University of Antwerp
Faculty of Science

Advanced Wireless & 5G Networks

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

Topics for today

- **3. From 2 to 5G**
  - We jump 2 generations.
- **4. WiFi**
  - Finally.

Planning

Session	Date	Topic
1	20231006	~~Introduction, history, market, industry, bands, licensed vs. unlicensed, …~~
2	20231013	~~Technology baselining (a.k.a. refreshing what you should have known): 2G, WiFi, …~~
	20231020	~~Cancelled~~
3	20231027	~~Shannon/Friis continued. 2G as a "low-complexity" example~~
~~4~~	~~20231110~~	~~L 2G~~
~~5~~	~~20231117~~	~~L 3GPP 2G-3G-4G-5G architecture evolution. 5G~~
~~6~~	~~20231124~~	~~L 5G~~
~~7~~	~~20231201-08~~	~~L 5G~~
8	**20231215 – 2h**	L5G and (woohoo) U IEEE Wifi Network Architecture: 802.11 abgn
9	**20231218 – 2h + 20231222 – 2h**	U QoS, 802.11 ac,ax and 802.11 ad,ay short range 802.15.4: Zigbee, BLE, and UWB
10.5		U Specials: LoRa, Sigfox (perhaps), proprietary, 802.11p
(12)	2231222	Extra: Technology enablers and acronyms you need to be aware of: ADC, FEM, PA, LSA, and other key analog and digital HW blocks, mMIMO, Beam management, 802.11be, AI, 6G, THz and their implications to the network

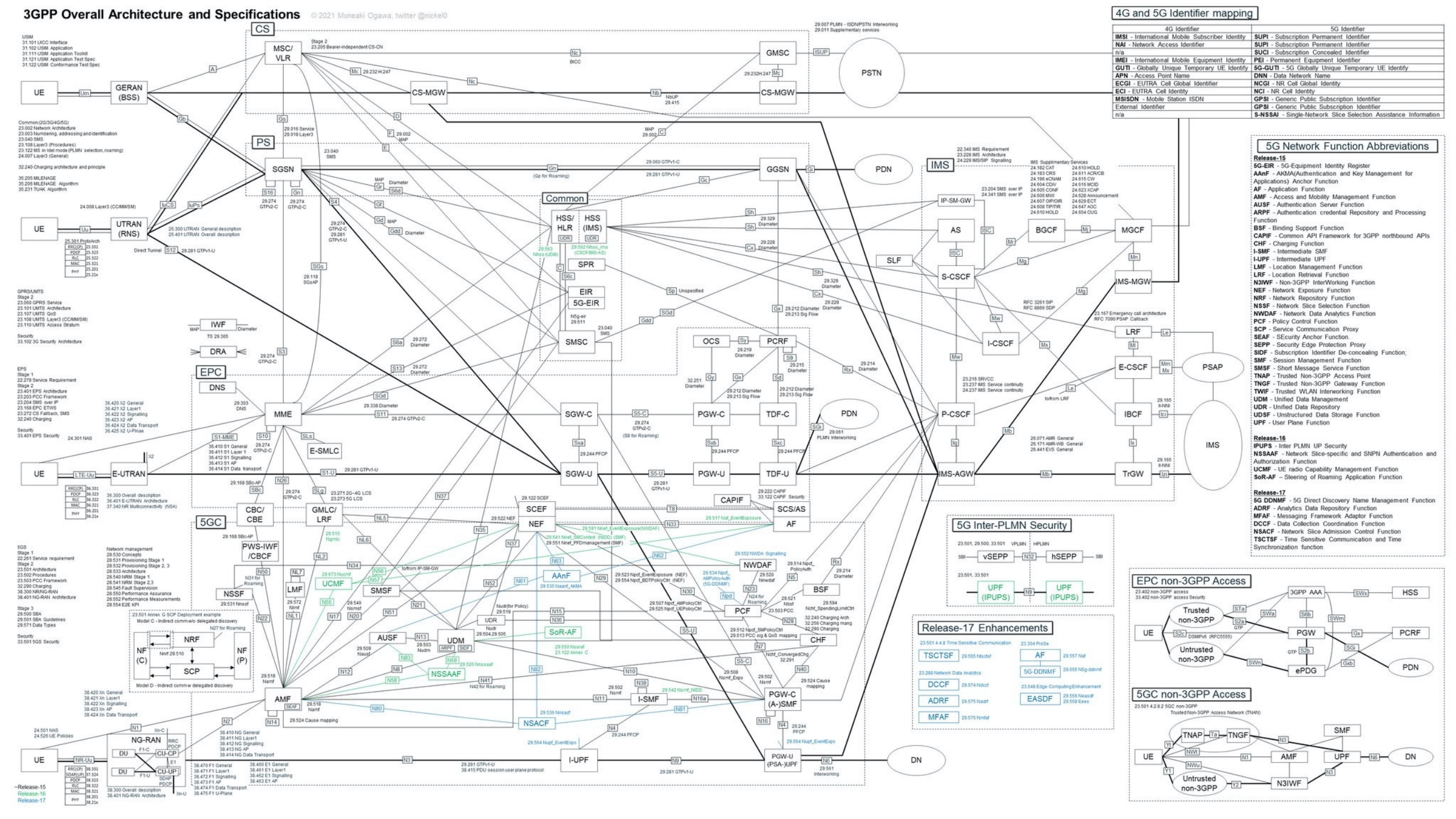
Your expectations

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

3. 2G to 5G

(concepts & toy examples)

3GPP Overall Architecture and Specifications



4G and 5G Identifier mapping

4G Identifier	5G Identifier
IMSI - International Mobile Subscriber Identity	**SUPI** - Subscription Permanent Identifier
NAI - Network Access Identifier	**SUPI** - Subscription Permanent Identifier
n/a	**SUCI** - Subscription Concealed Identifier
IMEI - International Mobile Equipment Identity	**PEI** - Permanent Equipment Identifier
GUTI - Globally Unique Temporary UE Identity	**5G-GUTI** - 5G Globally Unique Temporary UE Identity
APN - Access Point Name	**DNN** - Data Network Name
ECGI - EUTRA Cell Global Identifier	**NCGI** - NR Cell Global Identity
ECI - EUTRA Cell Identity	**NCI** - NR Cell Identity
MSISDN - Mobile Station ISDN	**GPSI** - Generic Public Subscription Identifier
External Identifier	**GPSI** - Generic Public Subscription Identifier
n/a	**S-NSSAI** - Single-Network Slice Selection Assistance Information

5G Network Function Abbreviations

Release-15

5G-EIR - 5G-Equipment Identity Register
AAnF - AKMA(Authentication and Key Management for Applications) Anchor Function
AF - Application Function
AMF - Access and Mobility Management Function
AUSF - Authentication Server Function
ARPF - Authentication credential Repository and Processing Function
BSF - Binding Support Function
CAPIF - Common API Framework for 3GPP northbound APIs
CHF - Charging Function
I-SMF - Intermediate SMF
I-UPF - Intermediate UPF
LMF - Location Management Function
LRF - Location Retrieval Function
N3IWF - Non-3GPP InterWorking Function
NEF - Network Exposure Function
NRF - Network Repository Function
NSSF - Network Slice Selection Function
NWDAF - Network Data Analytics Function
PCF - Policy Control Function
SCP - Service Communication Proxy
SEAF - SEcurity Anchor Function.
SEPP - Security Edge Protection Proxy
SIDF - Subscription Identifier De-concealing Function;
SMF - Session Management Function
SMSF - Short Message Service Function
TNAP - Trusted Non-3GPP Access Point
TNGF - Trusted Non-3GPP Gateway Function
TWIF - Trusted WLAN Interworking Function
UDM - Unified Data Management
UDR - Unified Data Repository
UDSF - Unstructured Data Storage Function
UPF - User Plane Function

Release-16

IPUPS - Inter PLMN UP Security
NSSAAF - Network Slice-specific and SNPN Authentication and Authorization Function
UCMF - UE radio Capability Management Function
SoR-AF - Steering of Roaming Application Function

Release-17

5G DDNMF - 5G Direct Discovery Name Management Function
ADRF - Analytics Data Repository Function
MFAF - Messaging Framework Adaptor Function
DCCF - Data Collection Coordination Function
NSACF - Network Slice Admission Control Function
TSCTSF - Time Sensitive Communication and Time Synchronization function

5G Inter-PLMN Security

23.501, 29.500, 33.501 VPLMN HPLMN

SBI vSEPP N32 hSEPP SBI

23.501, 33.501

UPF (IPUPS) N9 UPF (IPUPS)

Release-17 Enhancements

23.501 4.4.8 Time Sensitive Communication
TSCTSF 29.565 Ntsctsf

23.288 Network Data Analytics
DCCF 29.574 Ndccf
ADRF 29.575 Nadrf
MFAF 29.576 Nmfaf

23.304 ProSe
AF 29.557 Naf
5G-DDNMF 29.555 N5g-ddnmf

23.548 Edge Computing Enhancement
EASDF 29.556 Neasdf 29.558 Eees

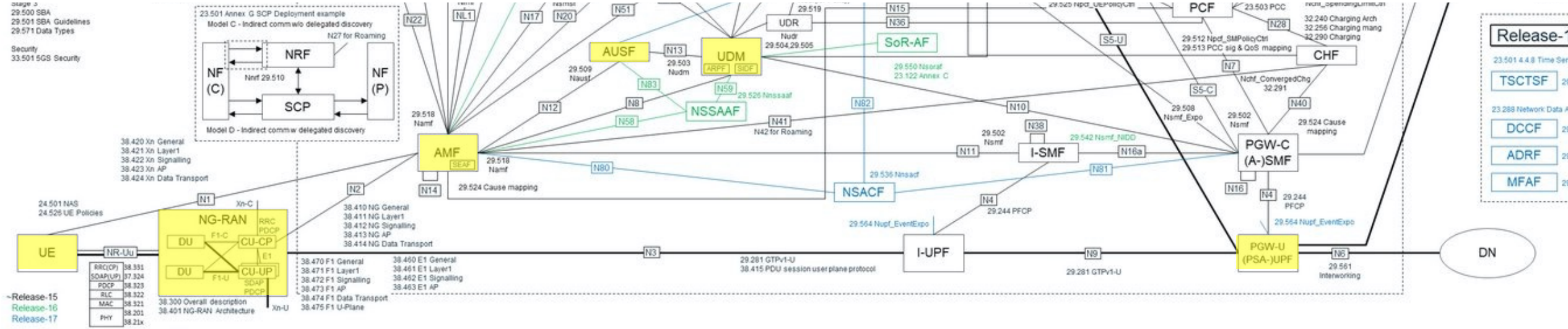
EPC non-3GPP Access

23.402 non-3GPP access
33.402 non-3GPP access Security

5GC non-3GPP Access

23.501 4.2.8.2 5GC non-3GPP
Trusted Non-3GPP Access Network (TNAN)

Release-15
Release-16
Release-17


29.500 SBA
29.501 SBA Guidelines
29.571 Data Types
Security
33.501 5GS Security
23.501 Annex G SCP Deployment example
Model C - Indirect comm w/o delegated discovery
N27 for Roaming
NRF
Nnrf 29.510
NF (C)
SCP
NF (P)
Model D - Indirect comm w delegated discovery
38.420 Xn General
38.421 Xn Layer1
38.422 Xn Signalling
38.423 Xn AP
38.424 Xn Data Transport
24.501 NAS
24.526 UE Policies
UE
NR-Uu
NG-RAN
RRC
PDCP
F1-C
F1-U
DU
DU
CU-CP
CU-UP
E1
SDAP
PDCP
Xn-C
Xn-U
RRC(CP) 38.331
SDAP(UP) 37.324
PDCP 38.323
RLC 38.322
MAC 38.321
PHY 38.201
38.21x
38.300 Overall description
38.401 NG-RAN Architecture
38.410 NG General
38.411 NG Layer1
38.412 NG Signalling
38.413 NG AP
38.414 NG Data Transport
38.470 F1 General
38.471 F1 Layer1
38.472 F1 Signalling
38.473 F1 AP
38.474 F1 Data Transport
38.475 F1 U-Plane
38.460 E1 General
38.461 E1 Layer1
38.462 E1 Signalling
38.463 E1 AP
Release-15
Release-16
Release-17
AMF
SEAF
29.518 Namf
29.524 Cause mapping
AUSF
29.509 Naust
UDM
ARPF
SIDF
29.503 Nudm
UDR
Nudr
29.504,29.505
29.519
NSSAAF
29.526 Nnssaaf
N42 for Roaming
NSACF
29.536 Nnsacf
SoR-AF
29.550 Nsoraf
23.122 Annex C
PCF
23.503 PCC
29.512 Npcf_SMPolicyCtrl
29.513 PCC sig & QoS mapping
32.240 Charging Arch
32.256 Charging mang
32.290 Charging
CHF
Nchf_ConvergedChg
32.291
29.508 Nsmf_Expo
29.502 Nsmf
29.524 Cause mapping
I-SMF
29.542 Nsmf_NIDD
PGW-C (A-)SMF
29.244 PFCP
29.564 Nupf_EventExpo
I-UPF
PGW-U (PSA-)UPF
29.281 GTPv1-U
38.415 PDU session user plane protocol
29.561 Interworking
DN
N1
N2
N3
N4
N6
N7
N8
N9
N10
N11
N12
N13
N14
N15
N16
N16a
N17
N20
N22
N28
N36
N38
N40
N41
N51
N58
N59
N80
N81
N82
N83
S5-C
S5-U
NL1
Release-1
23.501 4.4.8 Time Ser
TSCTSF
23.288 Network Data A
DCCF
ADRF
MFAF

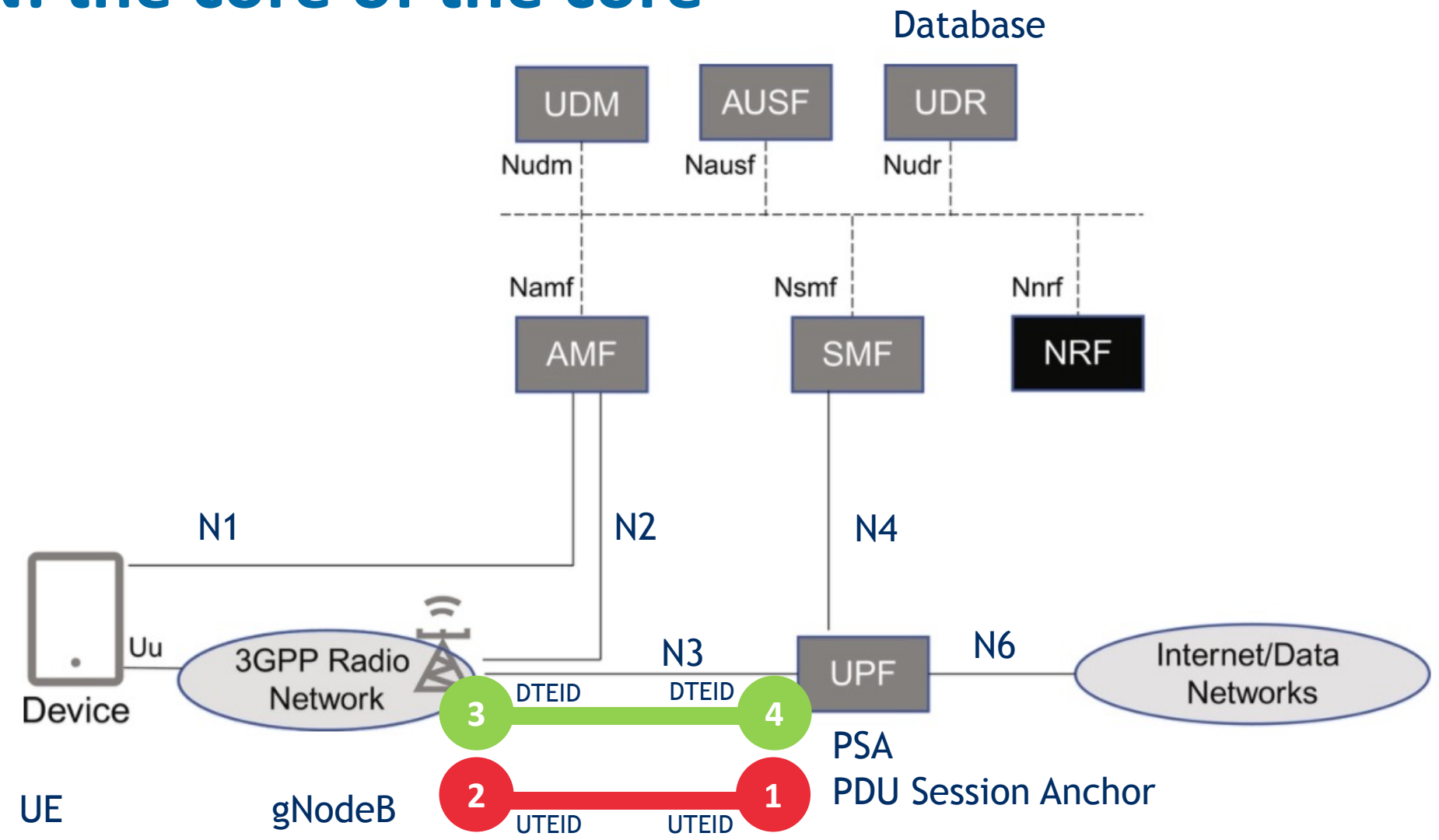
What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel~~
8. ~~Authenticate~~
9. Ask to send data (or get some data)
10. Ask to make a call
11. Move around
12. … (location update, release call, handover, etc …)

5G CN: the core of the core

U

D



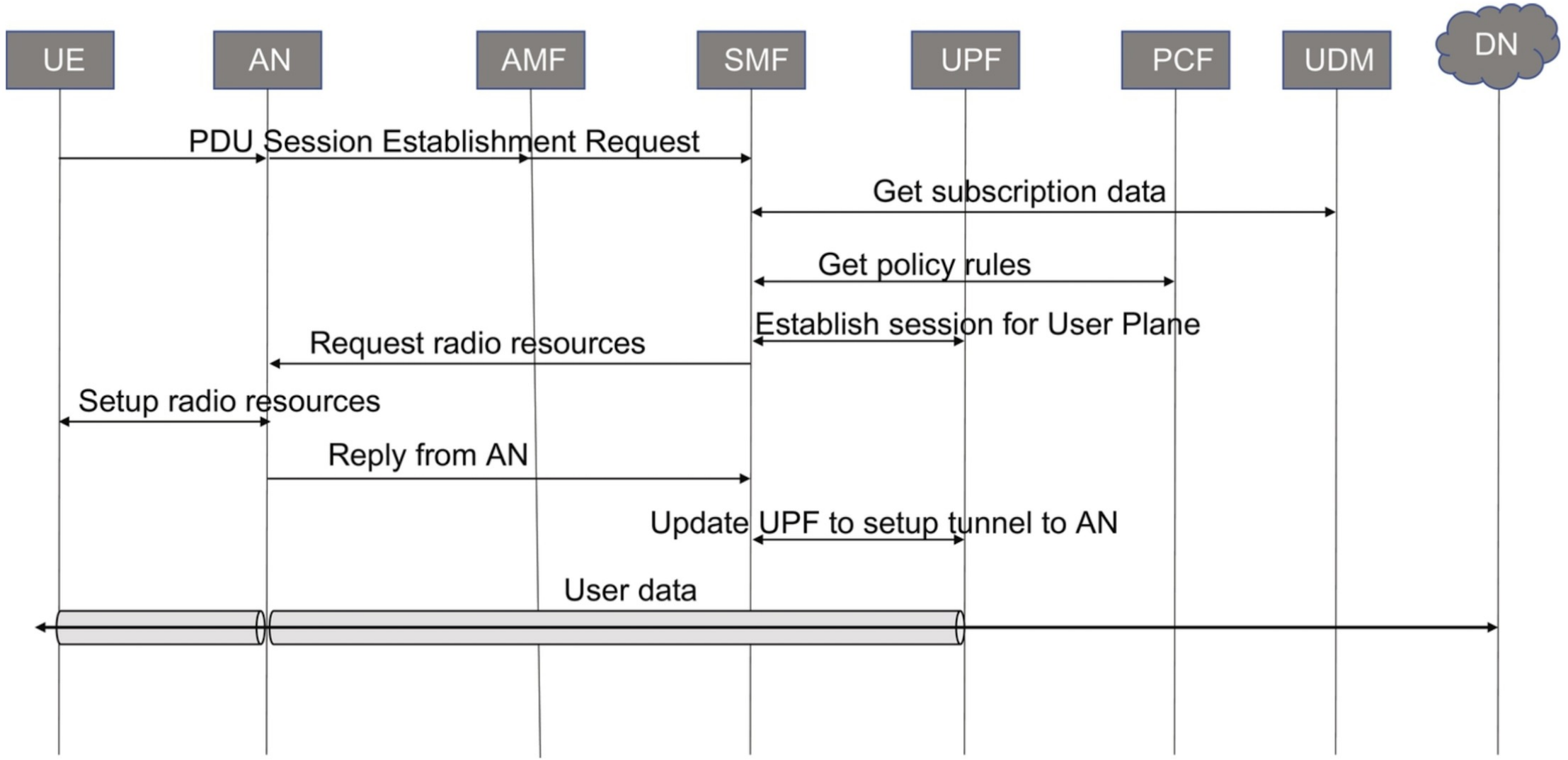
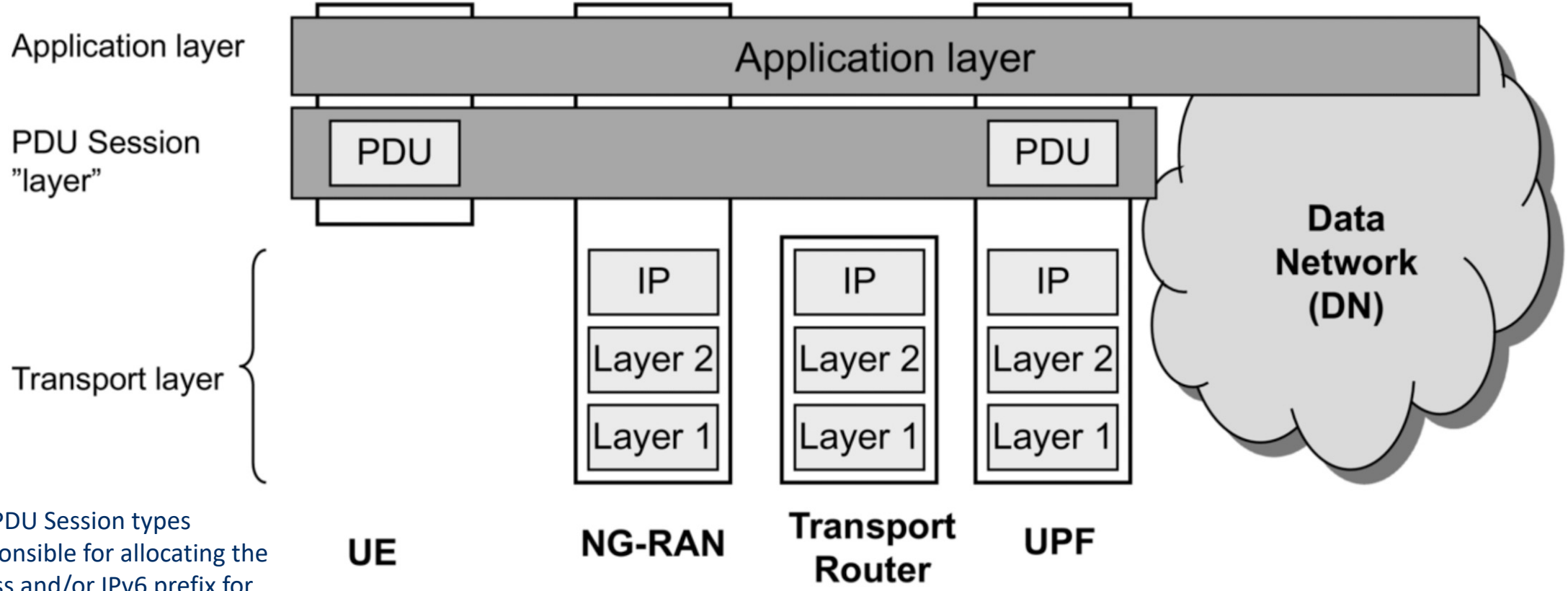


FIG. 6.1 Simplified PDU Session Establishment procedure.



For IP based PDU Session types

- 5GC is responsible for allocating the IPv4 address and/or IPv6 prefix for the UE (static or DHCPv4).
- The IP address allocated to the UE belongs to the DN where the UE is accessing.
- Different from the IP network (or backbone) that provides the IP transport between entities within the 5GC, or between the (R)AN and 5GC (private)

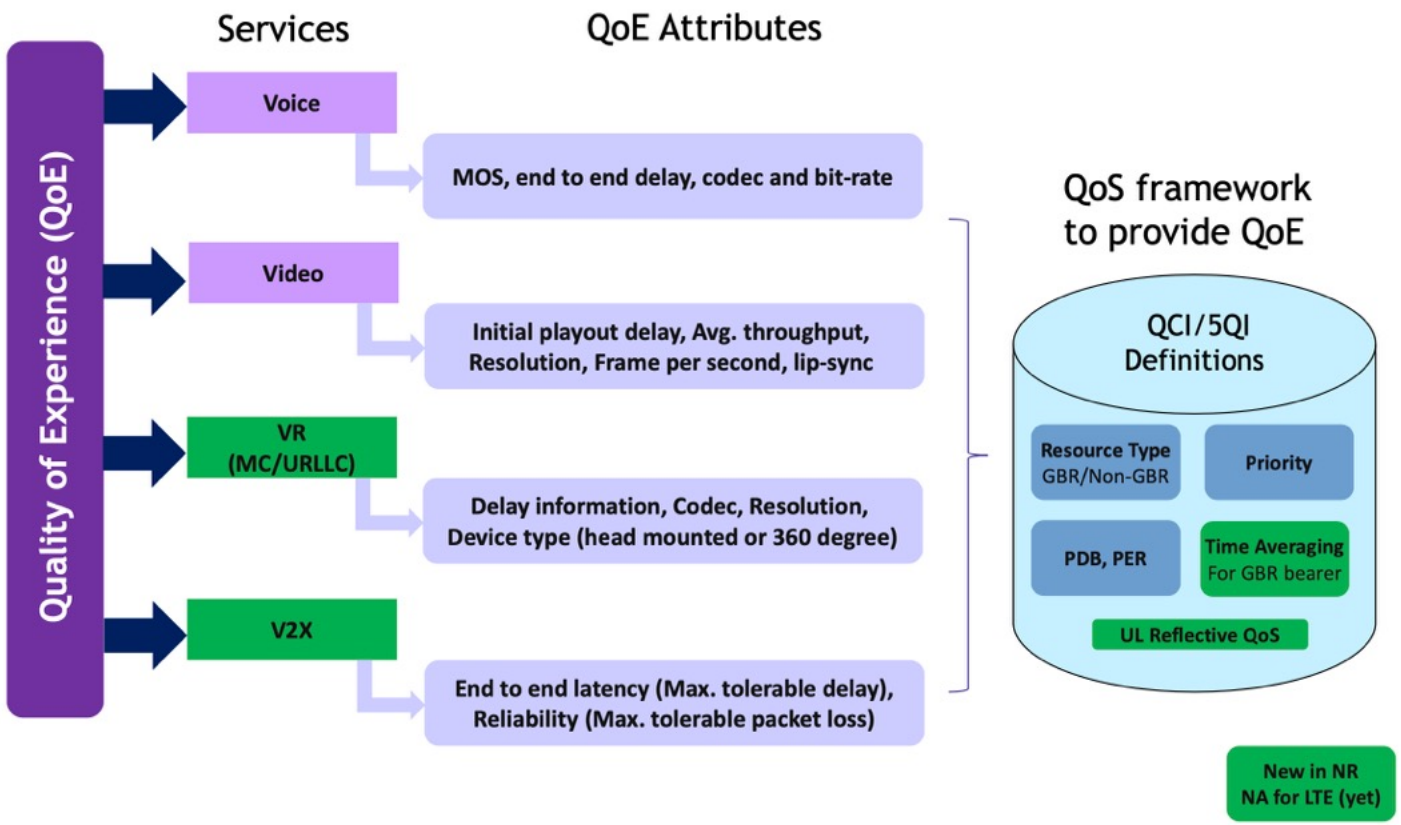
Main properties that characterize a PDU Session

PDU Session property	Description
PDU Session Identifier	An identifier of the PDU Session in the UE and network
Slice identifier (S-NSSAI)	Refers to the network slice in which the PDU Session is established
Data Network Name (DNN)	Name of the DN to which the PDU Session provides connectivity
PDU Session type	The basic end-user protocol type carried by the PDU Session. It can be IPv4, IPv6, dual-stack IPv4/IPv6, Ethernet or Unstructured
Service and Session Continuity (SSC) mode	Refers to the longevity of the User Plane anchor point of the PDU Session, whether it can be re-allocated or not
User Plane Security Enforcement information	Information indicating whether user-plane ciphering and/or use-plane integrity protection is to be activated for the PDU Session

Session management

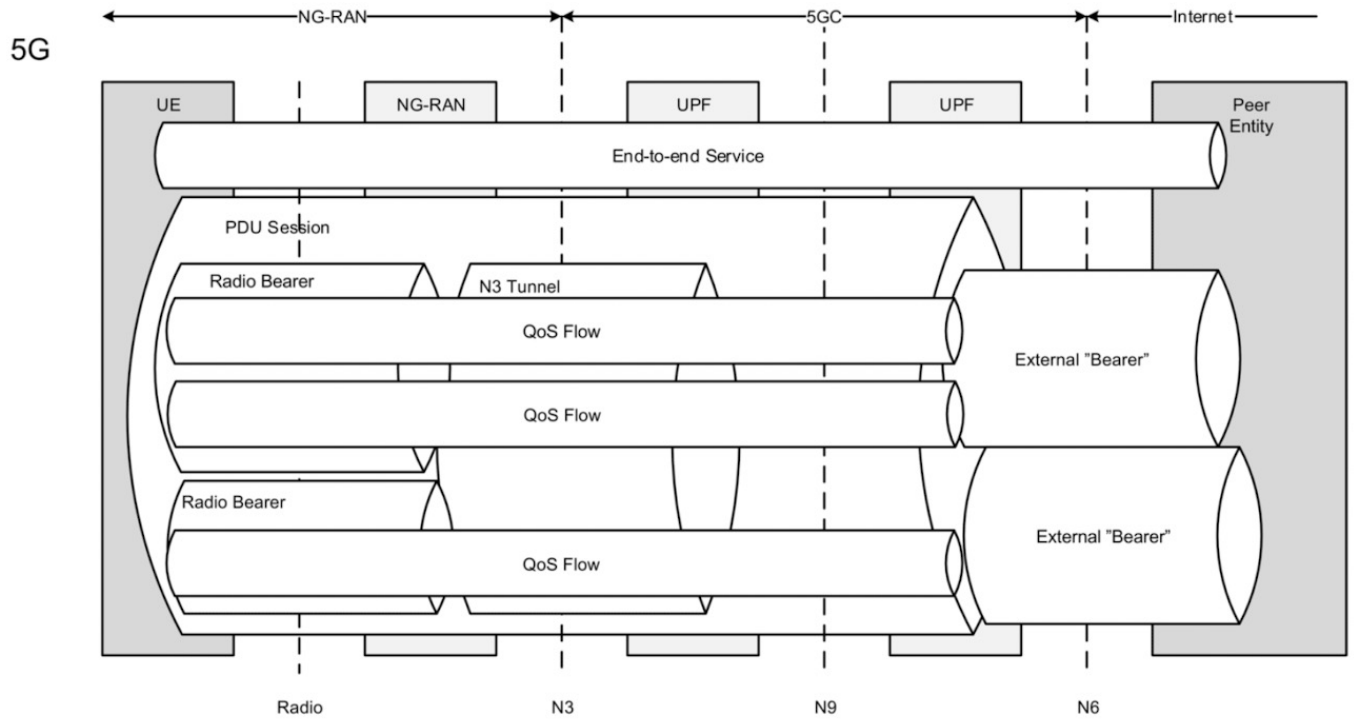
- Main task: User Plane for the PDU Session, consisting of a concatenation of multiple legs.
  1. User Plane connection over the access technology used (e.g. NG-RAN).
     - one or more Data Radio Bearers (DRBs) managed by the NG-RAN
  2. From the gNB/AN (access node) there is then a User Plane connection toward a UPF in the core network (over the N3 reference point)
     - data is carried in GTP-U tunnels
  3. Possibly additional hops between UPFs in the core network (over the N9 reference point)
     - data is carried in GTP-U tunnels
  4. Then the User Plane connection continues into the DN (over the N6 reference point).

From QoS to QoE: Quality of Service/Experience



QoS in 5G

- The concept of QoS in 5G is flow based. Packets are classified and marked using QFI (QoS Flow Identifier). The 5G QoS flows are mapped in the AN (Access Network) to DRBs (Data Radio Bearers; unlike 4G LTE where mapping is one to one between EPC and radio bearers).

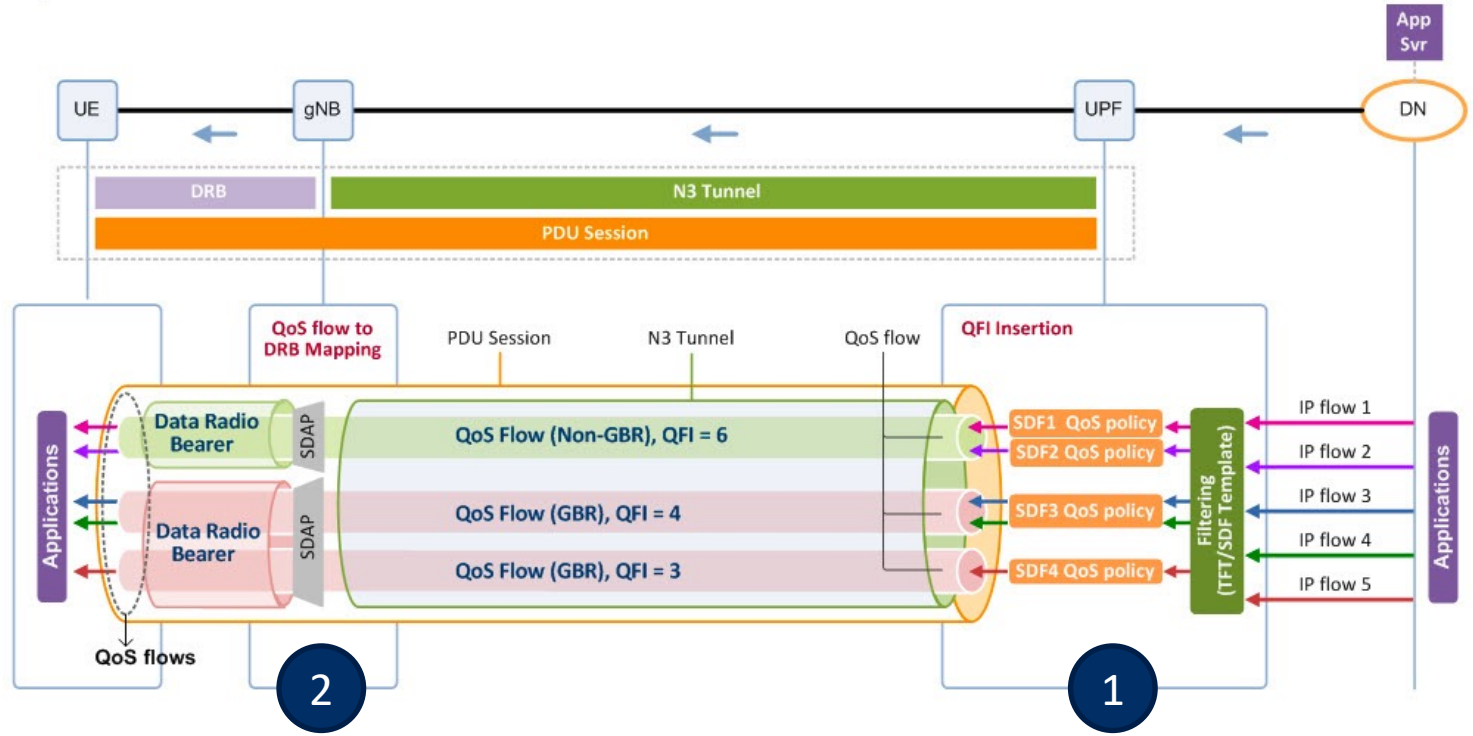


SDAP

- **Service Data Application Protocol (SDAP)** is responsible for mapping QoS bearers to radio bearers according to their quality-of-service requirements. This protocol layer is not present in LTE but introduced in NR when connecting to the 5G core network due to the new quality-of-service handling. It also tackles Reflective **QoS.**

Overall view: 2 step process

The QoS differentiation within a PDU session



5QI : 5G QoS Identifier
ARP : Allocation and Retention Priority
GFBR : Guaranteed Flow Bit Rate
MFBR : Maximum Flow Bit Rate
PDB : Packet Delay Budget
PER : Packet Error Rate
QFI : QoS Flow Identifier
RQA : Reflective QoS Attribute

QoS Flow type		QoS Flow parameters
GBR flow	Non-GBR flow	5QI
		ARP
		RQA
		GFBR
		MFBR
		Notification Control
		Maximum Packet Loss Rate

5QI

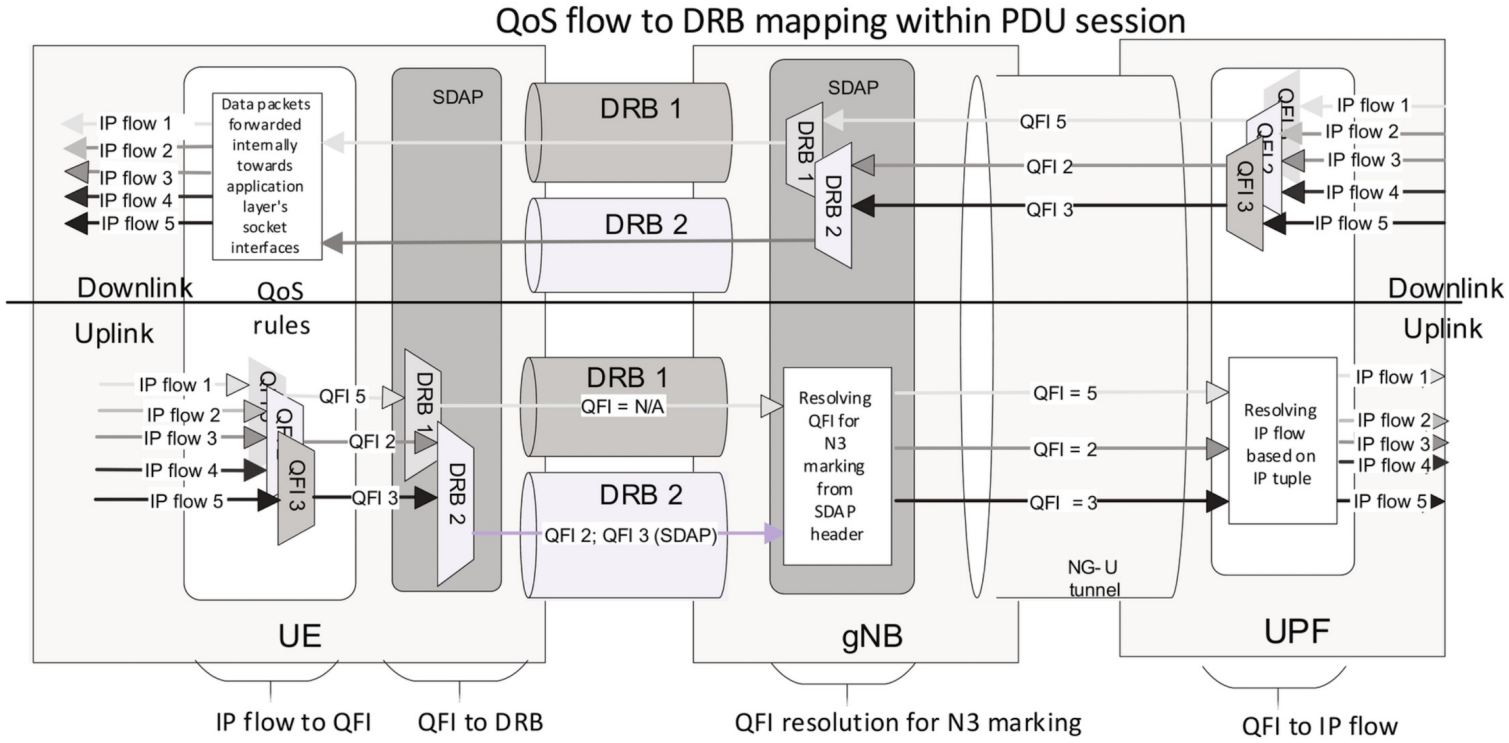
Resource Type*
Default Priority Level
PDB
PER
Default Maximum Data Burst Volume
Default Averaging Window

* GBR, non-GBR or delay critical GBR

QCI to 5QI

5QI - (5G QoS Indicators)							
5QI Value	ResourceType	DefaultPriorityLevel	PacketDelayBudget	PacketErrorRate	DefaultMaximumData BurstVolume	DefaultAveragingWindow	Example Services
1	GBR	20	100 ms	10^{-2}	N/A	2000 ms	Conversational Voice
2	GBR	40	150 ms	10^{-3}	N/A	2000 ms	Conversational Video(Live Streaming)
3	GBR	30	50 ms	10^{-3}	N/A	2000 ms	Real Time Gaming,V2X messagesElectricity distribution –medium voltage,Process automation -monitoring
4	GBR	50	300 ms	10^{-6}	N/A	2000 ms	Non-ConversationalVideo (BufferedStreaming)
65	GBR	7	75 ms	10^{-2}	N/A	2000 ms	Mission Critical userplane Push To Talkvoice (e.g., MCPTT)
66	GBR	20	100 ms	10^{-2}	N/A	2000 ms	Non-Mission-Criticaluser plane Push ToTalk voice
67	GBR	15	100 ms	10^{-3}	N/A	2000 ms	Mission Critical Videouser plane
75	GBR	This 5QI is not supported in this Release(16.4) of the specification as it is only used for transmission of V2X messagesover MBMS bearers as defined in TS 23.285 but the value is reserved for future use.					
71	GBR	56	150 ms	10^{-3}	N/A	2000 ms	Live" Uplink Streaming(e.g. TS 26.238)
72	GBR	56	300 ms	10^{-8}	N/A	2000 ms	Live" Uplink Streaming(e.g. TS 26.238)
73	GBR	56	300 ms	10^{-8}	N/A	2000 ms	Live" Uplink Streaming(e.g. TS 26.238)
74	GBR	56	500 ms	10^{-8}	N/A	2000 ms	Live" Uplink Streaming(e.g. TS 26.238)
76	GBR	56	500 ms	10^{-4}	N/A	2000 ms	Live" Uplink Streaming(e.g. TS 26.238)
5	Non-GBR	10	100 ms	10^{-6}	N/A	N/A	IMS Signalling
6	Non-GBR	60	300 ms	10^{-6}	N/A	N/A	Video (BufferedStreaming)TCP-based (e.g., www,e-mail, chat, ftp, p2pfile sharing, progressivevideo, etc.)
7	Non-GBR	70	100 ms	10^{-3}	N/A	N/A	Voice,Video (Live Streaming)Interactive Gaming
8	Non-GBR	80	300 ms	10^{-6}	N/A	N/A	Video (BufferedStreaming)TCP-based (e.g., www,e-mail, chat, ftp, p2pfile sharing, progressive video, etc.)
9	Non-GBR	90	300 ms	10^{-6}	N/A	N/A	Video (BufferedStreaming)TCP-based (e.g., www,e-mail, chat, ftp, p2pfile sharing, progressive video, etc.)
69	Non-GBR	5	60 ms	10^{-6}	N/A	N/A	Mission Critical delaysensitive signalling(e.g., MC-PTTsignalling)
70	Non-GBR	55	200 ms	10^{-6}	N/A	N/A	Mission Critical Data(e.g. example servicesare the same as 5QI6/8/9)
79	Non-GBR	65	50 ms	10^{-2}	N/A	N/A	V2X messages
80	Non-GBR	68	10 ms	10^{-6}	N/A	N/A	Low Latency eMBBapplicationsAugmented Reality
82	DelayCriticalGBR	19	10 ms	10^{-4}	255 Bytes	2000 ms	Discrete Automation(see TS 22.261)
83	DelayCriticalGBR	22	100 ms	10^{-4}	1354 Bytes	2000 ms	Discrete Automation(see TS 22.261)
84	DelayCriticalGBR	24	30 ms	10^{-5}	1354 Bytes	2000 ms	Intelligent transportsystems (TS 22.261)
85	DelayCriticalGBR	21	50 ms	10^{-5}	255 Bytes	2000 ms	Electricity Distributionhigh voltage (TS 22.261)
							By: Mohammed Ameen G S - 5G/LTE(RNO Engineer)

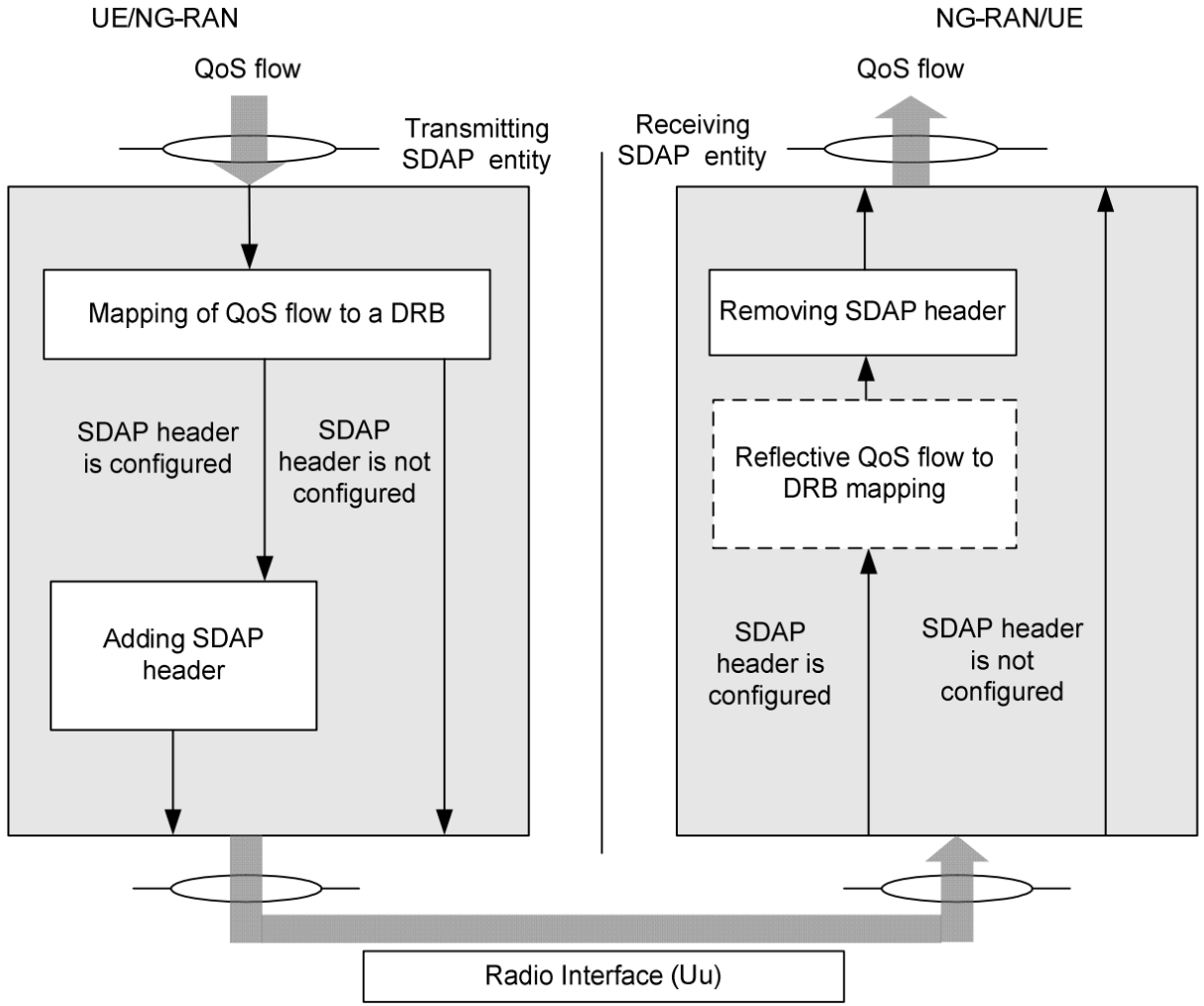
What about the uplink?



- UPF uses PDR (Packet Detection rules. 5-tuples) to QFI
- The **NG-RAN**, based on the QFI marking and the corresponding per QFI QoS Profile received e.g. during the establishment of the PDU Session, **decides how to map the QoS Flows to DRBs**. The Service Data Adaptation Protocol (SDAP) is used to enable multiplexing if more than one QoS Flow is sent on a DRB, i.e. if the NG-RAN decides to setup a DRB per QFI then the SDAP layer is not needed, unless Reflective QoS is used.

Reflective QoS

- In the case of **reflective mapping**, which is a new feature in NR when connected to the 5G core network, the device observes the QFI in the downlink packets for the PDU session. This provides the device with knowledge about which IP flows are mapped to which QoS flow and radio bearer. The device then uses the same mapping for the uplink traffic.



Protocol Layers in the RAN

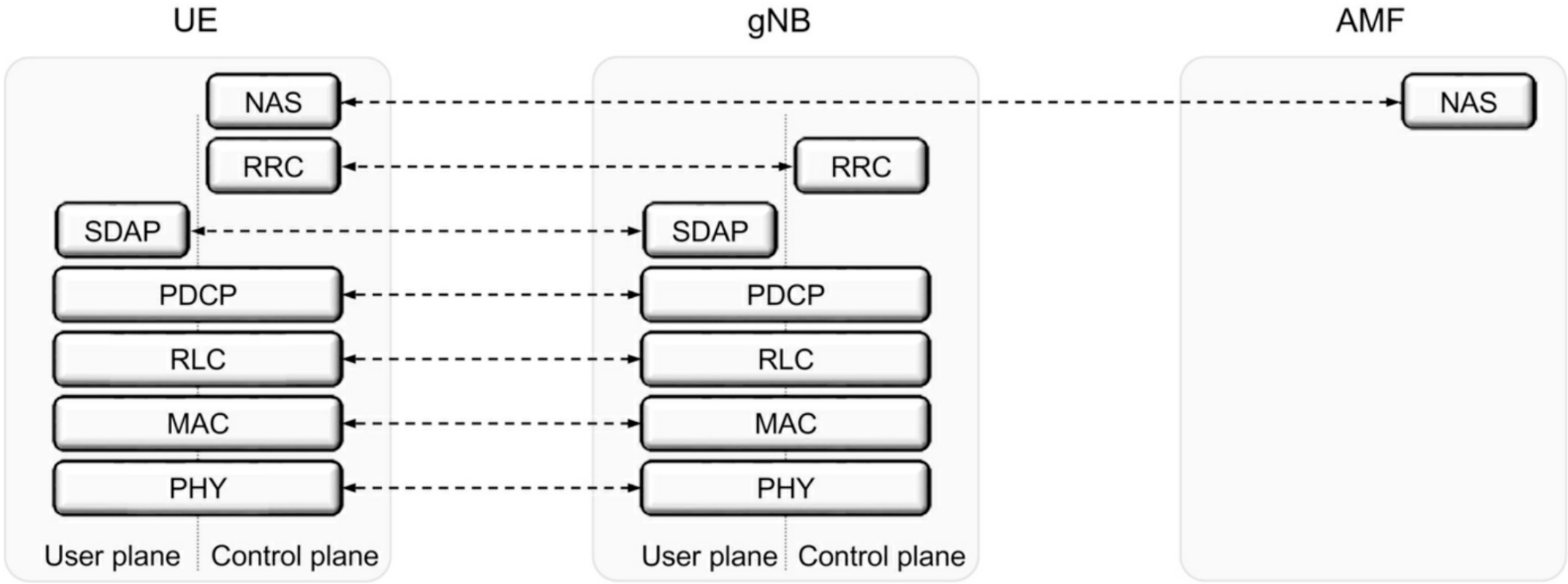
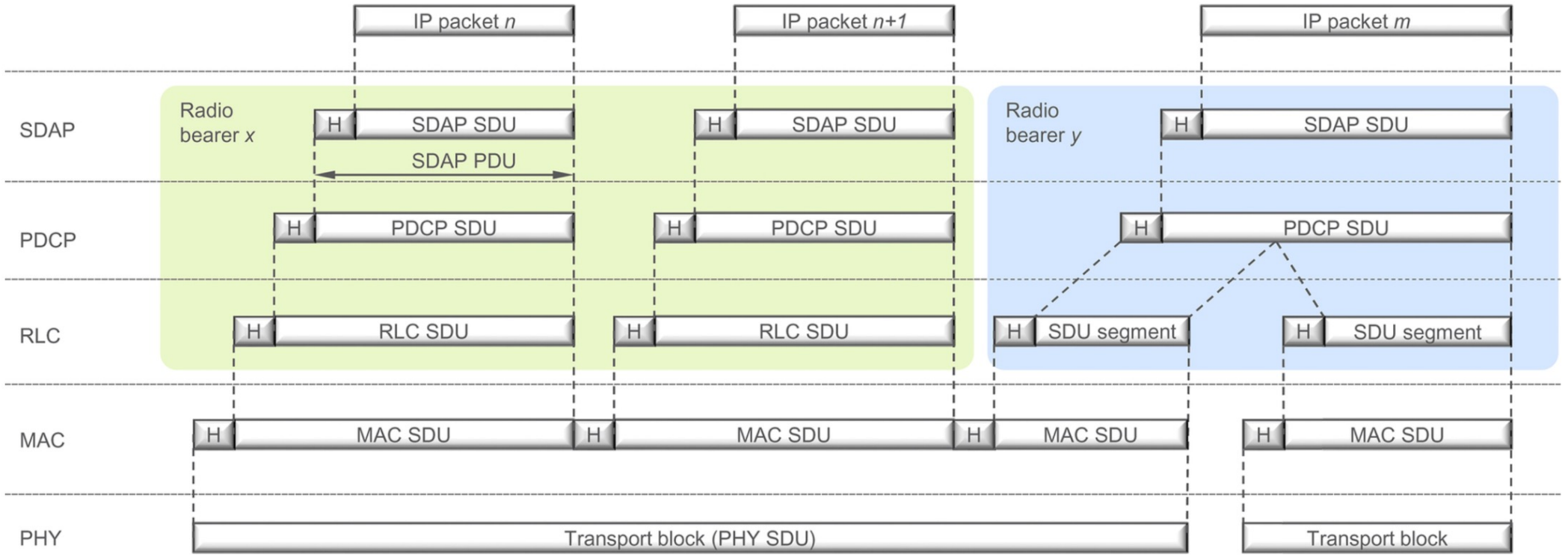


FIG. 6.6 User-plane and control-plane protocol stack.

SDAP = service data adaptation protocol flows (QoS)

Through the layers



SDU = Service Data Unit
PDU = Protocol Data Unit

http://www.techplayon.com/5g-nr-qos-architecture-qos-attribute-and-qos-flow/
http://5gblogs.com/5g-quality-of-services-qos/

Summarizing

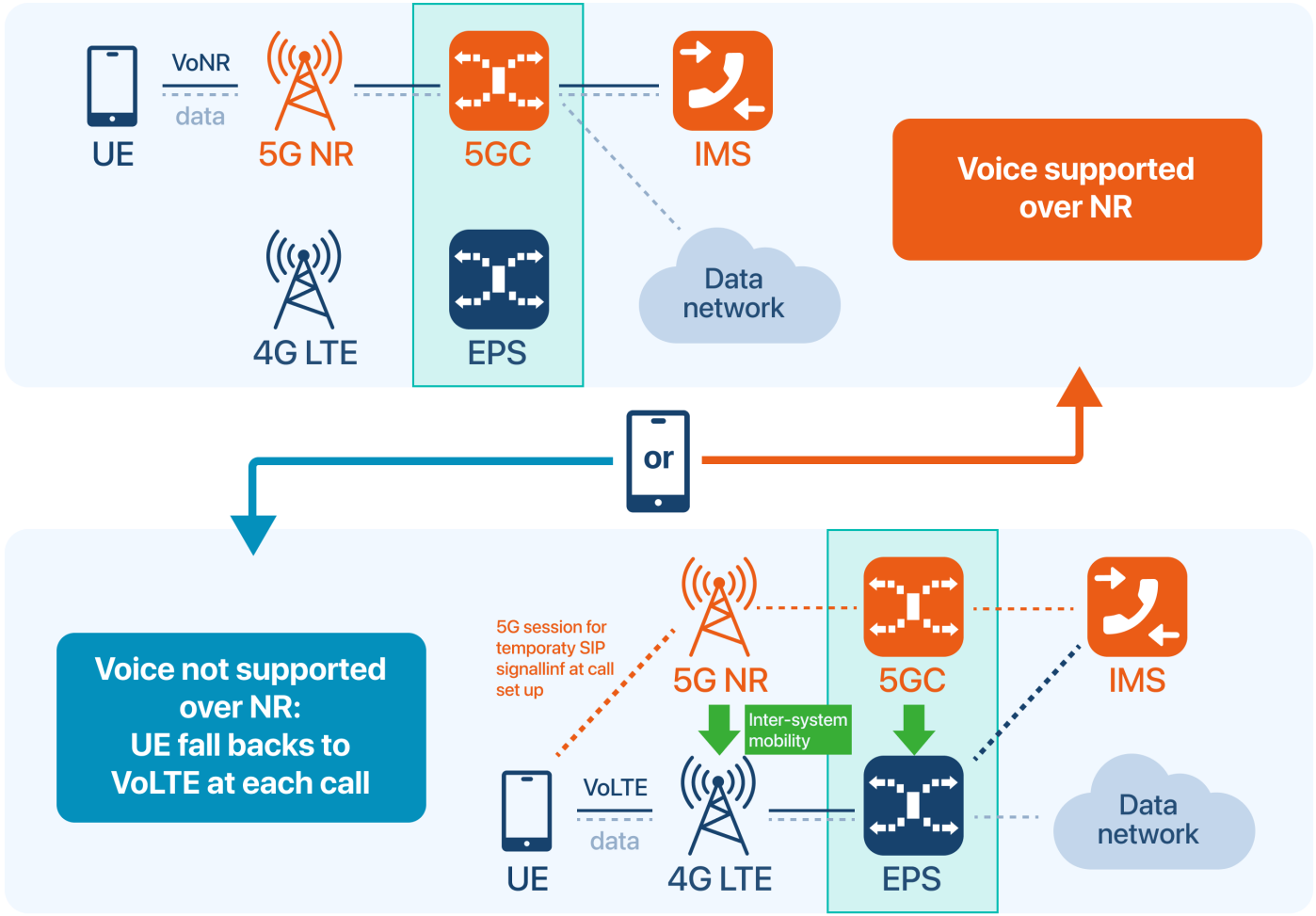
- In 5G, QoS is enforced at the **QoS flow level**.
- 5G uses QoS Flows, each identified by a **QoS Flow ID (QFI)**. Both **non-GBR flows and GBR** flows are supported in 5G, along with a new delay-critical GBR. 5G also introduces a new concept - **Reflective QoS.**
- The QoS flow is the lowest level granularity within the 5G system and is where policy and charging are enforced. One or more **Service Data Flows (SDFs)** can be transported in the same QoS flow, if they share the same policy and charging rules. All traffic within the same QoS flow receives the same treatment.
- 5G QoS to be assured on application basis, so we can create a QoS flow for each application and QoS flows are created dynamically without the need for E2E signaling. Also, short lived QoS flows (e.g., low latency requirements) can receive differentiated QoS treatment (without the overhead of establishing EPS bearers from E2E as in 4G).

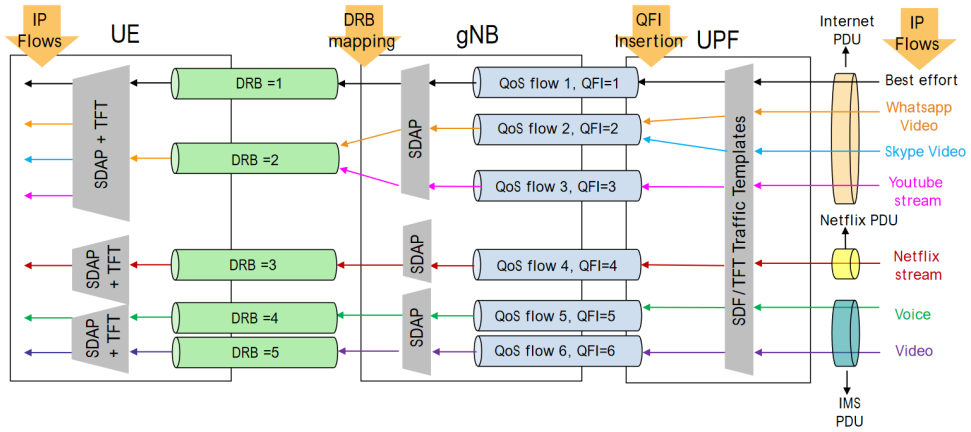
Parameter	5G	4G LTE
QoS Identifier	5G QoS Identifier - 5QI	Quality Class Indicator - QCI
IP Flow: UE to UPF/P-GW flow	QoS Flow	EPS Bearer
Flow/Bearer identifier	QoS Flow Identifier - QFI	EPS Bearer ID- EBI
Reflective QoS	Reflective QoS Indicator - RQI	N/A

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel~~
8. ~~Authenticate~~
9. ~~Ask to send data (or get some data)~~
10. Ask to make a call
11. Move around
12. … (location update, release call, handover, etc …)

A voice call… is data (over a different PDU)



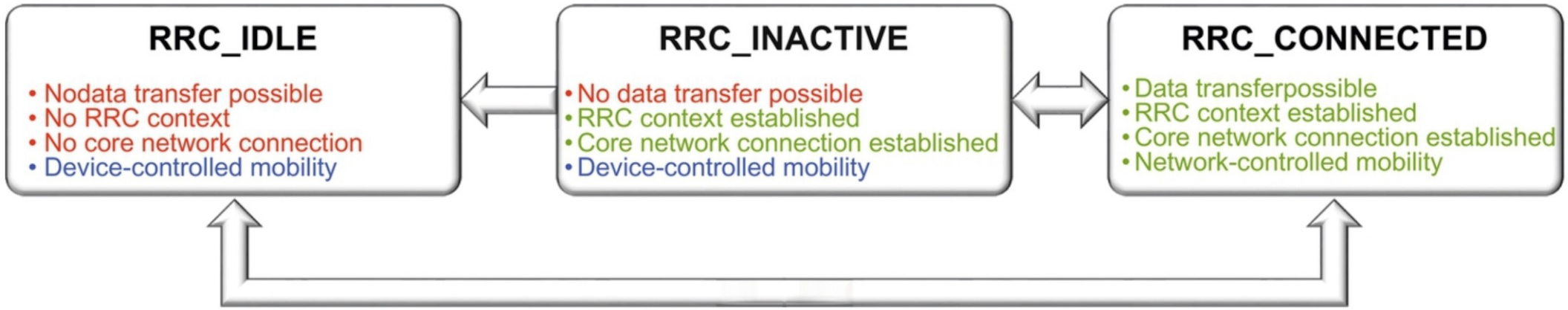


Different Packet Data Unit session associated with each PDN (“APN”).

What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel~~
8. ~~Authenticate~~
9. ~~Ask to send data (or get some data)~~
10. ~~Ask to make a call~~
11. Move around
12. … (location update, release call, handover, etc …)

Radio Resource Control State Machine

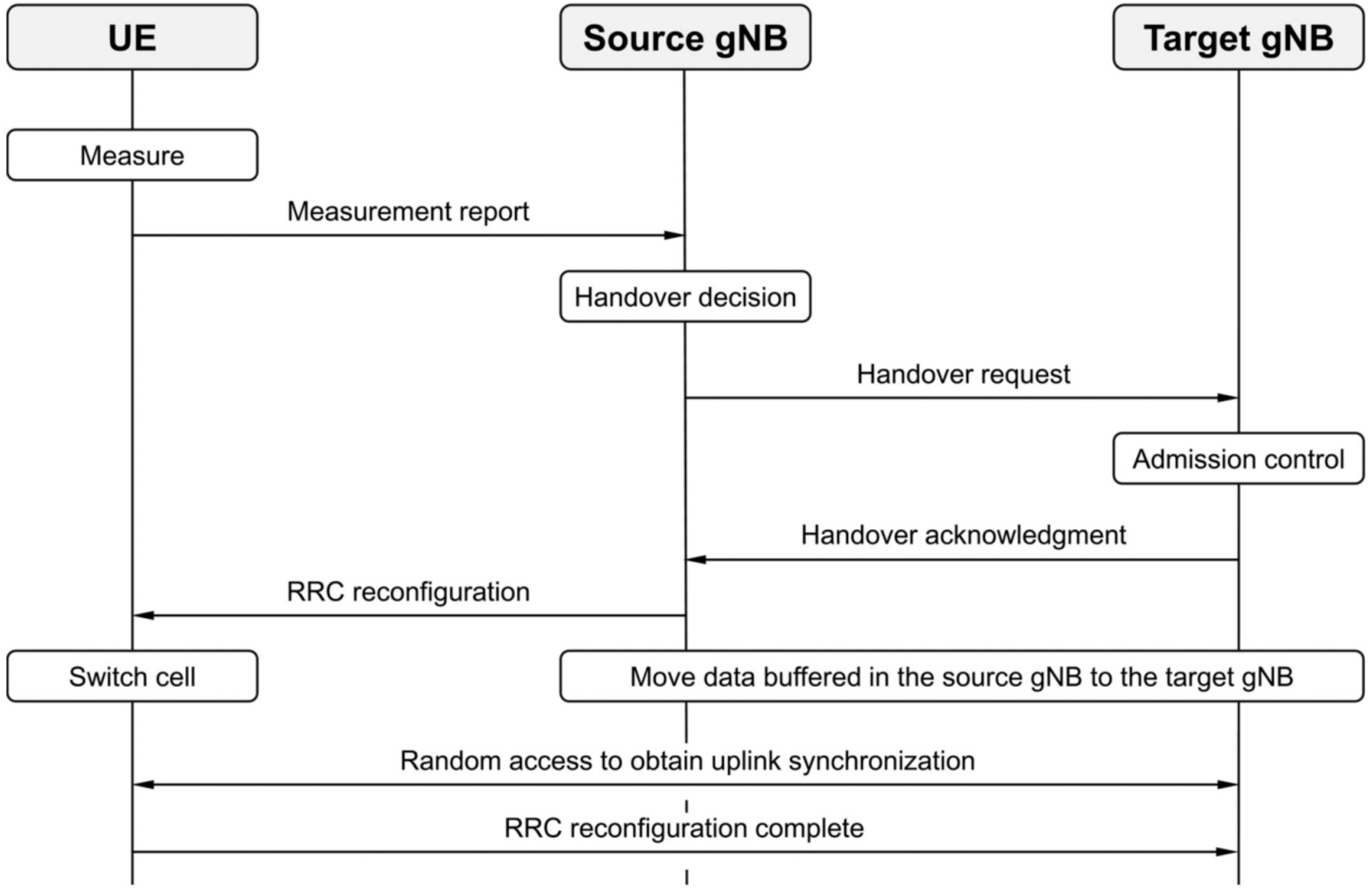


- In most wireless communication systems, the device can be in different states depending on the traffic activity. This is true also for NR and an NR device can be in one of three RRC states
  - RRC_IDLE: device sleeps most of the time to reduce battery consumption; periodically wakes up to receive paging messages; the only uplink transmission activity that may take place is random access.
  - RRC_CONNECTED: the device provides neighboring-cell measurements to the network, which instructs the device to perform a handover when needed.
  - RRC_INACTIVE: (new in 5G), transition to connected state for data transfer is fast as no core network signaling is needed; a mix.

Mobility: Handover/handoff

- **Classification based on system**
  - Inter-system (vertical)
  - Intra-system (horizontal)
- **Classification based on cell**
  - Intra-cell = channel or beam change vs.
  - Inter-cell = due to mobility
- **Classification based on action**
  - Hard = break-before-make
  - Soft = make-before-break
  - Dual connectivity = make-and-keep
- **Classification based on control**
  - Network-controlled
    - **Mobile-assisted (5G)**
  - Mobile-controlled

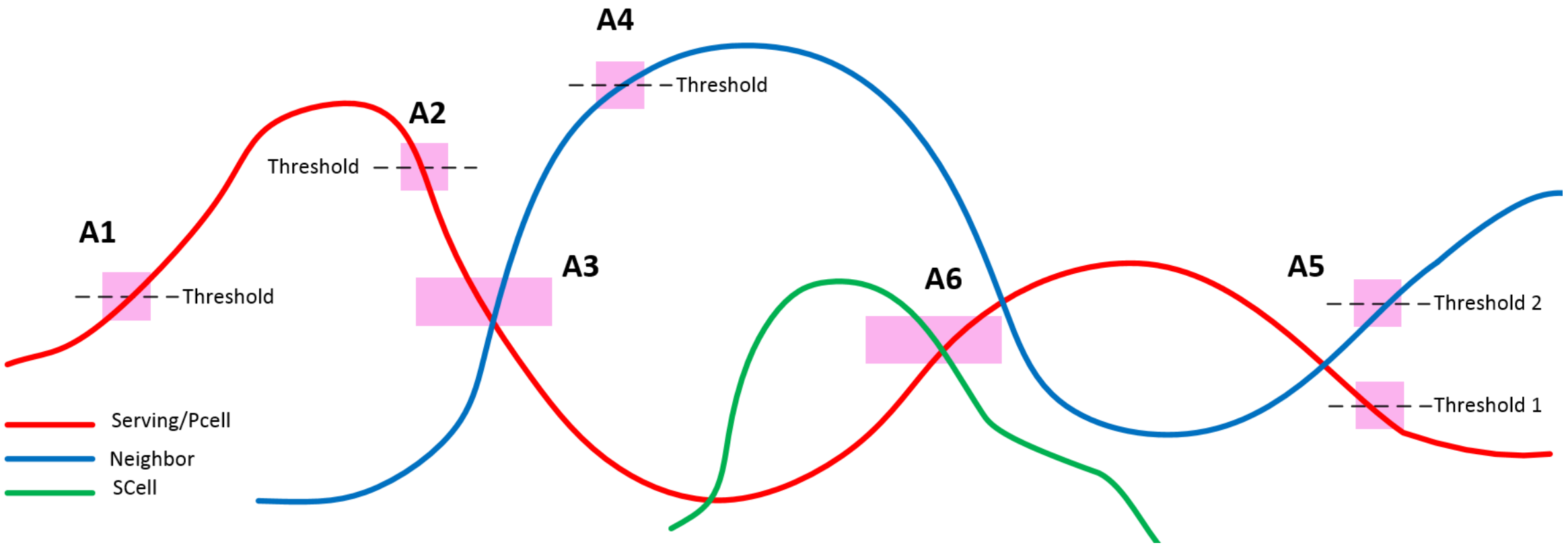
Handover procedure



Measurements set by Events and Timers

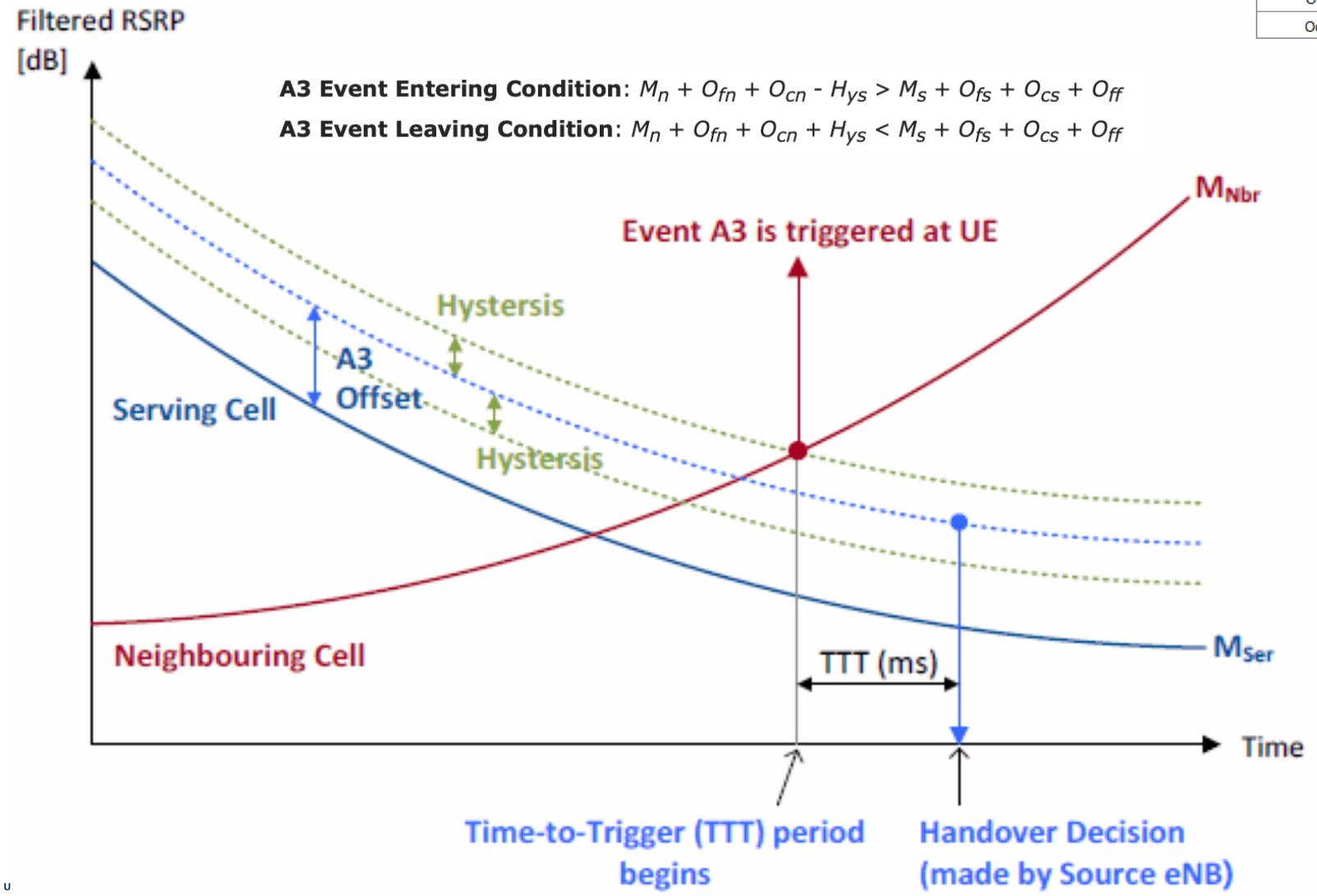
- The first step in cell-level mobility, which is continuously executed when in connected state, is to search for candidate cells using the cell search mechanism (listening to neighbour SSB)
- A measurement **event** is a **condition**, which should be fulfilled before the **measured value** is reported to the **network**.
- In NR, 6+2 different triggering conditions, or events:
  - Event A1 (Serving becomes better than threshold), triggered when the serving cell becomes better than a threshold. It is typically used to cancel an ongoing handover procedure.
  - Event A2 (Serving becomes worse than threshold), triggers a mobility procedure when a UE moves towards cell edge. Event A2 does not involve any neighbor cell measurements so it may be used to trigger a blind mobility procedure or it may be used to triggers neighbor cell measurements.
  - **Event A3 (Neighbor becomes offset better than SpCell)**, triggered when a neighbor cell becomes better than a special cell (typically serving cell) by an offset – relative measurement. The offset can be either positive or negative. There is also a configurable threshold included to avoid triggering the event if the difference between the two cells is very small. This event is typically used for intra-frequency or inter-frequency handover procedures.
  - Event A4 (Neighbor becomes better than threshold), triggered when neighbor cell becomes better than defined threshold. This event can be used for handover procedures which does not depend upon the coverage of the serving cell. For example, in load balancing.
  - Event A5 (SpCell becomes worse than threshold1 and neighbor becomes better than threshold2), like A3, but with absolute measures (a combo of A2 and A4)
  - Event A6 (Neighbour becomes offset better than SCell), like A3 for for carrier aggregation (SCell = Secondary Cell != SpCell = Serving Cell) It is also possible to configure other events in the device; the configuration and choice of events to use depend on the mobility strategy implemented in the network for a particular deployment. The purpose of using configurable events is to avoid unnecessary measurement reports to the network.
- **The decision to HO is made by the gNB.**

Events

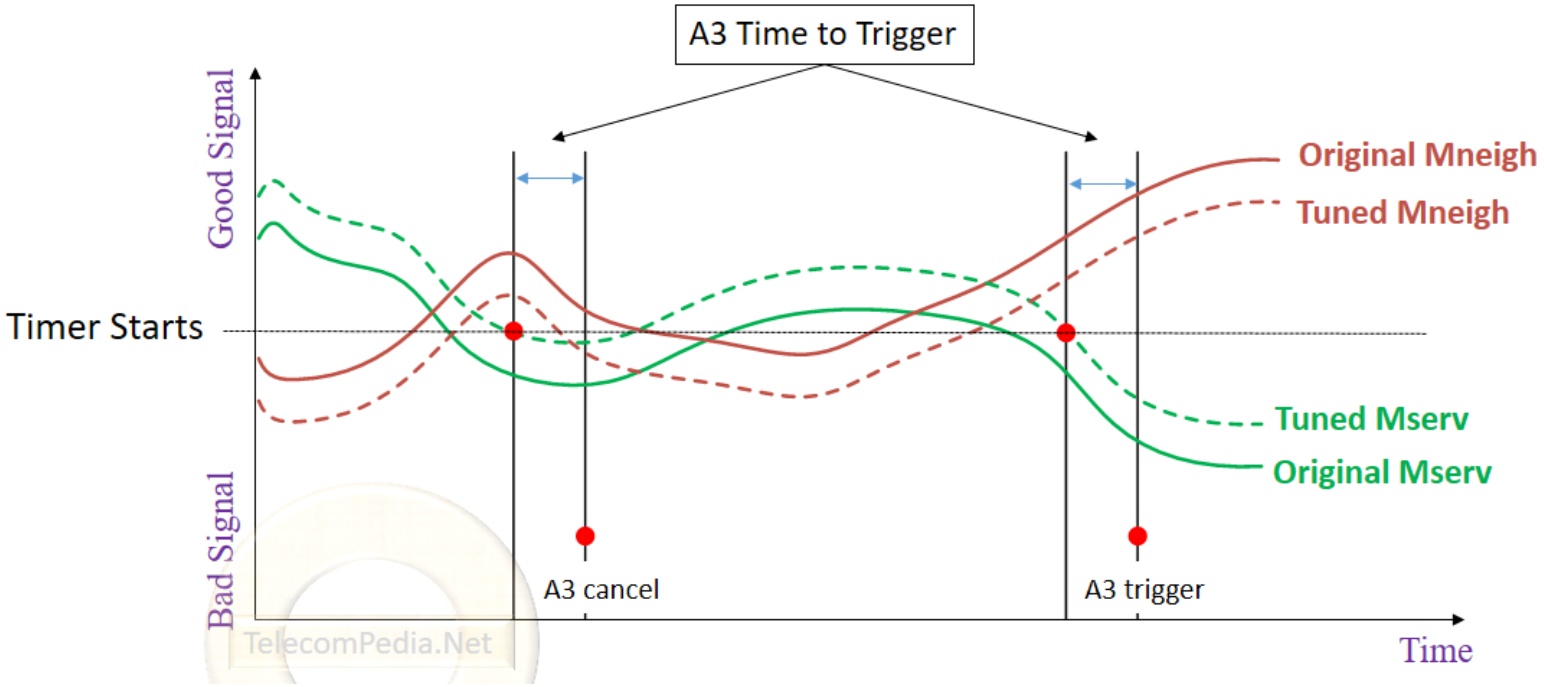

A4
Threshold
A2
Threshold
A1
Threshold
A3
A6
A5
Threshold 2
Threshold 1
Serving/Pcell
Neighbor
SCell

Example (TTT algo is unspecified)

Symbol	Definition
Mn	Measurement result of the neighbor cell
Ms	Measurement result of the serving cell
Hys	Hysteresis parameter for Event A3
Off	Offset parameter of Event A3
Ofn	Frequency specific offset of the frequency of the neighbor cell
Ocn	Cell specific offset of the neighbor cell
Ofs	Frequency specific offset of the serving frequency
Ocs	Cell specific offset of the serving cell

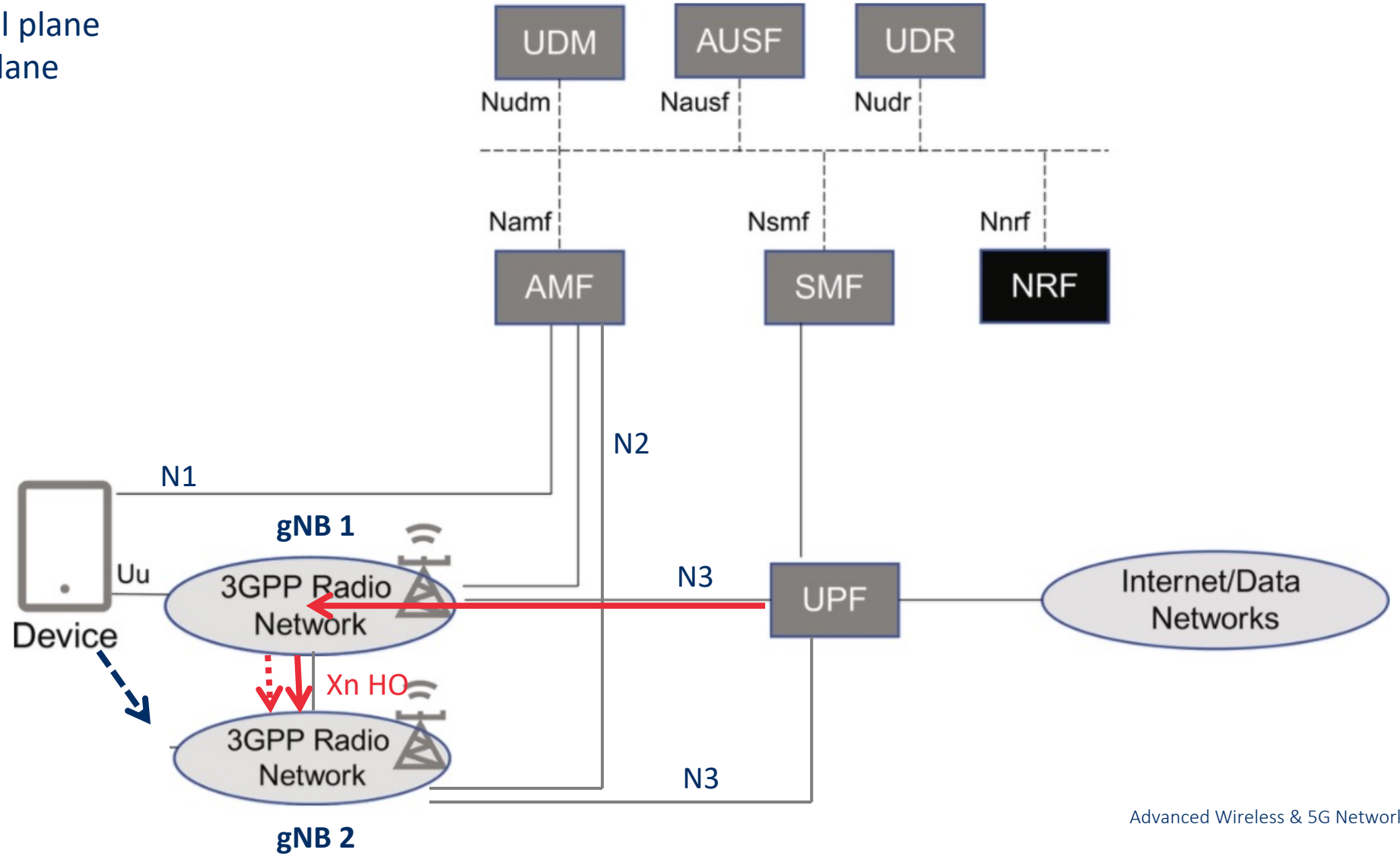


Example

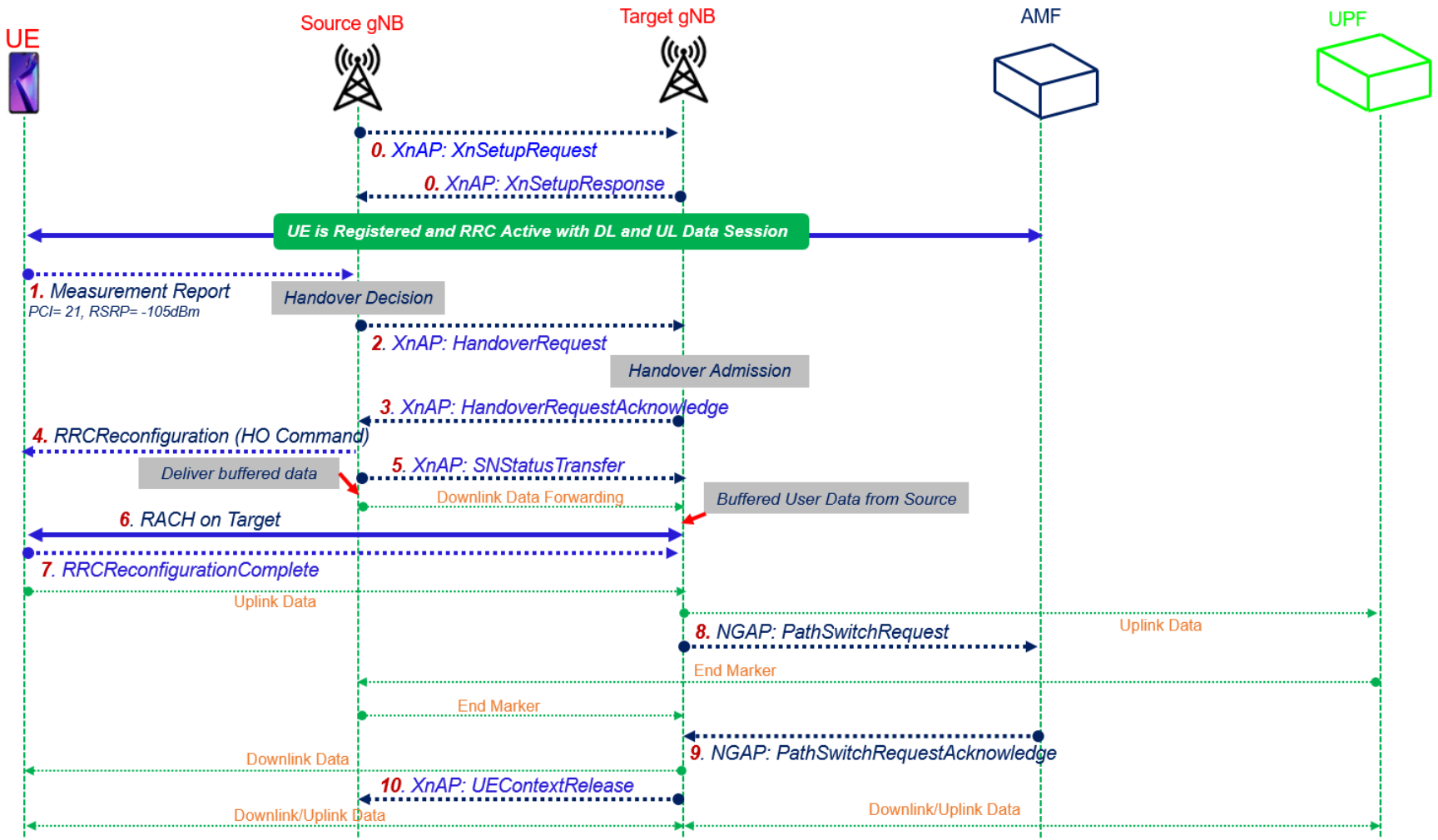

A3 Time to Trigger
Good Signal
Timer Starts
Bad Signal
Original Mneigh
Tuned Mneigh
Tuned Mserv
Original Mserv
A3 cancel
A3 trigger
Time
TelecomPedia.Net

2 main types: Xn and N2/NGAP HO

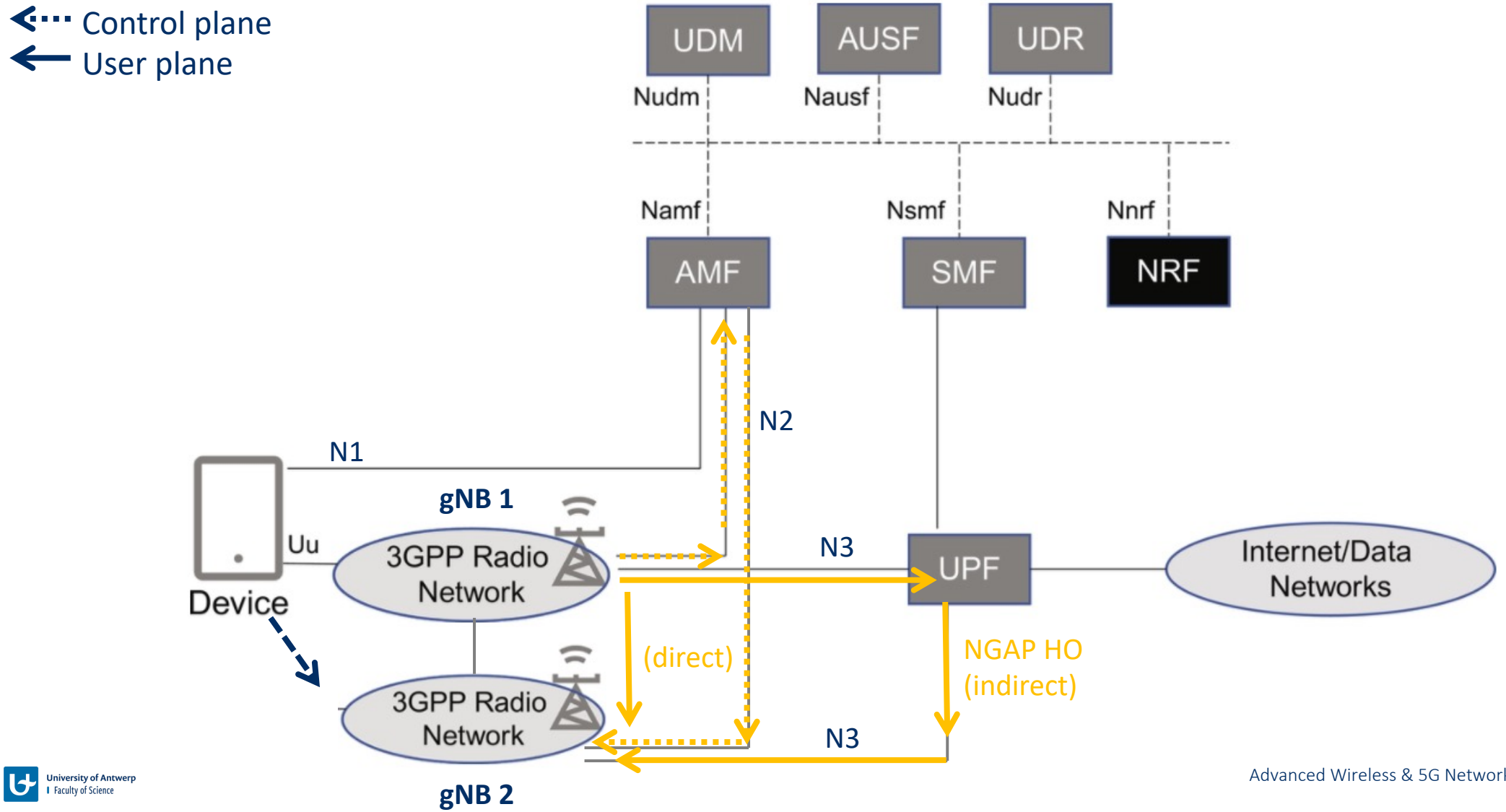
Control plane
User plane



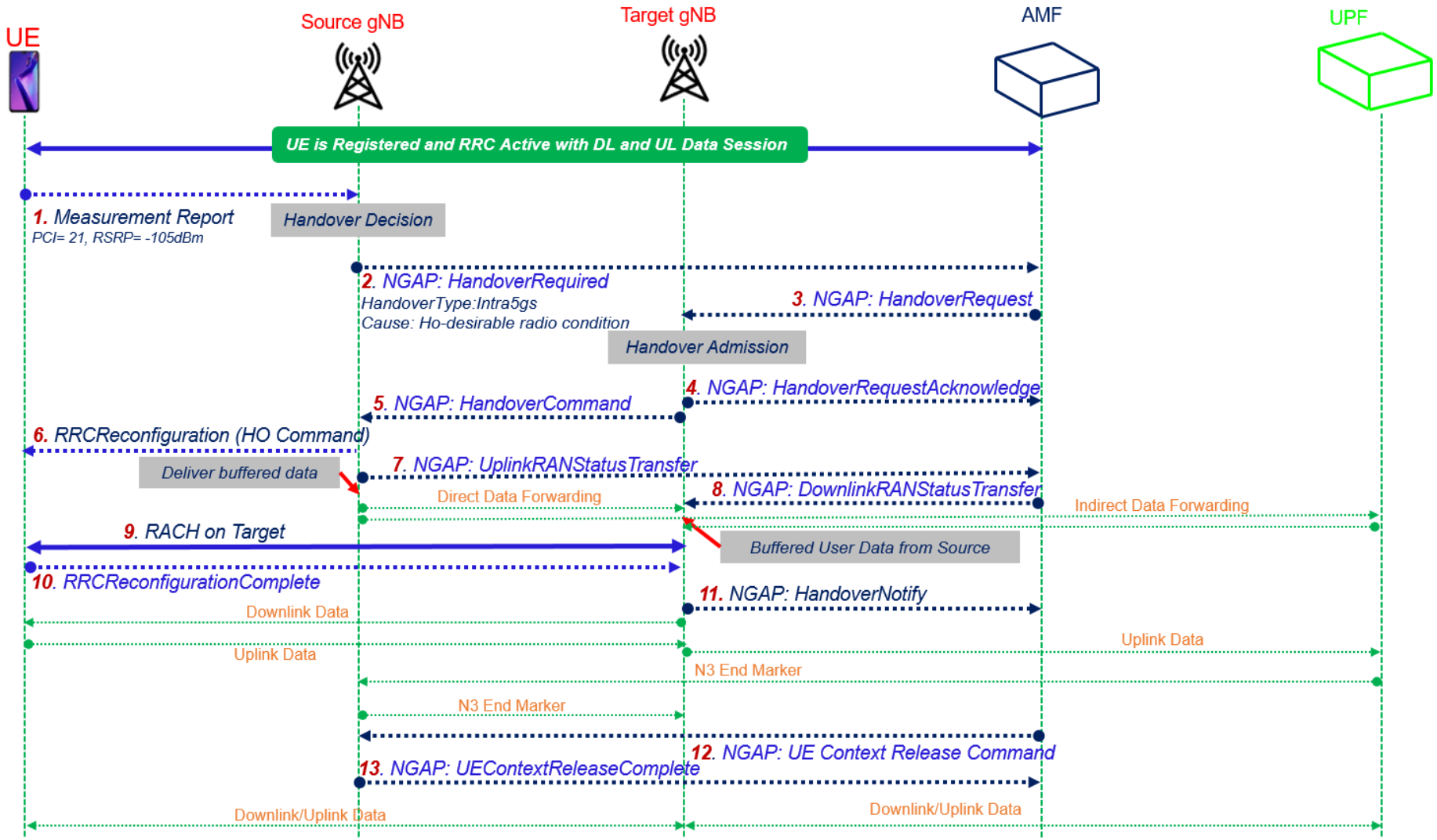
Xn Handover


UE
Source gNB
Target gNB
AMF
UPF
0. XnAP: XnSetupRequest
0. XnAP: XnSetupResponse
UE is Registered and RRC Active with DL and UL Data Session
1. Measurement Report
PCI= 21, RSRP= -105dBm
Handover Decision
2. XnAP: HandoverRequest
Handover Admission
3. XnAP: HandoverRequestAcknowledge
4. RRCReconfiguration (HO Command)
Deliver buffered data
5. XnAP: SNStatusTransfer
Downlink Data Forwarding
Buffered User Data from Source
6. RACH on Target
7. RRCReconfigurationComplete
Uplink Data
Uplink Data
8. NGAP: PathSwitchRequest
End Marker
End Marker
9. NGAP: PathSwitchRequestAcknowledge
Downlink Data
10. XnAP: UEContextRelease
Downlink/Uplink Data
Downlink/Uplink Data

2 main types: Xn and N2/NGAP HO



N2 or NGAP Handover

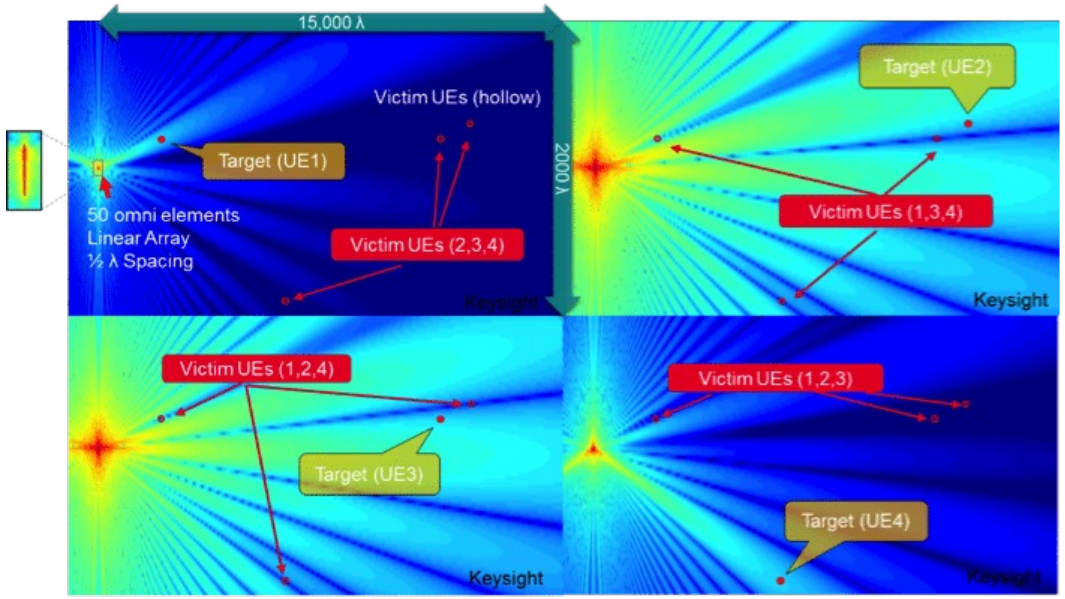


What are the steps?

1. ~~Switch on the mobile (& infrastructure)~~
2. ~~Select a frequency band to receive & send~~
3. ~~Pick a way to send and receive digital bits~~
4. ~~Define how we are going to organize the bits for multiple users~~
5. ~~Listen to synchronize and get system information~~
6. ~~Random Access~~
7. ~~Get a channel~~
8. ~~Authenticate~~
9. ~~Ask to send data (or get some data)~~
10. ~~Ask to make a call~~
11. ~~Move around~~
12. ~~… (location update, release call, handover, etc …)~~

Next

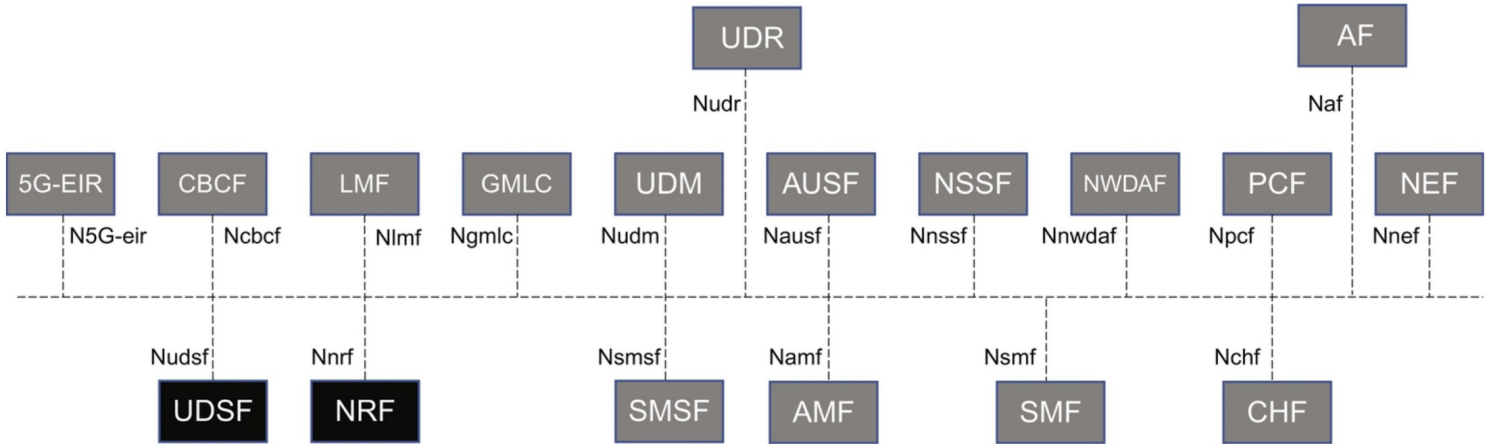
- **So what about cloud?**
  - architectural principles
  - REST interfaces
- **This was all for 5G SA, what about NSA**
  - dual connectivity (DC)
- **5G has a lot of fancier ways to send bits (for the AMA session)**
  - MIMO
  - beamforming
  - …
- **5G Slicing (for the AMA session)**
  - Edge Compute/AI



5G and the “cloud”?

- **Virtualization:** migrate application-specific blades to virtualized resources such as virtual machines (VMs) and later containers. ETSI NFV (Network Function Virtualisation) and OPNFV was created to facilitate and drive virtualization of the telecoms networks by harmonizing the approach across operators.
- **Cloud native:** Infrastructure agnostic + Software decomposition + LCM + Resiliency + State-optimized design + Orchestration.
- **Containers:** System-level virtualization allows multiple instances of OS on a single server on top of a hypervisor. Containers on the other hand are isolated from each other and share OS kernels among all containers.
- **Microservices:** where rather than be developed in a monolithic fashion, software is composed of small independent services that communicate over well-defined APIs. Microservice instances have a much smaller scope of functionality and therefore changes can be developed more quickly. They can be added/removed on demand to increase/decrease the scalability of their functions and can have independent software upgrade cycles.
- **Automation:** automation within Release 15 and Release 16 refer mainly to Self-Organising Networks (SON), which provide Self-Configuration, Self-Optimisation and Self-Healing. These three concepts hold the promise of greater reliability for end-users and less downtime.

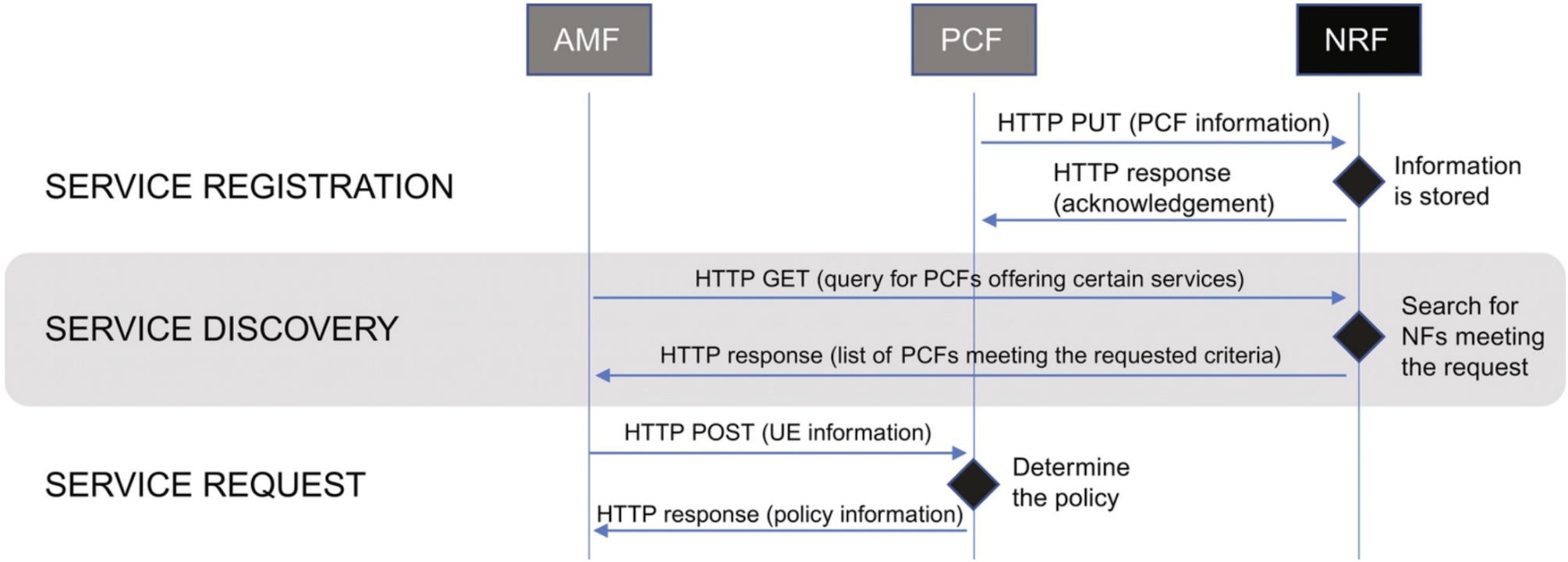
Service-based architecture & REST



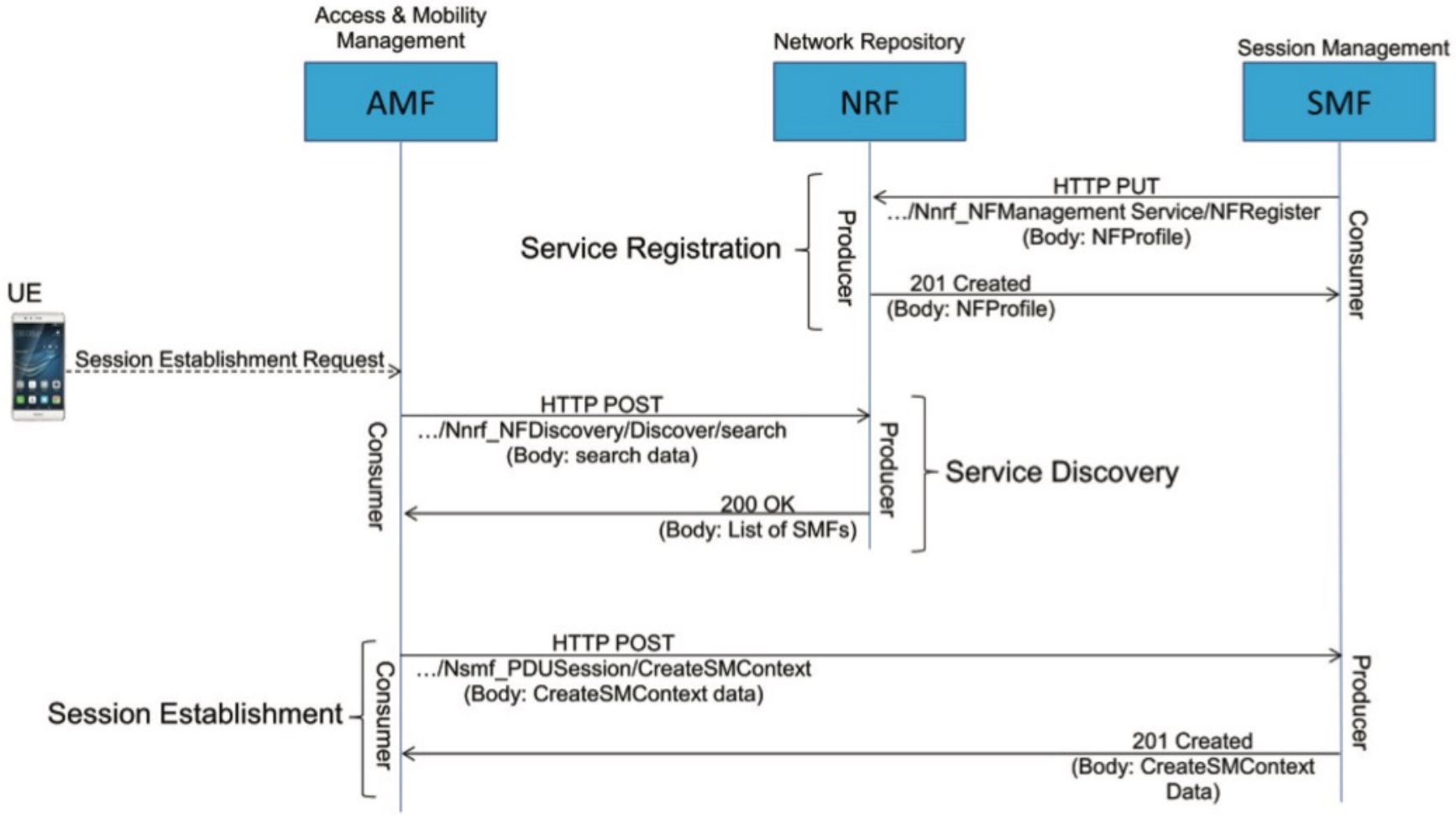
“Representational State Transfer” – HTTP2 REST

- All communication must include the full set of information needed for a specific processing action. It must not rely on previous messages, and hence it can be considered as stateless.
- **GET**—this is used to fetch data from a server. It shall not change any
- **POST**—this is used to send data to a server.
- **PUT**—this is also used to send data to a server, but it replaces existing data.
- **DELETE**—this is used to remove data from a server.

REST Flow example

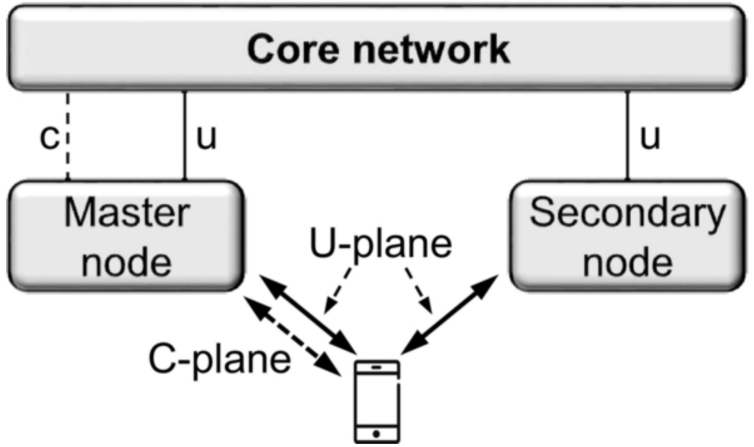


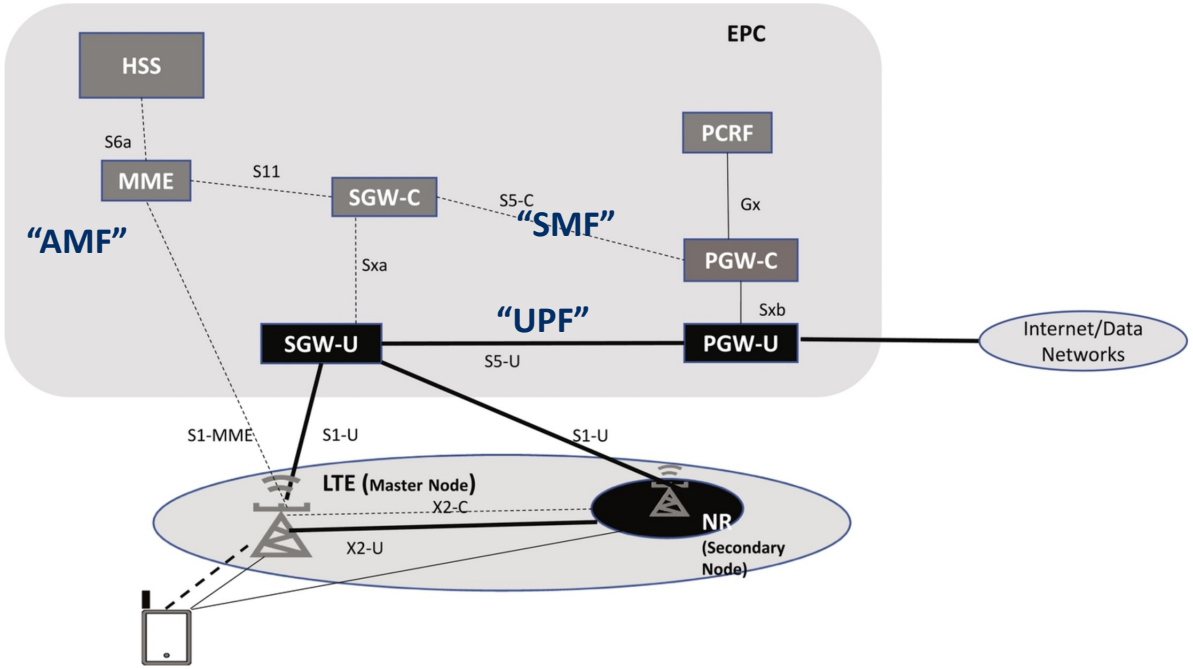
REST Flow example (2)



NSA (non-stand alone)

- Basic principle: **dual connectivity** (DC) = connect to 4G (LTE), and add 5G base stations for capacity.
- Control is purely through 4G, just uses new NR in the RAN.
- EN-DC: “E-UTRAN-NR Dual Connectivity”.





4. Wi-Fi, the 802.11 family

(from licensed to unlicensed)

Characteristics of wireless LANs

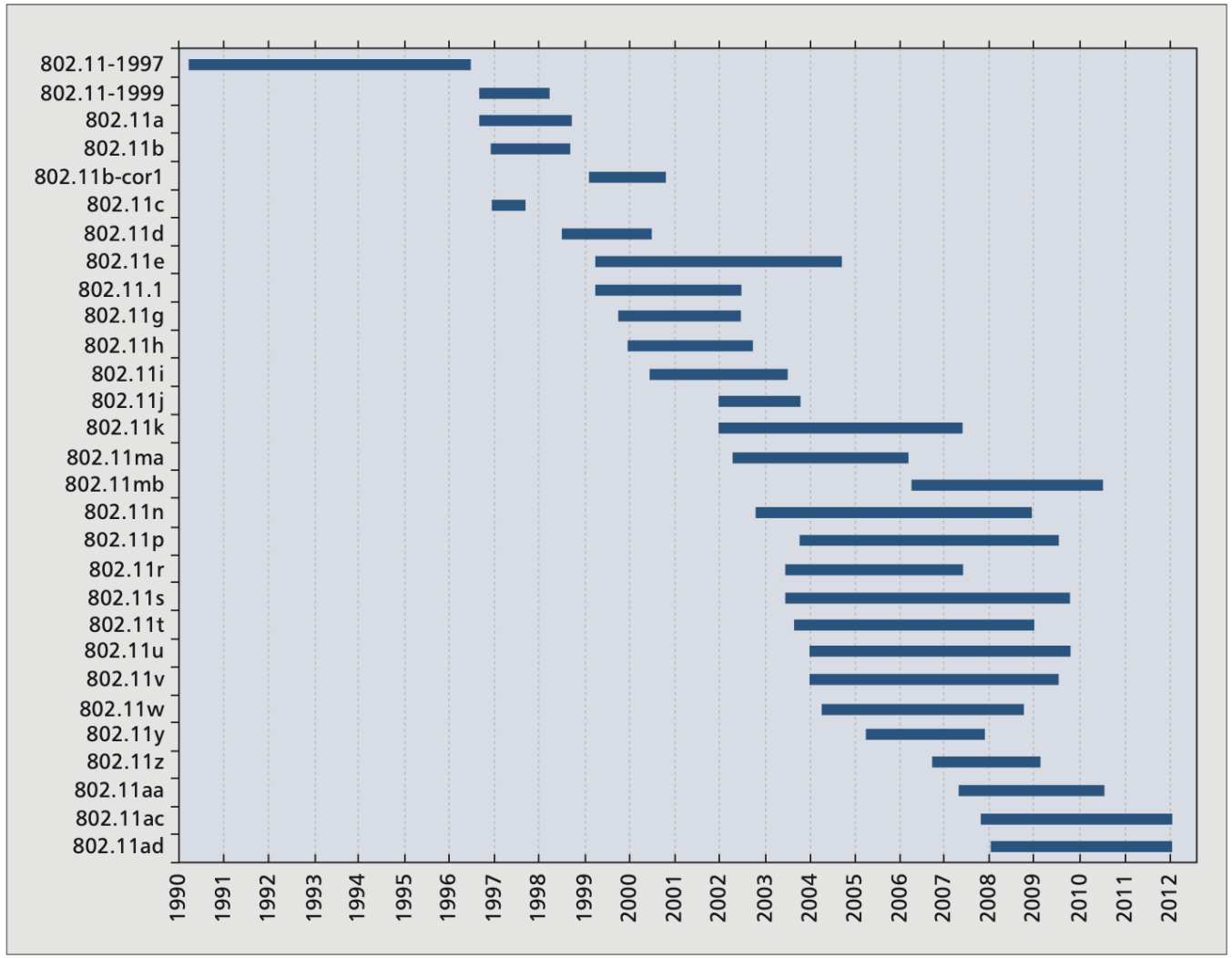
- **Advantages**
  - very flexible within the reception area, senders and receivers can be placed anywhere; radio waves can penetrate walls
  - Ad-hoc networks without previous planning possible (e.g. disaster)
  - (almost) no wiring difficulties (e.g. historic buildings, firewalls)
  - more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...
- **Disadvantages**
  - many proprietary solutions, especially for higher bit-rates, standards take their time
  - products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions

Design goals for wireless LANs

- **global**, seamless operation
- **low power** for battery use
- no special **permissions** or licenses needed to use the LAN (ISM band)
- **robust** transmission technology
- simplified **spontaneous** cooperation at meetings
- easy to use for everyone, **simple** management
- protection of investment in **wired** networks (**interoperability**)
- **security** (no one should be able to read my data), privacy (no one should be able to collect user profiles), **safety** (low radiation)
- **transparency** concerning applications and higher layer protocols, but also location awareness if necessary

G. R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa and B. Walke, "The IEEE 802.11 universe," in *IEEE Communications Magazine*, vol. 48, no. 1, pp. 62-70, January 2010, doi: 10.1109/MCOM.2010.5394032.

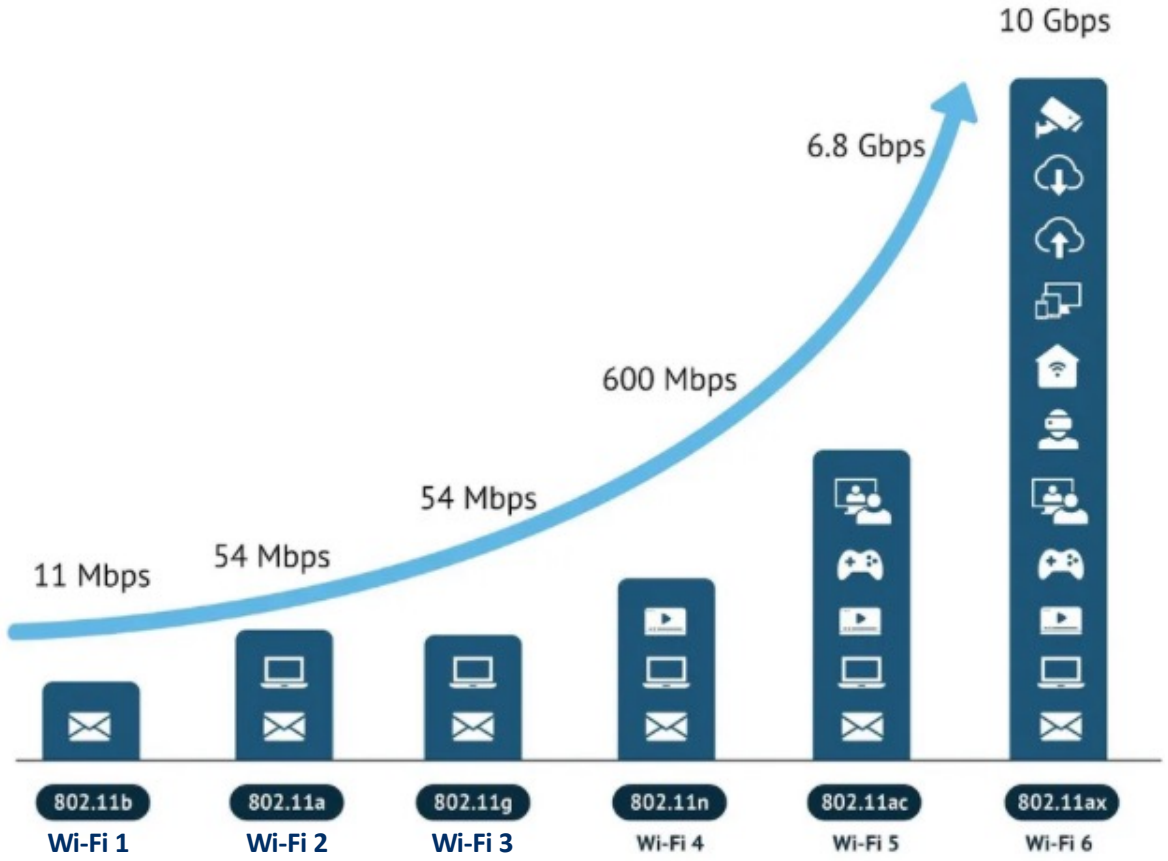
IEEE 802.11 WLAN



IEEE 802.11 vs. Wi-Fi

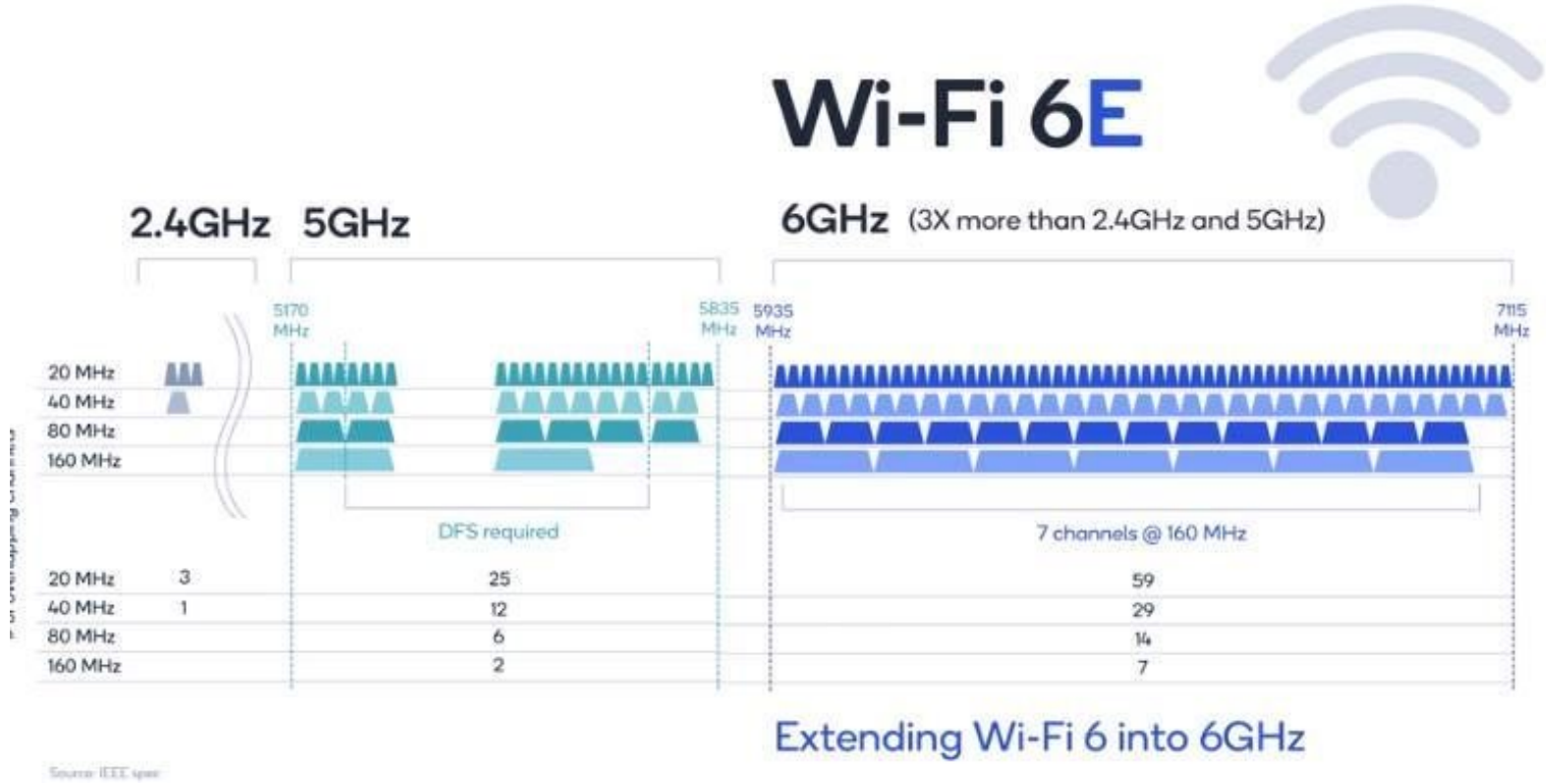
- IEEE 802.11 is a **standard**
- Wi-Fi = “Wireless Fidelity” is a **trademark**
- **Fidelity** = Compatibility between wireless equipment from different manufacturers
- **WiFi Alliance** is a non-profit organization that does the compatibility testing (WiFi.org)
  - And now has also done the new naming (next slide)
- 802.11 has **many options** and it is possible for two equipment based on 802.11 to be **incompatible**.
- All equipment with “Wi-Fi” logo have selected options such that they will interoperate.

Wi-Fi Renamed: 1 to 6E and now 7

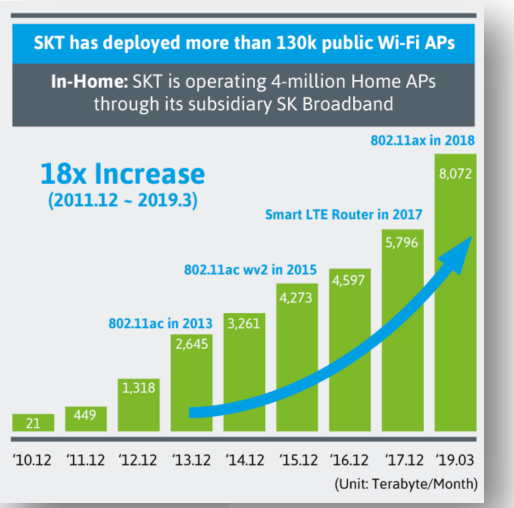


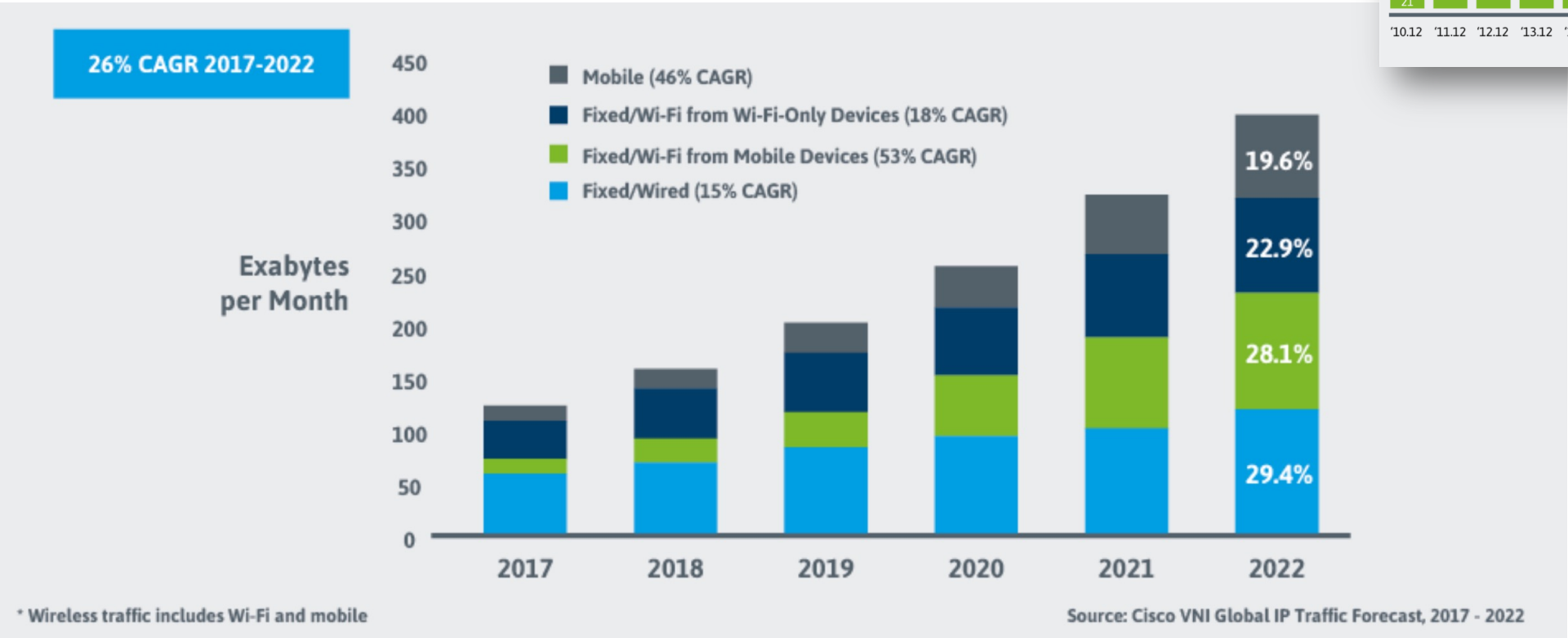
IEEE 802.11 Protocol	Release Date	Frequency Band(s)	Bandwidth	Max Throughput
802.11-1997	1997	2.4	22	2 Mbps
11b	1999	2.4	22	11 Mbps
11a	1999	5	20	54 Mbps
11g	2003	2.4	20	54 Mbps
11n (Wi-Fi 4)	2009	2.4/5	20/40	600 Mbps
11ac (Wi-Fi 5)	2013	5	20/40/80/160	6.8 Gbps
11ax (Wi-Fi 6)	2019	2.5/5	20/40/80/160	9.6 Gbps
11ax (WiFi 6E)	2020	2.5/5/6	20/40/80/160	9.6 Gbps
11be (WiFi 7)	2024 (expected)	2.5/5/6	20/40/80/160/320	46.1 Gbps

WiFi 6E (it’s all about bandwidth)



Licensed and unlicensed





What are the steps?

1. Switch on the mobile (& infrastructure)
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel
8. Authenticate
9. Ask to send data (or get some data)
10. Ask to make a call
11. Move around
12. … (location update, release call, handover, etc …)

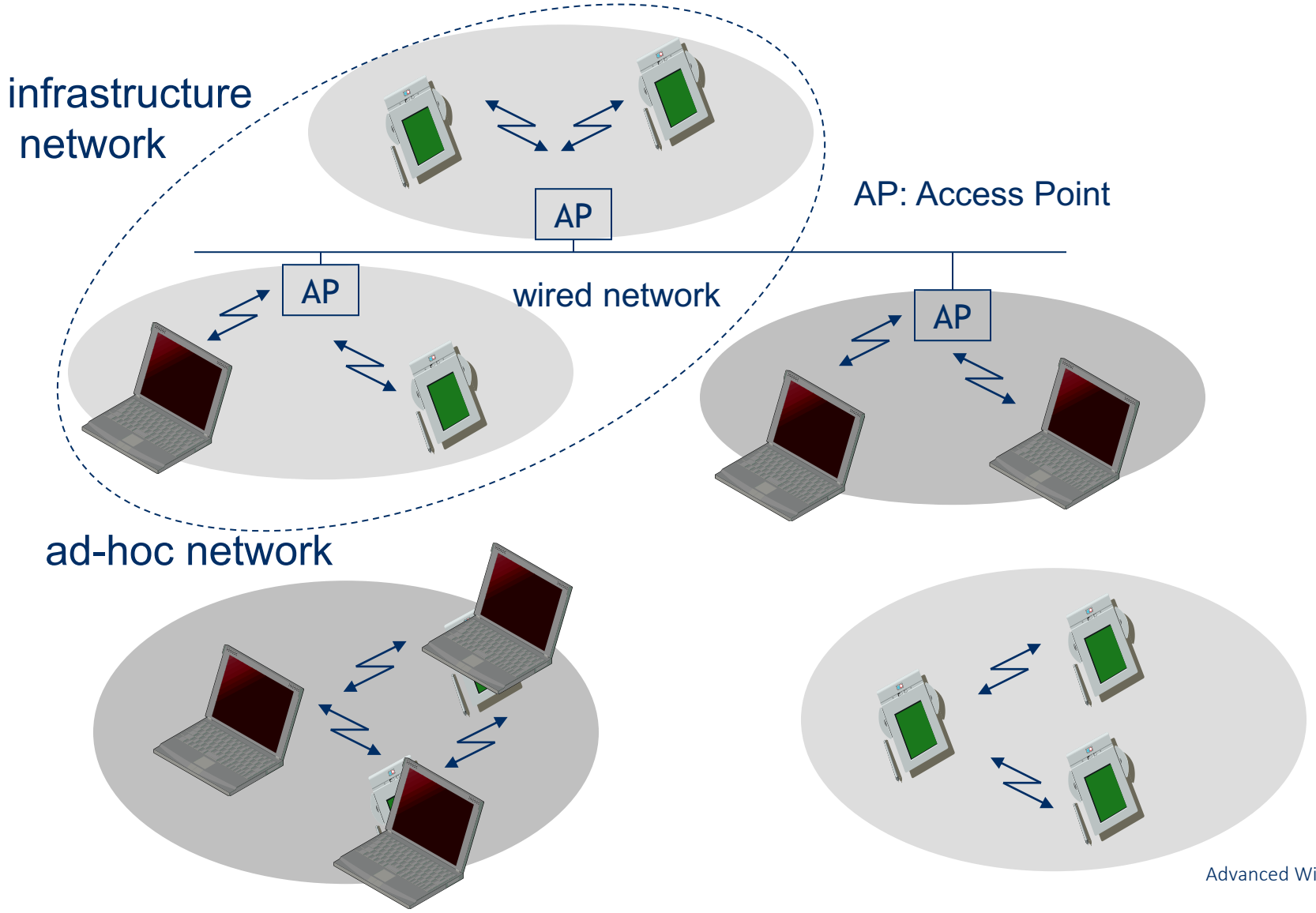
What are the steps?

1. Switch on the mobile (& infrastructure)
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. *Random Access*
7. *Get a channel*
8. *Authenticate*
9. *Ask to send data (or get some data)*
10. ~~Ask to make a call~~
11. Move around
12. ~~… (location update, release call, handover, etc …)~~

What are the steps?

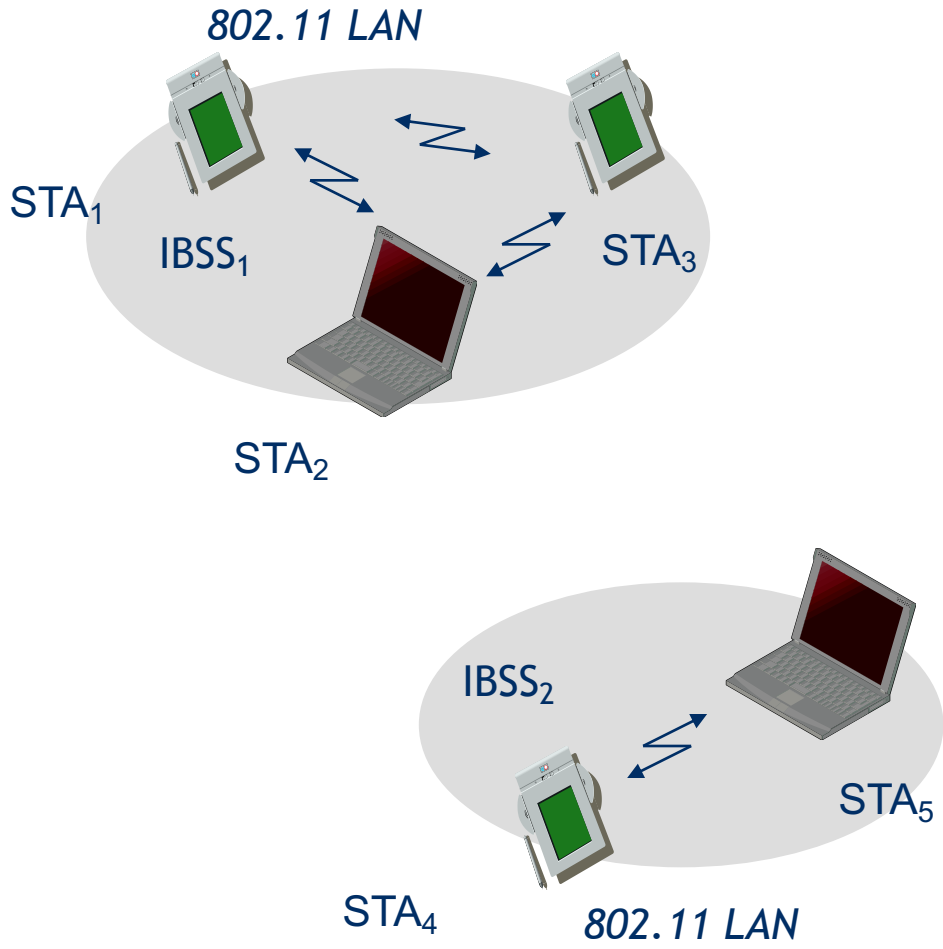
1. Switch on the stations (& access points)
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel (well, not exactly…)
8. Authenticate (uh, does this happen earlier?)
9. Try to send data
10. Move around

WLAN Architecture: Infrastructure vs. ad-hoc networks



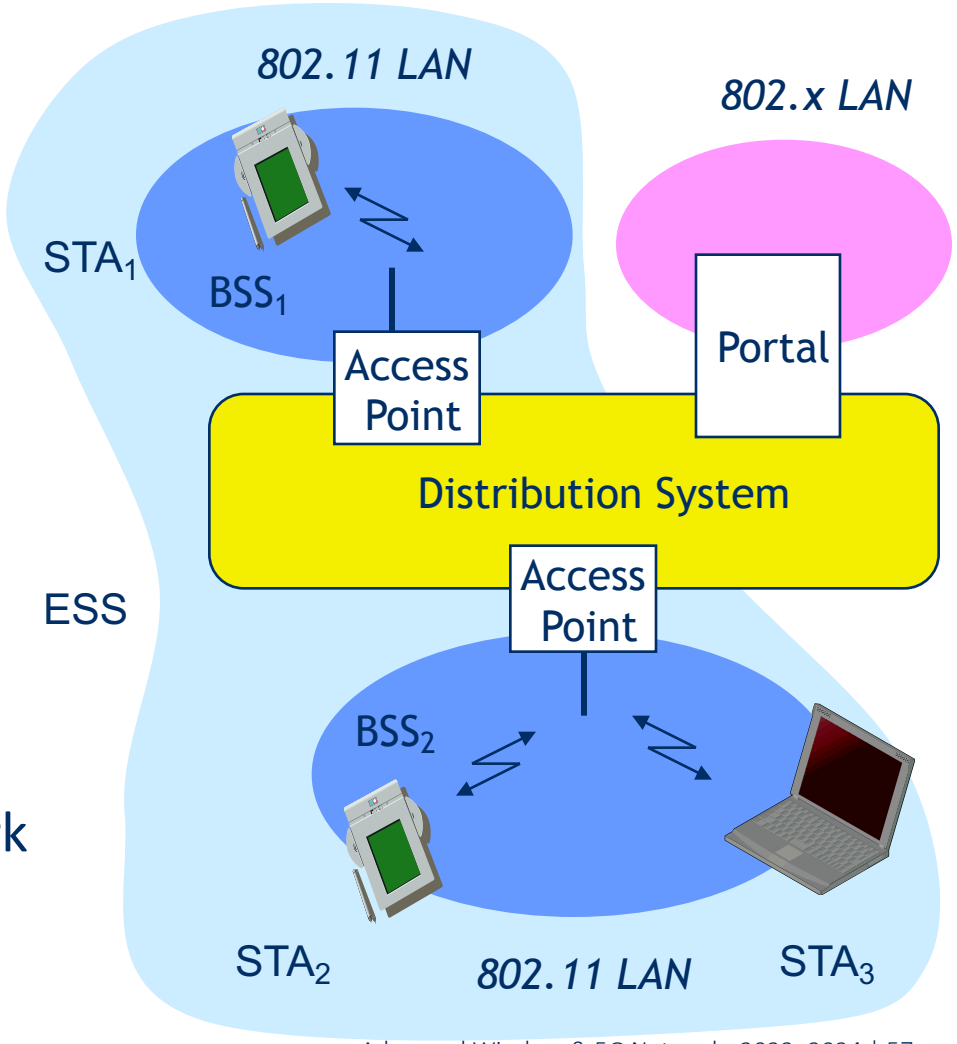
IEEE 802.11 - Architecture of an ad-hoc network

- **Direct communication within a limited range**
  - Station (STA):
    terminal with access mechanisms to the wireless medium
  - Independent Basic Service Set (IBSS):
    group of stations using the same radio frequency



IEEE 802.11 - Architecture of an Infrastructure Network

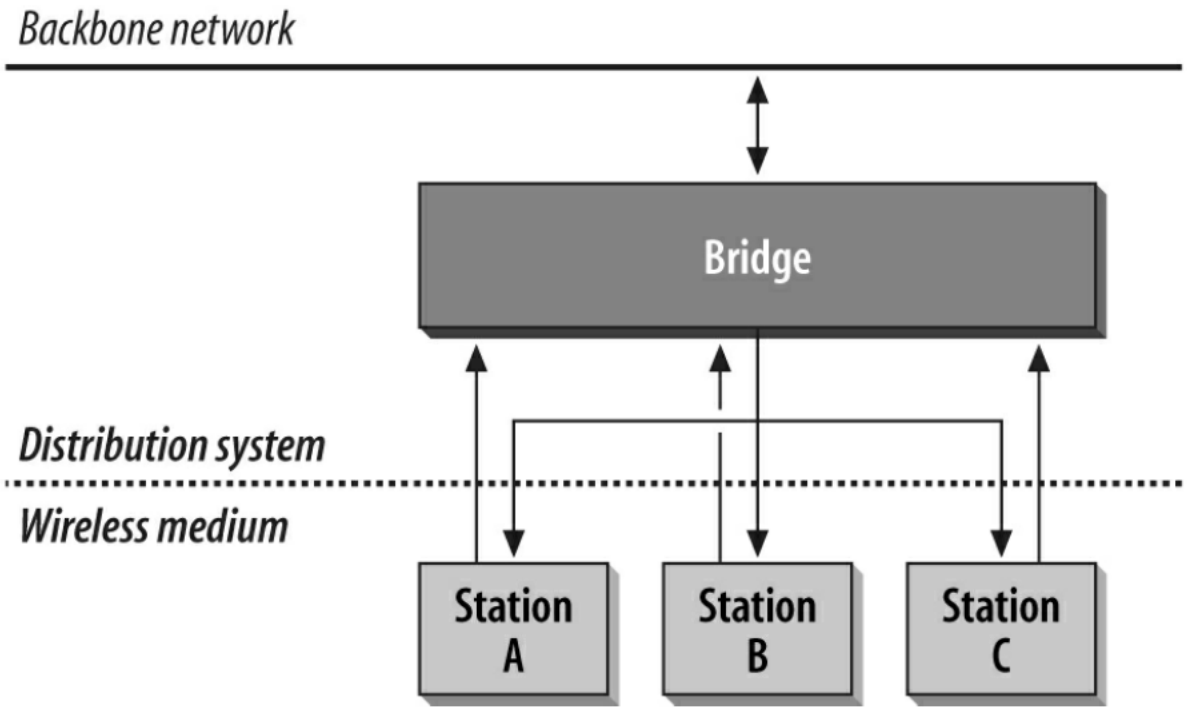
- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Basic Service Set (BSS)**
  - group of stations using the same radio frequency
- **Access Point**
  - station integrated into the wireless LAN and the distribution system
- **Portal**
  - bridge to other (wired) networks
- **Distribution System**
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS



ESS

Needed in a distribution system is a method to manage associations. A wireless station is associated with only one access point at a time. If a station is associated with one access point, all the other access points in the ESS need to learn about that station. To fully implement the distribution system, access points must inform other access points of associated stations. Access points on the market use **an interaccess point protocol (IAPP)** over the backbone medium. This is mostly proprietrary.

There is no standardized “core”, nor robust mobility, handovers or session management



What are the steps?

1. ~~Switch on the stations (& access points)~~
2. Select a frequency band to receive & send
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel (well, not exactly…)
8. Authenticate (uh, does this happen earlier?)
9. Try to send data
10. Move around

Spectrum allocation

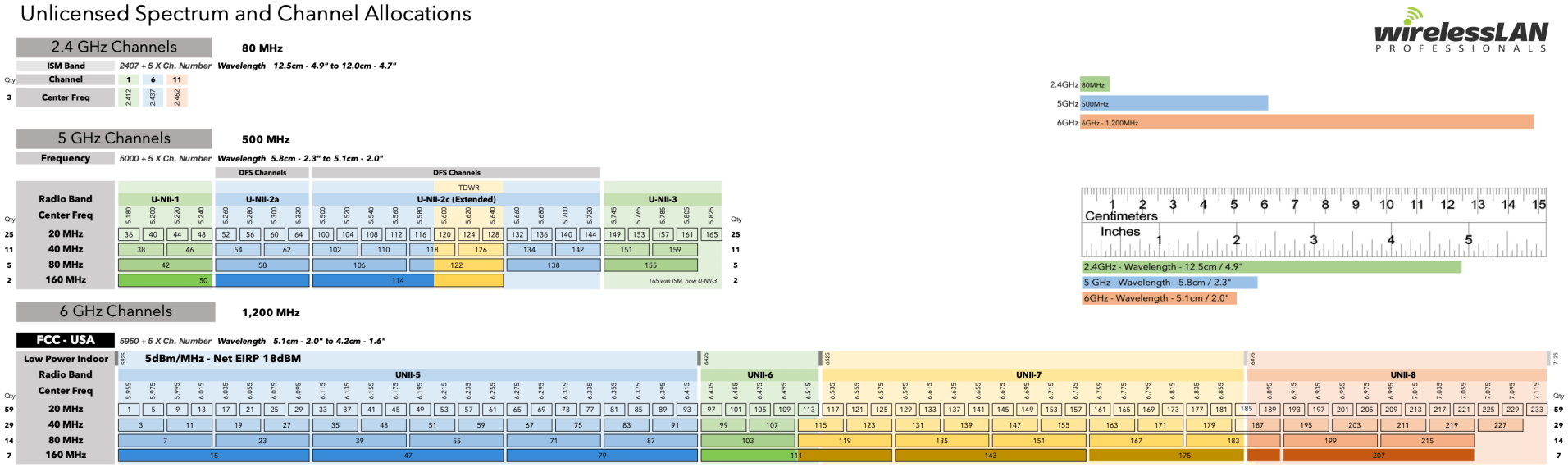
Model	Description	Deployment	Technologies
Licensed access	Exclusive assignment of frequency band	Single mobile operator	Traditional cellular networks (e.g. GSM, UMTS, LTE, 5G)
Unlicensed shared access	License-free operation according to regional regulation	Many providers	Uncoordinated operation of many technologies: ***short range*** (IEEE802.11, IEEE802.15.4, Bluetooth, MulteFire...), ***long range*** (LoRa, SigFox, Dash, IEEE802.11ah...)
Licensed assisted access (LAA)	Use of unlicensed band(s) in addition to licensed band to boost performance	Mobile operator + unlicensed network providers	Coexistence of cellular + unlicensed technologies (e.g. LTE-LAA)
Sharing in application-specific bands	Frequency band assigned to specific applications	Multiple providers	DSRC 5.9 GHz for ITS: IEEE802.11p + LTE V2X
Licensed Spectrum Sharing	Frequency band assigned to multiple providers based on sharing rules (location, spectrum)	Authorized provider (micro-operators) + mobile operators	Private LTE/5G networks (e.g. CBRS) Directive from FCC (US) : SAS Directive from RSC (EC) : LSA

Wifi Spectrum – ISM bands

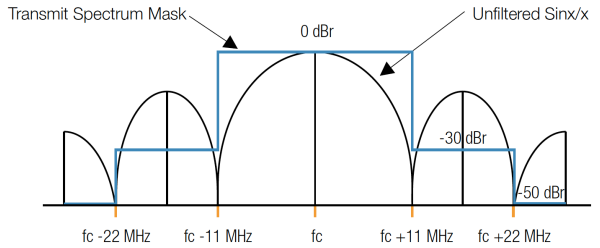
Industrial
Scientific
Medical

Always TDD/TDM
(i.e. one frequency)

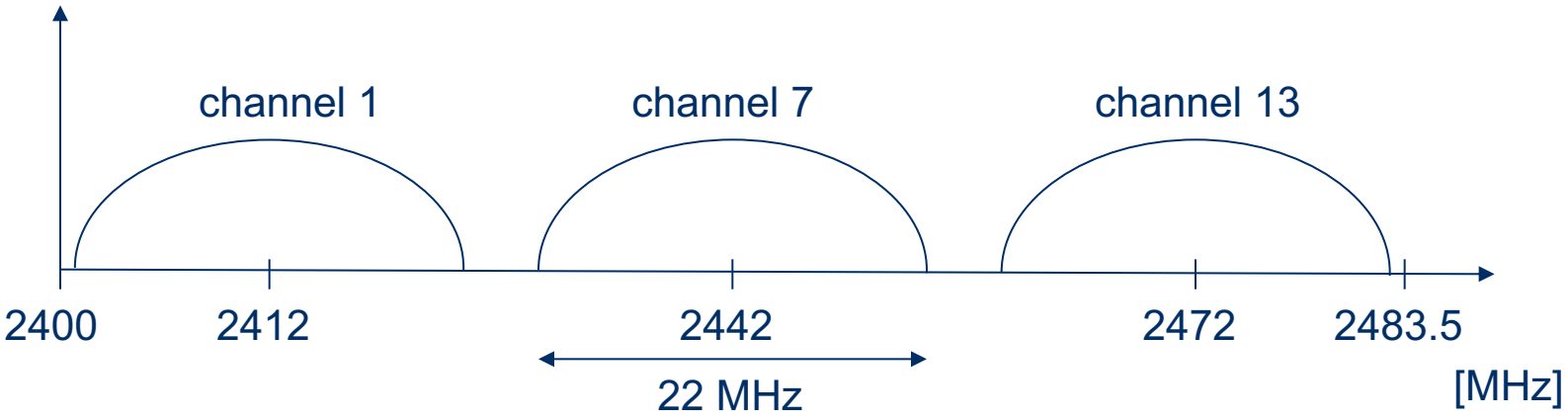
(well, until recently)



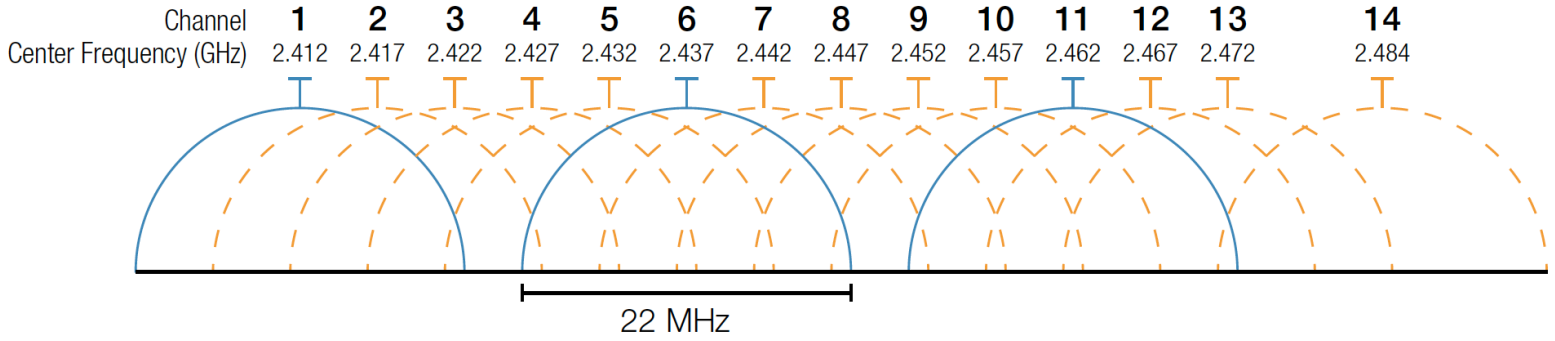
2.4 GHz Channels



Europe (ETSI)

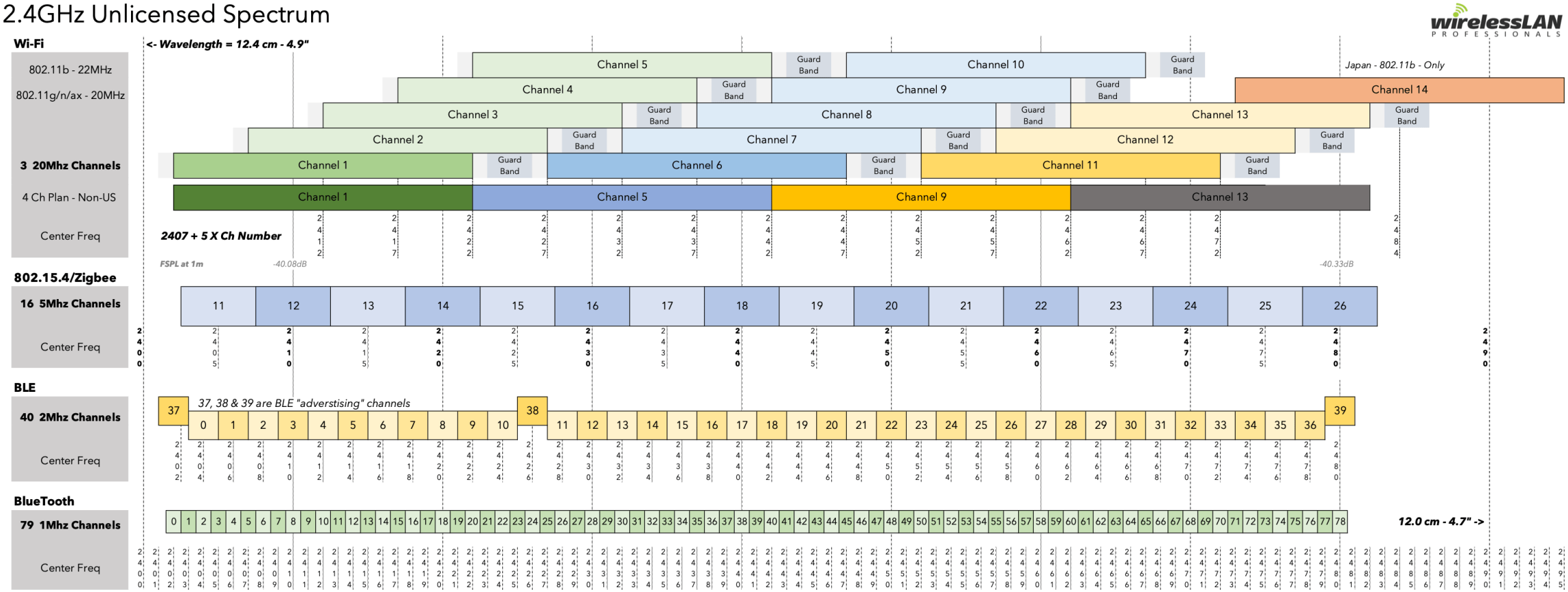


US (FCC)/Canada (IC)

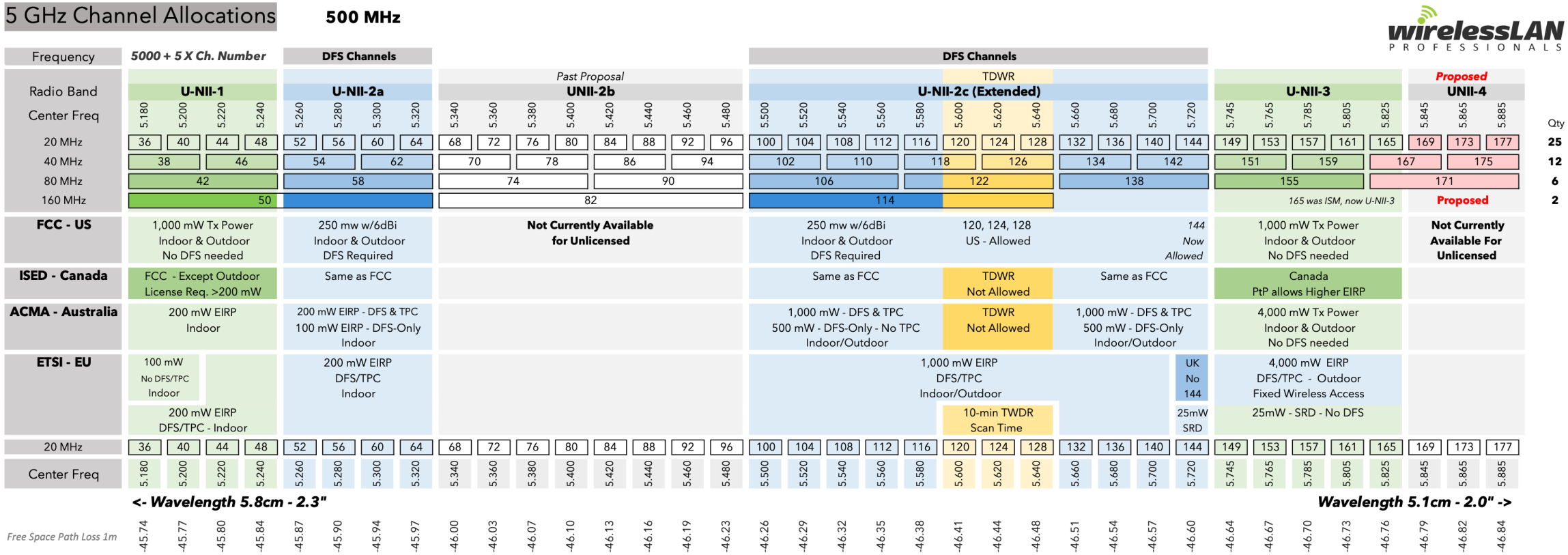


2.4 GHz

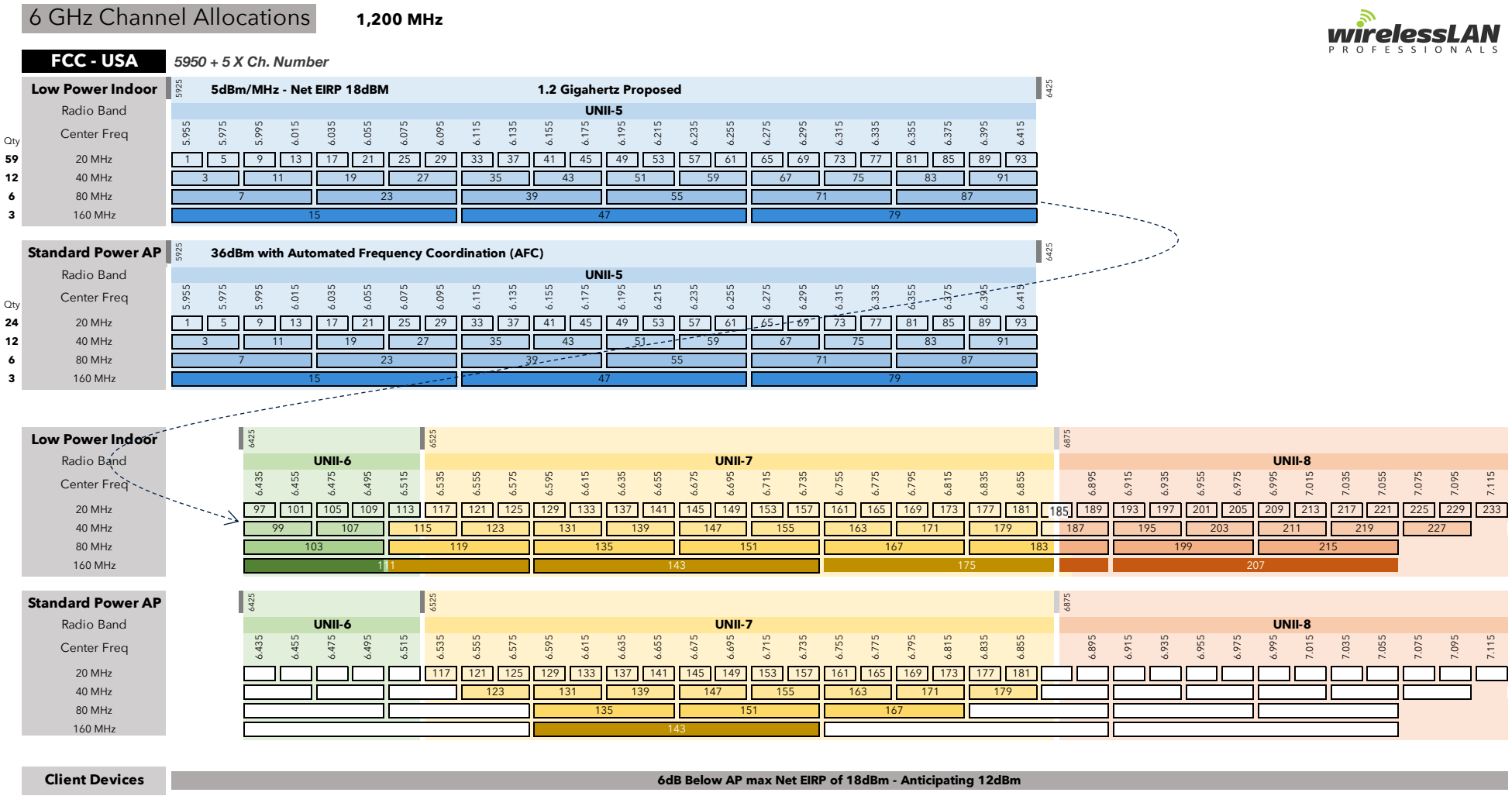
2.4GHz Unlicensed Spectrum



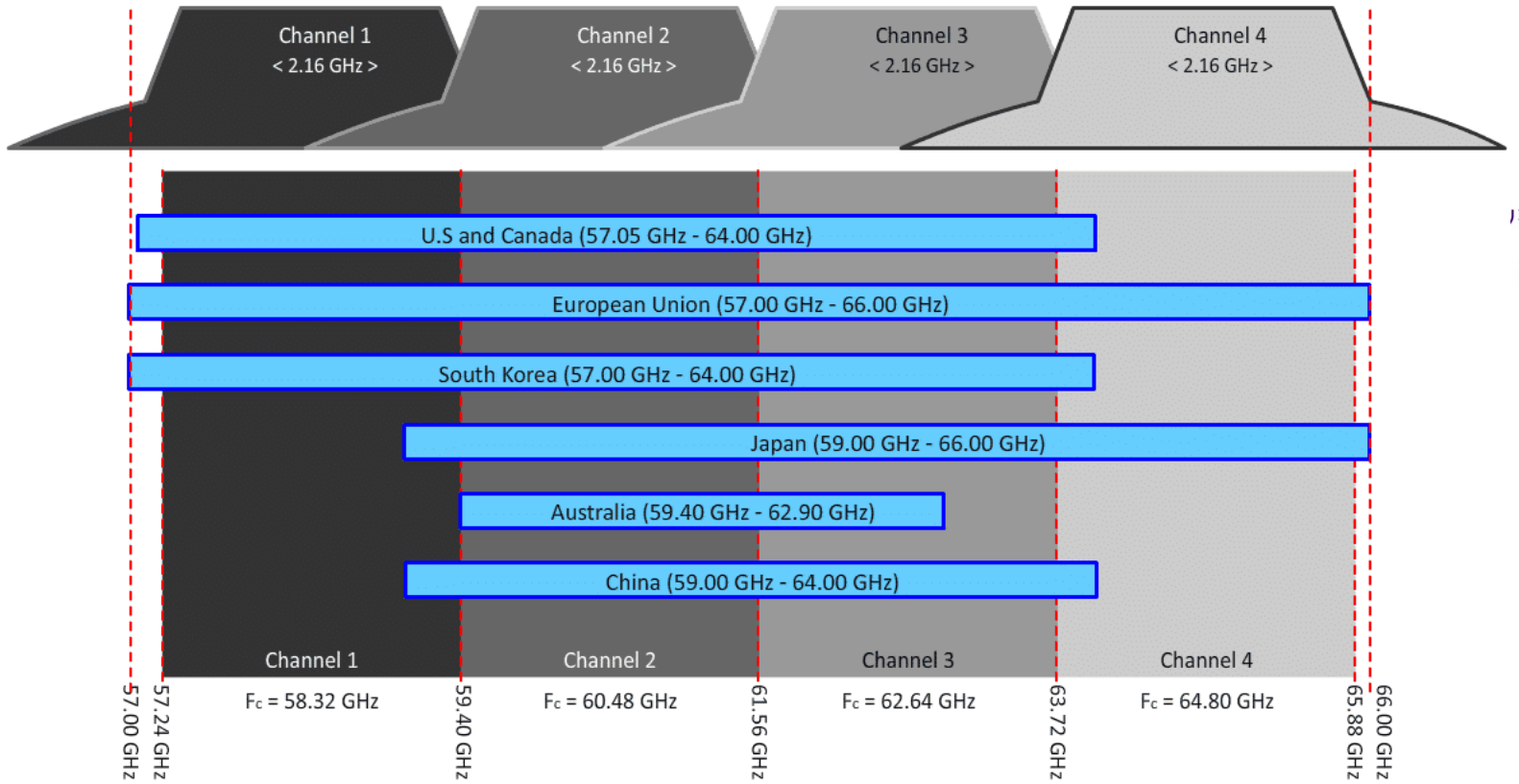
5 GHz


5 GHz Channel Allocations
500 MHz
wirelessLAN PROFESSIONALS
Frequency
5000 + 5 X Ch. Number
DFS Channels
DFS Channels
Past Proposal
TDWR
Proposed
Radio Band
U-NII-1
U-NII-2a
UNII-2b
U-NII-2c (Extended)
U-NII-3
UNII-4
Center Freq
Qty
20 MHz
40 MHz
80 MHz
160 MHz
FCC - US
1,000 mW Tx Power Indoor & Outdoor No DFS needed
250 mw w/6dBi Indoor & Outdoor DFS Required
Not Currently Available for Unlicensed
250 mw w/6dBi Indoor & Outdoor DFS Required
120, 124, 128 US - Allowed
144 Now Allowed
1,000 mW Tx Power Indoor & Outdoor No DFS needed
Not Currently Available For Unlicensed
ISED - Canada
FCC - Except Outdoor License Req. >200 mW
Same as FCC
Same as FCC
TDWR Not Allowed
Same as FCC
Canada PtP allows Higher EIRP
ACMA - Australia
200 mW EIRP Indoor
200 mW EIRP - DFS & TPC 100 mW EIRP - DFS-Only Indoor
1,000 mW - DFS & TPC 500 mW - DFS-Only - No TPC Indoor/Outdoor
TDWR Not Allowed
1,000 mW - DFS & TPC 500 mW - DFS-Only Indoor/Outdoor
4,000 mW Tx Power Indoor & Outdoor No DFS needed
ETSI - EU
100 mW No DFS/TPC Indoor
200 mW EIRP DFS/TPC - Indoor
200 mW EIRP DFS/TPC Indoor
1,000 mW EIRP DFS/TPC Indoor/Outdoor
10-min TWDR Scan Time
UK No 144
25mW SRD
4,000 mW EIRP DFS/TPC - Outdoor Fixed Wireless Access
25mW - SRD - No DFS
<- Wavelength 5.8cm - 2.3"
Wavelength 5.1cm - 2.0" ->
Free Space Path Loss 1m

6 GHz

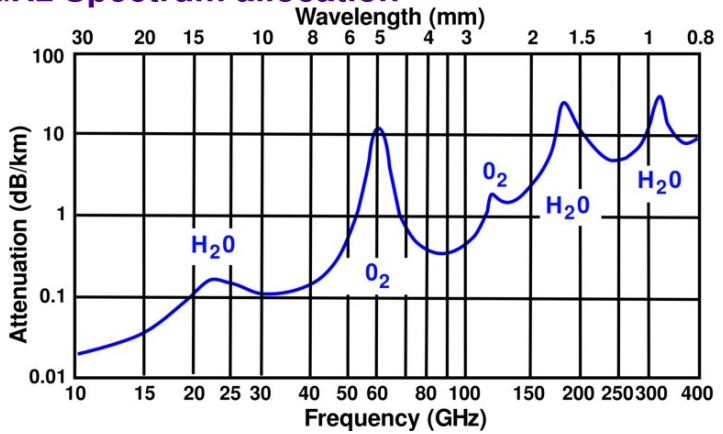

6 GHz Channel Allocations
1,200 MHz
wirelessLAN PROFESSIONALS
FCC - USA
5950 + 5 X Ch. Number
Low Power Indoor
5dBm/MHz - Net EIRP 18dBM
1.2 Gigahertz Proposed
Radio Band
UNII-5
Center Freq
Qty
59 20 MHz 1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69 73 77 81 85 89 93
12 40 MHz 3 11 19 27 35 43 51 59 67 75 83 91
6 80 MHz 7 23 39 55 71 87
3 160 MHz 15 47 79
Standard Power AP
36dBm with Automated Frequency Coordination (AFC)
24 20 MHz 1 5 9 13 17 21 25 29 33 37 41 45 49 53 57 61 65 69 73 77 81 85 89 93
12 40 MHz 3 11 19 27 35 43 51 59 67 75 83 91
6 80 MHz 7 23 39 55 71 87
3 160 MHz 15 47 79
Low Power Indoor
UNII-6
UNII-7
UNII-8
20 MHz 97 101 105 109 113 117 121 125 129 133 137 141 145 149 153 157 161 165 169 173 177 181 185 189 193 197 201 205 209 213 217 221 225 229 233
40 MHz 99 107 115 123 131 139 147 155 163 171 179 187 195 203 211 219 227
80 MHz 103 119 135 151 167 183 199 215
160 MHz 111 143 175 207
Standard Power AP
20 MHz 117 121 125 129 133 137 141 145 149 153 157 161 165 169 173 177 181
40 MHz 123 131 139 147 155 163 171 179
80 MHz 135 151 167
160 MHz 143
Client Devices
6dB Below AP max Net EIRP of 18dBm - Anticipating 12dBm

60 GHz (for Wi-Gig, 802.11ad)



Tampere University
Tampere University of Applied Sciences

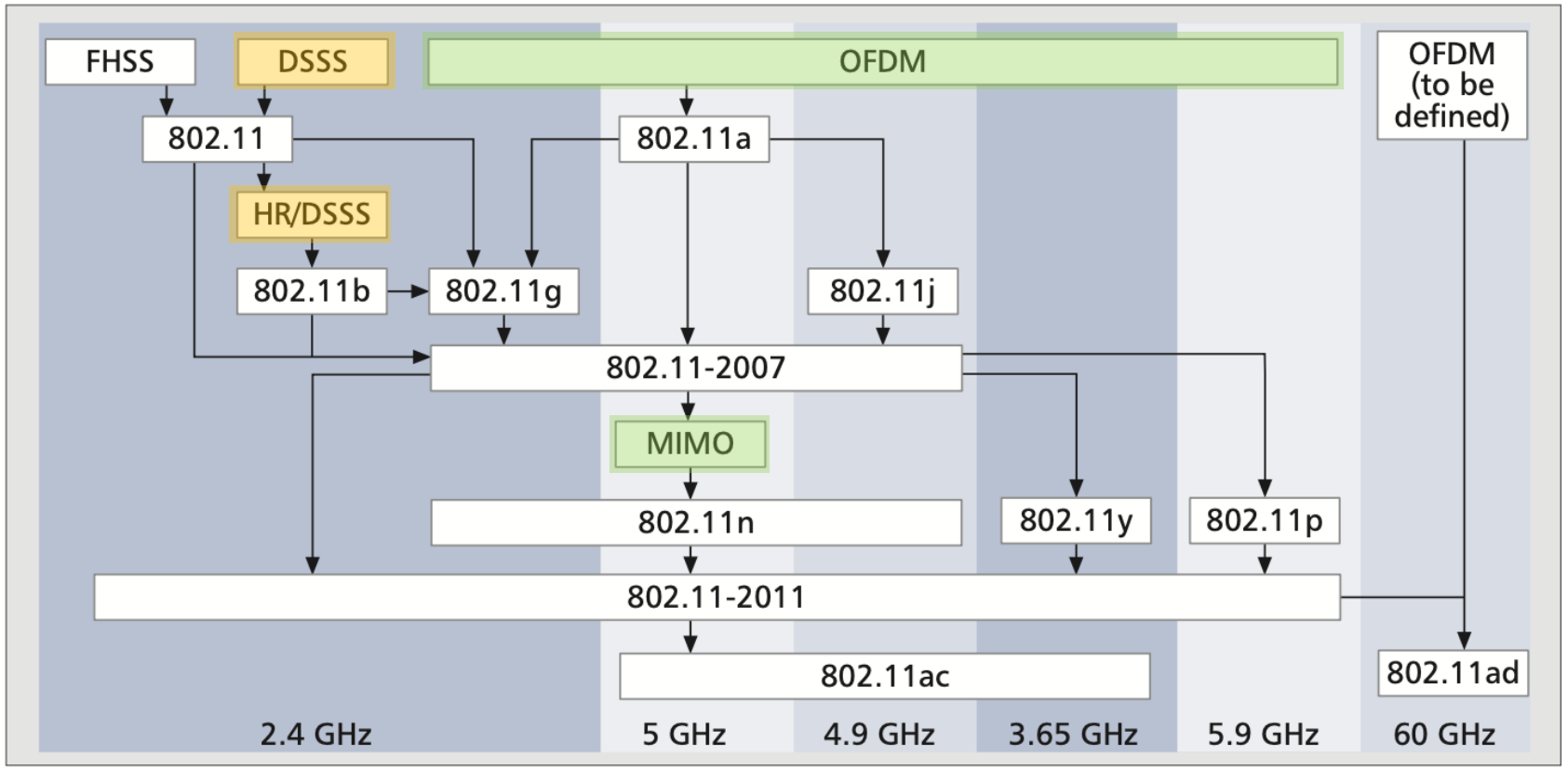
60 GHz Spectrum allocation



What are the steps?

1. ~~Switch on the stations (& access points)~~
2. ~~Select a frequency band to receive & send~~
3. Pick a way to send and receive digital bits
4. Define how we are going to organize the bits for multiple users
5. Listen to synchronize and get system information
6. Random Access
7. Get a channel (well, not exactly…)
8. Authenticate (uh, does this happen earlier?)
9. Try to send data
10. Move around

Only 2 ways that are really different.



FHSS: Frequency Hopping Spread Spectrum
DSSS: Direct Sequence Spread Spectrum
HR: High Rate
OFDM: Orthogonal Frequency Division Multiplexing
MIMO: Multiple Input/Multiple Output

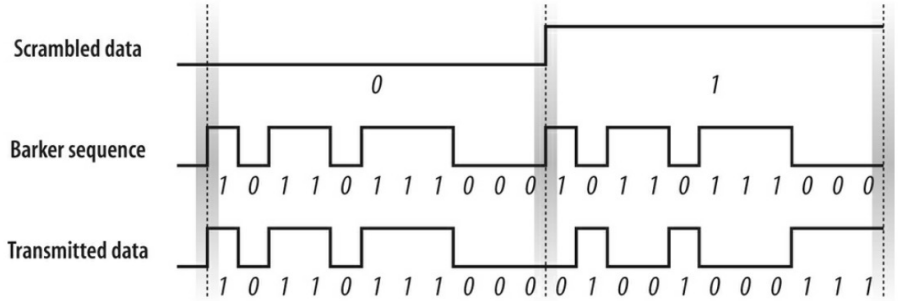
Today, grouped in IEEE 802.11-2016
MIMO = multiple-input, multiple-output = capacity increasing, on top of OFDM (last session)

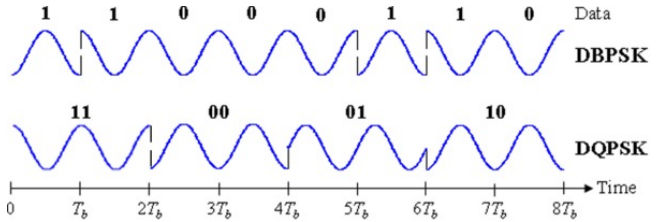
Legacy IEEE 802.11 - Physical layer

- **3 versions: 2 radio (typical 2.4 GHz), 1 IR: data rates 1 or 2 Mbit/s**
- **FHSS (Frequency Hopping Spread Spectrum) – Google Hedy Lamarr**
  - spreading, de-spreading, signal strength, typical 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- **DSSS (Direct Sequence Spread Spectrum)**
  - DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- **Infrared**
  - 850-950 nm, diffuse light, typical 10 m range
  - carrier detection, energy detection, synchronization

Direct Sequence Spread Spectrum

- **DSSS**
  - Spreading is achieved by the use of codes
  - Spreading using 11-chip Baker sequence:
    - Symbol rate is 1 MHz resulting in 11 MHz chipping rate
  - Implementation more complex than FHSS
  - Robust against interference and insensitivity to multipath propagation
  - Modulation scheme:
    - 1 Mbit/s: Differential Binary Phase Shift Keying (DBPSK)
    - 2 Mbit/s: Differential Quadrature Phase Shift Keying (DQPSK)

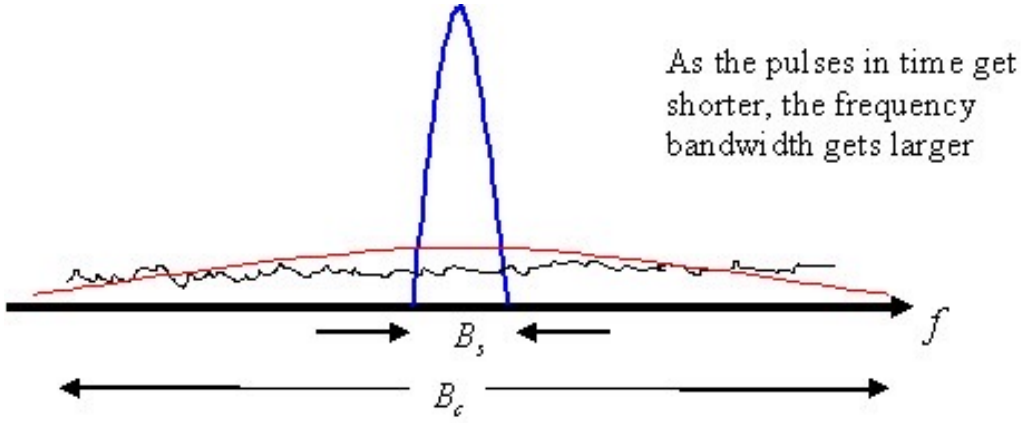


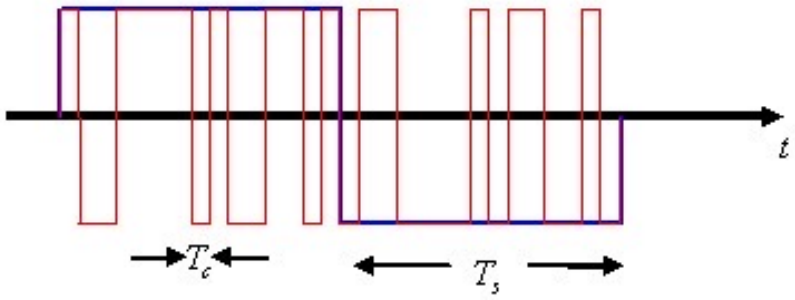


Note: first the chipping, then the BPSK

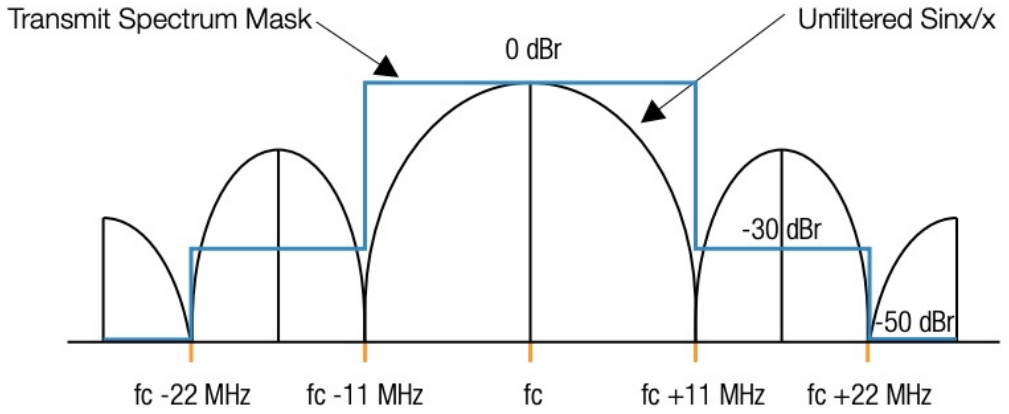
DSSS

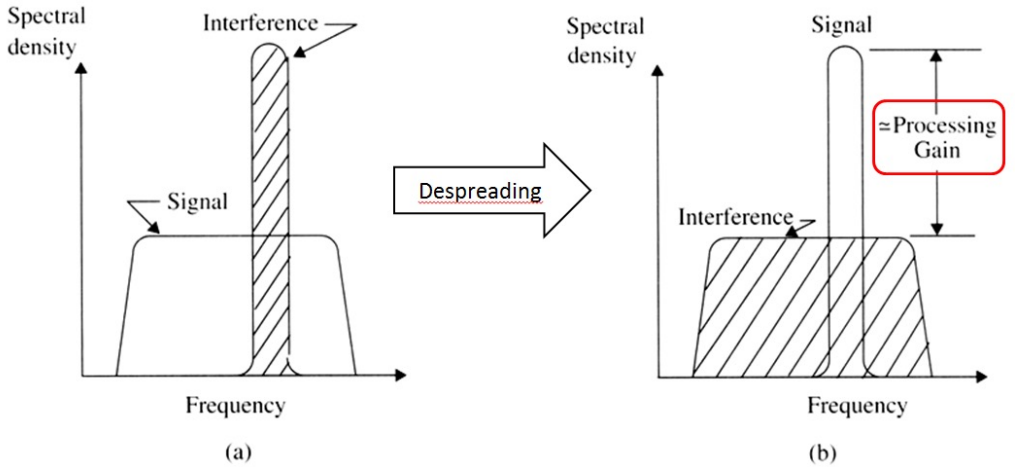
Shorter pulses = wider bandwidth





Needs to fit into mask, so additional filter is needed





Despreading mitigates narrowband noise

IEEE 802.11b: HR-DSSS

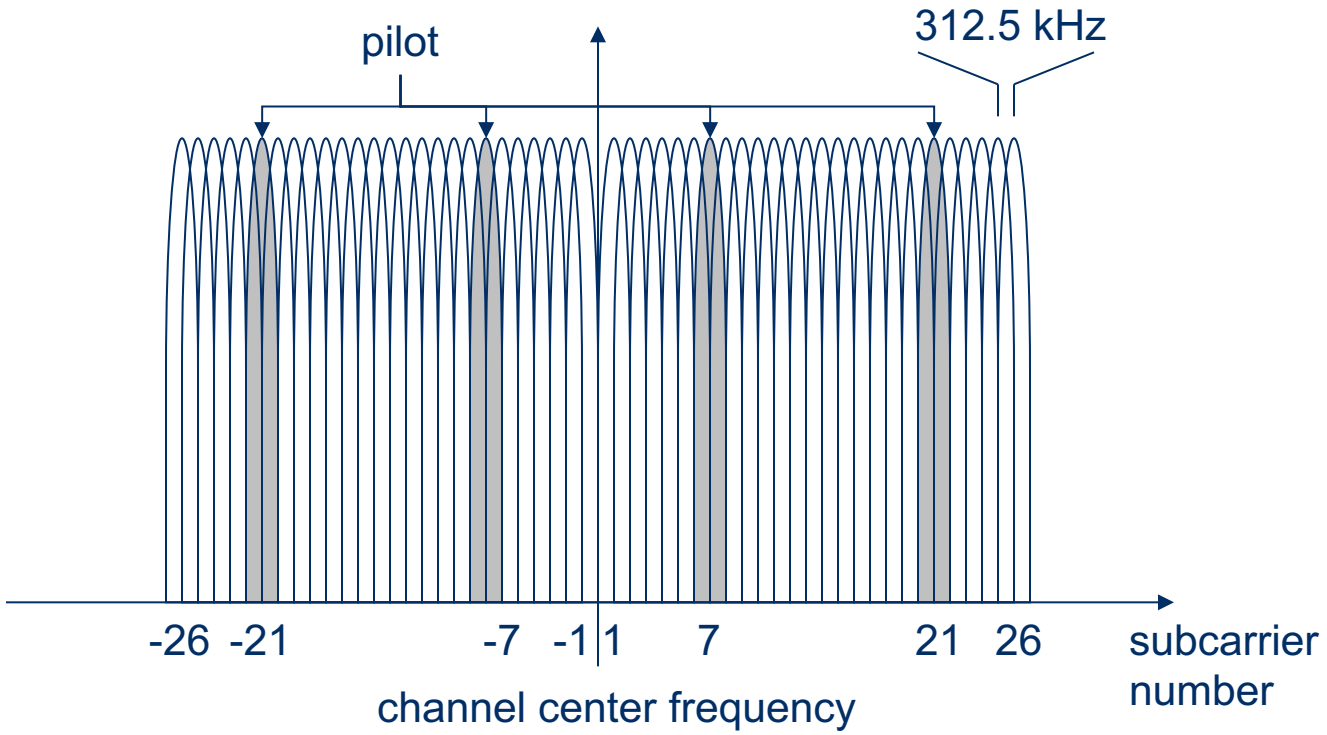
- **Data rate**
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR, User data rate max. 6 Mbit/s
- **DSSS**
  - 1,2 Mbit/s: 11-chip Baker code
  - 5.5, 11 Mbit/s: 8-chip code using Complementary Code Keying (CCK)
    - 4,8 bit symbols at 1.375 Msym/s
  - Still 22 MHz BW
- **Transmission range**
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
  - Free 2.4 GHz ISM-band
- **Security**
  - Limited, WEP Wired Equivalent Protection) insecure
- **Connection set-up time**
  - Connectionless/always on
- **Quality of Service**
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
  - **Slot duration 20µs (!)**
- **Manageability**
  - Limited (no automated key distribution, sym. Encryption)
- **Special Advantages/Disadvantages**
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11a: OFDM at 5GHz

- **Data rate**
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- **Transmission range**
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m
- **Frequency**
  - Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band
- **Security**
  - Limited, WEP insecure
- **Connection set-up time**
  - Connectionless/always on
- **Quality of Service**
  - Typ. best effort, no guarantees (same as all 802.11 products)
- **Manageability**
  - Limited (no automated key distribution, sym. Encryption)
- **Special Advantages/Disadvantages**
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, data rates may drop fast with distance, no QoS

OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers (64 = 2^6 in total)
- 48 data + 4 pilot (plus 12 virtual subcarriers)
- 312.5 kHz spacing = >16.6MHz



IEEE 802.11g: OFDM at 2.4GHz

Extended Rate PHY (ERP): flavors

- **ERP-DSSS** and ERP-CCK These modes are backwards compatible with the original direct sequence specification (1 Mbps and 2 Mbps) as well as the 802.11b enhancements (5.5 Mbps and 11 Mbps)
- **ERP-OFDM** This is the major mode of 802.11g. It is essentially running 802.11a in the ISM frequency band (2.4 GHz), with a few minor changes to provide backwards compatibility. It supports the same speeds as 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Speeds of 6, 12, and 24 Mbps are mandatory.
- ERP-PBCC and DSSS-OFDM: not widely used

IEEE802.11n: OFDM

- **IEEE802.11a and 802.11g use OFDM**
  - 20 MHZ OFDM channels
  - Each channel: 52 subcarriers (48 subcarriers + 4 pilot tones)
- **IEEE802.11n uses OFDM**
  - 20 MHz OFDM channels and 40 MHz OFDM channels
    - 20 MHz OFDM channels have 56 subcarriers (52 subcarriers + 4 pilot tones)
    - 40 MHz OFDM channels have 112 subcarriers (108 subcarriers + 4 pilot tones)
    - 40 MHz channels by bonding two 20 MHz channels