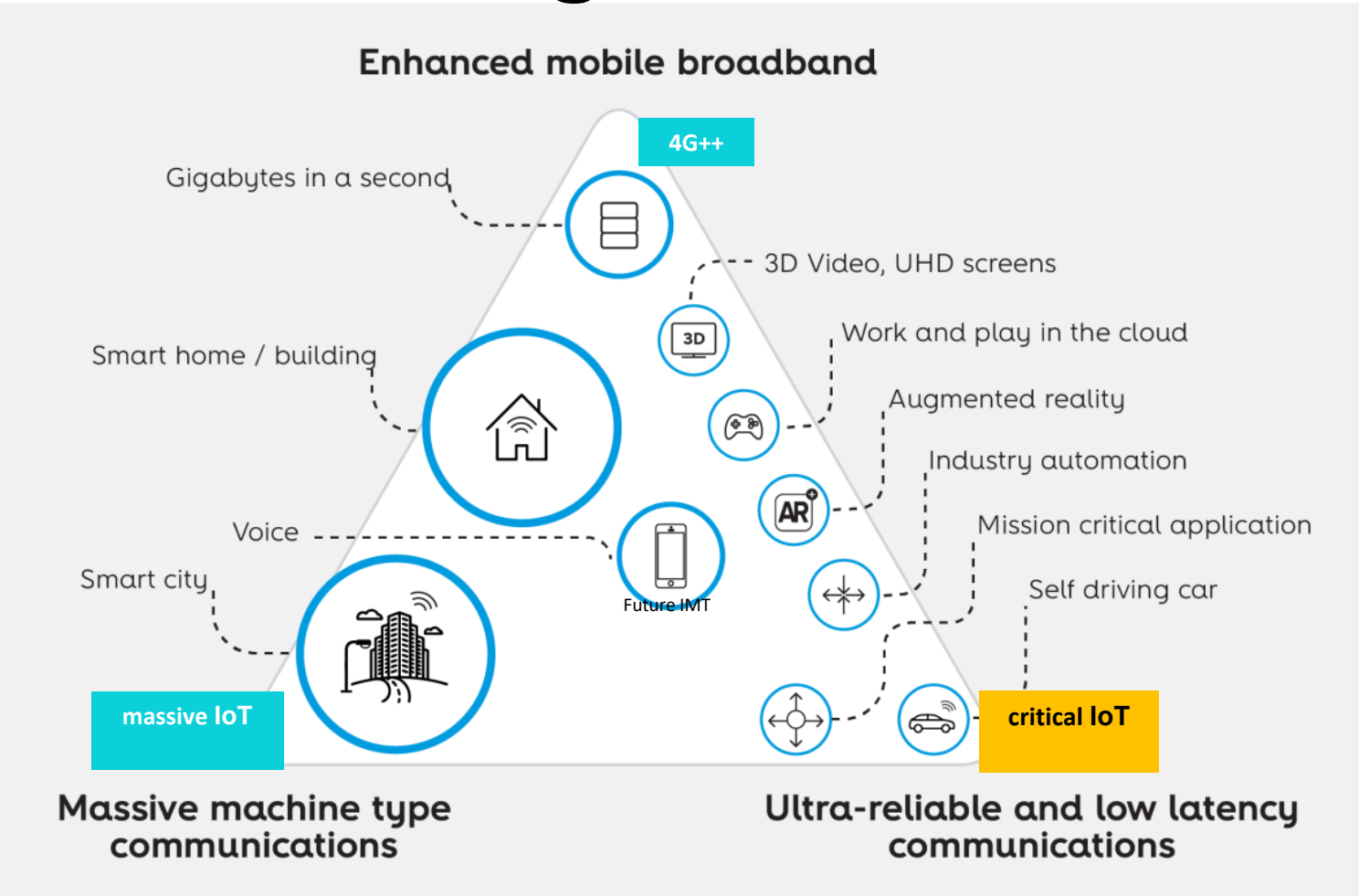
5G Introduction
5G RAN
5G Core
5G Identifiers
Protocols

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*)

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

A trillion of devices with different needs	GB transferred in an instant	Mission-critical wireless control and automation

…while driving down the cost per managed bit

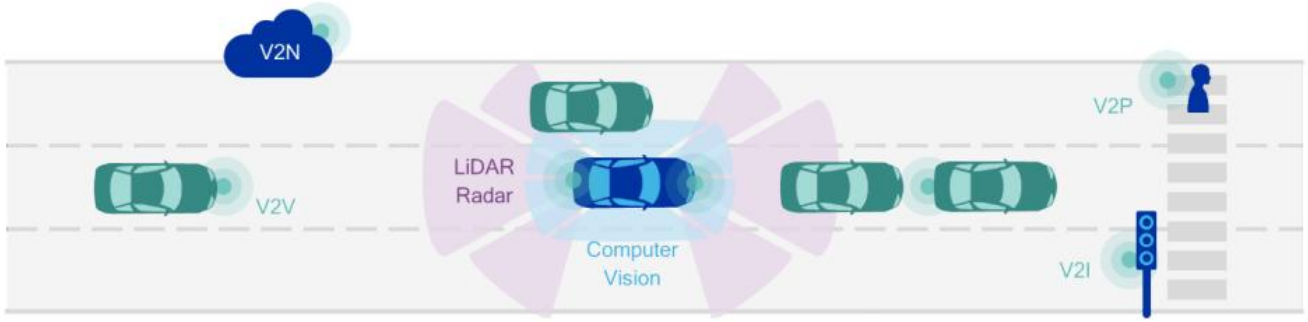
Example of verticals: 5GAA (*5G Automotive Association*)

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:

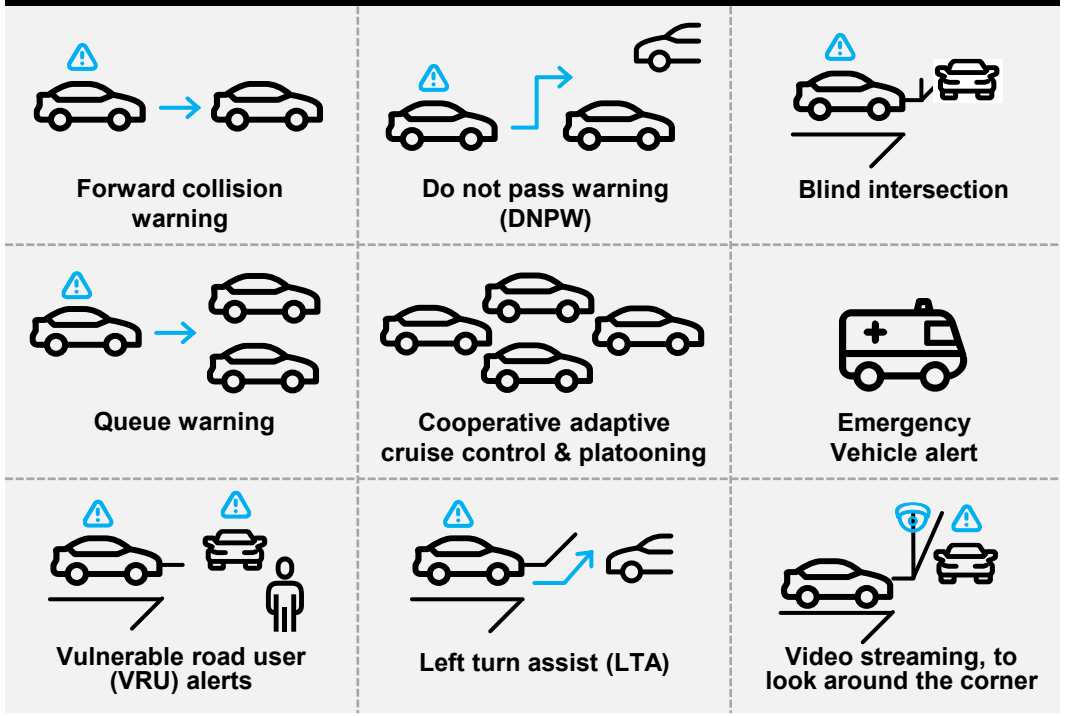
- Vehicle to Vehicle (V2V)
- Vehicle to Network (V2N)
- Vehicle to Infrastructure (V2I)
- Vehicle to Pedestrian (V2P)



MEMBERS

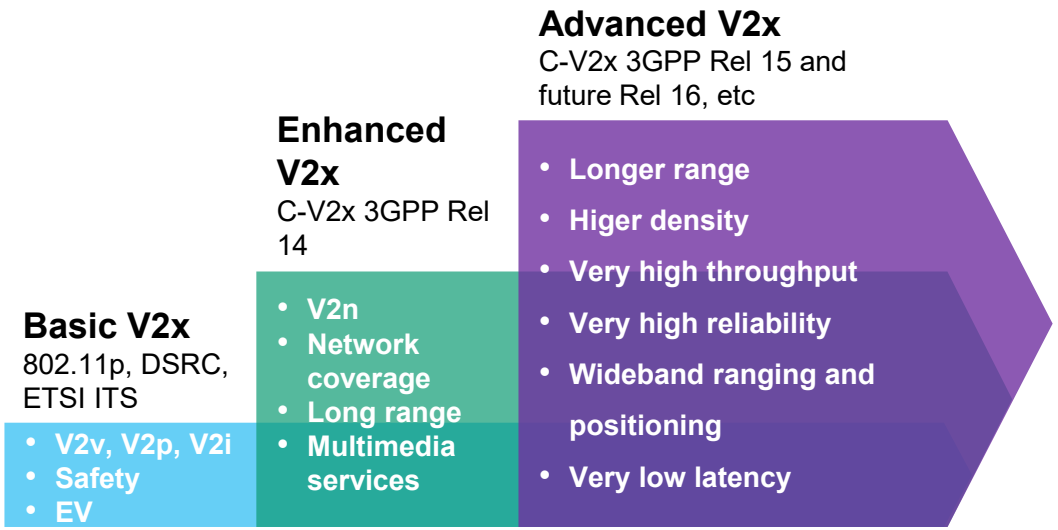
V2x Use Cases

V2x enables a broad set of use cases



Adapted from Qualcomm

3GPP V2x evolutionary support



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

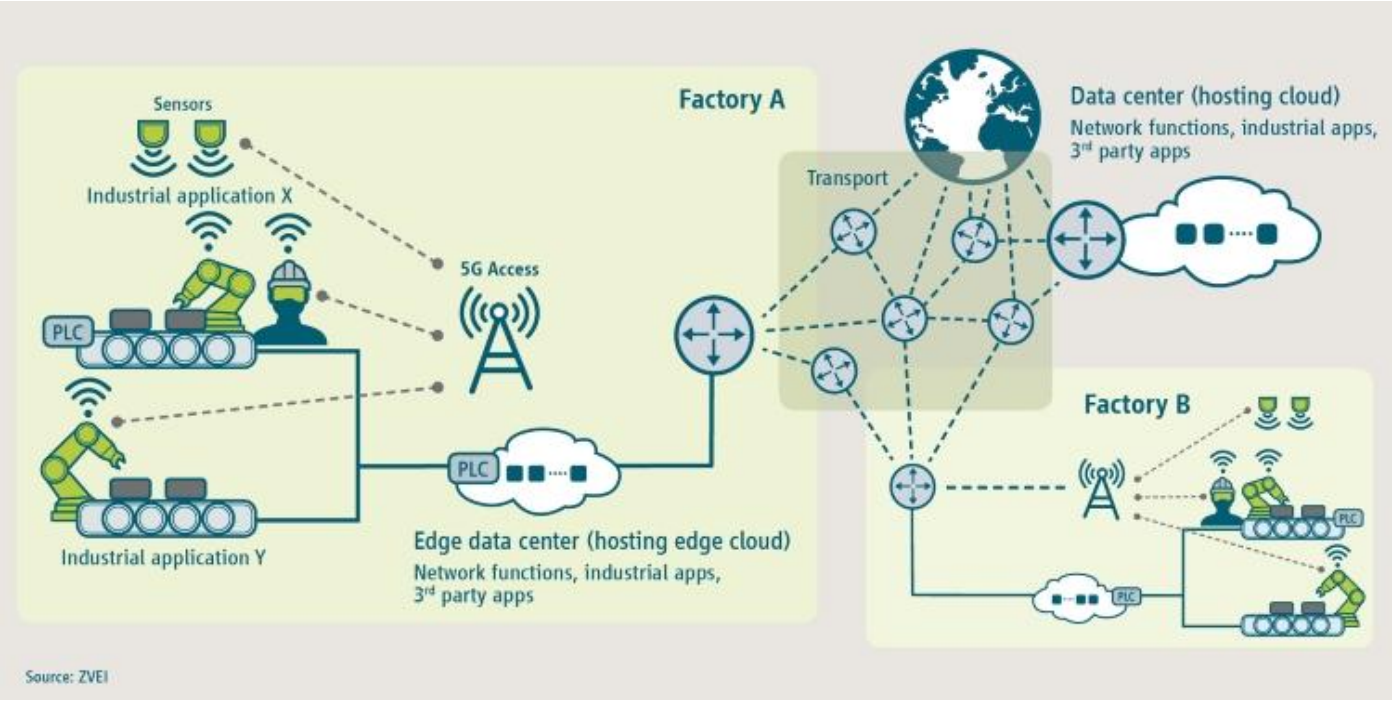
Communication scenario description	Max end-to-end latency (ms)	Reliability (%)
Information exchange between a UE supporting V2X application and a V2X Application Server	5	99.999
Cooperative driving for vehicle platooning Information exchange between a group of UEs supporting V2X application.	10	99.99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

3GPP TS 22.186

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

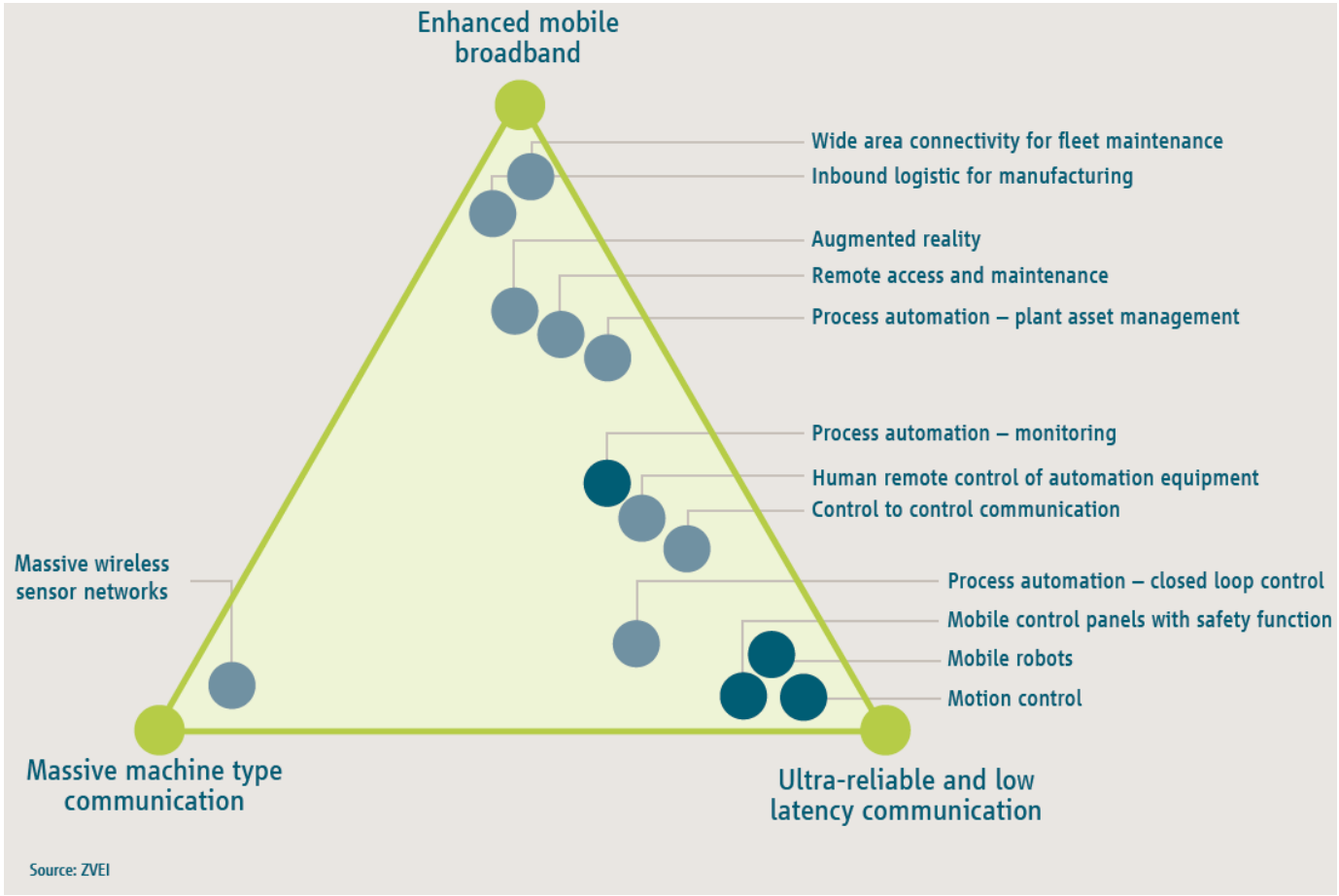
5G ACIA

5G Alliance for Connected Industries and Automation

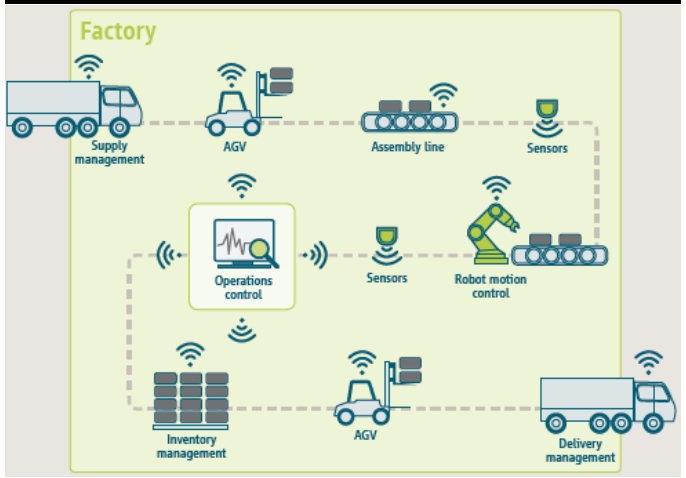
Industry use cases

- 5G in the private domain

Overview of selected industrial use cases and arrangement according to their basic service requirements (5G-ACIA)



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	Printing machine	>99.9999%	< 2 ms	20 bytes	>100	100 m x 100 m x 30 m
	Machine tool	>99.9999%	< 0.5 ms	50 bytes	~20	15 m x 15 m x 3 m
	Packaging machine	>99.9999%	< 1 ms	40 bytes	~50	10 m x 5 m x 3 m
Mobile robots	Cooperative motion control	>99.9999%	1 ms	40-250 bytes	100	< 1 km²
	Video-operated remote control	>99.9999%	10 – 100 ms	15 – 150 kbytes	100	< 1 km²
Mobile control panels with safety functions	Assembly robots or milling machines	>99.9999%	4-8 ms	40-250 bytes	4	10 m x 10 m
	Mobile cranes	>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 km²	

Service unavailability <31,5s / Year

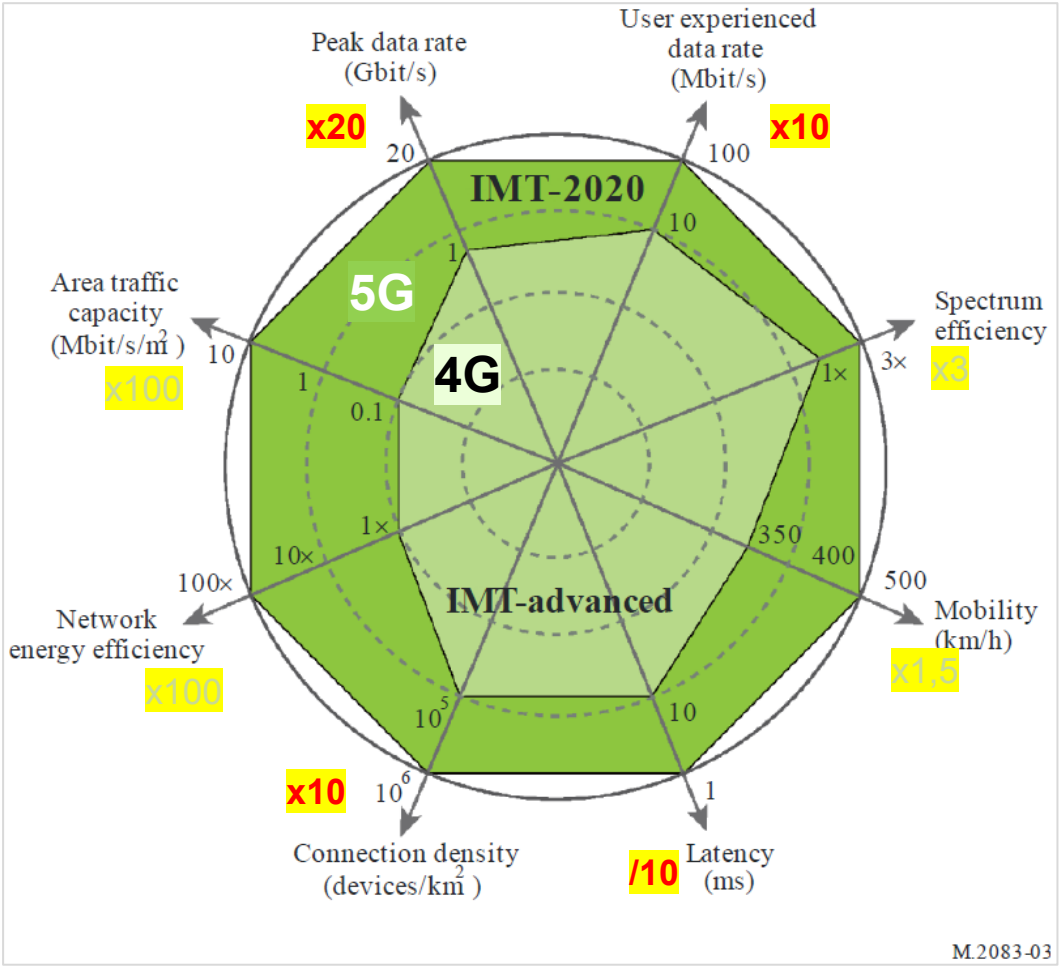
Cycle time shall be measured from command execution to feedback received ➔ 5G latency < half the cycle time

Pictures from: 5G-ACIA, "5G for Connected Industries and Automation", Whitepaper, Apr'18

5G performance improvement requirements

Metric	Requirement	Comments
Peak data rate	**DL: 20 Gbit/s** **UL: 10 Gbit/s**	assignable to a single mobile station
Peak spectral efficiency	**DL: 30 bit/s/Hz** **UL: 15 bit/s/Hz**	assignable to a single mobile station
User experienced data rate	**DL: 100 Mbit/s** **UL: is 50 Mbit/s**	5% point of the cumulative distribution function (CDF) of the user
Area traffic capacity	**10 Mbit/s/m^2**	indoor hotspot, eMBB
User plane latency	**4 ms for eMBB** **1 ms for URLLC**	contribution of the radio network; one-way; small IP packets (0 byte payload + IP header), for UL and DL
Control plane latency	**20 ms**	transition time from Idle to Active state; eMBB and URLLC
Connection density	**1 000 000 devs per km2**	mMTC
Mobility	**500 km/h**	High speed vehicular, Rural – eMBB
Reliability	**1-10^{-5}**	32 bytes, L2 PDU, within 1 ms, 20 bytes application data + protocol overhead

ITU-R, "M.2410-0 - Minimum requirements related to technical performance for IMT-2020 radio interface(s)," 2017.

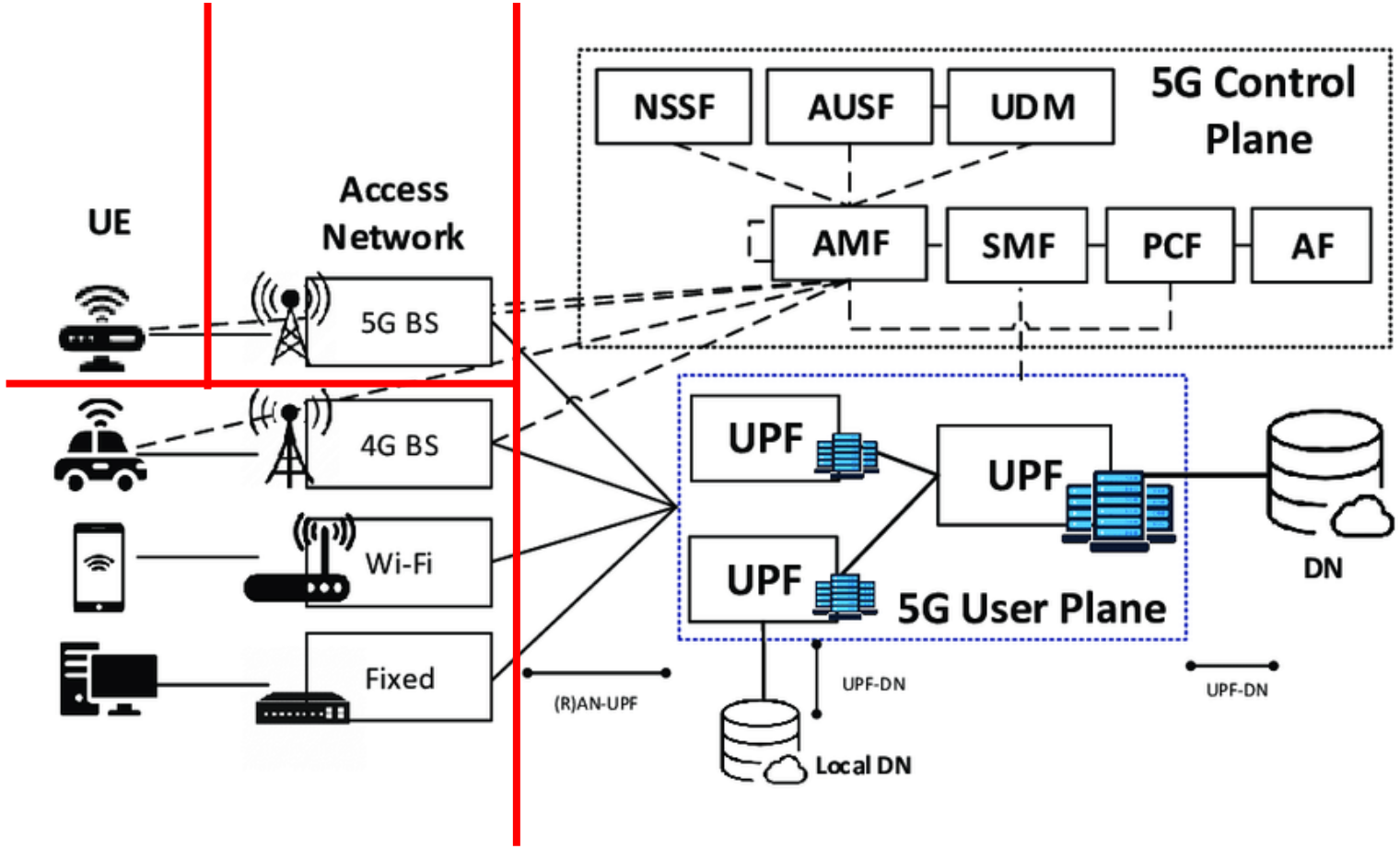


ITU-T, M.2083

5G System

Three major sub-systems:

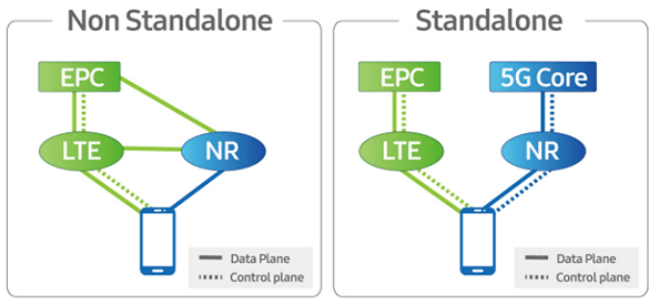
1. UEs (or MT)
2. RAN
3. Core



4G-5G migration paths: 5G SA vs NSA

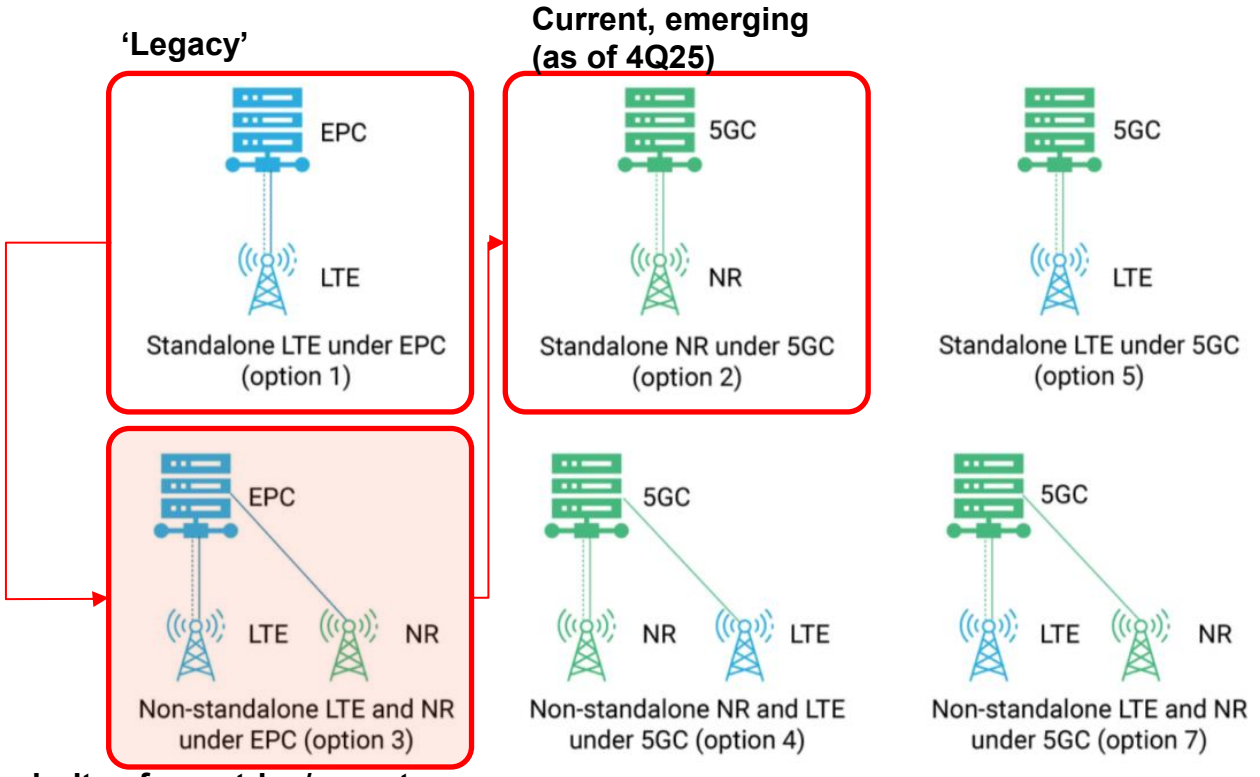
Non Stand Alone (NSA) architecture

- Uses 4G as an anchor for radio access
- The 4G Core controls the sessions
- Adds 5G spectrum for higher bitrates
- It will basically bring more speed, less latency and densification



Stand Alone (SA) architecture

- Works without 4G
- Uses a dedicated core (5G Core) that can be convergent (support ng-eNB)
- Allows new services to exploit network slicing and edge computing
- With pure 5G SA, bandwidth may decrease!



https://www.5g-networks.net/5g-nsa-and-5g-sa-networks-compared/

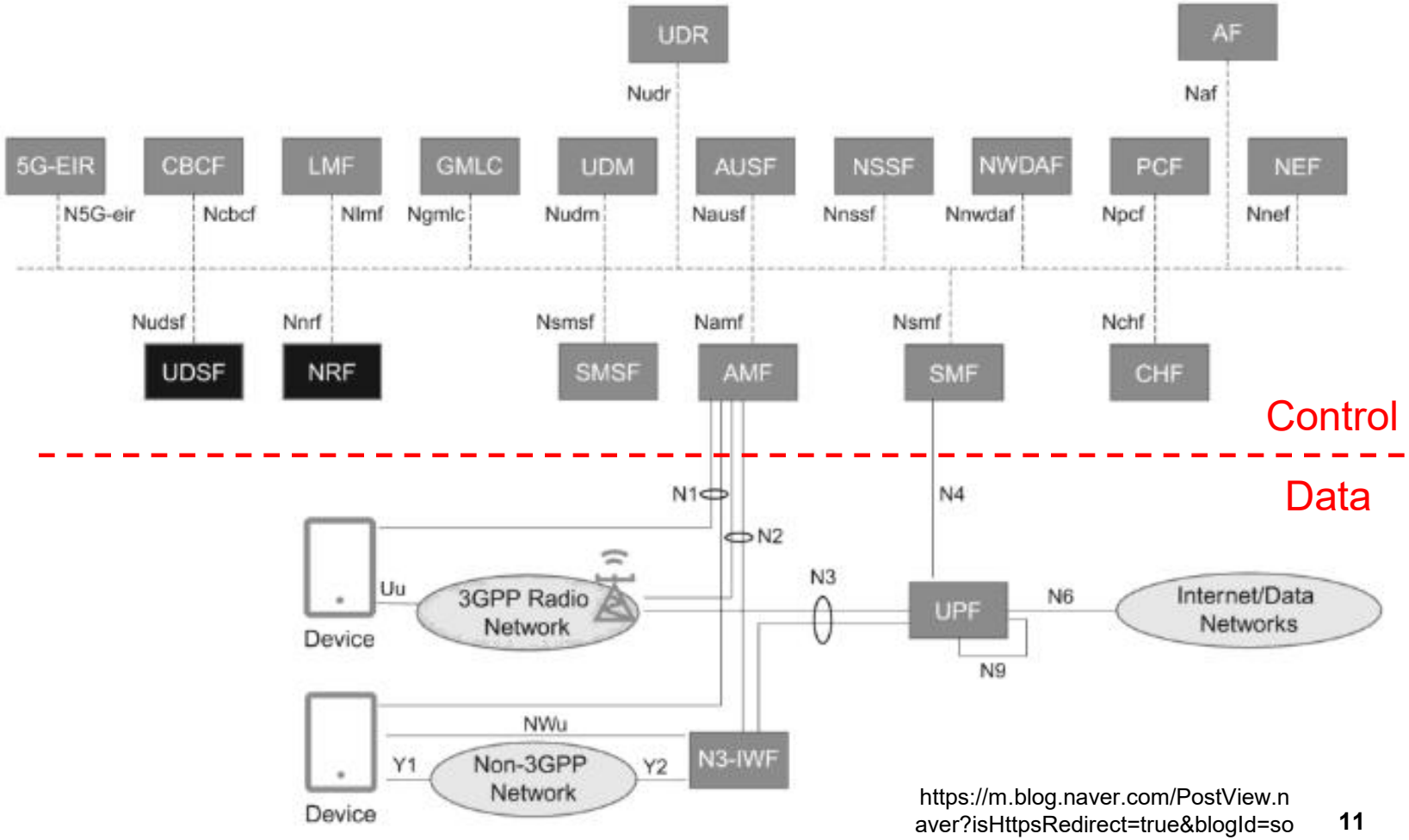
5G System architecture

SBA: *Service Based Architecture*; Service based representation, where *Network Functions* (NF), e.g. AMF, within the control plane, enables other authorized network functions to access their services

Network Funtions (NFs) follow the web-based approach using RESTful client server communication

Each NF service exposes and makes available its functionality (services) through a *Service Based Interface* (SBI), which employs a well-defined REST interface using HTTP/2.

NFs are self-contained, independent and reusable



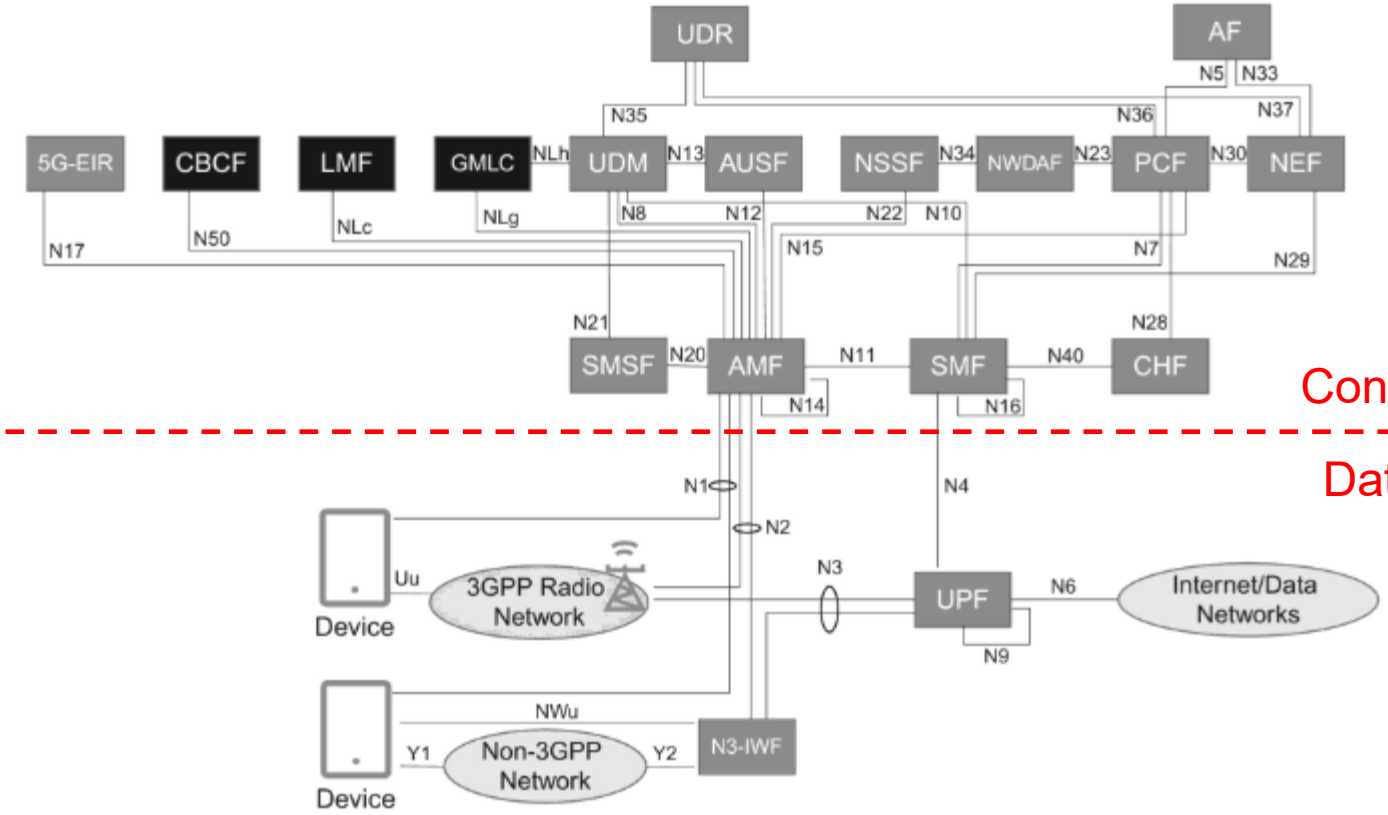
https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=song_sec&logNo=222025295180

5G System architecture

References points representation

- **Shows the existing interactions between NFs, requesting services from others NF**
- **Interactions identified by point-to-point reference point (e.g. N11)**
- **Between communicating NFs (e.g. AMF and SMF)**

There is no all to all communication (only the ones that make sense)



AF: Application Function
AUSF: Authentication Server Function
AMF: Access and Mobility Management Function
DN: Data Network
LMF: Location Management Function
NEF: Network Exposure Function
NRF: Network Repository Function
NSSF: Network Slice Selection Function
PCF: Policy Control Function
SMF: Session Management Function
UDM: User Data Management
UPF: User Plane Function

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

https://infohub.delltechnologies.com/p/the-5g-core-network-demystified/

PDU Sessions, QoS Flows, Slices and DNN

A PDU Session, via a QoS Flow, grants connectivity between a UE and a destination in a DNN, established in a certain slice

1. PDU Session

- A **PDU (*Protocol Data Unit*) Session** is the fundamental unit of user plane connectivity in 5G
- It logically connects the **UE (User Equipment)** to a **DN (*Data Network*)** via the **UPF (*User Plane Function*)**
- Each PDU Session supports one or more **QoS Flows**, which are mapped to specific service requirements

2. Network Slice

- A **Network Slice** is a virtual network instance optimized for a specific service type (e.g., eMBB, URLLC).
- Each slice is identified by an **S-NSSAI** (***Single Network Slice Selection Assistance Information***), which includes:
  - **SST (*Slice/Service Type*)**: Defines the service category (eMBB, URLLC, mMTC, …)
  - **SD (*Slice Differentiator*)**: Optional, used to distinguish slices with the same SST
- The slice contributes to the network behavior and resource allocation for the PDU Session

3. DNN (*Data Network Name*)

- The **DNN** specifies the external DN at the UPF, the UE wants to access (similar to an APN in 4G)
- It helps route the PDU Session to the correct DN (e.g., Internet, IMS, private enterprise network) and apply suitable policies
- The DNN is associated with a specific slice and influences how the PDU Session is established
- 5G equivalent of 4G's APN

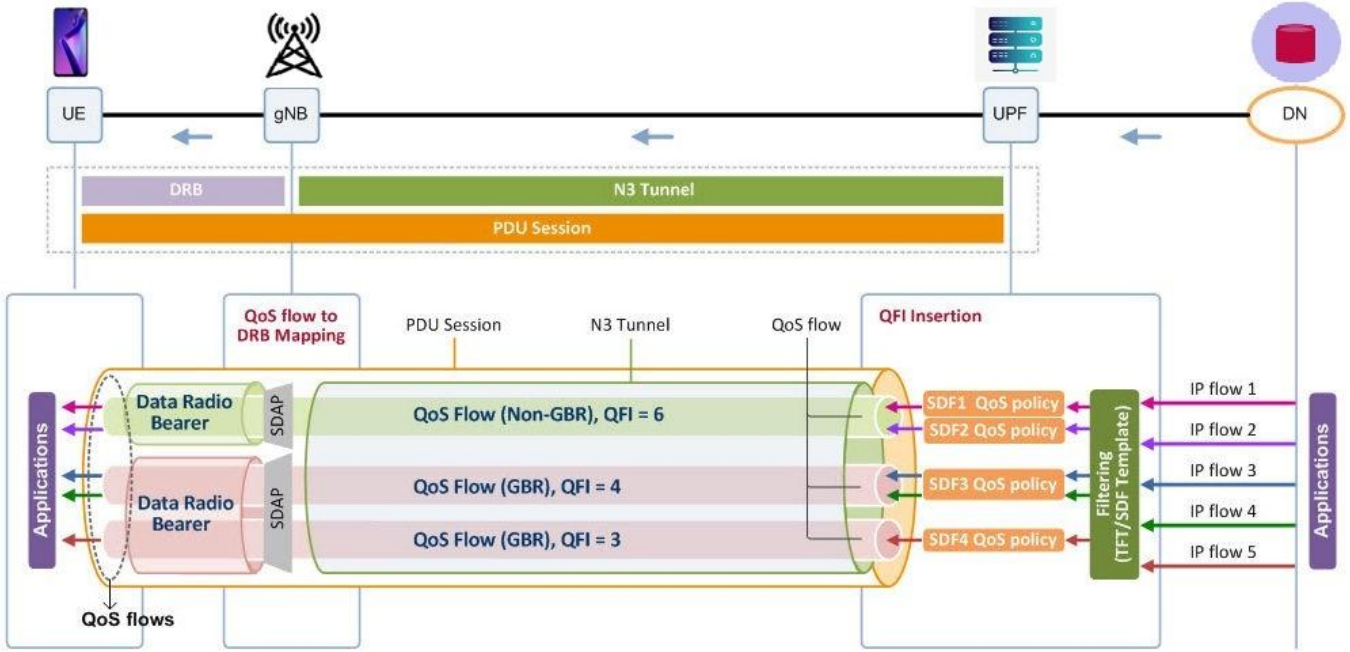
One PDU Session is mapped to a single specific Slice

Multiple PDU Sessions will exist per Slice

DNN are accessible via specific slices and multiple PDU Sessions

Multiple PDU sessions to different DNNs, maybe over different slices, can be active for a single device

PDU Sessions, QoS Flows, Slices and DNN



https://www.techplayon.com/5g-nas-pdu-session-reject-cause-values-and-reasons/

Different QoS flows: Web browsing, Video call, background synchronization…

How They Work Together

1. When a UE wants to connect to a service (e.g., Internet or an enterprise cloud), it requests a PDU session specifying both the S-NSSAI (slice) and DNN

2. The 5G Core examines these parameters to:
   - Assign the session to the appropriate network slice (determining isolation, QoS, and resources)
   - Route the session towards the correct data network as identified by the DNN

3. The selected slice and DNN govern user traffic for that session, ensuring that it receives the proper quality, security, and isolation

The combination of DNN and S-NSSAI in the PDU session ensures the correct user experience and supports use cases like network slicing for vertical industries, enterprise networks, and tailored QoS.

This architecture underpins 5G's flexibility and support for massively diverse services on a single network infrastructure.

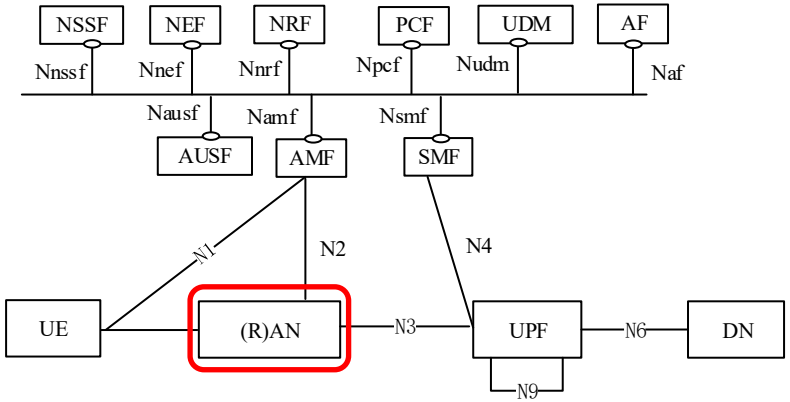
5G RAN
(NR: *New Radio*)

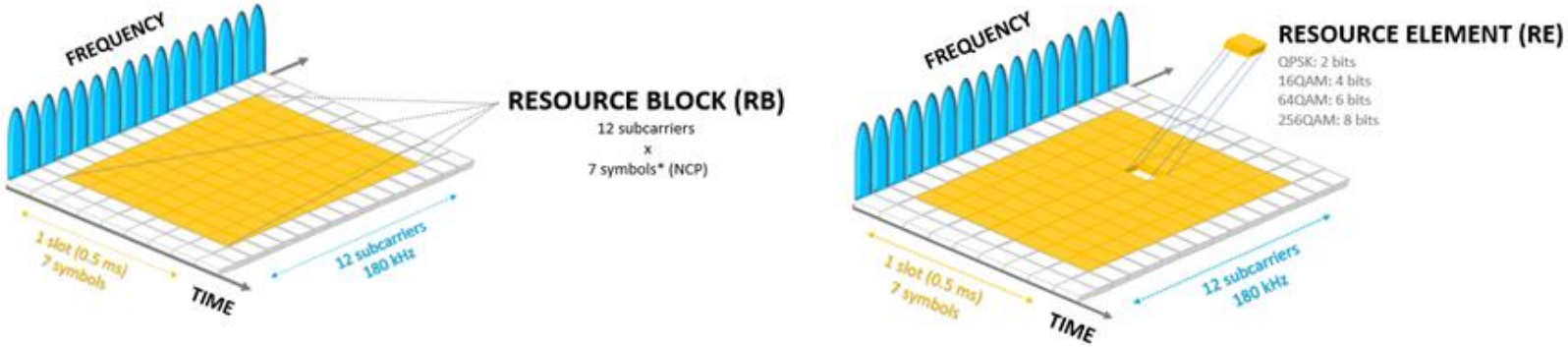
RAN

(3GPP TS 23.501)

Radio Access Network (RAN)

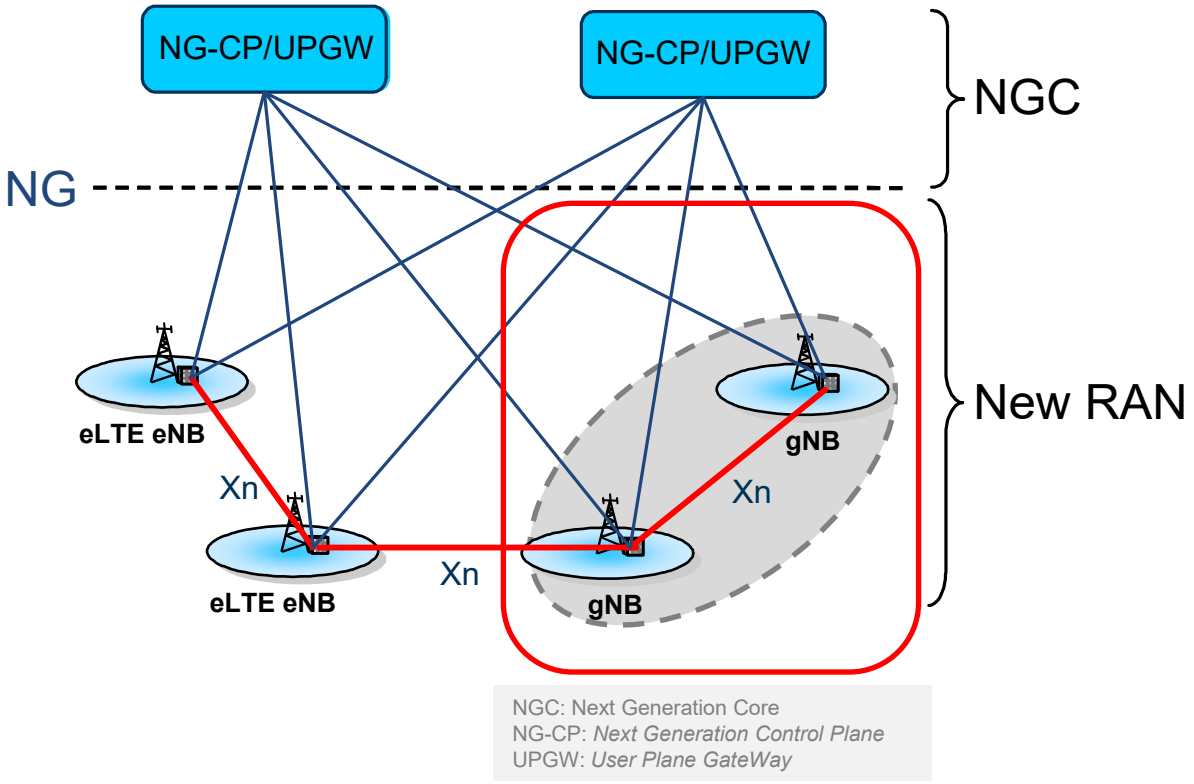
1. *Radio Resources Management* (RRM)
2. Control, Dynamic allocation of resources to UEs in both uplink and downlink (scheduling)
3. Selection of an AMF at UE attachment
4. Routing of Control Plane information towards AMF
5. Routing of User Plane data towards UPF(s)
6. Connection setup and release
7.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



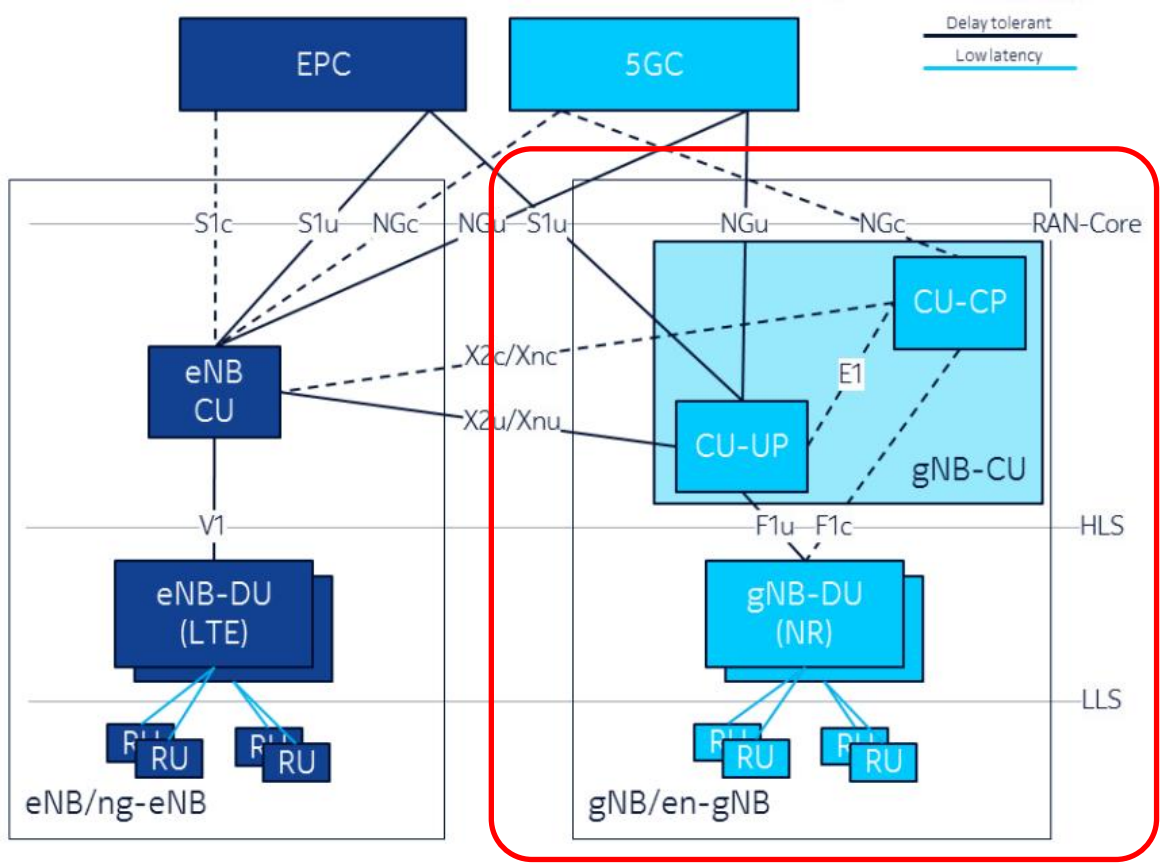


https://www.telecomhall.net/t/radio-physical-resources/11945

5G New Radio



NGC: Next Generation Core
NG-CP: *Next Generation Control Plane*
UPGW: *User Plane GateWay*



5G for URLLC

- **The <u>Ultra Reliability</u> versus <u>Low Latency</u> challenge**

Ultra-**R**eliable and **L**ow-Latency **C**ommunications

(URLLC)

Connected Vehicles (V2x)

e-Health

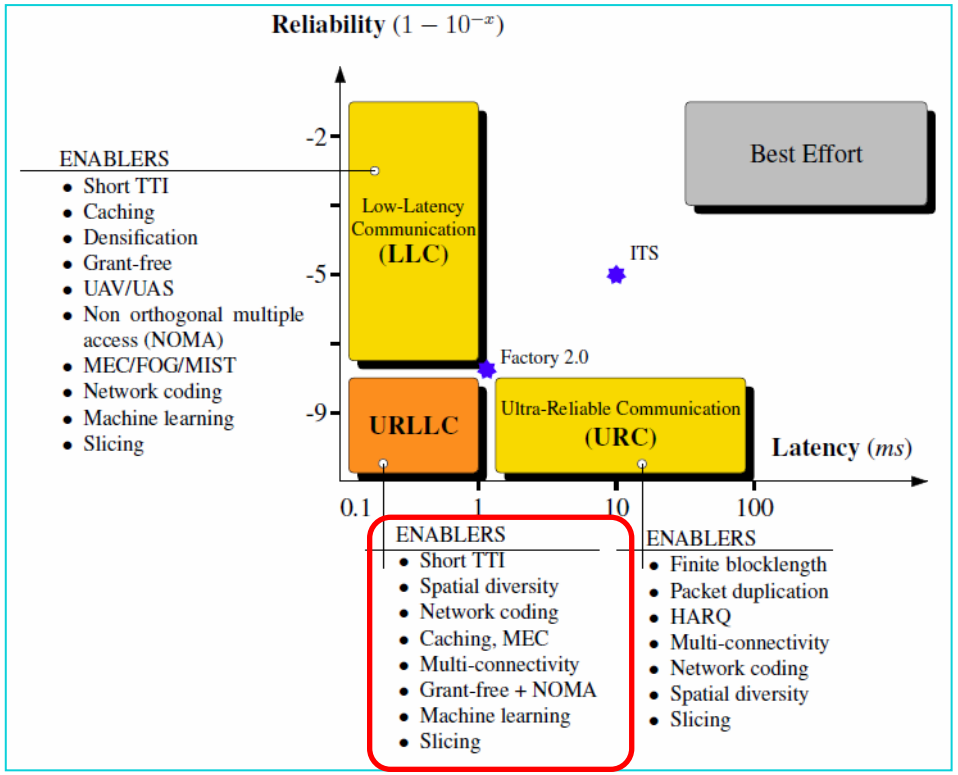
Robots / Drones

Industry 4.0

Tactile Internet

Two conflicting requirements: **Low latency and ultra-high reliability**
→ Rel-16 objective: **<u>0.5-1ms</u> one-way Latency + Reliability of up to <u>99.9999%</u>**

Mainly an access/edge problem (radio interface and edge positioning)

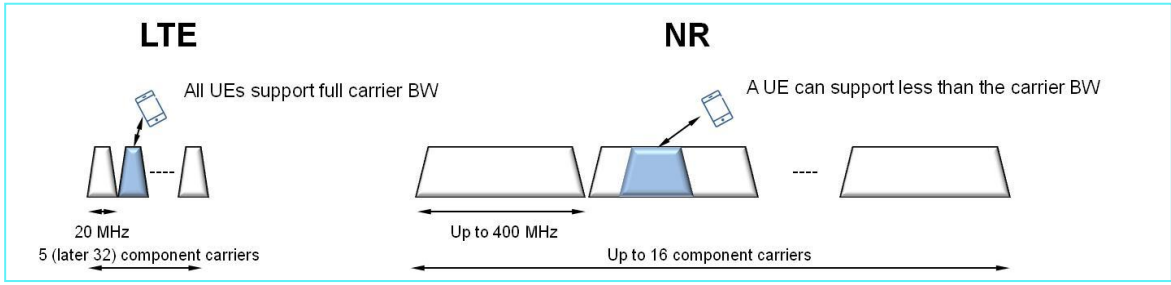


Retransmissions (e.g. HARQ) and packet duplications in time (e.g. PDCP duplications) are useless, considering the low latency budget

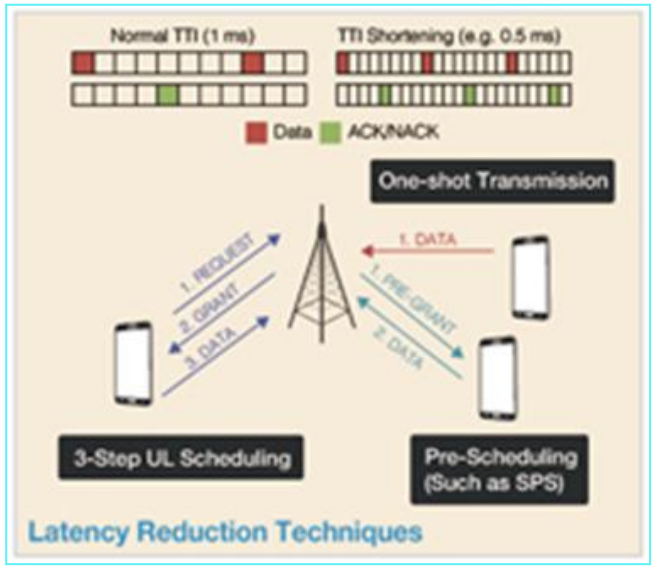
"Ultra-Reliable and Low-Latency Wireless Communication: Tail, Risk and Scale"
Mehdi Bennis, Senior Member IEEE, M'erouane Debbah, Fellow IEEE, and H. Vincent Poor, Fellow IEEE

5G-NR main characteristics

Workshop on 3GPP submission towards IMT-2020, Brussels, October 24/25, 2018
"NR Physical Layer Design: Physical layer structure, numerology and frame structure"
Havish Koorapaty 3GPP TSG RAN WG1 vice-chairman (Ericsson)



- **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



http://developer.samsung.com/sd2_images/program/content/mtech_5g09.jpg (adapted)

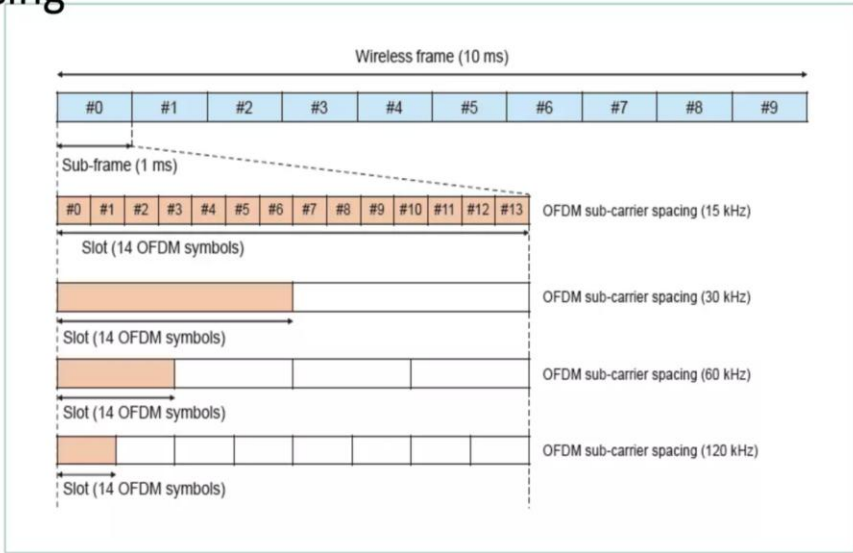
LDPC (*Low-Density Parity-Check*):
- **Improved performance**: block error rate (BLER) around or below 10^{-5} for all code sizes and code rates
- Reduced decoding complexity and **improved decoding latency** (lower overall latency)
- Better **area throughput efficiency** and **higher peak throughput**

4G/LTE:
- **Turbo codes** for **data** channels
- **TBCCs** (*Tail-Biting Convolutional Codes*) for **control** channels

https://www.sharetechnote.com/html/5G/5G_Phy_Numerology.html

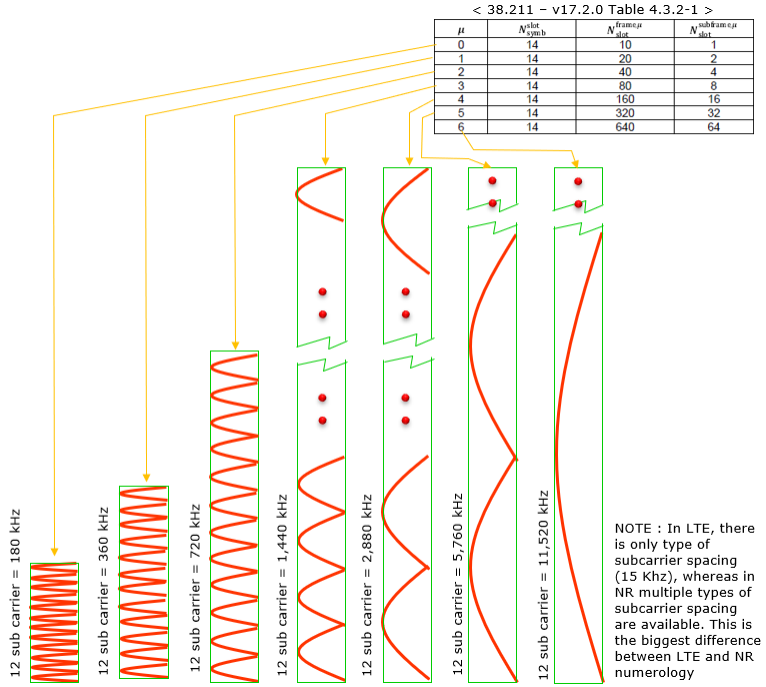
5G NR Radio Frame

- 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



< 38.211 – v17.2.0 Table 4.3.2-1 >

μ	N^{slot}_{symb}	$N^{frame,\mu}_{slot}$	$N^{subframe,\mu}_{slot}$
0	14	10	1
1	14	20	2
2	14	40	4
3	14	80	8
4	14	160	16
5	14	320	32
6	14	640	64



Source: NTT Docomo

SCP: sub-carrier spacing
Operation in higher frequencies → higher numerology

5G numerology

μ	$\Delta f = 2^{\mu} \cdot 15$ [kHz]	Cyclic prefix
0	15	Normal
1	30	Normal
2	60	Normal, Extended
3	120	Normal
4	240	Normal

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 carry 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:

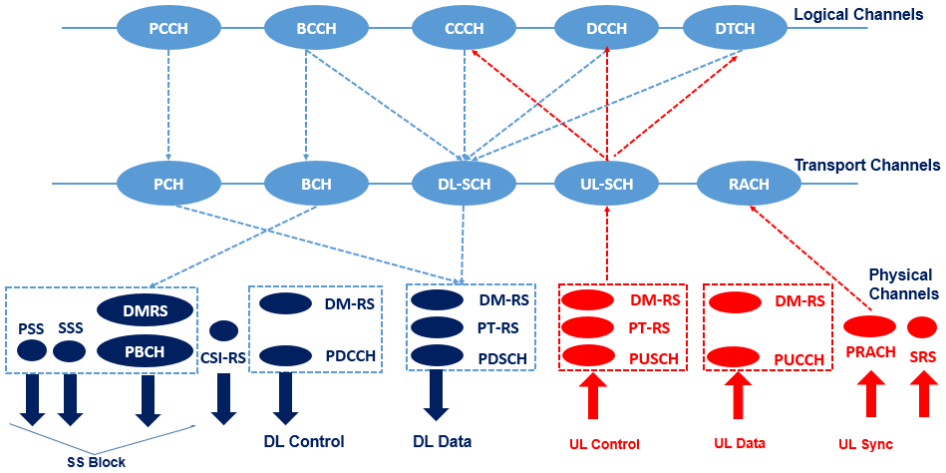
- **Broadcast Control Channel** (BCCH): Transmit system information from the network to UEs in a cell coverage.
- **Paging Control Channel** (PCCH): Page the UEs whose location at cell level is not known to the network.
- **Common Control Channel** (CCCH): It is used for transmission of control information 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.

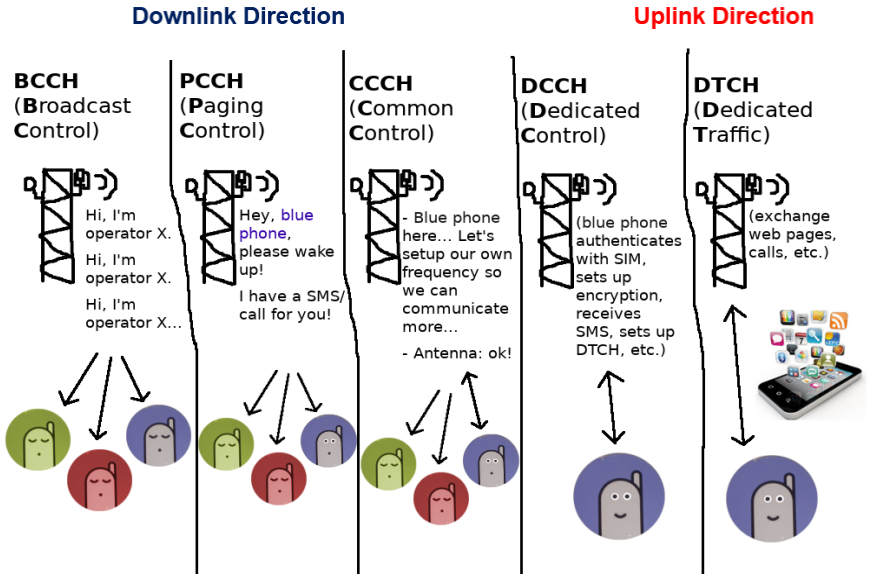
Transport Channel Definition: A transport channel is defined by how and with what characteristics the information is transmitted over the radio interface. From the physical layer, the MAC layer uses services in the form of transport channels. Data on a transport channel are organized into transport blocks.

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 DLSCH 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.

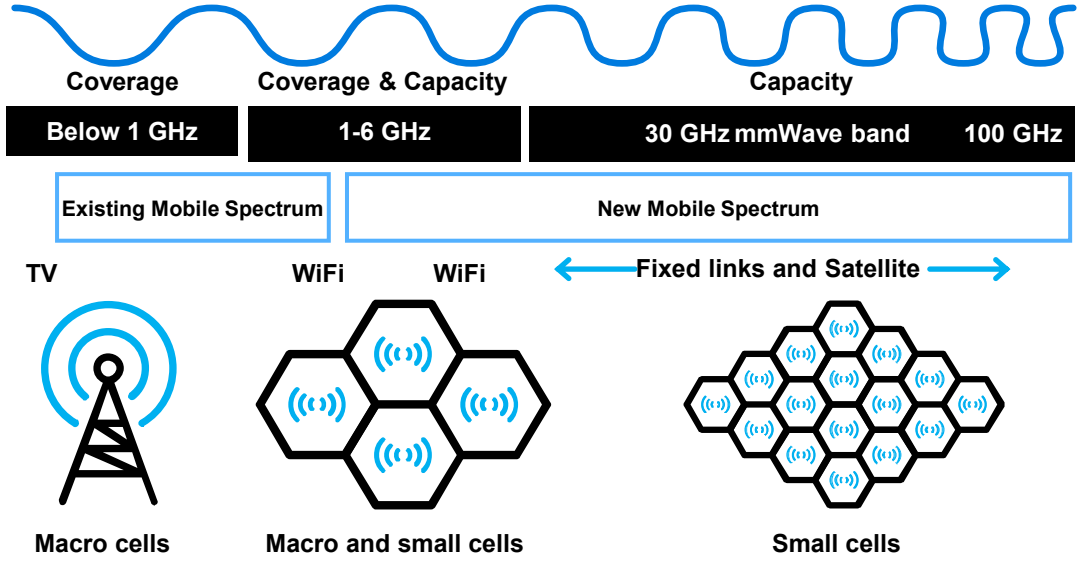
Logical, Transport and Physical Channel Mapping

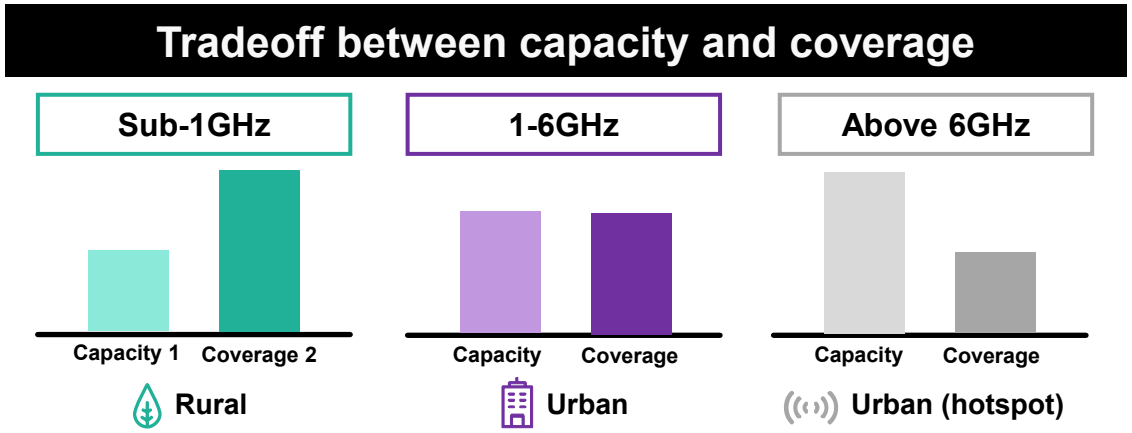




https://labs.p1sec.com/2019/07/09/presenting-qcsuper-a-tool-for-capturing-your-2g-3g-4g-air-traffic-on-qualcomm-based-phones/

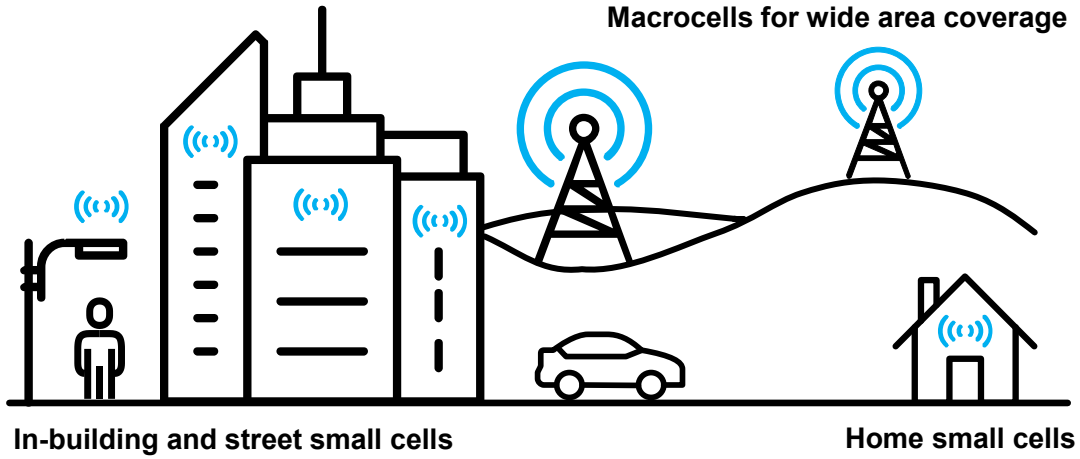
Larger spectrum usage to cover all applications





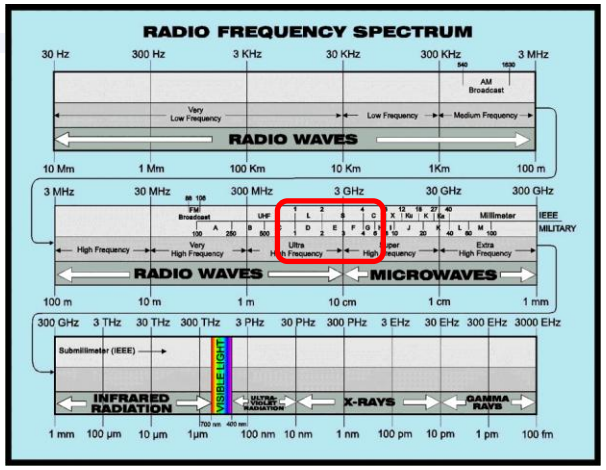
5G-NR to operate on a larger spectrum range

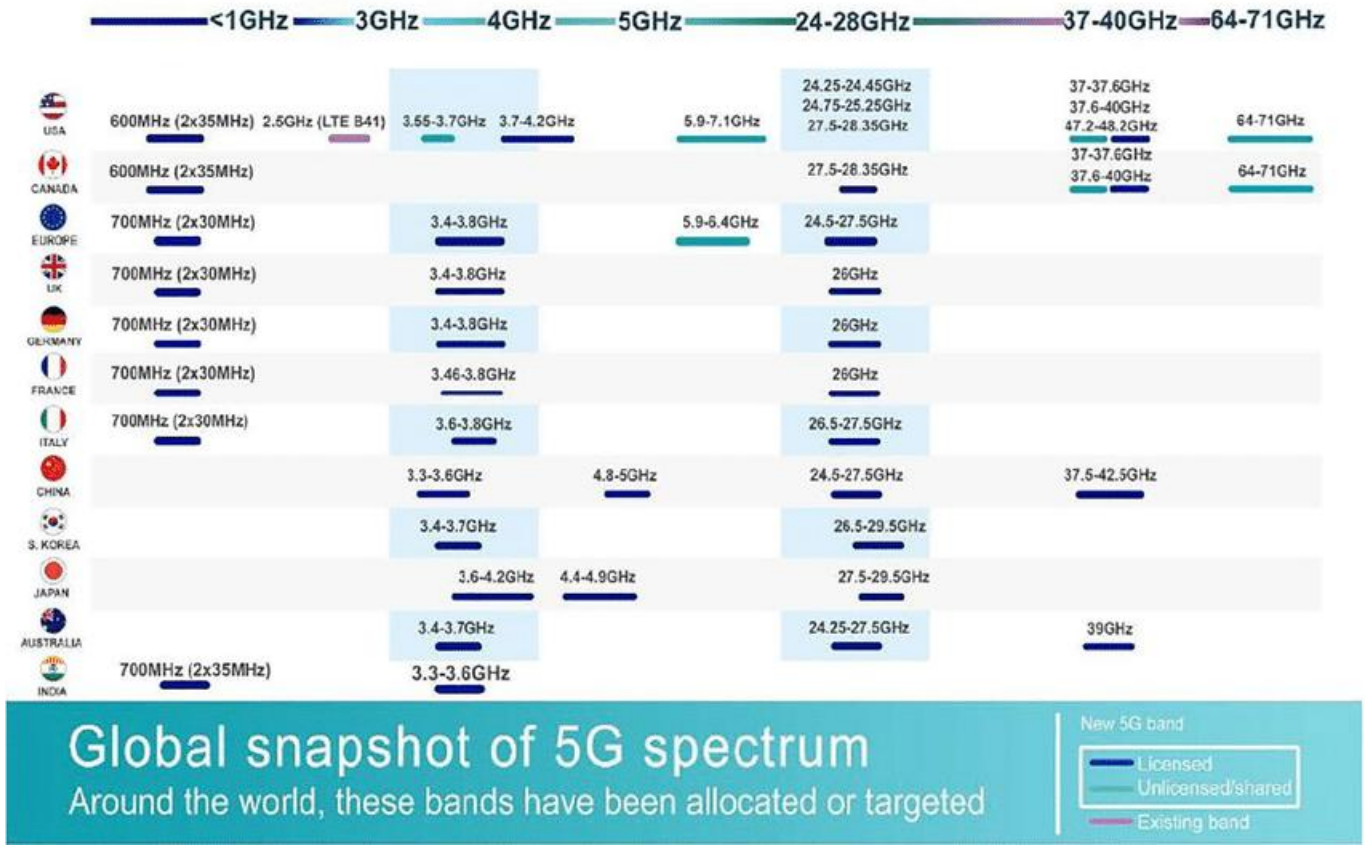
- Expanding to lower freqs. for coverage and penetration
- Expanding to higher freqs. for capacity and low latency

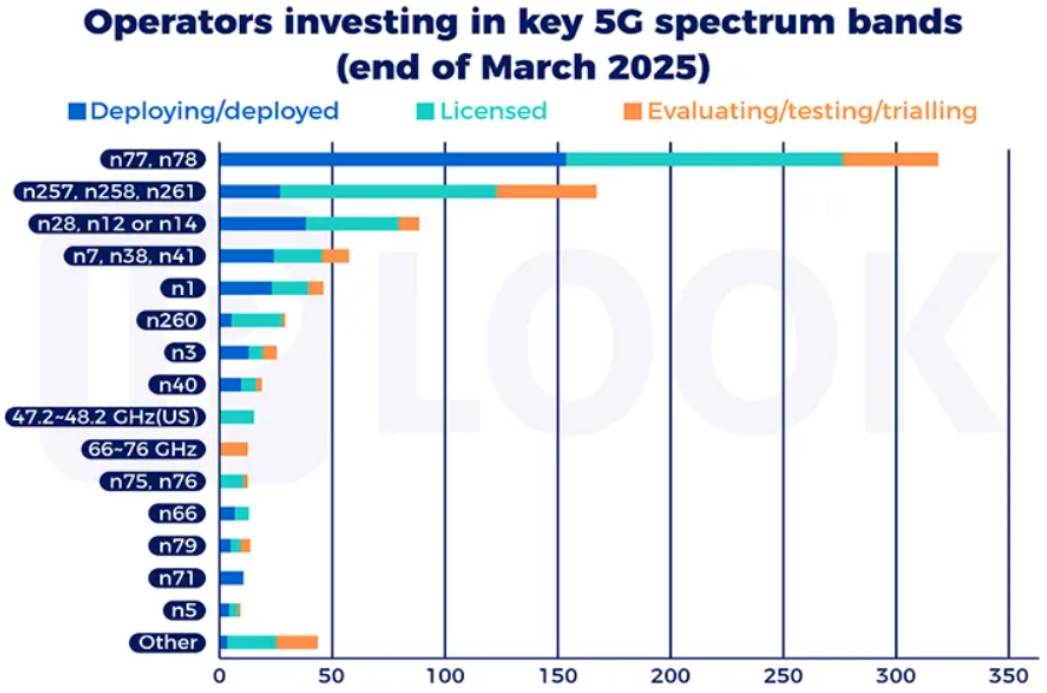


altice labs

5G Spectrum





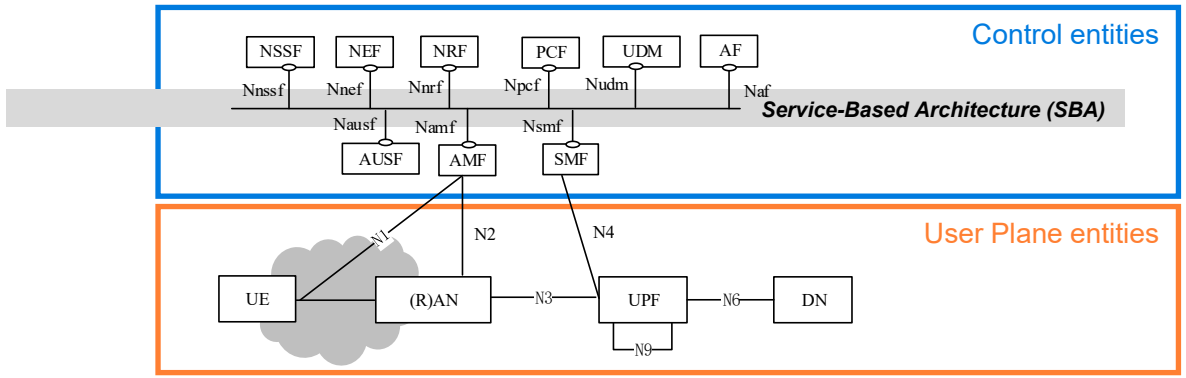


http://donsnotes.com/tech/em-spectrum.html

5G Core

5G System arch. and functional modules (parcial)

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



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)

1. Authentication Server Function (AUSF)
2. Access and Mobility Management Function (AMF)
3. Session Management Function (SMF)

1. Unified Data Repository (UDR)
2. Unstructured Data Storage Function (UDSF)
3. 5G-Equipment Identity Register (5G-EIR)
4. Security Edge Protection Proxy (SEPP)
5. Network Data Analytics Function (NWDAF)

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

- **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**

AMF, SMF and PCF

Access and Mobility Management Function (AMF)

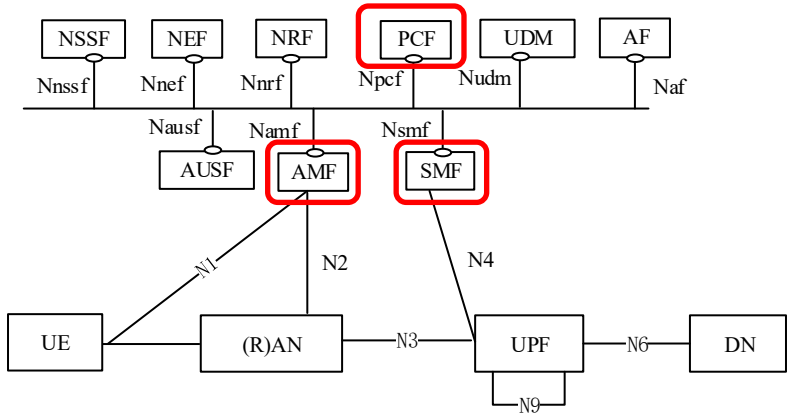
- Termination of NAS (Non-Access Stratum) signalling
- NAS ciphering & integrity protection
- Registration management
- Connection management
- Mobility management
- Access authentication and authorization
- Security context management

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)



(3GPP TS 23.501)

Security Anchor Function (SEAF)

Part of AMF

Security anchor for authentication and key management between the user equipment (UE) and the 5G Core network

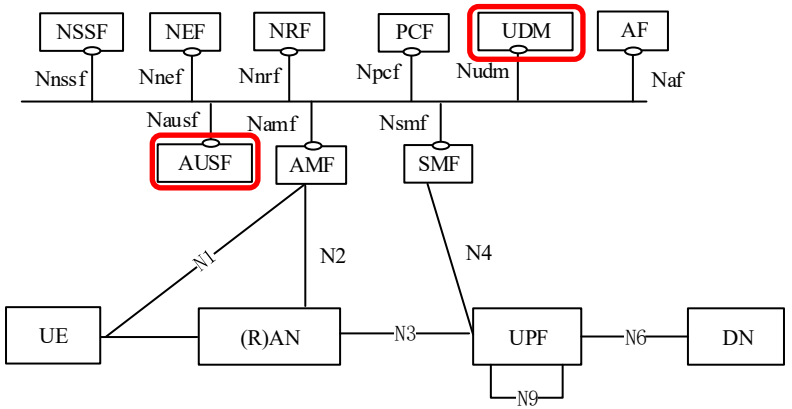
AUSF and UDM

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**



(3GPP TS 23.501)

NEF, NRF and NSSF

NF Repository function (NRF)

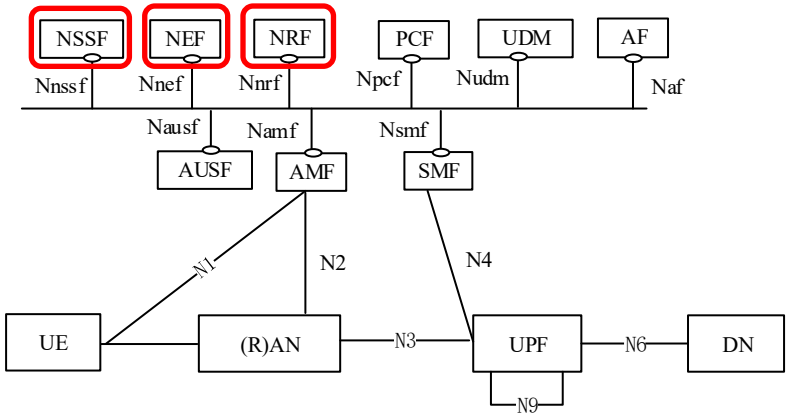
- **Supports service discovery function**
- **Maintains the NF profile of available NF instances and their supported services**

Network Exposure function (NEF)

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

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**

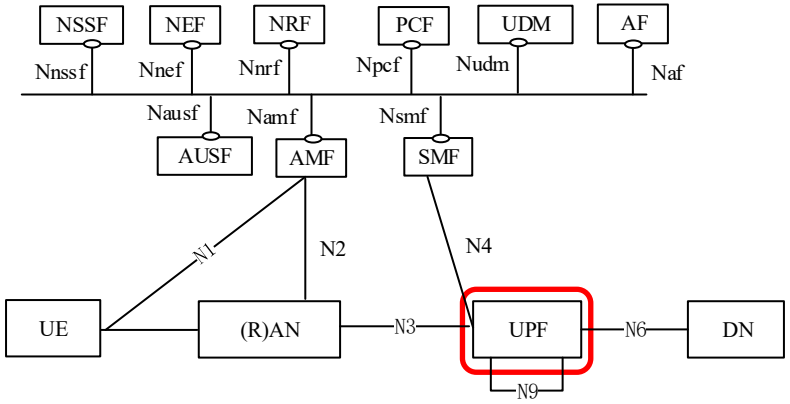


(3GPP TS 23.501)

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**

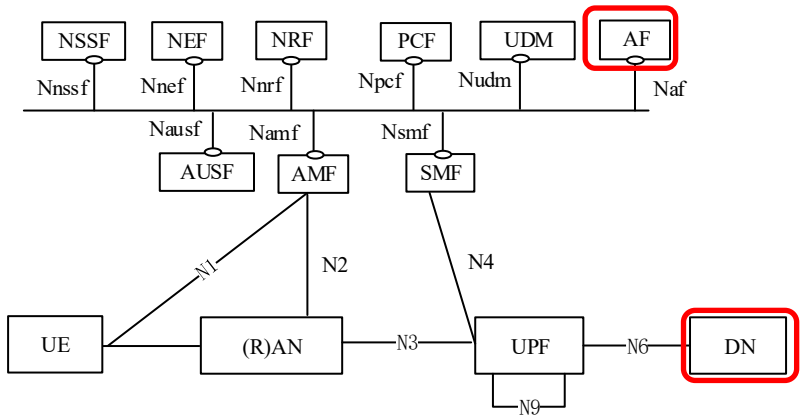


AF and DN

Application Function (AF)

(Not a specific NF)

- **Application influence on traffic routing**
- **Accessing Network Exposure Function (NEF)**
- **Interacting with the Policy framework for policy control (PCF)**



(3GPP TS 23.501)

Data Network (DN)

(Not a specific NF)

- **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)

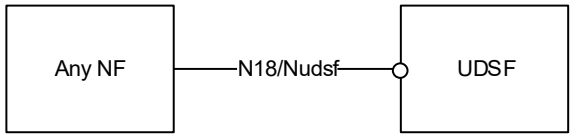


Figure 4.2.5-1: Data storage architecture for unstructured data from any NF (3GPP TS 23.501)

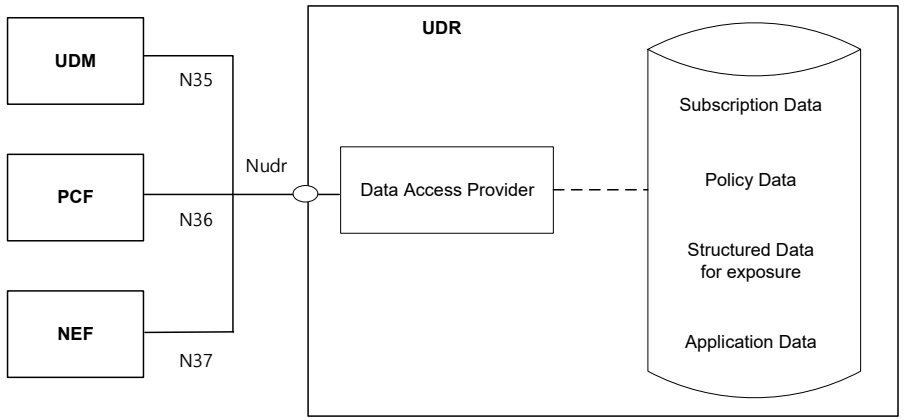


Figure 4.2.5-2: Data storage architecture (3GPP TS 23.501)

(3GPP TS 23.501)

5G Identifiers

5G Network associated identifiers: RAN

https://mcc-mnc.net/

Show 25 entries Search: Portugal

MCC	MNC	ISO	Country	Country Code	Network
268	04	pt	Portugal	351	Lycamobile
268	08	pt	Portugal	351	MEO
268	06	pt	Portugal	351	MEO
268	80	pt	Portugal	351	MEO
268	03	pt	Portugal	351	NOS
268	93	pt	Portugal	351	NOS
268	91	pt	Portugal	351	Vodafone
268	01	pt	Portugal	351	Vodafone

PLMNID: **Public Land Mobile Network Identity** (MCC+MNC); unique code that identifies a mobile network

MCC: Mobile Country Code

MNC: Mobile Network Code

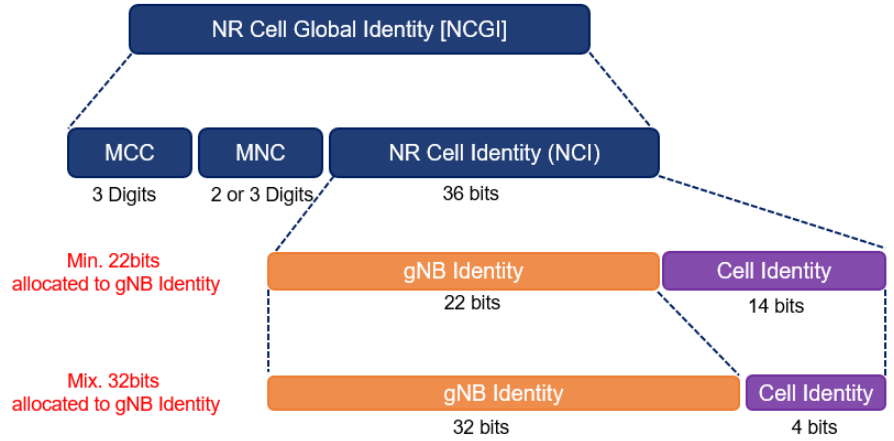
PCI: Physical Cell ID, unique, 24-bit physical layer identifier for each cell, ranging from 0 to 1007, and is used by user devices for cell selection, synchronization, and to distinguish signals from different cells; not unique

CellID: A specific identifier for a cell within a gNB (remaining bits to make total 36 bits); identifies a specific cell on a particular base station

CGI: Cell Global Identity, unique, combination of CellID, MCC, MNC and TAC; identify NR cells globally

gNB-ID: A unique identifier for a 5G gNB (22-32 bits); a networks with a large numbers of small cells may require a larger gNB ID

TAC: Tracking Area Code, logical identifier for a Tracking Area, which is a group of cell towers



5G Network associated identifiers: RAN

IMEI: International Mobile Equipment Identity; unique 15-digit number assigned to each device on a mobile network that helps identify that specific device

PEI : Permanent Equipment Identifier; a globally unique identifier for the network equipment (e.g., the UE), independent of the subscriber; for devices that are capable of accessing a 3GPP network, the PEI will be an IMEI (thus, for most 5G devices PEI will be the IMEI)

EID: Embedded Identity Document; is a unique 32-digit eSIM identifier used to identify a device's internal eSIM chip, enabling cellular network connectivity without a physical SIM card; is the digital equivalent of a physical SIM card's identifier (ICCID)

Dial *#06# on your phone, to get IMEIs and EID

SNSSAI: Single Network Slice Selection Assistance Information; network identifier for a specific network slice, composed of two parts: SST and optional SD

- **SST: Slice/Service Type**, identifies the general purpose of the network slice; standardized and operator-specific values
- **SD: Slice Differentiator**, when more than one network slice has the same SST

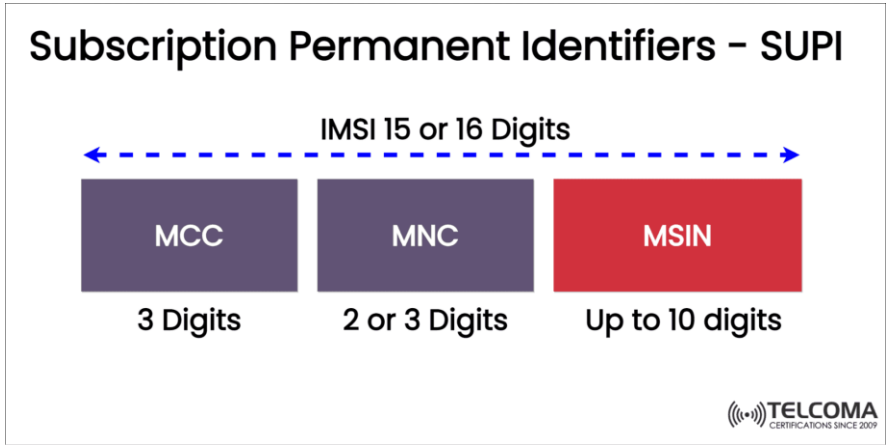
NR-ARFCN: **NR Absolute Radio Frequency Channel Number**; used to identify RF channels in 5G New Radio (NR) networks. This calculator helps convert between frequency (MHz) and NR-ARFCN values based on 3GPP specifications

https://nrcalculator.web.app/nrarfcn_tw.html

5G subscription identifiers

https://www.telcomaglobal.com/p/5g-identifiers

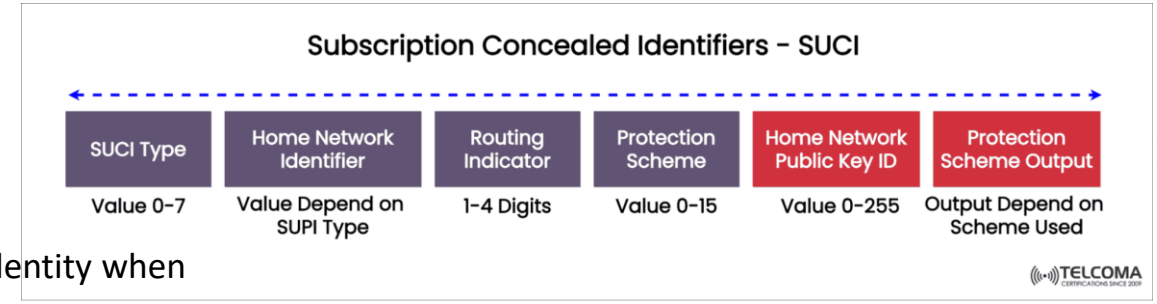
5G subscription identifiers are used to uniquely identify subscribers in the network



SUPI (Subscription Permanent Identifier)

Globally unique identifier that is assigned to each subscriber identifying him in the 5G system
The SUPI must contain the address of the home network in order to enable roaming scenarios
Equivalent to 4G IMSI (*International Mobile Subscriber Identity*)
Provisioned in the UDM/UDR and at the Universal Subscriber Identity Module (USIM)
String of 15 decimal digits:

- Mobile Country Code (MCC) and Mobile Network Code (MNC) identifying the network operator.
- **MSIN**



MSIN (Mobile Subscriber identification number)

Represents the individual user of that particular operator

SUCI (Subscription Concealed Identifier)

Encrypted, concealed version of the SUPI, used to protect the subscriber's permanent identity when communicating with the network
The UE generates a SUCI using the public key of the Home network that was securely provisioned to the USIM during the USIM registration process. It contains:

- protection scheme ID
- home network public key ID
- home network ID, e.g MCC and MNC, the SUCI calculation indication, either USIM or ME calculating the SUCI, based on the home operator's decision indicated by the USIM

The SUCI calculation shall be performed either by the USIM or by the ME

5G subscription identifiers

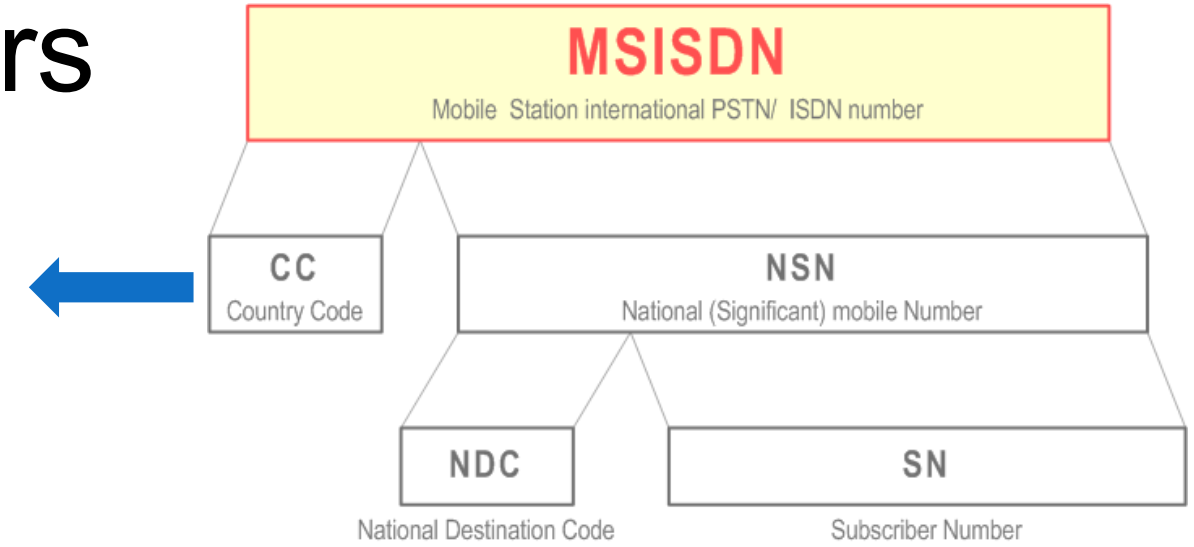
MSISDN (*Mobile Station International Subscriber Directory Number*)
User's phone number in 5G, just as it did in previous generations

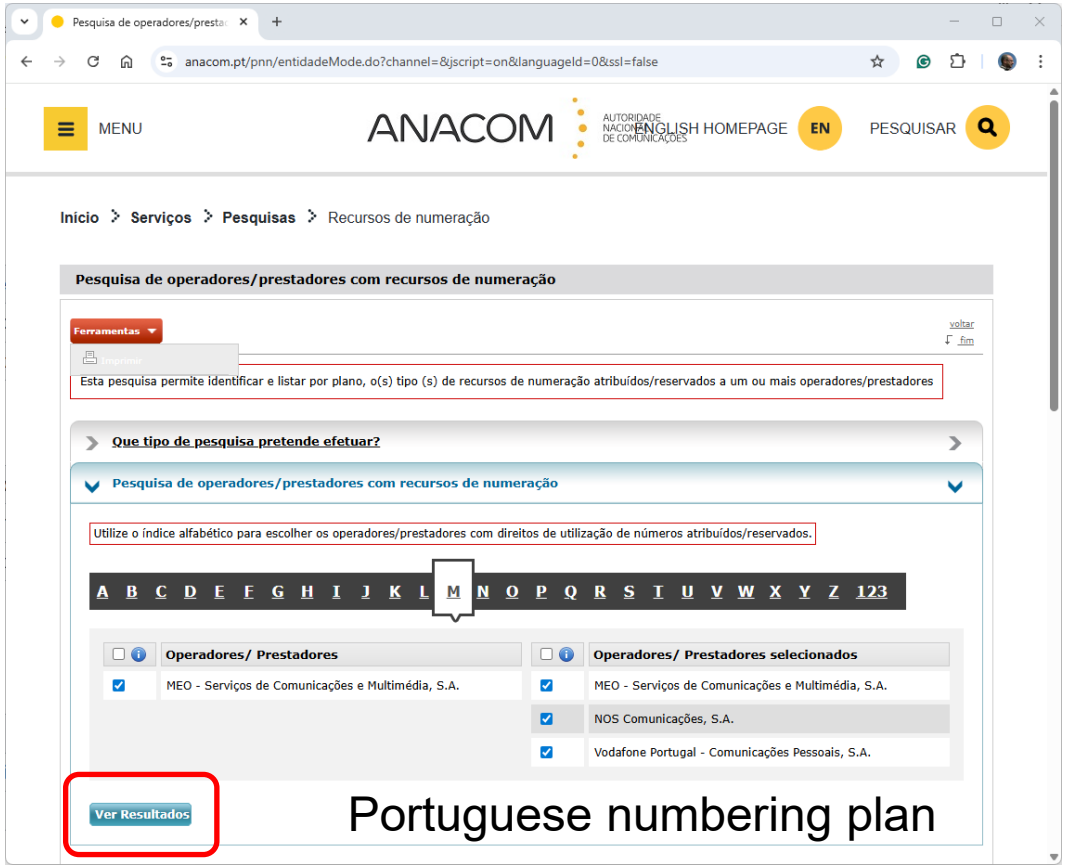
- **Call and SMS routing**: Continues to be the public telephone number used to route calls and messages to the correct destination
- **User-facing identifier**: It's the number that the end-user knows and uses, acting as the public interface for the subscriber
- **SIM independence**: The MSISDN can be changed or ported to another operator, unlike the SUPI (IMSI) that is tied to the SIM card

Characteristic	MSISDN	SUPI (4G/IMSI)
Identifier type	Public (phone number)	Internal (permanent identifier)
Visibility	Visible to the user and third parties	Used only within the 3GPP system
Function	Routes calls and SMS	Identifies the subscriber on the network for internal management
Security	Not encrypted during transmission	Transmitted in a concealed form (SUCI) for greater privacy

5G subscription identifiers

E.164 is an international standard (ITU-T Recommendation), titled “The international public telecommunication numbering plan”, that defines a numbering plan for the worldwide public switched telephone network (PSTN) and some other data networks.

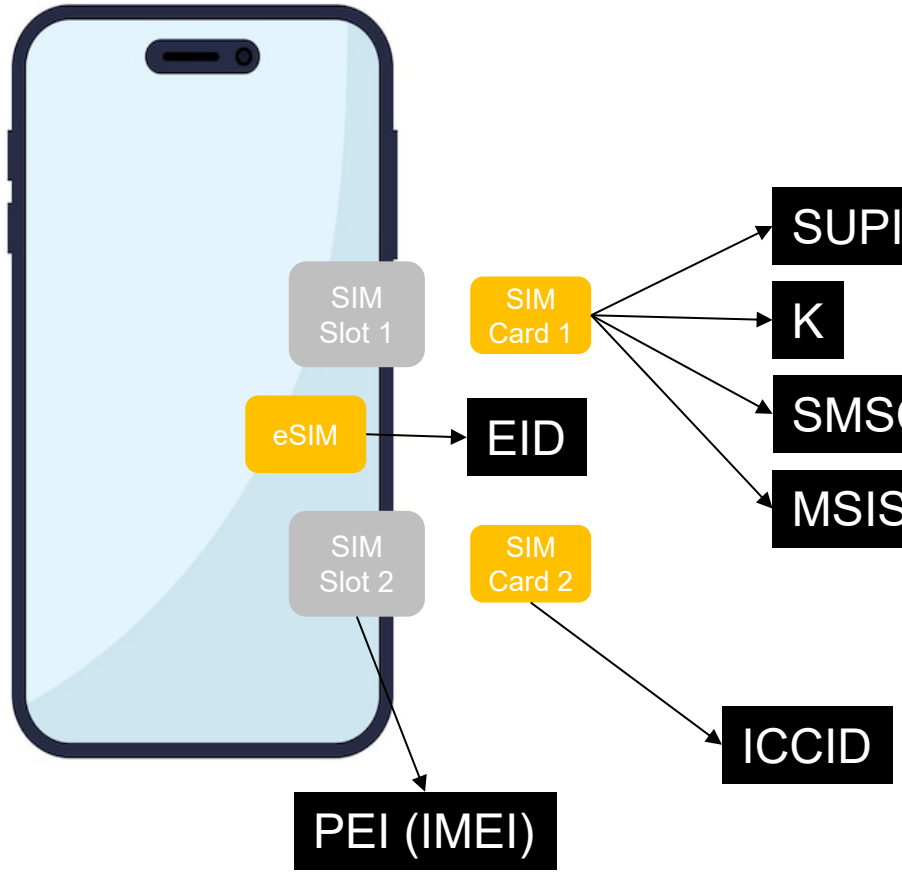




Portuguese numbering plan

Telephone country codes

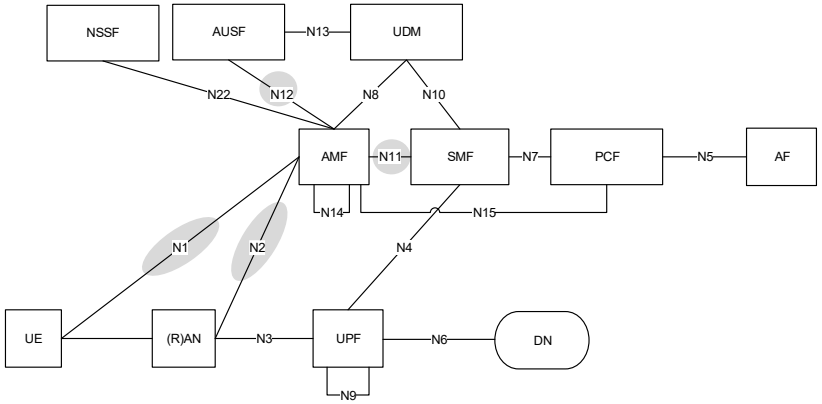
5G information in the UE and SIM

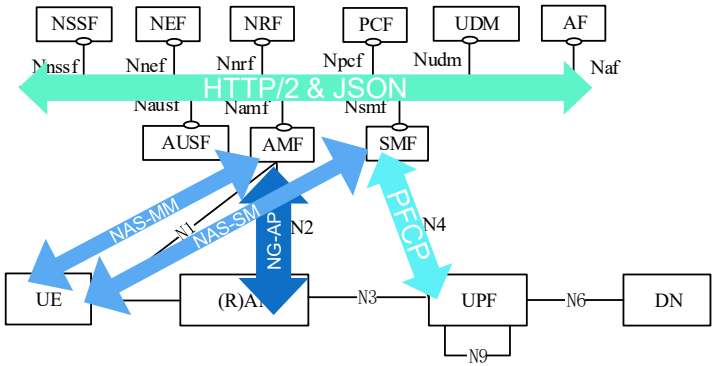


PEI – Permanent Equipment Identifier (replaces IMEI in 5G)
EID – Embedded Identity Document
IMEI – International Mobile Equipment Identity
SUPI – Subscriber Permanent Identifier (unique subscriber identity)
IMSI – International Mobile Subscriber Identity
MSISDN – Mobile Station International Subscriber Directory Number
K – long term Key
OPc – Operator Derived Key
SMSC – SMS Center
ICCID – Integrated Circuit Card Identifier

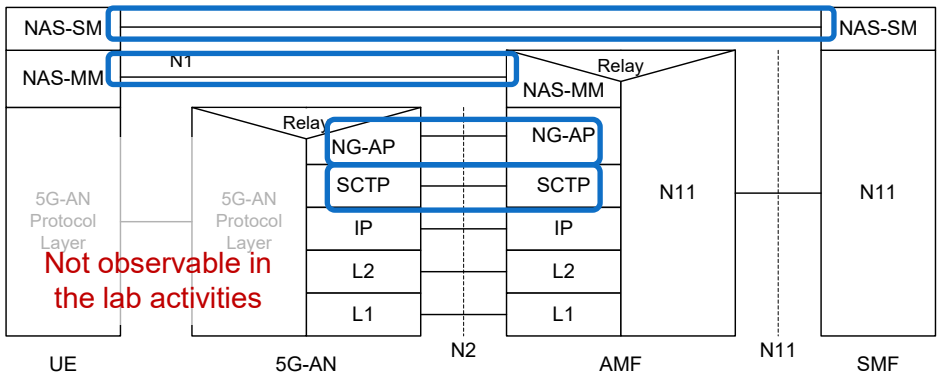
Protocols

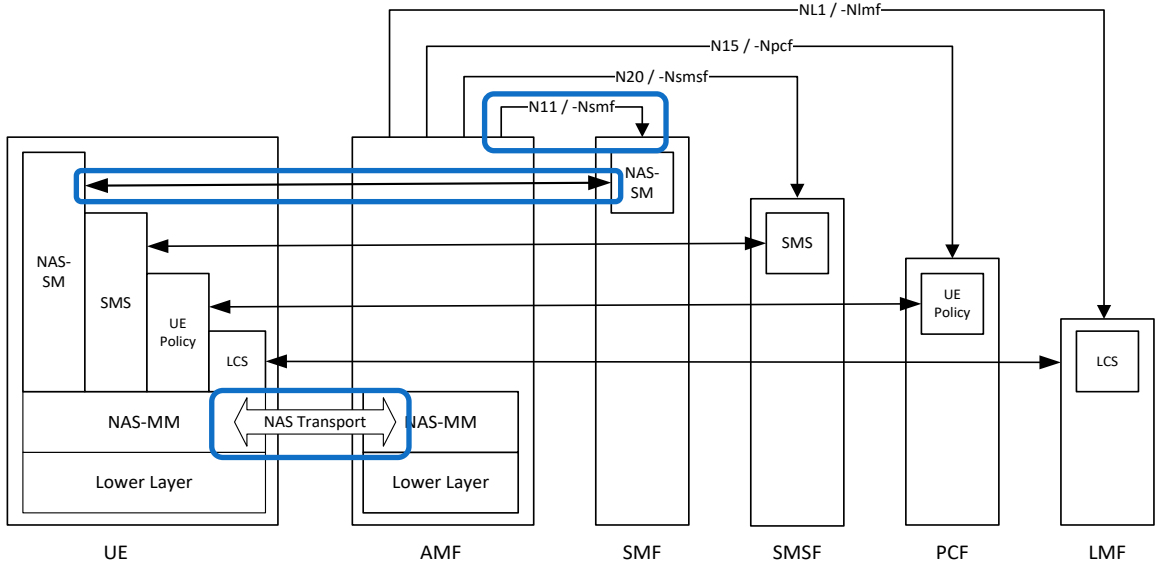
Protocol stacks: Control Plane





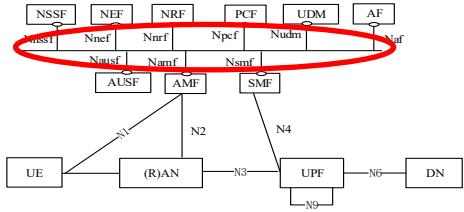
PFCP Packet Forwarding Control Protocol
SCTP: Stream Control Transmission Protocol
NG-AP: NG Application Protocol
NAS-MM: NAS Mobility Management
NAS-SM: NAS Session Management
NAS: Non-Access-Stratum





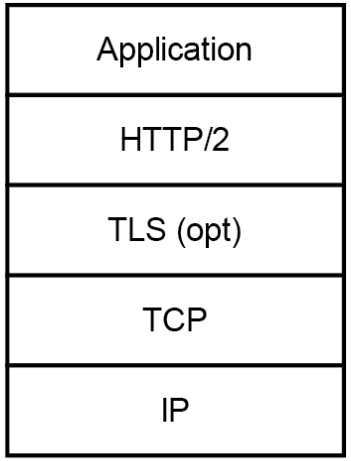
HTTP/2 & JSON

https://forge.3gpp.org/rep/all/5G_APIs
https://spec.openapis.org/oas/v3.0.0



5G SBA (*Service-Based Architecture*)

- *Service-Based Interfaces* (SBIs): *Network functions* (NFs) expose services and communicate via RESTful APIs, using HTTP/2 and JSON
- Shift from legacy telecom-specific protocols like Diameter and SS7 to web technologies (HTTP/2, JSON, RESTful APIs, cloud-native principles): greater flexibility, scalability, and easier integration with cloud infrastructure



sw1411

HTTP2

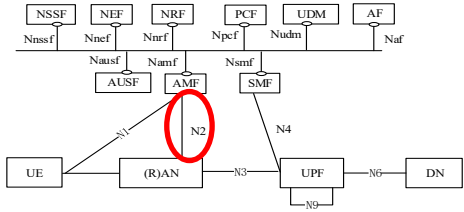
- Major revision of the HTTP protocol, designed to improve performance and efficiency

HTTP Method	CRUD Action
GET	Retrieve a resource
POST	Create a resource
PUT	Update a resource
DELETE	Delete a resource

JSON (*JavaScript Object Notation*)

- Lightweight data-interchange format, easy for humans to read and write, easy for machines to generate and parse

Stream Control Transmission Protocol (SCTP)



RFC 9260, "Stream Control Transmission Protocol"

Transport protocol (L4) for signaling messages between the 5G-AN (gNB) and the AMF (over the N2 interface)

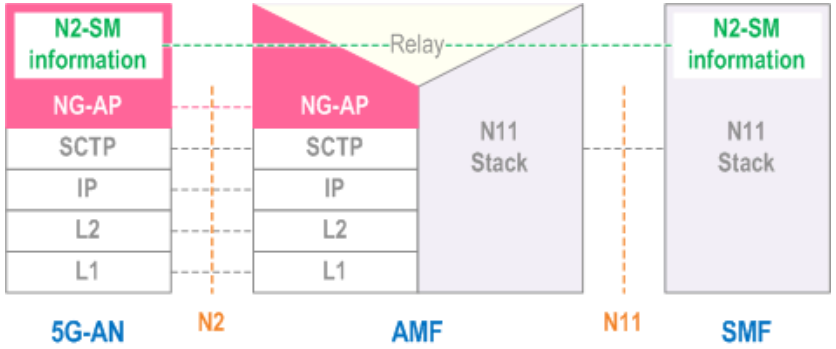
Guaranteed Delivery:
• SCTP ensures that signaling messages reach their destination reliably and in order.

Message-Oriented:
• Unlike TCP (which is stream-oriented), SCTP maintains message boundaries, providing a more structured and efficient way to send data.

Multi-streaming:
• SCTP allows multiple independent data streams within a single connection (association), preventing a single congested stream from blocking others, which enhances overall throughput and avoids head-of-line blocking.

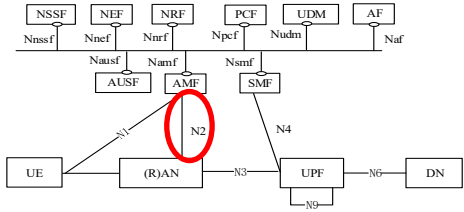
Multi-homing:
•This is a significant advantage for 5G networks. It allows a single SCTP association to use multiple IP addresses, providing built-in redundancy and fault tolerance. If one connection fails, traffic can automatically switch to another available path.

Security Features:
•SCTP includes mechanisms like a four-way handshake and a cookie mechanism to prevent man-in-the-middle attacks and masquerades.



This makes it ideal for the demanding signaling requirements of 5G networks, especially in core network interfaces and in cloud-native deployments.

Control Plane: NG-AP (*Next Generation Application Protocol*)



3GPP TS 38.413, "NG Application Protocol (NGAP)"

Statefull application layer protocol, operating over SCTP

Point-to-point communication between the NG-RAN node (gNB) and the AMF (*Access and Mobility Management Function*)

Defines a set of **elementary procedures**, each consisting of one or more messages exchanged over the NG interface

Table 8.1-1: Class 1 procedures

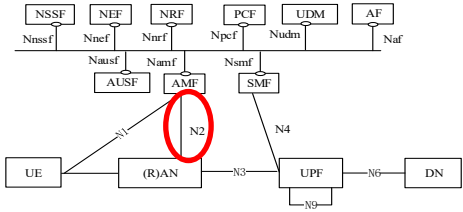
Elementary Procedure	Initiating Message	Successful Outcome	Unsuccessful Outcome
		Response message	Response message
AMF Configuration Update	AMF CONFIGURATION UPDATE	AMF CONFIGURATION UPDATE ACKNOWLEDGE	AMF CONFIGURATION UPDATE FAILURE
RAN Configuration Update	RAN CONFIGURATION UPDATE	RAN CONFIGURATION UPDATE ACKNOWLEDGE	RAN CONFIGURATION UPDATE FAILURE
Handover Cancellation	HANDOVER CANCEL	HANDOVER CANCEL ACKNOWLEDGE	
Handover Preparation	HANDOVER REQUIRED	HANDOVER COMMAND	HANDOVER PREPARATION FAILURE
Handover Resource Allocation	HANDOVER REQUEST	HANDOVER REQUEST ACKNOWLEDGE	HANDOVER FAILURE
Initial Context Setup	INITIAL CONTEXT SETUP REQUEST	INITIAL CONTEXT SETUP RESPONSE	INITIAL CONTEXT SETUP FAILURE
NG Reset	NG RESET	NG RESET ACKNOWLEDGE	
NG Setup	NG SETUP REQUEST	NG SETUP RESPONSE	NG SETUP FAILURE
Path Switch Request	PATH SWITCH REQUEST	PATH SWITCH REQUEST ACKNOWLEDGE	PATH SWITCH REQUEST FAILURE
PDU Session Resource Modify	PDU SESSION RESOURCE MODIFY REQUEST	PDU SESSION RESOURCE MODIFY RESPONSE	
PDU Session Resource Modify Indication	PDU SESSION RESOURCE MODIFY INDICATION	PDU SESSION RESOURCE MODIFY CONFIRM	
PDU Session Resource Release	PDU SESSION RESOURCE RELEASE COMMAND	PDU SESSION RESOURCE RELEASE RESPONSE	
PDU Session Resource Setup	PDU SESSION RESOURCE SETUP REQUEST	PDU SESSION RESOURCE SETUP RESPONSE	
UE Context Modification	UE CONTEXT MODIFICATION REQUEST	UE CONTEXT MODIFICATION RESPONSE	UE CONTEXT MODIFICATION FAILURE
UE Context Release	UE CONTEXT RELEASE COMMAND	UE CONTEXT RELEASE COMPLETE	
Write-Replace Warning	WRITE-REPLACE WARNING REQUEST	WRITE-REPLACE WARNING RESPONSE	
PWS Cancel	PWS CANCEL REQUEST	PWS CANCEL RESPONSE	
UE Radio Capability Check	UE RADIO CAPABILITY CHECK REQUEST	UE RADIO CAPABILITY CHECK RESPONSE	

Elementary Procedure	Initiating Message	Successful Outcome	Unsuccessful Outcome
		Response message	Response message
UE Context Suspend	UE CONTEXT SUSPEND REQUEST	UE CONTEXT SUSPEND RESPONSE	UE CONTEXT SUSPEND FAILURE
UE Context Resume	UE CONTEXT RESUME REQUEST	UE CONTEXT RESUME RESPONSE	UE CONTEXT RESUME FAILURE
UE Radio Capability ID Mapping	UE RADIO CAPABILITY ID MAPPING REQUEST	UE RADIO CAPABILITY ID MAPPING RESPONSE	
Broadcast Session Setup	BROADCAST SESSION SETUP REQUEST	BROADCAST SESSION SETUP RESPONSE	BROADCAST SESSION SETUP FAILURE
Broadcast Session Modification	BROADCAST SESSION MODIFICATION REQUEST	BROADCAST SESSION MODIFICATION RESPONSE	BROADCAST SESSION MODIFICATION FAILURE
Broadcast Session Release	BROADCAST SESSION RELEASE REQUEST	BROADCAST SESSION RELEASE RESPONSE	
Distribution Setup	DISTRIBUTION SETUP REQUEST	DISTRIBUTION SETUP RESPONSE	DISTRIBUTION SETUP FAILURE
Distribution Release	DISTRIBUTION RELEASE REQUEST	DISTRIBUTION RELEASE RESPONSE	
Multicast Session Activation	MULTICAST SESSION ACTIVATION REQUEST	MULTICAST SESSION ACTIVATION RESPONSE	MULTICAST SESSION ACTIVATION FAILURE
Multicast Session Deactivation	MULTICAST SESSION DEACTIVATION REQUEST	MULTICAST SESSION DEACTIVATION RESPONSE	
Multicast Session Update	MULTICAST SESSION UPDATE REQUEST	MULTICAST SESSION UPDATE RESPONSE	MULTICAST SESSION UPDATE FAILURE
Timing Synchronisation Status	TIMING SYNCHRONISATION STATUS REQUEST	TIMING SYNCHRONISATION STATUS RESPONSE	TIMING SYNCHRONISATION STATUS FAILURE
MT Communication Handling	MT COMMUNICATION HANDLING REQUEST	MT COMMUNICATION HANDLING RESPONSE	MT COMMUNICATION HANDLING FAILURE
Broadcast Session Transport	BROADCAST SESSION TRANSPORT REQUEST	BROADCAST SESSION TRANSPORT RESPONSE	BROADCAST SESSION TRANSPORT FAILURE

Table 8.1-2: Class 2 procedures

Elementary Procedure	Message
Downlink RAN Configuration Transfer	DOWNLINK RAN CONFIGURATION TRANSFER
Downlink RAN Status Transfer	DOWNLINK RAN STATUS TRANSFER
Downlink NAS Transport	DOWNLINK NAS TRANSPORT
Error Indication	ERROR INDICATION
Uplink RAN Configuration Transfer	UPLINK RAN CONFIGURATION TRANSFER
Uplink RAN Status Transfer	UPLINK RAN STATUS TRANSFER
Handover Notification	HANDOVER NOTIFY
Initial UE Message	INITIAL UE MESSAGE
NAS Non Delivery Indication	NAS NON DELIVERY INDICATION
Paging	PAGING
PDU Session Resource Notify	PDU SESSION RESOURCE NOTIFY
Reroute NAS Request	REROUTE NAS REQUEST
UE Context Release Request	UE CONTEXT RELEASE REQUEST
Uplink NAS Transport	UPLINK NAS TRANSPORT
AMF Status Indication	AMF STATUS INDICATION
PWS Restart Indication	PWS RESTART INDICATION
PWS Failure Indication	PWS FAILURE INDICATION
Downlink UE Associated NRPPa Transport	DOWNLINK UE ASSOCIATED NRPPA TRANSPORT
Uplink UE Associated NRPPa Transport	UPLINK UE ASSOCIATED NRPPA TRANSPORT
Downlink Non UE Associated NRPPa Transport	DOWNLINK NON UE ASSOCIATED NRPPA TRANSPORT
Uplink Non UE Associated NRPPa Transport	UPLINK NON UE ASSOCIATED NRPPA TRANSPORT
Trace Start	TRACE START
Trace Failure Indication	TRACE FAILURE INDICATION
Deactivate Trace	DEACTIVATE TRACE
Cell Traffic Trace	CELL TRAFFIC TRACE
Location Reporting Control	LOCATION REPORTING CONTROL
Location Reporting Failure Indication	LOCATION REPORTING FAILURE INDICATION
Location Report	LOCATION REPORT
UE TNLA Binding Release	UE TNLA BINDING RELEASE REQUEST
UE Radio Capability Info Indication	UE RADIO CAPABILITY INFO INDICATION
RRC Inactive Transition Report	RRC INACTIVE TRANSITION REPORT
Overload Start	OVERLOAD START
Overload Stop	OVERLOAD STOP
Secondary RAT Data Usage Report	SECONDARY RAT DATA USAGE REPORT
Uplink RIM Information Transfer	UPLINK RIM INFORMATION TRANSFER
Downlink RIM Information Transfer	DOWNLINK RIM INFORMATION TRANSFER
Retrieve UE Information	RETRIEVE UE INFORMATION
UE Information Transfer	UE INFORMATION TRANSFER
RAN CP Relocation Indication	RAN CP RELOCATION INDICATION
Connection Establishment Indication	CONNECTION ESTABLISHMENT INDICATION
AMF CP Relocation Indication	AMF CP RELOCATION INDICATION
Handover Success	HANDOVER SUCCESS
Uplink RAN Early Status Transfer	UPLINK RAN EARLY STATUS TRANSFER
Downlink RAN Early Status Transfer	DOWNLINK RAN EARLY STATUS TRANSFER
Multicast Group Paging	MULTICAST GROUP PAGING
Broadcast Session Release Required	BROADCAST SESSION RELEASE REQUIRED
Timing Synchronisation Status Report	TIMING SYNCHRONISATION STATUS REPORT
RAN Paging Request	RAN PAGING REQUEST

(some) NG-AP messages



NG Setup Request/Response: Exchanged between the gNB and AMF to establish the initial connection over the N2 interface.

Initial UE Message: The first message a gNB sends to the AMF when a UE initially contacts the network.

Uplink/Downlink NAS Transport: Messages used to carry encapsulated NAS

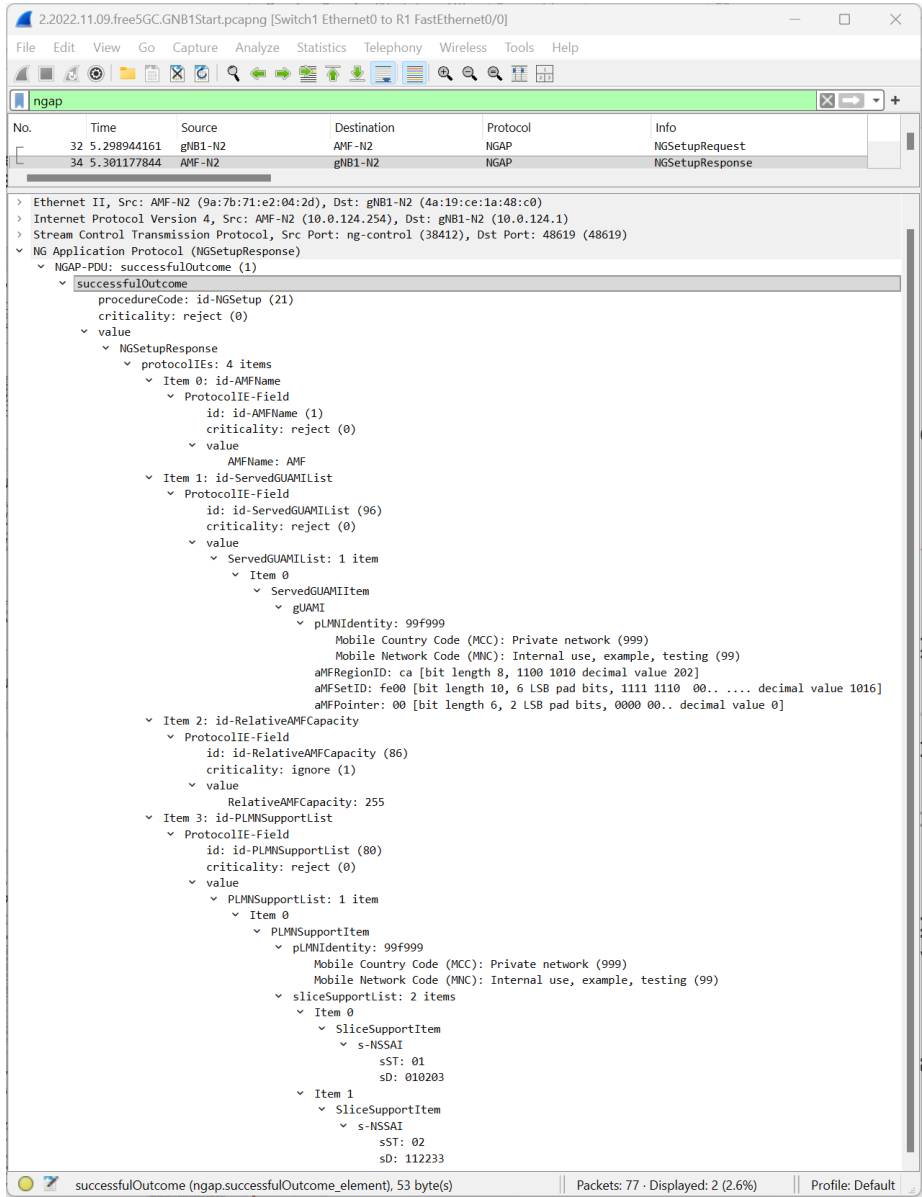
Initial Context Setup Request/Response: These messages set up the necessary UE context and PDU session resources after initial access.

UE Context Release Command/Complete: Used to tear down the UE connection and free up resources.

Handover Request/Request Acknowledge: Sent between different RAN nodes (gNBs) and the AMF to facilitate the handover of a UE.

Paging: Sent from the core network (via the AMF) to the UE via the gNB to notify the UE of incoming data when it is in an idle state.

N2: gNB start



3GPP TS 24.501, “Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3”

Control Plane: NAS-MM (*Mobility Management*) and NAS-SM (*Session Management*)

Feature	NG-MM (Mobility Management)	NG-SM (Session Management)
Core Function	AMF	SMF
Message Type	NAS Mobility Messages	NAS Session Messages
Focus	Identification, mobility, security	Data session setup, QoS, policy
Example Messages	Registration Request, TAU, Service Request	PDU Session Establishment, Modification
Protocol Layer	Control Plane	Control + User Plane

The main function of the 5GSM sublayer is to support the PDU session handling in the UE and in the SMF (transferred via the AMF)

TAU- Tracking Area Update

Control Plane:
NAS-MM (*Mobility Management*) and NAS-SM (*Session Management*)

3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"

3 types of 5GMM procedures can be distinguished:

a) 5GMM common procedures:
- network-initiated NAS transport
- primary authentication and key agreement
- security mode control
- generic UE configuration update
- Identification
- network slice-specific authentication and authorization
- UE-initiated NAS transport
- 5GMM status

b) 5GMM specific procedures:
- registration
- de-registration
- eCall inactivity procedure

c) 5GMM connection management procedures:
- service request
- paging
- notification

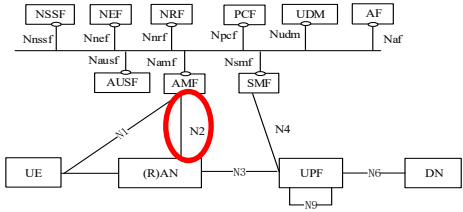
3 types of 5GSM procedures can be distinguished:

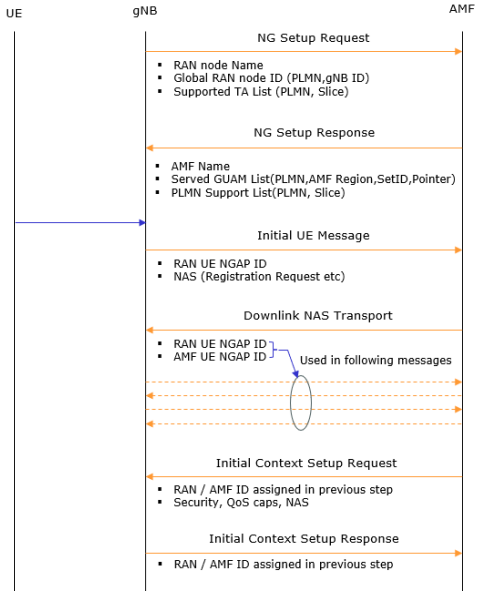
a) Procedures related to PDU sessions:
- PDU authentication and authorization;
- network-requested PDU session modification;
- network-requested PDU session release
- service-level authentication and authorization.
- UE-requested PDU session establishment.

b) Transaction related procedures:
- UE-requested PDU session modification; and
- UE-requested PDU session release.
- remote UE report.

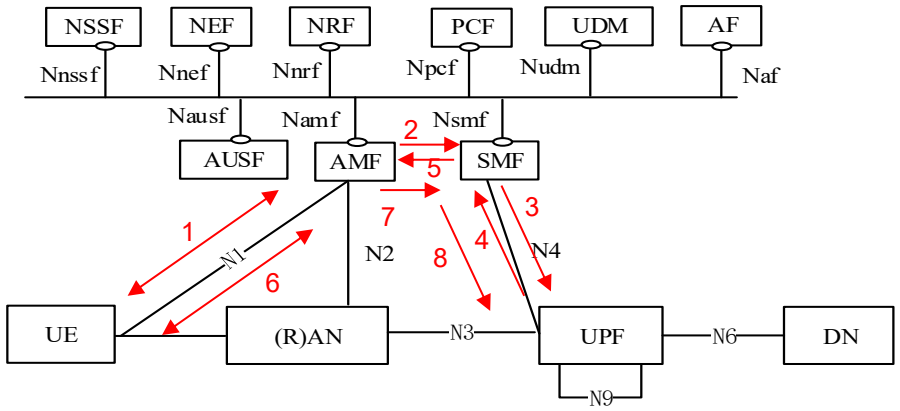
c) Common procedure:
- 5GSM status procedure

NG-AP (MM & SM) messages





https://www.sharetechnote.com/html/5G/5G_NGAP.html



N2: UE start

*4.2022.11.09.free5GC.UE11start.pcapng [Switch1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

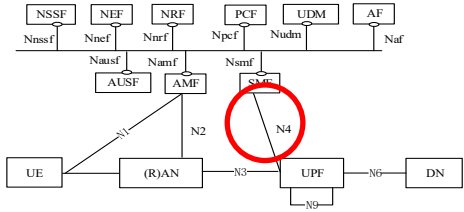
ngap || nas-5gs || pfcp

No.	Time	Source	Destination	Protocol	Info
	34 7.070844223	gNB1-N2	AMF-N2	NGAP/NAS-5GS	InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
1	175 7.095180911	AMF-N2	gNB1-N2	NGAP/NAS-5GS	SACK (Ack=0, Arwnd=106496) , DownlinkNASTransport, Authentication request
	179 7.095809403	gNB1-N2	AMF-N2	NGAP/NAS-5GS	SACK (Ack=0, Arwnd=106496) , UplinkNASTransport, Authentication failure (Synch failure)
	289 7.126650474	AMF-N2	gNB1-N2	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=106496) , DownlinkNASTransport, Authentication request
	292 7.127320735	gNB1-N2	AMF-N2	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=106496) , UplinkNASTransport, Authentication response
	362 7.175939031	AMF-N2	gNB1-N2	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=106496) , DownlinkNASTransport, Security mode command
	367 7.176821676	gNB1-N2	AMF-N2	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=106496) , UplinkNASTransport
	674 7.337237542	AMF-N2	gNB1-N2	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=106496) , InitialContextSetupRequest
	675 7.337538888	gNB1-N2	AMF-N2	NGAP	SACK (Ack=3, Arwnd=106496) , InitialContextSetupResponse
	688 7.541150417	gNB1-N2	AMF-N2	NGAP/NAS-5GS	UplinkNASTransport, UplinkNASTransport
2	756 7.549101194	AMF-SPI	SMF-SPI	HTTP2/JSON/NAS-5GS	DATA[3], JSON (application/json), PDU session establishment request
3	916 7.575561222	SMF-N4	UPF-N4	PFCP	PFCP Session Establishment Request
4	919 7.576759436	UPF-N4	SMF-N4	PFCP	PFCP Session Establishment Response
5	929 7.579055197	SMF-SPI	AMF-SPI	HTTP2/JSON/NAS-5GS/NGAP	DATA[3], JSON (application/json), PDU session establishment accept, PDUSessionResourceSetupRequestTransfer
6	937 7.580135953	AMF-N2	gNB1-N2	NGAP/NAS-5GS	SACK (Ack=6, Arwnd=106496) , PDUSessionResourceSetupRequest
	942 7.582203712	gNB1-N2	AMF-N2	NGAP	SACK (Ack=4, Arwnd=106496) , PDUSessionResourceSetupResponse
7	951 7.583173003	AMF-SPI	SMF-SPI	HTTP2/JSON/NGAP	DATA[3], JSON (application/json), PDUSessionResourceSetupResponseTransfer
8	958 7.584659733	SMF-N4	UPF-N4	PFCP	PFCP Session Modification Request
	963 7.585547591	UPF-N4	SMF-N4	PFCP	PFCP Session Modification Response

```
> Frame 34: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface br1, id 0
> Ethernet II, Src: gNB1-NR (4a:19:ce:1a:48:c0), Dst: AMF-N2 (9a:7b:71:e2:04:2d)
> Internet Protocol Version 4, Src: gNB1-N2 (10.0.124.1), Dst: AMF-N2 (10.0.124.254)
> Stream Control Transmission Protocol, Src Port: 48619 (48619), Dst Port: ng-control (38412)
v NG Application Protocol (InitialUEMessage)
  v NGAP-PDU: initiatingMessage (0)
    v initiatingMessage
        procedureCode: id-InitialUEMessage (15)
        criticality: ignore (1)
      v value
        v InitialUEMessage
          v protocolIEs: 5 items
            > Item 0: id-RAN-UE-NGAP-ID
            > Item 1: id-NAS-PDU
            > Item 2: id-UserLocationInformation
            > Item 3: id-RRCEstablishmentCause
            > Item 4: id-UEContextRequest
```

4.2022.11.09.free5GC.UE11start.pcapng | Packets: 1190 · Displayed: 19 (1.6%) | Profile: Default

Packet Forwarding Control Protocol (PFCP)



In 5G Core (5GC), the control and user plane are separated:

- SMF (*Session Management Function*) = Control Plane
- UPF (*User Plane Function*) = User Plane

Protocol for the communication between SMF ↔ UPF

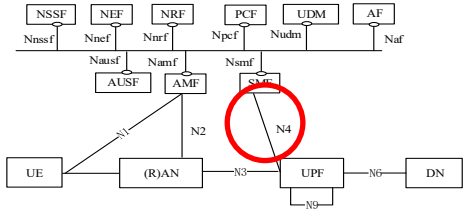
PFCP runs over UDP port 8805

PFCP uses sequence numbers and response timers to ensure reliability over UDP. If no response is received, messages are retransmitted

Enables the SMF to dynamically configure how the UPF handles user traffic, including routing, QoS, and charging, being responsible for:

- Session establishment & modification
- Packet Detection Rules (PDRs)
- QoS enforcement
- Traffic forwarding actions (buffer, drop, redirect, etc.)

PFCP Session lifecycle



1.Association Setup:

SMF establishes a PFCP association with UPF

2. Session Establishment:

SMF sends rules to UPF:

1. **PDR (Packet Detection Rule)**

   Defines how to detect user traffic.

2. **FAR (Forwarding Action Rule)**:

   Specifies forwarding behavior

3. **QER (QoS Enforcement Rule)**:

   Applies QoS policies

4. **URR (Usage Reporting Rule)**:

   Enables traffic usage reporting

5. **BAR (Buffering Action Rule)**:

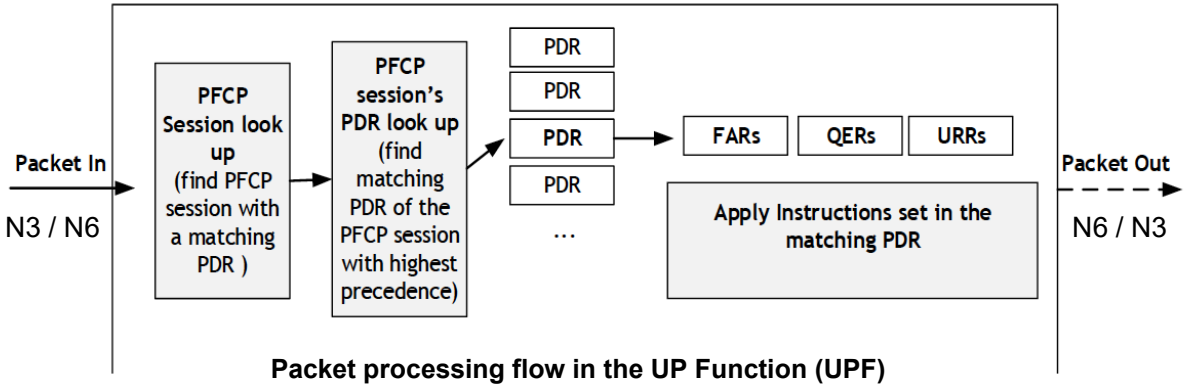
   Handles buffering during mobility

3. Session Modification:

Updates rules (e.g., handover, QoS changes)

4. Session Deletion:

Removes session and all associated rules



Packet processing flow in the UP Function (UPF)

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.

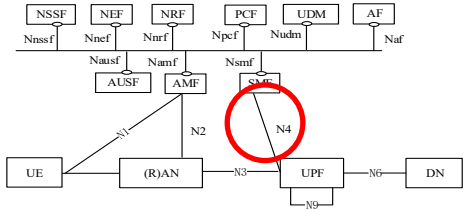
QoS Enforcement Rule *(QER)*: This rule contains information on how to enforce QoS, e.g., bit rate parameters.

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.

https://www.sciencedirect.com/topics/computer-science/user-data-traffic

PFCP Messages



Message Type value (Decimal)	Message	Applicability				
		Sxa	Sxb	Sxc	N4	N4 mb
0	Reserved					
	PFCP Node related messages					
1	PFCP Heartbeat Request	X	X	X	X	X
2	PFCP Heartbeat Response	X	X	X	X	X
3	PFCP PFD Management Request	-	X	X	X	-
4	PFCP PFD Management Response	-	X	X	X	-
5	PFCP Association Setup Request	X	X	X	X	X
6	PFCP Association Setup Response	X	X	X	X	X
7	PFCP Association Update Request	X	X	X	X	X
8	PFCP Association Update Response	X	X	X	X	X
9	PFCP Association Release Request	X	X	X	X	X
10	PFCP Association Release Response	X	X	X	X	X
11	PFCP Version Not Supported Response	X	X	X	X	X
12	PFCP Node Report Request	X	X	X	X	X
13	PFCP Node Report Response	X	X	X	X	X
14	PFCP Session Set Deletion Request	X	X	-	X	-
15	PFCP Session Set Deletion Response	X	X	-	X	-
16	PFCP Session Set Modification Request	-	X	-	X	-
17	PFCP Session Set Modifcation Response	-	X	-	X	-
18 to 49	For future use					
	PFCP Session related messages					
50	PFCP Session Establishment Request	X	X	X	X	X
51	PFCP Session Establishment Response	X	X	X	X	X
52	PFCP Session Modification Request	X	X	X	X	X
53	PFCP Session Modification Response	X	X	X	X	X
54	PFCP Session Deletion Request	X	X	X	X	X
55	PFCP Session Deletion Response	X	X	X	X	X
56	PFCP Session Report Request	X	X	X	X	X
57	PFCP Session Report Response	X	X	X	X	X
58 to 99	For future use					
	Other messages					
100 to 255	For future use					

Node-Related Messages

Used for managing CP-UP associations:

- **Association Setup / Update / Release**
- **Heartbeat Request / Response**
- **Load Control / Overload Control**
- **Node Report**
- **Packet Flow Description (PFD) Management**

Session-Related Messages

Used for per-session packet handling:

- **Session Establishment / Modification / Deletion**
- **Session Report Request / Response**

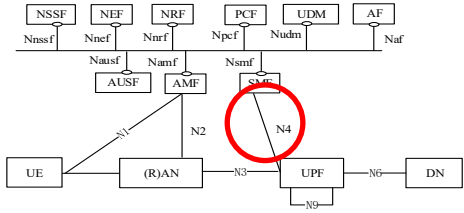
PFCP message structure

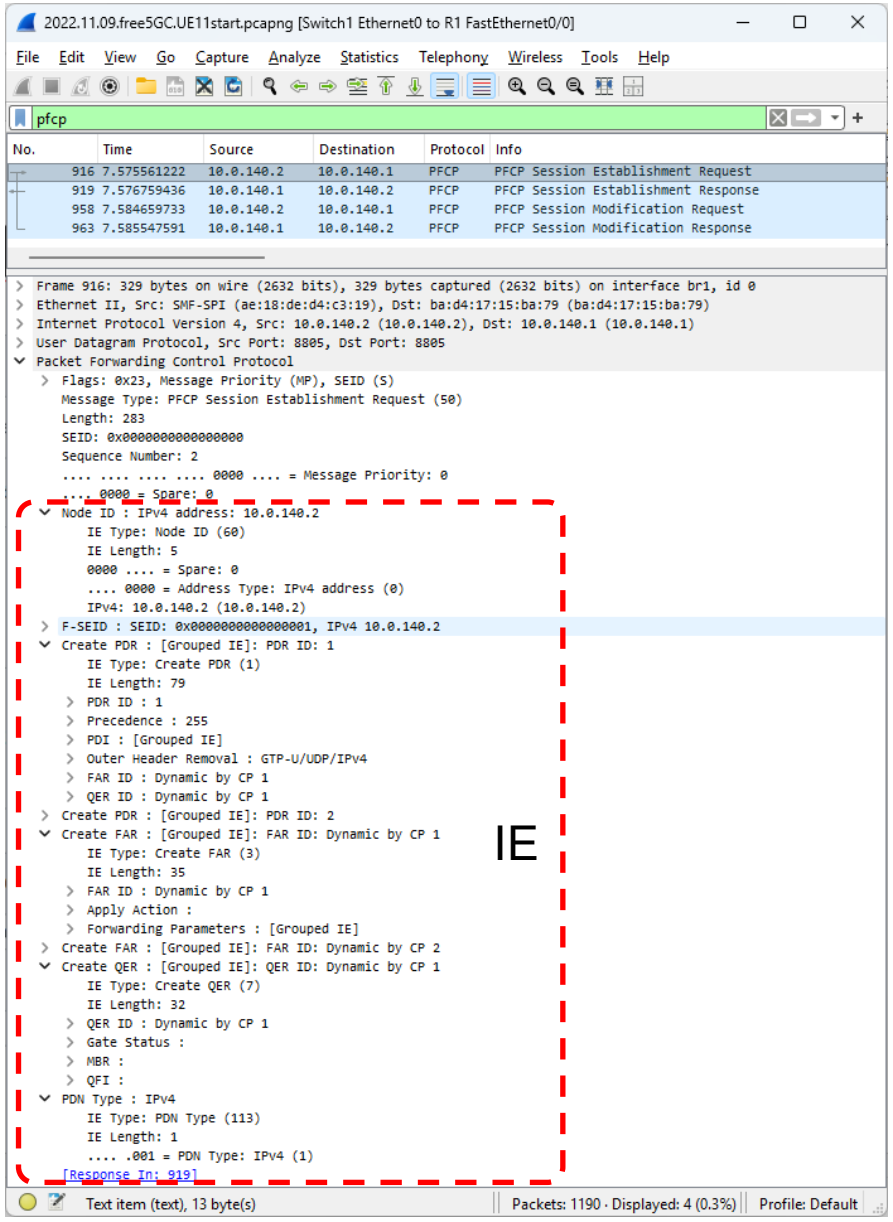
PFCP Message Format

Bit/Byte offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Bytes 0..3	Version (1)			(spare 0s)		FO	MP	S	Message Type								Message Length (in bytes, not including the first 4)															
Bytes 4..11 Bytes 8..11	if (S flag set) then SEID; else these bytes are missing																															
Bytes 4..7 or 12..15	Sequence Number																								if (MP flag set) then Message Priority; else (spare 0s)				(spare 0s)			
Bytes 8.. (MsgLen+4) or 16.. (MsgLen+4)	Zero or more Information Elements																															

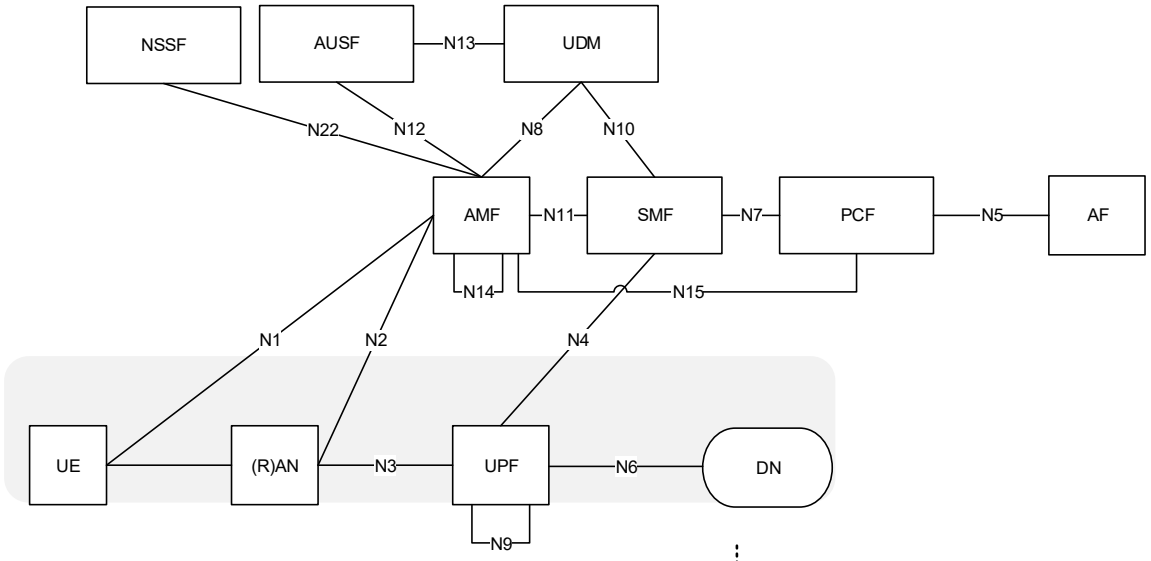
PFCP Information Element Format

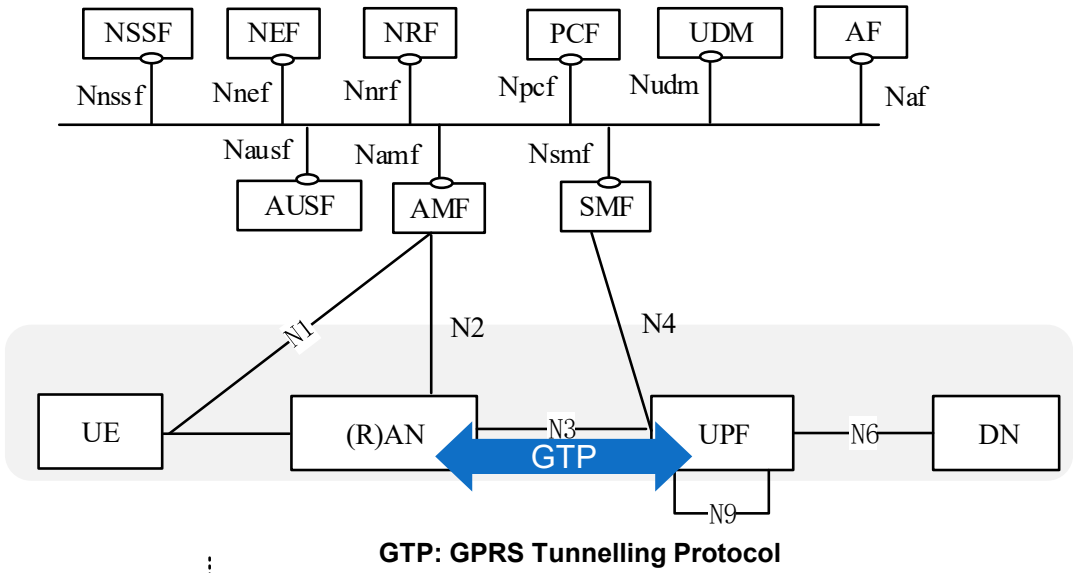
Bit/Byte offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Bytes 0..3	Type																IE Length (in bytes, not including the first 4)															
Bytes 4..IELen+4	if (Type >= 32768) then Enterprise-ID; else this is part of the Payload																Payload (cont.) ...															
	Payload cont. ...																															



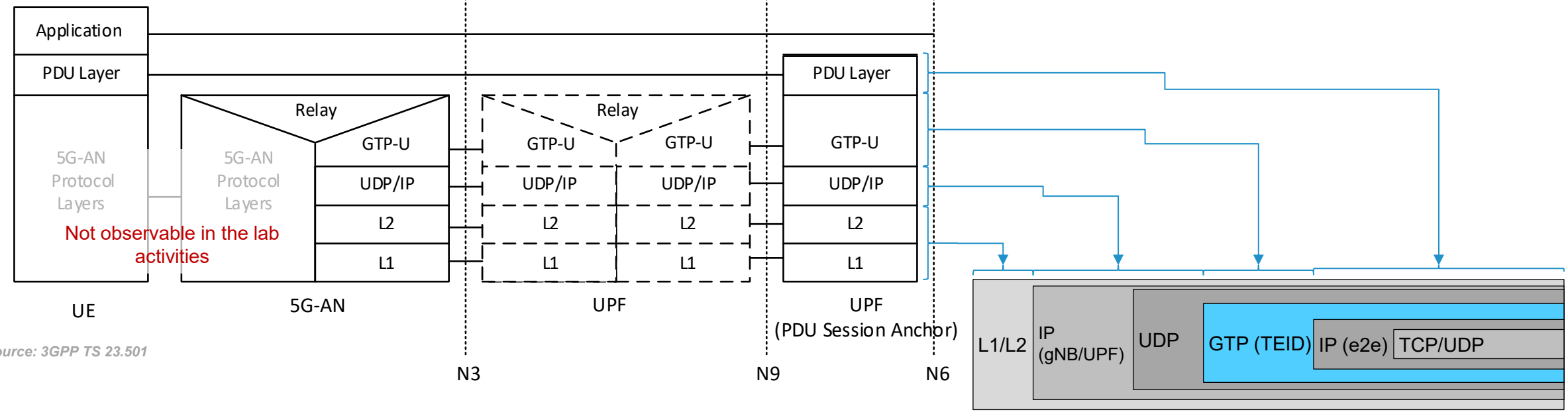


Protocol stacks: User Plane

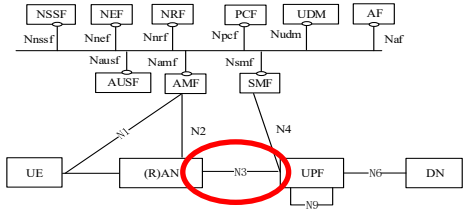




GTP: GPRS Tunnelling Protocol

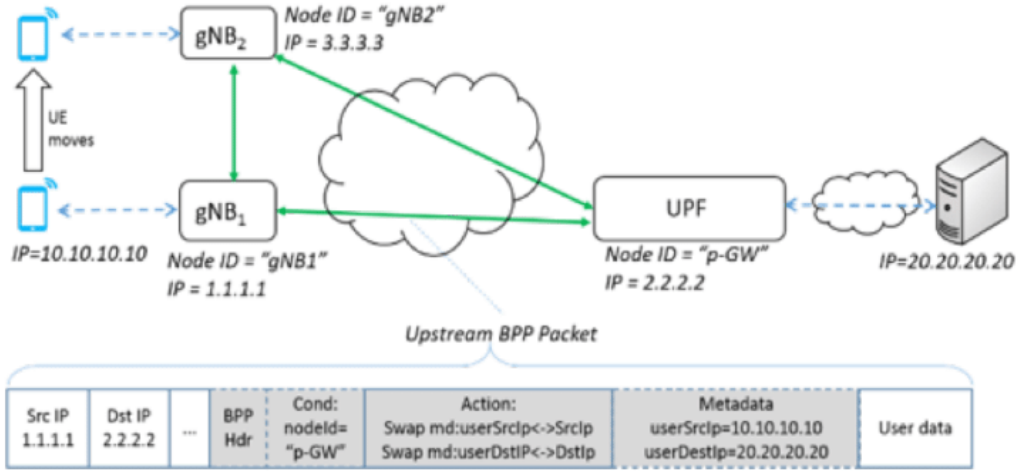


Source: 3GPP TS 23.501

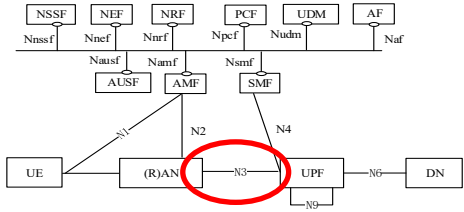


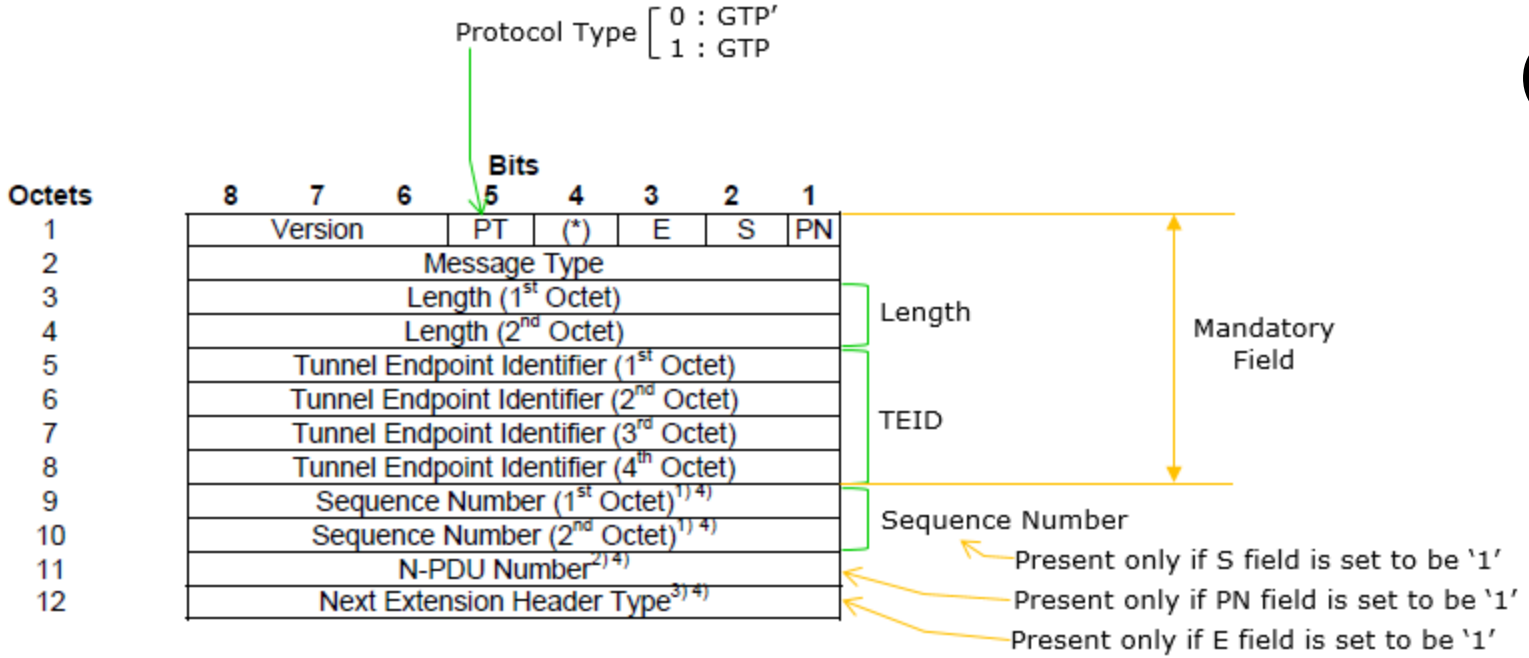
GTP: GPRS Tunneling Protocol

- Runs over UDP/IP and defines tunnels with unique identifiers (*TEIDs = Tunnel Endpoint Identifiers*)
  - The TEID is crucial for identifying the specific user and tunnel on the receiving end, allowing the correct user plane entity to process the encapsulated packet
- GTP works by encapsulating IP packets within other IP packets
- Enables seamless data and service continuity, allowing users to move between network cells and even roaming to other operators without interrupting their connection
  - GTP tunnels switching, without impact in upper layers
- GTP Versions
  - GTP-C (Control Plane) → Used for signaling between core network elements
    - Example: Session creation, modification, deletion.
    - Used in 4G; substituted by NGAP in 5G
  - GTP-U (User Plane) → Used for transporting user traffic (IP packets, voice, video, etc.)



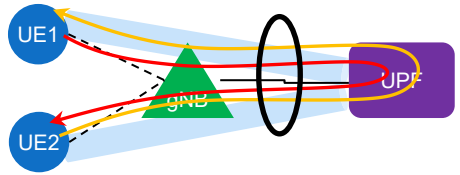
GTP

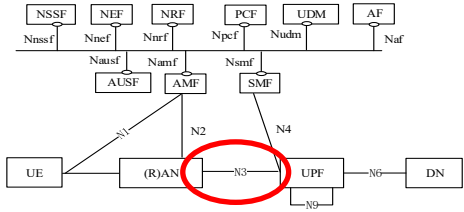




- **Version**: A 3-bit field indicating the GTP version (e.g., 1)
- **Protocol Type (PT)**: Differentiates between GTP-U (user plane) and GTP-C (control plane)
- **Flags**: Indicate various options, such as the presence of a sequence number, N-PDU number, or extension headers
- **Message Type**: Specifies the control message type, such as a Create PDP Context Request
- **Message Length**: The length of the entire GTP message, including the header
- **Tunnel Endpoint Identifier (TEID)**: A unique identifier for the tunnel, essential for routing and de-multiplexing traffic
- **Sequence Number**: Used for message ordering and reliability in the GTP tunnel
- **Information Elements (IEs)**: Optional or grouped elements that carry additional information, such as IMSI (International Mobile Subscriber Identity) or QoS parameters
- **Extension Headers**: Can be added to carry per-packet information, like QoS Flow Identifiers (QFI) or timestamps

GTP example





Ping: echo req UE1 → UE2

6.2022.11.09.free5GC.UE11pingUE21.pcapng [Switch1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Info
373	32.174772649	10.60.0.1	10.60.0.2	GTP/ICMP	Echo (ping) request id=0x21cf, seq=9/2304, ttl=64 (no response found!)
374	32.174887091	10.60.0.1	10.60.0.2	GTP/ICMP	Echo (ping) request id=0x21cf, seq=9/2304, ttl=63 (reply in 379)
379	32.176006870	10.60.0.2	10.60.0.1	GTP/ICMP	Echo (ping) reply id=0x21cf, seq=9/2304, ttl=64 (request in 374)
380	32.176066511	10.60.0.2	10.60.0.1	GTP/ICMP	Echo (ping) reply id=0x21cf, seq=9/2304, ttl=63

```
> Frame 373: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface br1, id 0
> Ethernet II, Src: 42:dc:f6:5c:fd:d3 (42:dc:f6:5c:fd:d3), Dst: ca:63:2e:36:6a:48 (ca:63:2e:36:6a:48)
v Internet Protocol Version 4, Src: 10.0.130.1 (10.0.130.1), Dst: 10.0.130.254 (10.0.130.254)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 128
    Identification: 0x9e49 (40521)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x8324 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.130.1 (10.0.130.1)
    Destination Address: 10.0.130.254 (10.0.130.254)
    [Stream index: 9]
> User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)
v GPRS Tunneling Protocol
  v Flags: 0x34
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .1.. = Is Next Extension Header present?: Yes
      .... ..0. = Is Sequence Number present?: No
      .... ...0 = Is N-PDU number present?: No
    Message Type: T-PDU (0xff)
    Length: 92
    TEID: 0x00000001 (1)
    Next extension header type: PDU Session container (0x85)
  v Extension header (PDU Session container)
      Extension Header Length: 1
    > PDU Session Container
      Next extension header type: No more extension headers (0x00)
v Internet Protocol Version 4, Src: 10.60.0.1 (10.60.0.1), Dst: 10.60.0.2 (10.60.0.2)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x1c6a (7274)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x09c5 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.60.0.1 (10.60.0.1)
    Destination Address: 10.60.0.2 (10.60.0.2)
    [Stream index: 10]
> Internet Control Message Protocol
```

Internet Control Message Protocol: Protocol | Packets: 638 · Displayed: 109 (17.1%) | Profile: Default

Ping: echo rep UE2 → UE1

6.2022.11.09.free5GC.UE11pingUE21.pcapng [Switch1 Ethernet0 to R1 FastEthernet0/0]

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Info
373	32.174772649	10.60.0.1	10.60.0.2	GTP/ICMP	Echo (ping) request id=0x21cf, seq=9/2304, ttl=64 (no response found!)
374	32.174887091	10.60.0.1	10.60.0.2	GTP/ICMP	Echo (ping) request id=0x21cf, seq=9/2304, ttl=63 (reply in 379)
379	32.176006870	10.60.0.2	10.60.0.1	GTP/ICMP	Echo (ping) reply id=0x21cf, seq=9/2304, ttl=64 (request in 374)
380	32.176066511	10.60.0.2	10.60.0.1	GTP/ICMP	Echo (ping) reply id=0x21cf, seq=9/2304, ttl=63

```
> Frame 379: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface br1, id 0
> Ethernet II, Src: 46:ed:b2:bb:0e:74 (46:ed:b2:bb:0e:74), Dst: ca:63:2e:36:6a:48 (ca:63:2e:36:6a:48)
v Internet Protocol Version 4, Src: 10.0.130.2 (10.0.130.2), Dst: 10.0.130.254 (10.0.130.254)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 128
    Identification: 0x1177 (4471)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: UDP (17)
    Header Checksum: 0x0ff6 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.130.2 (10.0.130.2)
    Destination Address: 10.0.130.254 (10.0.130.254)
    [Stream index: 11]
> User Datagram Protocol, Src Port: gtp-user (2152), Dst Port: gtp-user (2152)
v GPRS Tunneling Protocol
  v Flags: 0x34
      001. .... = Version: GTP release 99 version (1)
      ...1 .... = Protocol type: GTP (1)
      .... 0... = Reserved: 0
      .... .1.. = Is Next Extension Header present?: Yes
      .... ..0. = Is Sequence Number present?: No
      .... ...0 = Is N-PDU number present?: No
    Message Type: T-PDU (0xff)
    Length: 92
    TEID: 0x00000003 (3)
    Next extension header type: PDU Session container (0x85)
  v Extension header (PDU Session container)
      Extension Header Length: 1
    > PDU Session Container
      Next extension header type: No more extension headers (0x00)
v Internet Protocol Version 4, Src: 10.60.0.2 (10.60.0.2), Dst: 10.60.0.1 (10.60.0.1)
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x2b1d (11037)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x3b12 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.60.0.2 (10.60.0.2)
    Destination Address: 10.60.0.1 (10.60.0.1)
    [Stream index: 10]
> Internet Control Message Protocol
```

Internet Control Message Protocol: Protocol | Packets: 638 · Displayed: 109 (17.1%) | Profile: Default