南京大学
NANJING UNIVERSITY

# 无线网络和移动网络

殷亚凤
智能软件与工程学院
苏州校区南雍楼东区225
yafeng@nju.edu.cn，https://yafengnju.github.io/

# 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 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)
  - wwww.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

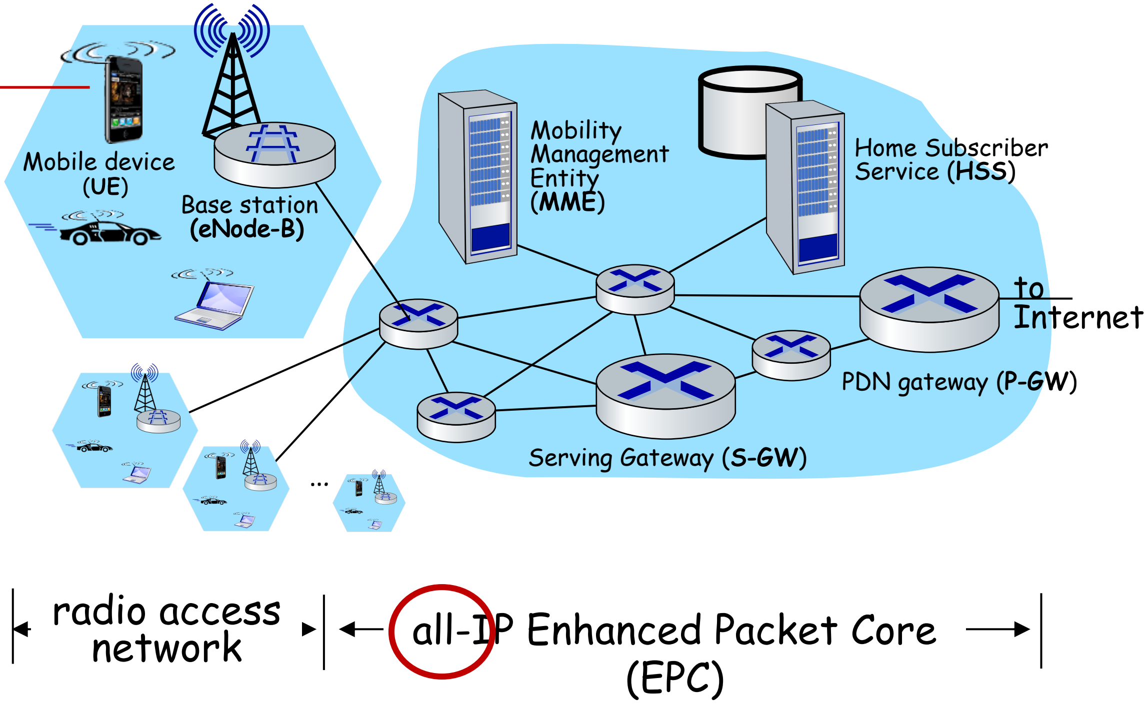
## differences from wired Internet

- different wireless link layer
- mobility as a 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

# Elements of 4G LTE architecture

Mobile device:

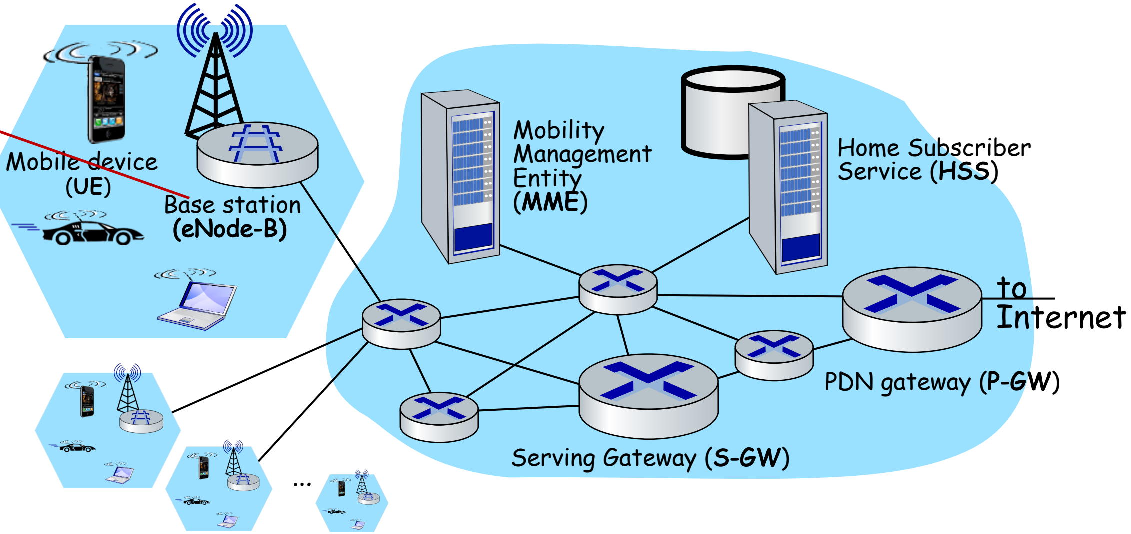
- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- LTE jargon: User Equipment (UE)



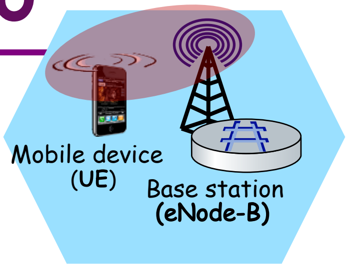
# Elements of 4G LTE architecture

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 nearly base stations to optimize radio use
- LTE jargon: eNode-B

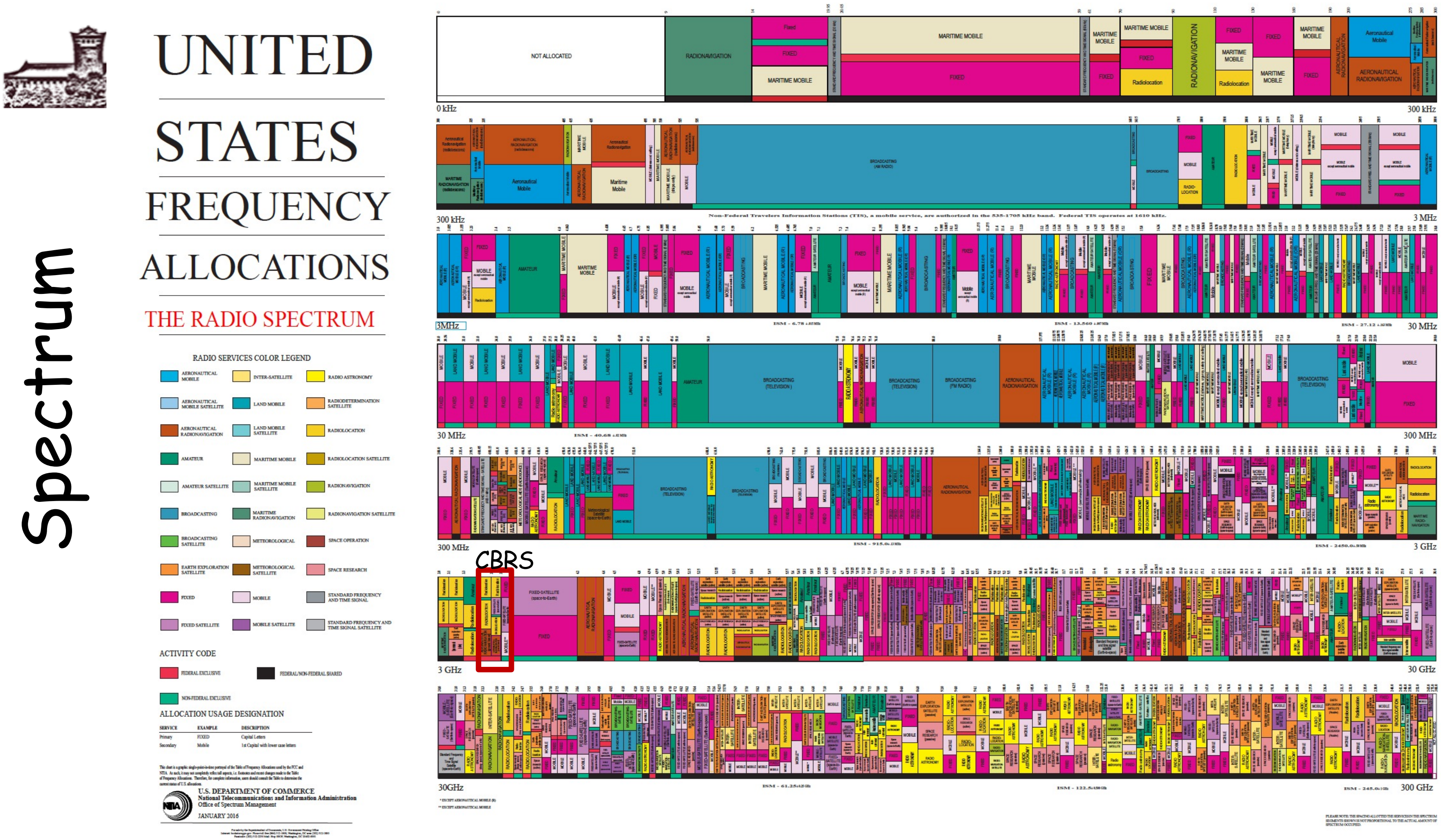


# Radio Access Network: 4G radio




- 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

# Spectrum

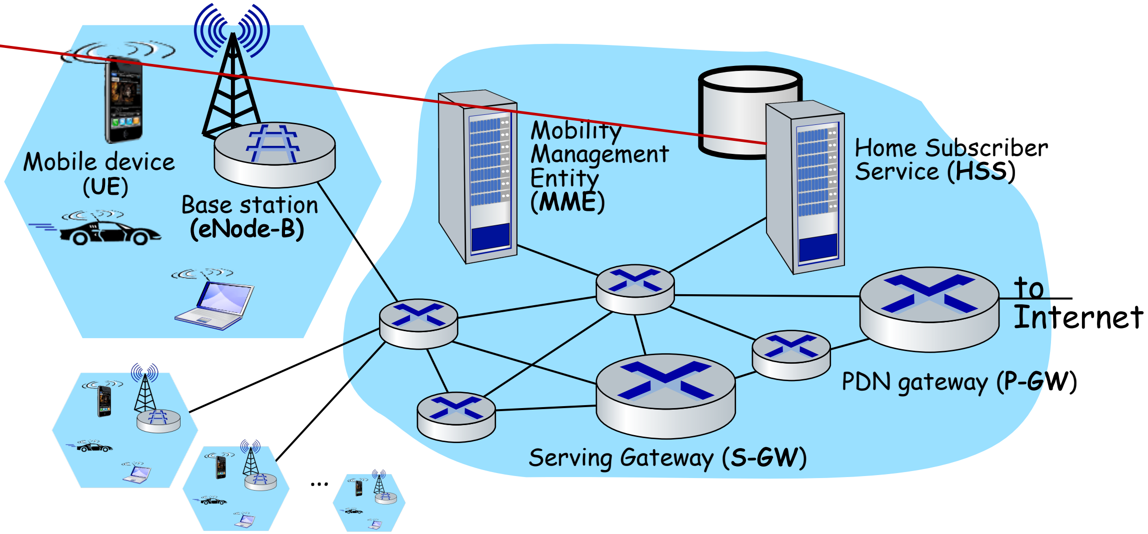


UNITED
STATES
FREQUENCY
ALLOCATIONS
THE RADIO SPECTRUM
RADIO SERVICES COLOR LEGEND
AERONAUTICAL MOBILE
AERONAUTICAL MOBILE SATELLITE
AERONAUTICAL RADIONAVIGATION
AMATEUR
AMATEUR SATELLITE
BROADCASTING
BROADCASTING SATELLITE
EARTH EXPLORATION SATELLITE
FIXED
FIXED SATELLITE
INTER-SATELLITE
LAND MOBILE
LAND MOBILE SATELLITE
MARITIME MOBILE
MARITIME MOBILE SATELLITE
MARITIME RADIONAVIGATION
METEOROLOGICAL
METEOROLOGICAL SATELLITE
MOBILE
MOBILE SATELLITE
RADIO ASTRONOMY
RADIODETERMINATION SATELLITE
RADIOLOCATION
RADIOLOCATION SATELLITE
RADIONAVIGATION
RADIONAVIGATION SATELLITE
SPACE OPERATION
SPACE RESEARCH
STANDARD FREQUENCY AND TIME SIGNAL
STANDARD FREQUENCY AND TIME SIGNAL SATELLITE
ACTIVITY CODE
FEDERAL EXCLUSIVE
FEDERAL/NON-FEDERAL SHARED
NON-FEDERAL EXCLUSIVE
ALLOCATION USAGE DESIGNATION
U.S. DEPARTMENT OF COMMERCE
National Telecommunications and Information Administration
Office of Spectrum Management
JANUARY 2016
0 kHz
300 kHz
3 MHz
30 MHz
300 MHz
3 GHz
30 GHz
300 GHz
CBRS

# Elements of 4G LTE architecture

Home Subscriber Service

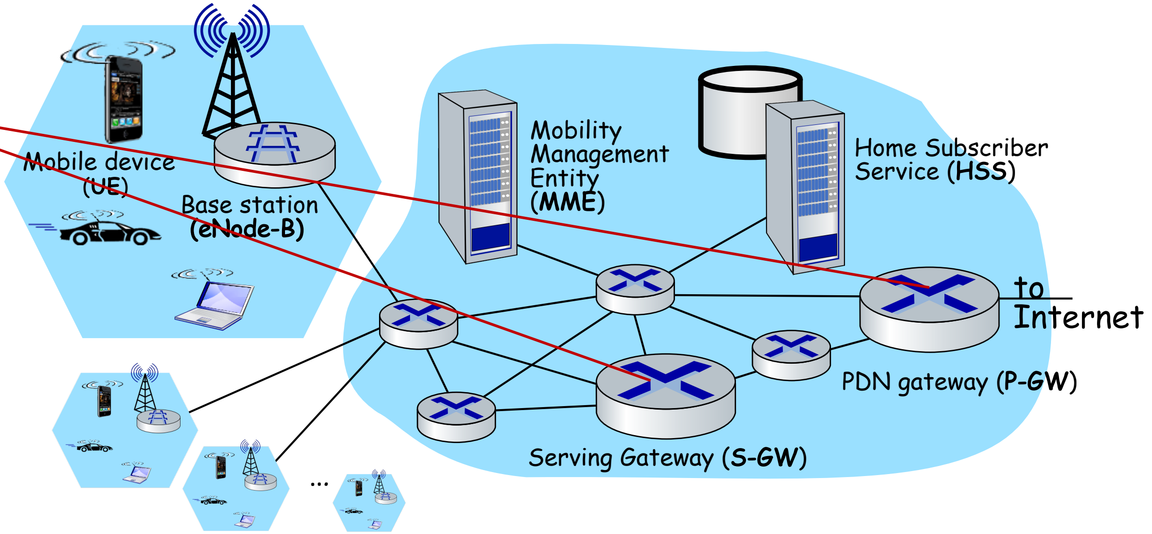
- stores info about mobile devices for which the HSS's network is their "home network"
- works with MME in device authentication



# Elements of 4G LTE architecture

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

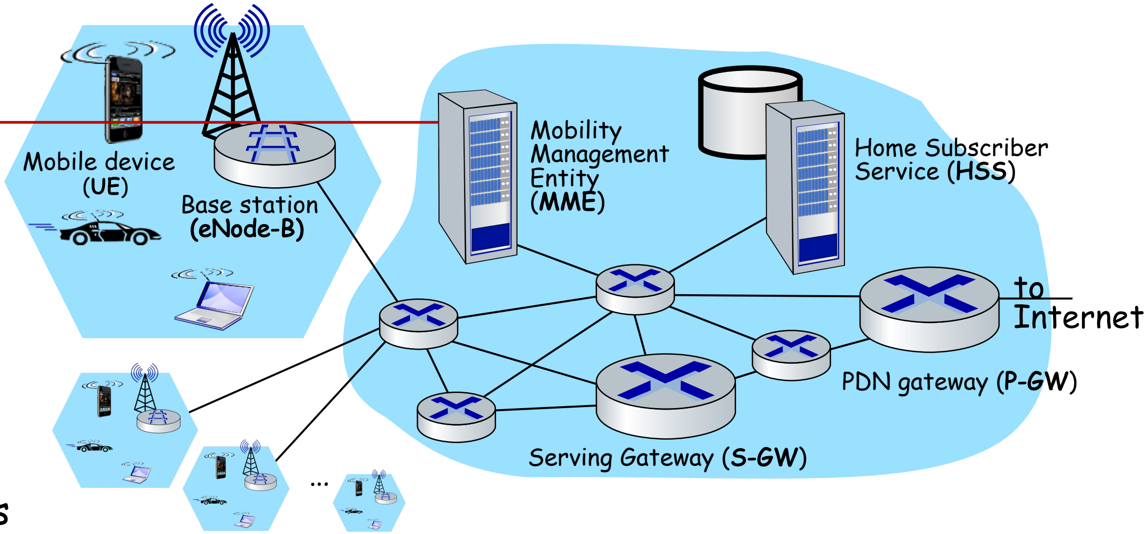
- lie on data path from mobile to/from Internet
- P-GW
  - gateway to mobile cellular network
  - Looks like nay other internet gateway router
  - provides NAT services
- other routers:
  - extensive use of tunneling



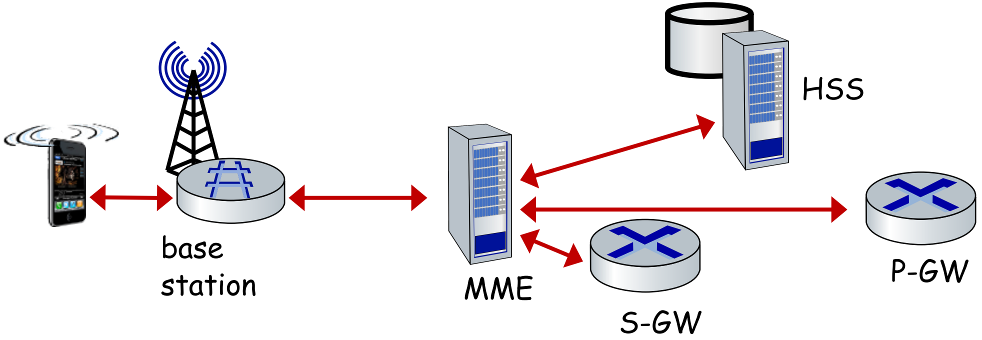
# Elements of 4G LTE architecture

Mobility Management Entity

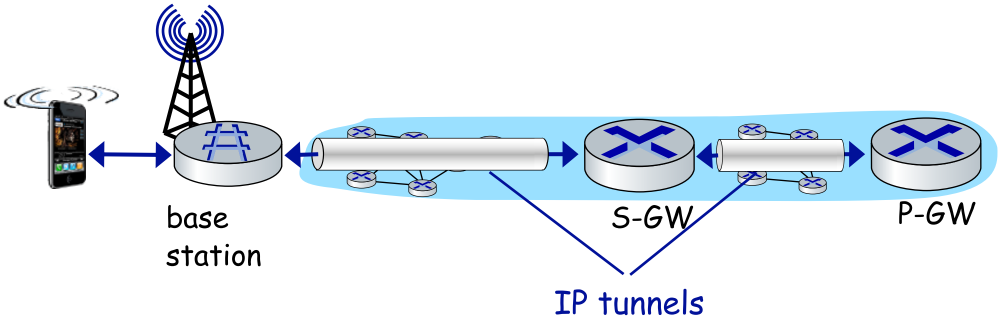
- device authentication (device-to-network, network-to-device) coordinated with mobile home network HSS
- mobile device management:
  - ➢ device handover between cells
  - ➢ tracking/paging device location
- path (tunneling) setup from mobile device to P-GW



# LTE: data plane control plane separation

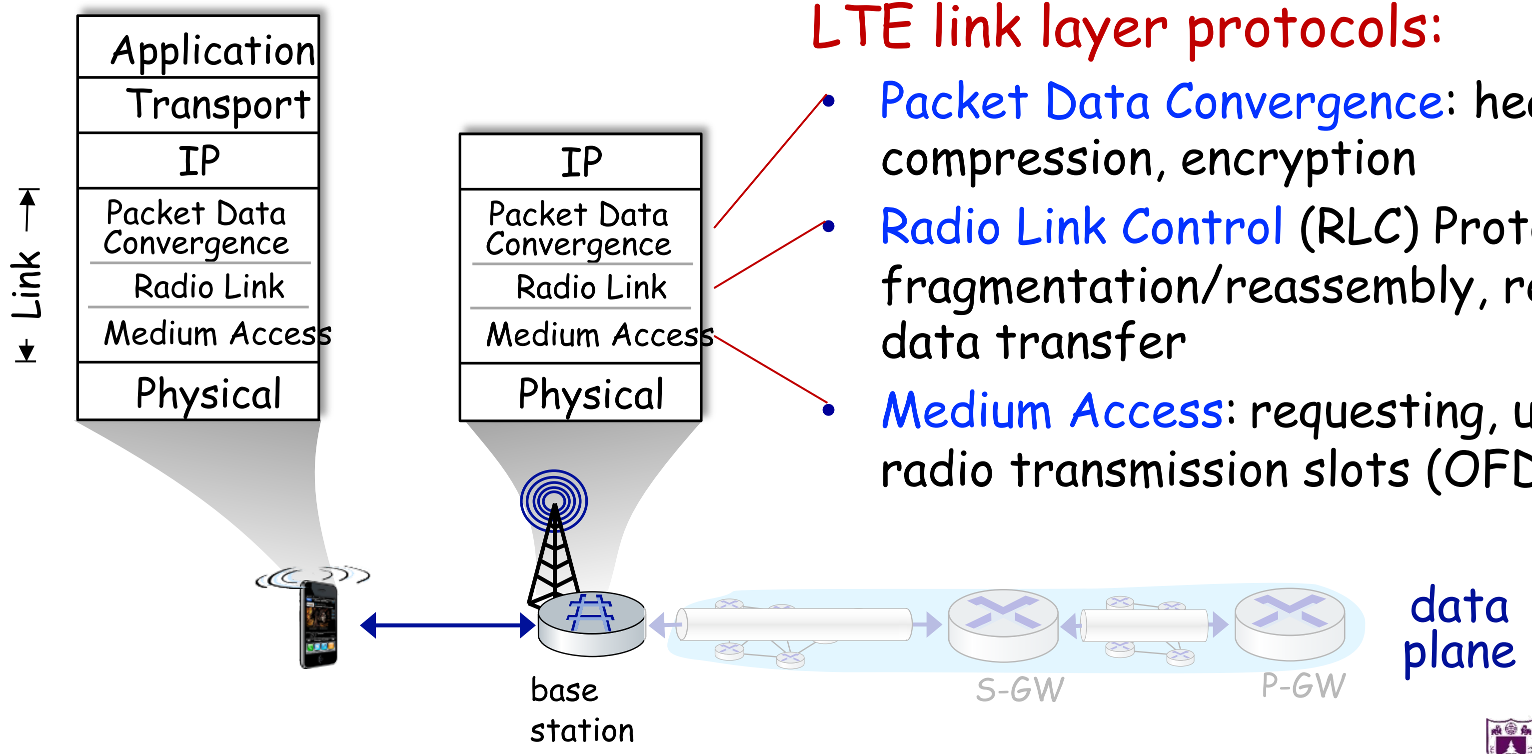



control plane
- new protocols for mobility management , security, authentication (later)




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

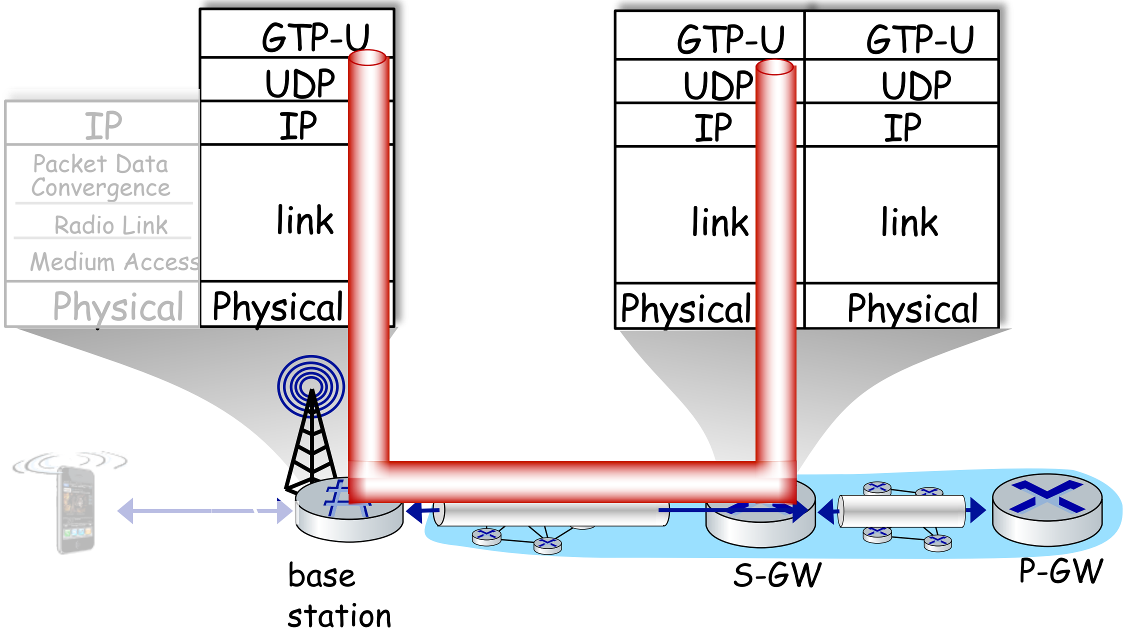
# LTE data plane protocol stack: first hop




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)

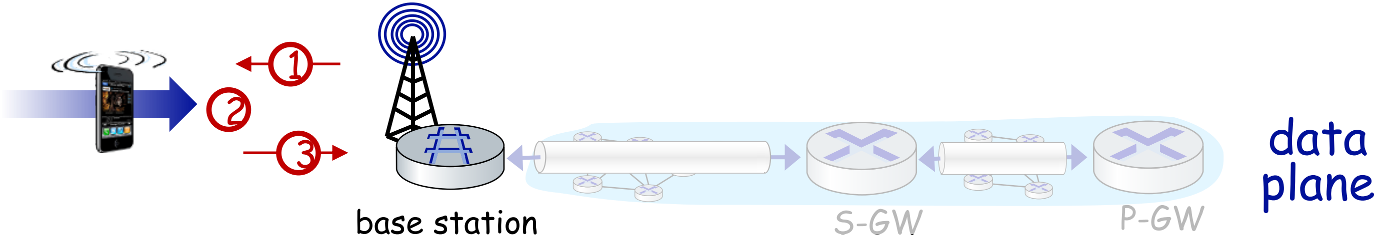
# LTE data plane protocol stack: packet core




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 BS



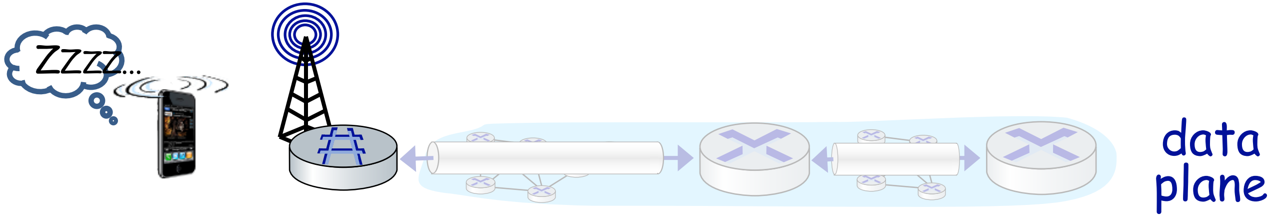

① BS broadcasts primary synch signal every 5 ms on all frequencies
- BSs from multiple carriers may be broadcasting synch signals

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 data plane

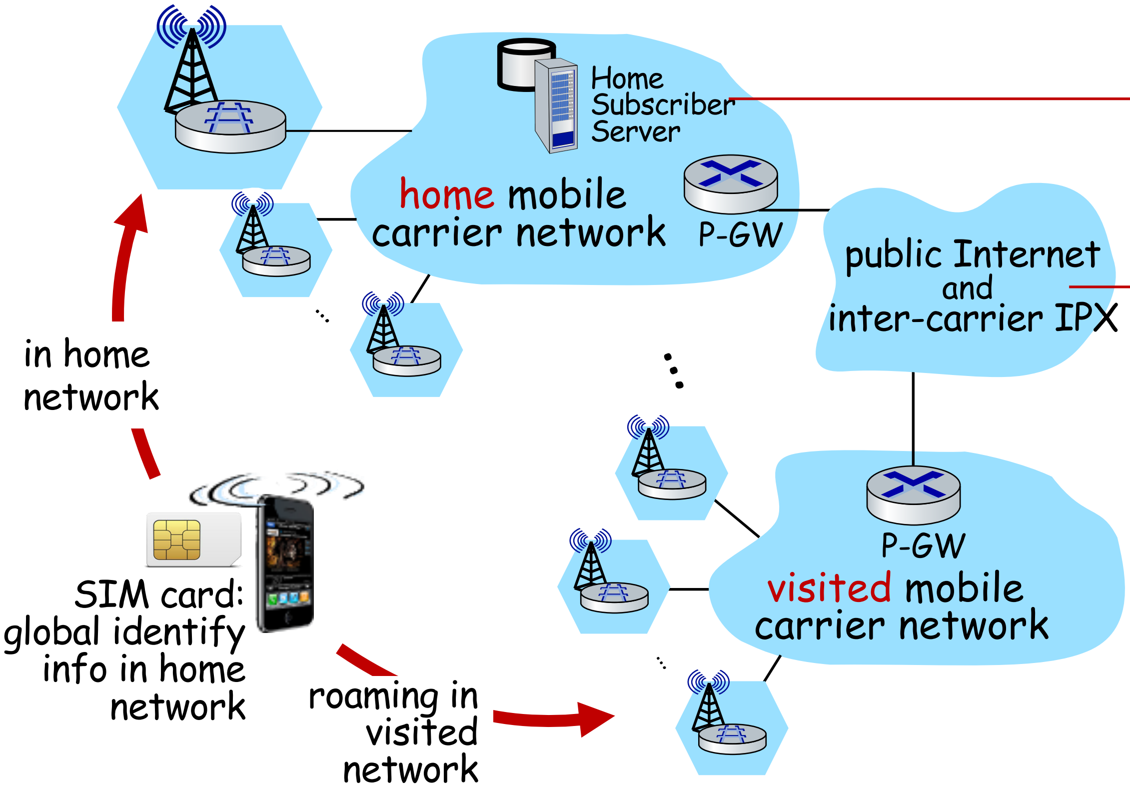
# LTE mobiles: sleep modes




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

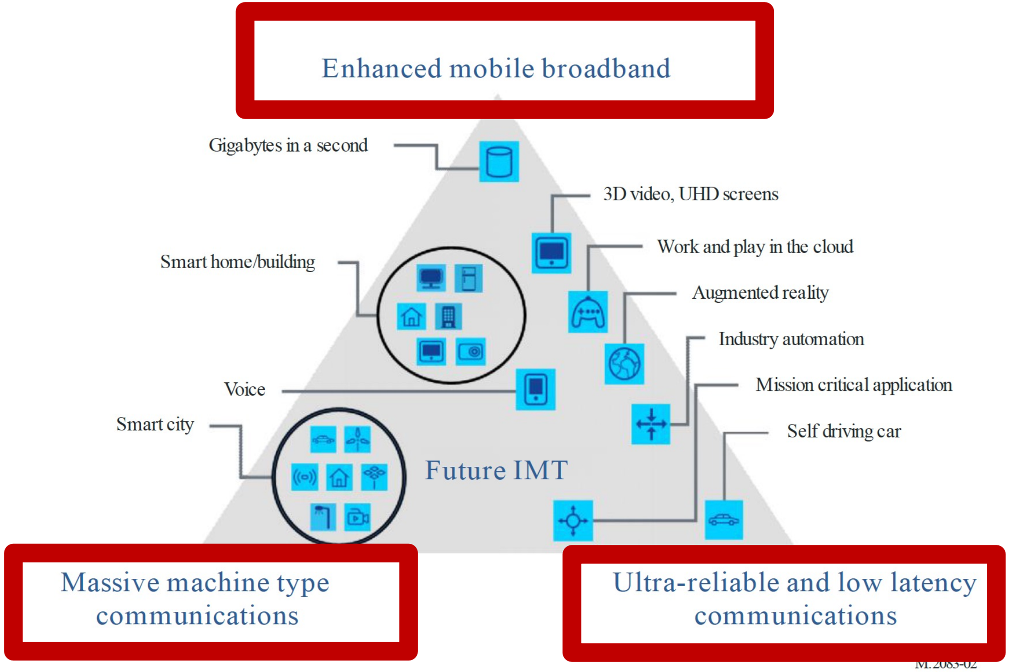
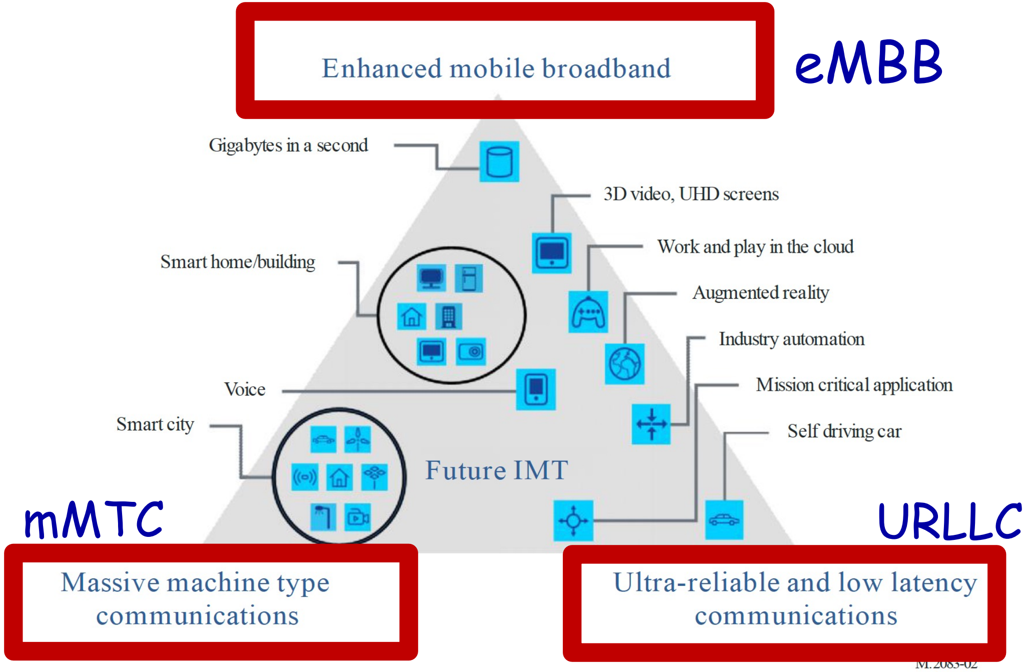



Figure: from Recommendation ITU-R M.2083-0 (2015)

"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."

# On to 5G: motivation




Industry verticals:

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

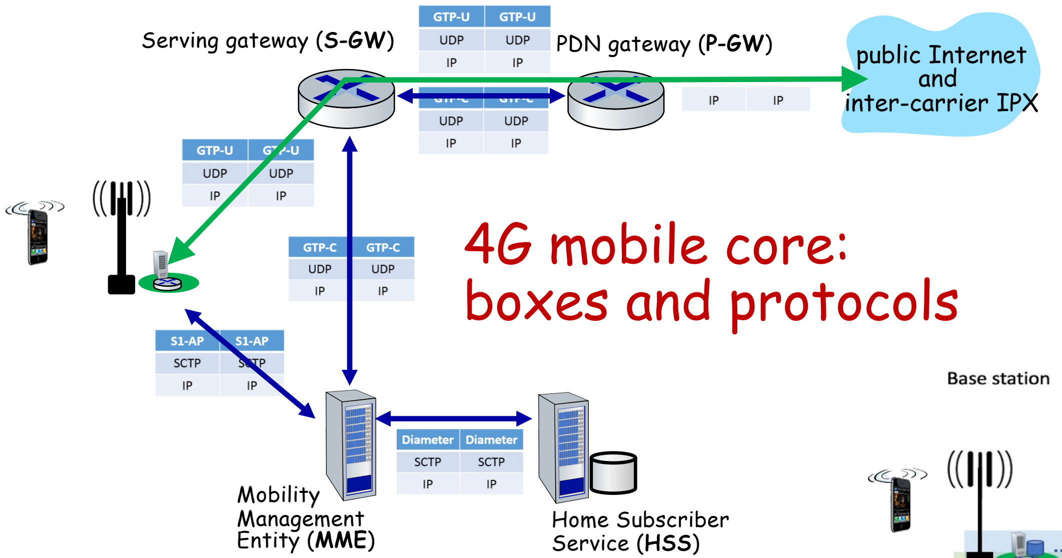
K. Schwab, "The Fourth Industrial Revolution," World Economic Forum.

NANJING UNIVERSITY

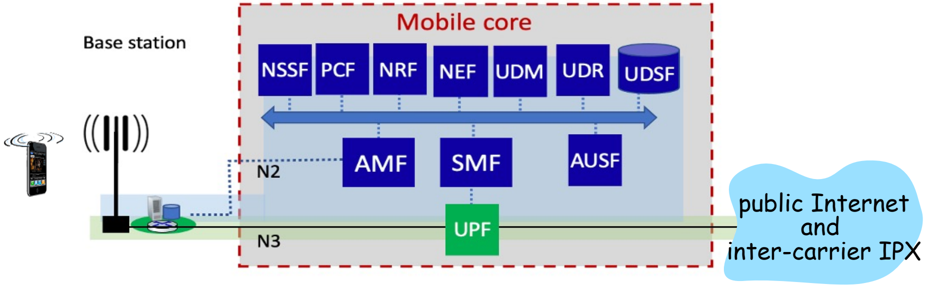
# On to 5G: Radio

- 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

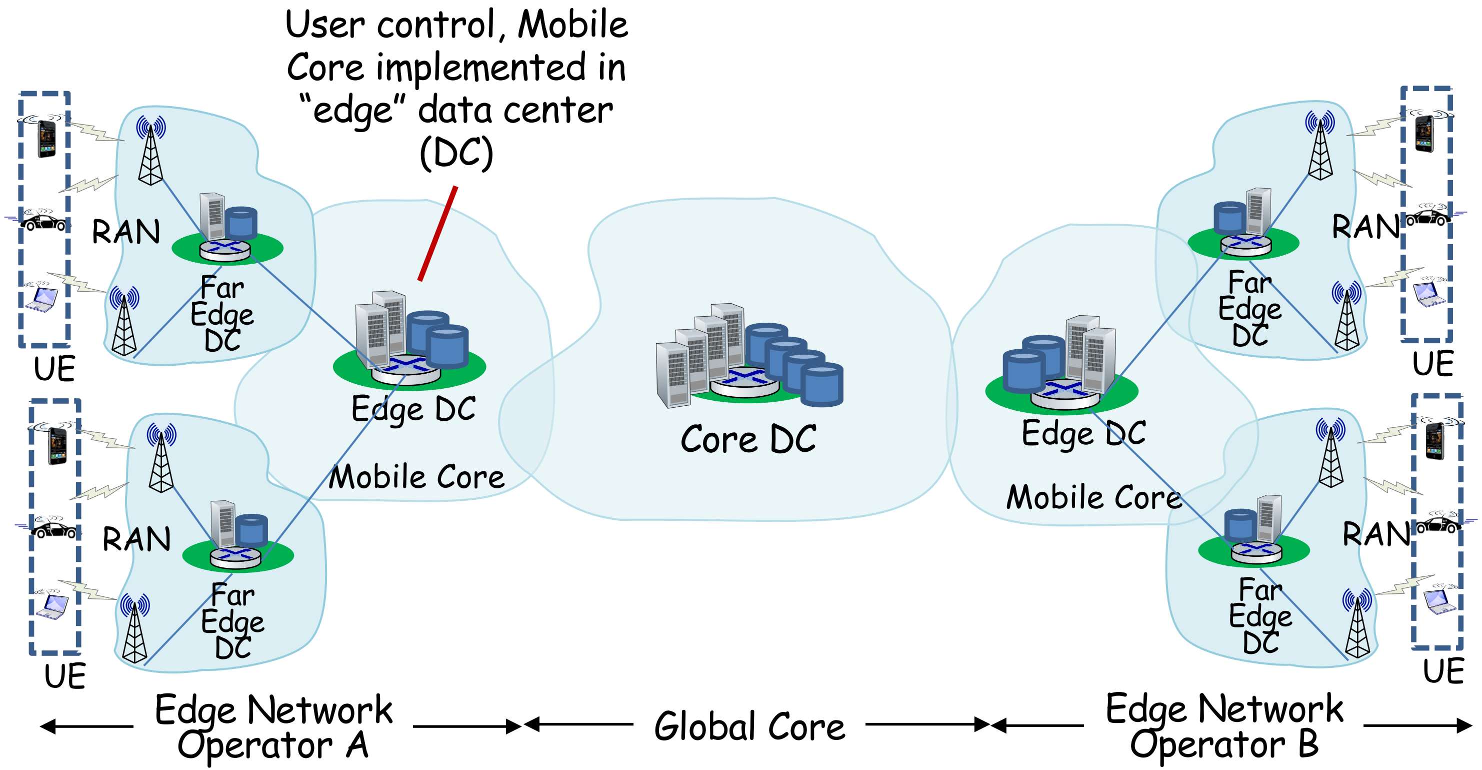



4G mobile core:
boxes and protocols

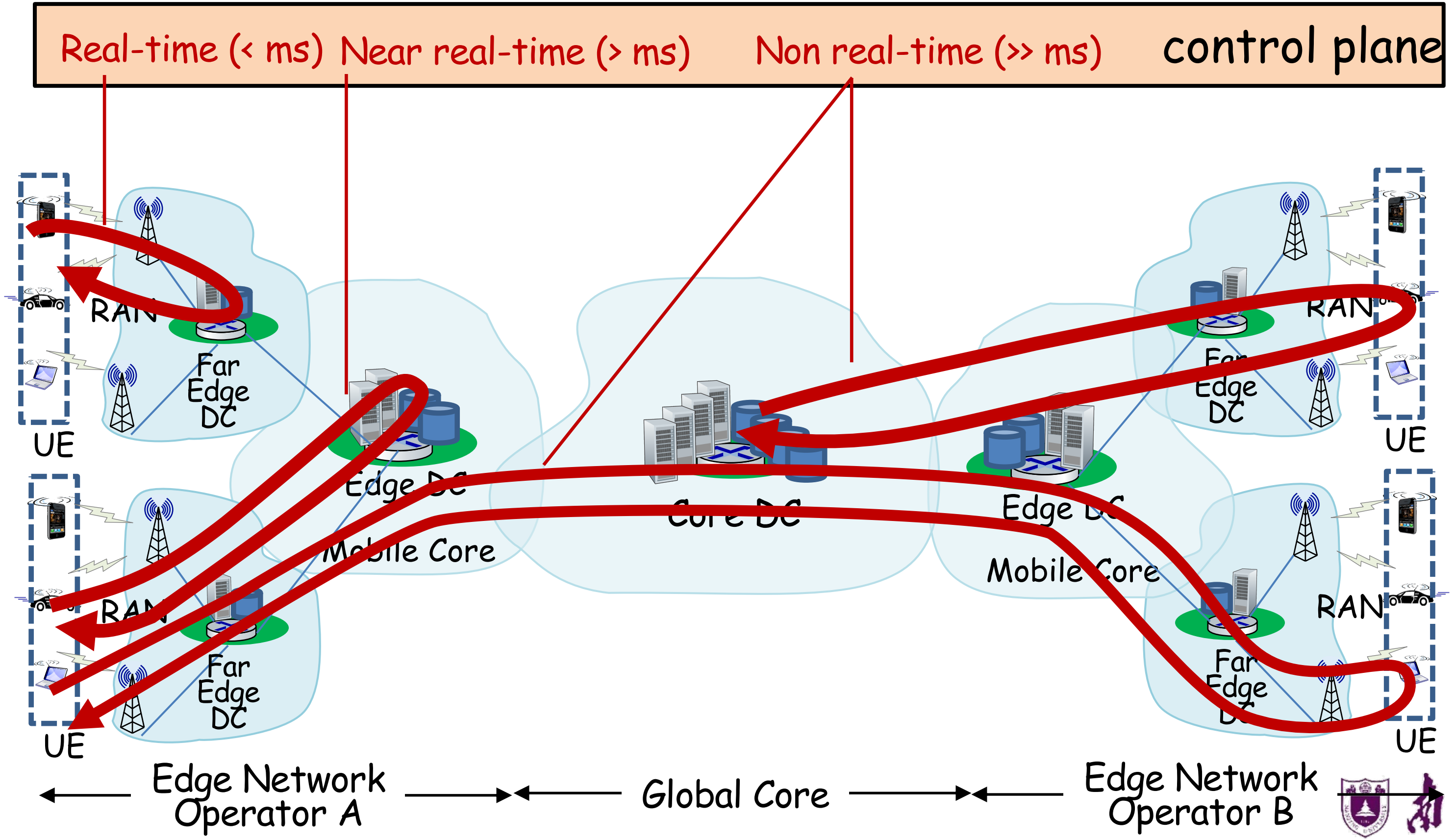



5G: microservice-like architecture

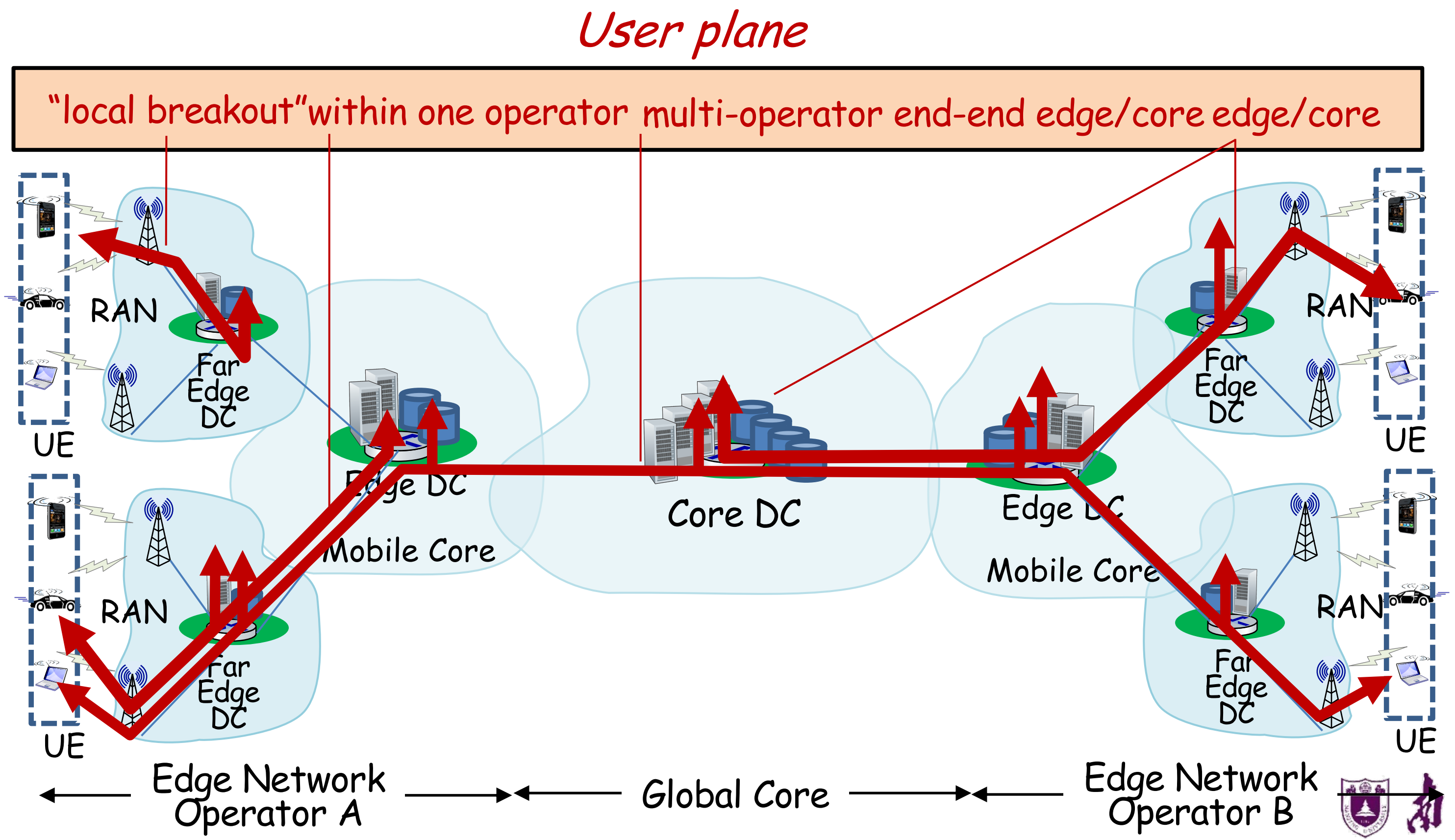
# Functional elements: communication, computation, data



# Control plane: resource control



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



# 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

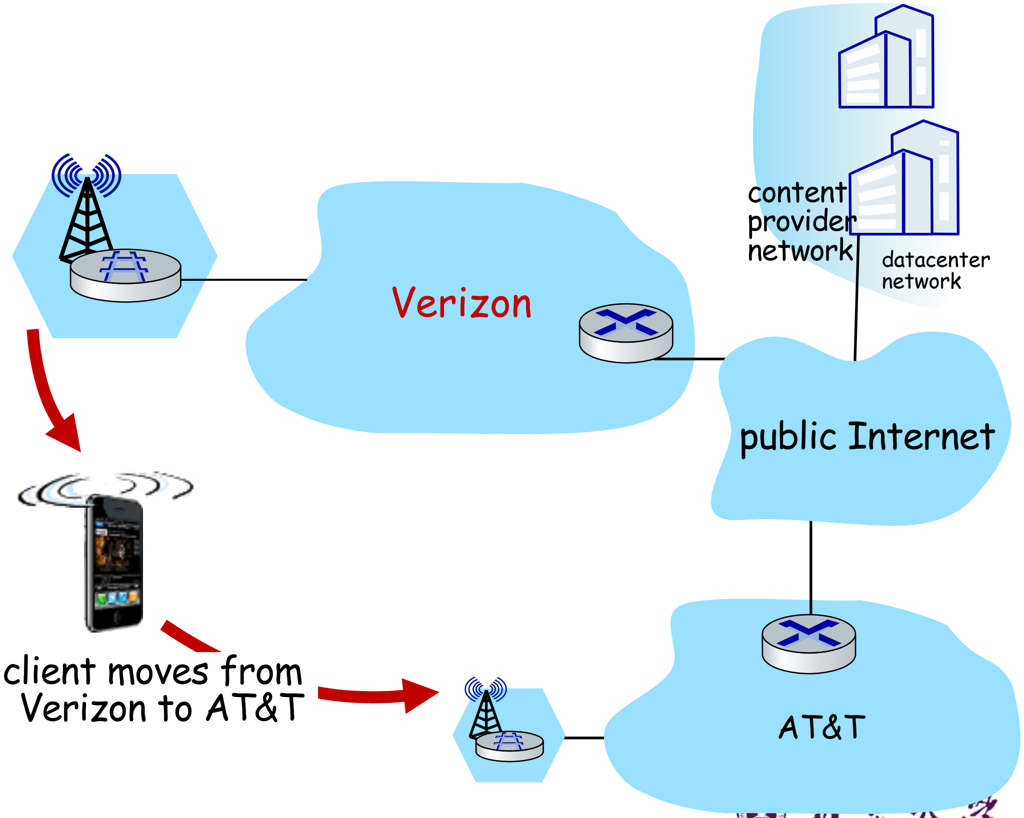
- device moves between networks, but powers down while moving
- device moves within same AP in one provider network
- device moves among APs in one provider network
- device moves among multiple provider networks, while maintaining ongoing connections

We're interested in these!

# Mobility challenge:

If a device moves from one network to 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- … me, address (e.g., permanent 32-bit IP … number (e.g., cell #) of visiting mobile node v … ing table exchange
  - Internet routing could … lready *with no* changes! Routing tables indicate where each mobile located via longest prefix match!

not
scalable
to billions of
mobiles

- 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:

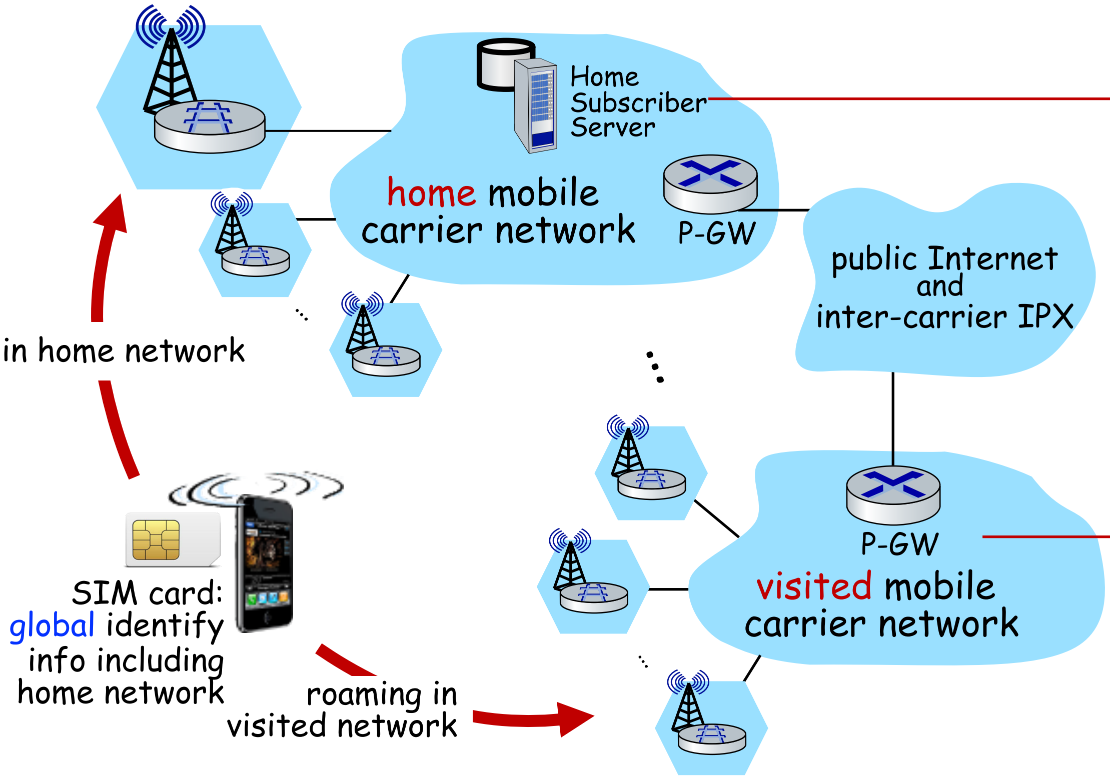
Consider friend frequently changing locations, how do you find him/her?

- 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



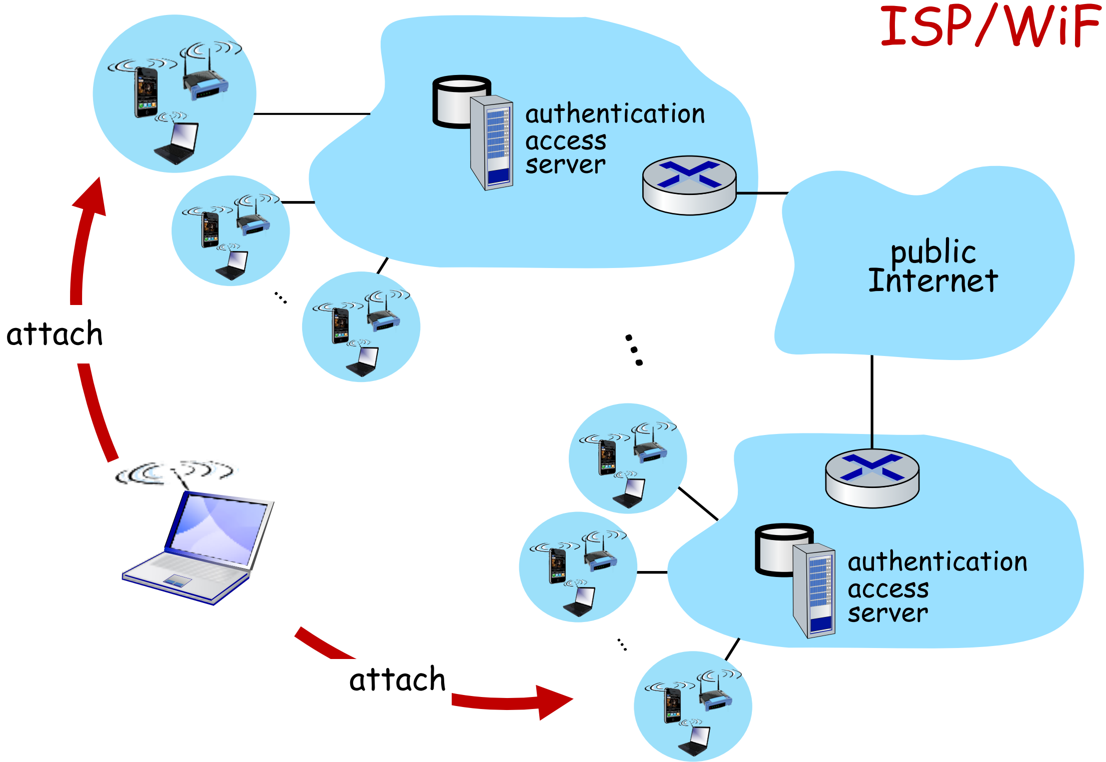

**home network:**

- (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

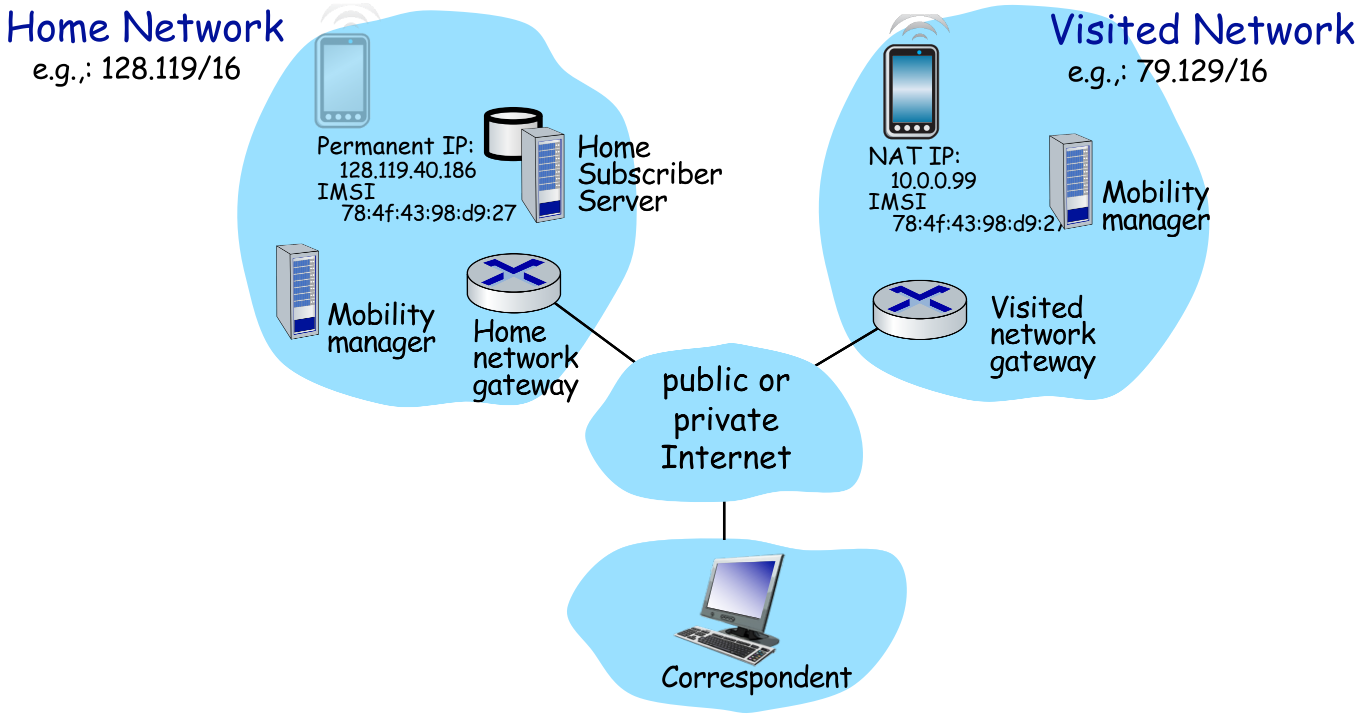
# Home network, visited network: ISP/WiFi



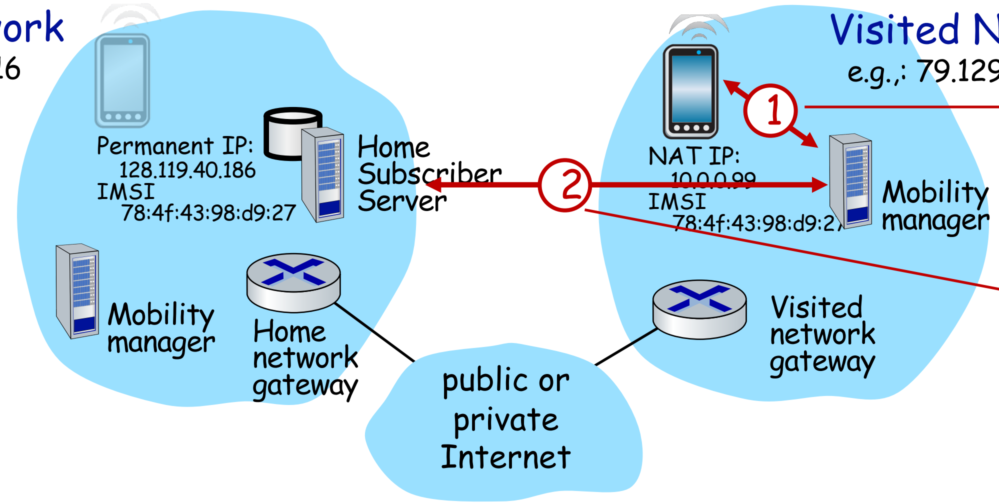

## ISP/WiFi: no notion of global "home"

- 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



# Registration: home needs to know where you are!



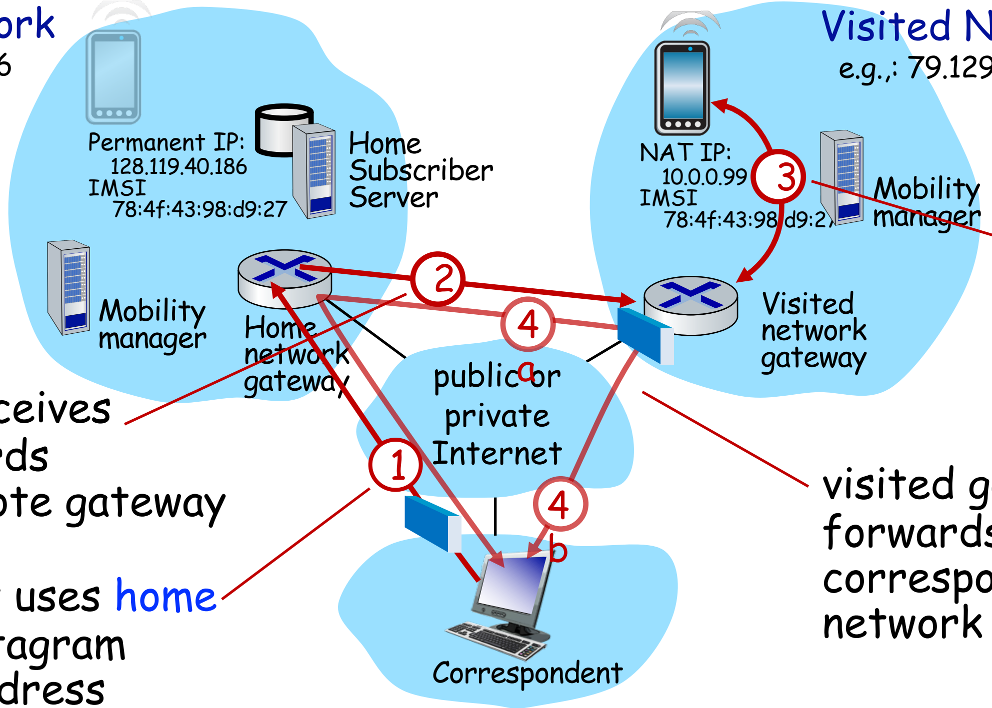

mobile associates with visited mobility manager

visited mobility manager registers mobile's location with home HSS

end result:

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

# Mobility with indirect routing




home gateway receives datagram, forwards (tunnels) to remote gateway

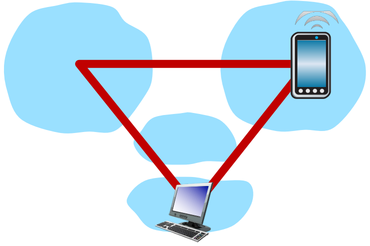
correspondent uses home address as datagram destination address

visited gateway router forwards to mobile

visited gateway router forwards reply to correspondent via home network (4a) or directly (4b)

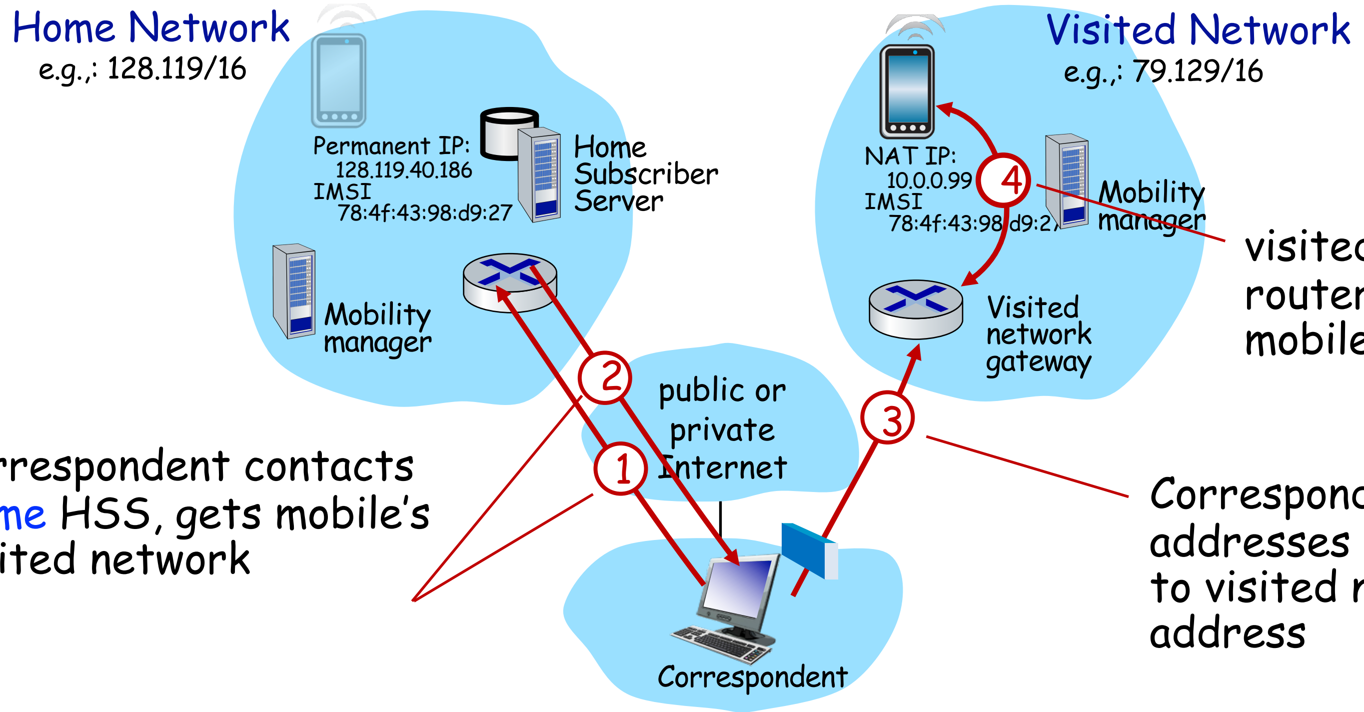
# Mobility with indirect routing: comments

- 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




correspondent contacts home HSS, gets mobile's visited network

Correspondent addresses datagram to visited network address

visited gateway router forwards to mobile

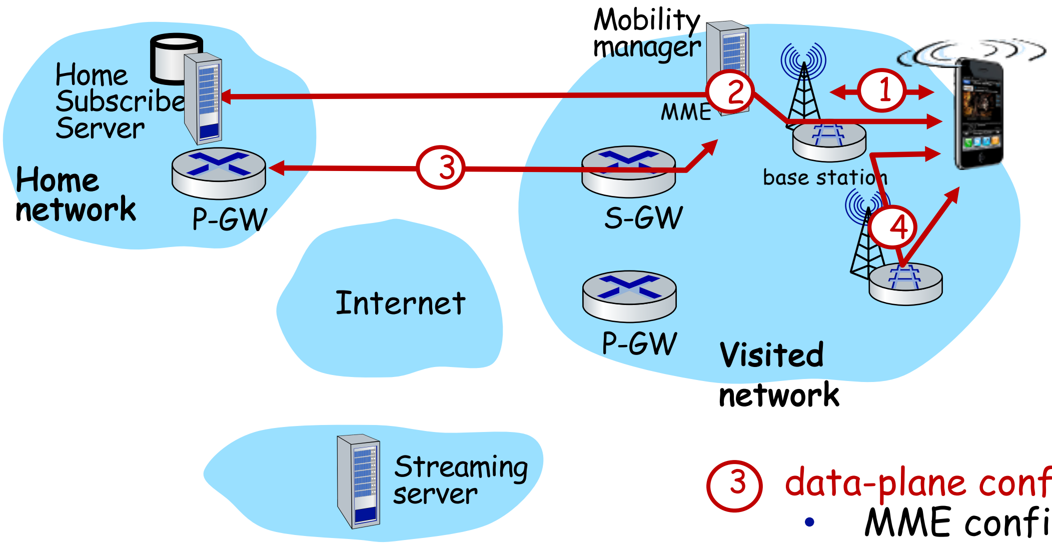
# Mobility with direct routing: comments

- 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

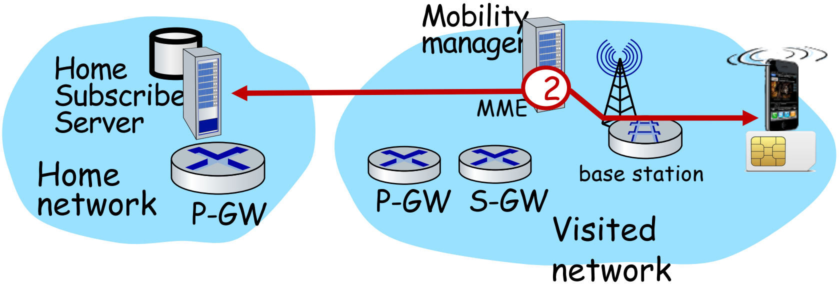
3 data-plane configuration:

- 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

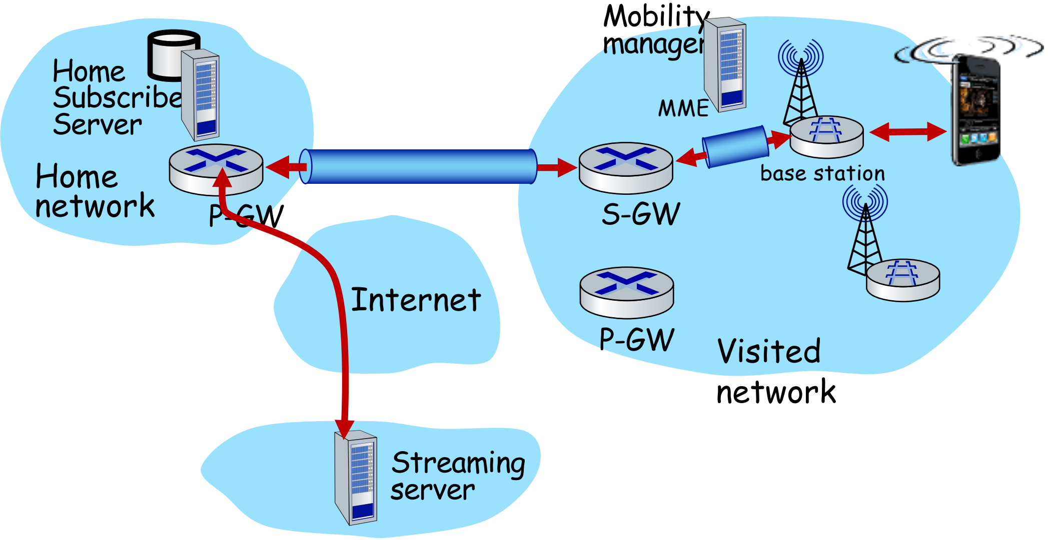
# Configuring LTE control-plane elements




- 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 HHS knows mobile now resident in visited network
- BS, mobile select parameters for BS-mobile data-plane radio channel

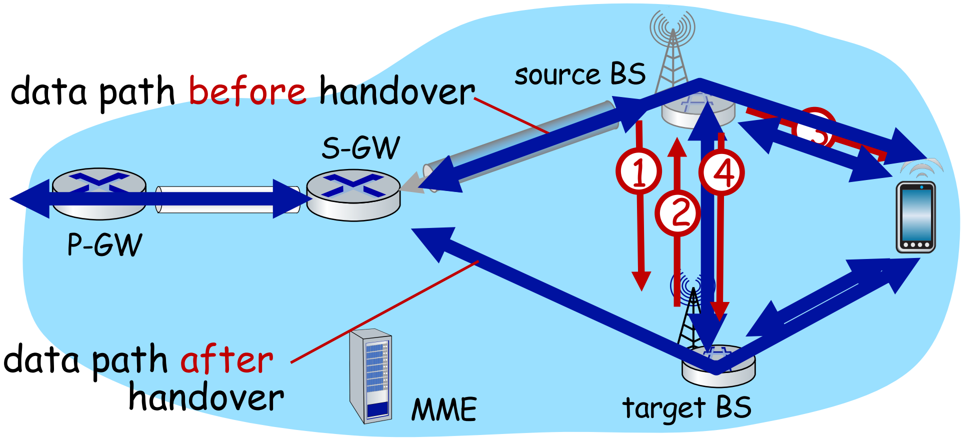
# Configuring data-plane tunnels for mobile

- **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



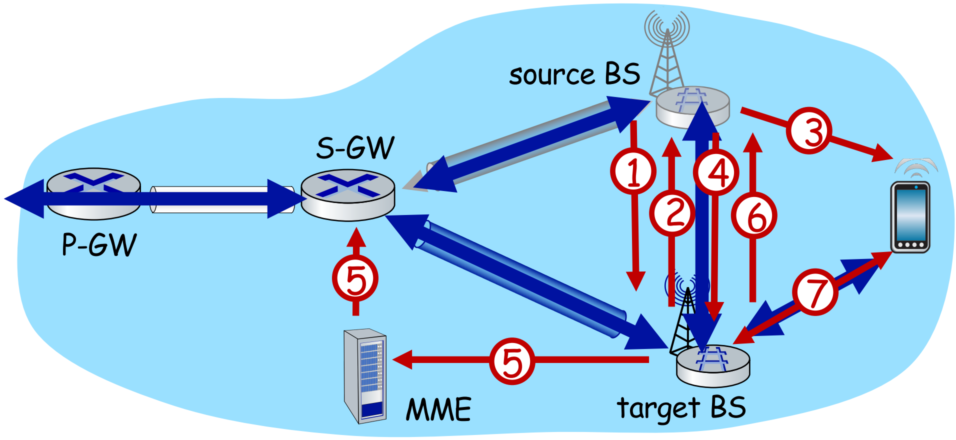

1 current (source) BS selects target BS, sends Handover Request message to target BS

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

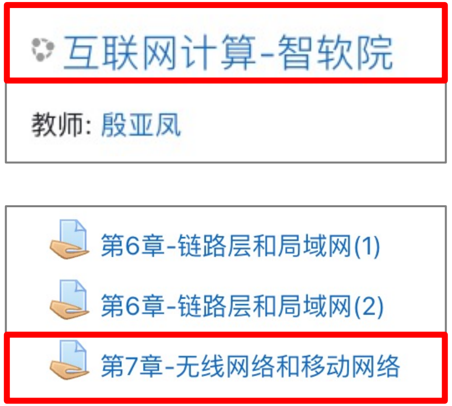
# Wireless, mobility: impact on higher layer protocols

- 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 scare resource for wireless links

# 课程习题（作业）——截止日期：5月27日晚23:59

- **课本393-396页**：R7、P5、P6、P8题

- 提交方式：https://selearning.nju.edu.cn/（教学支持系统）


第7章-无线网络和移动网络

课本393-396页：R7、P5、P6、P8题

- 命名：学号+姓名+第*章。

- 若提交遇到问题请及时发邮件或在下一次上课时反馈。

南京大学 NANJING UNIVERSITY

# 课程习题（作业）——截止日期：5月27日晚23:59

R7. 为什么 802.11 中使用了确认，而有线以太网中却未使用？

P5. 假设有两个 ISP 在一个特定的咖啡馆内提供 WiFi 接入，并且每个 ISP 有其自己的 AP 和 IP 地址块。

a. 进一步假设，两个 ISP 都意外地将其 AP 配置运行在信道 11。在这种情况下，802.11 协议是否将完全崩溃？讨论一下当两个各自与不同 ISP 相关联的站点试图同时传输时，将会发生什么情况。

b. 现在假设一个 AP 运行在信道 1，而另一个运行在信道 11。你的答案将会有什么变化？

P6. 在 CSMA/CA 协议的第 4 步，一个成功传输一个帧的站点在第 2 步（而非第 1 步）开始 CSMA/CA 协议。通过不让这样一个站点立即传输第 2 个帧（如果侦听到该信道空闲），CSMA/CA 的设计者是基于怎样的基本原理来考虑的呢？

# 课程习题（作业）——截止日期：5月27日晚23:59

P8. 考虑在图 7-31 中显示的情形，其中有 4 个无线节点 A、B、C 和 D。这 4 个节点的无线电覆盖范围显示为其中的椭圆形阴影；所有节点共享相同的频率。当 A 传输时，仅有 B 能听到/接收到；当 B 传输时，A 和 C 能听到/接收到；当 C 传输时，B 和 D 能听到/接收到；当 D 传输时，仅有 C 能听到/接收到。

假定现在每个节点都有无限多的报文要向每个其他节点发送。如果一个报文的目的地不是近邻，则该报文必须要中继。例如，如果 A 要向 D 发送，来自 A 的报文必须首先发往 B，B 再将该报文发送给 C，C 则再将其发向 D。时间是分隙的，报文所用的传输时间正好是一个时隙，如在时隙 Aloha 中的情况一样。在一个时隙中，节点能够做下列工作之一：（i）发送一个报文（如果它有报文向 D 转发）；（ii）接收一个报文（如果正好一个报文要向它发送）；（iii）保持静默。如同通常情况那样，如果一个节点听到了两个或更多的节点同时发送，出现冲突，并且重传的报文没有一个能成功收到。你这时能够假定没有比特级的差错，因此如果正好只有一个报文在发送，它将被位于发送方传输半径之内的站点正确收到。

a. 现在假定一个无所不知的控制器（即一个知道在网络中每个节点状态的控制器）能够命令每个节点去做它（无所不知的控制器）希望做的事情，例如发送报文，接收报文，或保持静默。给定这种无所不知的控制器，数据报文能够从 C 到 A 传输的最大速率是什么，假定在任何其他源/目的地对之间没有其他报文？

b. 现在假定 A 向 B 发送报文，并且 D 向 C 发送报文。数据报文能够从 A 到 B 且从 D 到 C 流动的组合最大速率是多少？

c. 现在假定 A 向 B 发送报文且 C 向 D 发送报文。数据报文能够从 A 到 B 且从 C 到 D 流动的组合最大速率是多少？

d. 现在假定无线链路由有线链路代替。在此情况下，重复问题（a）~（c）。

e. 现在假定我们又在无线状态下，对于从源到目的地的每个数据报文，目的地将向源回送一个 ACK 报文（例如，如同在 TCP 中）。对这种情况重复问题（a）~（c）。

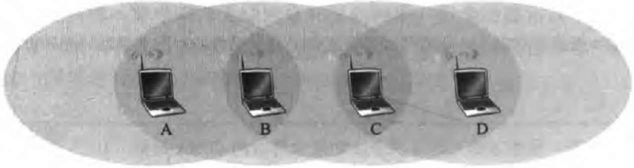
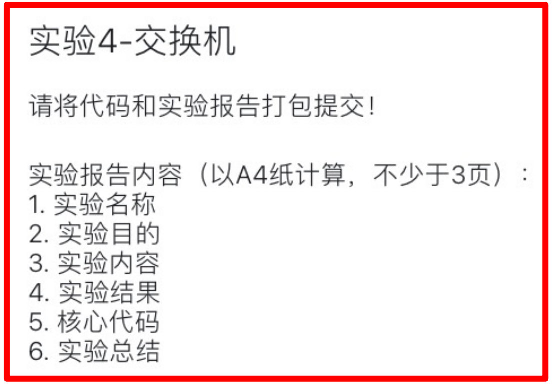



图 7-31 习题 P8 的情形

# 实验4——截止日期：6月3日晚23:59

- 实验4：交换机
- 提交方式：https://selearning.nju.edu.cn/（教学支持系统）






- 命名：学号+姓名+实验*。
- 若提交遇到问题请及时发邮件或在下一次上课时反馈。

# Lab 4: Learning Switch

## Overview

Your task is to implement the logic of a switch. As it is described in the last paragraph of the "Ethernet Learning Switch Operation" section, your switch will also handle the frames that are intended for itself and the frames whose Ethernet destination address is the broadcast address FF:FF:FF:FF:FF:FF.

In addition to these, you will also implement three different mechanisms to purge the outdated/stale entries from the forwarding table. This will allow your learning switch to adapt to changes in the network topology.

These mechanisms are:

- Remove an entry from the forwarding table after 10 seconds have elapsed.
- Remove the least recently used (LRU) entry from the forwarding table. For this functionality assume that your table can only hold 5 entries at a time. If a new entry comes and your table is full, you will remove the entry that has not been matched with a Ethernet frame destination address for the longest time.
- Remove the entry that has the least traffic volume. For this functionality assume that your table can only hold 5 entries at a time. Traffic volume for an entry is the number of frames that the switch received where Destination MAC address == MAC address of entry.

You will implement these mechanisms in three separate Python files. The core functionalities that are explained above will be the same for these implementations.

# 实验4——截止日期：6月3日晚23:59

## Lab 4: Learning Switch

**Task 1: Preparation**
Initiate your project with our template.
Start the task here

**Task 2: Basic Learning Switch**
Start with the basic learning switch.
Start the task here

**Task 3: Timeouts**
Implement timeouts based on the previous task.
Start the task here

**Task 4: LRU Rule Replacement Algorithm**
Implement LRU rule replacement algorithm based on Task 2.
Start the task here

**Task 5: Least Traffic Volume Rule Replacement Algorithm**
Implement least traffic volume rule replacement algorithm based on Task 2.
Start the task here

# 提问

# Q & A

殷亚凤
智能软件与工程学院
苏州校区南雍楼东区225
yafeng@nju.edu.cn，https://yafengnju.github.io/