Wireless Networks & Network Security

Dec 3, 2024

Min Suk Kang
Associate Professor
School of Computing/Graduate School of Information Security

NetS&P
Research Lab @ KAIST

KAIST

Chapter 7 outline

LAN 4- half network & half security (last concept

- Introduction

Wireless

- Wireless links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G

prevalent (안 영향) — 가장 흔한 wireless 연결

Mobility

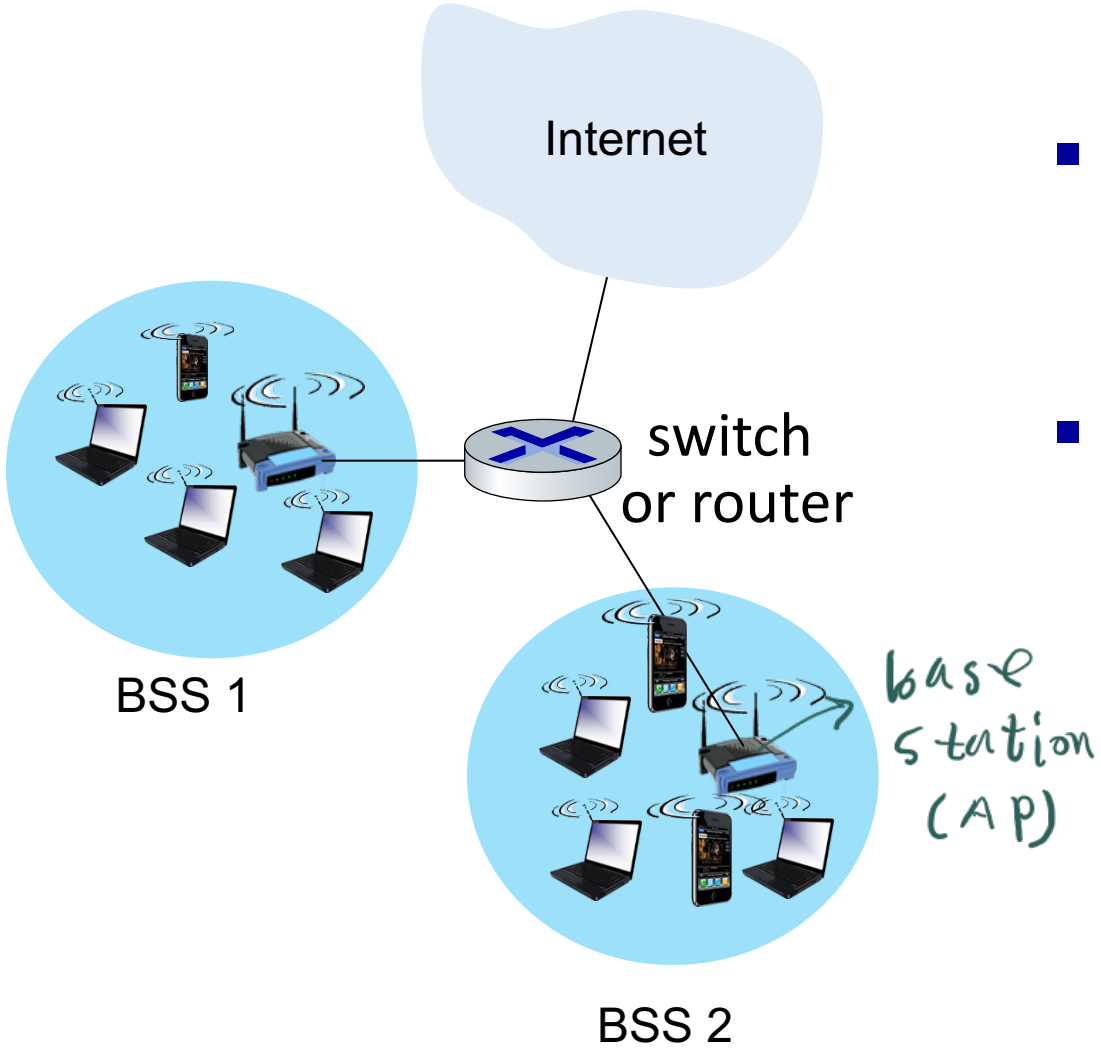
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

IEEE 802.11 Wireless LAN

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2020 (exp.)	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz

- all use CSMA/CA for multiple access, and have base-station and ad-hoc network versions

802.11 LAN architecture



- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

↳ base station 없이 host끼리만

802.11: Channels

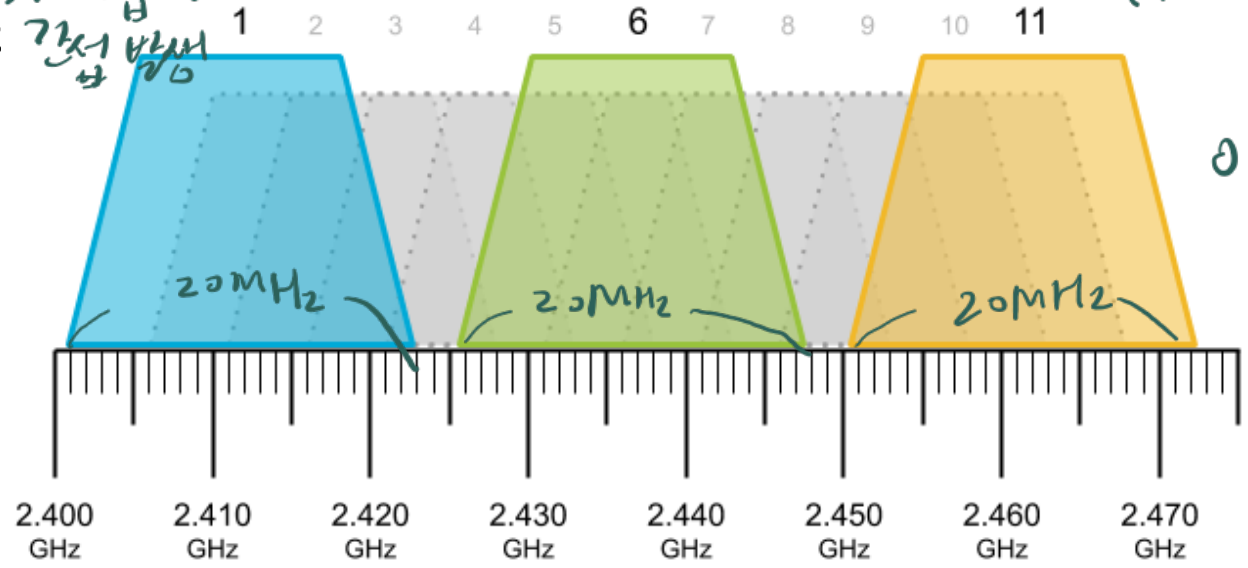
ex) FDM

- spectrum divided into channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!

↳ 인접한 AP에서 주파수와 겹칠때 간섭발생

선택할 frequency channel is free

Example: 2.4 GHz



overlapping시 동시 발송불가

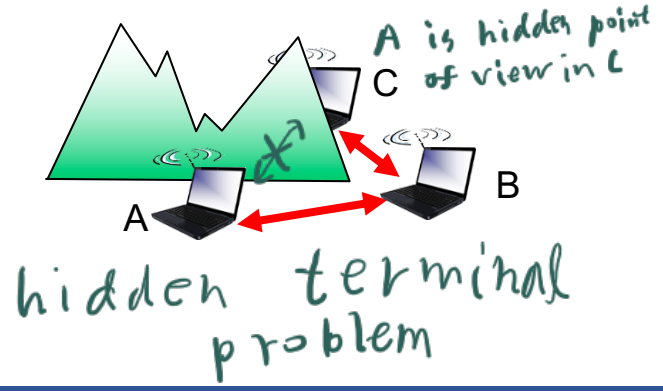
⇒ 각 AP는 간섭을 피해 non-overlapping channel 선택

802.11: Association

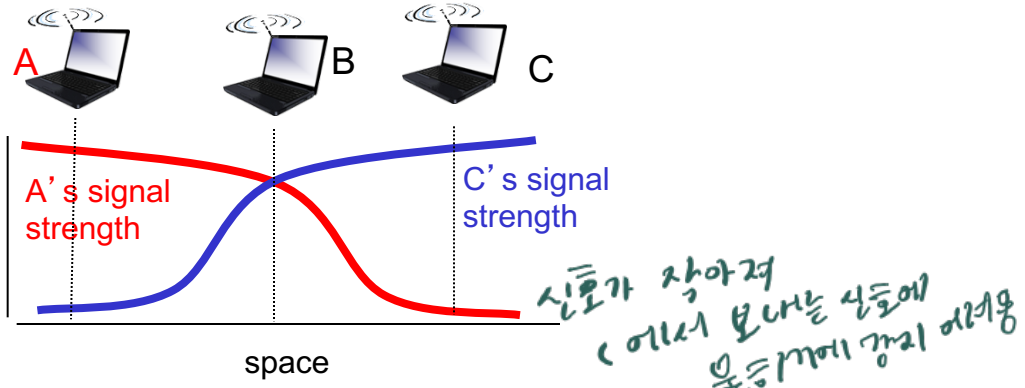
- arriving host: must associate with an AP → host가 네트워크 접속을 위해 AP 연결 필수
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address → AP가 주기적으로 beacon frame (이름(SSID), MAC주소 등) 전송 → host가 이를 듣고 연결 가능한 AP 인식
  - selects AP to associate with → AP선택
  - then may perform authentication [Chapter 8] → 인증
  - then typically run DHCP to get IP address in AP's subnet → DHCP 서버 (ip 자동 할당)

IEEE 802.11: multiple access

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
  - don't collide with detected ongoing transmission by another node
- 802.11: *no* collision detection!
  - difficult to sense collisions: high transmitting signal, weak received signal due to fading
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/CollisionAvoidance



hidden terminal problem



IEEE 802.11 MAC Protocol: CSMA/CA

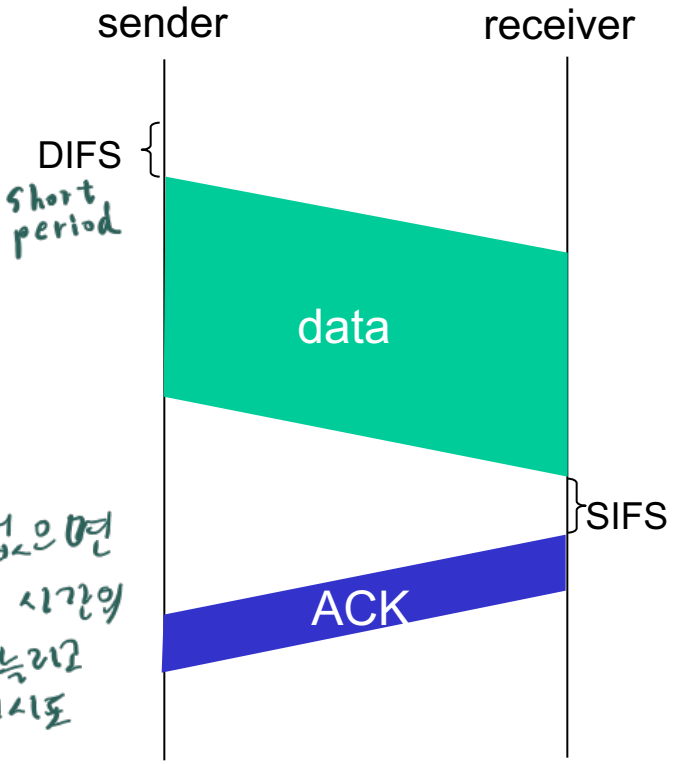
CSMA/H : CSMA + handshake

802.11 sender

1 if sense channel idle for **DIFS** then
transmit entire frame (no CD)

DIFS 동안 대기 후 전송 x시 전송

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2



전송 끝이면 랜덤 대기시간 생성 후 전송 x시 전송 ⇒ ACK 없으면 랜덤 대기 시간의 최댓값 늘리고 재시도

802.11 receiver

if frame received OK
return ACK after **SIFS** (ACK needed due to hidden terminal problem)

SIFS 대기 후 ACK 전송

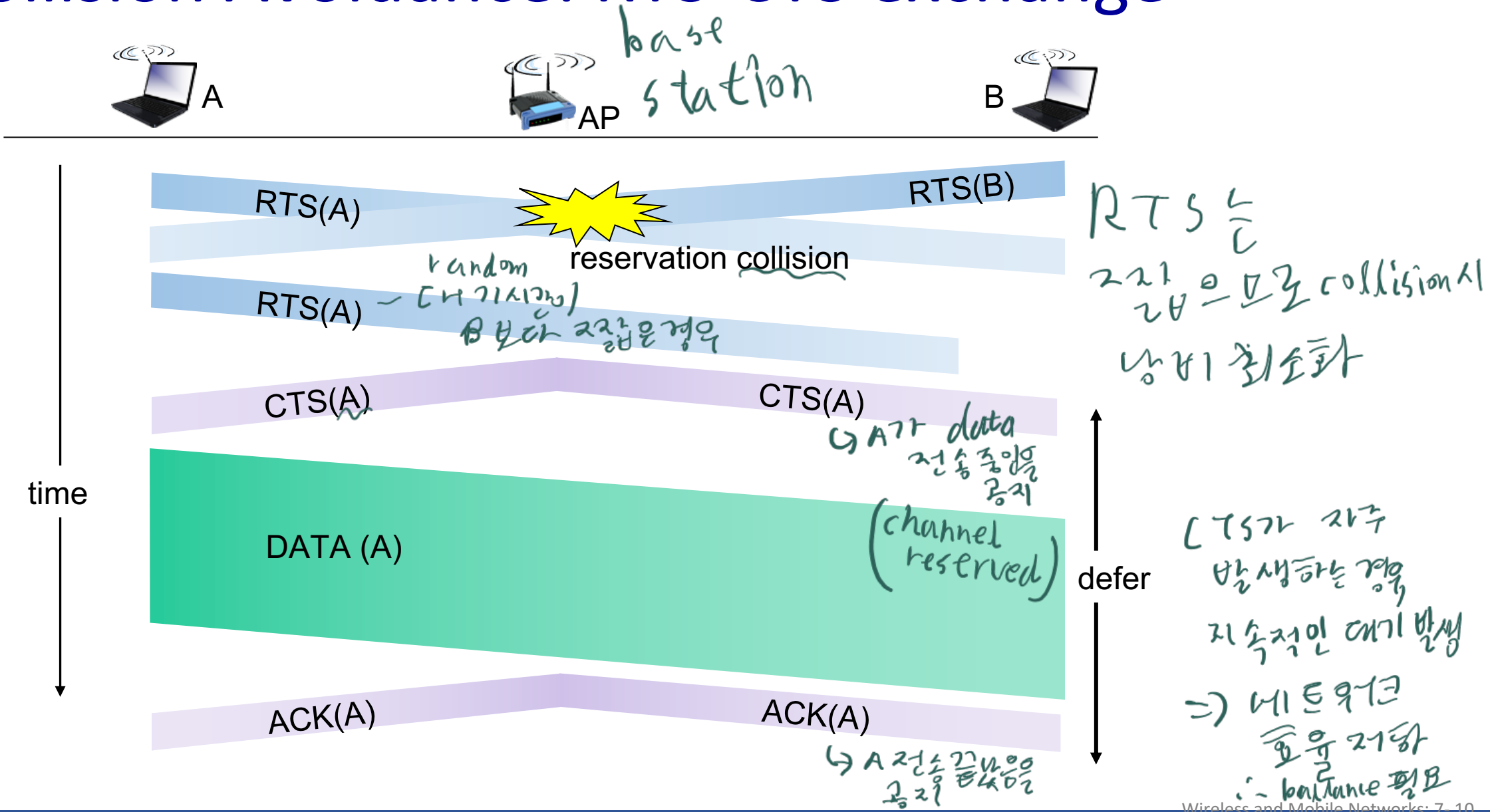
⇒ ACK로 collision 여부 확인

Avoiding collisions (more)

idea: sender "reserves" channel use for data frames using small reservation packets

- sender first transmits *small* request-to-send (RTS) packet to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Collision Avoidance: RTS-CTS exchange



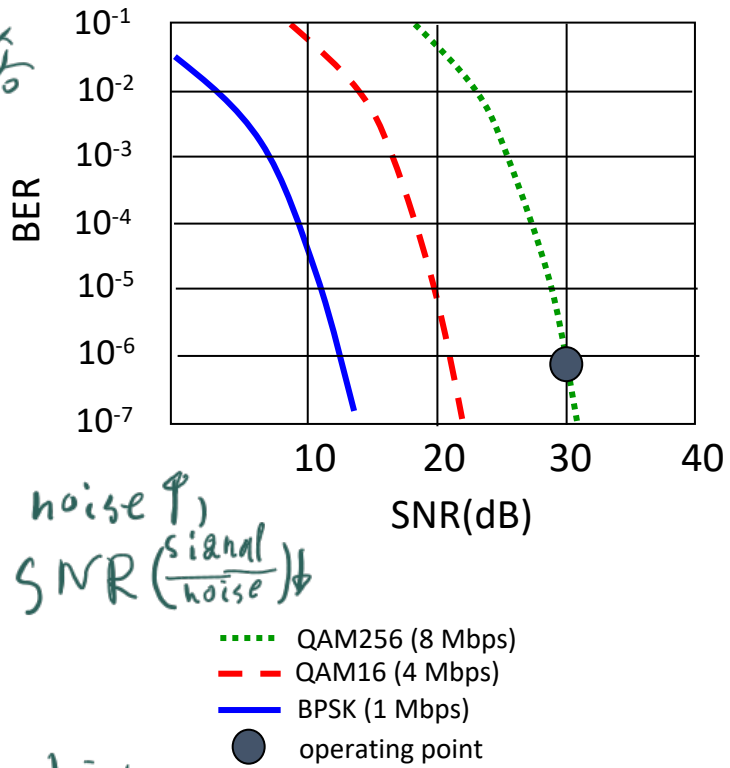
802.11: advanced capabilities

Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies

1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER



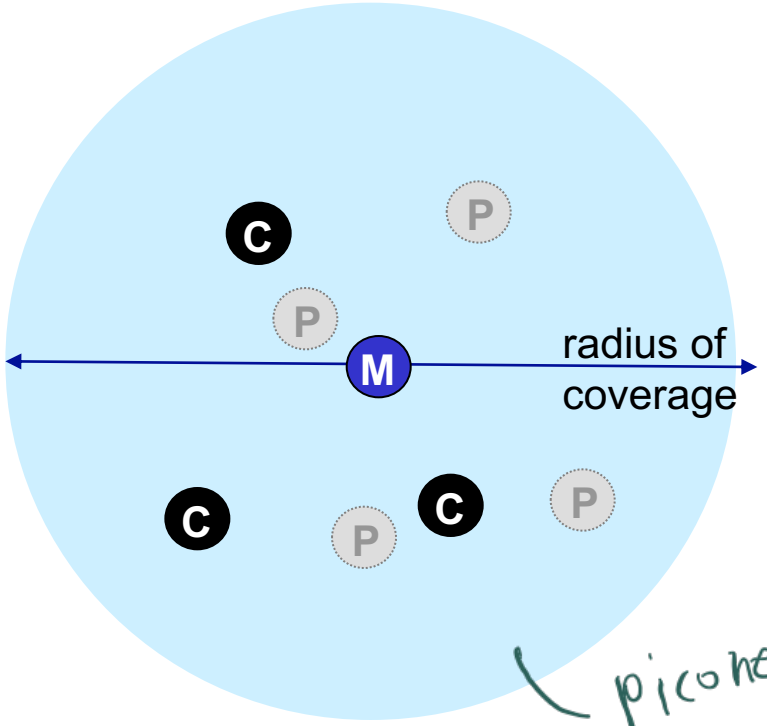
802.11: advanced capabilities

power management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

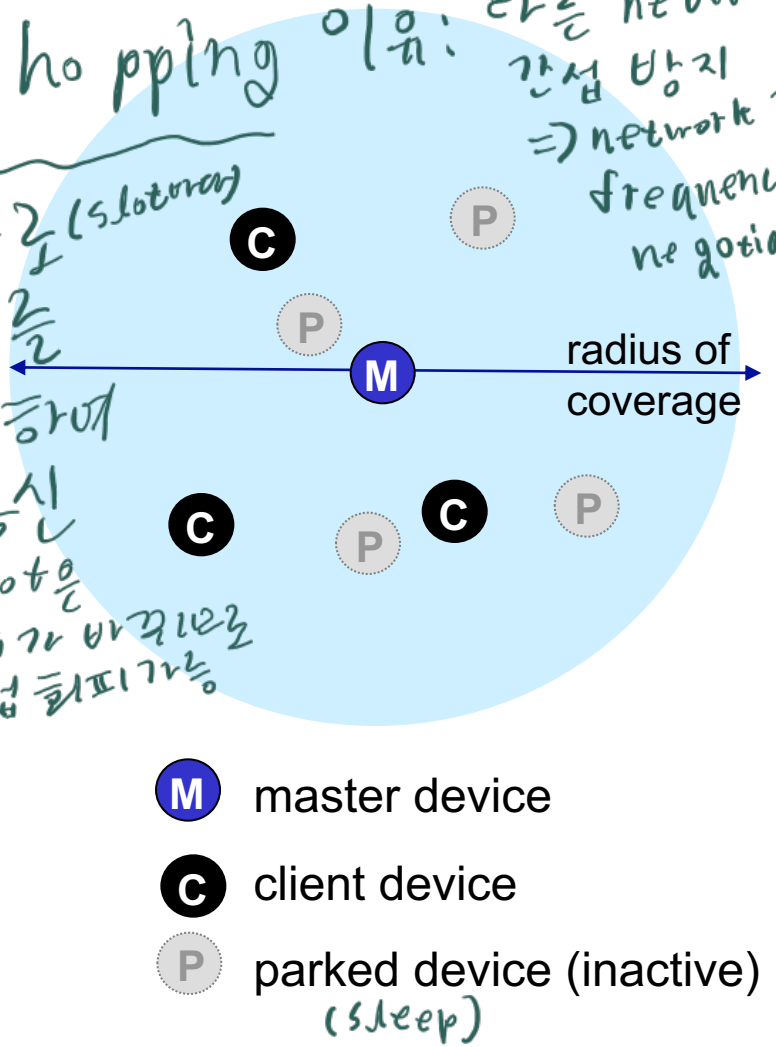
Personal area networks: Bluetooth

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- 2.4-2.5 GHz ISM radio band, up to 3 Mbps
- master controller / clients devices:
  - master polls clients, grants requests for client transmissions



Personal area networks: Bluetooth

- TDM, 625 μsec sec. slot
- FDM: sender uses 79 frequency channels in known, pseudo-random order slot-to-slot (spread spectrum)
  - other devices/equipment not in piconet only interfere in some slots → 간섭이 발생해도, 다음 slot은 주파수가 바뀌므로 간섭 회피가능
- parked mode: clients can "go to sleep" (park) and later wakeup (to preserve battery) → Power management 참조
- bootstrapping: nodes self-assemble (plug and play) into piconet
  ↳ 연결 즉시 사용가능하도록 자가 설정



Chapter 7 outline

bluetooth 등등
wifi
· using in LAN
· random algorithm

- Introduction

Wireless

- Wireless links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G

Mobility

- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

4G/5G cellular networks

2009년부터 4G 상업적 도입, open source화

- *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 → 초고속
- 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

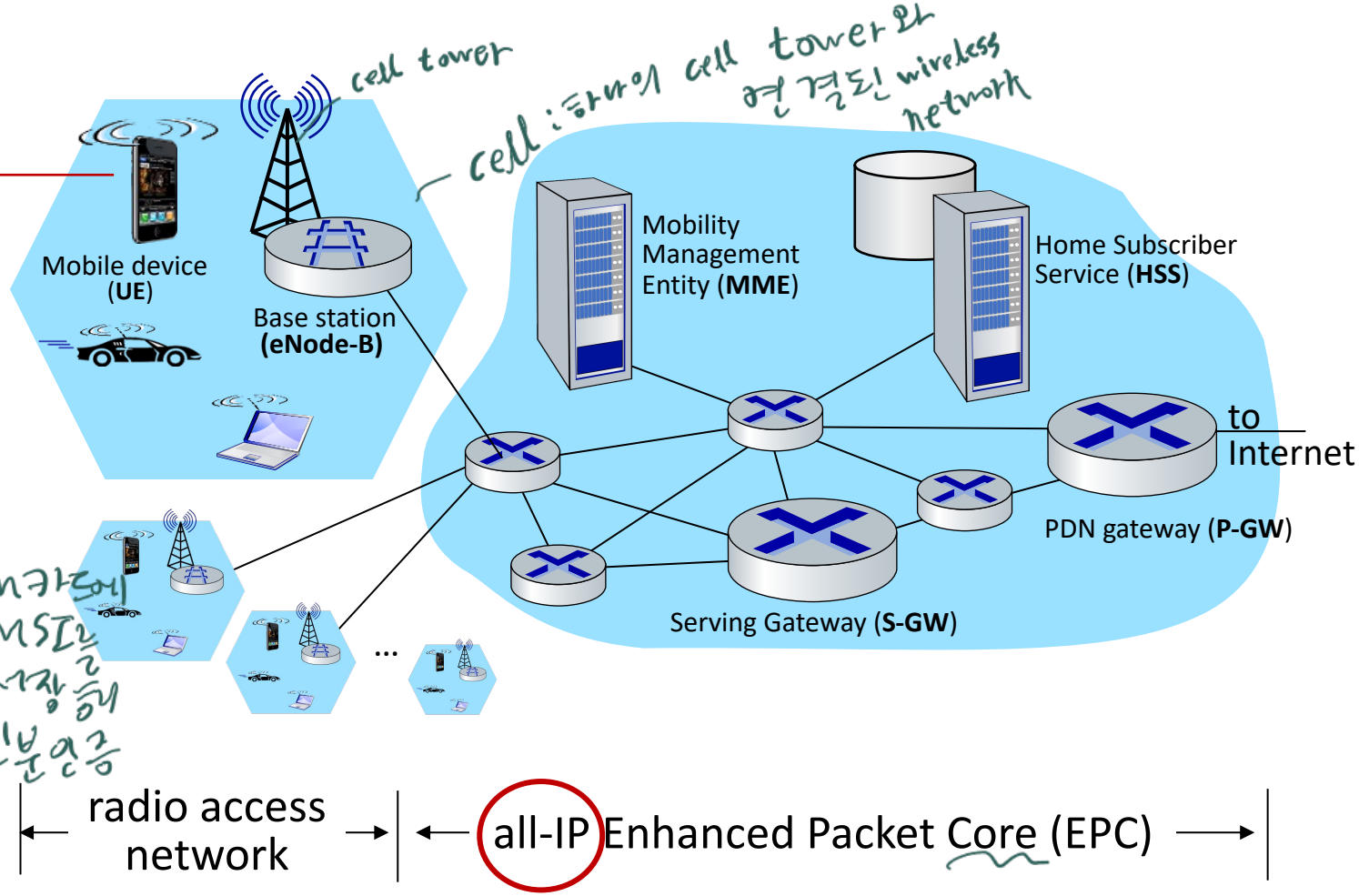
differences from wired Internet

- 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

Elements of 4G LTE architecture

Mobile device:

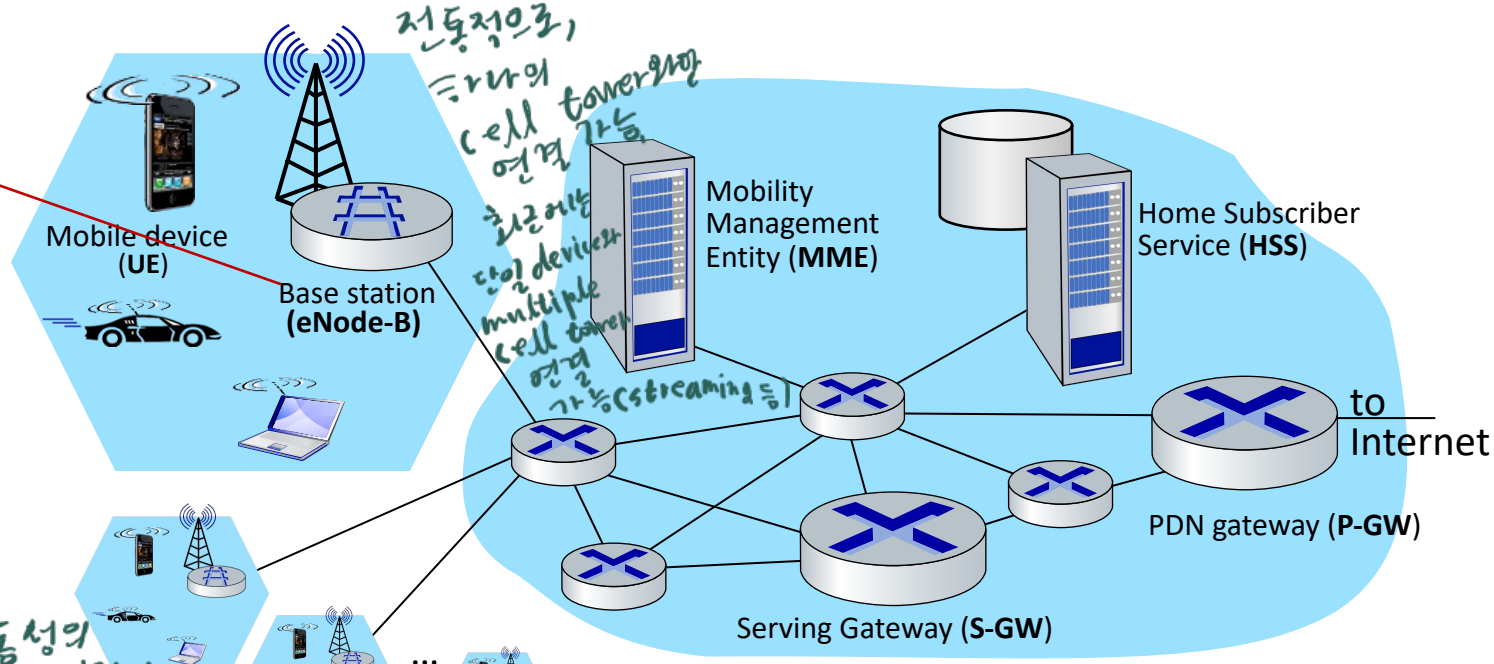
- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- LTE jargon: User Equipment (UE)



Elements of 4G LTE architecture

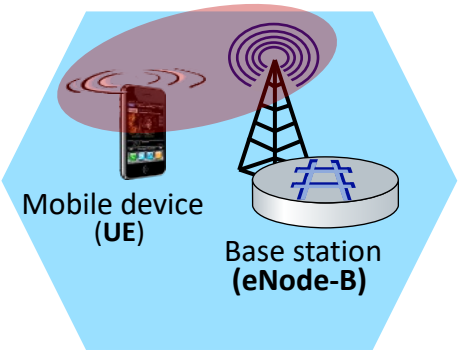
Base station:

- 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

RAN



- connects device (UE) to a base station (eNode-B) → UE와 eNode-B 연결
  - multiple devices connected to each base station 다:1 연결
- 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 업로드/다운로드 채널 분리
- sharing 4G radio channel among users:
  - OFDM: Orthogonal Frequency Division Multiplexing
  - combination of FDM, TDM
- 100's Mbps possible per user/device

eNode-B ↑ ↓ UE

↳ 수직인 주파수 band를 중첩하여 전달률 다시 높임 ⇒ 수직이라 간섭X

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

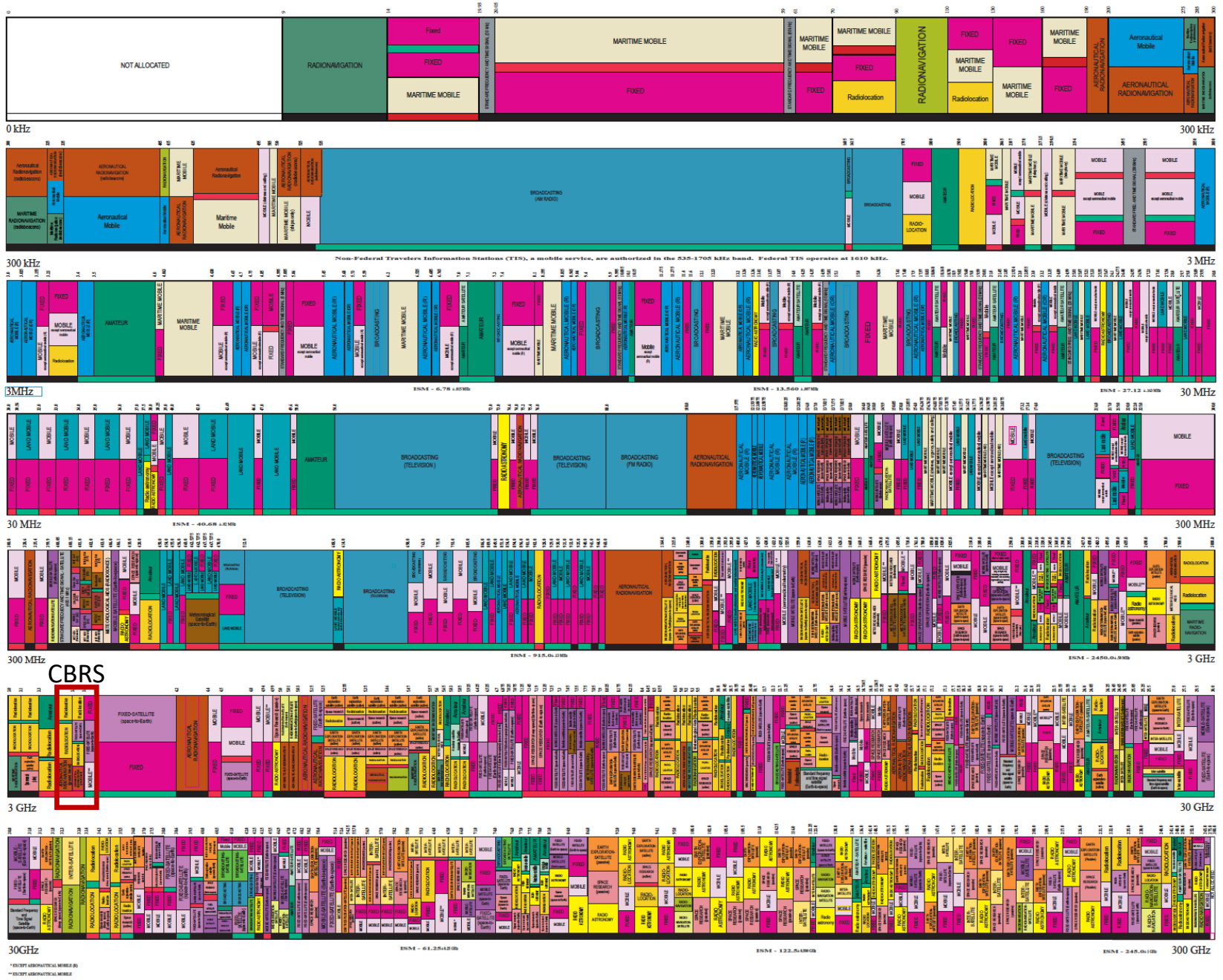
ALLOCATION USAGE DESIGNATION

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 U.S. allocations.

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

JANUARY 2016

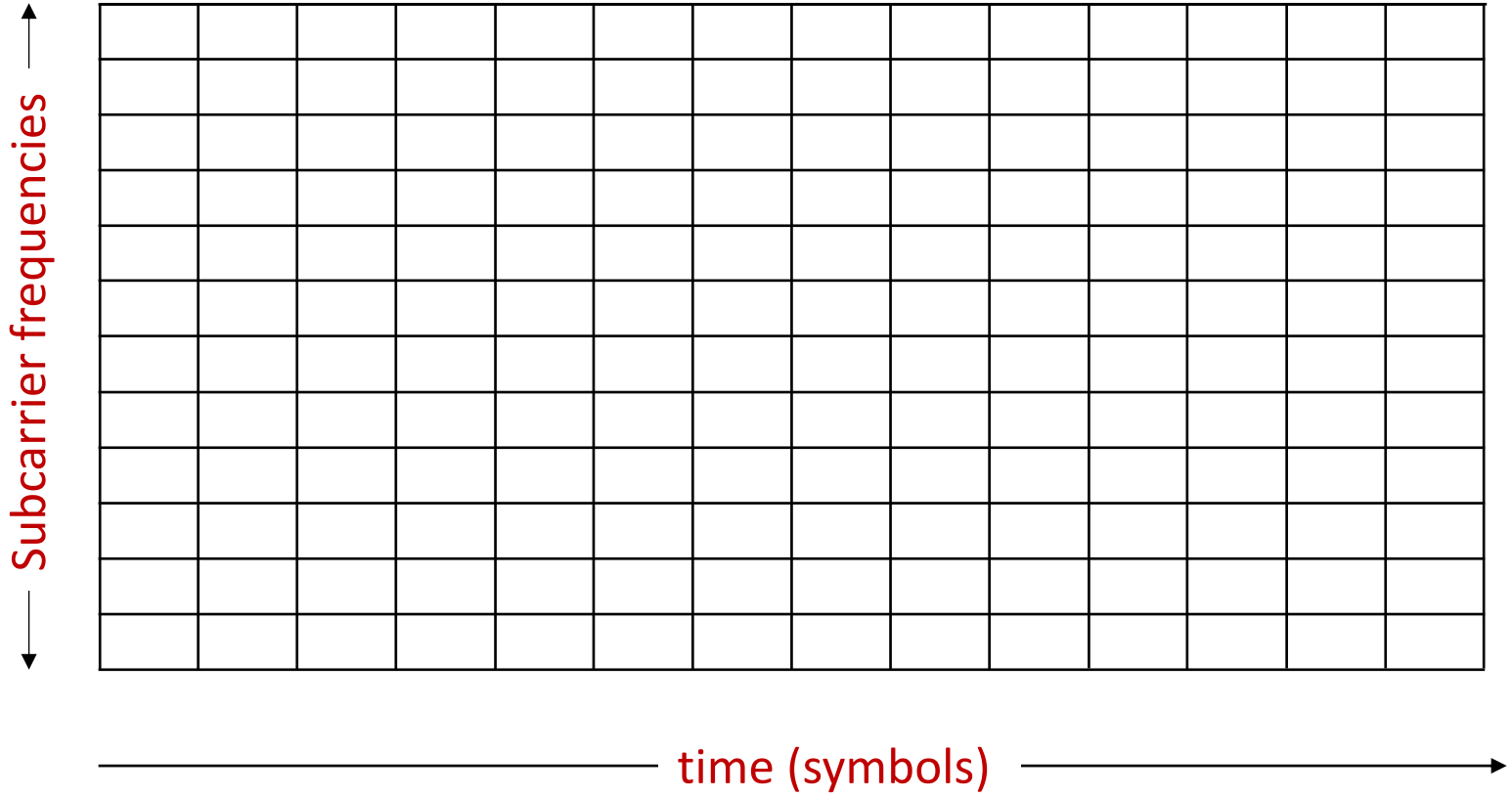


* EXCEPT AERONAUTICAL MOBILE (R)
** EXCEPT AERONAUTICAL MOBILE

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

대역 별 frequency band allocate 상황

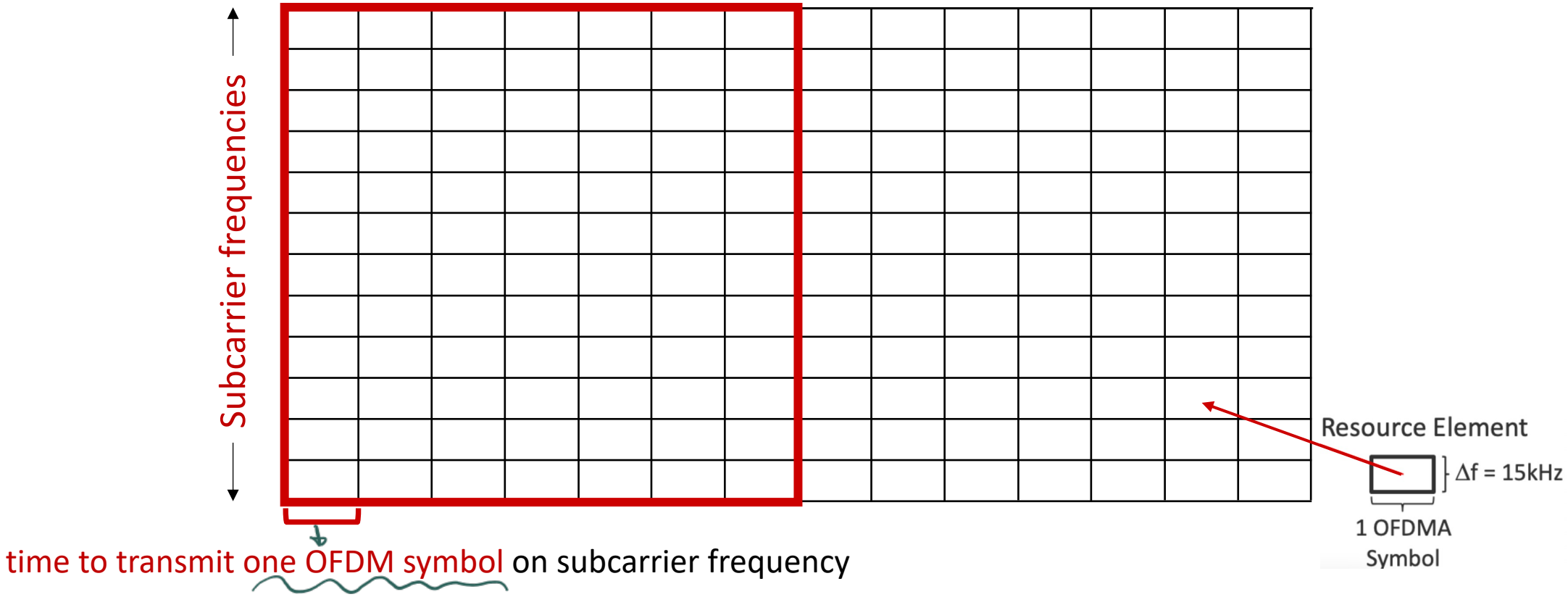
OFDMA: time division (LTE)



OFDMA: time division (LTE)

Physical Resource Block (PRB): blocks of 7x12=84 resource elements

- unit of transmission scheduling



OFDMA:

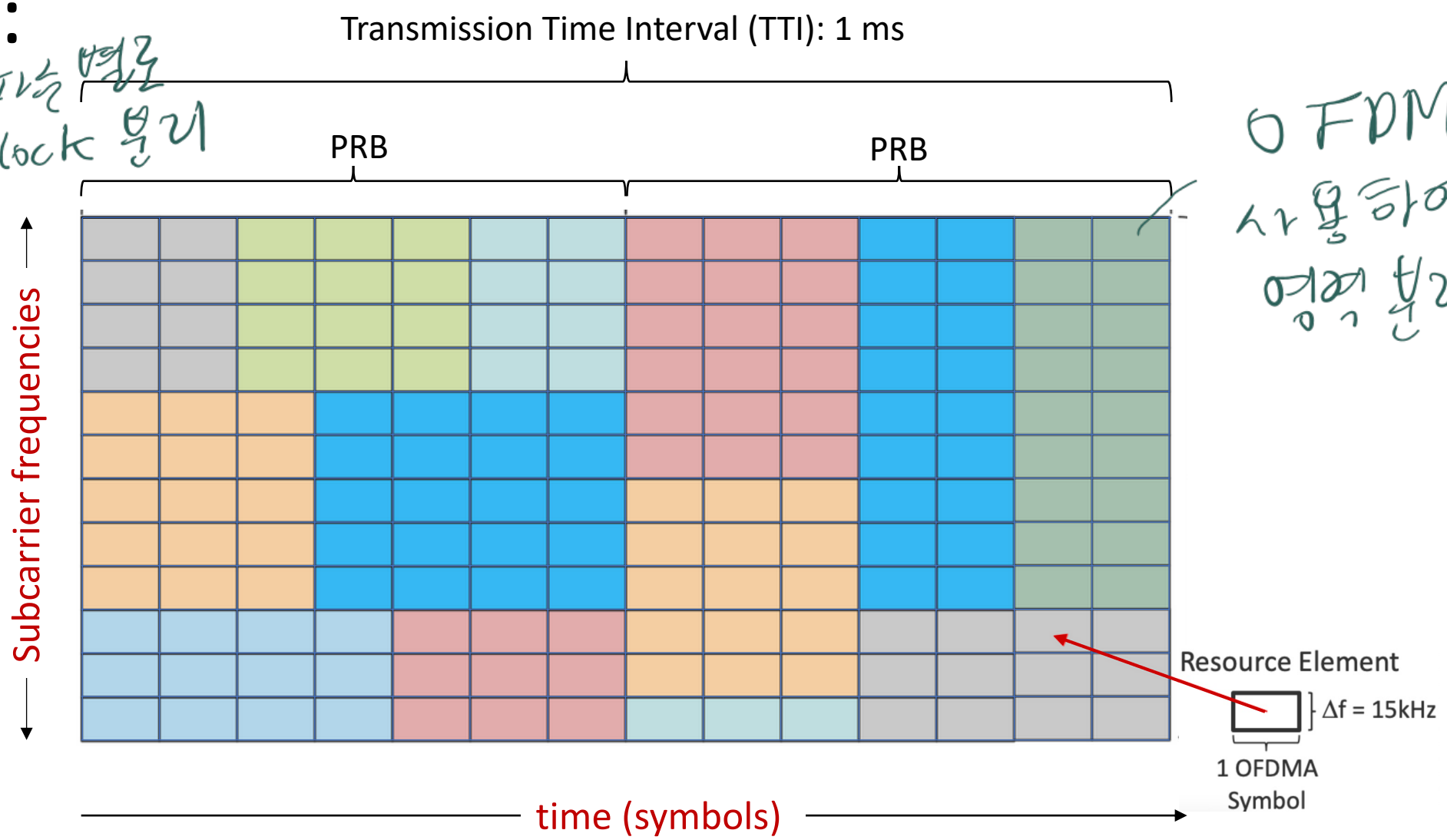
시간 & 주파수 영역 block 묶기

OFDM을 사용하여 영역 묶기

Transmission scheduling example:

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

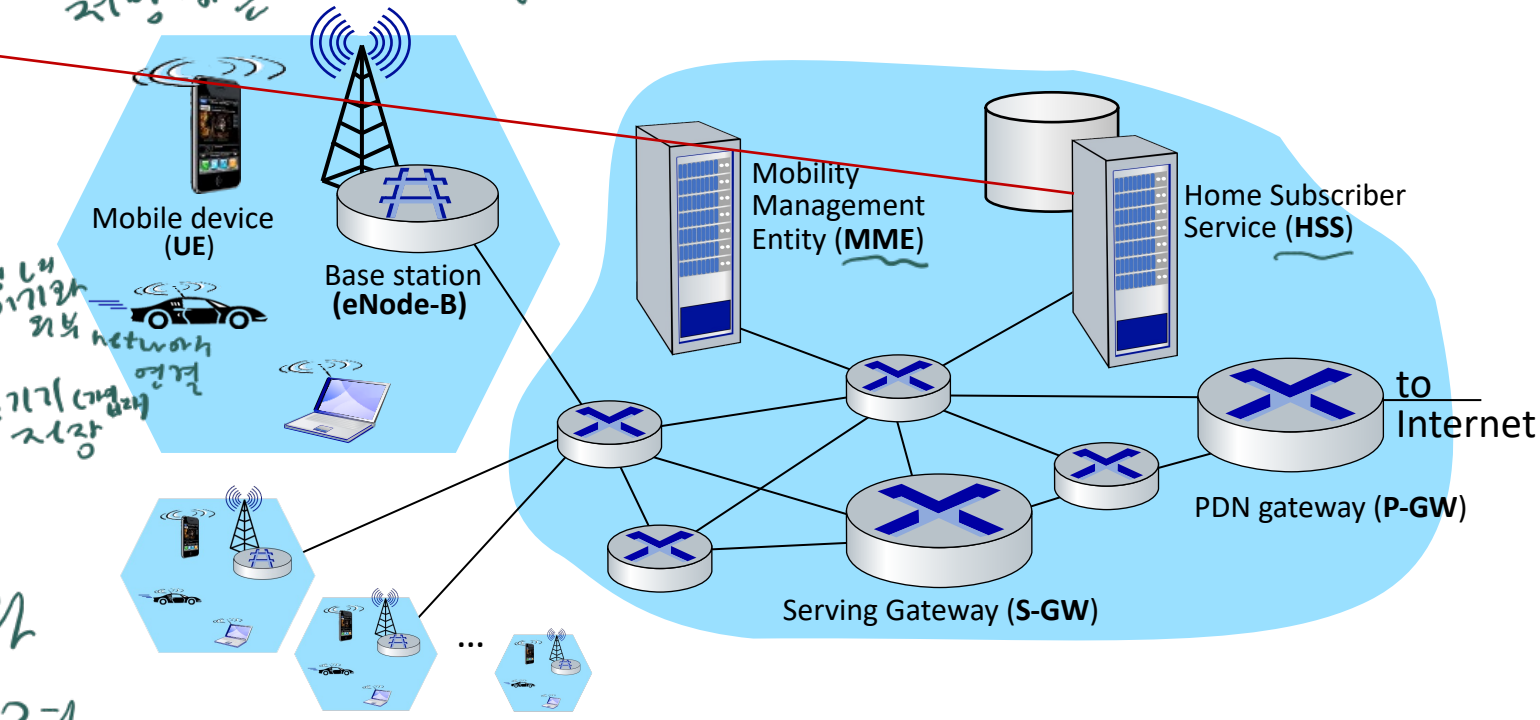
UE_1
UE_2
UE_3
UE_4
UE_5
UE_6
UE_7



Elements of 4G LTE architecture

Home Subscriber Service

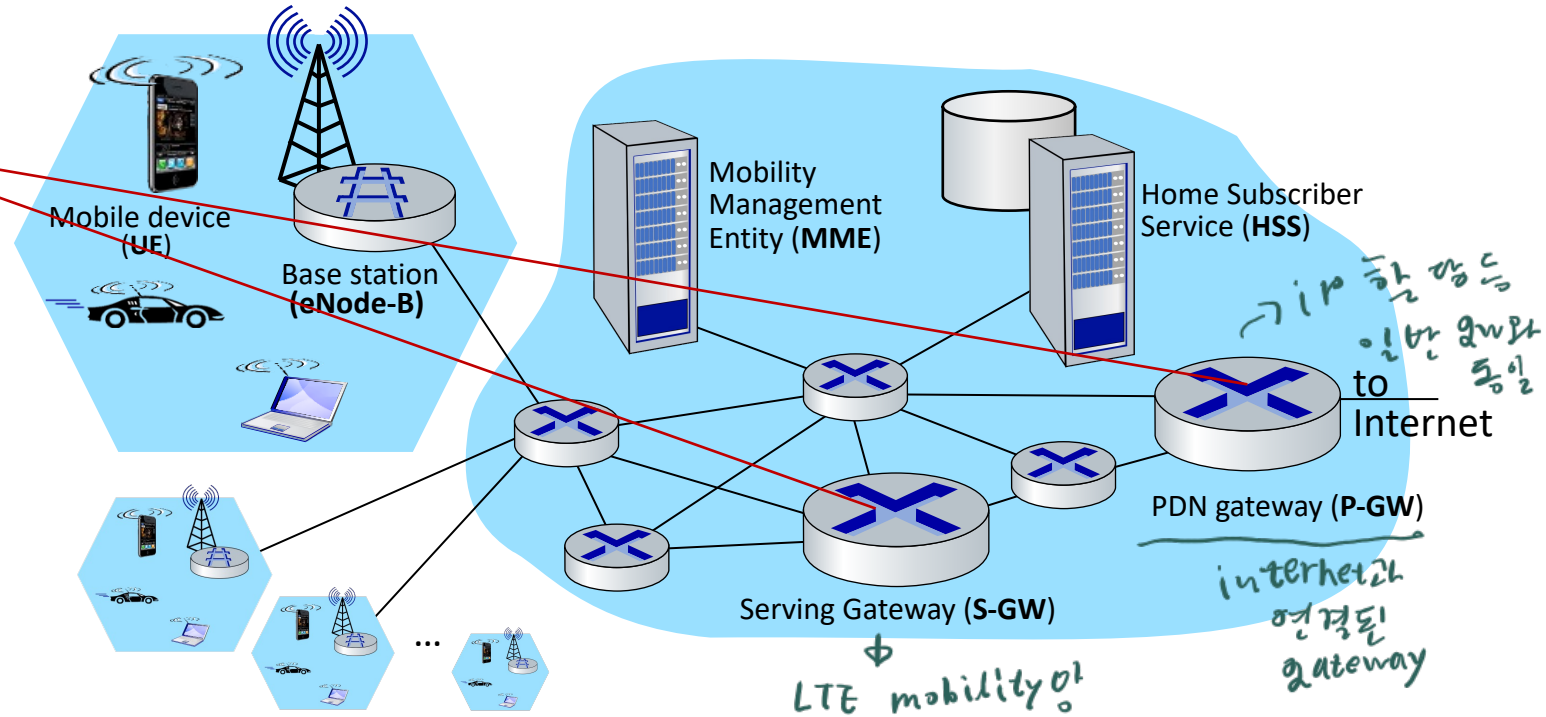
- stores info about mobile devices for which the HSS's network is their "home network"
- works with MME in device authentication



Elements of 4G LTE architecture

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

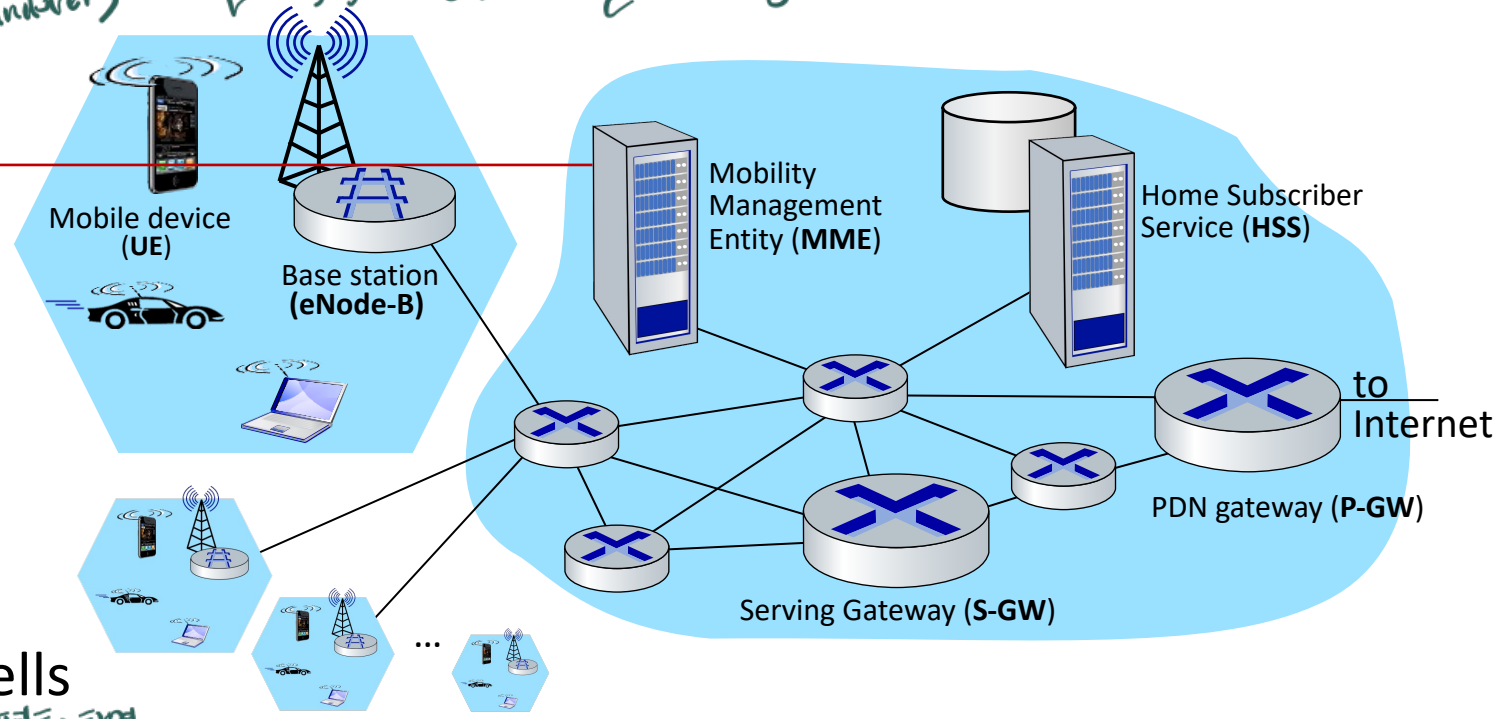
- lie on data path from mobile to/from Internet
- P-GW
  - gateway to mobile cellular network
  - Looks like any other internet gateway router
  - provides NAT services
- other routers:
  - extensive use of tunneling



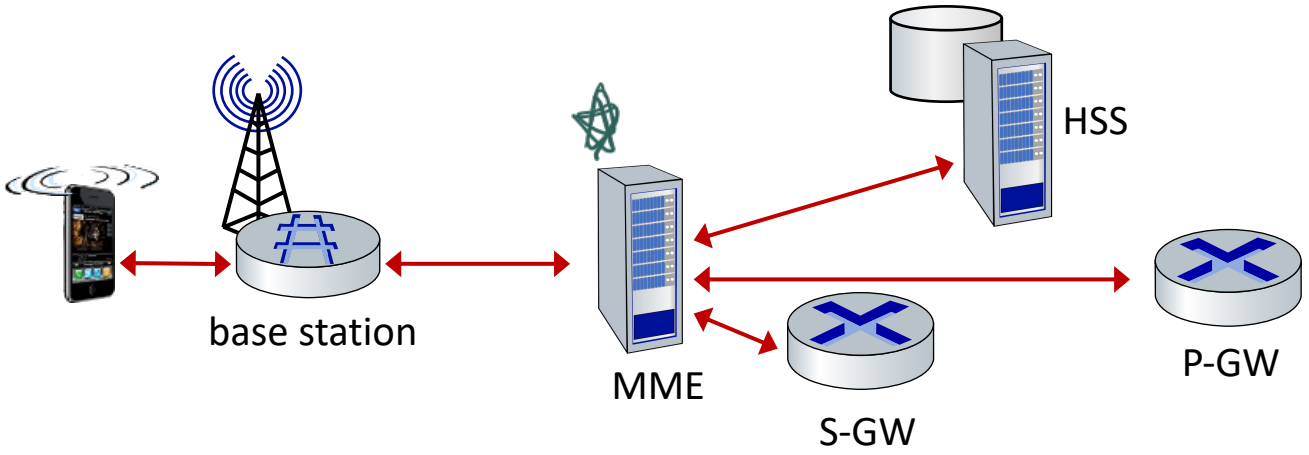
Elements of 4G LTE architecture

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

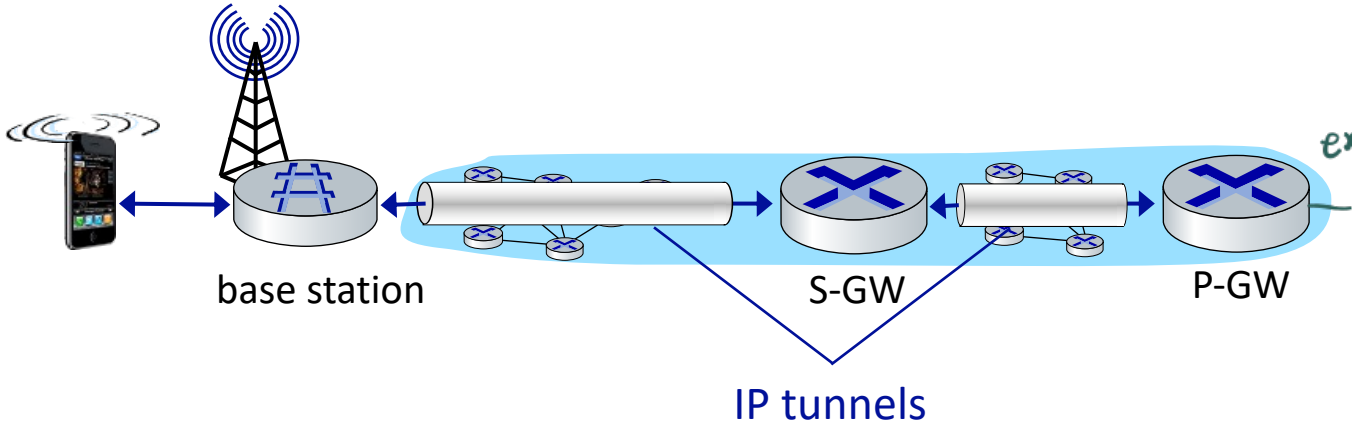


LTE: data plane control plane separation



control plane

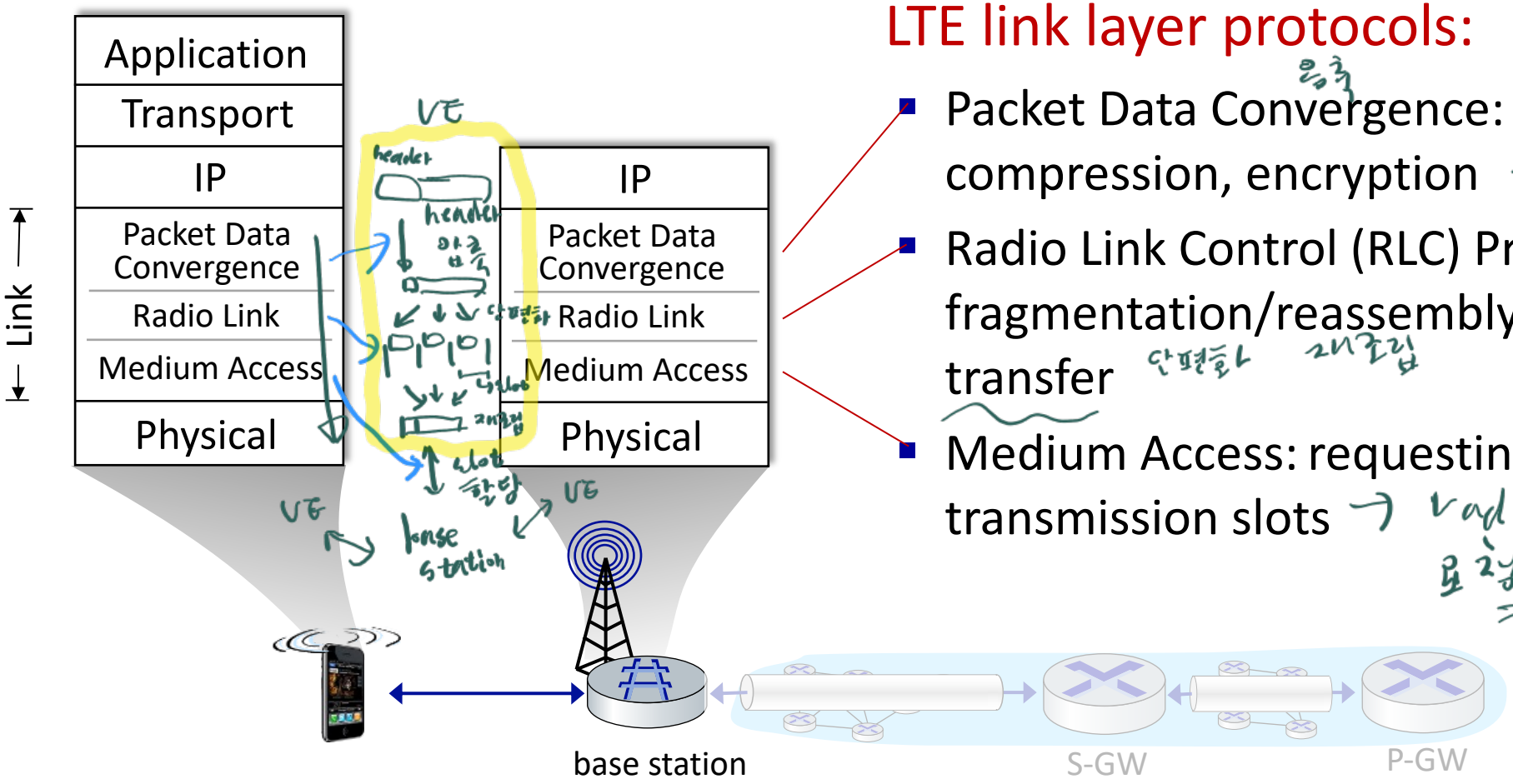
- new protocols for mobility management , security, authentication (later)



data plane

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

LTE data plane protocol stack: first hop

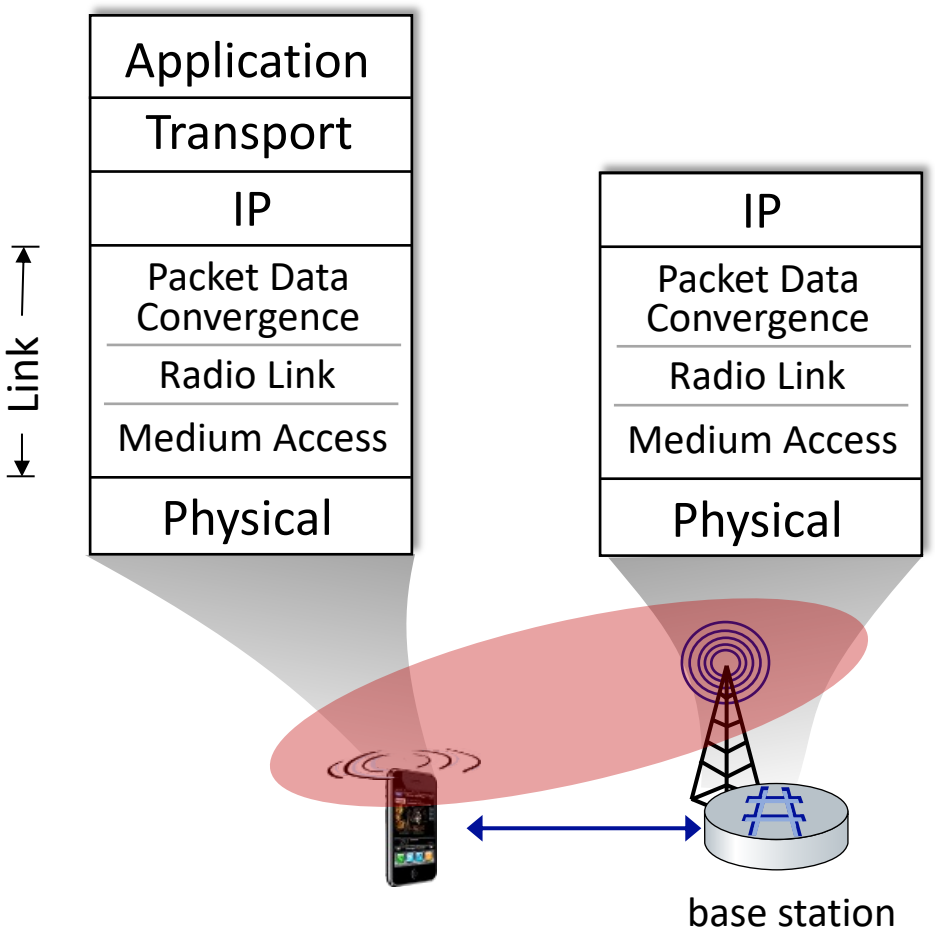


LTE link layer protocols:

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

data plane

LTE data plane protocol stack: first hop



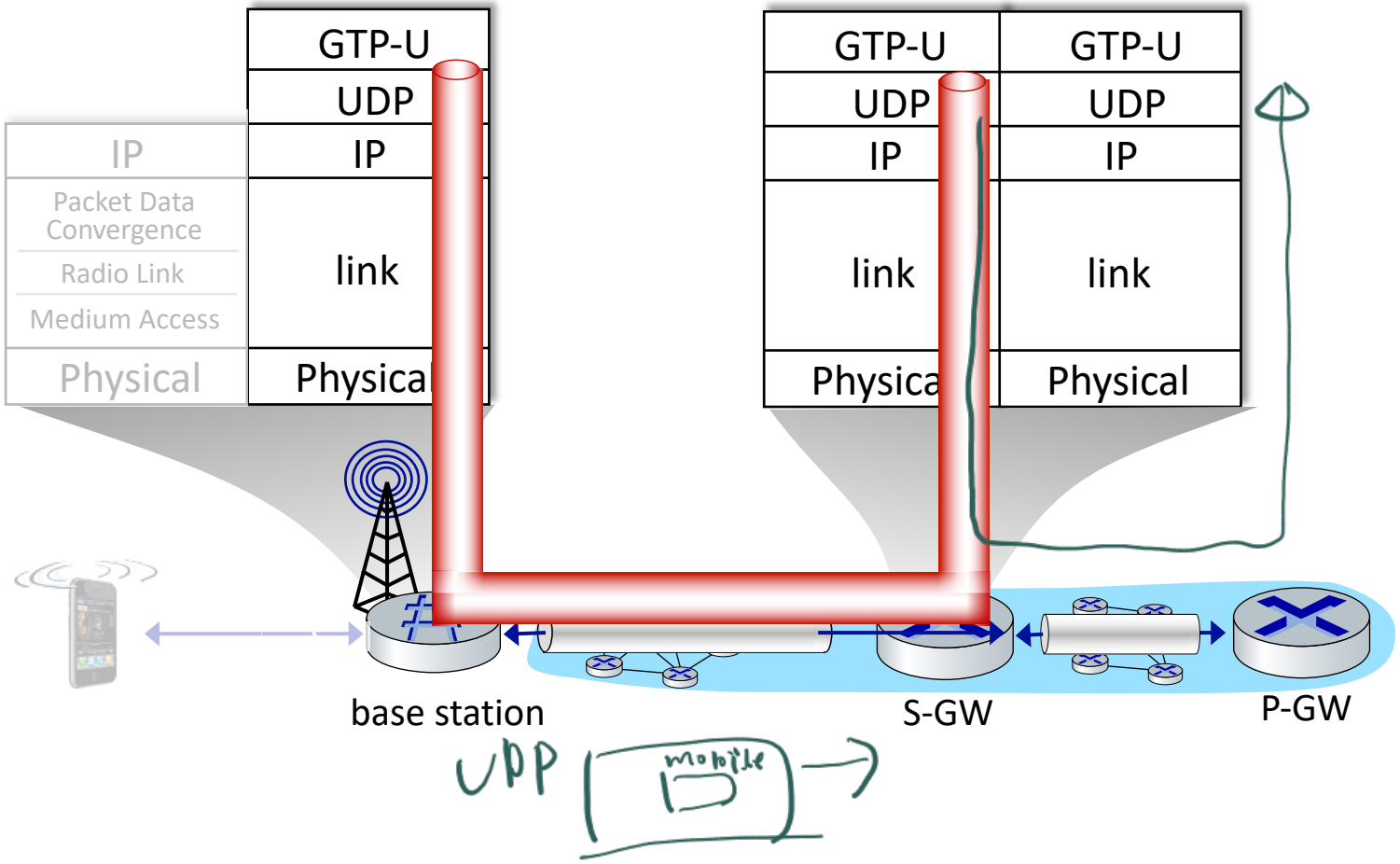
skip

LTE radio access network:

- downstream channel: FDM, 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 over 12 frequencies
  - scheduling algorithm not standardized – up to operator → 스케줄은 운영자에 따라 다름
  - 100's Mbps per device possible

LTE data plane protocol stack: packet core

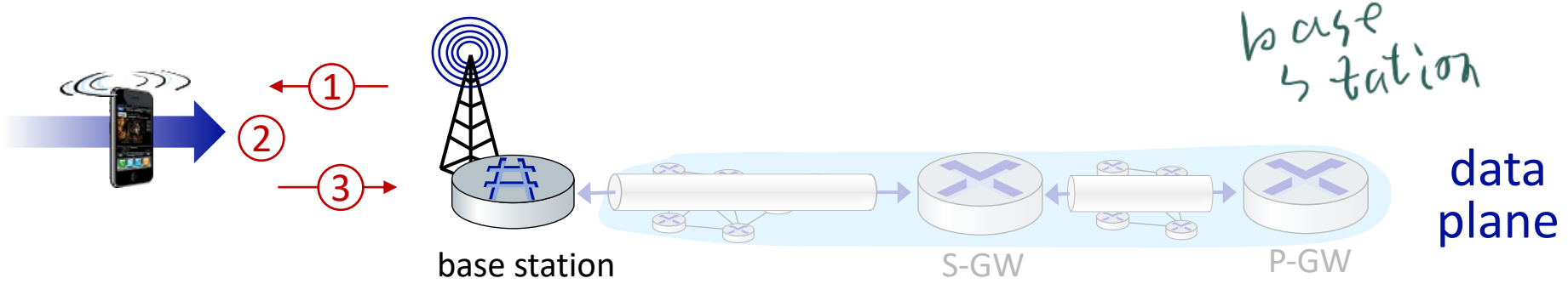
상위 layer 정보 이동



tunneling:

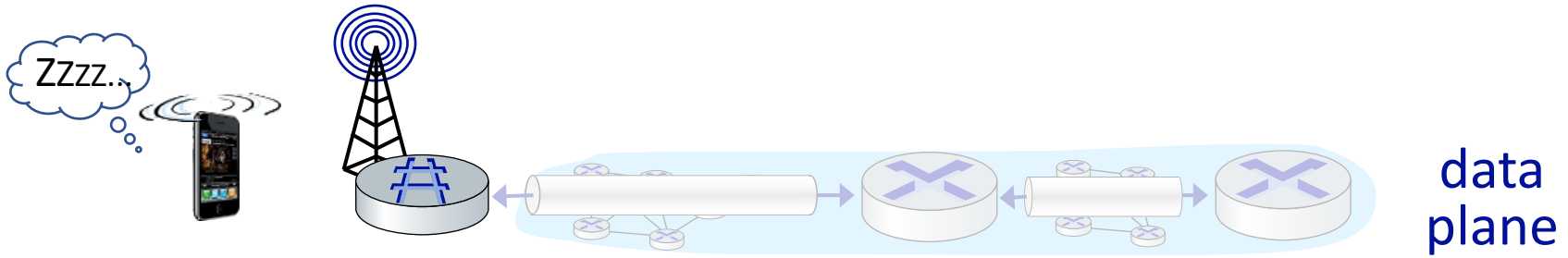
- mobile datagram encapsulated using GPRS Tunneling Protocol (GTP), sent inside UDP datagram to S-GW
- S-GW re-tunnels datagrams to P-GW
- supporting mobility: only tunneling endpoints change when mobile user moves (base station 변경)

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

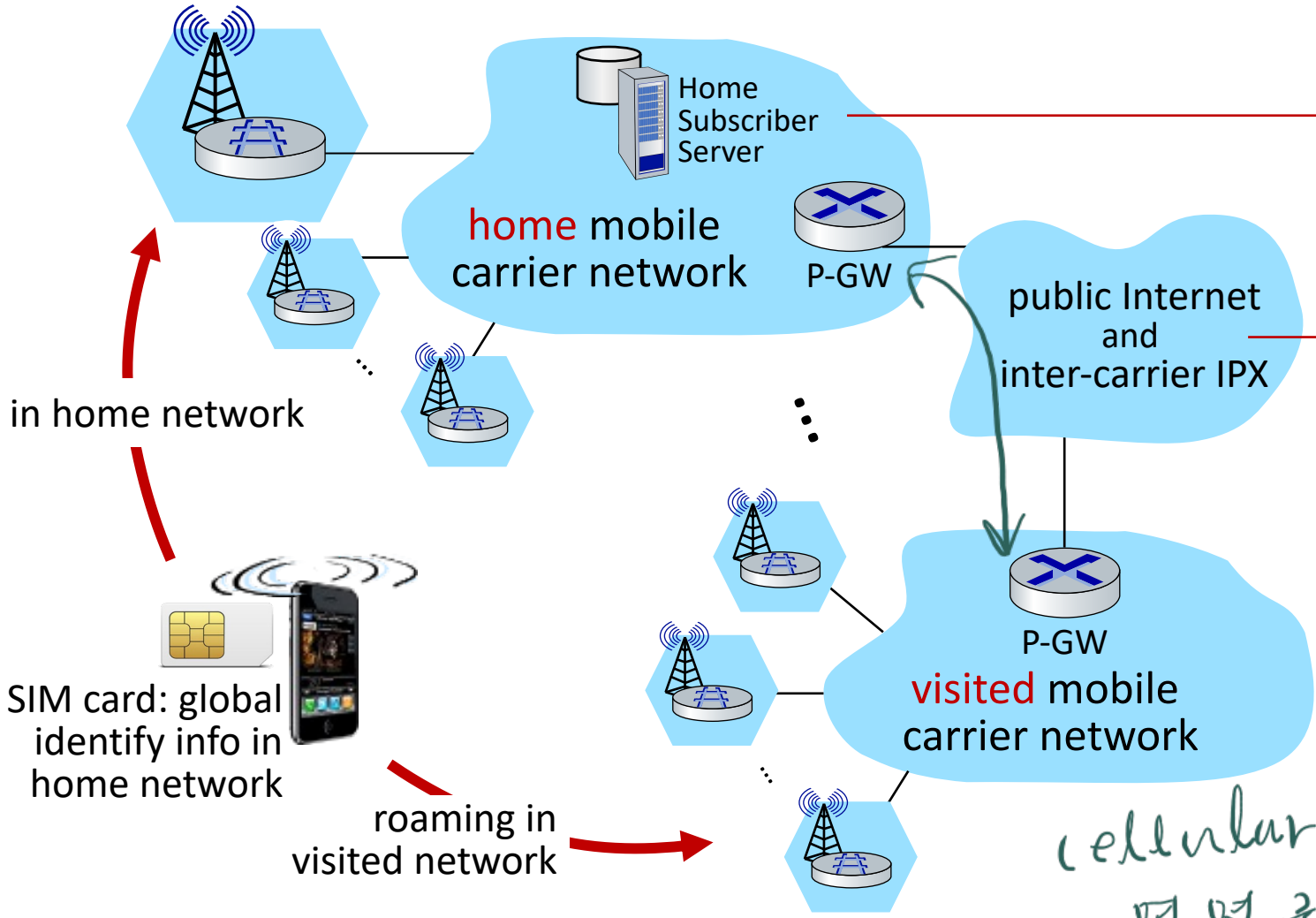
LTE mobiles: sleep modes



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:

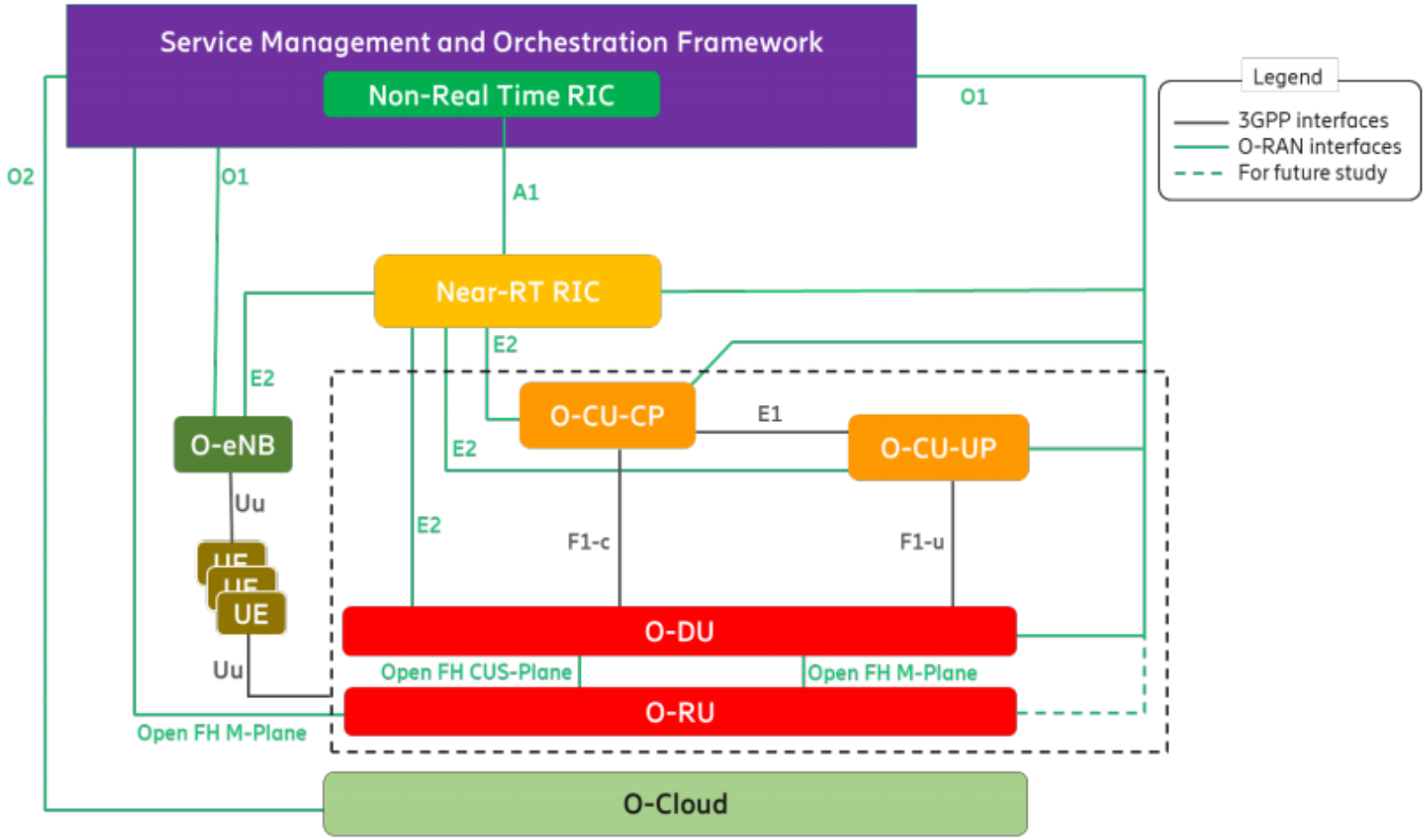
- carriers interconnect with each other, and public internet at exchange points
- legacy 2G, 3G: not all IP, handled otherwise

(cellular network는 phone network, 몇 몇 국가는 감청 가능 (lawful interception)
⇒ 정부 개입으로 인해 security hole 존재

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

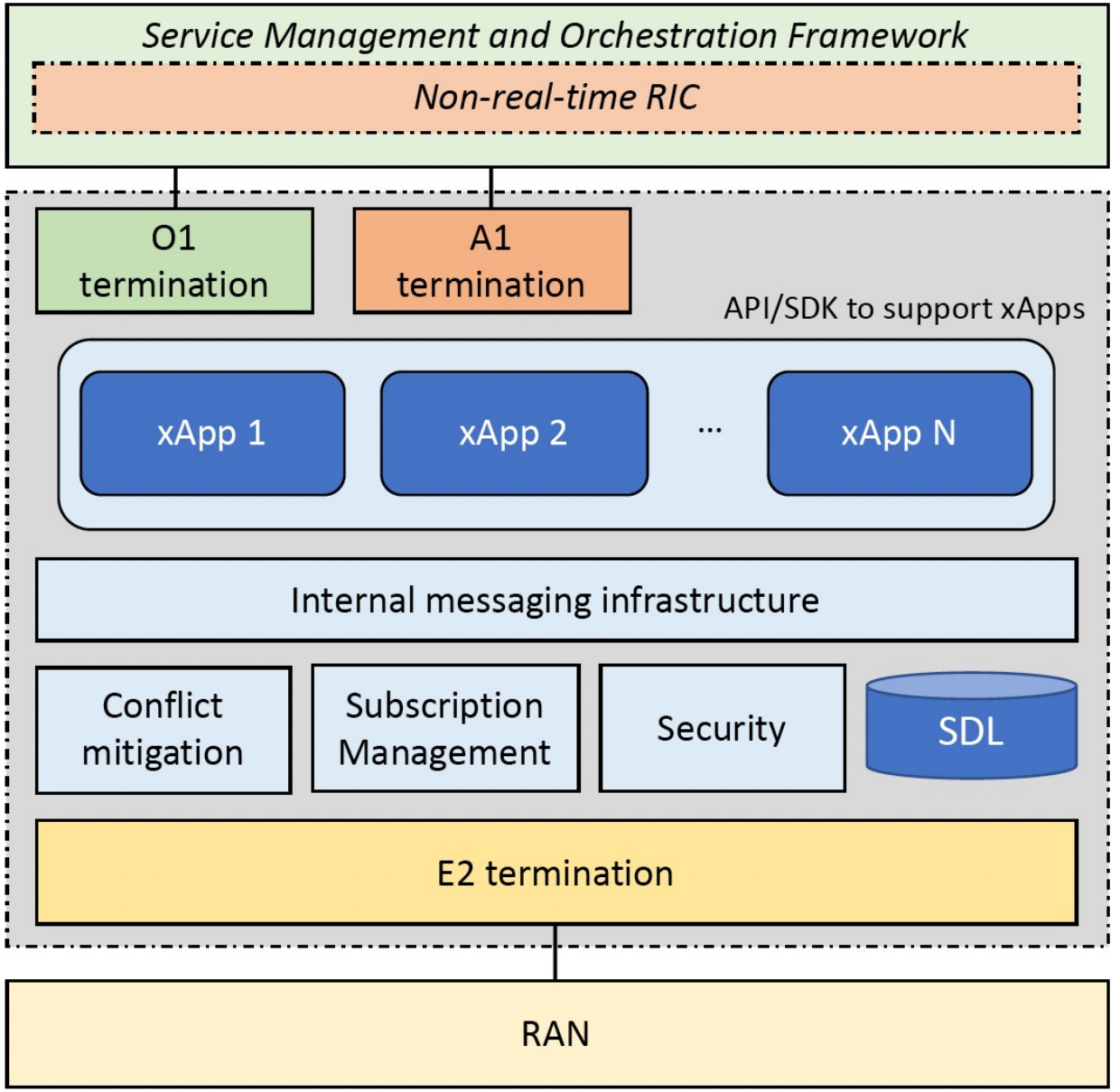
O-RAN Architecture



[source: : O-RRAN Alliance, O-RAN.WG1.O-RAN-Architecture-Description-v06.00]

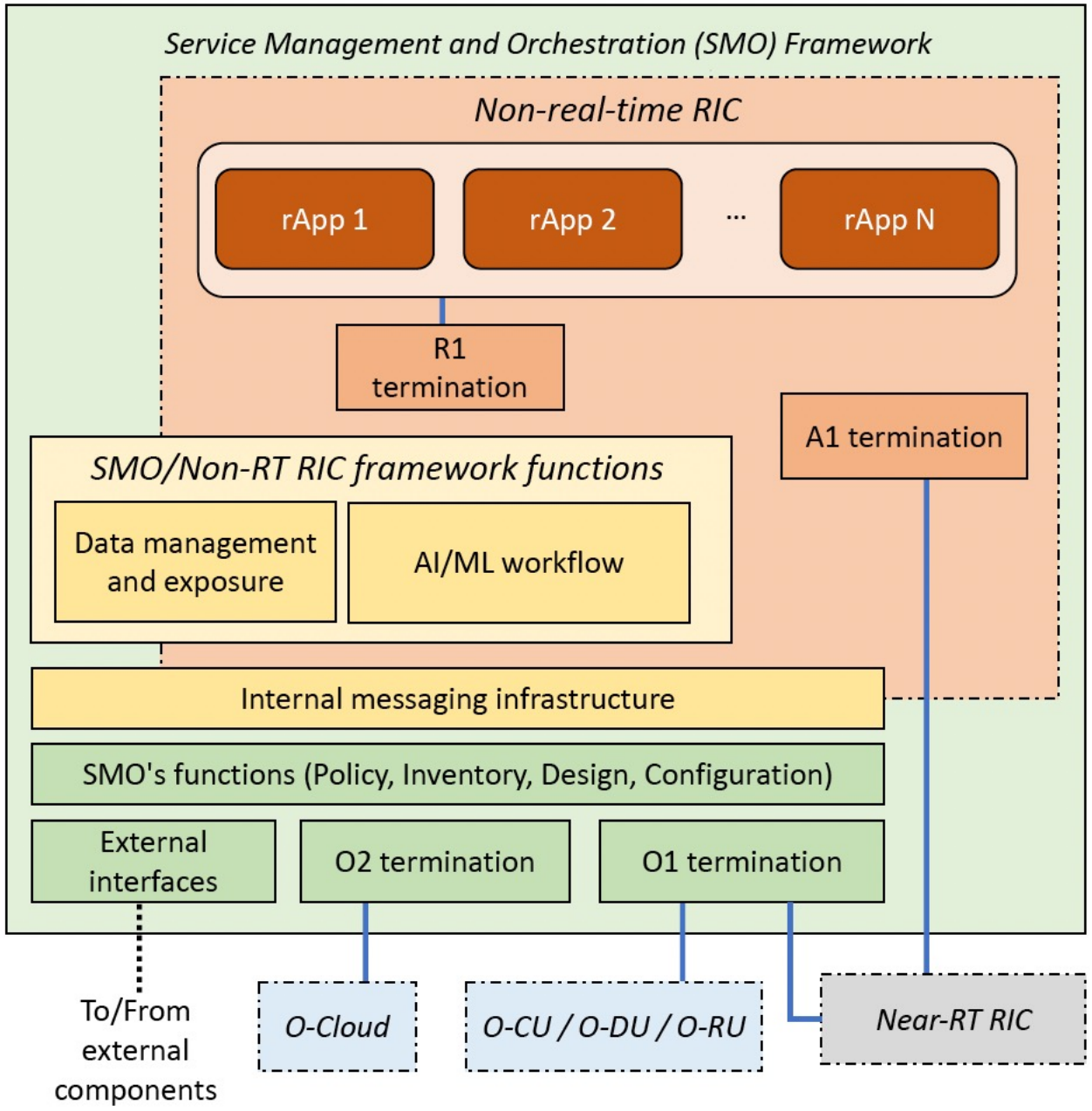
O-RAN

- Near-RT RIC architecture



O-RAN

- Non-RT RIC architecture



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)

Chapter 7 summary

Wireless

- Wireless Links and network characteristics
- WiFi: 802.11 wireless LANs
- Cellular networks: 4G and 5G

Mobility

- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

Next…

- *Chapter 8.1 What Is Network Security?*
- *Chapter 8.2 Principles of Cryptography*
- *Chapter 8.3 Message Integrity and Digital Signatures*