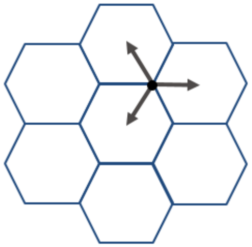
5G Review Session

Cellular mobile communications

Mobility (not nomadicity) is achieved by *handoff* (Joel) between *cells*

Each cell is served by a Base Station transceiver
at the corners so that each BS covers 3 *sectors* (Porter)



The user equipment UE communicates with the Base Station
over the air interface

Cells tessellate the area to be covered

- macrocell
- small cells
  - microcell < 2 km about 5w (often used to supplement coverage)
  - picocell < 200 m < 1w (inside buildings, underground parking, etc.)
  - femtocell ≈ 10 m 100 mW (home, small business)

Many users can use a single cell using a *multiple access* method
(TDMA FDMA CDMA)

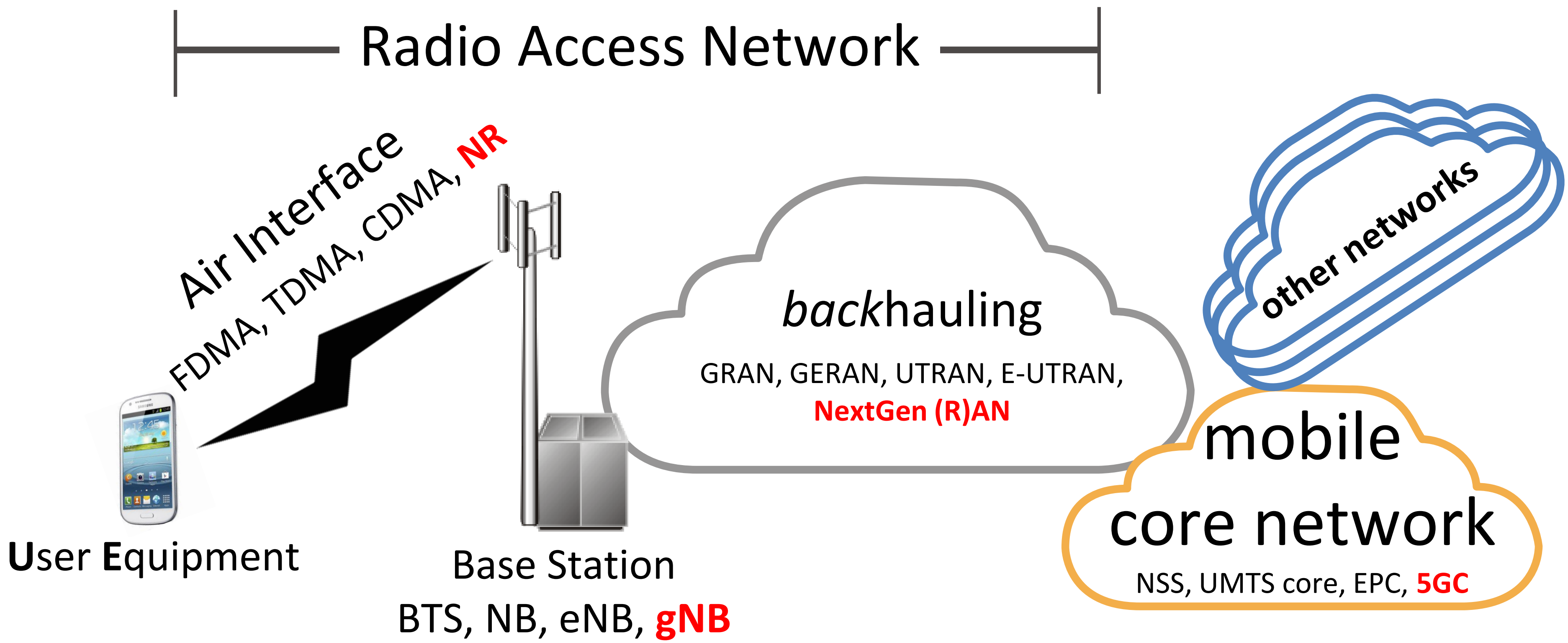
Each user both receives and transmits to the cell using a *duplexing* method
(FDD, TDD)

Generations of cellular technologies

	1G	2G	3G	4G	5G
standards	AMPS	IS-136, GSM Groupe Spécial Mobile	UMTS 3GPP R4 - R7	LTE R8-R9, R10-R14	3GPP 15, 16
era	1980s	1990s	2000s	2010s	2020s
services	analog voice	digital voice messages	WB voice packet data	video, Internet *(no longer voice-centric)*	*everything* *(no longer human-centric)*
devices					
data rate	0	100 kbps (GPRS)	10 Mbps (HSPA)	100+ Mbps (LTE/LTE-A)	10 Gbps (NR)
delay		500 ms	100 ms	10s ms	5 ms

Basic cellular segments (all generations)

Note: 5G requires upgrade of all segments
not just the air interface (NR) !



- user traffic
- control traffic
  - Access Stratum (AS) UE-RRC(BS)
  - Non Access Stratum (NAS) UE-MME(core)

What's wrong with 4G?

4G made possible:

- fast Internet access
- video reception and creation
- apps relying on location and identity
- always-on behavior

but suffers from numerous limitations:

- for some applications: data-rate too low
- for some applications: delay too high
- too few simultaneous connections (insufficient density)
- coverage too low / drop rate too high
- weak (if any) QoS guarantees
- price per bit too high (inefficient spectral use)
- power consumption too high (and thus battery life too low)
- poor support for new applications/markets (e.g., IoT, AR/VR, connected cars)
- no support for new mobility requirements (mobile hot spots, high speed)
- insufficient security/privacy

5G is being developed
to address 4G limitations

5G application classes

SPEED

eMBB **first to be deployed**

10 Gbps, 10 Mbps/m²

video streaming

AR/VR

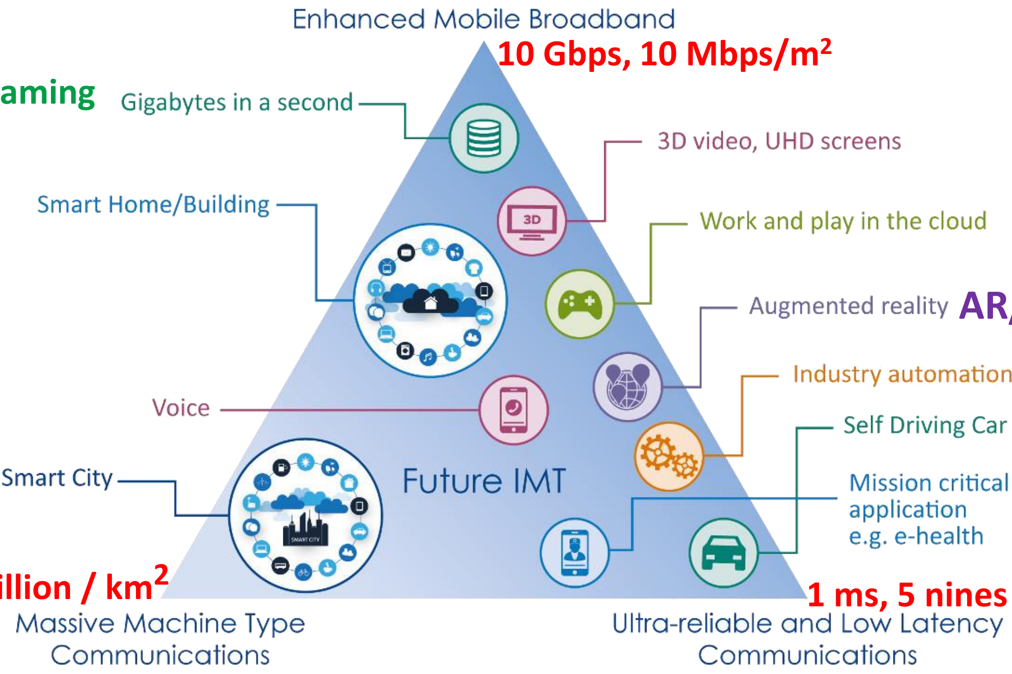
IIot

V2x

meter reading

1 Million / km²

1 ms, 5 nines



mMTC

MIoT

DENSITY

URLLC

Performance Parameters

DELAY

RELIABILITY

Use cases

Unlike earlier generations

which were designed for general purpose connectivity

without considering requirements for specific use cases

initial 5G work focused on vertical markets of interest, such as :

- mobile broadband
- Fixed Wireless Access
- video up and downstreaming
- smart city
- automotive (V2X)
- Industry 4.0 (incl. industrial robots)
- entertainment and gaming
- AR/VR/MR
- critical infrastructure
- smart utilities
- business services
- agriculture

and collected specific requirements for each

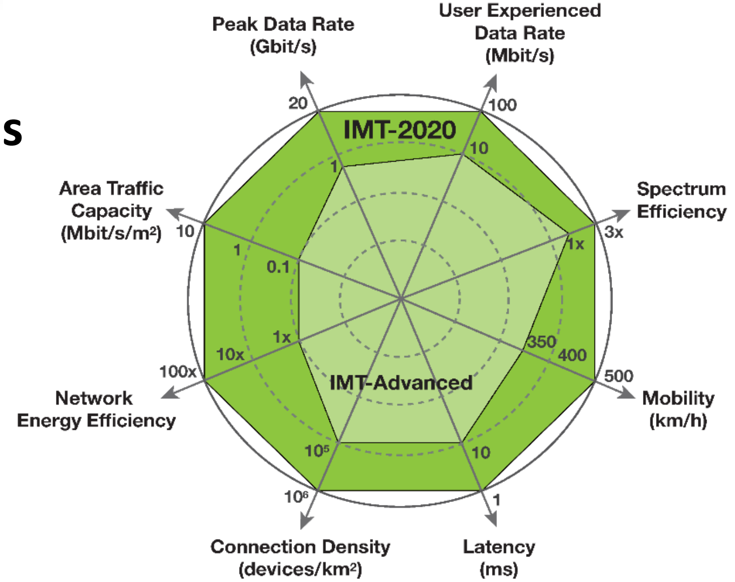
IMT-2020 goals

ITU-R published M.2083.0

IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond

which defined performance targets for 5G

that are 10 to 100 times *more* than 4G* :



- **Peak data rate** (20 Gbps/device)
- **User experienced data rate** (100 Mbps)
- **Latency** (1 ms)
- **Mobility** (500 km/h and seamless transfer)
- **Connection density** (10^6 devices/km^2)
- **Energy efficiency** (1/100 Joule/bit for both air interface and network)
- **Spectrum efficiency** (3 times the bps/Hz of LTE-A)
- **Area traffic capacity** (10 Mbps/m^2)

Note: larger coverage area is not a goal!

Note: it may not be possible to attain all of these *at the same time*

How does 5G attain higher speed?

Air interface

- NR more efficient (factor of 3 improvement)
- wider spectral bands (100 MHz, 1GHz), which requires
  - new RF bands (sub-1GHz, 24/28 GHz mmWave, 30-90GHz)
  - use of licensed/unlicensed unshared/shared spectrum
- smaller cells and higher cell density (i.e., many more antennas)
- massive MIMO
  - in 5G massive is defined as 16 or more antennas (4-by-4 array)
  - 5G envisages up to 256 antennas
    - < 6 GHz use multipath for spatial mux and multiuser MIMO
    - > 6 GHz use *coherent beamforming* (i.e., personal cells)

RAN

- functional split options – split 2 and 7.2 standardized
- upgrade from 1Gbps to 10Gbps to 100Gbps
- 25 GbE (802.3by), 1-lane 50 GbE (802.3cd), NG 100/200/400 GbE (802.3bs)
- FlexE bonding

R15 operating bands

FR1 (< 6GHz)

NR operating band	Uplink (UL) *operating band* BS receive / UE transmit F_{UL_low} – F_{UL_high}	Downlink (DL) *operating band* BS transmit / UE receive F_{DL_low} – F_{DL_high}	Duplex Mode
n1	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz	FDD
n2	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz	FDD
n3	1710 MHz – 1785 MHz	1805 MHz – 1880 MHz	FDD
n5	824 MHz – 849 MHz	869 MHz – 894 MHz	FDD
n7	2500 MHz – 2570 MHz	2620 MHz – 2690 MHz	FDD
n8	880 MHz – 915 MHz	925 MHz – 960 MHz	FDD
n20	832 MHz – 862 MHz	791 MHz – 821 MHz	FDD
n28	703 MHz – 748 MHz	758 MHz – 803 MHz	FDD
n38	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz	TDD
n41	2496 MHz – 2690 MHz	2496 MHz – 2690 MHz	TDD
n50	1432 MHz – 1517 MHz	1432 MHz – 1517 MHz	TDD
n51	1427 MHz – 1432 MHz	1427 MHz – 1432 MHz	TDD
n66	1710 MHz – 1780 MHz	2110 MHz – 2200 MHz	FDD
n70	1695 MHz – 1710 MHz	1995 MHz – 2020 MHz	FDD
n71	663 MHz – 698 MHz	617 MHz – 652 MHz	FDD
n74	1427 MHz – 1470 MHz	1475 MHz – 1518 MHz	FDD
n75	N/A	1432 MHz – 1517 MHz	SDL
n76	N/A	1427 MHz – 1432 MHz	SDL
n77	3300 MHz – 4200 MHz	3300 MHz – 4200 MHz	TDD
n78	3300 MHz – 3800 MHz	3300 MHz – 3800 MHz	TDD
n79	4400 MHz – 5000 MHz	4400 MHz – 5000 MHz	TDD
n80	1710 MHz – 1785 MHz	N/A	SUL
n81	880 MHz – 915 MHz	N/A	SUL
n82	832 MHz – 862 MHz	N/A	SUL
n83	703 MHz – 748 MHz	N/A	SUL
n84	1920 MHz – 1980 MHz	N/A	SUL

WRC-19 Sharm El-Skeikh Nov 2019
expanded RF bands available for 5G
from 1.9 GHz to 17.25 GHz

New bands:

- 24.25-27.5 GHz
- 37-43.5 GHz
- 45.5-47 GHz
- 47.2-48.2 GHz
- 66-71 GHz

Additional bands will be considered for WRC-23
including low and mid frequencies

FR2 (>6GHz)

NR Operating Band	Uplink (UL) operating band BS receive UE transmit F_{UL_low} – F_{UL_high}	Downlink (DL) operating band BS transmit UE receive F_{DL_low} – F_{DL_high}	Duplex Mode
n257	26500 MHz – 29500 MHz	26500 MHz – 29500 MHz	TDD
n258	24250 MHz – 27500 MHz	24250 MHz – 27500 MHz	TDD
n260	37000 MHz – 40000 MHz	37000 MHz – 40000 MHz	TDD

Millimeter waves

How does 5G attain lower latencies?

Air interface

- more flexible frame structure
- self contained integrated subframe

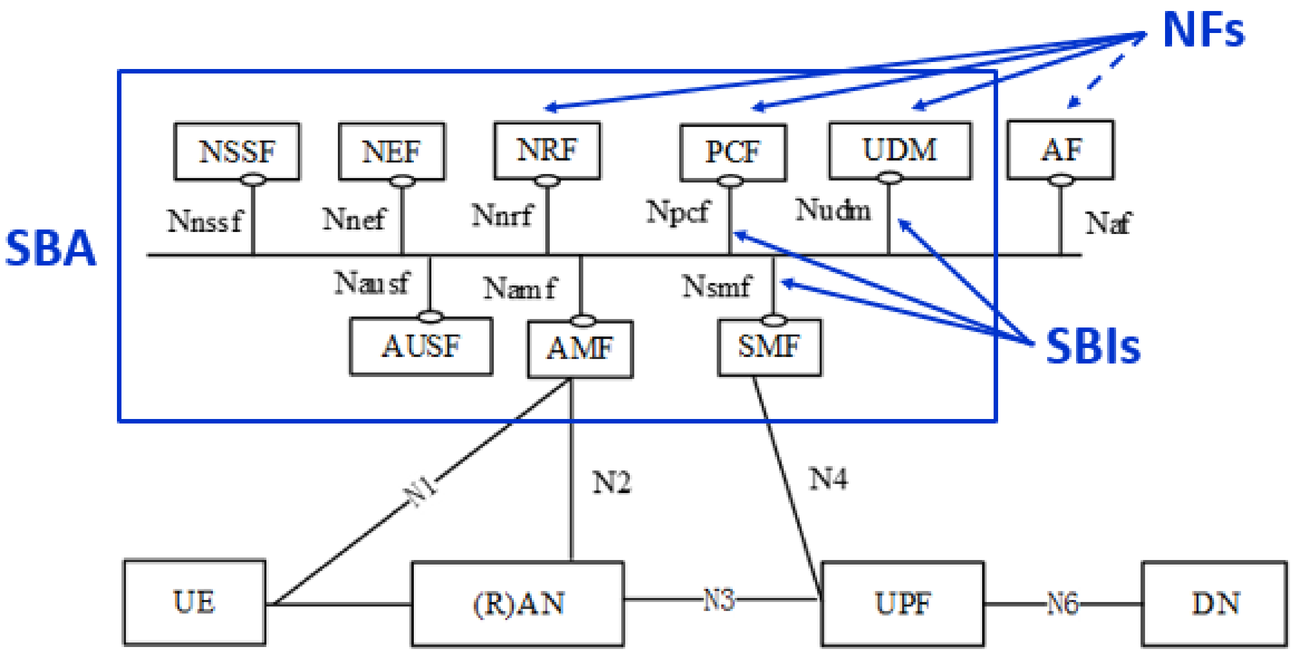
RAN

- network slicing
- **T**ime **S**ensitive **N**etworking / **Det**erministic **Net**working
  - IEEE 802.1CM for Ethernet fronthaul
  - IEEE 802.1Qbv scheduled traffic enhancements
  - IEEE 802.1Qbu frame pre-emption
  - IETF DetNet (Deterministic Networking) for IP
- **S**oftware **D**efined **N**etworking
- **N**etwork **F**unctions **V**irtualization
- **M**obile **E**dge **C**omputing

How does 5G support new applications?

Cloud-based **S**ervice **B**ased **A**rchitecture **core**

- based on Network Functions and exposure functions (NRF, NEF)
- client/server with RESTful interfaces (CRUD operations)
- **A**pplication **F**unctions

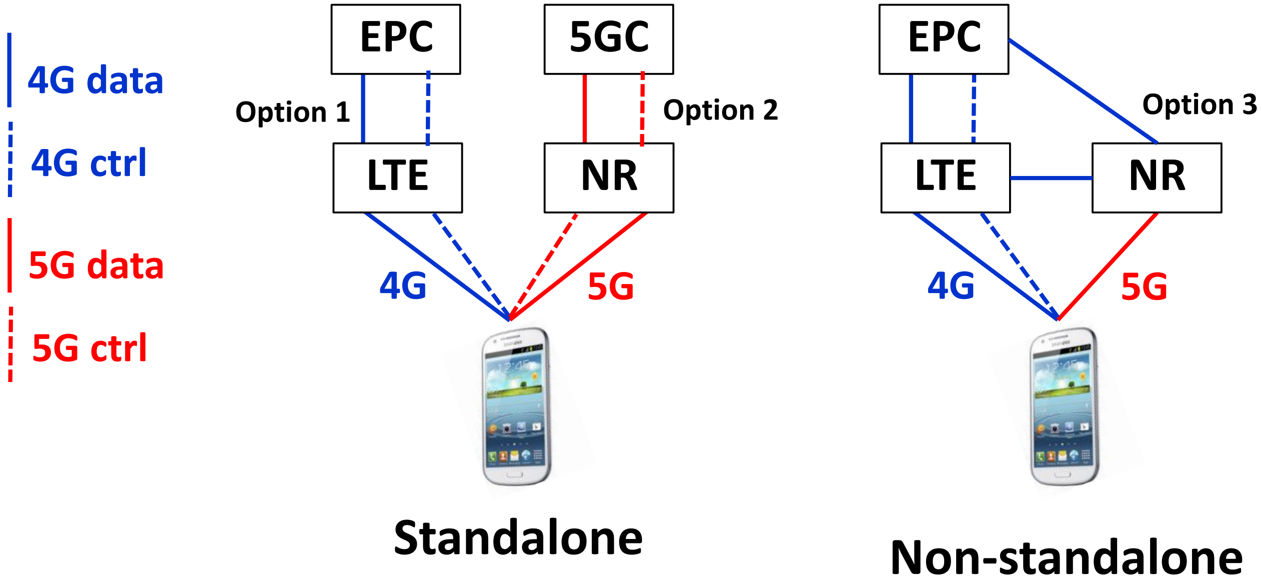


Coexistence options

Initial 5G deployments will focus on eMBB
and mostly rely on deployment of NR in new frequency bands

In order to facilitate this first stage 3GPP defined **N**on **S**tand**A**lone (NSA)
i.e., 5G supported by the existing 4G infrastructure (E-UTRAN, EPC)

Later deployments will tackle URLLC and mMTC
requiring more RAN and core support, leading to **S**tand**A**lone operation

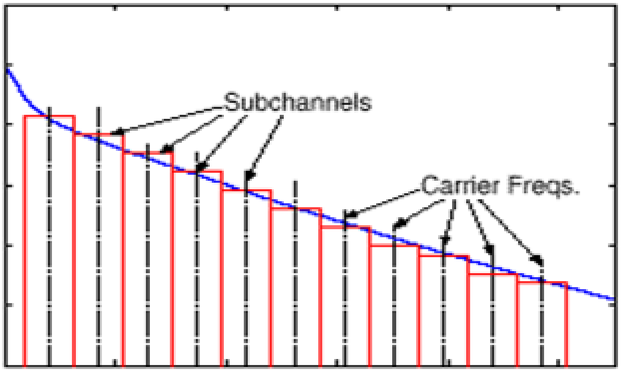


Note: there are other options for long term

FDM and OFDM

With Frequency Domain Multiplexing

we divide a single information stream into blocks of bits
and mux them together using distinct carrier frequencies (sub-carriers)



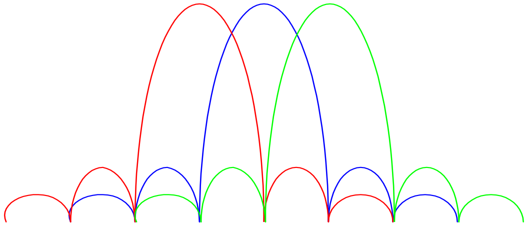
Each sub-carrier signal
has its own power level and modulation
thus directly implementing *water pouring*

Equalization in the frequency domain (FEQ)

No ISI since each channel has low rate

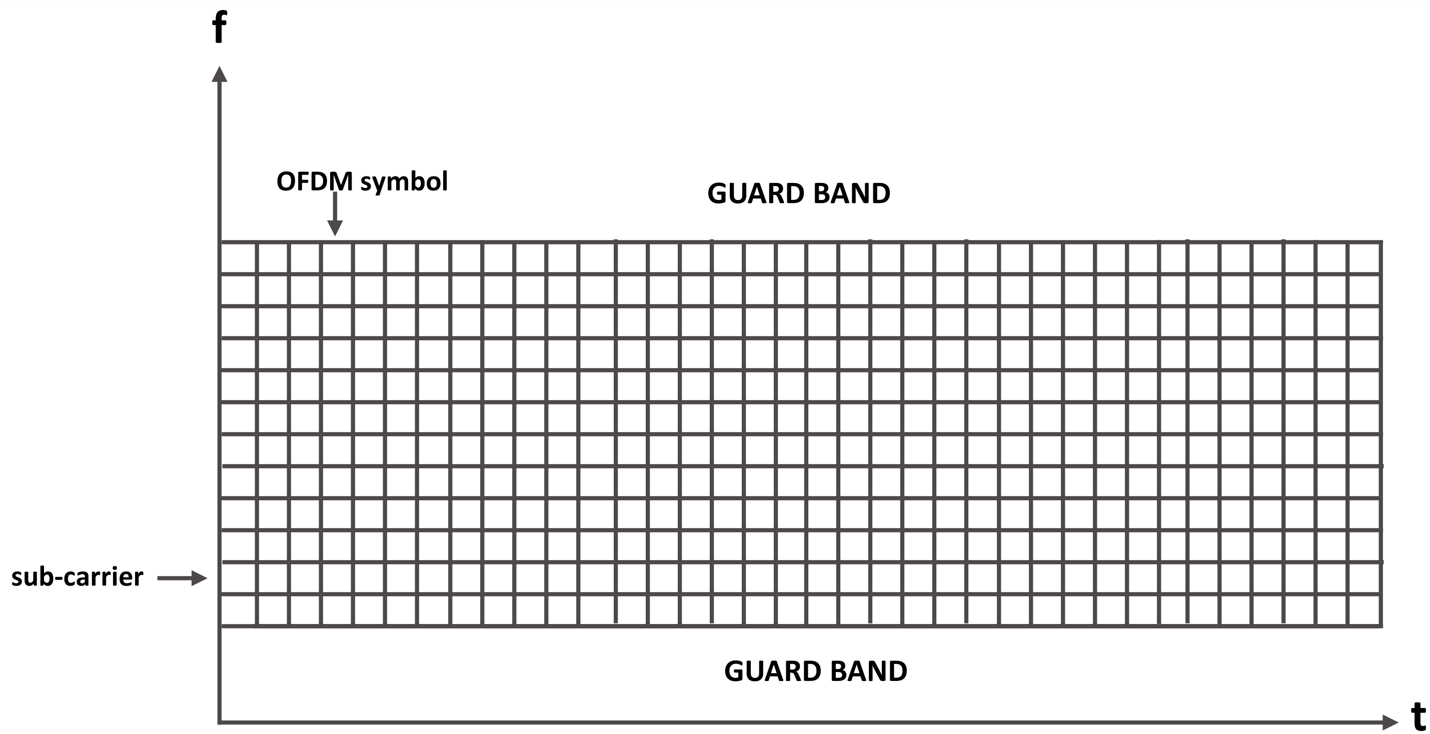
To eliminate ICI we use OFDM

- all sub-channels use the same symbol rate (even if different modulations)
- sub-carriers are spaced at precisely the symbol rate
- the sub-carriers are the precisely orthogonal
  and hence do not interfere with each other



OFDM has a high **P**eak to **A**verage **R**atio
which is demanding for transmission amplifiers

OFDM signal structure



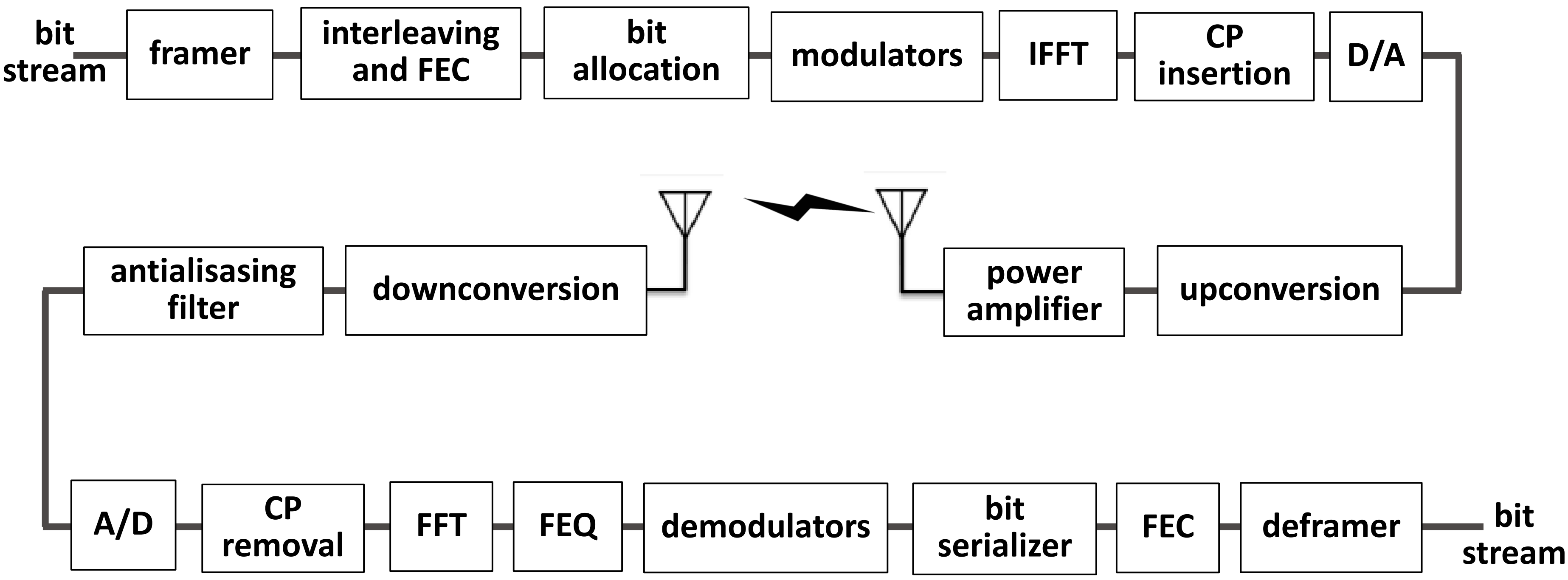
For LTE:

- **channel bandwidth ..., 5, 10, 15, or 20 MHz**
- **guard band overhead is 10%**
- **sub-carrier spacing = 15 kHz**
- **OFDM symbol duration = 1/15KHz = 66.67 µsec**
    - **short CP = 4.7 µsec so total duration = 71.367 µsec**
        - **1 *slot* = 7 symbols ≈ ½ msec***
    - **long CP = 16.7 µsec so total duration = 83.367 µsec**
        - **1 *slot* = 6 symbols ≈ ½ msec***

BW (MHz)	usable BW (MHz)	subchannels	FFT
5	4.5	300	512
10	9	600	1024
15	13.5	900	1536
20	18	1200	2048

* CP durations are *adjusted* so that the slot is precisely ½ msec

OFDM modem



bit stream
framer
interleaving and FEC
bit allocation
modulators
IFFT
CP insertion
D/A
upconversion
power amplifier
downconversion
antialisasing filter
A/D
CP removal
FFT
FEQ
demodulators
bit serializer
FEC
deframer
bit stream

Cyclic prefix

$Y(\omega) = H(\omega)\, X(\omega)$

$Y_k = H_k\, X_k$

For **analog** **digital** signal processing

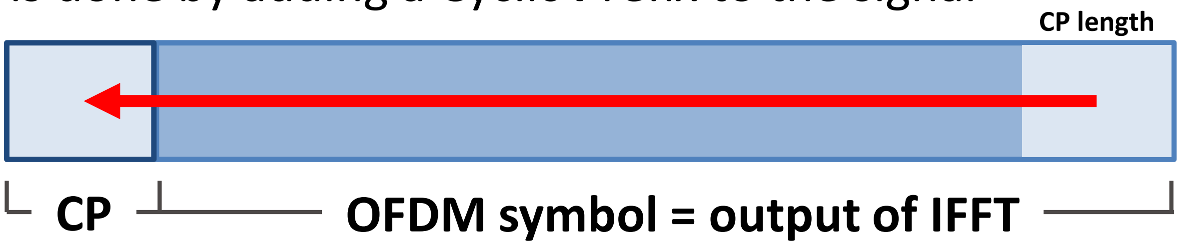
linear cyclic convolution in the time domain **y = h * x**

is equivalent to multiplication in the frequency domain

So, the linear convolution in the analog channel

has to be converted into cyclic convolution for the digital channel

This is done by adding a **C**yclic **P**refix to the signal



For ISI due to multipath

the CP must be long enough to incorporate

the difference between longest and shortest delays

HARQ

In **F**orward **E**rror **C**orrection (FEC)

an error *correction* code corrects incorrectly received data

but FECs can only correct when there are a limited number of errors

In **A**utomatic **R**epeat re**Q**uest (ARQ)

an error *detection* code triggers a repeat request (NACK)

(it is easier to detect bit errors than to correct them)

Hybrid **ARQ** (HARQ) is a hybrid (combination) of FEC and ARQ

if the FEC can correct the errors, then it does so

if more errors are detected than can be corrected, ARQ is used

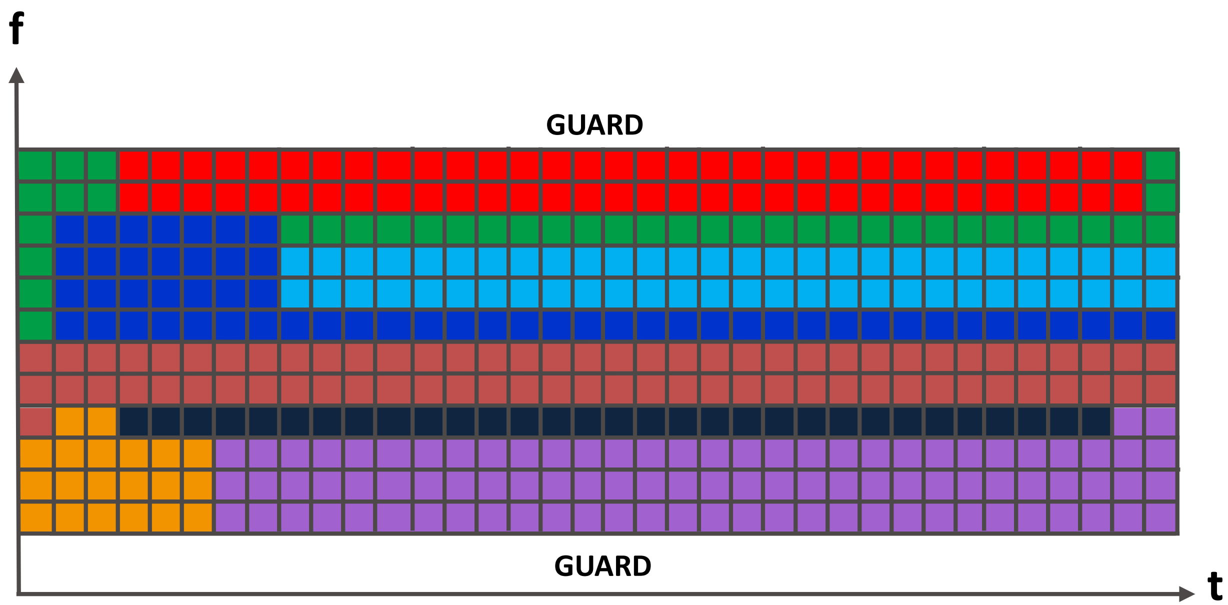
OFDMA

The basic OFDM paradigm can be readily extended to *multiple access*

Each UE must transmit at

- precisely the correct symbol rate
- precisely the correct symbol timing (*as seen at the BS*)
- sub-carrier frequencies allocated to it
- time(s) allocated to it

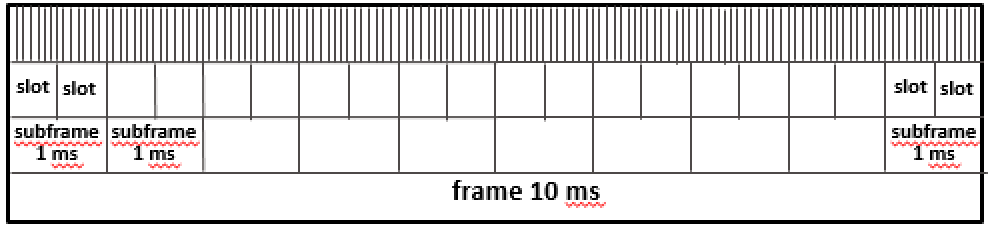
All of this necessitates very accurate synchronization!



Signals and physical channels

OFDMA transmission is divided in to *frames, subframes, slots,* and *symbols*

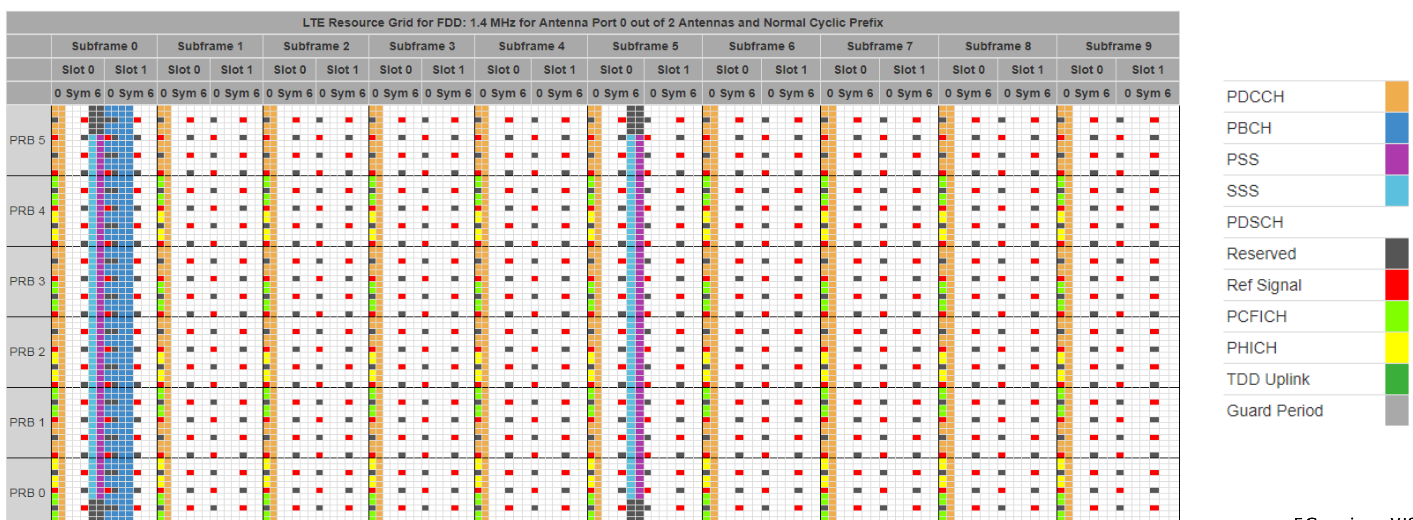
frame = 10 ms



Frames contain various *signals* and *physical channels*

A signal is a special position in the frame needed for specific purposes such as synchronization or channel estimation

A channel is a position in the frame that carries information



RBs

The smallest unit that can be allocated to a user is a **R**esource **B**lock

Usually many RBs are simultaneously allocated to a UE

depending on user needs and cell resource availability

Each RB spans 12 consecutive subcarriers and 1 slot

For LTE

- 12 channels * 15kHz = 180 kHz
- 1 slot = ½ msec

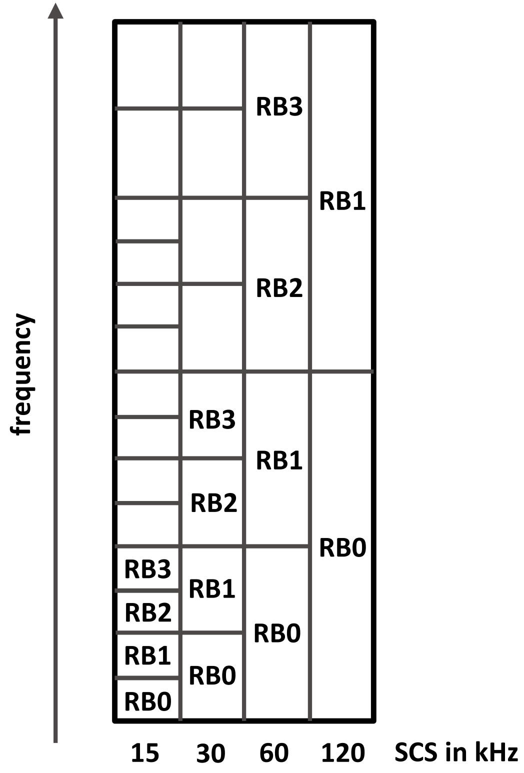
For NR only the RB frequency width is defined

- for SCS=15 kHz 1 RB = 180 kHz
- for SCS=30 kHz 1 RB = 360 kHz
- for SCS=60 kHz 1 RB = 720 kHz

allocation in the time domain can be

- slot aggregation (2 or more slots)
- mini-slots (2, 4, or 7 OFDM symbols)
- flexible (mixed DL/UL) slots for TDD operation

  including the *self-contained integrated* subframe



5G Scalable numerology

While LTE had a constant subcarrier spacing SCS of 15 kHz

5G introduces a scalable SCS with $\Delta f = 2^{\mu} * 15$ kHz

(i.e., SCS = 15, 30, 60, 120, 240, 480)

but not all SCS options are available for all operating bands

μ	SCS	RF	CP
0	15	< 6GHz	normal
1	30	< 6GHz	normal
2	60	both	normal/extended
3	120	> 6 GHz	normal
4	240	not in R15	normal
5	480	not in R15	normal

Of course OFDM requires the symbol rate to equal the SCS

so the symbol durations are shorter for higher μ

Channel bandwidth

LTE defined channel bandwidths of 1.4, 3, 5, 10, 15, 20 MHz

5G has more options, and higher bandwidth efficiency (>98%!)

- for RF bands under 6 GHz
  - 5, 10, 15, 20, 25, 30, 40, 50, 60, 70, 80, 90, 100 MHz
- for RF bands above 6GHz
  - 50, 100, 200, 400 MHz (and maybe higher later)

For example:

SCS (slot)	20 MHz	50 MHz	100 MHz	200 MHz	400 MHz
15 kHz 1 ms	**1320** FFT 2048 OH = 1%	**3300** FFT 4096 OH = 1%			
30 kHz 500 µs	**660** FFT 1024 OH = 1%	**1644** FFT 2048 OH = 1.36%	**3300** FFT 4096 OH = 1%		
60 kHz 250 µs	**324** FFT 512 OH = 2.8%	**816** FFT 1024 OH = 2.08%	**1644** FFT 2048 OH = 1.36%	**3300** FFT 4096 OH = 1%	
120 kHz 125 µs		**408** FFT 512 OH = 2.08%	**816** FFT 1024 OH = 2.08%	**1644** FFT 2048 OH = 1.36%	**3300** FFT 4096 OH = 1%

subcarriers
FFT size
guard overhead

LTE
SCS=15kHz/BW=20MHz used only 1200 subcarriers (OH = 10%)

higher efficiency
higher frequency sync requirements

MIMO

While LTE supports 4*2 MIMO (4 BS and 2 UE antennas)

R15 supports 32*4 MIMO (and this will increase significantly!)

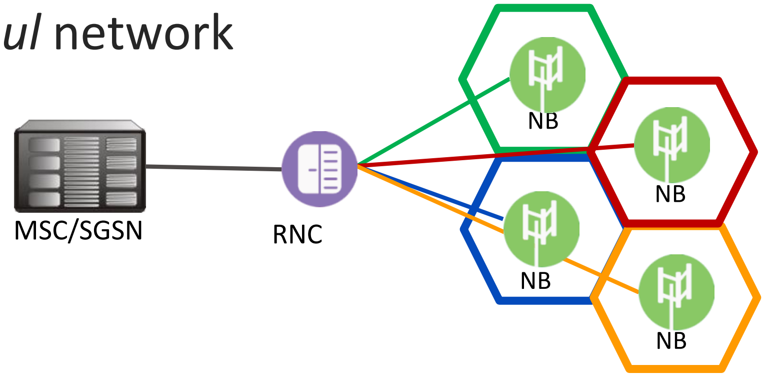
MIMO is critical for both < 6 GHz and > 6 GHz operating bands

but for different reasons

- for < 6 GHz
  - cells are large
  - there will be rich multipath
  - many users in cell
  - users will be highly mobile
  - so MIMO will use spatial mux to help achieve spectral efficiency goals
- for > 6 GHz
  - signal attenuation much higher (100 times higher?)
  - cells are small and little multipath
  - few users in cell
  - users are relatively static in the cell
  - so MIMO will use beamforming to overcome the high attenuation

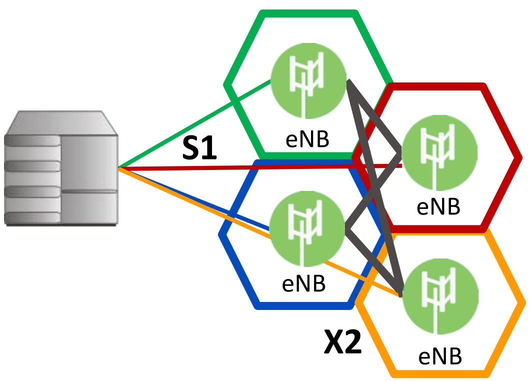
Splitting up the RAN (1)

In 3G the RAN was a pure *backhaul* network

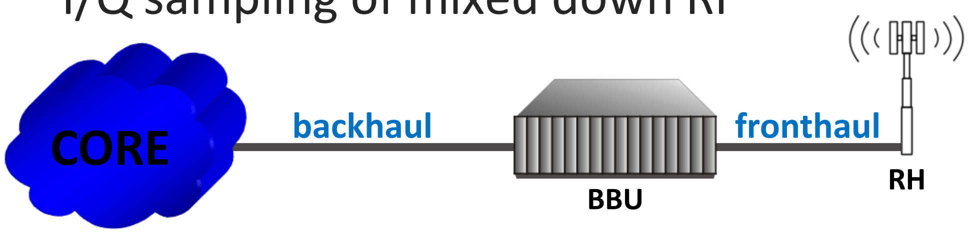


In 4G this changed in 2 ways

- the X2 interface interconnected eNBs (at least logically)

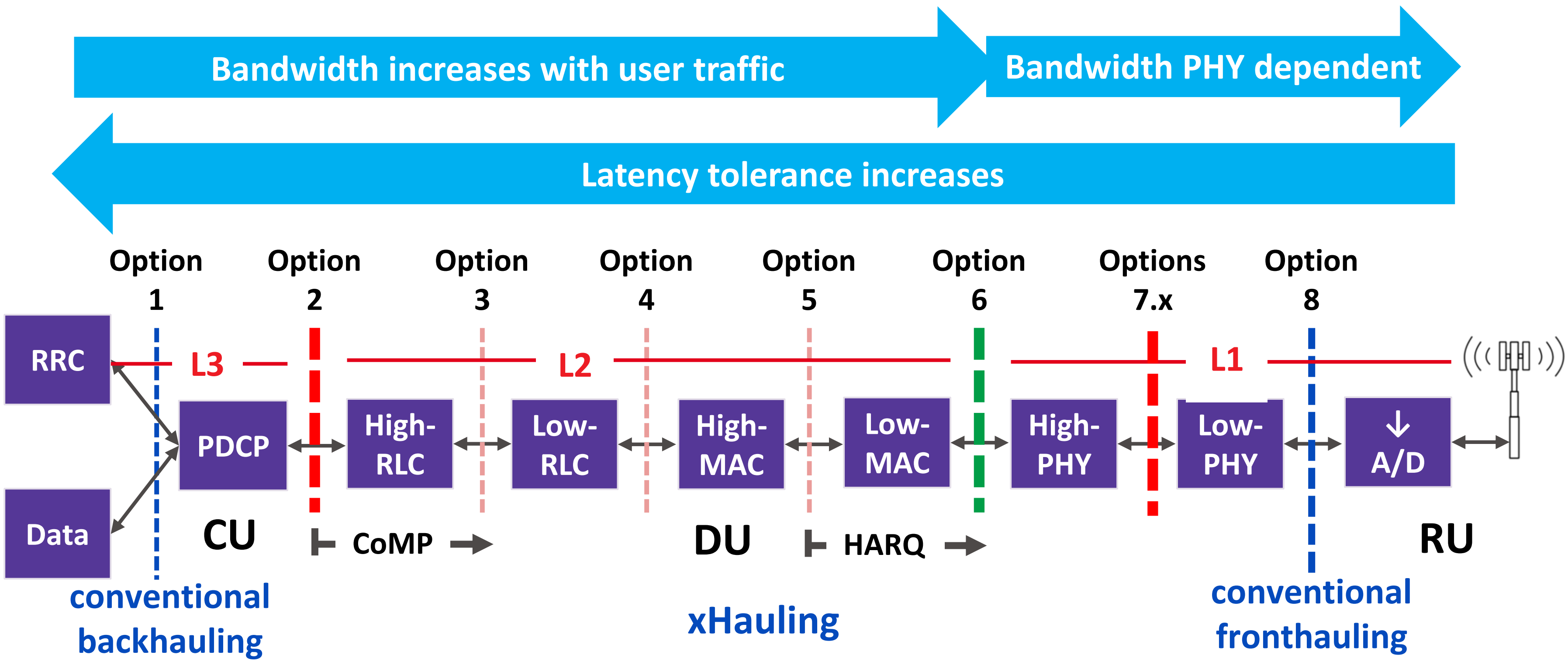


- fronthaul (CPRI)
  I/Q sampling of mixed down RF



In 5G this must change more drastically

5G RAN Functional Splits



LTE uses splits 1 and 8

3GPP has developed F1 = split 2 (CU/DU split)

ORAN has developed F2 = split 7.2 (RU/DU split)

Note: split 7.2 requires lower bit rate than split 8!

Decomposed base station transceiver
- PHY – Physical layer processing
- MAC – Medium Access Control
- RLC – Radio Link Control
- PDCP – Packet Data Convergence Protocol

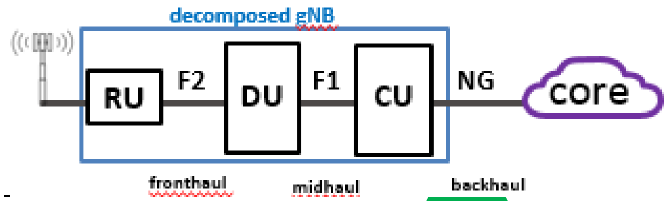
Network based control functionality
- RRC – Radio Resource Control

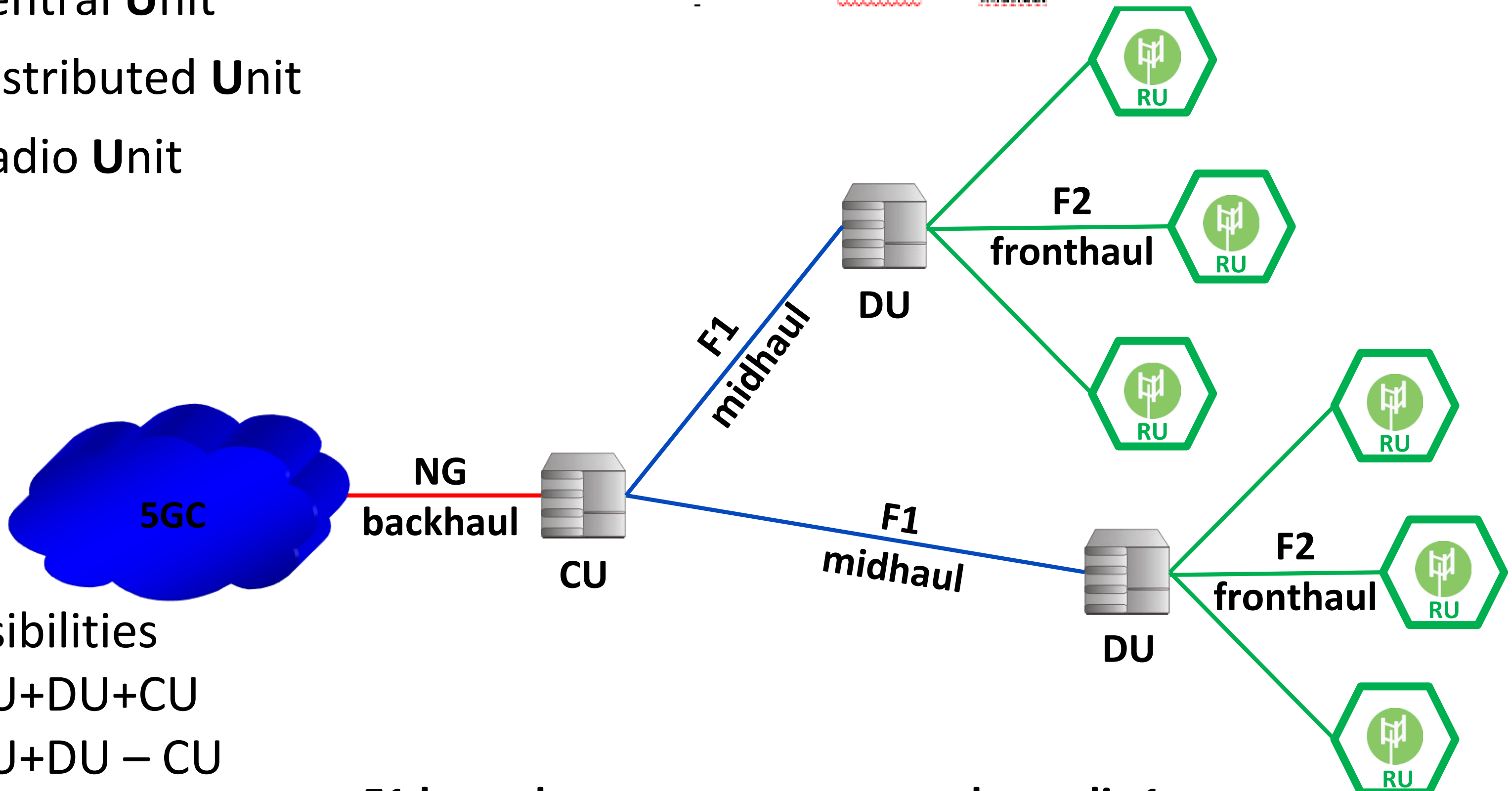
5G interfaces

Using intermediate split options

decomposes the BBU into

- **C**entral **U**nit
- **D**istributed **U**nit
- **R**adio **U**nit





Possibilities

- RU+DU+CU
- RU+DU – CU
- RU – DU+CU
- RU – DU – CU

F1 has advantages as compared to split 1
F2 has advantages as compared to split 8

Potential 5G RAN transport technologies

Here are a few transport innovations that can support 5G xHaul requirements

- 10GbE, XGS-PON
  - but 10 Gbps is only satisfactory for initial 5G deployments
- 25 GbE (802.3by), 1-lane 50 GbE (802.3cd)
  100/200/400 GbE (802.3bs)
- FlexE
- **M**obile (**M**ulti-access) **E**dge **C**omputing
- Synchronization (SyncE, IEEE 1588, DGM)
- Network slicing
- **T**ime **S**ensitive **N**etworking (and **Det**erministic **Net**working)
- **F**rame **R**eplication and **E**limination (IEEE 802.1CB)

high data rates

low latency

ultra high reliability

Time Sensitive Networking

TSN and **Det**erministic **Net**working are Ethernet and IP/MPLS technologies that enable:

- *very low* and *guaranteed* packet propagation *latency*
  - time aware scheduling/queuing
  - time coordinated forwarding
  - frame preemption
- *very high reliability*
  - zero congestion loss (PLR of 10^{-10})
  - resource reservation
  - seamless redundancy
- dynamicity – flows can be removed or added w/o impacting other flows
- co-existence of TSN traffic with regular traffic
  - up to 75% express traffic

for applications such as IIoT, V2x, fronthaul

TSN is being developed for Ethernet by a task group in IEEE 802.1

DetNet is being developed for IP and MPLS by the DetNet WG in the IETF

SDN and NFV for 5G

Software **D**efined **N**etworking or **S**egment **R**outing
and
Network **F**unctions **V**irtualization or
are widely considered to be essential technologies for 5G

- **Slicing** depends on SDN to be dynamic, obey constraints, efficient, and end-to-end
- **Mobile** (Multi-access) **Edge Computing** depends on NFV to dynamic place functionality where needed

SDN advocates replacing standardized networking protocols
with centralized software applications
that configure *whitebox switches* in the network

SR achieves SDN-like control over packet forwarding
by adding routing information to packet headers

NFV advocates replacing hardware network elements
with software running on *whitebox servers*
that may be housed in data-centers or POPs or cell-sites

Mobile core networks

Like all core networks, the mobile core handles transport of user data, with

- very high data rates
- relatively small number of network elements and links
- relatively stable environment

Mobile core networks were originally circuit switched (SDH)
but have migrated to packet switching

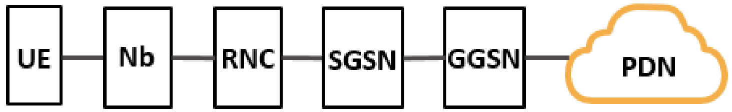
The mobile core network is more like a PSTN core than an Internet AS core
since it supports:

- voice traffic (at least until 4G)
- *user* (not necessarily true end-user) management
  - mobility management (tracking where users are)
  - user profile, home location
  - authentication and registration
  - billing (charging)
- session management (call establishment, management and termination)
- lawful interception (CALEA)
- QoS (network neutrality may not be relevant for mobile)

Cores from 3G to 5G

3G data the Nb+RNC connect to the SGSN and GGSN

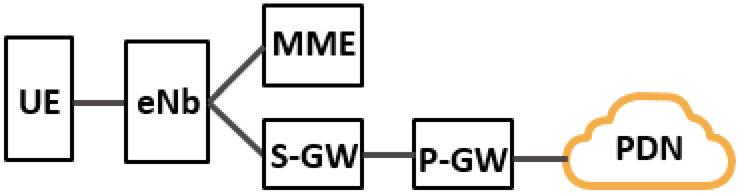
SGSN and GGSN handle both user and control



4G Nb+RNC were unified into the eNB

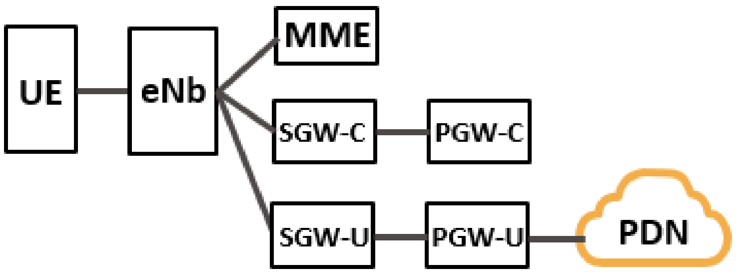
eNB connects to S-GW and P-GW

Mobility management was separated



4G CUPS (R14) separates into UPF and CPFs

S-GW-C and S-GW-U,   P-GW-C, P-GW-U



5G

- decomposes the MME into AMF and SMF
- unifies all UPF (S-GW-U and P-GW-U) into the UPF
- unifies S-GW-C, P-GW-C and MME session management into SMF
- reorganizes functions as *micro-services*

Simplified 5G core – reference points

AUthentication **S**erver **F**unction

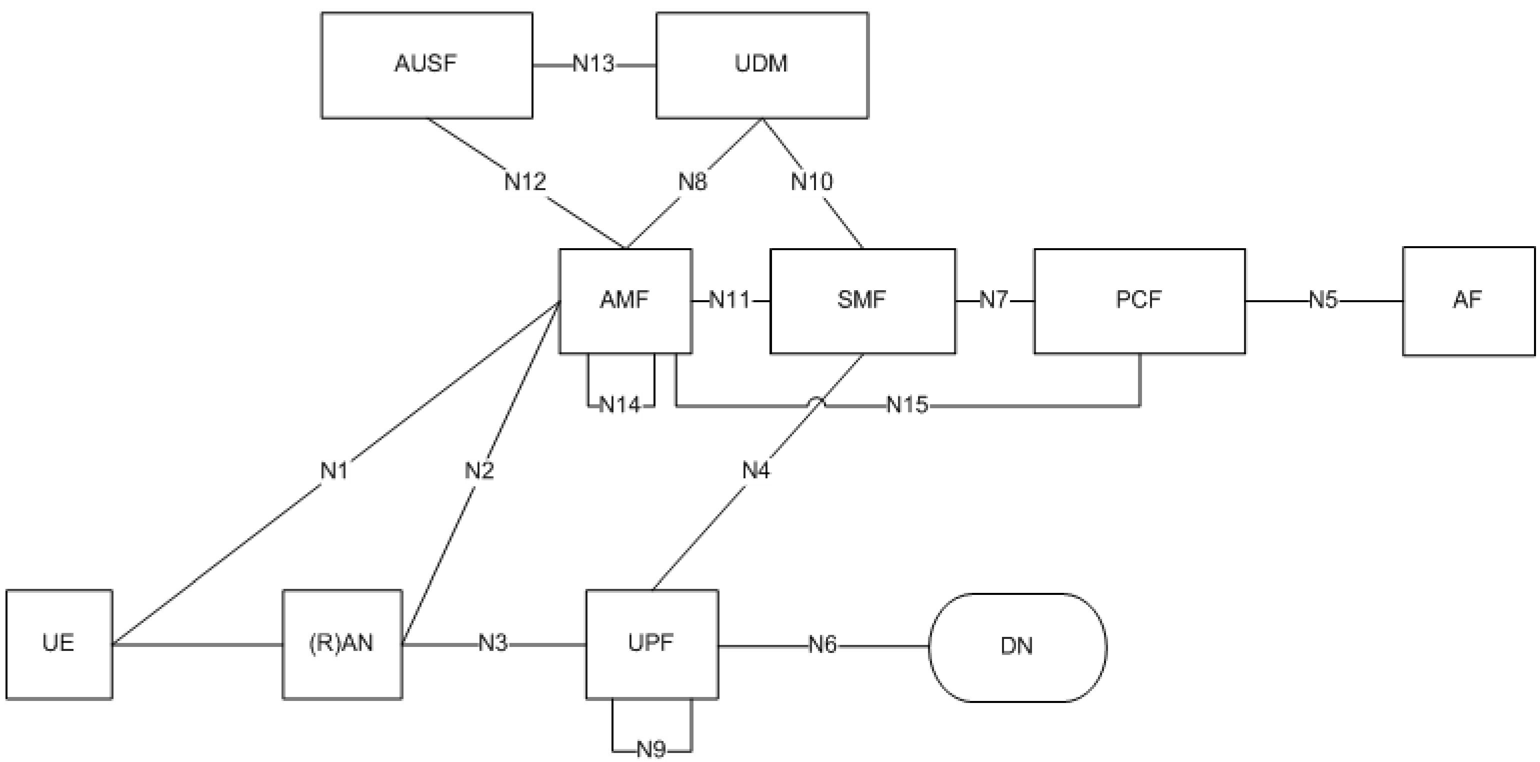
Unified **D**ata **M**anagement

Access & **M**obility Management **F**unction
Policy **C**ontrol **F**unction

Session **M**anagement **F**unction
Application **F**unction

User **P**lane **F**unction

Data **N**etwork



UPF, AMF, SMF

The **U**ser **P**lane **F**unction performs all the user plane functions handled in 4G by S-GW-U, P-GW-U (and TDF) including:

- packet routing and forwarding
- anchor for mobility and connection to external data networks (Internet)
- optionally Firewall and Network Address Translation (NAT) functions

The **A**ccess and **M**obility **F**unction performs the access and mobility functions that were handled by the 4G MME, S-GW-C and P-GW-C

- mobility/reaachability management
- NAS signaling for access and mobility management
- UE authentication
- allocation of **T**emporary **M**obile **S**ubscriber **I**dentity

The **S**ession **M**anagement **F**unction performs the session management functions that were handled by the 4G MME, SGW-C, and PGW-C

- NAS signaling for session management
- managing the PDU sessions
- allocates IP addresses to UEs (DHCP server)
- selection and control of UPF

AFs and capability exposure

In order to enable new service types and integrate with vertical industries
5G core functionalities will be made available to 3rd parties, including

- application service providers
- end-users (vehicles, factories, smart cities, etc.)

5G learned from MEC the importance of capability exposure
and defined the **N**etwork **E**xposure **F**unction

The NEF, like MEC's **M**obile **E**dge **P**latform, can be queried via an API
to discover available services

Capability exposure is a very common feature of web-based services
and the modern way of providing such services is via RESTful APIs

3GPP completely re-architected the core to be RESTful
resulting in the **S**ervice **B**ased **A**rchitecture

In SBA, all the core network functions are defined as RESTful servers
with APIs called **S**ervice **B**ased **I**nterfaces

5GC Architecture Principles

Modular Function design based on **N**etwork **F**unctions – not boxes

- NFs can be hardware or (virtual) software – even in cloud
- reference points between NFs
- function separation for scaling (e.g., AMF/SMF, AUSF/PCF)

Use of

- **N**etwork **F**unctions **V**irtualizaiton
- **REST** APIs
- **micro-services**
- **function chaining**
- automation and programmability

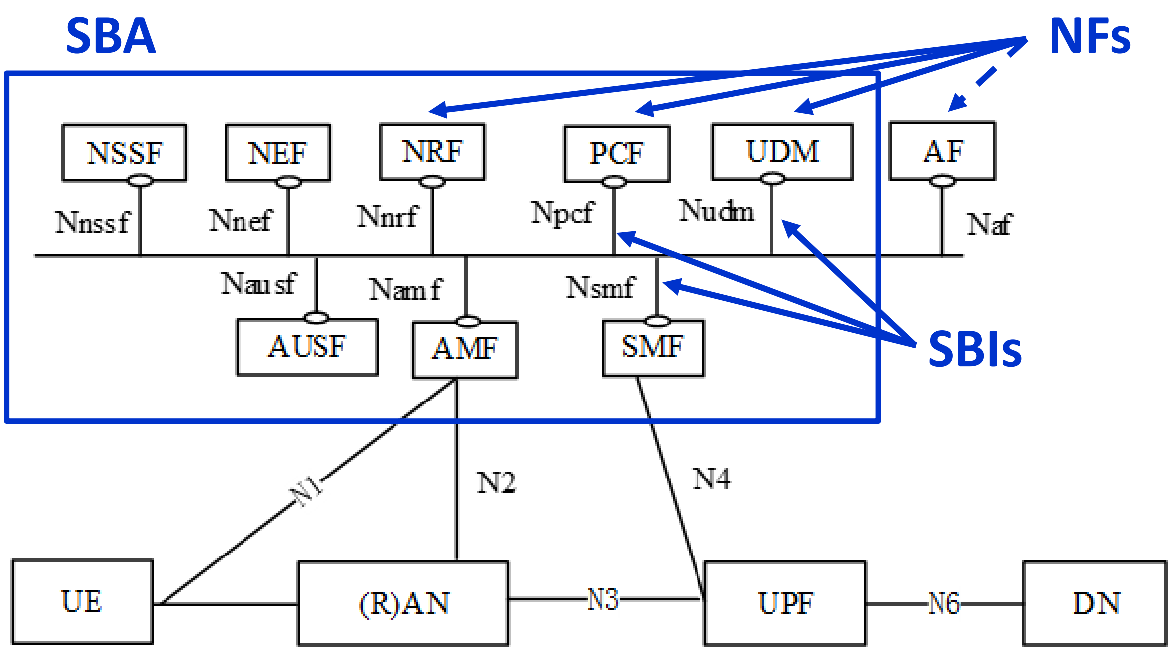
Service **B**ased **A**rchitecture

- define procedures as services (enable reuse)
- NFs in **C**ontrol **P**lane enable authorized functions to directly access services

Minimize dependencies between Access Network and Core Network

Unified database and single authentication server

Simplified 5G core – SBA



The NFs are interconnected via a *logical* bus

i.e., every NF can communicate with every other NF

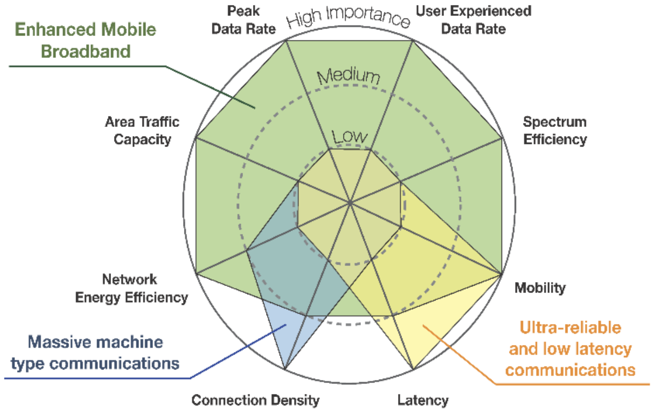
The software of one NF may or may not be on the same server as another NF

Network slicing

We already said that 5G can't reach all of its goals simultaneously
but it doesn't have to

For example:

- enhanced mobile broadband
  - needs high data rates
  - doesn't need very low latency
- massive IoT
  - needs high connection density
  - doesn't need high data rates



So, 5G using *network slicing* to satisfy needs of different devices/apps

Network slicing means:

- *on-demand* assignment of networking/computational resources
  - resources: bandwidth, forwarding tables, processing capacity, etc.
- resources can be physical or virtual, but
- each slices acts as a (strongly) isolated network or cloud
  - isolation of performance, security, and management aspects

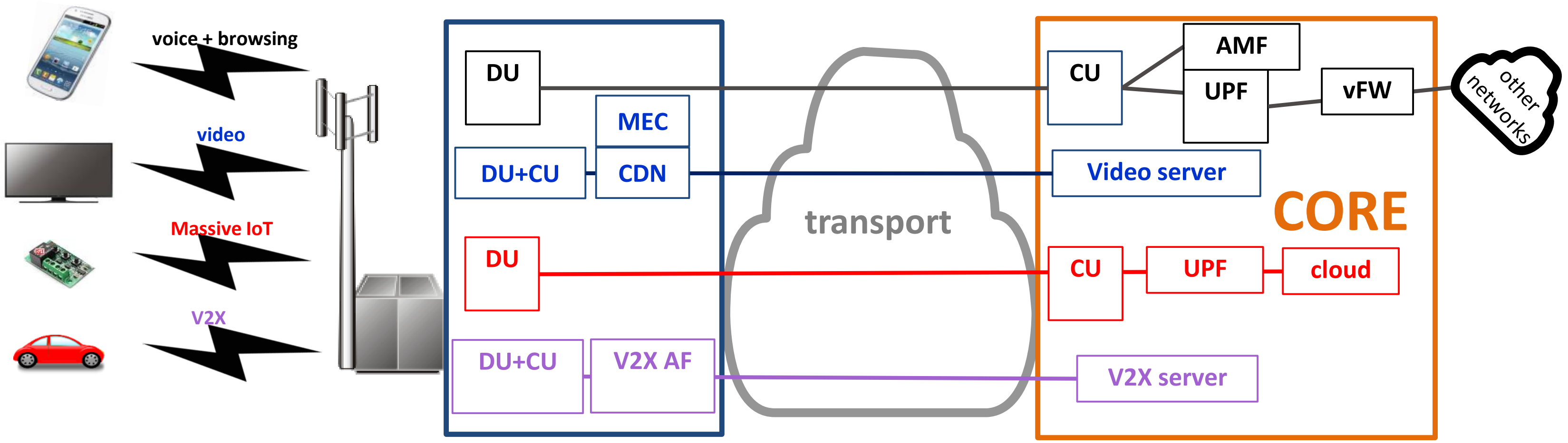
Slicing, again

Slicing is not only about dynamically separating *transport flows*

The decomposition of the gNB and virtualized functions
play an essential role in network slicing

A slice that requires a definitive response within a short time
needs edge computation which is only possible after the PDCP in the CU
and probably needs edge computation (MEC)

A slice that serves video can benefit from local breakout and CDN



Privacy and security

5G needs to address various security and privacy threats

- Privacy enforcement – protecting user's identity and blocking impersonation
- Authorization – preventing unauthorized access to resources
- Source authentication – confirming the source of a message
- Integrity – preventing tampering with messages
- Confidentiality – preventing eavesdropping

5G's trust model includes more actors than previous generations

- UE
- new host types (laptops, IoT, vehicles)
- home network
- serving network
- new transport mechanisms
- cloud service providers
- third-party application function providers
- private network operators
- direct peer-to-peer connections (e.g., for V2V)

and a priori no entity trusts any other entity

5G privacy

5G enhances user *privacy* as compared to previous generations

- user identity cloaking
- user location confidentiality
- user activity masking

by *never* sending an IMSI in plaintext

5G defines

- **SU**bscription **P**ermanent **I**dentifier
  (IMSI or *email address* user@network for non-3GPP)
  which is never sent over the air interface
- **SU**bscription **C**oncealed **I**dentifier (pronounced Suchi ☺)
  which is freshly cryptographically generated by the UE
  before being sent *once* over the air interface

5G security

5G defines 3 hierarchical *strata*

- Transport stratum
- Network stratum - *Serving* and *Home* Networks
- Application stratum

and 5 *security domains*

- Network access security
- Network domain security
- User domain security
- Application domain security
- SBA domain security

The 5GC is secured by

- TLS (https)
- Oauth
- SEPPs using *telescopic FQDNs*
- SEAF