

Lecture 11

Wireless Networks

ELEC 3506/9506
Communication Networks

Dr Wibowo Hardjawana
School of Electrical and Information
Engineering

Topics of the Day

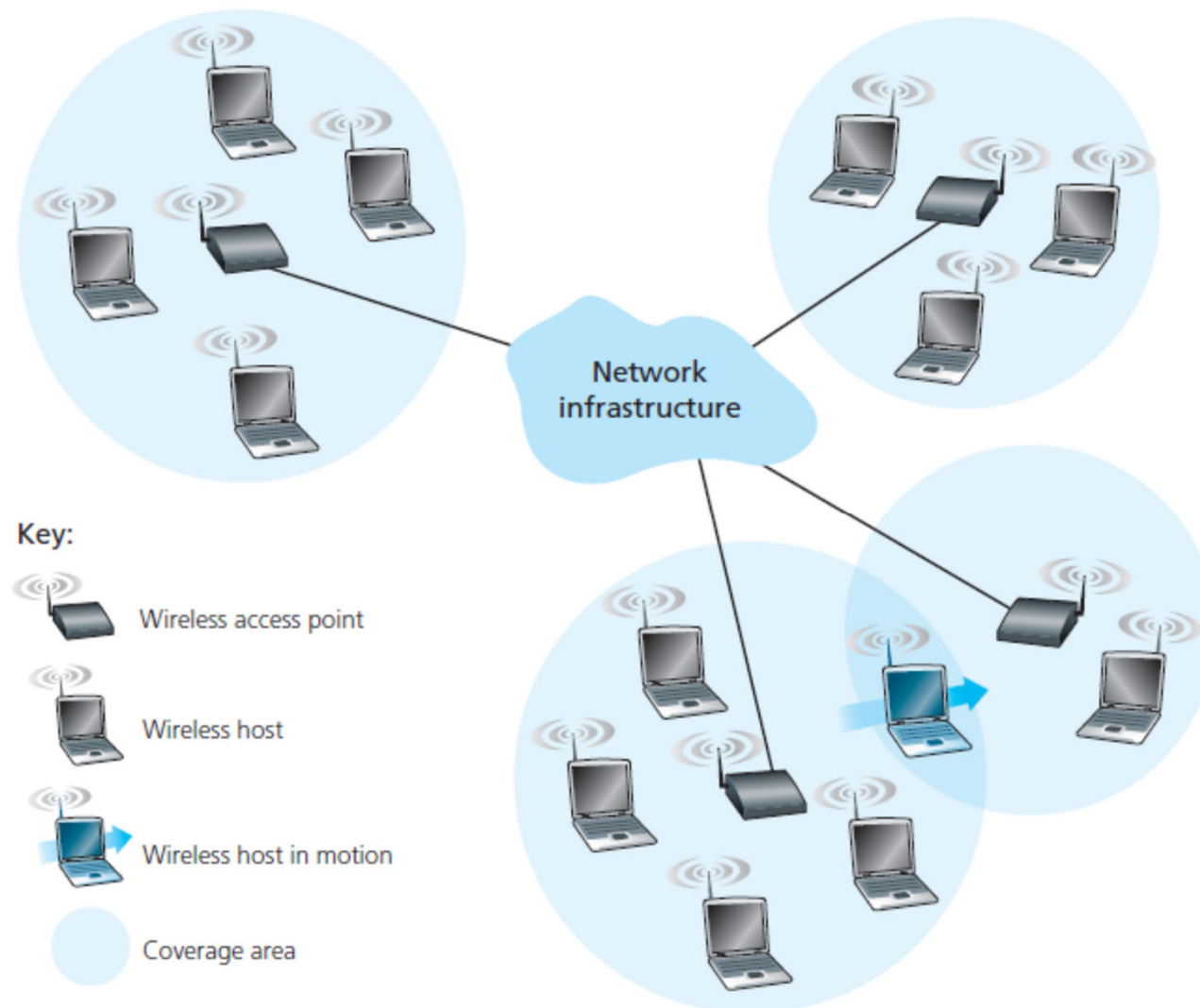
- Introduction to Wireless Networks
- Wireless Local Area Networks (WLANs):
 - IEEE 802.11 Architectures
 - Multiple Access
 - Related Issues
- Cellular Networks:
 - Cellular Telephony Evolution: ~~1G, 2G, 2.5G, 3G, 4G~~, 5G.....
 - Network Architectures
- Satellite
- Bluetooth

Introduction

- Number of wireless (mobile) phone subscribers now exceeds the number of wired phone subscribers !
- Demand for anytime, anywhere, and anyhow Internet access
- **Challenges/Issues**
 - Mobility management
 - QoS Management
 - Channel conditions
 - Security



Elements of Wireless Network

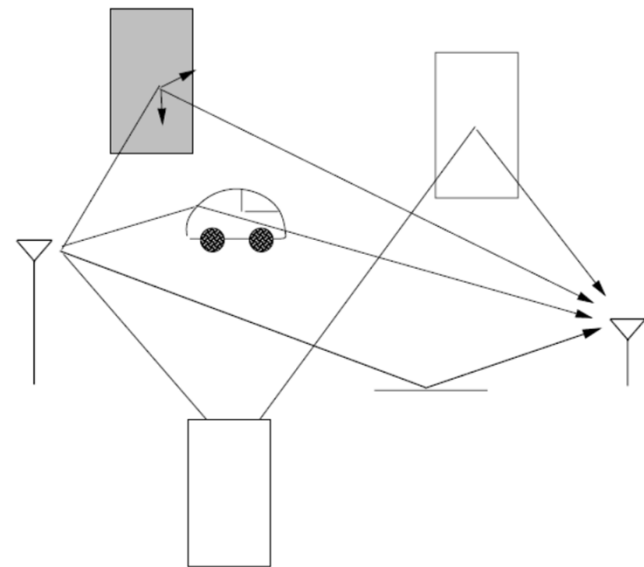
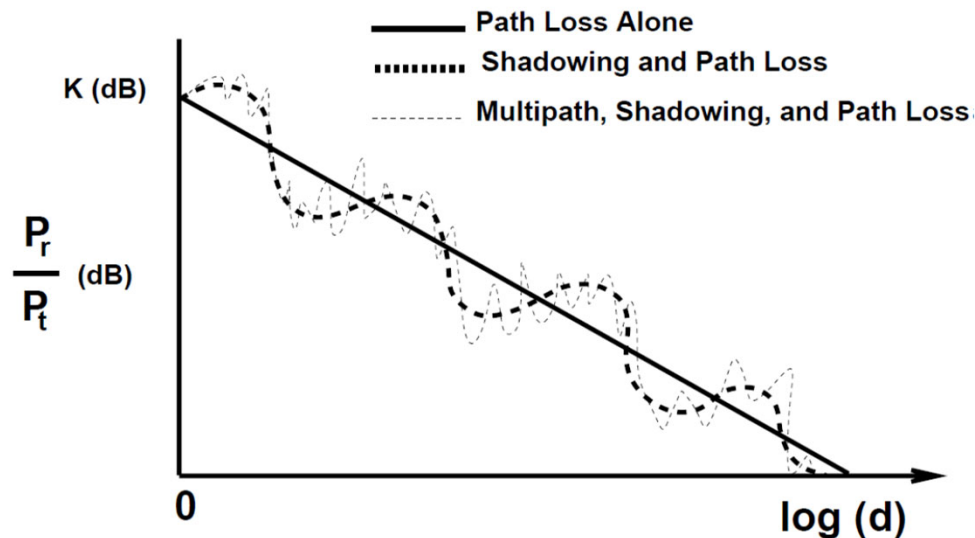


Elements of Wireless Network

- **Wireless hosts:** the end-system devices that run applications, e.g., laptop, smartphone
- **Base station:** responsible for
 - sending and receiving to and from a wireless host that is associated with that base station.
 - coordinating the transmission of multiple wireless hosts
 - E.g. cell towers and access points
- **Wireless links:** the connection between host and base station. Key characteristics: coverage and rate
- **Network infrastructure:** the larger network with which a wireless host may wish to communicate.

Wireless v.s. Wired Links

- **Signal attenuation:** Electromagnetic signal attenuates over distance (Path Loss)
- **Interference from other source:** broadcast nature of wireless signals
- **Multipath propagation:** due to signal reflection. May cause fading, inter-symbol interference (ISI)
- **Error:** errors are more serious issues in wireless links than wired links



Wireless Networks

■ Wireless LAN (WLAN):

- IEEE 802.11
- IEEE 802.11 a, b, g, n, h, ax
- Ad-hoc, Wireless Mesh

■ Satellite:

- IRIDIUM
- Globalstar

■ Other:

- Sensor Networks (BAN)
- PAN (Bluetooth / ANT)
- LP-WAN - IOT

■ Cellular:

- 1G: *AMPS*
- 2G: *D-AMPS, GSM, IS-95 (CDMA-ONE)*
 - *2.5G - GPRS*
 - *2.75G - EDGE*
- 3G: UMTS (WCDMA), CDMA2000
 - *3.5G - HSPA*
 - *3.75G - HSPA+*
- 4G: LTE, LTE-A, WiMAX (Some Versions)
- 5G NR

Wireless Local Area Networks (WLANs)

- **WLAN:** one of the most important access network technologies in the Internet today
- Provides **high speeds** with **limited mobility:** home, office, airport...
- Low-cost network scalability, and high-speed access
- **Unlicensed spectrum** reduces the user's cost

Wireless LANs

- IEEE specifications for a wireless LAN
 - IEEE 802.11 (WiFi)
 - Covers the physical and data link layers
 - 802.11a/b/g/n
- Defines two kinds of services
 - Basic service set (BSS): building block of a wireless LAN
 - Extended service set (ESS) : made up of two or more BSSs with access points (APs)

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

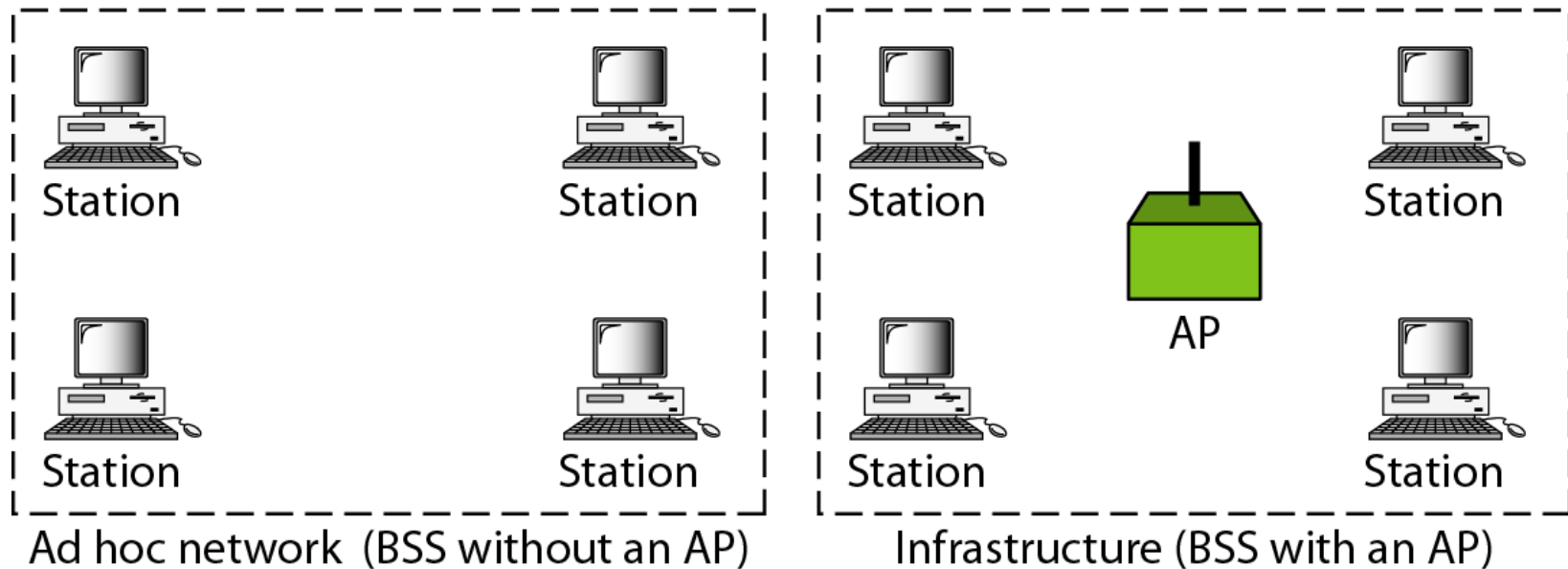
- The three 802.11 standards use the same medium access protocol: **CSMA/CA**
- Use the same frame structure for the link-layer frames
- Allow both “infrastructure mode” and “ad hoc mode ”

Basic Service Set (BSS)

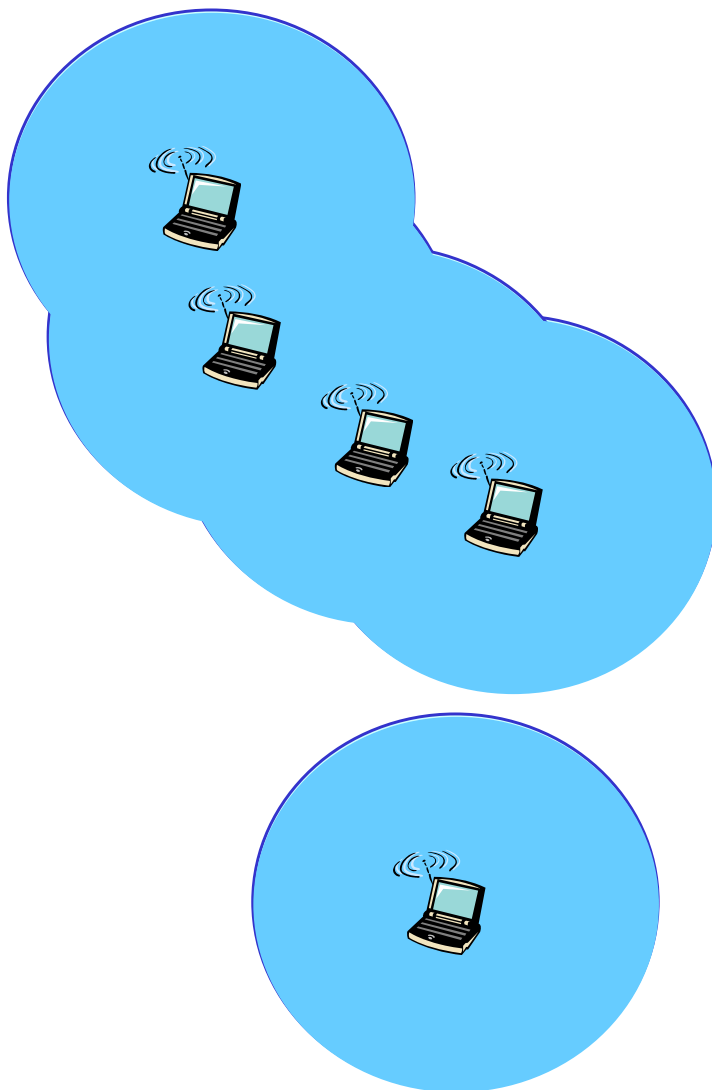
- BSS without an AP is called an **ad hoc network**
- BSS with an AP is called an **infrastructure network**

BSS: Basic service set

AP: Access point



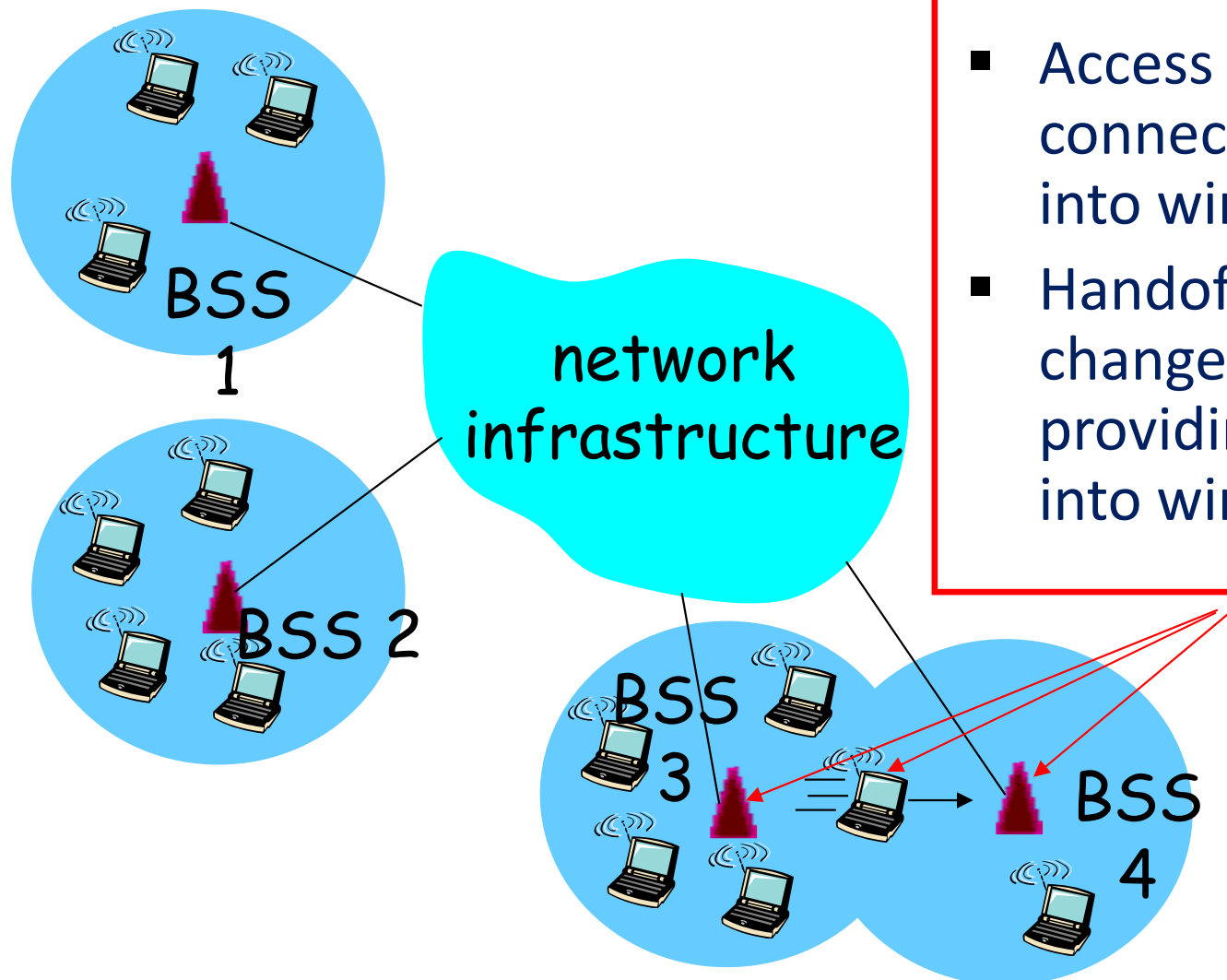
802.11 WLAN – Ad Hoc Mode



Ad Hoc Mode

- No Access Points
- Nodes can only transmit to other nodes within link coverage
- Nodes organize themselves into a network: route among themselves

802.11 – Infrastructure (BSS) Mode



Infrastructure Mode

- Access Point (AP) connects mobiles into wired network
- Handoff: mobile changes AP providing connection into wired network

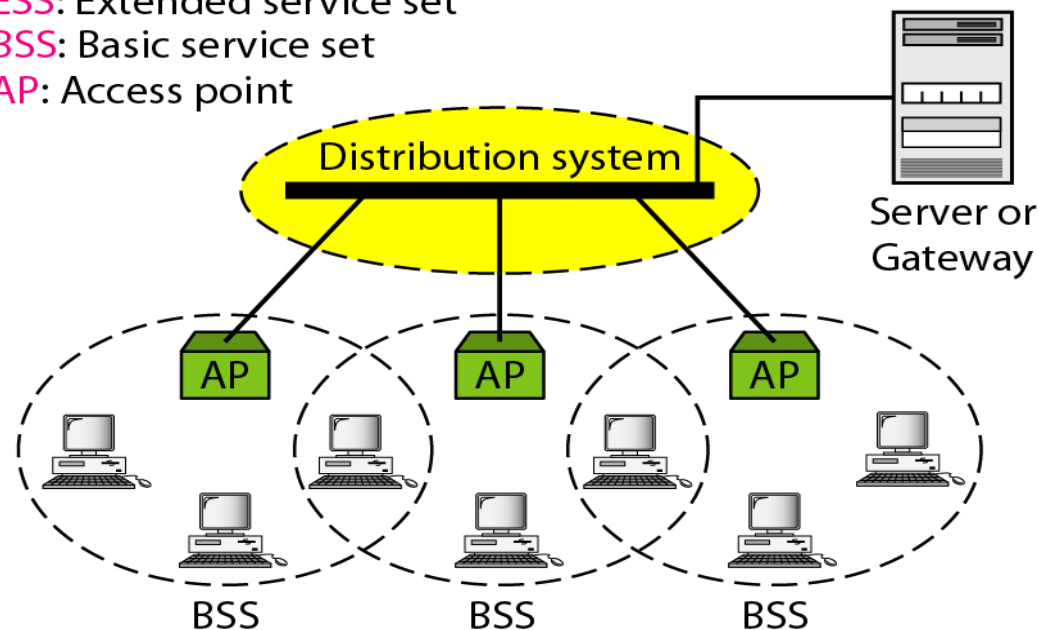
Extended Service Set

- An **ESS** is made up of two or more BSSs with APs.
- All BSSs are connected via a **distribution system**.
- A mobile station can belong to more than one BSS
- **Mobility** between BSS-to-BSS and ESS-to-ESS are possible, but **service continuity** not guaranteed by IEEE 802.11.

ESS: Extended service set

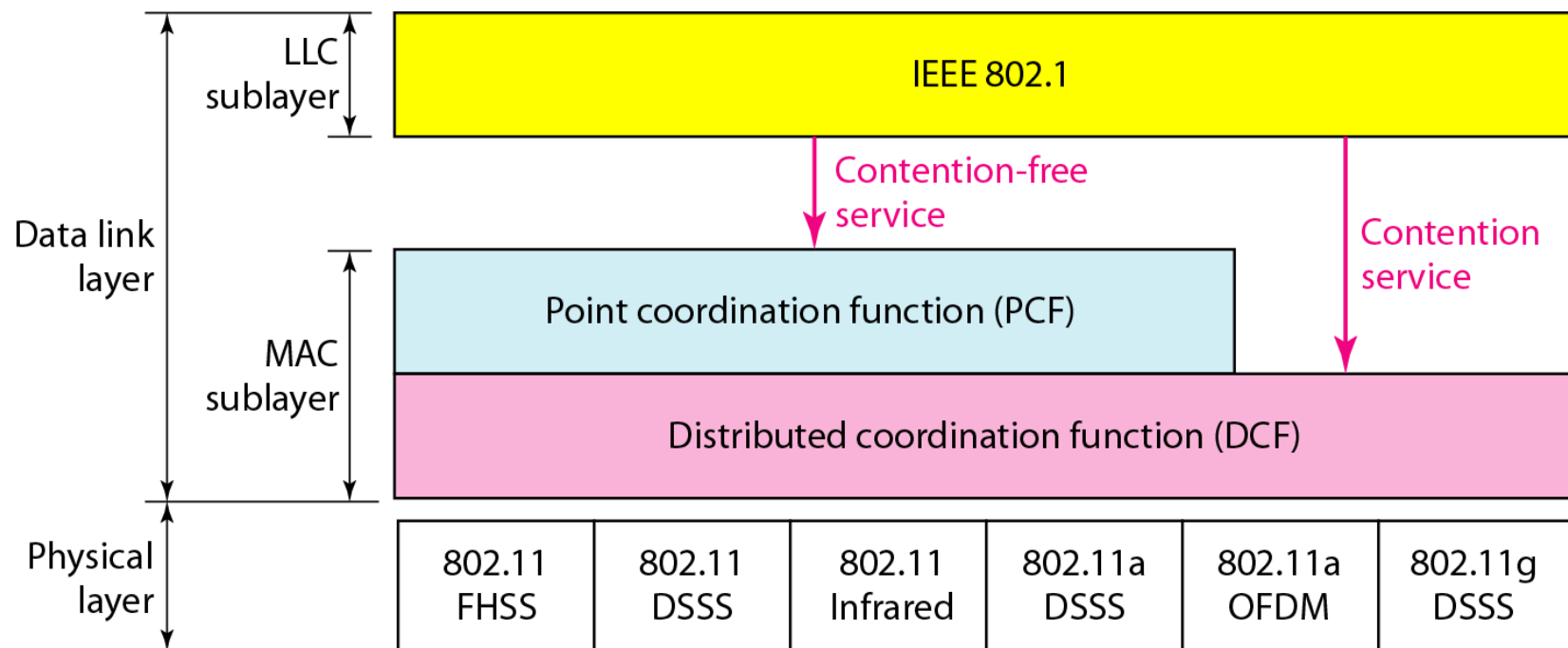
BSS: Basic service set

AP: Access point



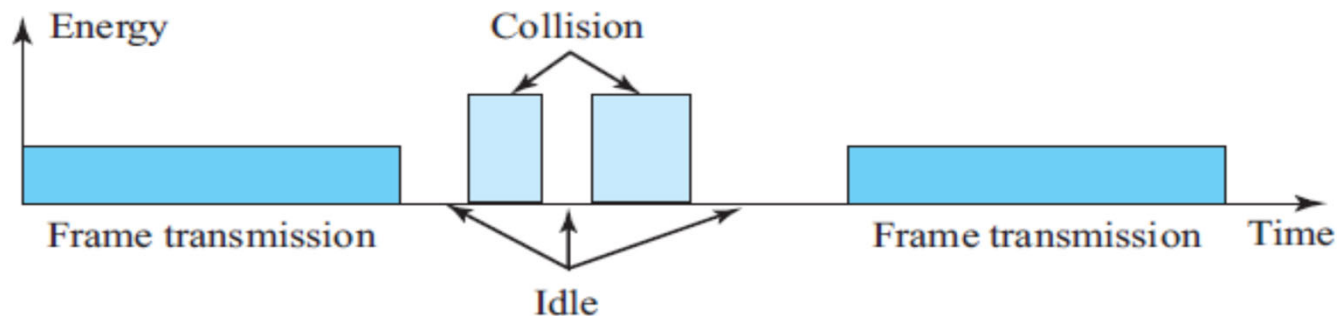
MAC Sublayers

- IEEE 802.11 defines **two MAC Sublayers**.
 - **Distributed coordination function (DCF)**: uses CSMA/CA
 - **Point coordination function (PCF)**: centralized, contention-free polling access method



Distributed Coordination Function (DCF)

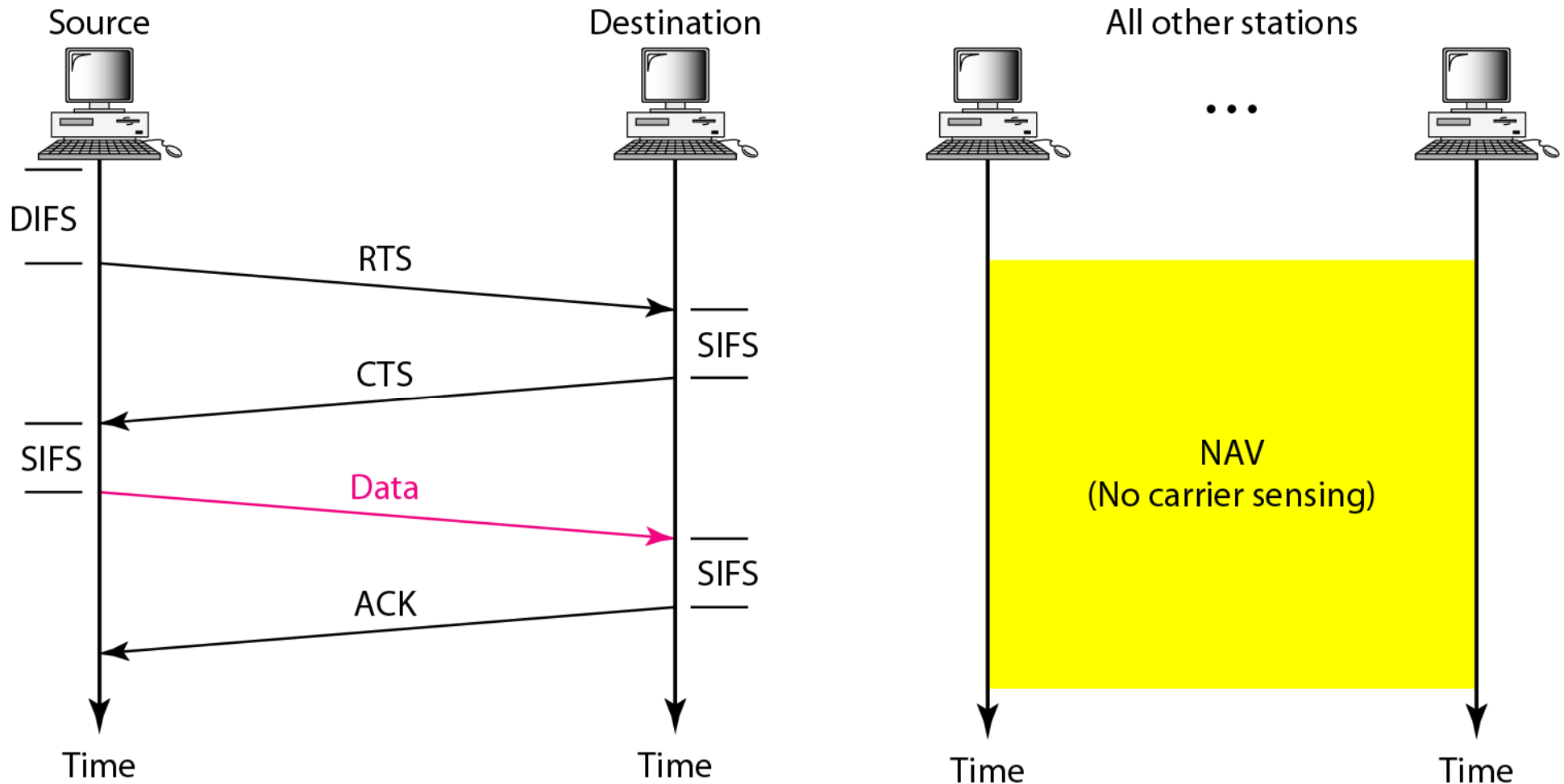
- CSMA/CD cannot be used because:
 - In wireless systems, collisions do not add enough energy for stations to effectively detect them
 - Hidden node problem
 - Signal fading could prevent a station at one end from hearing a collision at the other end
- Therefore, collisions are avoided by the CSMA/CA strategy



CSMA/CA

- The source senses the channel until it is idle
- After finding an idle channel, source waits for a period of time called **distributed inter frame space (DIFS)**
- Then source sends a control frame to destination called **request to send (RTS)**
- After receiving RTS, destination waits for another period of time called **short inter frame space (SIFS)**, then sends a control frame called **clear to send (CTS)** to the source
- The source **sends data** after waiting another time equal to **SIFS**
- The destination sends an **ACK** after waiting another time equal to **SIFS**

CSMA/CA and NAV



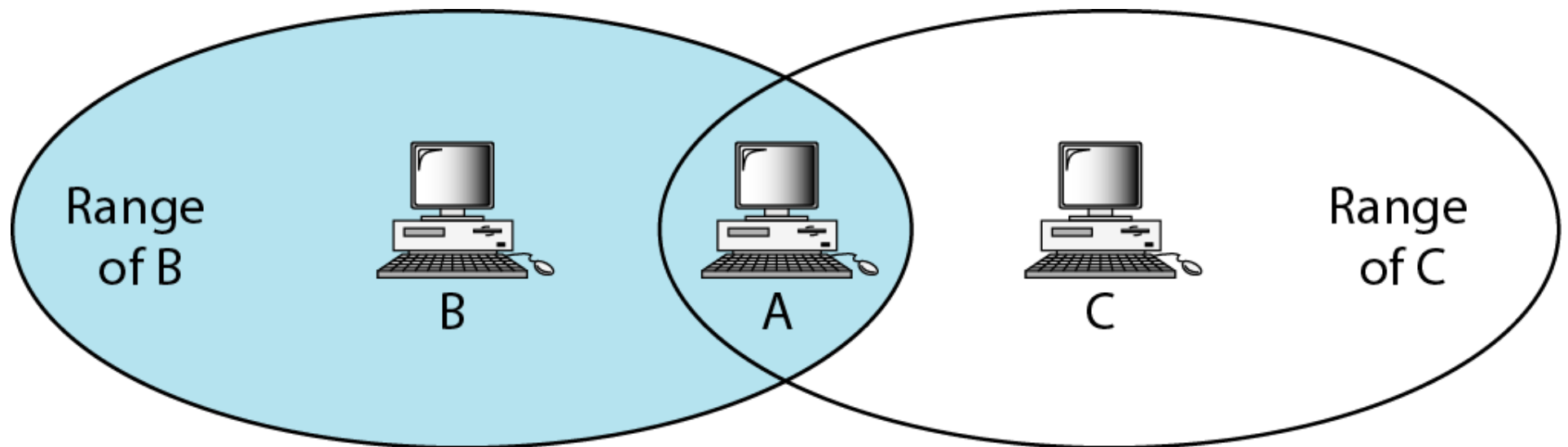
Network Allocation Vector (NAV)

- How is collision avoidance accomplished?
 - When a station sends a RTS frame, it includes the duration of time that it needs to occupy the channel.
 - Other stations that are affected create a timer called a Network Allocation Vector (NAV).
 - The NAV shows the time that must pass before these stations are allowed to check the channel for idleness.
 - Each time a station access the system and sends a RTS frame, other stations start their NAV.
- Collision during handshake
 - Two or more stations may try to send RTS frames at the same time and these may collide
 - Sender assumes that there may have been a collision since it does not receive a CTS frame
 - The back-off strategy is employed and the sender tries again

Point Coordination Function (PCF)

- PCF has a centralized contention free polling access method
- This is implemented over the DCF and used for time sensitive transmissions
- This can only be implemented in an infrastructure network (not in ad-hoc network)
- The AP performs polling for the stations
- To give priority to PCF over DCF, another set of inter frame spaces are defined: PIFS and SIFS
 - SIFS are the same as in DCF
 - PIFS (PCF IFS) are shorter than DIFS (this means if at the same time a station wants to use only DCF and the AP wants to use PCF, the AP gets priority)

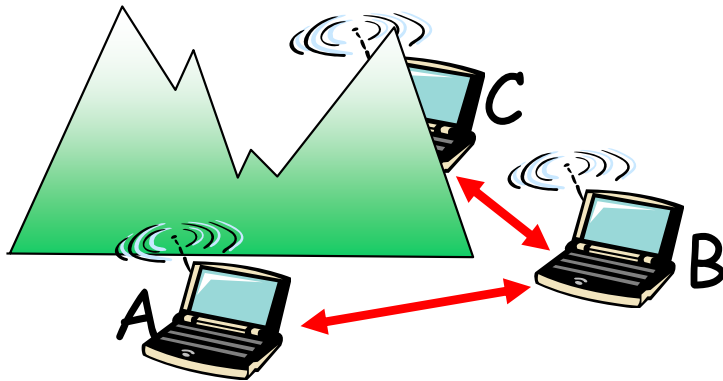
Hidden Station Problem



B and C are hidden from each other with respect to A.

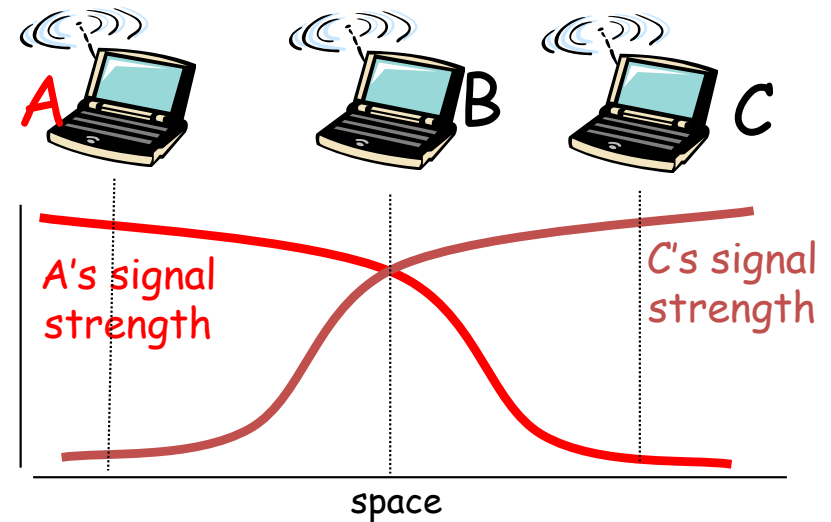
Hidden Terminal Problem in WLANs

- Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden terminal problem

- B, A hear each other
 - B, C hear each other
- A, C can not hear each other
- means A, C unaware of their interference at B

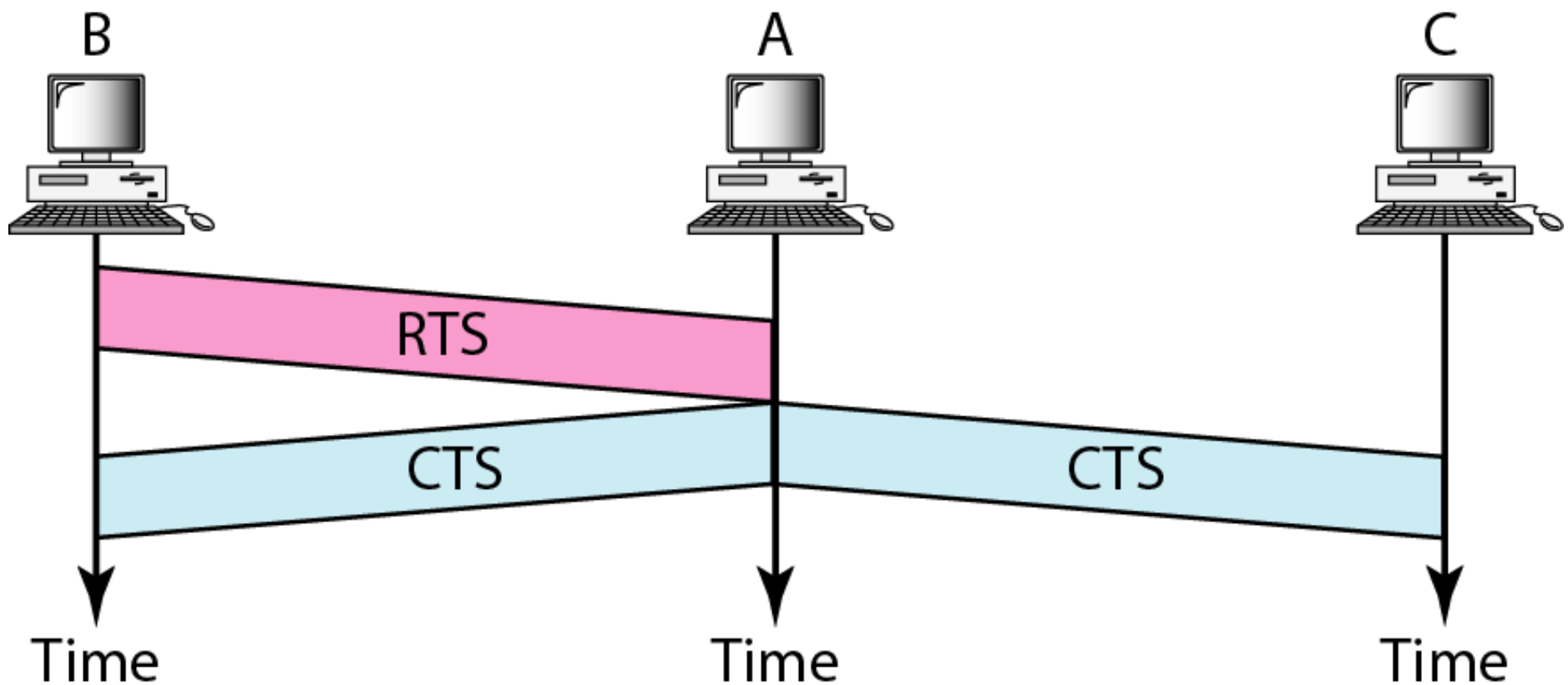


Signal fading

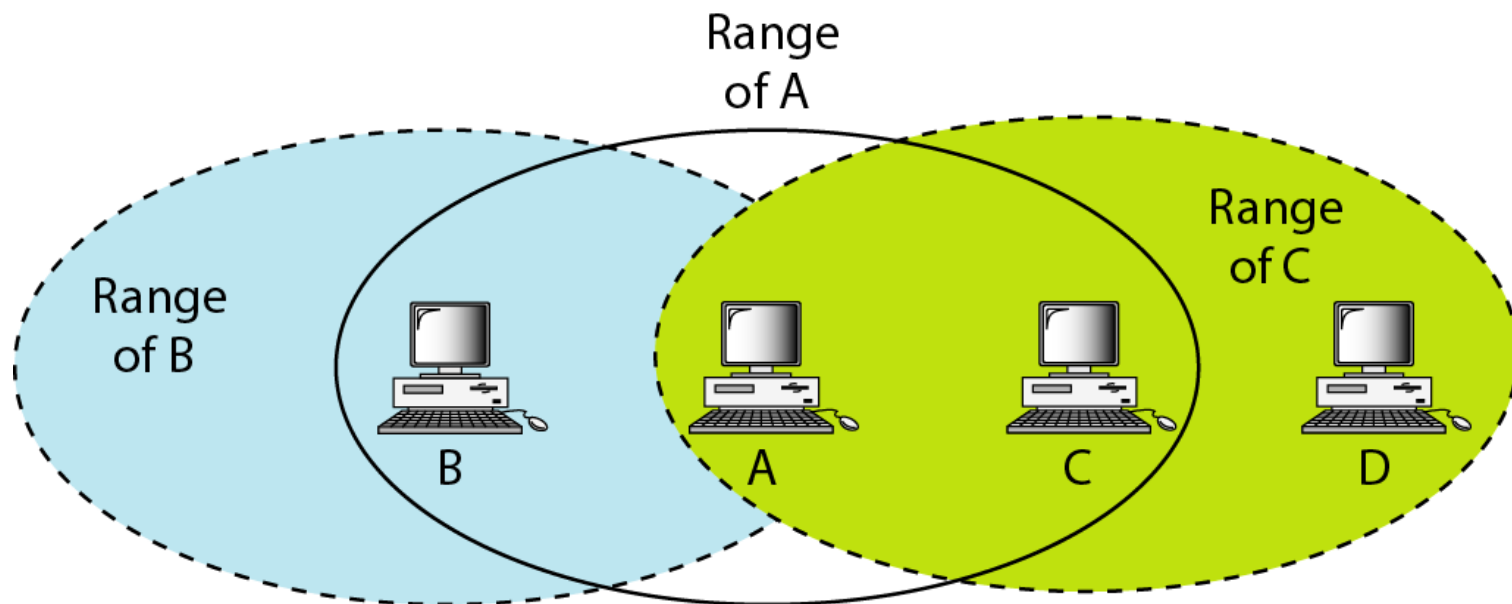
- B, A hear each other
 - B, C hear each other
- A, C can not hear each other interfering at B

Hidden Station Problem

- The CTS frame in CSMA/CA handshake can prevent collision from a hidden station.

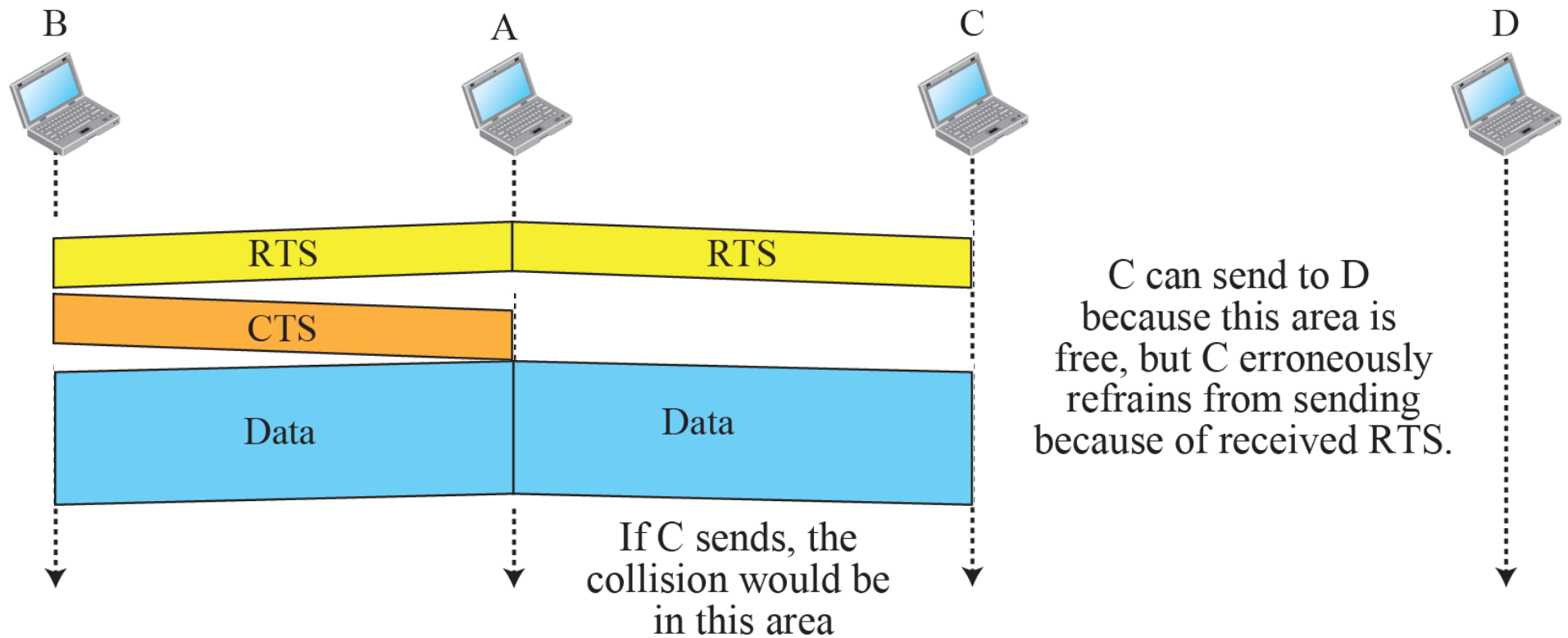


Exposed Station Problem



C is exposed to transmission from A to B.

Exposed Station Problem

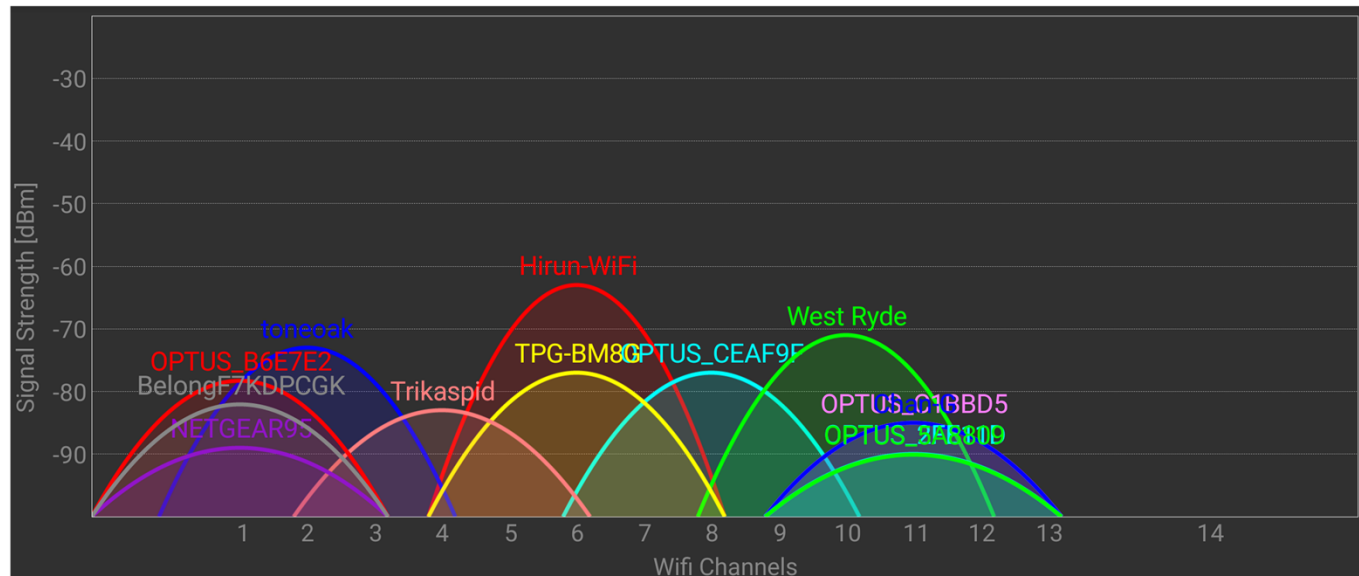
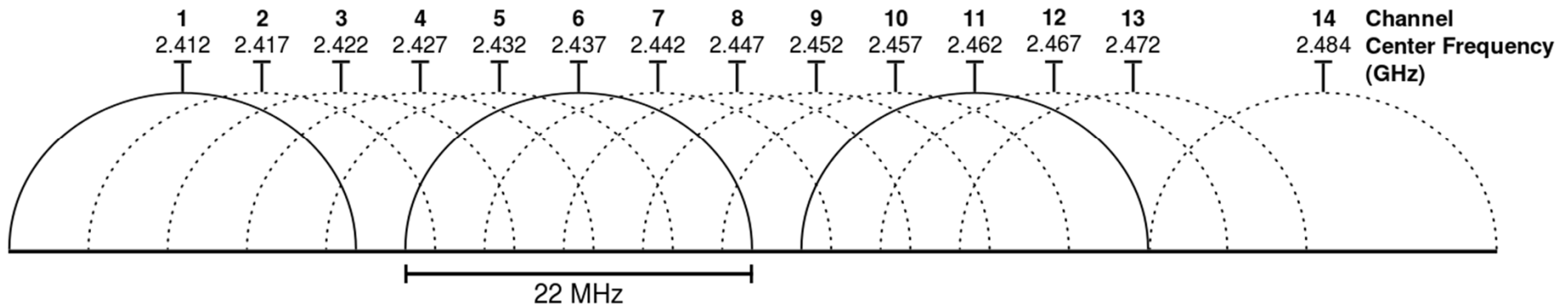


802.11: Channels, Association

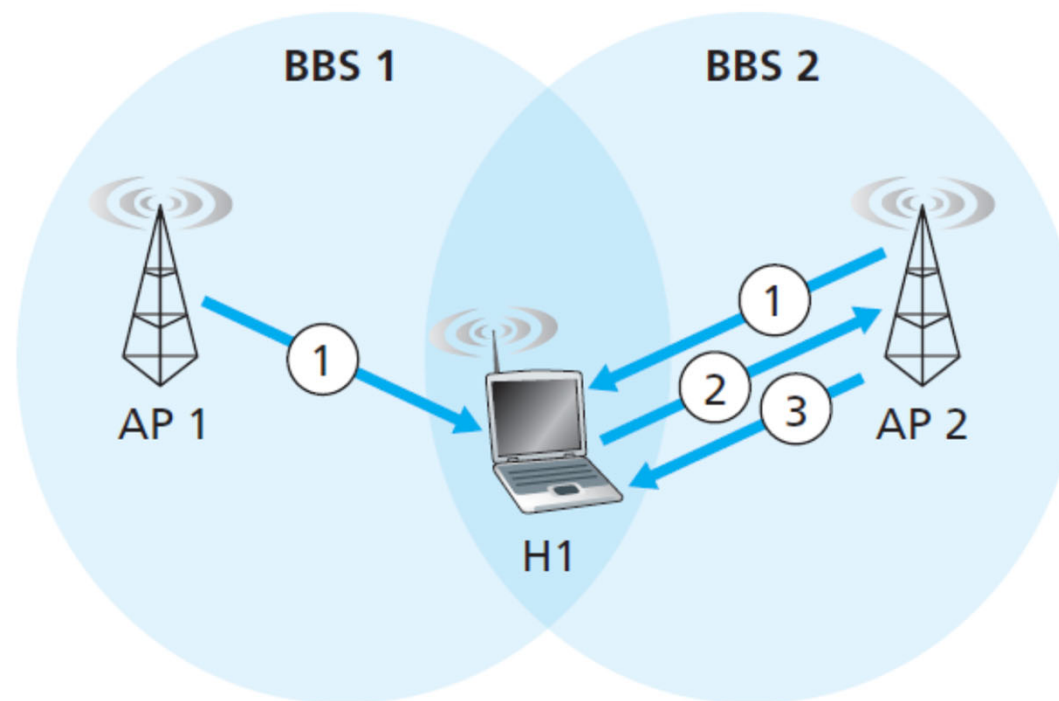
- **802.11:** 2.4GHz or 5 GHz bands
 - AP admin chooses frequency for AP
 - Interference possible: channel can be same as that chosen by neighboring AP!
 - ISM = Industrial, Scientific and Medical
- Host: must **associate** with an AP
 - scans channels, listening for *beacon frames* containing AP's name i.e. **Service Set Identifier (SSID)** and MAC address
 - Selects AP to associate with
 - May perform authentication
 - Will typically run DHCP to get IP address in AP's subnet



802.11 Channels (2.4 GHz band)



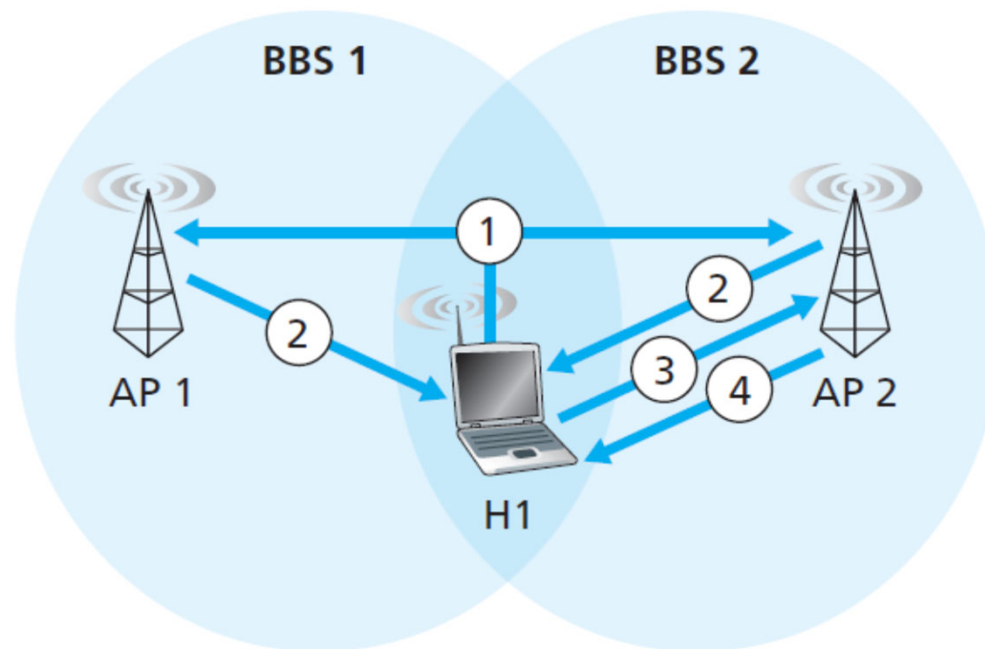
802.11 Association: Passive Scanning



a. Passive scanning

1. Beacon frames sent from APs
2. Association Request frame sent:
H1 to selected AP
3. Association Response frame sent:
Selected AP to H1

802.11 Association: Active Scanning



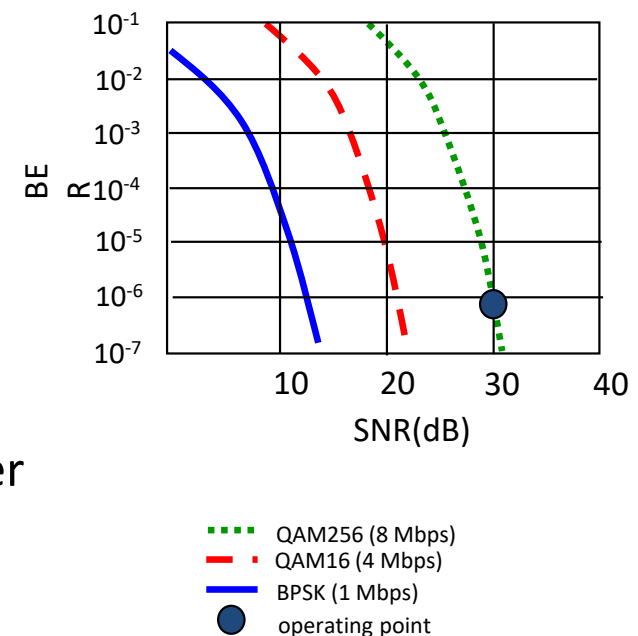
a. Active scanning

1. Probe Request frame broadcast from H1
2. Probes Response frame sent from APs
3. Association Request frame sent:
H1 to selected AP
4. Association Response frame sent:
Selected AP to H1

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 a lower transmission rate but with lower BER
- Most common is Minstrel or proprietary RA by vendors or even AI-based RA.



802.11: advanced capabilities (others)

- up to 16 spatial streams and Multiple-Input-Multiple Output (MIMO) protocol enhancements
- up to 4096-QAM (4K-QAM) enables each symbol to carry 12 bits rather than 10 bits
- Multi-Access Point (AP) Coordination
- Enhanced link adaptation and retransmission protocol (e.g. Hybrid Automatic Repeat Request (HARQ))
- Integrating Time-Sensitive Networking (TSN) IEEE 802.1Q extensions for low-latency real-time traffic

802.11: Evolution

Wi-Fi generations

V • T • E

Generation	IEEE standard	Adopted	Maximum link rate (Mbit/s)	Radio frequency (GHz)
Wi-Fi 7	802.11be	(2024)	1376 to 46120	2.4/5/6
Wi-Fi 6E	802.11ax	2020	574 to 9608 ^[1]	6 ^[2]
Wi-Fi 6		2019		2.4/5
Wi-Fi 5	802.11ac	2014	433 to 6933	5 ^[3]
Wi-Fi 4	802.11n	2008	72 to 600	2.4/5
(Wi-Fi 3)*	802.11g	2003	6 to 54	2.4
	802.11a	1999		5
(Wi-Fi 2)*	802.11b	1999	1 to 11	2.4
(Wi-Fi 1)*	802.11	1997	1 to 2	2.4
*(Wi-Fi 1, 2, and 3 are by retroactive inference) ^{[4][5][6][7][8]}				

https://en.wikipedia.org/wiki/IEEE_802.11be

802.11: Long-range WiFi 802.11ah

Wi-Fi CERTIFIED HaLow™ for IoT

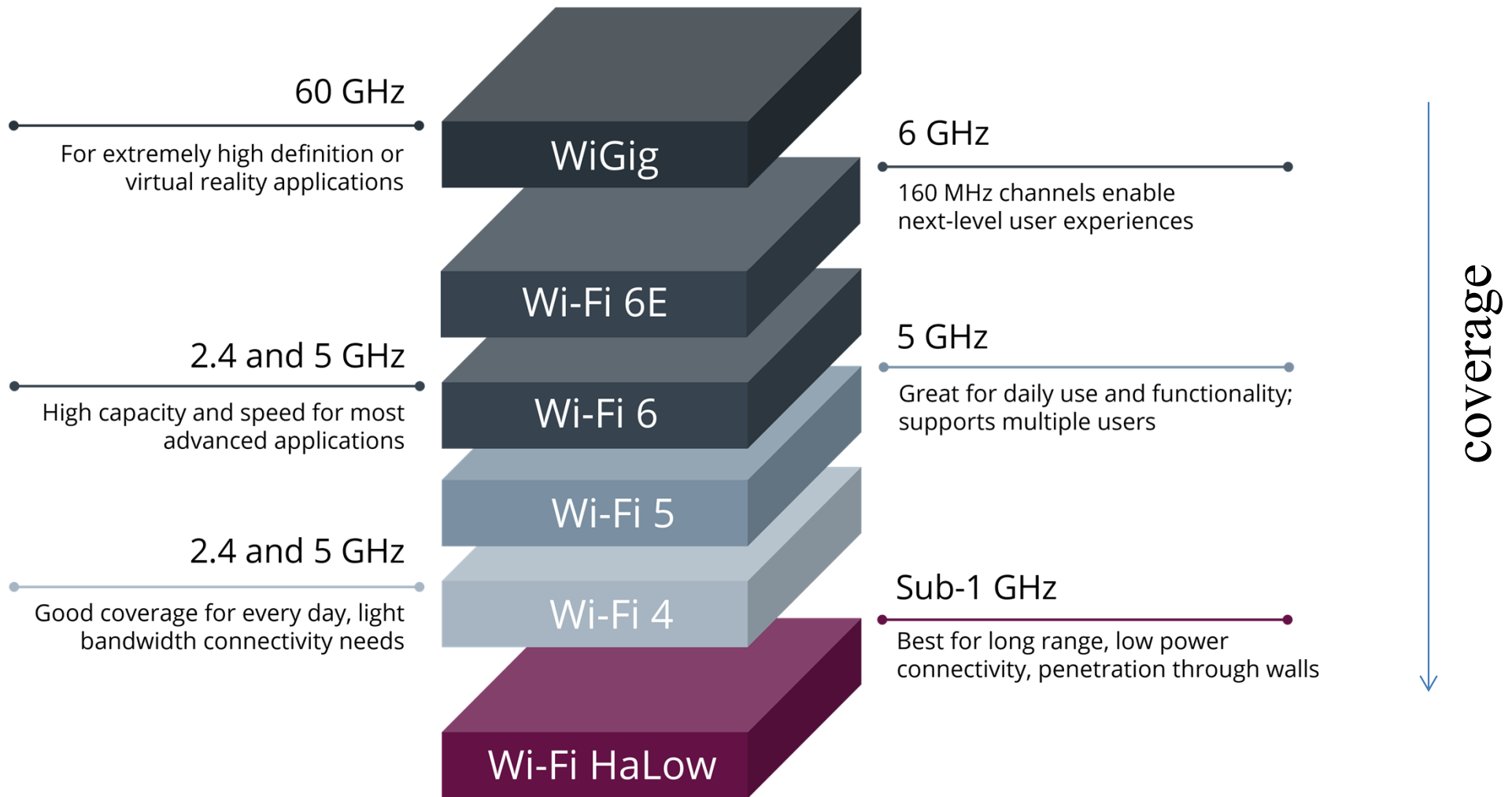
Features

-  Sub-1 GHz spectrum operation
-  Narrow band OFDM channels
-  Several device power saving modes
-  Native IP support
-  Latest Wi-Fi® security

Benefits

-  Long range: approximately 1 km
-  Penetration through walls and other obstacles
-  Supports coin cell battery devices for months or years
-  No need for proprietary hubs or gateways

802.11: Wi-Fi Radio Coverage



Personal area networks: Bluetooth

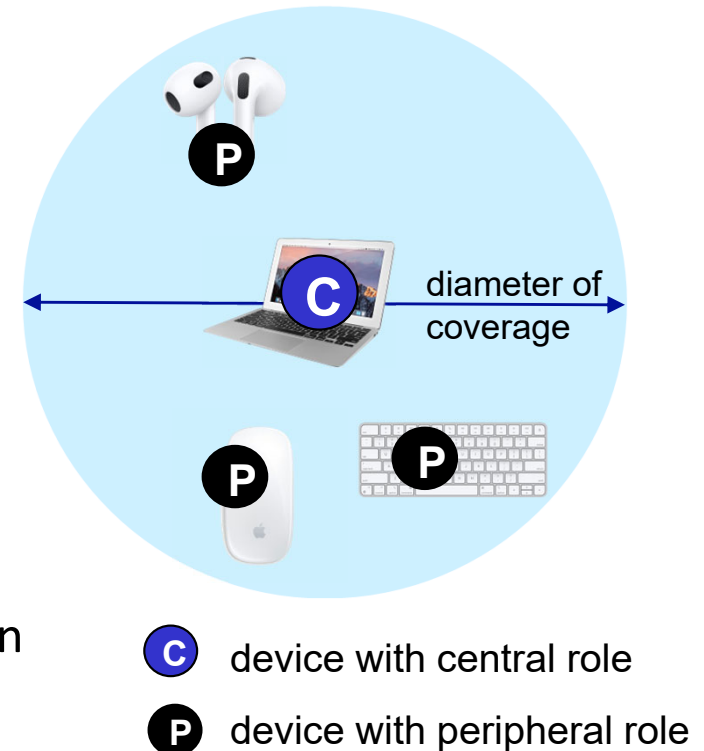
example of *wireless ad hoc network*: devices have no “infrastructure” (e.g., access point, base station) to connect to

- BT devices must find other BT devices, *organize themselves* into a network from scratch!
 - connect devices at link layer, providing channel allocation
 - addressing assignment
 - service discovery
 - application-to-application communication over Bluetooth network
 - security

An entirely new architecture and protocol stack (different from Internet) is needed!

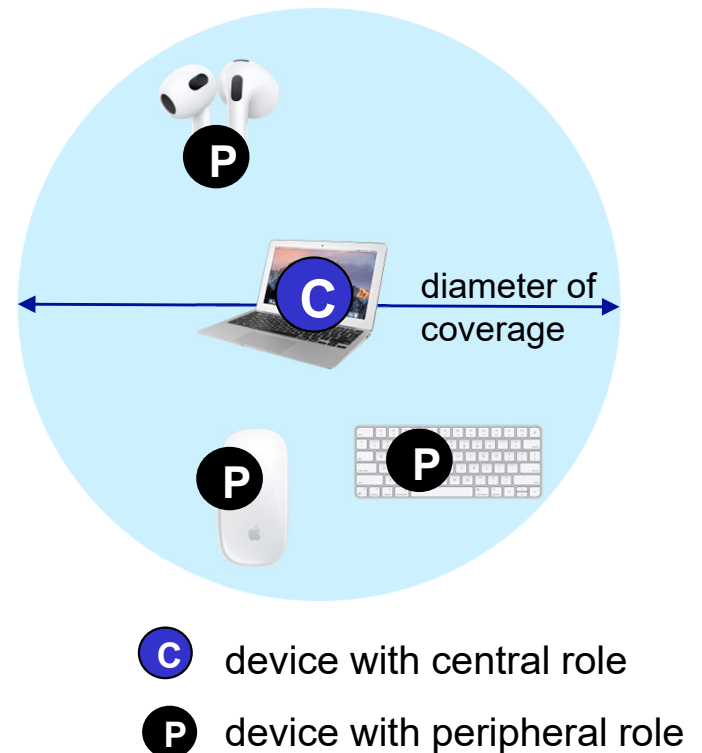
Personal area networks: Bluetooth

- Bluetooth network: **piconet**
- coverage: generally <10 m diameter
- no more than 8 devices per piconet
 - device initially forming network: **central** role
 - up to 7 more devices: **peripheral** role
- *communication only between central and peripheral node*
 - no direct peripheral-to-peripheral communication
- BT device has unique 48-bit address
- Operate in unlicensed ISM band: 2.4 GHz

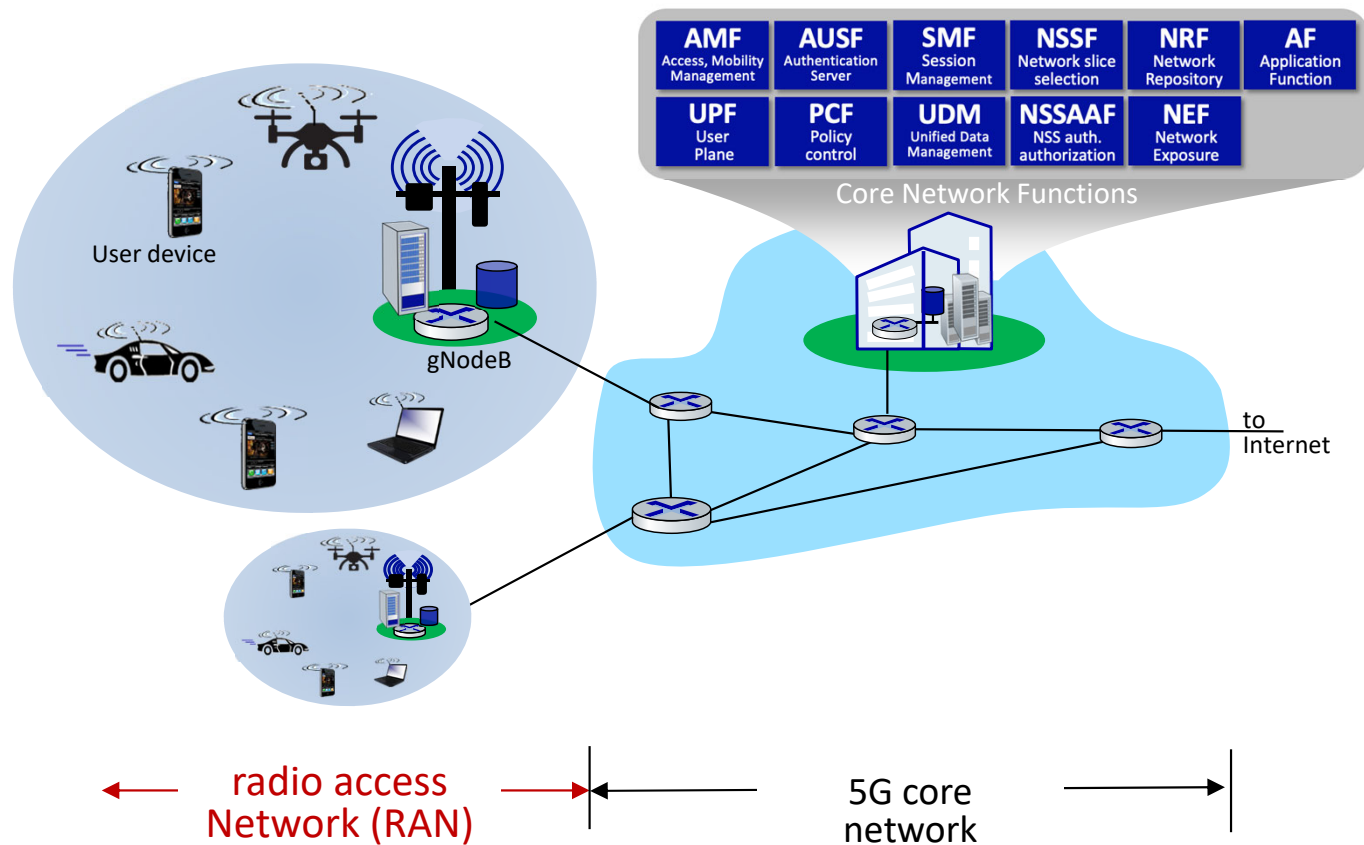


Personal area networks: Bluetooth

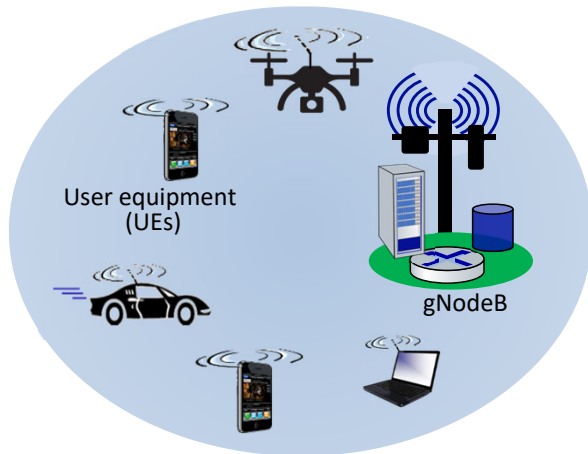
- operates in 2.4-2.5 GHz ISM radio band
 - **Classic BT**: 1 MHz bandwidth/channel, 79 channels, 2.1 Mbit network max rate
 - **BLE**: 2 MHz bandwidth/channel, 40 channels. 3 advertising, 37 data channels
- BT channel: TDM, 625 μ sec slot length
- **channel access via polling**: central device advertises, grants channel access to peripherals in its BT network
- uses **frequency hopping** (form of “spread spectrum”) transmissions



Architectural Elements of 5G



5G Radio Access Network (RAN)

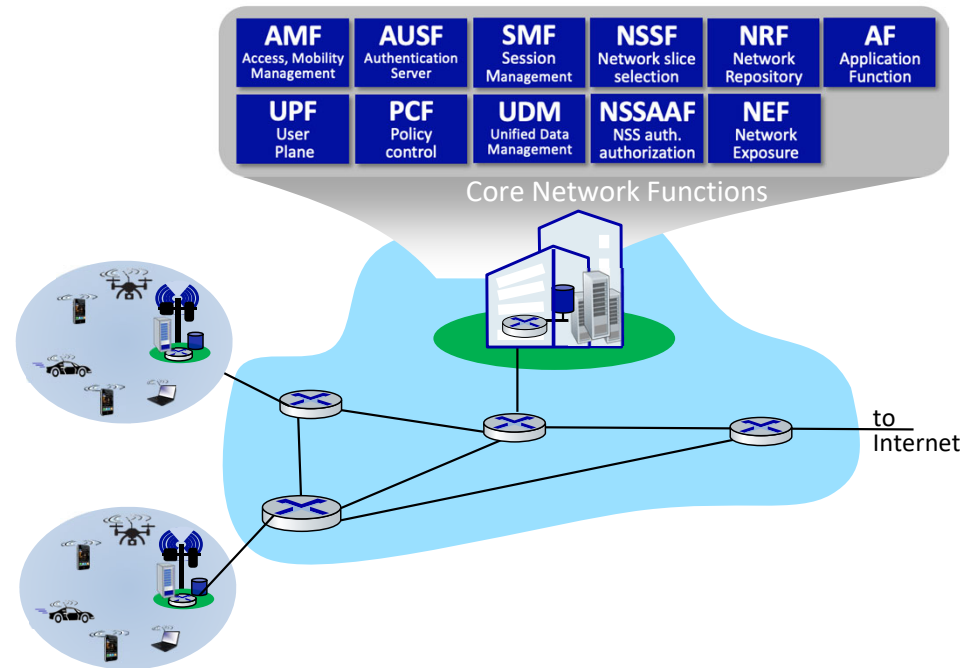


5G RAN: edge network connecting devices to base station

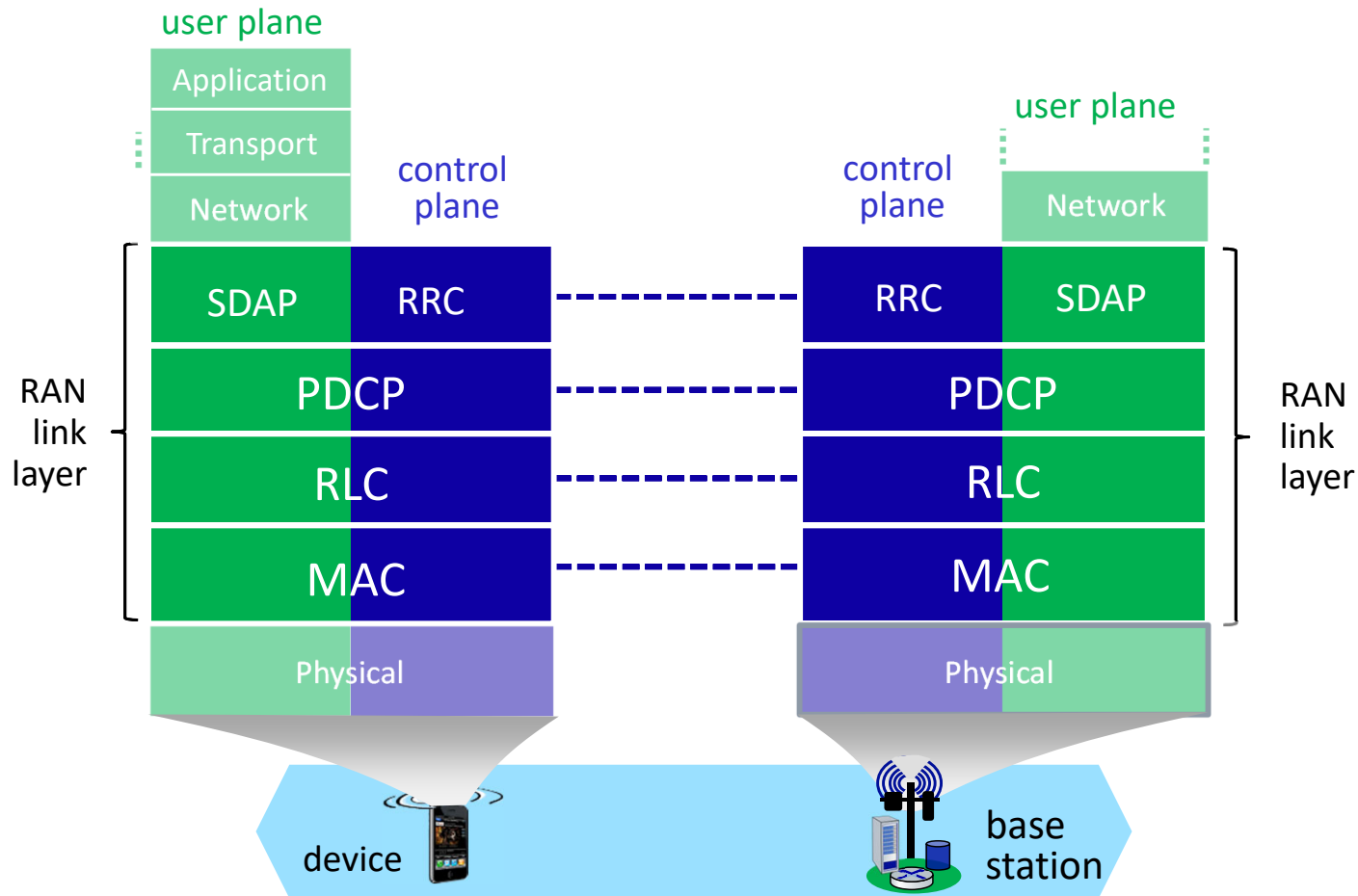
- provides link-layer service, as first hop between devices and larger network
- limited geographic scope
- under control of a single service provider
- somewhat analogous to WiFi LAN
- RAN components:
 - many devices (User Equipment: UE)
 - radio channel (New Radio: NR)
 - one base station (Next Generation Node B: gNodeB, gNB)

5G Core Network

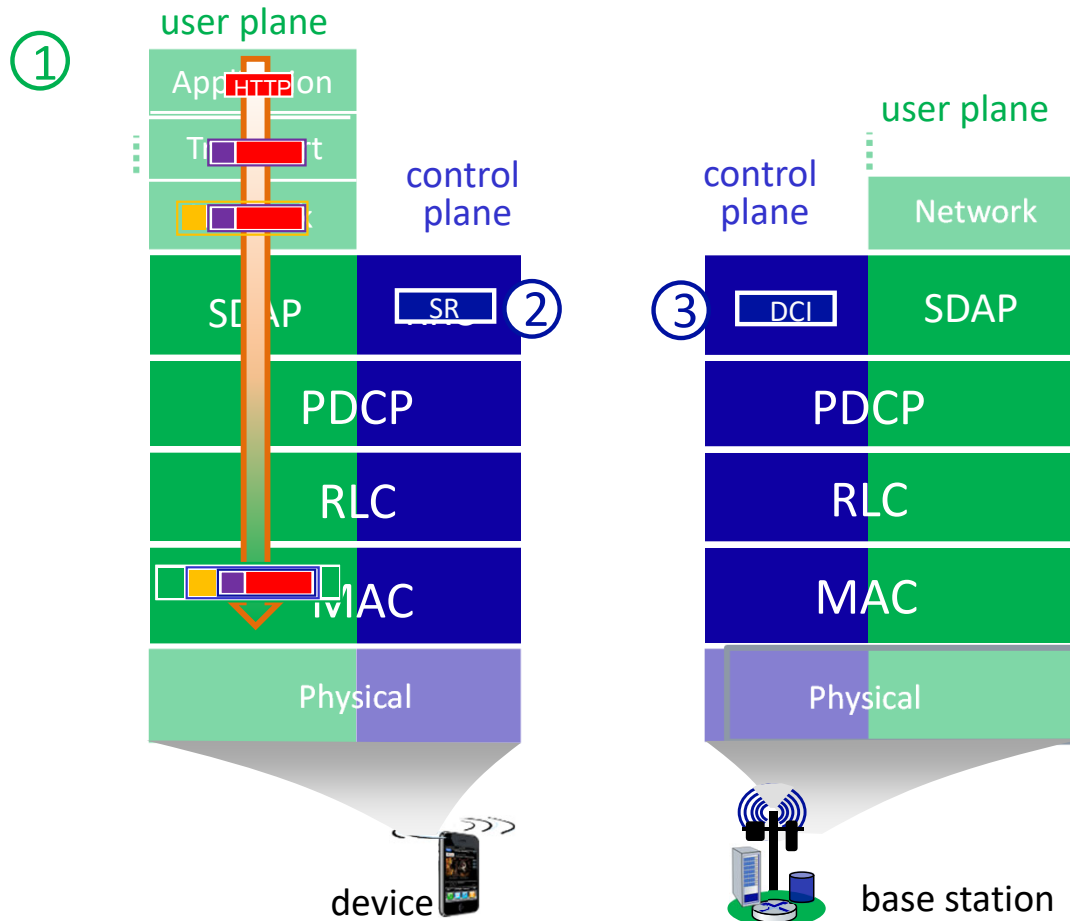
- Core situated between RAN and other endpoints (Core, larger Internet)
 - single Core; multiple RANs
- consist of links, routers, servers, providing services to devices and base stations
 - “all IP” Core, but very different services than traditional Internet apps
- clear logical separation between control-plane, user plane:
 - **CUPS**: Control-Plane and User-Plane Separation



RAN protocol stack (at device, base station)



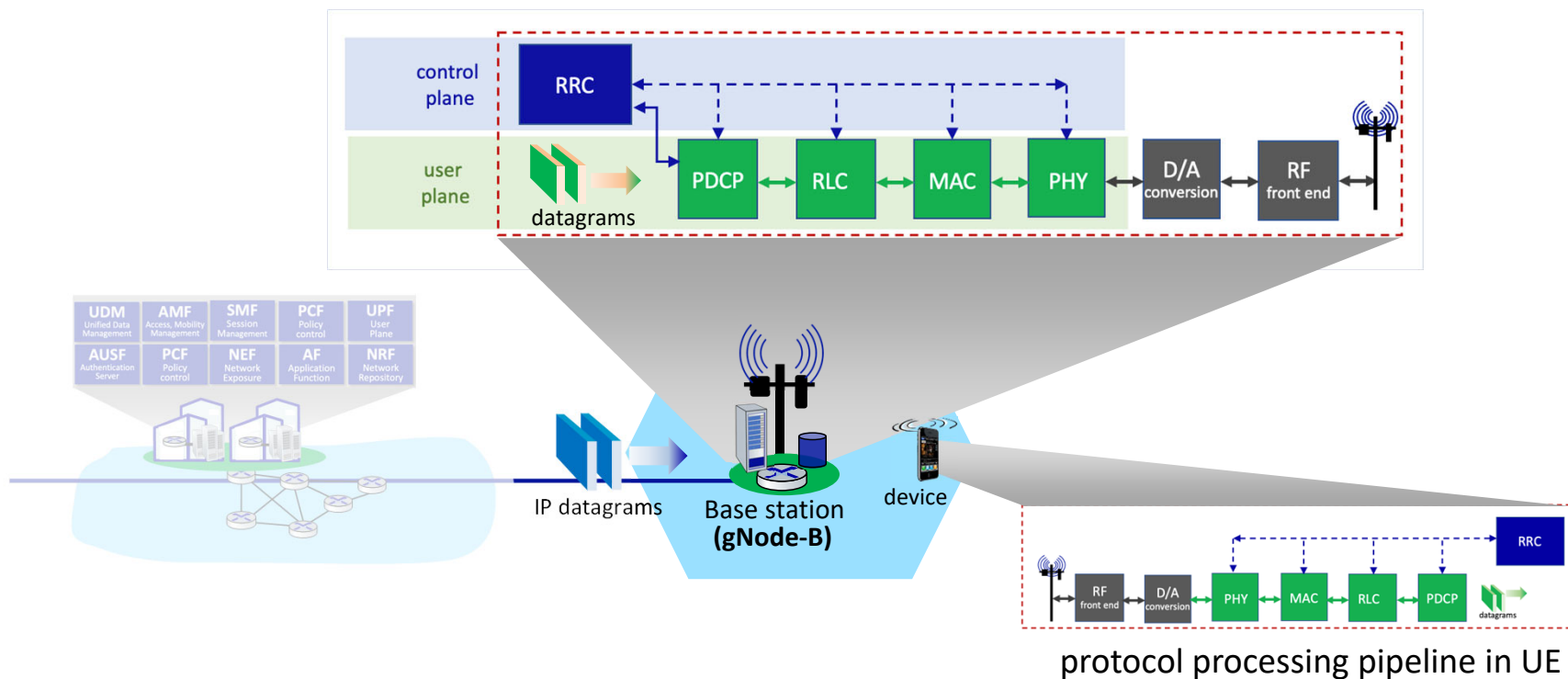
Retrospective: “A day in the life”* (5G RAN)



- ① HTTP/3 request in UDP segment, in IP datagram, into 5G frame. Enter, wait, 5G MAC frame scheduling queue
- ② device's control plane sends SR (Scheduling Req) to base station
- ③ base station control plane send control info/config and granting upstream transmission
- ④ device sends the frame by using PHY

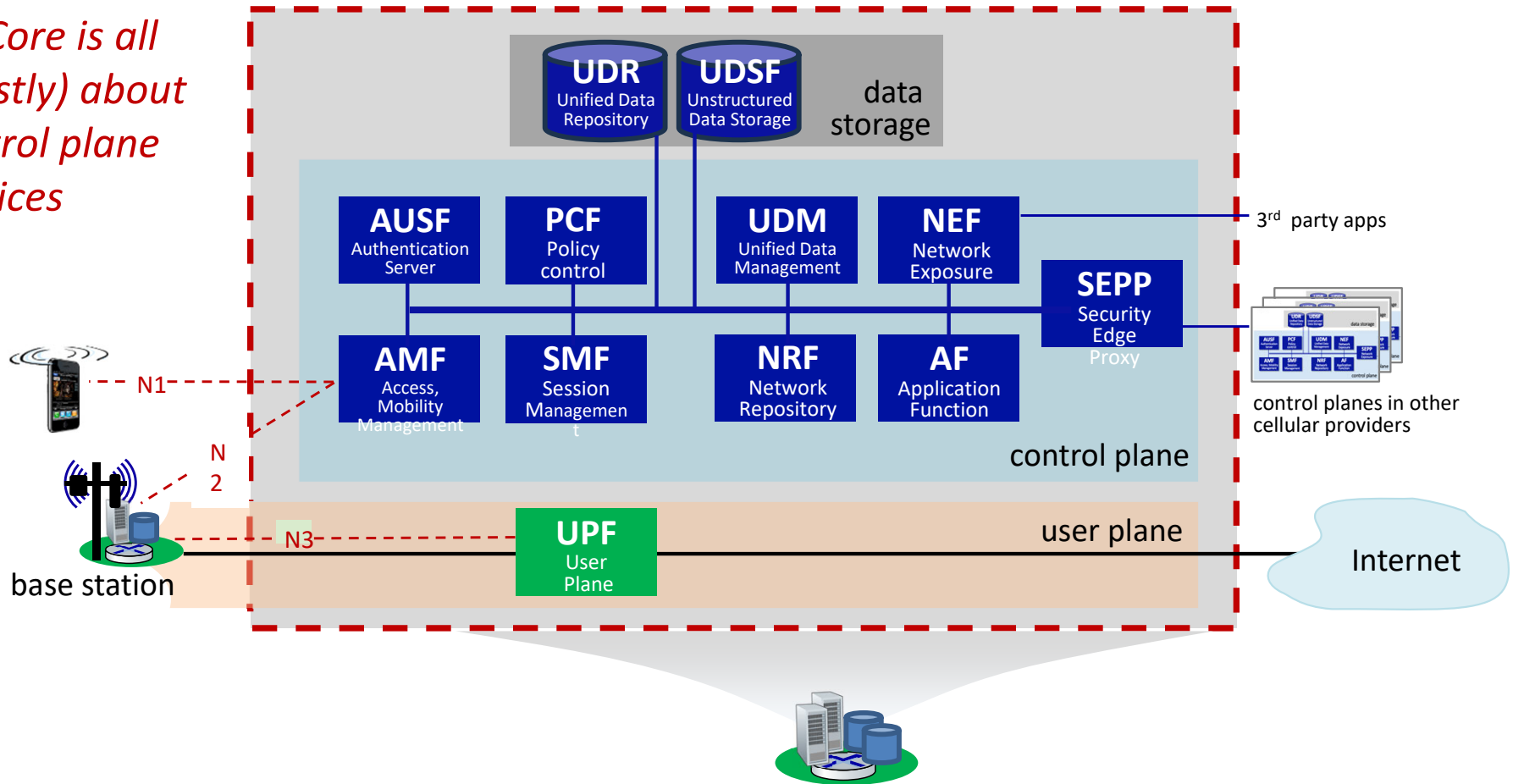
RAN packet processing pipeline: context

RAN: transfers datagrams between mobile core and devices

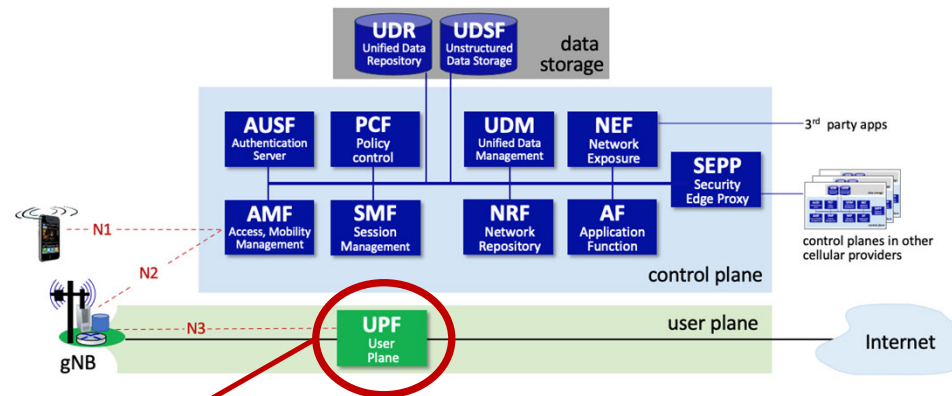


5G Core Functional Components

*5G Core is all
(mostly) about
control plane
services*



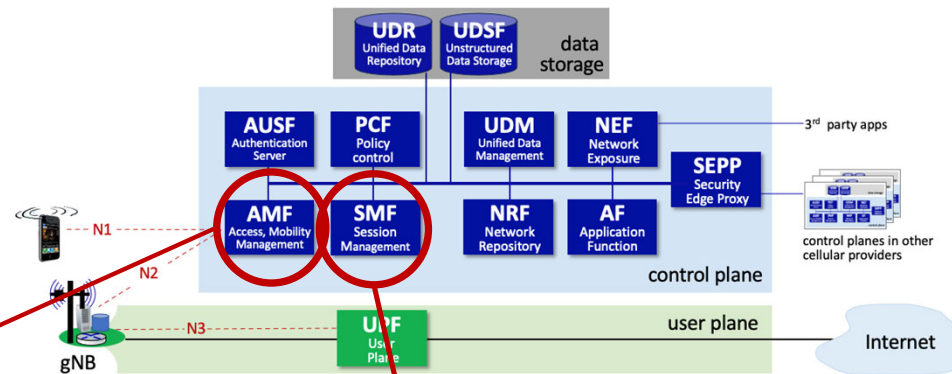
5G Core Functional Components



UPF (User Plane Function)

- each device is assigned to a UPF, which acts as relay, forwarding traffic between UE, Internet
- UPF responsible for policy enforcement, lawful intercept, traffic usage measurement, QoS policing
- responsible for tunneling (i.e., encapsulating, decapsulating) traffic to/from base station over N3 interface

5G Core Functional Components



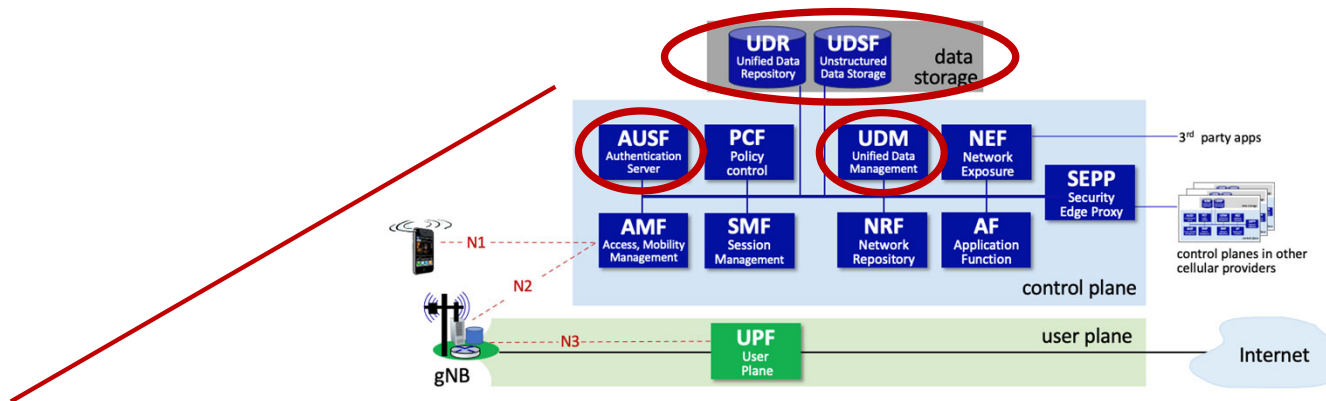
AMF (Access, Mobility Management Function)

- connection, reachability management; mobility management; access authorization; and location services

SMF (Session Management Function)

- manages each UE session, including IP address allocation, selection of associated UP function, QoS control, control aspects of UP routing

5G Core Functional Components



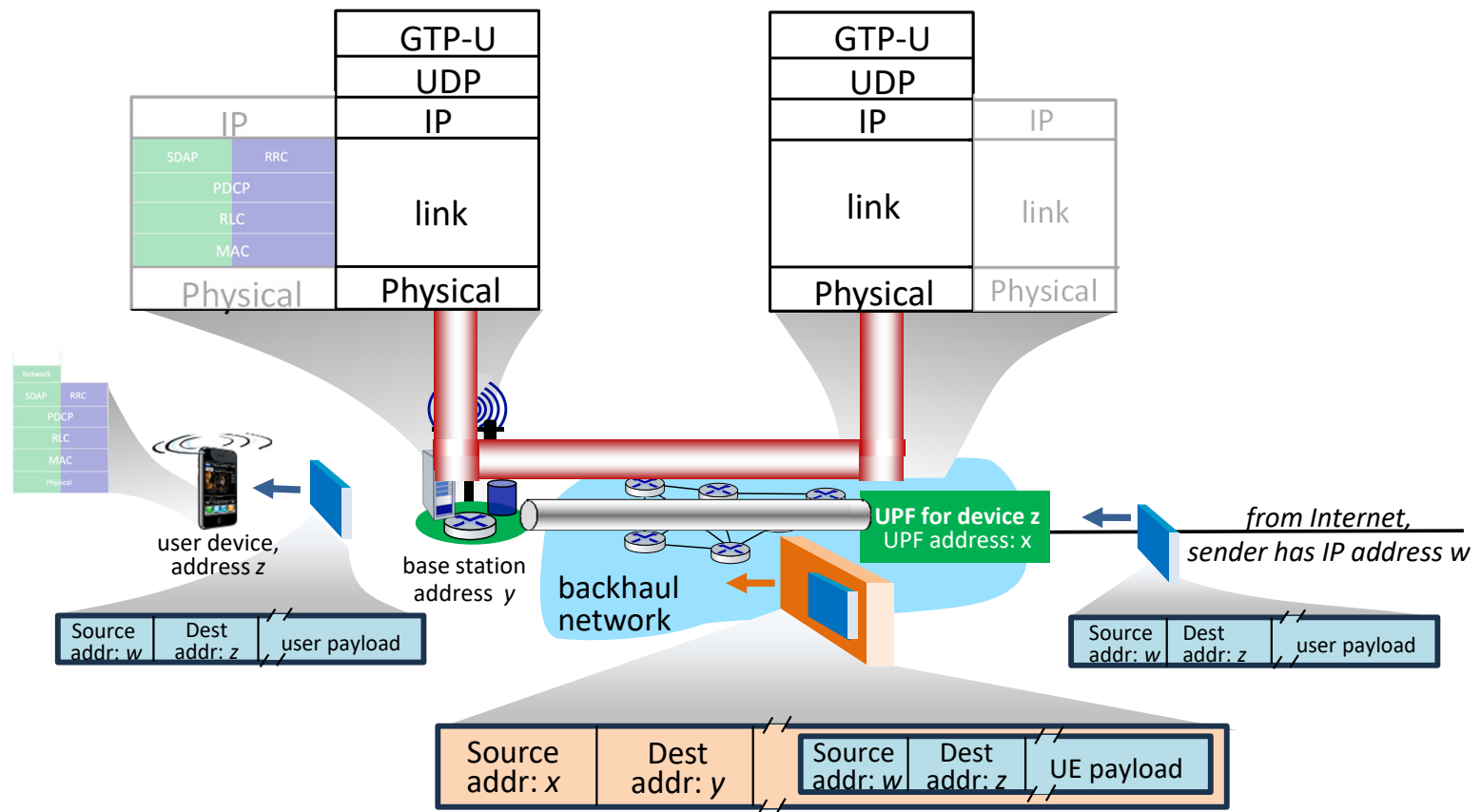
- **AUSF (Authentication Server Function):** Authenticates devices.
- **UDM (Unified Data Management):** Manages user identity, including the generation of authentication credentials.
- **UDR (Unified Data Repository):** Manages user static subscriber-related information.
- **UDSF (Unstructured Data Storage Network Function):** Used to store unstructured data, and so is similar to a *Key/Value Store*.



- emphasis on functions and services
- **well-defined interfaces** defines between services

- 5-layer Internet data plane
- extensive use of tunneling

5G Core: User plane tunnels



Identity: who are you?

4G/5G:

- You're a **customer** to a wireless service provider, with a home cellular network (who you pay)
- you have a SIM (Subscriber Identity Module) card or vSIM
 - identifies you, your home network to all cellular networks globally
 - has cryptographic key info also known to your home network



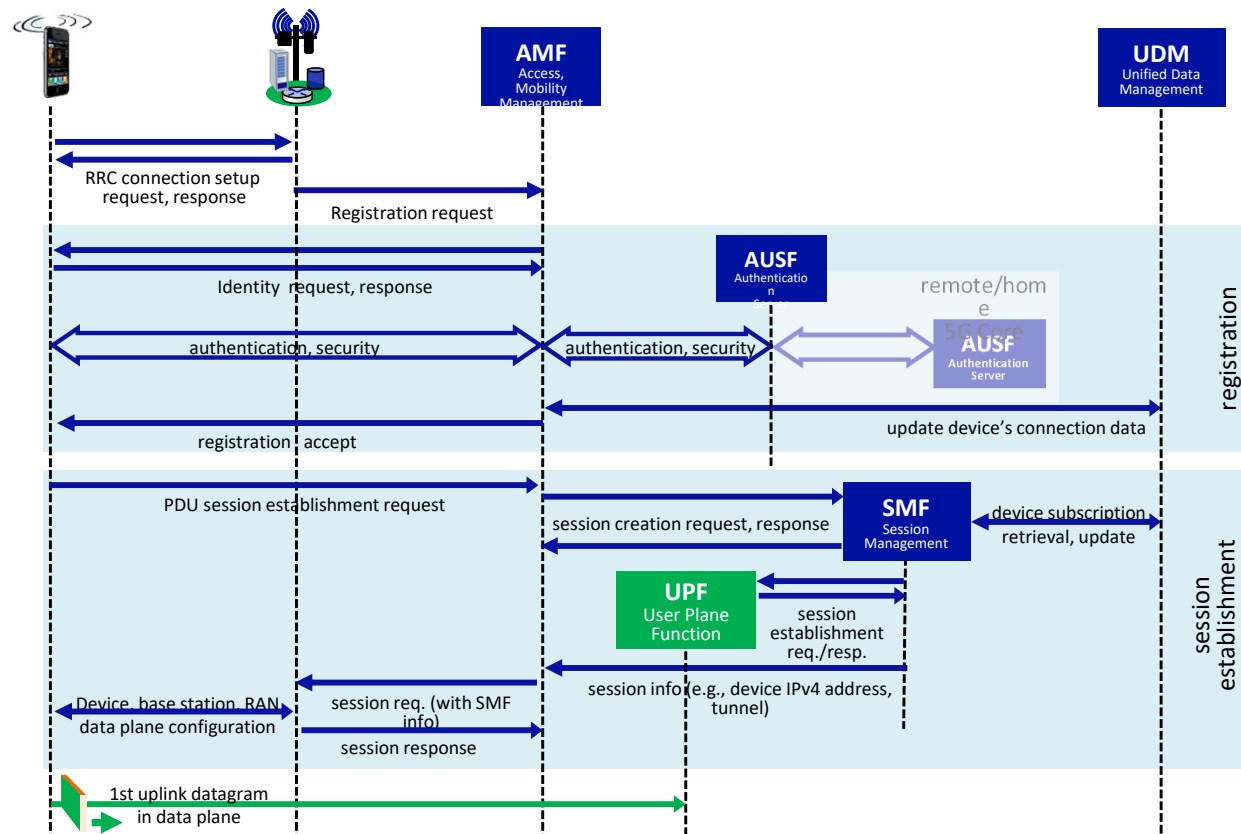
Internet approaches:

- You're a **name, password**
 - different names, password for different applications, services
- You're a **name, public key certificate**
 - servers often have public keys, users not so much (yet)

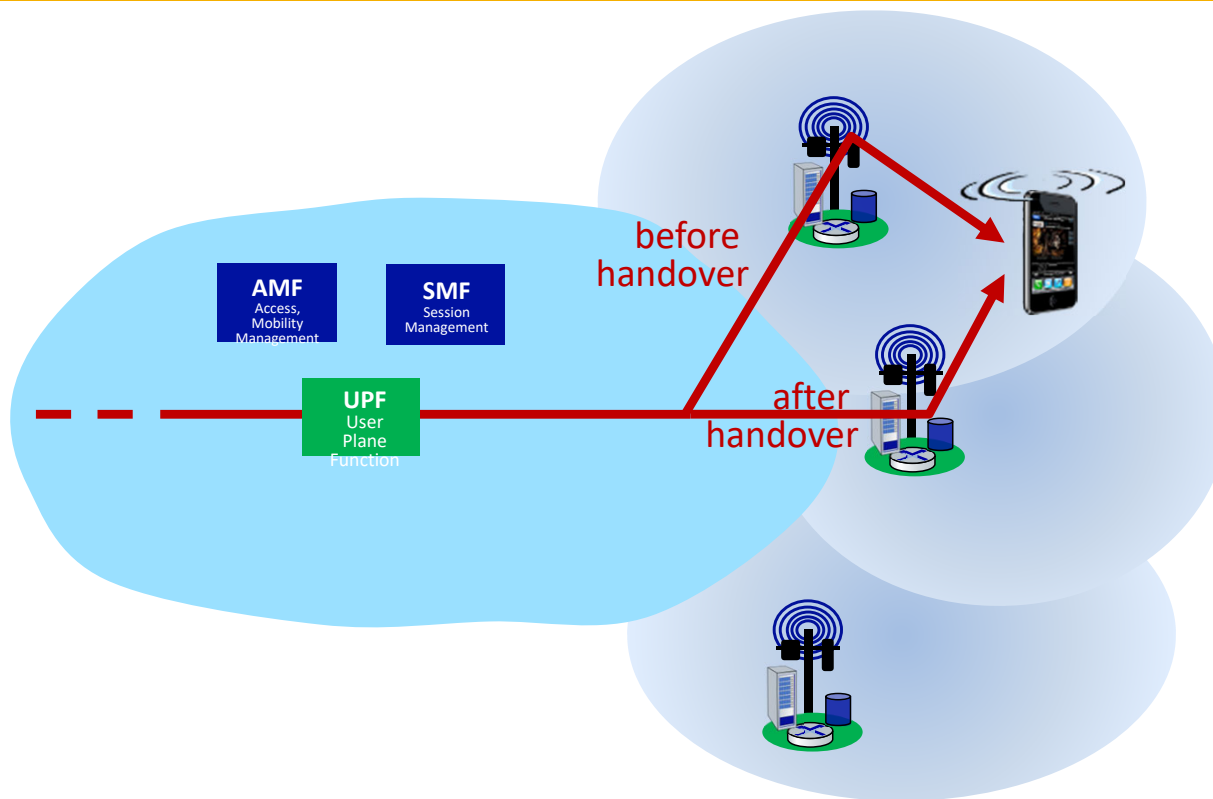
Joining a 5G network

- Two major phases:
 - *Registration*: device identifies, authenticates itself to network, and *vice versa*
 - *PDU Session establishment*: Core network functions allocate IP address to device, create data-plane path between device and device's UPF
 - PDU: protocol data unit, aka, “packet”
- *Access and Mobility Management Function (AMF)* plays key role in joining arriving device into network

Joining a 5G network: steps



Mobility in 5G networks: handover



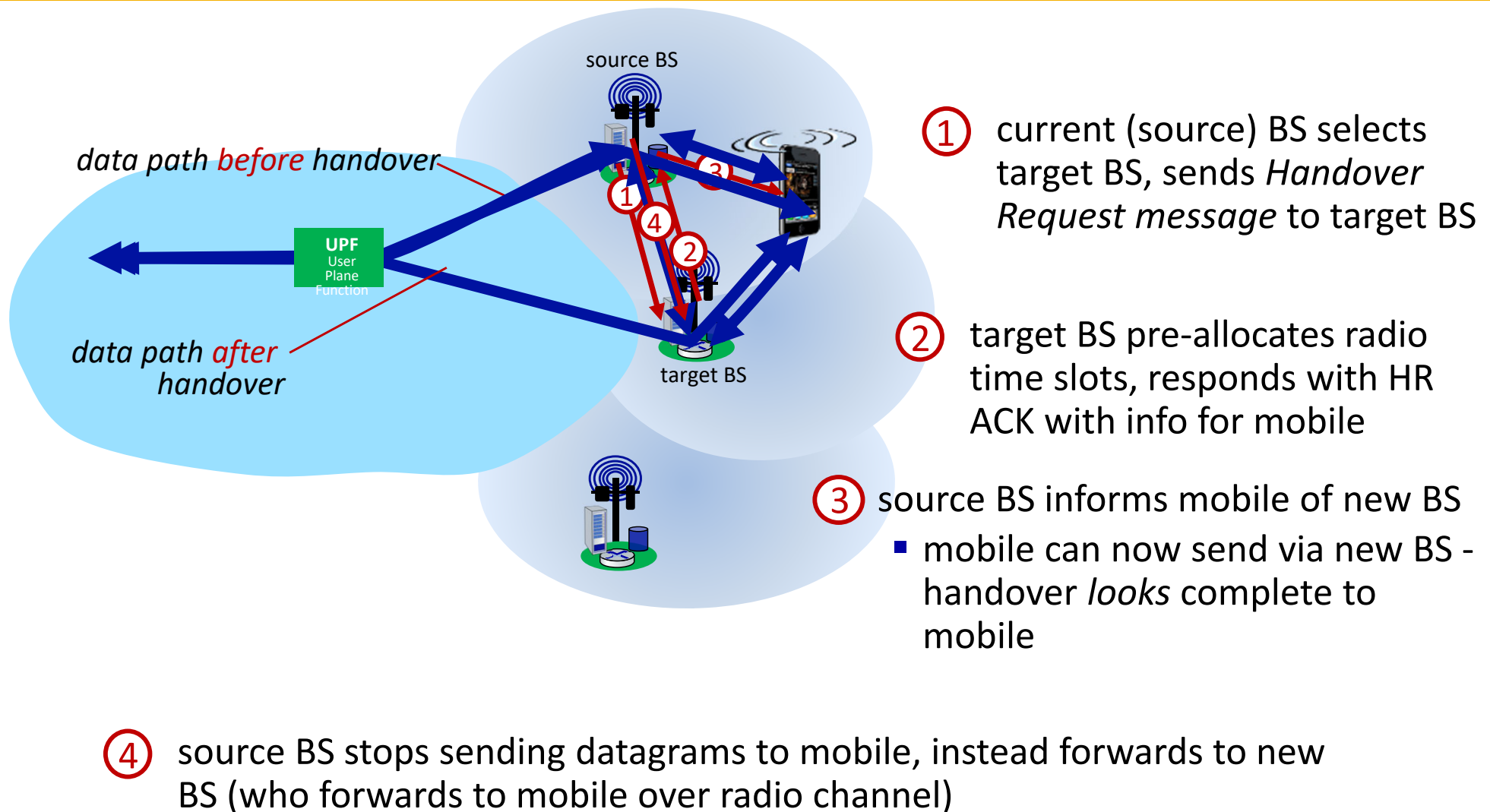
Handover:

- mobile device changes its point of attachment to the network
- data flow to device changes from *source* base station to *target* base station

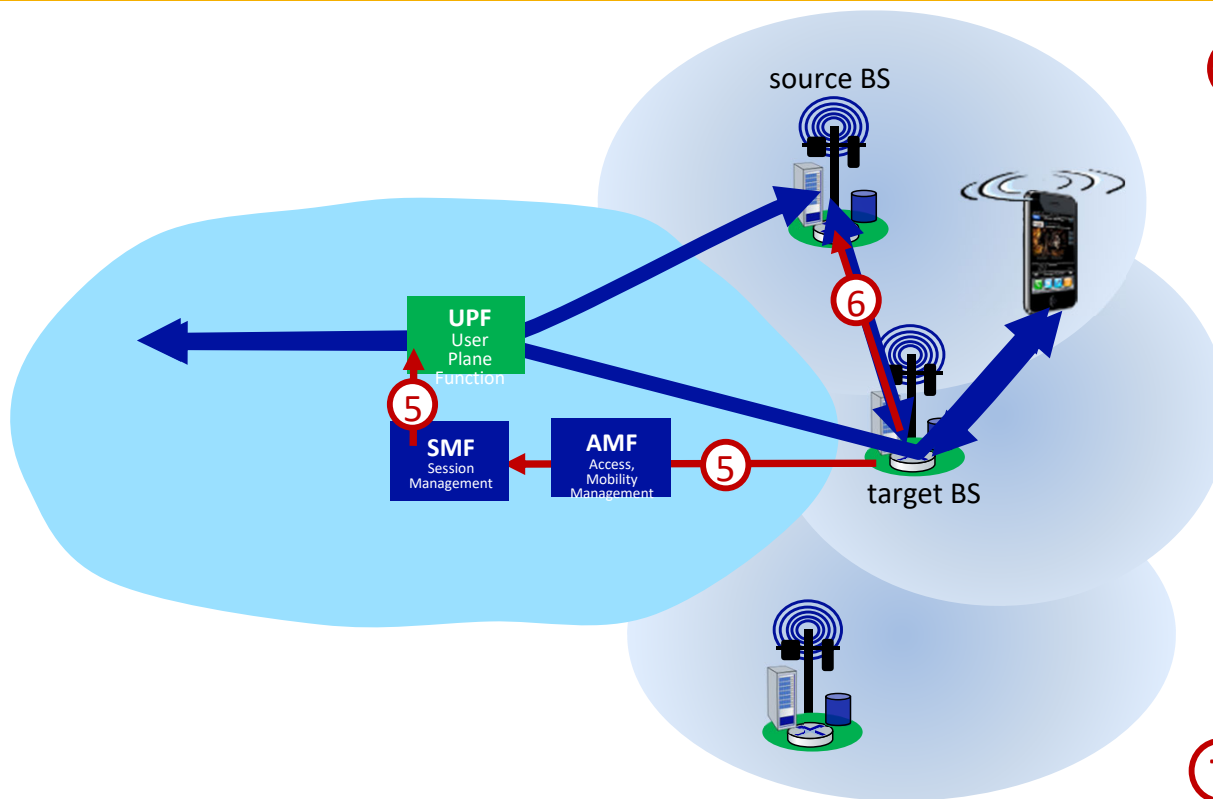
Why perform handover?

- stronger signal from target base station
- target base station has less devices, less traffic

Mobility in 5G networks: handover

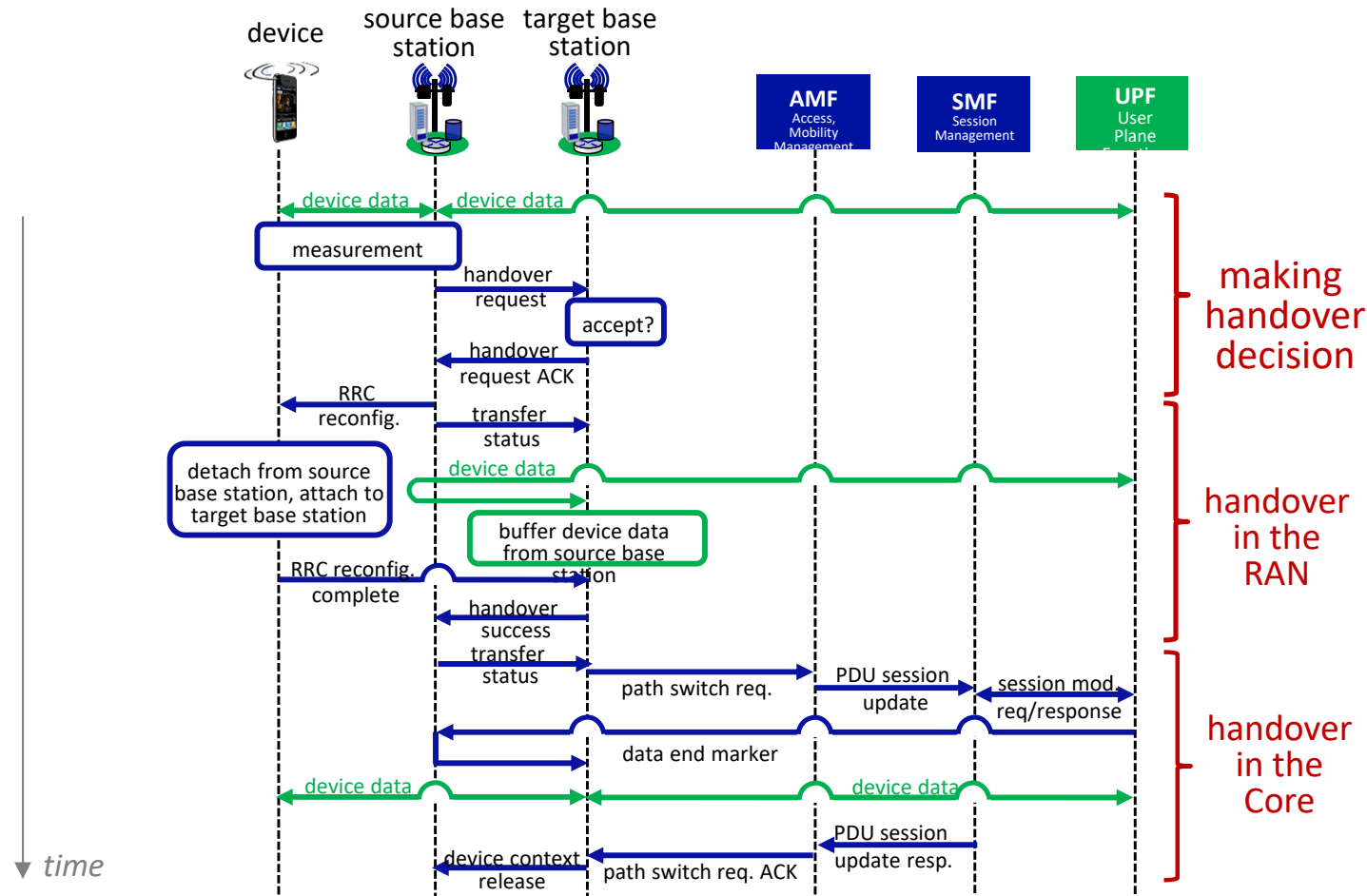


Mobility in 5G networks: handover



- ⑤ target BS informs AMF, SMF that it is new BS for mobile
 - SMF instructs UPF 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 UPF

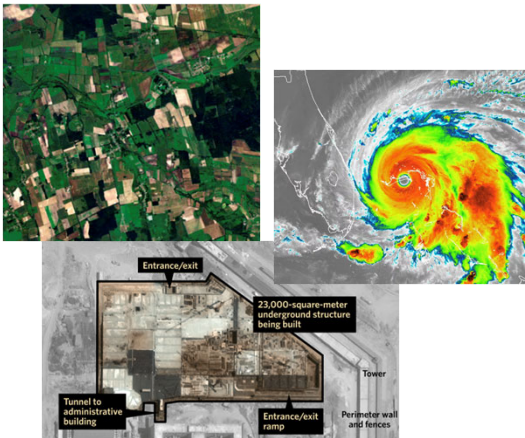
Handover: timeline, signaling



Satellite applications

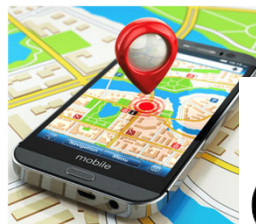
Sensing:

- environment: weather, land use, various human activity
- resolution: $\sim$ m/pixel



Broadcast:

- consumer: Direct to Home TV/video, radio (Dish, SiriusXM)
- business: content to many cable head ends
- GPS
- leverage broadcast: one send reaches many users

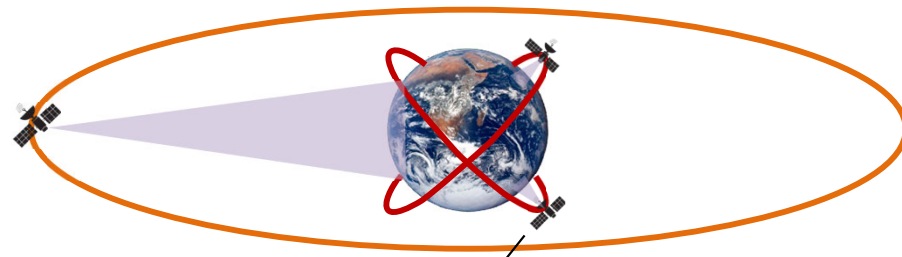


Internet:

- connectivity to unserved regions, alternative to wired Internet
- low latency over long distances
- access i



GEO and LEO satellites

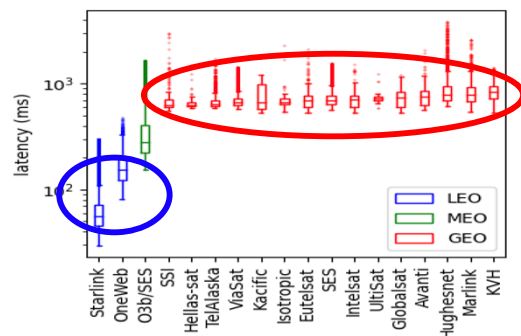


GEO:

- *geosynchronous*: stationary with respect to ground
- 35,768 km above earth
- ~800 msec RTT
- wide area coverage / satellite

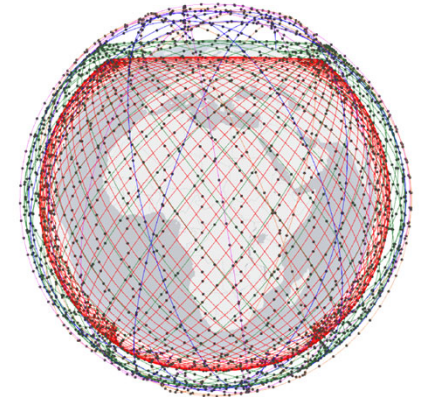
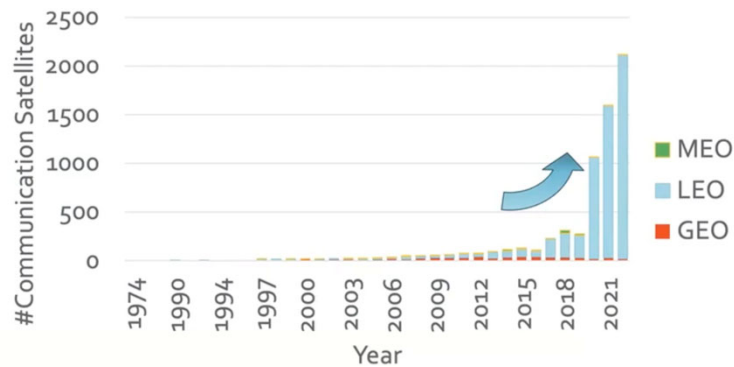
LEO:

- *Low Earth Orbit*: satellite moves with respect to ground: 27,000 km/hour
 - within line of sight (LOS) of ground station for 5-15 mins
- 550 - 1200 km above earth
- ~30 msec RTT in practice
- smaller area coverage / satellite
 - constellation (network) of multiple LEO satellites to cover wide area
 - inter-satellite links (ISL)



Satellites: why all the fuss?

Lots of (LEOS) satellites being launched



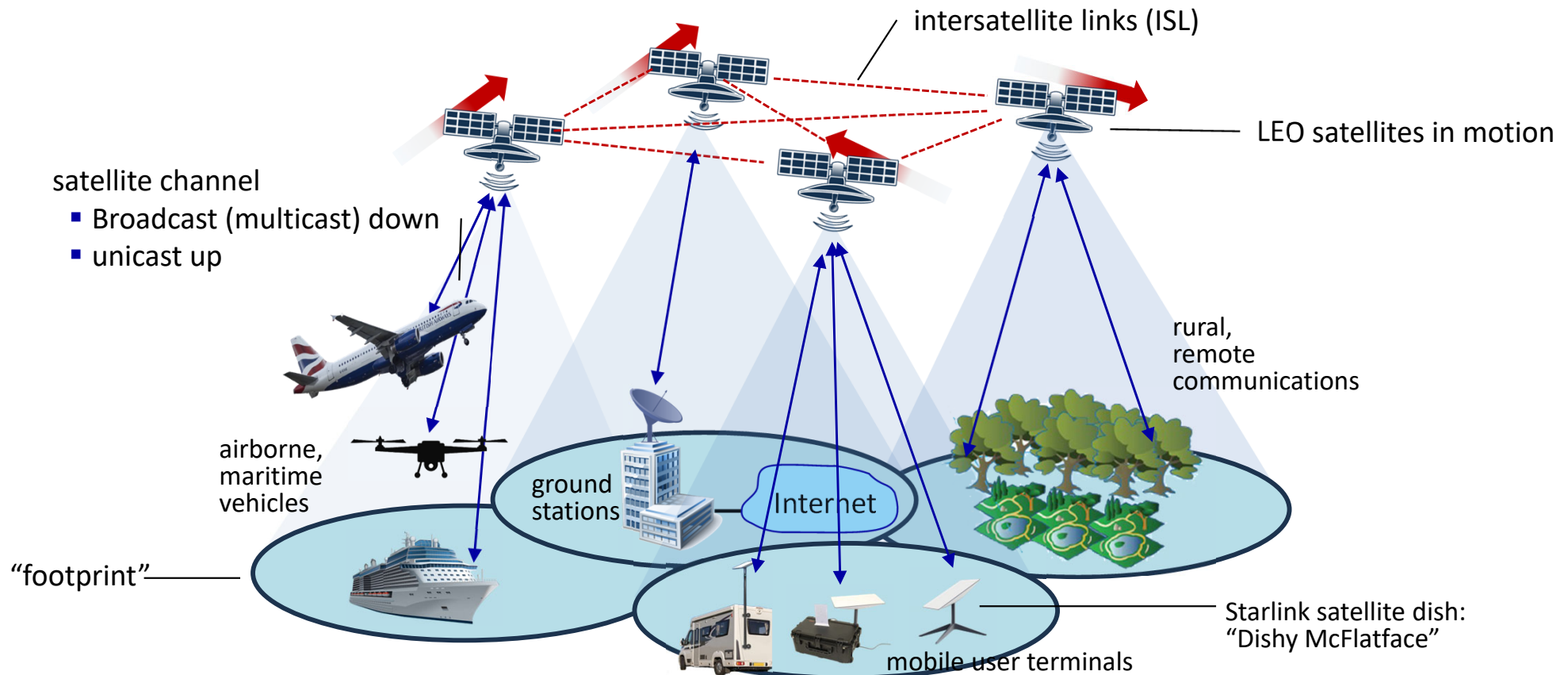
LEOS constellations

	# deployed (2025)	# planned	ISL planned?
Starlink	7,239	12,000 - 42,000	Yes
EutelSat Oneweb	648	716 – 6,372	No
Kuipers (Amazon)	27	3,236	?
Telesat	1	298 - 1671	Yes

Sources: A. Raman, LEO Satellite Mega Constellations, networkingchannel.eu;

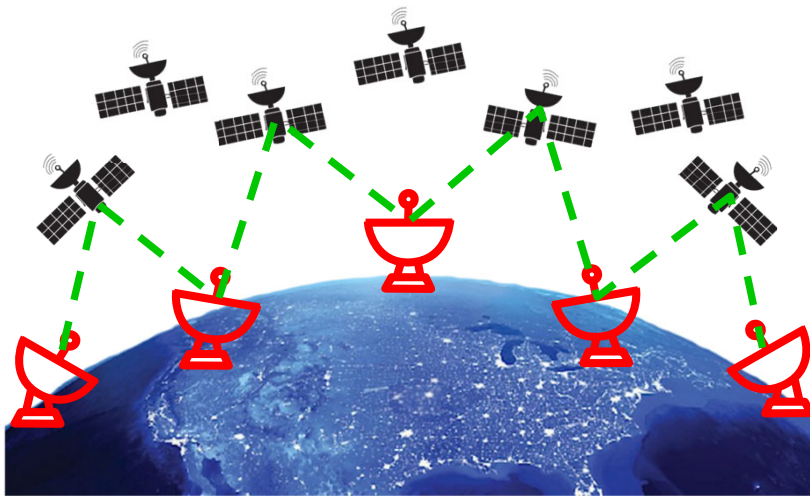
N.Pachler et al., An Updated Comparison of Four Low Earth Orbit Satellite Constellation Systems to Provide Global Broadband; company literature

Components of a LEO satellite network



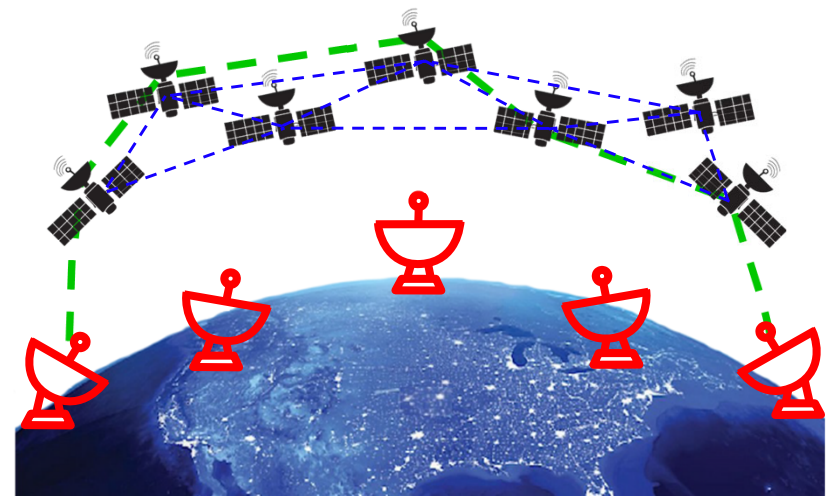
Satellite networking: a link or a network?

links in the sky



- single satellite hop between base stations
- AKA “bent pipe” architecture

network in the sky:



- multiple satellite hops between base stations
- routing among satellites

Starlink

- April 2025: ~7,239 operational LEO satellites (planned: 12K, requested: 30K)
 - first launches: 2019
 - three low-Earth-orbit [orbital shells](#), at 525, 530, 535 km
 - satellites: 500 – 2700 lbs
- services:
 - Internet service: 4M subscribers in Sept 2024 (residential US: \$120/mo)
 - service in Ukraine (terrestrial networks damaged)
 - 2024: testing direct-to-smartphone tests would use cellular spectrum from SpaceX's U.S. mobile partner T-Mobile



60 Starlink satellites stacked together before deployment on 24 May 2019

Recommended Reading

- Behrouz A. Forouzan, Data Communications and Networking with TCP/IP Protocol Suite, 6th ed., 2022, Chapter 5
- J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 8th ed., 2022, Chapter 7
- J. F. Kurose and K. W. Ross, Computer Networking: A Top-Down Approach, 9th ed., 2025, Chapter 7