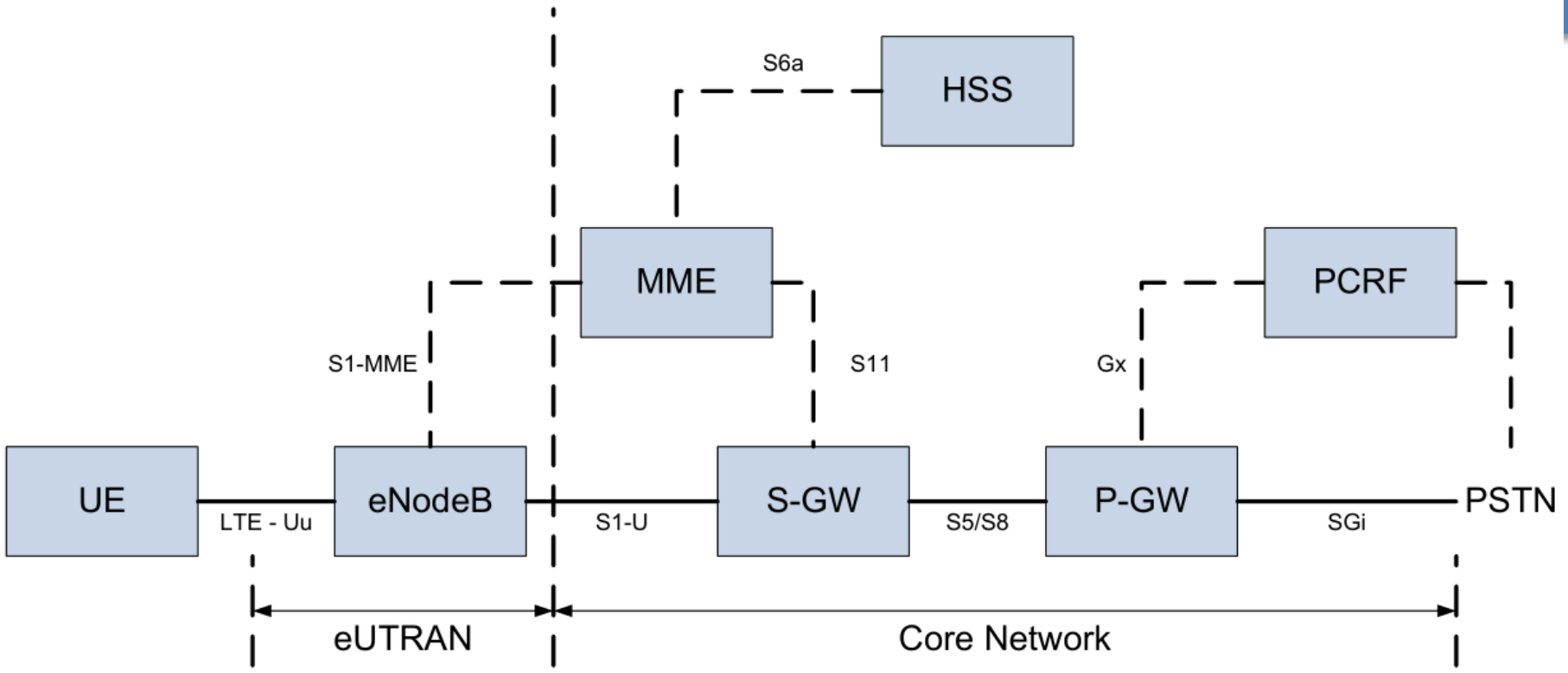
LTE Core

Evolved Packet System (EPS)

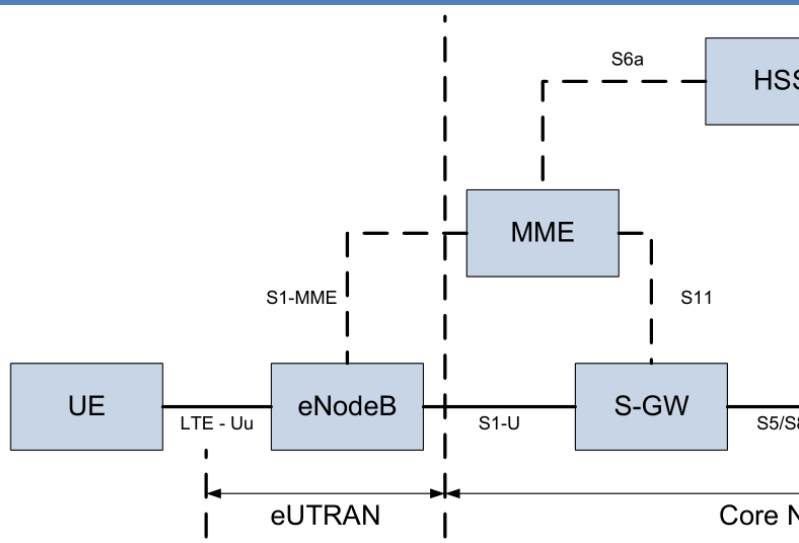


Source: Alexander Schill. TU Dresden

- UE = User Equipment (MS in GSM)
- HSS = Home Subscriber Server (lHLR in GSM)
- eNodeB = Evolved Node B (BSS in GSM)
- E-UTRAN = Evolved UTRAN
- EPC = Evolved Packet Core (Network). Completely IP based.

eNodeB

- eNodeB = “evolved” Node B
- Does the job of
  - GSM: BSS
  - UMTS: Node B + RNC



- eNodeB can directly communicate with each other
  - Interference coordination: UE reports signal measurements from neighbor cells to its eNodeB; the node can contact the eNodeB of those cells
  - Handover: eNodeB can decide and prepare handover (without involvement of an MSC in GSM)

Bearers and channels

- Like in UMTS, the different traffic requirements of applications are mapped to bearers which provide 9 classes of standardized QoS in the access network and the core network

QCI	Resource Type	Priority	Packet Delay Budget(ms)	Packet Error Loss Rate	Example Service
1	GBR	2	100	10^{-2}	Conversational voice
2	GBR	4	150	10^{-3}	Conversational video (live streaming)
3	GBR	5	300	10^{-6}	Non-conversational video (buffered streaming)
4	GBR	3	50	10^{-3}	Real-time gaming
5	Non-GBR	1	100	10^{-6}	IMS signaling
6	Non-GBR	7	100	10^{-3}	Voice, video (live streaming), interactive gaming
7	Non-GBR	6	300	10^{-6}	Video (buffered streaming)
8	Non-GBR	8	300	10^{-6}	TCP-based (for example, WWW, e-mail), chat, FTP, p2p file sharing, progressive video and others
9	Non-GBR	9	300	10^{-6}	

- On the MAC layer, the communication between the UE and the network is organized in logical, transport, and physical channels

Protocol stack for air interface

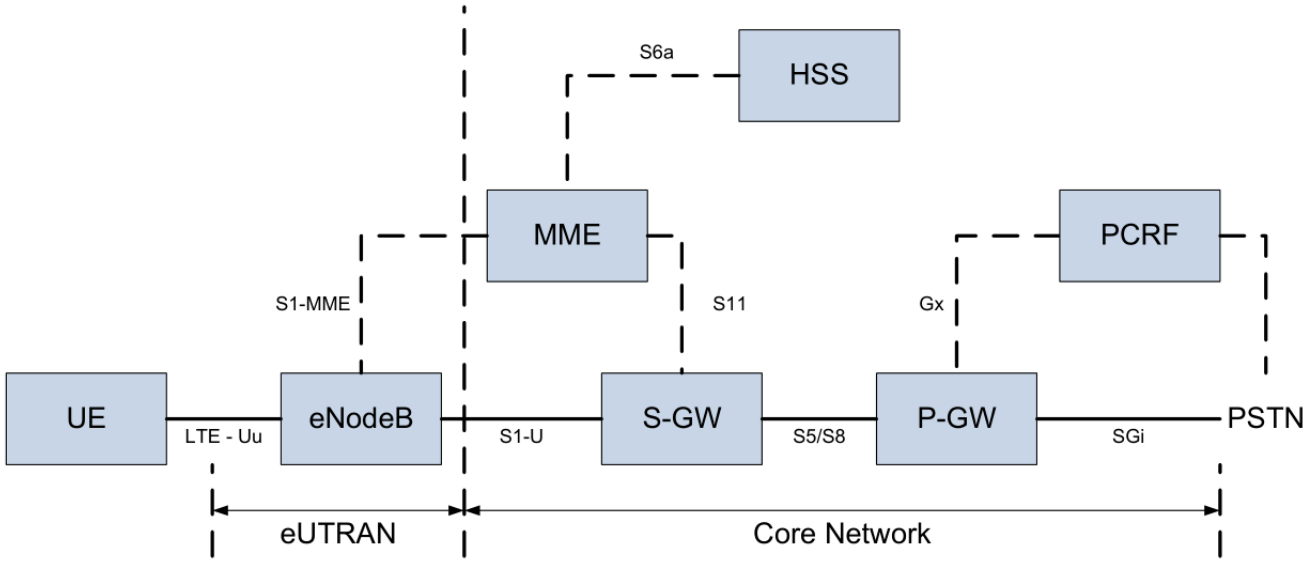
Signaling traffic exchanged with the core network	
Signaling protocols	
RRC	Radio Resource Management. Broadcasting, notification of UE about incoming calls, etc.

User traffic
TCP/UDP
IP

PDCP	Security, header compression.
RLC	Radio Link Control. Error detection and correction, acknowledgments, segmentation,...
MAC	Maps logical channels to transport channels. Scheduling, priority handling, multiplexing,...
PHY	Maps transport channels to physical channels

Mobility Management Entity (MME)

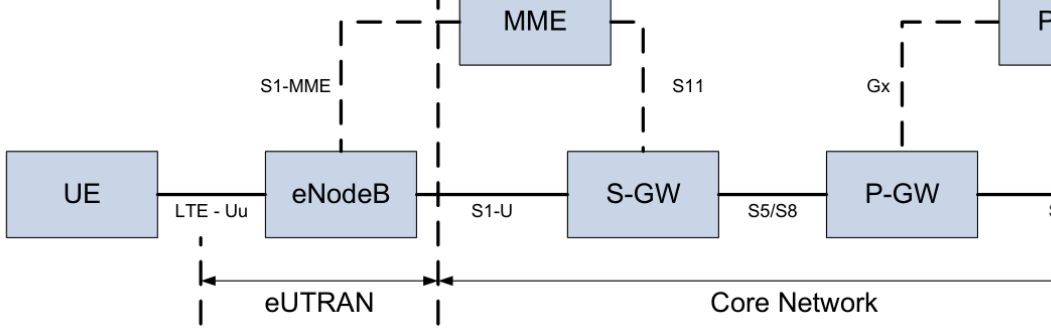
- Responsible for signaling
  - Authentication (access to HSS)
  - Establishing tunnels (GTP, like in GPRS) and modifying them if handover
  - Helping to handover if two eNodeB cannot communicate to each other



Localization

- The MME knows the location of the UE
  - If the UE is active, the location is known on cell level
  - If the UE is idle (inactive):
    - Operator combines cells to tracking areas
    - To save energy, the UE only notifies the MME when it moves to a different tracking area
- If there is incoming traffic for an idle UE, the MME initiates *paging*
  - MME broadcasts paging message to tracking area of the UE
  - The UE wakes up every 128 radio frames, i.e., 1.28 seconds to check whether there is paging message

Data transfer



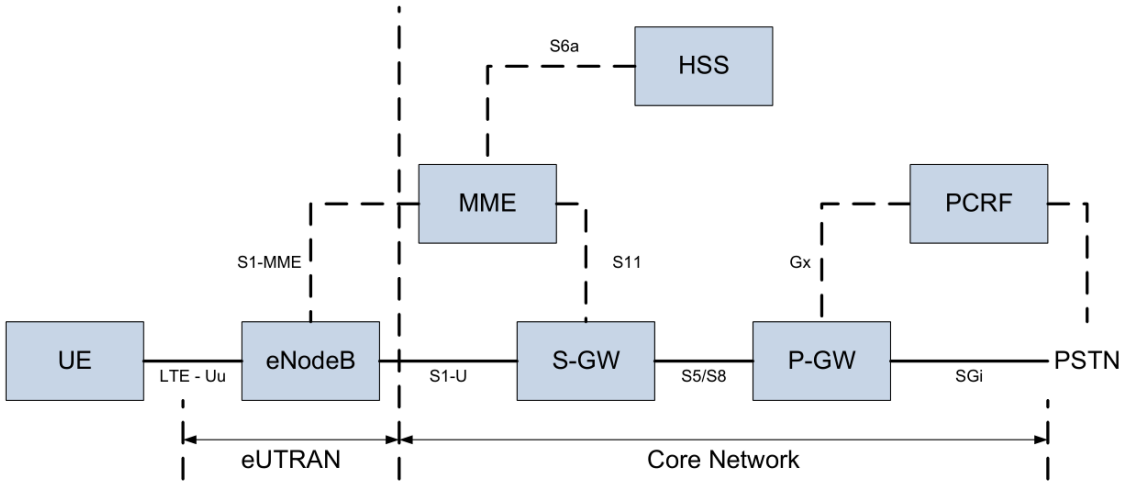
- A UE gets an IP address assigned by the P-GW in the moment it connects to the LTE network
  - P-GW = Packet Data Network (PDN) Gateway.
  - P-GW connects to the Internet or intranets of large companies
- Incoming Internet traffic is tunneled from the P-GW to the S-GW and then to the eNodeB of the UE
  - S-GW = Servicing Gateway. Responsible for several eNodeB
- If device is in an area with only GSM/UMTS:
  - The MME will talk with the SGSN of the GSM/UMTS network and establish a connection between the SGSN and the S-GW

Voice calls

- The LTE network is only made for packet traffic
- To do voice calls, there are different possibilities:
  - Phone falls back to 2G/3G. This was the solution used at the beginning of LTE. Still used.
  - 2G/3G voice traffic is sent over the LTE network. Not widely deployed.
  - Voice-over-IP for LTE (VoLTE): Voice data is sent in IP packets (similar to Skype). Since 2014.
    - Higher voice quality
    - Does not require 2G/3G infrastructure
    - Ultimatively, no difference anymore between phone calls over LTE or WiFi

PCRF

- Policy and Charging Rules Function
- Responsible for
  - deciding whether connection is allowed
  - billing
- Billing and filtering can be depending on type of service

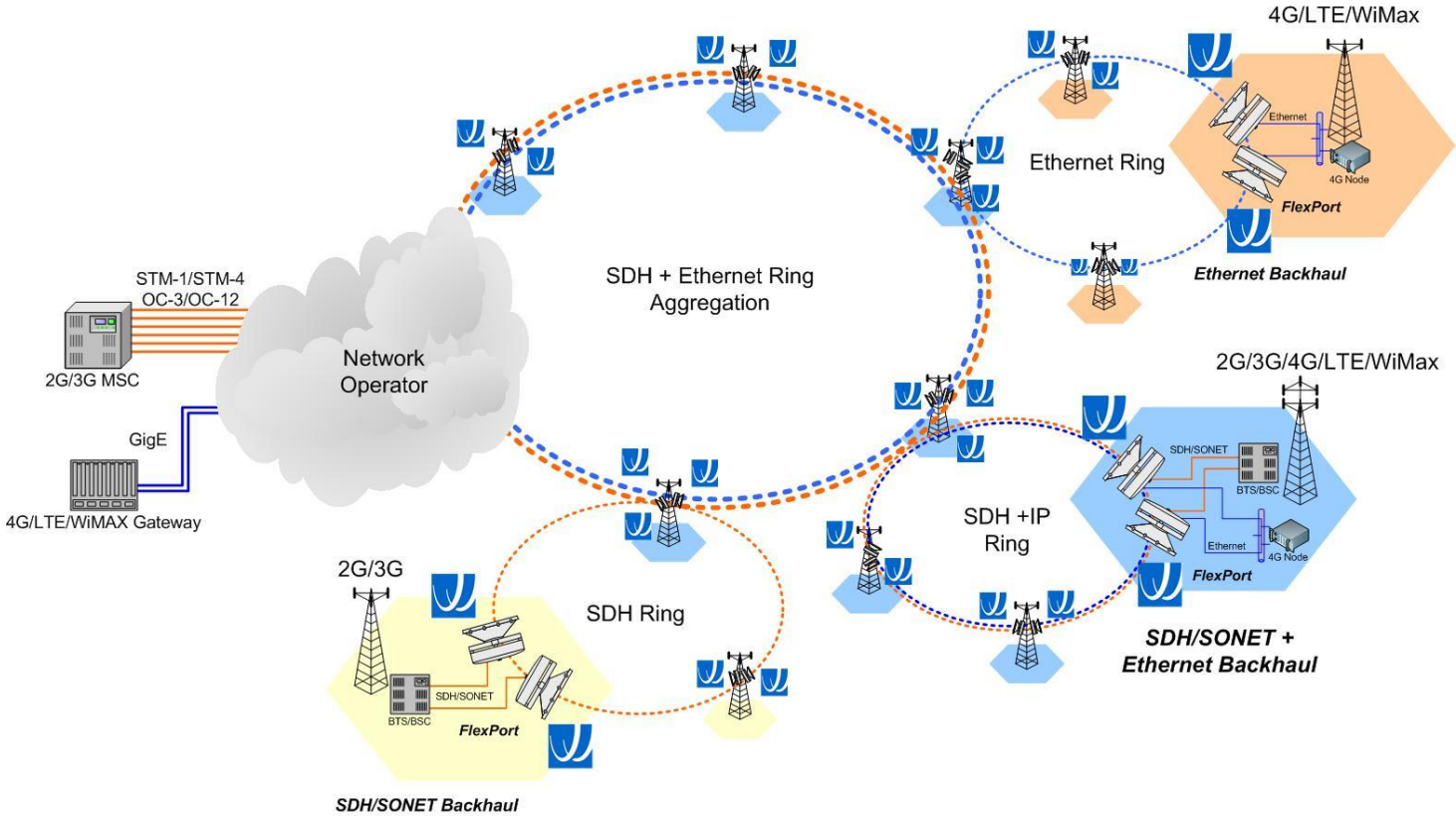


Security

- Handled by MME and HSS
- Authentication
  - Initiated when an UE sends an *attach request* to the MME
  - Authentication is mutual: the phone and the network authenticate to each other
  - The user and network keys are stored in the SIM card and in the HSS
- Encryption between UE and eNodeB
- It is up to the operator to use secure protocols (such as IPsec) inside the core network
- Downgrade attack: Put a fake base station with a strong signal that tells the UE that LTE is not available and it should downgrade to GSM

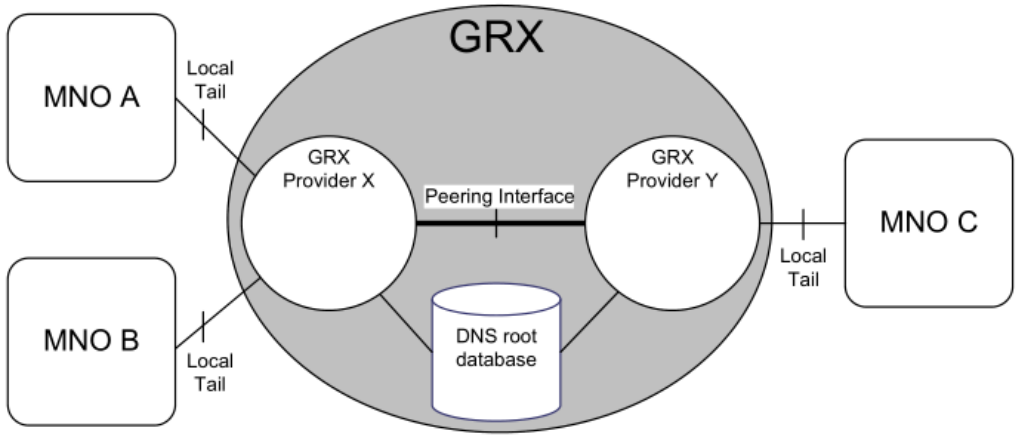
Backhaul

- Backhaul = The link between (multiple) eNodeB and the EPC
- Can become a bottleneck with the high data rates of LTE and LTE-A
- Modern backhauls are quite complex. Example by Bridge Wave:



Connection between operators (1)

- Roaming requires connections between the EPC of different Mobile Network Operators (MNO)
- Voice traffic in GSM: Exchanged between the G-MSC (managed with SS7)
- GPRS/UMTS:
  - At the beginning: direct connections between the GGSN
  - Later, GRX (GPRS Roaming eXchange). GRX networks are private IP networks. Different companies provide GRX services to MNOs. They are also inter-connected.



Connection between operators (2)

- In LTE, GRX has evolved to IPX (Internet Protocol Packet Exchange), which interconnects not only MNOs but also ISPs.
- Here is for example a company that provides IPX to MNOs: https://www.teliacarrier.com/products-and-services/voice-mobile-data-and-iot/mobile-data-roaming.html
- Again, the different IPX networks are also interconnected. Example of a company providing this service: https://www.ams-ix.net/ams/service/mobile-peering

LTE for IoT

LTE for IoT

- GSM/GPRS has been switched off/will be switched off soon in many countries
- What can IoT networks use for long-range communication?
  - We have already seen LoRa for long-range low-power communication
- Using LTE network for IoT would have several advantages:
  - Infrastructure already exists
  - Network is regulated →more predictable quality of service than license-free bands
- But:
  - LTE networks and protocols are much more complex than LoRa or Sigfox
  - LTE networks not optimized for low power devices

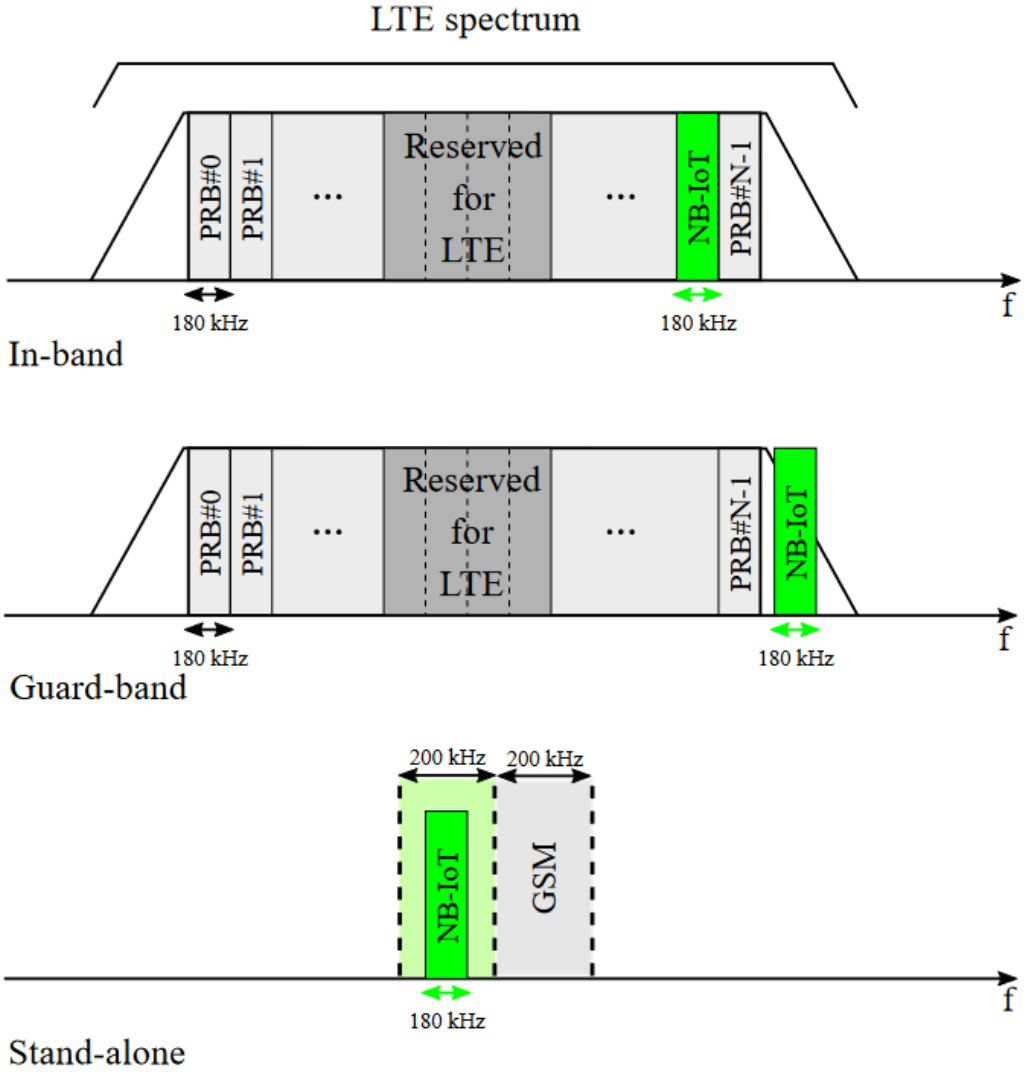
Narrow-Band IoT (NB-IoT)

- Category NB1 (Release 13): peak 26kbit/s down, 16.9kbit/s (if 3.75kHz carriers are used) or 66kbit/s ("multitone") up
- Category NB2 (Release 14): peak 127kbit/s down, 159kbit/s up
  - Supports power saving: Base stations knows when device wakes up again
- Radio: IoT devices coexist with normal LTE devices
  - 1x1 "MIMO", half-duplex
  - OFDMA downlink, SC-FDMA uplink
  - Latency up to 10s
- Does not support handover
- Lot of simplifications in channel coding, maximum message size,...

NB-IoT deployment modes

Deployment modes:

1. In band: LTE operator allocates one resource block (180kHz) to NB-IoT
2. Guard-band: LTE operator uses the guard-band between the existing LTE bands for NB-IoT
3. Stand alone: NB-IoT signal uses 180kHz band of GSM



Source: Kanj et al.

LTE-M

- Category 0 (Release 12): peak 1 Mbit/s down, 1 Mbit/s up, never deployed
- Category M1 (Release 13): 1 Mbit/s down, 1 Mbit/s up
- Category M2 (Release 14): 4 Mbit/s down, 7 Mbit/s up
- Bandwidth high enough for audio streaming
- Radio: IoT devices coexist with normal LTE devices
  - 1x1 “MIMO”, half-duplex or full duplex
  - OFDMA downlink, SC-FDMA uplink
  - Latency <15ms
- 6 resource blocks
- Devices can do handover
- Hardware more expensive & power consuming than NB-IoT