



南京大學

NANJING UNIVERSITY

# 无线网络和移动网络



# Outline

---

- Introduction
- Wireless
  - Wireless Links and network characteristics
  - CDMA: code division multiple access
  - WiFi: 802.11 wireless LANs
  - Cellular networks: 4G and 5G
- Mobility
  - Mobility management: principles
  - Mobility management: practice
  - Mobility: impact on higher-layer protocols





# 4G/5G cellular networks

---

- the solution for wide-area mobile Internet
- widespread deployment/use:
  - more mobile-broadband-connected devices than fixed-broadband-connected devices (5-1 in 2019)!
  - 4G availability: 97% of time in Korea (90% in US)
- transmission rates up to 100's Mbps
- technical standards: 3rd Generation Partnership Project (3GPP)
  - [www.3gpp.org](http://www.3gpp.org)
  - 4G: Long-Term Evolution (LTE) standard





# 4G/5G cellular networks

## similarities to wired Internet

- edge/core distinction, but both belong 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 1<sup>st</sup> 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



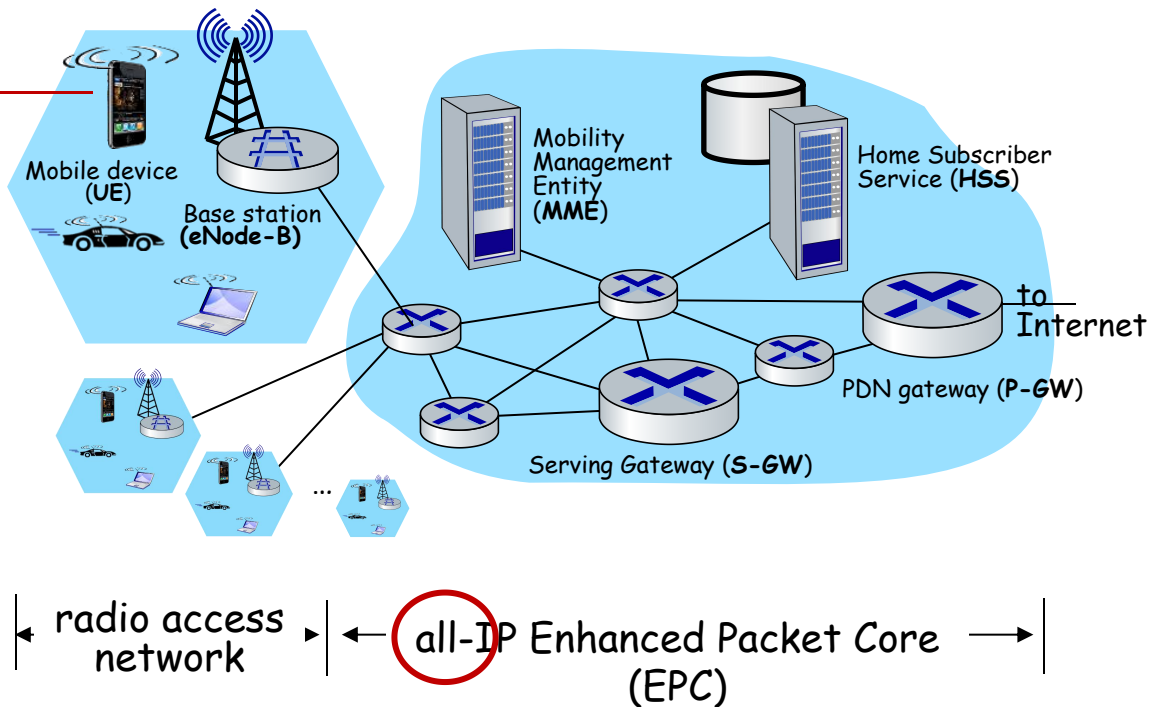




# Elements of 4G LTE architecture

## 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)

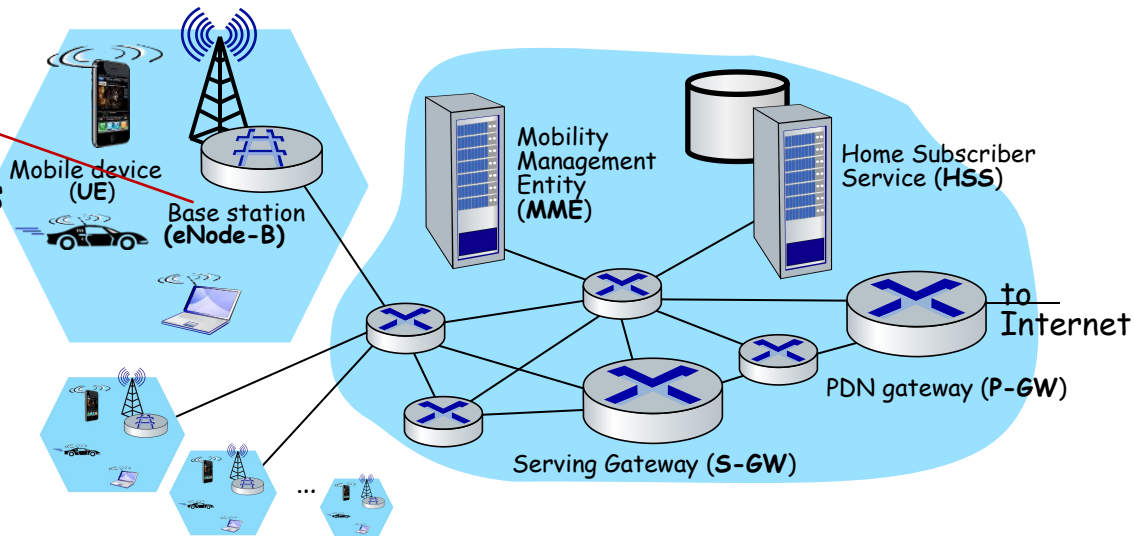




# Elements of 4G LTE architecture

## Base station:

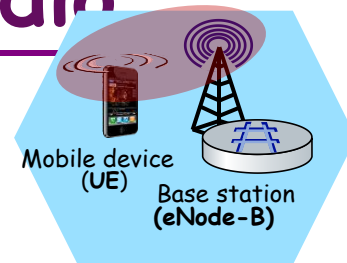
- at “edge” of carrier’s network
- manages wireless radio resources, mobile devices in its coverage area (“cell”)
- coordinates device authentication with other elements
- similar to WiFi AP but:
  - active role in user mobility
  - coordinates with nearby base stations to optimize radio use
- LTE jargon: eNode-B





# Radio Access Network: 4G radio

- connects device (UE) to a base station (eNode-B)
  - multiple devices connected to each base station
- many different possible frequencies bands, multiple channels in each band
  - popular bands: 600, 700, 850, 1500, 1700, 1900, 2100, 2600, 3500 MHz
  - separate upstream and downstream channels
- sharing 4G radio channel among users:
  - **OFDM**: Orthogonal Frequency Division Multiplexing
  - combination of FDM, TDM
- 100's Mbps possible per user/device





# UNITED STATES FREQUENCY ALLOCATIONS

## THE RADIO SPECTRUM

# Spectrum

### RADIO SERVICES COLOR LEGEND



ACTIVITY CODE

 FEDERAL EXCLUSIVE  FEDERAL/NON-FEDERAL SHARED

 NON-FEDERAL EXCLUSIVE

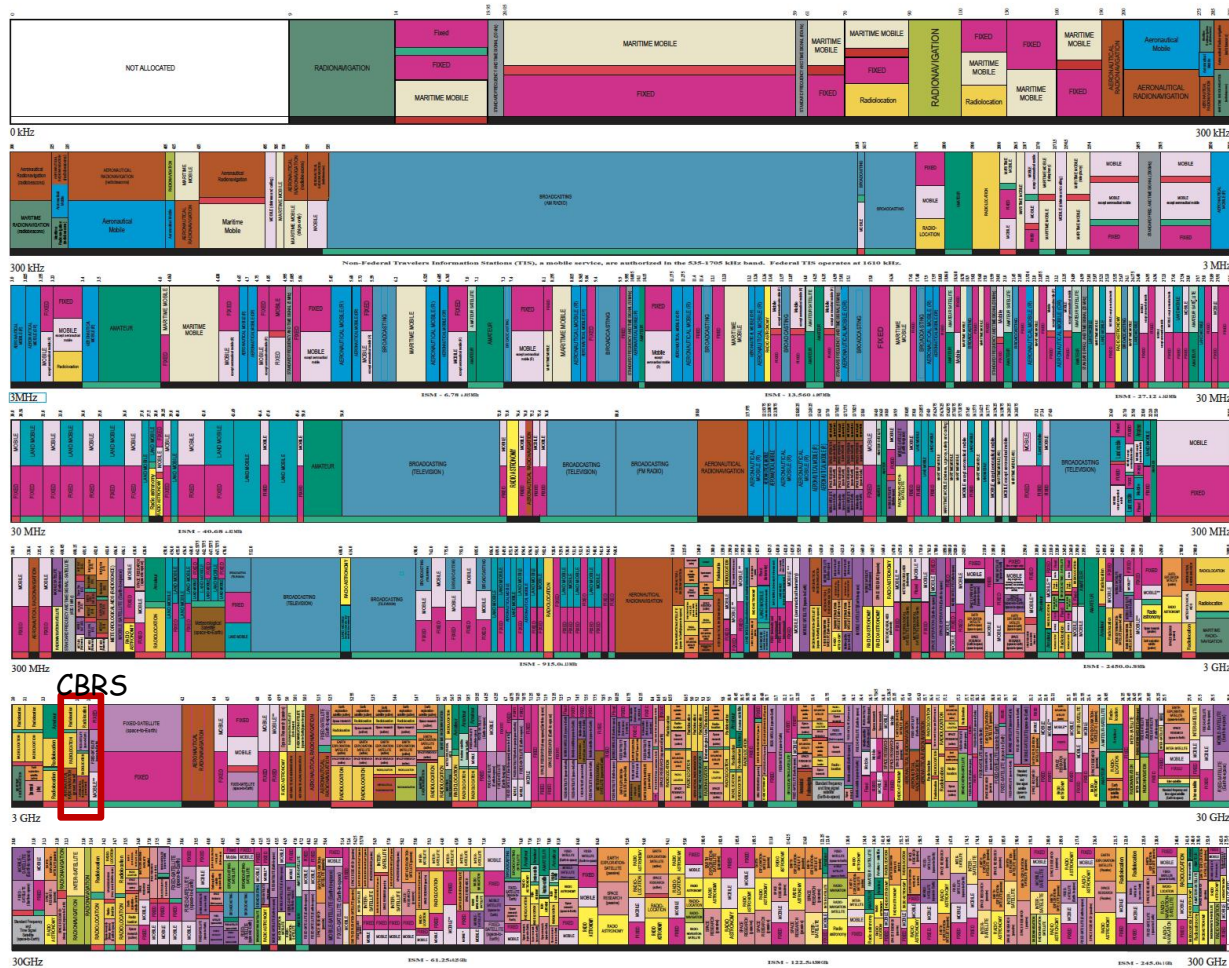
## ALLOCATION USAGE DESIGNATION

SERVICE	EXAMPLE	DESCRIPTION
Primary	FIXED	Capital Letters
Secondary	Mobile	1st Capital with lower case letters

This chart is a graphic single-point-in-time portrayal of the Table of Frequency Allocations used by the FCC and NTIA. As such, it may not completely reflect all aspects, i.e. footnotes and recent changes made to the Table of Frequency Allocations. Therefore, for complete information, users should consult the Table to determine the current status of each allocation.

 U.S. DEPARTMENT OF COMMERCE  
National Telecommunications and Information Administration  
Office of Spectrum Management  
JANUARY 2016

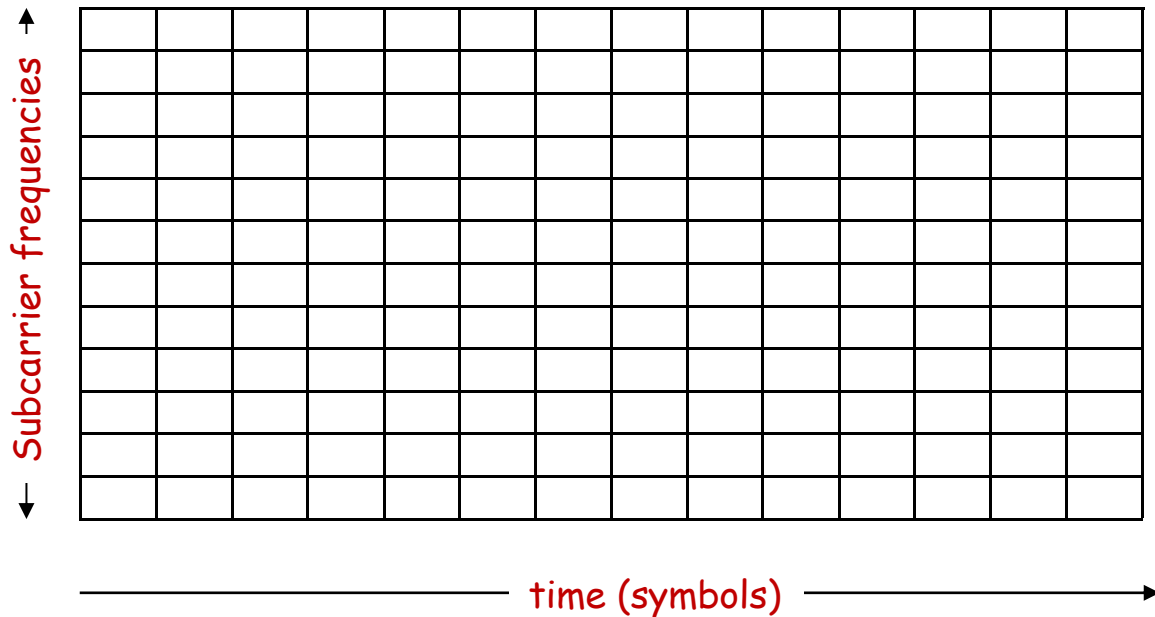
For sale by the Superintendent of Documents, U.S. Government Printing Office  
 Federal Acquisition Regulation, Revised May 2005, Washington, DC 20540-7001  
 GPO : 2005 : 569-100/1-50000-1000 : 2005 : 569-100/1-50000-1000 : 2005 : 569-100/1-50000-1000



PLEASE NOTE: THE SPACING ALLOTTED THE SERVICES IN THE SPECTRUM SEGMENTS SHOWN IS NOT PROPORTIONAL TO THE ACTUAL AMOUNT OF SPECTRUM OCCUPIED.



# OFDMA: time division (LTE)

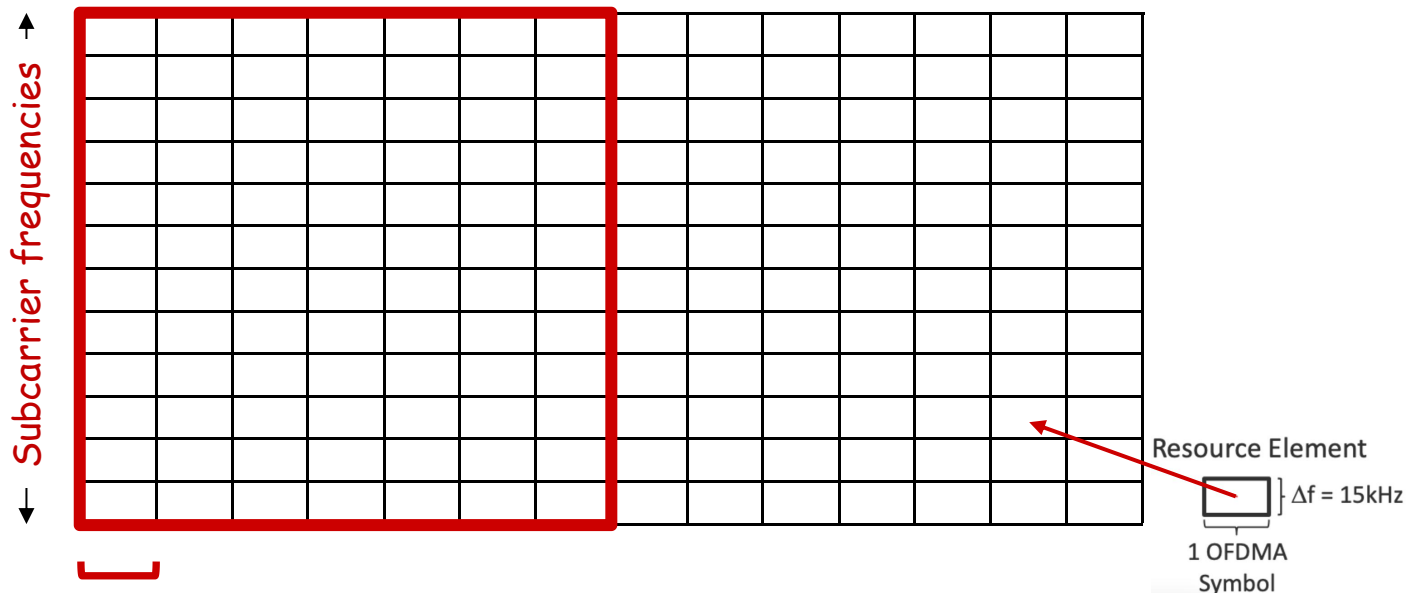




# OFDMA: time division (LTE)

Physical Resource Block (PRB ): blocks of  $7 \times 12 = 84$  resource elements

- unit of transmission scheduling



time to transmit one OFDM symbol on subcarrier frequency






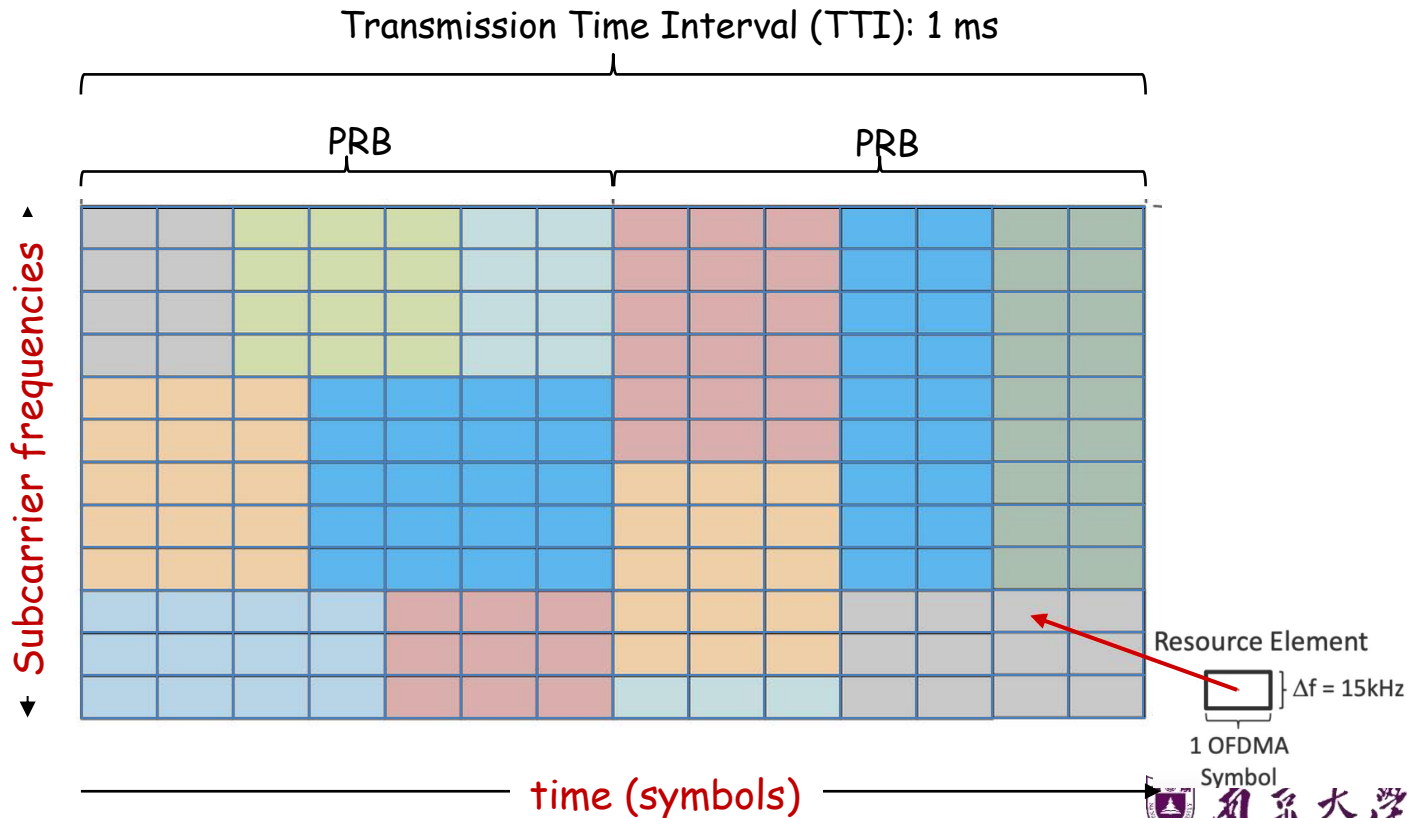


# OFDMA

## Transmission scheduling example:

- Send to 7 UEs in 7 blocks of REs in one PRB

UE<sub>1</sub>   
UE<sub>2</sub>   
UE<sub>3</sub>   
UE<sub>4</sub>   
UE<sub>5</sub>   
UE<sub>6</sub>   
UE<sub>7</sub> 



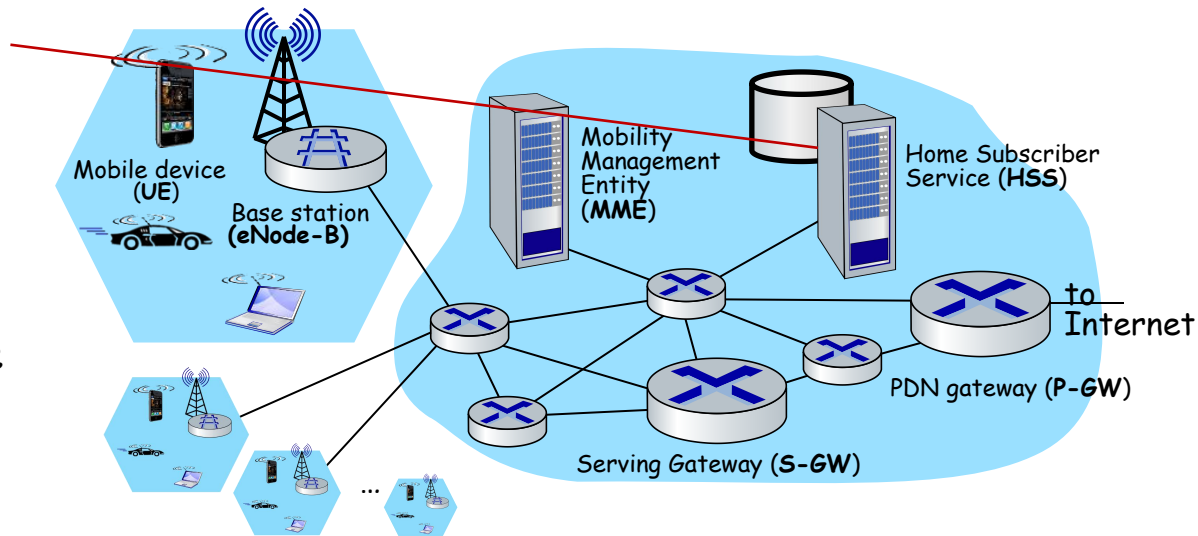




# Elements of 4G LTE architecture

## Home Subscriber Service

- stores info about mobile devices for which the HSS's network is their "home network"
- works with MME in device authentication



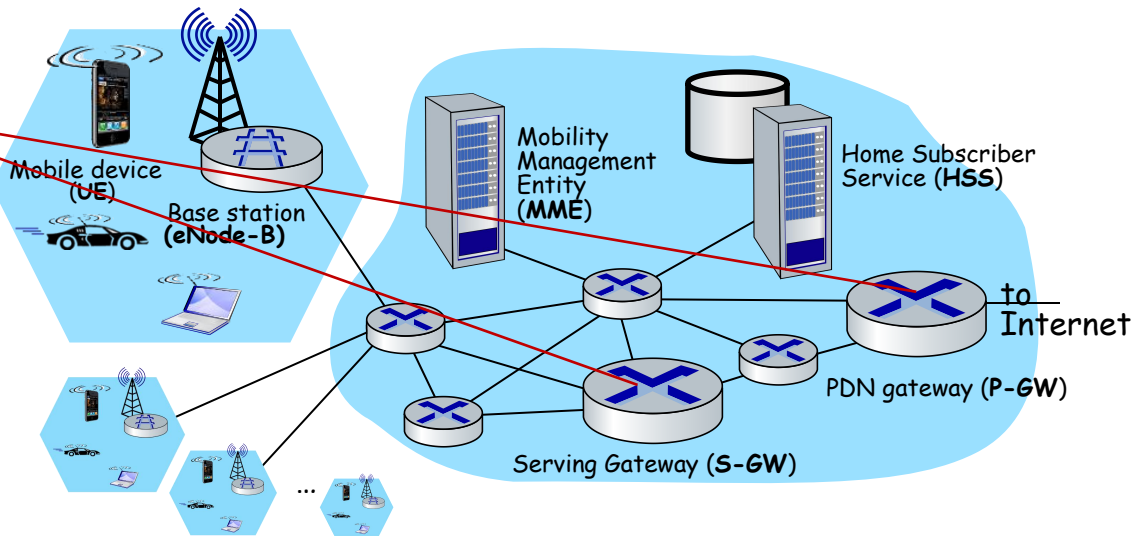




# Elements of 4G LTE architecture

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

- lie on data path from mobile to/from Internet
- P-GW
  - gateway to mobile cellular network
  - Looks like any other internet gateway router
  - provides NAT services
- other routers:
  - extensive use of tunneling

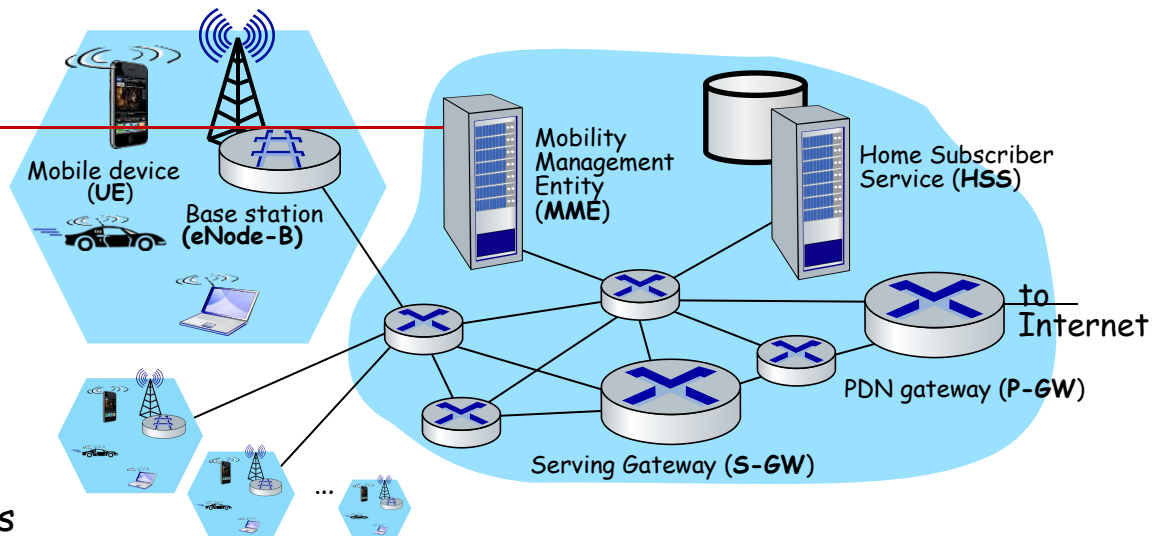




# Elements of 4G LTE architecture

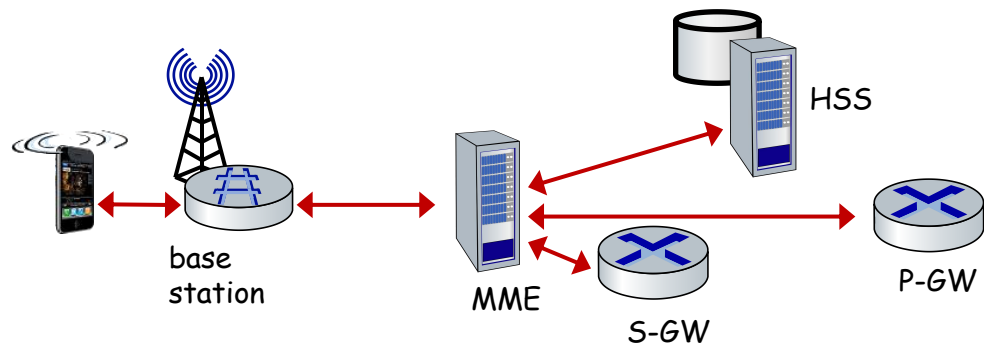
## Mobility Management Entity

- 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



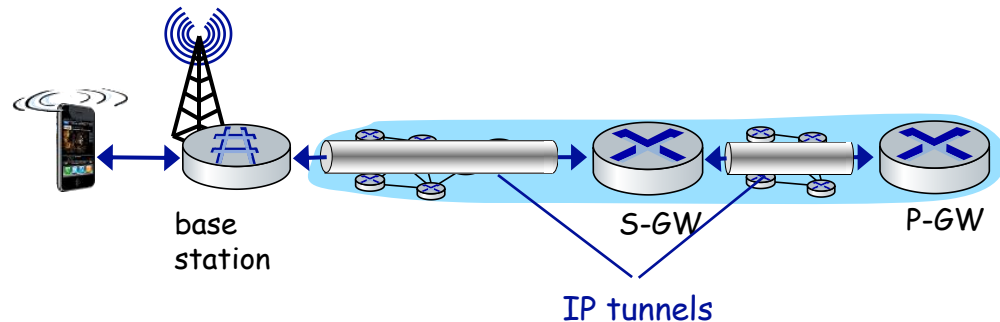


# LTE: data plane control plane separation



## control plane

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



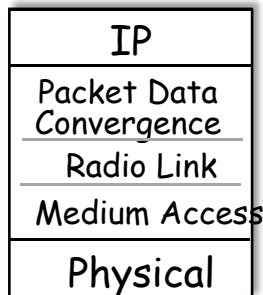
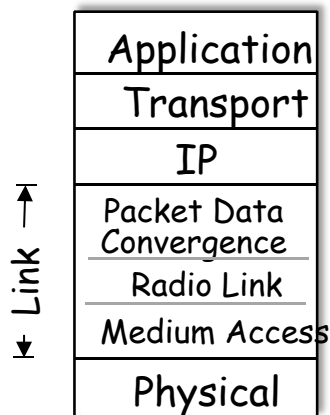
## data plane

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



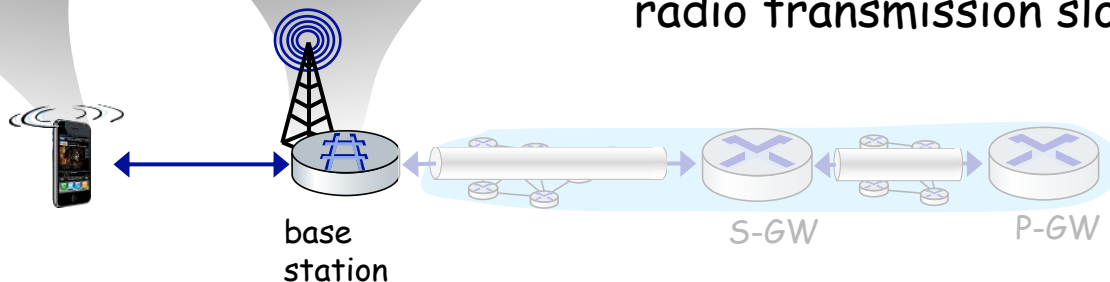


# LTE data plane protocol stack: first hop



## LTE link layer protocols:

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



data  
plane

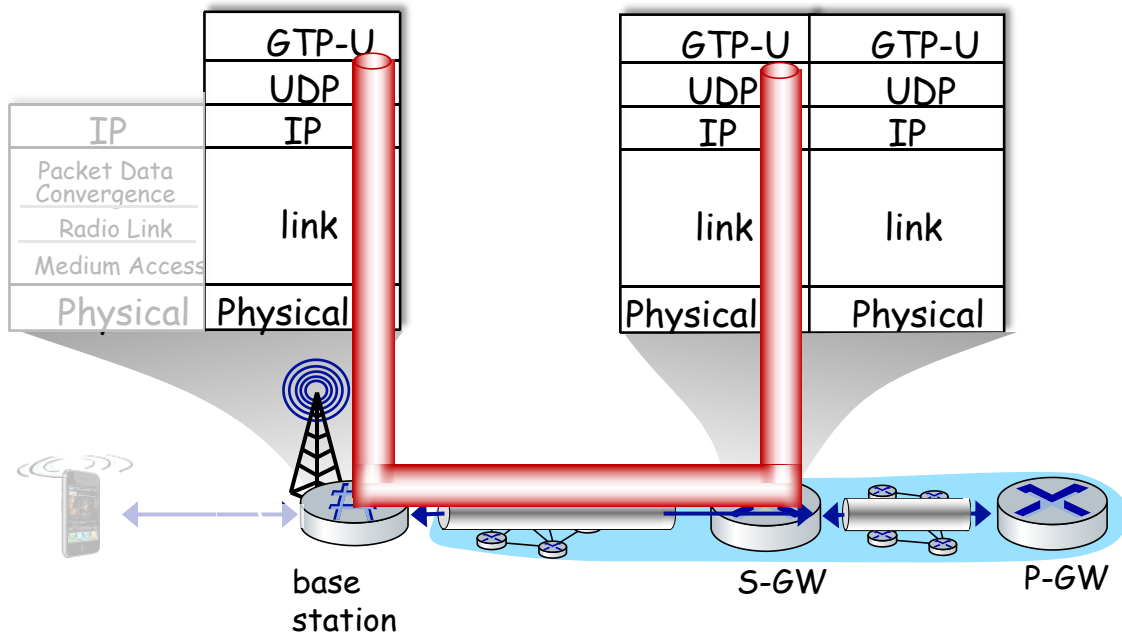




# LTE data plane protocol stack: packet core

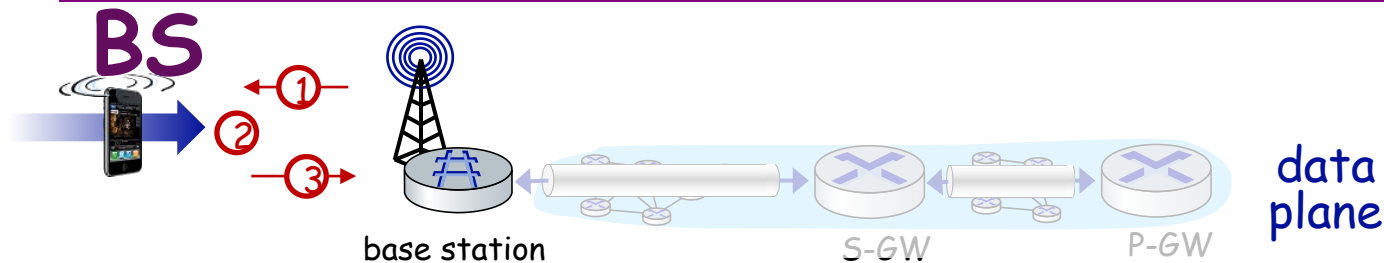
## tunneling:

- 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: associating with a

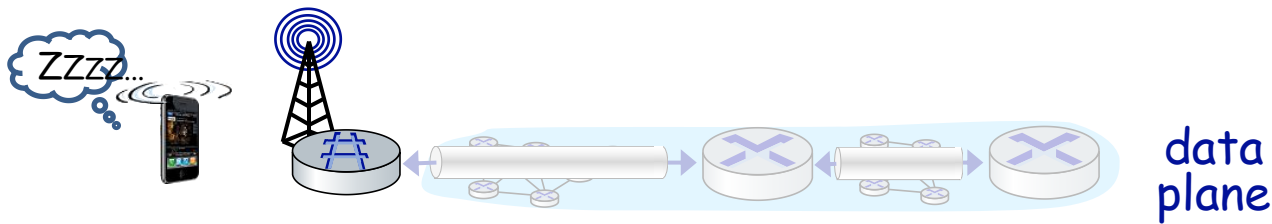


- ① BS broadcasts primary synch signal every 5 ms on all frequencies
  - BSs from multiple carriers may be broadcasting synch signals
- ② mobile finds a primary synch signal, then locates 2<sup>nd</sup> synch signal on this freq.
  - mobile then finds info broadcast by BS: channel bandwidth, configurations; 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 data plane





# LTE mobiles: sleep modes



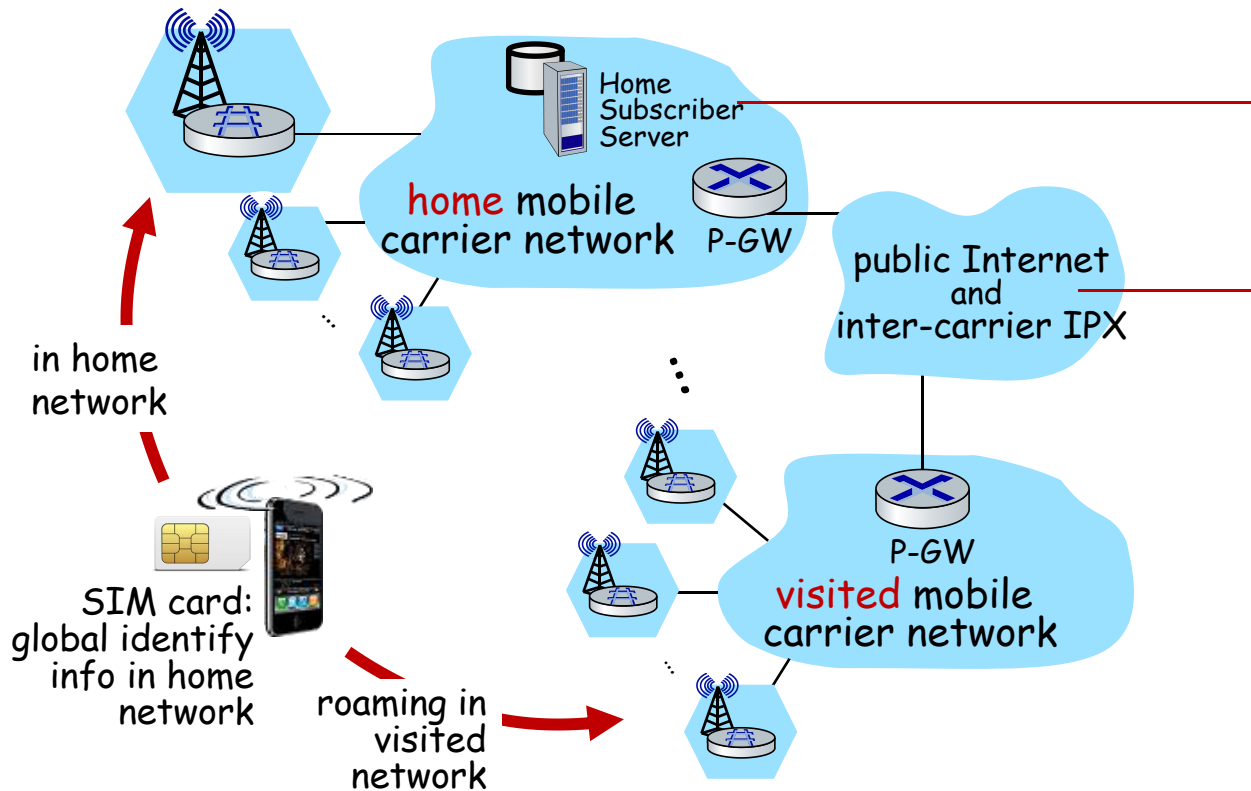
as in WiFi, Bluetooth: LTE mobile may put radio to “sleep” to conserve battery:

- **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





# Global cellular network: a network of IP networks



## home network HSS:

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

## all IP:

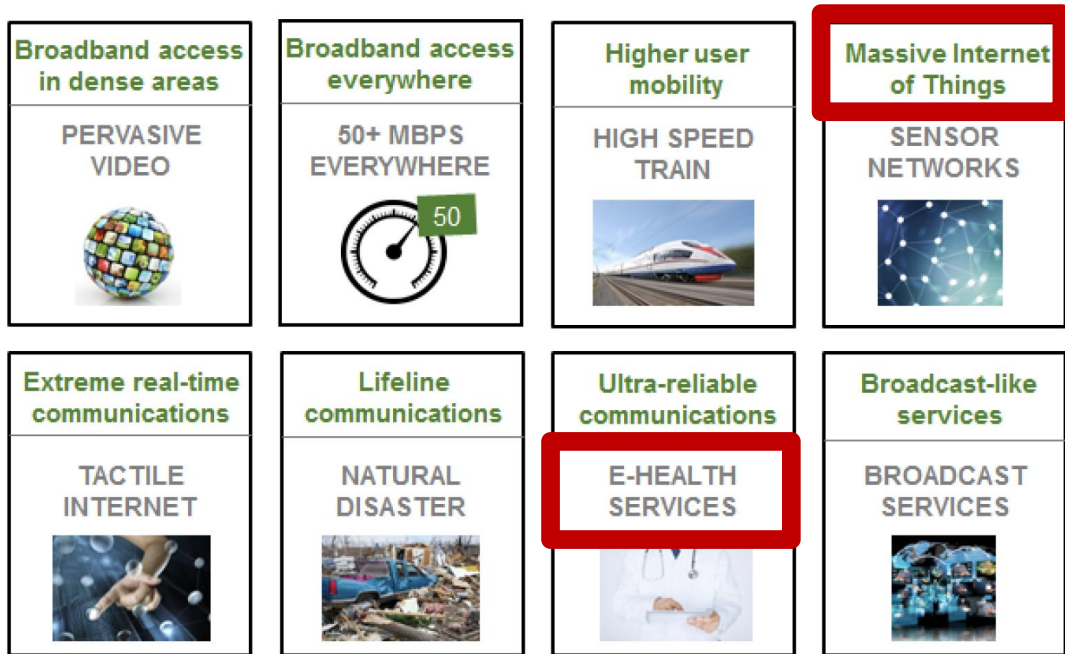
- carriers interconnect with each other, and public internet at exchange points
- legacy 2G, 3G: not all IP, handled otherwise







# On to 5G: motivation



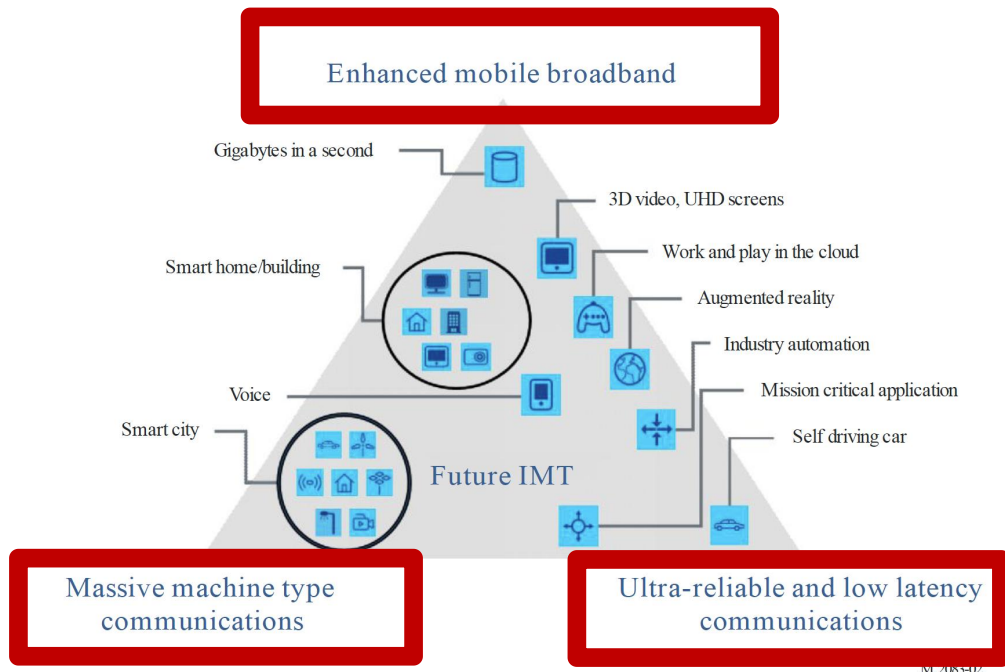
From Next Generation Mobile Networks (NGMS) alliance: 2020 white paper

Hype/wishes need to be separated from reality or likely nearer-term reality





# On to 5G: motivation



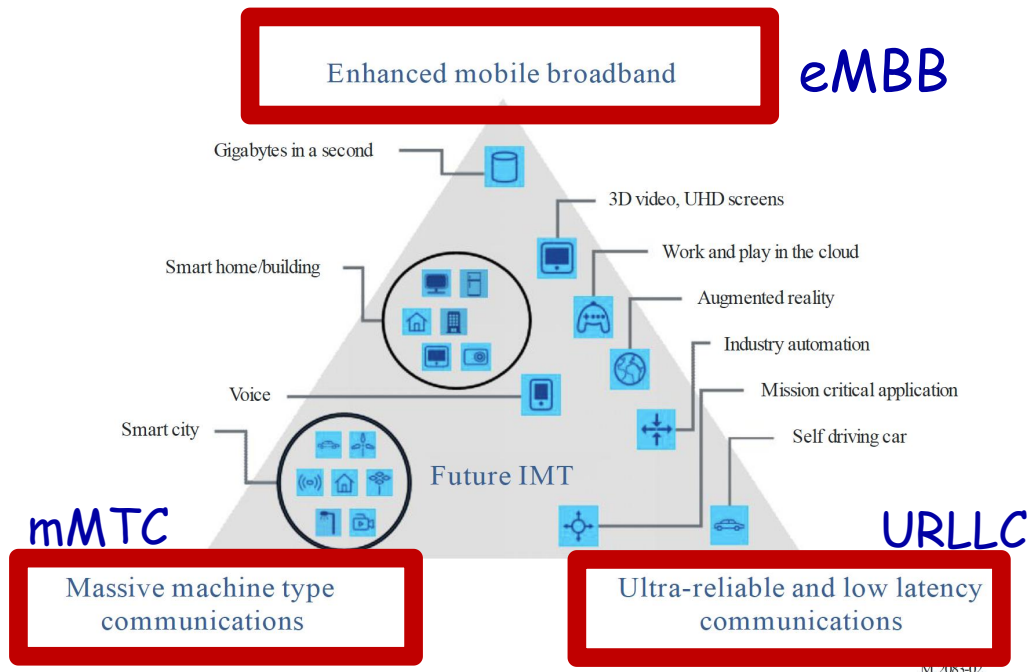
"initial standards and launches have mostly focused on **enhanced Mobile Broadband**, 5G is expected to increasingly enable new business models and countless new use cases, in particular those of **massive Machine Type Communications** and **Ultra-reliable and Low Latency Communications**."

Figure: from Recommendation ITU-R M.2083-0 (2015)





# On to 5G: motivation



## Industry verticals:

- Manufacturing
- Constructions
- Transport
- Health
- Smart communities
- Education
- Tourism
- Agriculture
- Finance

K. Schwab, "The Fourth Industrial Revolution," World Economic Forum.



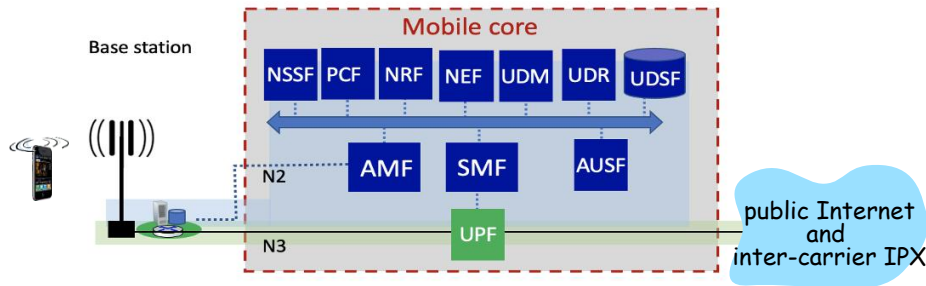
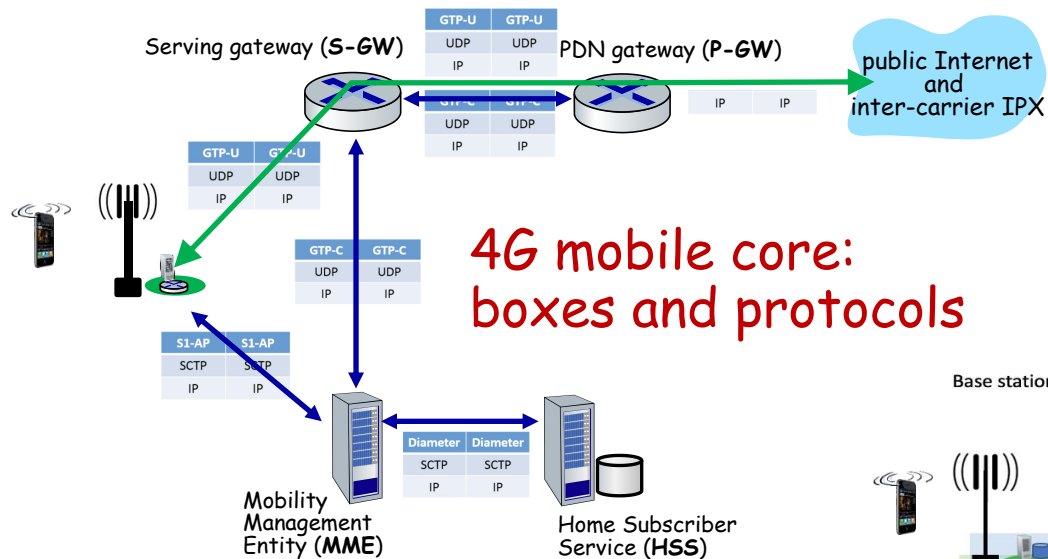
# On to 5G: Radio

- **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



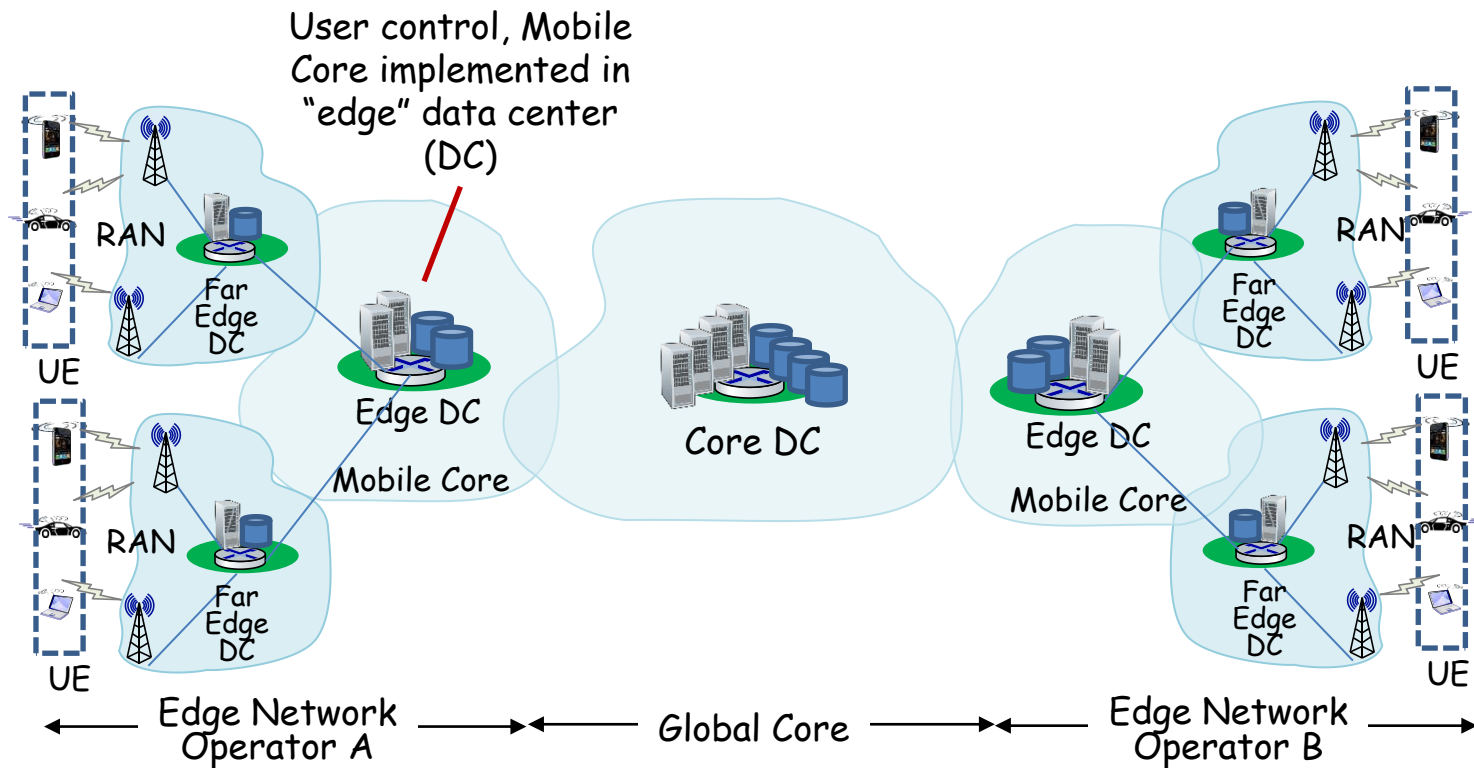


# On to 5G: SDN-like architecture



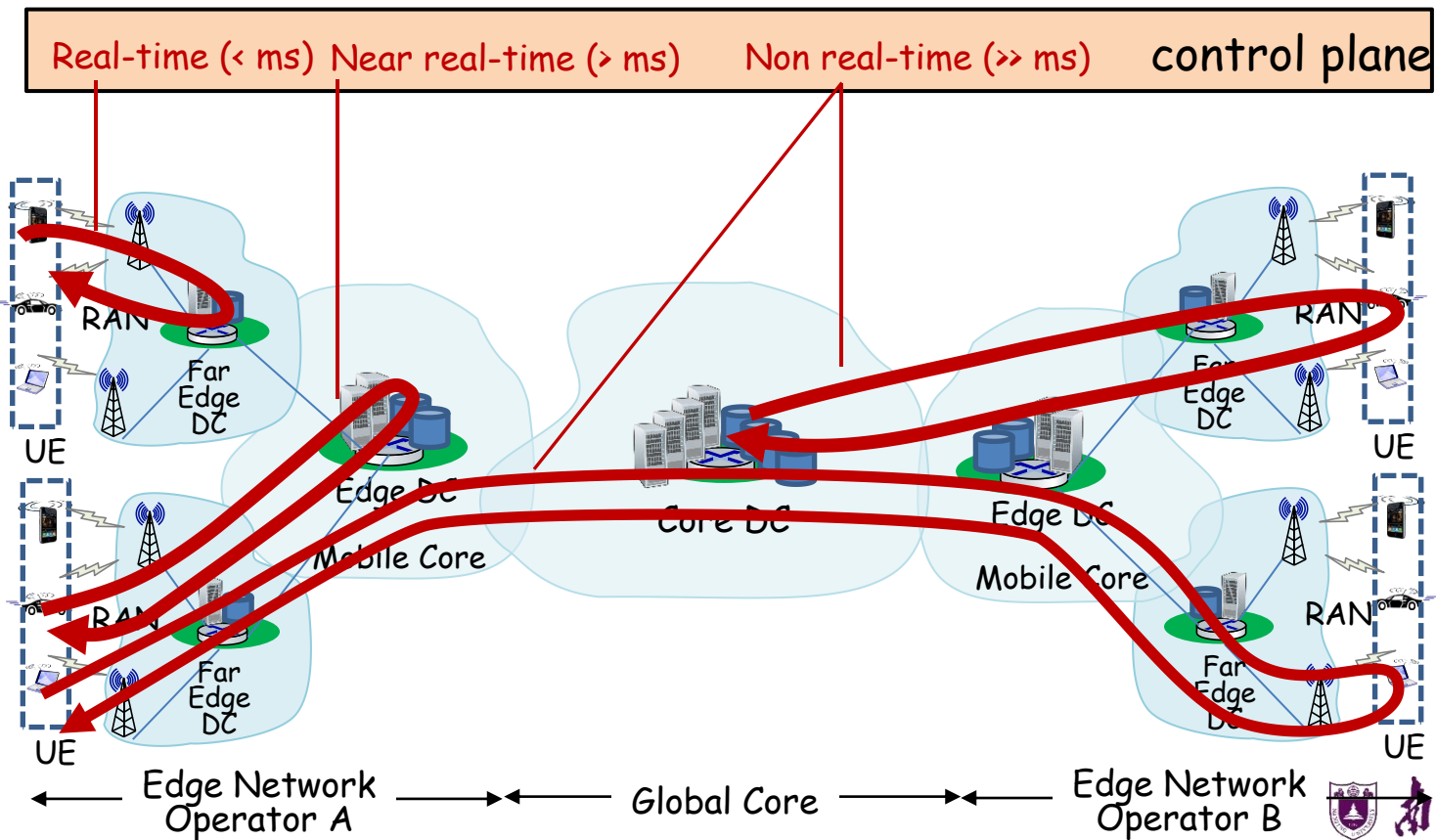


# Functional elements: communication, computation, data





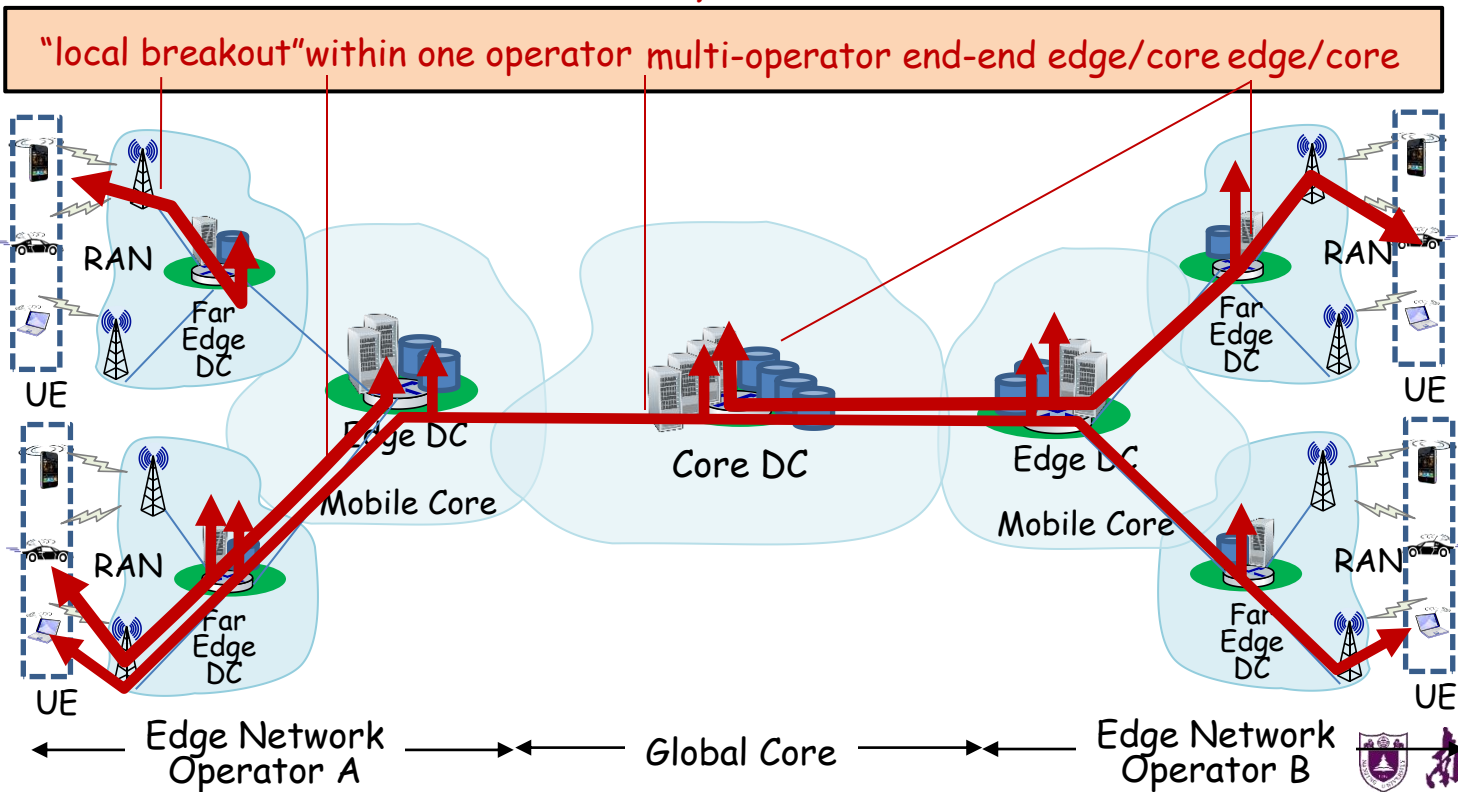
# Control plane: resource control





# User plane: resources, as used by users (application)

*User plane*







# On beyond 5G?

---

- "6G" not obviously next: "NextG" and "Beyond 5G" heard more often than "6G"
- 5G on an evolutionary path (like the Internet)
  - **agility**: cloud technologies (SDN) mean new features can be introduced rapidly, deployed continuously
  - **customization**: change can be introduced bottom-up (e.g., by enterprises and edge cloud partners with Private 5G)
    - ✓ No need to wait for standardization
    - ✓ No need to reach agreement (among all incumbent stakeholders)





# Outline

---

- Introduction
- Wireless
  - Wireless Links and network characteristics
  - CDMA: code division multiple access
  - WiFi: 802.11 wireless LANs
  - Cellular networks: 4G and 5G
- Mobility
  - Mobility management: principles
  - Mobility management: practice
  - Mobility: impact on higher-layer protocols





# What is mobility?

- spectrum of mobility, from the **network** perspective:

no mobility

high mobility



device moves  
between  
networks, but  
powers down  
while moving

device moves  
within same AP  
in  
one provider  
network

device moves  
among APs in  
one provider  
network

device moves  
among multiple  
provider networks,  
while maintaining  
ongoing  
connections

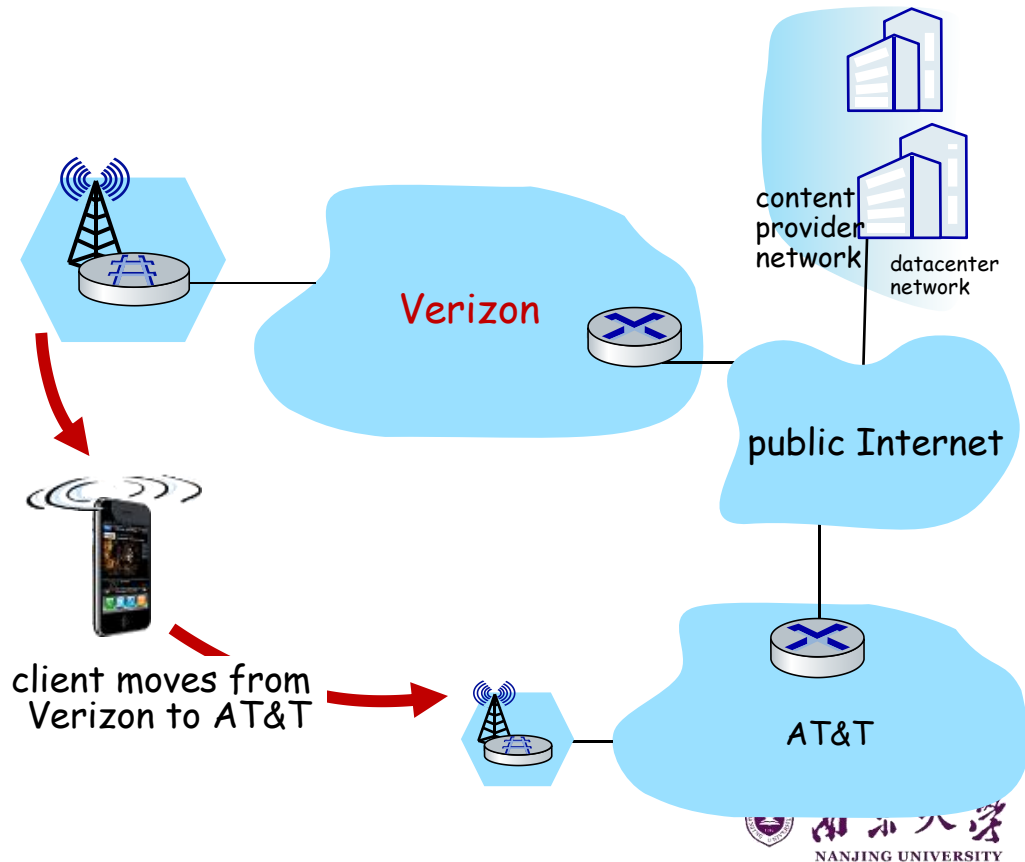
We're interested in these!



# Mobility challenge:

If a device moves from one network another:

- How will the "network" know to forward packets to the new network?





# Mobility approaches

---

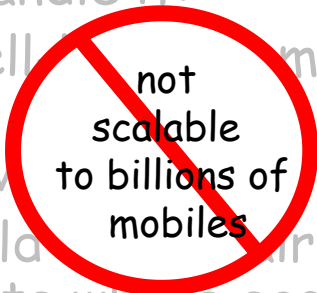
- let network (routers) handle it:
  - routers advertise well-known name, address (e.g., permanent 32-bit IP address), or number (e.g., cell #) of visiting mobile node via usual routing table exchange
  - Internet routing could do this already with no changes! Routing tables indicate where each mobile located via longest prefix match!





# Mobility approaches

- let network (routers) handle it:
  - routers advertise well known home address (e.g., permanent 32-bit IP) and foreign address (e.g., cell #) of visiting mobile node via routing table exchange
  - Internet routing could be used already *with no changes!* Routing tables indicate where each mobile located via longest prefix match!
- **let end-systems handle it:** functionality at the “edge”
  - **indirect routing:** communication from correspondent to mobile goes through home network, then forwarded to remote mobile
  - **direct routing:** correspondent gets foreign address of mobile, send directly to mobile





# Contacting a mobile friend:

Consider friend frequently changing locations, how do you find him/her?

- search all phone books?
- expect her to let you know where he/she is?

- call his/her parents?
- Facebook!

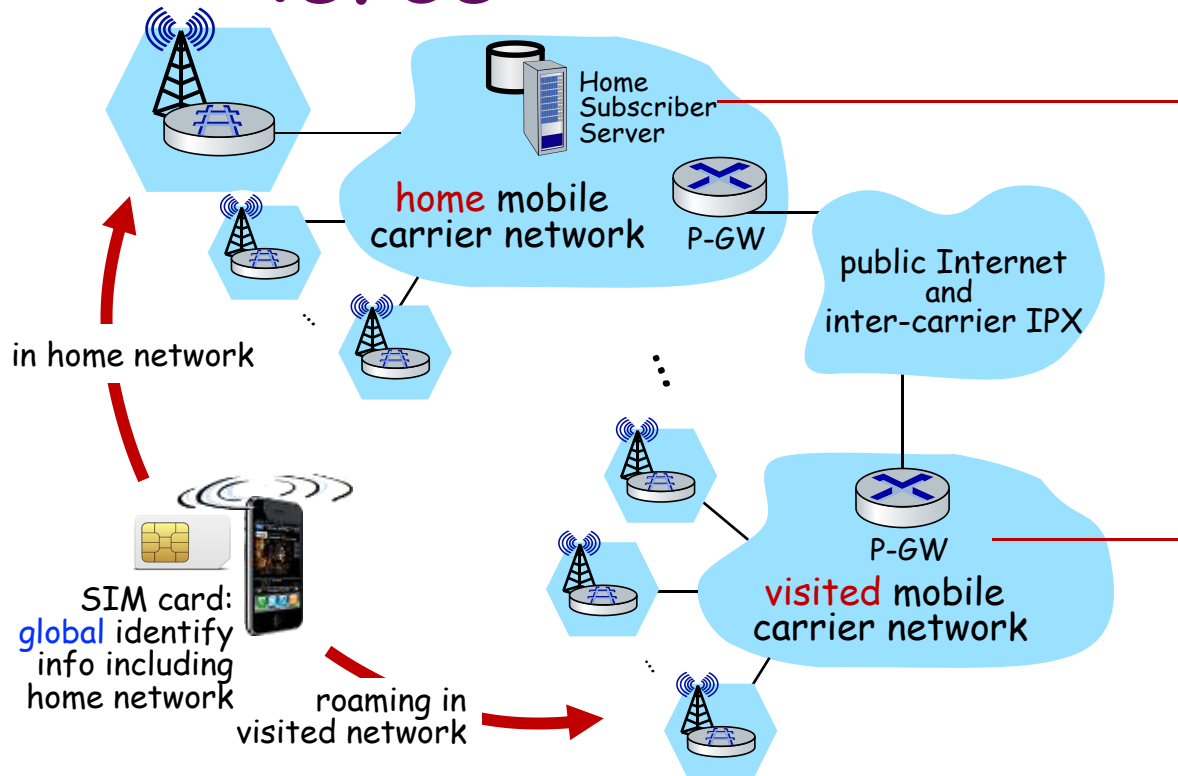
The importance of having a "home":

- a definitive source of information about you
- a place where people can find out where you are





# Home network, visited network: 4G/5G



## home network:

- (paid) service plan with cellular provider, e.g., Verizon, Orange
- home network HSS stores identify & services info

## visited network:

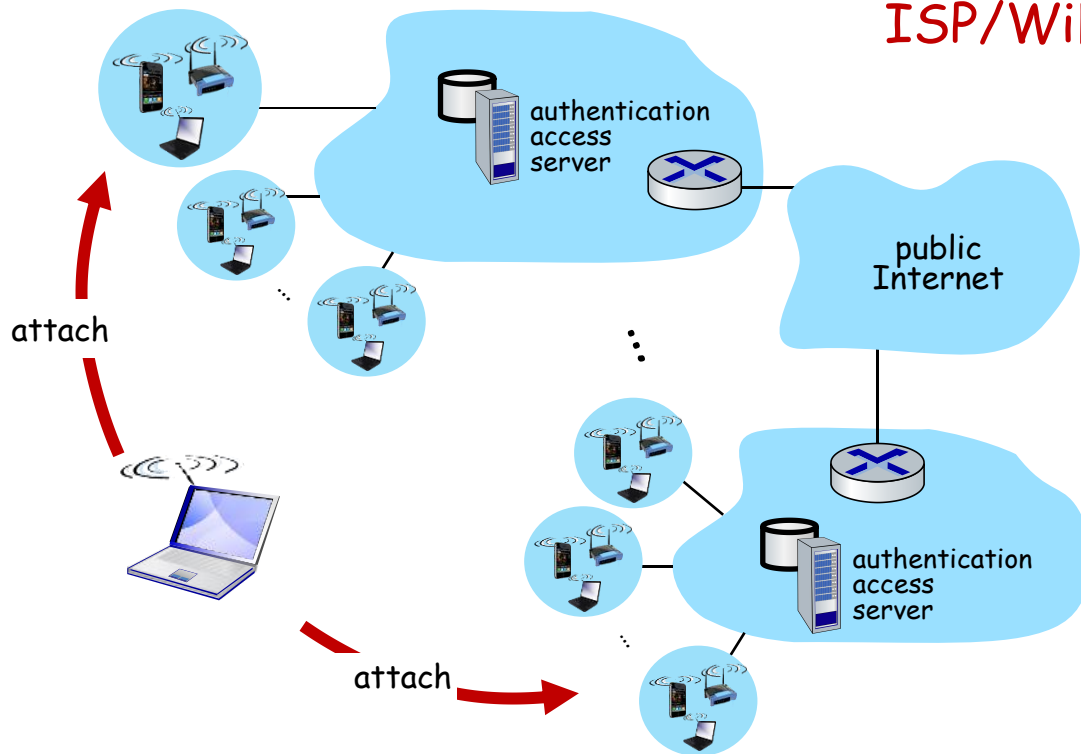
- any network other than your home network
- service agreement with other networks: to provide access to visiting mobile







# Home network, visited network: ISP/WiFi



ISP/WiFi: no notion of global "home"

- credentials from ISP (e.g., username, password) stored on device or with user
- ISPs may have national, international presence
- different networks: different credentials
  - some exceptions (e.g., eduroam)
  - architectures exist (mobile IP) for 4G-like mobility, but not used

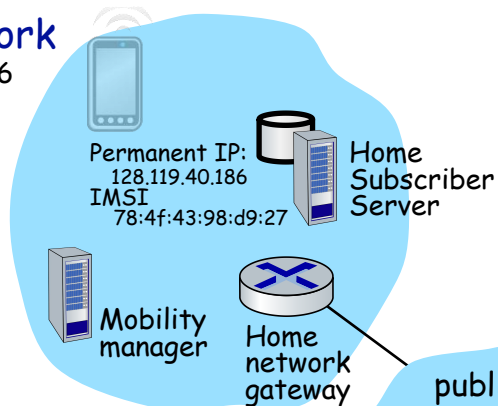




# Home network, visited network: generic

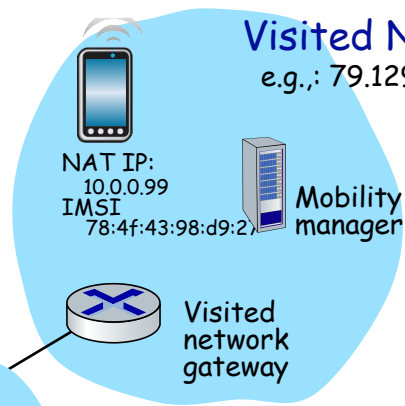
Home Network

e.g.: 128.119/16



Visited Network

e.g.: 79.129/16



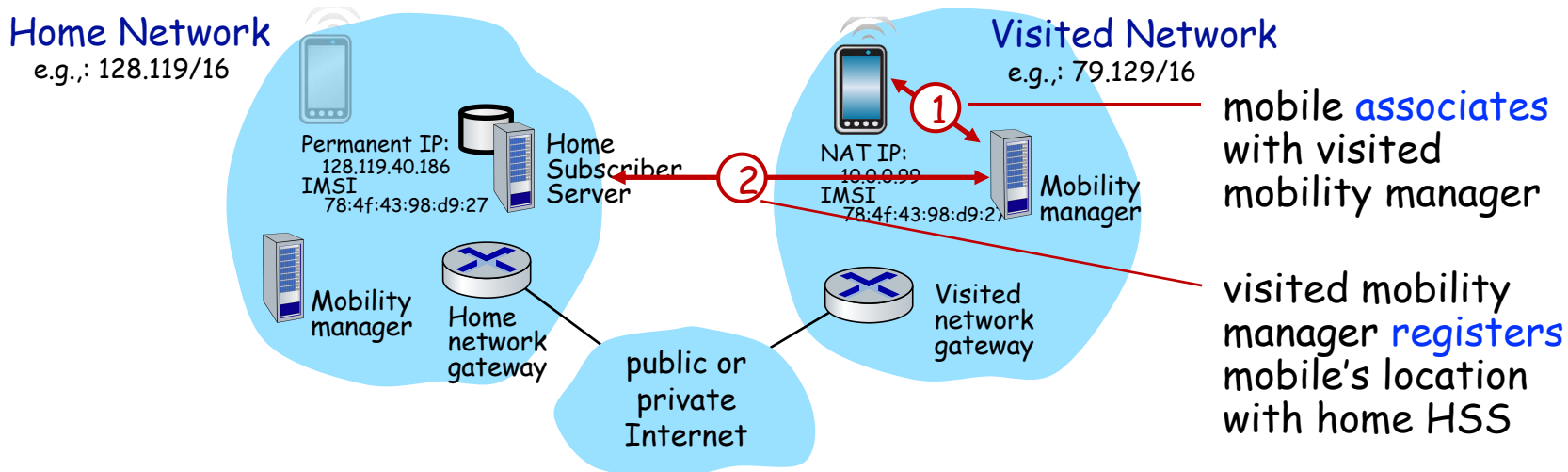
public or  
private  
Internet

Correspondent





# Registration: home needs to know where you are!



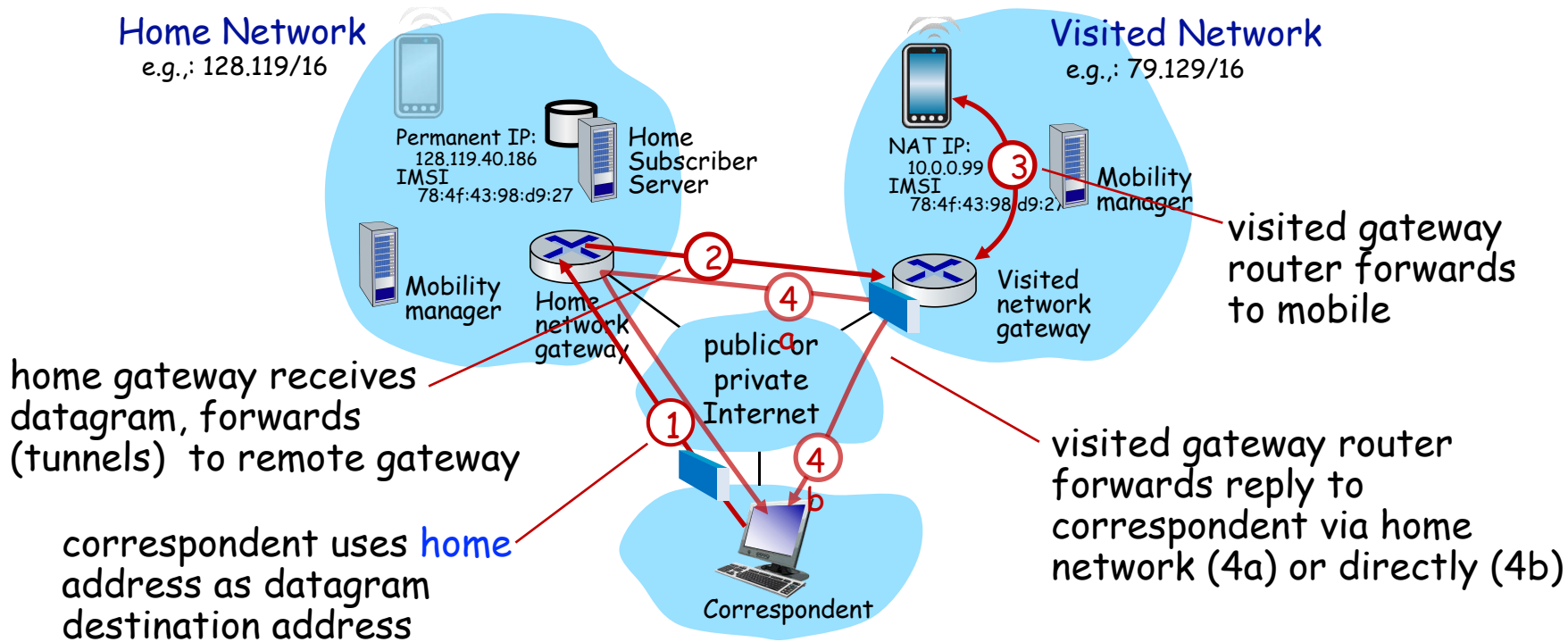
end result:

- visited mobility manager knows about mobile
- home HSS knows location of mobile





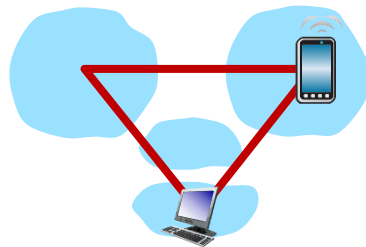
# Mobility with indirect routing





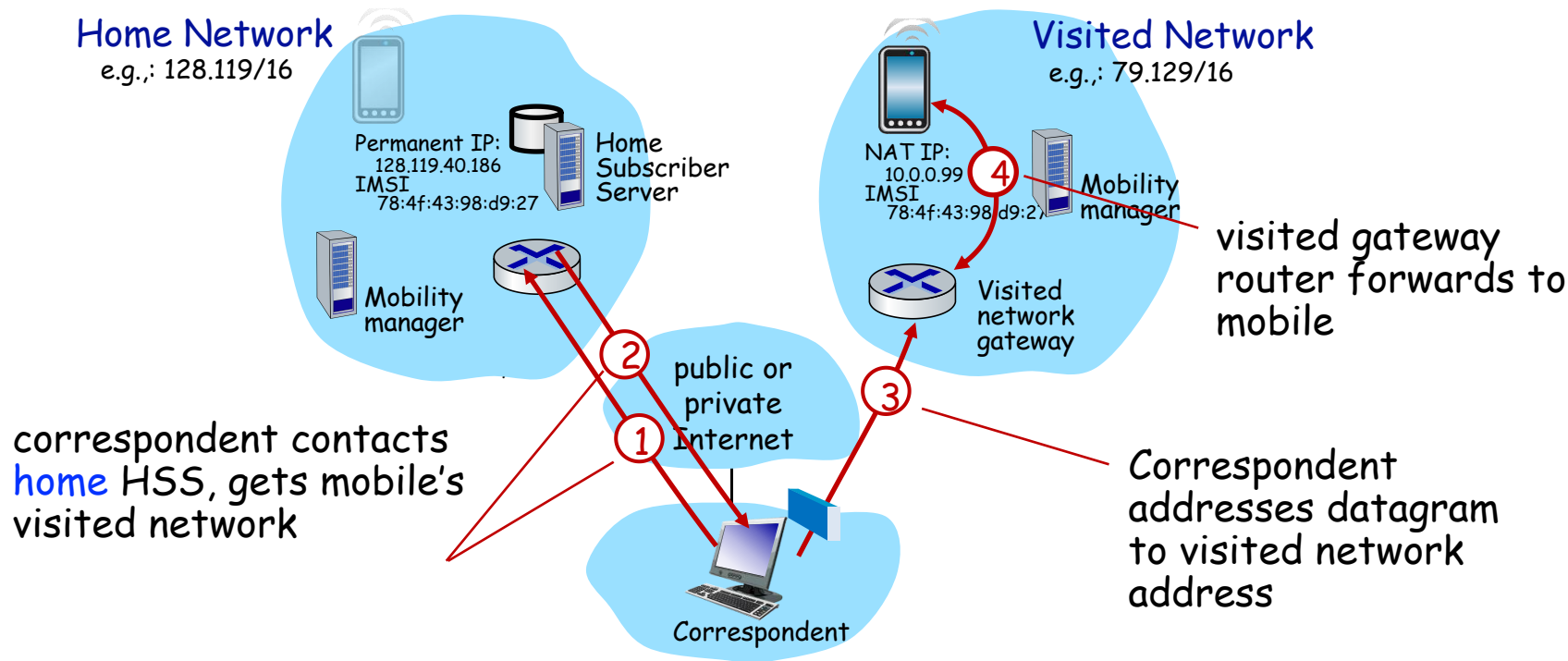
# Mobility with indirect routing: comments

- triangle routing:
  - inefficient when correspondent and mobile are in same network
- mobile moves among visited networks: transparent to correspondent!
  - registers in new visited network
  - new visited network registers with home HSS
  - datagrams continue to be forwarded from home network to mobile in new network
  - on-going (e.g., TCP) connections between correspondent and mobile can be maintained!





# Mobility with direct routing





# Mobility with direct routing:

---

## comments

- overcomes triangle routing inefficiencies
- **non-transparent to correspondent:** correspondent must get care-of-address from home agent
- what if mobile changes visited network?
  - can be handled, but with additional complexity





# Outline

---

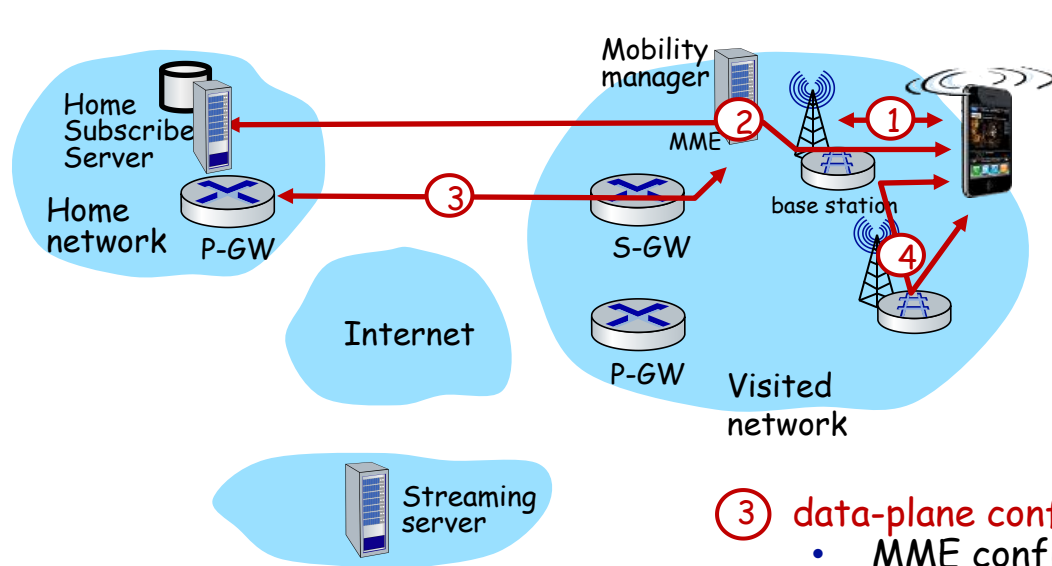
- Introduction
- Wireless
  - Wireless Links and network characteristics
  - CDMA: code division multiple access
  - WiFi: 802.11 wireless LANs
  - Cellular networks: 4G and 5G
- Mobility
  - Mobility management: principles
  - Mobility management: practice
  - Mobility: impact on higher-layer protocols







# Mobility in 4G networks: major mobility tasks



## ① base station association:

- covered earlier
- mobile provides IMSI - identifying itself, home network

## ② control-plane configuration:

- MME, home HSS establish control-plane state - mobile is in visited network

## ③ data-plane configuration:

- MME configures forwarding tunnels for mobile
- visited, home network establish tunnels from home P-GW to mobile

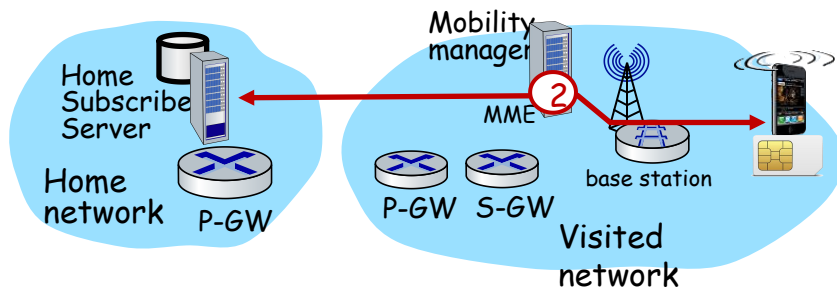
## ④ mobile handover:

- mobile device changes its point of attachment to visited network





# Configuring LTE control-plane elements



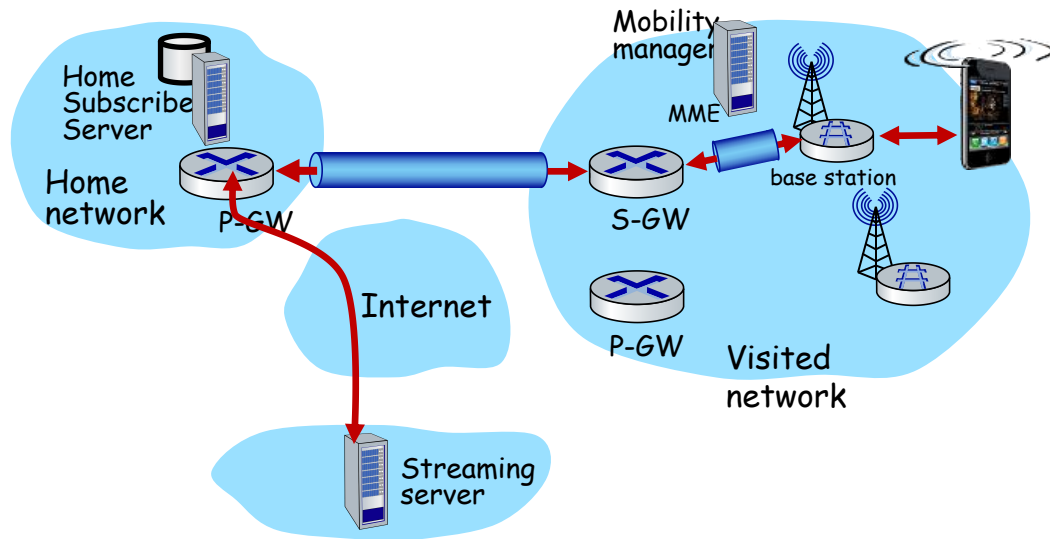
- Mobile communicates with local MME via BS control-plane channel
- MME uses mobile's IMSI info to contact mobile's home HSS
  - retrieve authentication, encryption, network service information
  - home HSS knows mobile now resident in visited network
- BS, mobile select parameters for BS-mobile data-plane radio channel





# Configuring data-plane tunnels for mobile

- **S-GW to BS tunnel:** when mobile changes base stations, simply change endpoint IP address of tunnel
- **S-GW to home P-GW tunnel:** implementation of indirect routing

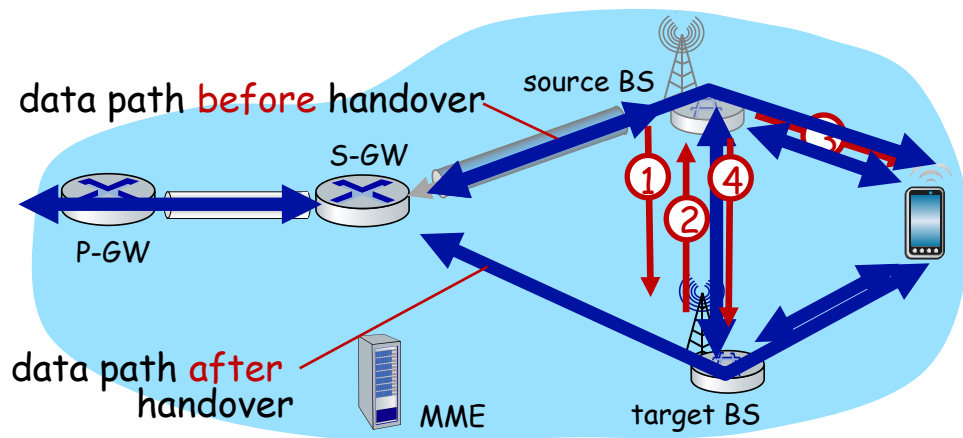


- **tunneling via GTP** (GPRS tunneling protocol): mobile's datagram to streaming server encapsulated using GTP inside UDP, inside datagram





# Handover between BSs in same cellular network



① current (source) BS selects target BS, sends **Handover Request message** to target BS

② target BS pre-allocates radio time slots, responds with HR ACK with info for mobile

③ source BS informs mobile of new BS

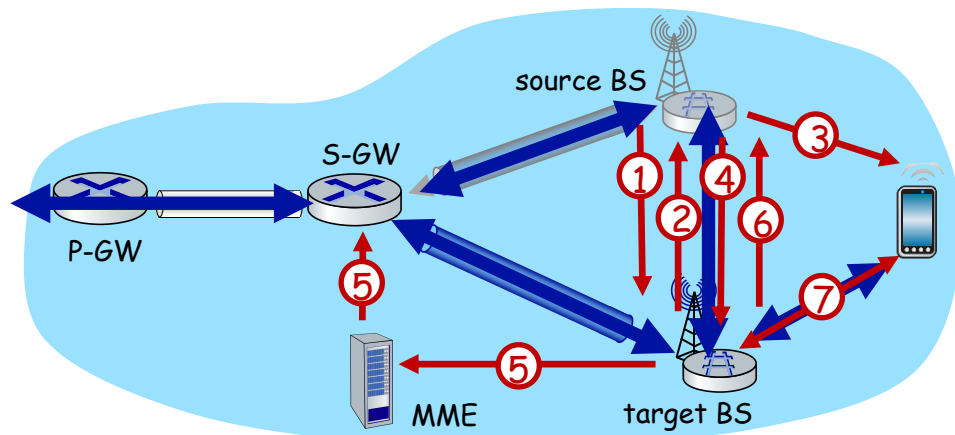
- mobile can now send via new BS - handover looks complete to mobile

④ source BS stops sending datagrams to mobile, instead forwards to new BS (who forwards to mobile over radio channel)





# Handover between BSs in same cellular network



- ⑤ target BS informs MME that it is new BS for mobile
- MME instructs S-GW to change tunnel endpoint to be (new) target BS

- ⑥ target BS ACKs back to source BS: handover complete, source BS can release resources
- ⑦ mobile's datagrams now flow through new tunnel from target BS to S-GW



# Mobile IP

---

- mobile IP architecture standardized ~20 years ago [RFC 5944]
  - long before ubiquitous smartphones, 4G support for Internet protocols
  - did not see wide deployment/use
  - perhaps WiFi for Internet, and 2G/3G phones for voice were “good enough” at the time
- mobile IP architecture:
  - indirect routing to node (via home network) using tunnels
  - mobile IP home agent: combined roles of 4G HSS and home P-GW
  - mobile IP foreign agent: combined roles of 4G MME and S-GW
  - protocols for agent discovery in visited network, registration of visited location in home network via ICMP extensions





# Wireless, mobility: impact on higher layer protocols

---

- logically, impact should be minimal ...
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- ... but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handover loss
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - bandwidth a scarce resource for wireless links





提问

---

Q & A



南京大學  
NANJING UNIVERSITY