Mobile Networks

Mobile and cyber-physical systems

Federica Paganelli

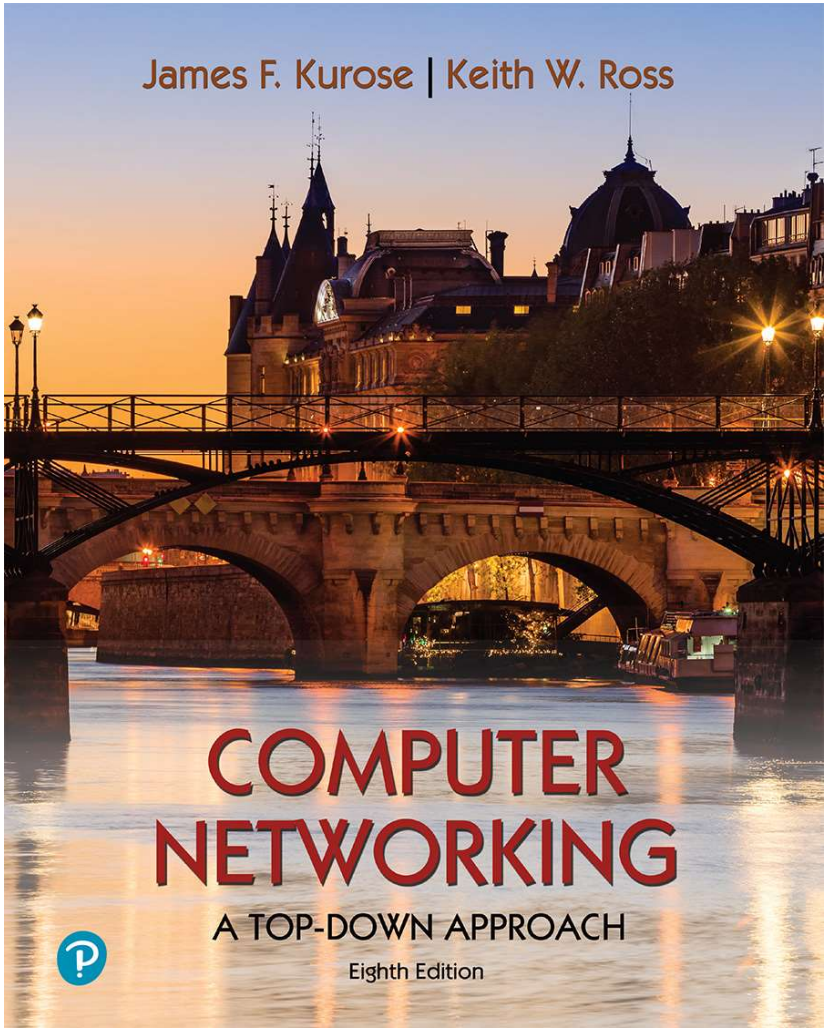
wireless used AES for AUTH

A NOTE ON THESE SLIDES

They are a (free) adaptation of the original slides provided with the book:

Computer Networking: A Top-Down Approach

8th edition, Jim Kurose, Keith Ross, Pearson, 2020



Wireless and Mobile Networks: context

- more wireless (mobile) phone subscribers than fixed (wired) phone subscribers (10-to-1 in 2019)!
- more mobile-broadband-connected devices than fixed-broadband-connected devices devices (5-1 in 2019)!
  - 4G/5G cellular networks now embracing Internet protocol stack, including SDN
- two important (but different) challenges
  - wireless: communication over wireless link
  - mobility: handling the mobile user who changes point of attachment to network

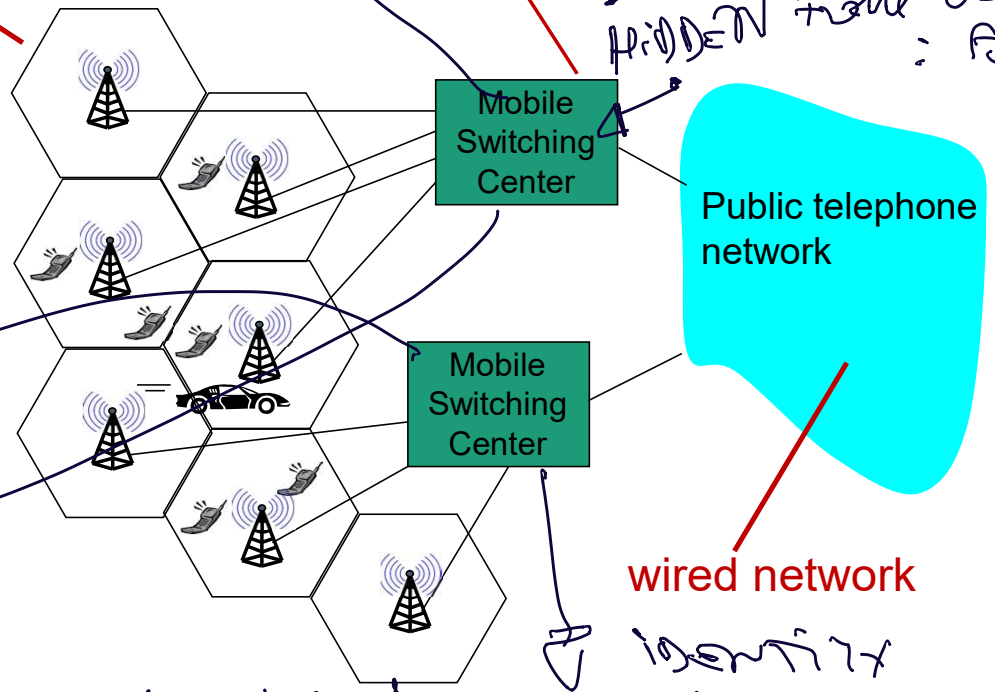
evolution of architecture of WD: wireless network

Outline

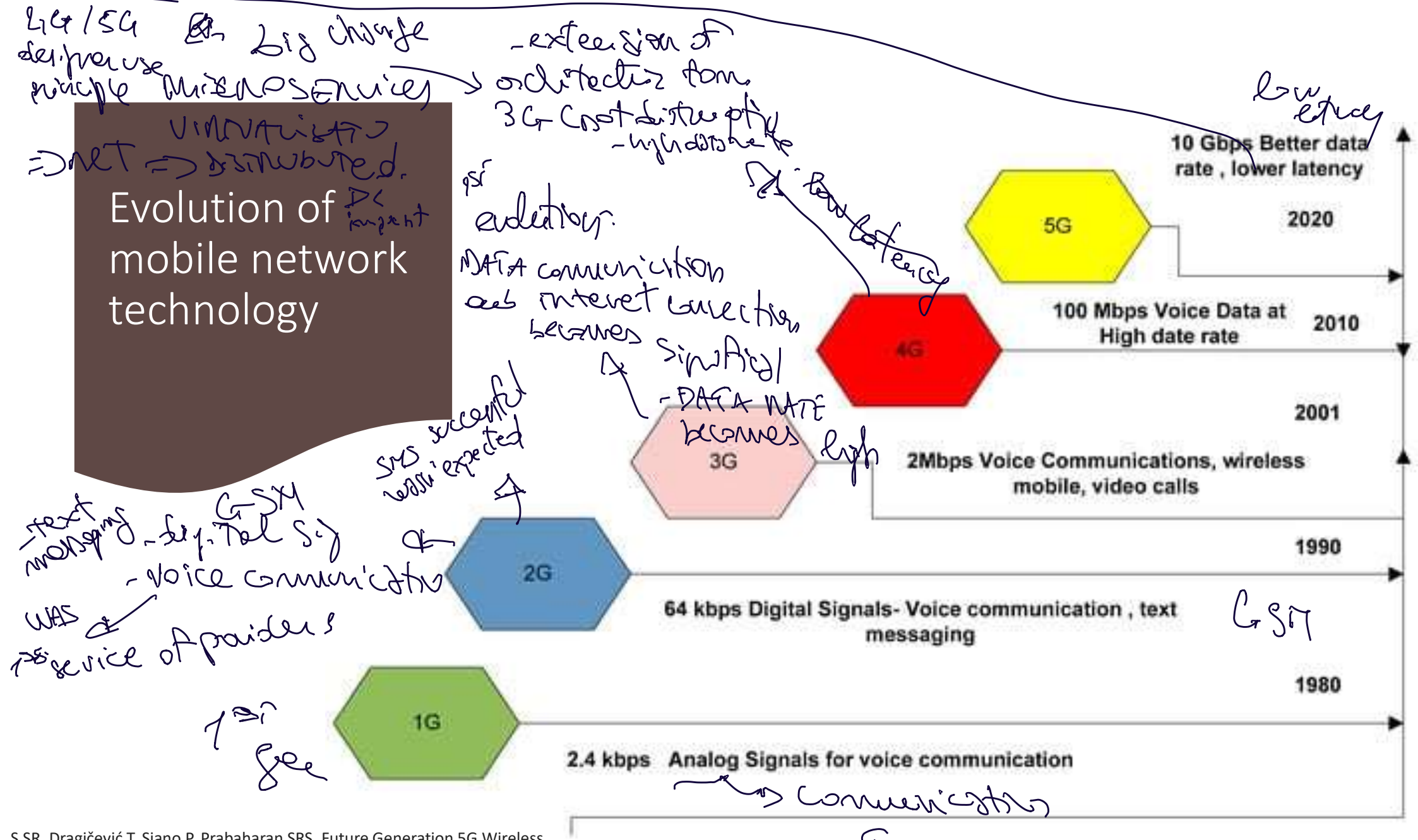
- Cellular networks
  - Cellular network evolution (1G, 2G, 3G)
  - 4G and 5G networks
- Mobility
  - Mobility management: principles
  - Mobility management: practice
    - Mobility management in 4G/5G networks
    - Mobile IP
- Mobility: impact on higher-layer protocols

HAND OFF: user move from BS (same or different provider BS)

Components of cellular network architecture

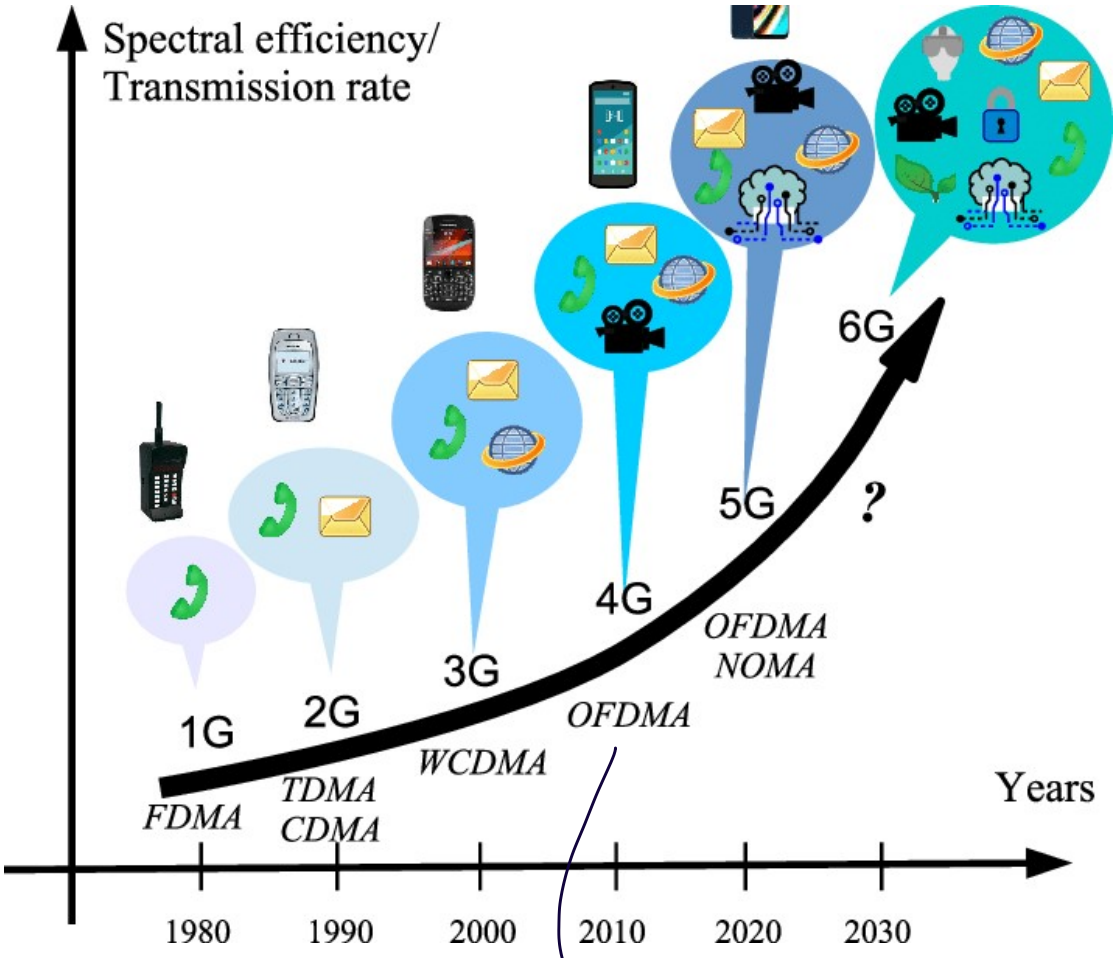


Evolution of mobile network technology



S SR, Dragičević T, Siano P, Prabaharan SRS. Future Generation 5G Wireless Networks for Smart Grid: A Comprehensive Review. *Energies*. 2019; 12(11):2140. https://doi.org/10.3390/en12112140

Different access technic FDM
To medium



use frequency division with specific choice to achiv higher DATA RANGE

Evolution of mobile network technology

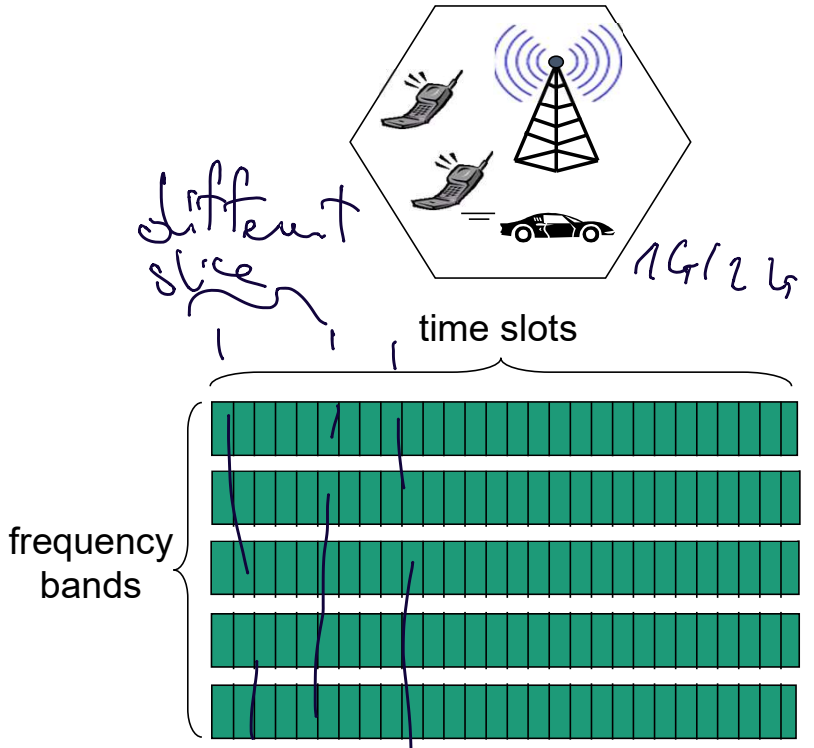
Access techniques

Gutierrez, Carlos & Caicedo, Mauricio & Campos Delgado, Daniel Ulises. (2021). 5G and Beyond: Past, Present and Future of the Mobile Communications (English Version). IEEE Latin America Transactions. 19. 1702-1736.

Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

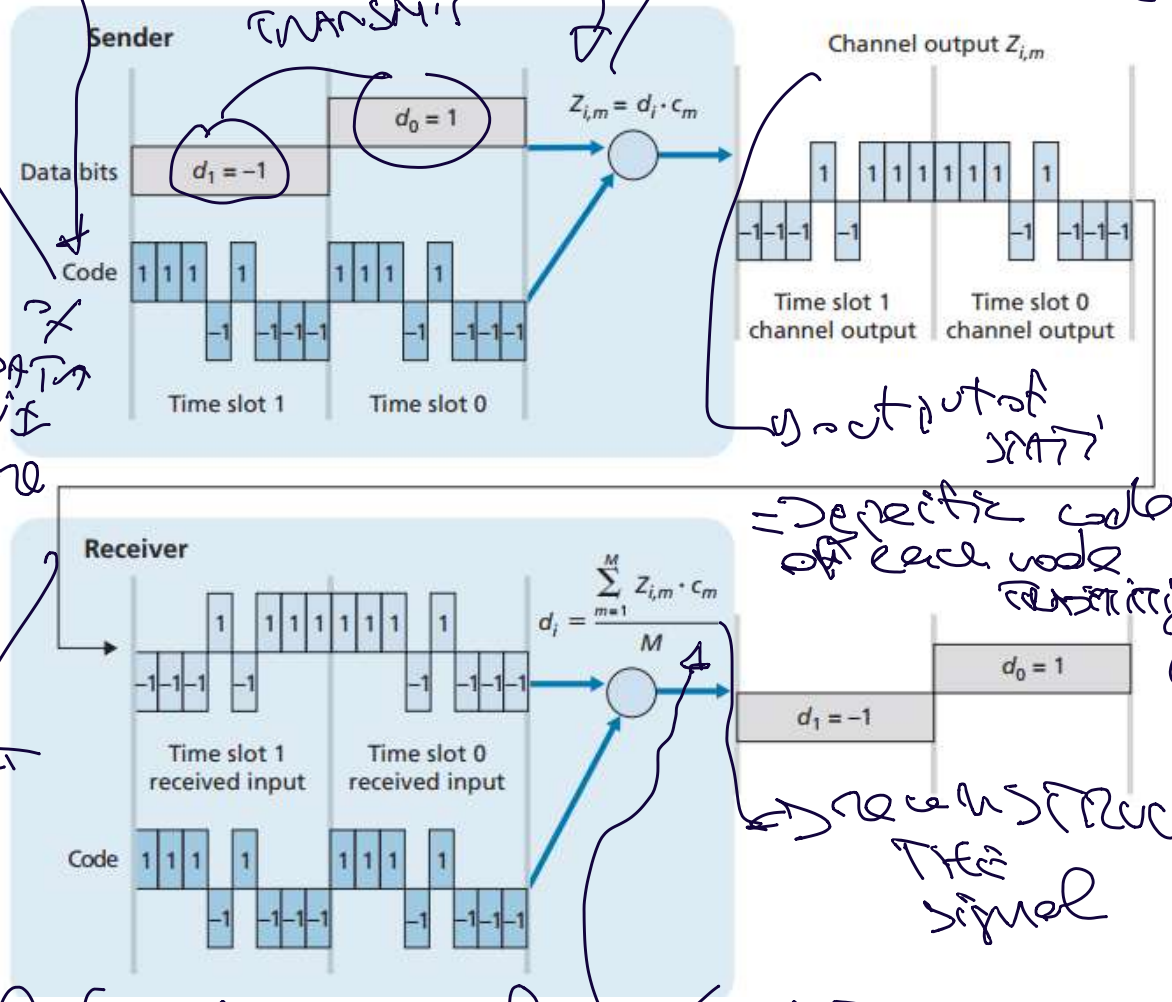
- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access



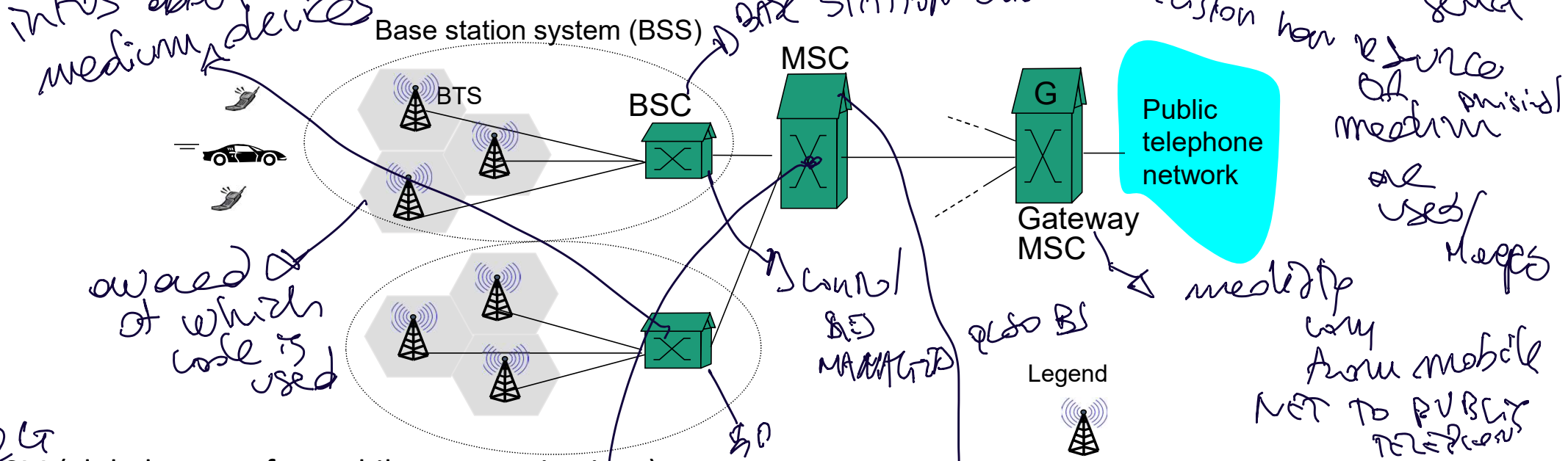
Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access
  - Partioning the code space



2G (voice) network architecture



GSM (global system for mobile communications)

- TDM+FDM: 200 Khz frequency band, each band supports 8 TDM calls

2.5G

- GPRS (2.5 G) General Packet Radio Service
  - Time slots dynamically reserved for data transfer(40-60 kbps)
- CDMA

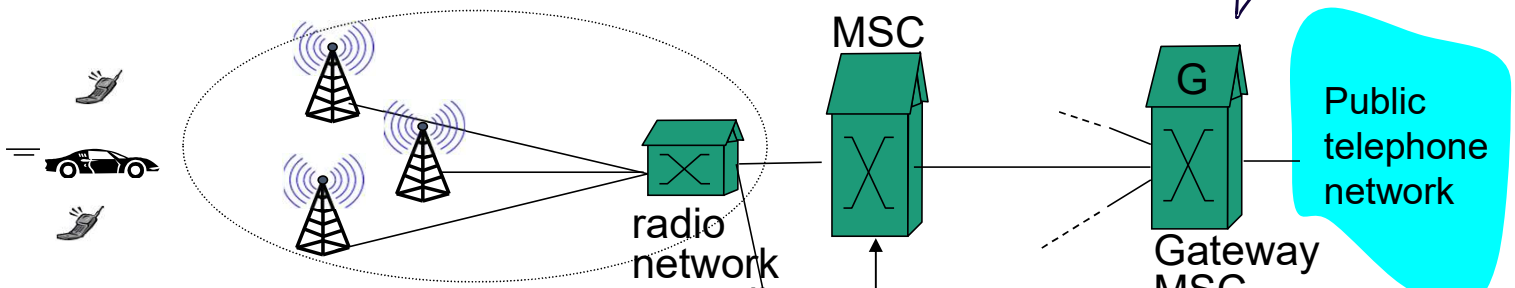
Base transceiver station (BTS)

Base station controller (BSC)

Mobile Switching Center (MSC)

Mobile subscribers

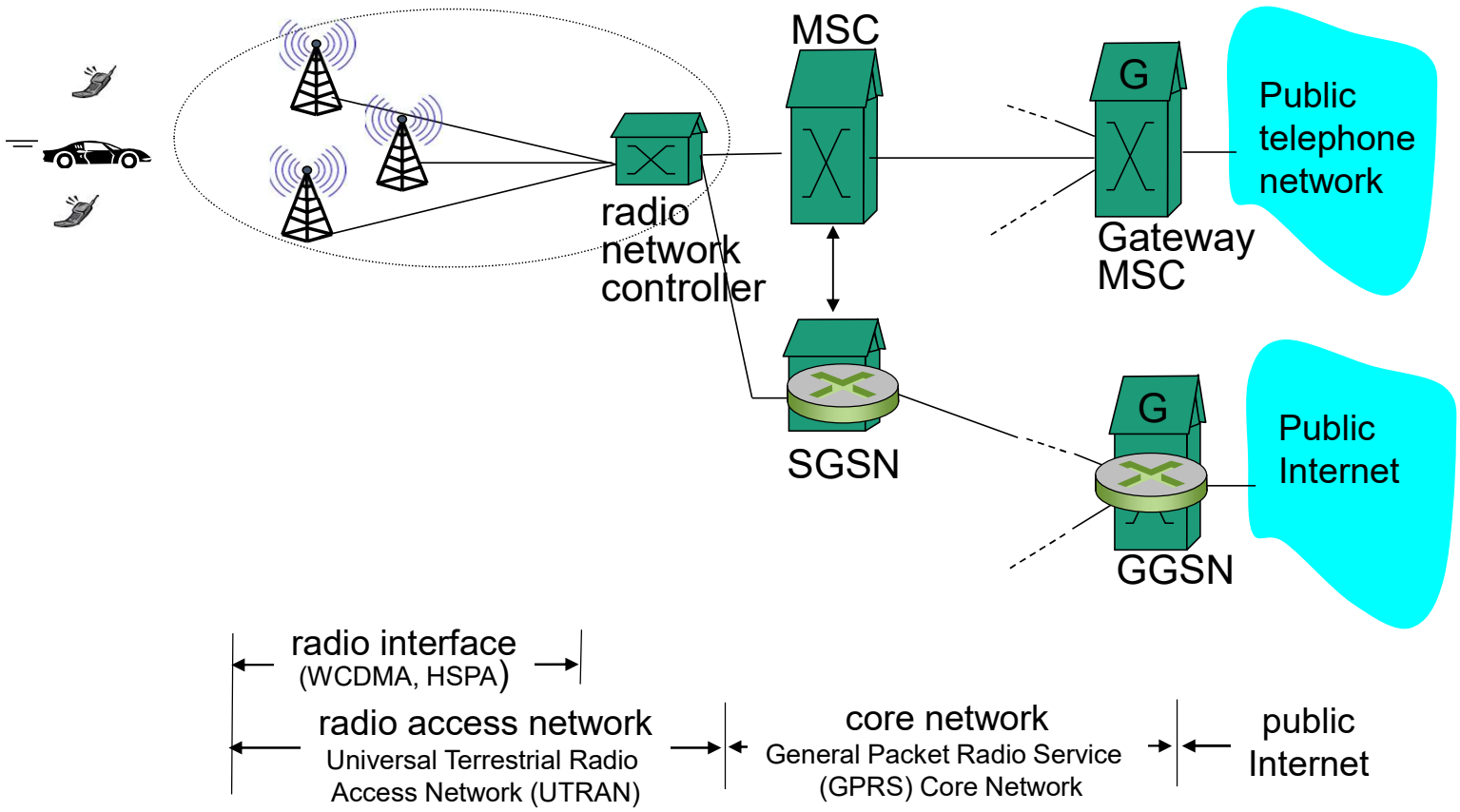
3G (voice+data) network architecture



Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

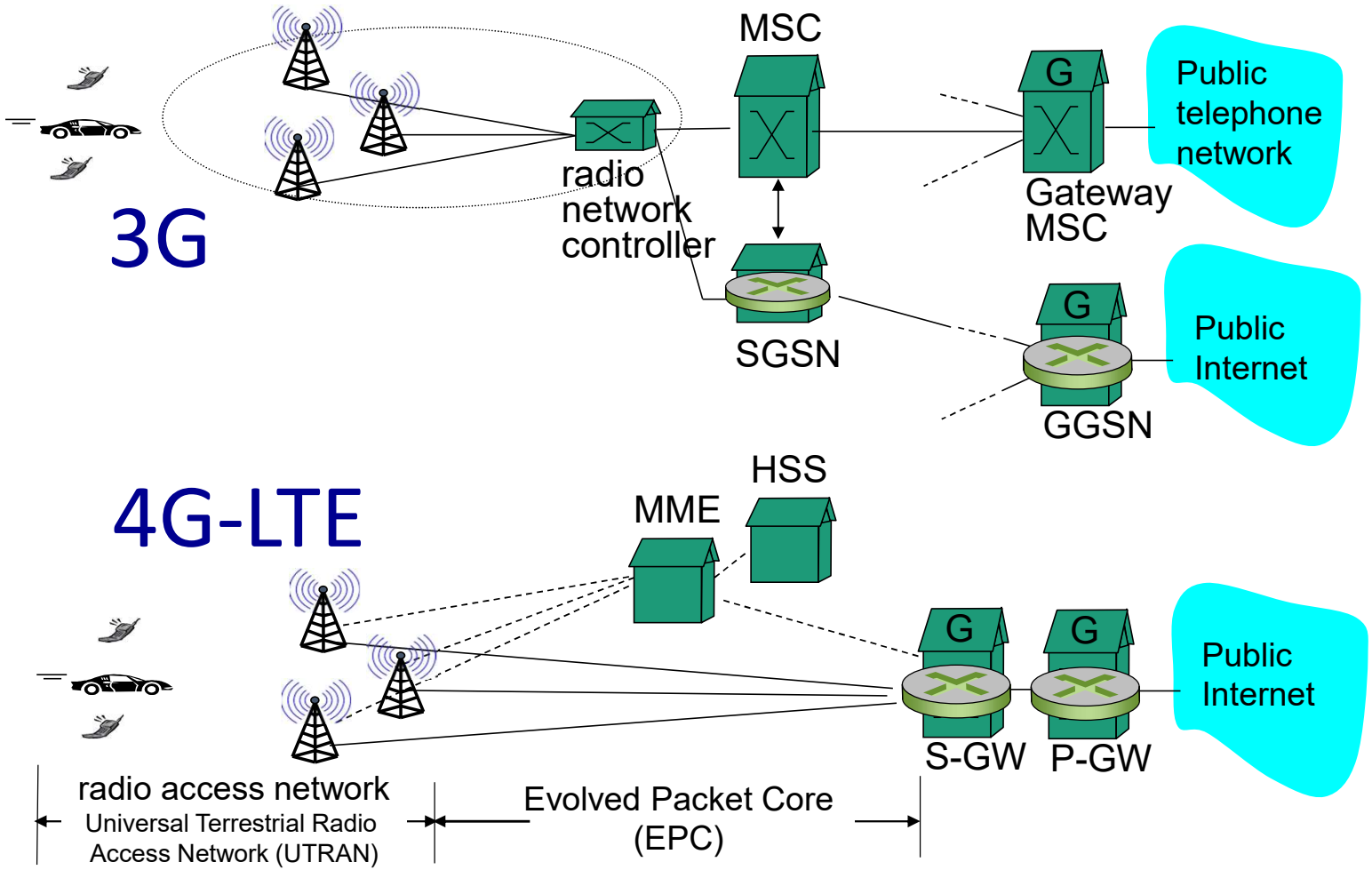
- voice network *unchanged* in core
  - Circuit switching
- data network operates in parallel
  - Packet switching

3G (voice+data) network architecture



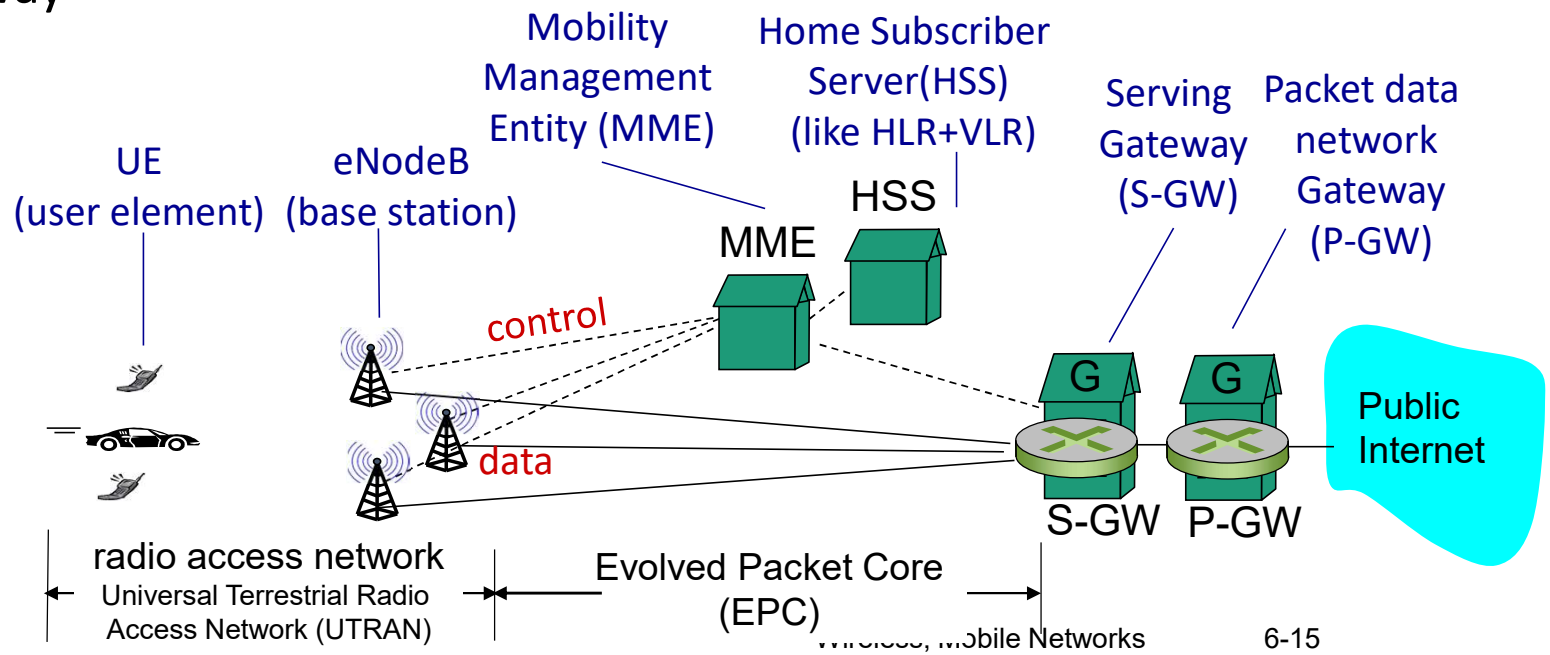
Example:
UMTS

3G versus 4G LTE network architecture



4G: main differences from 3G

- All-IP core: IP packets tunneled (through core IP network) from base station to gateway
- **no separation between voice and data** – all traffic carried over IP core to gateway



4G/5G cellular networks

- the solution for wide-area mobile Internet
- widespread deployment/use:
- transmission rates up to 100’s Mbps
- technical standards: 3rd Generation Partnership Project (3GPP)
  - wwww.3gpp.org
  - 4G: Long-Term Evolution (LTE) standard

4G/5G cellular networks

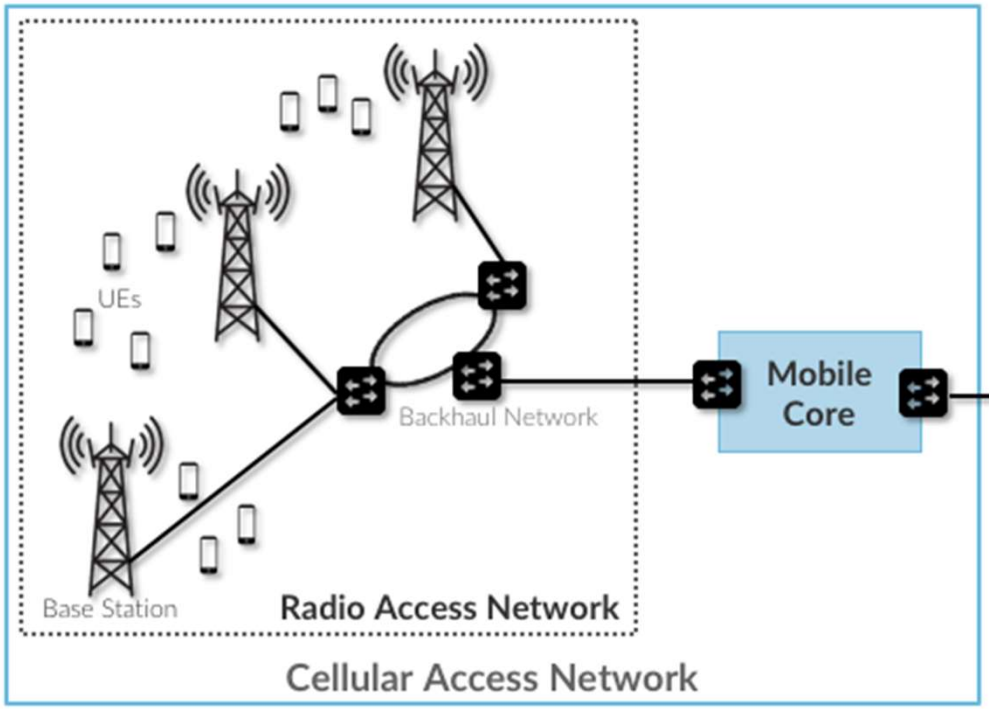
similarities to wired Internet

- edge/core distinction, but both below to same carrier
- global cellular network: a network of networks
- widespread use of protocols we've studied: HTTP, DNS, TCP, UDP, IP, NAT, separation of data/control planes, SDN, Ethernet, tunneling
- interconnected to wired Internet

differences from wired Internet

- different wireless link layer
- mobility as a 1st class service
- user "identity" (via SIM card)
- business model: users subscribe to a cellular provider
  - strong notion of "home network" versus roaming on visited nets
  - global access, with authentication infrastructure, and inter-carrier settlements

4G/5G cellular network architecture



Mobile Core
- Provides Internet (IP) connectivity for both data and voice services
- Ensures QoS requirements
- Tracks user mobility to ensure uninterrupted service
- billing and charging

Backhaul Network
- interconnects the RAN with the Mobile Core
- Wired network (e.g. fiber-optic)
- Emerging wireless solution (Integrated Access Backhaul – IAB)

Radio Access Network (RAN)
- distributed collection of BSs
- manages the radio spectrum

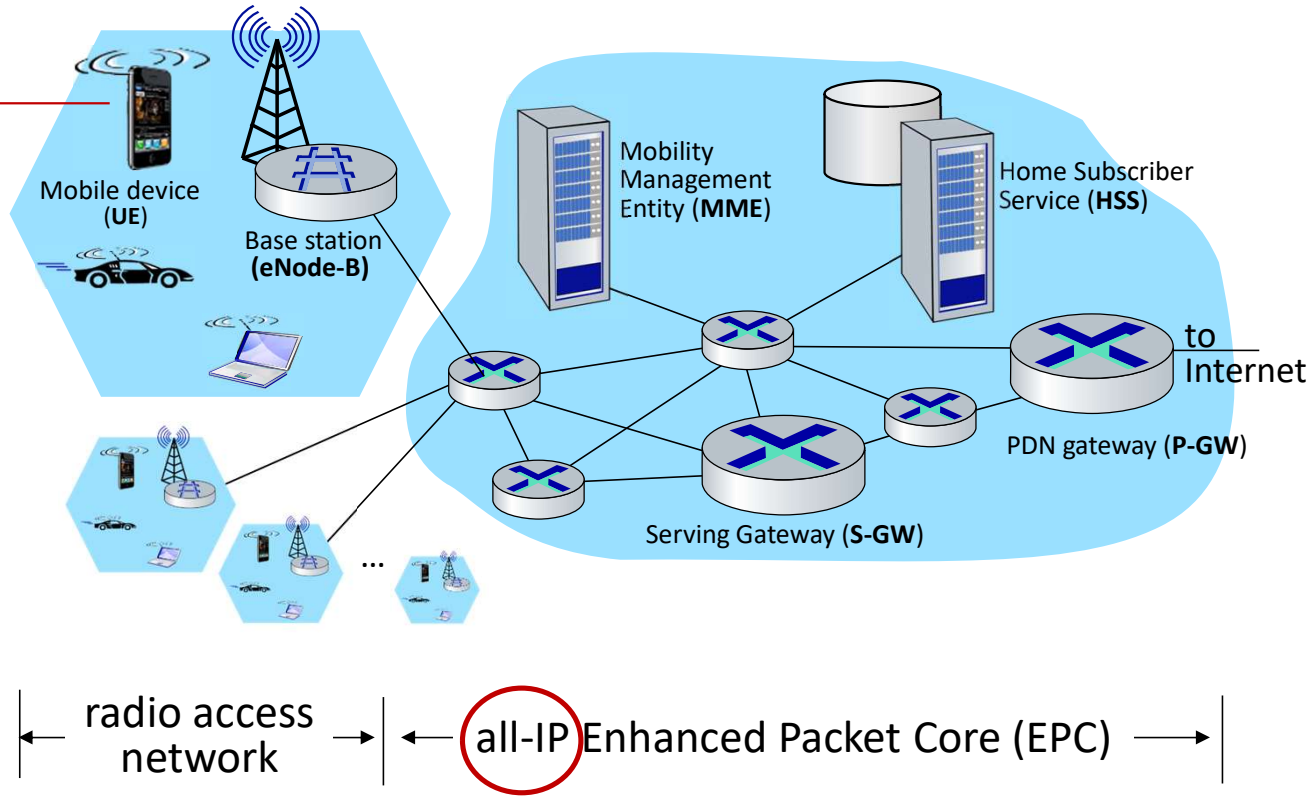
Elements of 4G architecture

Mobile device:

- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- LTE jargon: User Equipment (UE)

Base station:

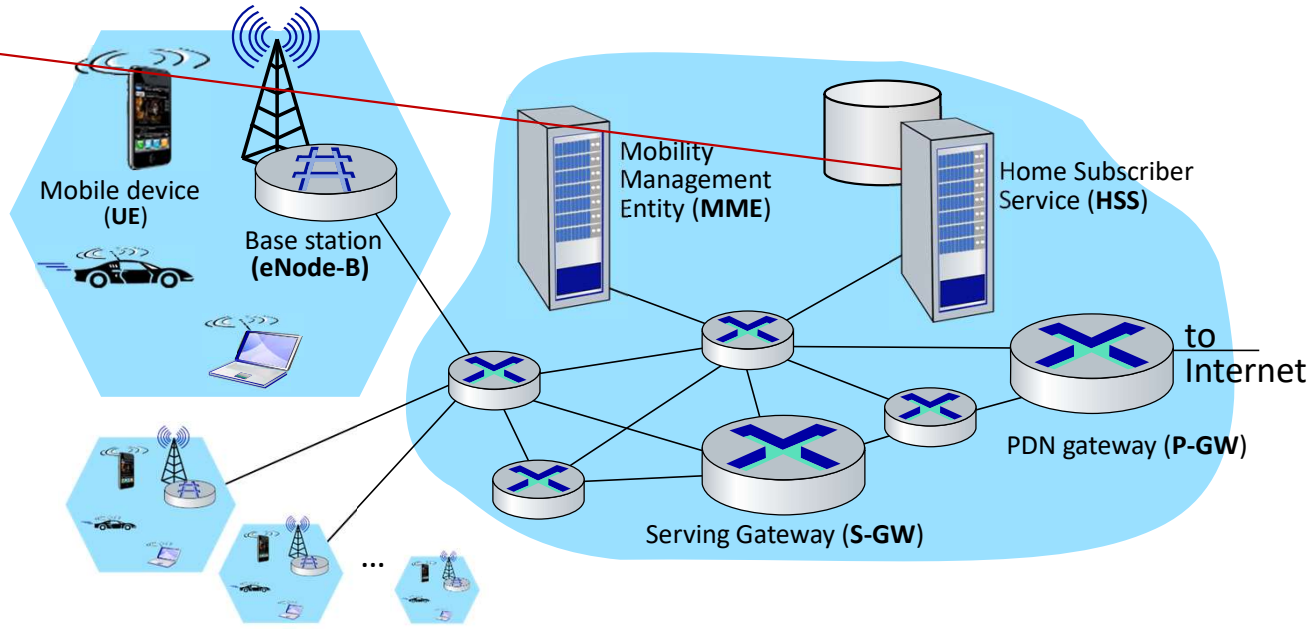
- at "edge" of carrier's network
- LTE jargon: eNode-B



Elements of 4G architecture

Home Subscriber Service

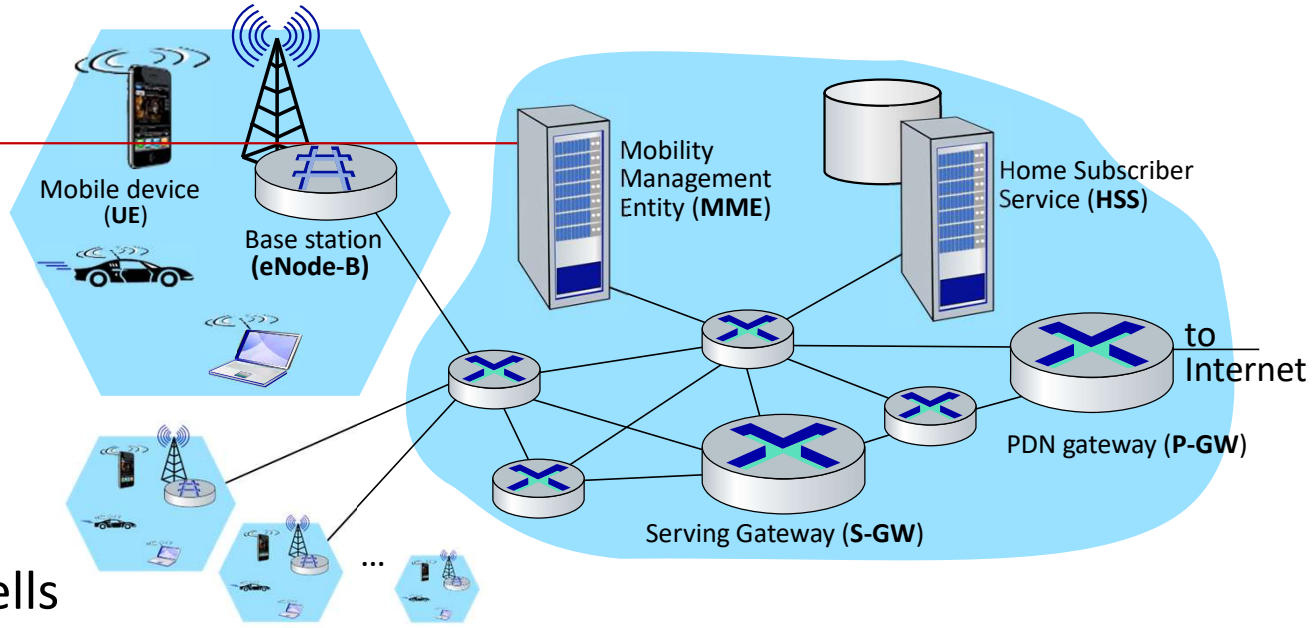
- A database that contains all subscriber-related information
- stores info about mobile devices for which the HSS's network is their "home network"
- works with MME in device authentication



Elements of 4G architecture

Mobility Management Entity

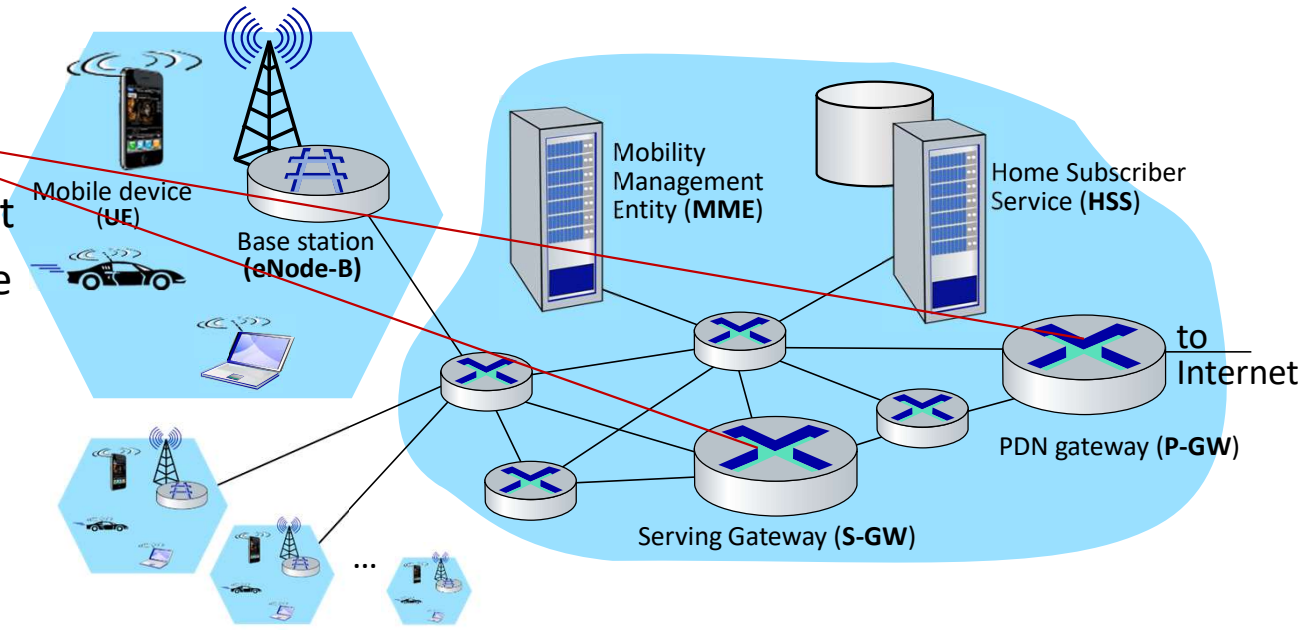
- device authentication (device-to-network, network-to-device) coordinated with mobile home network HSS
- mobile device management:
  - device handover between cells
  - tracking/paging device location
- path (tunneling) setup from mobile device to P-GW



Elements of 4G architecture

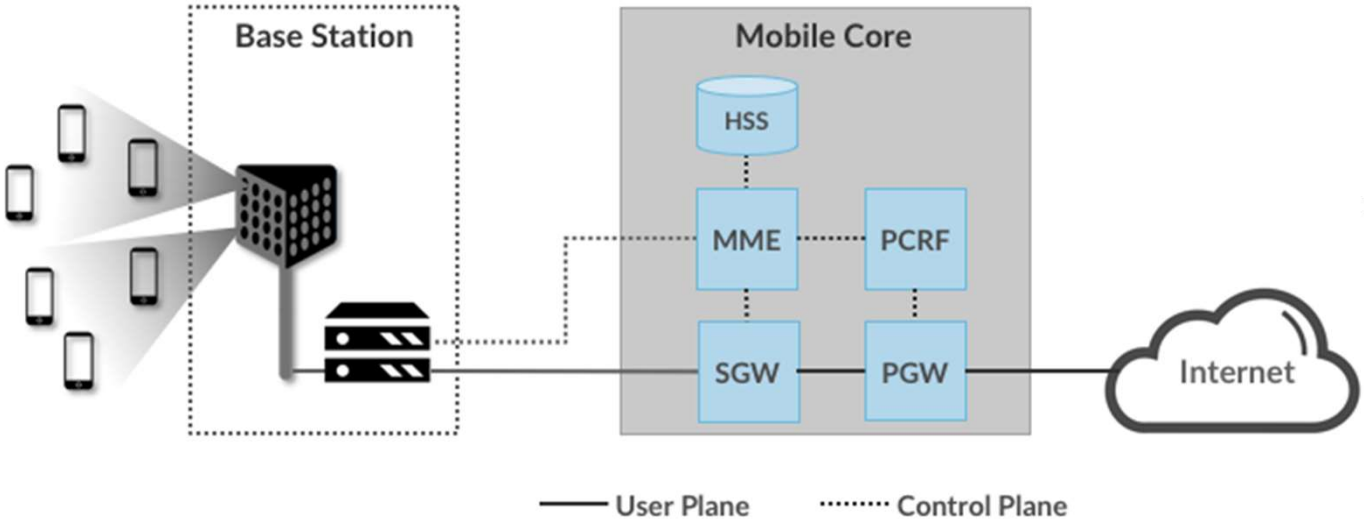
Serving Gateway (S-GW), PDN Gateway (P-GW)

- on data path from mobile to/from Internet
- S-GW: forwards IP packets to and from the RAN
- P-GW
  - a gateway to mobile cellular network
  - looks like any other internet gateway router
  - provides NAT services
  - supports additional access-related functions, including policy enforcement, traffic shaping, and charging.
- other routers: forwarding packets



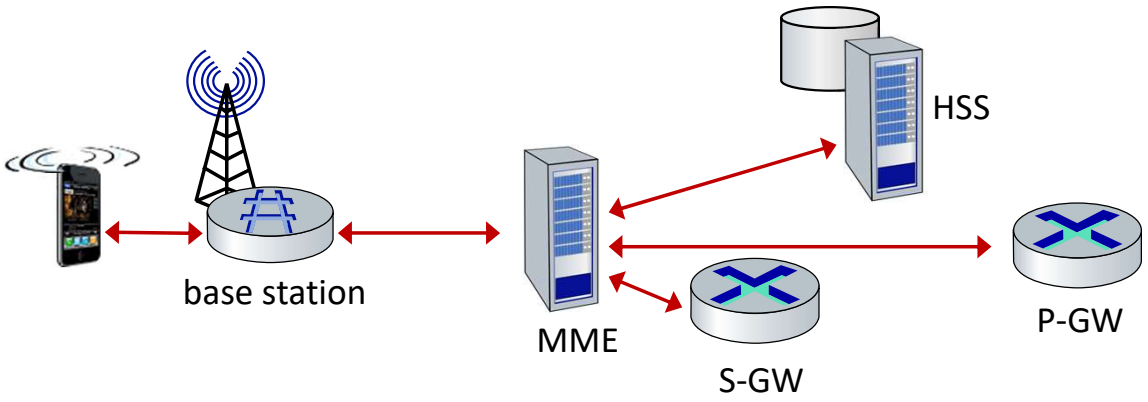
4G Architecture

- Mobile Core components can be flexibly deployed to serve a geographic area



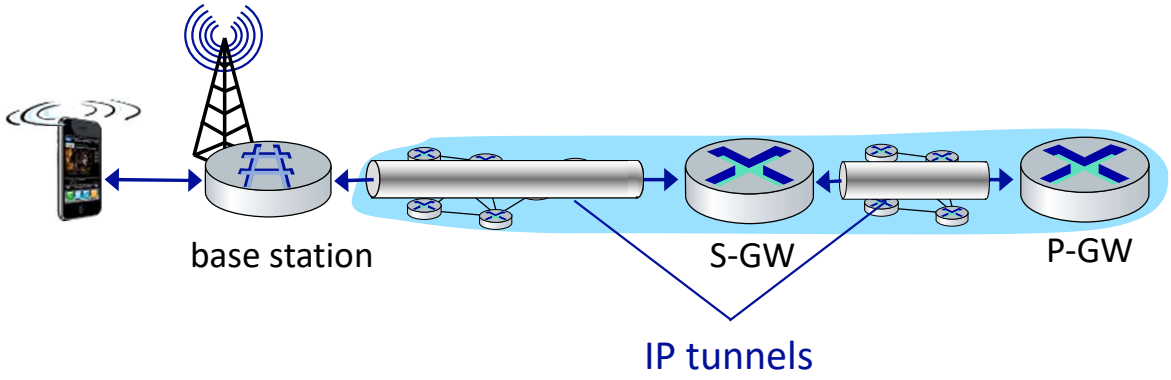
- For example, a single MME/PGW pair might serve a metropolitan area, with SGWs deployed across ~10 edge sites spread throughout the city, each of which serves ~100 base stations
- alternative deployment configurations are allowed by the specifications (3GPP)

4G: data plane control plane separation



control plane

- new protocols for mobility management (later), security, authentication



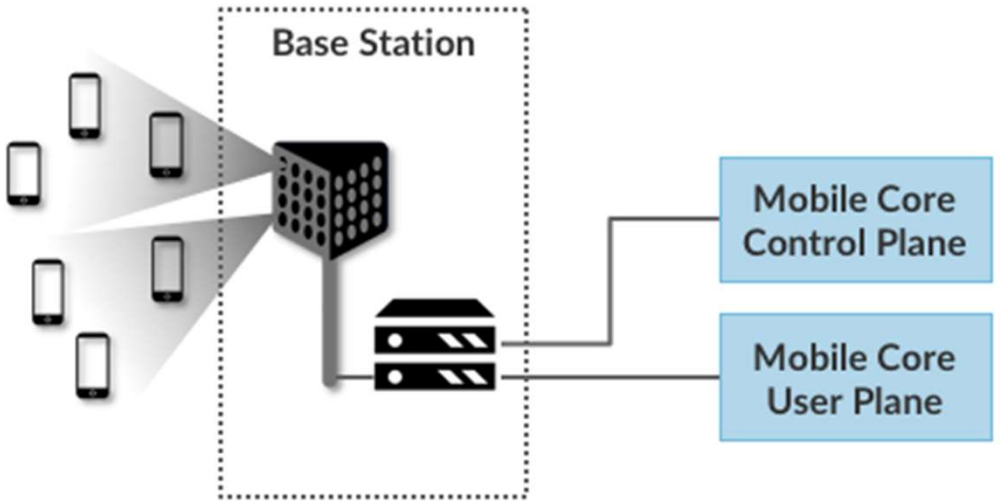
data plane

- new protocols at link, physical layers
- extensive use of tunneling to facilitate mobility

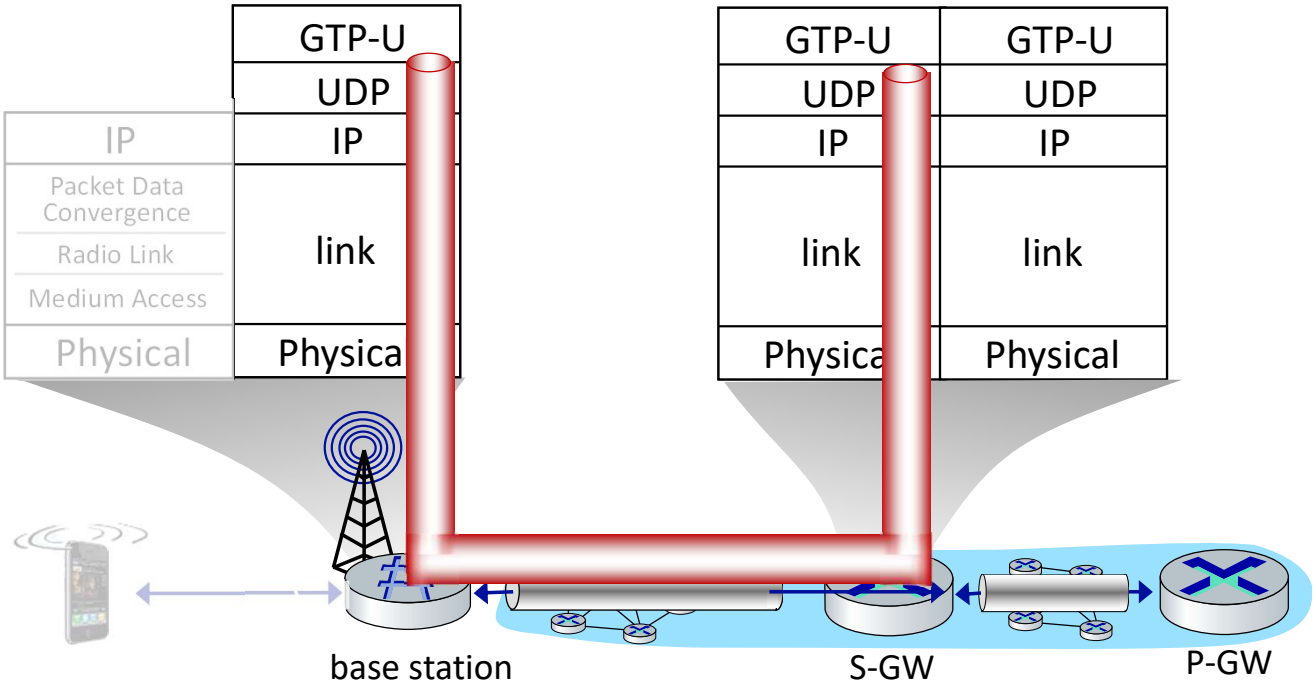
? Have you already heard about control and data plane separation? Where?

4G: data plane control plane separation

- The BS forwards both control and user plane packets between the Mobile Core and the UE.
- **Control plane**: packets are tunnelled over SCTP/IP
  - SCTP (Stream Control Transport Protocol) is an alternative reliable transport to TCP, tailored to carry signaling (control) information for telephony services.
  - UE authentication, registration, and mobility tracking
- **User Plane**: packets are tunnelled over GTP (General Packet Radio Service) Tunneling Protocol)
  - GTP is a 3GPP-specific tunneling protocol designed to run over UDP



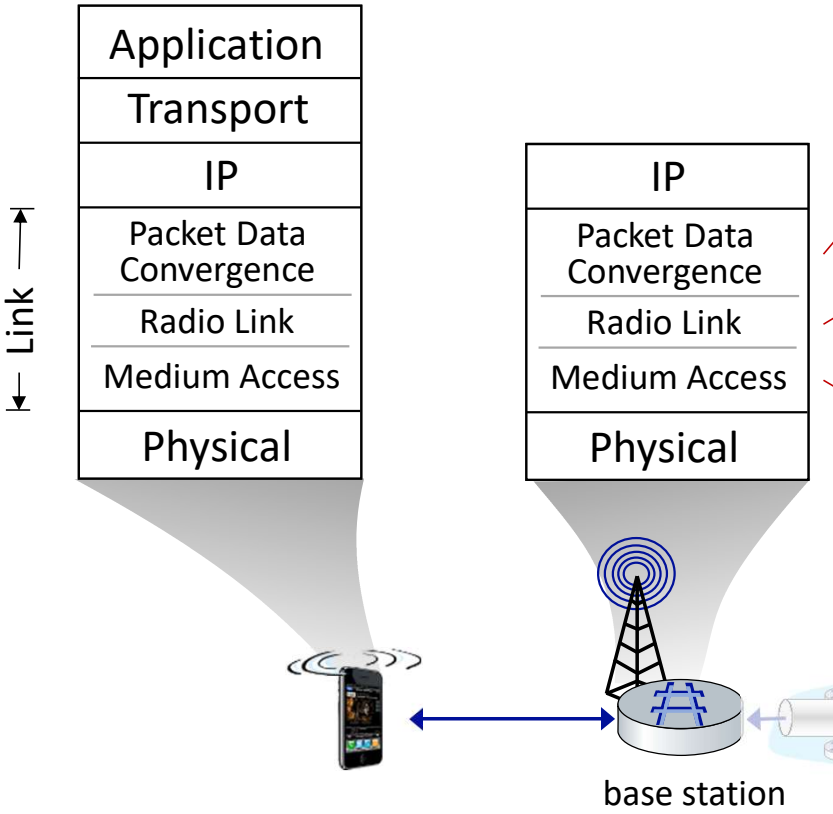
LTE data plane protocol stack: packet core



tunneling:

- mobile datagram encapsulated using GPRS Tunneling Protocol (GTP), sent inside UDP datagram to S-GW
- S-GW re-tunnels datagrams to P-GW
- supporting mobility: only tunneling endpoints change when mobile user moves

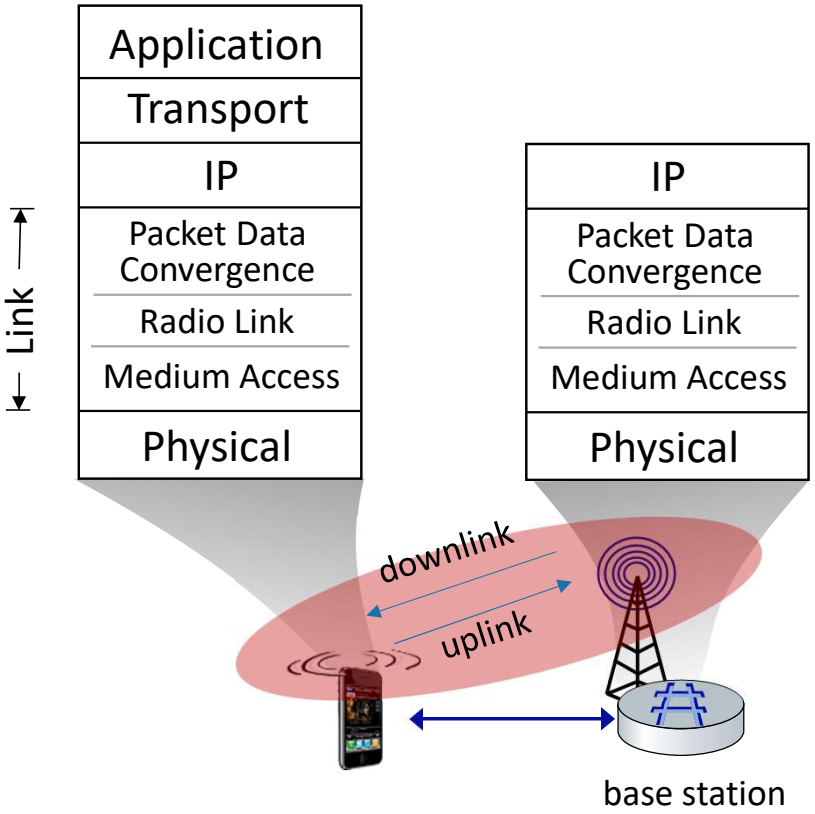
LTE data plane protocol stack: first hop



LTE link layer protocols:

- Packet Data Convergence: header compression/decompression, encryption/decryption
- Radio Link Control (RLC) Protocol: fragmentation/reassembly, reliable data transfer
- Medium Access: requesting and use of radio transmission slots

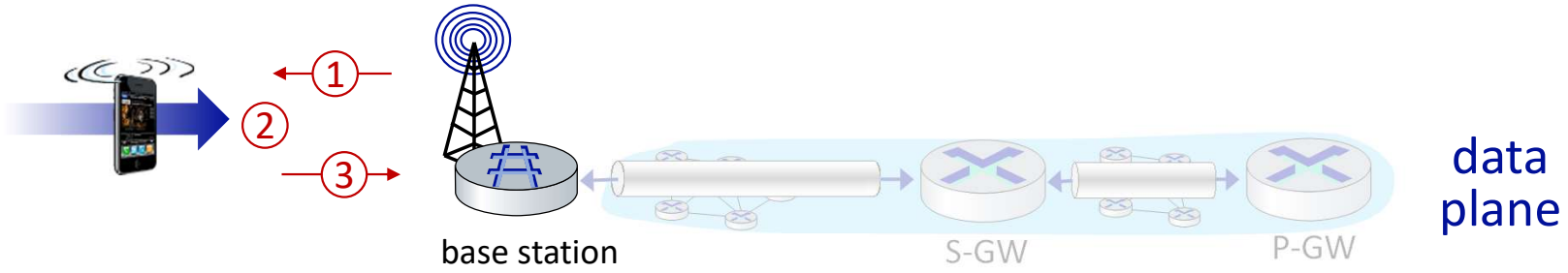
LTE data plane protocol stack: first hop



LTE radio access network:

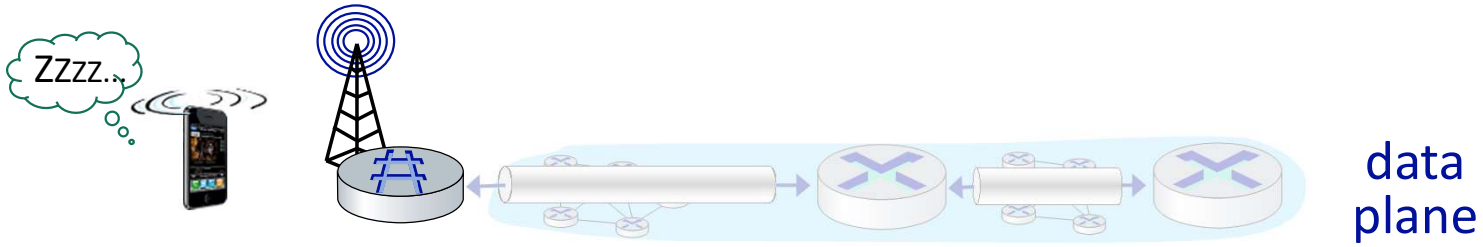
- downstream channel: combination of FDM and TDM within frequency channel (OFDM - orthogonal frequency division multiplexing)
  - "orthogonal": minimal interference between channels
- upstream: FDM, TDM similar to OFDM
- each active mobile device allocated two or more 0.5 ms time slots in or more channel frequencies
  - scheduling algorithm not standardized – up to operator
  - 100's Mbps per device possible

LTE data plane: associating with a BS



1. BS broadcasts primary synch signal every 5 ms on all frequencies
   - BSs from multiple carriers may be broadcasting synch signals
2. mobile finds a primary synch signal, then locates 2nd synch signal on this freq.
   - mobile then finds info broadcast by BS: channel bandwidth, configurations; BS's cellular carrier info
   - mobile may get info from multiple base stations, multiple cellular networks
3. mobile selects which BS to associate with (*e.g.,* preference for home carrier)
4. more steps still needed to authenticate, establish state, set up control plane

LTE mobiles: sleep modes



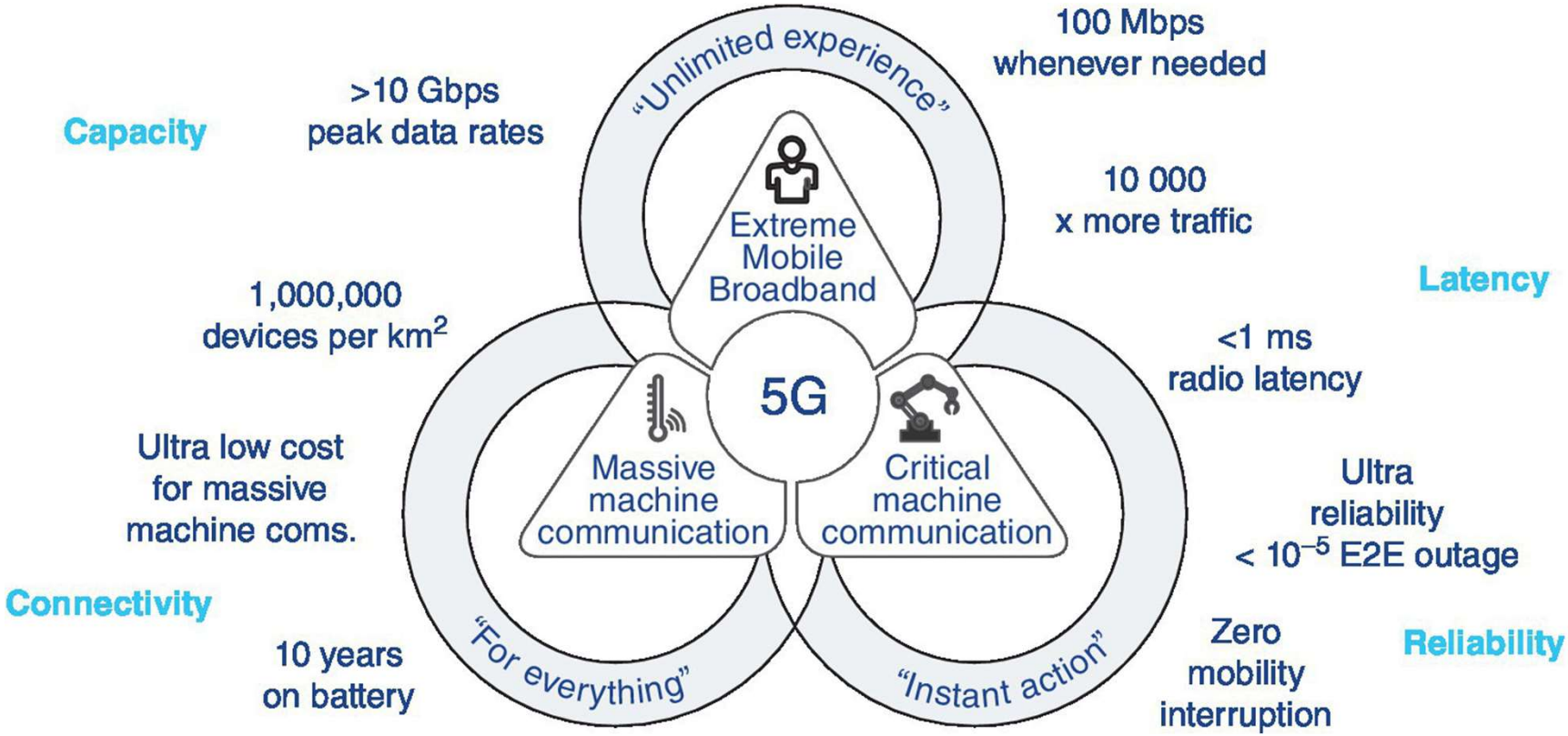
as in WiFi, Bluetooth: LTE mobile may put radio to "sleep" to conserve battery:

- light sleep: after 100's msec of inactivity
  - wake up periodically (100's msec) to check for downstream transmissions
- deep sleep: after 5-10 secs of inactivity
  - mobile may change cells while deep sleeping – need to re-establish association

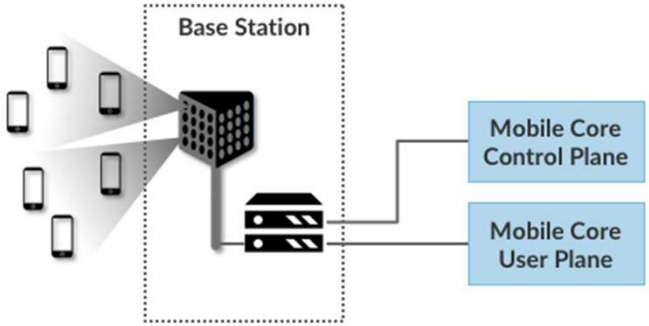
On to 5G!

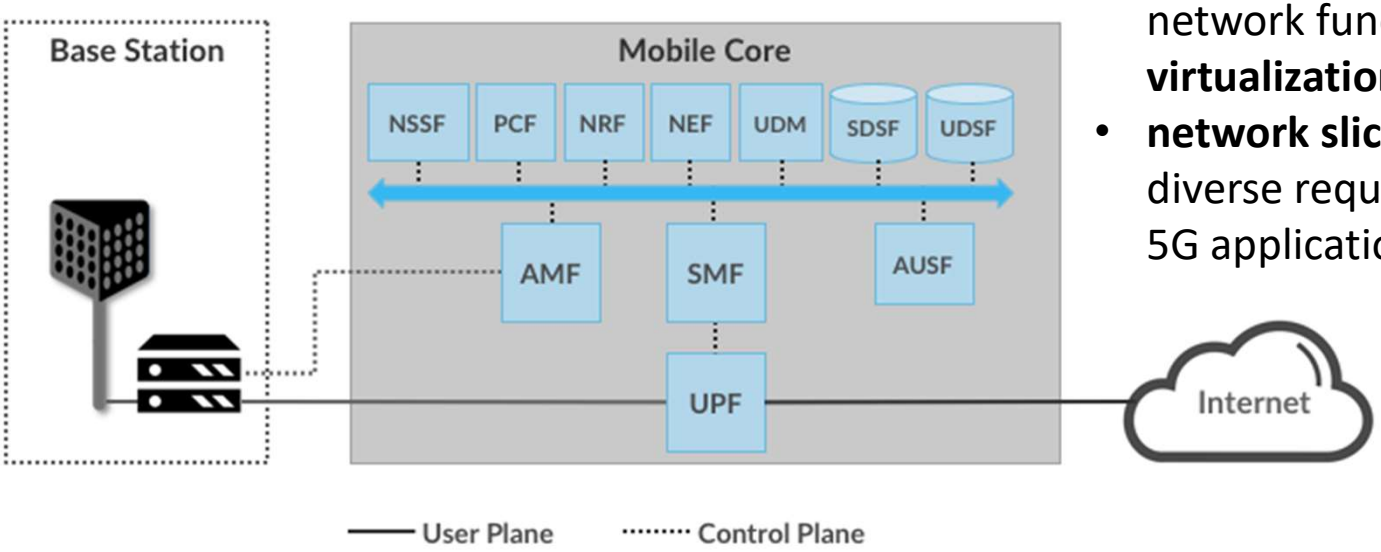
- goal: 10x increase in peak bitrate, 10x decrease in latency, 100x increase in traffic capacity over 4G
- 5G NR (new radio):
  - two frequency bands: FR1 (450 MHz–6 GHz) and FR2 (24 GHz–52 GHz): millimeter wave frequencies
  - not backwards-compatible with 4G
  - MIMO: multiple directional antennae
- millimeter wave frequencies: much higher data rates, but over shorter distances
  - pico-cells: cells diameters: 10-100 m
  - massive, dense deployment of new base stations required

5G use cases


"Unlimited experience"
100 Mbps
whenever needed
Capacity
>10 Gbps
peak data rates
Extreme
Mobile
Broadband
10 000
x more traffic
Latency
1,000,000
devices per km2
<1 ms
radio latency
5G
Massive
machine
communication
Critical
machine
communication
Ultra low cost
for massive
machine coms.
Ultra
reliability
< 10−5 E2E outage
Connectivity
10 years
on battery
"For everything"
"Instant action"
Zero
mobility
interruption
Reliability

5G Architecture





The 5G Core network

- redesigned to better integrate with the Internet and cloud-based services
- Complete control and user plane separation
- distributed servers and caches across the network to reduce latency
- Consists of virtualized software network functions (**network function virtualization**)
- **network slicing** to flexibly meet the diverse requirements of the different 5G applications

next lectures

5G Architecture - User Plane

UPF (User Plane Function)

- forwards traffic between RAN and the Internet, corresponding to the S/PGW combination in EPC. It also is responsible for:
  - Packet inspection & application detection
  - QoS management
  - traffic usage reporting
- flexibility to deliver user plane functionality at the edge as well as the network core.
  - UPF can be co-located with edge and central data centers at both locations
  - Multi-Access Edge Computing (MEC)

next lectures

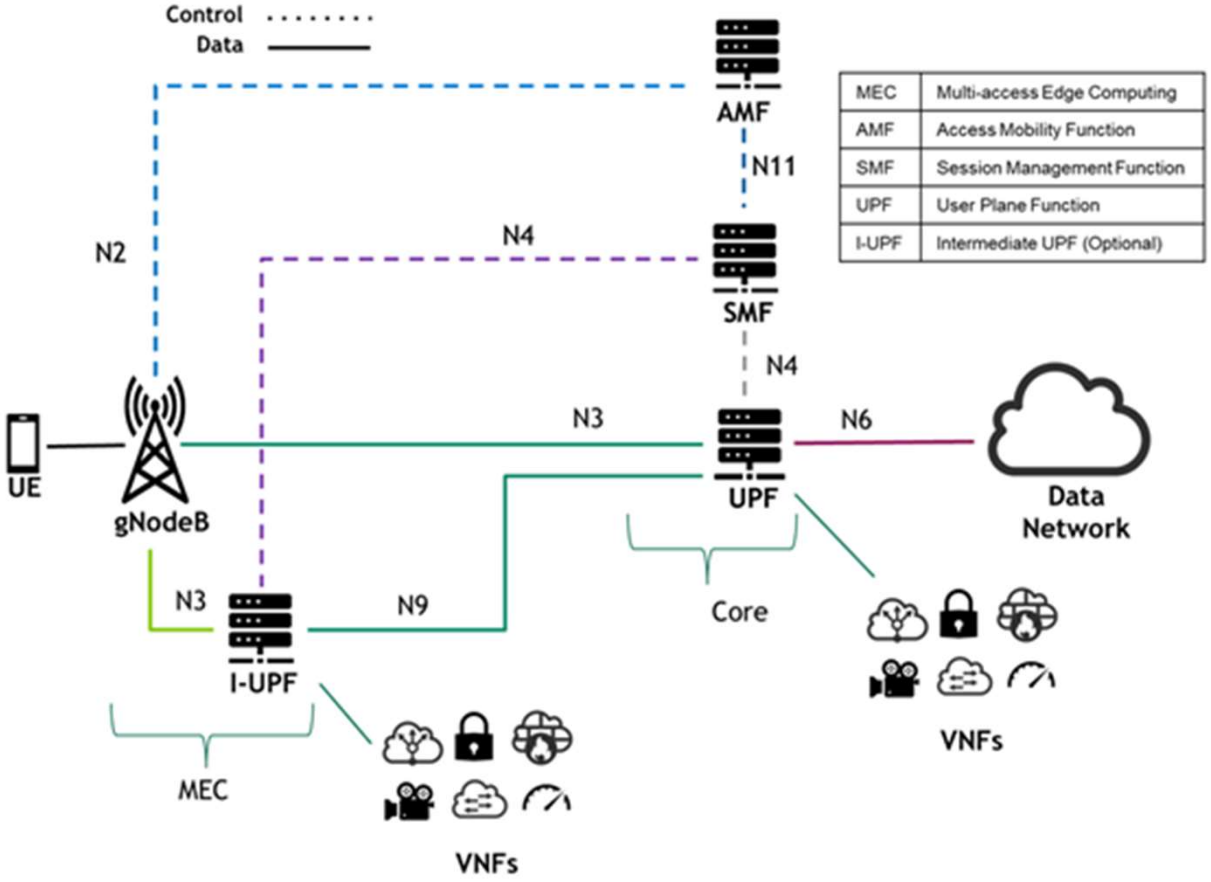
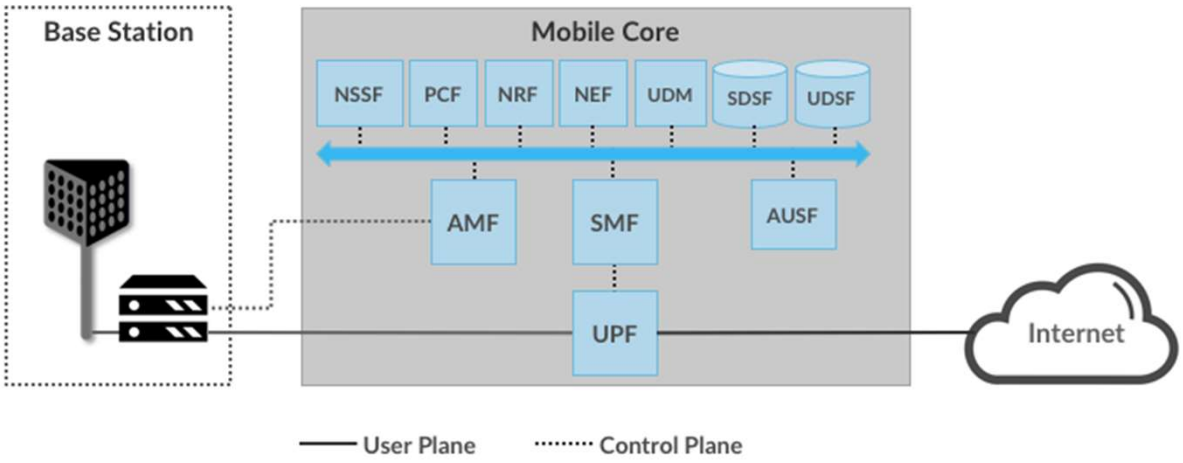


Image from: https://developer.nvidia.com/blog/accelerating-iva-using-ultra-efficient-5g-core-with-mavenir-and-nvidia-edge-ai/

5G Architecture - Control Plane

(inheriting from 4G)

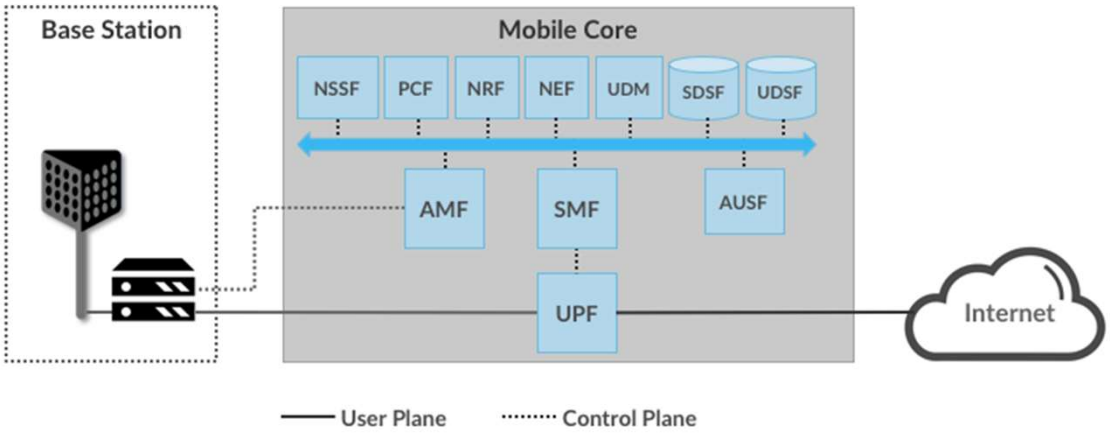
- AMF (Core Access and Mobility Management Function): connection and reachability management, mobility management, access authentication and authorization, and location services ->MME
- SMF (Session Management Function): manages each UE session, including IP address allocation, selection of associated UP function, control aspects of QoS, and control aspects of UP routing. -> MME and the control-related aspects of PGW.
- PCF (Policy Control Function): manages the policy rules that other CP functions then enforce. -> PCRF.
- UDM (Unified Data Management): Manages user identity, including the generation of authentication credentials. -> HSS.
- AUSF (Authentication Server Function): Essentially an authentication server. -> HSS.



5G Architecture - Control Plane

Control Plane (not existing in from 4G)

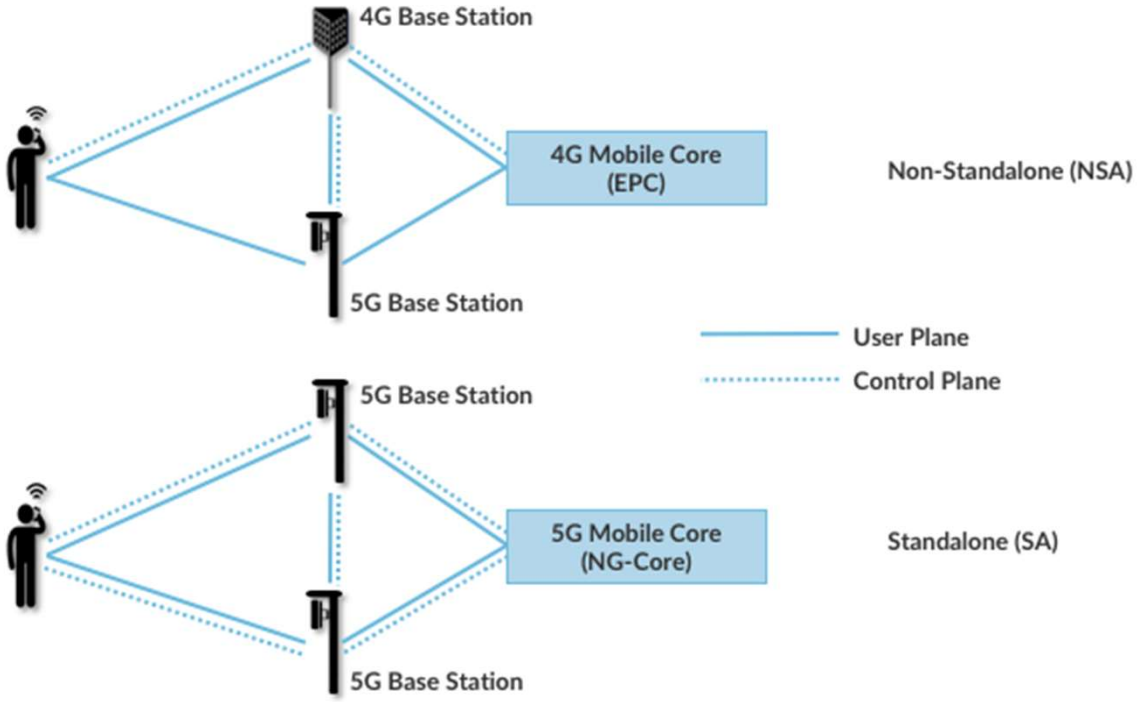
- SDSF (Structured Data Storage Network Function): a “helper” service used to store structured data.
- UDSF (Unstructured Data Storage Network Function): A “helper” service used to store unstructured data.
- NEF (Network Exposure Function): A means to expose select capabilities to third-party services
- NRF (NF Repository Function): A means to discover available services.
- NSSF (Network Slicing Selector Function): A means to select a Network Slice to serve a given UE. Network slices are essentially a way to partition network resources in order to differentiate service given to different users.



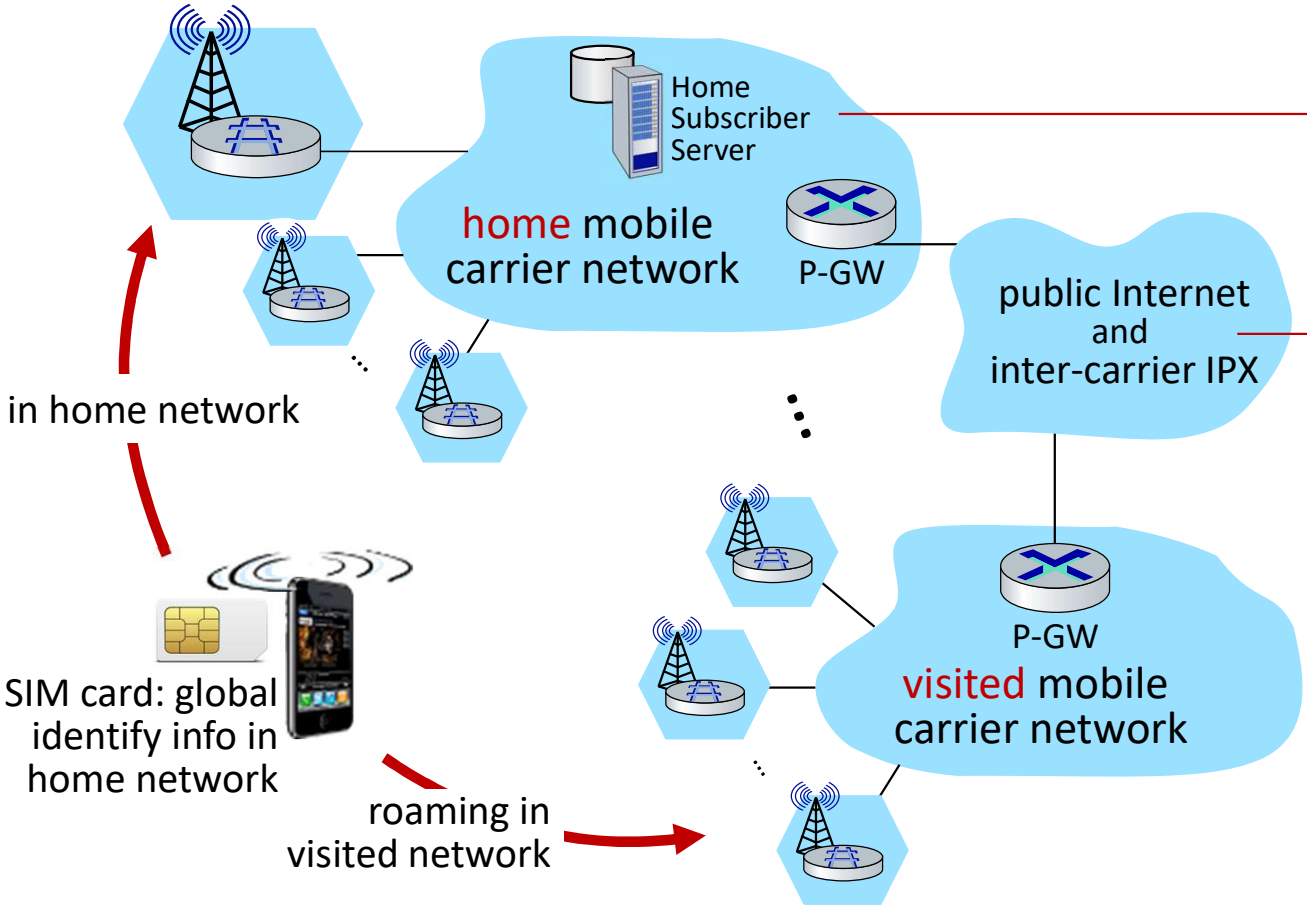
- cloud native solution
- distinct storage services means that all the other services can be stateless, and hence, more readily scalable.

Deployment Options

- Standalone 4G / Stand-Alone 5G
- Non-Standalone (4G+5G RAN) over 4G's EPC
  - 5G base stations being deployed alongside the existing 4G base stations in a given geography to provide a data-rate and capacity boost.
  - In NSA, control plane traffic between the user equipment and the 4G Mobile Core utilizes (i.e., is forwarded through) 4G base stations, and the 5G base stations are used only to carry user traffic
- Non-Standalone (4G+5G RAN) over 5G's NG-Core



Global cellular network: a network of IP networks



home network HSS:

- identify & services info, while in home network and roaming

all IP:

- carriers interconnect with each other, and public internet at exchange points
- legacy 2G, 3G: not all IP, handled otherwise