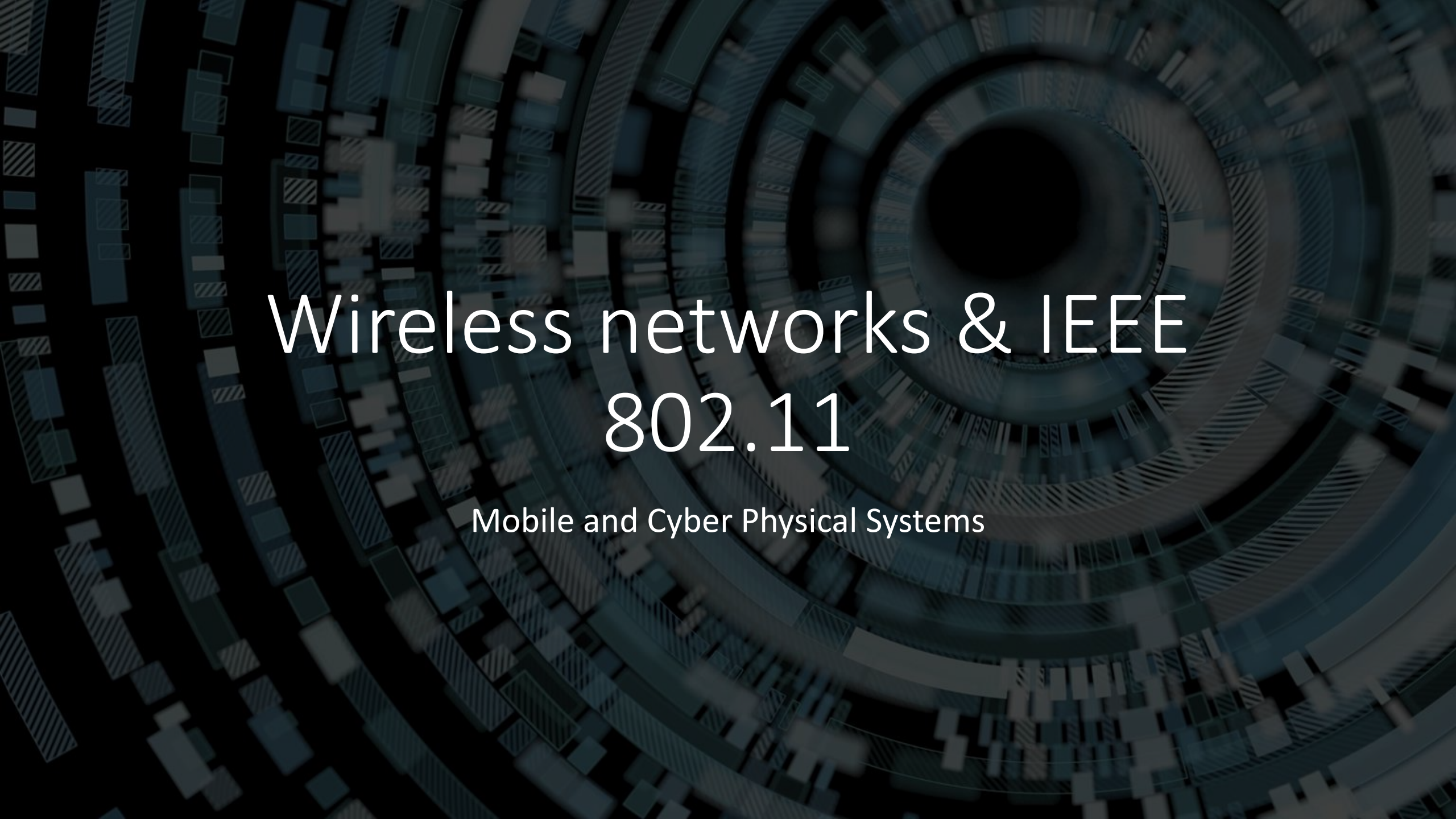


Wireless networks & IEEE 802.11

Mobile and Cyber Physical Systems

Overview

Wireless networks basics

Wireless networks architectures

IEEE 802.11 (Wi-Fi) a/b/g/n/…

Why Wireless Networks?

1. Cables in computers to:
   - communicate
   - provide power
2. Cyber-physical systems embed computers in (any kind of) physical objects
   - Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.
   - can't wire everything…

Hence:

- wireless to replace cables in communications…
- … & batteries to replace cables in power supply

Wireless Networks

WIRELESS NETWORKS

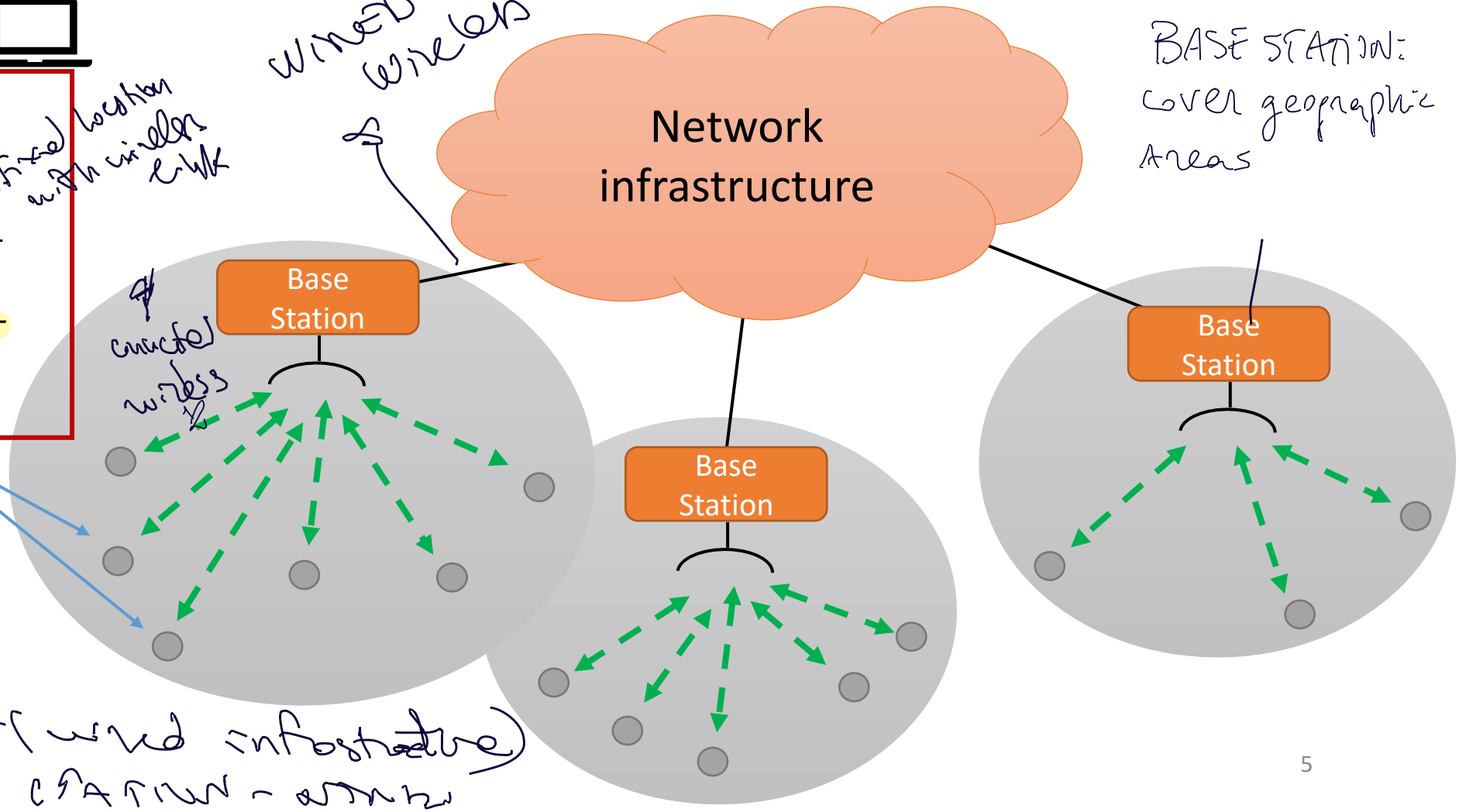
- Networks of **hosts** connected by **wireless links**
- Hosts: end-system devices that run applications
  - often mobile, but not necessarily
  - battery-powered (typically)
  - e.g. smartphone, tablet, sensor, home appliance, vehicle, etc…
- Two modes of operations:
  1) **Infrastructure**
     - with base station(s) or
     - with wired access points
  2) **ad hoc networking**
     - no centralized coordinators

we have nodes that must be coordinated
- core network provides: AUTHENTICATION
- BILLING

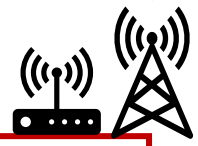
Elements of a Wireless network (I)

Wireless hosts

- LAPTOPS, SMARTPHONES
- RUN APPLICATIONS
- MAY BE STATIONARY (NON-MOBILE) OR MOBILE
- WIRELESS DOES *NOT ALWAYS* MEAN MOBILITY



Elements of a Wireless network (II)



Base station

- TYPICALLY CONNECTED TO A WIRED NETWORK
- RELAY - RESPONSIBLE FOR SENDING PACKETS BETWEEN WIRED NETWORK AND WIRELESS HOST(S) IN ITS "AREA"
- E.G., CELL TOWERS, IEEE 802.11 ACCESS POINTS

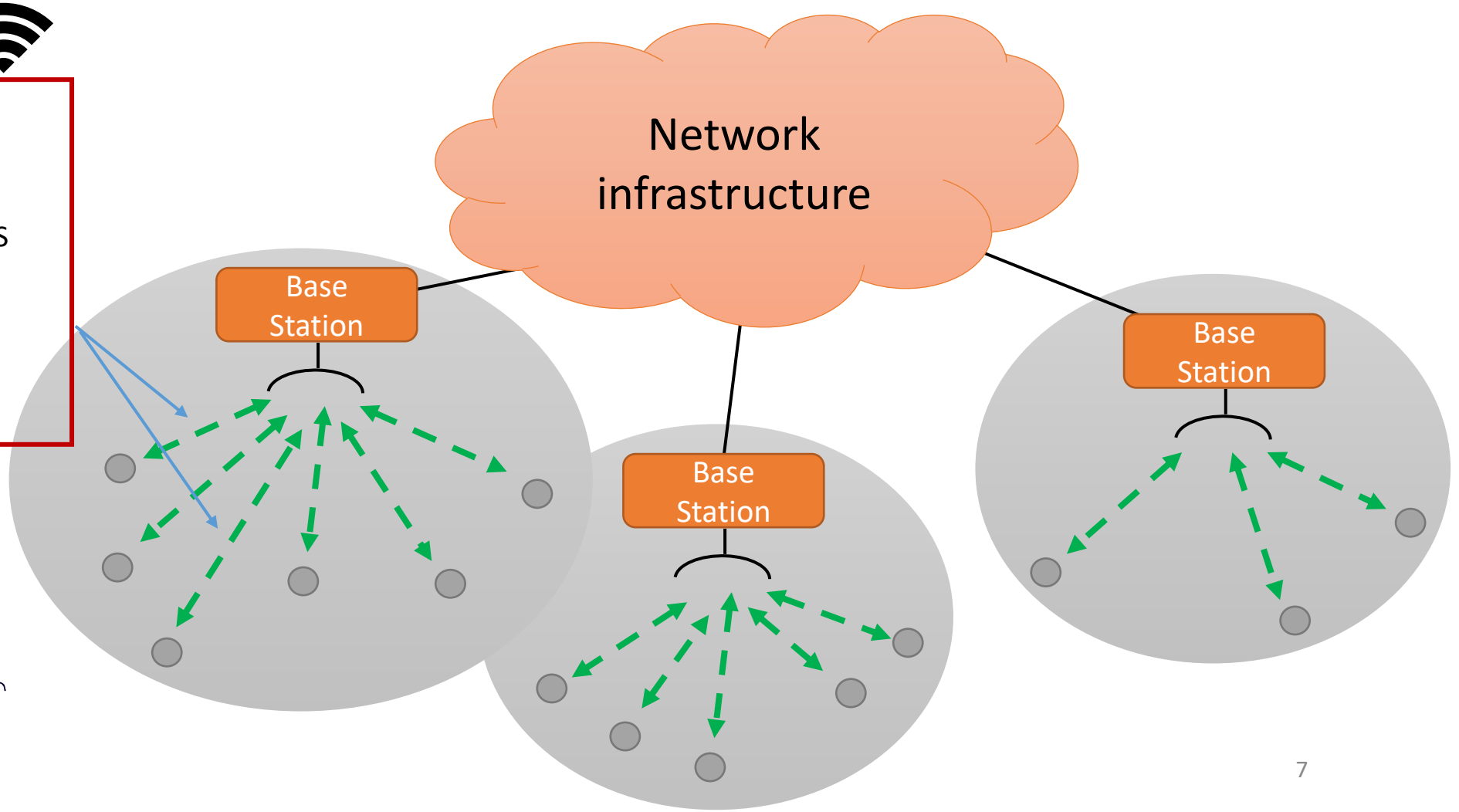
Elements of a Wireless network (III)

Wireless links

- CONNECT MOBILE(S) TO BASE STATION
- ALSO USED AS BACKBONE LINKS
- MULTIPLE ACCESS PROTOCOL COORDINATES LINK ACCESS
- VARIOUS DATA RATES, TRANSMISSION RANGE,…

PROBLEM to SOLVE FOR ACCESS POINTS

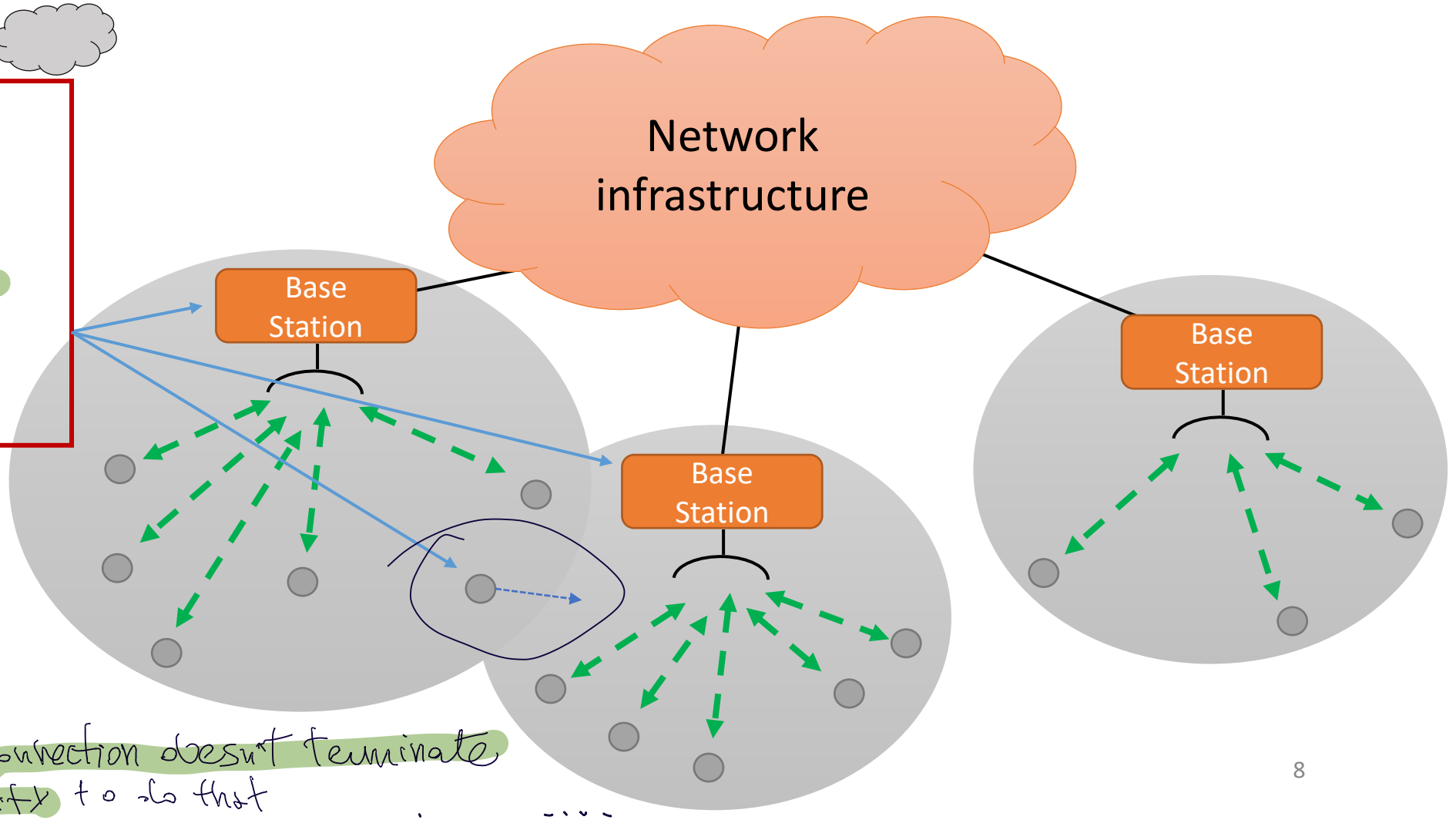
- How accesses
- coexisting medium



Elements of a Wireless network (IV)

Infrastructure mode

- BASE STATION CONNECTS MOBILES INTO WIRED NETWORK
- HANDOFF: MOBILE CHANGES BASE STATION PROVIDING CONNECTION INTO WIRED NETWORK

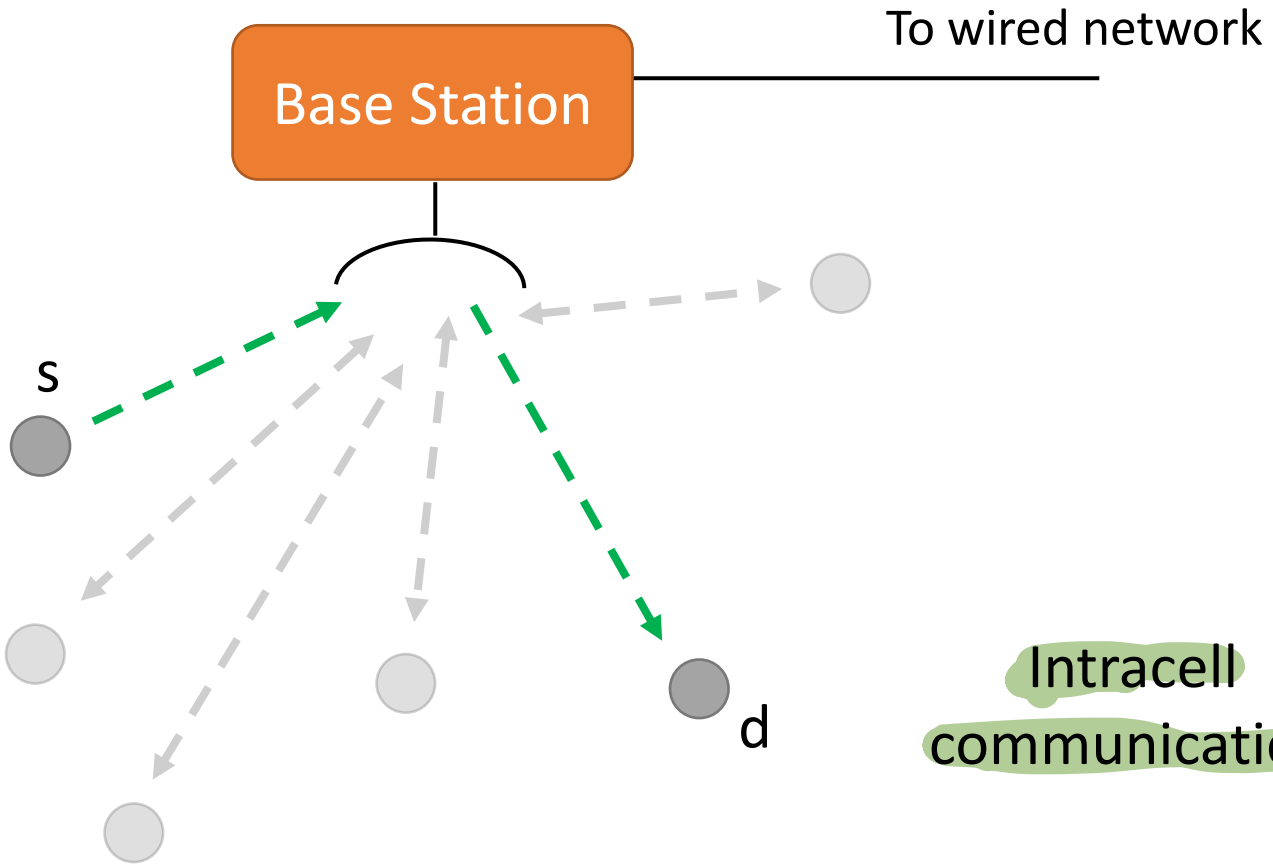


problem

- a node can be moved between base-stations
- Behind: it exchanging CONTROL MESSAGES => connection doesn't terminate => exchange of responsibility to do that

LL> (example: cellphones move on same/different operators/providers → AUTHENTICATION, BILLING

Elements of a Wireless network (V)

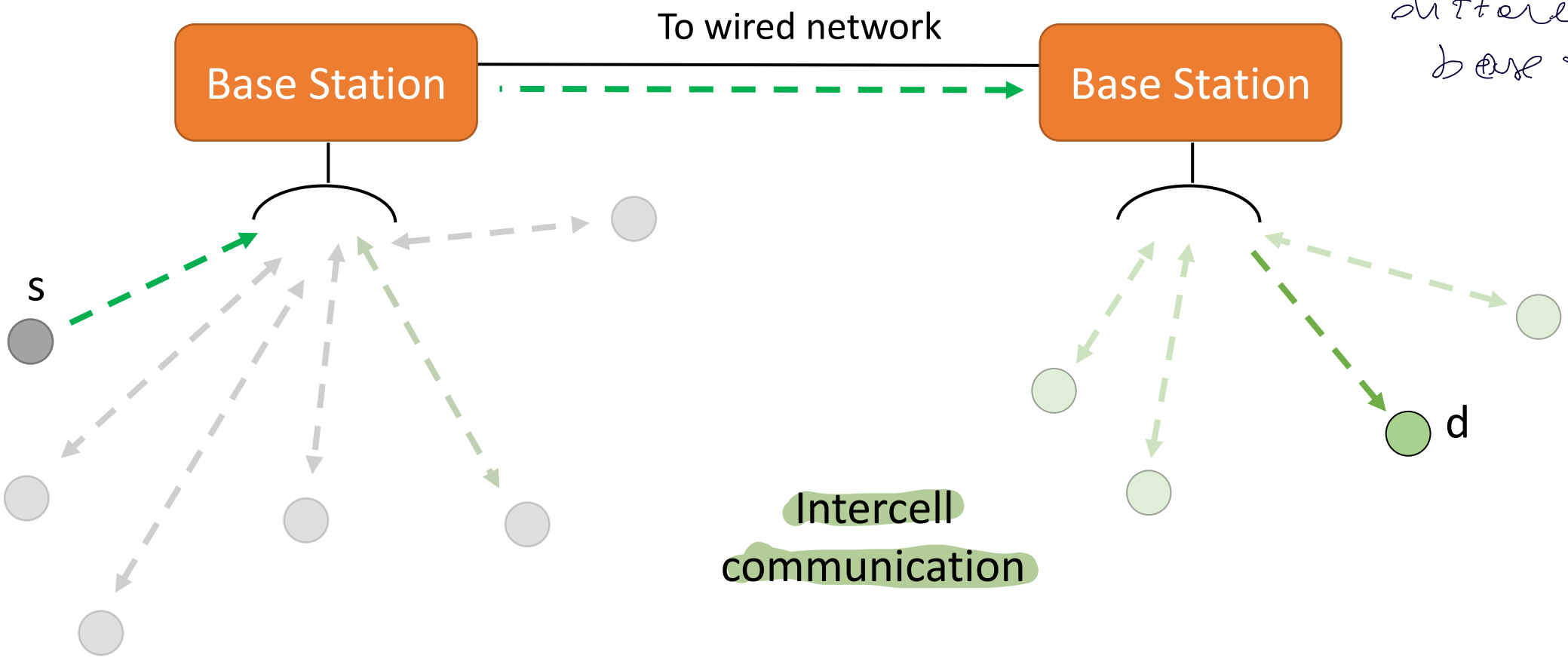


• the two host (end-devices) communicate on the same base station

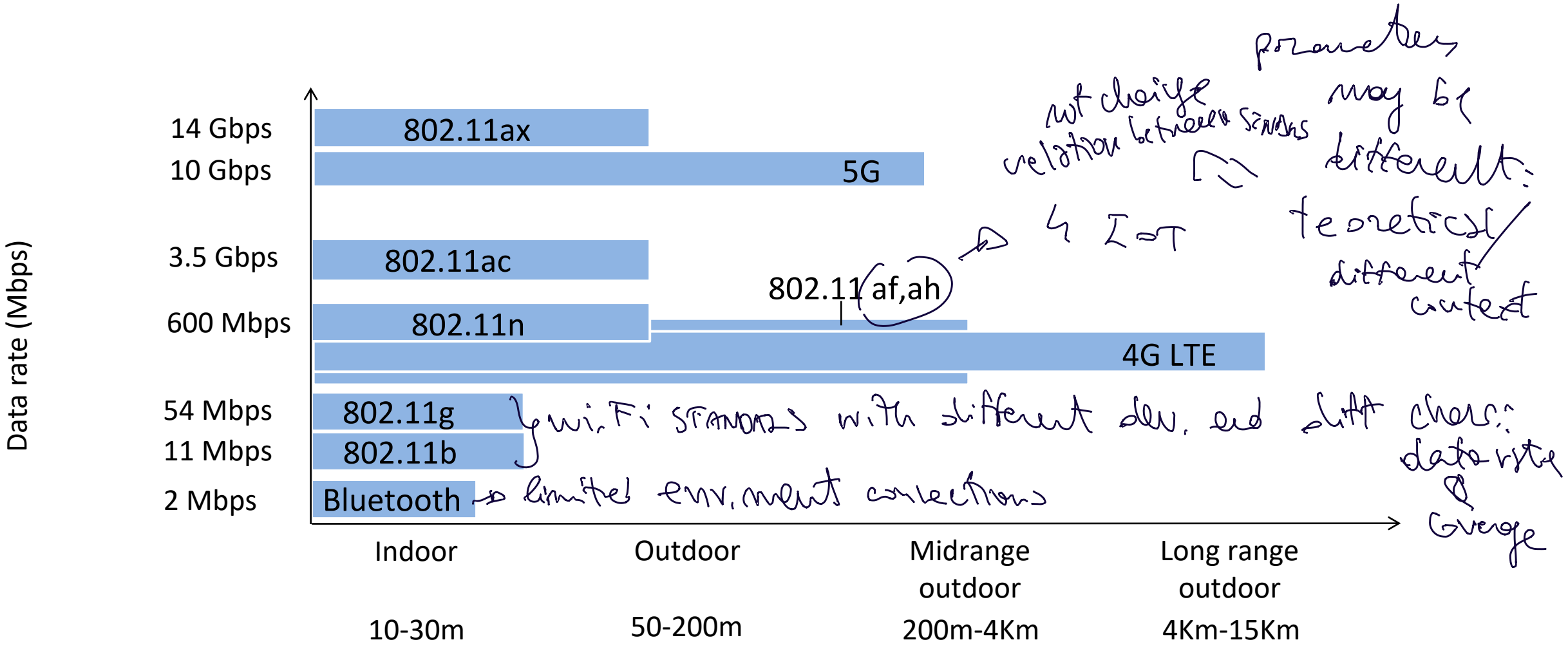
Intracell communication

Elements of a Wireless network (VI)

the two hosts communicates between 2 different base stations



Characteristics of selected wireless links



Wireless network taxonomy

	Single hop	Multiple hops
1) infrastructure (e.g., APs)	host connects to base station (WiFi, WiMAX, cellular 3G,4G,5G) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: MESH networks
2) no infrastructure	• no base station, not necessarily connection to larger Internet (e.g. Bluetooth)	• no base station, no connection to larger Internet. May have to relay on other nodes to reach a given wireless node (ZigBee, ad hoc, VANET)

Wireless Links Characteristics (I)

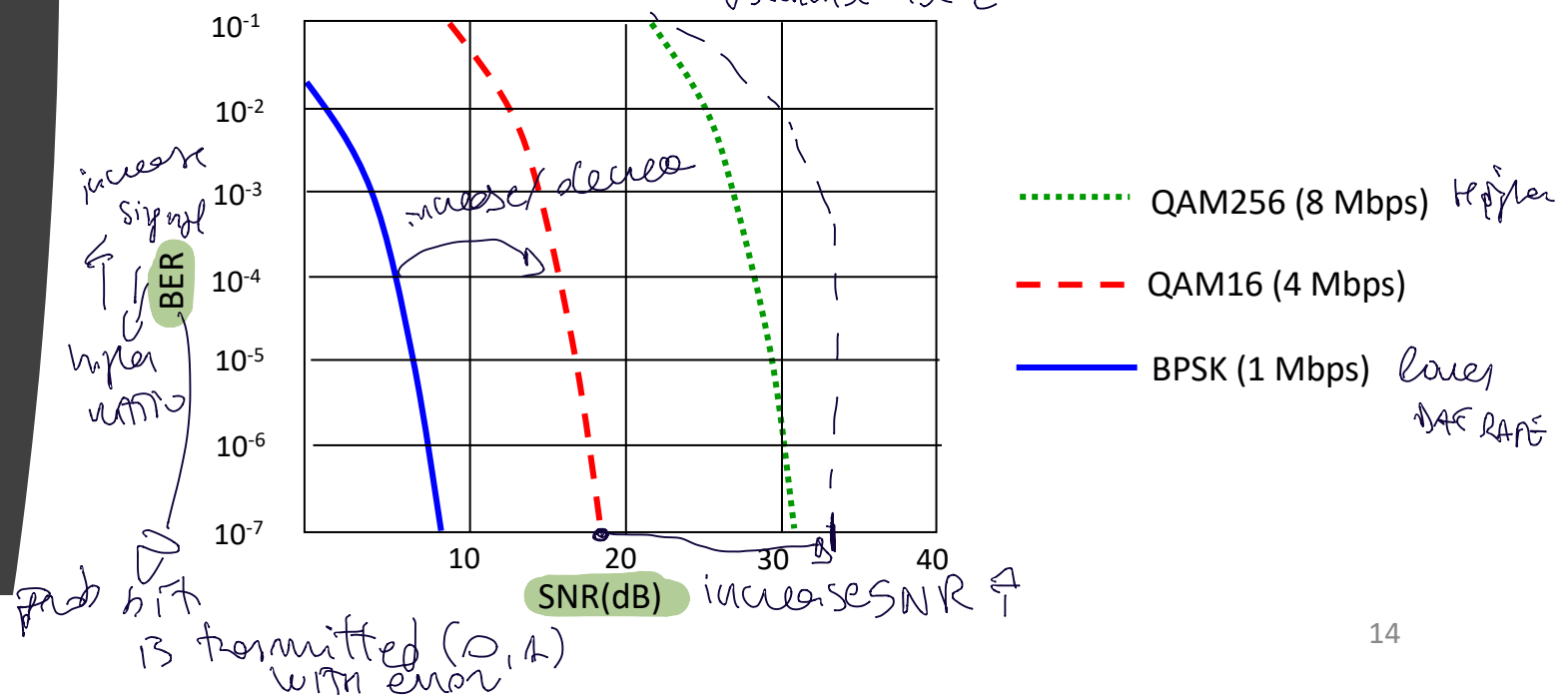
important differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other wireless devices (e.g., mobile phones). Engines, appliances (microwave ovens…),… may interfere as well
- multipath propagation: radio signal reflects off objects or ground, arriving at destination at slightly different times

…. make communication across wireless links much more "difficult" (even a point to point)

Wireless Links Characteristics (II)

- **SNR: signal-to-noise ratio**
  - larger SNR – easier to extract signal from noise (a "good thing")
  - SNR in dB = 20*log(signal/noise)
- SNR versus BER tradeoffs
  - bit error rate (BER): probability that a transmitted bit is received in error at the receiver
  - given physical layer: increase power -> increase SNR->decrease BER
  - given SNR: choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

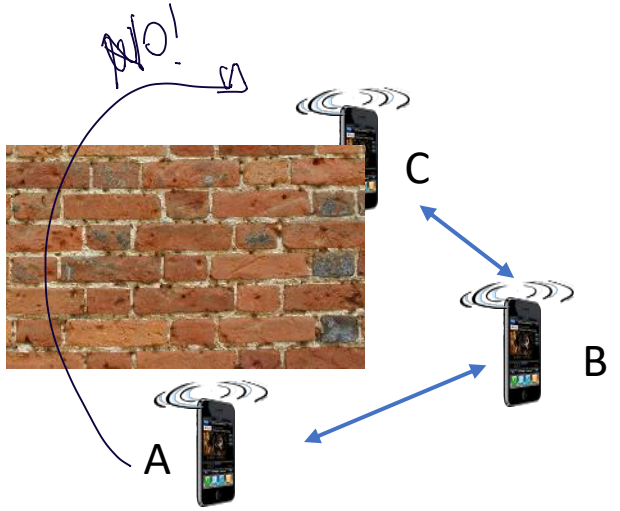


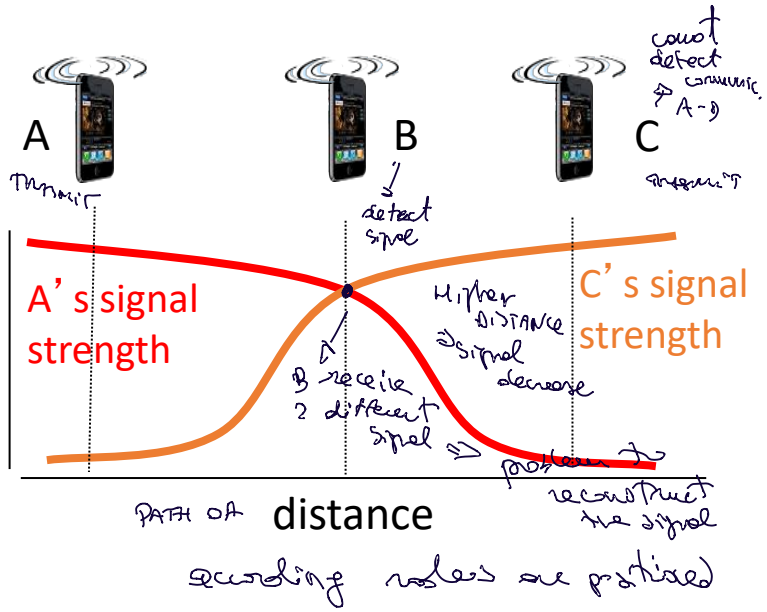
Wireless Links Characteristics (III)

Difficult: hosts in env => situations is different while nodes send stuff

Signal attenuation or obstacles limit transmission ranges

SIGNAL STRENGTH: potenza del segnale





according rules are defined

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

Wireless networks challenges

WIRELESS NETWORKS PROBLEMS

1) **Limited knowledge** a node detect e (s.Trection) (maybe 2 nodes) but not all communications

- a terminal cannot hear all the others
- hidden/exposed terminal problems (DISAPPEARS) Join/Disappears

2) **Mobility/Failure of terminals**

- terminals move in the range of different BS (Join/Exit): base Station
- terminals move away from each other

3) **Limited terminals** limited battery power

- battery life, memory, processing and transmission range

4) **Privacy**

- eavesdropping of ongoing communications
  - intercettazioni

Wireless networks: required mechanisms

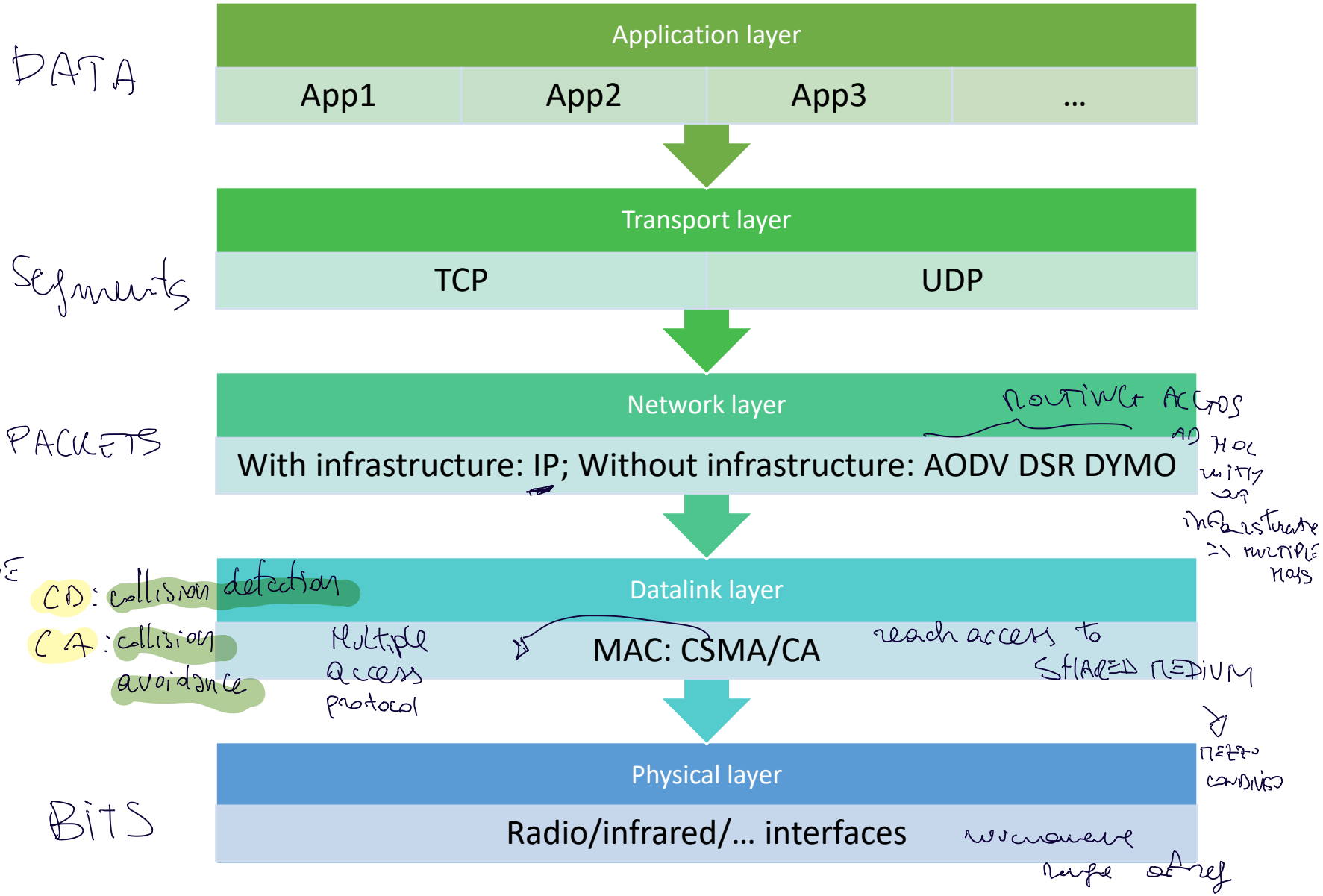
WIRELESS NETWORKS REQUIREMENTS

1) • Access to a shared wireless channel
  - CSMA/CD cannot be used… → MULTIPLE ACCESS PROTOCOL

2) • Hand-off (Networks with infrastructure) → TRASPASSO
  - moving a terminal into the range of a different BS

3) • Routing (multi-hop ad hoc networks)
  - finding a path from source to destination in multi hop networks
  - dealing with arbitrary changes in neighborhood

Wireless networks protocol stack



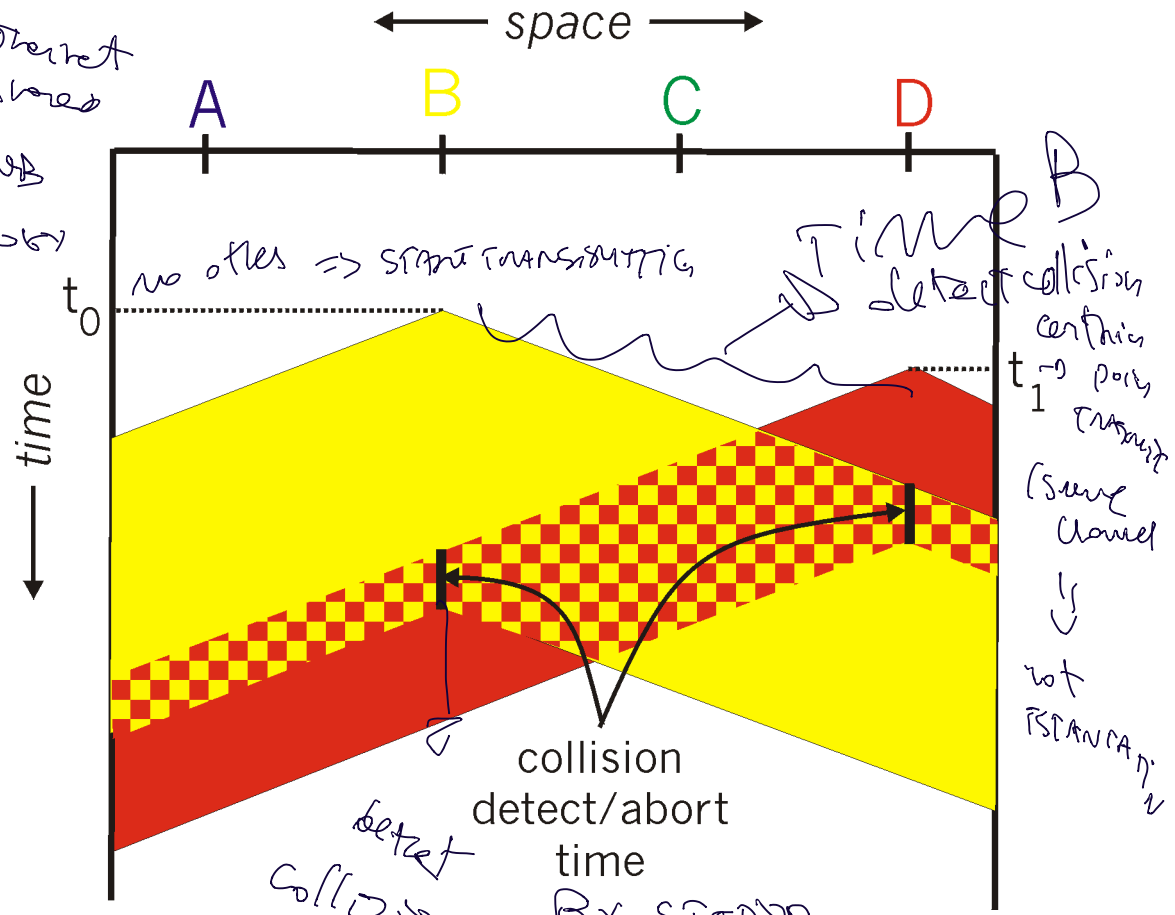
RECAP: MAC protocols for **wired networks**

- Basic assumptions:
  - a single channel is available for all communications
  - all stations can transmit on it and receive from it
  - if frames are sent simultaneously on the channel the resulting signal is garbled (a **collision**)
  - all stations can detect collisions

- Different protocols
  - ALOHA, slotted ALOHA, CSMA, CSMA/CD, …

Carrier Sense Multiple Accesses with Collision Detection (CSMA/CD)

- Basic idea of CSMA:
  - When a station has a frame to send it listens to the channel to see if anyone else is transmitting
  - *if the channel is busy*, the station waits until it becomes idle
  - when channel is idle, the station transmits the frame
  - if a collision occurs the station waits a random amount of time and repeats the procedure.



CSMA/CD (2)

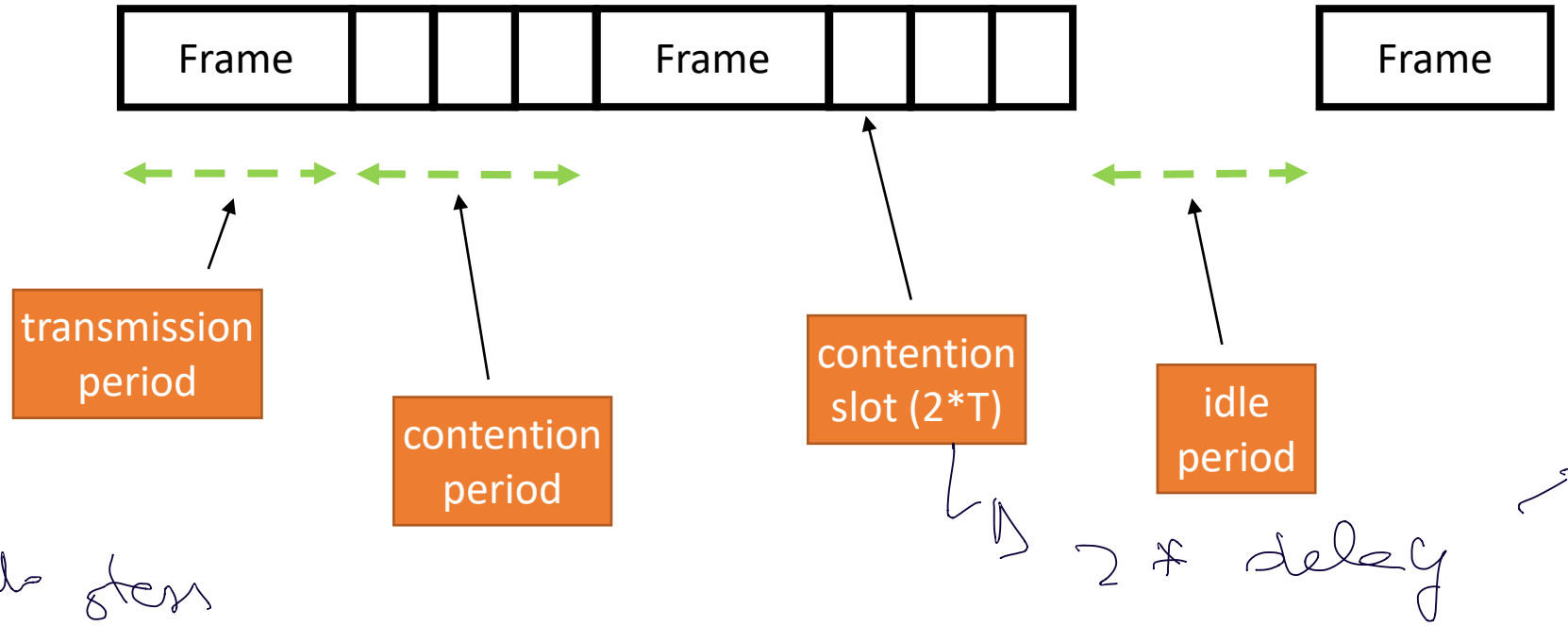
- CSMA with *Collision Detection*
  - a station aborts its transmission as soon as it detects a collision
    - if two stations sense the channel idle simultaneously and start transmitting, they quickly abort the frame as soon as collision is detected
  - it is widely used on LANs in MAC sub-layer
  - IEEE 802.3 Ethernet

ALGO:

CSMA/CD (3)

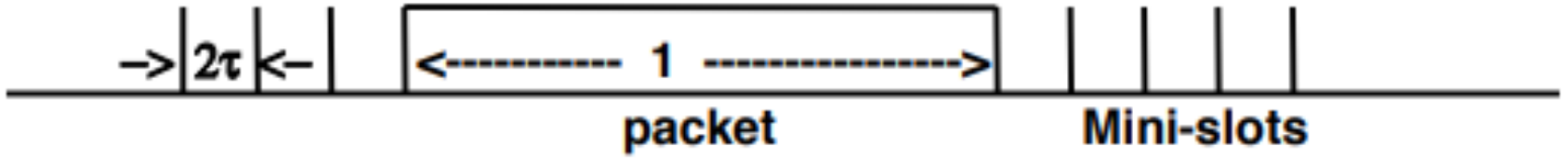
CSMA/CD behavior

- T is the time required to reach the farthest station
- It takes minimum of RTT time (2*T) to detect collision.



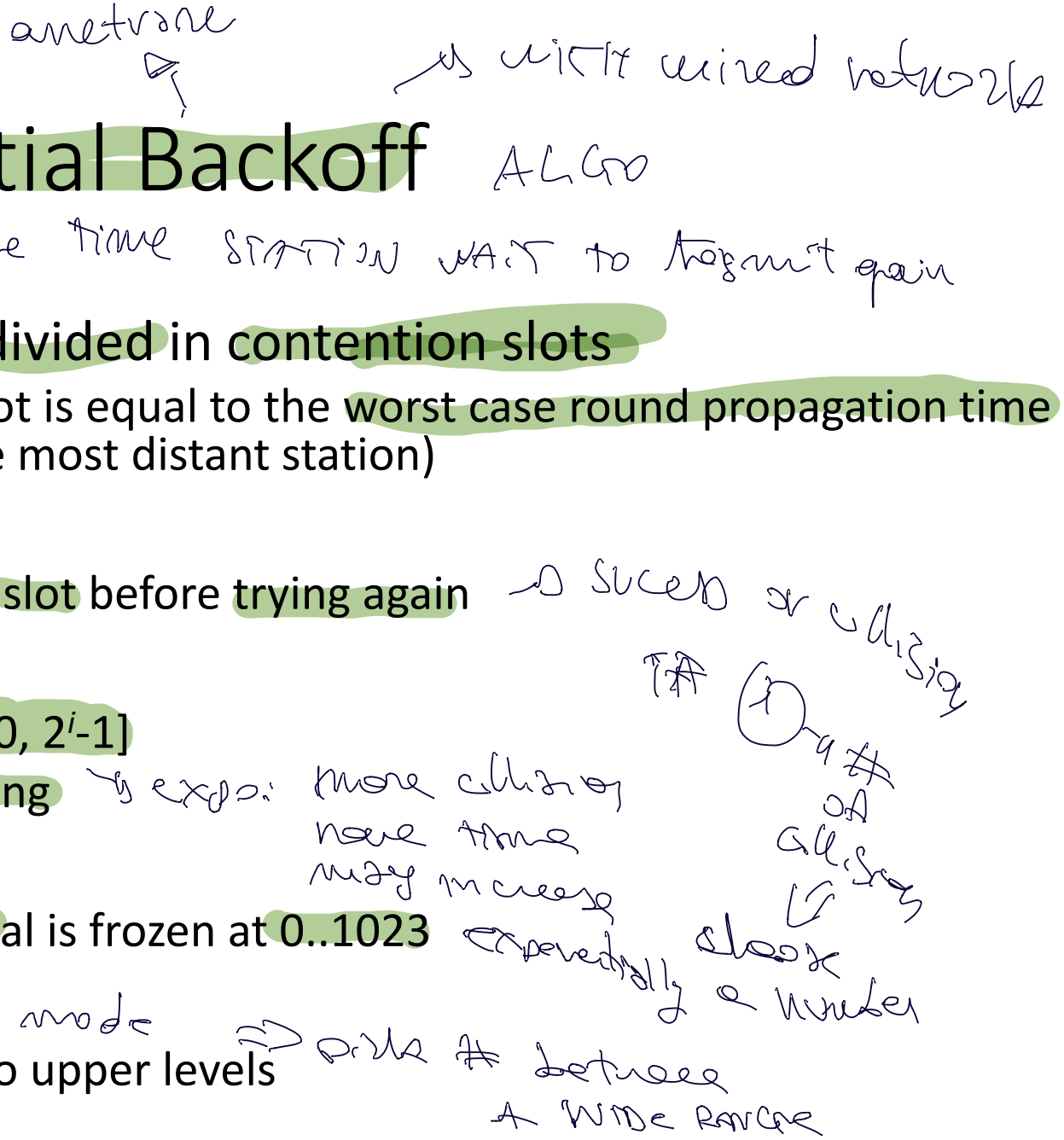
CSMA/CD (4)

- Consider a slotted system with “mini-slots” of duration 2τ
- If a node starts transmission at the beginning of a mini-slot, by the end of the mini- slot either
  - No collision occurred and the rest of the transmission will be uninterrupted
  - A collision occurred, but by the end of the mini-slot the channel would be idle again
- • Hence a collision at most affects one mini-slot



Binary Exponential Backoff

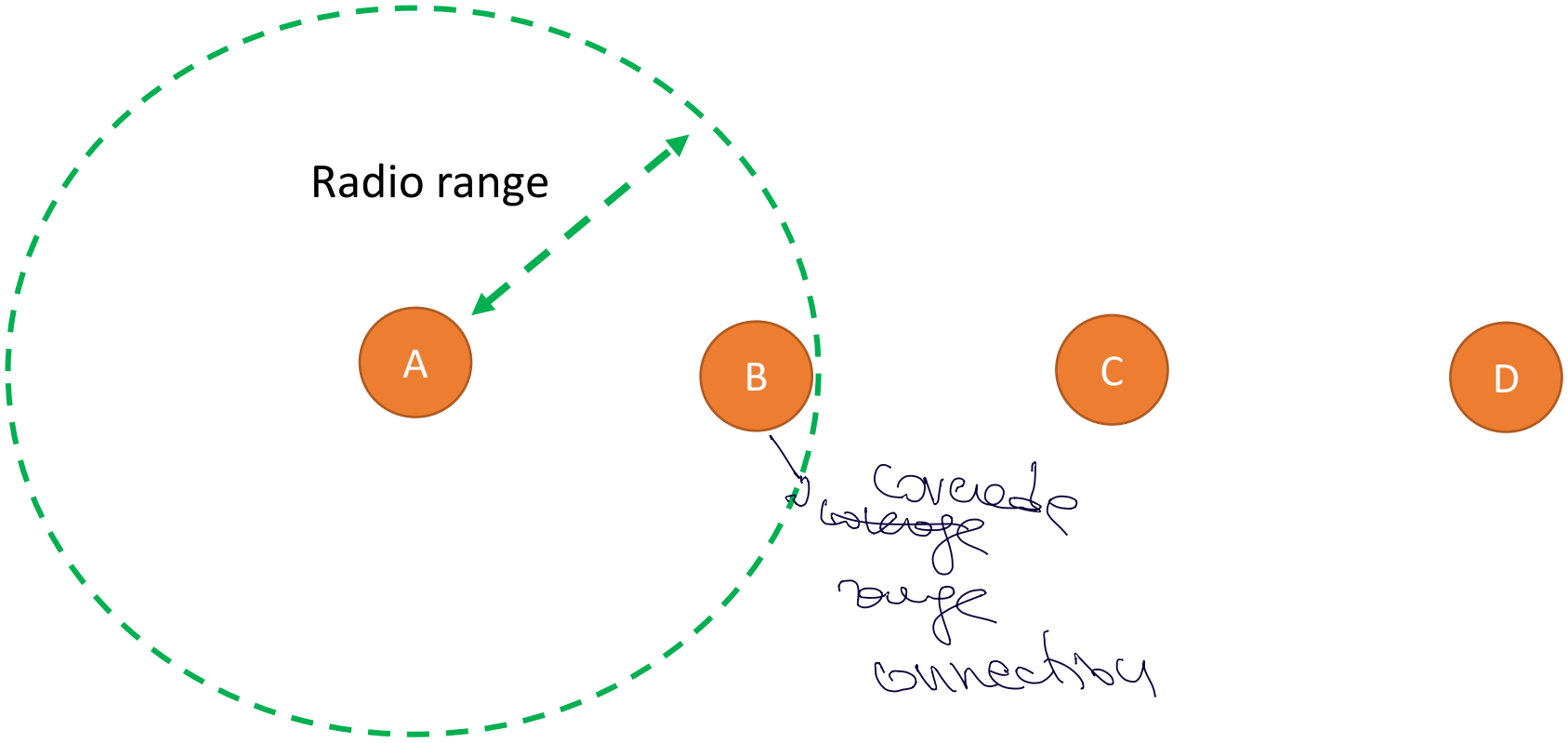
- Time after a collision is divided in contention slots
  - length of a contention slot is equal to the worst case round propagation time (2T if T is the time to reach the most distant station)
- After the first collision
  - each station waits 0 or 1 slot before trying again
- After collision *i*
  - chooses *x* at random in [0, 2^i-1]
  - skips *x* slots before retrying
- After 10 collisions:
  - the randomization interval is frozen at 0..1023
- After 16 collisions
  - failure is reported back to upper levels



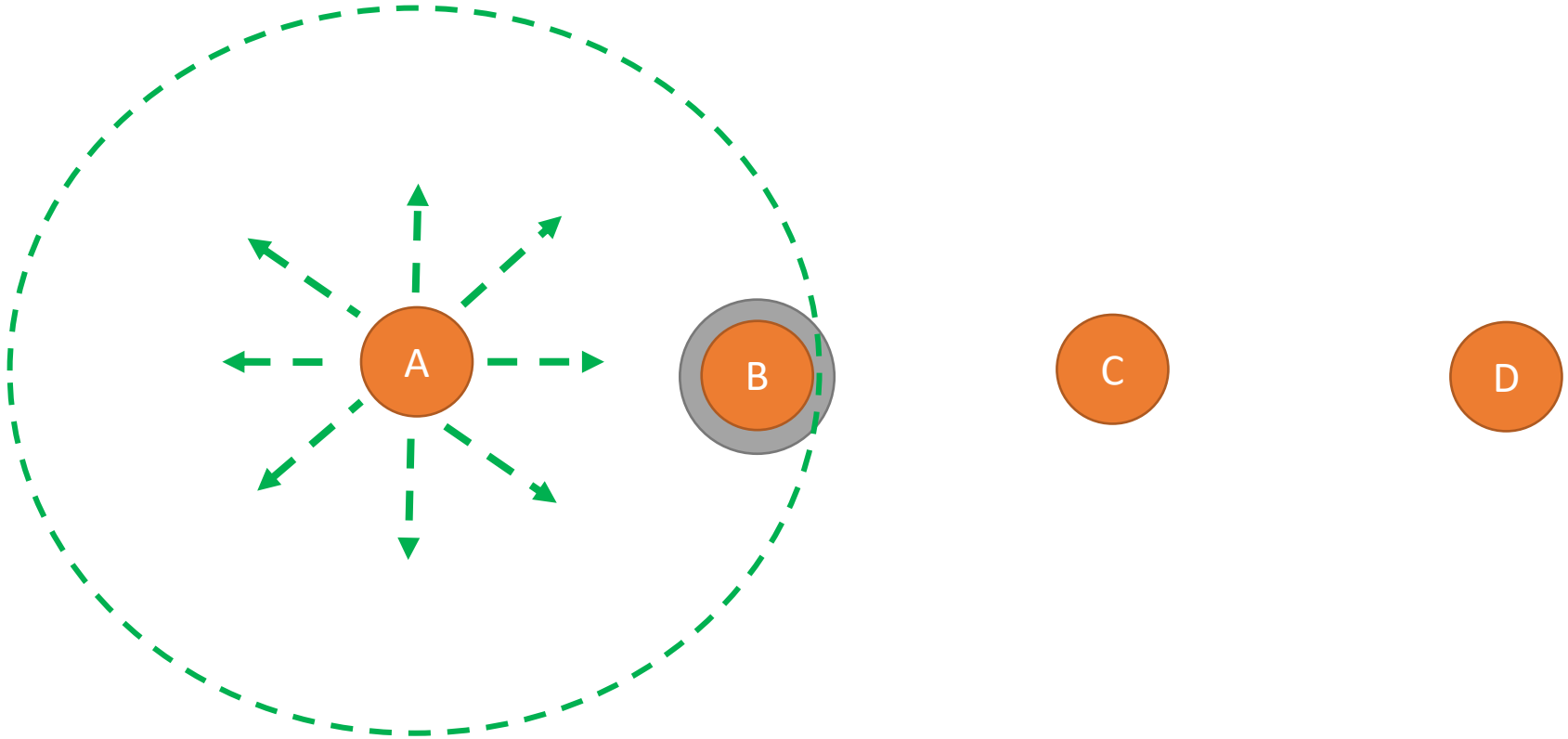
Wireless networks: MAC

CSMA/CD detects interference while trasmitting!	in wired networks it's OK, but not in wireless!
Hidden terminal problem	what matters is ◦ **interference at the receiver** *not* at the sender
Exposed terminal problem	what matters is **interference at the receiver** *not* at the sender

The hidden terminal problem

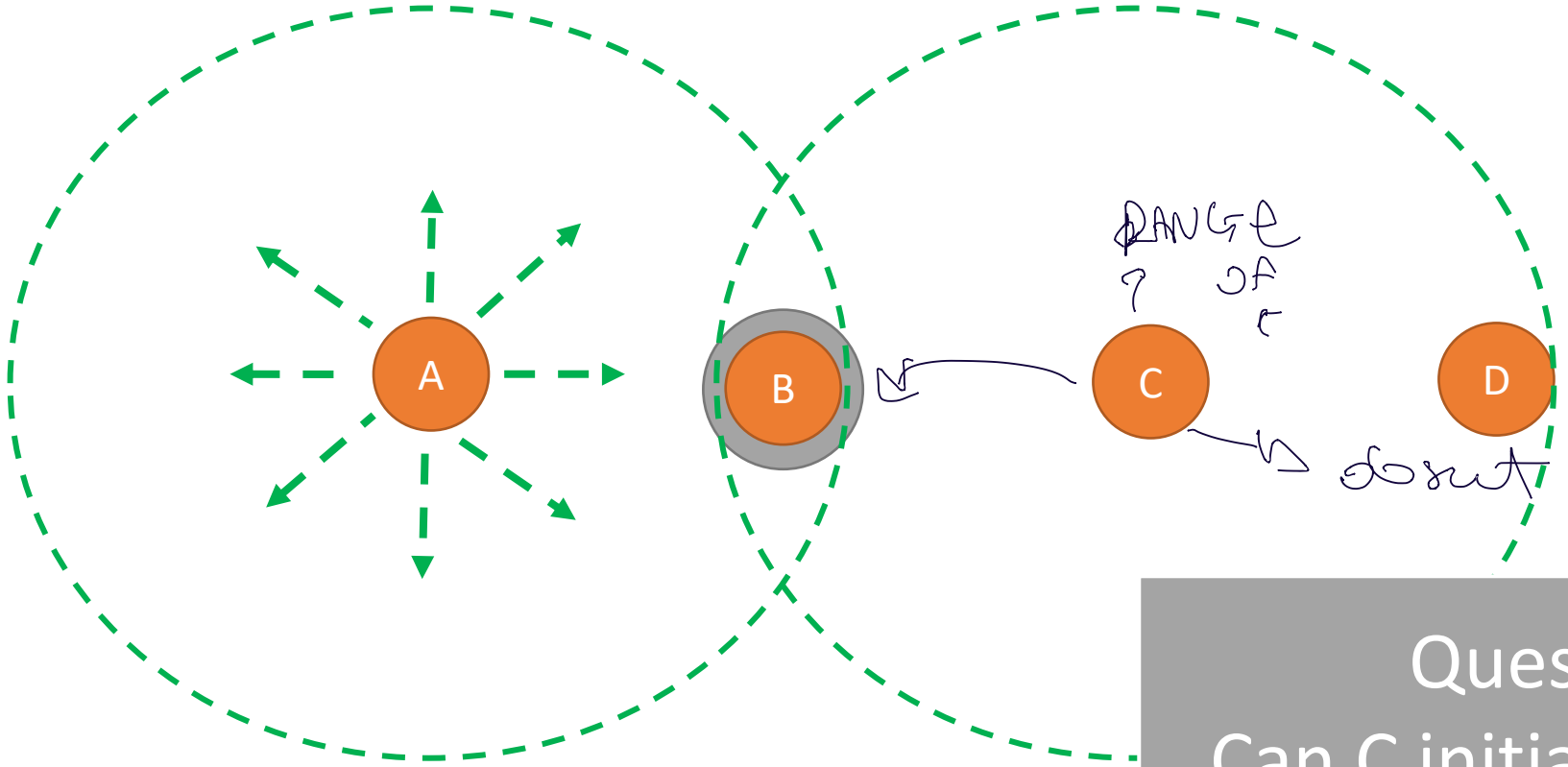


The hidden terminal problem (2)



A is sending to B

The hidden terminal problem (3)



A is sending to B

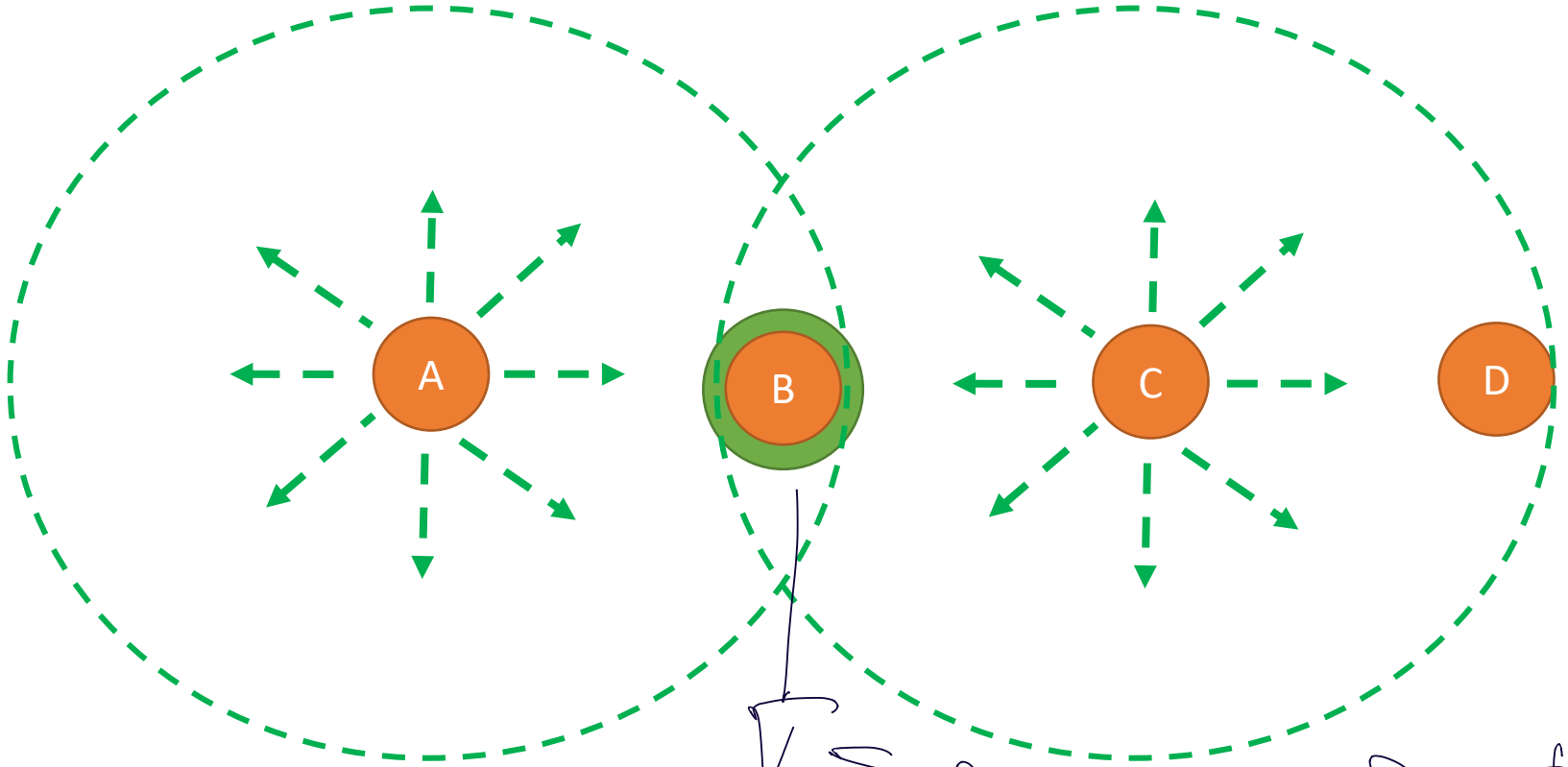
C senses the medium: it will NOT hear A, out of range

Question for you:

Can C initiate a transmission?

What happens if C transmits?

The hidden terminal problem (4)



A is sending to B

C senses the medium: it will NOT hear A, out of range

C transmits to anybody (either B or to D) : **COLLISION at B!**

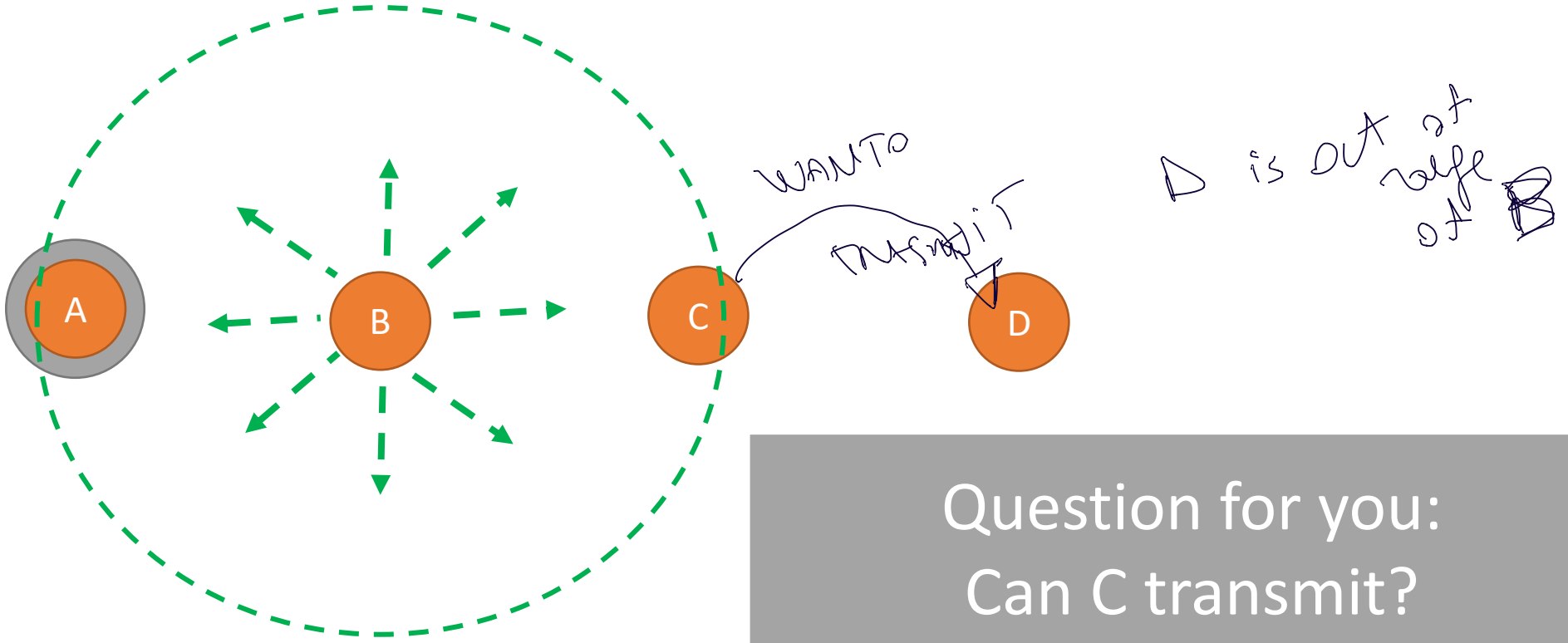
Hidden terminal problem	C is not able to detect a potential competitor because it is out of range: a collision happens at B (the receiver) For the same reason A does not detect the collision C is **hidden** with respect to the communication from A to B

Hidden terminal problem

two or more stations which are out of range of each other transmit simultaneously to a common recipient

ANOTHER SITUA

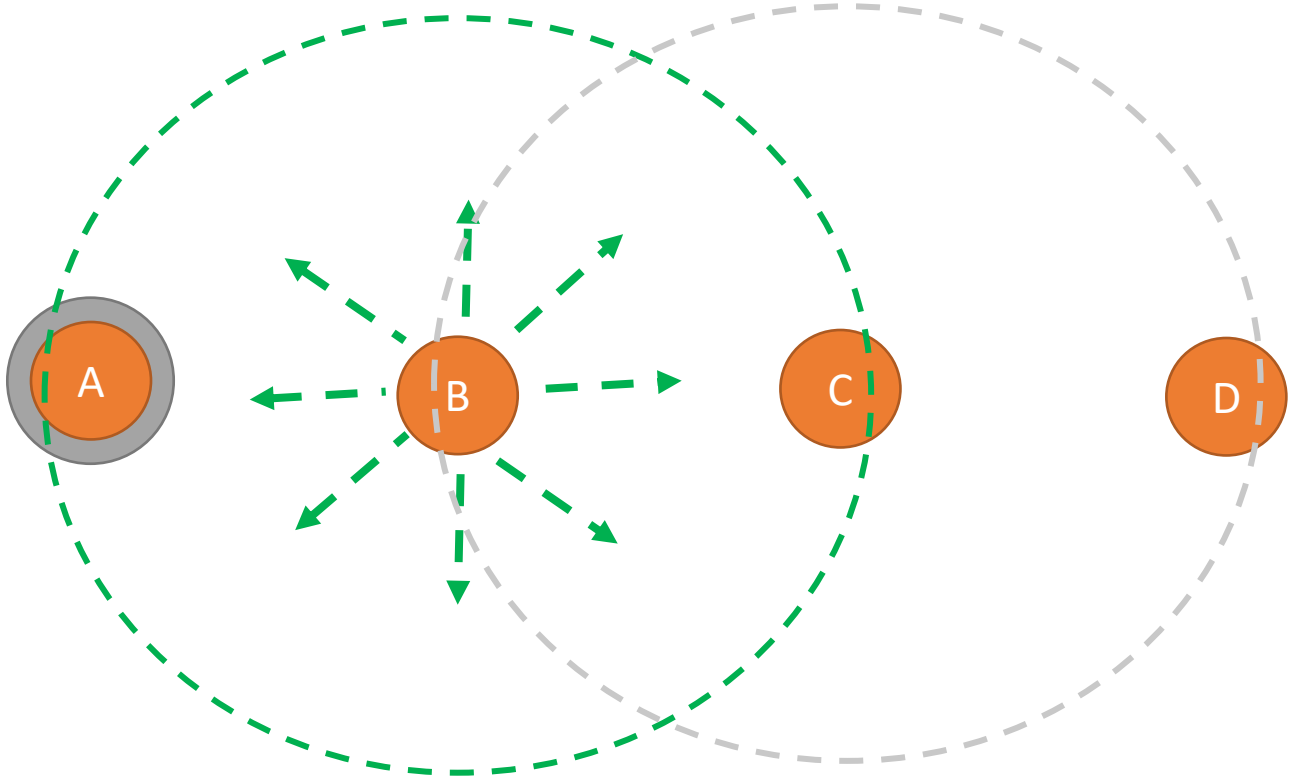
The exposed terminal problem



1. B is transmitting to A, C wants to transmit to D

Question for you:
Can C transmit?
What happens if C transmits?

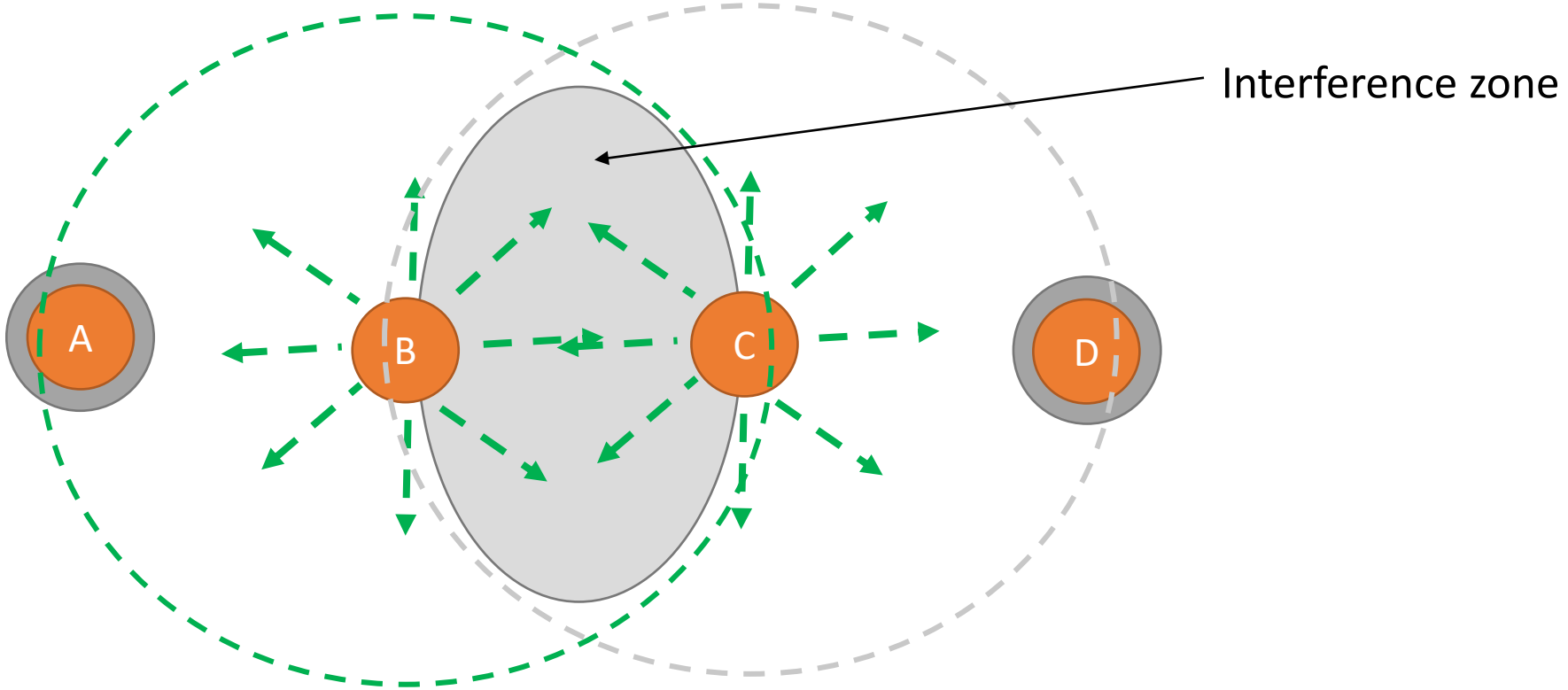
The exposed terminal problem (2)



1. B is transmitting to A, C wants to transmit to D
2. C senses the medium, concludes: **cannot transmit** to D

L'ascolta che B sta inviando frame ad A => 1 solo canale di comunicazione

The exposed terminal problem (3)



1. B is transmitting to A, C wants to transmit to D
2. C senses the medium, concludes: **cannot transmit** to D
3. The two transmissions can actually happen in parallel.

We have

Exposed terminal problem

C hears a transmission from B to A

C does not send to D although its transmission would be OK

C is **exposed** with respect to the communication from B to A

Exposed terminal problem

a transmitting station is prevented from sending frames due to interference with another transmitting station

Wireless networks

What matters **is interference at the receiver** not at the sender

- this cannot be checked by sensing the carrier at the sender

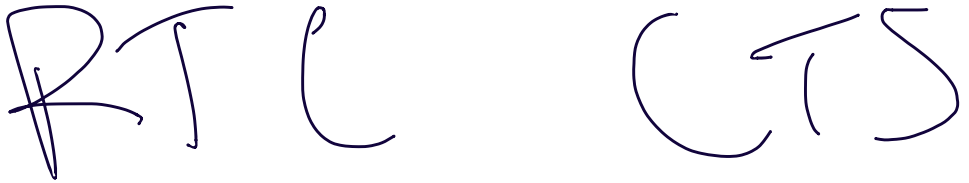
Multiple transmissions can occur simultaneously if destinations are out of range of each other

- a station may hear a transmission and be able to transmit without interfere with it

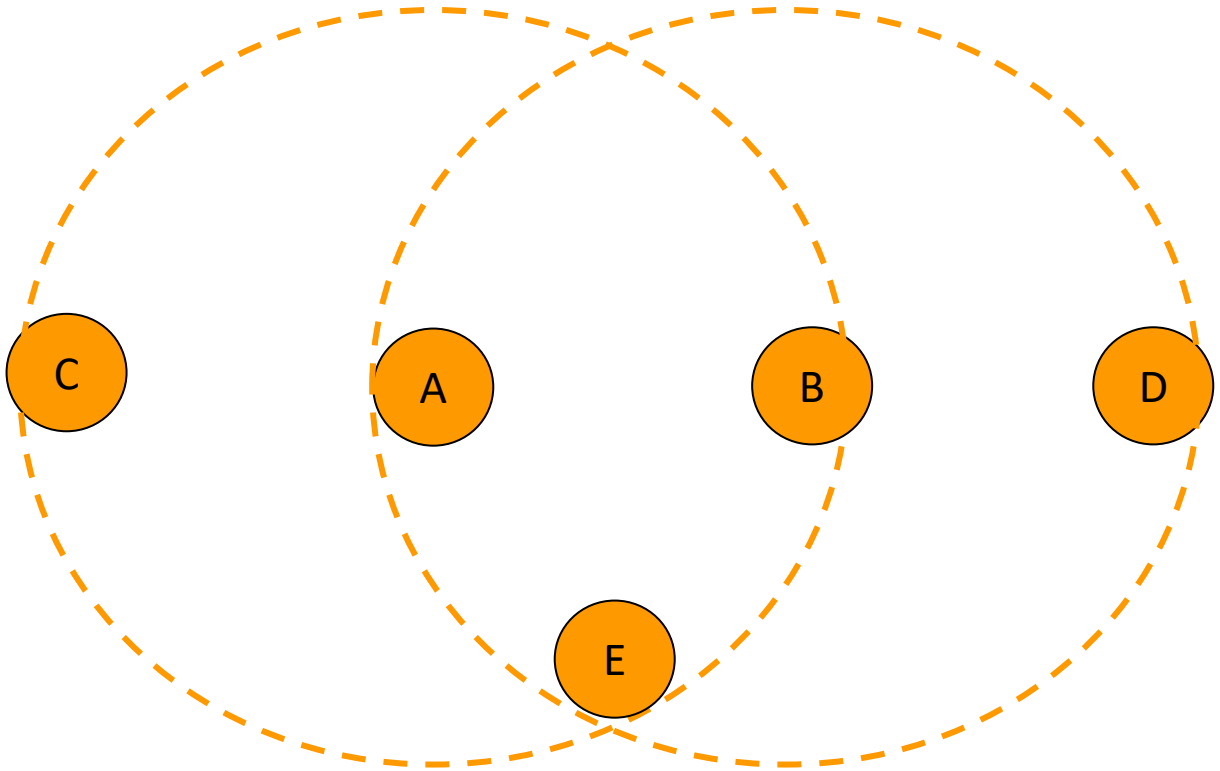
Need sensibly different MAC protocols from wired LANs

The MACA protocol

- Multiple Accesses with Collision Avoidance
- Basic idea:
  - stimulate the receiver into transmitting a short frame first
  - then transmit a (long) data frame
  - stations hearing the short frame **refrain from transmitting** during the transmission of the subsequent data frame

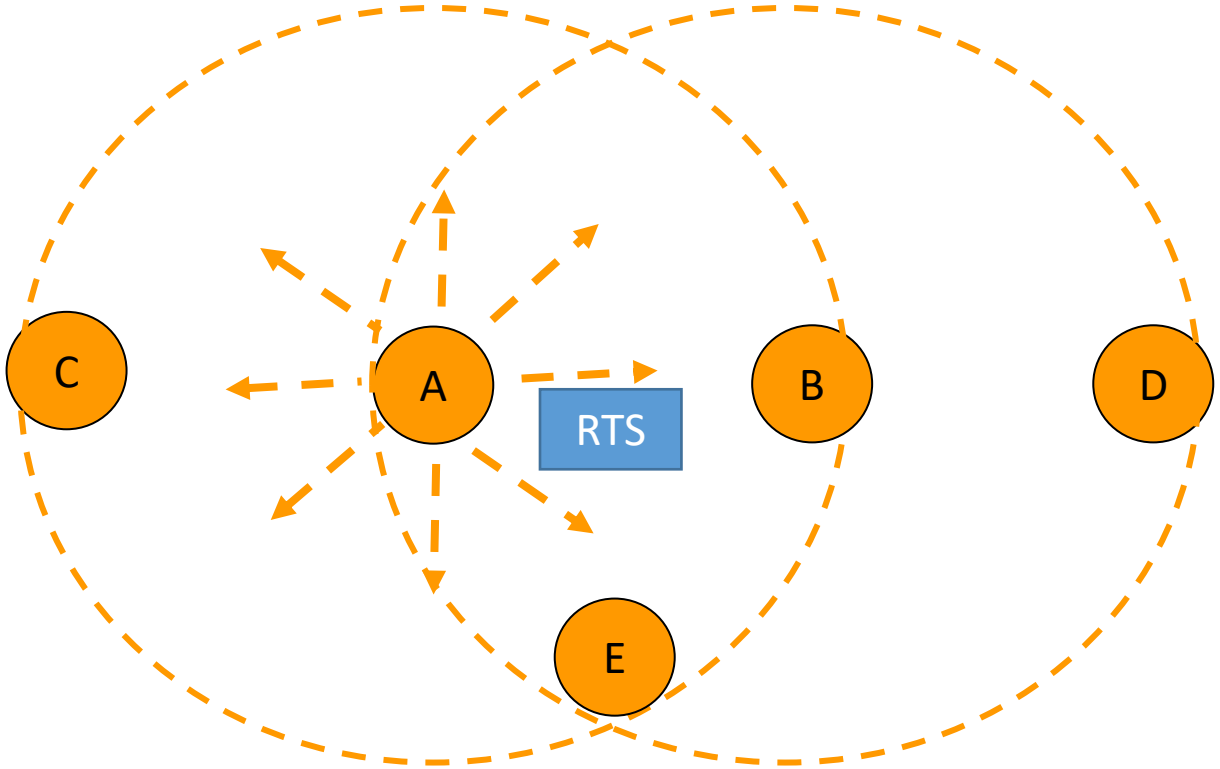


The MACA protocol



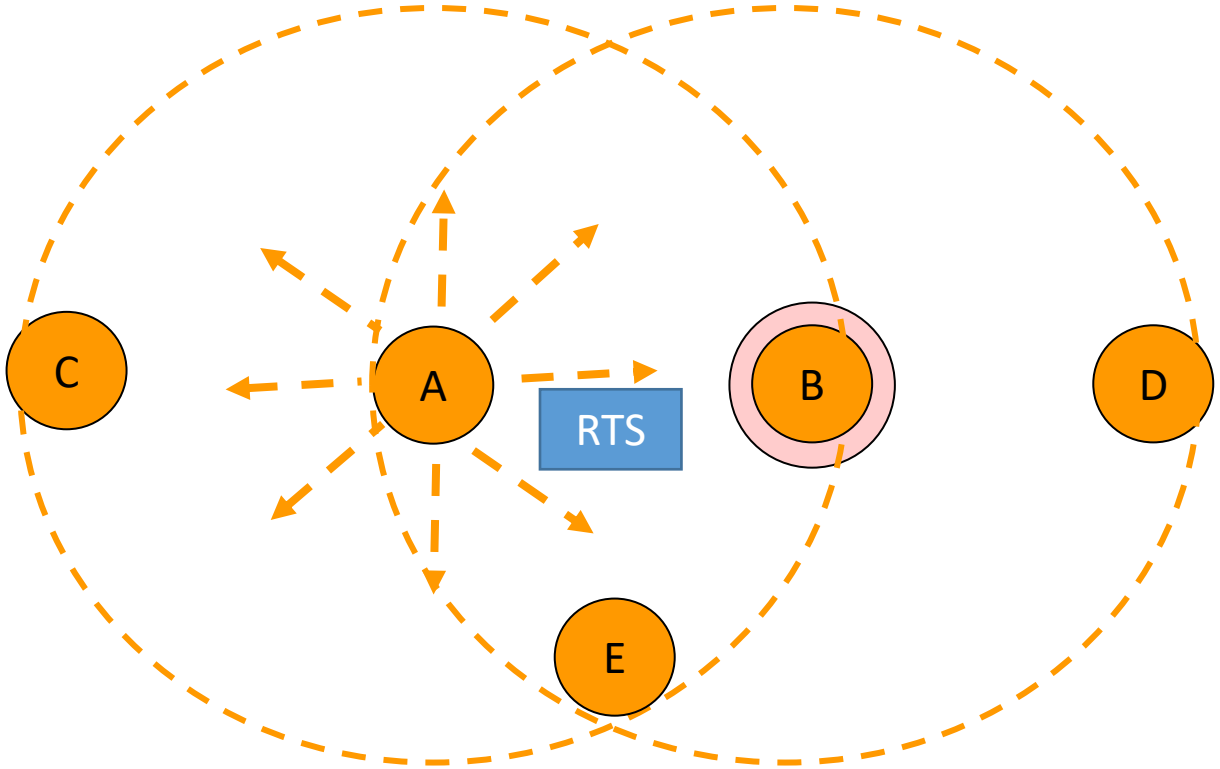
C is within range of A and *out of range of B and D*
D is within range of B and *out of range of A and C*
E is within range of both A and B

The MACA protocol (2)



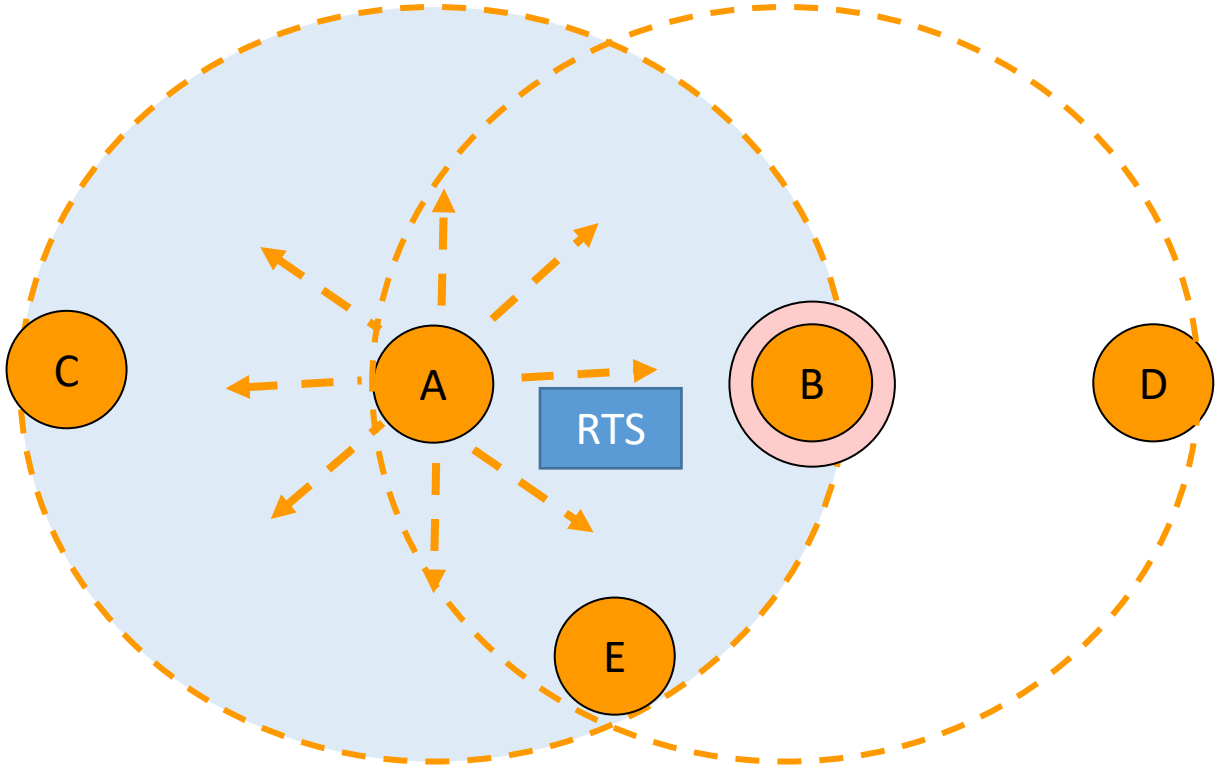
1. A wants to transmit to B, sends a **Request To Send (RTS)** to B

The MACA protocol (3)



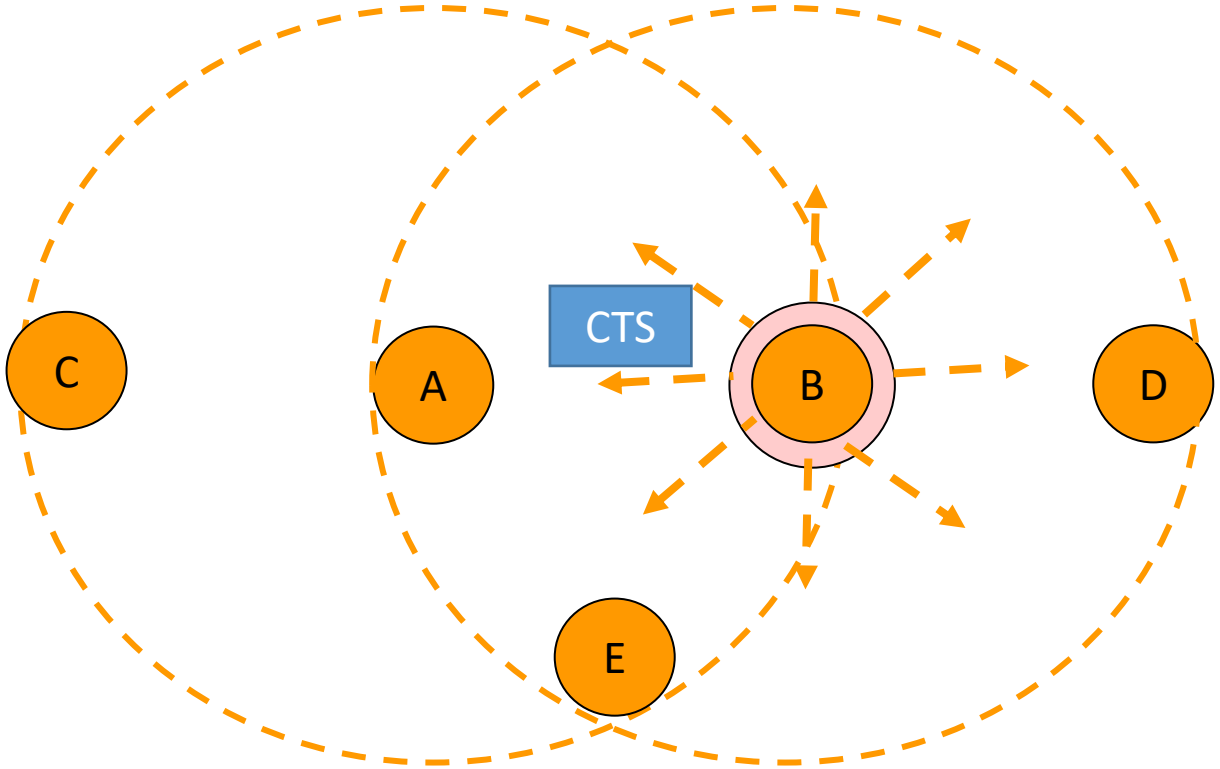
1. A wants to transmit to B, sends a **Request To Send** to B
   RTS is a short frame including the length of the data frame that will eventually follow

The MACA protocol (4)



1. A wants to transmit to B, sends a **RTS** to B
   B, C and E receive the **RTS** from A

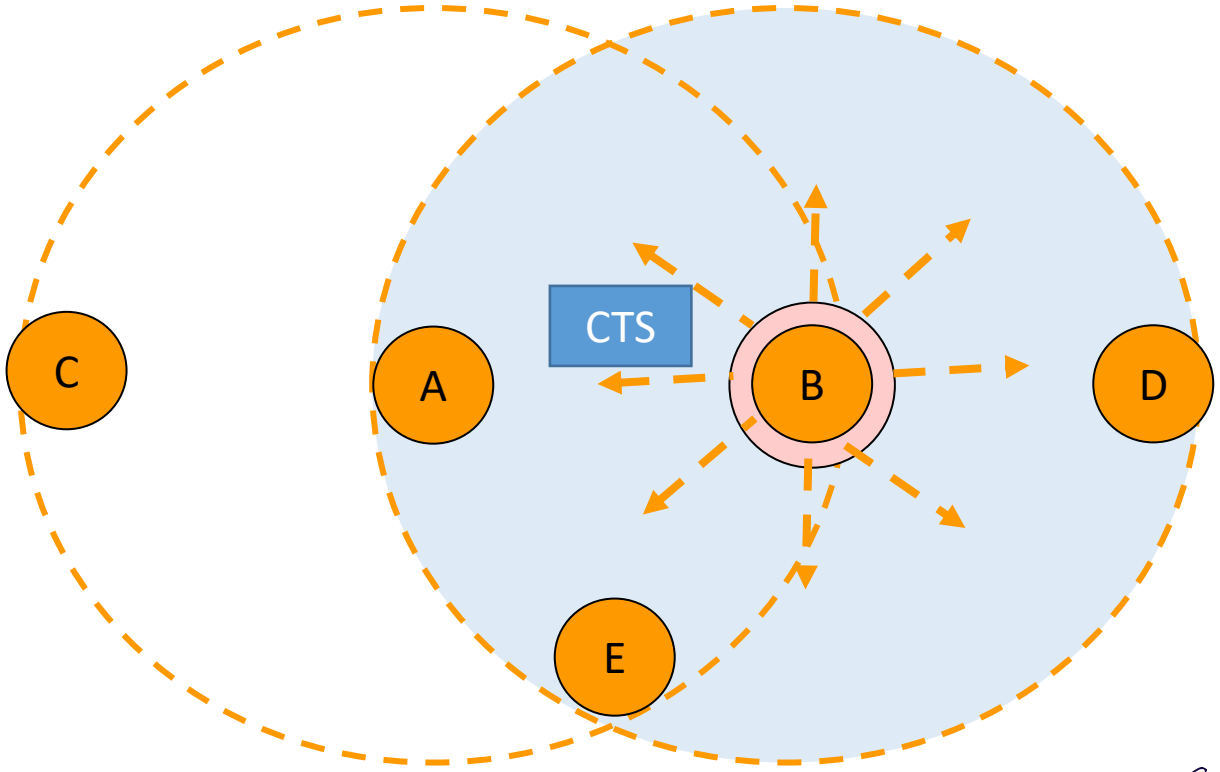
The MACA protocol (5)



1. A wants to transmit to B, sends a **RTS** to B
2. If B wants to receive the message, it replies with a **Clear To Send**

   CTS is a short frame with data length copied from RTS

The MACA protocol (6)

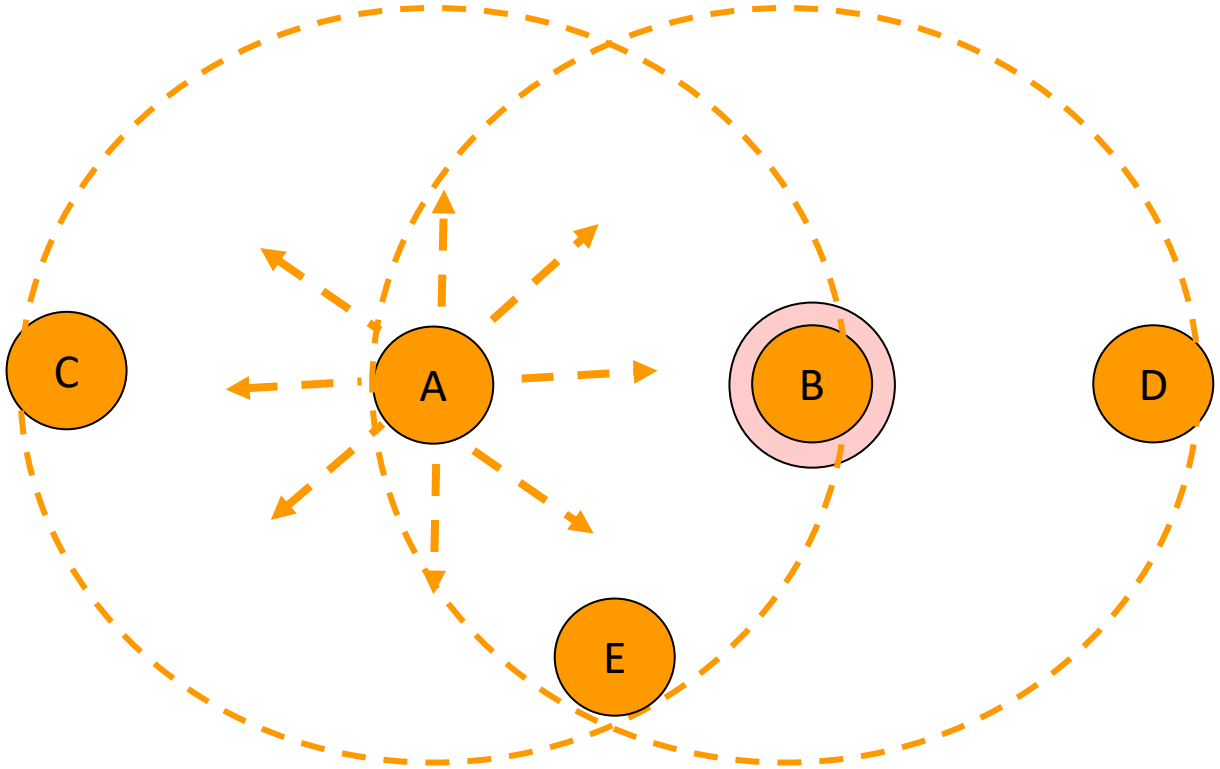


1. A wants to transmit to B, sends a **RTS** to B
2. If B wants to receive the message replies with a **CTS**

   CTS received by A, D, E

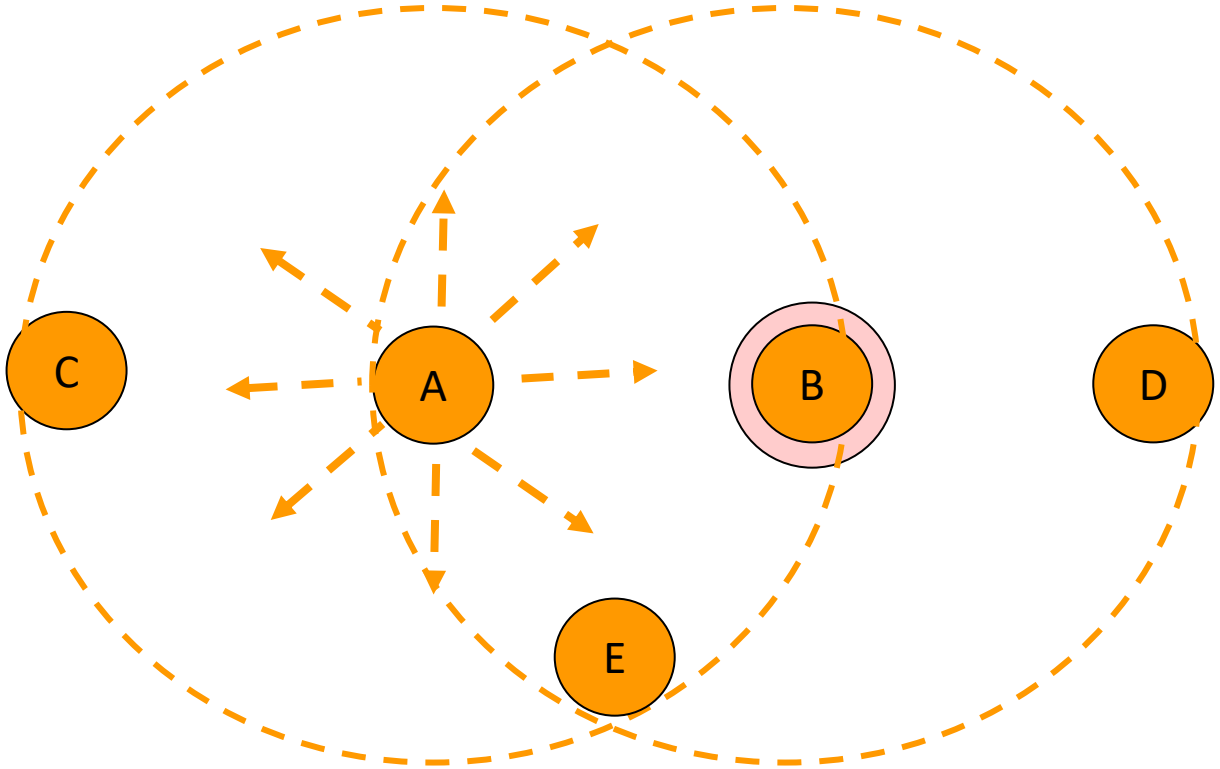
CTS received by A D E

The MACA protocol (7)



1. A wants to transmit to B, sends a **RTS** to B
2. If B wants to receive the message replies with a **CTS**
3. Upon reception of the CTS frame, A transmits the data frame

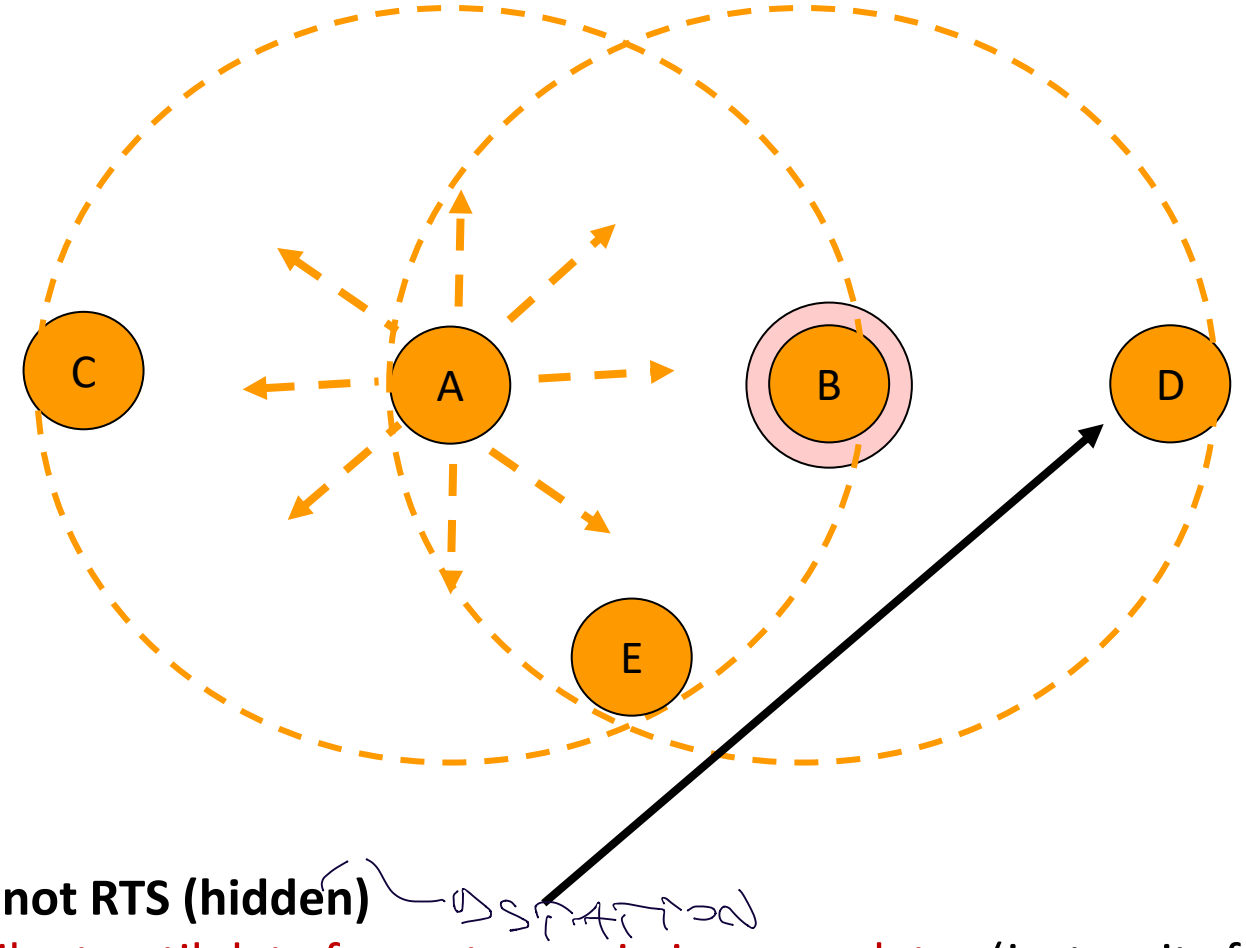
The MACA protocol (8)



C hears RTS, but not CTS (exposed)

it is free to transmit

The MACA protocol (9)

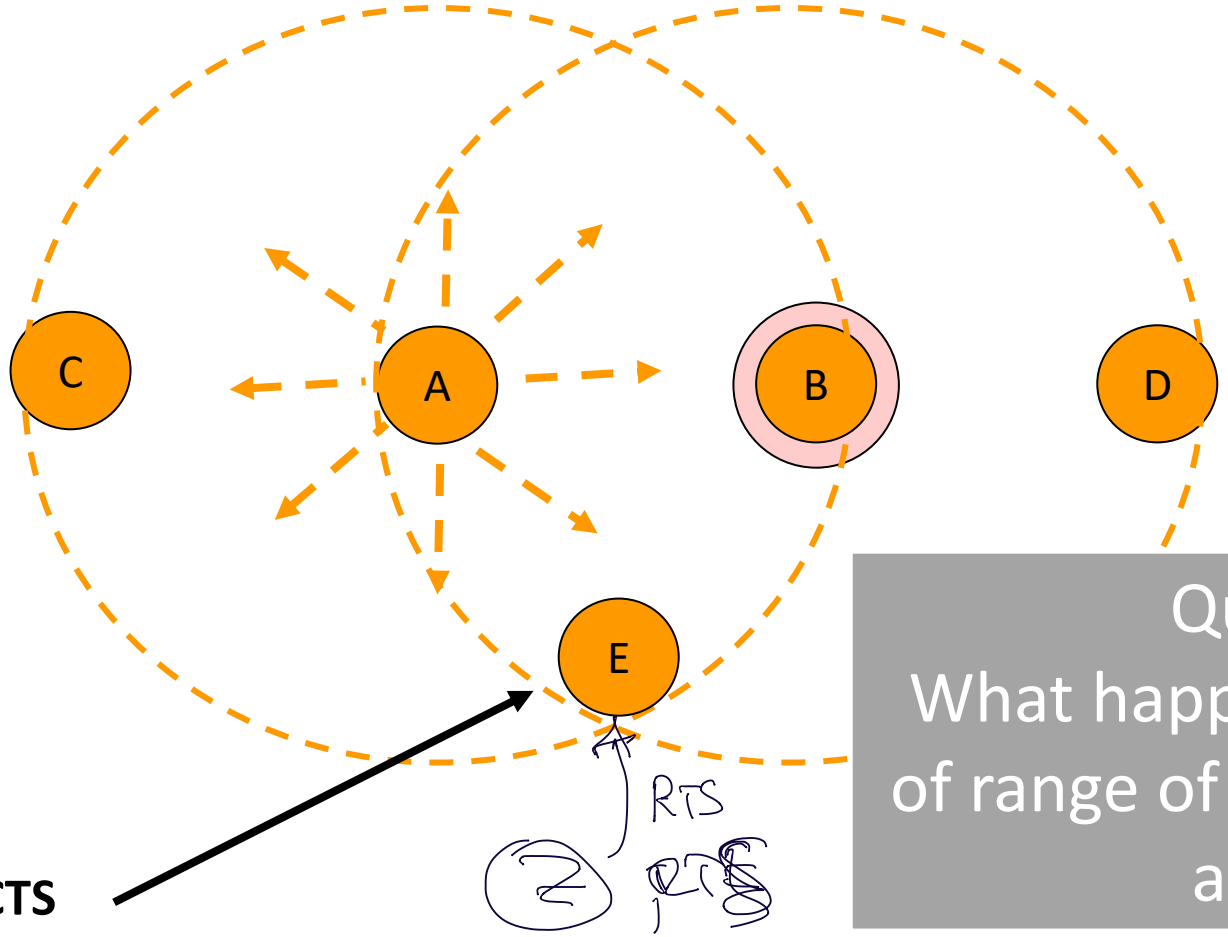


D hears CTS, but not RTS (hidden)

it should stay silent until data frame transmission completes (just waits for the required time)

The MACA protocol (10)

E not able to recognise CTS MACA



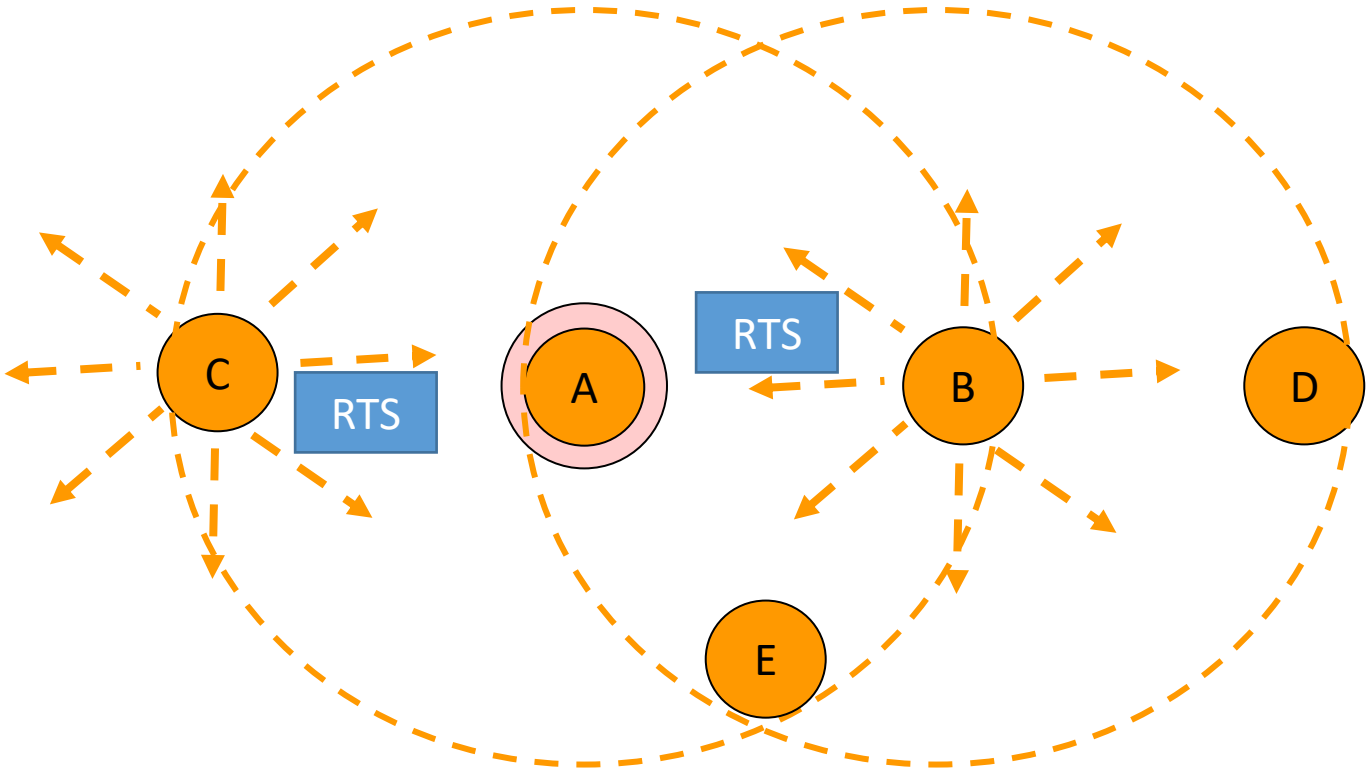
E hears RTS and CTS

it should stay silent until data frame transmission completes

Question for you:
What happens if another node out of range of A and B wish to transmit a message to E?

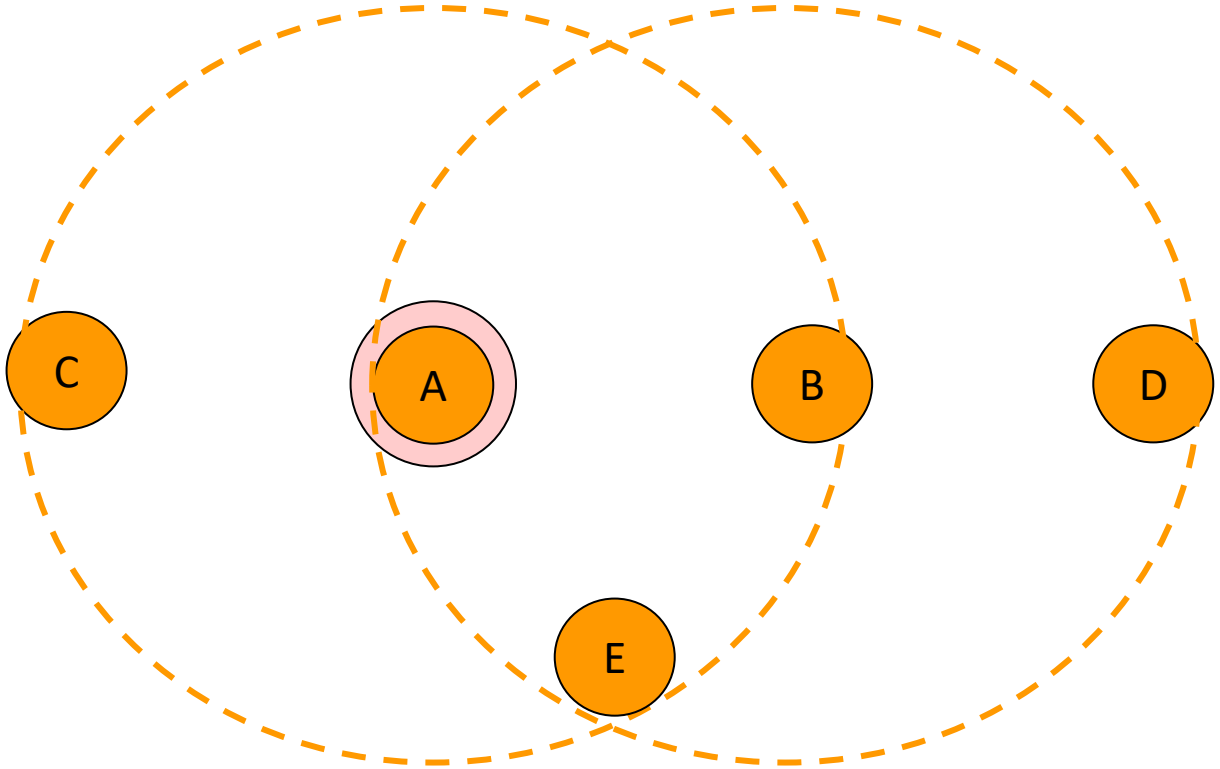
E) channel is already busy

The MACA protocol: collisions



C and B send RTS simultaneously to A

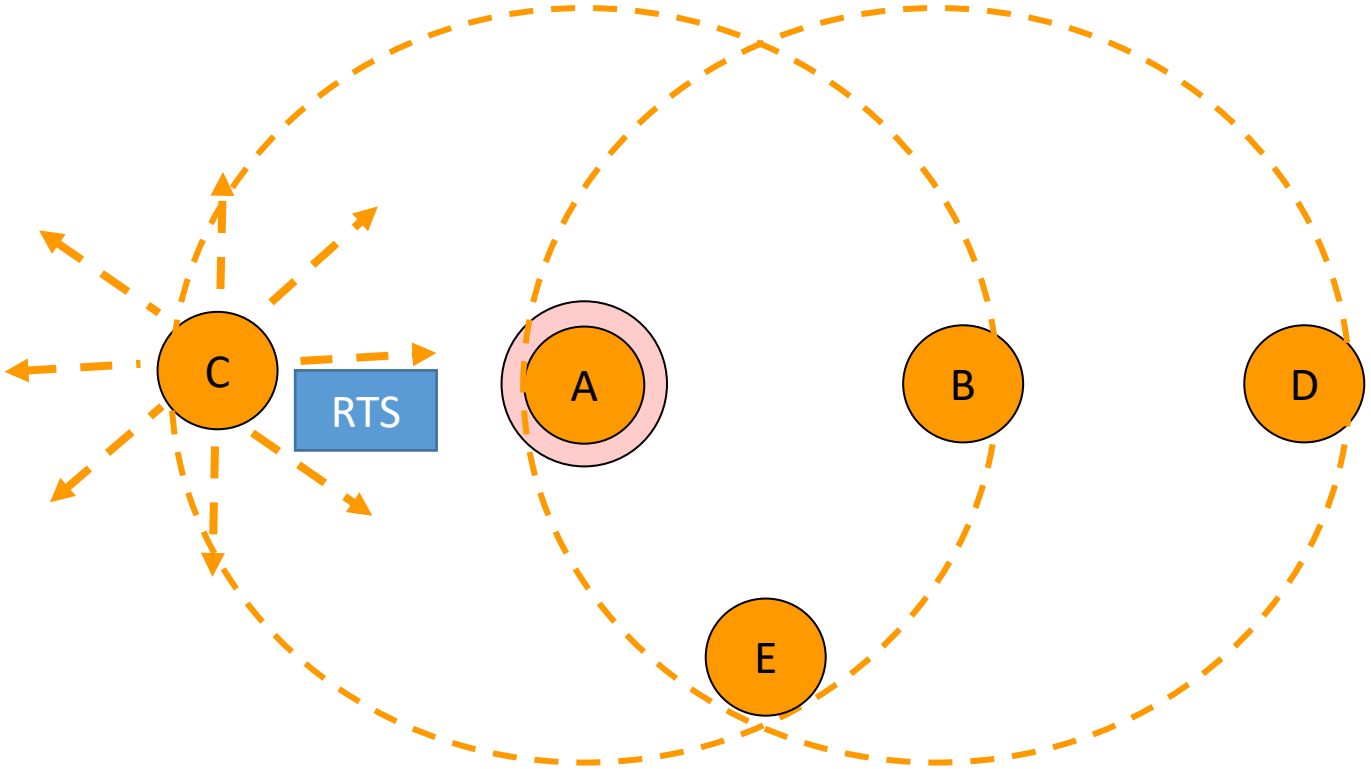
The MACA protocol: collisions (2)



C and B send RTS simultaneously to A

The two messages collide: No CTS is generated

The MACA protocol: collisions (3)



C and B use *Binary Exponential Backoff* (same as Ethernet) to retry RTS

MACAW: MACA for Wireless networks

receiving send RTS

Fine tunes MACA to improve performance:

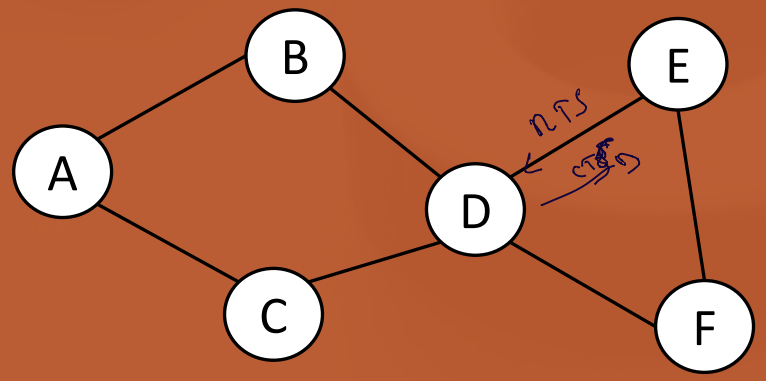
- introduces an ***ACK frame*** to acknowledge a successful data frame
- added ***Carrier Sensing*** to keep a station from transmitting RTS when a nearby station is also transmitting an RTS to the same destination
- exponential backoff is run for each separate pair source/destination and not for the single station
- mechanisms to exchange information among stations and recognize temporary congestion problems
- CSMA/CA used in IEEE 802.11 is based on MACAW

Question

Given the network in the figure, assume that the MAC protocol uses the RTS/CTS mechanism for the channel access.

Discuss which nodes detect themselves as hidden or exposed as consequence of the RTS/CTS handshake in the following cases:

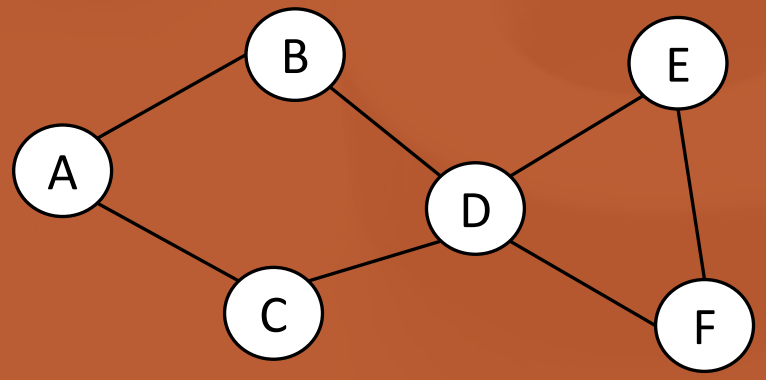
1. Hidden terminals with respect to a transmission from E to D
2. Hidden terminals with respect to a transmission from D to C
3. Exposed terminals with respect to a transmission from D to B
4. Exposed terminals with respect to a transmission from B to A

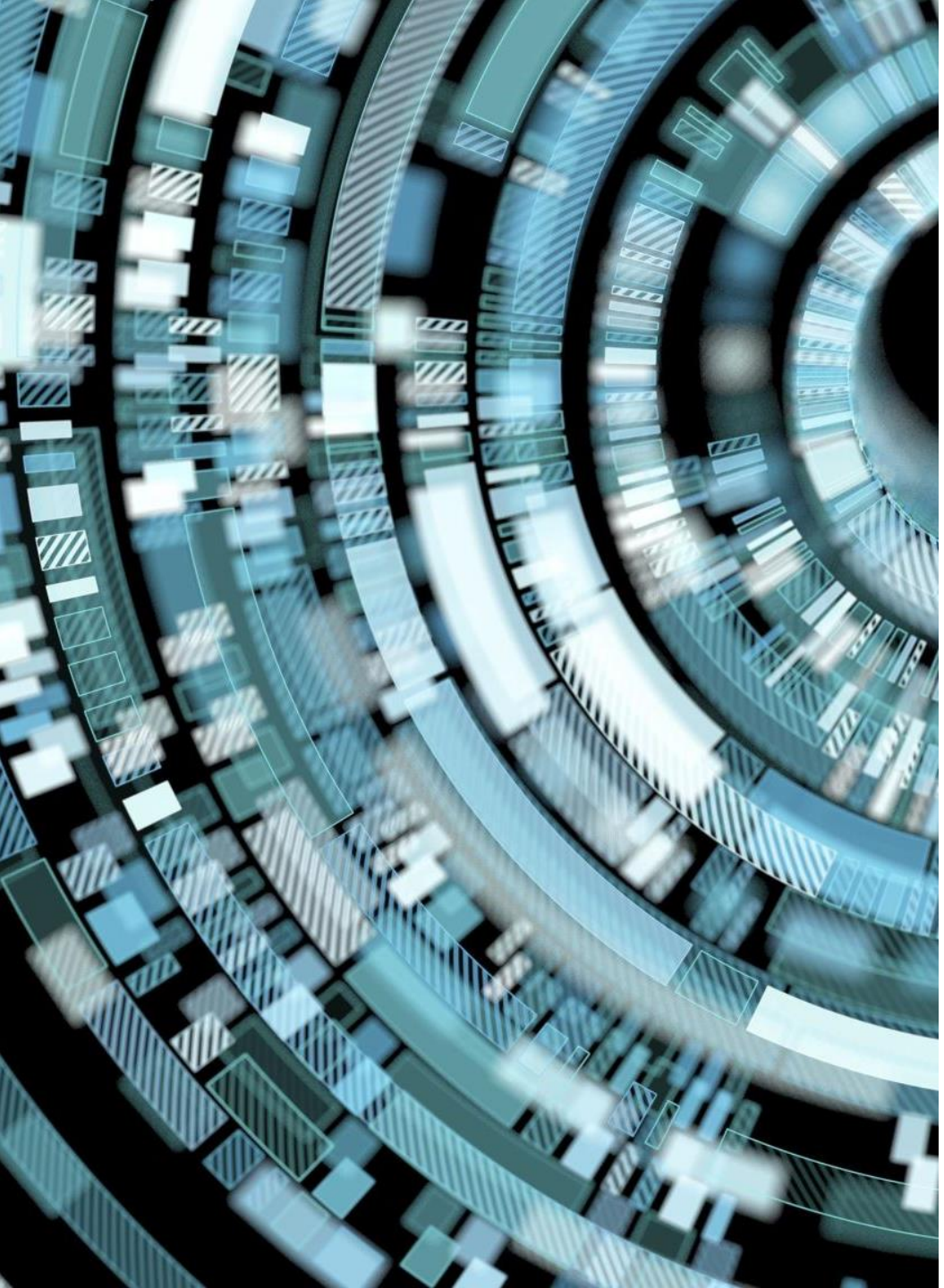


Question

Given the network in the figure:

1. assume that D hears the RTS sent by E but it does not hear the corresponding CTS. What does D can do?
2. assume that B hears the CTS sent by D but it does not hear the corresponding RTS. What does B can do?
3. Assume D is receiving a communication from a node, and B did not receive the corresponding RTS & CTS and it does not hear the signal transmitted to D. If B wishes to transmit to D what happens?





VRiMAB

Giovedì
ore 12-13

Prof Merz
2-3

IEEE 802.11

STD 4 wireless

The IEEE 802.11 family

- IEEE 802.11 (Legacy mode)
  - First released in 1997 and clarified in 1999
  - rarely used today
  - 1-2 Mbps data rate implemented via:
    - infrared (IR) signals,
    - radio frequencies in the 2.4GHz band (ISM -- Industrial Scientific Medical Frequency band)
  - many degrees of freedom: interoperability among different products was a challenge
  - rapidly supplemented (and made popular) by 802.11b
  - most used today 802.11a/b/g/n

IEEE 802.11 family (2)

- IEEE 802.11a
  - Released in 1999
  - Operating frequency: 5 GHz band (Unlicensed National Information Infrastructure U-NII band)
  - Throughput (typ): 23 Mbps
  - Data rate (max): 54 Mbps
- IEEE 802.11b
  - Released in 1999
  - Operating frequency: 2.4GHz band (ISM band)
    - potential interference with other appliances : cordless telephones, microwave ovens etc
  - Throughput (typ): 4.3 Mbps
  - Data rate (max): 11 Mbps

IEEE 802.11 family (3)

- IEEE 802.11g
  - Released in 2003
  - Operating frequency: 2.4GHz band (ISM band)
  - Throughput (typ): 19 Mbps and more…
  - Data rate (max): 54 Mbps
- IEEE 802.11n
  - Released in 2009
  - Operating frequency: 2.4GHz band and 5GHz band
  - Throughput (typ): 74 Mbps
  - Data rate (max): 248 Mbps
  - Support of MIMO technologies for using multiple antennas at the transmitter and the receiver

IEEE 802.11 family (4)

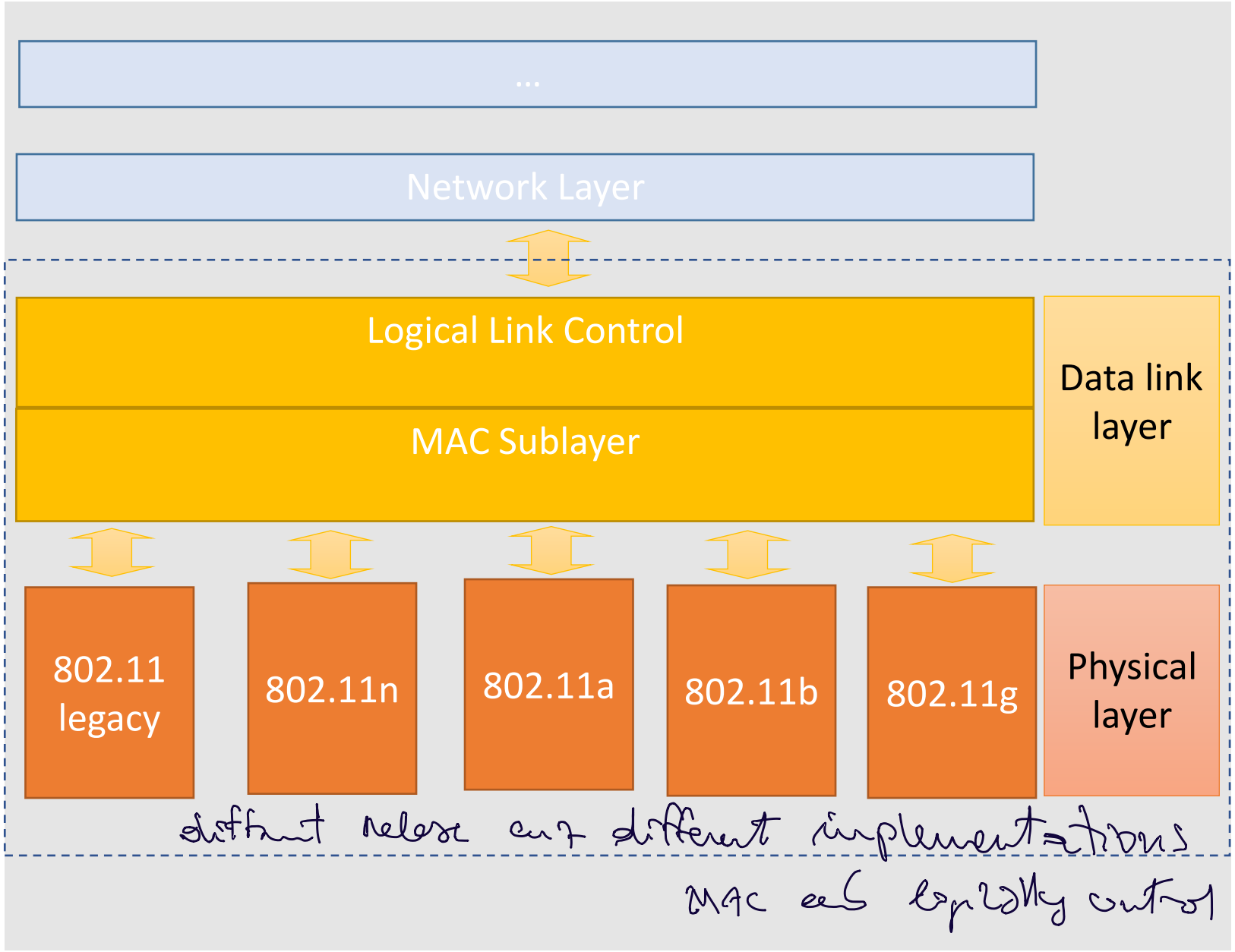
- Now available newer versions:
- WiFi 5 - IEEE 802.11ac
  - Released in 2013
  - Operating frequency: 2.4GHz and 5 GHz bands
  - Data rate (max): 1.3 Gbps at 5 GHz
  - Data rate (max): 450 Mbps at 2.4 GHz
- WiFi 6 - IEEE 802.11ax
  - Released in 2019
  - reaches up to 10 Gbps
  - improvements in power consumption and security

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

IEEE 802.11: protocol stack



IEEE 802.11 Architecture

- A group of stations operating under a given coordination function
  - may (or may not) use a base station (Access Point - AP)
  - if using AP a station communicates with another by channeling all the traffic through a centralized AP
  - AP can provide connectivity with other APs and other groups of stations via fixed infrastructure

IEEE 802.11 Architecture

- Supports ad hoc networks, which are, in the IEEE 802.11 view :

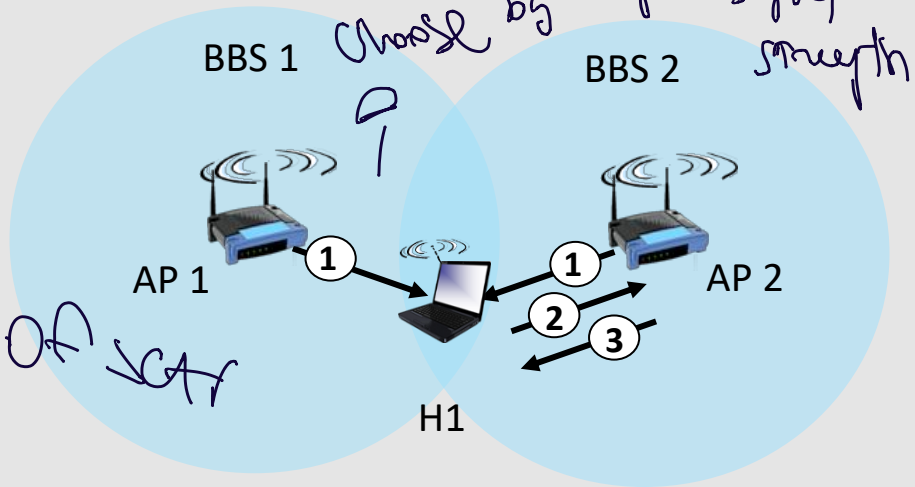
a group of stations that are under the direct control of a single coordination function without the aid of an infrastructure network

- a station can communicate directly with another without channeling all the traffic through AP

IEEE 802.11 Channels, association

- 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!
- arriving host: must associate with an AP
  - scans channels, listening for *beacon frames* containing network's name (SSID) and MAC address of the AP (BSSID)
  - selects AP to associate with
  - then may perform authentication
  - then typically run DHCP to get IP address in AP's subnet

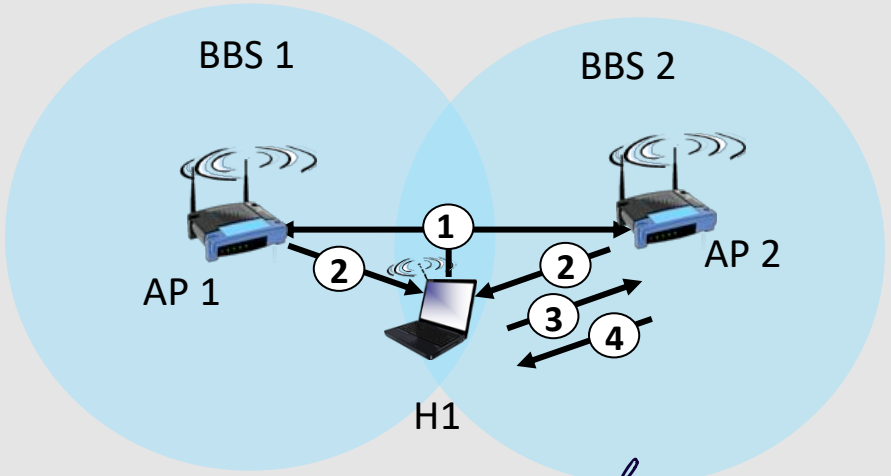
IEEE 802.11 passive/active scanning



passive scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

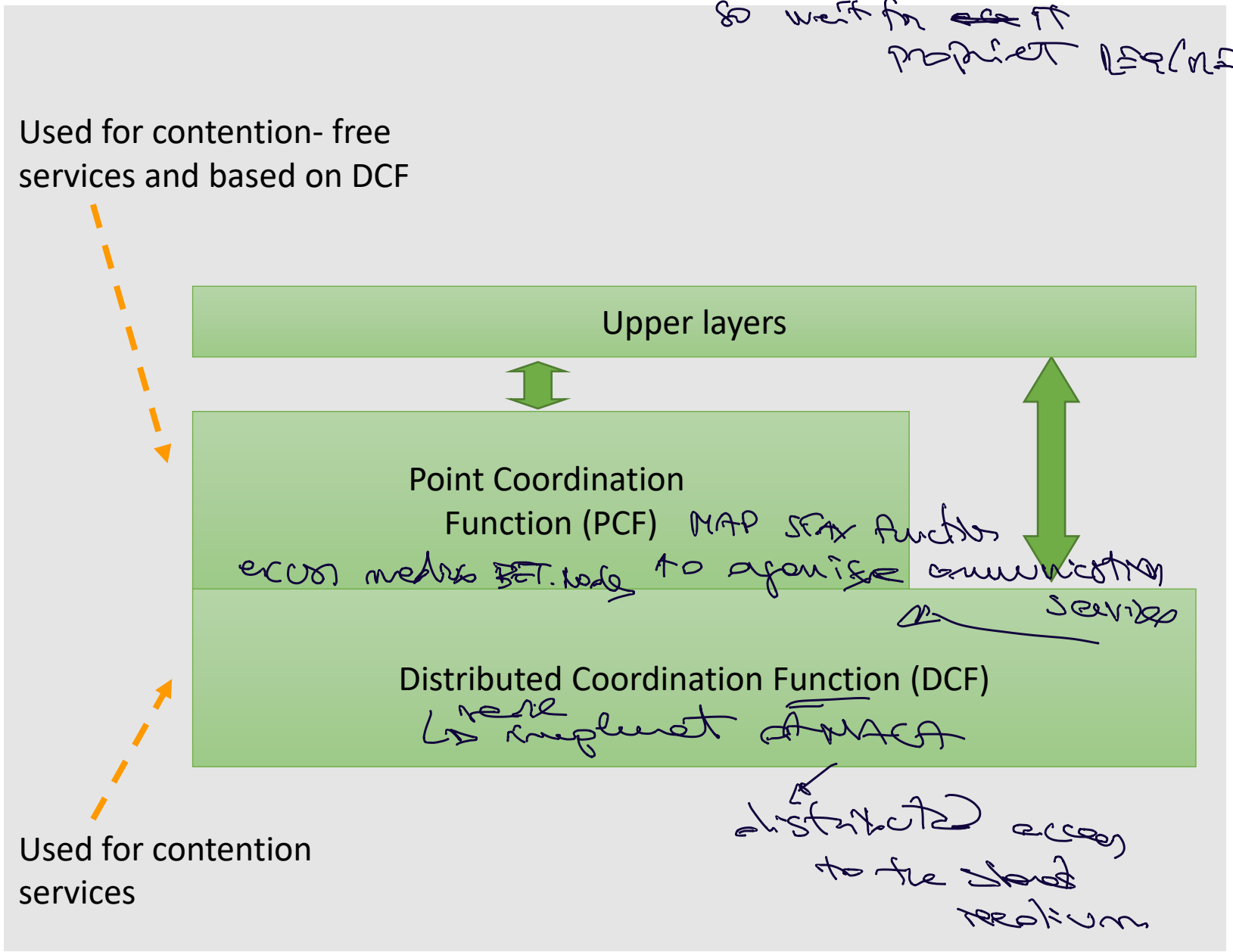
IEEE 802.11 passive/active scanning



active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

IEEE 802.11 Architecture: MAC Sublayer



IEEE 802.11 Architecture: MAC Sublayer

Two modes of operations:

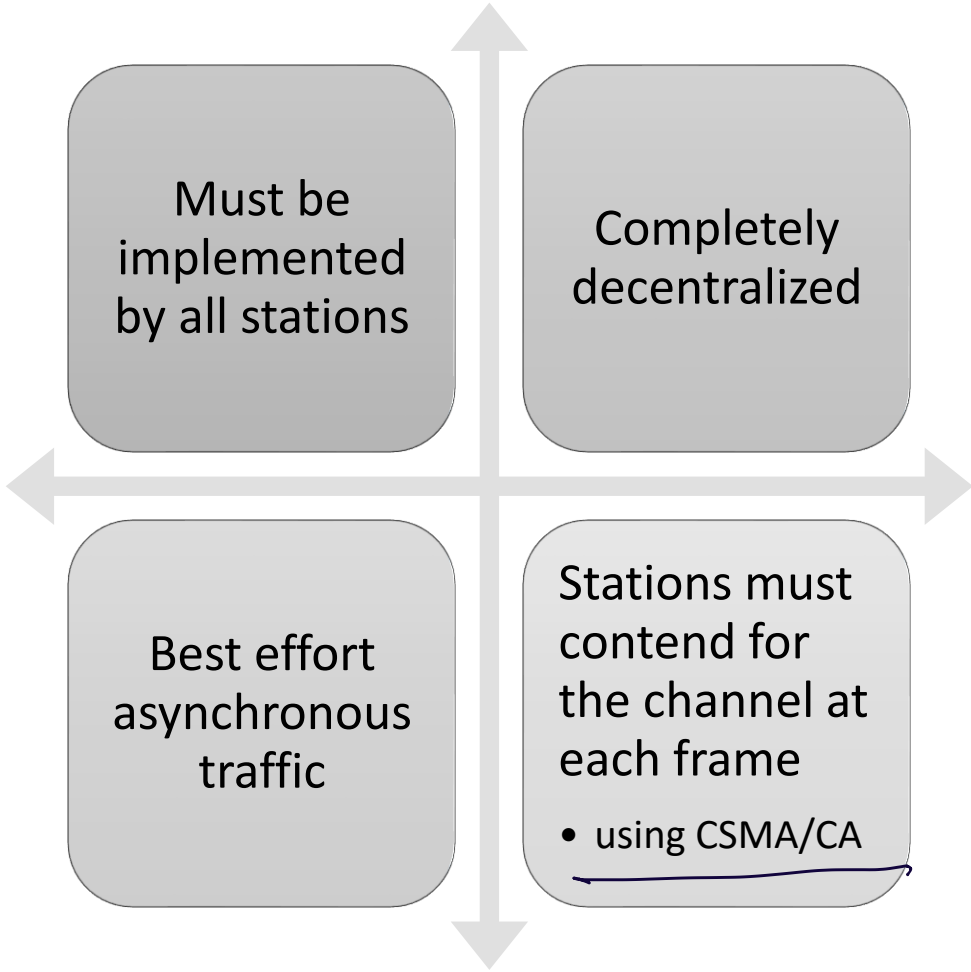
- DCF : Distributed Coordination Function
  - completely decentralized
  - thought for best effort asynchronous traffic
- PCF : Point Coordination Function
  - uses base station to control all activity in its cell
  - thought for delay-sensitive traffic
  - AP polls stations for transmissions
  - based on DCF

DCF **must** be implemented by all stations

DCF and PCF can be active at the same time in the same cell

IEEE 802.11:

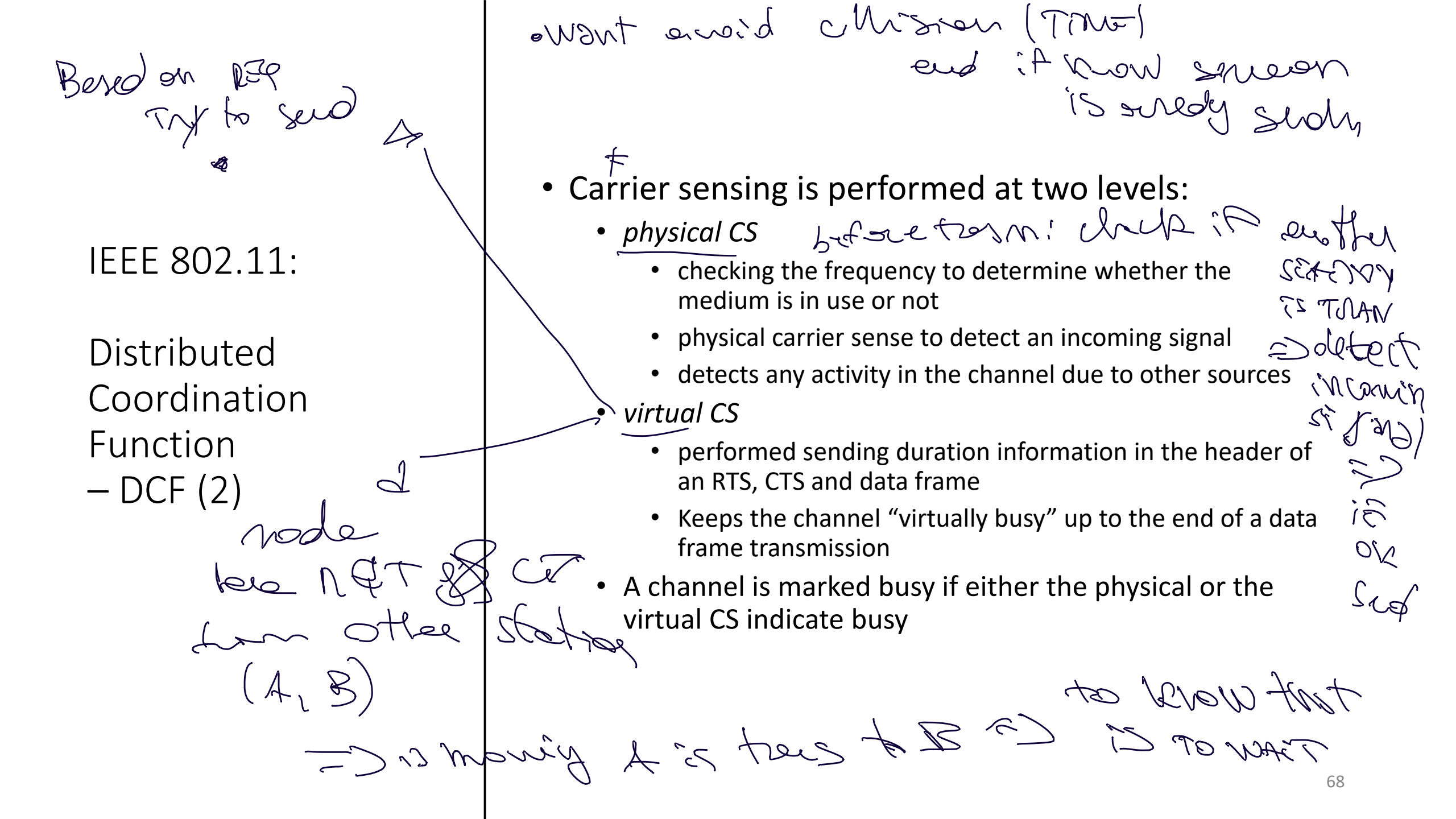
Distributed Coordination Function – DCF (1)



IEEE 802.11:

Distributed Coordination Function – DCF (2)

- Carrier sensing is performed at two levels:
  - *physical CS*
    - checking the frequency to determine whether the medium is in use or not
    - physical carrier sense to detect an incoming signal
    - detects any activity in the channel due to other sources
  - *virtual CS*
    - performed sending duration information in the header of an RTS, CTS and data frame
    - Keeps the channel "virtually busy" up to the end of a data frame transmission
- A channel is marked busy if either the physical or the virtual CS indicate busy



IEEE 802.11:

Distributed Coordination Function – DCF (3)

- Priority access to the medium is controlled through the use of interframe space (IFS) time intervals
  - IFS: mandatory periods of idle time on the transmission medium
- Three IFS specified by the standard:
  - short IFS (SIFS)
  - point coordination function IFS (PIFS)
  - Distributed coordination function IFS (DIFS)
  - SIFS < PIFS < DIFS
  - stations only required to wait a SIFS have the highest priority

Summary

INFRASTRUCTURED AND INFRASTRUCTURE-LESS WIRELESS NETWORKS

PROPERTIES OF WIRELESS CHANNELS

HIDDEN AND EXPOSED TERMINALS

MACA PROTOCOL

IEEE 802.11