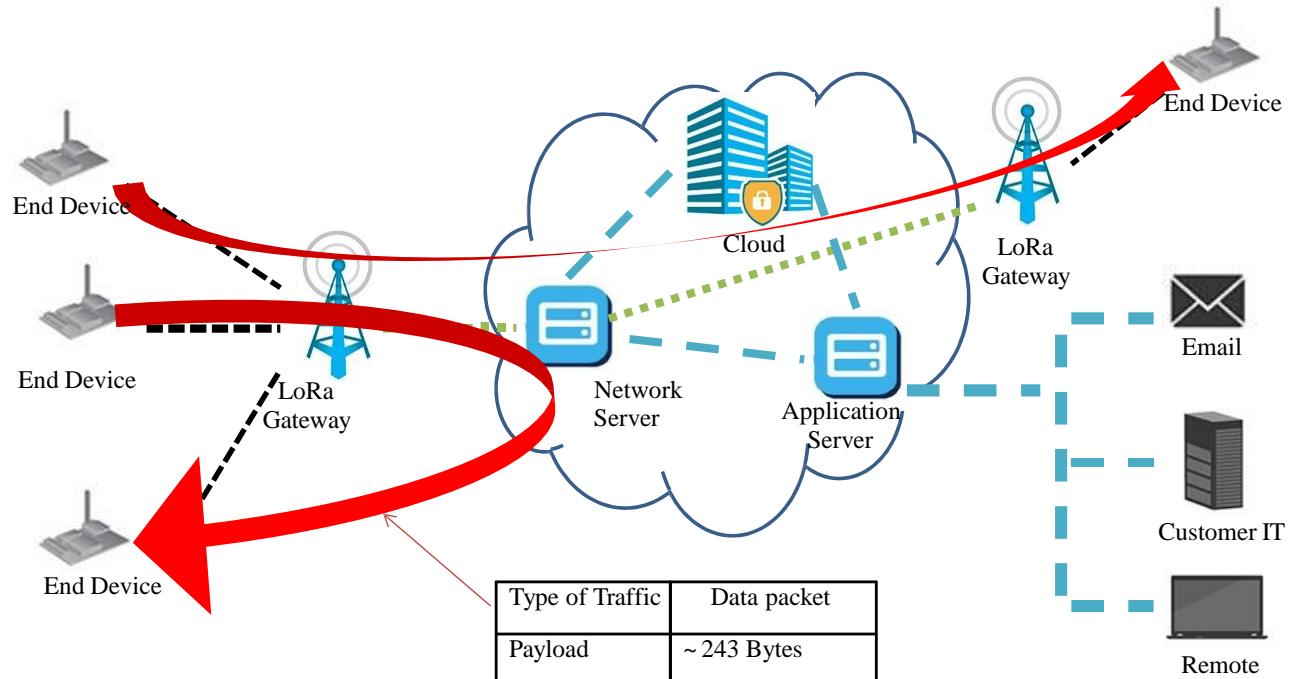
- MAC mechanism for controlling communications between end devices and LoRaWAN gateways. For all devices, it manages:
 - Communication frequencies
 - Data rate
 - Power
- Open Standard developed by the LoRa Alliance

LoRA Network

- Star of stars topology
- Devices transmit data asynchronously
 - Data is received by multiple gateways
 - Each gateway forwards received data to a centralized network server, using a backhaul link (Ethernet or cellular)
 - The network server:
 - Filters duplicate packets
 - Packet with the strongest signal gets decoded
 - Realizes security checks
 - Manages the network



LORA - Architecture



Modulation	LoRa RF (Spread Spectrum)
Range	~ 15 Km
Throughput	~ 50 Kbps

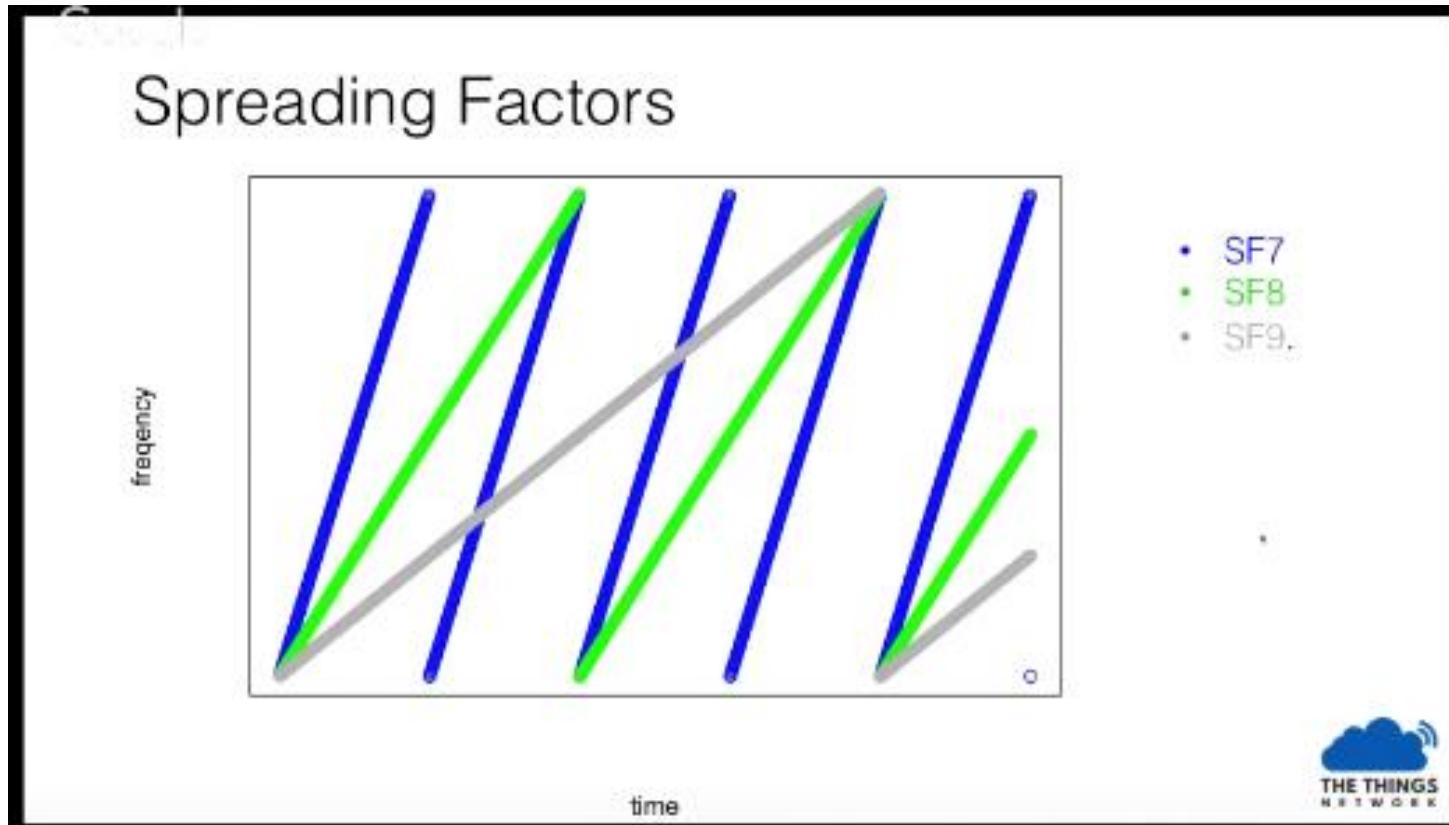
LoRa Physical Layer

- Modulation
 - (changing a signal, the carrier, in a way that allows it to contain information to be transmitted)
- LoRa uses a proprietary Spread-Spectrum modulation technique: Chirp Spread Spectrum (CSS)
 - (A chirp is a signal in which frequency raises or lowers with time)
 - Tries to increase range by:
 - Sending information with more power (within regulated values - <14dBm or 25mW)
 - Or by lowering the data rate
 - Increases link budget
 - Increases immunity to in-band interference
- This, along with Forward Error Correction techniques, contribute to extend the range and robustness of radio communication links
 - Compared to FSK

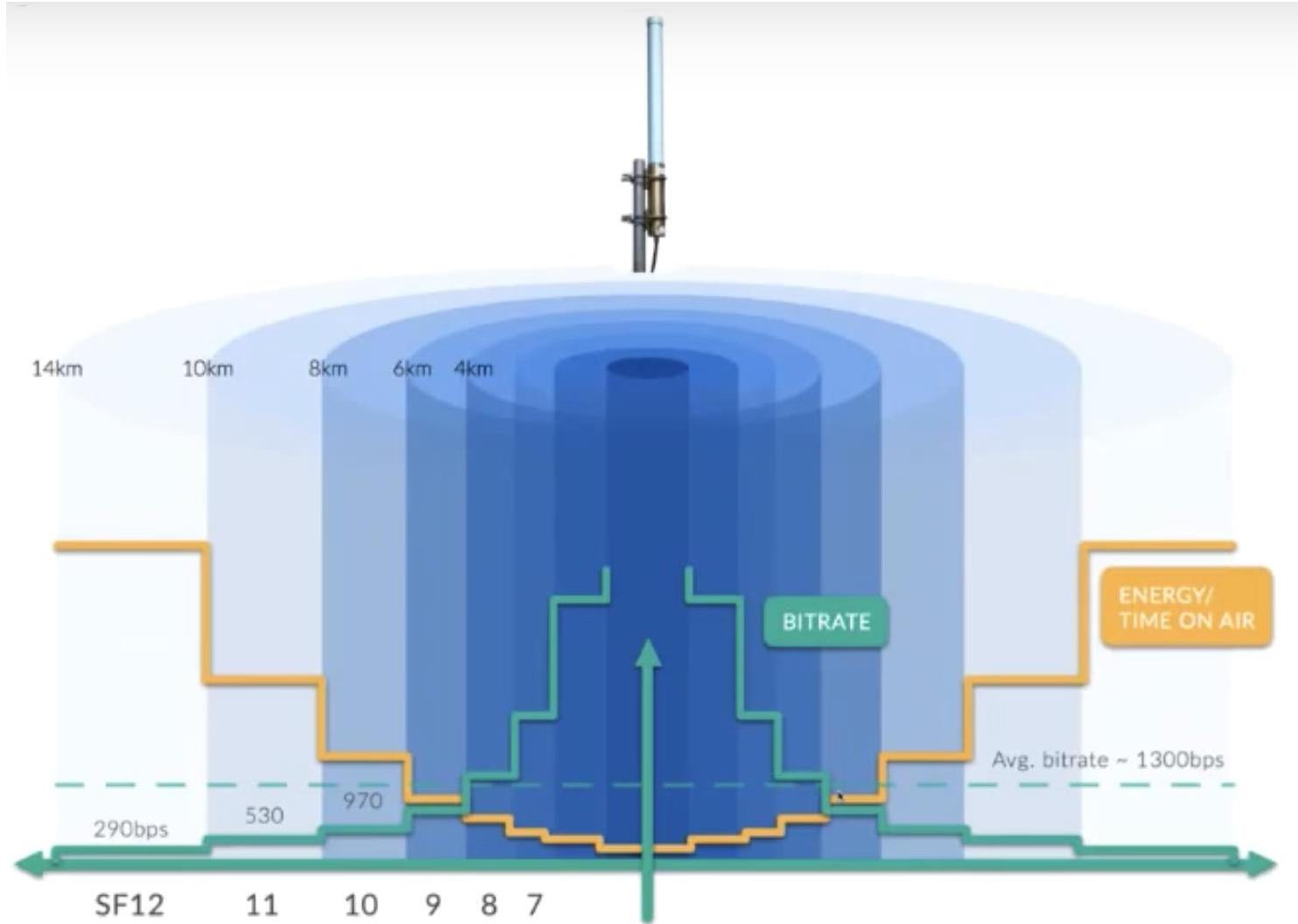
LoRa Physical Layer

- Has different Spread Factors (SF7 to SF12)
 - Spread factors can set the modulation rate and tune the distance
 - They indicate how fast or slow is the chirp (how many chirps you get per second) → **how much data you can encode per second**
 - The higher the SF, the lower the datarate
 - Each SF is 2x slower than the one before
 - The slower you send your data, the farther you can send it
 - The higher the SF, the more energy is required (time on air)
 - The interface has more time to decode and sensitivity is increased
- This helps on scaling the network
 - Closer nodes receive data much faster
 - Air is "cleared" for other nodes to transmit
 - By adding more gateways, devices get nearer to them, applying the above

LoRa Physical Layer



Source: Thomas Telkamp



LoRa Physical Layer

- For a 125kHz bw (configurable by design)

Spreading Factor	Symbols/second	SNR limit	Time-on-air (10 byte packet) - ms	Bitrate - bps
7	976	-7.5	56	5469
8	488	-10	103	3125
9	244	-12.5	205	1758
10	122	-15	371	977
11	61	-17.5	741	537
12	30	-20	1483	293

LoRa Physical Layer

- The Bandwidth (kHz), Spreading Factor and Coding Rate are design variables that allow a system to optimize the trade-off between
 - Occupied bandwidth
 - Data rate
 - Link budget
 - Interference immunity
- By using software, it is possible to combine these values to define a transmission mode

LoRa Physical Layer

- Bandwidth
 - Show how wide is going to be the transmission signal
 - 3 options: 125 kHz, 250 kHz or 500 kHz
 - Greater reach: 125 kHz
 - Greater transmission speed: 500 kHz
 - Less bandwidth = more airtime = more sensitivity = more battery consumed

LoRa Physical Layer

- Coding Rate
 - 4 options: 4/5, 4/6, 4/7 and 4/8
 - Meaning:
 - Every 4 useful bytes are going to be encoded by 5, 6, 7 or 8 transmission bits
 - Smaller coding rate: 4/8
 - Lower coding rate = more airtime

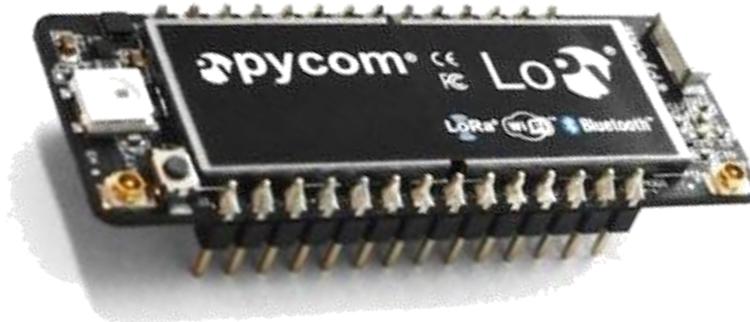
LoRa Physical Layer

- Spreading Factor
 - Number of chips per symbol used in data treatment before the transmission signal
 - 7 options: 6, 7, 8, 9, 10, 11 and 12
 - Greater Spreading Factor = Greater Range = more air time

LoRa Physical Layer

Mode	BW	CR	SF	Sensitivity (dB)	Transmission time (ms) for a 100-byte packet sent	Transmission time (ms) for a 100-byte packet sent and ACK received	Comments
1	125	4/5	12	-134	4245	5781	max range, slow data rate
2	250	4/5	12	-131	2193	3287	-
3	125	4/5	10	-129	1208	2120	-
4	500	4/5	12	-128	1167	2040	-
5	250	4/5	10	-126	674	1457	-
6	500	4/5	11	-125,5	715	1499	-
7	250	4/5	9	-123	428	1145	-
8	500	4/5	9	-120	284	970	-
9	500	4/5	8	-117	220	890	-
10	500	4/5	7	-114	186	848	min range, fast data rate, minimum battery impact

LoRa Physical Layer - Practical



- On the LoPy
 - Method
 - `lora.init(mode, *, frequency=868000000, tx_power=14,
bandwidth=LoRa.BW_125KHZ, sf=7, preamble=8,
coding_rate=LoRa.CODING_4_5,
power_mode=LoRa.ALWAYS_ON, tx_iq=False, rx_iq=False,
adr=False, public=True, tx_retries=1, device_class=LoRa.CLASS_A)`
 - Bandwidth: **LoRa.BW_125KHZ / LoRa.BW_250KHZ /
LoRa.BW_500KHZ**
 - SF: **sf=6 / sf=7 / sf=8 / sf=9 / sf=10 / sf=11 / sf=12**
 - Coding Rate: **LoRa.CODING_4_5 / LoRa.CODING_4_6 /
LoRa.CODING_4_7 / LoRa.CODING_4_8**

LoRaWAN

- Components
 - End-Device
 - Devices (low-power) that communicate with the LoRa Gateway
 - They are not associated to a particular gateway.
 - They are, however, associated to a Network Server.
 - Gateway
 - Intermediate devices that relay packets between end-devices and a network server.
 - Linked to the Network server via a higher bandwidth backhaul network.
 - They add information about the quality of reception, when forwarding a packet from an end-device to a network server.
 - They are transparent to the end-devices.
 - There are multiple gateways in a network
 - Multiple gateways can receive the same packet transmitted from the same end-device
 - Network Server
 - Decodes and de-duplicates packets sent from devices.
 - Generates packets to be sent towards devices
 - Chooses the appropriate gateway to send packets to a specific end-device

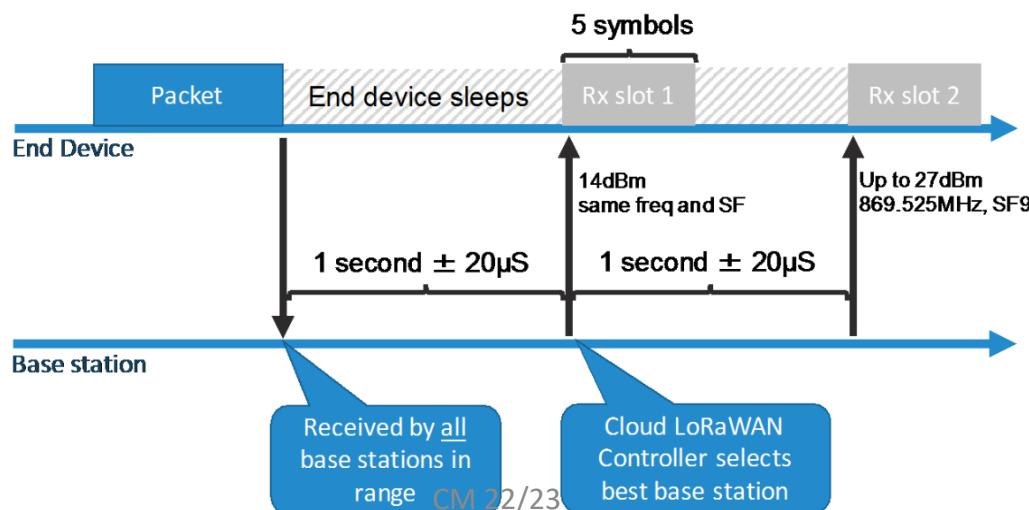
LORA – Device Classes

Classes	Description	Intended Use	Consumption	Examples of Services
A (`` all '')	Listens only after end device transmission	Modules with no latency constraint	The most economic communication Class energetically.. Supported by all modules. Adapted to battery powered modules	<ul style="list-style-type: none"> • Fire Detection • Earthquake Early Detection
B (`` beacon '')	The module listens at a regularly adjustable frequency	Modules with latency constraints for the reception of messages of a few seconds	Consumption optimized. Adapted to battery powered modules	<ul style="list-style-type: none"> • Smart metering • Temperature rise
C (`` continuous '')	Module always listening	Modules with a strong reception latency constraint (less than one second)	Adapted to modules on the grid or with no power constraints	<ul style="list-style-type: none"> • Fleet management • Real Time Traffic Management

Any LoRa object can transmit and receive data

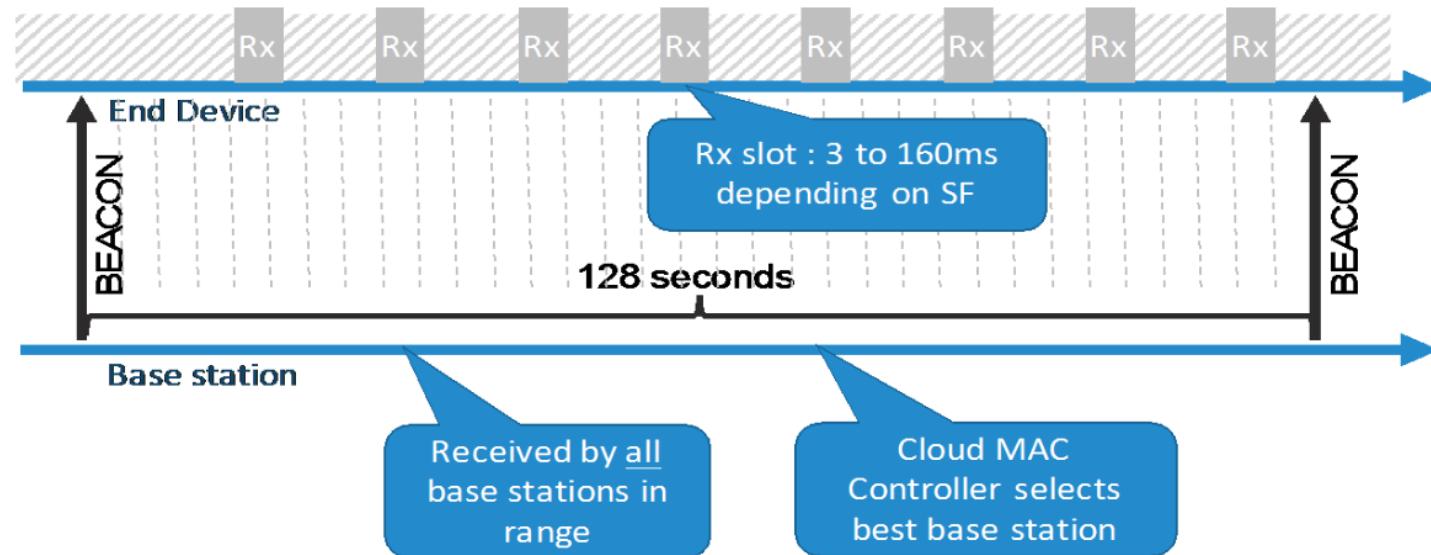
LoRaWAN

- End-devices classes
 - Class A – bi-directional
 - Lowest power consumption
 - Devices schedule uplink transmissions according to their requirements, with a small variation before transmission.
 - Each uplink transmission is followed by two short downlink receive windows
 - Downlink transmissions at any other time have to wait until the next uplink transmission
 - Less flexibility for downlink



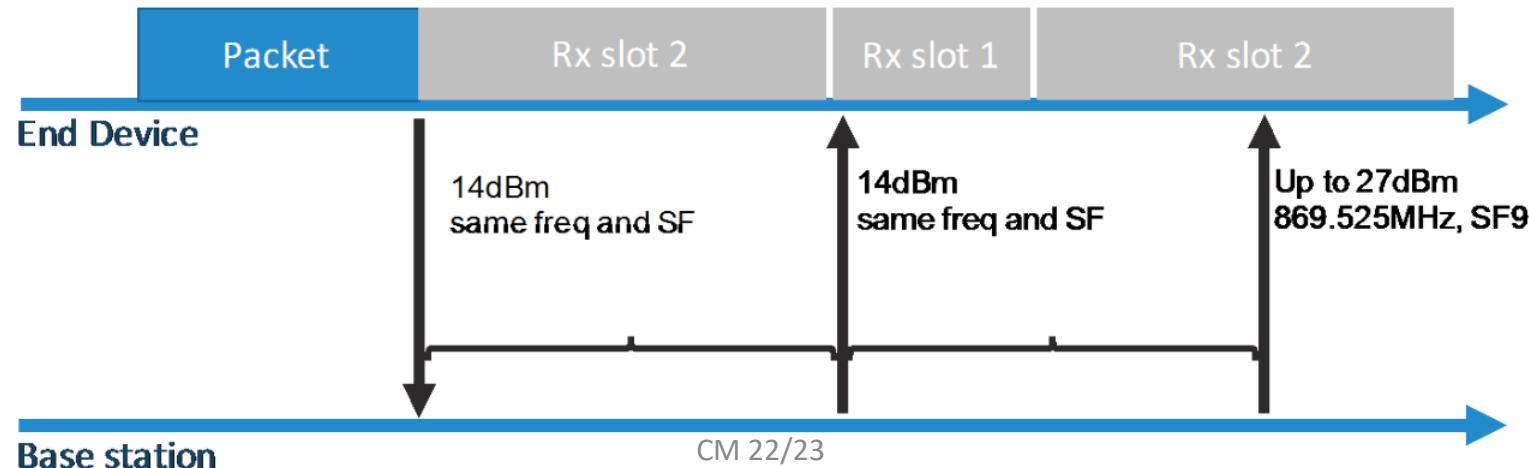
LoRaWAN

- End-devices classes
 - Class B – bi-directional with scheduled receive slots
 - Devices open more receive windows at scheduled times
 - There is a synchronized beacon from the gateway to the network server, indicating when the device is listening



LoRaWAN

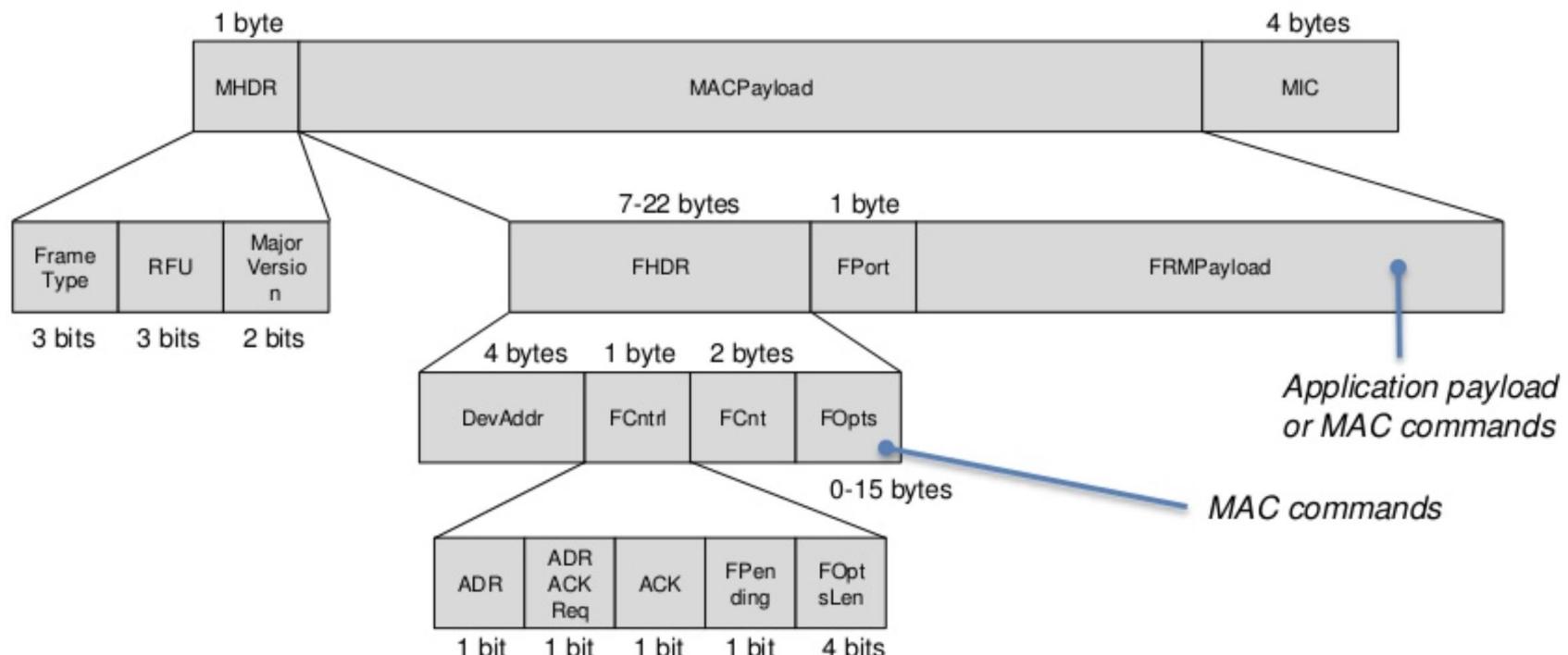
- End-devices classes
 - Class C – bi-directional with maximal receive slots
 - Greatest power consumption
 - Almost continuous receiving windows
 - Server can initiate transmission almost anytime



LoRaWAN

- End-Device Duty Cycle
 - Besides transmission frequency, duty cycle regulations apply
 - Delay between successive frames sent by a device
 - 1% limitation for end-devices
 - Device has to wait 100x the time it took for it to send the message, in order to be able to send again in the same channel
 - Gateways: 10%

LoRaWAN - Payload



Source: Stephen Pharrell

LoRaWAN

- *DevAddr* - short address of the device.
- *FPort* - multiplexing port field.
- *FCnt* - frame counter.
- *MIC* - cryptographic message integrity code
- *MType* - message type (uplink, downlink, confirmed (requires an ACK, ...)).
- *Major* - LoRaWAN version
- *ADR* and *ADRACKReq* - data rate control adaptation mechanism by the network server.
- *ACK* - acknowledges the last received frame.
- *Fpending* - indicates that there is still data to be sent by the network server (end-device is required to send another message to open a receive window).
- *FOptsLen* - length of the *FOpts* field in bytes.
- *FOpts* - contains MAC commands on a data message.
- *CID* - MAC command ID.
- *Args* -optional arguments of the command.
- *FRMPayload* - payload, encrypted using AES with a key length of 128 bits.

The minimal size of the MAC header is 13 bytes; its maximal size is 28 bytes.

There is no destination address on uplink packets, or source address on downlink packets.

LoRaWAN

- MAC Commands
 - Allows the network to customize end-device parameters
- Checks
 - Link status (this can be send by the end-device itself)
 - Device battery
 - Device margin (SNR)
- Settings
 - Datarate
 - TX power
 - TX and RX channels
 - RX timing
 - Repetition
 - Duty cycle
 - Dwell time

LoRaWAN

- End-Device Connection to a network
 - Also known as ***Activation***
- This process provides the end-device with:
 - End-device address (*DevAddr*): An identifier composed by the network identifier (7bit) and by the end-device's network address (25bit)
 - App identifier (*AppEUI*): Unique identification of the end-device owner
 - Network Session Key (*NwkSKey*): A key used by both the network server and end-device to verify and ensure message integrity
 - App Session Key (*AppSKey*): A key used by both the network server and end-device to encrypt the payload of received messages
- Note on security:
 - LoRaWAN protocol security is based on 802.15.4
 - AES-128

LoRaWAN

- To activate the device, there are two procedures:
 - Over-the-Air Activation (OTAA)
 - *Join-Request* and *Join-Response* messages are exchanged in each new session, allowing the end-devices to obtain the network and application session keys
 - Activation By Personalization (ABP)
 - The devices have both keys already stored internally

LoRaWAN

- Adaptive Data Rate
 - The network tells the node at which data rate it can send data
 - Manages the SF for each end-device
 - The aim is to:
 - Optimize for fastest data rate versus range
 - Maximize battery life
 - Maximize network capacity

LoRaWAN

- Typically, there is no node-to-node direct communication
 - LoRaWAN allows this by having 2 gateways and a network server in between the nodes
 - However, most end-device vendors also include (for testing, mostly) a raw form of LoRa
 - Allows peer-to-peer communication between nodes
 - Contains only the link layer protocol
 - Only allows a very small number of nodes in a topology
 - There is no packet management
- (useful for a first try with LoRa)

LoRaWAN vs NB-IoT

Table 5. NB-IoT vs. LoRaWAN average power consumption, latency, and throughput.

Features	NB-IoT	LoRaWAN
Joining network	3 mAh	1 mAh
Uplink message (44 bytes)	1.8 mAh	100 µAh
UE class	Cat NB1	A
Data rate (20 bytes)	0.6–4 bps	
Frequency	28 Mhz	EU868 MHz

The Things Network

- Built in a crowdsourced manner by companies and enthusiasts
 - Low density coverage, mostly in larger cities (5 GW in Aveiro)
 - 1-2Km range in cities, 10km in open space
- Provides a Free connectivity service, and broker with APIs
- Composed by:
 - Nodes: owned by companies and citizens, send data to Gateways
 - Gateways: owned by companies and citizens, interface with TTN
 - TTN Servers: Hosted by TTN, routing data to/from user apps

Cellular Networks

Mobile cellular networks

GSM to 5G

Wireless cellular network

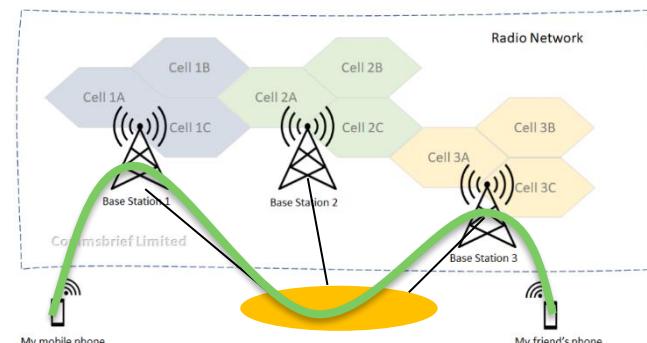
- **G = Generation**
- **Basic principle (at beginning): re-use of frequencies**
- **Single hop widespread wireless connectivity to the wired world**
 - **Usually space divided into cells, and MTs assigned to a cell**
 - **A base station is responsible for communicating with MTs in its cell**
 - Communications: a voice call or a data session.
 - **Handoff/handover occurs when a MT moves to a new base station, while busy on a call**
 - **Highly supported by a fixed (wired) transport network**
- **Cell size:**
 - **Highly variable**
 - **Technology dependent**
 - **Varies with expected number of users**

wikipedia

In telecommunication, a **public land mobile network (PLMN)** is a combination of wireless communication services offered by a specific operator in a specific country.^{[1][2]} A PLMN typically consists of several cellular technologies like **GSM/2G**, **UMTS/3G**, **LTE/4G**, offered by a single operator within a given country, often referred to as a **cellular network**.

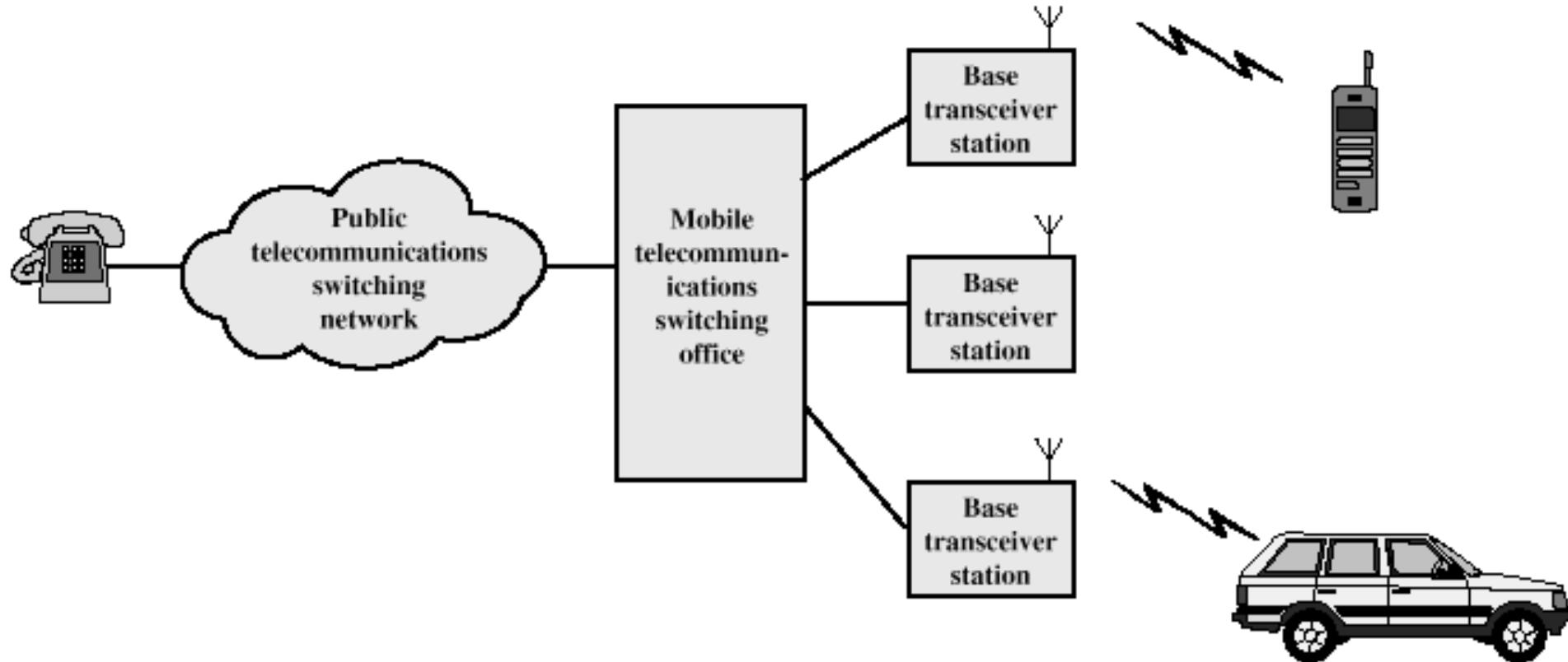
A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code).

Portugal, MCC: 268



<https://commsbrief.com/what-are-cells-in-mobile-communications/>

Cellular System Generic



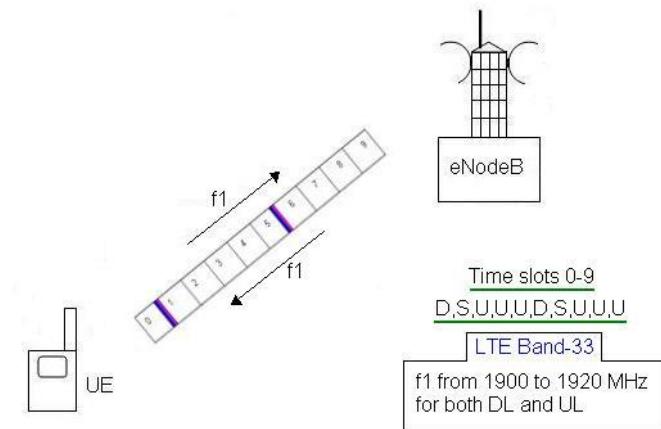
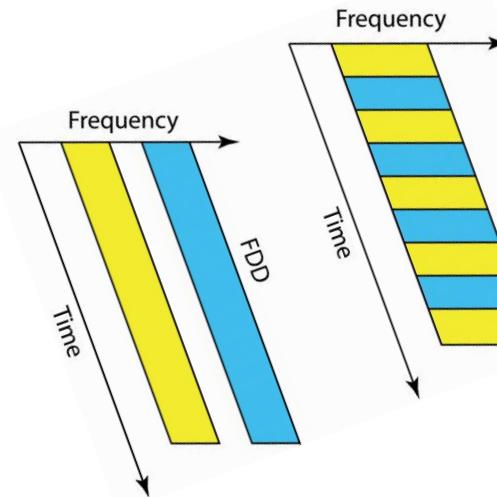
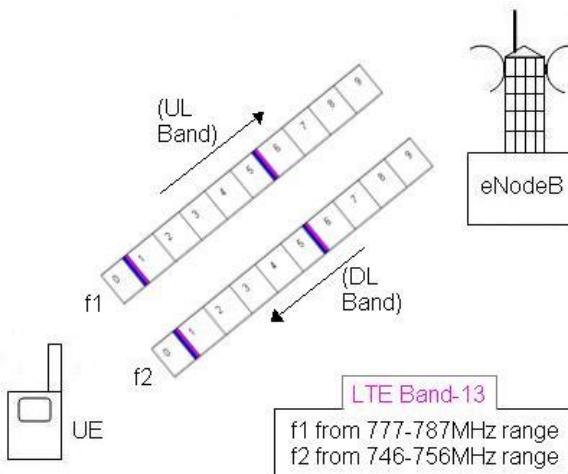
Service usage phases

- Mobile unit initialization/registration
- Mobile-originated call
- Paging
- Call accepted
- Ongoing call
- Handoff

FDD: Frequency Division Duplex

TDD: Time Division Duplex

FDD vs TDD



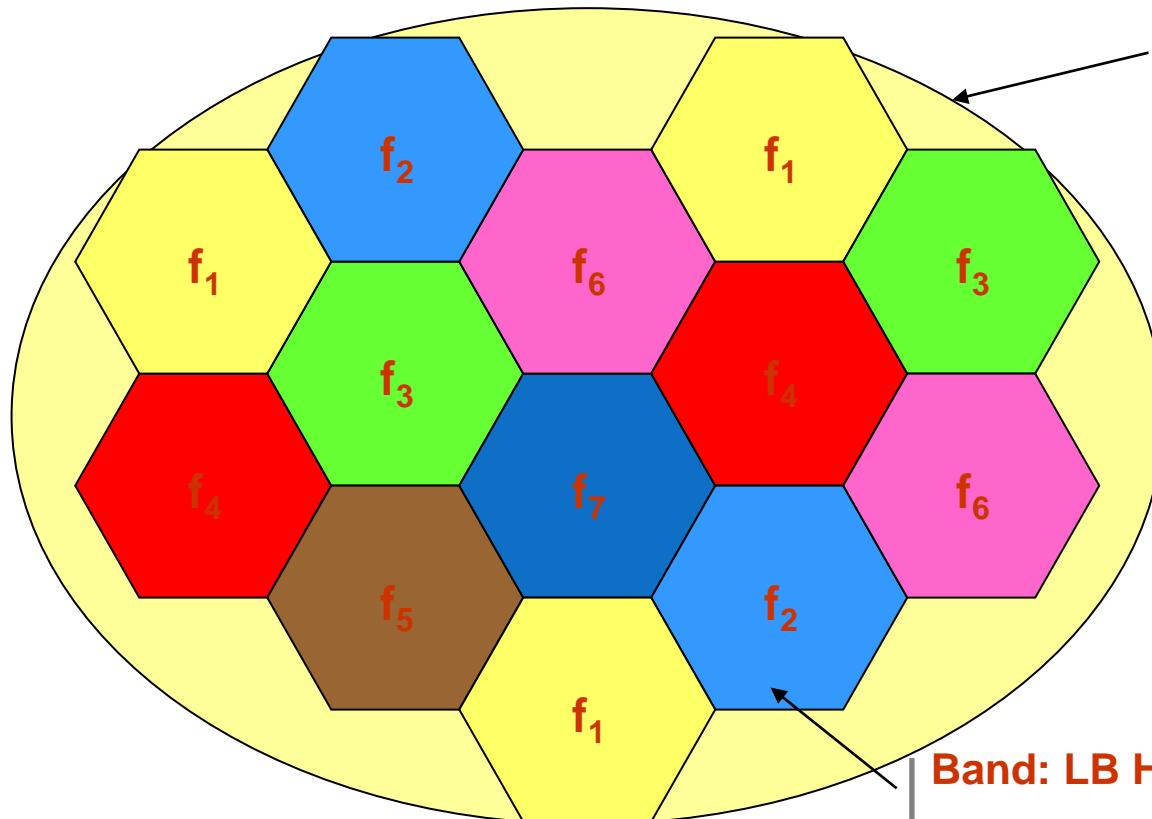
Advantages of TDD

- It does not use paired spectrum. Hence it benefits operators in terms of **efficient usage of spectrum**.
- It is used for **dynamic resource** requirements based on application and quality of service. This is possible due to **dynamic allocation of time slots** without changing the bandwidth once allocated. Hence TDD is best suited for unpaired spectrum scenarios requiring asymmetric data rates.
- FDD does not allow special techniques like multiple antennas, multiple input-output (MIMO), and beamforming

Disadvantages of TDD

- As TDD operates based on allocated time slots, it **requires stringent phase/time synchronization** to avoid interference between UL (Uplink) and DL (Downlink) transmissions.
- Uplink and downlink transmissions occur at different time instants at same carrier frequency. As transmissions are not continuous, the required data rates can not be achieved as compare to FDD at similar distances from Base Station.
- As **TDD supports lesser distances compare to FDD**, it needs more base stations to achieve given coverage area.
- Due to requirements of more Base stations, deployment and operating costs are higher in TDD.

Cells and spectrum efficiency



Band: LB Hz

$LB \rightarrow k$ sub-bands (f_1, \dots, f_k)

1 sub-band $\rightarrow n$ channels (TDMA)

Capacity = $k \times n$ channels

($7 \times 10 = 70$ channels)



Band: LB Hz (the same)

sub-bands:

$$3 \times f_1 + 2 \times f_2 + 2 \times f_3 + 2 \times f_4 + 1 \times f_5 + 2 \times f_6 + 1 \times f_7 \\ = 13 \text{ sub-bands}$$

Capacity = $13 \times 10 = 130$ channels!

Cell: Pros/Cons

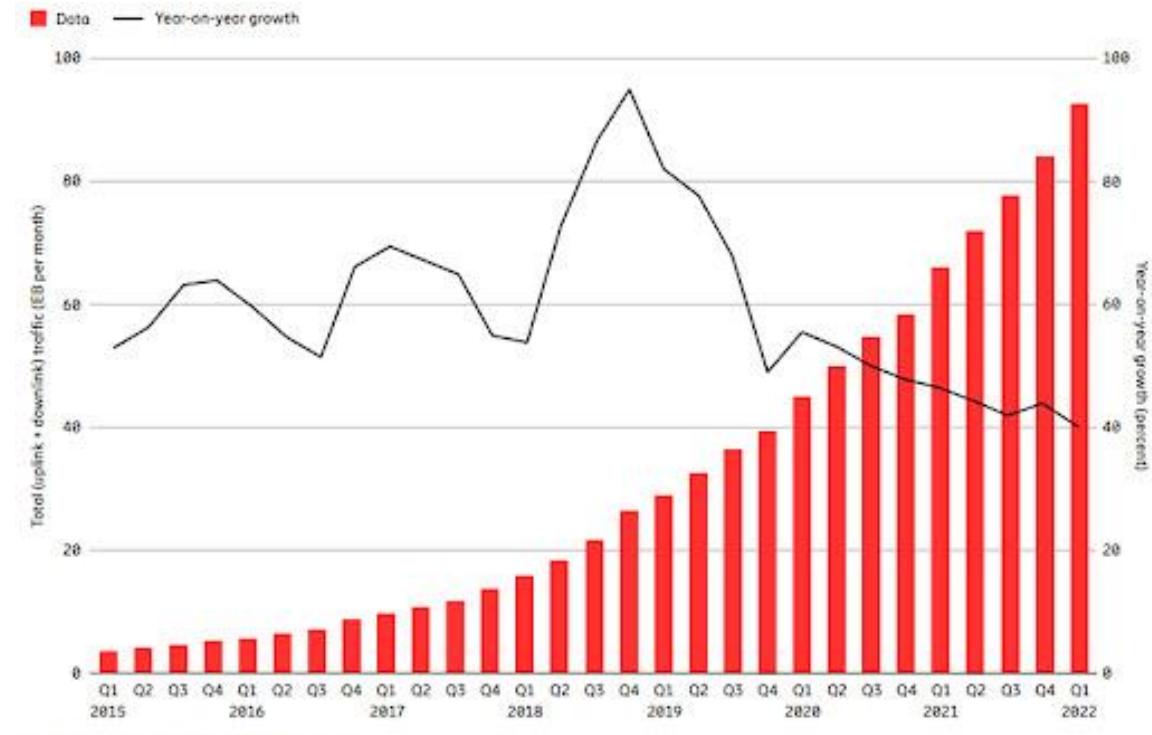
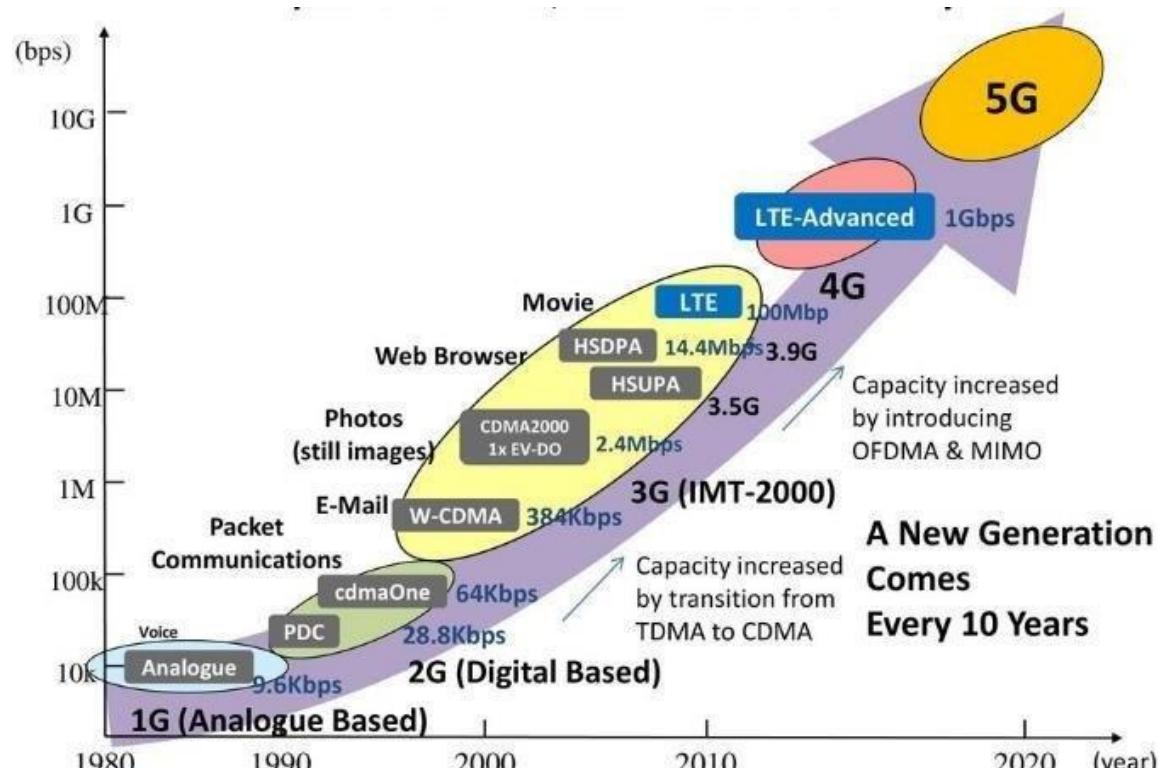
- **Fundamental:**
 - Each cell handles interferences, coverage areas, etc... locally
 - Cell planning
 - Cell size
 - Frequency/code usage
 - Channels (logical/physical) reservation
- **Advantages:**
 - > capacity
 - > # users
 - < power
 - Reliability (distributed system)
- **Disadvantages**
 - Needs interconnection network between cells
 - Needs to support Handovers!
 - Needs to handle inter-cell interference!

Technological waves

Adaptado de: Qualcomm "What's in the future of 5G?"

Mobile voice communication	Digital mobile voice SMS/MMS	Broadband mobile data	Broadband mobile data massification	Unified future-proof platform
1G	2G	3G	4G	5G
1980	1990	2000	2010	2020
Analogue voice C450, NMT, AMPS, TACS	D-AMPS, GPRS, GSM, SMS/MMS, CDMA	UMTS/CDMA2000, HSPA+, Smartphones	LTE, LTE Advanced, Gigabit LTE, OFDM	5G New Radio, SDN, NFV, ML/AI
Analogue system Copper cables	PSTN, X.25, Frame Relay, ATM, DOCSIS	xDSL, IP/MPLS, Digital Television, SD Video	Data < 1 Gbps	eMBB 10 Gbps
			IMS, VoLTE, IoT, IPTV, GPON/FTTH, Cloud, Video HD	Massive MIMO, Beam forming, Slicing, mIoT, XGS-PON, Ultra HDTV

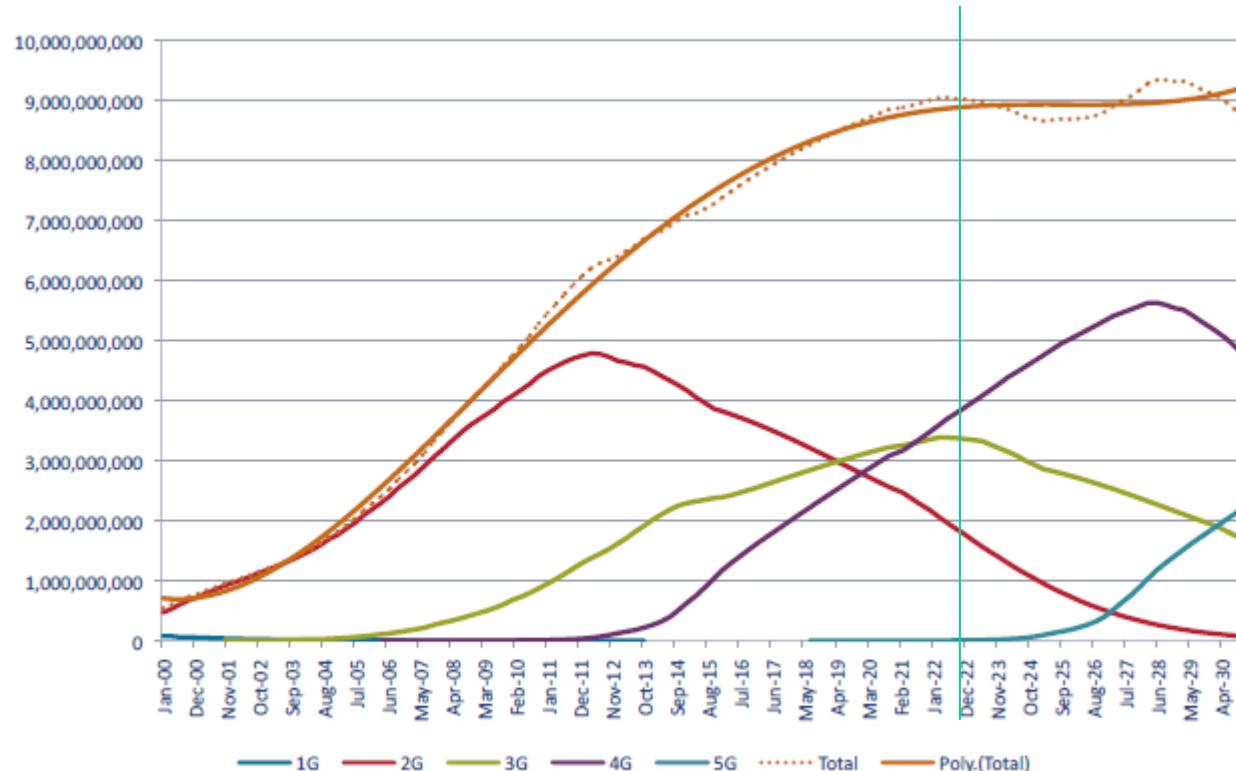
Technologies and usage evolution



Number of mobile subscriptions worldwide

Mobile Subscriber Evolution (excluding m2m) extrapolated to 2030

INSTITUTE FOR COMMUNICATION SYSTEMS
5G INNOVATION CENTRE



Assumptions

- Growth rate and profile follow previous generations
- April 2016 to 2020 GSMA forecasts
- 2020 to 2030 Extrapolated scenario using historical profiles by RTACS ltd.

Source: GSMA and RTACS Ltd.

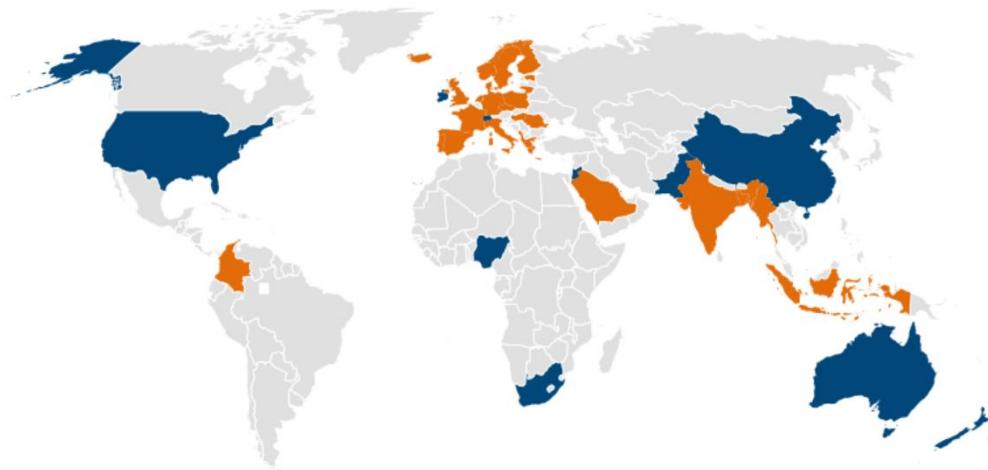
Stuart Revell, 5G Huddle 26th April 2016

<https://blog.3g4g.co.uk/2016/05/4g-lte-by-stealth.html>

2G and 3G Switch-Off

2G

■ Completed ■ Planned



■ Completed ■ Planned ■ In Progress

3G

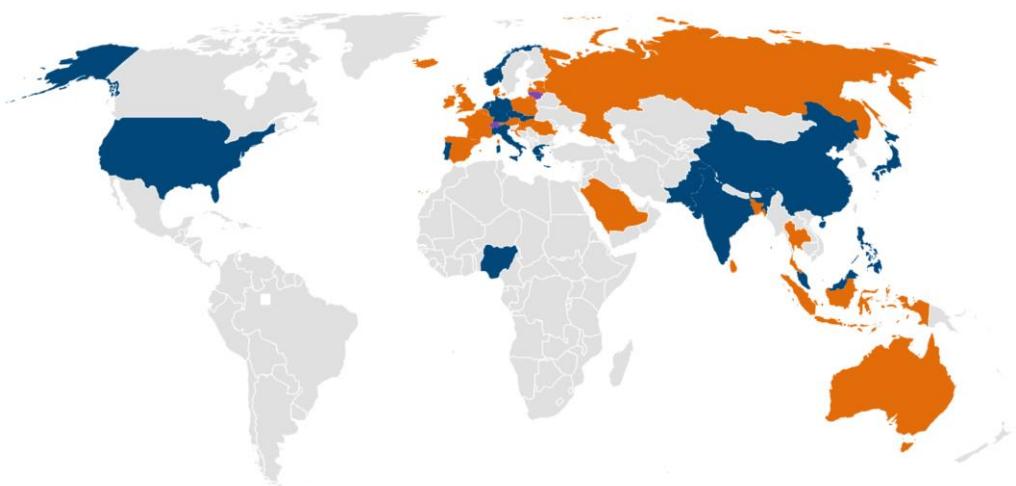
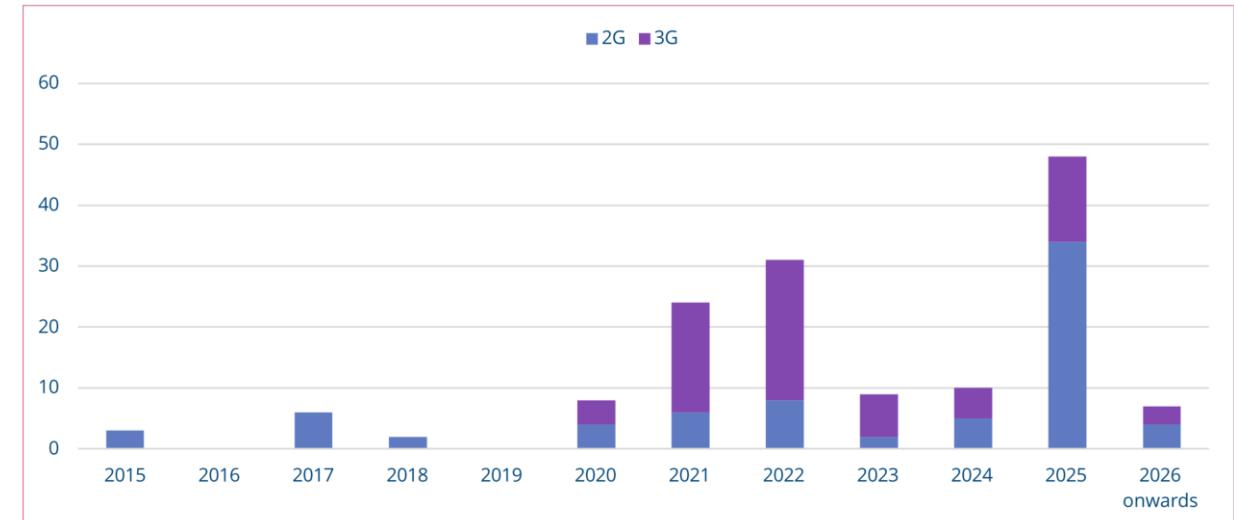


Figure 2. 2G and 3G network switch-offs by year



The rate of switch-off for both technologies will continue to increase, with the shutdown of 3G in particular outpacing that of its predecessor

By the end of June 2022, GSA had identified 135 operators that have either completed, planned or are in progress with 2G and 3G switch-offs in 68 countries and territories

75 operators in 42 countries and territories have either completed or planned 2G switch-offs

- Of those, 23 operators in 14 countries and territories have completed 2G switch-offs
- 52 operators in 32 countries and territories have planned 2G switch-offs

75 operators in 40 countries and territories have either completed, planned or are in progress with 3G switch-offs

- Of those, 26 operators in 15 countries and territories have completed 3G switch-offs
- 44 operators in 30 countries have planned 3G switch-offs
- 5 operators in 5 countries and territories have 3G switch-offs in progress

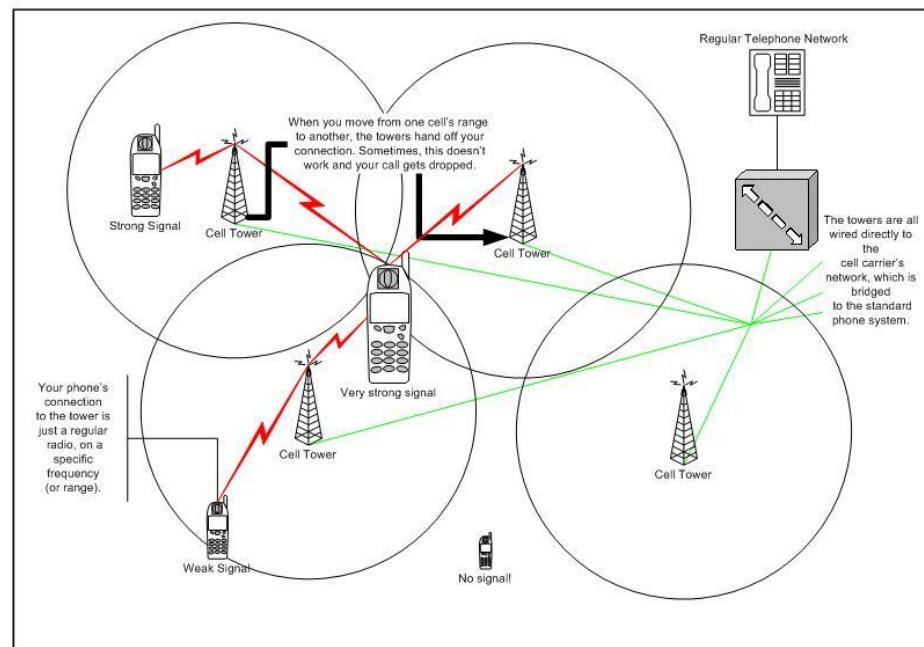
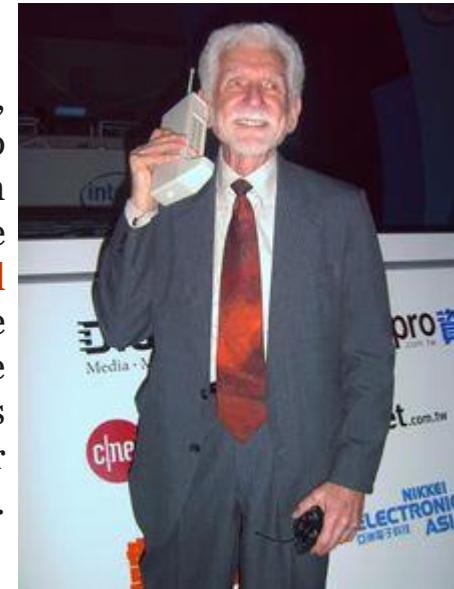
1G

Mobile voice

First-Generation Analog

- Advanced Mobile Phone Service (AMPS)
 - In North America, two 25-MHz bands allocated to AMPS
 - One for transmission from base to mobile unit
 - One for transmission from mobile unit to base
 - Each band split in two to encourage competition
 - Frequency reuse exploited

Martin Cooper, American engineer who led the team that in 1972–73 built the first mobile cell phone and made the first cell phone call. He is widely regarded as the father of the cellular phone.



<https://telephoneworld.org/cellular-phone-history/analog-cellular-amps-1g/>

1G characterization

Most popular 1G system during 1980s

- Advanced Mobile Phone System (AMPS)
- Nordic Mobile Phone System (NMTS)
- Total Access Communication System (TACS)
- European Total Access Communication System (ETACS)

Key features (technology) of 1G system

- Frequency 800 MHz and 900 MHz
- Bandwidth: 10 MHz (666 duplex channels with bandwidth of 30 KHz)
- Technology: Analogue switching
- Modulation: Frequency Modulation (FM)
- Mode of service: voice only
- Access technique: Frequency Division Multiple Access (FDMA)

Disadvantages of 1G system

- Poor voice quality due to interference
- Poor battery life
- Large sized mobile phones (not convenient to carry)
- Less security (calls could be decoded using an FM demodulator)
- Limited number of users and cell coverage
- Roaming was not possible between similar systems

2G

**Global System for Mobile Communications
(GSM)**

2nd Generation: GSM

- Defined by CEPT/ETSI
- Requirements in terms of:
 - Services Portability, =PSTN
 - QoS = PSTN
 - Security Low cost cipher
 - RF Usage Efficiency
 - Network Numbering ITU-T, SS-7
 - Cost Low

Differences with the first Generation Systems

- Digital traffic channels
 - first-generation systems are almost purely analog; second-generation systems are digital
- Encryption
 - all second generation systems provide encryption to prevent eavesdropping
- Error detection and correction
 - second-generation digital traffic allows for detection and correction, giving clear voice reception
- Channel access
 - second-generation systems allow channels to be dynamically shared by a number of users

Basic Architecture

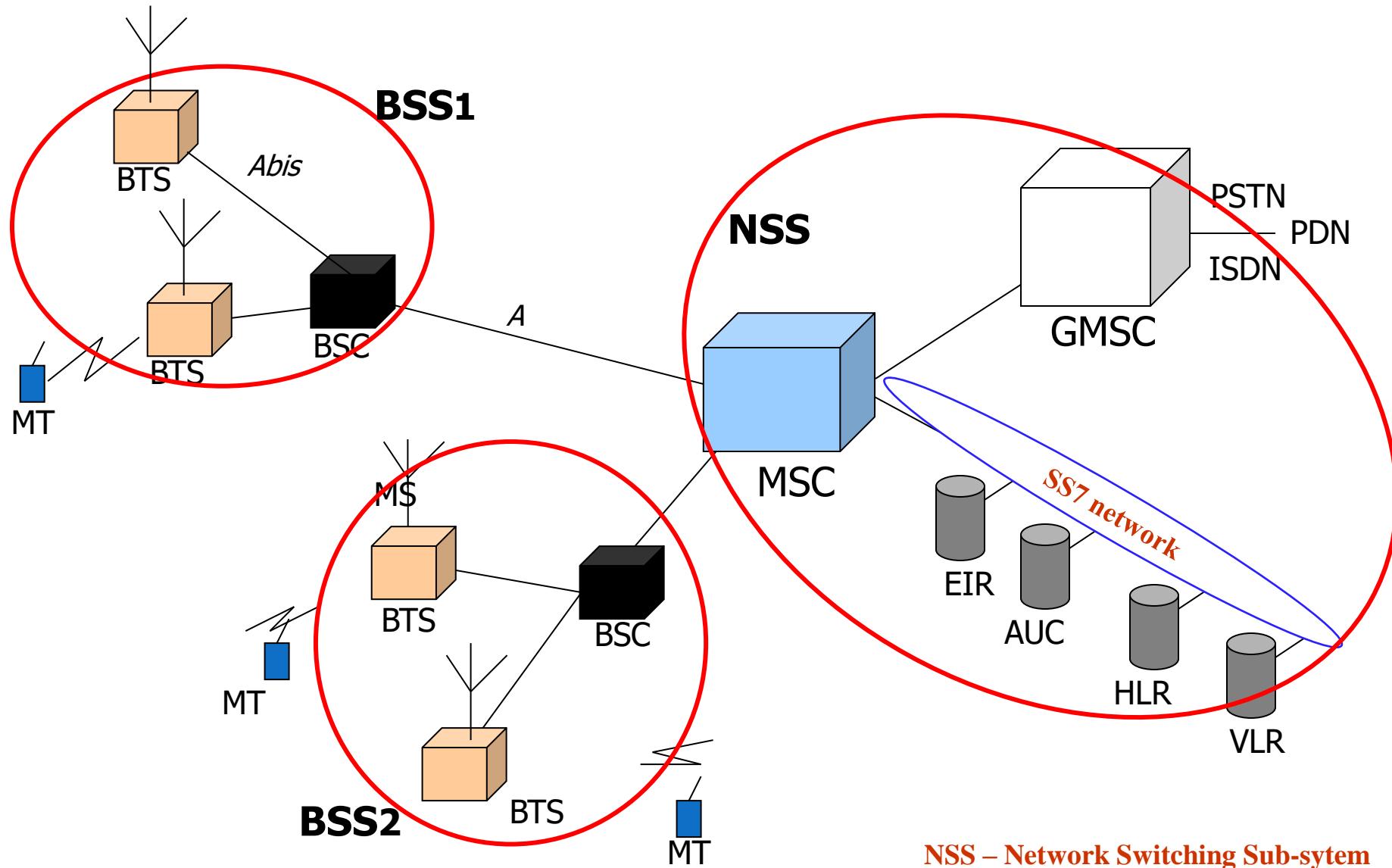
- Defines cells
- Defines a Mobile Terminal

Mobile Equipment + Subscriber Identity Module
(etc...; e.g. International Mobile Station Equipment Identity (IMEI))
- Uses a Network Subsystem

MSC; HLR, VLR
- Uses a Radio Subsystem

BSS; BT_{ransceiver}S, BSC_{ontroller}
- Defines an Operation Support Subsystem
 - The Base Station Subsystem (BSS) is structured as **Base Station Controllers (BSC)** + **Base Transceiver Station (BTS)**
 - BSCs are connected to the **Mobile Switching Center (MSC)** through physical lines
 - MSCs are interconnected to each other
 - There are MSCs connected to the public network (PSTN), the **Gateway Mobile Switching Center (GMSC)**.

GSM Architecture



NSS – Network Switching Sub-system
BSS – Base Station Sub-system

Mobile Switching Center

- **MSC = local switching center**
 - **Contains:**
 - Home Location Register (HLR)
 - Visitor Location Register (VLR)
 - Authentication Center (AuC)
 - Equipment Identity Registry (EIR)
- **Connects the BSS (Base Station Subsystem)**
 - **Master of the cell, define channels and access to them...**
- **Contains the registers for “their” mobile terminals**
- **Specific signalling channels**
 - **MT-BS (MSC): location, call setup, received call answer**
 - **BS (MSC)-MT: cell identification, location update, received call setup**

Network Subsystem DBs

- **HLR - Home Location Register**
 - **maintains permanent information about the subscribers of a GSM network (subscriber record)**
 - Subscription data: IMSI, MSISDN, subscription type (restrictions, supplementary services, ...)
 - **tracks the location and state of the mobile terminal within the network**
 - Location information: mobile VLR number.
- **VLR - Visitor Location Register**
 - **maintains temporary information about the subscribers registered on a GSM network (including subscribers in roaming)**
 - Data: IMSI, MSISDN, TMSI, MSRN, subscription type, location area, ...
 - **keeps up-to-date information about the location of the user within the network**

Network Subsystem DBs

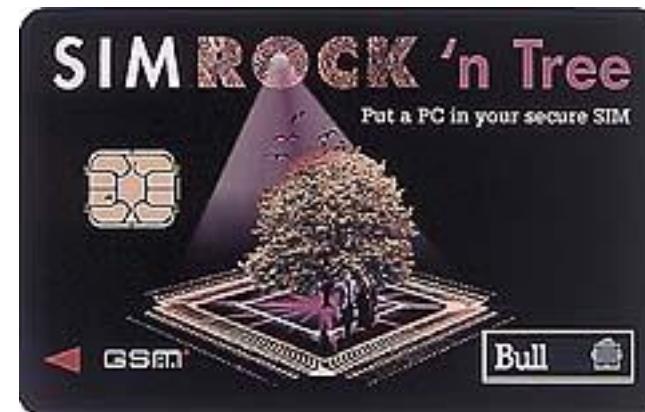
- AuC – Authentication Center
 - service responsible for the authentication of the subscribers
 - maintains the encryption algorithms
 - maintains the secret key (ki) for each subscriber
 - generates the session keys
- EiR – Equipment Identity Register
 - provides security mechanisms for the mobile equipments
 - keeps lists of mobile equipments
 - white list (authorized)
 - gray list (under “observation”)
 - black list (blocked)

Mobile Station

- Mobile Station (MS) communicates across Um interface (air interface) with base station transceiver in same cell as mobile unit
- Mobile equipment (ME) – physical terminal, such as a telephone
 - ME includes radio transceiver, digital signal processors and subscriber identity module (SIM)
- GSM subscriber units are generic until SIM is inserted

SIM: Subscriber Identity Module

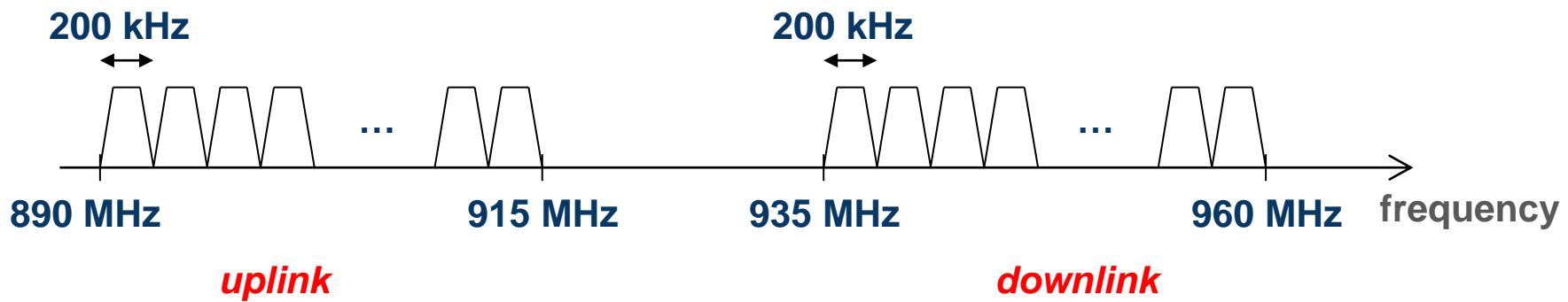
- **Informations:**
 - subscriber identity, password (PIN), subscription information (authorized networks, call restrictions, ...), security algorithms, short numbers, last received/dialed numbers, last visited location area, ...
- **SIM card + GSM terminal = access to GSM services**



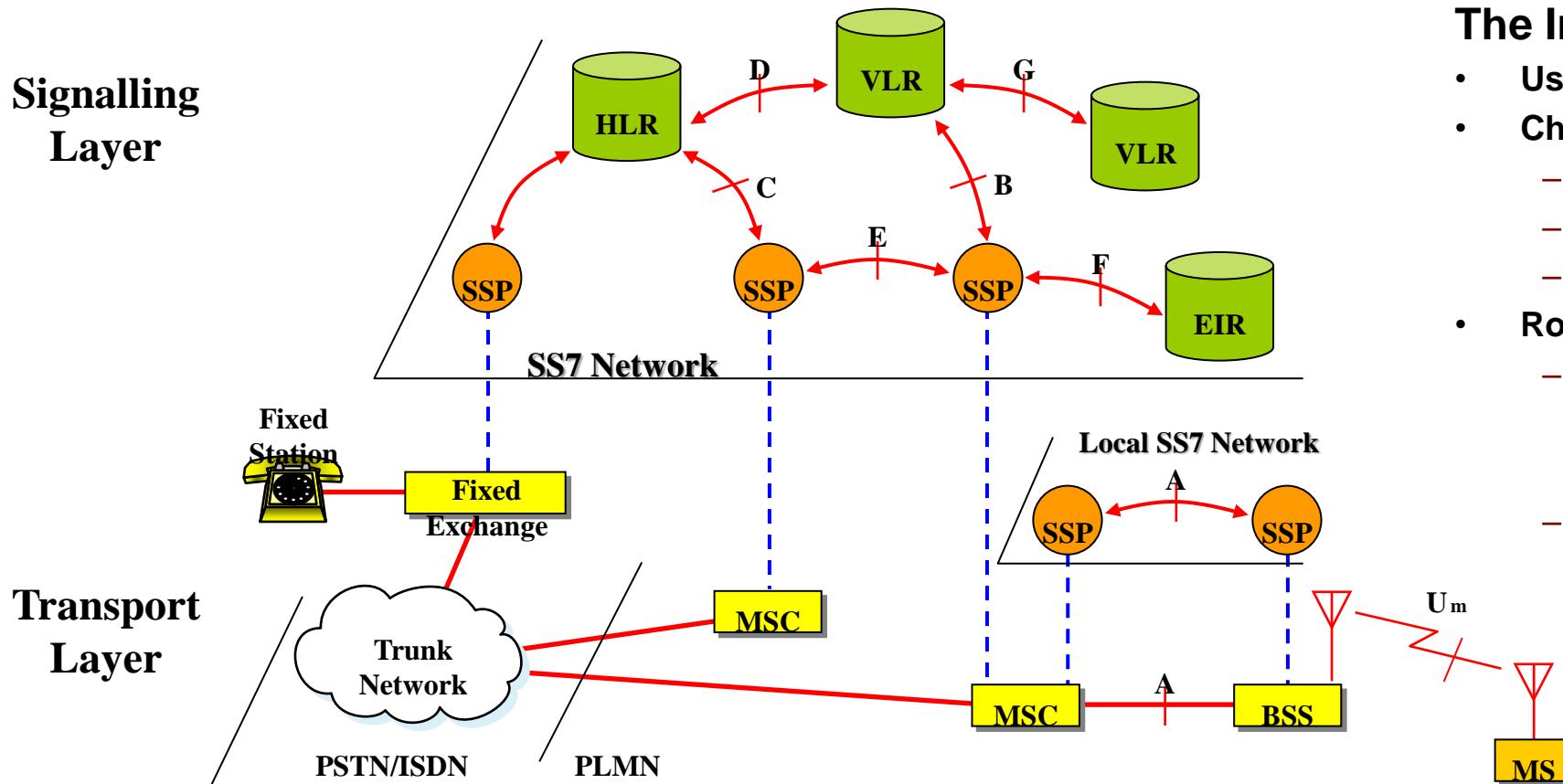
Air interface (Um) – channel allocation

- **GSM uses:**

- FDD (Frequency Division Duplexing) for duplexing
- TDMA (Time Division Multiple Access) with 8 time-slots for multiple access
 - Three slots delay (up and down) → avoids simultaneous rx/tx
- 200 kHz frequency channels (124 in GSM 900) for each cell, 124 channels per band (=> maximum 8 users per channel)



GSM Signalling and Transport Layers



MSC - Mobile Services Switching Centre
BSS - Base Station System
HLR - Home Location Register
VLR - Visitor Location Register

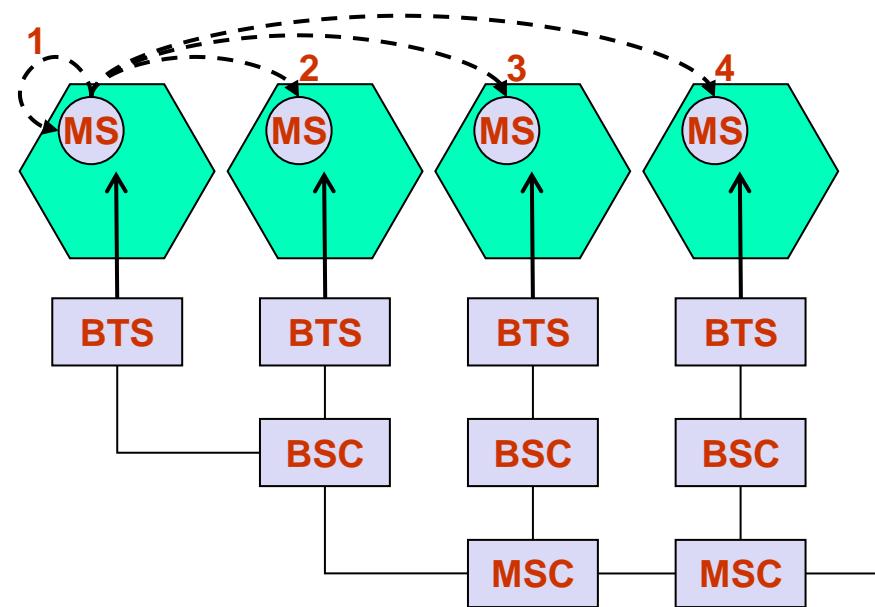
EIR - Equipment Identity Register
MS - Mobile Station
SSP - Service Signalling Point in SS7 Network

The Intelligent Network (IN)

- Uses Signalling System No. 7 (SS7)
- Charging options
 - Freephone
 - Local rates
 - Premium rates
- Routing options
 - Group calls
 - Network call centre options
 - Virtual Private Networks
 - Personal calls
 - one number
 - configurable routing

Types of handover (GSM)

1. Intra-cell: from a channel to another within the same cell
2. Inter-cell, Intra-BSC: from a channel in one cell to a channel in another cell, both controlled by the same BSC
3. Inter-BSC, Intra-MSC: from a channel in one cell to a channel in another cell, controlled by different BSCs, under the same MSC control
4. Inter-MSC: from a channel in one cell to a channel in another cell connected to different MSCs



Short Message Service - SMS

- Supports the transmission of messages up to 160¹ characters, between mobile terminals
- Messages are transmitted through the signalling channels
- Is used for a variety of applications:
 - text messages between users (very popular)
 - broadcast of information by the network operator (e.g. promotions)
 - broadcast of location-dependent information (e.g. local restaurants)
 - access to computing applications (e.g. home banking and e-mail)
 - configuration of mobile terminals over the air

¹ When using (7 bits/character); only 70 characters when using other codes (8 bits).

Twitter began as an SMS text-based service. This limited the original Tweet length to 140 characters (which was partly driven by the 160 character limit of SMS, with 20 characters reserved for commands and usernames). Over time as Twitter evolved, the maximum Tweet length grew to 280 characters - still short and brief, but enabling more expression.

2.5G

General Packet Radio Service (GPRS)

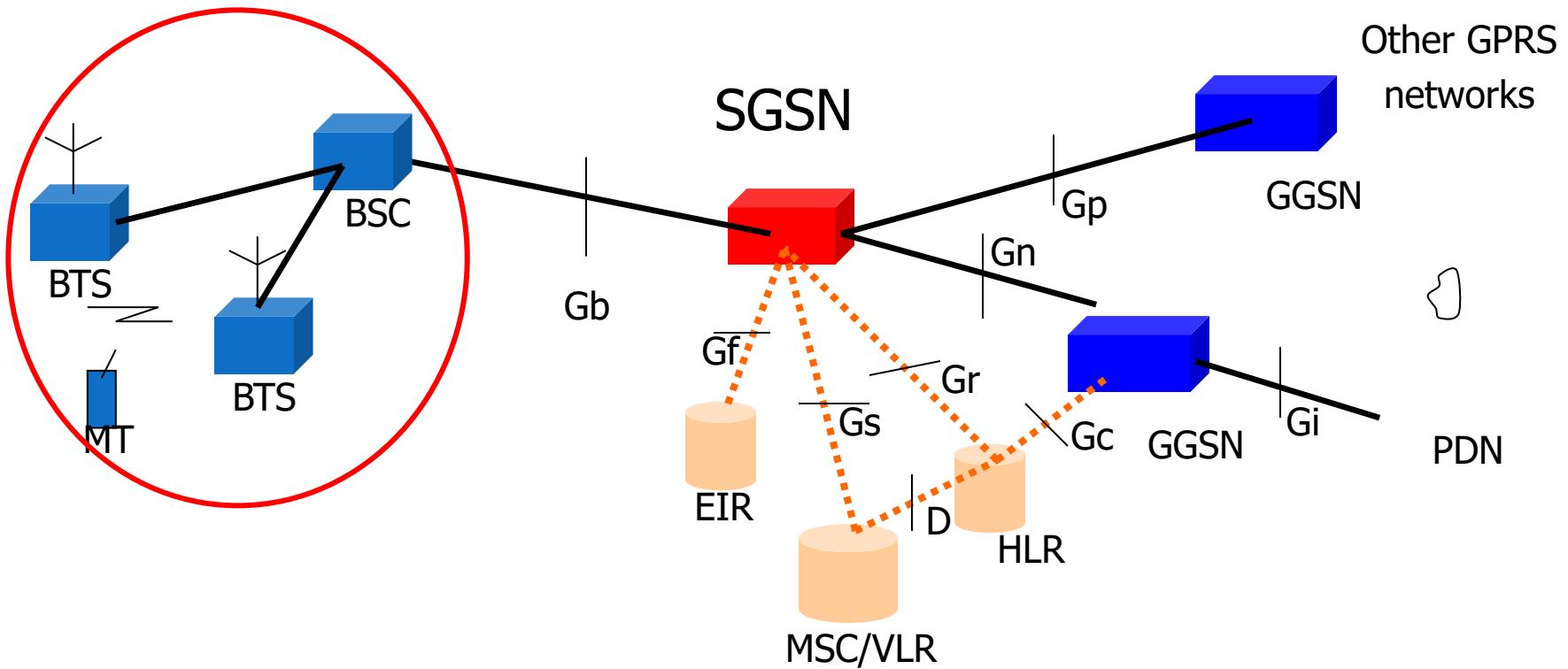
GPRS

- GPRS: *General Packet Radio Service*
- Packet-oriented transport service, for data network connections (Internet)
 - Better transmission bit rates (max 150kbps)
 - Allows burst communications (“immediate”: connections in <1s)
 - New network applications
 - New billing mechanisms (user-oriented: by traffic, p.ex.)

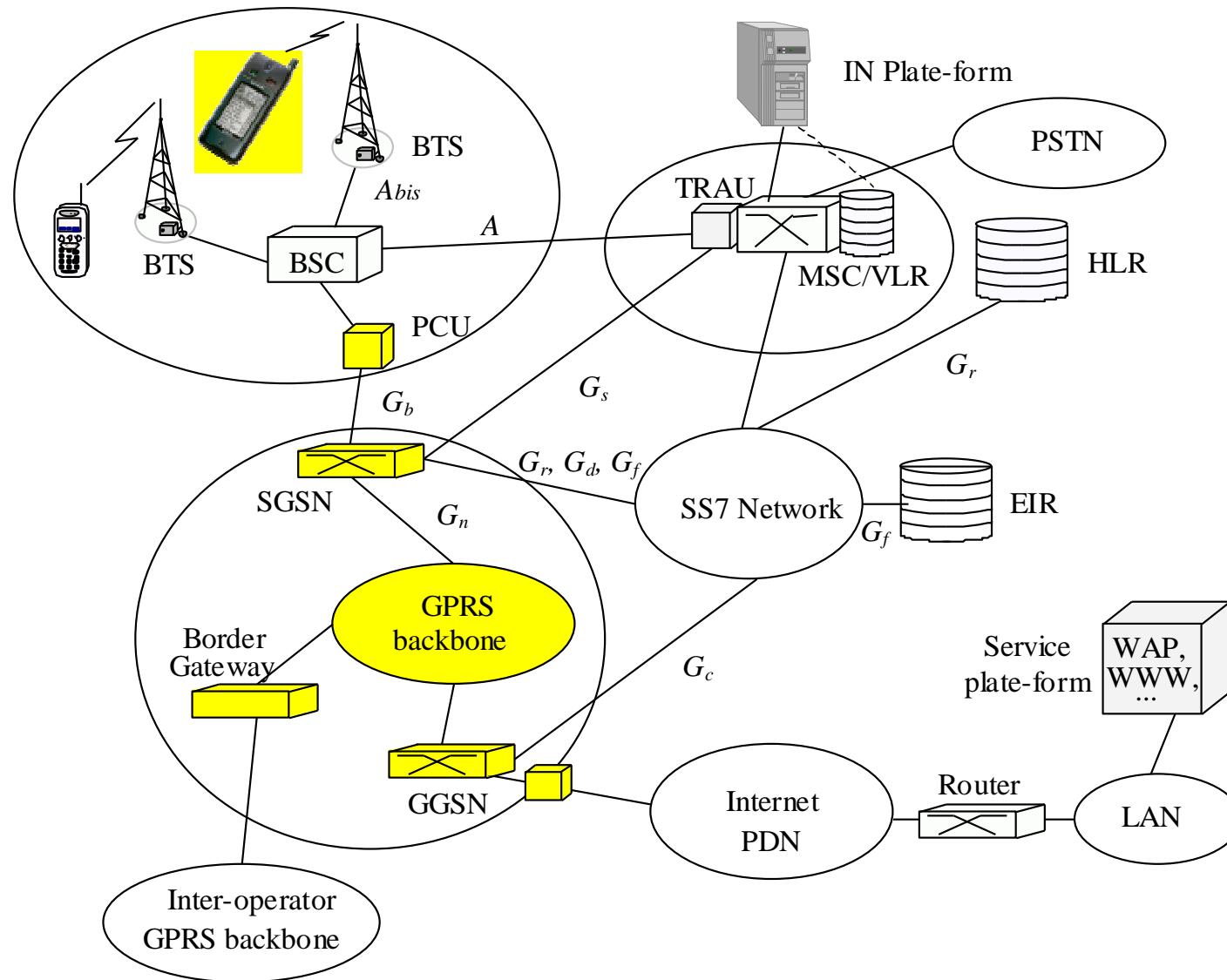
GPRS Architecture

- New entities are defined
 - SGSN – serving GPRS support node
 - GGSN – gateway GPRS support node
 - Interfaces between entities GPRS, GSM, core and PSTN
- Transmission plane
 - Data packets are transmitted by a tunnel mechanism
- Control plane
 - GTP: a protocol for tunnel management (create, remove, etc..)
- Radio interface
 - Changed the logical channels and how they are managed
 - Remains the concept of “master-slave”

GPRS Architecture



GPRS introduction in a GSM network



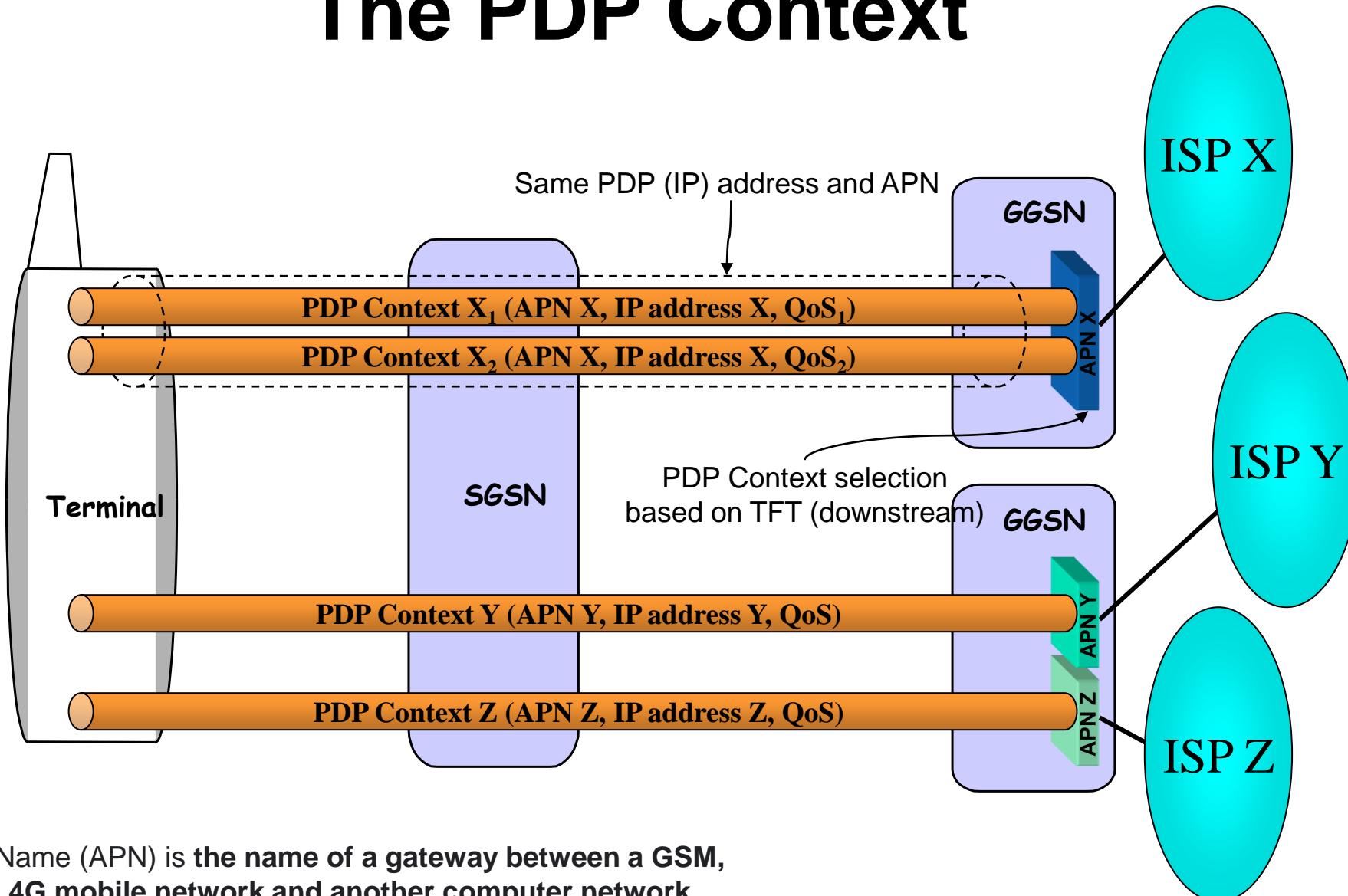
GGSN (*Gateway GPRS Support Node*) Functions

- **Gateway:**
 - Allows the connection to other IP or GPRS networks.
- **Routing:**
 - IP router which supports dynamic or static routing,
- **Mobility management:**
 - Use of *routing areas*.
 - Handover management between the BSCs and other SGSNs.
 - Allows the routing of the packets towards the users SGSNs, according to their mobility.
- **Sessions management:**
 - At each session, the SGSN activates a PDP (*Packet Data Protocol*) context, and allocates an IP address to the MT.

GGSN (*Gateway GPRS Support Node*) Functions

- **Security:**
 - Ciphers the communications towards or from the mobiles.
 - Includes firewalls for filtering the packets coming from external IP networks.
- **Authentication:**
 - At *Attach* and inter-SGSN RA updates.
- **Billing:**
 - Production of the CDRs according to the quantity of information and the session duration (attachment, duration of active PDP context).
- **SMS:**
 - Supports the Gd interface for the communications with the SMS-GMSC and the SMS-IWMSC.

The PDP Context



An Access Point Name (APN) is **the name of a gateway between a GSM, GPRS, 3G and 4G mobile network and another computer network, frequently the public Internet.**

Later called DNN in 5G

GTP and PDP Context

- GTP
 - GPRS Tunneling Protocol is a simple tunneling protocol based on UDP/IP - used both in GSM/GPRS and UMTS.
 - Identified by a Tunnel Endpoint Identifier (TEID)
 - For every MS:
 - one GTP-C tunnel is established for signalling
 - Multiple GTP-U tunnels, one per PDP context (i.e. session), are established for user traffic.
- PDP Context
 - When an MS attaches to the Network:
 - SGSN creates a Mobility Management context with information about mobility and security for the MS.
 - At PDP Context Activation (PDP - Packet Data Protocol), both SGSN and GGSN create a PDP context, with information about the session (e.g. IP address, QoS, routing information , etc.),

3G

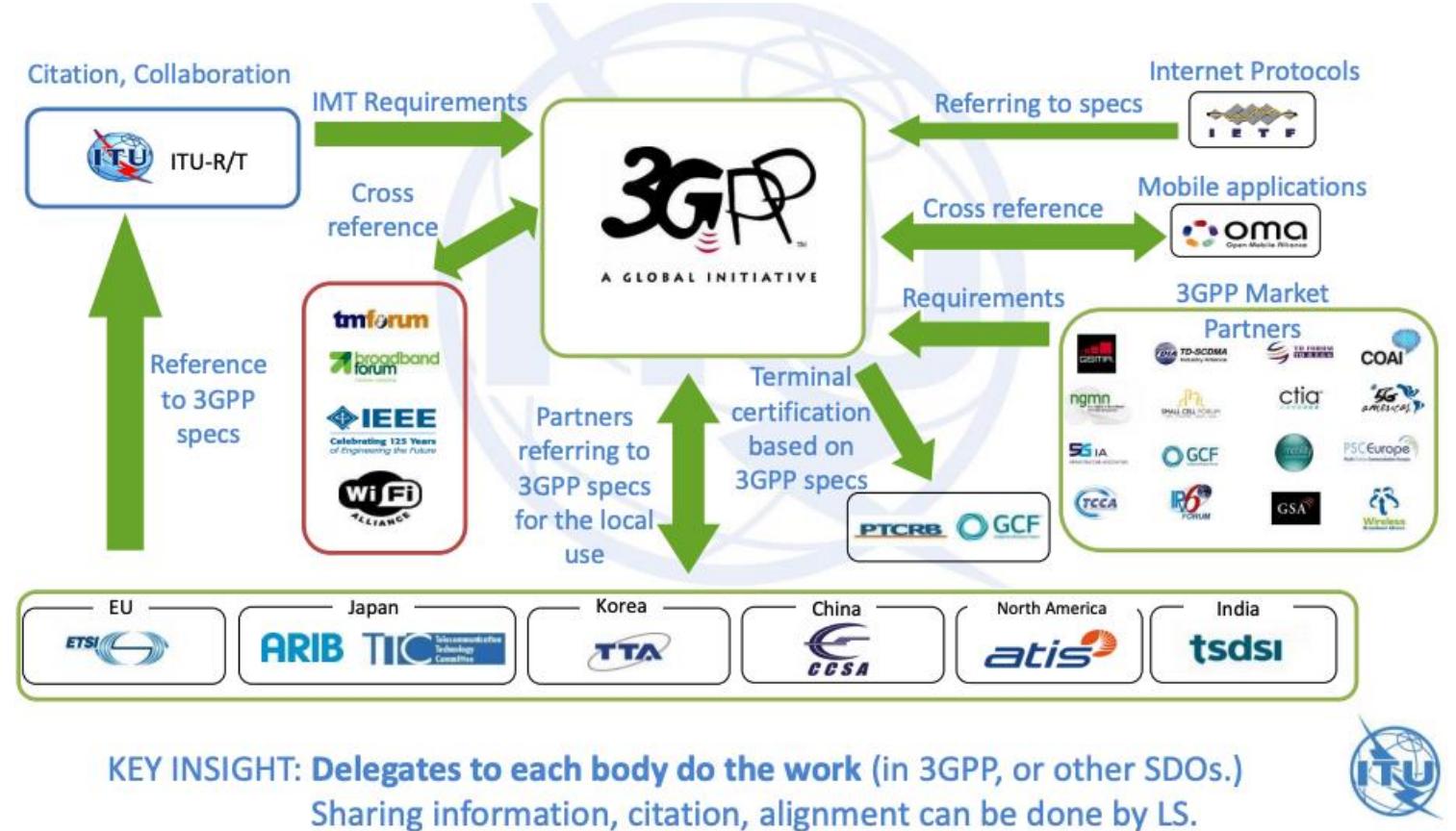
**Universal Mobile Telecommunication
System**

What is 3GPP?

3rd Generation Partnership Project - partnership of regional SDOs

"The original scope of 3GPP (1998) was to **produce Technical Specifications and Technical Reports for a 3G Mobile System** based on evolved GSM core networks and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both Frequency Division Duplex (FDD) and Time Division Duplex (TDD) modes).

The scope was subsequently amended to include the maintenance and development of the Technical Specifications and Technical Reports for evolved 3GPP technologies, **beyond 3G.**"

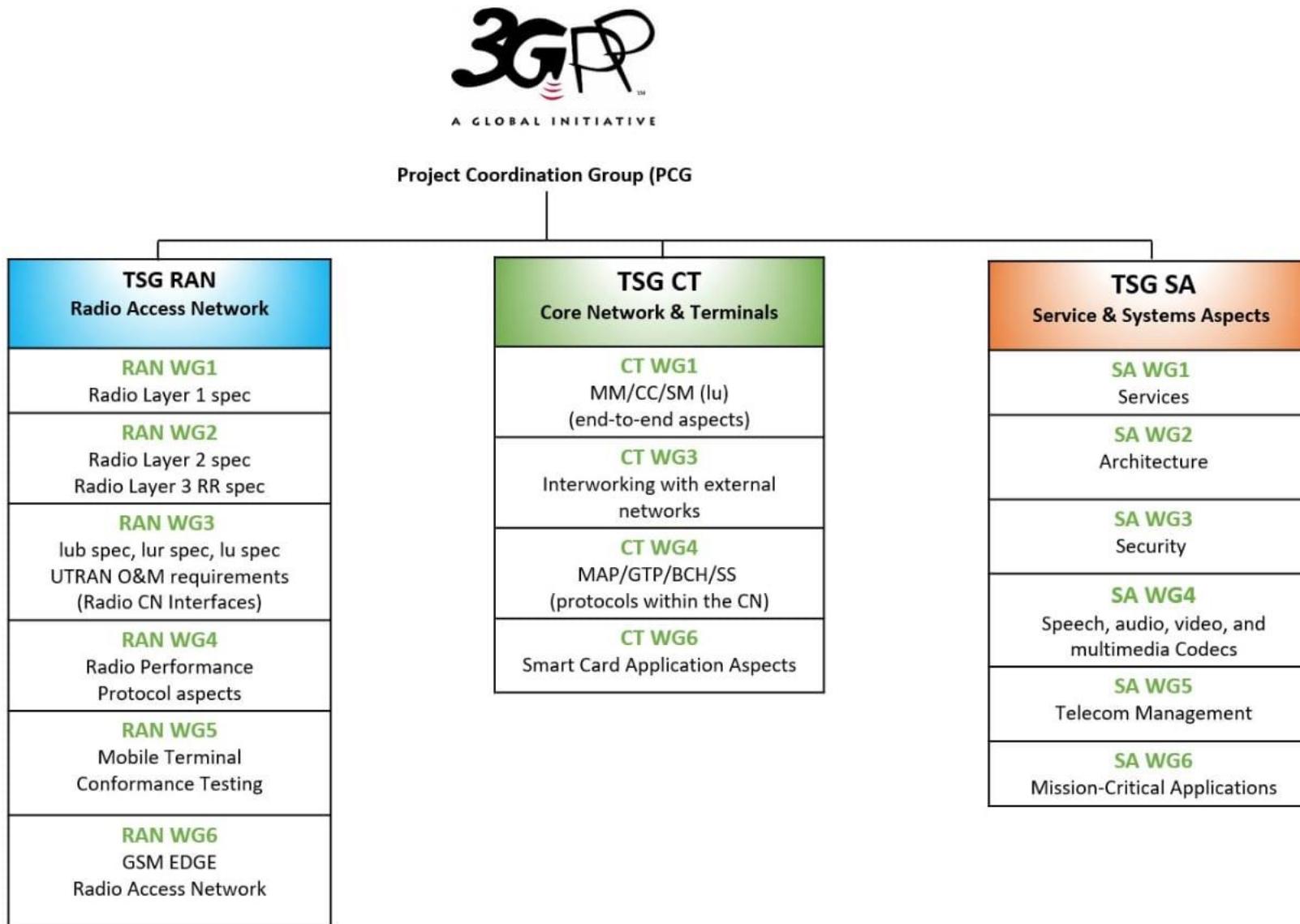


SDOs take 3GPP specifications and transpose them to regional standards. Addresses:

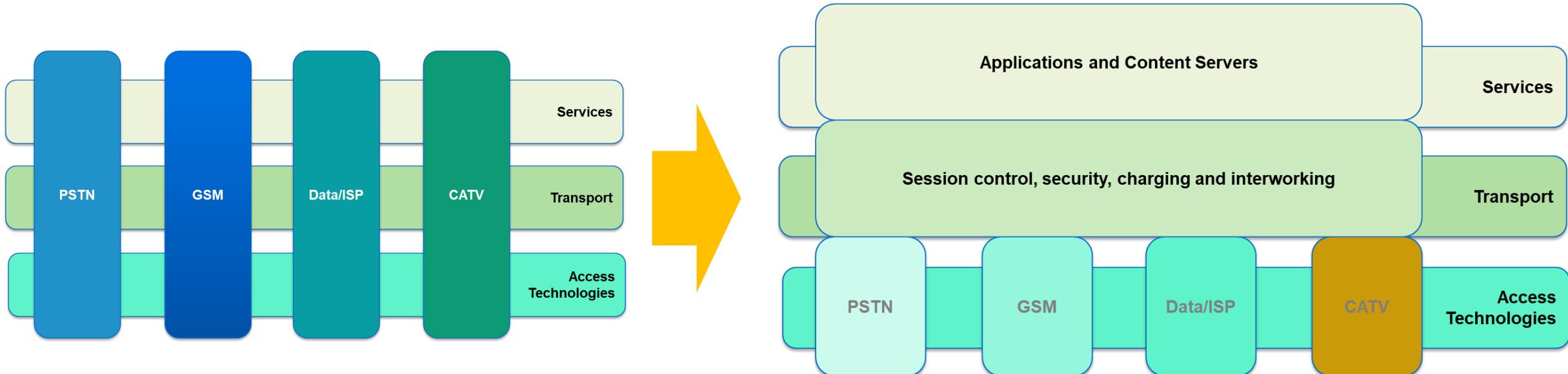
3G (IMT-2000) systems based on the evolved GSM core network and the Universal Terrestrial Radio Access (UTRA), in FDD and TDD modes; GSM, including GSM evolved radio access technologies (GPRS/EDGE/GERAN)

SDO: Standards Development Organization

Actual 3GPP structure



3GPP/TISPAN Telecom Model



Telecoms & Internet converged Services & Protocols for Advanced Networks
is a standardization body of ETSI, specializing in fixed networks and Internet convergence

UMTS

- Universal Mobile Telecommunication System – 3G system
- Oriented towards generalized service diffusion, and future user trends: combines “cellular”, “wireless”, “internet”, etc...
- “multimedia everywhere”
- Developed in order to have an evolutionary path from 2.5G systems; progressive evolution (GPRS-EDGE-UMTS)

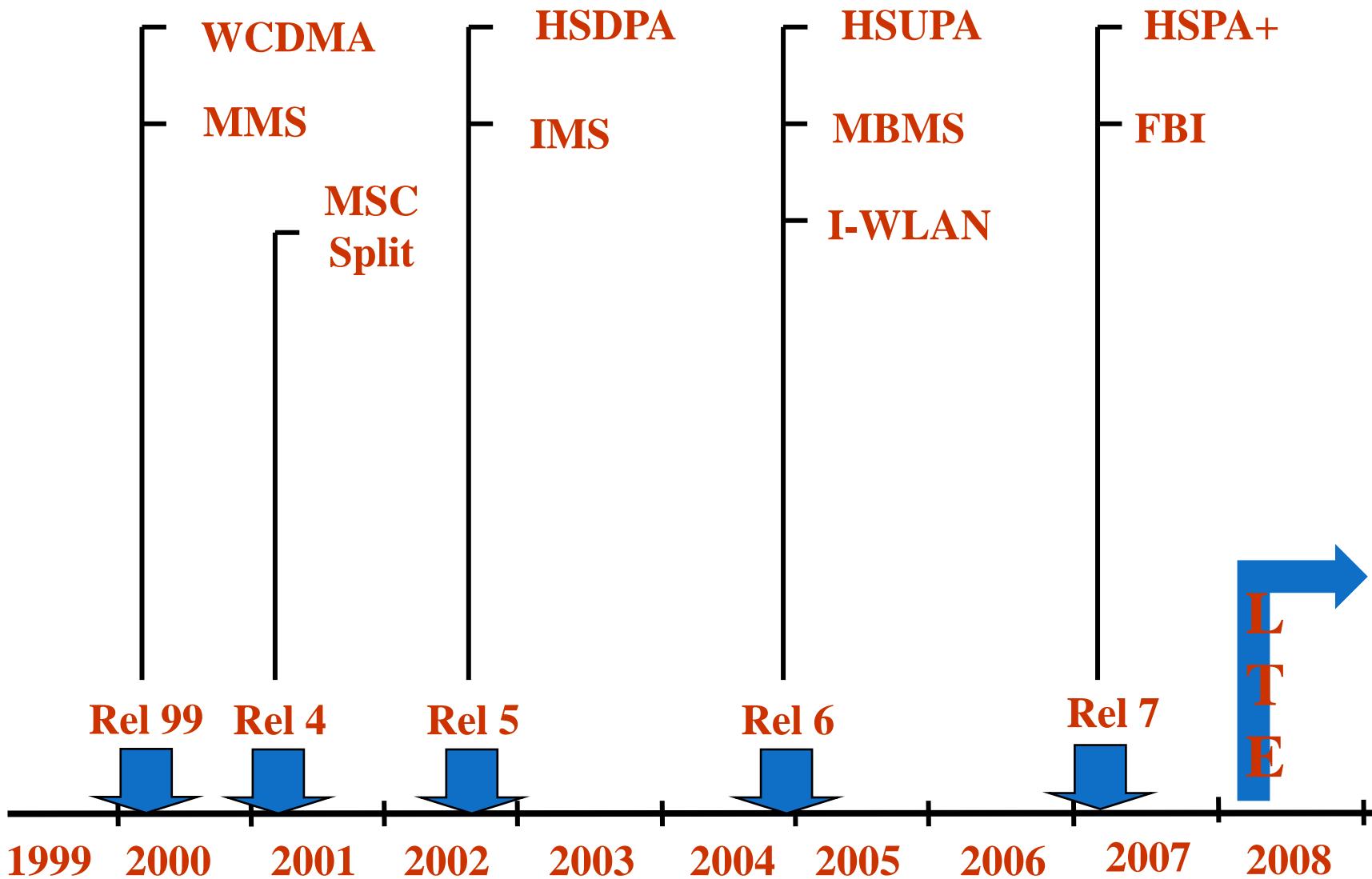
Any Device
Any Access Technology
Any Where
ALWAYS BEST CONNECTED

Specification

- Flexible
 - Handles multiple multimedia flows in a single connection.
 - Support to packet transport
 - Flexible coding mechanisms (FDD/TDD WCDMA)
 - Variable transmission rates
 - Max. 384 Kbps for global coverage (initially)
 - Max. 2Mbps for local coverage (initially)

One Network, multiple access technologies
Common Session Control
Generic Application Servers
Single set of services that apply network wide
Consistent user experience
Operational efficiency
New services/applications

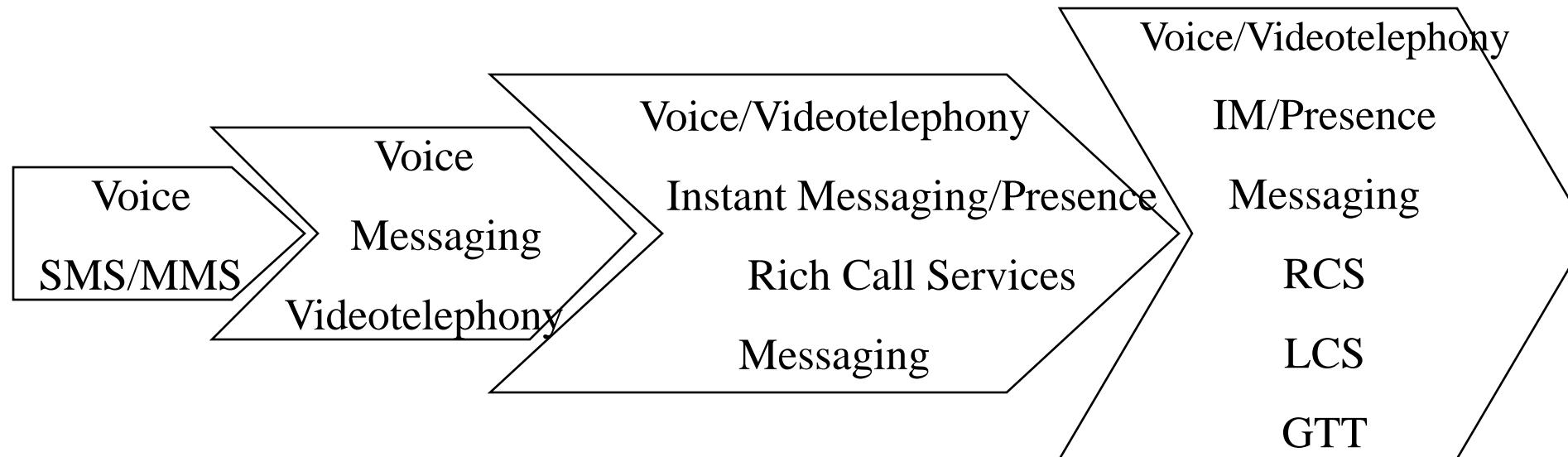
UMTS evolution (3GPP Releases)



Services evolution in UMTS R99/R4/R5/R6 networks

Release	Services
R99	MMS, streaming, LCS (cell), MExE, SAT, VHE,
R4	TrFO, VHE, OSA, LCS in PS and CS,
R5	VoD, IMS, HSDPA, Wideband AMR, GTT
R6	MBMS, IMS phase 2

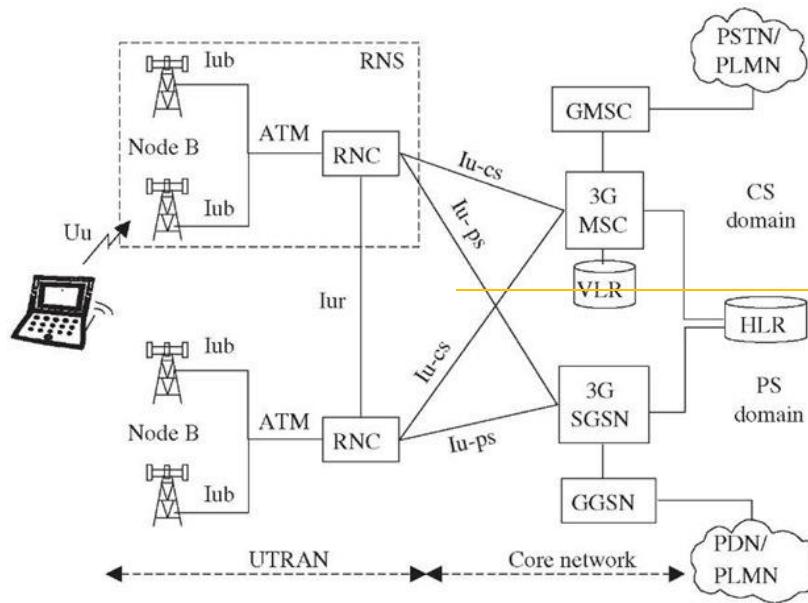
Evolution of the services (voice and interpersonal services)



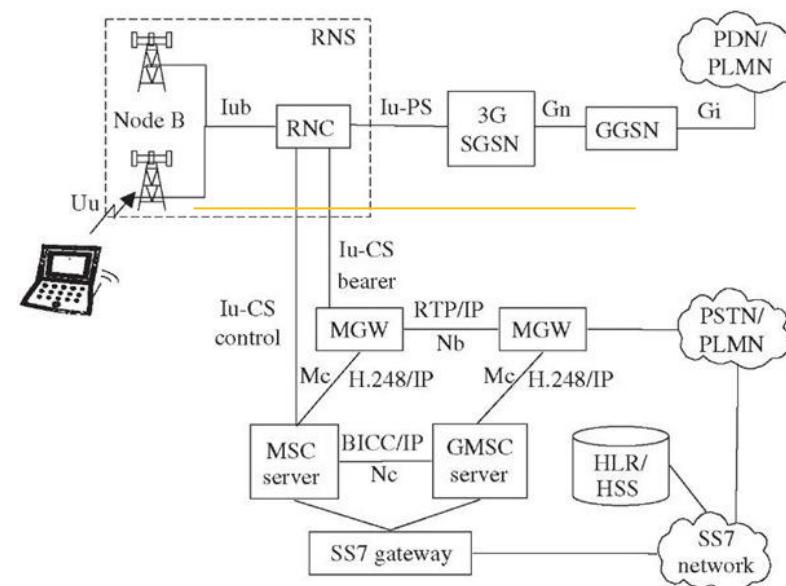
3G Releases

<http://what-when-how.com/roaming-in-wireless-networks/umts-network-architecture-third-generation-networks/>

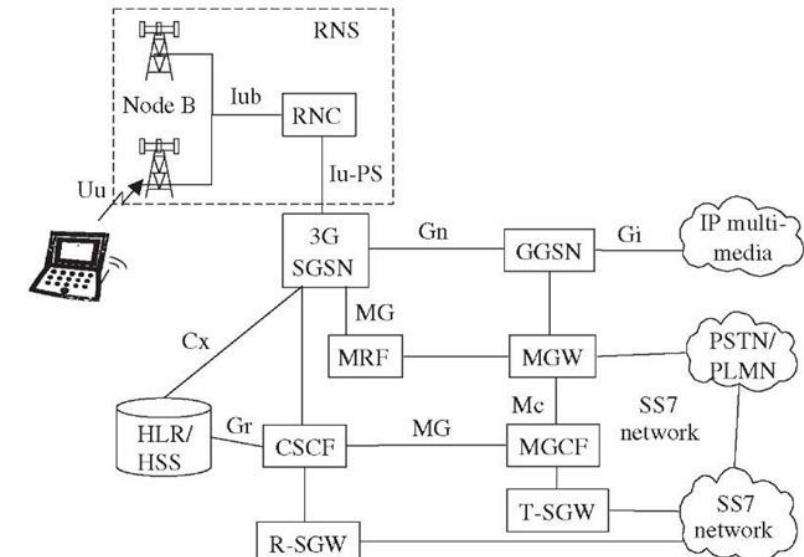
3GPP Release 99



Release 4



Release 5

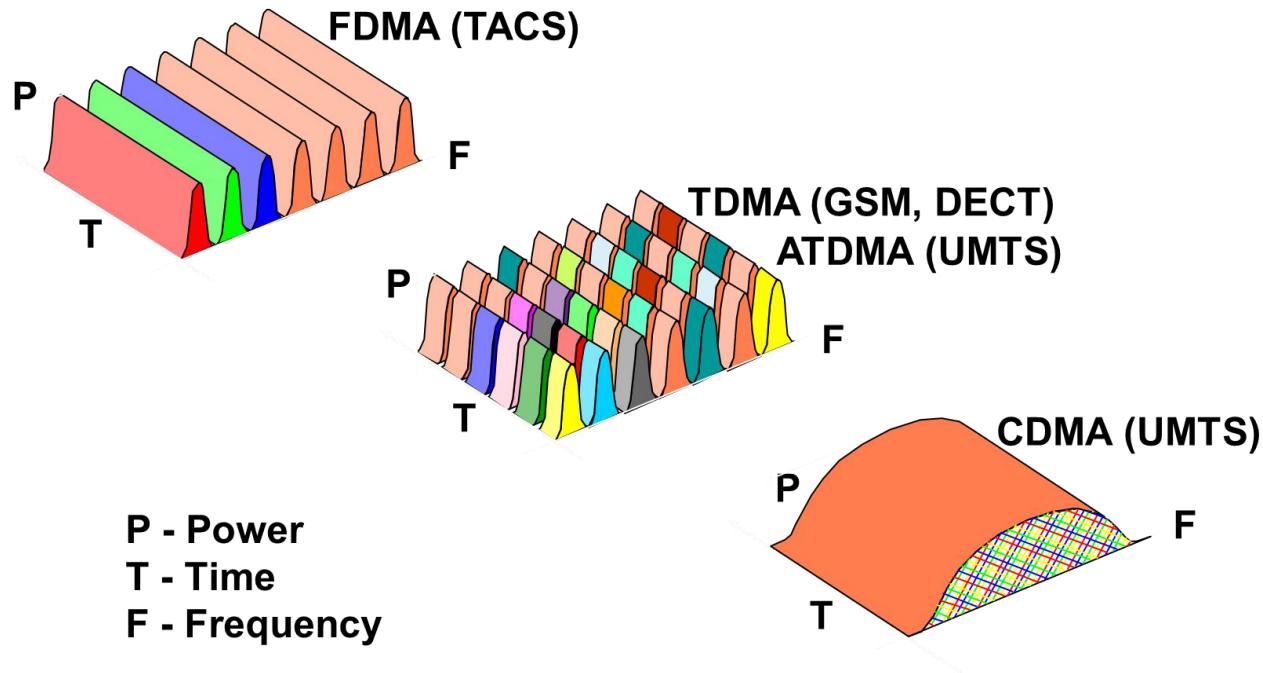


Release 6 – Integrated operation with Wireless LAN networks and added HSUPA (enables broadband uploads and services), MBMS, and enhancements to IMS such as Push-to-Talk over Cellular (PoC), video conferencing, messaging, etc.

UMTS – air interface

- UTRA-FDD:
 - *uplink*: 1920 – 1980 MHz (60 MHz)
 - *downlink*: 2110 – 2170 MHz (60 MHz)
- UTRA-TDD:
 - 1900 – 1920 MHz (20 MHz)
 - 2010 – 2025 MHz (15 MHz)
- In Portugal:
 - 2x15 MHz for UTRA-FDD
 - 1x5 MHz for UTRA-TDD

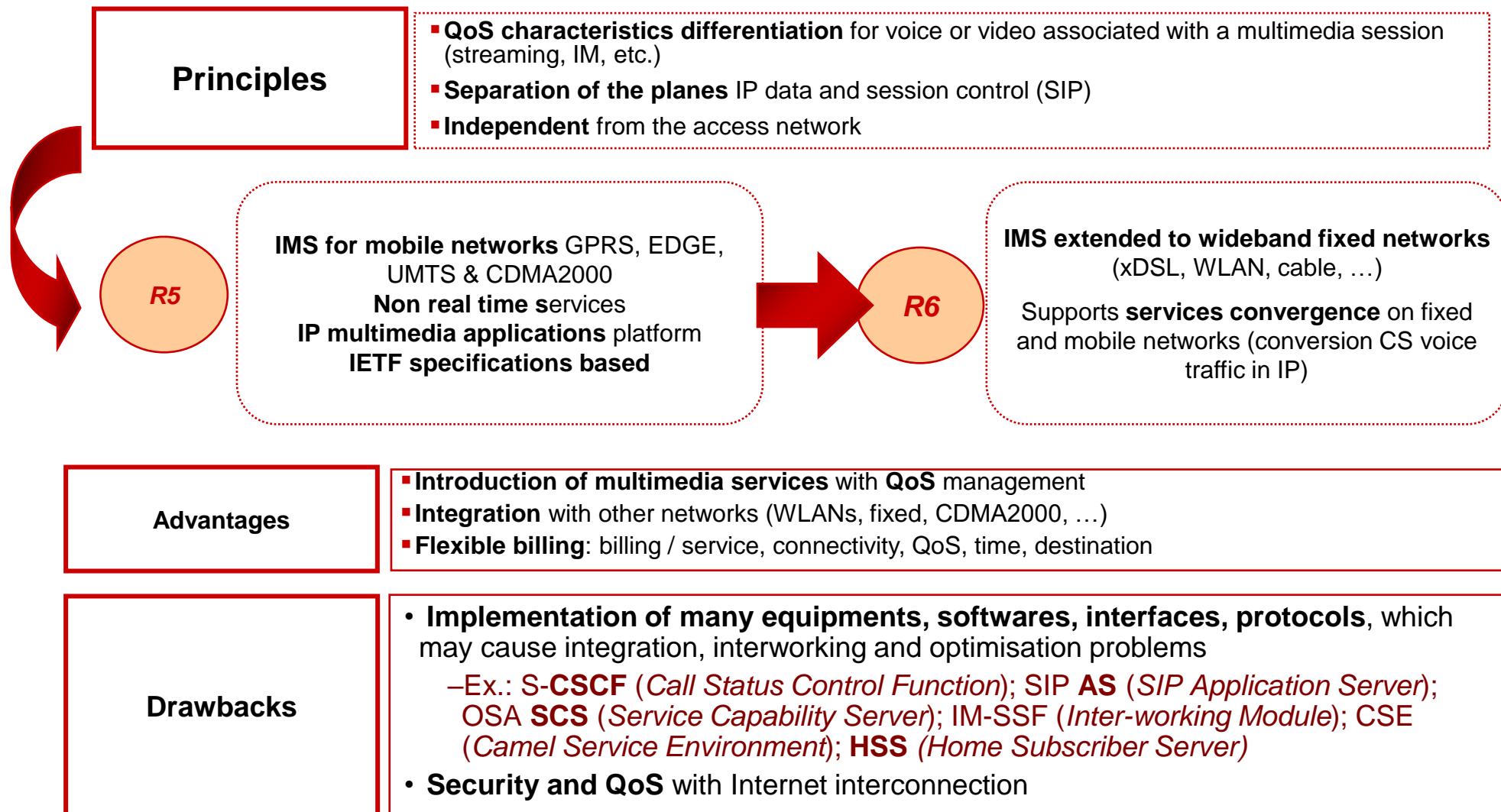
Multiplexing mechanisms



CDMA is a form of direct-sequence spread-spectrum technology that allows many users to occupy the same time and frequency allocations in a given band/space. CDMA assigns each user a unique spreading code to spread the baseband data before transmission, in order to help differentiate signals from various users in the same spectrum.

- Larger capacity and coverage, keeping compatibility with 2G
- Supports the flexibility required, with multiple parallel connections
- Efficient packet access

IMS - IP Multimedia Subsystem



IMS – Key Architectural Principles

- **Border Functions**
 - Access and Network Border Security
 - QoS and Admission Control
 - Media and Signaling Adaptation
- **Core Functions**
 - Subscriber Management – Registration
 - Session Switching – Set-up and tear-down of session legs, Session state maintenance, Application Server invocation
 - Session Routing – Breakout to external networks
 - Centralized Provisioning – Subscriber and Routing data
- **Application Functions**
 - Access to legacy applications
 - Native SIP Applications
 - Service Brokering

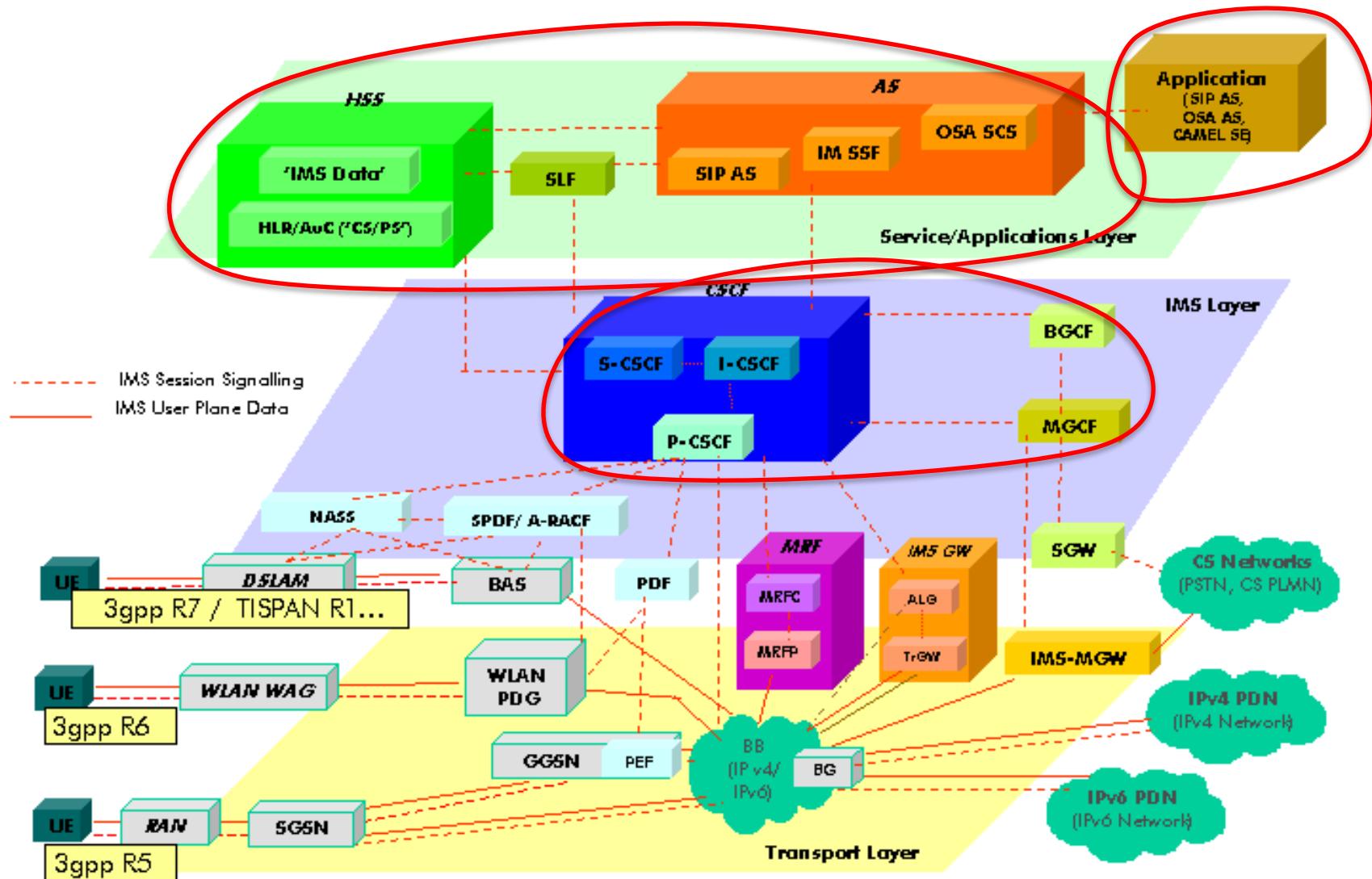
SIP Protocol

- Defined in IETF RFC 3261
 - “... an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include Internet telephone calls, multimedia distribution, and multimedia conferences.”
- SIP is to the Internet what SS#7 is to telephony
- In IMS, SIP is extended to include extra functionality
 - E.g. 3GPP TS 23.228
- At the core of IMS there are several SIP proxies:
 - I-CSCF, S-CSCF, P-CSCF
 - The Call Session Control function (CSCF) is the heart of the IMS architecture
 - The main functions of the CSCF:
 - provide session control for terminals and applications using the IMS network
 - secure routing of the SIP messages,
 - subsequent monitoring of the SIP sessions and communicating with the policy architecture to support media authorization.
 - responsibility for interacting with the HSS.
- Serving - CSCF
 - Controls the user's SIP Session
 - very few per domain
 - Located in the home domain
 - Is a SIP registrar (and proxy)
- Proxy – CSCF
 - IMS contact point for the user's SIP signaling
 - Several in a domain
 - Located in the visited domain
 - Terminals must know this proxy (e.g. DHCP used)
 - Compresses and decompresses SIP messages
 - Secures SIP messages
 - Assures correctness of SIP messages
- Interrogating – CSCF
 - domain's contact point for inter-domain SIP signaling
 - one or more per domain
 - In case there are more than one S-CSCFs in the domain, locates which S-CSCF is serving a user

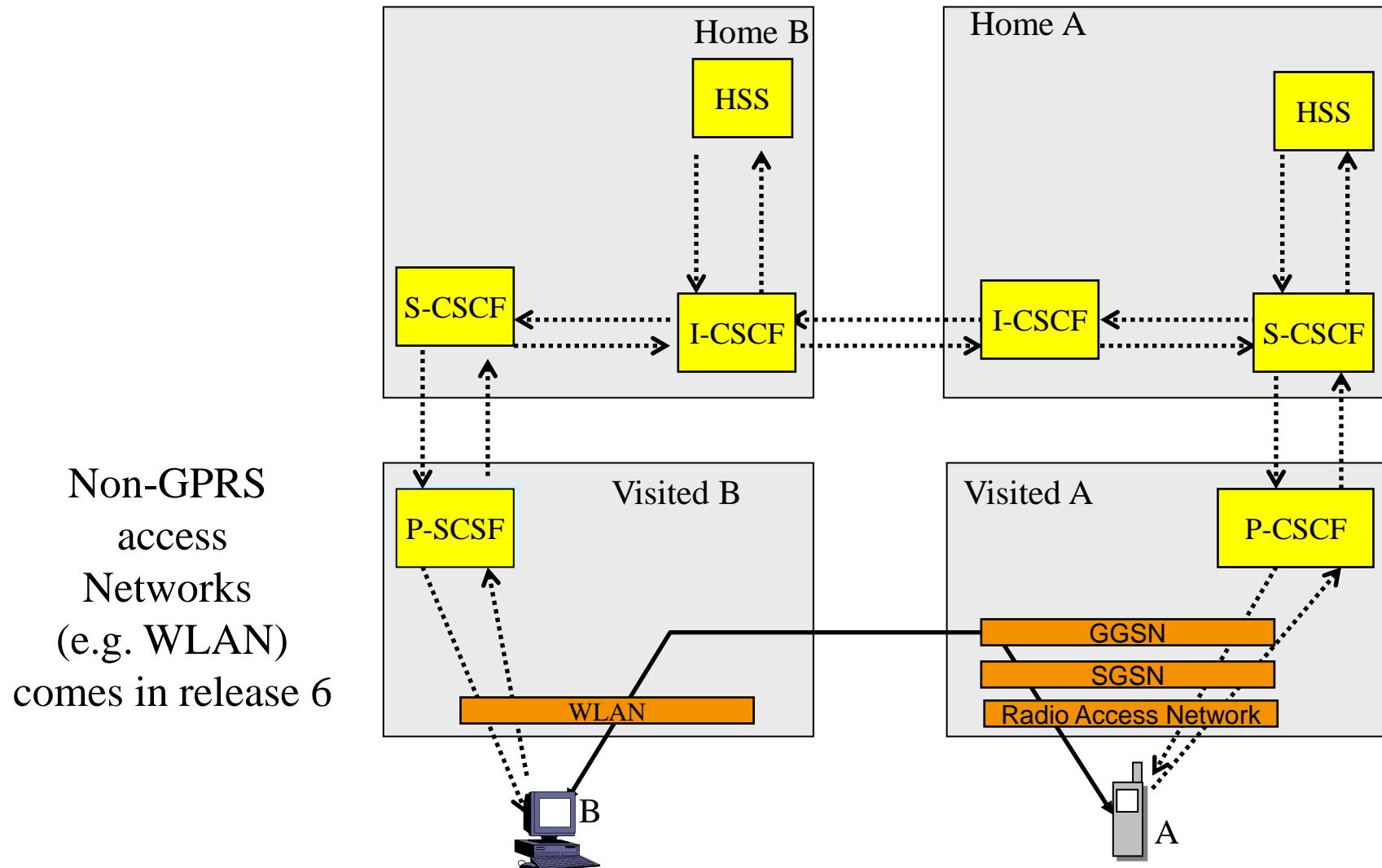
Services in IMS

- **IMS is an advanced infrastructure enabling services. But the services are in the end points or peers (calls, etc.), not in the IMS**
- **Application Servers (AS) are the key part to endow IMS with services**
- **AS offered services enjoy all IMS advantages**
- **AS interact – using SIP - with the S-CSCF (which controls user's SIP session)**
- **AS can behave as another SIP proxy or as a SIP UA (terminal)**

Where is IMS ?



UMTS IMS: basic call flow

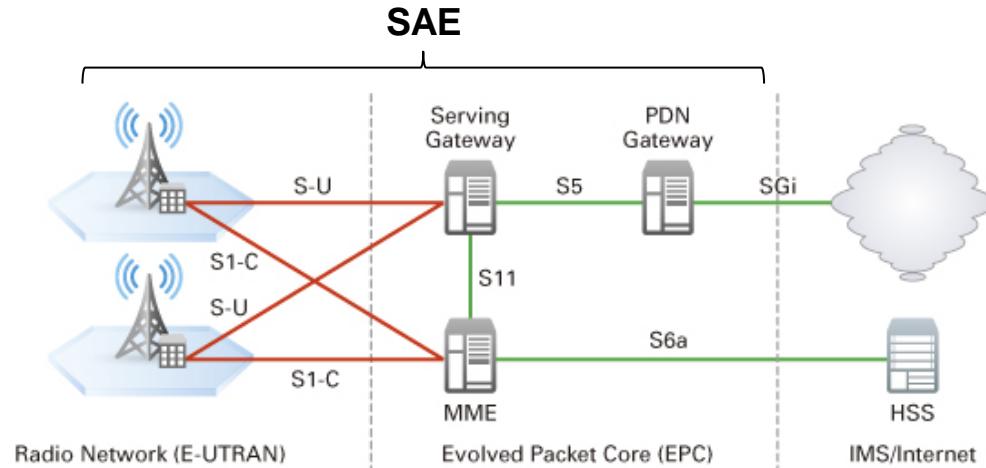


4G

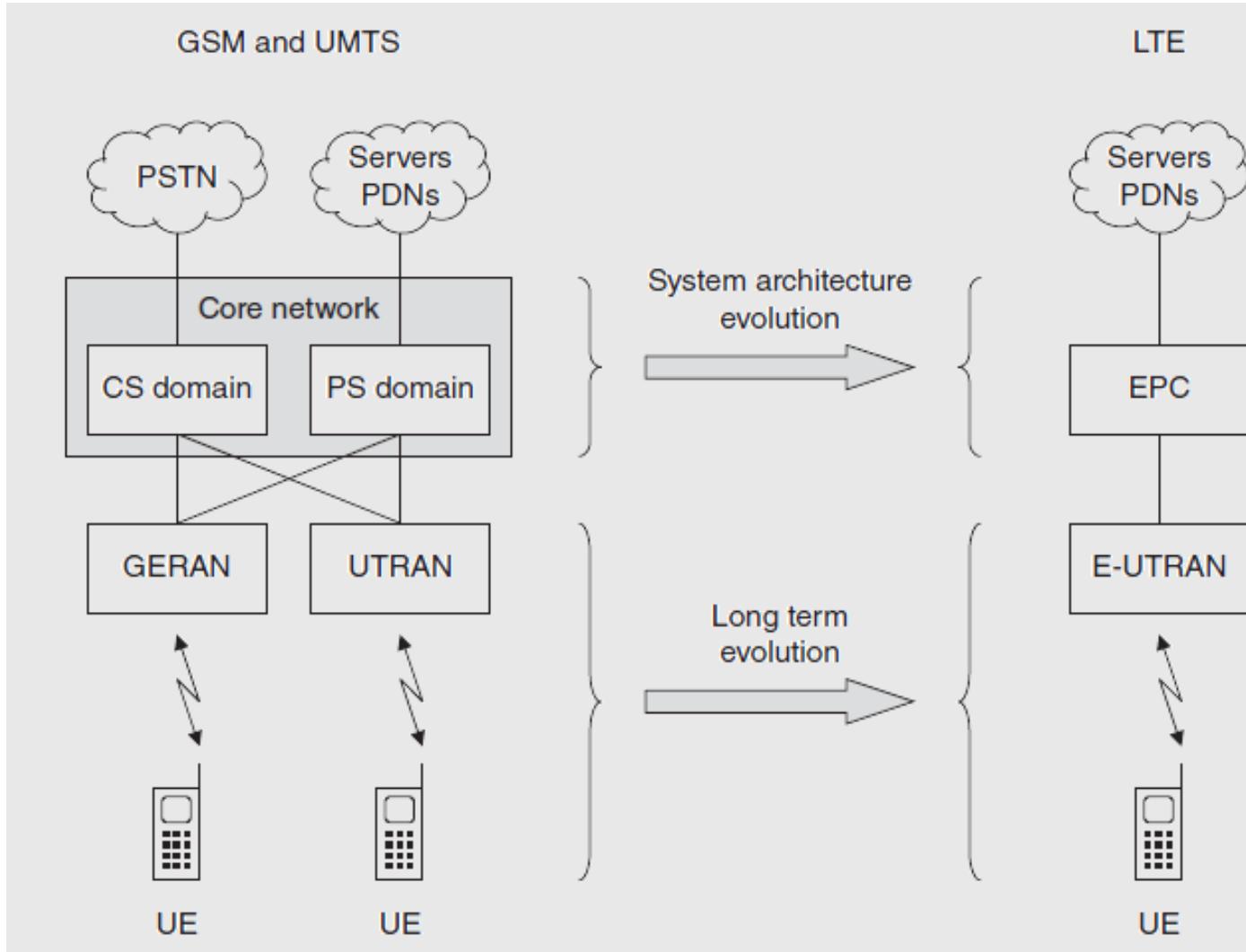
**Long Term Evolution/Evolved Packet Core
(LTE/EPC)**

3GPP System Architecture Evolution (SAE) philosophy

- SAE focus is on:
 - enhancement of Packet Switched technology to cope with rapid growth in IP traffic
 - higher data rates
 - lower latency
 - packet optimised system
 - through
 - fully IP network
 - In addition to IMS services available in the current system, equivalent CS Services may be provided by IMS core since CS domain is not supported in LTE
 - simplified network architecture
 - Reduced number of nodes in the evolved packet core may be achieved compared to current architecture to provide connectivity to IMS
 - distributed control
 - Flexible accommodation and deployment of existing and new access technologies with mobility by a common IP-based network



Network simplification



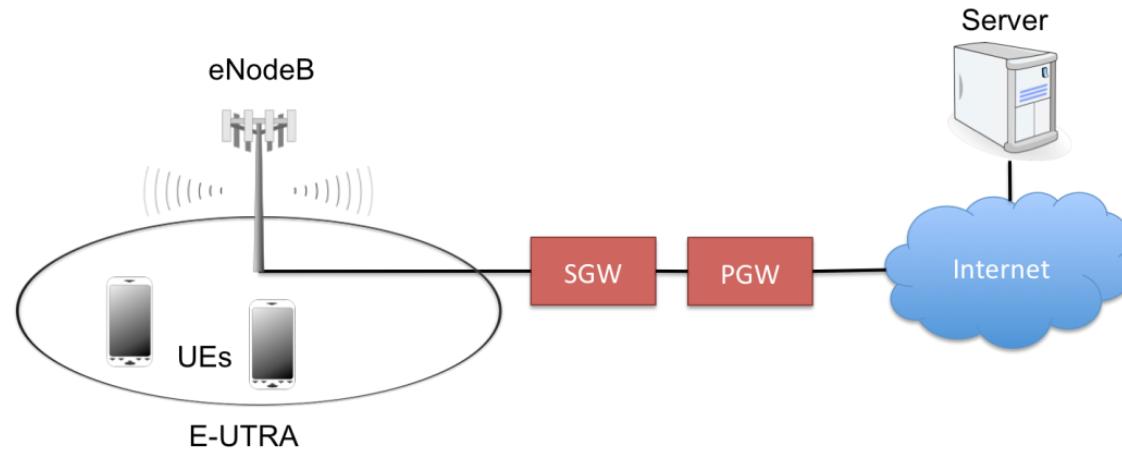
Feature	UMTS	LTE
IP version support	IPv4 and IPv6	IPv4 and IPv6
USIM version support	Release 99 USIM onwards	Release 99 USIM onwards
Transport mechanisms	Circuit & packet switching	Packet switching
CS domain components	MSC server, MGW	n/a
PS domain components	SGSN, GGSN	MME, S-GW, P-GW
IP connectivity	After registration	During registration
Voice and SMS applications	Included	External

Long Term Evolution (LTE)

- Long Term Evolution (LTE) – Standard created by the 3rd Generation Partnership Project
 - Deployed globally
 - All packet switched network
 - High throughput and QoS considerations
 - Provides wireless retransmissions of lost data

Technology	3G	4G
Data Transfer Rate	3.1MB /sec	100MB/sec
Internet services	Broadband	Ultra Broadband
Mobile -TV Resolution	Low	High
Bandwidth	5 - 20 MHz	100 +MHz
Frequency	1.6- 2 GHZ	2 – 8 GHz
Network Architecture	Wide Area Network	Hybrid Network

LTE Network



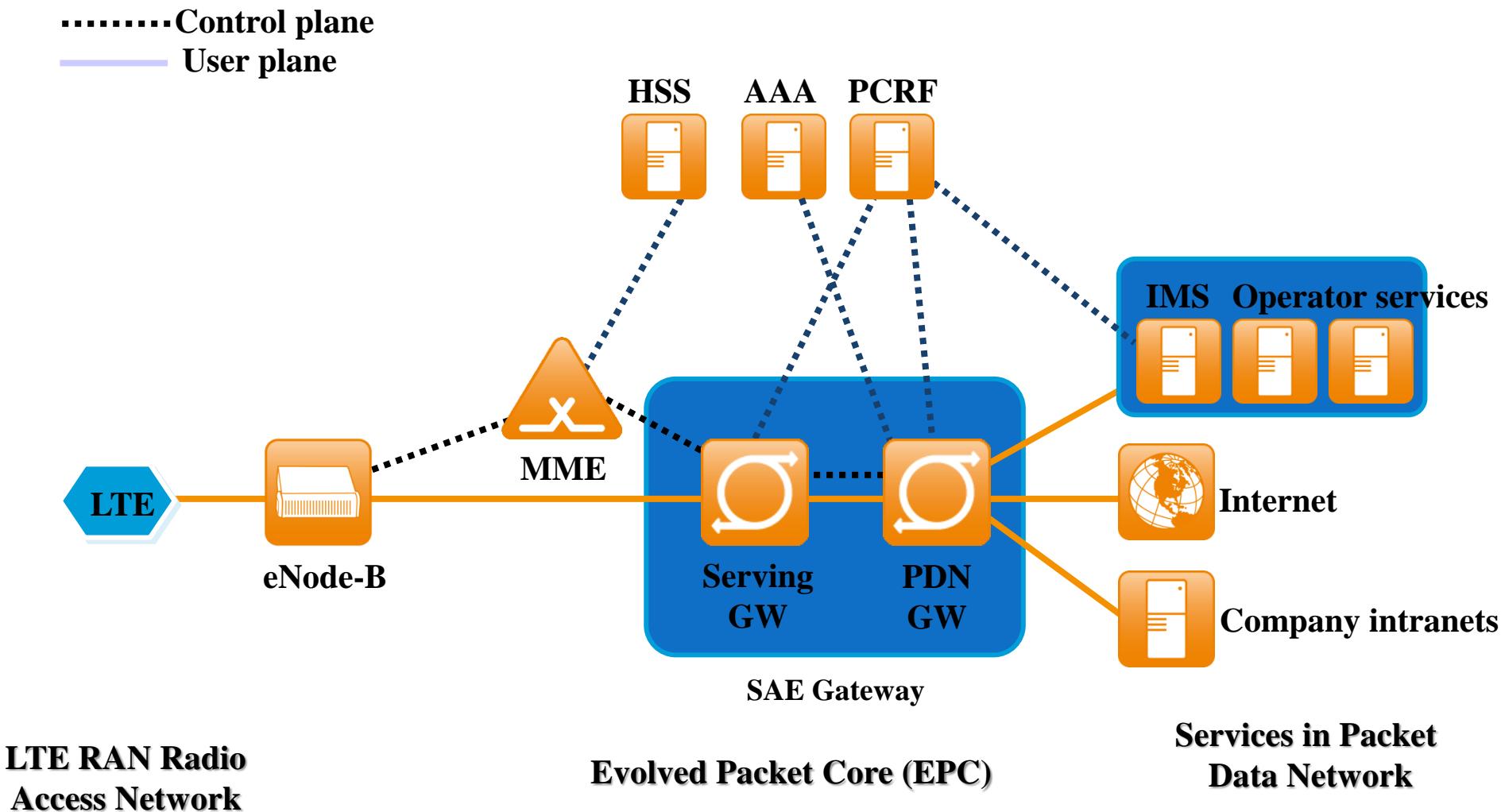
- **Packet Delivery Network Gateway (PGW)**
 - Connects LTE network to IP networks
- **Serving Gateway (SGW)**
 - Route packets to and from wireless access points
- **Enhanced Node B (eNodeB)**
 - Wireless access point
- **User Equipment (UE)**
 - End user devices

Radio evolution

More flexible and resilient radio technology

Feature	WCDMA	LTE
Multiple access scheme	WCDMA	OFDMA and SC-FDMA
Frequency re-use	100%	Flexible
Use of MIMO antennas	From Release 7	Yes
Bandwidth	5 MHz	1.4, 3, 5, 10, 15 or 20 MHz
Frame duration	10 ms	10 ms
Transmission time interval	2 or 10 ms	1 ms
Modes of operation	FDD and TDD	FDD and TDD
Uplink timing advance	Not required	Required
Transport channels	Dedicated and shared	Shared
Uplink power control	Fast	Slow
Radio access network components	Node B, RNC	eNB
RRC protocol states	CELL_DCH, CELL_FACH, CELL_PCH, URA_PCH, RRC_IDLE	RRC_CONNECTED, RRC_IDLE
Handovers	Soft and hard	Hard
Neighbour lists	Always required	Not required

EPC architecture



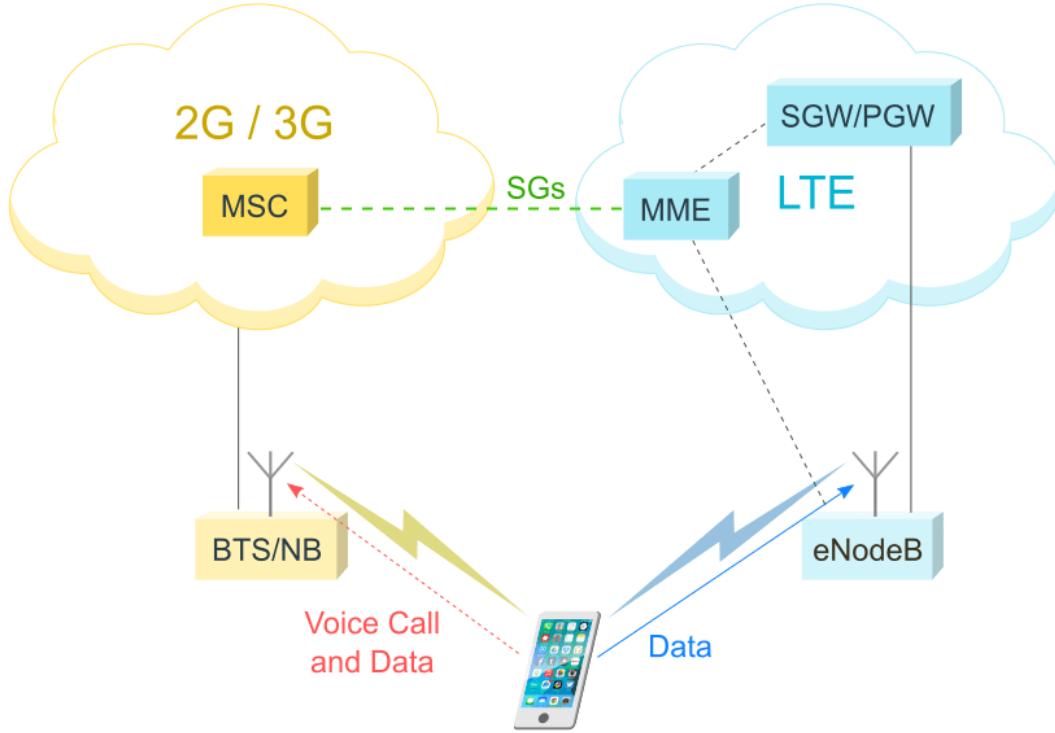
LTE RAN Radio Access Network

Evolved Packet Core (EPC)

Services in Packet Data Network

Voice: CSFB or VoLTE

https://yatebts.com/solutions_and_technology/csfb-to-volte-evolution/



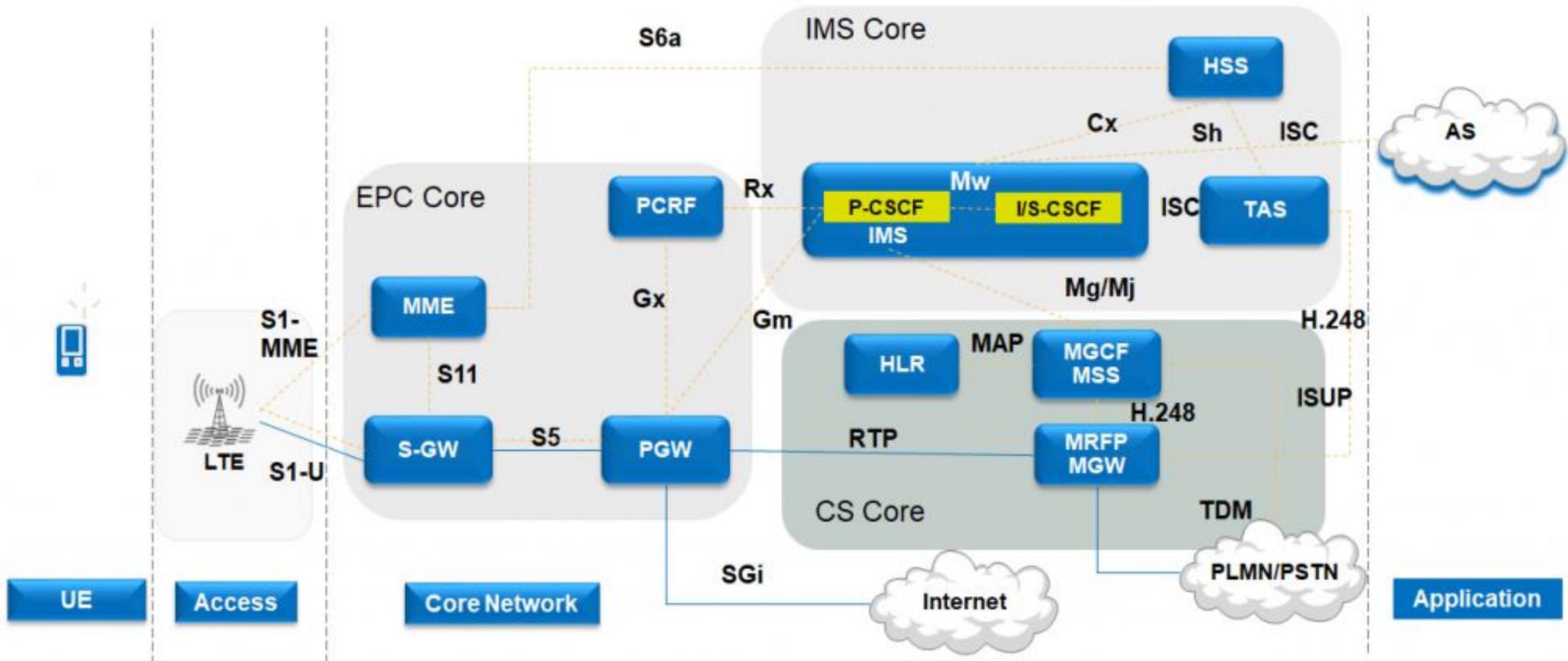
<https://www.mpirical.com/blog/delivering-5g-voice-services>

Feature	CSFB	VoLTE
Easy of Deployment	Challenging, but not as difficult as VoLTE	Numerous major challenges to overcome
Economic Considerations	Minor	Major
LTE Coverage Requirements	Low	High
Call Setup Time	Approx. 3-7 secs	Approx. 2-4 secs
Voice Quality	Acceptable	HD Voice
Lifespan	2G and 3G limited life	IMS forms basis for 5G voice and beyond

CSFB (Circuit Switch Fallback) is a technology that supports voice and SMS services in 4G networks using the 2G/3G systems.

VoLTE (Voice over LTE), on the other hand, means that a call is made through a 4G network (Making calls over IP).

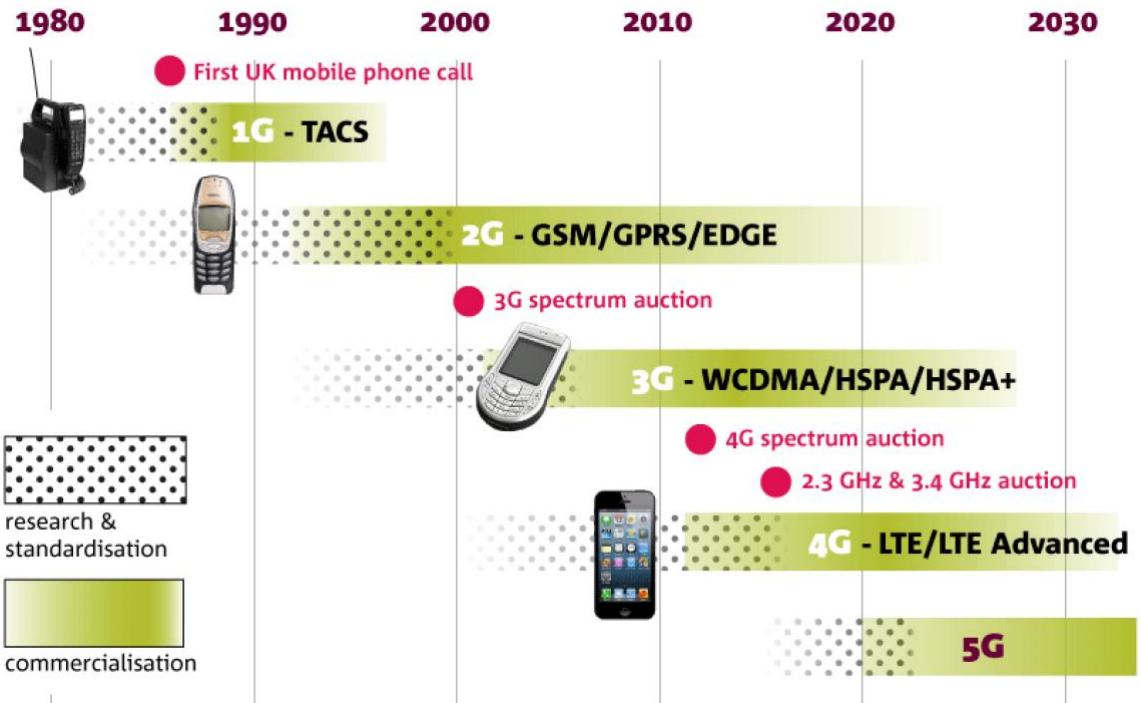
VoLTE Network Architecture



<https://cafetele.com/volte-architecture/>

Summary

1G to 4G summary



https://its-wiki.no/images/c/c8/From_1G_to_5G_Simon.pdf

		Real World (avg)		Theoretical (max)		Availability
		Download	Upload	Download	Upload	
2.5G	GPRS	32-48Kbps	15Kbps	114Kbps	20Kbps	Today
2.75G	EDGE	175Kbps	30Kbps	384Kbps	60Kbps	Today
	UMTS	226Kbps	30Kbps	384Kbps	64Kbps	Today
	W-CDMA	800Kbps	60Kbps	2Mbps	153Kbps	Today
3G	EV-DO Rev. A	1Mbps	500Kbps	3.1Mbps	1.8Mbps	Today
	HSPA 3.6	650Kbps	260Kbps	3.6Mbps	348Kbps	Today
	HSPA 7.2	1.4Mbps	700Kbps	7.2Mbps	2Mbps	Today
Pre-4G	WiMAX	3-6Mbps	1Mbps	100Mbps+	56Mbps	Today
	LTE	5-12Mbps	2-5Mbps	100Mbps+	50Mbps	End 2010
	HSPA+	-	-	56Mbps	22Mbps	2011
	HSPA 14	2Mbps	700Kbps	14Mbps	5.7Mbps	Today*
4G	WiMAX 2 (802.16m)	-	-	100Mbps mobile / 1Gbps fixed	60Mbps	2012
	LTE Advanced	-	-	100Mbps mobile / 1Gbps fixed	-	2012+

Features	1G	2G	3G	4G	5G
Start/Development	1970/1984	1980/1999	1990/2002	2000/2010	2010/2015
Technology	AMPS, NMT, TACS	GSM	WCDMA	LTE, WiMax	MIMO, mm Waves
Frequency	30 KHz	1.8 Ghz	1.6 - 2 GHz	2 - 8 GHz	3 - 30 Ghz
Bandwidth	2 kbps	14.4 - 64 kbps	2 Mbps	2000 Mbps to 1 Gbps	1 Gbps and higher
Access System	FDMA	TDMA/CDMA	CDMA	CDMA	OFDM/BDMA
Core Network	PSTN	PSTN	Packet Network	Internet	Internet

<http://net-informations.com/q/diff/generations.html>

5G

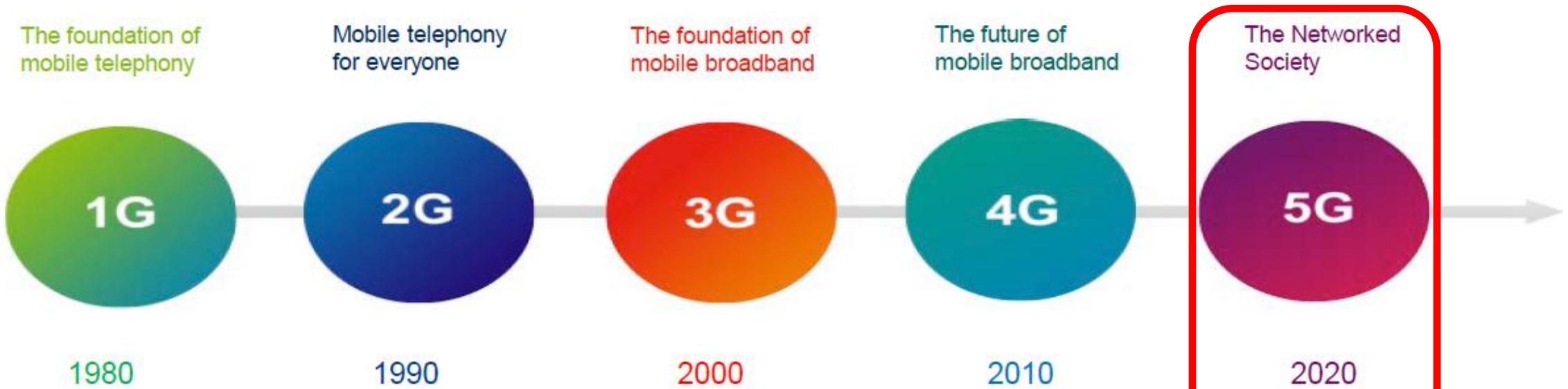
"Enabling a seamlessly connected society in the 2020 timeframe and beyond that brings together people along with things, data, applications, transport systems and cities in a smart networked communications environment"

ITU-R (*International Telecommunication Union*)

w i r e l e s s a c c e s s g e n e r a t i o n s



Non-limiting access to information and sharing of data anywhere and anytime for anyone and anything



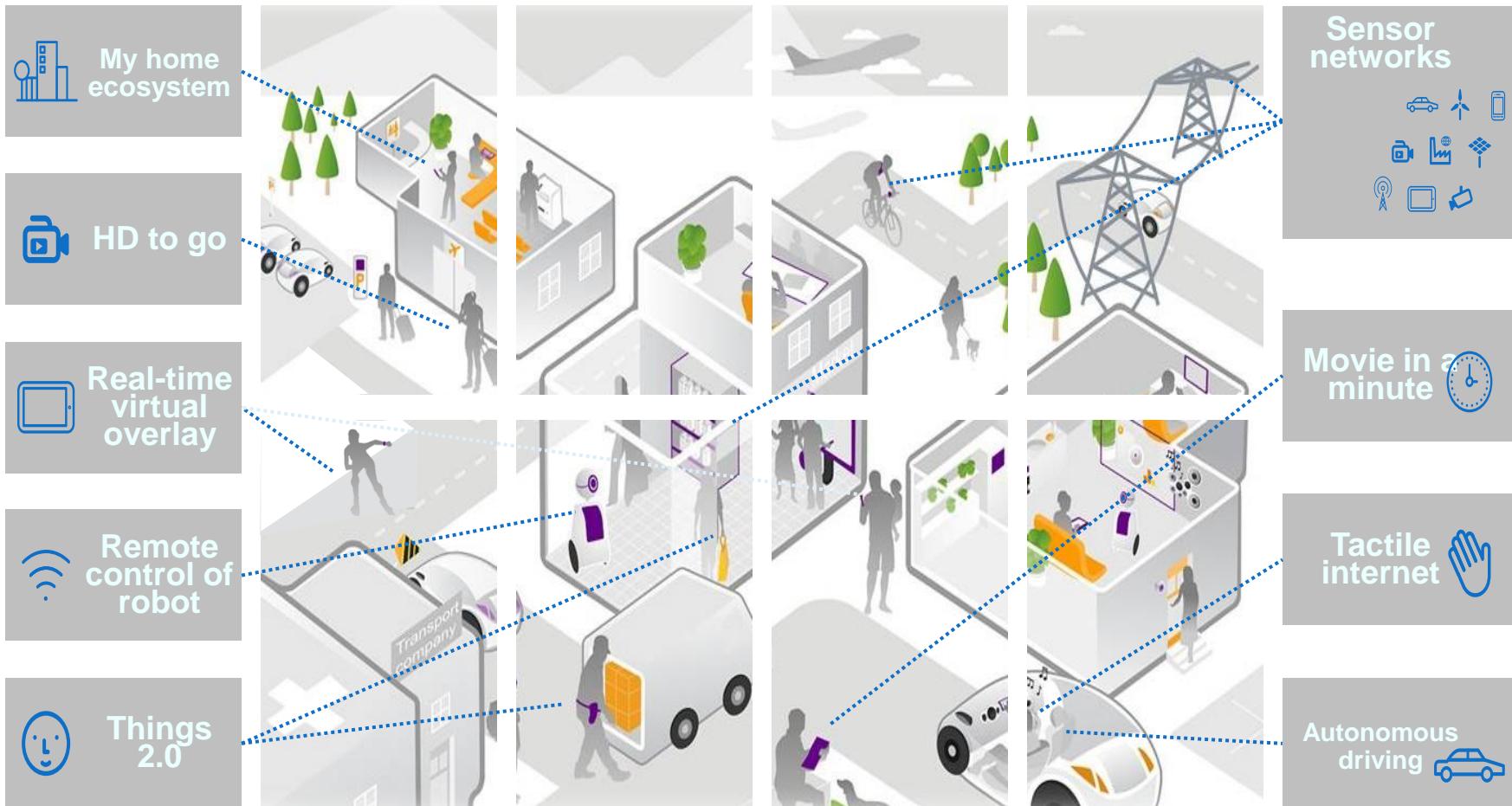
IMT-2000

IMT-Advanced

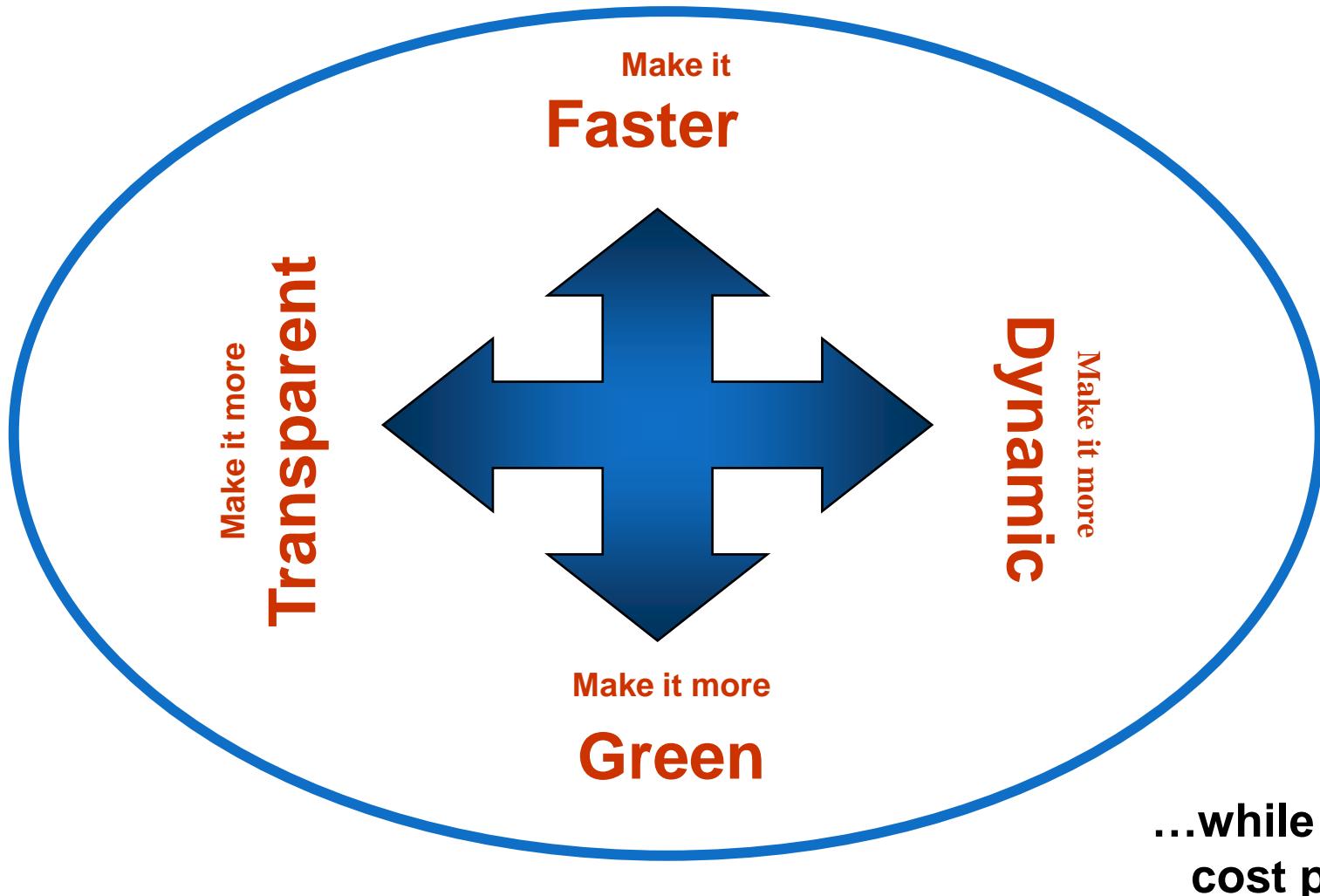
"IMT-2020"

"International Mobile Telecommunications": requirements set by ITU

The 2020+ experience



Networks technology trends



Expected Technology – trends besides radio layers

- **Integration of different technologies (not only physical layer)**
 - Following the current trends....
- **Complex radio environment**
 - CRAN, HCRAN, microcells, as now but device # explosion
- **Separation between infrastructure, network, computation and service**
 - Reconfigurable network and service provision (SDN, NFV, virtualization, cloud...)
 - Edge becoming an entity per se
- **Multi-tenant environment**
 - Different types of providers, different types of interrelations
 - Slicing of resources: deep virtualization (cloud and network)

5G use cases

reinforce B2C, embrace B2B

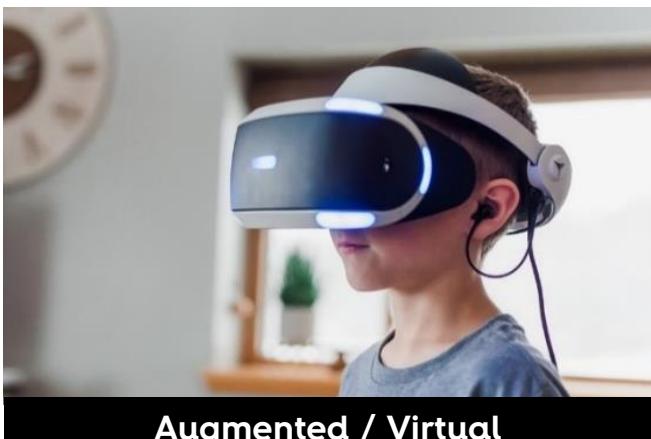
Enhanced Mobile BroadBand (eMBB)



Vídeo UHD- 8K



Mass Events



Augmented / Virtual Immersive Reality

Massive Machine Type Communications (mMTC)



Logistic / Management



Ultra-Reliable and Low-Latency Communications (URLLC)



Industry 4.0



E-Health



Smart Meter



Wearables



Tactile Internet



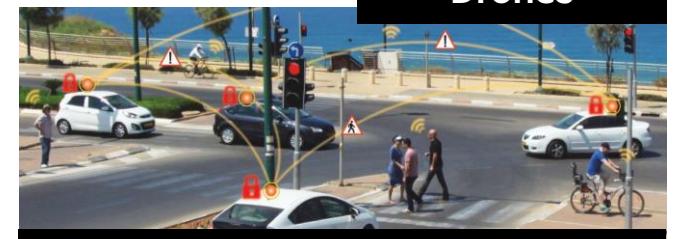
Robots / Drones



Smart Cities

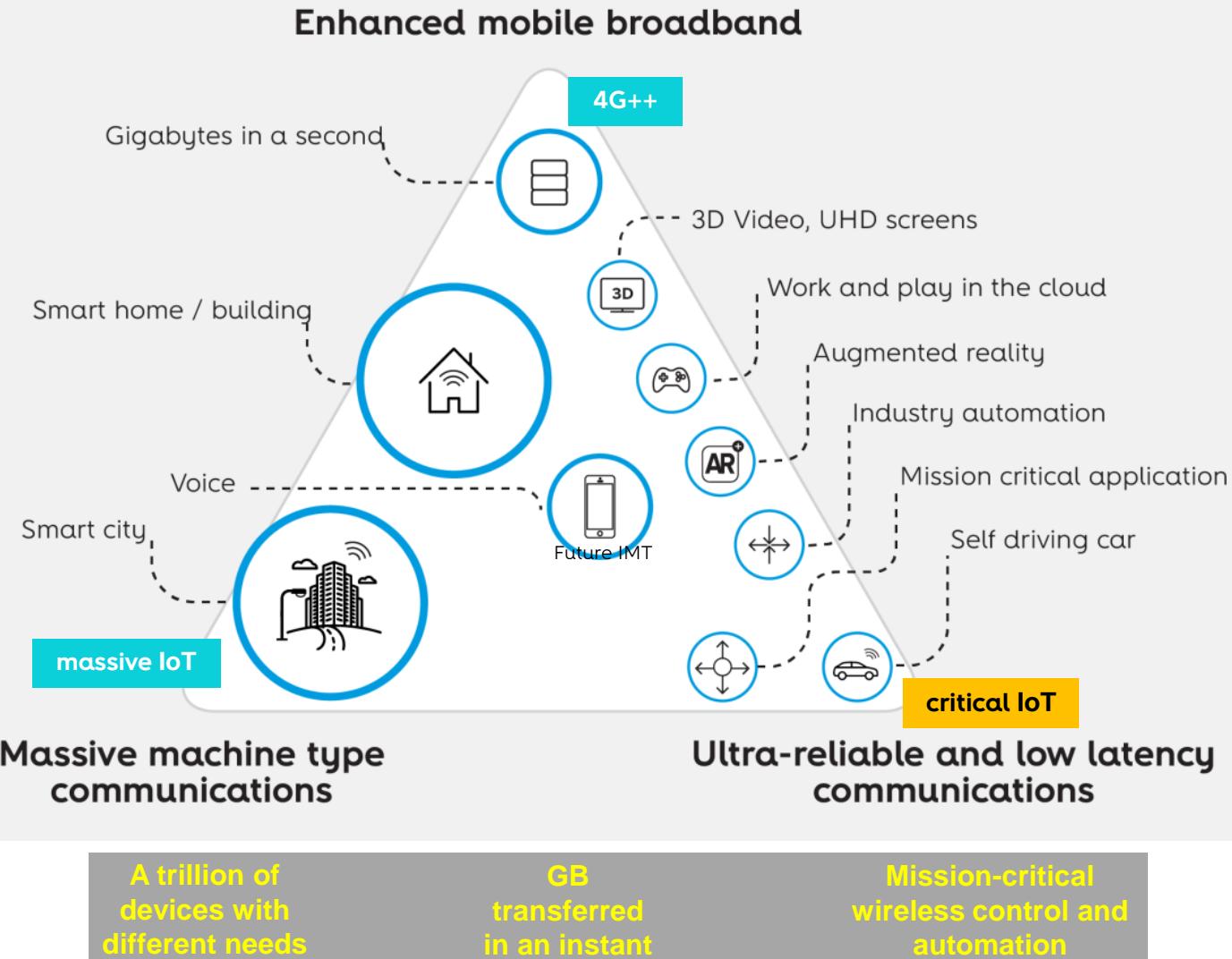


Smart Cities



Connected vehicles (V2x)

5G organization of ‘Usage Scenarios’



5G will power a **new generation of services and applications** in the areas of:

Enhanced Mobile BroadBand (eMBB)
Make it faster!

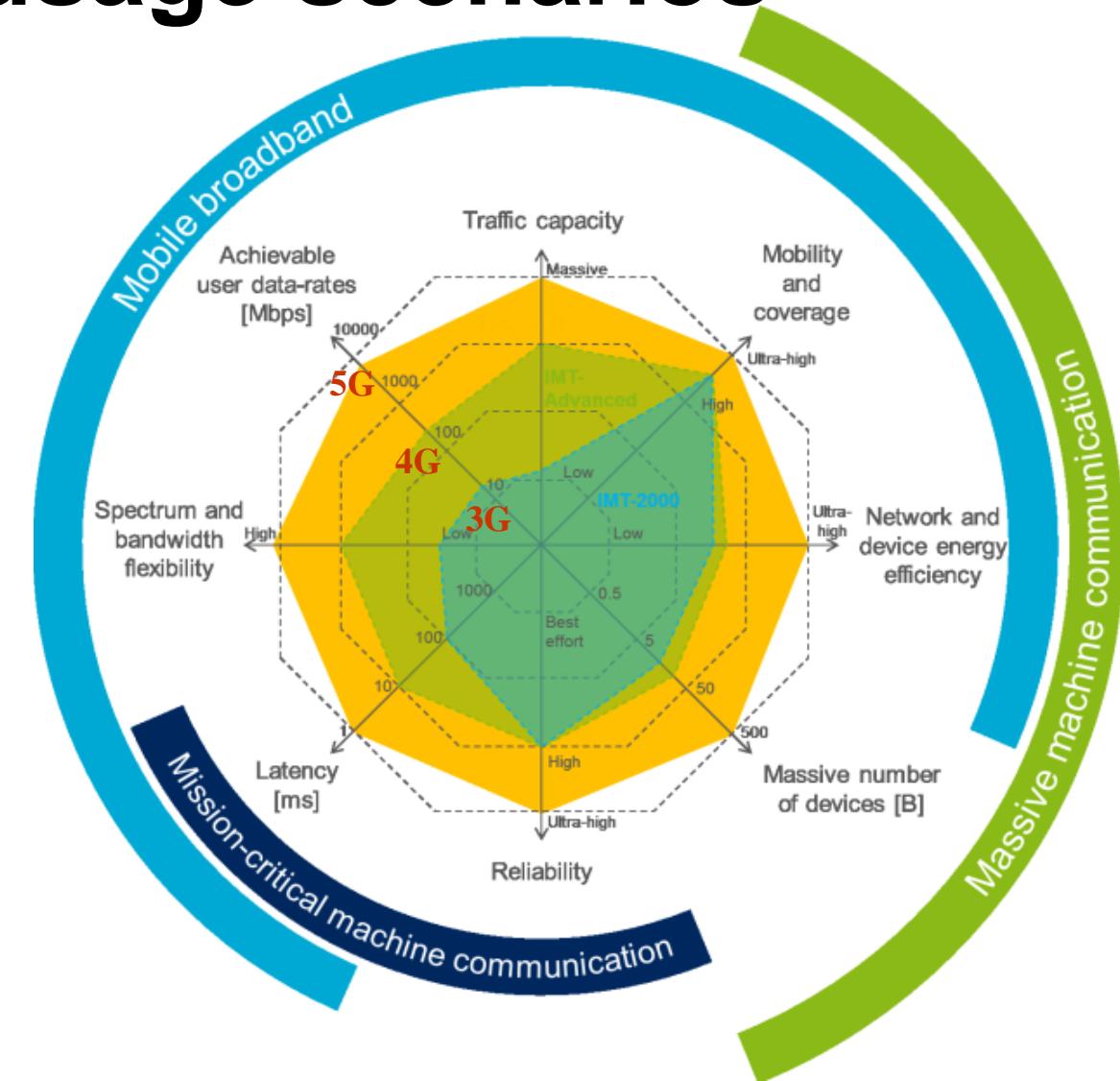
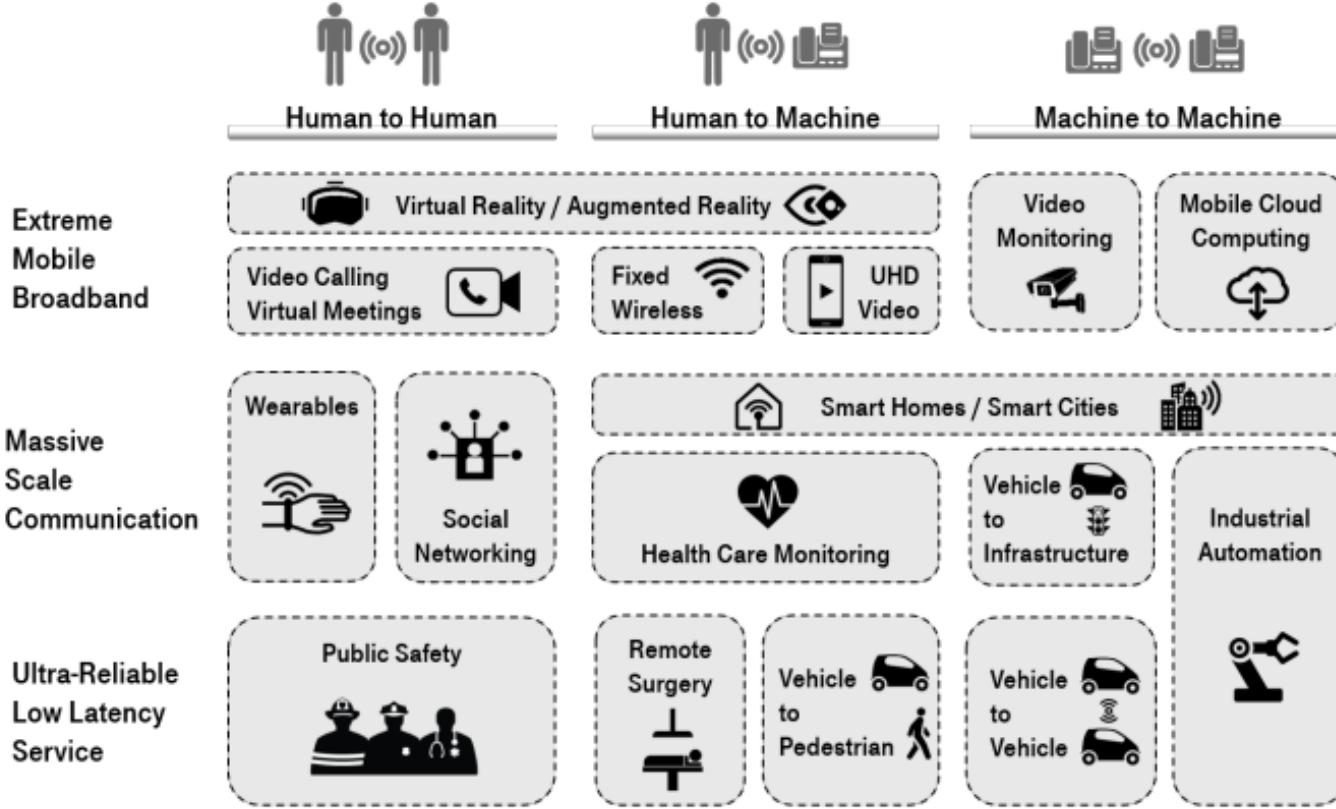
Massive Machine Type Communications (mMTC)
Make it massive!

Ultra-Reliable, Low Latency Communications (URLCC)
Make it trustable and responsive!

All with a single, unified technology

...while driving down the cost per managed bit

5G organization of usage scenarios



5G: From Research to Standardisation,
http://www.irisa.fr/dionysos/pages_perso/ksentini/R2S/pres/Bernard-EC-Panel-R2S-2014.pdf

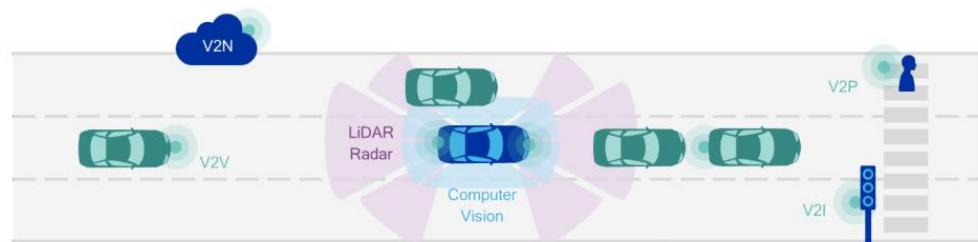
Example of verticals: 5GAA (5G Automotive Association)

<http://5gaa.org/>

“Develop, test and promote communications solutions, initiate their standardization and accelerate their commercial availability and global market penetration to address society’s connected mobility and road safety needs with applications such as autonomous driving, ubiquitous access to services and integration into smart city and intelligent transportation”

Vehicle to anything (V2x) communications:

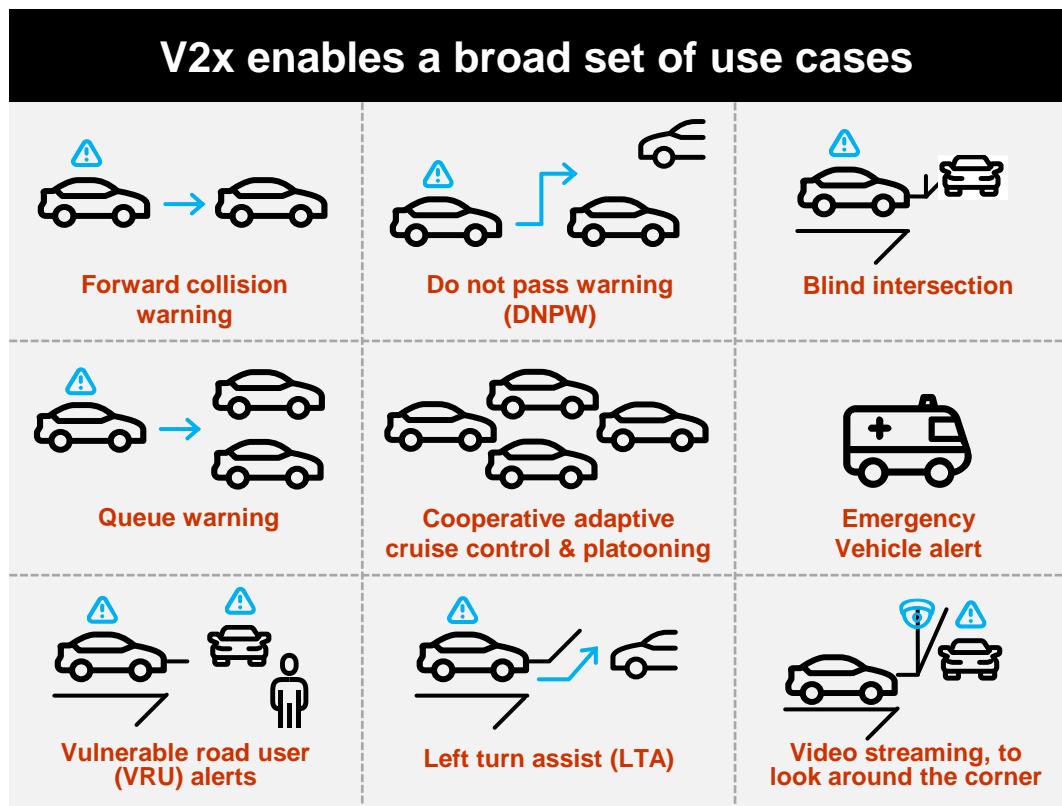
- Vehicle to Vehicle (V2V)
- Vehicle to Network (V2N)
- Vehicle to Infrastructure (V2I)
- Vehicle to Pedestrian (V2P)



V2x Use Cases

3GPP V2x evolutionary support

Adapted from Qualcomm



Enhanced V2x C-V2x 3GPP Rel 14

Basic V2x 802.11p, DSRC, ETSI ITS

- V2v, V2p, V2i
- Safety
- EV

Advanced V2x C-V2x 3GPP Rel 15 and future Rel 16, etc

- Longer range
- Higher density
- Very high throughput
- Very high reliability
- Wideband ranging and positioning
- Very low latency

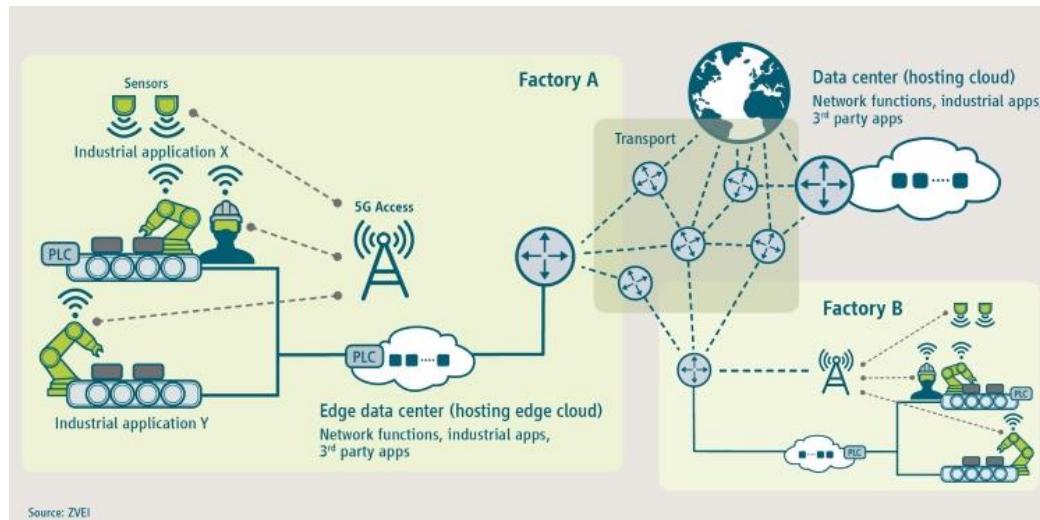
Source: 5G Americas Whitepaper, "Cellular V2x Communications towards 5G", Mar'18

Communication scenario description	Max end-to-end latency (ms)	Reliability (%)
Information exchange between a UE supporting V2X application and a V2X Application Server	5	99.999
Cooperative driving for vehicle platooning		
Information exchange between a group of UEs supporting V2X application.	10	99.99
Emergency trajectory alignment between UEs supporting V2X application.	3	99.999
Sensor information sharing between UEs supporting V2X application	3	99.999

Example of verticals: 5G-ACIA

<https://www.5g-acia.org/>

“5G-ACIA ensures the best possible applicability of 5G technology and 5G networks for the manufacturing and process industries by addressing, discussing and evaluating relevant technical, regulatory and business aspects.”

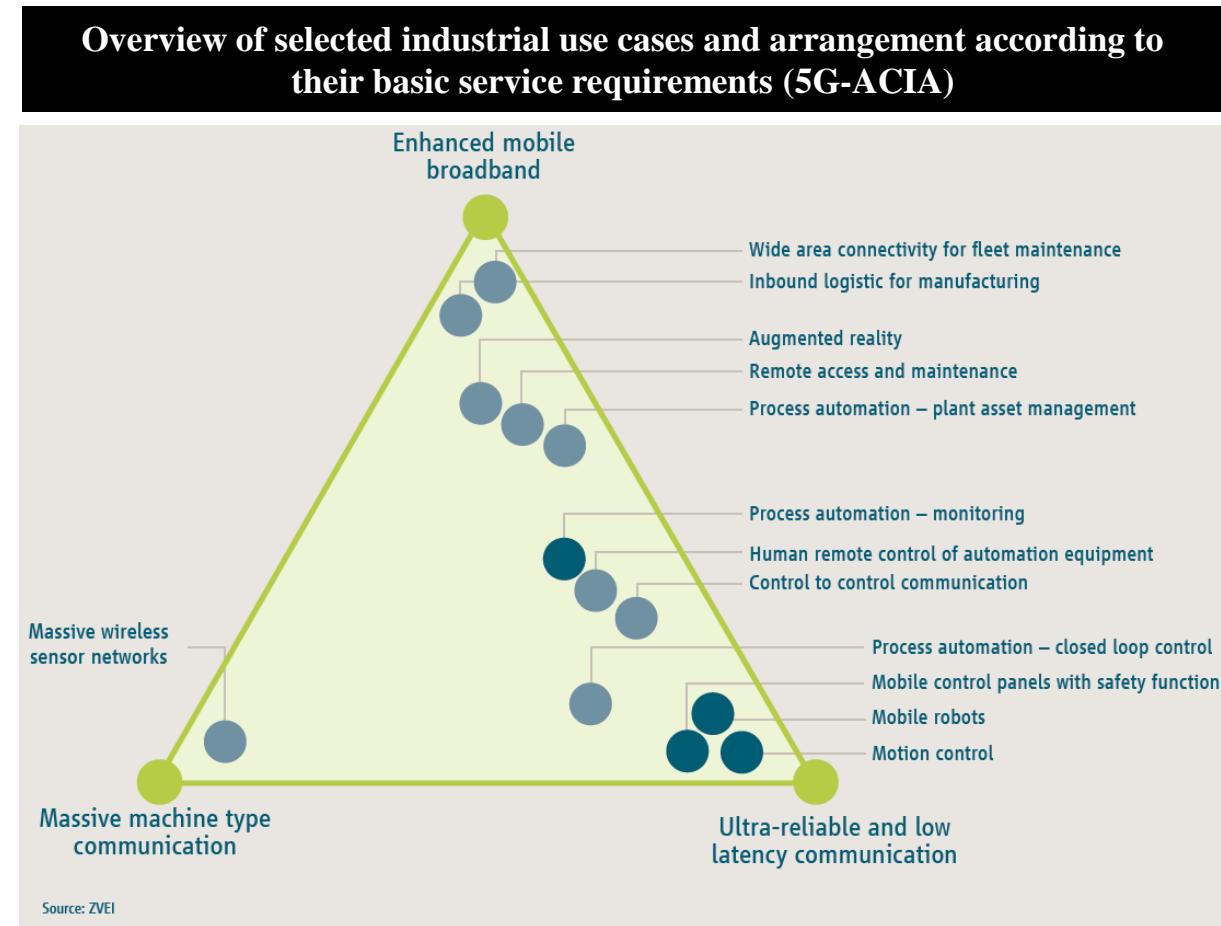


Source: 5G-ACIA, “5G for Connected Industries and Automation”, Whitepaper, Apr'18

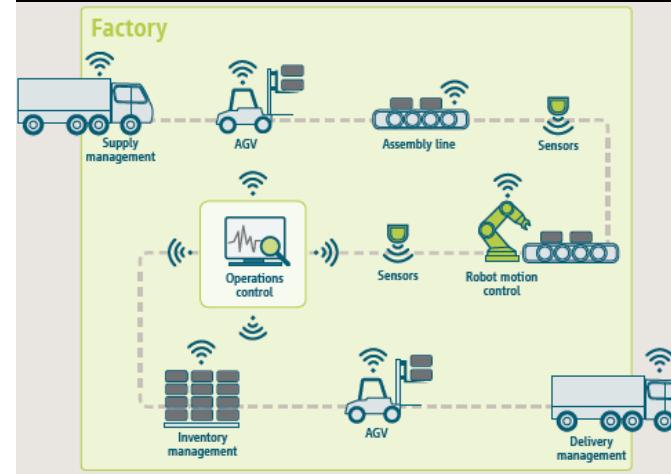


Industry use cases

- 5G in the private domain



Exemplary application areas of 5G in the factory of the future (5G-ACIA)



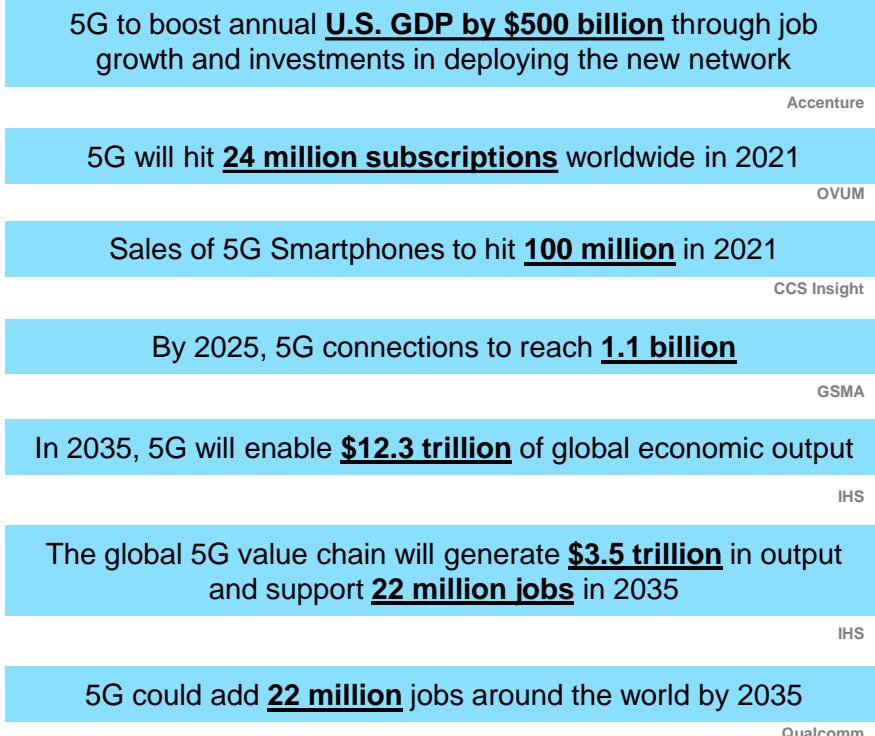
Selected use cases requirements (5G-ACIA)

Use case (high level)	Availability	Cycle time	Typical payload size	# of devices	Typical service area
Motion control	>99.9999%	< 2 ms	20 bytes	>100	100 m x 100 m x 30 m
	>99.9999%	< 0.5 ms	50 bytes	~20	15 m x 15 m x 3 m
	>99.9999%	< 1 ms	40 bytes	~50	10 m x 5 m x 3 m
Mobile robots	>99.9999%	1 ms	40-250 bytes	100	< 1 km ²
	>99.9999%	10 – 100 ms	15 – 150 kbytes	100	< 1 km ²
Mobile control panels with safety functions	>99.9999%	4-8 ms	40-250 bytes	4	10 m x 10 m
	>99.9999%	12 ms	40-250 bytes	2	40 m x 60 m
Process automation (process monitoring)	>99.99%	> 50 ms	Varies	10000 devices per km ²	

Service unavailability <31,5s / Year

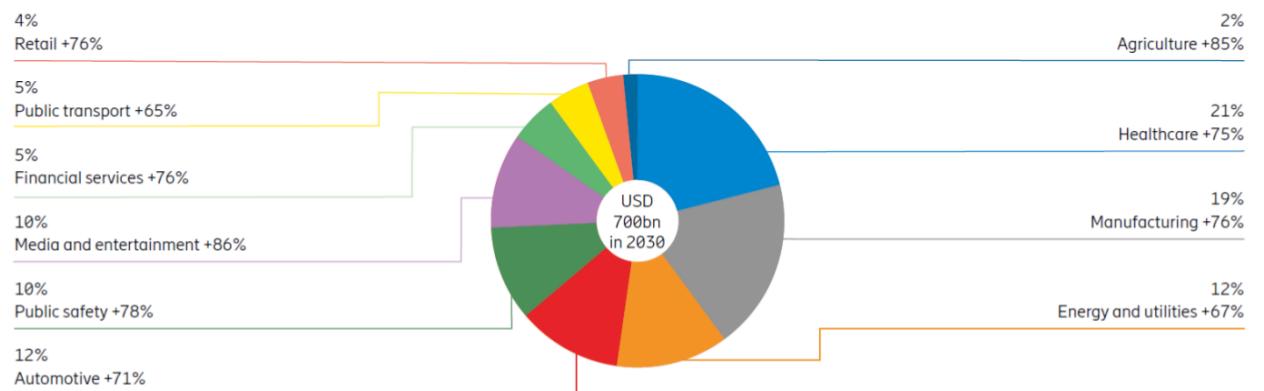
Cycle time shall be measured from command execution to feedback received ➔ 5G latency < half the cycle time

5G expectations



Confirmed significant 5G-enabled revenue potential across 10 industries

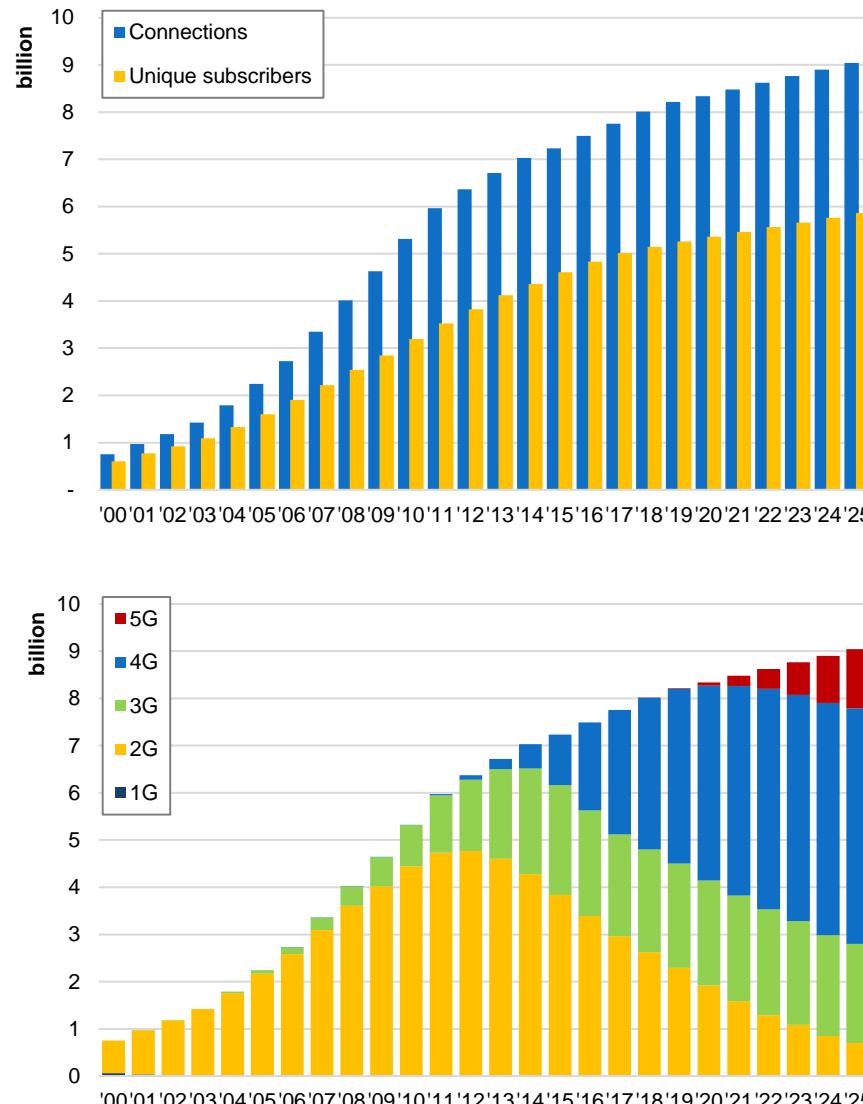
Share and growth rate for global total 5G-enabled B2B potential for service providers



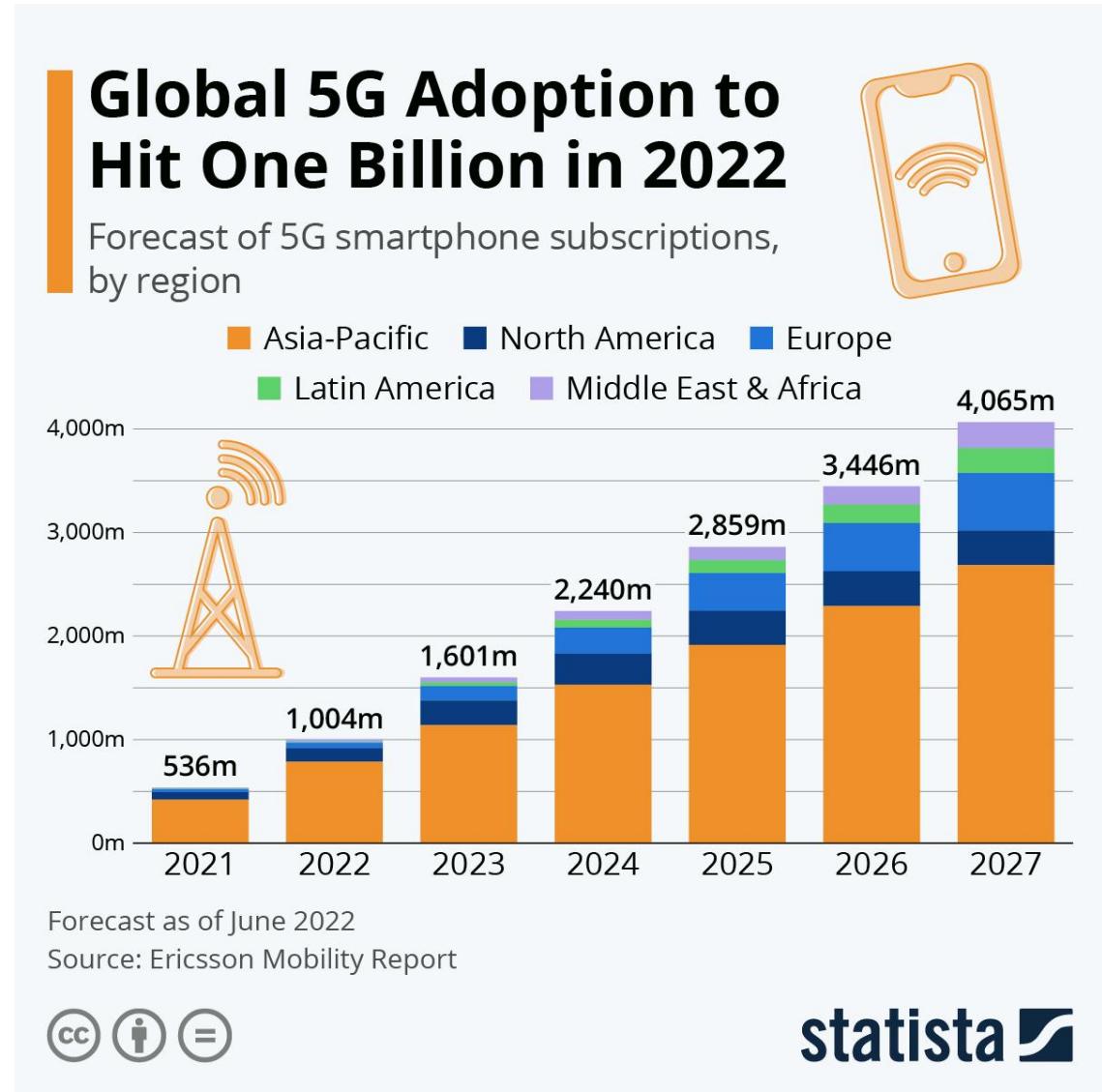
Global service creator, 5G for business addressable market, 2030 share, 2020-2030 CAGR
(Worldwide figures)

Source: Ericsson and Arthur D. Little
5G for business: a 2030 market compass

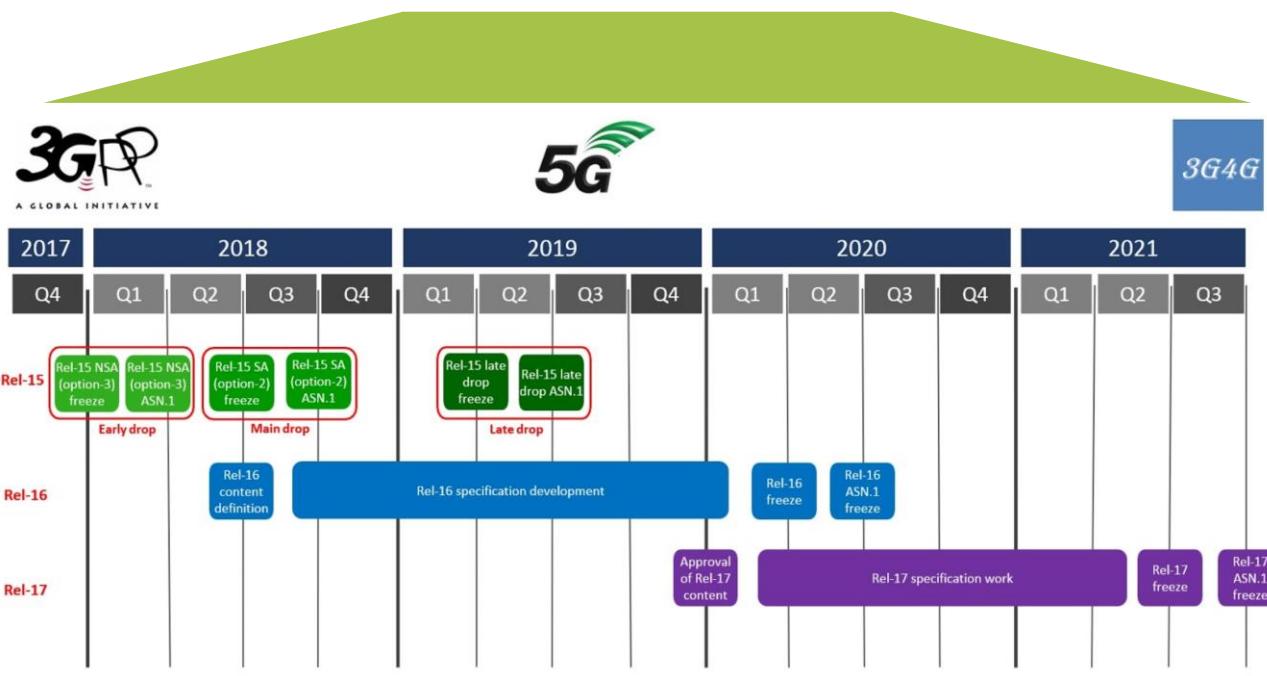
Market Forecast



[GSMA Market data, Apr. 2018]



5G roadmap



Designed by 3G4G, based on roadmap from 3GPP, July 2019

3GPP Releases detail (I)



Release 15

- NR
- The 5G System – Phase 1
- Massive MTC and Internet of Things (IoT)
- Vehicle-to-Everything Communications (V2x) Phase 2
- Mission Critical (MC) interworking with legacy systems
- WLAN and unlicensed spectrum use
- Slicing – logical end-2-end networks
- API Exposure – 3rd party access to 5G services
- Service Based Architecture (SBA)
- Further LTE improvements
- Mobile Communication System for Railways (FRMCS)



Release 16

Radio enhancements:

- Enh. for NR URLLC
- NR Industrial Internet of Things (NR_IoT)
- NR-based access to unlicensed spectrum (NR_unic)
- Integrated Access and Backhaul (IAB)
- MTC enh. for LTE (LTE_eMTC5)
- NB-IoT (NB_IoTenh3)
- NR Vehicle-to-Everything (NR_V2X)
- 5G V2X with NR sidelink (5G_V2X_NRSL)
- NR positioning support (NR_pos)
- Optimisations on UE radio capability signalling (RACS-RAN)
- UE Power Saving in NR (NR_Ue_pow_sav)
- Enh. on MIMO for NR (NR_eMIMO)
- NR mobility enh. (NR_Mob_enh)
- 2-step RACH for NR (NR_2step_RACH)
LTE-NR & NR-NR Dual Connectivity and NR Carrier
- Aggregation enh. (LTE_NR_DC_CA_enh)
- LTE-based 5G terrestrial broadcast (LTE_terr_bcast)
Cross Link Interference handling and Remote Interference
- Management for NR (NR_CLI_RIM)
- DL MIMO efficiency enh. for LTE (LTE_DL_MIMO_EE)
- Navigation Satellite System for LTE (LCS_NAVIC)
- Non-Orthogonal Multiple Access Study (NR_NOMA)

The detail in this graphic is a snap-shot
of some of the key features. Full details
of all of the Release 16 features are at:

www.3gpp.org/specifications/work-plan

System enhancements:

- 5G System (5GS) enablers for new verticals:
Industrial automation, including Time Sensitive
Communication (TSC), Ultra Reliable and
Low Latency Communication (URLLC) and
Non-Public Networks (NPNs)
Cellular Internet of Things (CIoT) support for 5G system
Vehicle-to-Everything (V2X) communication
- Mobile Communication System for Railways (FRMCS Phase 2)
- Satellite Access in 5G
- NR-based access to unlicensed spectrum (nr-U)
- 5G Wireless Wireline Convergence (5WWC)
- Enh. for Network Analytics (eNA)
- Support for Access Traffic Steering, Switching and Splitting (ATSSS)
- Optimized UE radio capability signalling (RACS)
- Enh. Network Slicing (eNS)
- Enh. Service Based Architecture (eSBA)
- Single Radio Voice Call Continuity (5G-SRVCC)
- Enh. Location Services (eLCS)
- Enh. Common API Framework for 3GPP Northbound APIs (eCAPIF)

5G Efficiency: Interference Mitigation, SON, eMIMO,
Location and positioning, Power Consumption, eDual
Connectivity, Device capabilities exchange, Mobility enh.

© 3GPP, 2021

5G Phase 1
With an early drop for 5G – NSA (Non-Stand Alone)

3GPP Releases detail (II)

Release 17

- NR MIMO
- NR Sidelink enh.
- 52.6 - 71 GHz with existing waveform
- Dynamic Spectrum Sharing (DSS) enh.
- Industrial IoT / URLLC enh.
- IoT over Non Terrestrial Networks (NTN)
- NR over Non Terrestrial Networks (NTN)
- NR Positioning enh.
- Low complexity NR devices
- Power saving
- NR Coverage enh.
- NR eXtended Reality (XR)
- NB-IoT and LTE-MTC enh.
- 5G Multicast broadcast
- Multi-Radio DCCA enh.
- Multi SIM
- Integrated Access and Backhaul (IAB) enh.

- NR Sidelink relay
- RAN Slicing
- Enh. for small data
- SON / Minimization of drive tests (MDT) enh.
- NR Quality of Experience
- eNB architecture evolution, LTE C-plane / U-plane split
- Satellite components in the 5G architecture
- Non-Public Networks enh.
- Network Automation for 5G - phase 2
- Edge Computing in 5GC
- Proximity based Services in 5GS
- Network Slicing Phase 2
- Enh. V2x Services
- Advanced Interactive Services
- Access Traffic Steering, Switch and Splitting support in the 5G system architecture

- Unmanned Aerial Systems
- 5GC LoCation Services
- Multimedia Priority Service (MPS)
- 5G Wireless and Wireline Convergence
- 5G LAN-type services
- User Plane Function (UPF) enh. for control and 5G Service Based Architecture (SBA)

These are the Rel-17 headline features, prioritized during the December 2019 Plenaries (TSG#86)

Release 18

TSG SA priorities*

SA2 led - System Architecture and Services

- XR (Extended Reality) & media services
- Edge Computing Phase 2
- System Support for AI/ML-based Services
- Enablers for Network Automation for 5G Phase 3
- Enh. support of Non-Public Networks Phase 2
- Network Slicing Phase 3
- 5GC LoCation Services Phase 3
- 5G multicast-broadcast services Phase 2
- Satellite access Phase 2
- 5G System with Satellite Backhaul
- 5G Timing Resiliency and TSC & URLLC enh.
- Evolution of IMS multimedia telephony service
- Personal IoT Networks
- Vehicle Mounted Relays

SA3 led - Security and Privacy

- Privacy of identifiers over radio access
- SECAM and SCAS for 3GPP virtualized network products and Management Function (MfN)
- Mission critical security enhancements Phase 3
- Security and privacy aspects of RAN & SA features

SA4 led - Multimedia Codecs, Systems and Services

Systems & Media Architecture:

- 5G Media, Service Enablers
- Spill-Rendering
- 5G AR Experiences Architecture

Media:

- Video codec for 5G
- Media Capabilities for Augmented Reality Glasses
- AI / ML Study

Real-time Communications:

- XR conversational services
- WebRTC-based services and collaboration models

Immersive Voice & Audio:

- EVS Codec Extension for Immersive Voice and Audio Services (IVAS_Codec)
- Terminal Audio quality performance and Test methods for Immersive Audio Services (ATAS)

Streaming & Broadcast services:

- 5GMS Enh. (Network slicing, Low latency, Background traffic, 5GMS Uplink)
- Further MBS Enh. (Free to air, Hybrid unicast/broadcast)

*These are preliminary lists (As at SA#94-e)

See the 3GPP Work Plan for full details, as Release 18 develops:
www.3gpp.org/specifications/work-plan

© 3GPP, Dec. 2021

RAN1 led - Radio Layer 1 (Physical layer)

- NR-MIMO Evolution
- AI/ML - Air Interface
- Evolution of duplex operation
- NR Sidelink Evolution
- Positioning Evolution
- RedCap Evolution
- Network energy savings
- Further UE coverage enhancement
- Smart Repeater
- DSS
- Low power WUS
- CA enhancements

RAN2 led - Radio layer 2 & layer 3 Radio Resource Control

- Mobility Enhancements
- Enhancements for XR
- Sidelink Relay Enhancements
- NTN (Non-Terrestrial Networks) evolution - NR
- NTN (Non-Terrestrial Networks) evolution - IoT
- UAV (Uncrewed Aerial Vehicle)
- Multiple SIM (MUSIM) Enhancements
- In-Device Co-existence (IDC) Enhancements
- Small data
- MBS

RAN3 led - UTRAN/E-UTRAN/NG-RAN architecture & related network interfaces

- Additional topological improvements – IAB/VMR
- AI/ML for NG-RAN WI
- AI/ML for NG-RAN SI
- SON/MDT Enhancements
- QoE Enhancements
- Resiliency of gNB-CU-CP

RAN4 led - Radio Performance and Protocol Aspects

- RAN4-led spectrum items
- <5MHz in dedicated spectrum

Rel-18 Workplan for TSG CT

CT will work on Stage 3 completion and ASN.1 code and OpenAPI freeze of Rel-17 until June 2022 (TSG#96).

Work item discussion on Rel-18 Stage 2 / Stage 3 (under CT) from June 2022.

TSG RAN priorities*

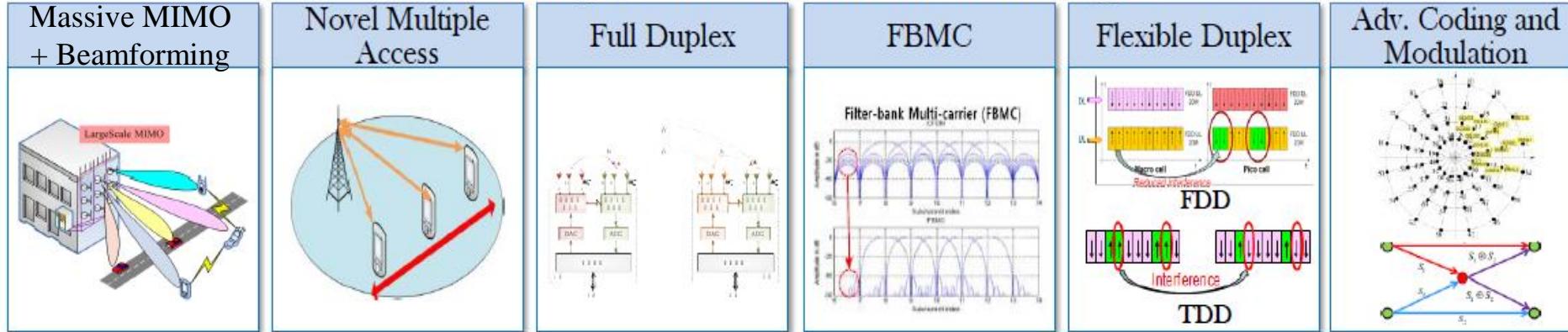
- NR1 led - Radio Layer 1 (Physical layer)
- NR-MIMO Evolution
- AI/ML - Air Interface
- Evolution of duplex operation
- NR Sidelink Evolution
- Positioning Evolution
- RedCap Evolution
- Network energy savings
- Further UE coverage enhancement
- Smart Repeater
- DSS
- Low power WUS
- CA enhancements

80

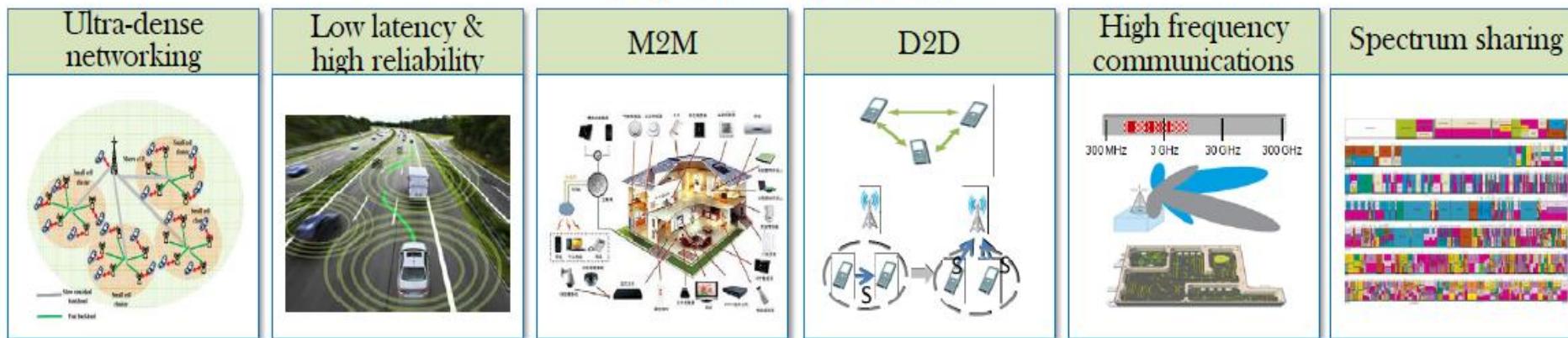
5G – TECHNOLOGIES

Key Wireless Technology Directions

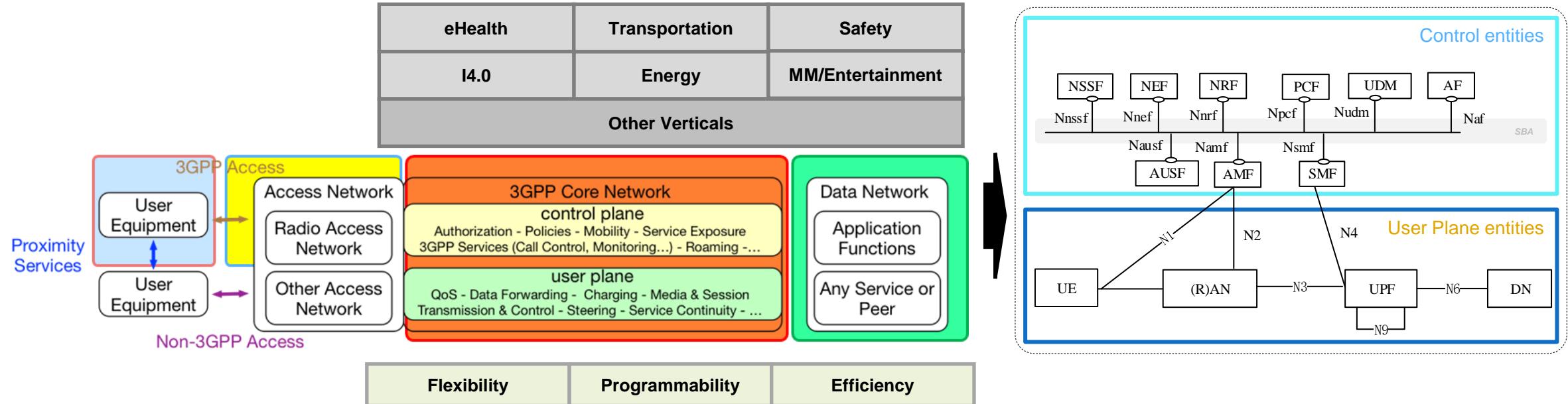
Enabling wireless transmission technologies



Key technical solutions



5G main building blocks



Based on a **new, unified, air interface** (*New Radio: NR - 5G-NR*) and a **new network architecture**, to connect everything

5G New Radio (NR) to “connect everything”:
A unified air interface

You will be seeing 5G NR connectivity in your smartphones, cars, utility meters, wearables and much more (Qualcomm)

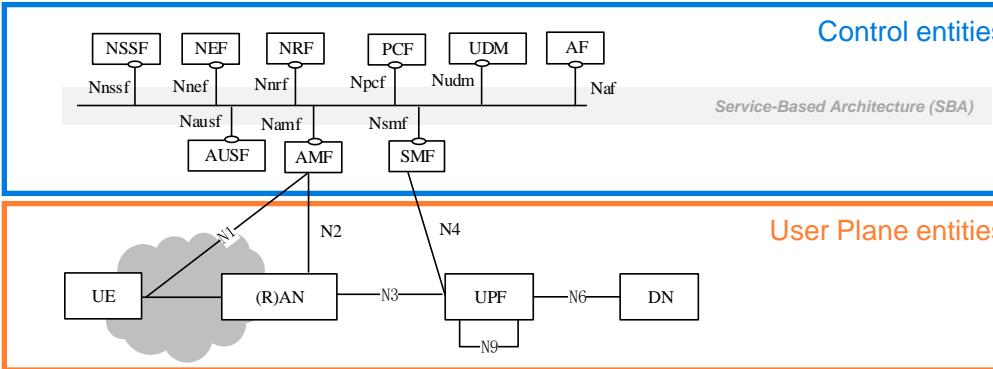
Able to **embrace all sort of wireless/wired accesses**, sharing a common core (5G Core Network – **5GC**)

5G new architecture to “interconnect everything”:
A common core network

The new architecture shall support at least the new RAT(s), the Evolved E-UTRA, non-3GPP accesses and minimize access dependencies (3GPP TR 23.799)

5G System arch. and functional modules (parcial)

3GPP TS 23.501 V0.3.1 (2017-03)



- Separate the User Plane (UP) functions from the Control Plane (CP) functions
- Modularize the function design, e.g. to enable flexible and efficient network slicing
- Define procedures (i.e. the set of interactions between network functions) as services
- Enable each Network Function to interact with other NF directly if required (direct interaction)
- Minimize dependencies between the Access Network (AN) and the Core Network (CN)
- Support a unified authentication framework
- Support "stateless" NFs, where the "compute" resource is decoupled from the "storage" resource
- Support capability exposure
- Support concurrent access to local and centralized services. To support low latency services and access to local data networks, UP functions can be deployed close to the Access Network

1. Network Slice Selection Function (NSSF)
2. Network Exposure Function (NEF)
3. NF Repository Function (NRF)
4. Policy Control Function (PCF)
5. Unified Data Management (UDM)
6. Application Function (AF)
7. Authentication Server Function (AUSF)
8. Access and Mobility Management Function (AMF)
9. Session Management Function (SMF)
10. Unified Data Repository (UDR)
11. Unstructured Data Storage Function (UDSF)
12. 5G-Equipment Identity Register (5G-EIR)
13. Security Edge Protection Proxy (SEPP)
14. Network Data Analytics Function (NWDAF)

1. User Equipment (UE)
2. (Radio) Access Network ((R)AN)
3. User Plane Function (UPF)
4. Data Network (DN)

5G: a New Radio is required

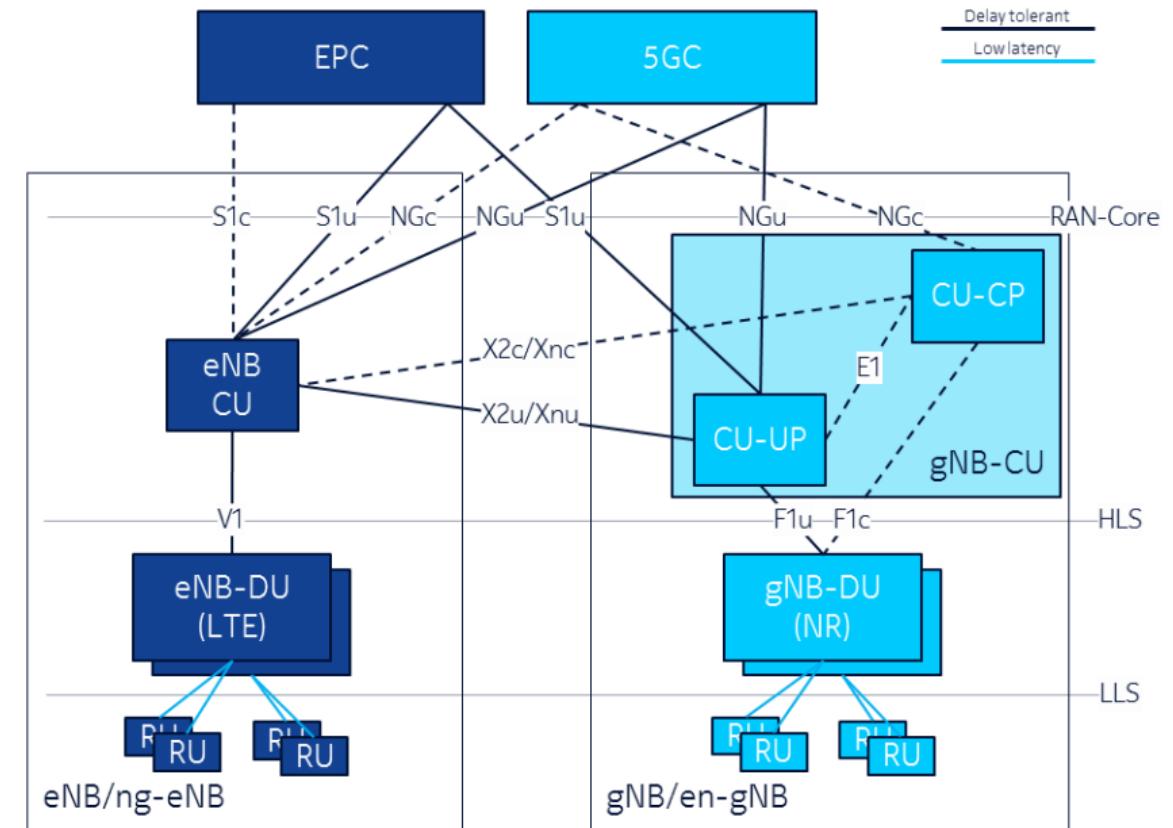
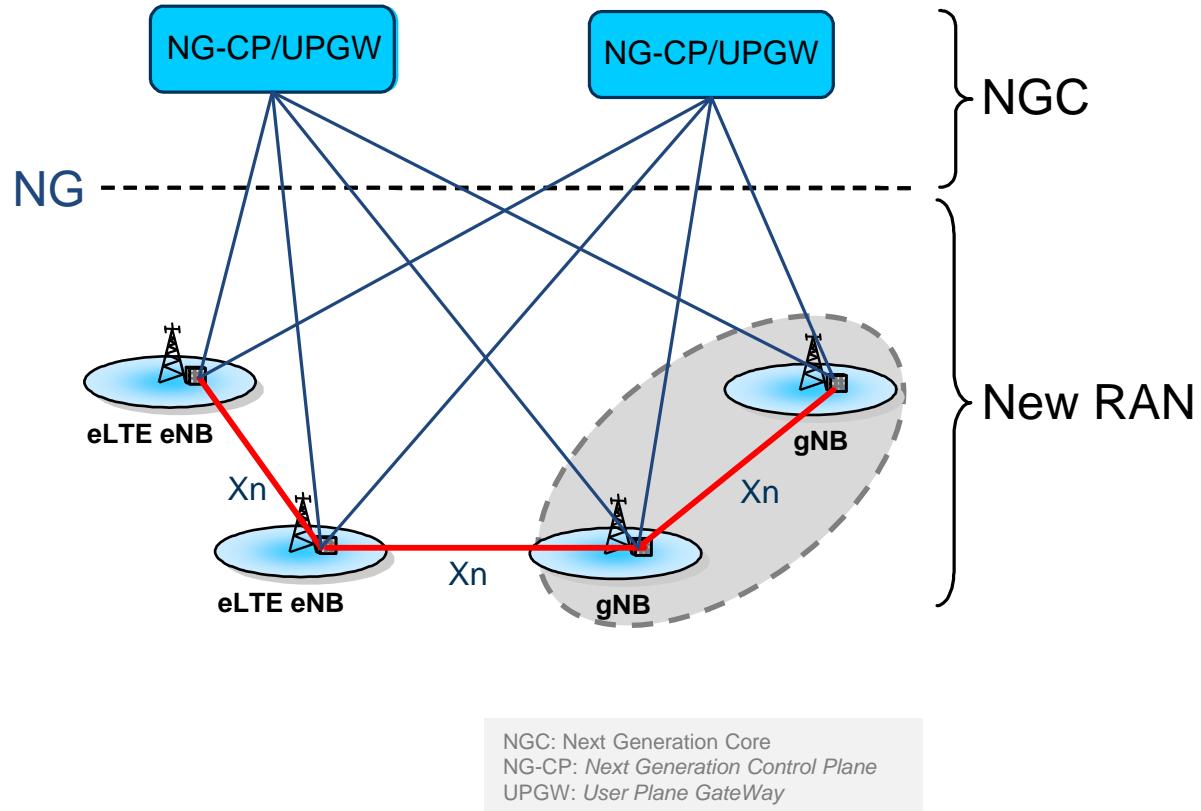
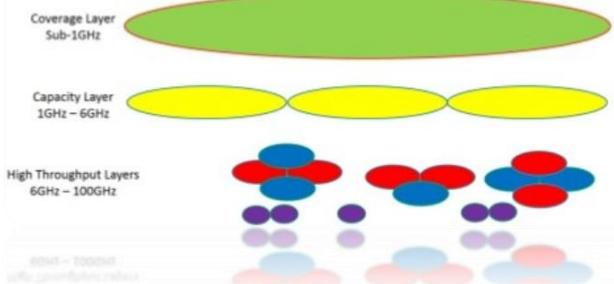
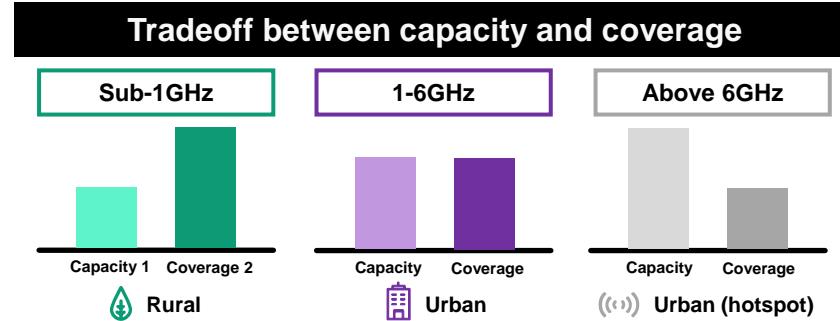
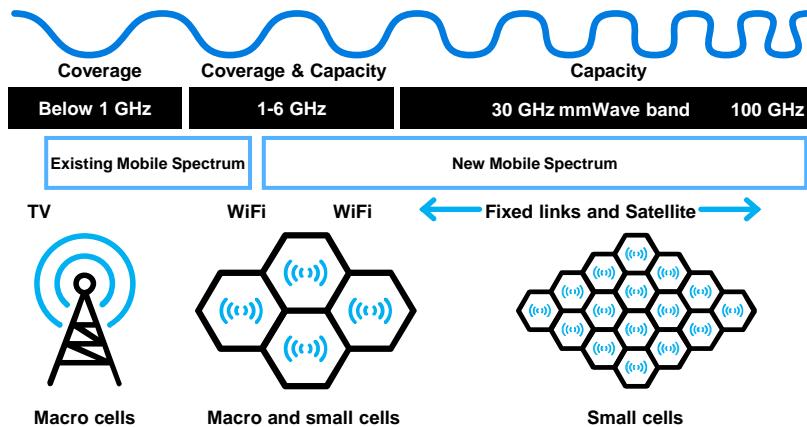
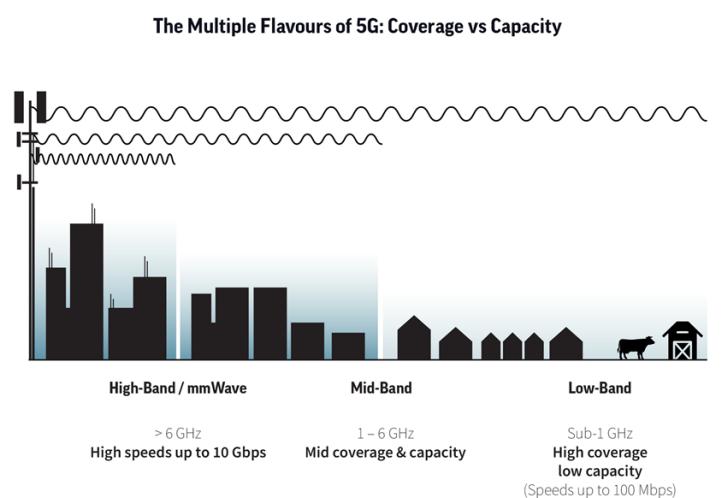


Figure 3: Overall RAN architecture

Larger spectrum usage to cover all applications



Universal coverage (10's of Mb/s) of reliable connectivity
Urban coverage with dense small cells (1-3 Gb/s) e.g. mobile Gb/s society, smart cities, option for connected highways
Hot spots coverage (up to 10 Gb/s) e.g. fixed wireless access, railway stations, sport events, smart factories,



5G-NR to operate on a larger spectrum range

- Expanding to lower freqs. for coverage and penetration
- Expanding to higher freqs. for capacity and low latency

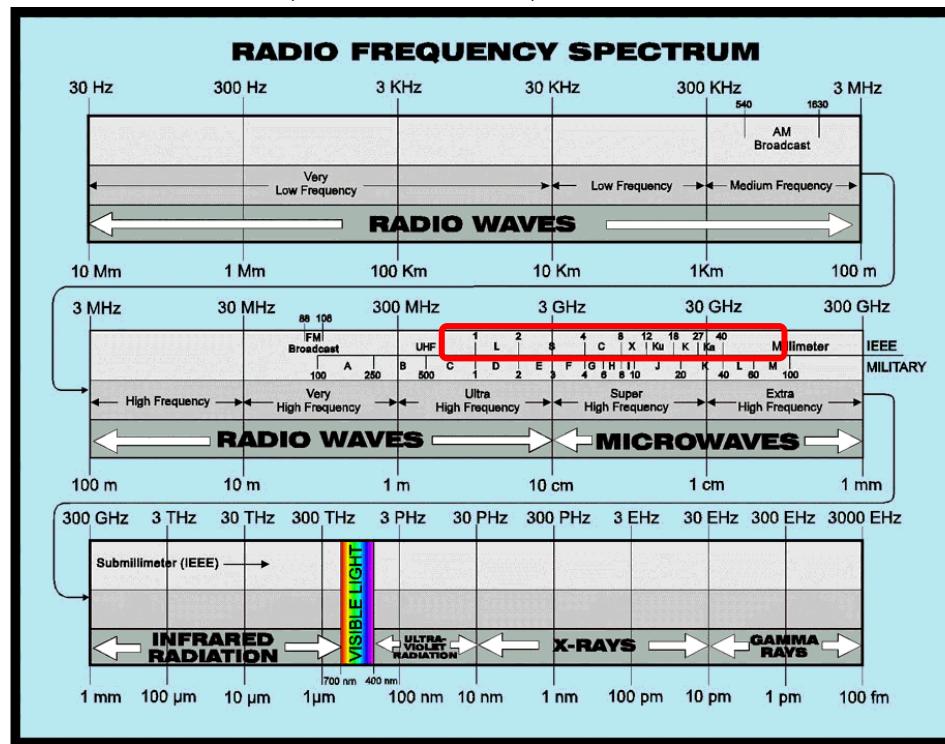
5G Spectrum

http://rspg-spectrum.eu/wp-content/uploads/2013/03/RPSG16-032-Opinion_5G.pdf

RADIO SPECTRUM POLICY GROUP, "STRATEGIC ROADMAP TOWARDS 5G FOR EUROPE"
"Opinion on spectrum related aspects for next-generation wireless systems (5G)", Nov/16

- <1GHz (e.g. 700MHz)
to "enable nationwide and indoor 5G coverage" < 1GHz
- 3400-3800 MHz GHz
 - >100MHz (400MHz) of continuous spectrum
to "put Europe at the forefront of the 5G deployment" > 1GHz
< 6GHz
- 24.25-27.5 GHz
"pioneer band for earlier implementation in Europe"
- 31.8-33.4 GHz
"looks a promising band which could be made available"
- 40.5-43.5 GHz
"is a viable option for 5G in the longer term" > 6GHz

IMT frequencies usage between 24.25 and 86GHz will be analysed at the ITU-T WRC'19 (Nov/19)

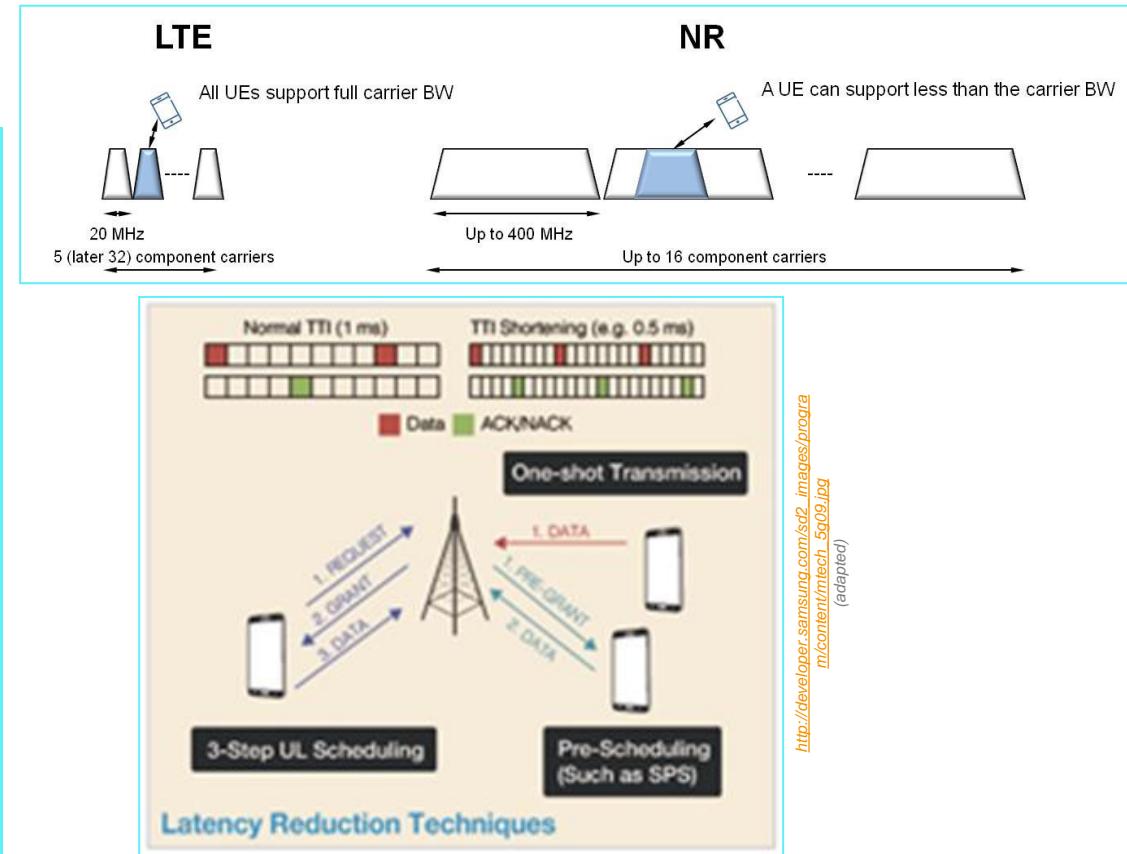


PT Auction results

	Quantidade de frequência adquirida									
	Dense Air	Dixarobil	MEO	NOS	NOWO	VODAFONE	TOTAL			
700 MHz	0	0	10 MHz	20 MHz	0	20 MHz	50 MHz			
900 MHz	0	10 MHz	4 MHz	4 MHz			18 MHz			
1800 MHz	0	10 MHz	0	0	20 MHz	0	30 MHz			
2,1 GHz	0	0	0	10 MHz	0	0	10 MHz			
2,6 GHz	0	35 MHz	0	0	10 MHz	0	45 MHz			
3,6 GHz	40 MHz	40 MHz	90 MHz	100 MHz	40 MHz	90 MHz	400 MHz			
Total	40 MHz	95 MHz	104 MHz	134 MHz	70 MHz	110 MHz	553 MHz			

5G-NR main characteristics

- Operation from low to very high bands: 0.4 – 100GHz
 - Including standalone operation in unlicensed bands
- Up to 400 MHz component-carrier bandwidth (20 MHz for LTE)
 - Up to 100MHz in <6GHz
 - Up to 400MHz in >6GHz
- Up to 16 component carriers
- Set of different numerologies for optimal operation in different frequency ranges
- Native support for Low Latency
 - Shortened Transmission Time Interval (TTI)
- Native support for Ultra Reliability (Multiple diversity mechanisms)
- Flexible and modular RAN architecture: split fronthaul, split control-and user-plane
- Support for devices connecting directly, with no network (D2D, V2X)
- Native end-to-end support for Network Slicing
- New channel coding
 - LDPC for data channel, Polar coding for control channel



4G/LTE:

- Turbo codes for data channels
- TBCCs (tail-biting convolutional codes) for control channels.

LDPC (Low-Density Parity-Check):

- Improved performance: block error rate (BLER) around or below 10^{-5} for all code sizes and code rates
- Reduced decoding complexity and improved decoding latency (lower overall latency)
- Better area throughput efficiency and higher peak throughput

5G NR Logical ,Transport and Physical Channels Mapping

Logical Channel Definition: Medium Access Control (MAC) Layer of NR provides services to the Radio Link Control (RLC) Layer in the form of logical channels. A logical channel is defined by the type of information it carries and is generally differentiated as a control channel, used for transmission of control and configuration information or as a traffic channel used for the user data.

List of Logical Channels for NR:

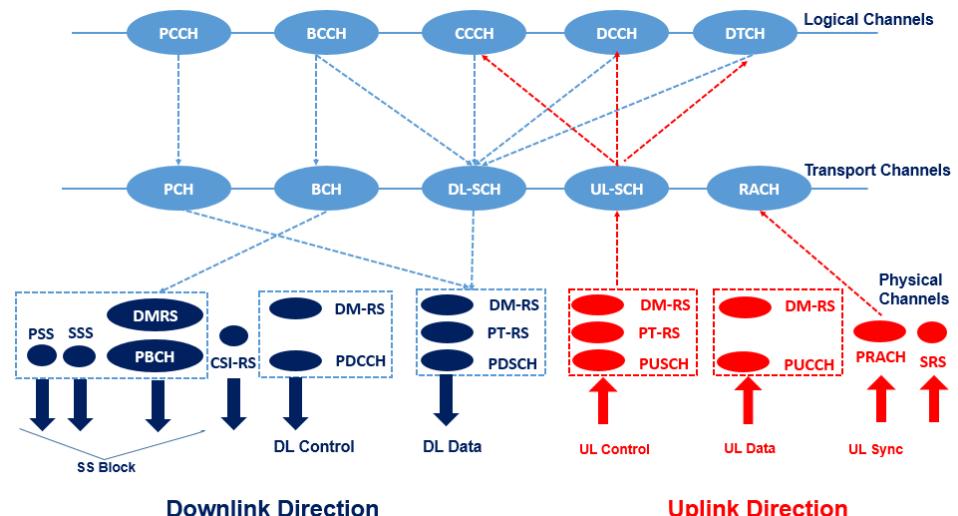
- **Broadcast Control Channel (BCCH):** It is used for transmitting system information from the network to UEs in a cell coverage.
- **Paging Control Channel (PCCH):** This is used to page the UEs whose location at cell level is not known to the network.
- **Common Control Channel (CCCH):** It is used for transmission of control information to UEs with respect to Random Access
- **Dedicated Control Channel (DCCH):** It is used for transmission of control information to/from a UE. This channel is used for individual configuration of UEs such as setting different parameters for different layers.
- **Dedicated Traffic Channel (DTCH):** It is used for transmission of user data to/from a UE. This is the logical channel type used for transmission of all unicast uplink and downlink user data.

Transport Channel Definition: A transport channel is defined by how and with what characteristics the information is transmitted over the radio interface. From the physical layer, the MAC layer uses services in the form of transport channels. Data on a transport channel are organized into transport blocks.

List of Transport Channels for NR:

- **Broadcast Channel (BCH) :** It is used for transmitting the BCCH system information, more specifically Master Information Block (MIB). It has a fixed transport format, provided by the specifications.
- **Paging Channel (PCH):** This channel is used for transmission of paging information from the PCCH logical channel. The PCH supports discontinuous reception (DRX) to allow the device to save battery power by waking up to receive the PCH only at predefined time instants.
- **Downlink Shared Channel (DL-SCH) :** This is the main transport channel used for transmitting downlink data in NR. It supports key all NR features such as dynamic rate adaptation and channel aware scheduling, HARQ and spatial multiplexing. DL-SCH is also used for transmitting some parts of the BCCH system info which is not mapped to the BCH. Each device has a DL-SCH per cell it is connected to. In slots where system information is received there is one additional DL-SCH from the device perspective.
- **Uplink Shared Channel (UL-SCH):** This is the uplink counterpart to the DL-SCH that is, the uplink transport channel used for transmission of uplink data.
- **Random-Access Channel (RACH):** RACH is also a transport channel, although it does not carry transport blocks.

Logical, Transport and Physical Channel Mapping



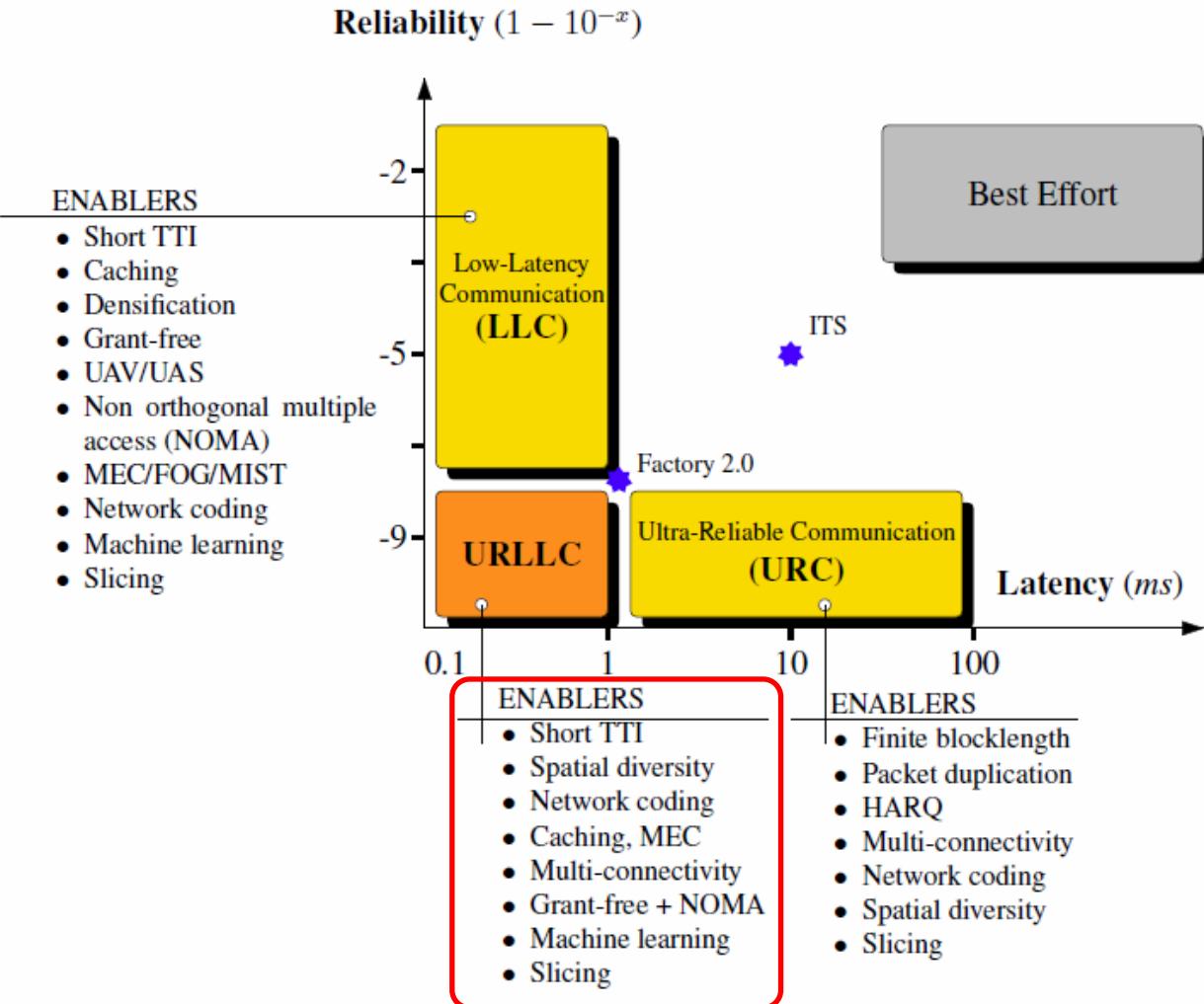
URLLC: The Ultra Reliability versus Low Latency challenge

Answering two conflicting requirements:
• **Low latency and ultra-high reliability**

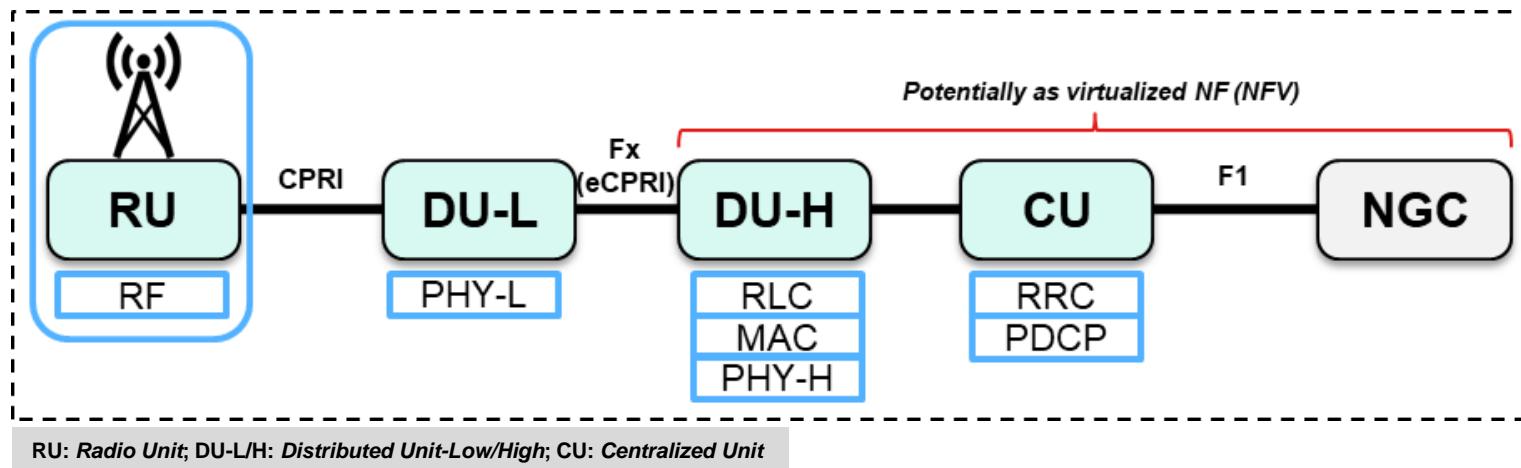
Release 16 objective:

- **0.5-1ms one-way latency**
- **Reliability of up to 99.9999%**

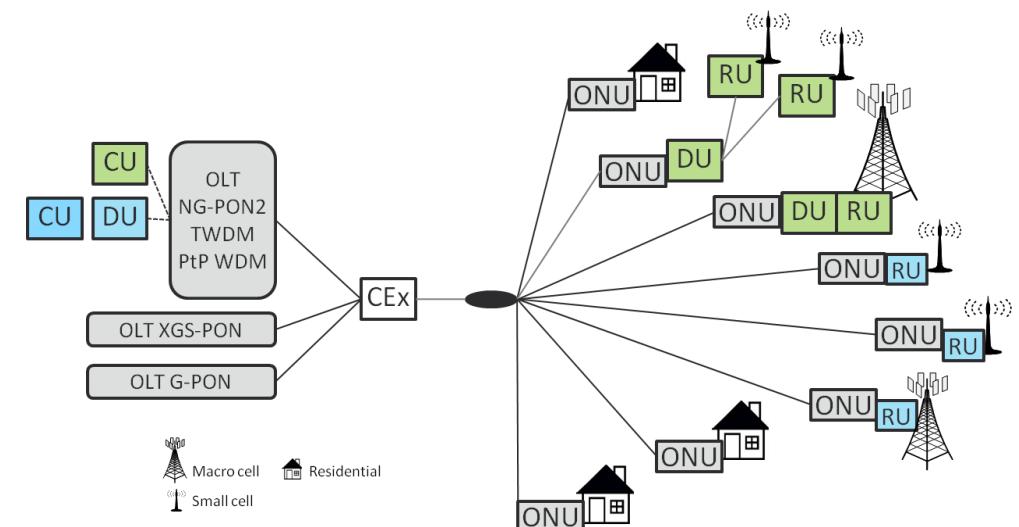
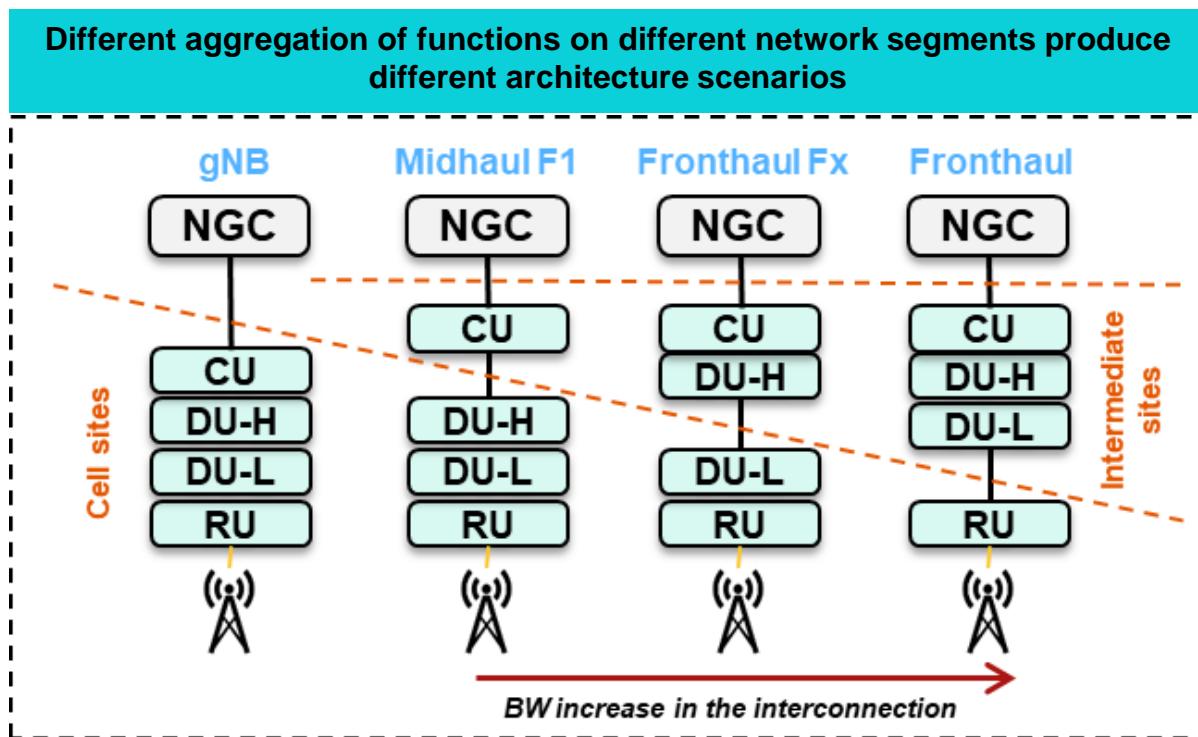
Retransmissions (e.g. HARQ) and packet duplications in time (e.g. PDCP duplications) are useless, considering the low latency budget



RAN decomposition: Distributed RAN (DRAN)



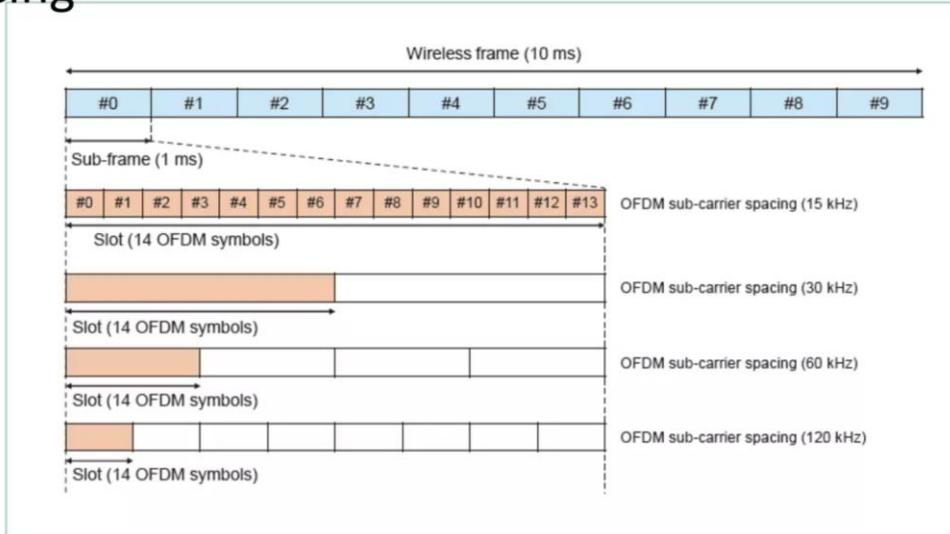
- Simplified cell site, allowing densification and reducing costs
- Centralize complex processing and coordination (CoMP)
- Enable transportation by packet based technologies (e.g. GPON)
- Reduce fronthaul traffic
- Benefit from softwarization
- Be flexible and extendable



Source: ITU-T SG15 – ZTE contribution to “PON use cases for 5G wireless fronthaul”

5G NR Radio Frame

- The 5G NR Radio Frame is in units of 10ms
- Subframes are defined in units of 1ms
- Slots are defines as 14 OFDM Symbols and their time interval depends on sub-carrier spacing

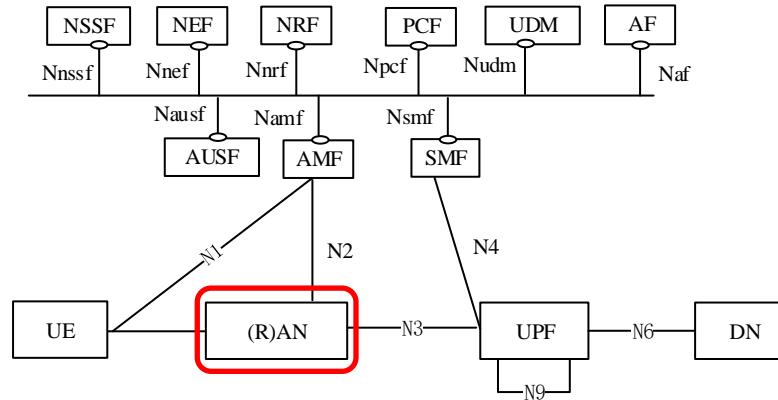


Source: NTT Docomo

RAN

Radio Access Network (RAN)

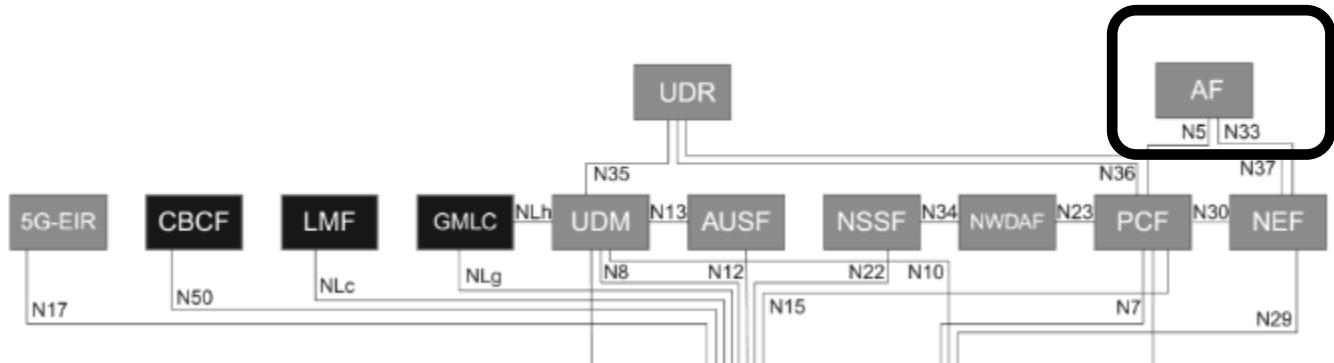
- Radio Resources Management (RRM)
- Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling)
- Selection of an AMF at UE attachment
- Routing of User Plane data towards UPF(s)
- Routing of Control Plane information towards AMF
- Connection setup and release
- Scheduling and transmission of paging messages and system broadcast information
- Measurement and measurement reporting configuration for mobility and scheduling
- Transport level packet marking in the uplink
- Session Management
- Support of Network Slicing
- QoS Flow management and mapping to data radio bearers



The 5G System architecture

- References points representation

- shows the interaction that exist between the NF services in the network
- functions described by point-to-point reference point (e.g. N11)
- between any two network functions (e.g. AMF and SMF)



AF – Application Function

AUSF – Authentication Server Function

AMF – Core Access and Mobility Management Function

SMF – Session Management Function

UPF – User plane Function

DN – Data Network

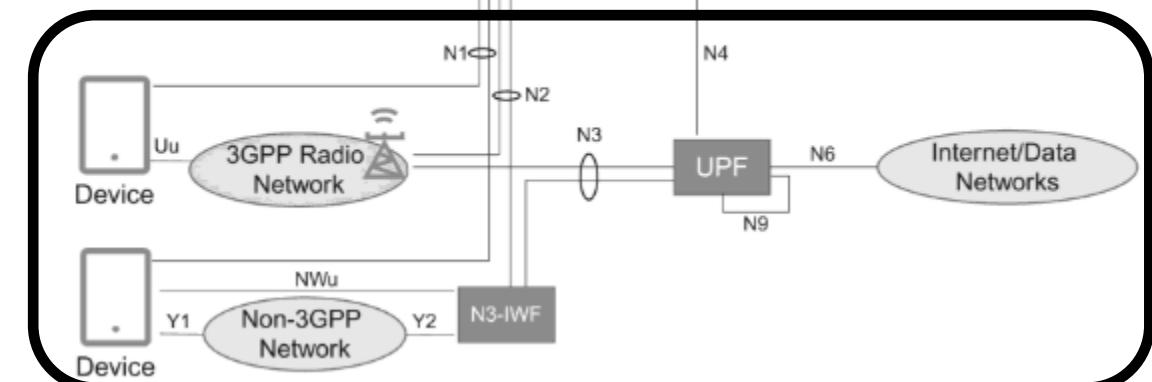
NSSF – network slice selection function

NEF – Network Exposure Function

NRF – Network Repository Function

PCF – Policy Control Function

UDM – User data management

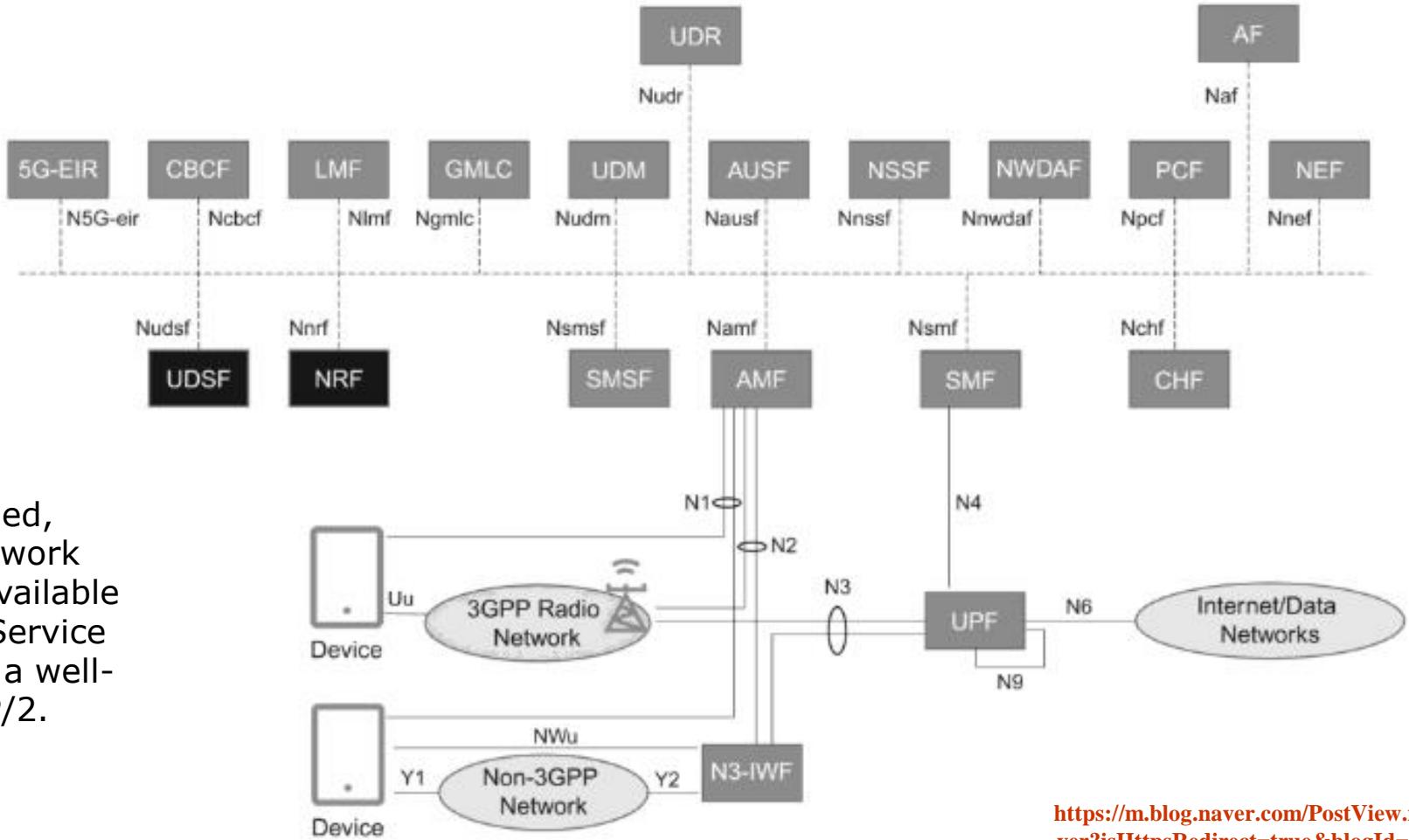


https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=so ng_sec&logNo=222025295180

The 5G System architecture

Service based representation where network functions (e.g. AMF) within the control plane enables other authorized network functions to access their services

Network Functions are self-contained, independent and reusable. Each Network Function service exposes and makes available its functionality (services) through a Service Based Interface (SBI), which employs a well-defined REST interface using HTTP/2.



https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=song_sec&logNo=222025295180

AMF, SMF and PCF

Access and Mobility Management Function (AMF)

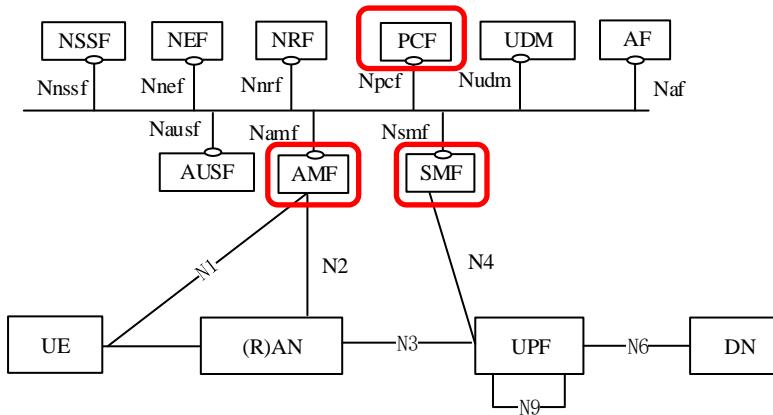
- Termination of NAS signalling
- NAS ciphering & integrity protection
- Registration management
- Connection management
- Mobility management
- Access authentication and authorization
- Security context management

Session Management Function (SMF)

- Session management (establishment, modification, release)
- UE IP address allocation & management
- UPF selection and configuration for QoS and traffic steering
- DHCP functions
- Lawful intercept functions
- Charging data collection and support of charging interfaces

Policy Control Function (PCF)

- Supports unified policy framework to govern network behaviour
- Provides policy rules to Control Plane function(s) to enforce them
- Accesses subscription information relevant for policy decisions in a Unified Data Repository (UDR)



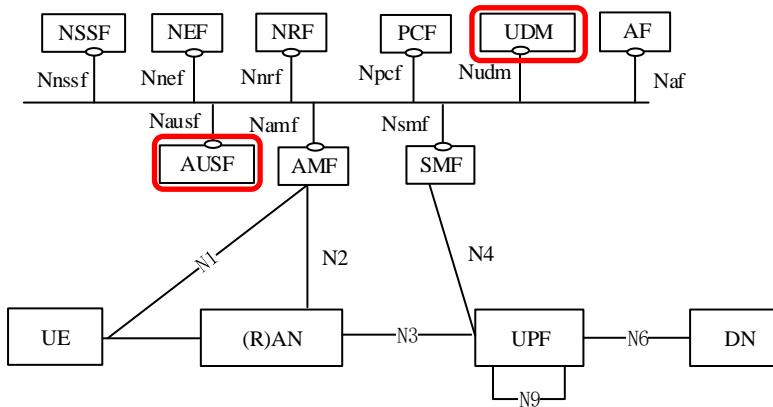
AUSF and UDM

Authentication Server Function (AUSF)

- Acts as an authentication server for 3GPP access and untrusted non-3GPP access

Unified Data Management (UDM)

- Generation of 3GPP Authentication and Key Agreement (AKA) credentials
 - User Identification handling
 - Access authorization based on subscription data
 - Lawful Intercept functionality
 - Subscription management



NEF, NRF and NSSF

Network Slice Selection Function (NSSF)

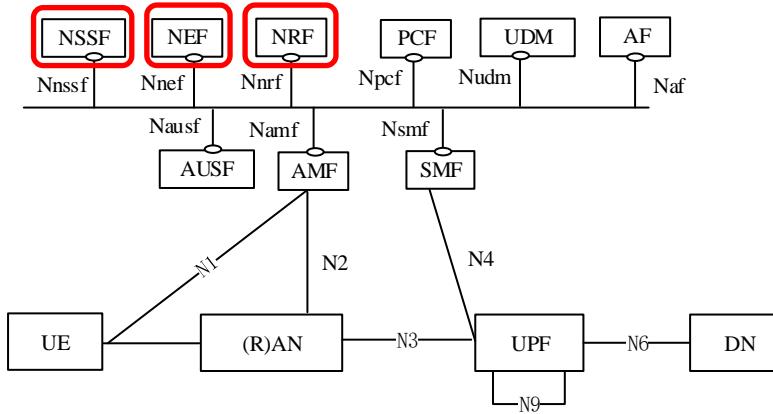
- Selecting of the Network Slice instances serving the UE
- Determining the Allowed NSSAI (*Network Slice Selection Assistance Information*)
- Determining the AMF set to be used to serve the UE

Network Exposure function (NEF)

- Exposure of capabilities and events
- Secure provision of information from external application to 3GPP network
- Translation of internal/external information

NF Repository function (NRF)

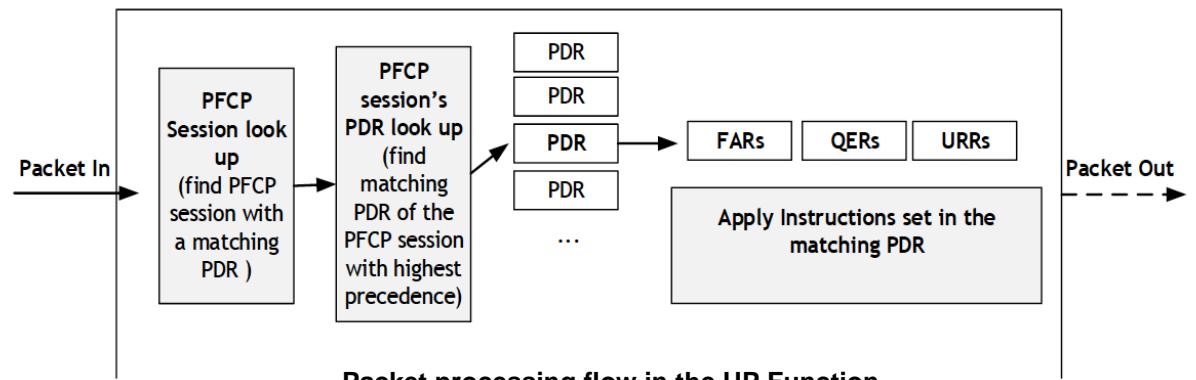
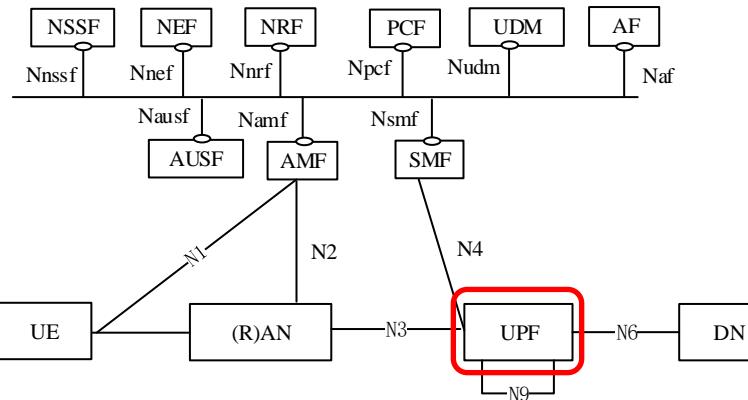
- Supports service discovery function
- Maintains the NF profile of available NF instances and their supported services



UPF

User Plane Function (UPF)

- Packet routing & forwarding
- Anchor point for Intra-/Inter-RAT mobility
- External PDU session point of interconnect to Data Network
- Packet inspection and User plane part of Policy rule enforcement
- Lawful intercept (UP collection)
- Traffic usage reporting
- Uplink classifier (ULCL) to support routing traffic flows to a data network
- QoS handling for user plane, e.g. packet filtering, gating, UL/DL rate enforcement
- Transport level packet marking in the uplink and downlink
- Downlink packet buffering and downlink data notification triggering



Sent from SMF to UPF in PFCP

- Packet Detection Rule (PDR):** This rule instructs the UPF how to detect incoming user data traffic (PDUs) and how to classify the traffic. The PDR contains Packet Detection Information (e.g., IP filters) used in the traffic detection and classification. There are separate PDRs for uplink and downlink.
- QoS Enforcement Rule (QER):** This rule contains information on how to enforce QoS, e.g., bit rate parameters.
- Usage Reporting Rule (URR):** This rule contains information on how the UPF shall measure (e.g., count) packets and bytes and report the usage to the SMF. The URR also contains information on events that shall be reported to SMF.
- Forwarding Action Rule (FAR):** This rule contains information for how a packet (PDU) shall be forwarded by the UPF, e.g., towards the Data Network in uplink or towards RAN in downlink.

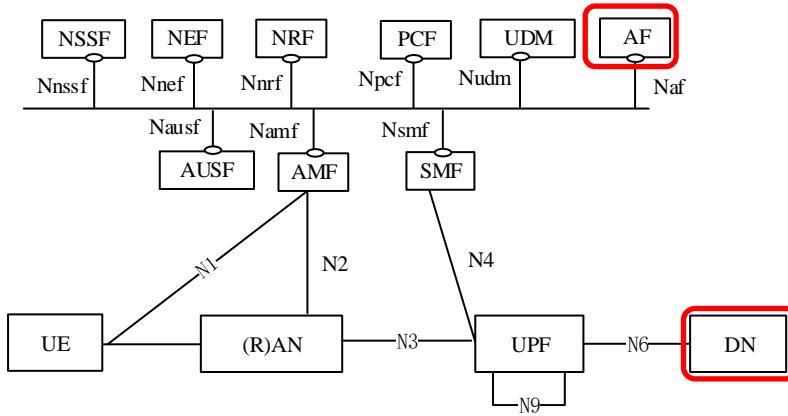
AF and DN

Application Function (AF)

- Application influence on traffic routing
- Accessing Network Exposure Function
- Interacting with the Policy framework for policy control

Data Network (DN)

- Operator services
- Internet access
- 3rd party services
- **May be a Local Area Data Network (LADN):**
 - a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific **Data Network Name (DNN)**, and whose availability is provided to the UE.



Data storage

Unstructured Data Storage Function (UDSF) Unified Data Repository (UDR)

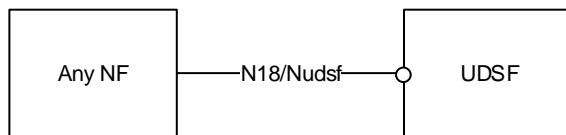


Figure 4.2.5-1: Data storage architecture for unstructured data from any NF (3GPP TS 23.501)

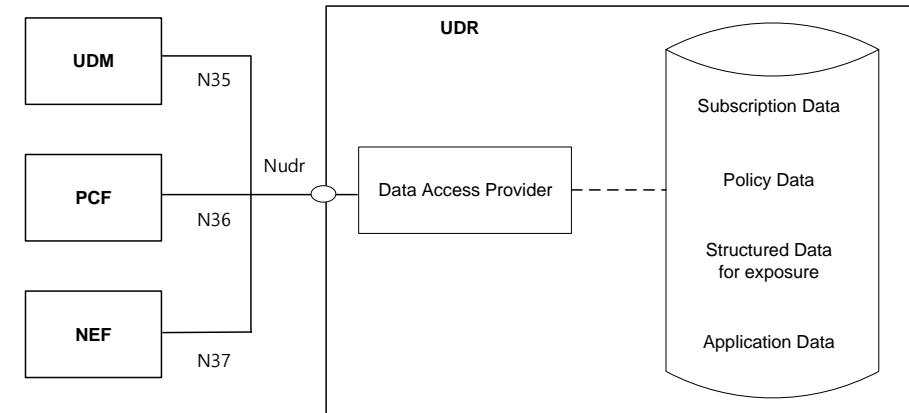
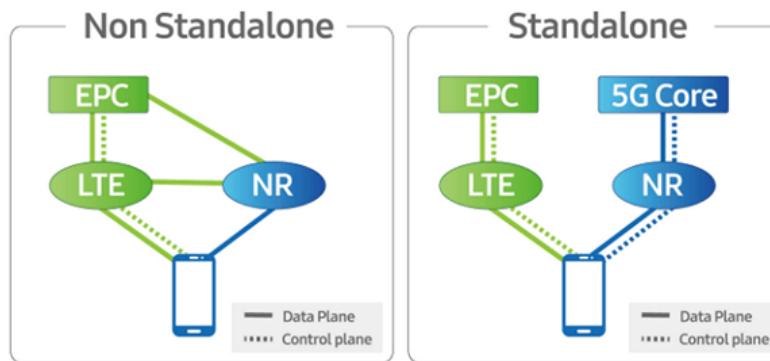


Figure 4.2.5-2: Data storage architecture (3GPP TS 23.501)

5G Non-stand Alone (NSA)

Non Stand Alone (NSA) architecture

- Uses 4G as an anchor for radio access
- The 4G Core controls the sessions
- It will basically bring us more speed, less latency and densification

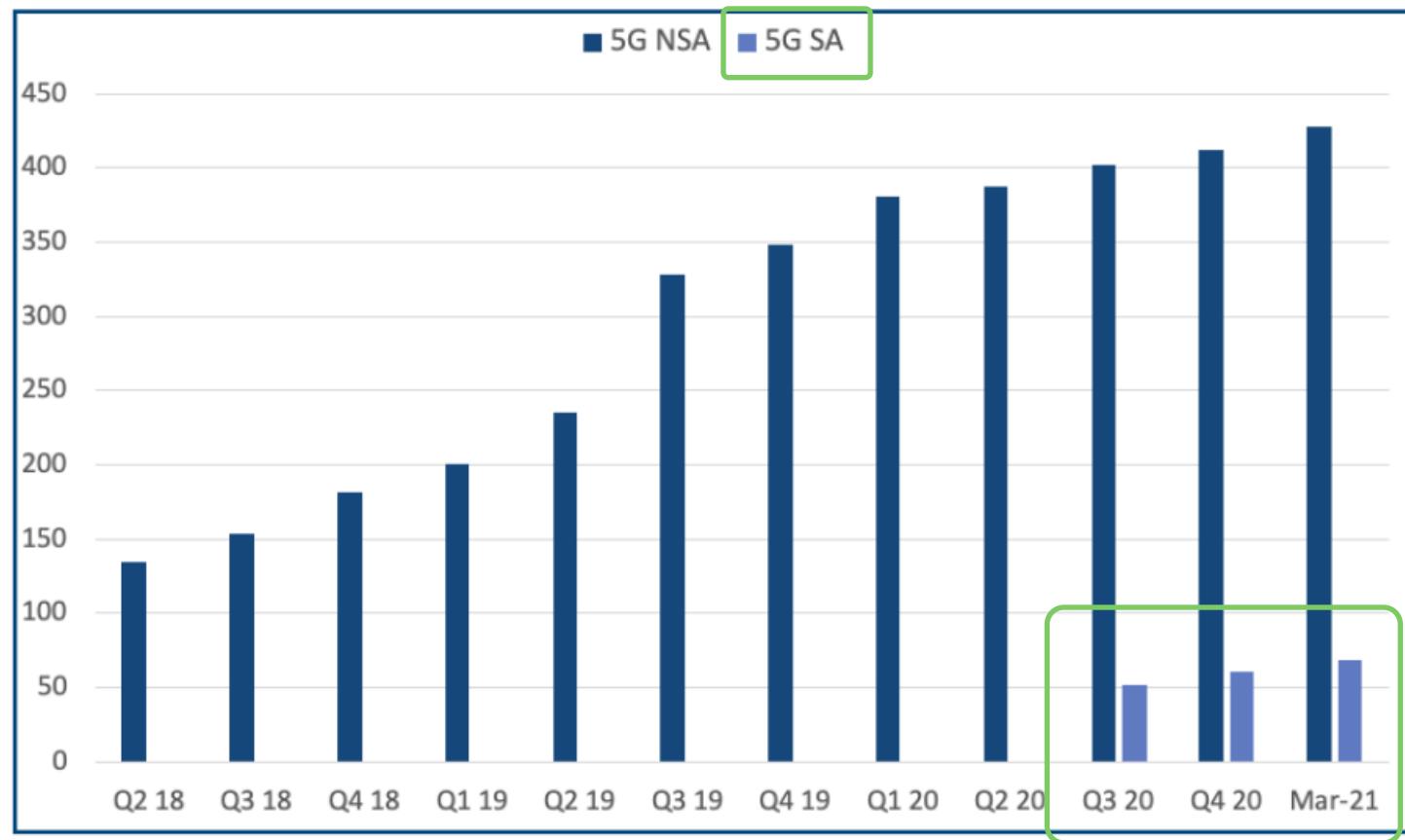


Stand Alone (SA) architecture (> 2023)

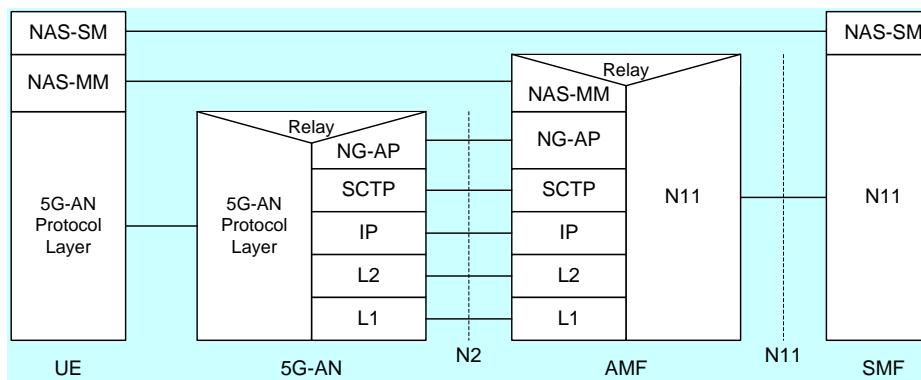
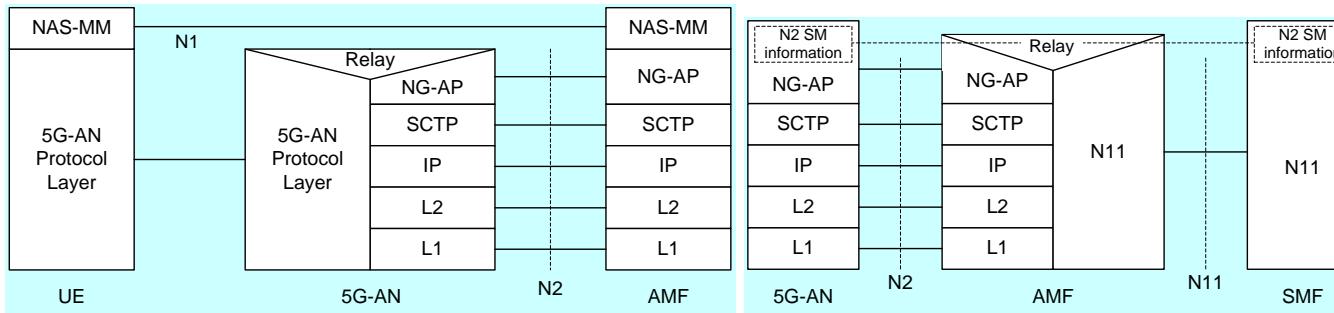
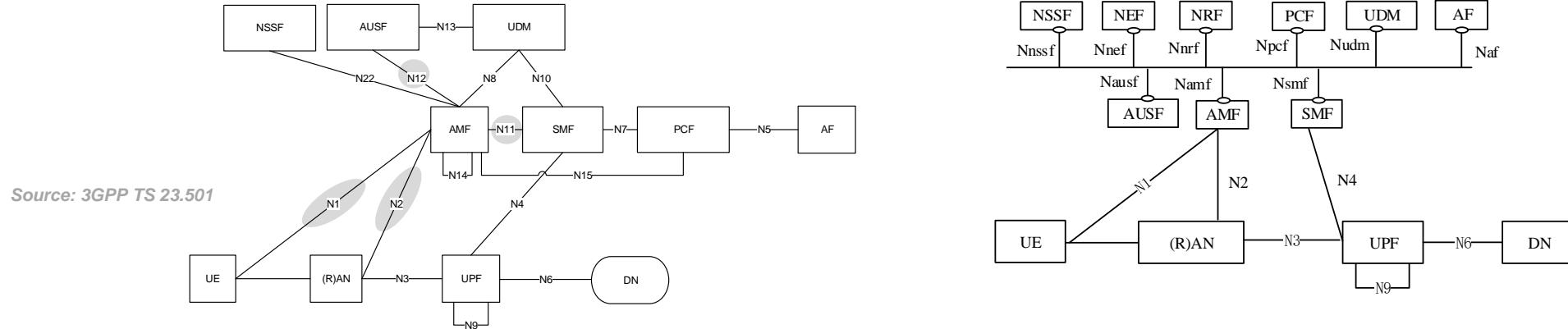
- Can work without 4G
- Uses a dedicated core that can be convergent
- Allows new services that use network slicing and edge computing

5G networks deployment

Figure 1: Number of operators investing in 5G standalone for public networks versus number investing in 5G non-standalone.

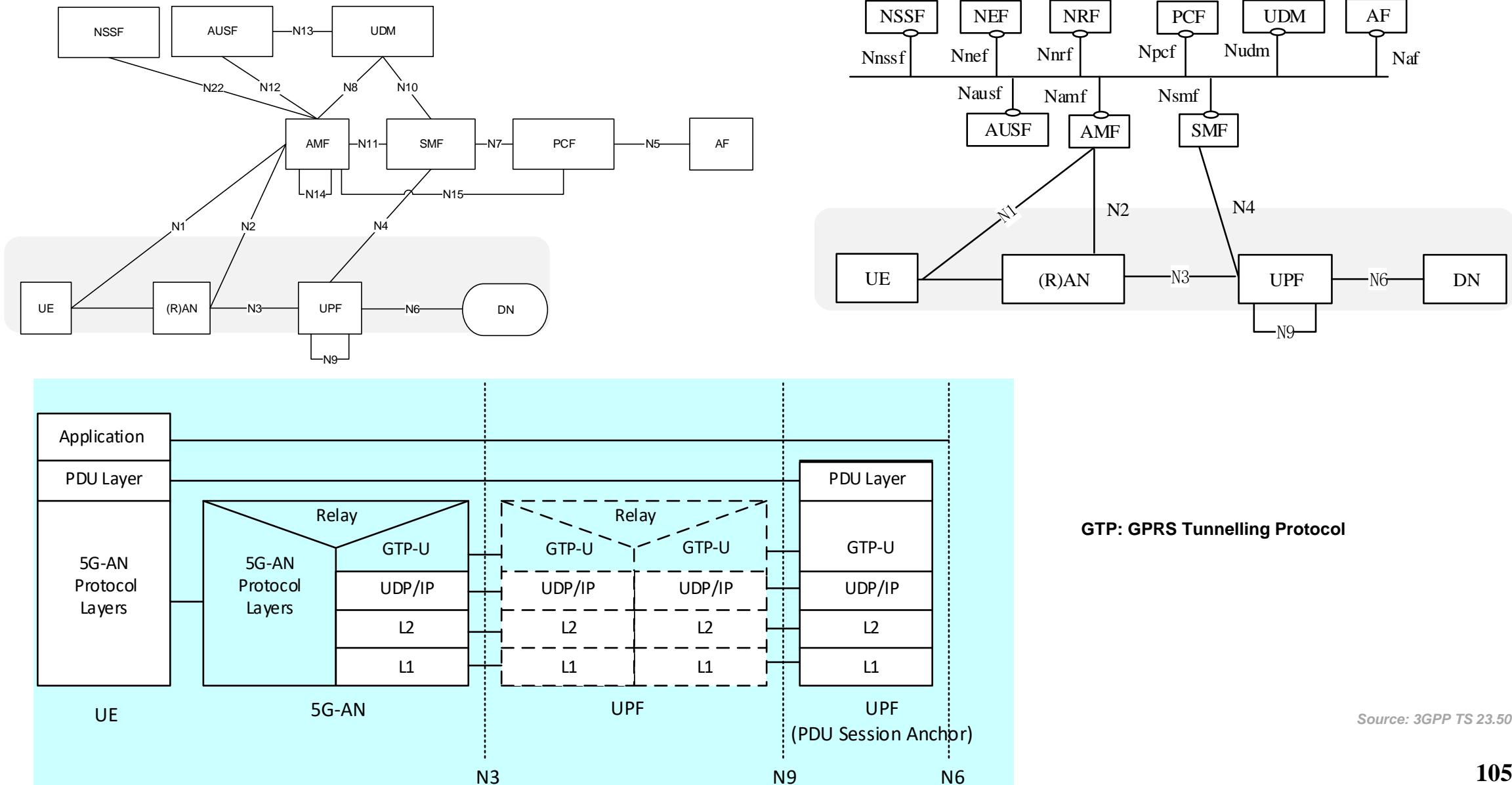


Protocol stacks – control plane



SCTP: Stream Control Transmission Protocol
PFCP: Packet Forwarding Control Protocol
NG-AP: NG Application Protocol
NAS-MM: NAS Mobility Management
NAS-SM: NAS Session Management
NAS: Non-Access-Stratum

Protocol stacks – user plane



Source: 3GPP TS 23.501

5G Procedures

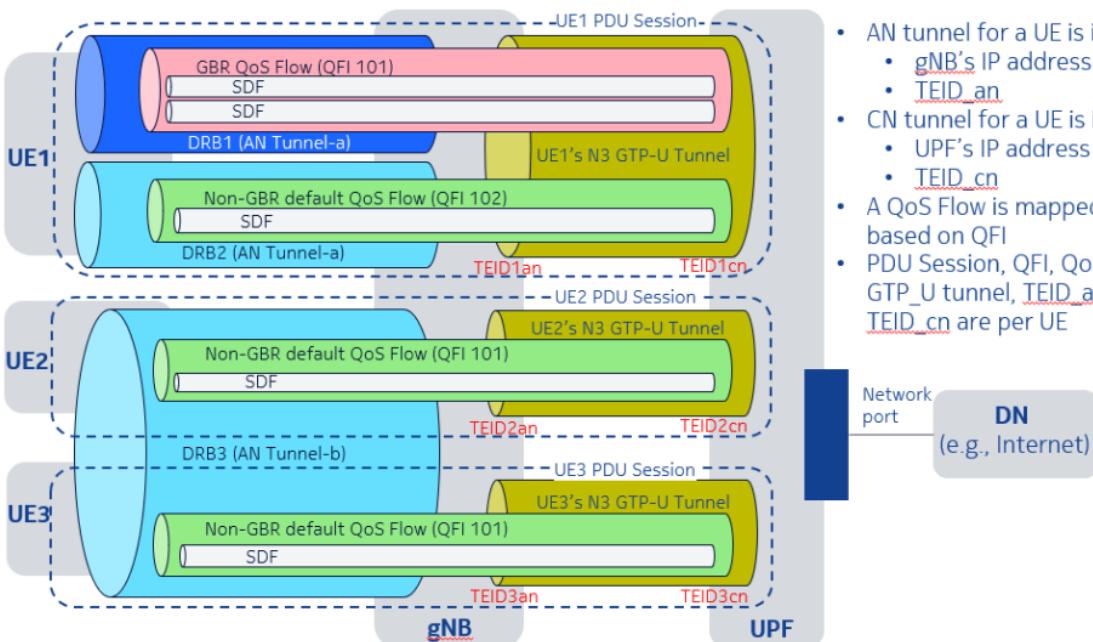
3GPP, TS 23.502, “Procedures for the 5G System (5GS)”

4 System procedures

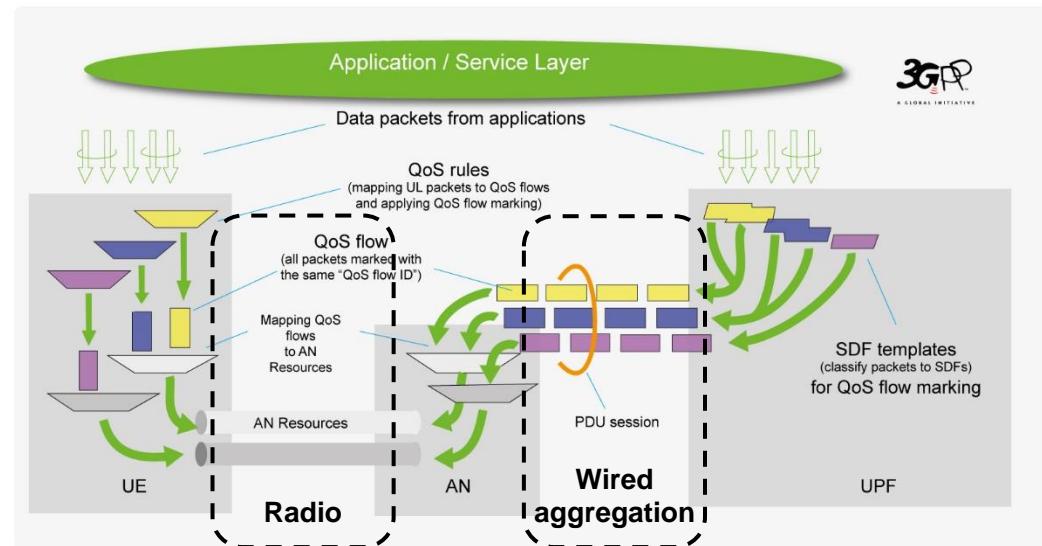
- ▷ 4.1 General
- ▷ 4.2 Connection, Registration and Mobility Management procedures
- ▷ 4.3 Session Management procedures
- ▷ 4.4 SMF and UPF interactions
- ▷ 4.5 User Profile management procedures
- ▷ 4.6 Security procedures
- ▷ 4.7 ME Identity check procedure
- ▷ 4.8 RAN-CN interactions
- ▷ 4.9 Handover procedures
 - 4.10 NG-RAN Location reporting procedures
 - ▷ 4.11 System interworking procedures with EPC
 - ▷ 4.12 Procedures for Untrusted non-3GPP access
 - ▷ 4.12a Procedures for Trusted non-3GPP access
 - ▷ 4.12b Procedures for devices that do not support 5GC NAS over WLAN access
 - ▷ 4.13 Specific services
 - ▷ 4.14 Support for Dual Connectivity
 - ▷ 4.15 Network Exposure
 - ▷ 4.16 Procedures and flows for Policy Framework
 - ▷ 4.17 Network Function Service Framework Procedure
 - ▷ 4.18 Procedures for Management of PFDs
 - ▷ 4.19 Network Data Analytics
 - ▷ 4.20 UE Parameters Update via UDM Control Plane Procedure
 - 4.21 Secondary RAT Usage Data Reporting Procedure
 - ▷ 4.22 ATSSS Procedures
 - ▷ 4.23 Support of deployments topologies with specific SMF Service Areas
 - ▷ 4.24 Procedures for UPF Anchored Data Transport in Control Plane CloT 5GS Optimisation
 - ▷ 4.25 Procedures for NEF based Non-IP Data Delivery
 - ▷ 4.26 Network Function/NF Service Context Transfer Procedures
 - ▷ 4.27 Procedures for Enhanced Coverage Restriction Control via NEF

- **Connection, Registration and Mobility Management procedures**
- **Session Management**
 - **PDU Session Establishment**
 - **PDU Session Modification**
 - **PDU Session Release**
 - **Session continuity, service continuity and UP path management**
- **Handover procedures**
- **Procedures for Trusted/Untrusted non-3GPP access**

QoS Model



- AN tunnel for a UE is identified by:
 - gNB's IP address
 - TEID_an
- CN tunnel for a UE is identified by:
 - UPF's IP address
 - TEID_cn
- A QoS Flow is mapped to a DRB based on QFI
- PDU Session, QFI, QoS Flow, N3 GTP_U tunnel, TEID_an and TEID_cn are per UE



The QoS profile of a QoS flow contains QoS parameters:

For each QoS flow:

- A 5G QoS Identifier (5QI)
- An Allocation and Retention Priority (ARP)

In case of a GBR QoS flow only:

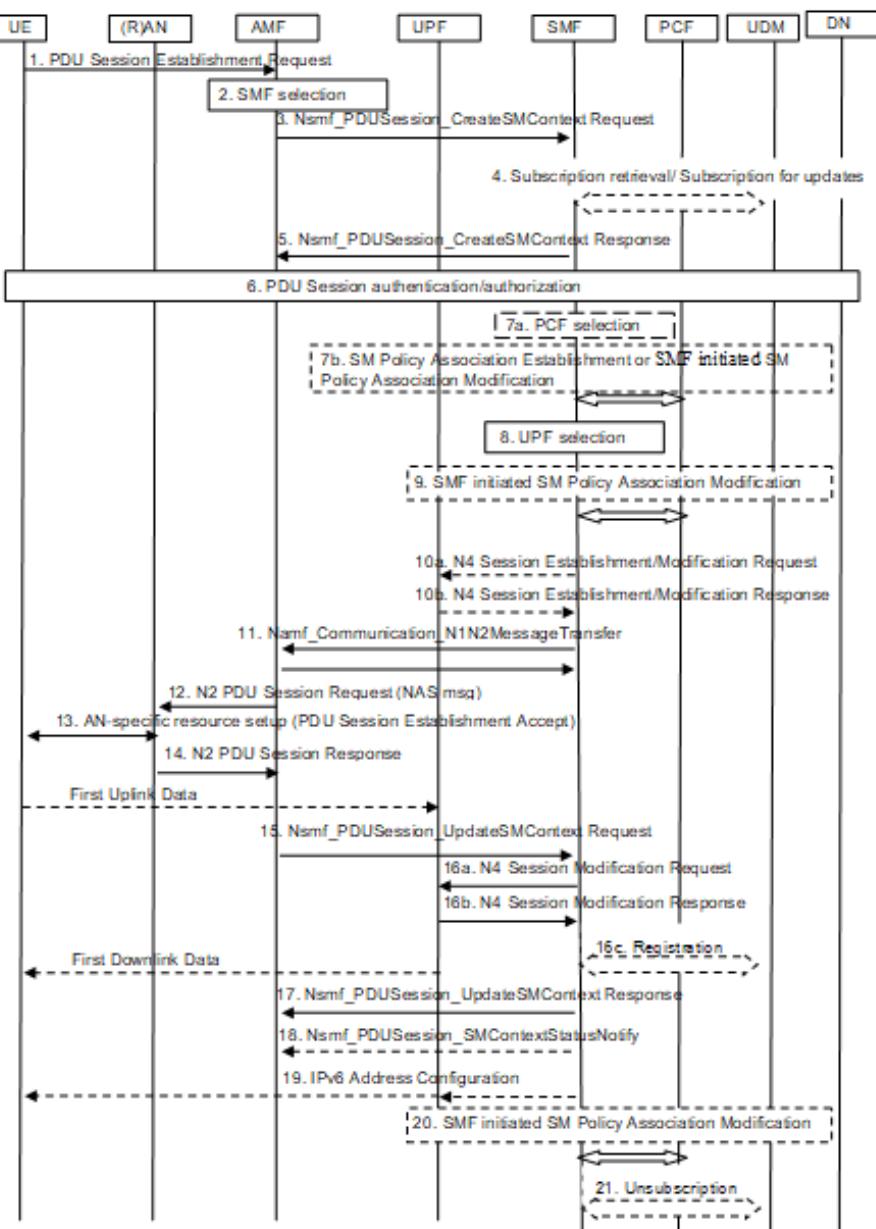
- Guaranteed Flow Bit Rate (GFR) for both uplink and downlink
- Maximum Flow Bit Rate (MFR) for both uplink and downlink
- Maximum Packet Loss Rate for both uplink and downlink

In case of Non-GBR QoS only

- Reflective QoS Attribute (RQA): the RQA, when included, indicates that some (not necessarily all) traffic carried on this QoS flow is subject to reflective quality of service (RQoS) at NAS.

Standardized 5QI to QoS characteristics mapping

5QI Value	Resource Type	Priority Level	Packet Delay Budget	Packet Error Rate	Default Averaging Window	Example Services
1	GBR	20	100 ms	10^{-2}	TBD	Conversational Voice
2		40	150 ms	10^{-3}	TBD	Conversational Video (Live Streaming)
3		30	50 ms	10^{-3}	TBD	Real Time Gaming, V2X messages
4		50	300 ms	10^{-6}	TBD	Non-Conversational Video (Buffered Streaming)
65		7	75 ms	10^{-2}	TBD	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66		20	100 ms	10^{-2}	TBD	Non-Mission-Critical user plane Push To Talk voice
75		25	50 ms	10^{-2}	TBD	V2X messages
5		10	100 ms	10^{-6}	N/A	IMS Signalling
6		60	300 ms	10^{-6}	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		70	100 ms	10^{-3}	N/A	Voice, Video (Live Streaming) Interactive Gaming
8	Non-GBR	80	300 ms	10^{-6}	N/A	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		90	60 ms	10^{-6}	N/A	Mission Critical delay sensitive signalling (e.g., MC-PTT signalling)
69		5	60 ms	10^{-6}	N/A	Mission Critical Data (e.g., example services are the same as QCI 6/8/9)
70		55	200 ms	10^{-6}	N/A	V2X messages
79		65	50 ms	10^{-2}	N/A	V2X messages



QoS protocols' flows

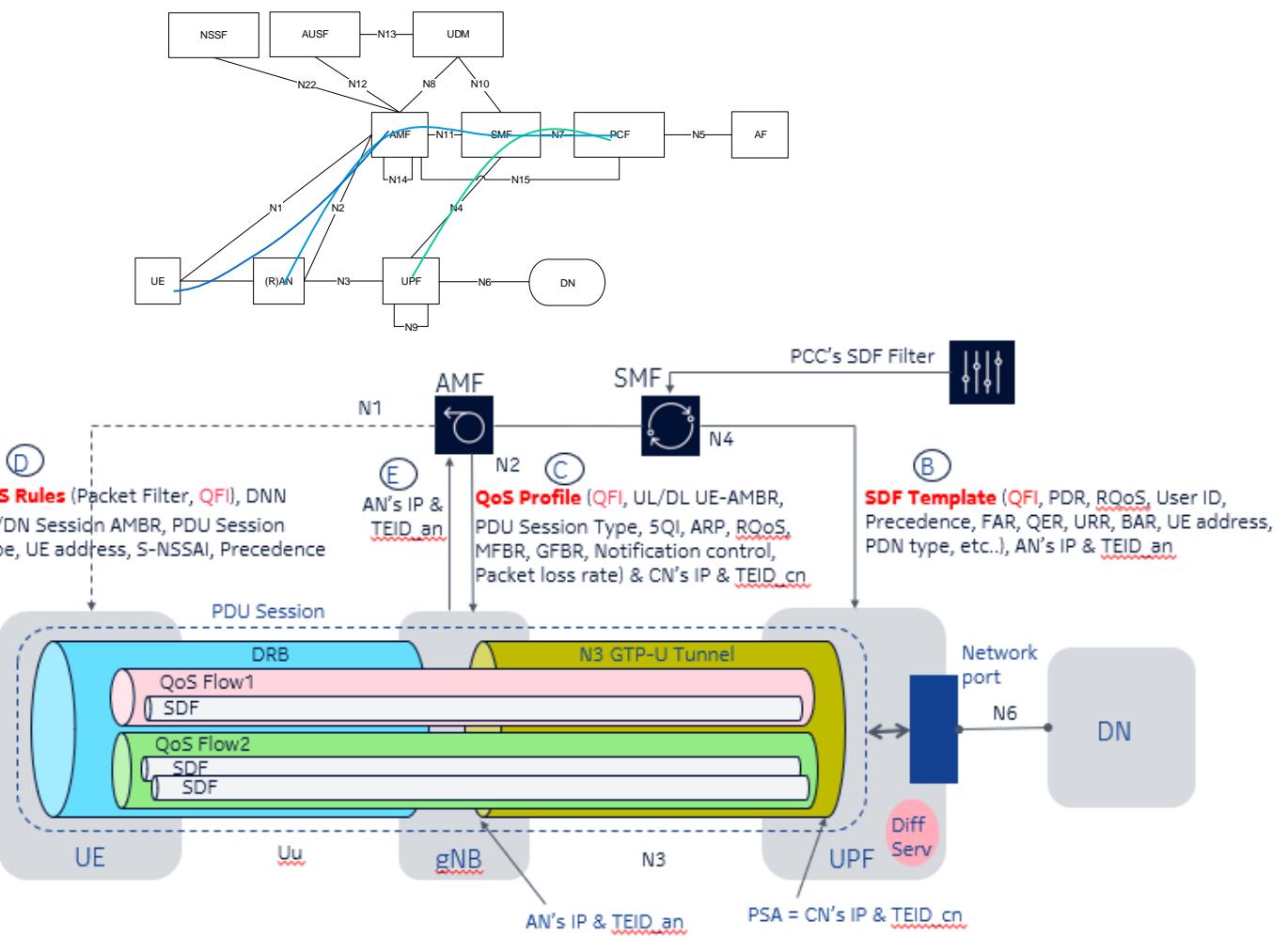
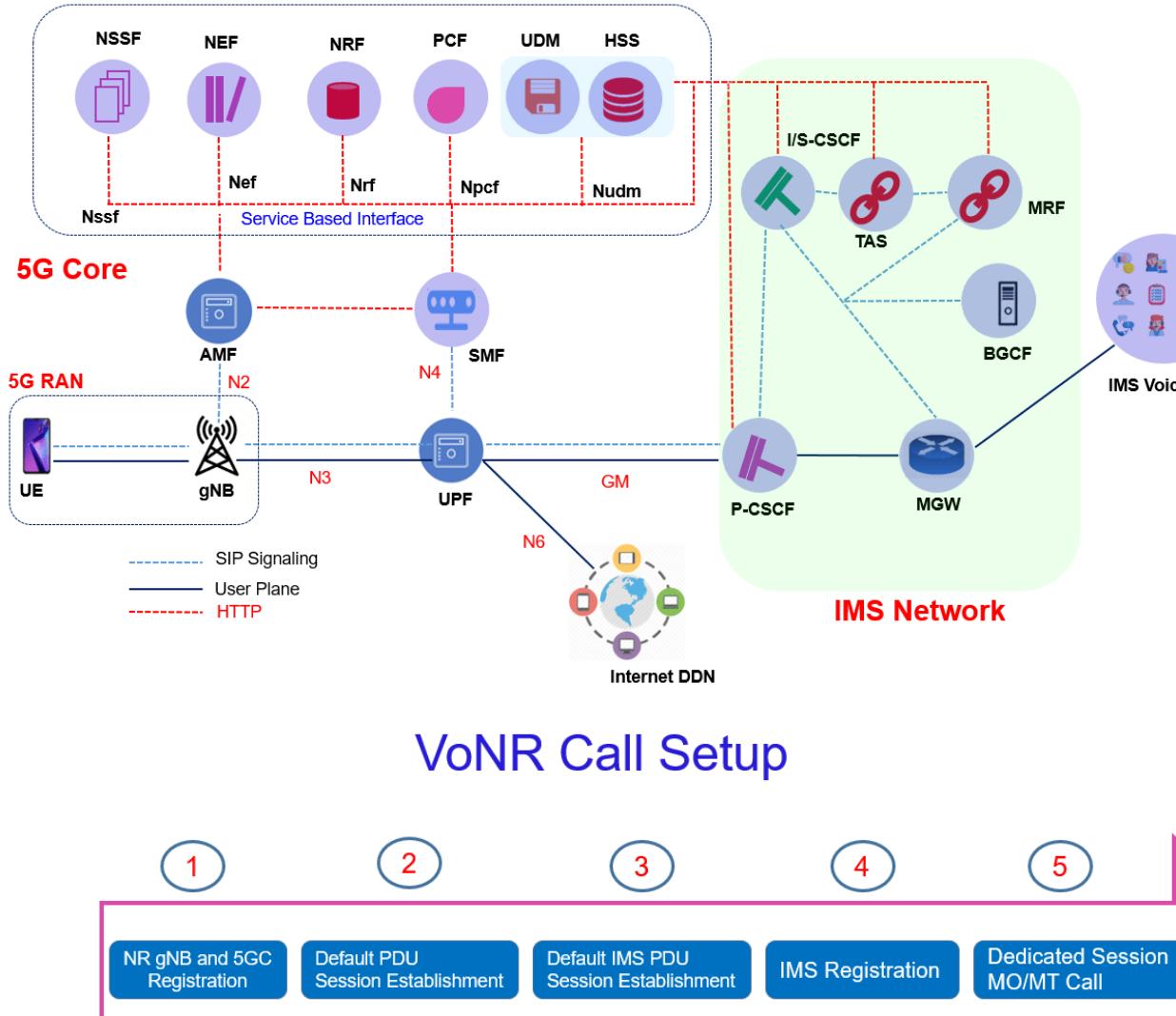
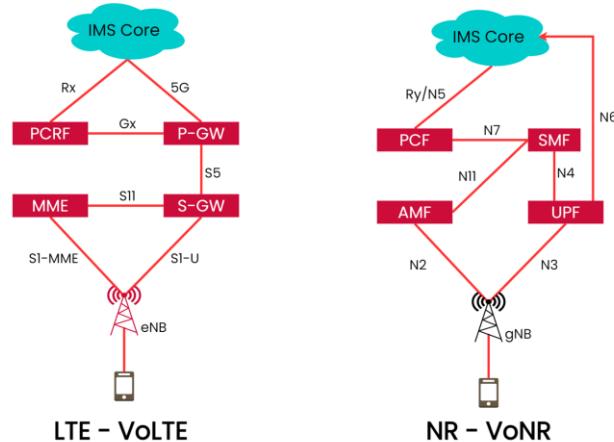


Figure 4.3.2.2.1-1: UE-requested PDU Session Establishment for non-roaming and roaming with local breakout

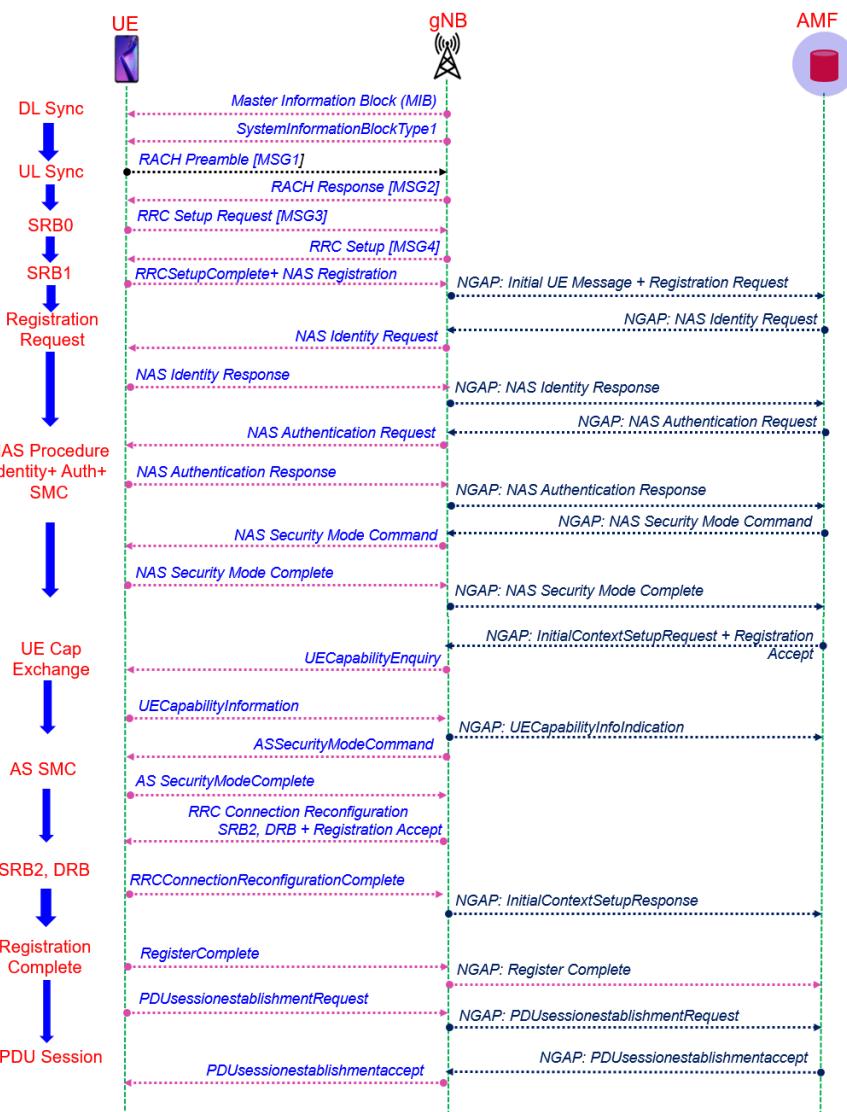
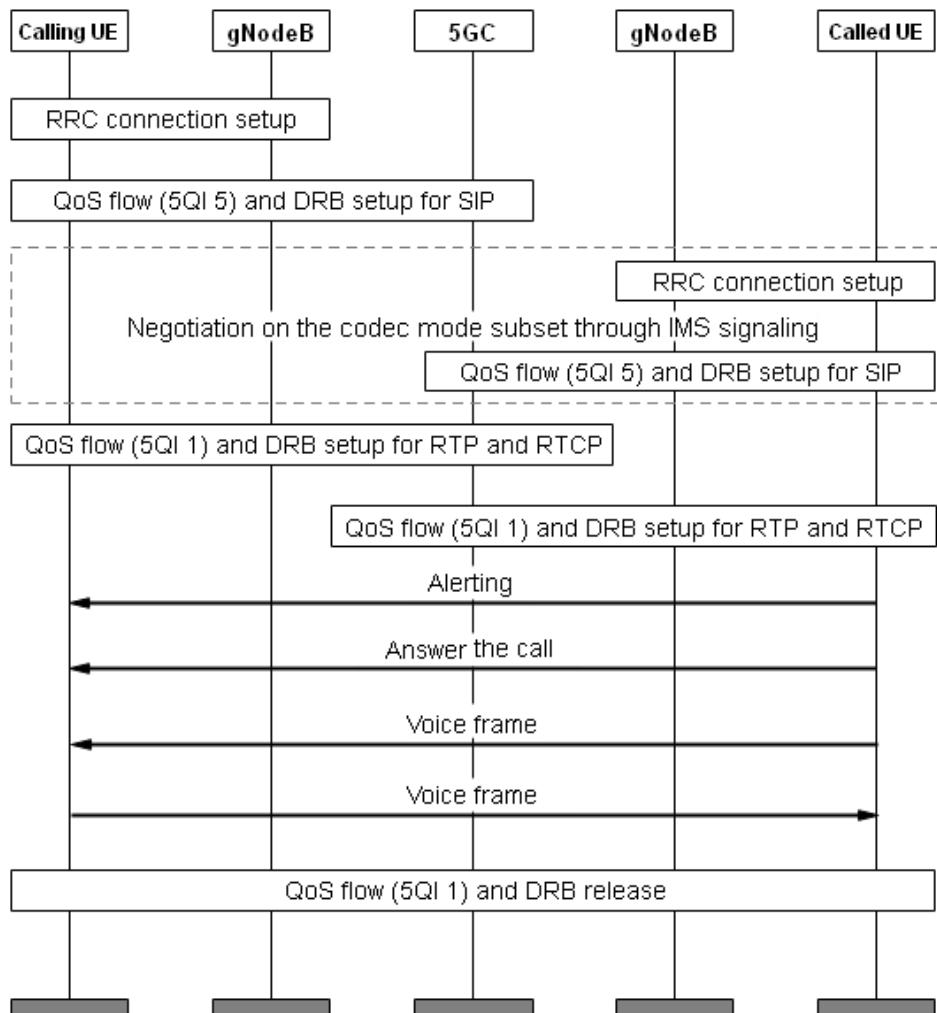
Example: VoNR



- Main componentes: 5G RAN, 5G Core, IMS
- Establishement of specific PDU sessions
- QoS



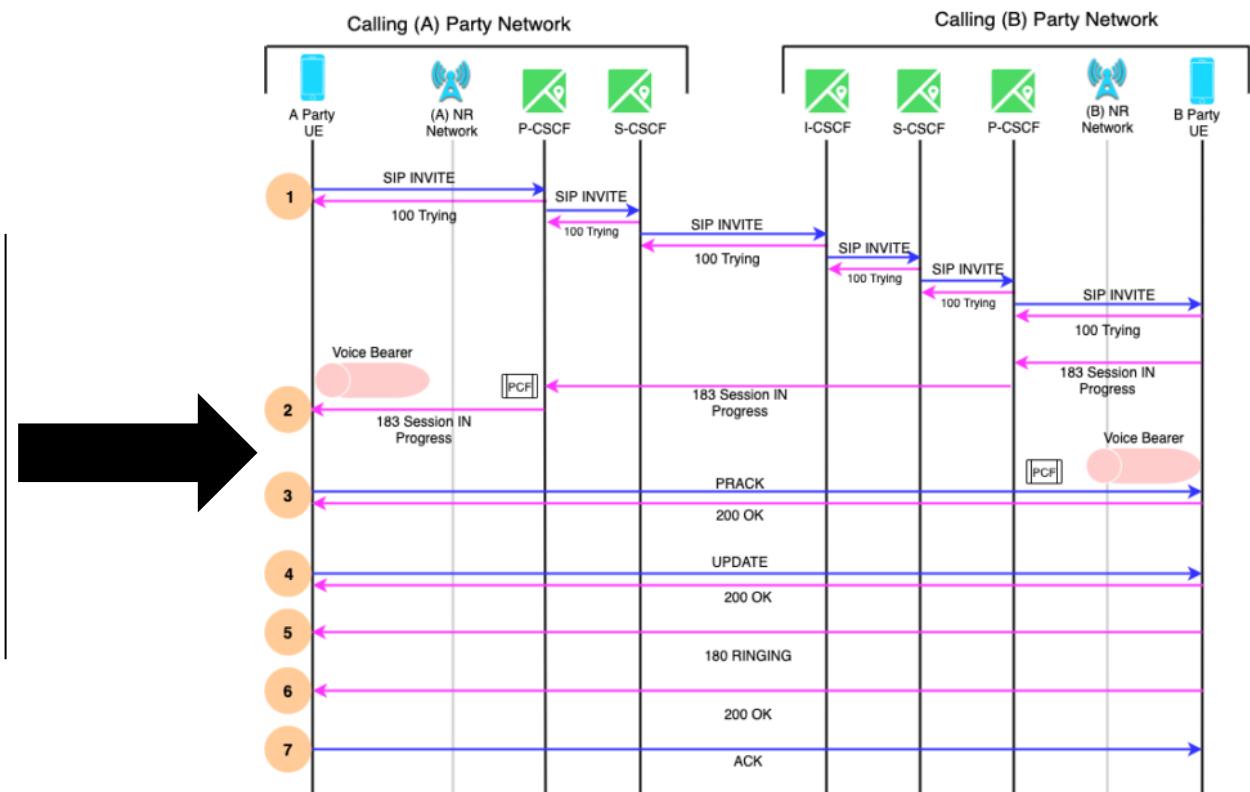
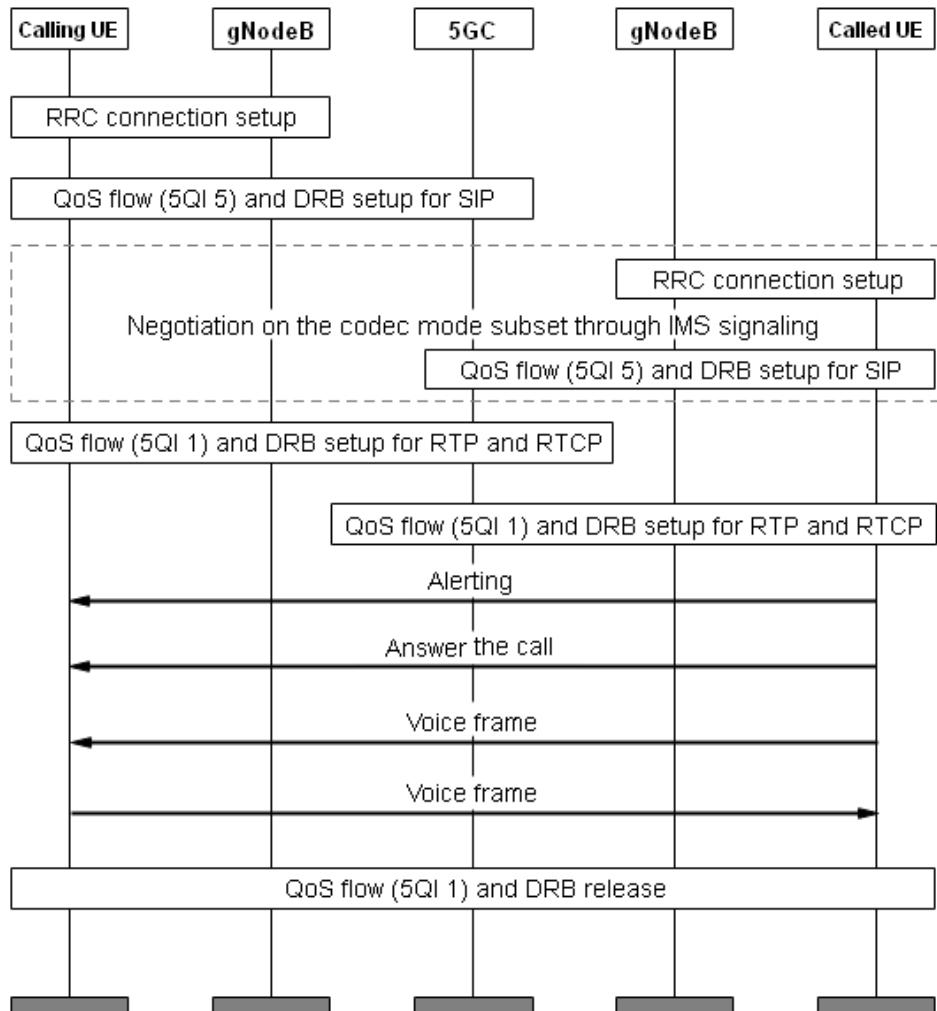
VoNR Call Flow



<https://www.5gworldpro.com/blog/2021/05/30/voice-over-nr-call-flow/>

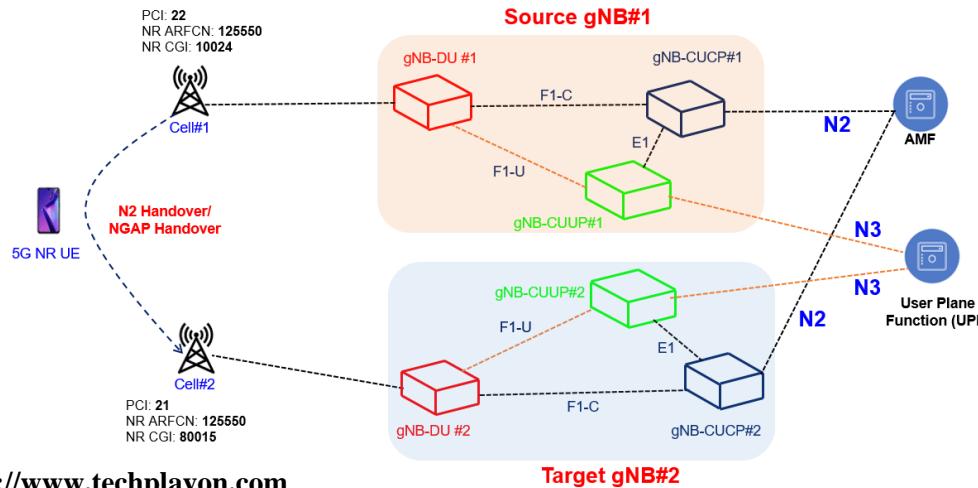
<https://www.techplayon.com/5g-nr-sa-registration-attach-call-flow/>

VoNR Call Flow



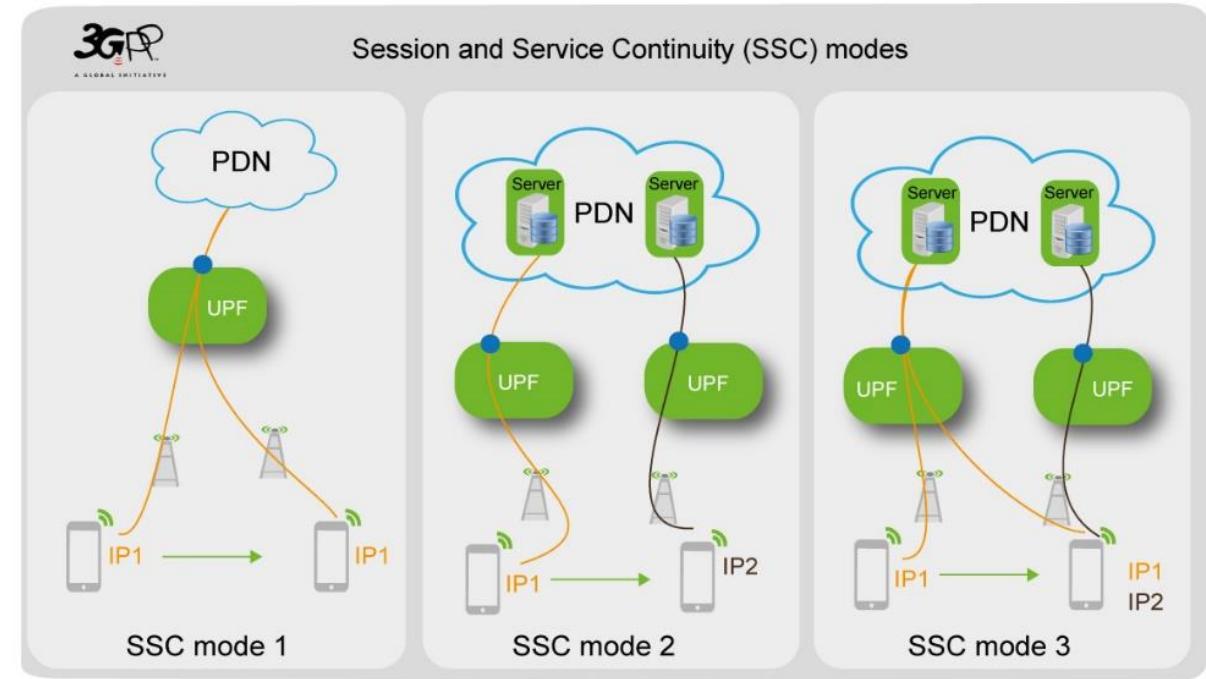
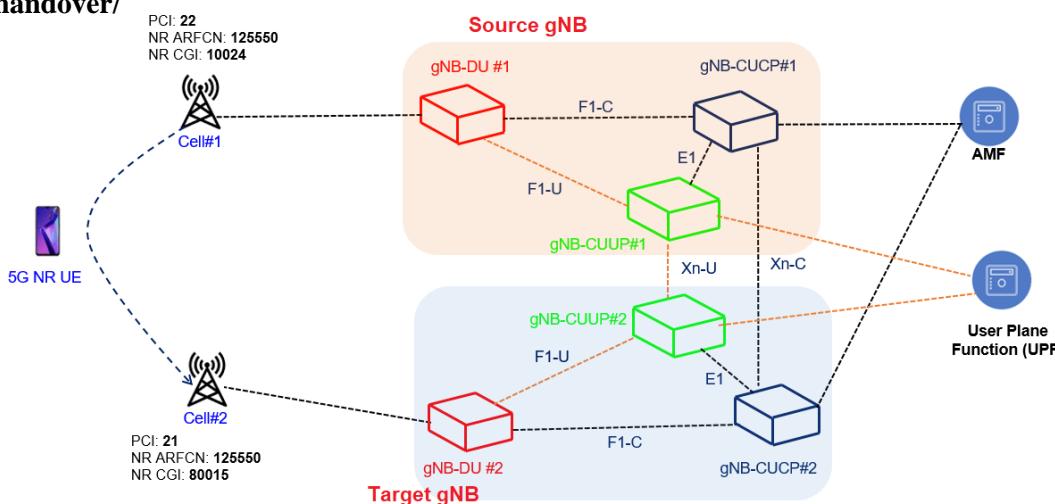
<https://www.5gworldpro.com/blog/2021/05/30/voice-over-nr-call-flow/>

Mobility in 5G



<https://www.techplayon.com/5g-sa-inter-gnb-handover-n2-or-ngap-handover/>

<https://www.techplayon.com/5g-sa-inter-gnb-hanodver-xn-handover/>

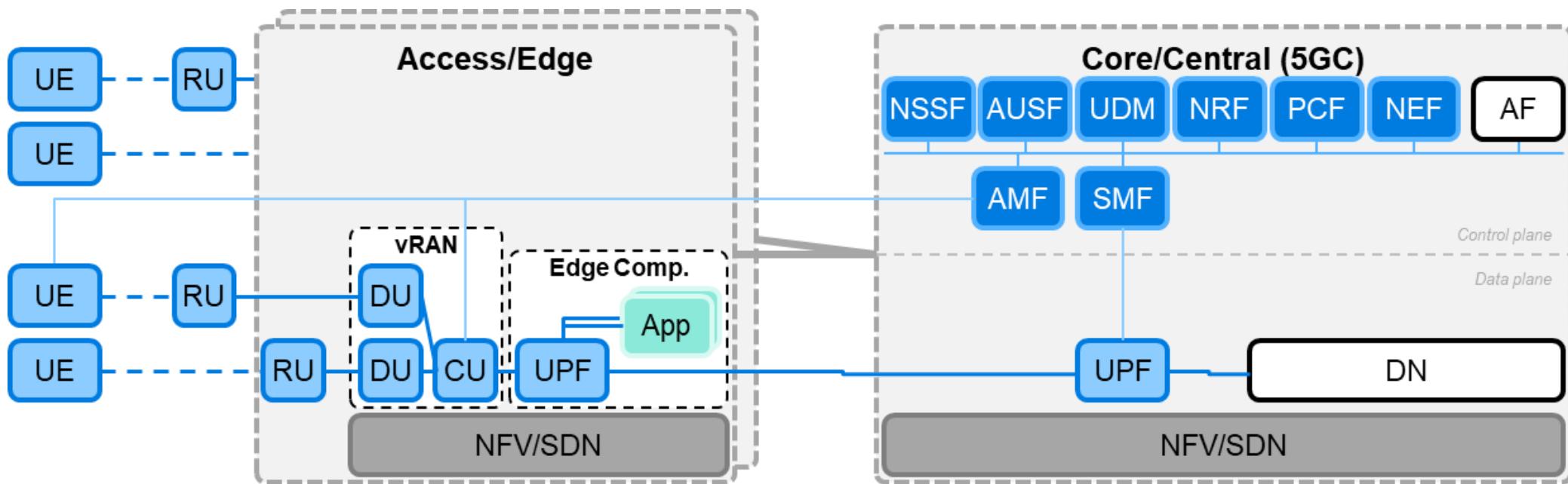


Mode 1: common mode in previous Releases, keeping anchor point during all the session duration

Modes 2 and 3: new modes to cope with edge computing Support; anchor point moves to the 'closest' UPF, following the EU (2: break-before-make; 3: make-before-brake)

Distributed cloud: Edge Computing and 5G

- Distributed, small data centres (NFV powered), placed close to the network edge
- Mandatory for 5G, to enable low latency services (Operator and 3rd-party Edge Applications)
- Allowing processing offloading from UEs
- Take benefit of NFV for lifecycle management (LCM) of VNF:
 - 5G RAN (CU/DU)
 - 5G user plane VNF (UPF)
 - Edge Applications
- 5G provides native support for (*Multi-access*) Edge Computing (MEC)



5G Slicing

Slicing enables the creation of distinct logical networks:

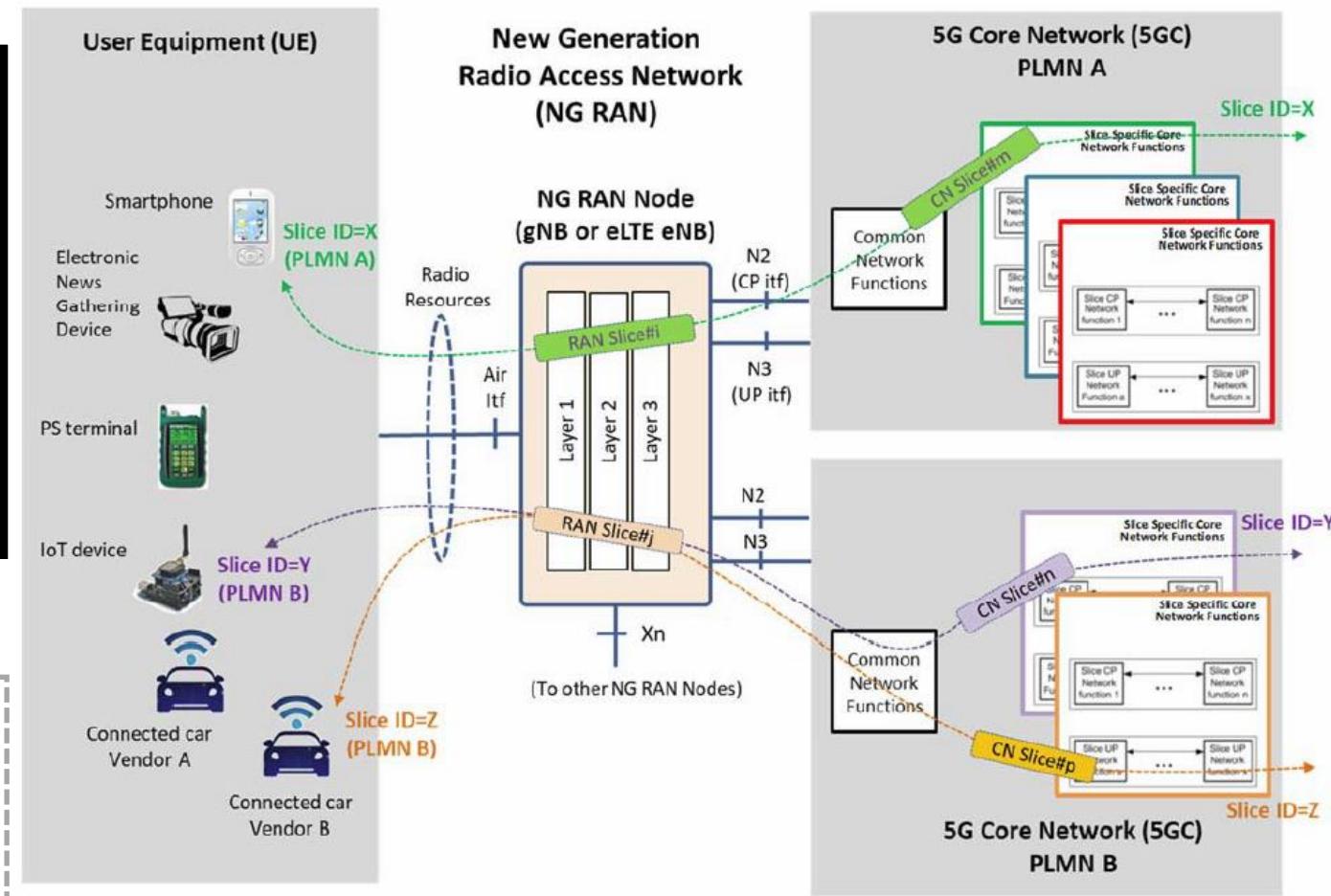
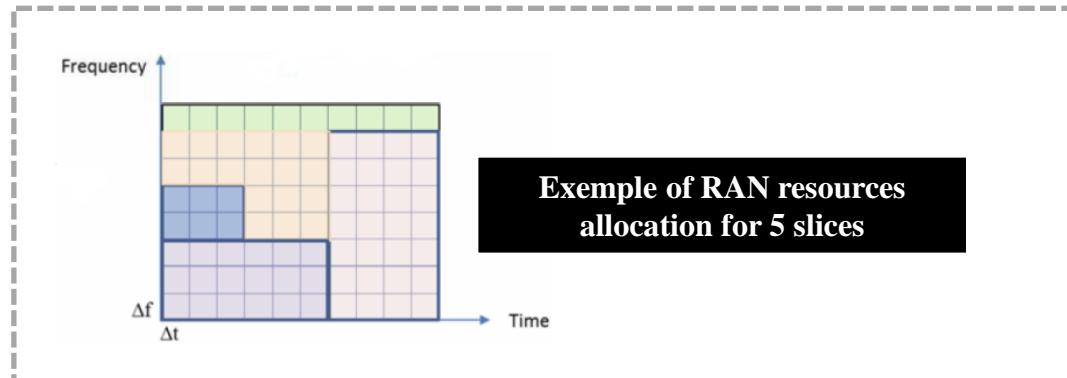
- Of the same type (different businesses)
- Providing differentiated behaviour (different services)

5G supports end-to-end slicing (radio and core)

- Resources isolation between services
- Customized functions and/or capacities, according to SLA

Each terminal (UE) may connect simultaneously to max 8 slices (no limit for the number of slices in the core)

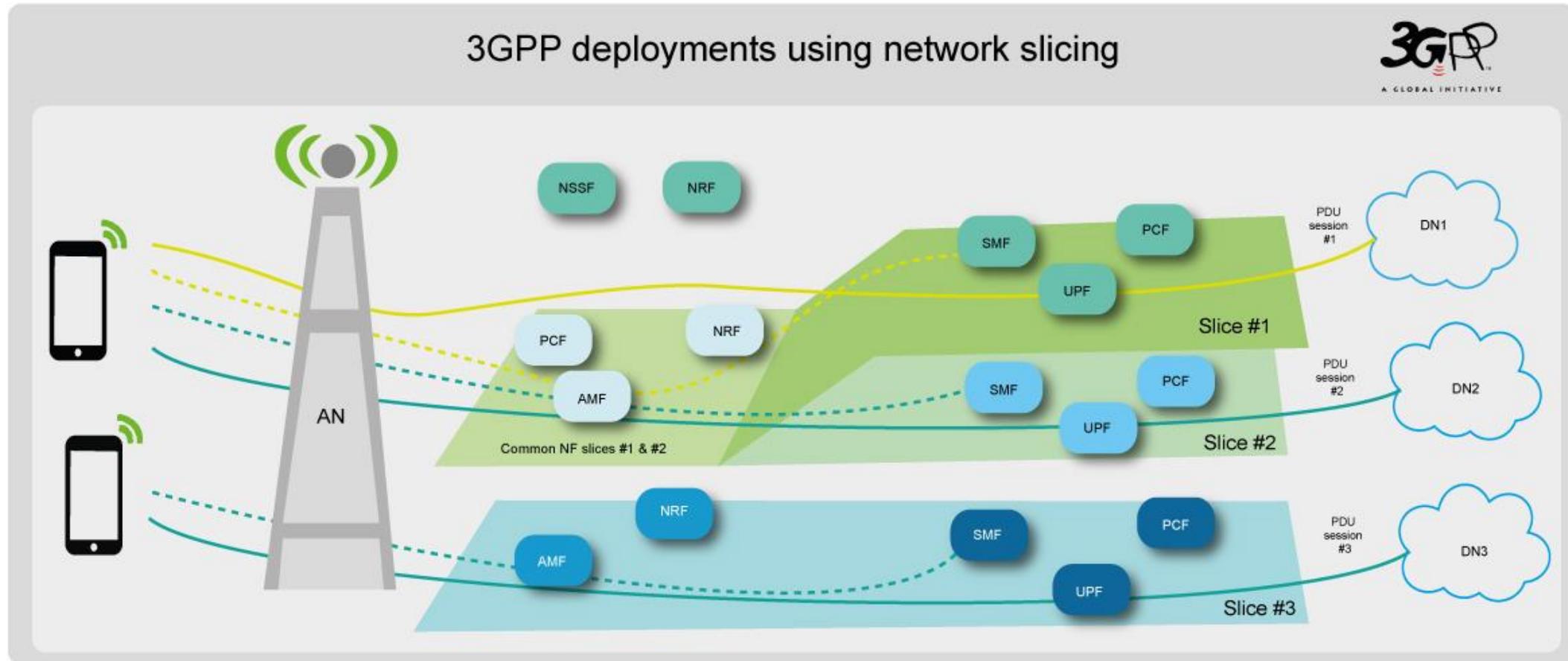
Takes benefit of NFV for easy slices creation and management (LCM)



5G Americas, NetWork Slicing for 5G networks & services, Nov/16
On 5G Radio Access Network Slicing: Radio Interface Protocol Features and Configuration, R. Ferrús

Network Slice definition (TR 23.799): complete logical network (providing Telecommunication Services and Network Capabilities) including AN and CN.

5G Slicing



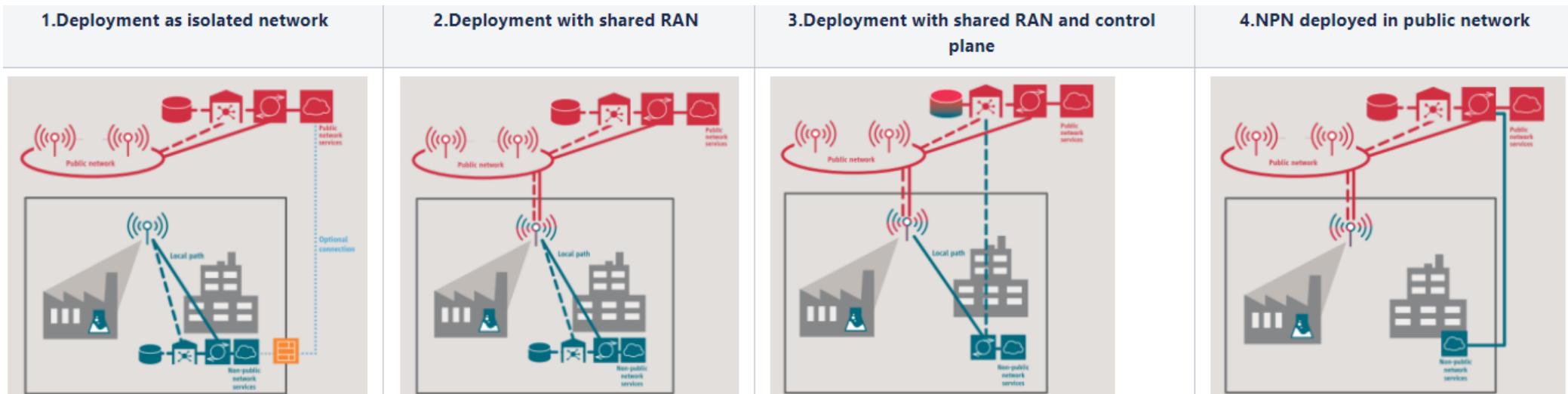
<https://www.3gpp.org/news-events/3gpp-news/sys-architecture>

Definition of a private 5G network

Non Public Network (NPN):

- “Intended for the sole use of a private entity such as an enterprise, may be deployed in a variety of configurations, utilizing both virtual and physical elements.
- Specifically, they may be deployed as completely standalone networks, they may be hosted by a public land mobile network (PLMN), or they may be offered as a slice of a PLMN”

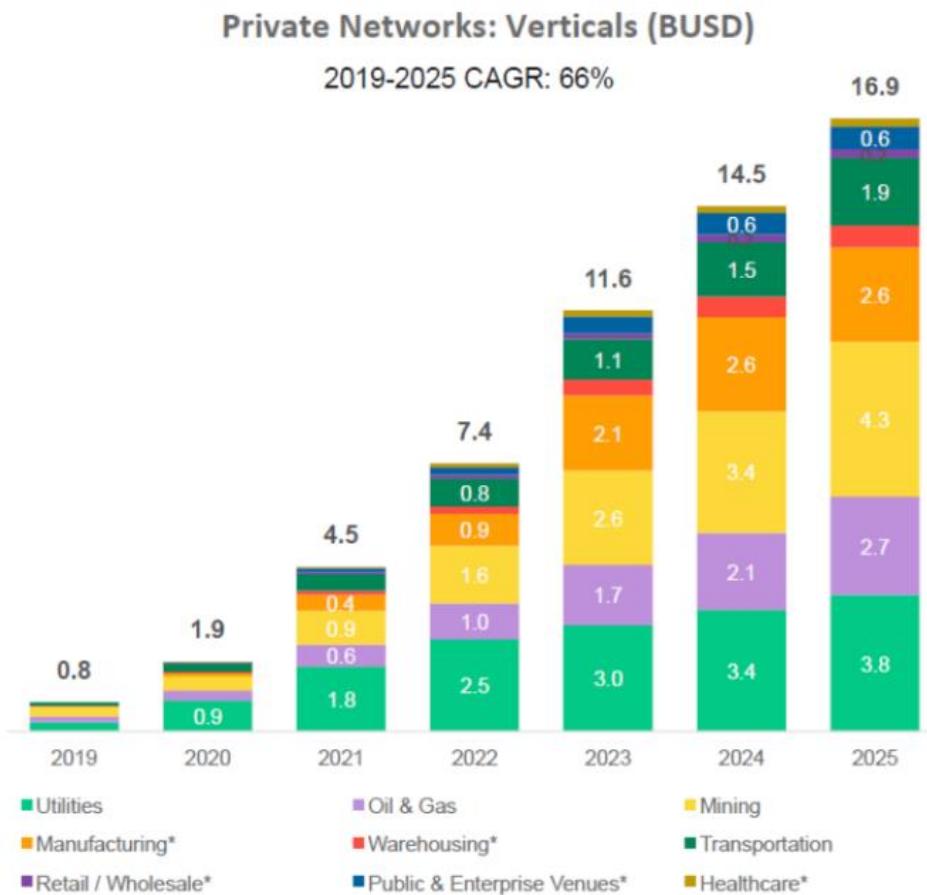
3GPP, TS 23.501



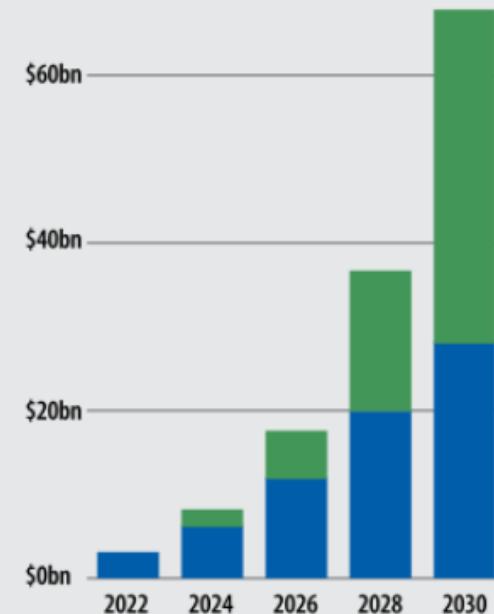
5G-ACIA

Private 5G network market growth

Target Addressable Market
By Industries - \$57.6B accumulative



Private LTE/5G deployments



Growth – the value-percentage of private 5G deployments will outrun private LTE deployments in 2029, according to ABI Research.

Private LTE (4G)
– market value

Private 5G –
market value

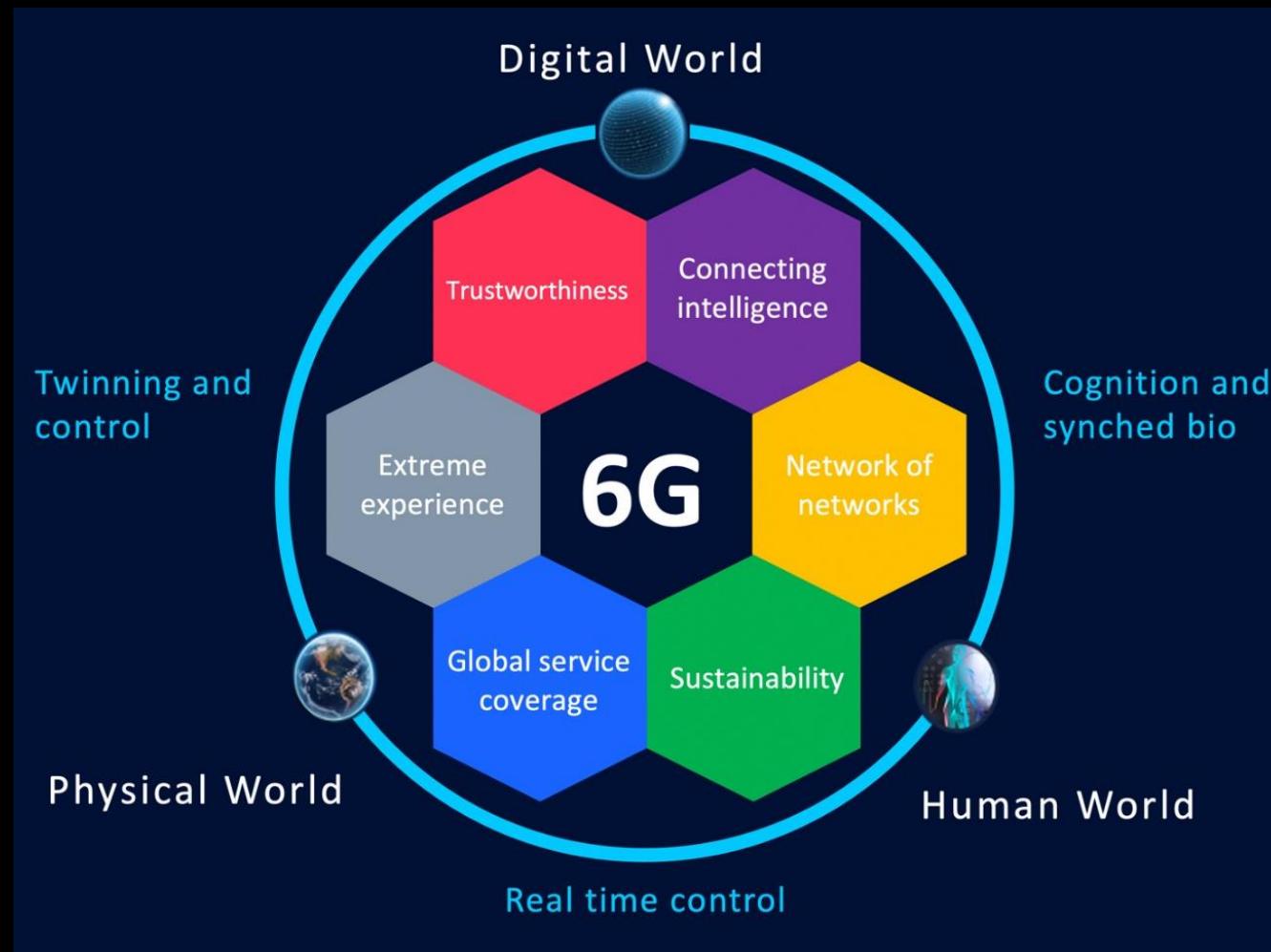
6G

The future ahead

“While 5G has enabled us to consume digital media anywhere, anytime, the technology of the future should enable us to embed ourselves in entirely virtual or digital worlds.

In the world of 2030, human intelligence will be augmented by being tightly coupled and seamlessly intertwined with the network and digital technologies.”

Hexa-X Consortium



- **Beyond 5G, towards 6G**

“The 6G network is likely to be a concept, a virtual one, and not a “real” network you can put a boundary around”, Roberto Saracco, EIT Digital

Perceived unlimited bandwidth with unperceived latency

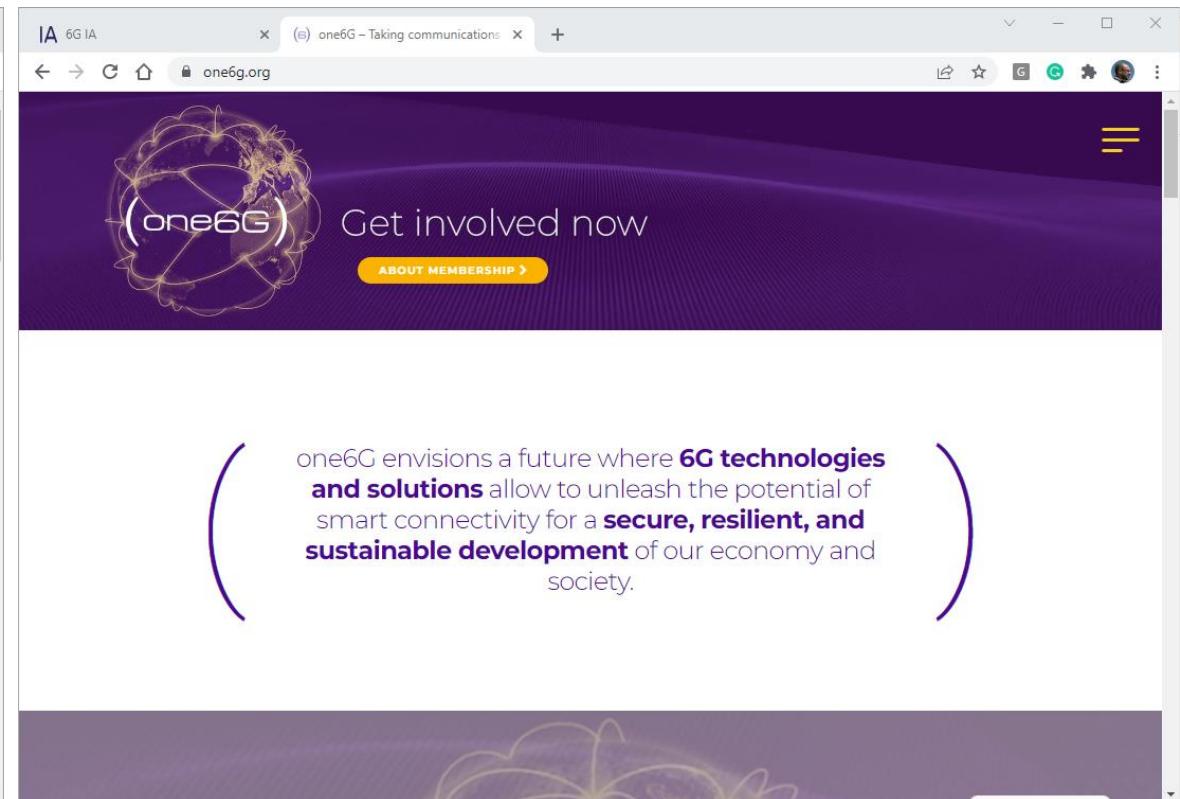
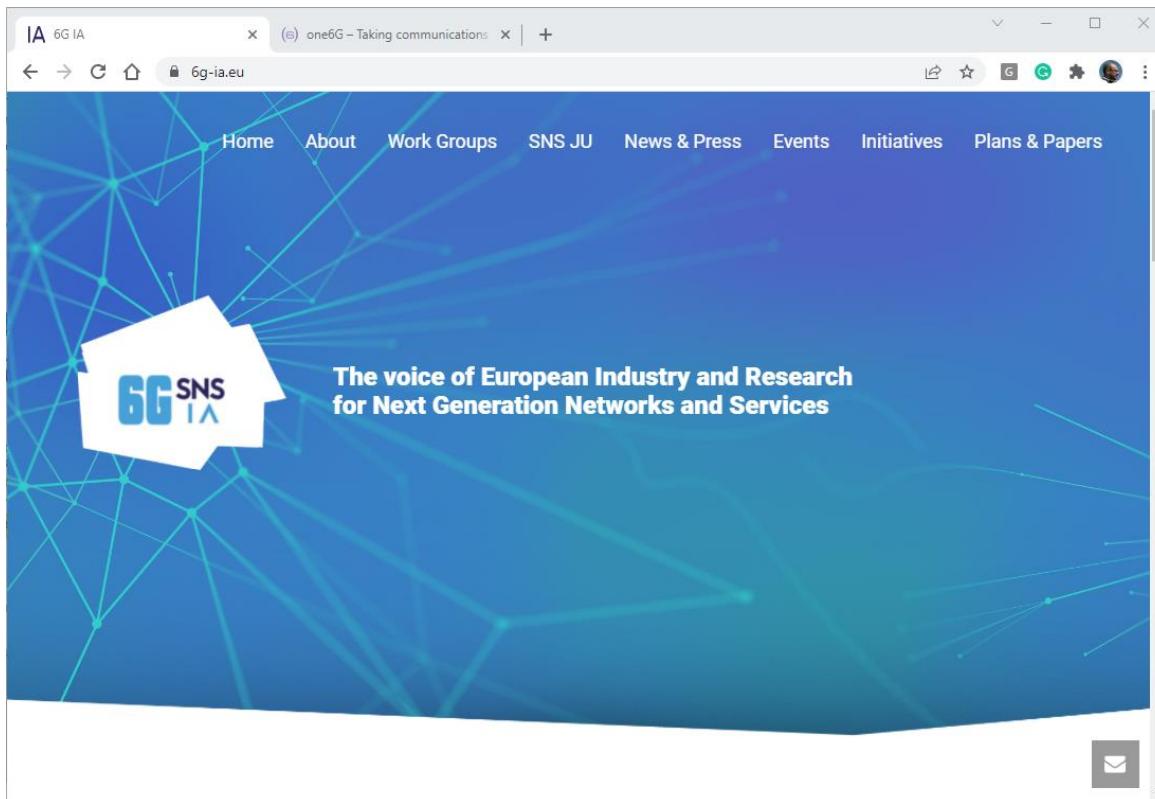
Technological pillars

- Operate at higher radio frequencies (Thz)
- Inclusive of all sort of access technologies, expanding to:
 - Non Terrestrial Networks (NTN), Optical Wireless Communications (OWC) and Large Intelligent Surfaces (LIS)
- Decentralized, flatter network with a stronger edge role, for close, distributed cloud services
- Increased direct devices interactions
- Artificial Intelligence presence at all layers, with cross-domain interactions
- Higher security, secrecy and privacy

Societal and economic impacts

- Ubiquitous connectivity, powered by wireless communications (radio and optics)
- Richer set of connected devices
 - Enabling:
 - The smartphone disaggregation
 - Multisensorial interactions
 - Via Brain-Computer Interactions (BCI), smart body implants and eXtended Reality (XR) devices
 - Massification of Machine Type Communications (MTC)
 - Connected Robotics and autonomous systems

- (some) Research activity around 6G



Software and Virtualization Technologies in Mobile Communication Networks

Comunicações Móveis

DETI – UA

2022/2023

Outline

- Network Function Virtualization
- Management and Orchestration
- Software Defined Networking
- Multi-access Edge Computing
- OpenRAN
- Network automation

Network Function Virtualization

NFV

Virtualization

- 5G brought new trends
- Virtualization
 - Simulate a hardware platform, in software: VM's, containers
 - Higher portability
 - Higher scalability
 - More cost-effective
- Virtualized networks
 - Logical software-based routers, switches, etc.
 - Network services are easier to deploy and manage
 - The physical part only needs to handle packet forwarding

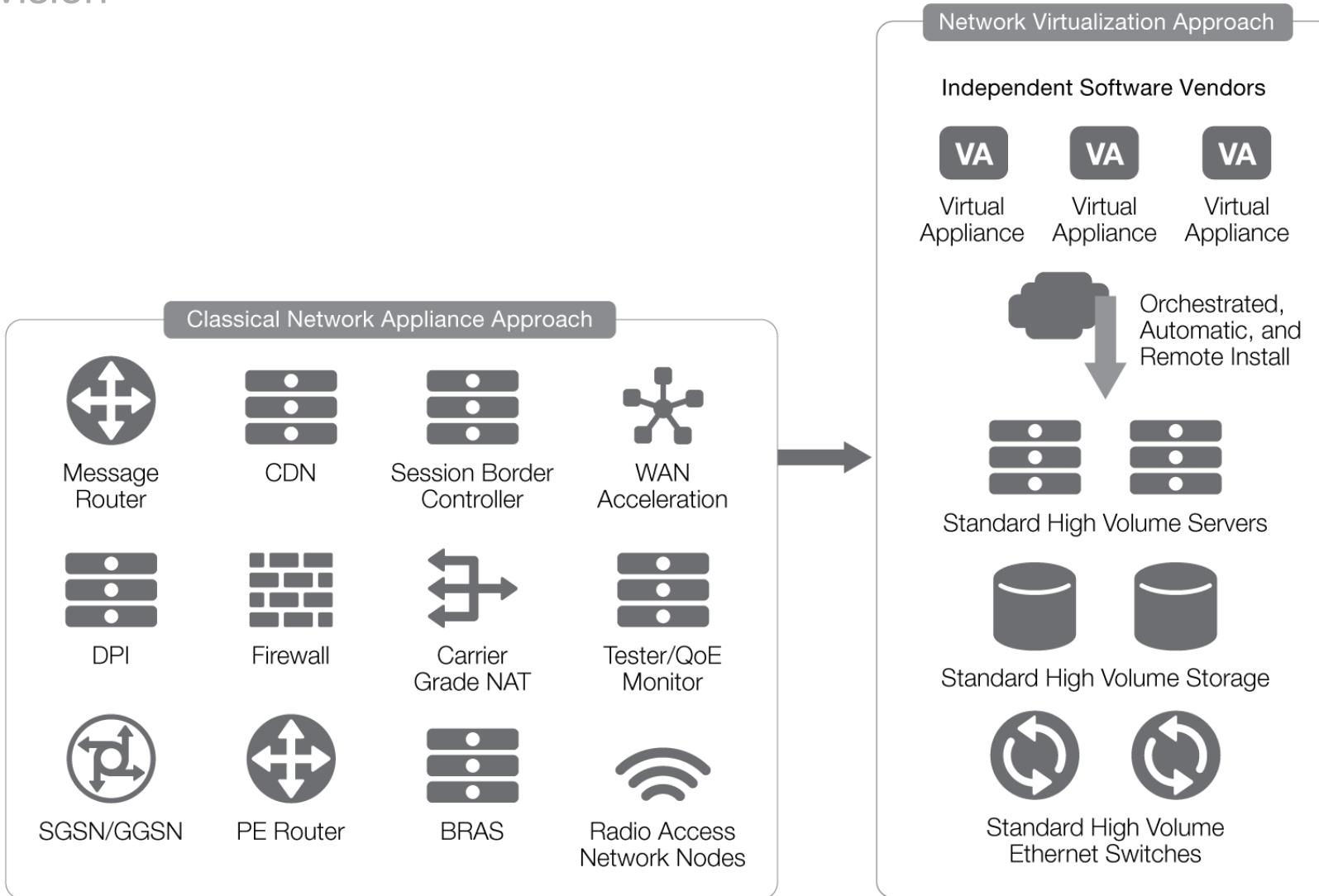
Virtualized Network Functions

- VNFs
- Network functions running in a virtual way
- ... over virtualization infrastructure
- As they are
 - Lift and shift
- Or employing cloud-native principles



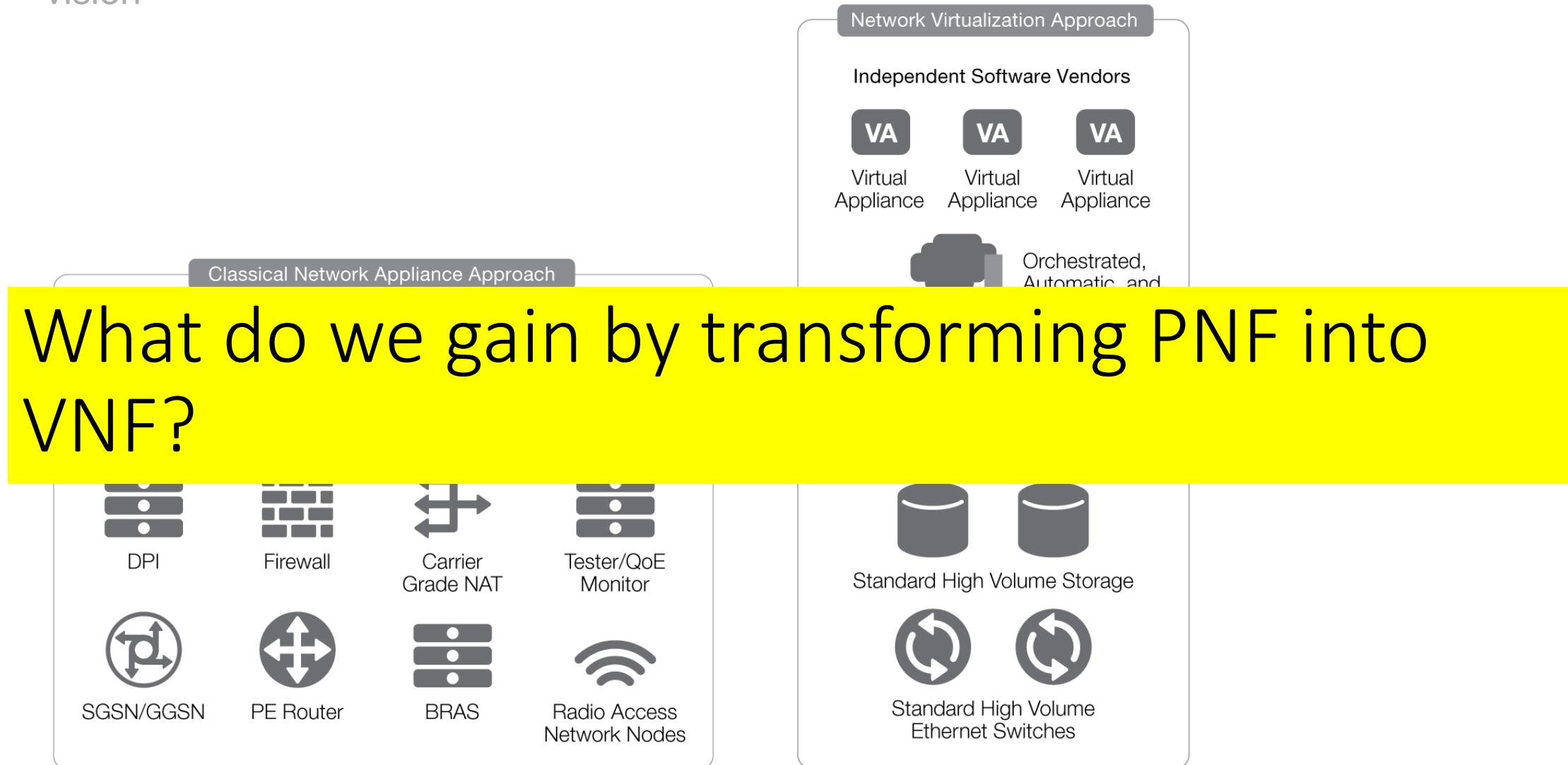
Network Function Virtualization

vision



Network Function Virtualization

vision

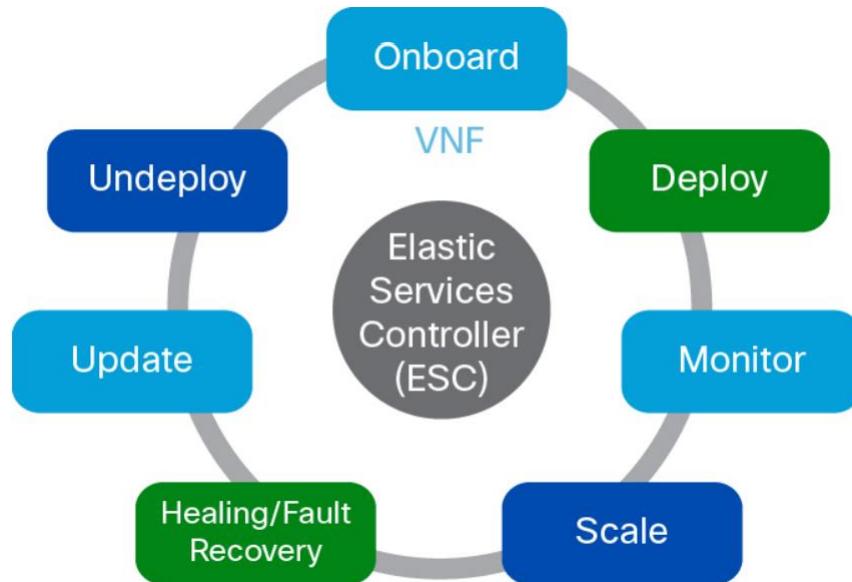


Economy of Scale and Flexibility

- Economy of scale
 - CAPEX – Capital Expenditure
 - <CAPEX → Less investment amounts in infrastructure
 - Less dedicated hardware
 - OPEX – Operational Expenditure
 - <OPEX → Lower costs in operating the infrastructure
 - Less upgrades
 - Less licenses
 - Less air conditioned
 - Less technicians
 - ...

Flexibility: VNF Lifecycle Management

- VNFs are deployed after a service request is done, via northbound interface
- That service request is composed of templates that consist of XML payloads and configuration parameters



Source: Cisco

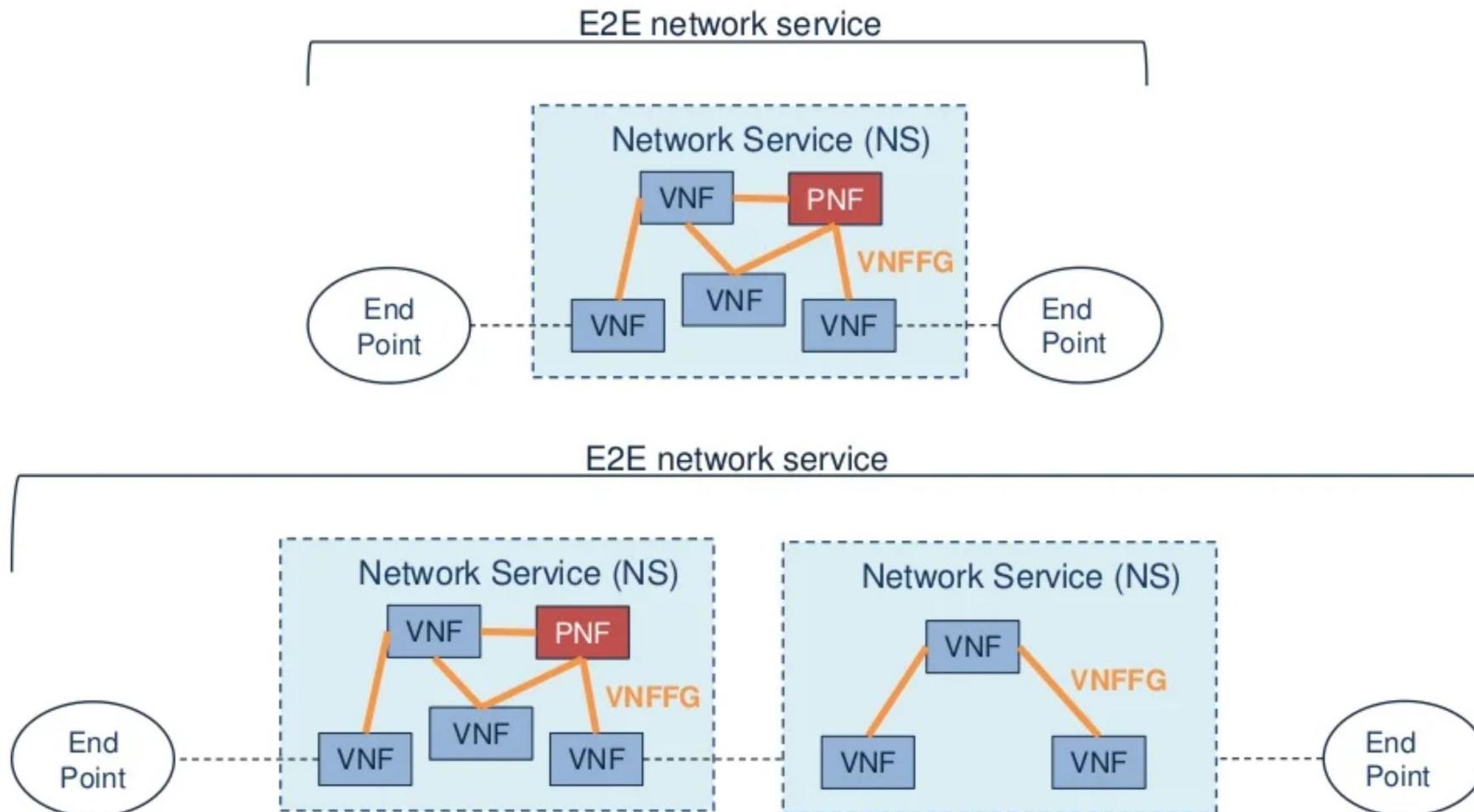
VNF Lifecycle Management

- Onboarding – placing the VNF image/template and configuration, in the system's catalogue;
 - Openstack qcow2 and cmdk disk formats and config drive
- Deploying – placing the resources in the virtualization infrastructure, along with zero-day configuration (credentials, licenses, network information, etc.)
- Monitoring – check the health of virtual machines regarding network status, CPU, memory consumption;
- Healing – after monitoring of failure conditions exposed as Key Performance Indicators (KPIs), the system can heal the VM (restart, expand, etc.)
- Updating – change the details of a virtual machine, set of virtual machines or networks that interconnect them
- Undeploy – remove a VM from the system.

Network Services

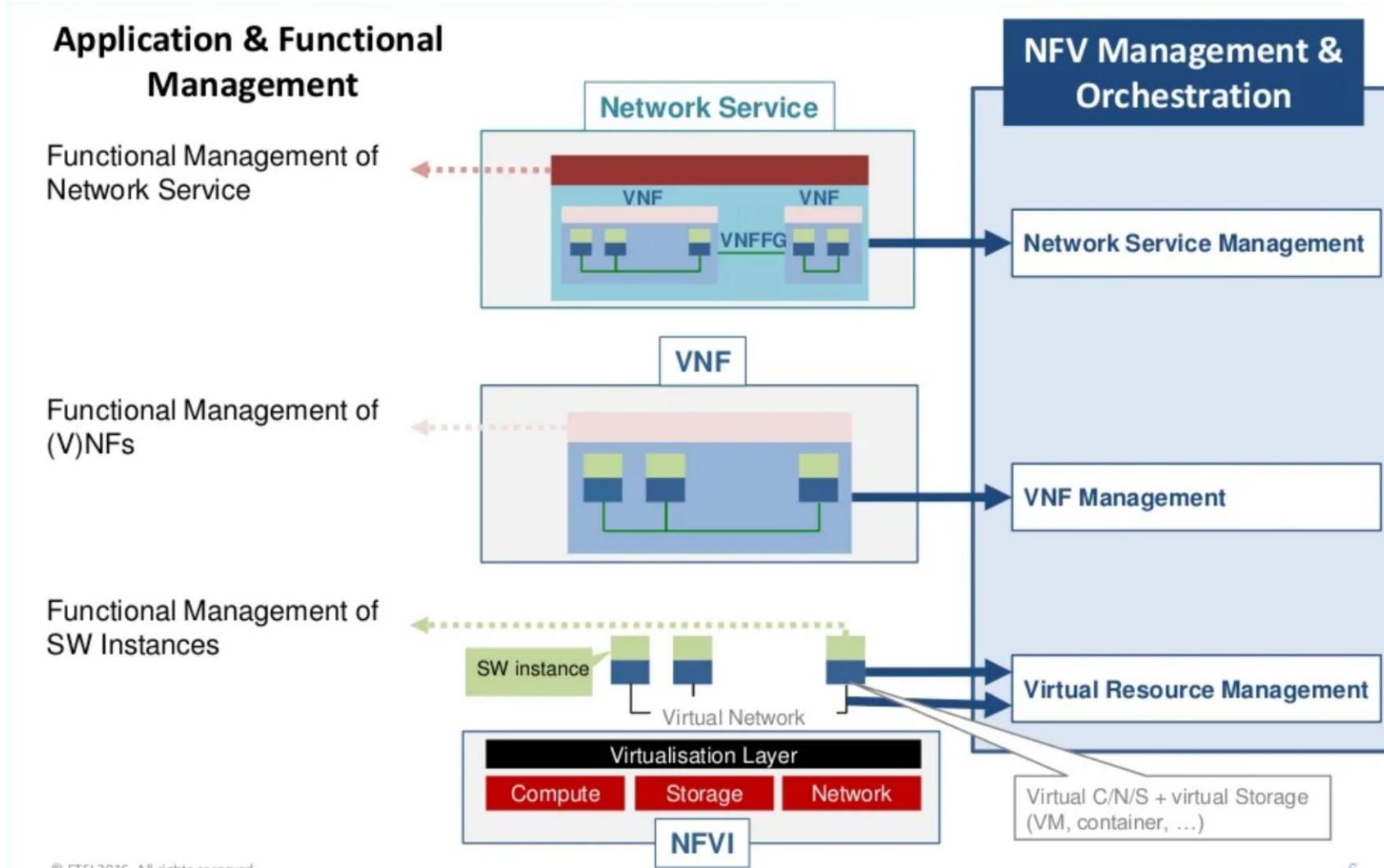
- A set of chained VNFs
- VNFs are interconnected and need to communicate with each other
 - Connectivity Forwarding Graph (FG) indicates how they are connected
 - VNFFG – VNF Forwarding Graph
- Can connect to physical network functions
 - Can also be part of the forwarding graph
- VNFs+VNFFG = Network Service
 - Is managed and orchestrated together
 - Lifecycle mgmt for VNFs
 - Management of the VNFFG and NS lifecycle mgmt is going to orchestrate across the whole lifecycle mgmt of those VNFs that form the NS
 - The NS defines some external connection points that can be connected to the end-points, defining na end-to-end service.
 - We can concatenate differente NS to for an end-2-end network service

Network Services

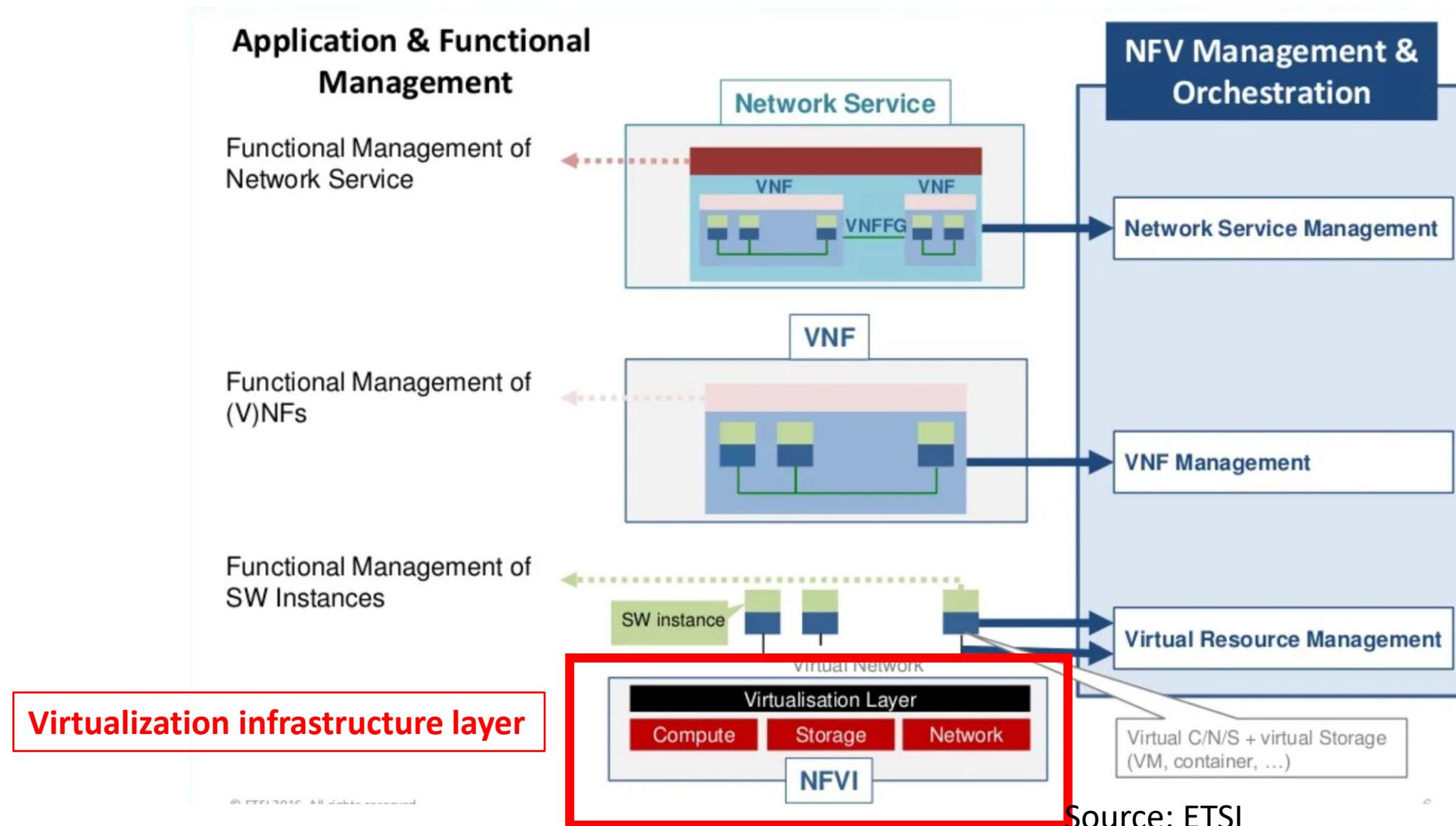


Source: ETSI

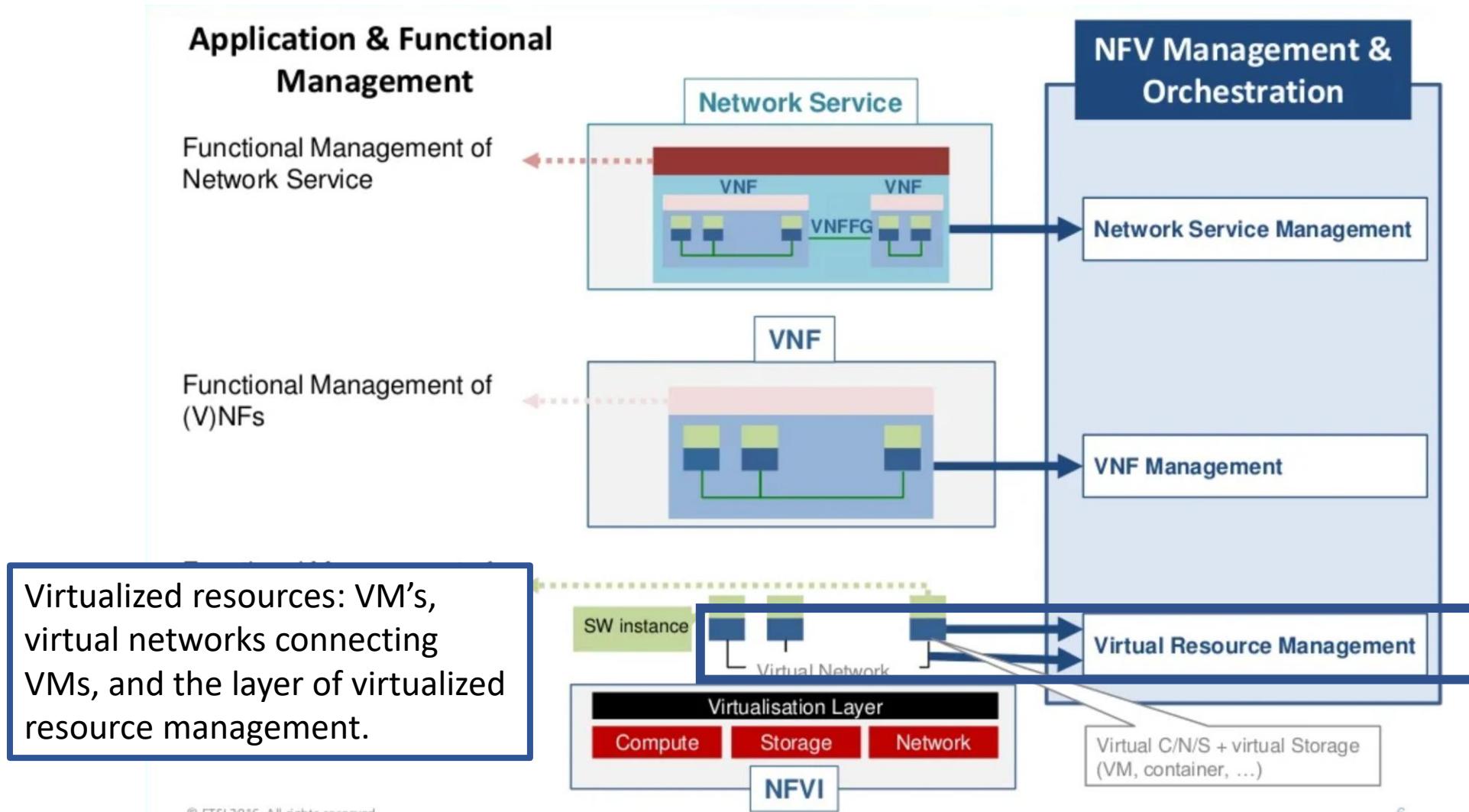
Overall Concepts and how they interconnect



Overall Concepts and how they interconnect

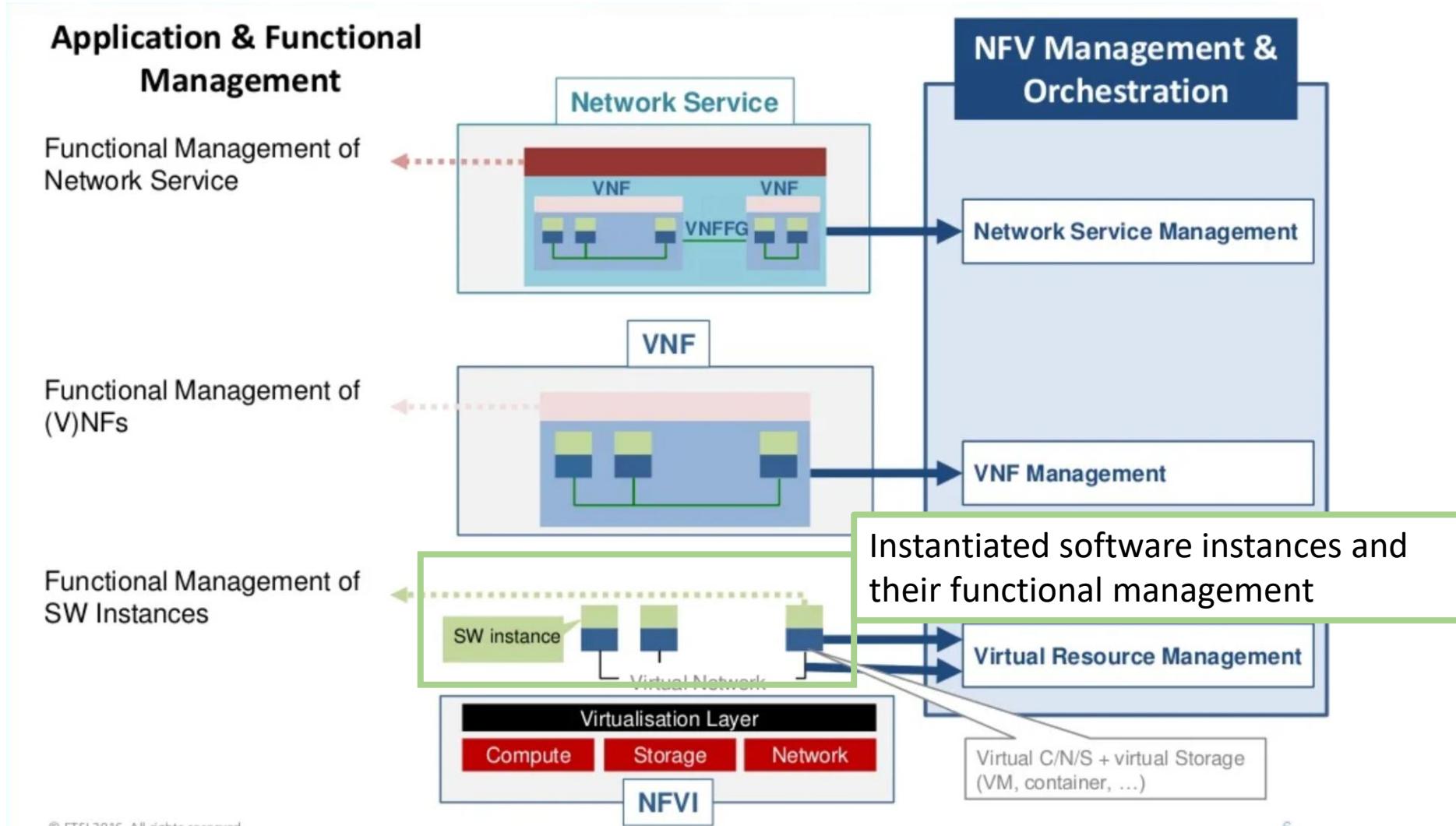


Overall Concepts and how they interconnect



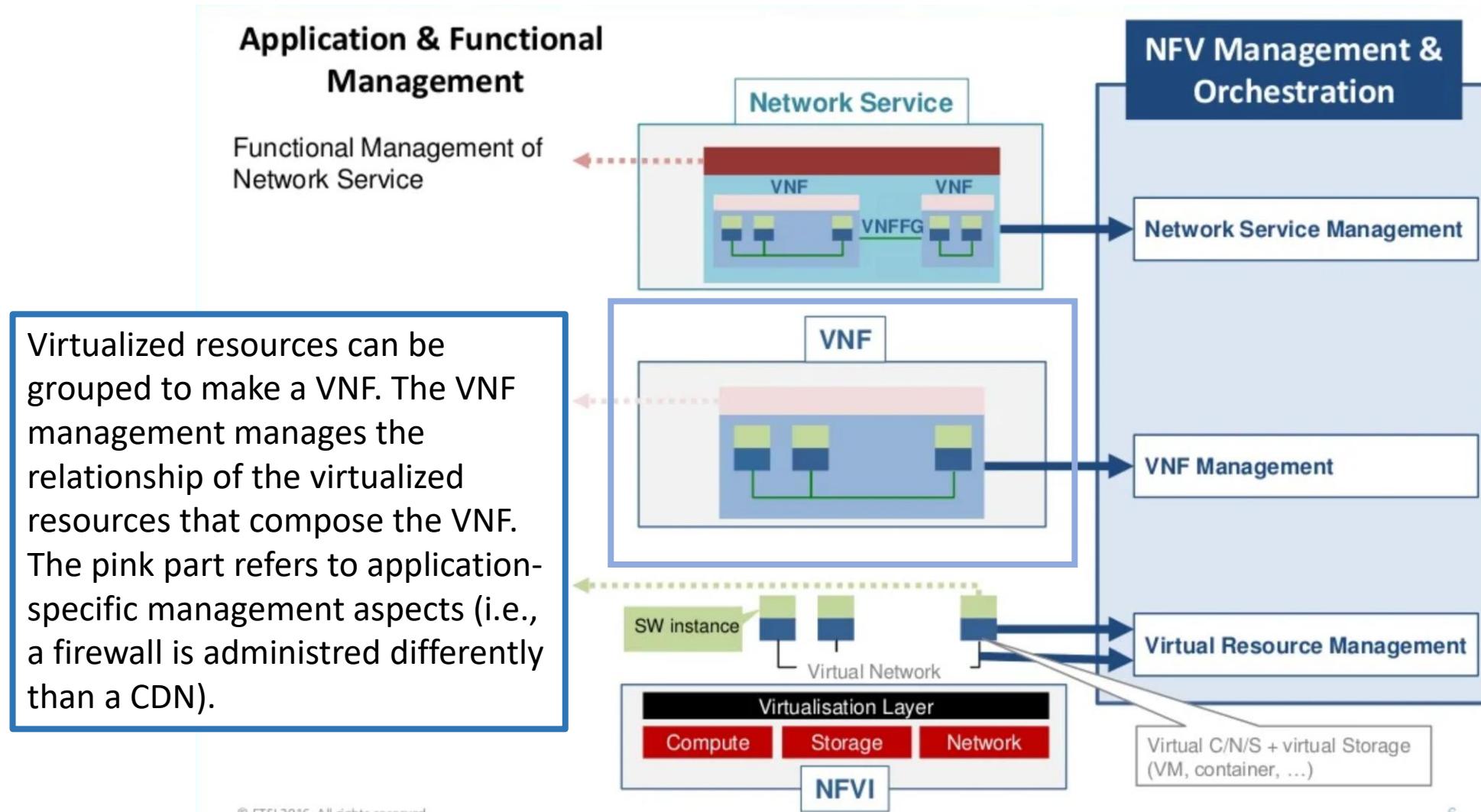
Source: ETSI

Overall Concepts and how they interconnect



Source: ETSI

Overall Concepts and how they interconnect



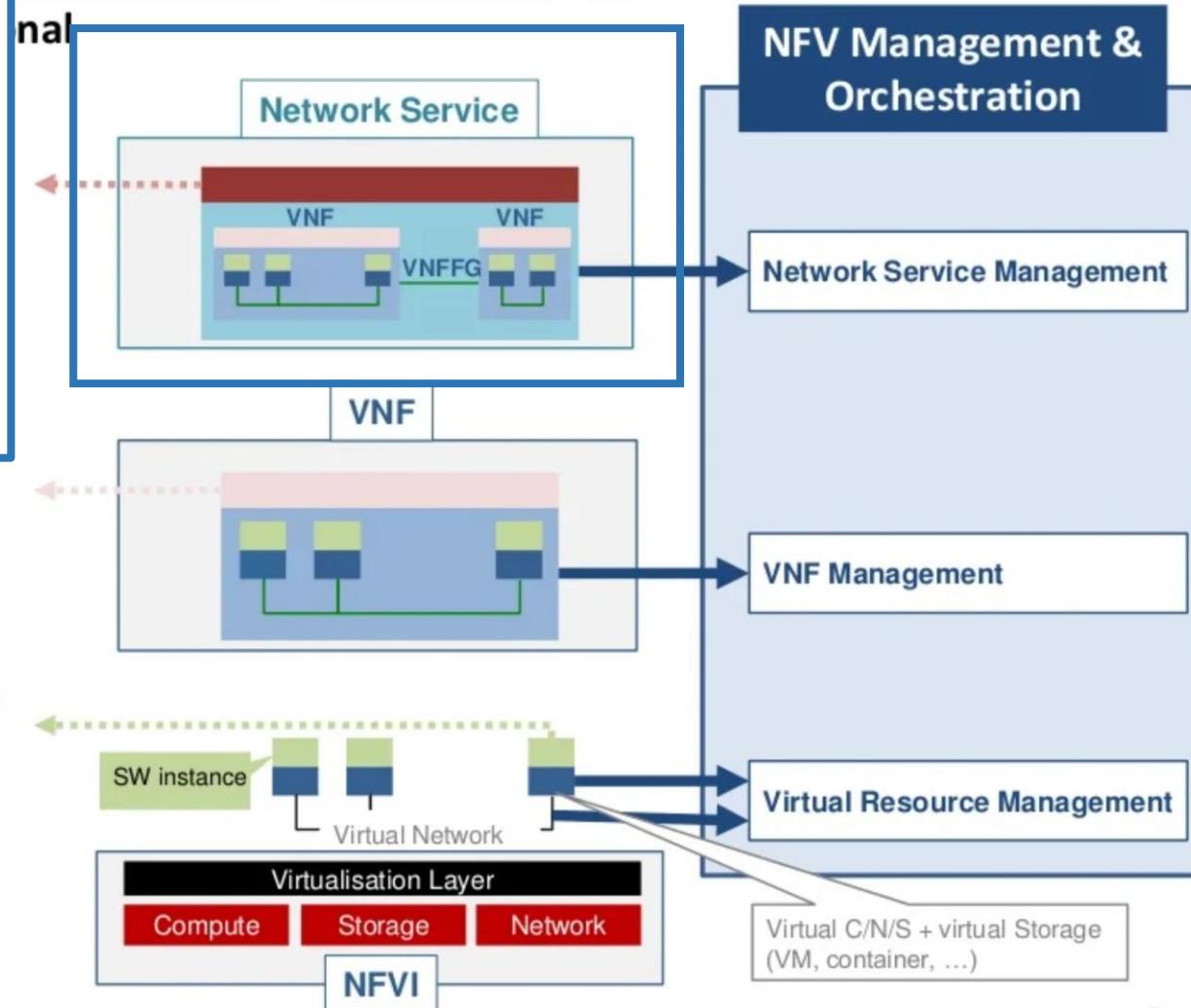
Source: ETSI

Overall Concepts and how they interconnect

A Network Service is a concatenation of VNFs. Example: a virtual network core, composed of virtual PGW, virtual MME, virtual SGW, forms a full NS with a network graph. It has the virtual part management, and the application part management.

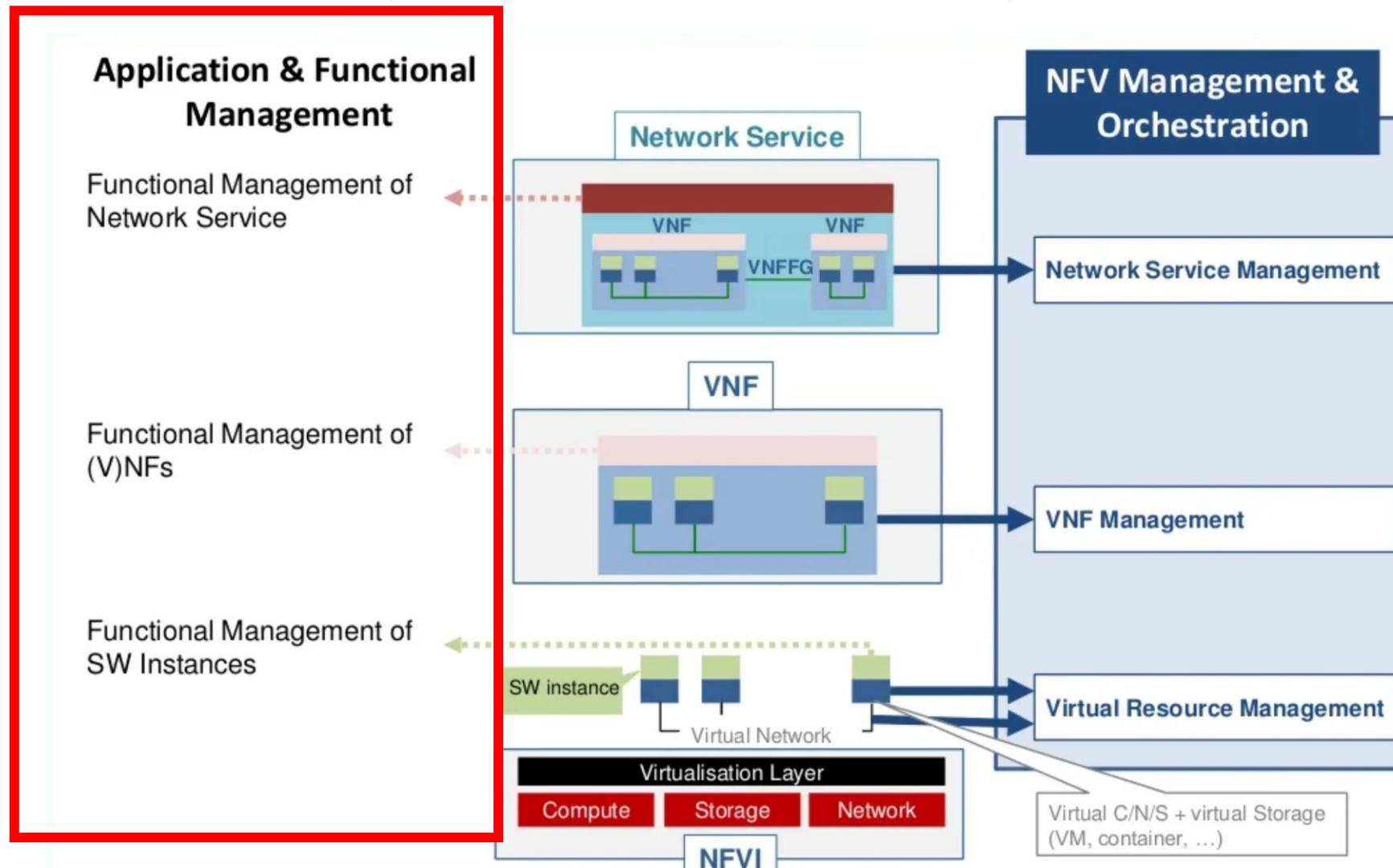
Functional Management of (V)NFs

Functional Management of SW Instances



Source: ETSI

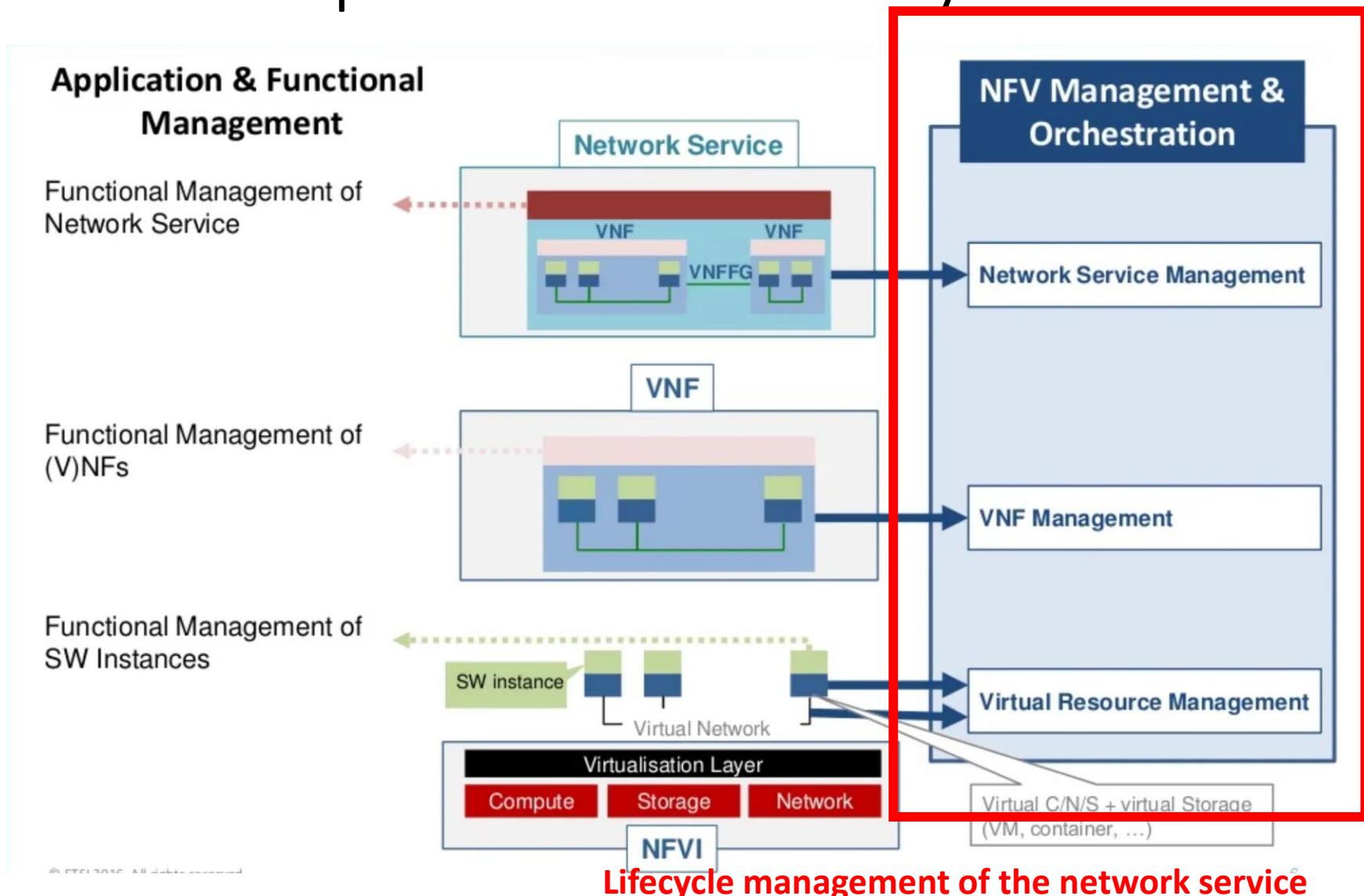
Overall Concepts and how they interconnect



Application/Function level management (not in scope of ETSI NFV)

Source: ETSI

Overall Concepts and how they interconnect

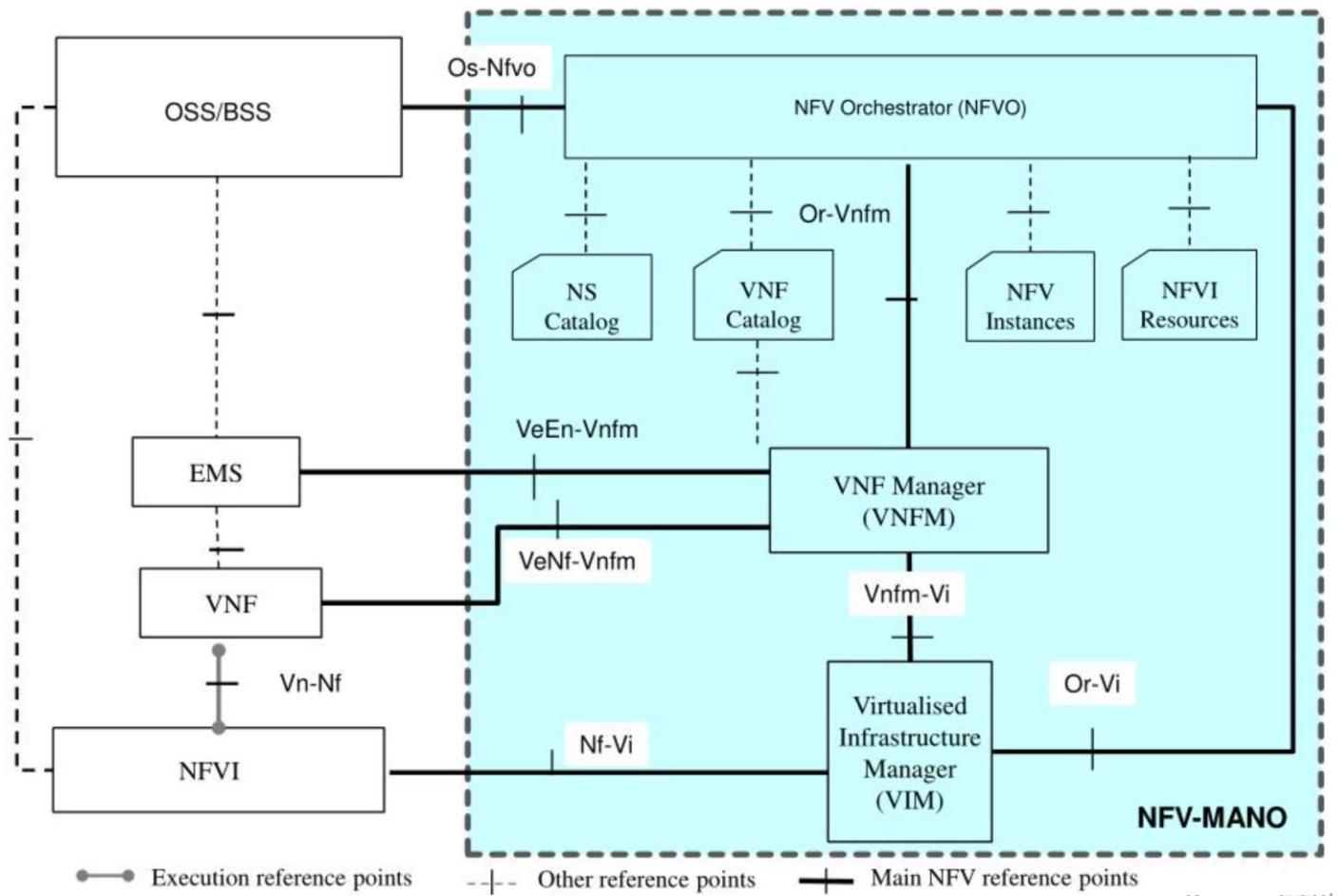


NFV Concept summary

- No longer isolated single purpose physical network services and functions
- A standards-based approach to manage network services, using virtualization infrastructure
- Network services are built from VNF aggregation
- VNFs have their own lifecycle
- But this is managed then at the NS level
 - And at the inter-NS level too (both require orchestration)
- There is the need for management (and orchestration) of the network services
 - Separate from the management of the applications/services themselves

Network Function Virtualization

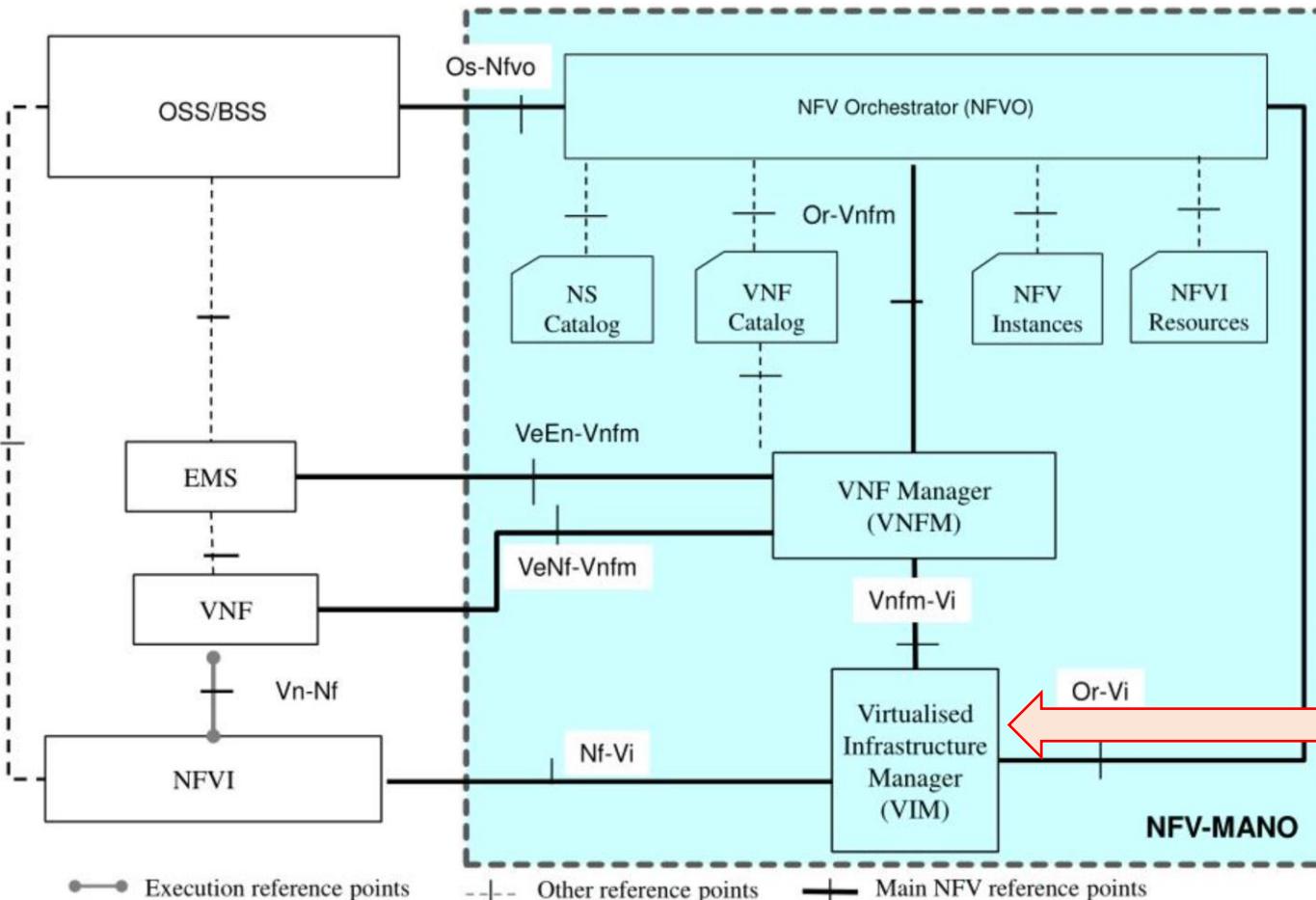
reference architecture



Source: ETSI

Network Function Virtualization

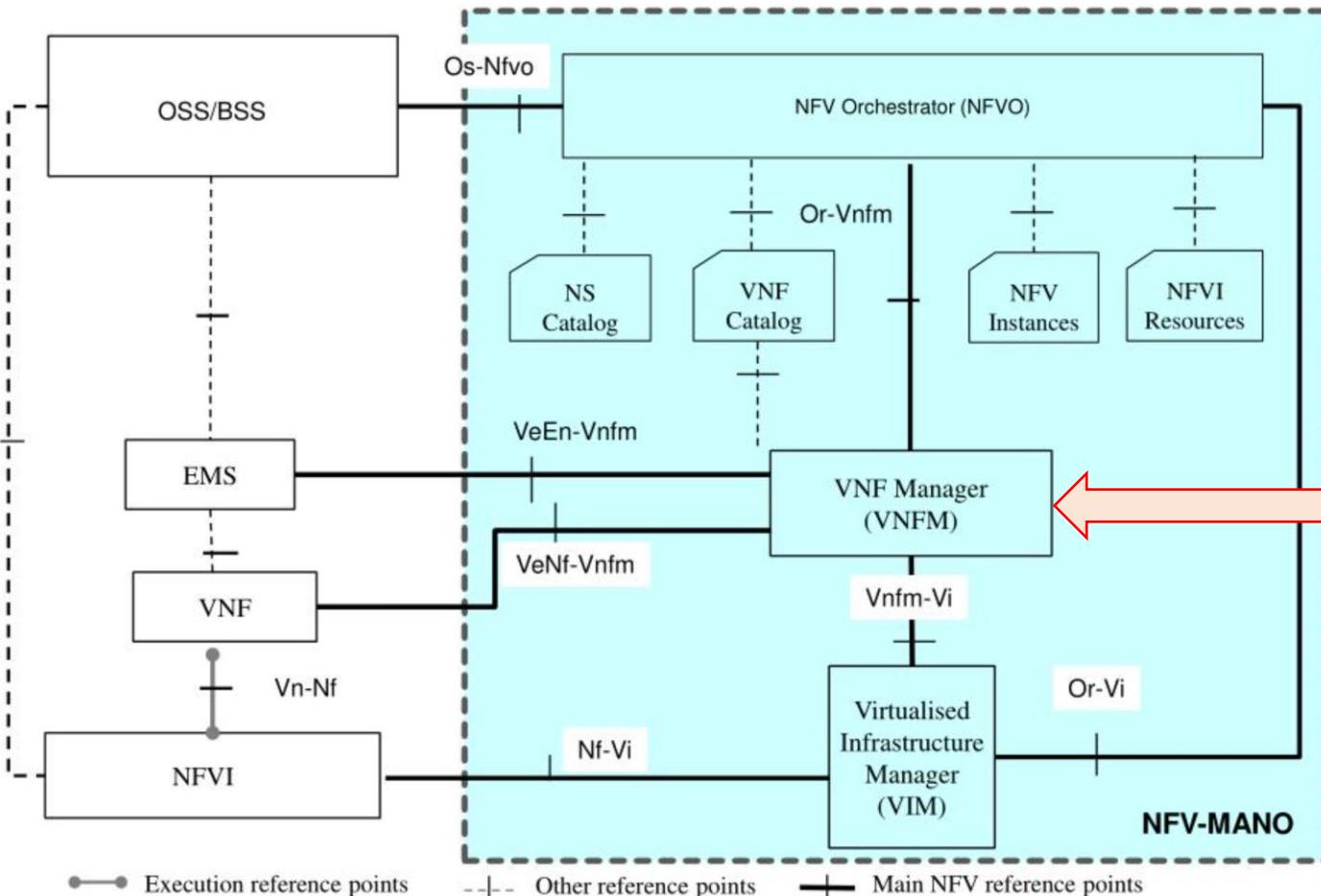
reference architecture



- Manages the NFV infrastructure resources (compute, network and storage) in one or more NFVI-PoPs
 - NFV Infrastructure Point of Presence
- Exposes virtualized resource management interfaces/APIs to the VNFM and NFVO
 - Management and Orchestration
- Sends virtualized resource management notifications to the VNFM and the NFVO

Network Function Virtualization

reference architecture



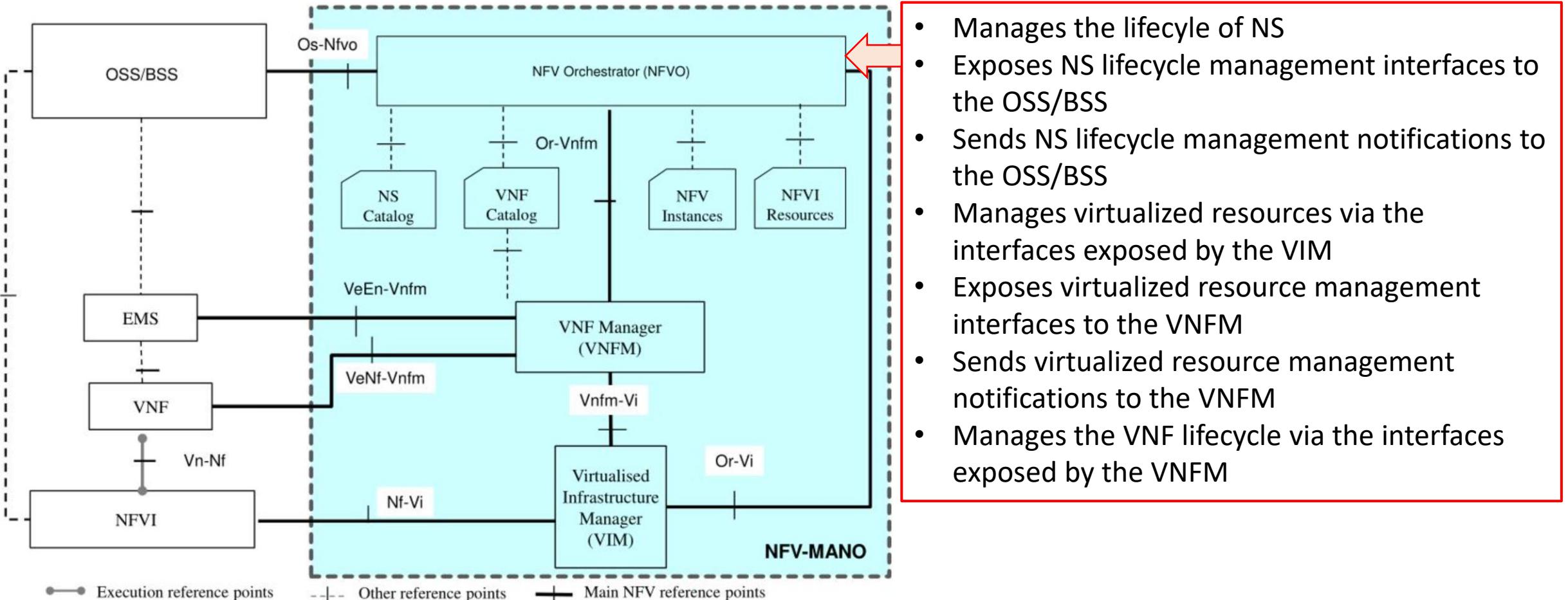
- Manages the lifecycle of VNFs
- Manages VNF initial configuration via the interfaces exposed by the VNF
- Exposes VNF lifecycle management interfaces/APIs to the VNF; EM and NFVO
- Sends VNF lifecycle management notifications to the VNF, EM and NFVO
- Manages virtualized resources associated to the VNF it manages via the interfaces exposed by the VIM or NFVO

VNF Descriptor

- One very important tool used by the VNF Manager (VNFM)
- VNF Deployment template that specifies
 - How the VNF needs to be instantiated
 - How many VM's the VNF has
 - How those VM's are connected
 - What are the external connection points
 - What are the requirements of the VNF, the virtualized resources, etc.
 - Contains scripts that define for VNF scaling, healing, ...
- Provided by the VNF vendor
- When the VNF is onboarded, the VNFD is onboarded in the VNFM

Network Function Virtualization

reference architecture



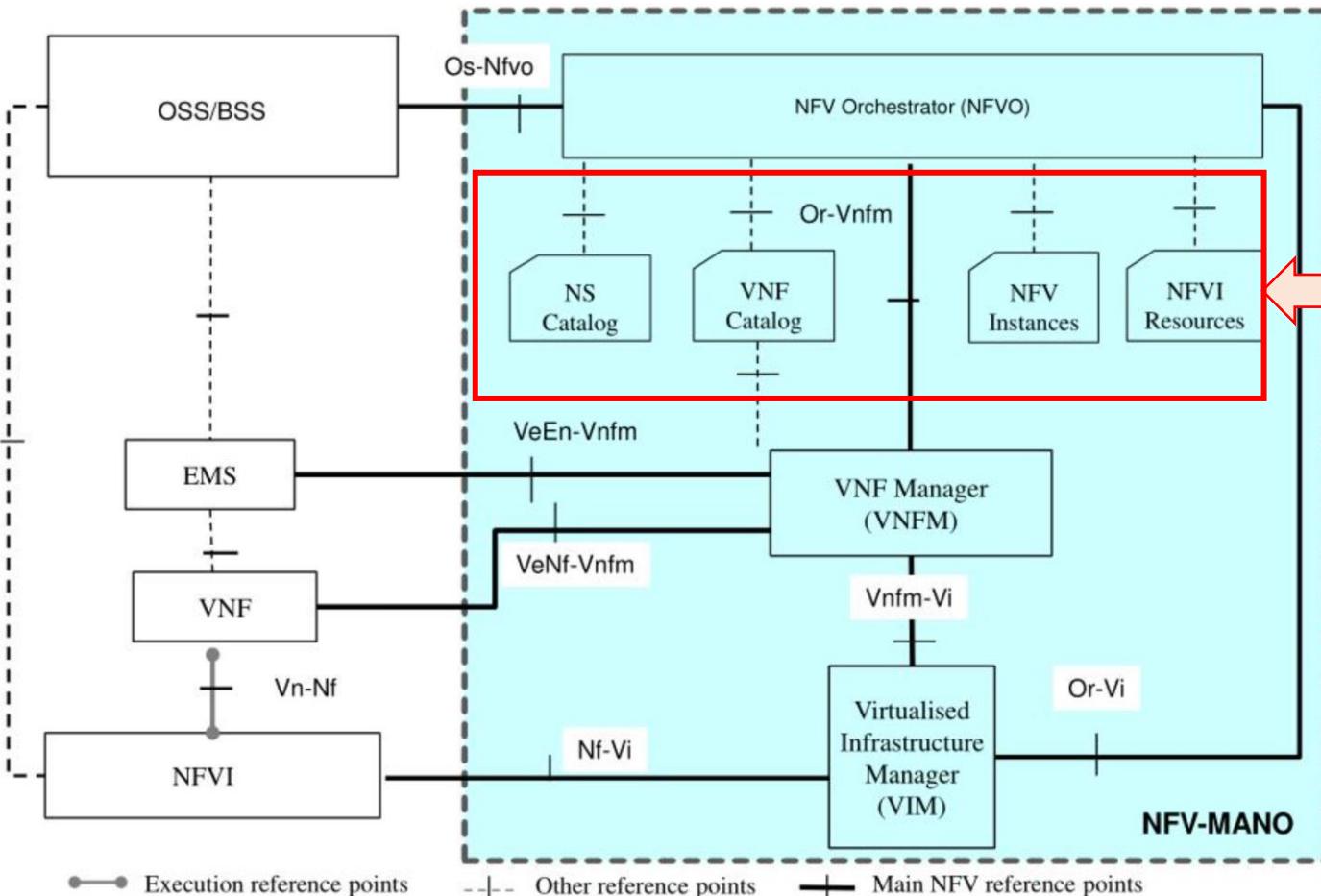
- Manages the lifecycle of NS
- Exposes NS lifecycle management interfaces to the OSS/BSS
- Sends NS lifecycle management notifications to the OSS/BSS
- Manages virtualized resources via the interfaces exposed by the VIM
- Exposes virtualized resource management interfaces to the VNFM
- Sends virtualized resource management notifications to the VNFM
- Manages the VNF lifecycle via the interfaces exposed by the VNFM

NS Descriptor

- Template that describes how the NS is composed
 - In terms of VNF
 - The VNFFG
 - Scripts and indicators that defines what the orchestrator needs to do when certain events or indicators are received
 - These appear during the lifecycle management of the NS

Network Function Virtualization

reference architecture



Catalogues

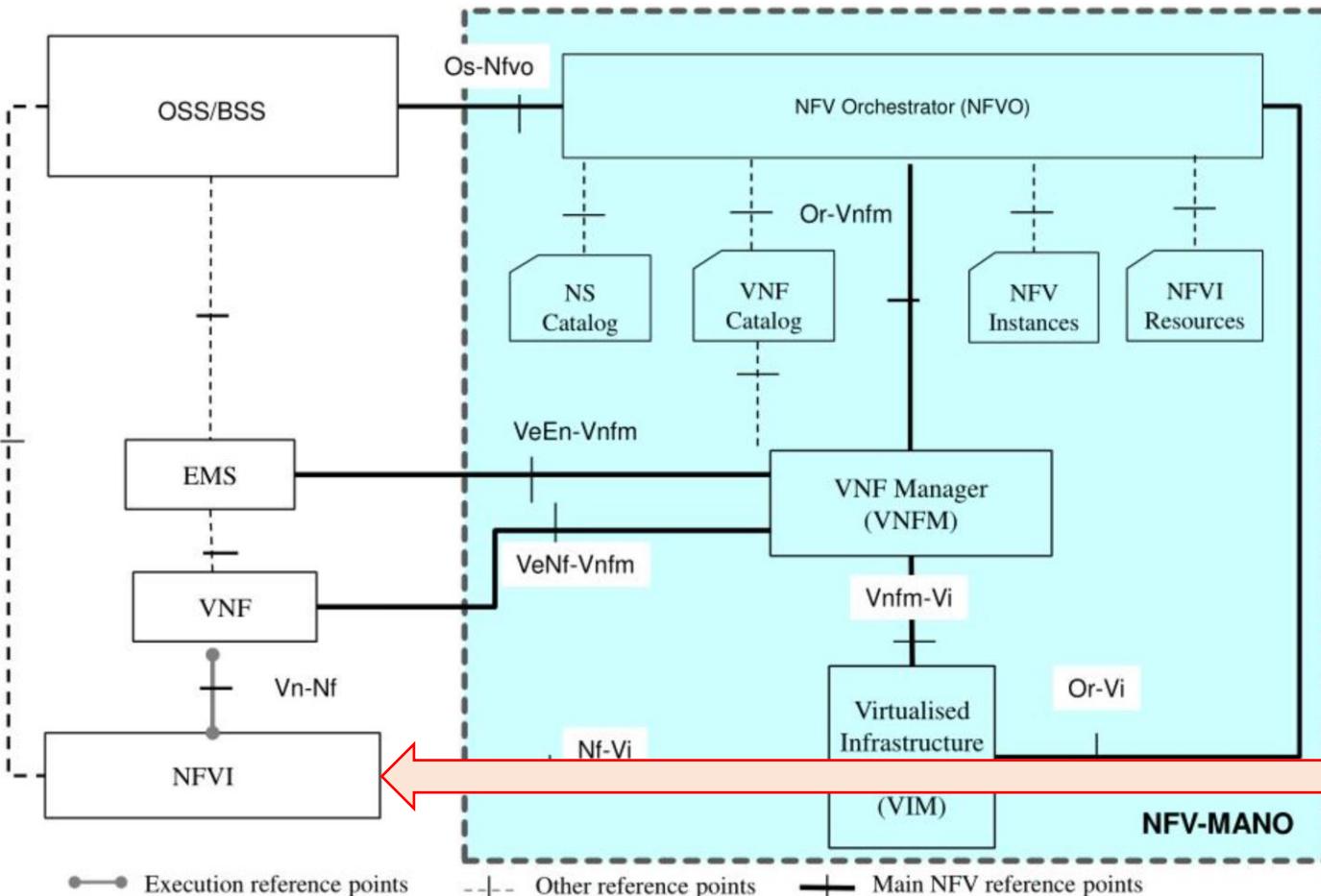
- NS Catalog – Network Services that can be instantiated in this NFVI, along with all the information for its instantiation (i.e., VNFFG, lists of VNFs, configurations, etc.)
- VNF Catalog – List of VNFs available at the NFVI and their lifecycle characteristics

Repositories

- NFV Instances – Indication of which NFV instances are operating
- NFVI Resources – provides information to the orchestrator about the NFVI resources

Network Function Virtualization

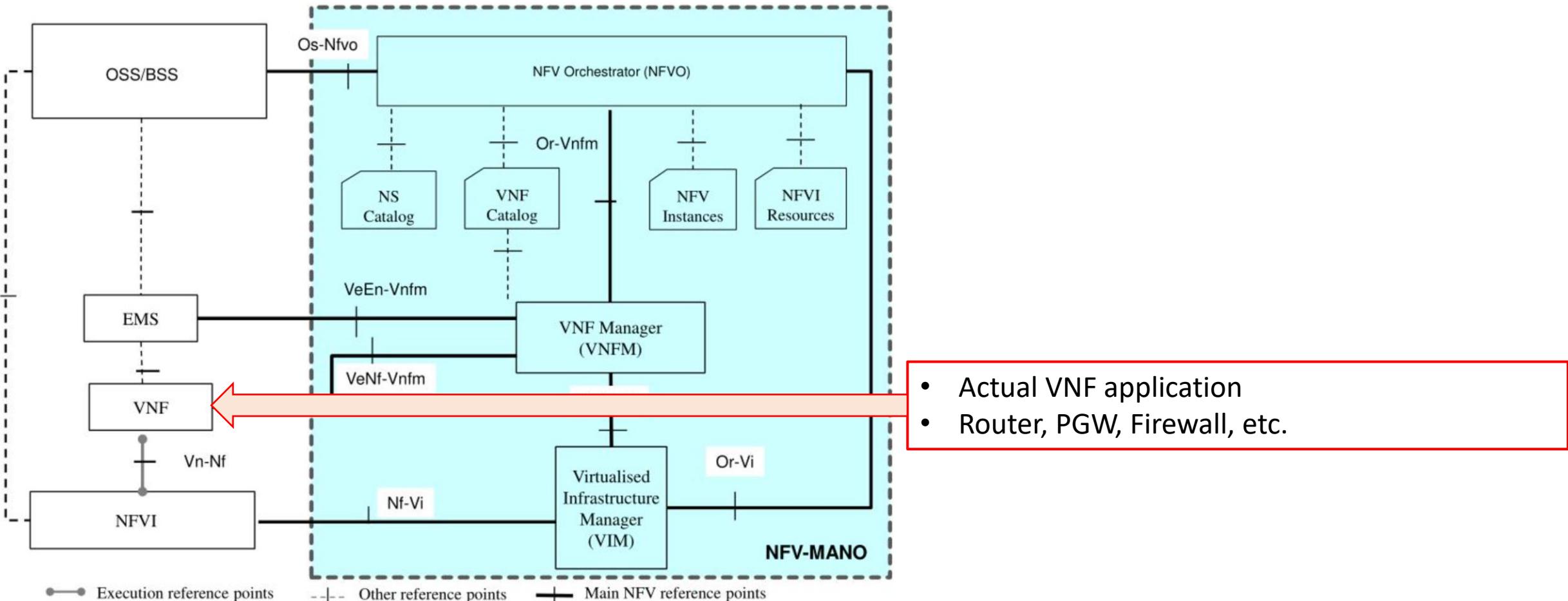
reference architecture



- Network Function Virtualization Infrastructure
- The actual infrastructure
- Servers
- Switches
- Routers
- Racks

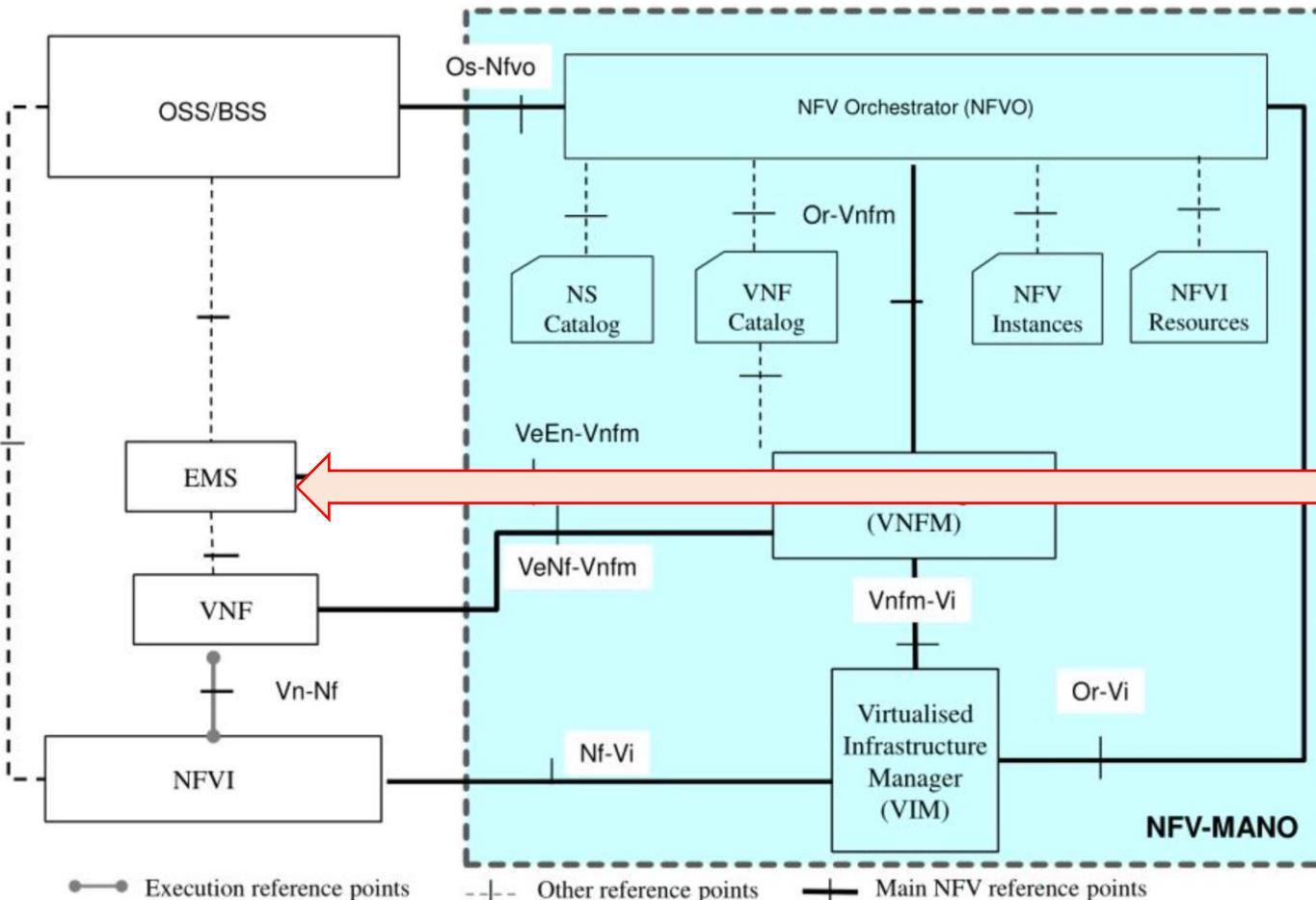
Network Function Virtualization

reference architecture



Network Function Virtualization

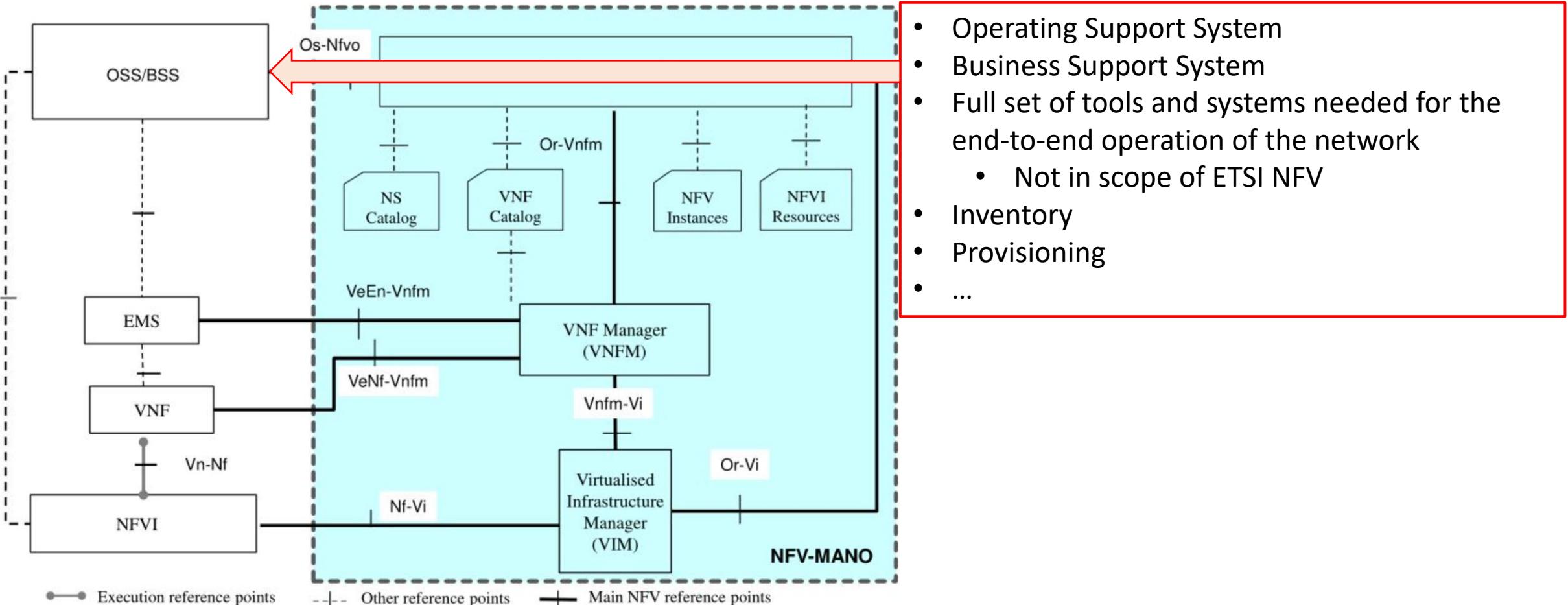
reference architecture



- Element Management Service/Function
- Management to the fault, alarm and configuration management associated to the application-level of a VNF

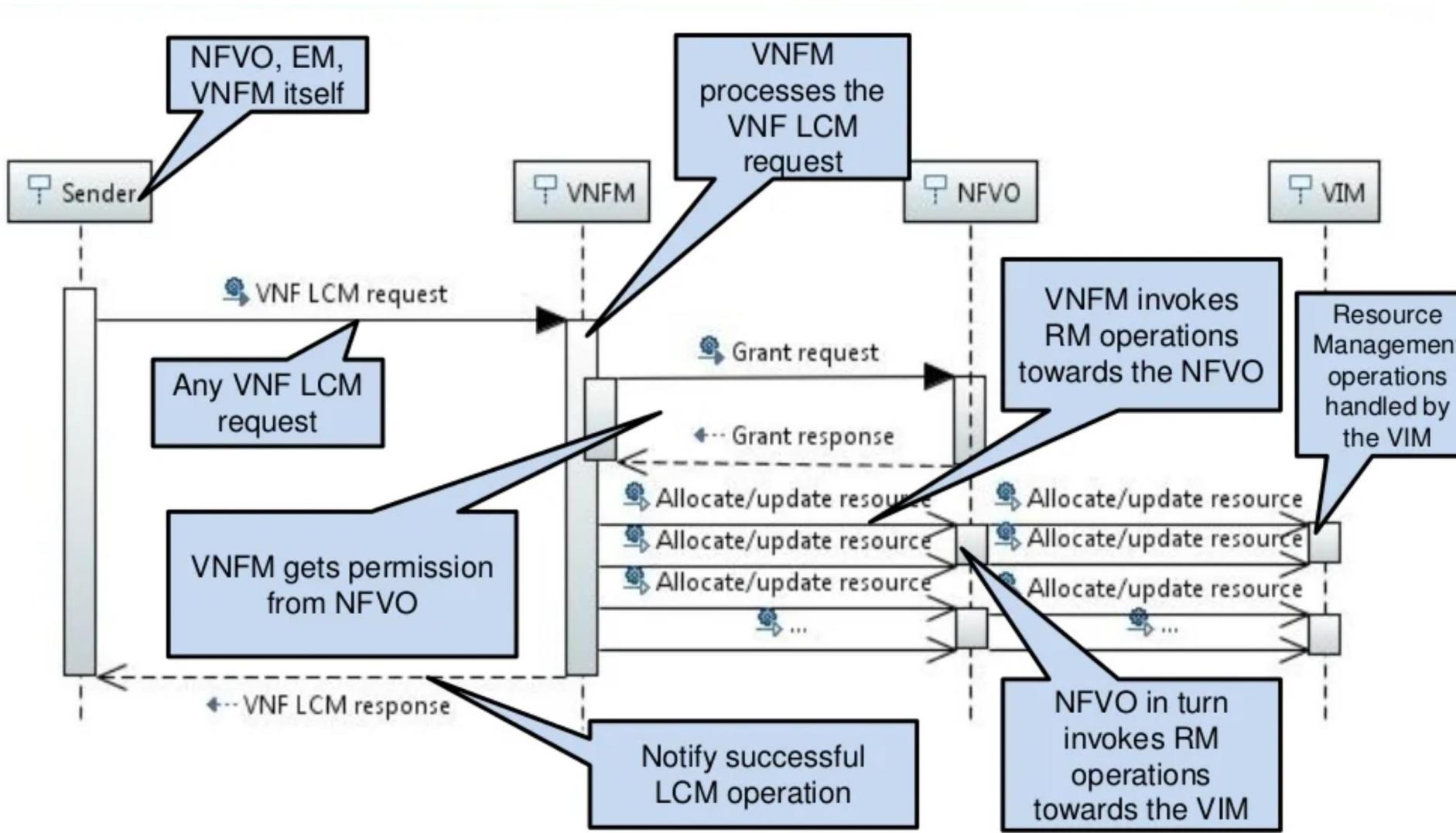
Network Function Virtualization

reference architecture



- Operating Support System
- Business Support System
- Full set of tools and systems needed for the end-to-end operation of the network
 - Not in scope of ETSI NFV
- Inventory
- Provisioning
- ...

Resource Management (Simplified)



Network Services

- Modeled through Information elements
 - VNF Forwarding Graph
 - Physical Network Function
 - Virtual Link
 - Virtual Network Function
 - Network Forwarding Path

NFV Standardisation



World Class Standards

- Started in 2012
 - Release 1 (2013-2014, “NFV” series of documents)
 - Use cases (NFV 001)
 - Requirements (NFV 004)
 - Architectural framework (NFV 002)
 - Terminology (NFV 003)
 - Proof of Concepts (NFV-PER 002)
 - Release 2 (2015-2016, “NFV-IFA” series of documents – Interfaces & Arch.)
 - Management aspects
 - Lifecycle management
 - Performance metrics
 - VNF package and software management
 - Information modelling

NFV Standardisation

- Started in 2012
 - Release 3 (2017-2018)
 - Interfaces and architecture refinement
 - Support for Edge computing and slicing
 - Virtualization advances (i.e., cloud-native) Support
 - Release 4 (2019-2020)
 - NFVI evolution
 - Automation capabilities
 - MANO evolution and exposure
 - Reliability
 - Policy models



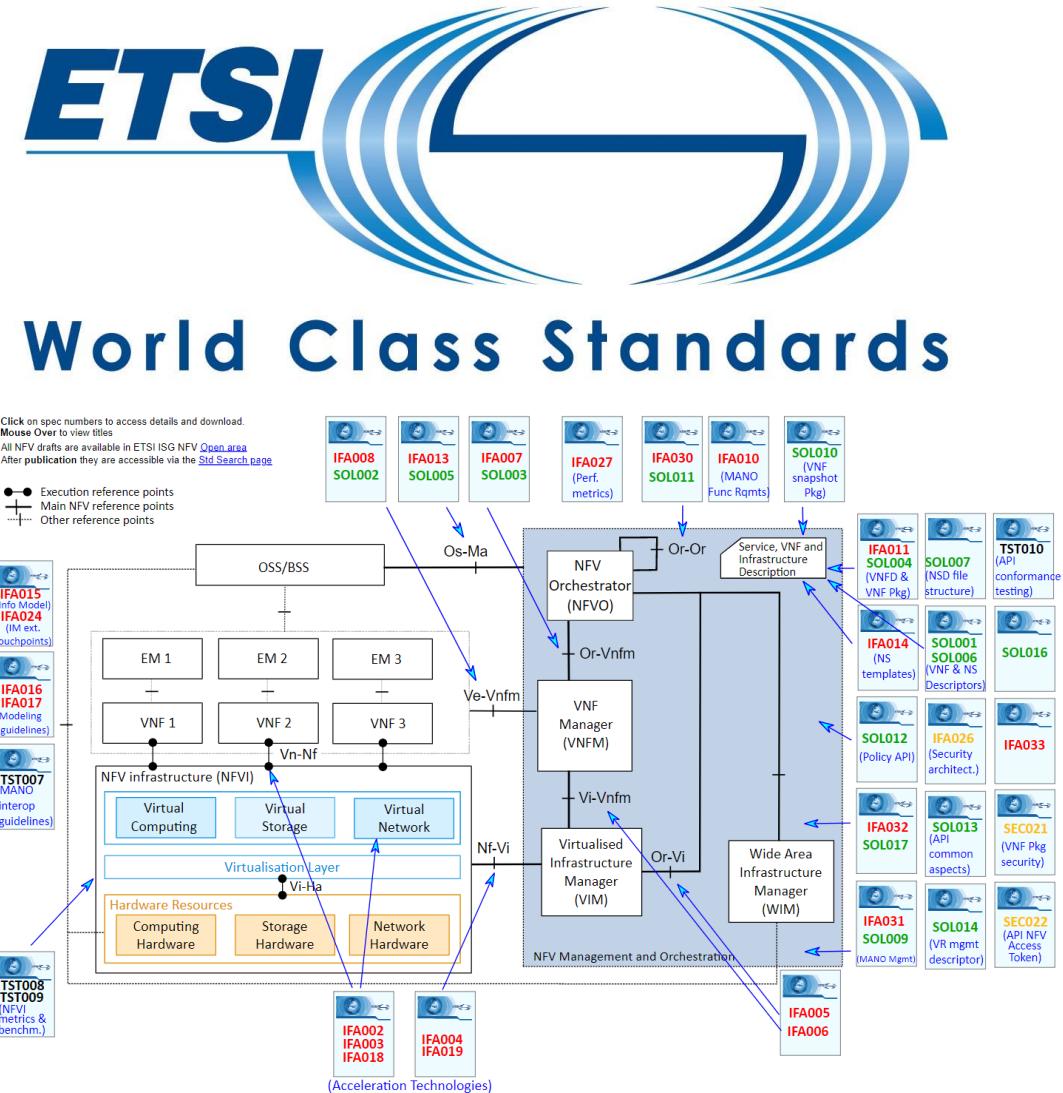
World Class Standards

NFV Standardisation

- ETSI NFV research groups
 - TST – Testing
 - SOL – Protocols and Data models
 - REL – Reliability
 - IFA – Interfaces and Architecture
 - EVE – Evolution and Ecosystem
 - SEC – Security

- Clickable architecture:

https://www.etsi.org/images/articles/NFV_Architecture.svg



VIM – Virtual Infrastructure Managers

- OpenStack
 - <https://www.openstack.org/>
- Vmware vCloud Director
 - <https://www.vmware.com/products/cloud-director.html>
- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- Sandboxes
 - DevStack
 - <https://docs.openstack.org/devstack/latest/>
 - MicroStack
 - <https://opendev.org/x/microstack>



Management and Orchestration

MANO

Virtualized Network Services

- Managing and coordinating resources and networks needs a special entity
 - NFV Orchestrator
- A powerful tool
 - Spans large numbers of networks
 - ... software elements
 - ... hardware platforms
- Needs to be able to work with many different standards

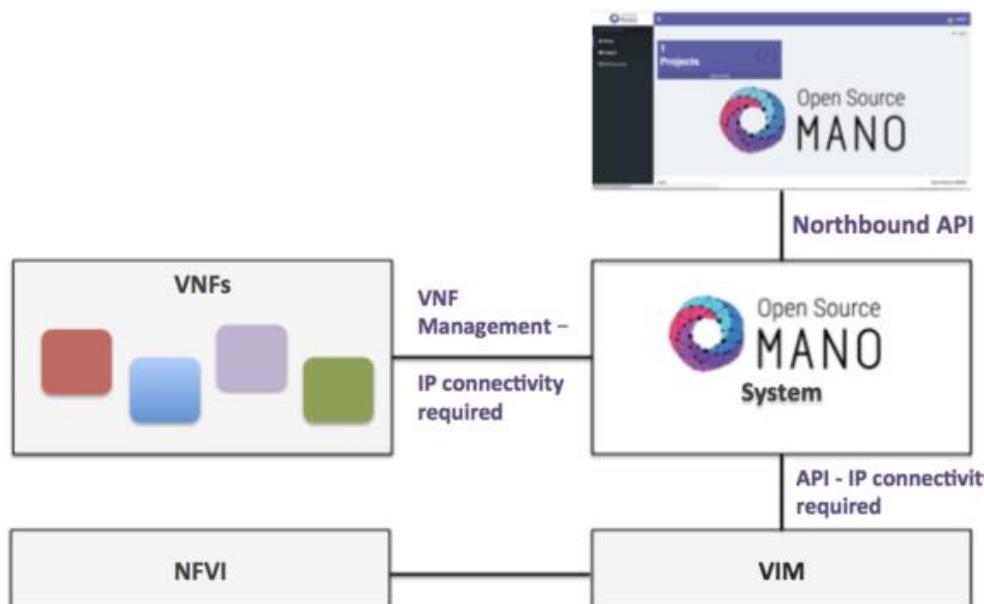
ETSI NFV MANO

- Framework for managing and orchestrating all resources in the cloud datacenter
 - Includes computing, networking, storage and VM resources
- Objective
 - Allow flexible on-boarding of network services
 - Handle network componentes spin-up
- The standard composes 3 elements
 - NFVO – NFV Orchestrator
 - VNF Manager – VNFM
 - Virtualized Infrastructure Manager – VIM

ETSI OSM – Open Source MANO



- Open source NFV Management and Orchestration stack
- Uses well established open source tools and working procedures
- Complements the standardisation work



<https://osm.etsi.org/docs/user-guide/latest/01-quickstart.html>

ONAP – Open Network Automation

- <https://www.onap.org/>
- Also Open Source
- More than just MANO
- Common platform for end-to-end service and infrastructure management and provisioning
- Support from major vendors
- Supports TOSCA and YANG unified design specifications



Software Defined Networking

SDN

Software Defined Networking

- Objective
 - A tool to enable a higher degree of control over network devices and traffic flow
- Main aspects
 - Control plane is separated from the device implementing the data plane
 - A single control plane is able to manage multiple network devices
- Initial deployments
 - Universities: to try out radical new protocols in parallel with existing traffic
 - Busy data centres: overcome the VLAN ID tag limit (4095)
- Protocols:
 - OpenFlow (first)
 - P4 (now)

OpenFlow



- Standardised by the ONF – Open Networking Foundation
- <https://opennetworking.org/software-defined-standards/specifications/>
- Currently on version 1.5

ABOUT BROADBAND PRIVATE 5G & EDGE OPEN RAN PROGRAMMABLE NETWORKS OTHER PROJECTS

OVERVIEW SPECIFICATIONS MODELS & APIs INFORMATIONAL ARCHIVES

Specifications

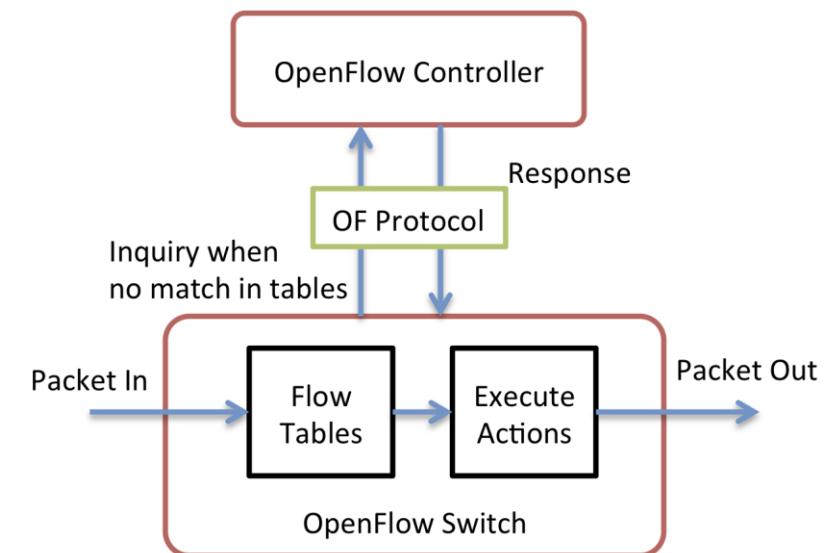
Technical Specifications include all standards that define a protocol, information model, functionality of components and related framework documents. It is this category of Technical Specification that is identified as such because it is a normative publication that has the [ONF RAND-Z IPR policy](#) and licensing guiding its further use.

Current Versions

Current Versions			
DATE	DOCUMENT NAME	DOCUMENT TYPE & ID	FORMAT
06/2017	SPTN OpenFlow Protocol Extensions	TS-029	PDF
04/2017	Optical Transport Protocol Extensions Ver. 1.0	TS-022	PDF
04/2015	OpenFlow® Switch Specification Ver 1.5.1	TS-025	PDF

OpenFlow

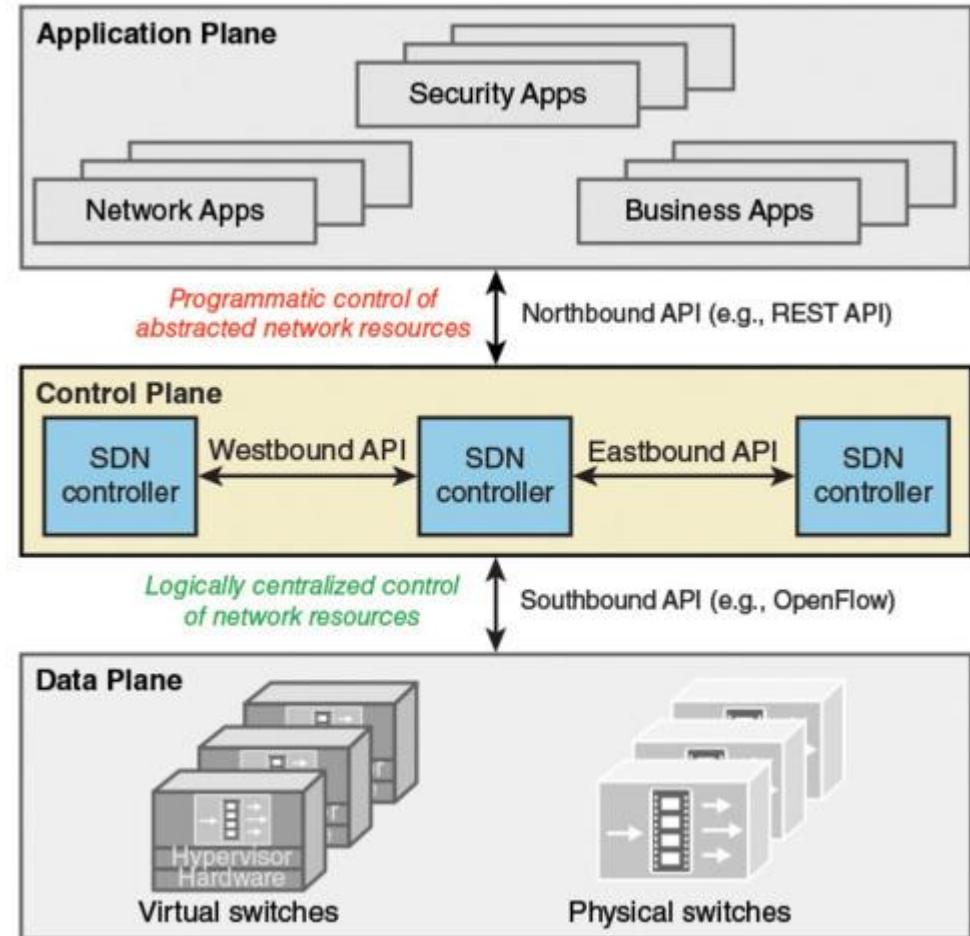
- A protocol existing between SDN switches and a new entity
 - SDN controller
- Allows the SDN controller to manage flow tables in SDN switches
- SDN switch contains
 - Openflow agent
 - Flow tables
 - Performs packet lookup and forwarding
 - Is able to communicate (securely) with the controller
- A flow table is composed of
 - Flow entries (matches properties in packets' headers)
 - Counters (for activity)
 - A set of actions to be applied (to matching packets)
 - When no actions are present, the switch can
 - Drop the packet
 - Ask the controller what to do



Source: fibre-optic-transceiver-module.com

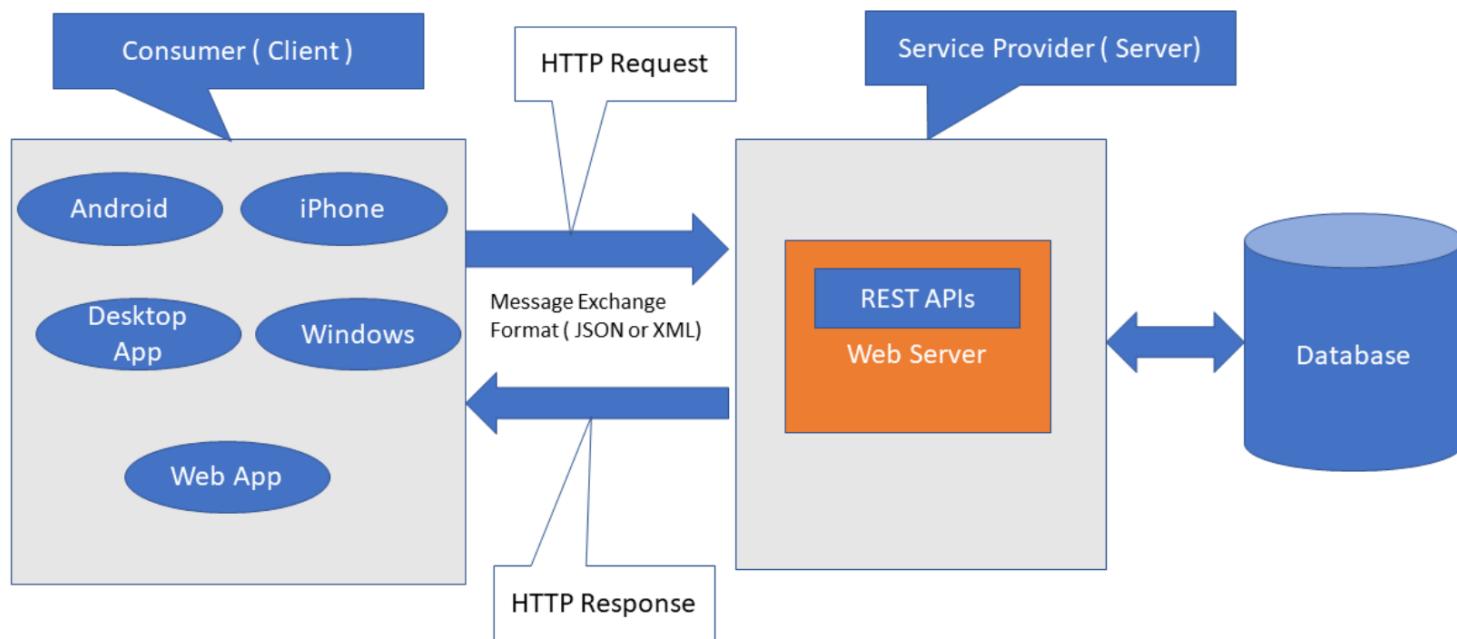
OpenFlow Controller

- Controller
 - Service existing in a server, which uses the OpenFlow protocol to interact with SDN switches
 - Formulates flows and programs switches
 - Is able to receive directives from external applications via northbound REST API



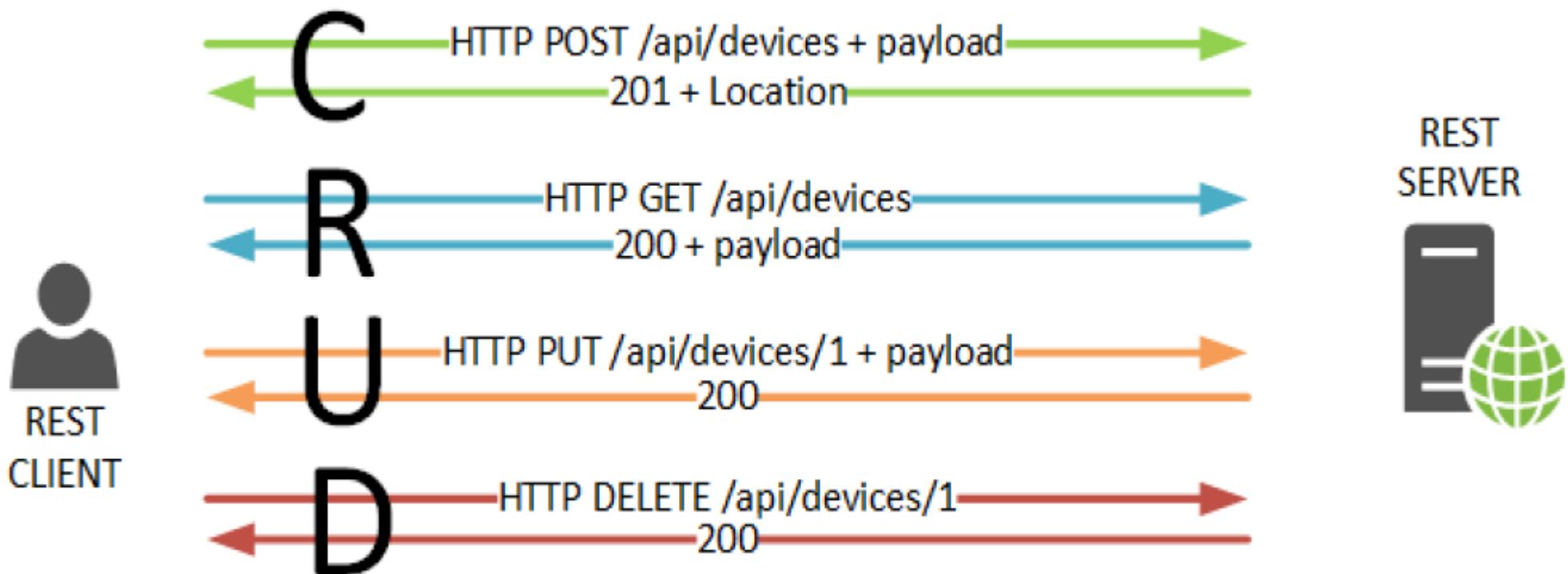
(REST API)

REST – Architecture



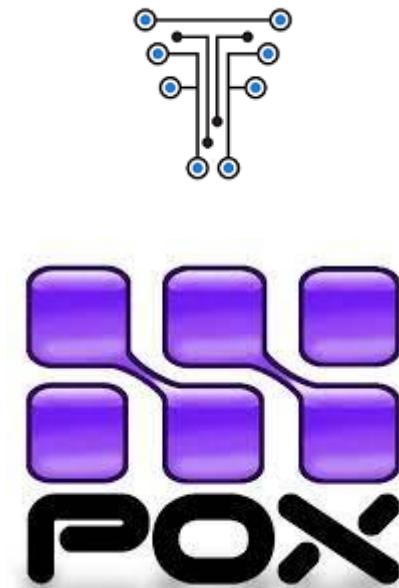
By Ramesh Fadatare (Java Guides)

(REST API???)



(Back to) OpenFlow Controller

- Many existing flavours
 - ONOS – Open Network Operating System
 - <https://opennetworking.org/onos/>
 - TeraFlow SDN
 - <https://tfs.etsi.org>
 - OpenDaylight
 - <https://.opendaylight.org>
 - Floodlight (last version from 2016)
 - <https://floodlight.atlassian.net>
 - NOX (10 w/o maintenance)
 - POX (Python version of NOX w/ some maintenance)
<https://noxrepo.github.io/pox-doc/html/>
 - Ryu (w/o maintenance since 2017)
 - <https://ryu-sdn.org/>
 - Trema (5y since last update)
 - <https://github.com/trema/trema>
 - Frenetic (last release: 2019)
 - <https://github.com/frenetic-lang/frenetic>



Differences between SDN Controllers

- Research vs production
- Programming language
- Performance
- Learning Curve
- User base and Support
- Focus
 - Southbound API Support
 - Northbound API
 - OpenFlow version

A Qualitative and Quantitative assessment of SDN Controllers

Pedro Bispo, Daniel Corujo, Rui L. Aguiar

Instituto de Telecomunicações e Universidade de Aveiro, Portugal
Email: {pedrobispo, rui.laa}@ua.pt; dcorujo@av.it.pt

Abstract—With the increasing number of connected devices, new challenges are being raised in the networking field. Software Defined Networking (SDN) enables a greater degree of dynamism and simplification for the deployment of future 5G networks. In such networks, the controller plays a major role by being able to manage forwarding entities, such as switches, through the application of flow-based rules via a southbound (SB) interface. In turn, the controller itself can be managed by means of actions and policies provided by high-level network functions, via a northbound (NB) interface.

The growth of SDN integration in new mechanisms and network architectures led to the development of different controller solutions, with a wide variety of characteristics. Despite existing studies, the most recent evaluations of SDN controllers are focused only on performance and are not up to date, since new versions of the most popular controllers are constantly being released. As such, this work provides a wider study of several open-source controllers, (namely, OpenDaylight (ODL), Open Network Operative System (ONOS), Ryu and POX), by evaluating not only their performance, but also their characteristics in a qualitative way. Taking performance as a critical issue among SDN controllers, we quantitatively evaluated several criteria by benchmarking the controllers under different operational conditions, using the Cbench tool.

Keywords—Software-Defined Networking, OpenFlow, SDN controller.

reachability optimization towards the users, and the users themselves want overall better service. Simultaneously satisfying involved actors is a highly complex task, whose harmonization is only achieved through careful planning and overprovisioning of networking resources. Nonetheless, the increase in generated data [1] and the need to dynamically adapt to changing situations in a cost-effective way, are demanding for more flexible and adaptive network control mechanisms. As a result, SDN has emerged.

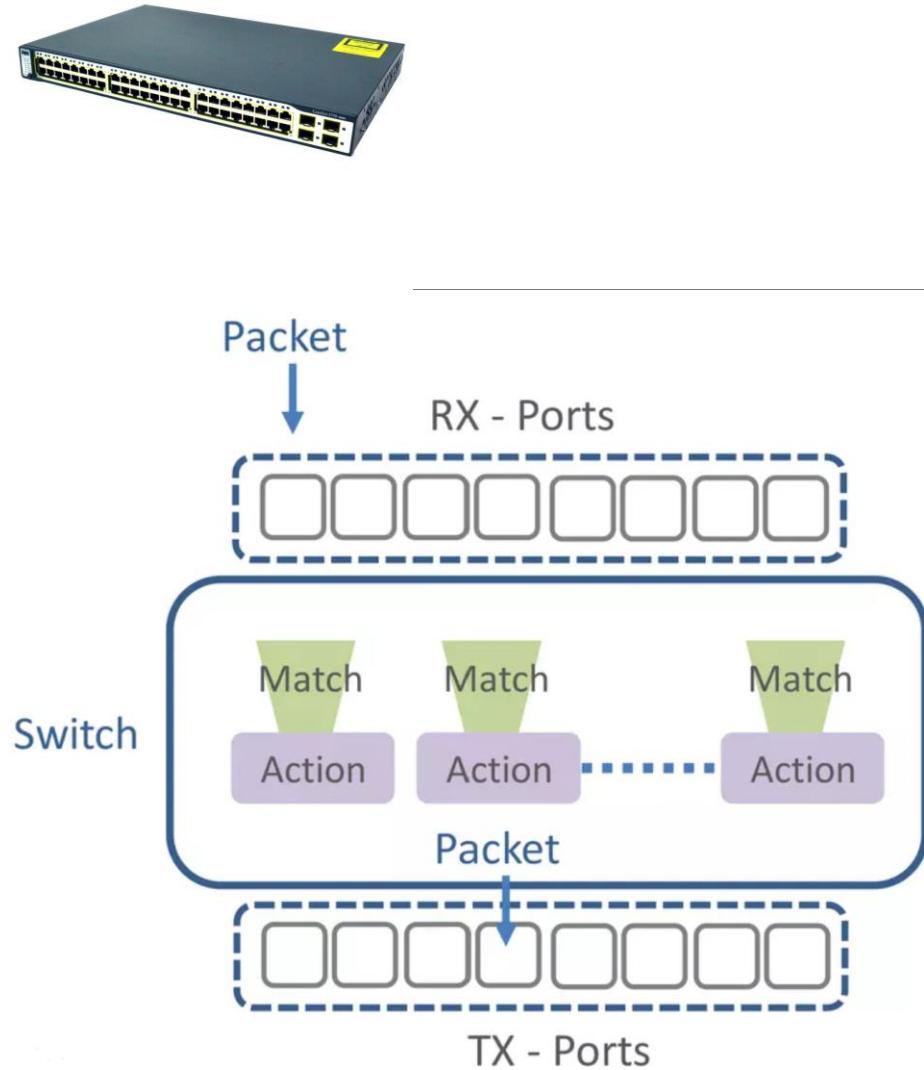
SDN provides the separation of the network control plane from the forwarding plane, allowing more control, adaptability, agility and overall cost reduction. By having a complete view of the network, an SDN controller plays an extremely important role in such networks as it can manage the network structure and services dynamically.

Several SDN controllers exist, with most of them under continuous development. This diversity, which originated from the different needs of operators and research teams that resulted in the development of their own controller versions, made comparison efforts more difficult.

This diversity is evidenced as each controller presents different Northbound (NB) and Southbound (SB) interfaces (which allow it to be interfaced by high-level entities and to control forwarding entities, respectively), development

SDN switch

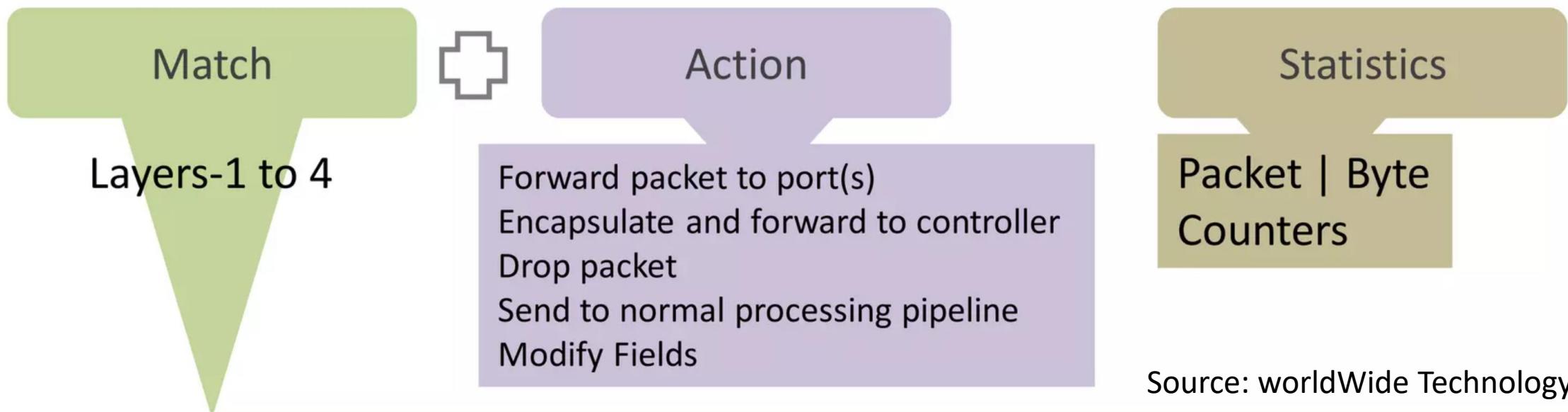
- Has an OpenFlow agent that is able to communicate with the controller
- Processes commands received by the controller
- Dataplane of a switch
 - Ports
 - Flow tables
 - Flows
 - Classifiers (Match)
 - Modifiers and actions
- Packets are matched to flows in flow tables using the match/classifiers
- Flows contain sets of modifiers and actions which are applied to each packet that it matches



Source: worldWide Technology, Inc.

SDN Switch – Flow table

- Each flow table entry contains: Match, Action and counters



Source: worldWide Technology, Inc.



SDN Switch - Flows

- Examples of matching
 - TCP port 80 for a /32 IP address (fine matching)
 - All in ingress port 4 (course matching)
- Matching can be done from layer 1 to layer 4 fields
 - OSI Network Stack model
 - **Layer1:** Input port of the switch
 - **Layer2:** Ethernet (L2 Data)
 - **Layer3:** IP (L3 Network, can be subnet masked)
 - **Layer4:** (L4 Transport, TCP/UDP ports)

SDN Switch - Flows

- Examples
 - TCP proxy
 - All in one
 - Matching
 - OSI Network
 - **Layer 2**
 - **Layer 3**
 - **Layer 4**
 - **Layer 5**
- This allows the SDN Switch to behave like a variety of network devices, such as switch, flow switch, router, firewall...

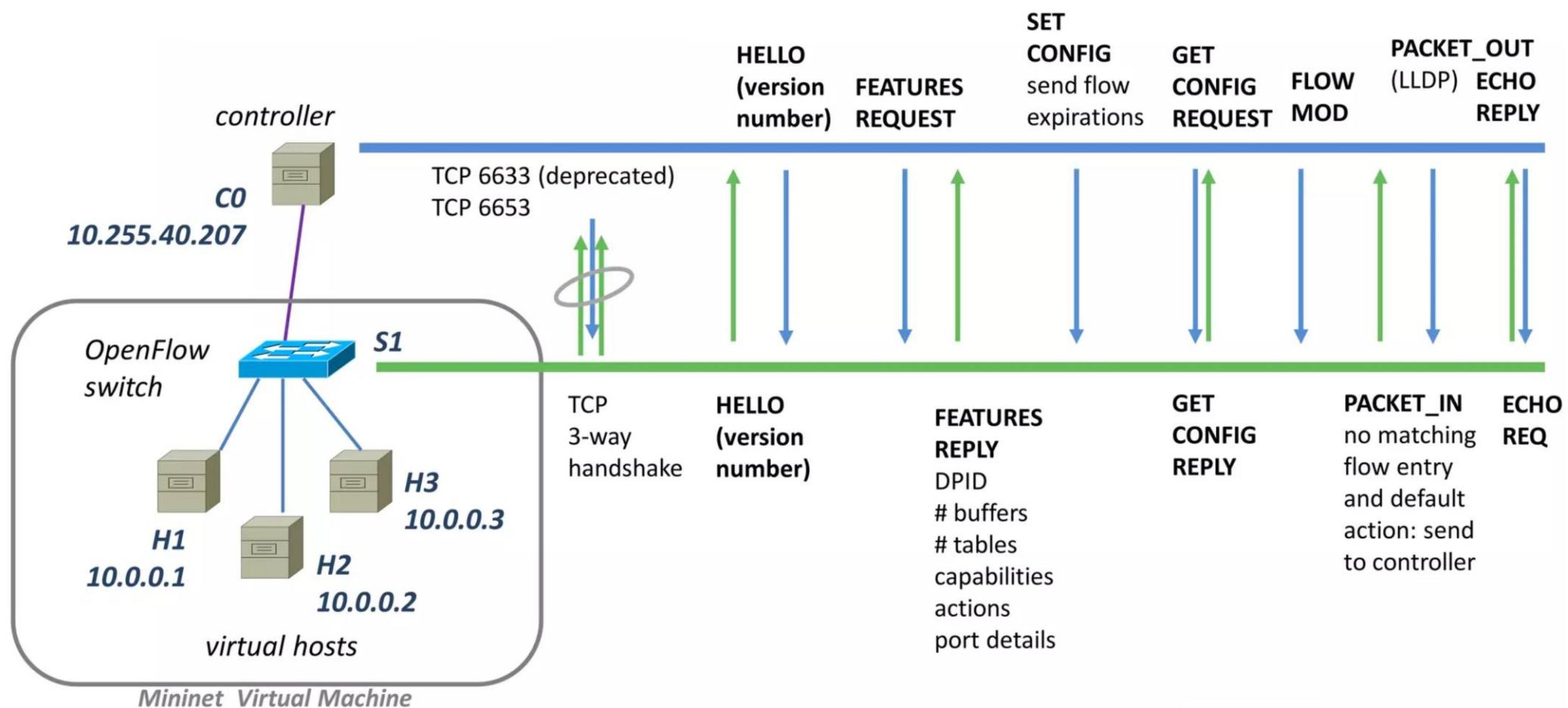
SDN Switch - Actions

- When a switch first connects to a controller, it specifies which actions are supported
 - Not all switches need to implement all OpenFlow actions
- Examples of actions
 - Forward a packet to a set of ports
 - Drop a packet
 - Add, modify or remove VLAN ID or priority on a per-destination-port basis
 - Modify the IP DSCP (i.e., QoS)
 - Modify the destination MAC address
 - Send the packet to the OpenFlow controller (Packet In)
 - Receive the packet from the OpenFlow controller and send it to ports (Packet out)

OpenFlow Protocol

- Supports three types of messages
 - Controller→switch: may not require a response
 - Feature request
 - Configuration
 - Modify state – used to add / delete / modify flows on the switch
 - Asynchronous: switch sends unsolicited message to controller
 - Packet-in
 - Flow removed
 - Symmetric: unsolicited sent by either switch or controller
 - Hello
 - Echo

OpenFlow Switch Start-up example



Source: world wide technology Inc.

Message Details

- Controller <-> Switch Connectivity keep alive
 - ECHO_REQUEST / ECHO_REPLY
- Implement flows into the switch's flow table
 - FLOW_MOD
- Switch acknowledges to the controller that actions were executed
 - BARRIER_REQUEST

Flow insertion into the switch

- Flows can be pre-loaded
 - But this is just like any ordinary non-SDN switch
- SDN supports two other ways, involving interaction between the controller and the switch
 - Reactive
 - Proactive

Reactive flow insertion

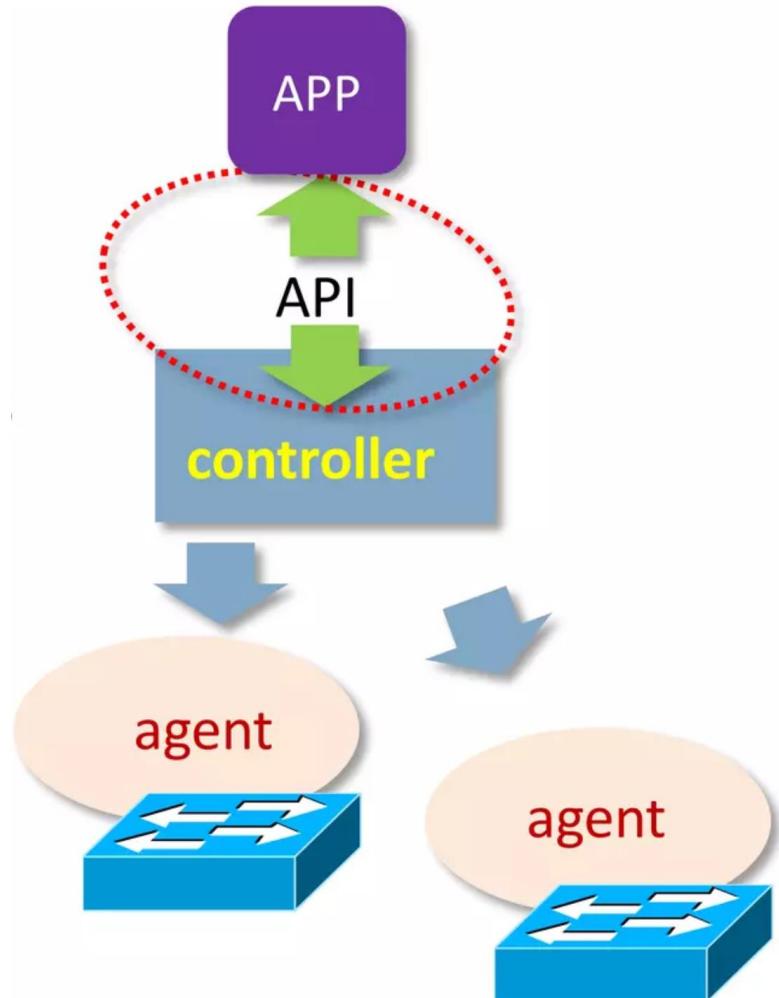
- The flow's first packet is sent to the controller (PACKET_IN)
- The controller analyses the packet. Based on the packet's information and directives present in the controller, the controller sends a FLOD_MOD message to the switch, telling it to insert a flow table entry for the packet
- Subsequent packets (in flow) match the entry until idle or hard timeout
- Loss of connectivity between switch and controller limit utility of switch

Proactive flow insertion

- The controller pre-populates flow table in the switch
- There is zero setup time for new flows
- Loss of connection between switches and the controller does not disrupt network traffic
- Switch in proactive forwarding mode only, would default to action = drop
- Northbound REST API used to populate proactive flows.

How to “direct” the controller?

- Northbound interface allows for Northbound protocols
- Allows applications and orchestration systems to program the network and request services
- Provides a network abstraction interface to applications
- The abstraction is important when managing dissimilar network elements

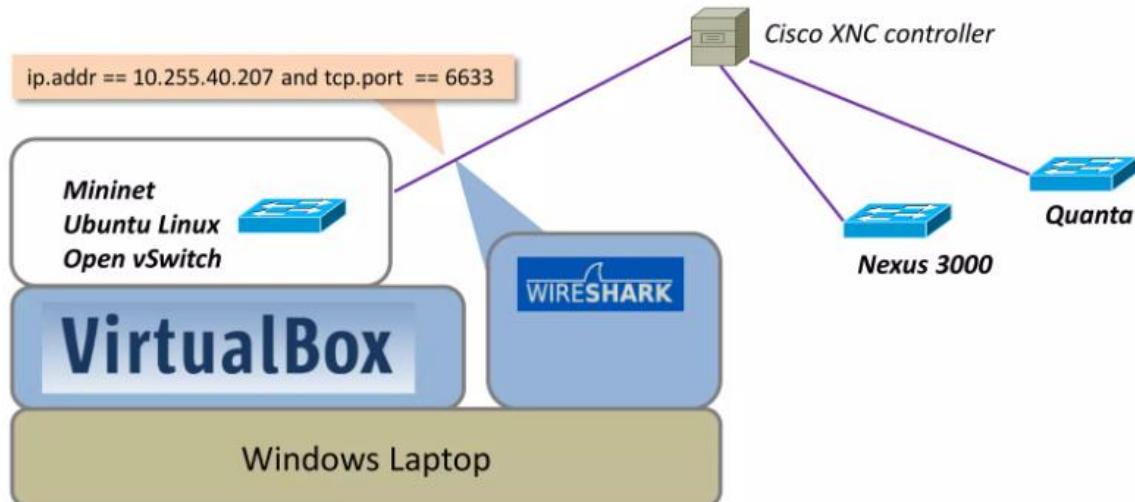


Northbound Protocol Examples

- There is nothing standardized, but there are “types” of protocols used
- REST (web based) API – applications which run on different machine or address space on the controller
- Web Browser
 - `http://<SDN Controller IP>:8080/ ...`
- WebSockets
- OSGi framework is used for applications that will run in the same address space as the controller.
 - Open Service Gateway Initiative

Emulation

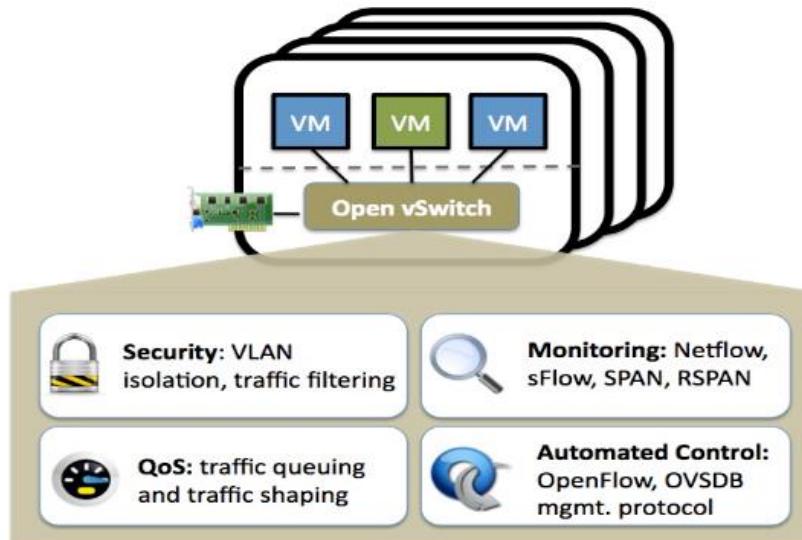
- How to “emulate” many switches easily?
 - Mininet
 - An instant Virtual Network on your Laptop
 - <http://mininet.org/>



Emulation



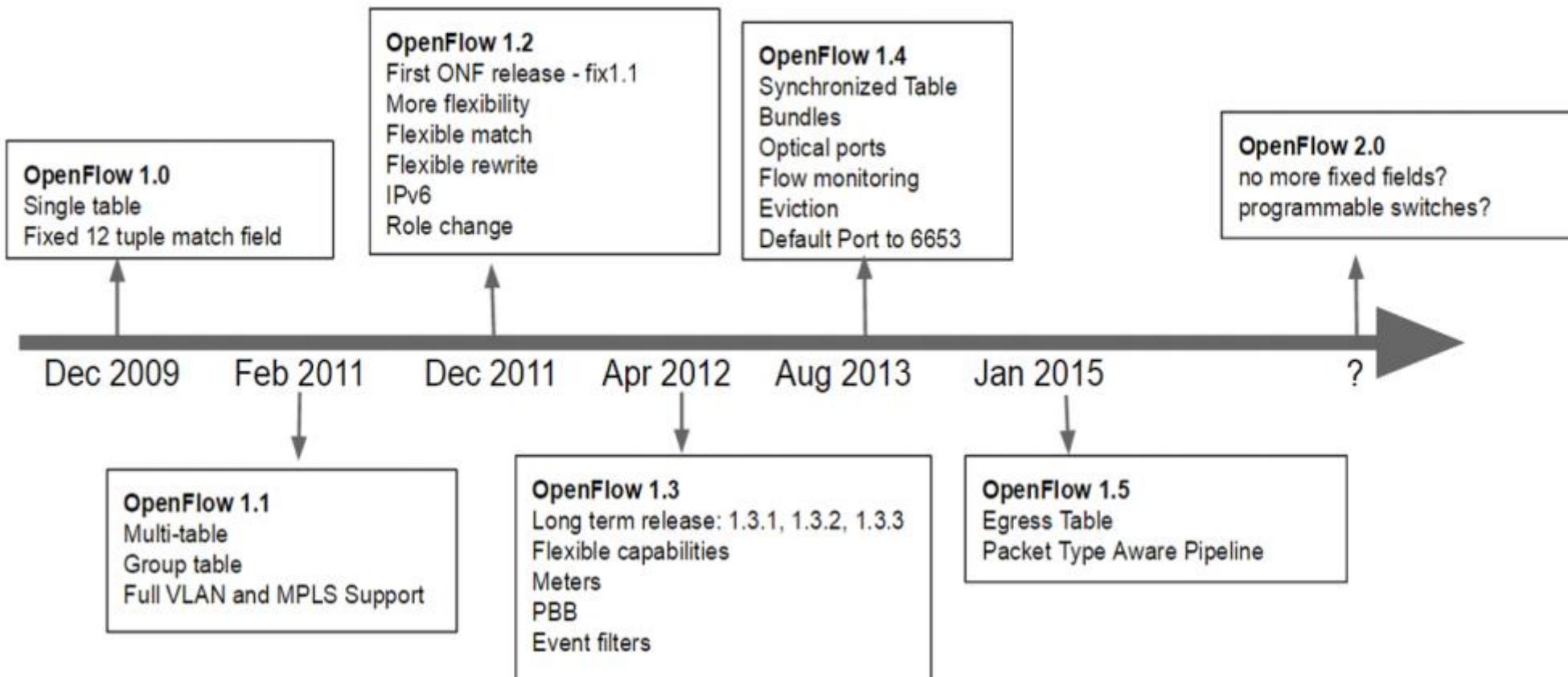
- Open vSwitch
 - <https://www.openvswitch.org/>
- Virtualized switch
- It is used in production environments (i.e., datacenters)
- You can use it in your projects
- Even with Mininet!



OpenFlow evolution

Version	Major Feature	Reason	Use Cases
1.0 - 1.1	Multiple table	Avoid flow entry explosion	
	Group Table	Enable Applying action sets to group of flows	Load balancing, Failover, Link Aggregation
	Full VLAN and MPLS Support		
1.1 - 1.2	OXM Match	Extend matching flexibility	
	Multiple Controller	HA/Load balancing/Scalability	Controller Failover, Controller Load Balancing
1.2 - 1.3	Meter table	Add QoS and DiffServ capability	
	Table miss entry	Provide flexibility	
1.3 - 1.4	Synchronized Table	Enhance table scalability	Mac Learning/Forwarding
	Bundle	Enhance switch synchronization	Multiple switch configuration
1.4 - 1.5	Egress Table	Enabling processing to be done in output port	
	Scheduled bundle	Further enhance switch synchronization	

OpenFlow Evolution



OpenFlow Problems

- It only controlled flow tables, not the switch pipeline
- Fragmentation adoption
 - Different pace in adopting versions
 - The protocol evolves slowly (i.e., slow adoption of new match fields)
 - Optional fields are not mandatory
- Limited tunnel support
- High codebase footprint
- Limited telemetry
- **It wasn't designed to be updated**
- **Lack of intelligence at the dataplane**

Also... new switch hardware appeared

- Terabit per second speed
- Application Specific Integrated Circuit (ASIC)
- But are very hard to program
- Have a custom, vendor-specific interface
- PISA: Flexible Match+Action ASICs
- A new higher-level interface is needed

Idea to solve issues

- Implement flexible mechanisms for
 - parsing packets
 - Matching header fields
 - ... through a common interface
- No longer need to keep extending OpenFlow

Towards the next generation SDN

OpenFlow: Enabling Innovation in Campus Networks

Nick McKeown
Stanford University

Tom Anderson
University of Washington

Hari Balakrishnan
MIT

Guru Parulkar
Stanford University

Larry Peterson
Princeton University

Jennifer Rexford
Princeton University

Scott Shenker
University of California,
Berkeley

Jonathan Turner
Washington University in
St. Louis

This article is an editorial note submitted to CCR. It has NOT been peer reviewed.

Authors take full responsibility for this article's technical content.

Comments can be posted through CCR Online.

ABSTRACT

This whitepaper proposes OpenFlow: a way for researchers to run experimental protocols in the networks they use every day. OpenFlow is based on an Ethernet switch, with an internal flow-table, and a standardized interface to add and remove flow entries. Our goal is to encourage networking vendors to add OpenFlow to their switch products for deployment in college campus backbones and wiring closets. We believe that OpenFlow is a pragmatic compromise: on one hand, it allows researchers to run experiments on heterogeneous switches in a uniform way at line-rate and with high port-density; while on the other hand, vendors do not need to expose the internal workings of their switches. In addition to allowing researchers to evaluate their ideas in real-world traffic settings, OpenFlow could serve as a useful campus component in proposed large-scale testbeds like GENI. Two buildings at Stanford University will soon run OpenFlow networks, using commercial Ethernet switches and routers. We will work to encourage deployment at other schools; and we encourage you to consider deploying OpenFlow in your university network too.

Categories and Subject Descriptors

C.2 [Internetworking]: Routers

General Terms

Experimentation, Design

Keywords

Ethernet switch, virtualization, flow-based

1. THE NEED FOR PROGRAMMABLE NETWORKS

Networks have become part of the critical infrastructure of our businesses, homes and schools. This success has been both a blessing and a curse for networking researchers; their work is more relevant, but their chance of making an impact is more remote. The reduction in real-world impact of any given network innovation is because the enormous installed base of equipment and protocols, and the reluctance

to experiment with production traffic, which have created an exceedingly high barrier to entry for new ideas. Today, there is almost no practical way to experiment with new network protocols (e.g., new routing protocols, or alternatives to IP) in sufficiently realistic settings (e.g., at scale carrying real traffic) to gain the confidence needed for their widespread deployment. The result is that most new ideas from the networking research community go untried and untested; hence the commonly held belief that the network infrastructure has "cristallized".

Having recognized the problem, the networking community is hard at work developing programmable networks, such as GENI [1] a proposed nationwide research facility for experimenting with new network architectures and distributed systems. These programmable networks call for programmable switches and routers that (using virtualization) can process packets for multiple isolated experimental networks simultaneously. For example, in GENI it is envisaged that a researcher will be allocated a *slice* of resources across the whole network, consisting of a portion of network links, packet processing elements (e.g. routers) and end-hosts; researchers program their slices to behave as they wish. A slice could extend across the backbone, into access networks, into college campuses, industrial research labs, and include wiring closets, wireless networks, and sensor networks.

Virtualized programmable networks could lower the barrier to entry for new ideas, increasing the rate of innovation in the network infrastructure. But the plans for nationwide facilities are ambitious (and costly), and it will take years for them to be deployed.

This whitepaper focuses on a shorter-term question closer to home: *As researchers, how can we run experiments in our campus networks?* If we can figure out how, we can start soon and extend the technique to other campuses to benefit the whole community.

To meet this challenge, several questions need answering, including: In the early days, how will college network administrators get comfortable putting experimental equipment (switches, routers, access points, etc.) into their network? How will researchers control a portion of their local network in a way that does not disrupt others who depend on it? And exactly what functionality is needed in network

P4: Programming Protocol-Independent Packet Processors

Pat Bosshart[†], Dan Daly^{*}, Glen Gibb[†], Martin Izzard[†], Nick McKeown[†], Jennifer Rexford^{**}, Cole Schlesinger^{**}, Dan Talayco[†], Amin Vahdat[†], George Varghese[§], David Walker^{**}

[†]Barefoot Networks ^{*}Intel [†]Stanford University ^{**}Princeton University [†]Google [§]Microsoft Research

ABSTRACT

P4 is a high-level language for programming protocol-independent packet processors. P4 works in conjunction with SDN control protocols like OpenFlow. In its current form, OpenFlow explicitly specifies protocol headers on which it operates. This set has grown from 12 to 41 fields in a few years, increasing the complexity of the specification while still not providing the flexibility to add new headers. In this paper we propose P4 as a strawman proposal for how OpenFlow should evolve in the future. We have three goals: (1) Reconfigurability in the field: Programmers should be able to change the way switches process packets once they are deployed. (2) Protocol independence: Switches should not be tied to any specific network protocols. (3) Target independence: Programmers should be able to describe packet-processing functionality independently of the specifics of the underlying hardware. As an example, we describe how to use P4 to configure a switch to add a new hierarchical label.

1. INTRODUCTION

Software-Defined Networking (SDN) gives operators programmable control over their networks. In SDN, the control plane is physically separate from the forwarding plane, and one control plane controls multiple forwarding devices. While forwarding devices could be programmed in many ways, having a common, open, vendor-agnostic interface (like OpenFlow) enables a control plane to control forwarding devices from different hardware and software vendors.

Version	Date	Header Fields
OF 1.0	Dec 2009	12 fields (Ethernet, TCP/IPv4)
OF 1.1	Feb 2011	15 fields (MPLS, inter-table metadata)
OF 1.2	Dec 2011	36 fields (ARP, ICMP, IPv6, etc.)
OF 1.3	Jun 2012	40 fields
OF 1.4	Oct 2013	41 fields

Table 1: Fields recognized by the OpenFlow standard

The OpenFlow interface started simple, with the abstraction of a single table of rules that could match packets on a dozen header fields (e.g., MAC addresses, IP addresses, protocol, TCP/UDP port numbers, etc.). Over the past five years, the specification has grown increasingly more complicated (see Table 1), with many more header fields and

multiple stages of rule tables, to allow switches to expose more of their capabilities to the controller.

The proliferation of new header fields shows no signs of stopping. For example, data-center network operators increasingly want to apply new forms of packet encapsulation (e.g., NVGRE, VXLAN, and STT), for which they resort to deploying software switches that are easier to extend with new functionality. Rather than repeatedly extending the OpenFlow specification, we argue that future switches should support flexible mechanisms for parsing packets and matching header fields, allowing controller applications to leverage these capabilities through a common, open interface (i.e., a new "OpenFlow 2.0" API). Such a general, extensible approach would be simpler, more elegant, and more future-proof than today's OpenFlow 1.x standard.

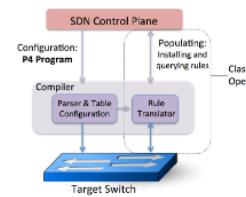


Figure 1: P4 is a language to configure switches.

Recent chip designs demonstrate that such flexibility can be achieved in custom ASICs at terabit speeds [1, 2, 3]. Programming this new generation of switch chips is far from easy. Each chip has its own low-level interface, akin to microcode programming. In this paper, we sketch the design of a higher-level language for Programming Protocol-independent Packet Processors (P4). Figure 1 shows the relationship between P4—used to configure a switch, telling it how packets are to be processed—and existing APIs (such as OpenFlow) that are designed to populate the forwarding tables in fixed function switches. P4 raises the level of abstraction for programming the network, and can serve as a

Programming Protocol-Independent Packet Processors (P4)

- Objectives
 - Reconfigurable
 - Data Plane program can be changed in the field
 - Protocol-Independence
 - No knowledge of low-level hardware organization is required
 - Compiler compiles the program for the target device
 - Architecture dependent – e.g. v1model.p4, p4c-xdp.p4, psa.p4
 - Switch/vendor Independence
 - Consistent Control Plane Interface
 - Control plane APIs are automatically generated by the compiler
 - Community-driven design
 - <https://p4.org>

Programming Protocol-Independent Packet Processors (P4)

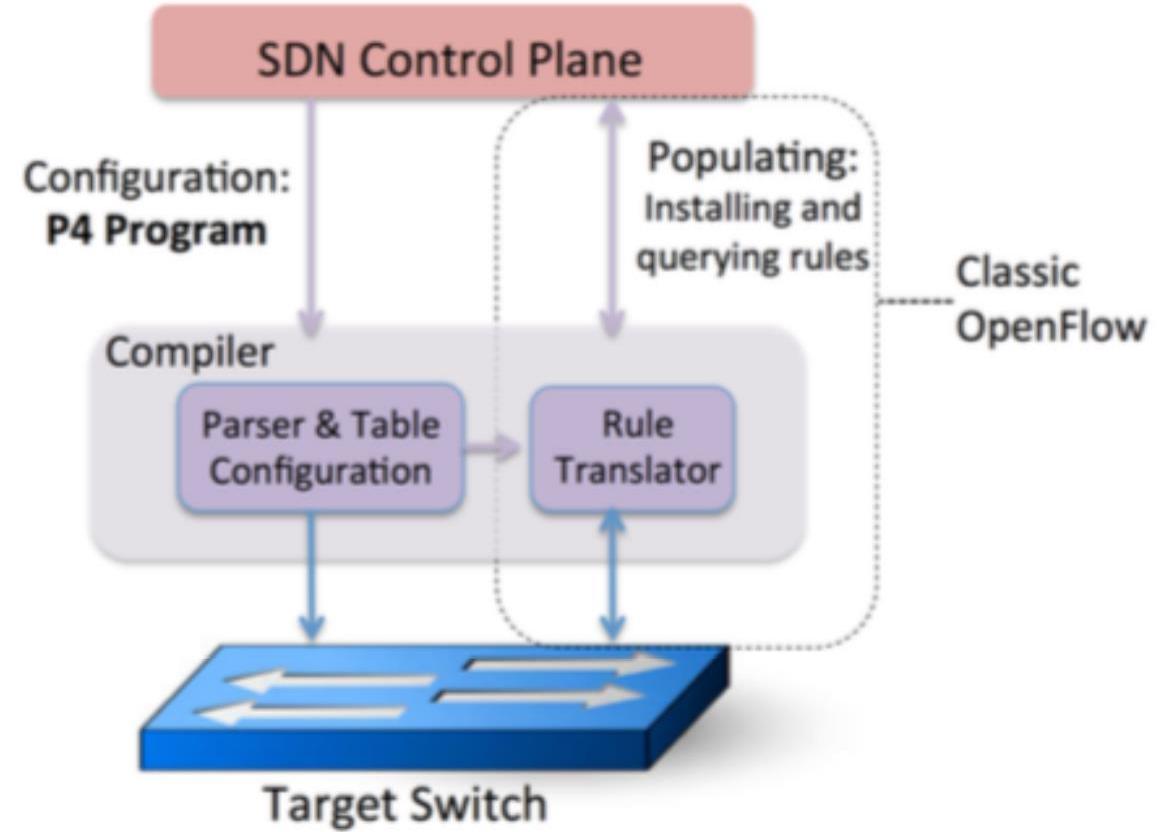
- Benefits
 - New features: add new protocols
 - Reduce complexity: remove unused protocols
 - Efficient use of resources – flexible use of tables
 - Greater visibility – new diagnostic techniques, telemetry, etc.
 - Software style development – rapid design cycle, fast Innovation, fix data plane bugs in the field
 - You keep your own ideas!

Programming Protocol-Independent Packet Processors (P4)

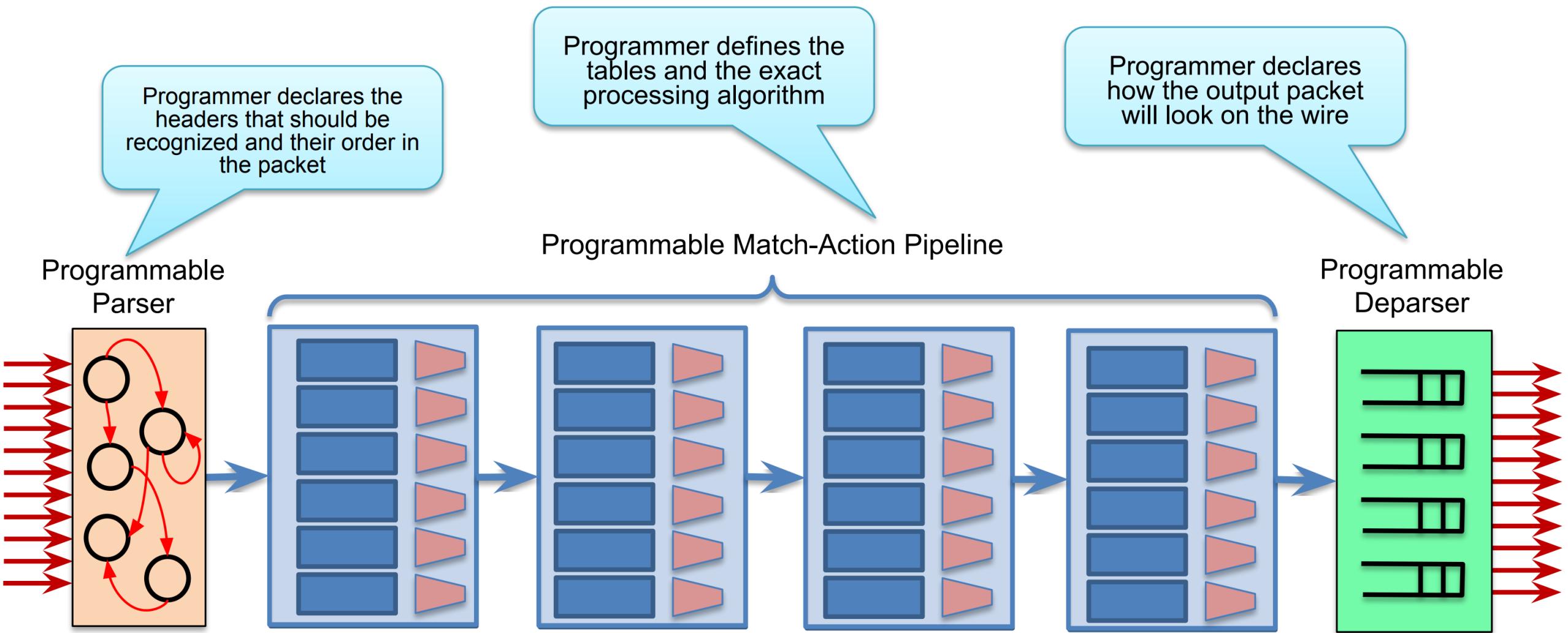
- Evolution
 - P4_14
 - Original version of the language
 - Assumed specific device capabilities
 - Good only for a subset of programmable switch/targets
 - P4_16
 - More mature and stable language definition
 - Does not assume device capabilities, which instead are defined by target manufacturer via external libraries/architecture definition
 - Good for many targets, e.g., switches and NICs, programmable or fixed-function

Programming Protocol-Independent Packet Processors (P4)

- P4 program is a high-level programm that configures forwarding behavior (abstract forwarding model)
- P4 compiler generates the low-level code to be executed by the desired target
- OpenFlow can still be used to install and query rules once forwarding model is defined
- Allows the definition of arbitrary headers and fields



Architecture of a programmable switch



P4 Header and Fields

- Fields have a bit width and other attributes
- Headers are collections of fields
 - Like an instantiated class in Java

```
header_type ethernet_t {
    fields {
        dstAddr      : 48;
        srcAddr      : 48;
        etherType    : 16;
    }
}

/* Instance of eth header */
header ethernet_t inner_ethernet;    metadata egress_metadata_t egress_metadata;
```

```
header_type egress_metadata_t {
    fields {
        nhop_type   : 8; /* 0: L2, 1: L3, 2: tunnel */
        encaps_type : 8; /* L2 Untagged; L2ST; L2DT */
        vniid       : 24; /* gnve/vxlan vniid/gre key */
        tun_type    : 8; /* vxlan; gre; nvgre; gnve*/
        tun_idx     : 8; /* tunnel index */
    }
}
```

Parser

- Extracts header instances
- Selects a next “state” by returning another parser function

```
parser parse_ethernet {
    extract(ethernet);
    return select(latest.etherType) {
        ETHERTYPE_CPU    : parse_cpu_header;
        ETHERTYPE_VLAN   : parse_vlan;
        ETHERTYPE_MPLS   : parse_mpls;
        ETHERTYPE_IPV4   : parse_ipv4;
        ETHERTYPE_IPV6   : parse_ipv6;
        ETHERTYPE_ARP    : parse_arp_rarp;
        ETHERTYPE_RARP   : parse_arp_rarp;
        ETHERTYPE_NSH    : parse_nsh;
    }
}
```

Match + Action table

- Parsed representation of headers gives context for processing of the packets
- An action function consists of several primitive actions

```
table acl {  
    reads {  
        ipv4.dstAddr : ternary;  
        ipv4.srcAddr : ternary;  
        ipv4.protocol : ternary;  
        udp.srcPort : ternary;  
        udp.dstPort : ternary;  
        ethernet.dstAddr : exact;  
        ethernet.srcAddr : exact;  
        ethernet.etherType : ternary;  
    }  
    actions {  
        no_op; /* permit */  
        acl_drop; /* reject */  
        nhop_set; /* policy-based routing */  
    }  
}
```

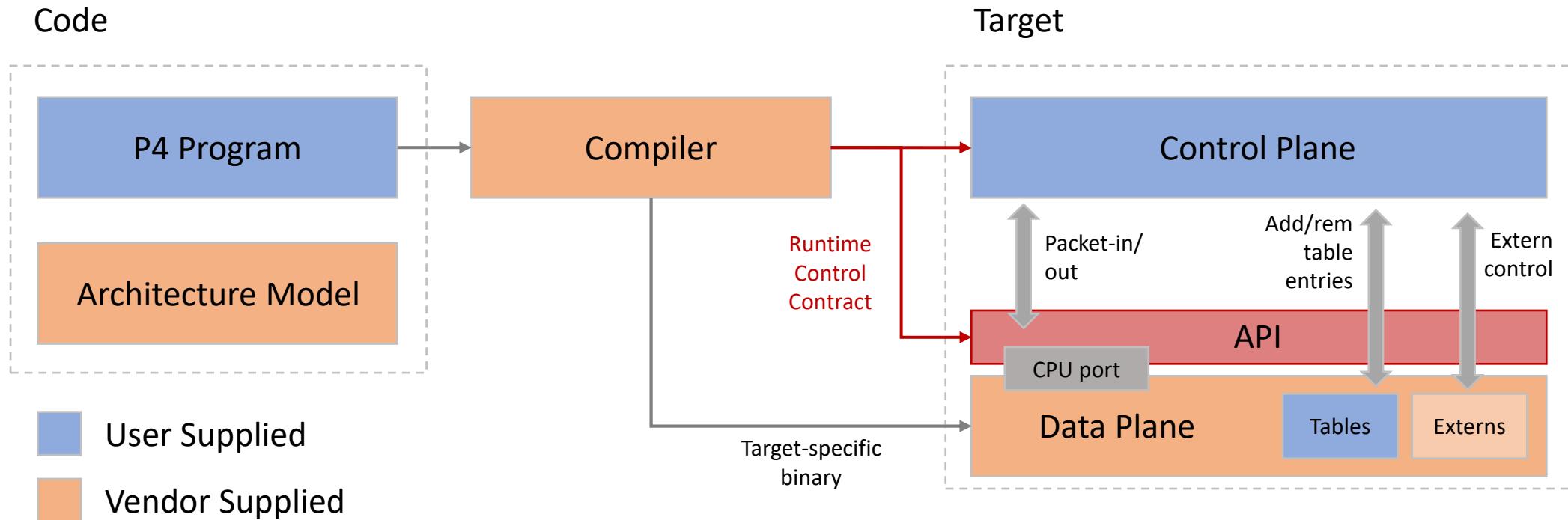
Match semantics

- **exact**
 - port_index : exact
- **ternary**
 - ethernet.srcAddr : ternary
- **valid**
 - vlan_tag[0] : valid
- **lpm**
 - ipv4.dstAddr : lpm
- **range**
 - udp.dstPort : range

Primitive actions

- modify_field, add_to_field, add, set_field_to_hash_index
- add_header, remove_header, copy_header
- push, pop
- count, meter
- generate_digest, truncate
- resubmit, recirculate
- clone_*
- no_op, drop

Programming a target



P4Runtime

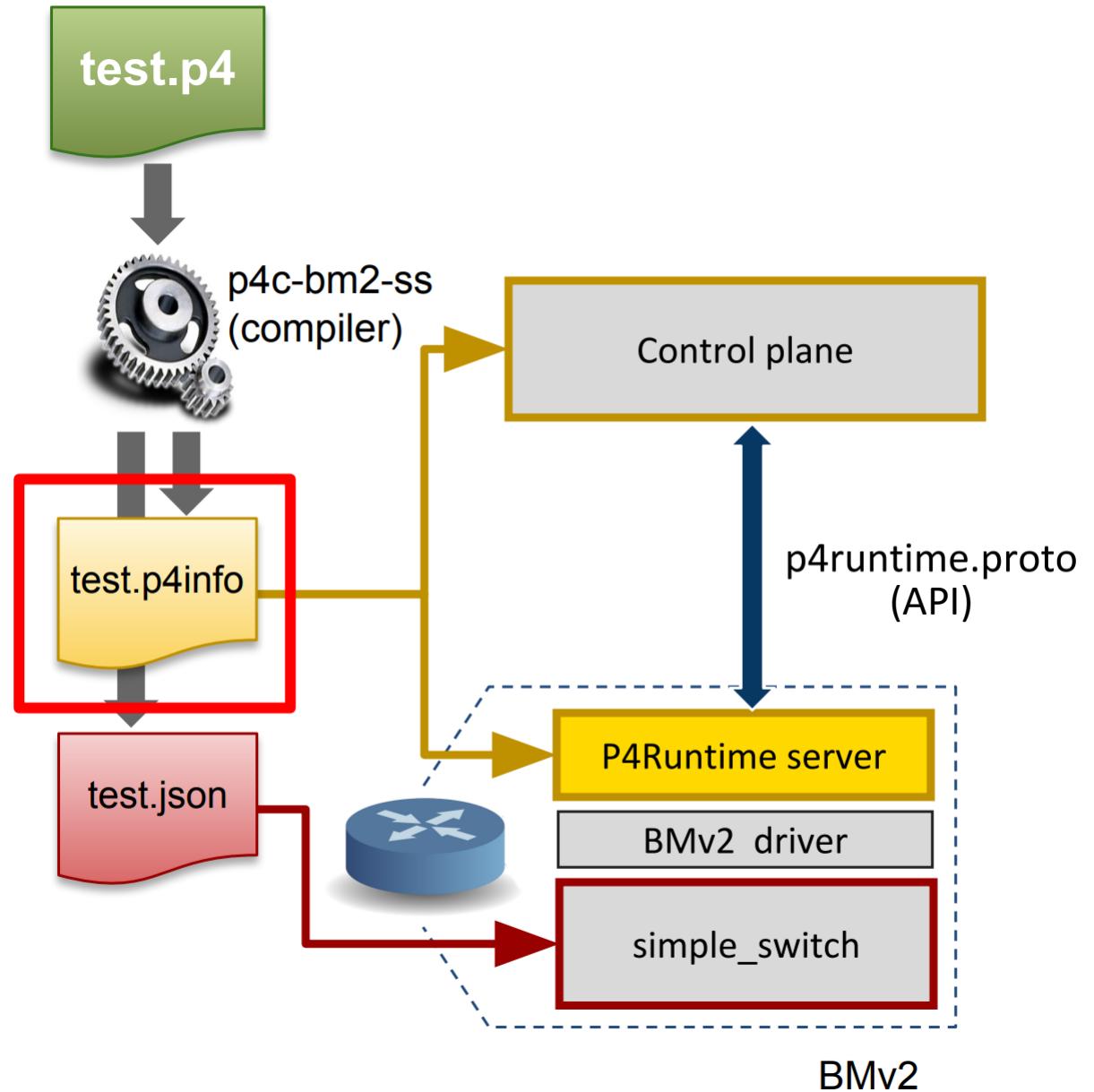
- Framework for runtime control of P4-defined data planes
 - Open-source API and a server implementation
- P4 program-independent
 - API doesn't change with the P4 program
- Enables field-reconfigurability
 - Ability to push new P4 program without recompiling the software stack of target switches
- API based on protobuf (serialization) and gRPC (cliente/server transport)
 - Makes it easy to implement a P4Runtime cliente/server by auto-generating code for different languages
- P4Info as a contract between control and data plane
 - Generated by P4 compiler
 - Needed by the control plane to format the body of P4Runtime messages

P4 and P4Runtime are two different things

- P4
 - Programming language used to define how a switch processes packets
 - Specifies the switch pipeline
 - Which fields does it match upon?
 - What actions does it perform on the packets?
 - In which order does it perform the matches and actions
 - Specify the behavior of an existing device
 - Specify a logical abstraction for the device
- P4Runtime
 - An API used to control switches whose behavior has already been specified in the P4 language
 - Works for different types of switches
 - Fixed
 - Semi-programmable
 - Fully programmable

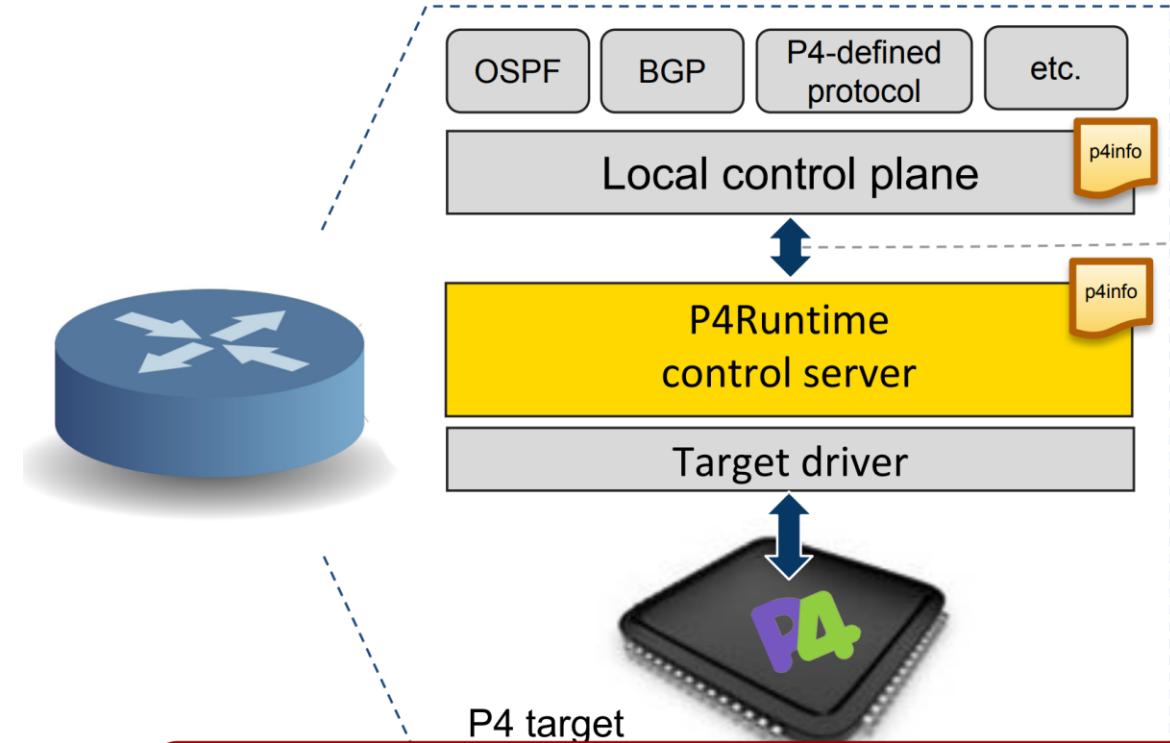
P4Runtime

- P4 compiler generates 2 outputs:
 - Target specific binary
 - Used to realize switch pipeline (i.e., binary config for specific target/switch)
 - P4Info file
 - “Schema” of pipeline for runtime control
 - Captures P4 program attributes such as tables, actions, parameters, etc.
 - Protobuf-based format
 - Target-independent compiler output
 - Same P4Info for different targets

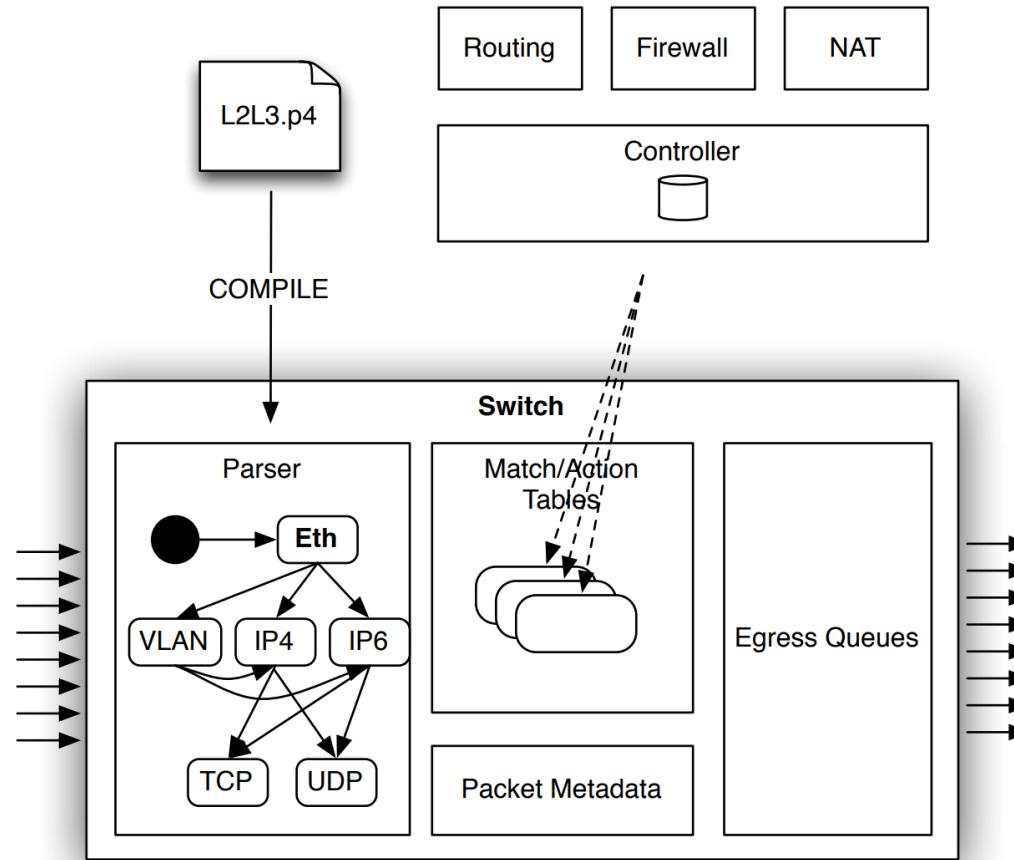


P4Runtime

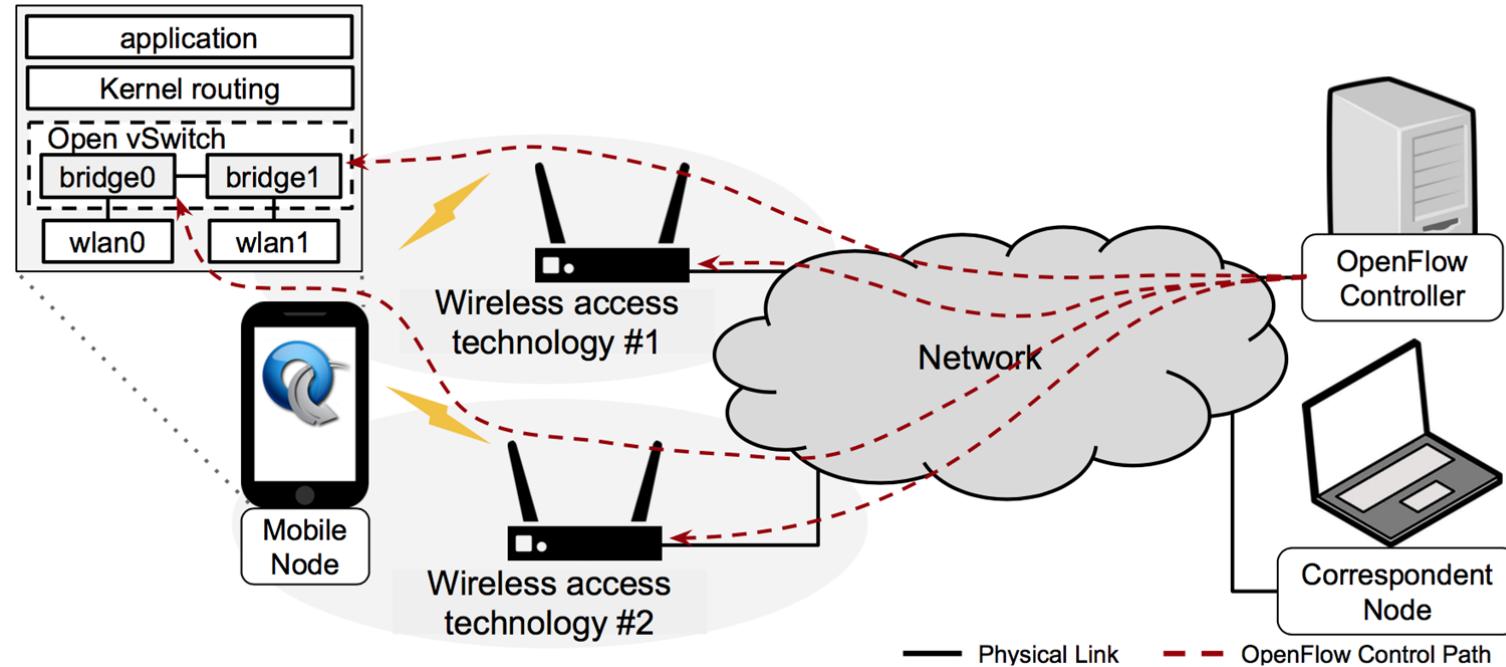
- The p4info file is used by a remote or local control plane
- This capability takes advantage of the fact that the p4info generates the same target-independent protobuf format
 - API between client and server



P4 Forwarding Model / Runtime

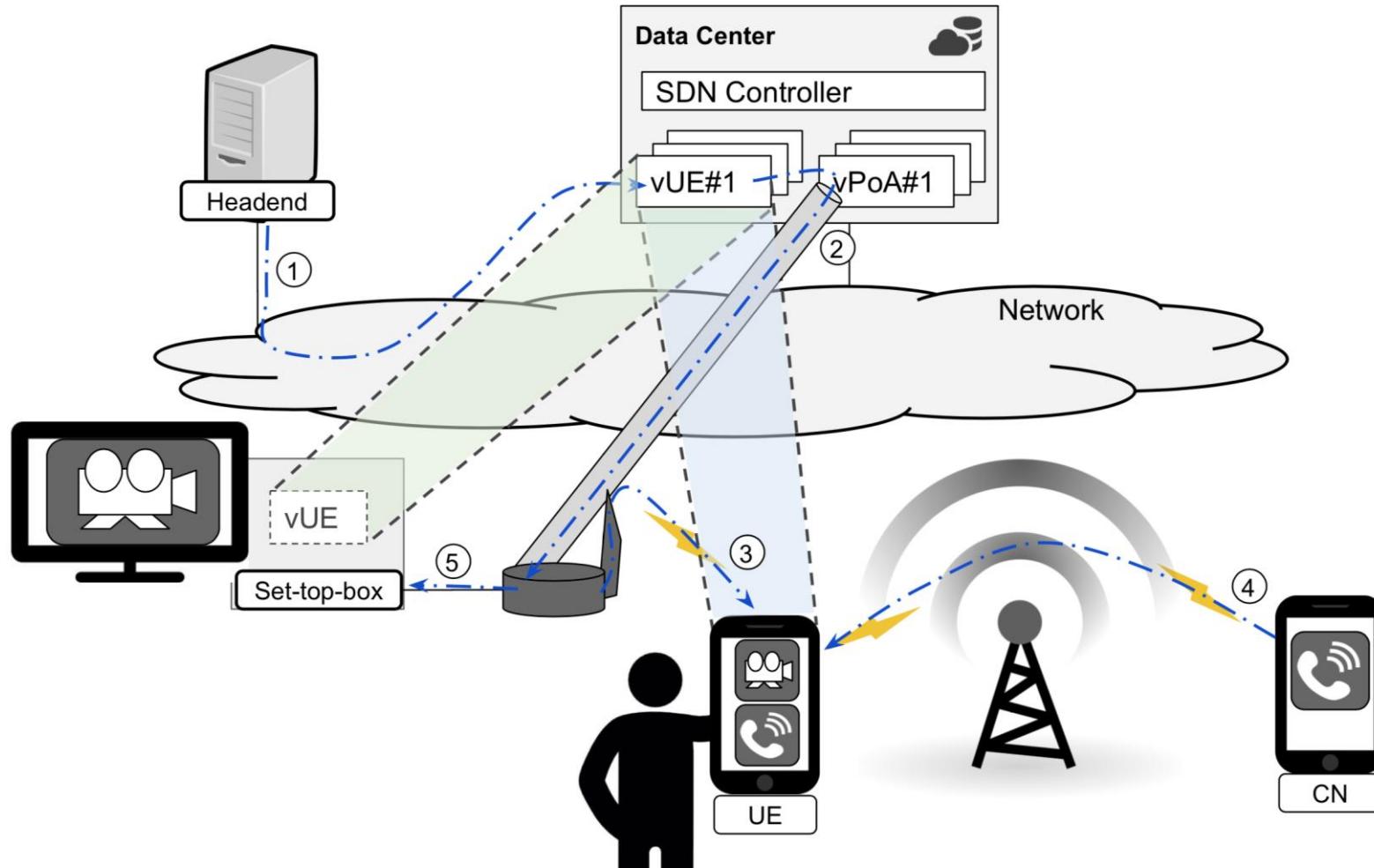


SDN+NFV - SDN in Wireless Environments (all the way to the terminal)



Source: F. Meneses, C. Guimarães, D. Corujo, R. Aguiar “SDN-based Mobility Management: Handover Performance Impact in Constrained Devices”, 9th IFIP NTMS, Paris, February 2018

Connectionless environments

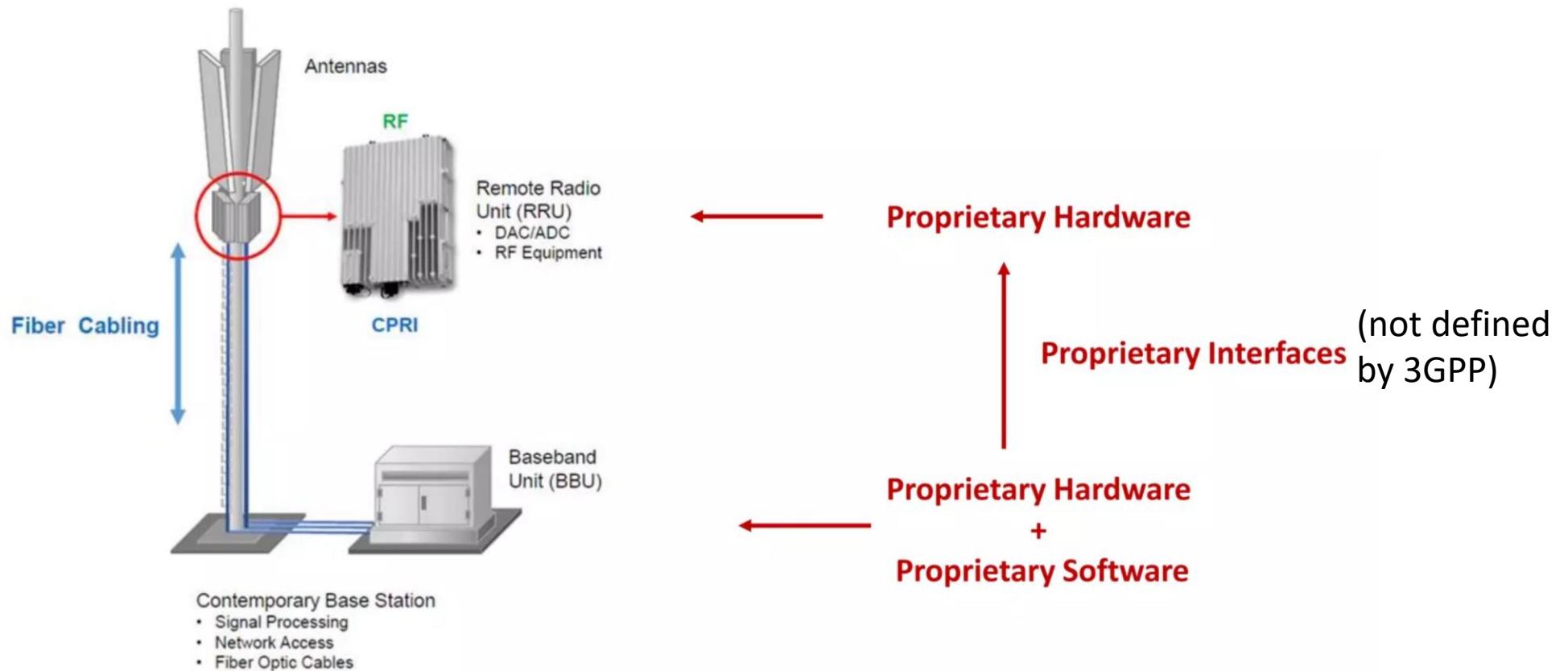


OpenRAN

Open RAN vs OpenRAN

- Open RAN (or O-RAN)
 - From the O-RAN Alliance
 - Aims to define open interfaces of split RAN architecture
 - Open and Virtualized RAN (vRAN)
- OpenRAN
 - From Telecom Infra Project
 - Aims to disintegrate mobile network RAN architecture
 - By having multi-vendor interoperable solutions
 - Built on general purpose COTS
 - Aims to speed up adoption and deployments
 - Uses O-RAN's interfaces
 - Works with 3GPP, ONF, ...

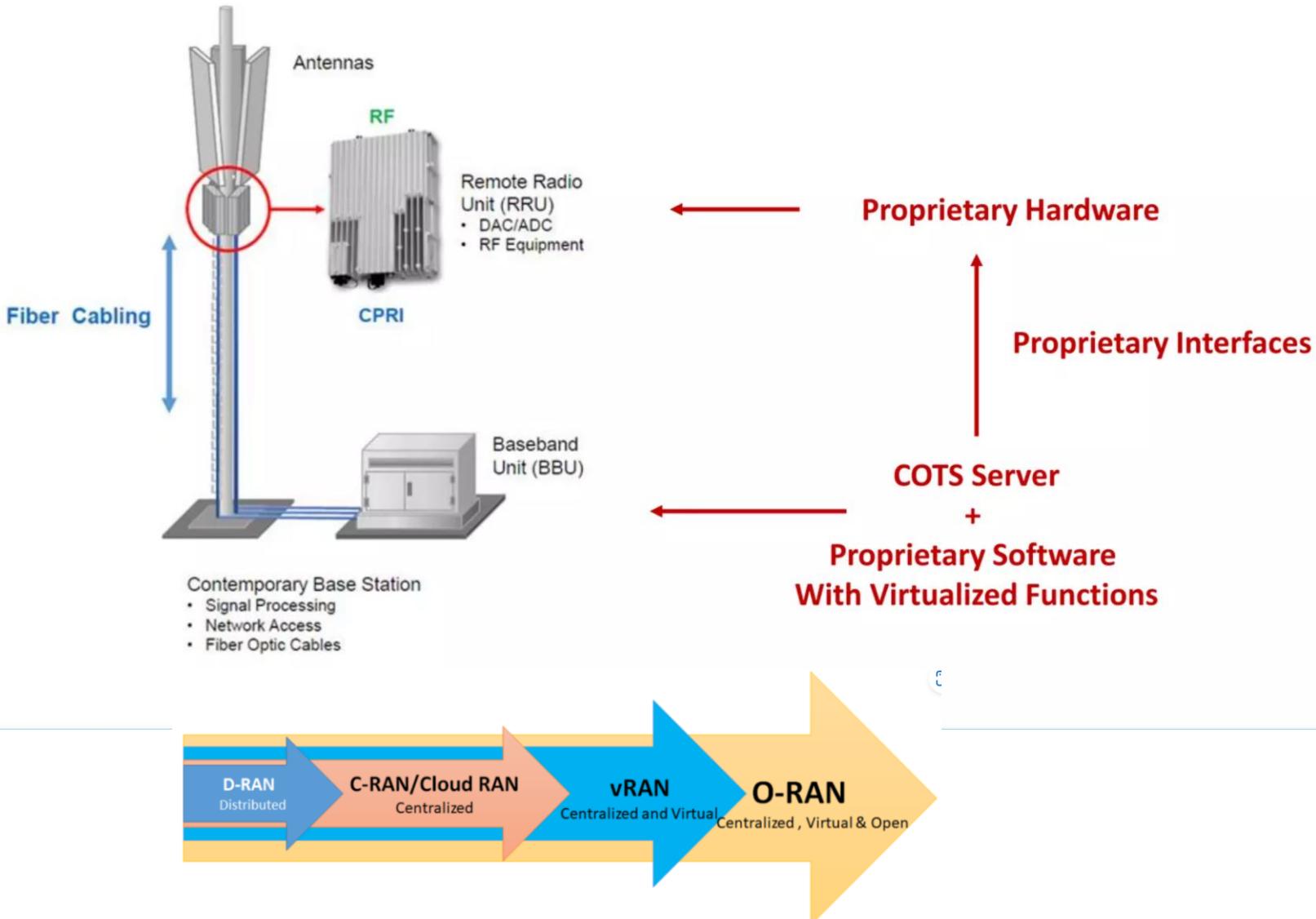
Contemporary RAN



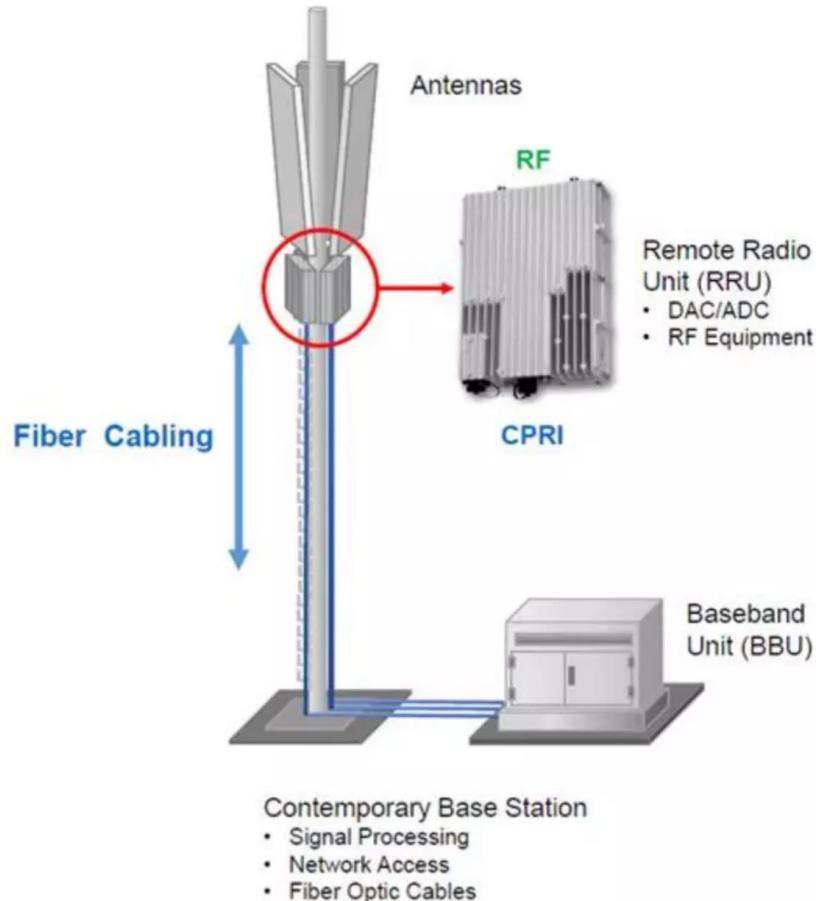
Operators need to buy both RRU and BBU from the same vendor!

5G NSA X2 interface (BBU<->BBU) w/ 4G Core: 4G and 5G same vendor!

Virtualized RAN (vRAN) approach



OpenRAN vision



GPP based COTS Hardware (SDR)
Can be purchased from any ODM / OEM / RAN Hardware Vendor

Open Interface
Any vendor software can work
on this hardware

COTS Server
+
**Proprietary Software
With Virtualized Functions**

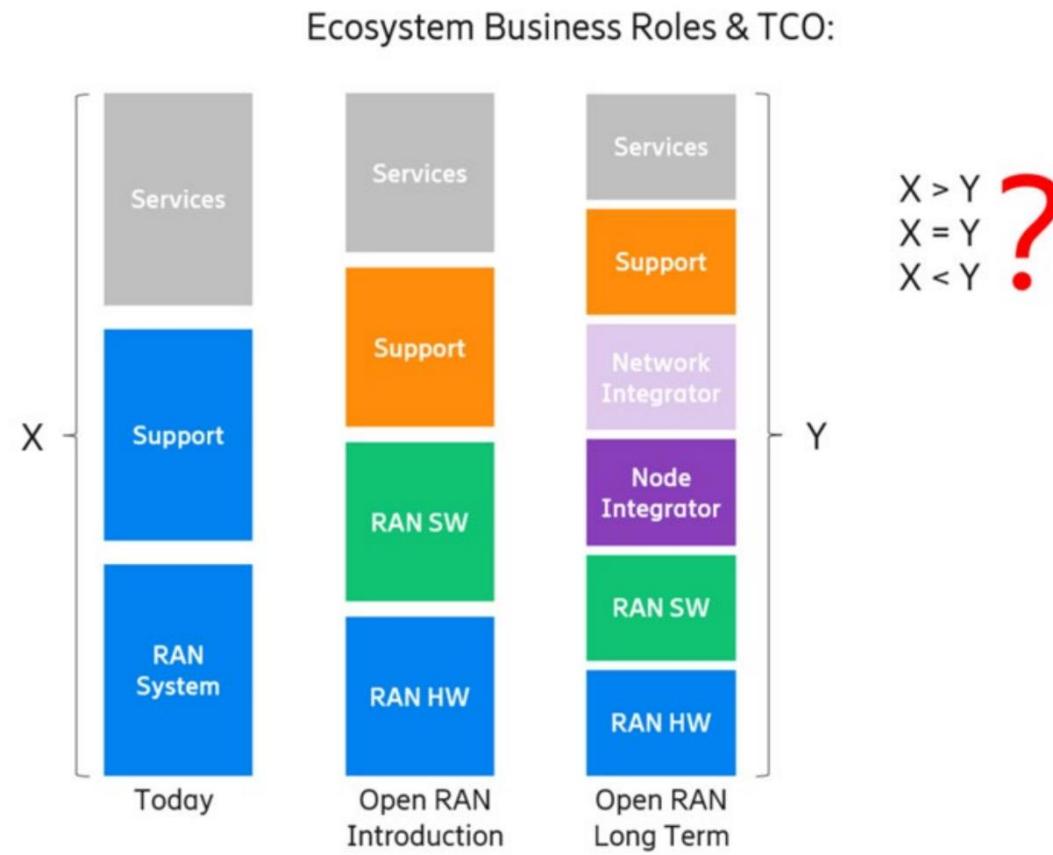
OpenRAN benefits

- Avoid Vendor lock-in
- Reduce cost
- Quick time to market
- Best of breed
- Spur Innovation
- Participate in HW/SW development

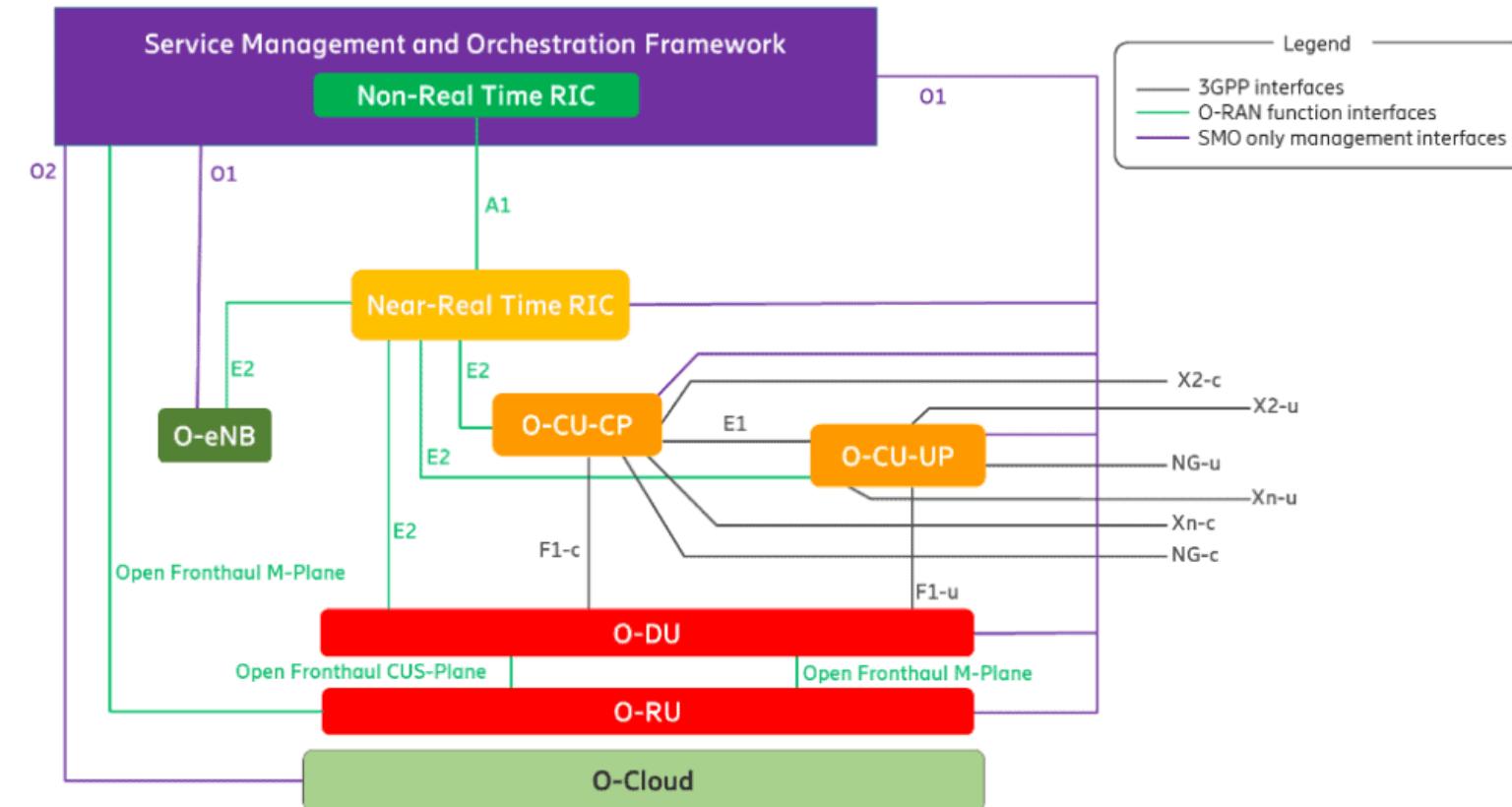
OpenRAN Challenges

- New HW and SW requirements
- Interoperability
- Complex automation
- Virtualization security
- Reliability and Availability
- High fronthaul bandwidth low-latency

Ecosystem and Business Roles

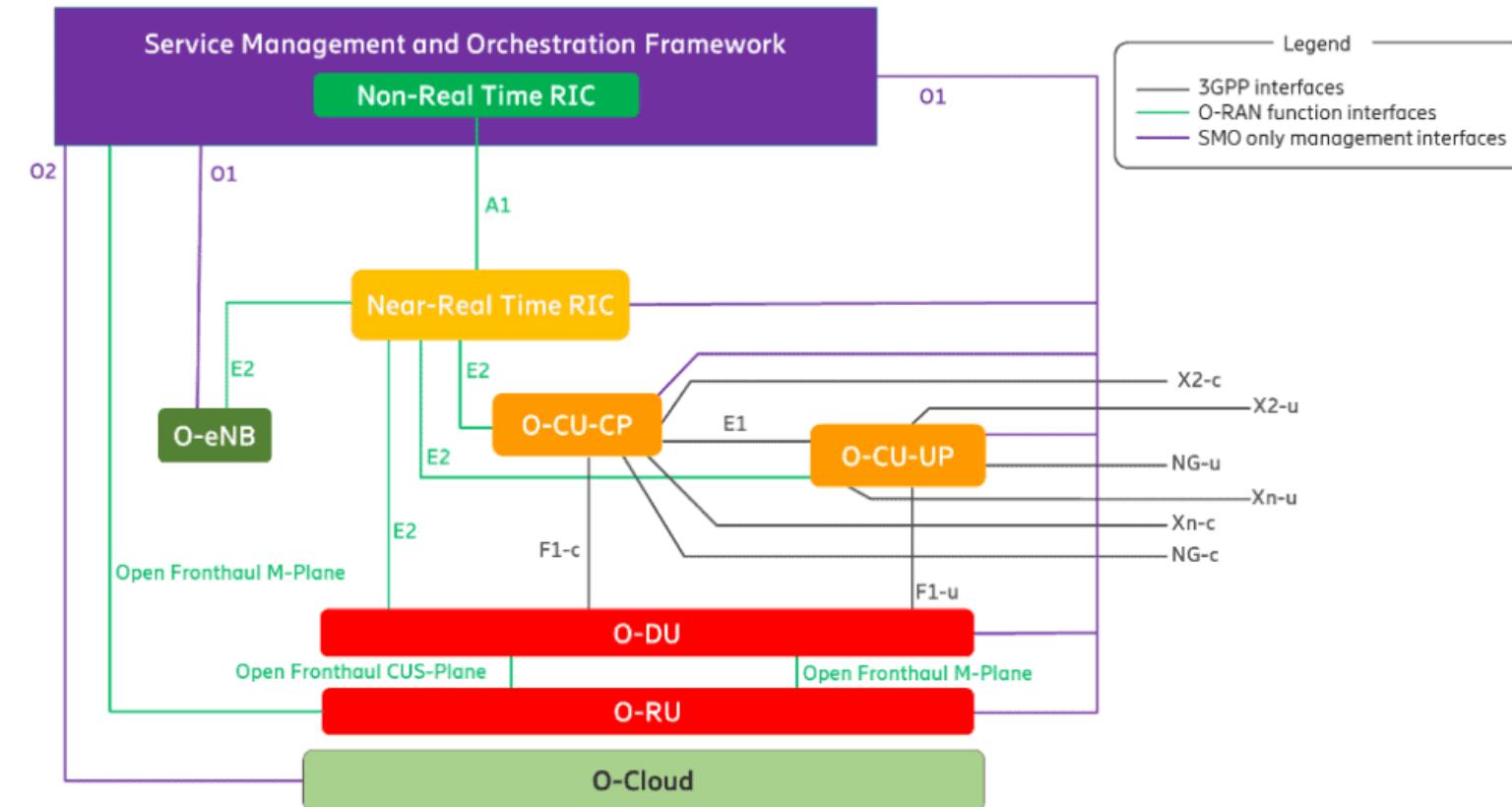


Logical Open RAN Architecture



- RIC → RAN Intelligent Controller
- Non-RT RIC
 - FCAPS of O-RAN network functions
 - Fault, configuration, accounting, performance and security
 - RAN optimization in Non-RT (>1 second)

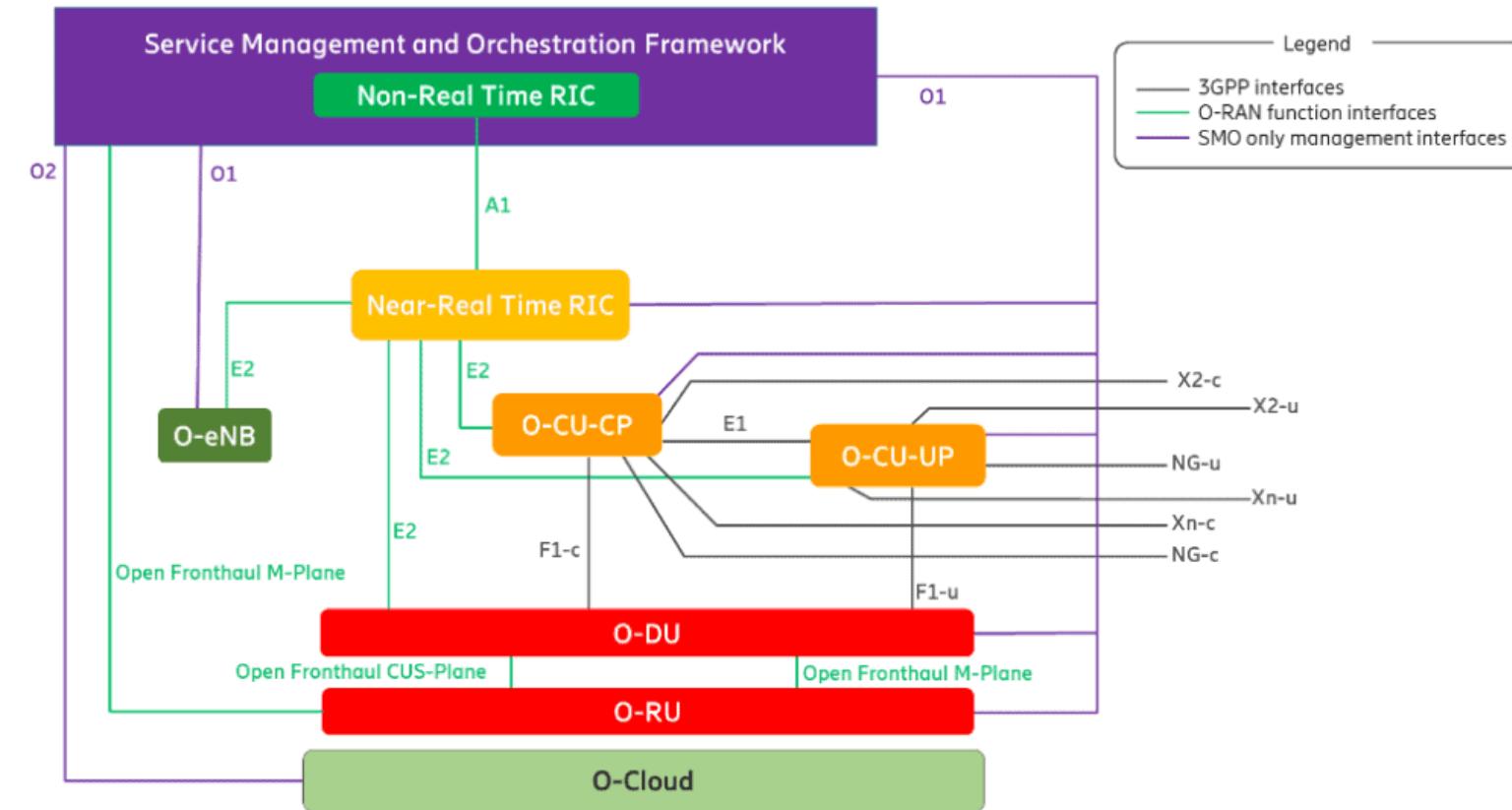
Logical Open RAN Architecture



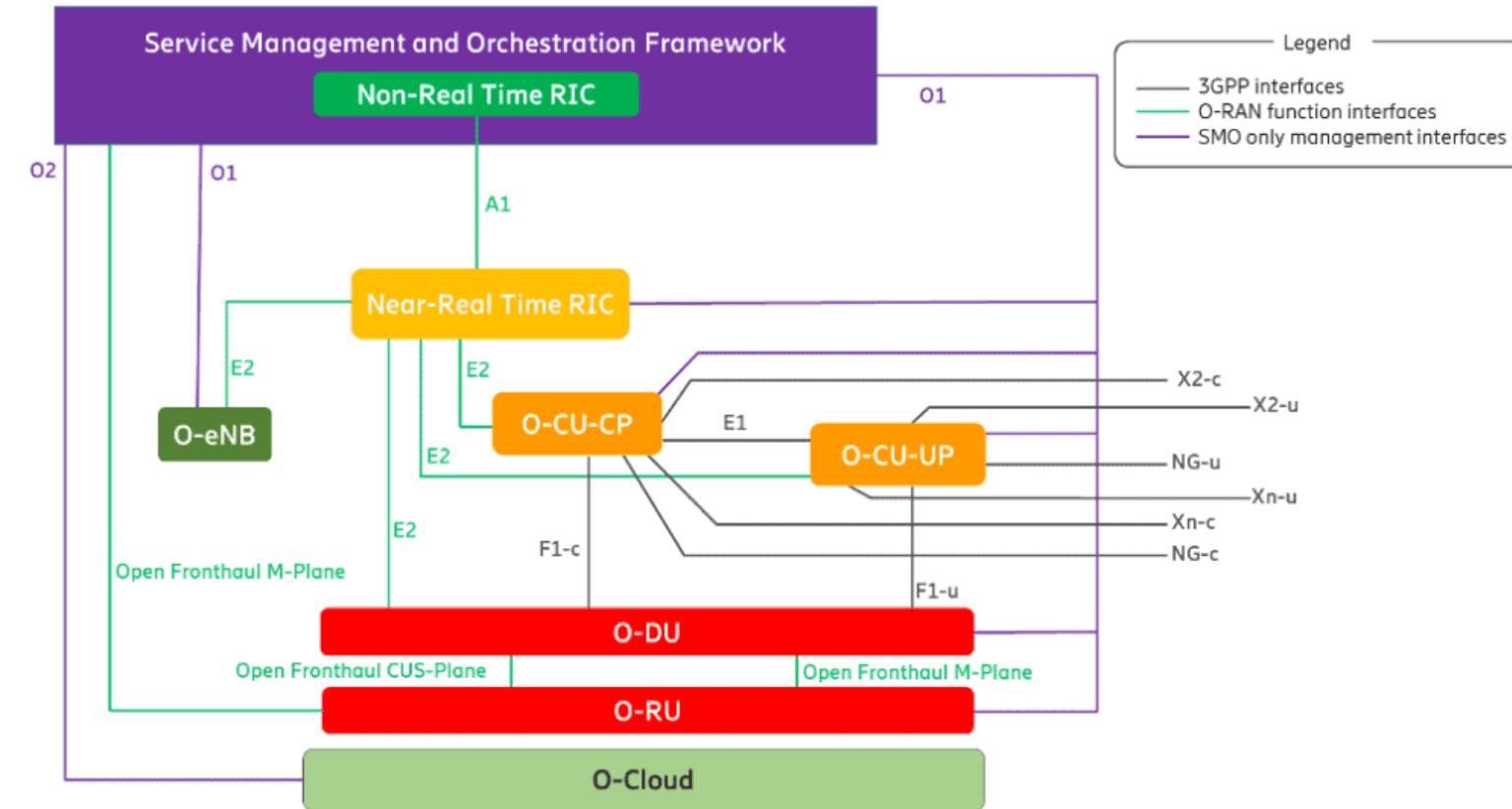
- **Near-RT RIC**

- Enables near-time control and optimization of O-RAN nodes (10ms to 1 sec)
 - O-CU
 - Centralized Unit
 - O-DU
 - Distributed Unit
- Here, decision latency is very important, thus has to be closer to the ran nodes

Logical Open RAN Architecture

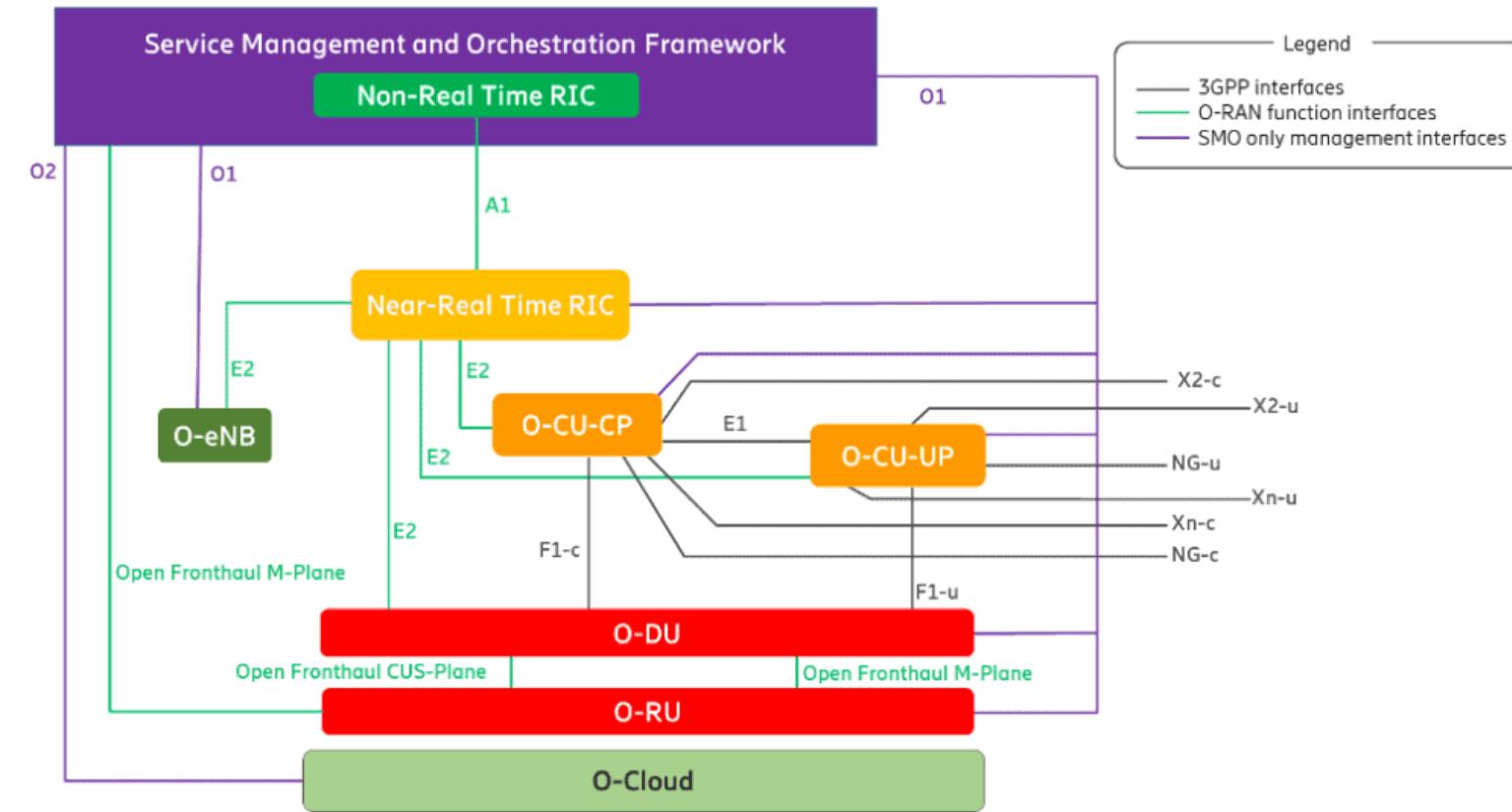


Logical Open RAN Architecture



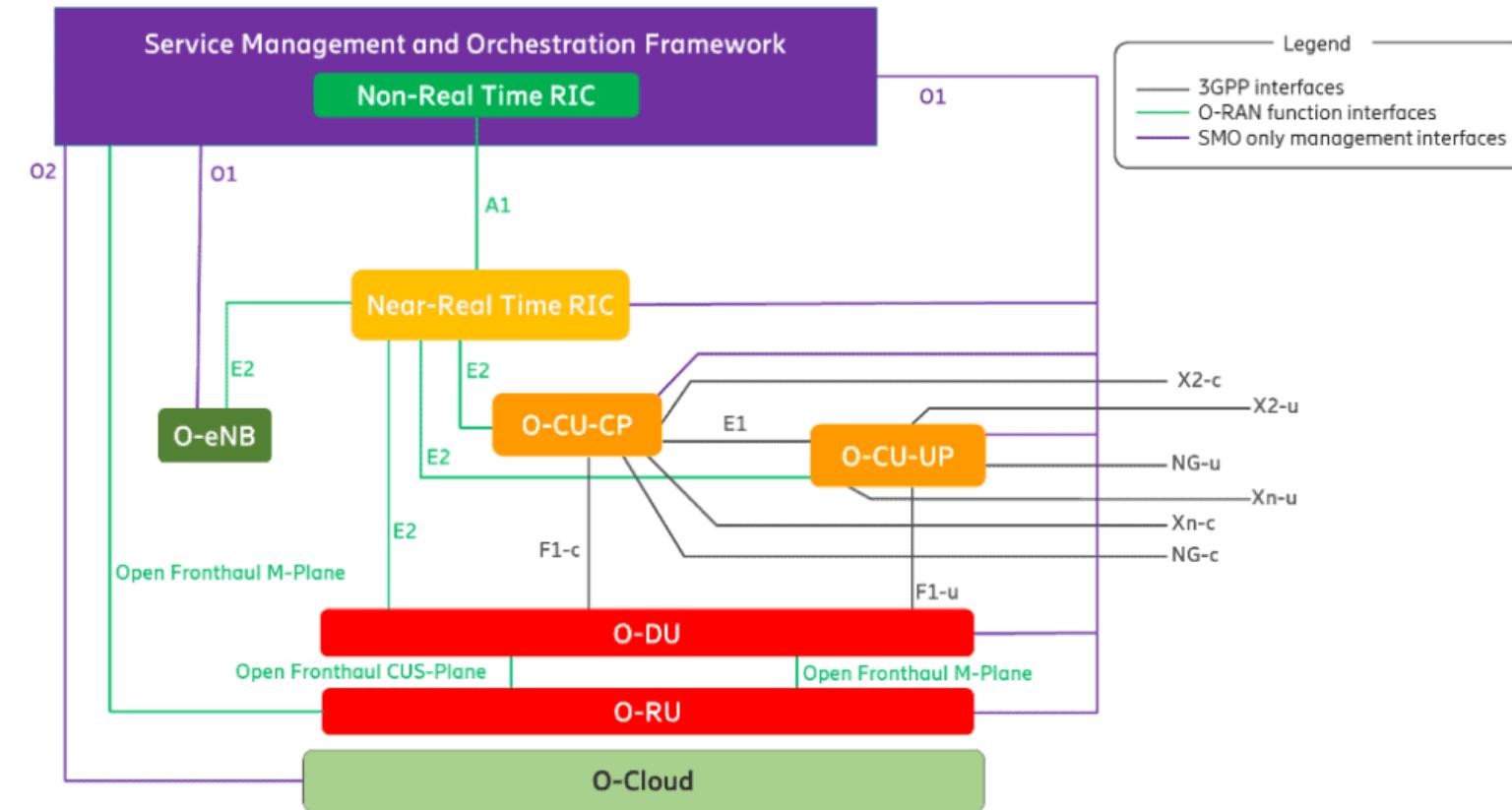
- **O-DU**
 - Open Distributed Unit
 - Terminates the fronthaul interface
 - Logical node hosting High-PHY layers based on a lower layer functional split

Logical Open RAN Architecture



- **O-CU-CP and O-CU-UP**
 - O-RAN Central Unit
 - Control Plane (CP)
 - User Plane (UP)
 - CP
 - Hosts the RRC (Radio Resource Control) and the control plane part of the PDCP (Packet Data Convergence) protocol
 - UP hosts the user plane part of the PDCP protocol and the SDAP (Service Data Adaptation) protocol

Logical Open RAN Architecture



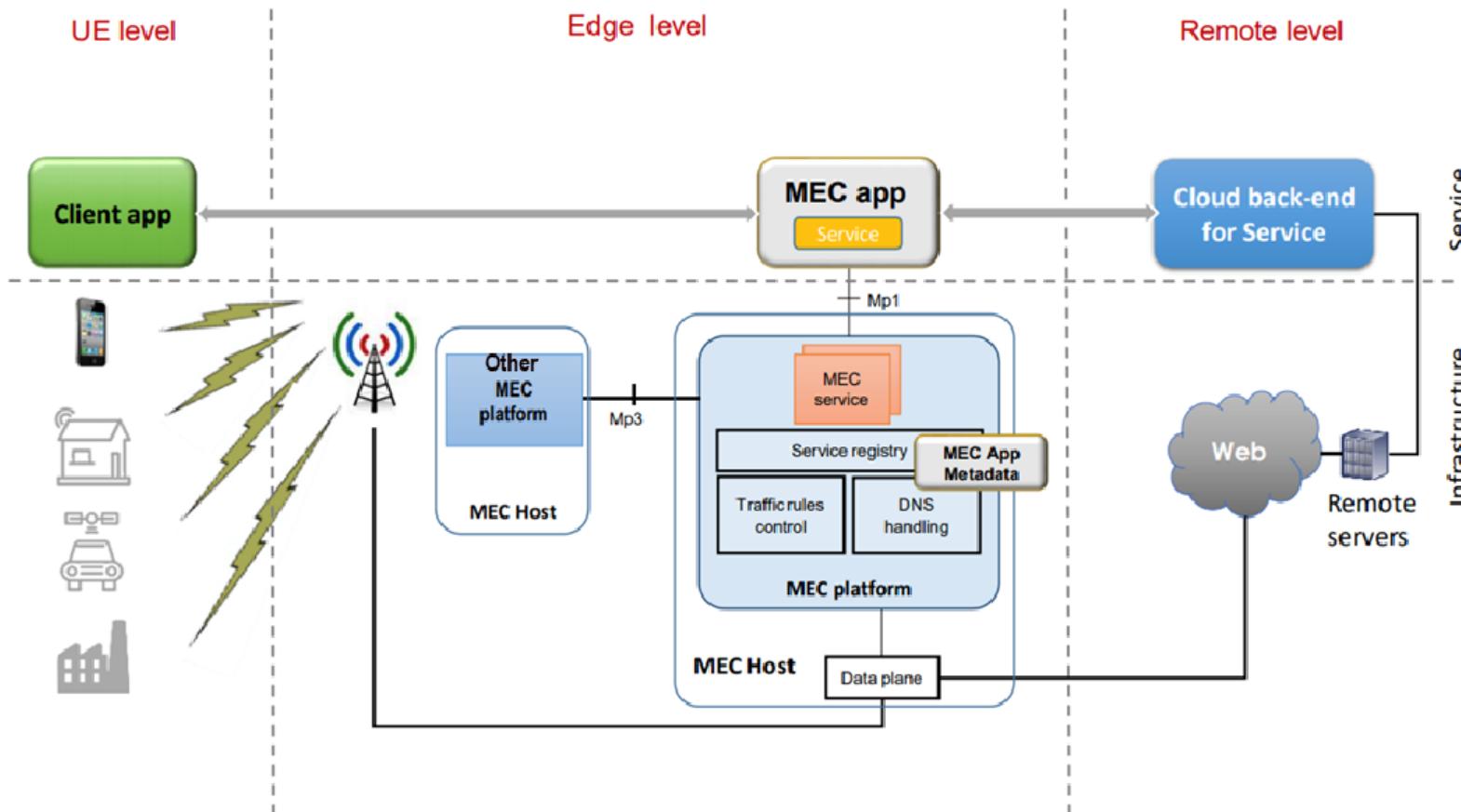
- **O-RU**
 - O-RAN Radio Unit
 - Hosts Low-PHY layers and RF processing
- **O-Cloud**
 - The generic cloud infrastructure

Multi-access Edge Computing

MEC

Multi-Access Edge Computing

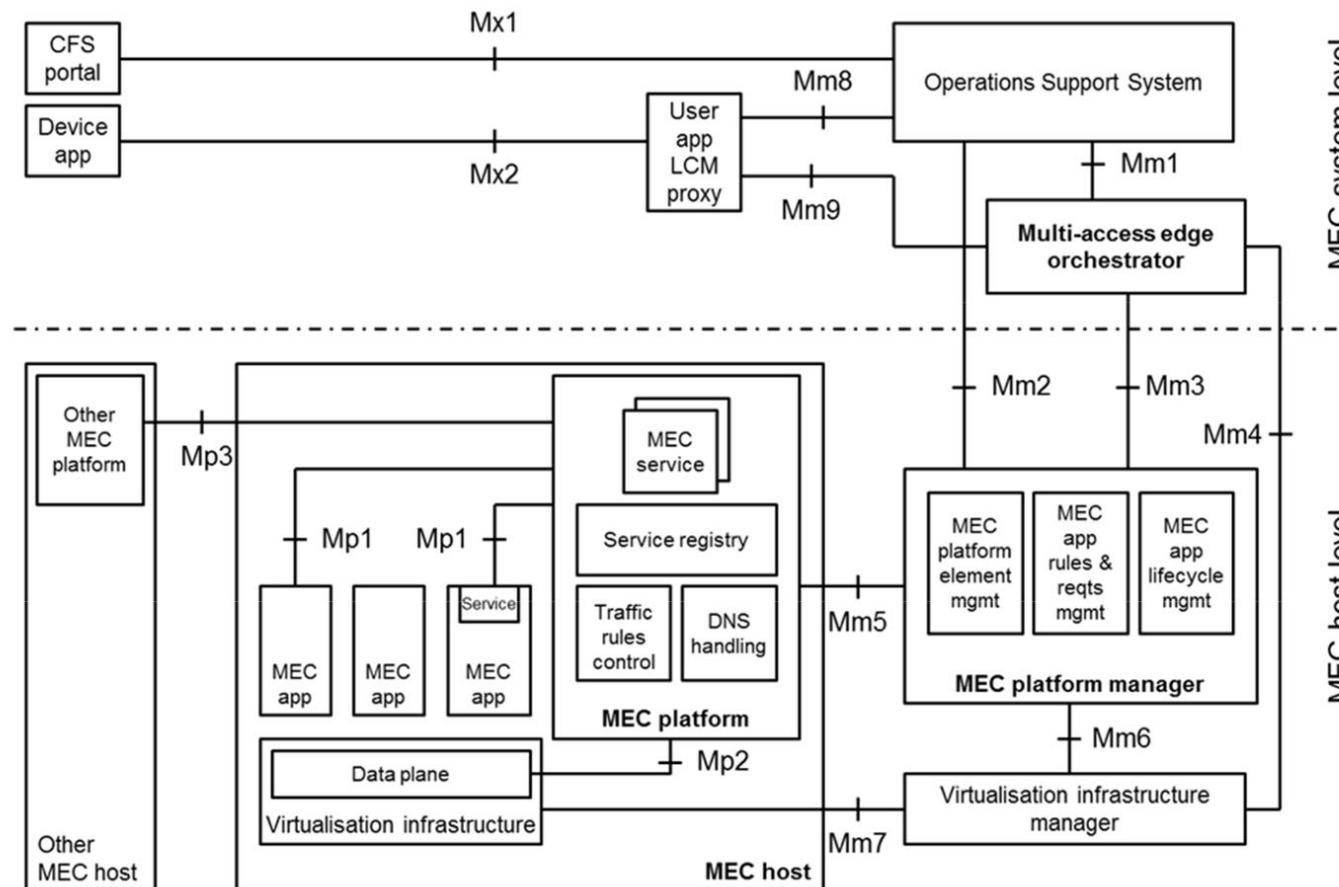
concept



Source: ETSI

Multi-Access Edge Computing

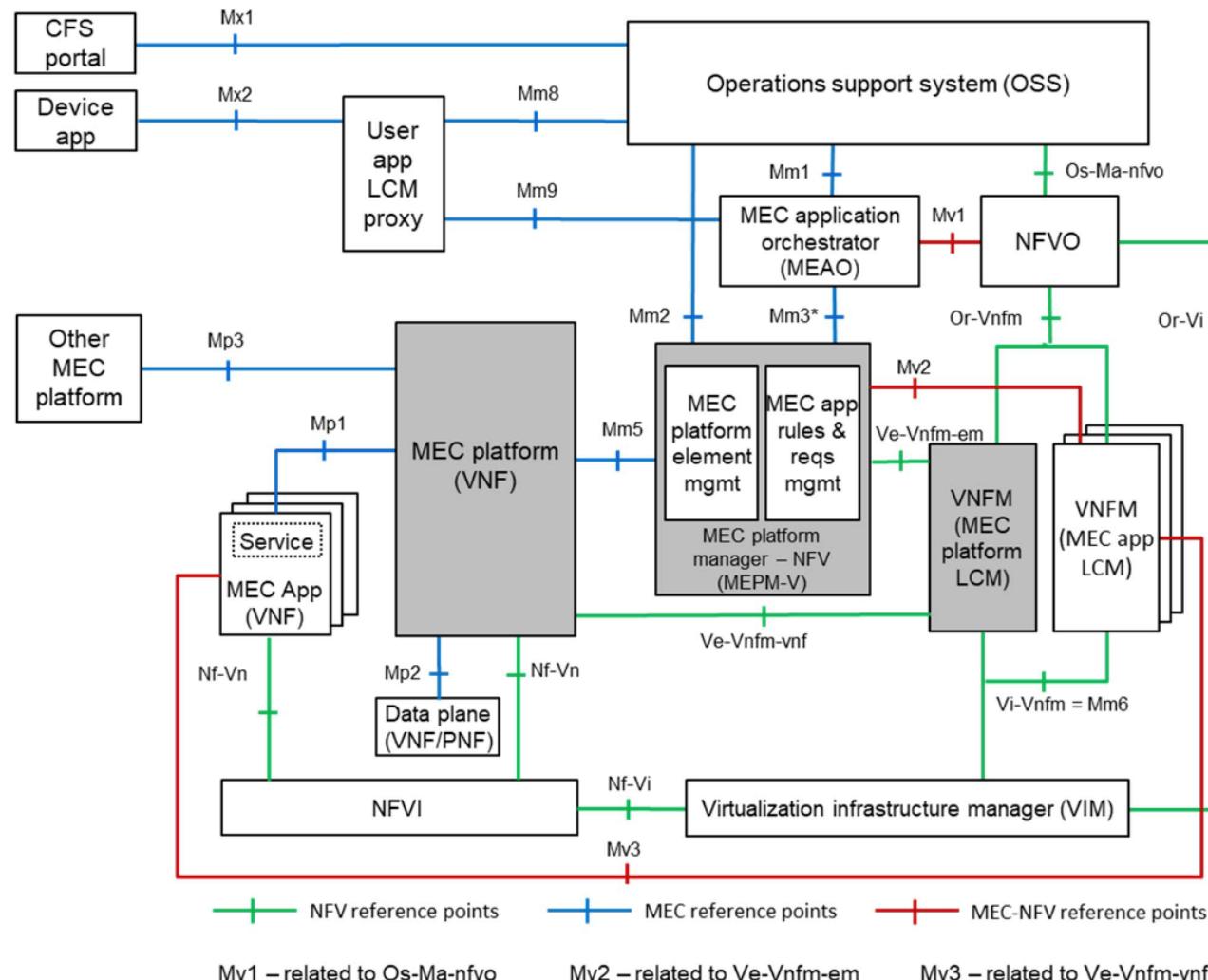
reference architecture



Source: ETSI

Multi-Access Edge Computing

mapping into NFV



Network automation

AI application to networks

- Accelerates service provisioning
 - Makes networks understand service intentions
- Reduces the probability of human errors
 - Automates complex networks
- Predicts and quickly rectifies faults
 - Enables networks to optimize themselves
- Improves efficiency of detecting threats
 - Enables networks to predict threats

A self-driving network

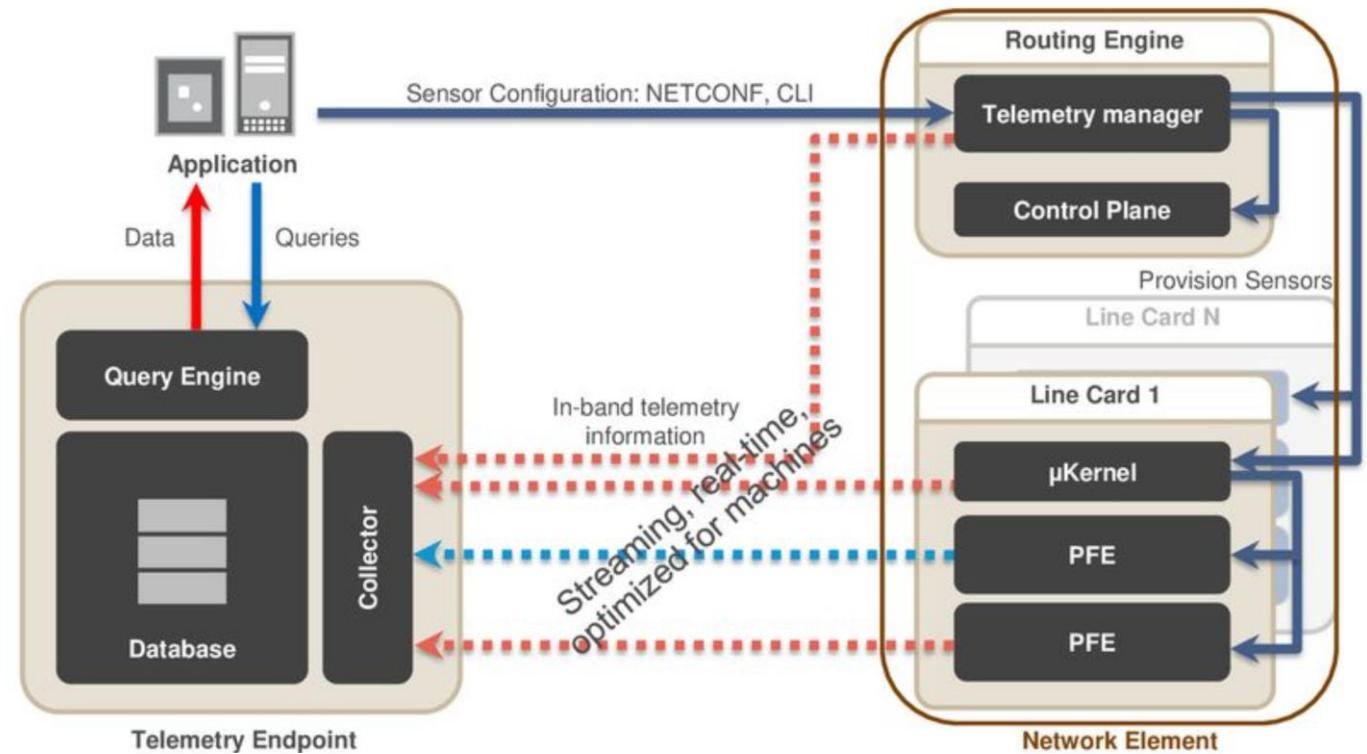
- A network that:
 - Accepts guidelines from the network operator
 - Self-discovers the components
 - Organizes and configures itself
 - Monitors itself using probes and other techniques
 - Auto-detects and auto-enables new customers
 - Automatically monitors and updates service delivery
 - Diagnoses itself using machine learning and heals itself
 - Periodically reports by itself

How can this become true?

- Telemetry
- Multidimensional views
- Automation
- Declarative intent
- Decision making

Telemetry

- Obtain information from the network, the data, services, etc.
- Real-time vs. Statistical
- Raw vs. pre-processed
- Key Performance Indicators



Multidimensional views

- What is useful information? To act, to account, to react...

Today

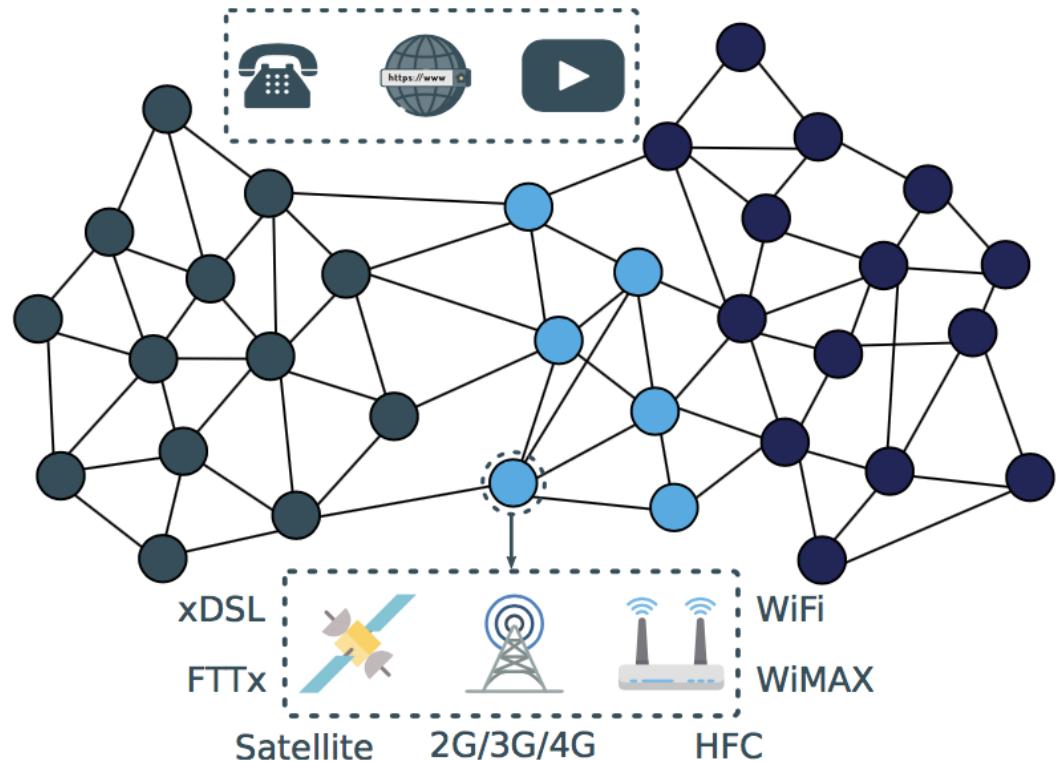
- Neighbors, links
- Exit points, peers
- Devices
- Middle boxes
- Global topology, traffic, flows
- Server and application performance
- Hackers, flash crowds, DDoS

Tomorrow

- Correlated information
 - Different geographies
 - Different layers, peers, clouds
- Root cause analysis via supervised learning**
- Time-based trending to establish and adapt baselines**
- Optimal local decisions based on global state**

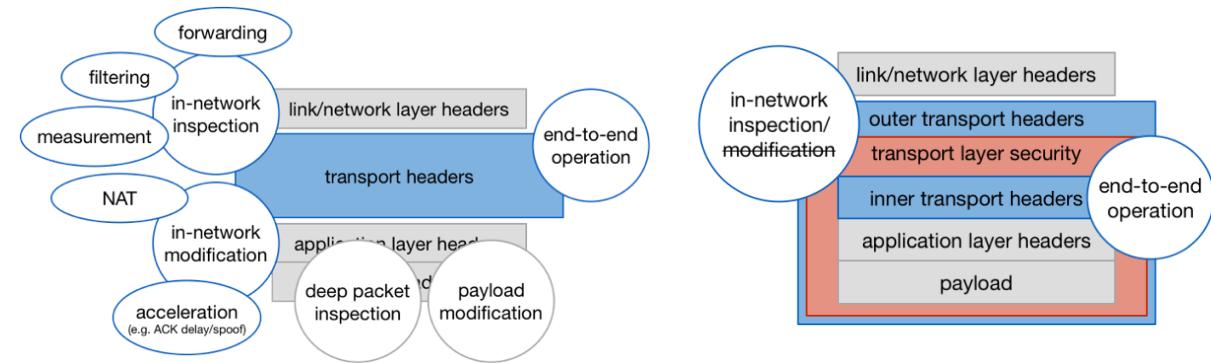
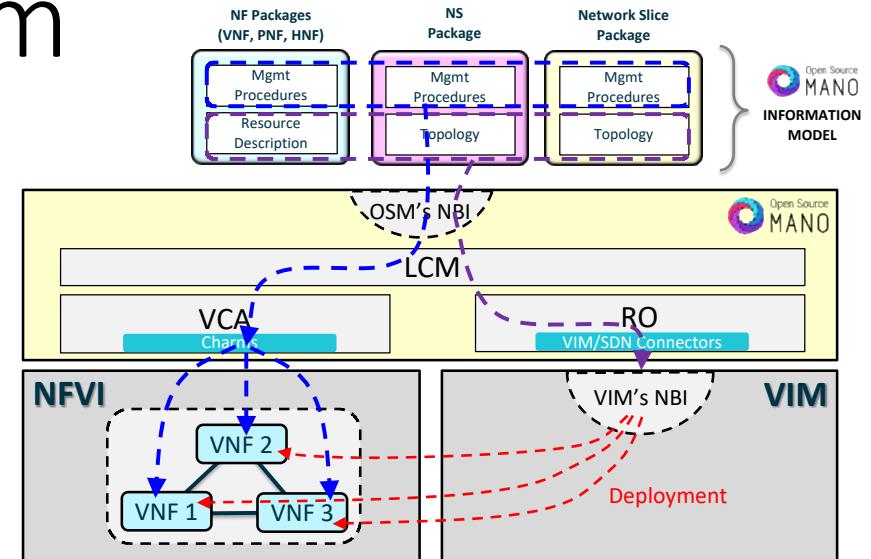
The Aggregation Scenario

- Support the integration of different data flows
 - Open
 - Automated
 - Secure
 - Scalable
- Deal with heterogeneity at all levels
 - Data sources
 - Data consumers
 - Data models
 - Deployment styles
 - Supporting infrastructures
- Not just data
 - Metadata becomes essential, including semantic mappings
 - What seems to claim for a data stream ontology
 - Not that far away: data modeling is a first step



The Actuating (Control) Stream

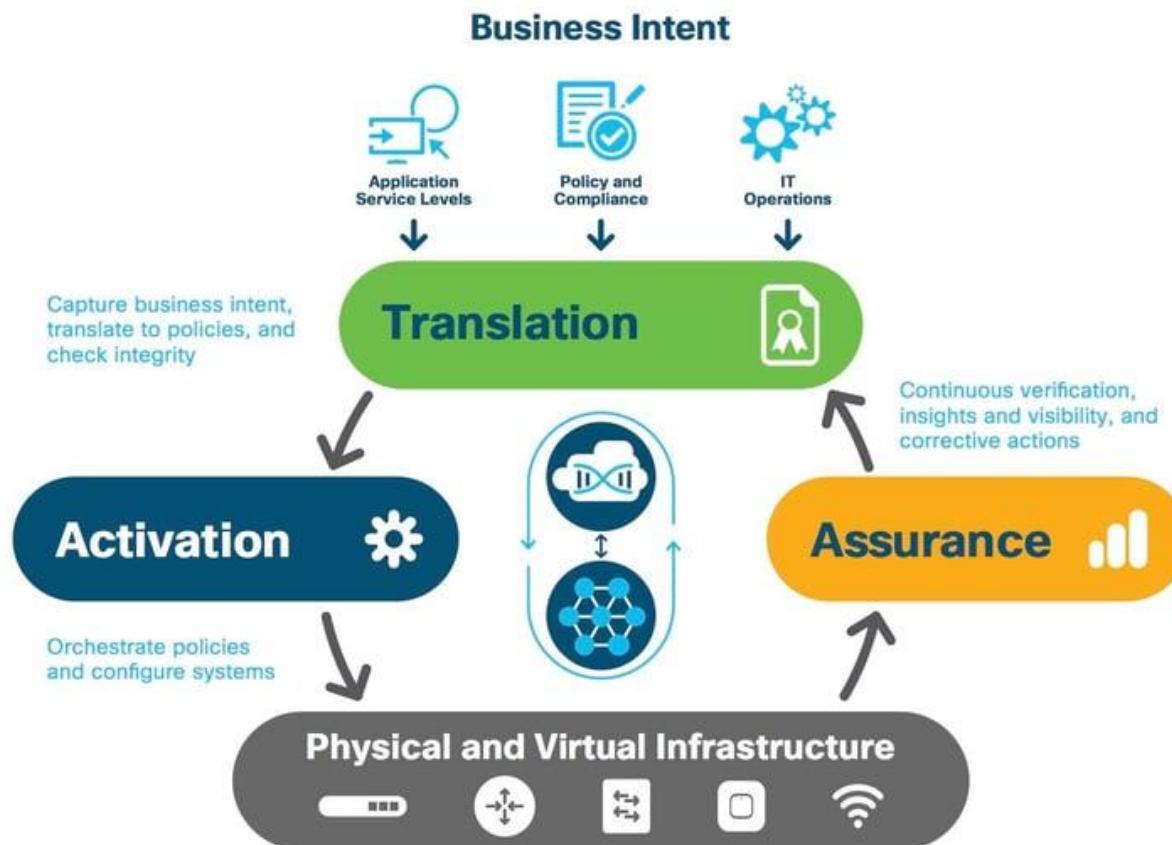
- OAM actions at a wide variety of different domains
 - Challenging, given the current state-of-the-art
- Initial strategies
 - Domain specific
 - Recommendation systems
 - Autonomic protocols
- SBA approaches and capability models
 - Reusable functionality description
 - Abstractions of network element functionalities usable as building blocks
 - Combined to provide more powerful features
 - Registration mechanisms to support CI/CD
 - Inter-domain collaboration for E2E management



Network Automation



Declarative Intent



Decision Making

- Rule-based learning
 - If 'X' happens, do 'Y'
 - Pros
 - Straightforward programming
 - Easy to predict and refine
 - Cons
 - Slow work
 - At scale, hard to manage
- Machine learning
 - Models, learning, percentage
 - Pros
 - Can become creative
 - Fastest way to learn complex behavior
 - Cons
 - Can come to strange conclusions
 - Hard to know what it knows

A transformation of the skillset

- Network engineering → Service design
- Network knowhow → Algorithm development
- The networks get out of the way
 - SLAs are automatically met
- Networks adapt, react, anticipate
- Security becomes Good Guy ‘Bot vs Bad Guy ‘Bot

Network automation

- Remove human from the loop of usual network management tasks
 - Provisioning
 - Detection
 - Diagnosis
 - Remediation
- In reality, is not to fully remove the humans, but remove them from the low-level painful tasks
- Why?
 - Humans are expensive
 - Reliable?
 - How to scale?

Closing the Closed Loops

- The use of closed loops is common everywhere
 - Automatics have been around for a long time
 - An essential aspect of industrial processes
- Not only about offering network data
 - An integral monitoring data substrate
- Well-defined data flow semantics
 - Data models for sources and consumers
 - Registry, discovery and dynamic orchestration
 - Full data sovereignty
- Going beyond
 - Key-Value Indicators distillation
 - Network-hosted AI and learning mechanisms
 - Support for serverless in-network computing

