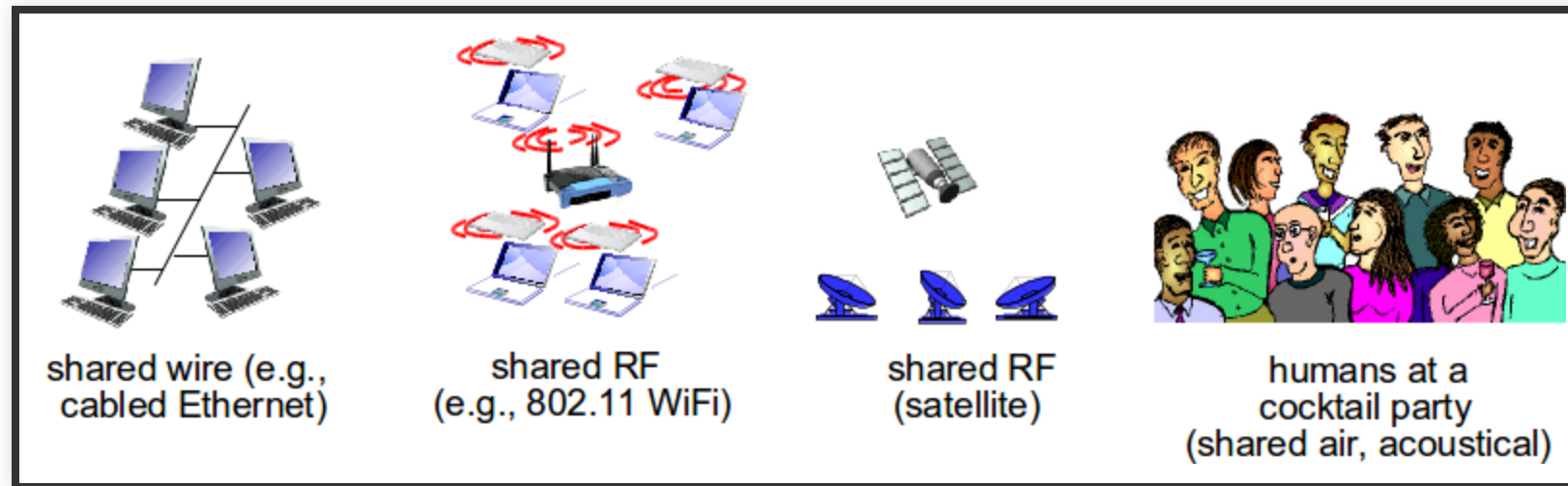


MULTIPLE ACCESS PROTOCOLS AND WIFI

MULTIPLE ACCESS PROTOCOLS

MULTIPLE ACCESS LINKS, PROTOCOLS



Two types of “links”:

- **point-to-point**
- **broadcast** (shared wire or medium)

POINT-TO-POINT

- PPP for dial-up access
- point-to-point link between Ethernet switch, host

BROADCAST

- shared wire or medium
 - Old-fashioned Ethernet
 - Cable Access Network
 - 802.11 wireless LAN

MULTIPLE ACCESS PROTOCOLS

- Single shared broadcast channel
- Two or more simultaneous transmissions by nodes: interference
 - Collision if node receives two or more signals at the same time

MULTIPLE ACCESS PROTOCOLS

- ❗ Definition: Multiple access protocol
 - Distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit
 - Communication about channel sharing must use channel itself!
 - no out-of-band channel for coordination

AN IDEAL MULTIPLE ACCESS PROTOCOL

Given: broadcast channel of rate R bps

Desiderata:

- When one node wants to transmit, it can send at rate R .
- When M nodes want to transmit, each can send at average rate R/M
- Fully decentralized:
 - No special node to coordinate transmissions
 - No synchronization of clocks, slots
- Simple

TAXONOMY: THREE BROAD CLASSES

Channel partitioning

- divide channel into smaller “pieces” (time slots, frequency, code)
- allocate piece to node for exclusive use

Random access

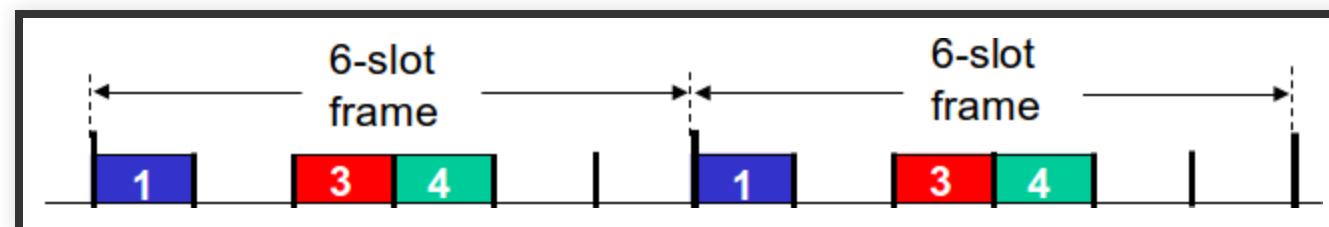
- channel not divided, allow collisions
- “recover” from collisions

“Taking turns”

CHANNEL PARTITIONING MAC PROTOCOLS: TDMA

TDMA: time division multiple access

- access to channel in "rounds"
- each station gets fixed length slot (length = pkt trans time) in each round
- unused slots go idle
- example: 6-station LAN, 1,3,4 have pkt, slots 2,5,6 idle



CHANNEL PARTITIONING MAC PROTOCOLS: FDMA

FDMA: frequency division multiple access

- channel spectrum divided into frequency bands
- each station assigned fixed frequency band
- unused transmission time in frequency bands go idle
- example: 6-station LAN, 1,3,4 have pkt, frequency bands 2,5,6 idle

RANDOM ACCESS PROTOCOLS

- when node has packet to send
 - transmit at full channel data rate R .
 - no a priori coordination among nodes
- two or more transmitting nodes → “collision”,
- **random access MAC protocol** specifies:
 - how to detect collisions
 - how to recover from collisions (e.g., via delayed retransmissions)

RANDOM ACCESS PROTOCOLS

- Examples of random access MAC protocols:
 - slotted ALOHA
 - ALOHA
 - Carrier Sense Multiple Access (CSMA)
 - CSMA/CD (Collision Detection)
 - CSMA/CA (Collision Avoidance)

SLOTTED ALOHA

Assumptions:

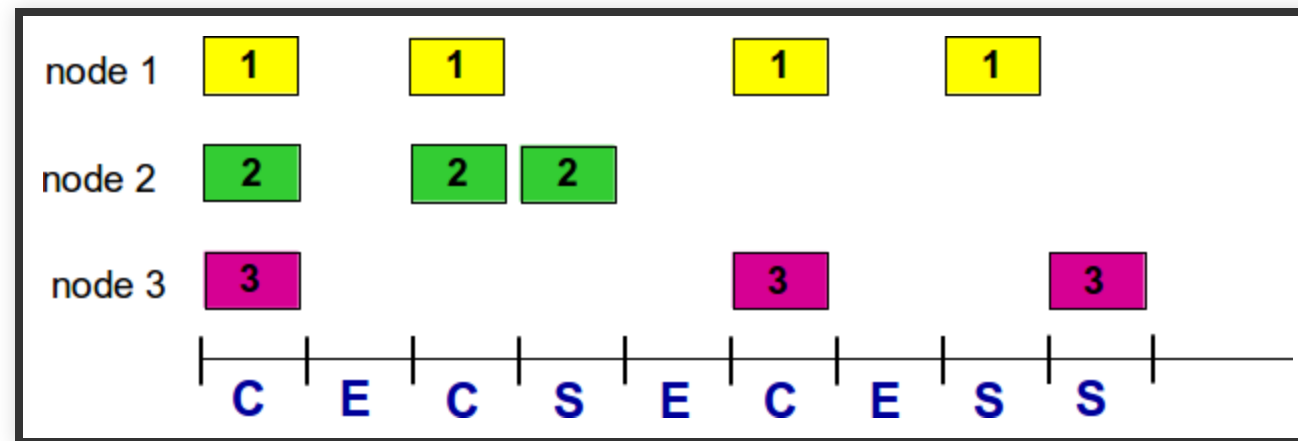
- all frames same size
- time divided into equal size slots (time to transmit 1 frame)
- nodes start to transmit only slot beginning
- nodes are synchronized
- if 2 or more nodes transmit in slot, all nodes detect collision

SLOTTED ALOHA

operation:

- when node obtains fresh frame, transmits in next slot
 - if no collision: node can send new frame in next slot
 - if collision: node retransmits frame in each subsequent slot with prob. p until success

SLOTTED ALOHA



SLOTTED ALOHA - PROS

- single active node can continuously transmit at full rate of channel
- highly decentralized: only slots in nodes need to be in sync
- simple

SLOTTED ALOHA - CONS

- collisions, wasting slots
- idle slots
- nodes may be able to detect collision in less than time to transmit packet
- clock synchronization

SLOTTED ALOHA: EFFICIENCY

- ❗ **Efficiency:** long-run fraction of successful slots (many nodes, all with many frames to send)

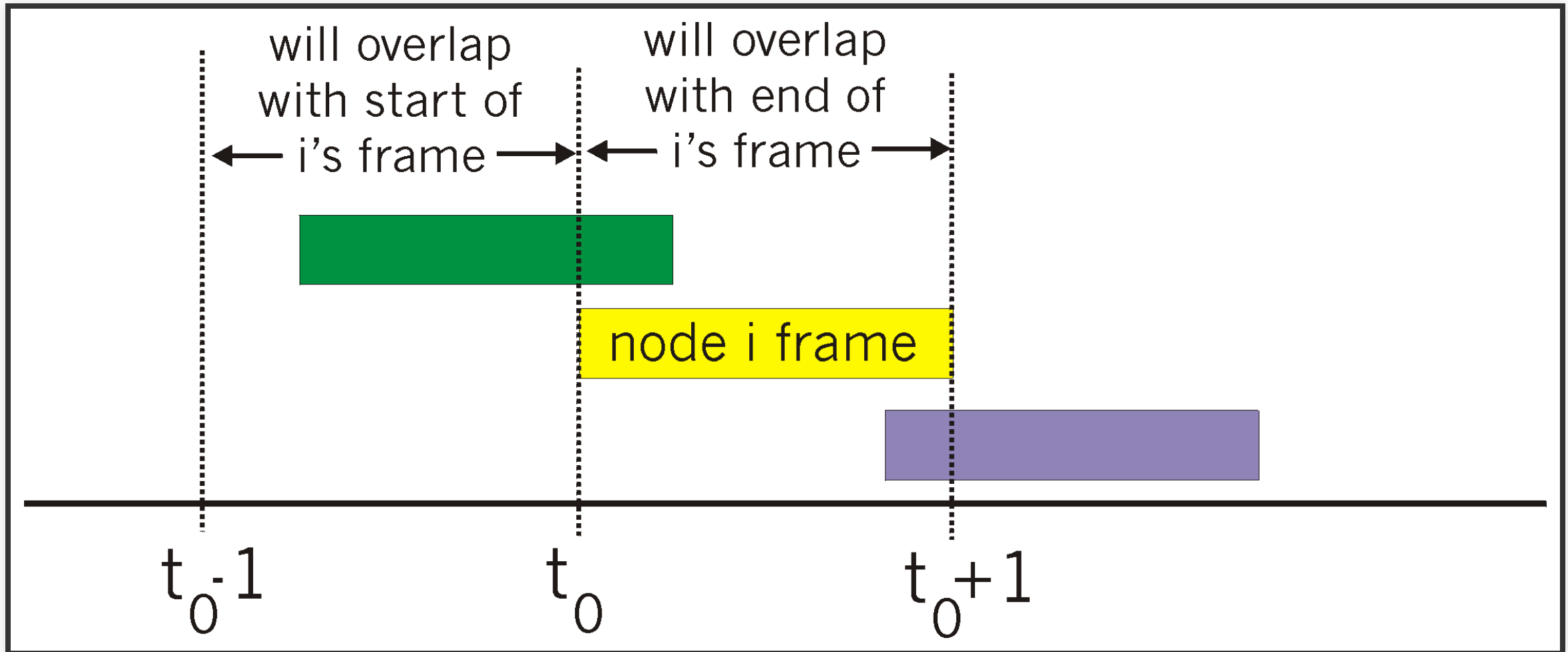
SLOTTED ALOHA: EFFICIENCY

- suppose: N nodes with many frames to send, each transmits in slot with probability p
- prob that given node has success in a slot = $p(1-p)^{N-1}$
- prob that any node has a success = $Np(1-p)^{N-1}$
- max efficiency: find p' that maximizes $Np'(1-p')^{N-1}$
- for many nodes, take limit of $Np'(1-p')^{N-1}$ as N goes to infinity, gives:
max efficiency = $1/e = 0.37$

SLOTTED ALOHA: EFFICIENCY

- ❗ At best: channel used for useful transmissions 37% of time!

PURE (UNSLOTTED) ALOHA



PURE (UNSLOTTED) ALOHA

- unslotted Aloha: simpler, no synchronization
- when frame first arrives
 - transmit immediately
- collision probability increases:
 - frame sent at t_0 collides with other frames sent in $[t_0-1, t_0+1]$

PURE ALOHA EFFICIENCY

$P(\text{success by given node}) =$

1. choosing optimum p and then letting $n \rightarrow \text{infinity}$

max efficiency = $1/2e$

even worse than slotted Aloha!

CSMA (CARRIER SENSE MULTIPLE ACCESS)

CSMA: listen before transmit:

- if channel sensed idle: transmit entire frame
- if channel sensed busy, defer transmission

human analogy: don't interrupt others!

CSMA COLLISIONS

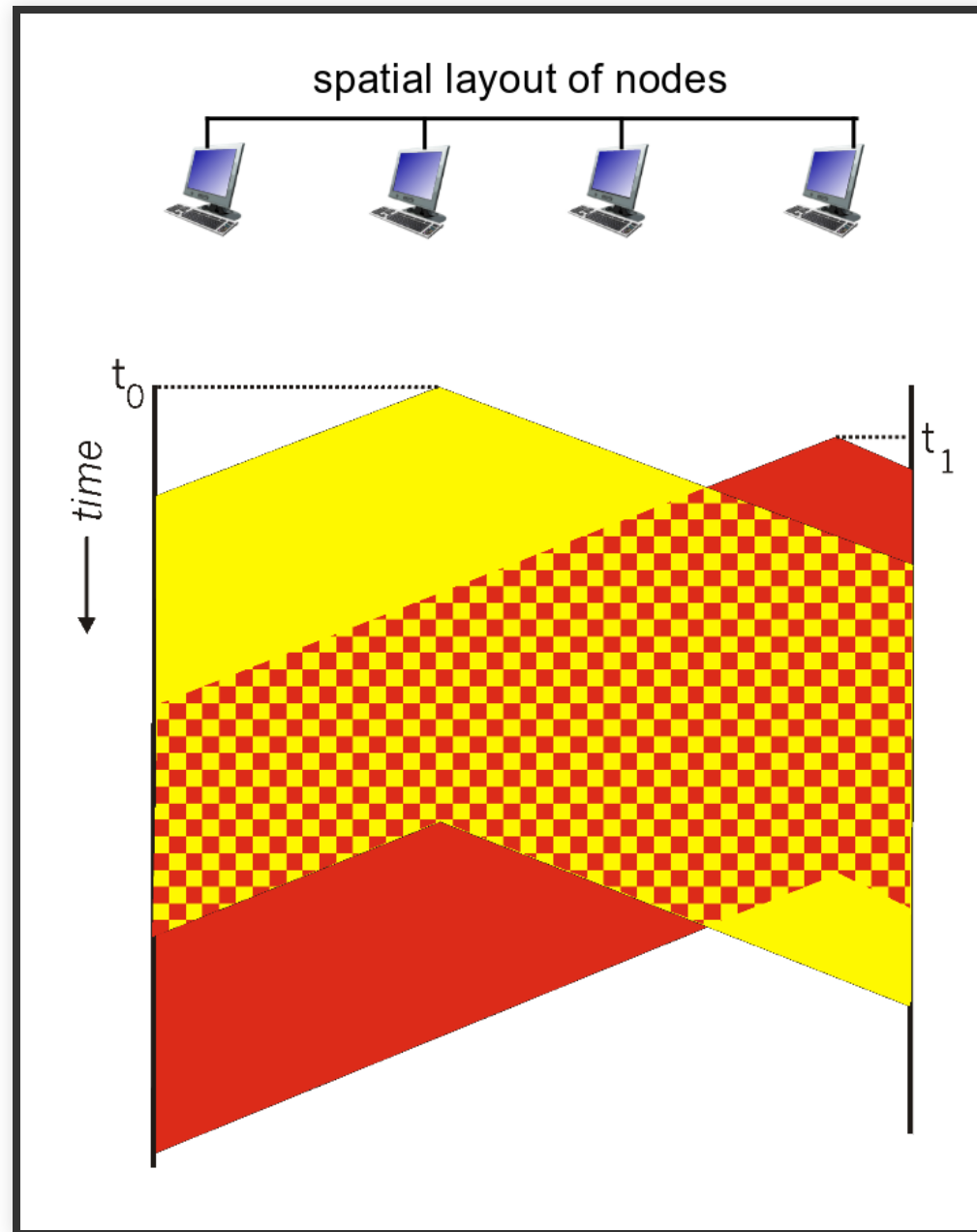
collisions can still occur:

- propagation delay means two nodes may not hear each other's transmission

collision:

- entire packet transmission time wasted
- distance and propagation delay play role in determining collision probability

CSMA COLLISIONS



CSMA/CD (COLLISION DETECTION)

CSMA/CD: carrier sensing, deferral as in CSMA

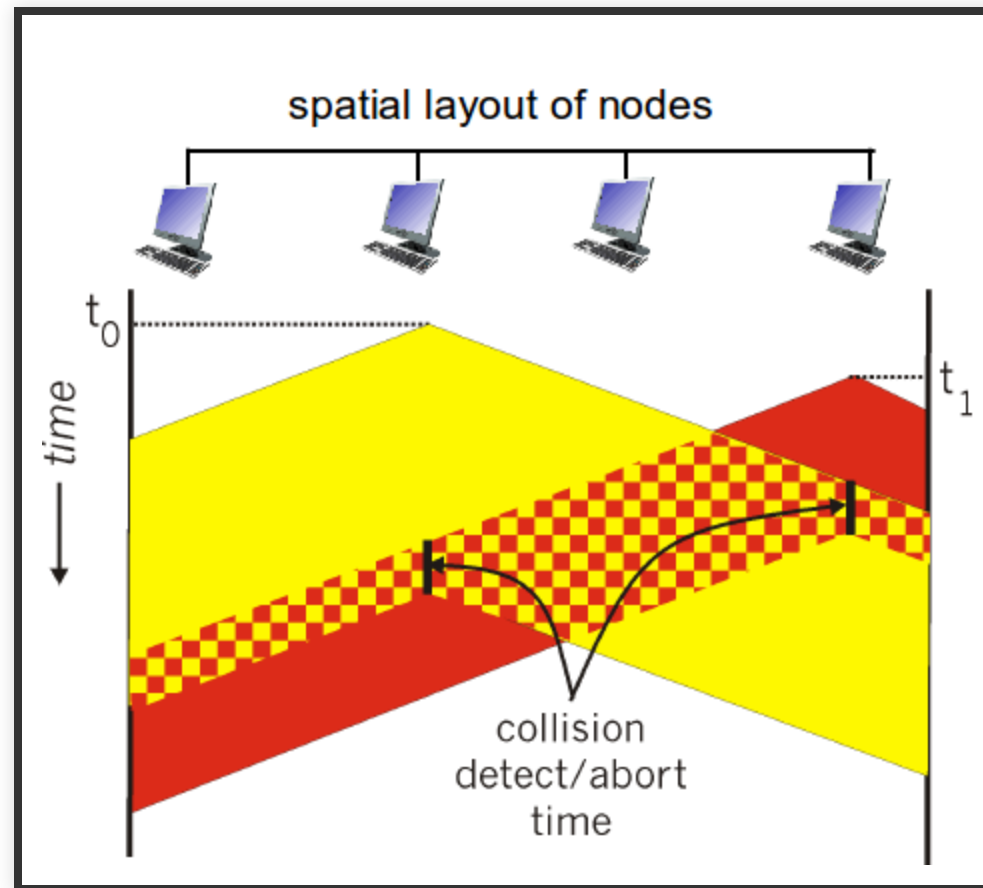
- collisions detected within short time
- colliding transmissions aborted, reducing channel wastage

collision detection:

- easy in wired LANs: measure signal strengths, compare transmitted, received signals
- difficult in wireless LANs: received signal strength overwhelmed by local transmission strength

Human analogy: the polite conversationalist

CSMA/CD (COLLISION DETECTION)



ETHERNET CSMA/CD ALGORITHM

- NIC receives datagram from network layer, creates frame
- If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
- If NIC transmits entire frame without detecting another transmission, NIC is done with frame!
- If NIC detects another transmission while transmitting it aborts, and sends a jam signal.
- After aborting, NIC enters **binary (exponential) backoff:**

EXPONENTIAL BACKOFF

- After m^{th} collision, NIC choose random K from $\{0,1,2, \dots, 2^m-1\}$.
NIC waits $K \cdot 512$ bit times, returns to sensing when channel is idle
 - Longer backoff interval with more collisions
- m capped at 10

CSMA/CD EFFICIENCY

"TAKING TURNS" MAC PROTOCOLS

channel partitioning MAC protocols:

- share channel efficiently and fairly at high load
- inefficient at low load: delay in channel access, $1/N$ bandwidth allocated even if only 1 active node!

random access MAC protocols

- efficient at low load: single node can fully utilize channel
- high load: collision overhead

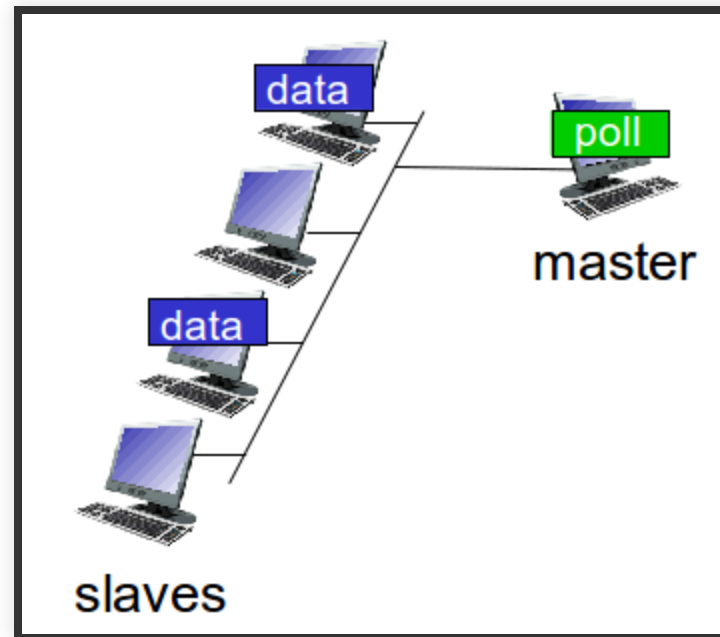
"taking turns" protocols: look for best of both worlds!

"TAKING TURNS" MAC PROTOCOLS

Polling:

- master node “invites” slave nodes to transmit in turn
- typically used with “dumb” slave devices
- concerns:
 - polling overhead
 - latency
 - single point of failure (master)

POLLING

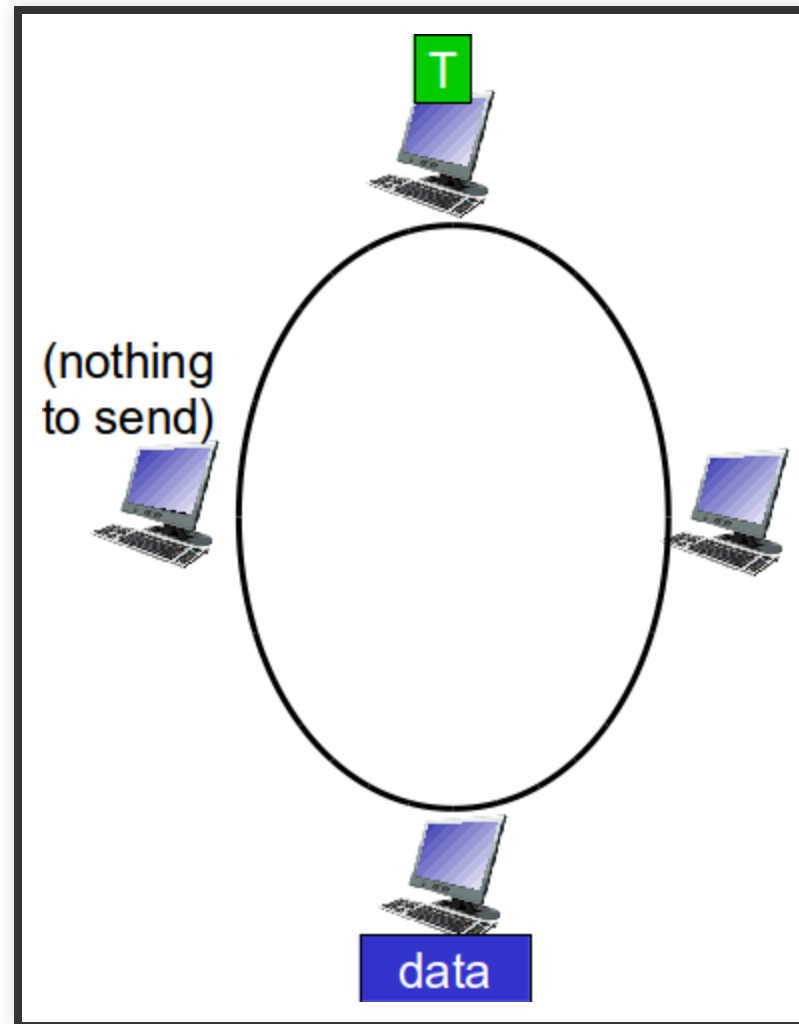


"TAKING TURNS" MAC PROTOCOLS

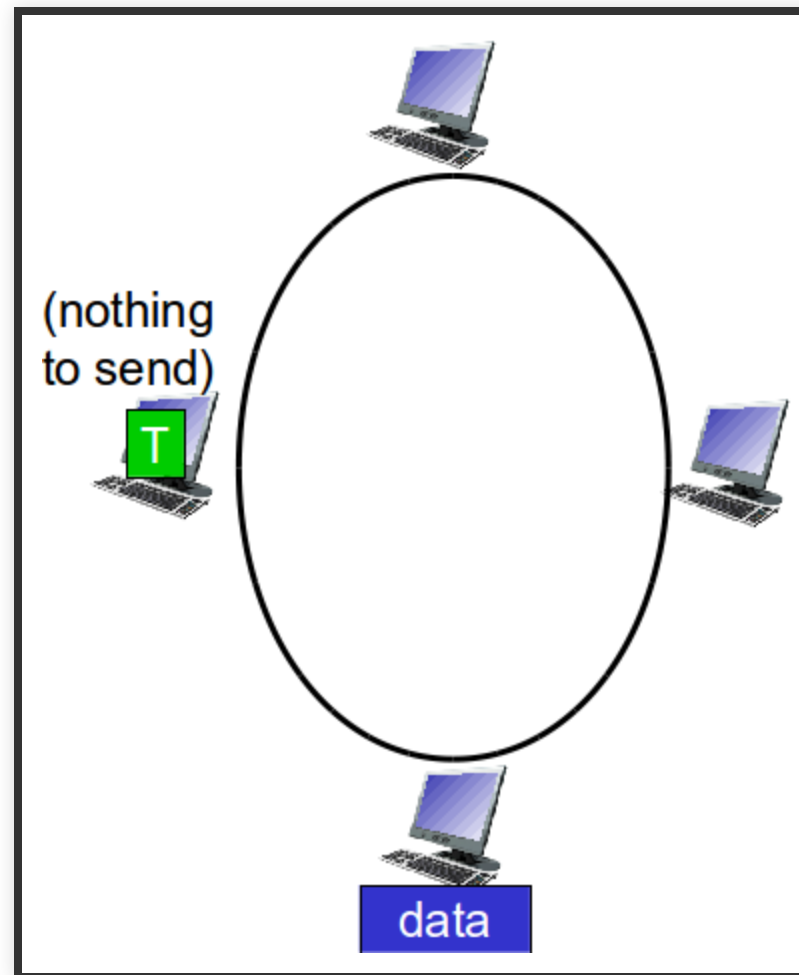
Token passing:

- control **token** passed from one node to next sequentially.
- token message
- concerns:
 - token overhead
 - latency
 - single point of failure (token)

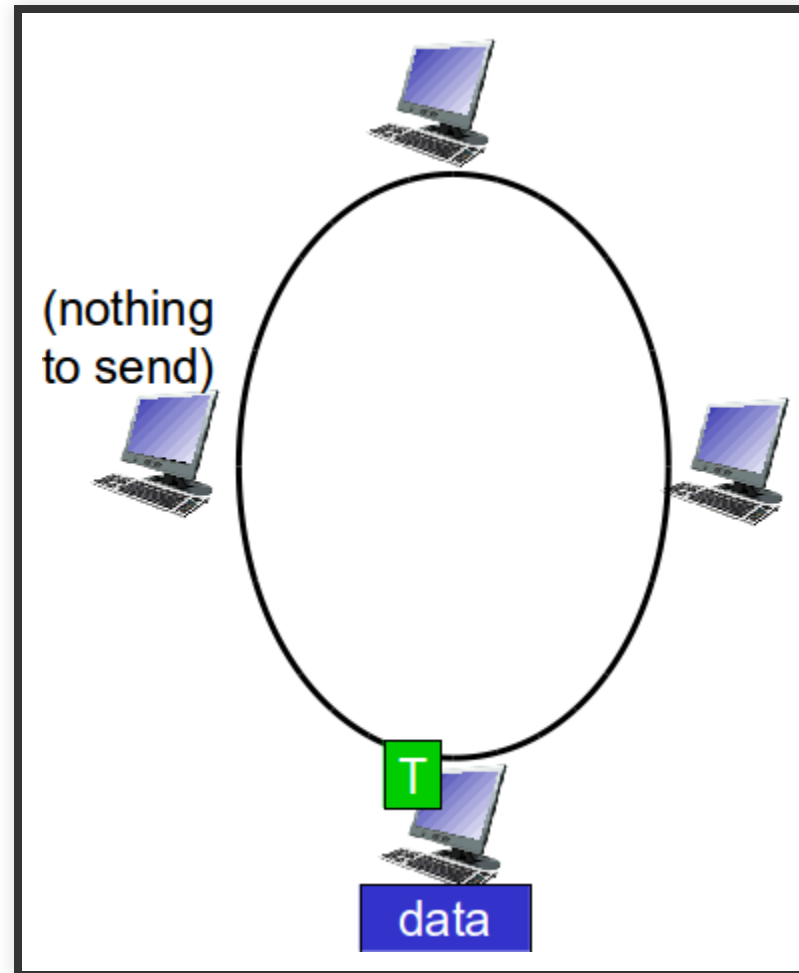
TOKEN PASSING



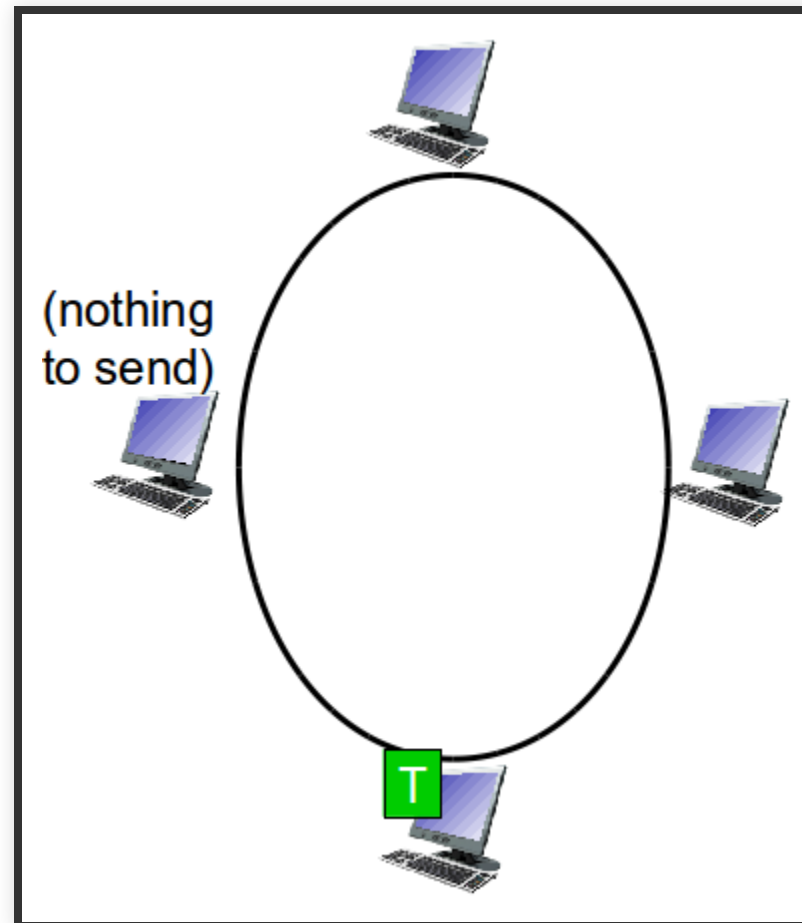
TOKEN PASSING



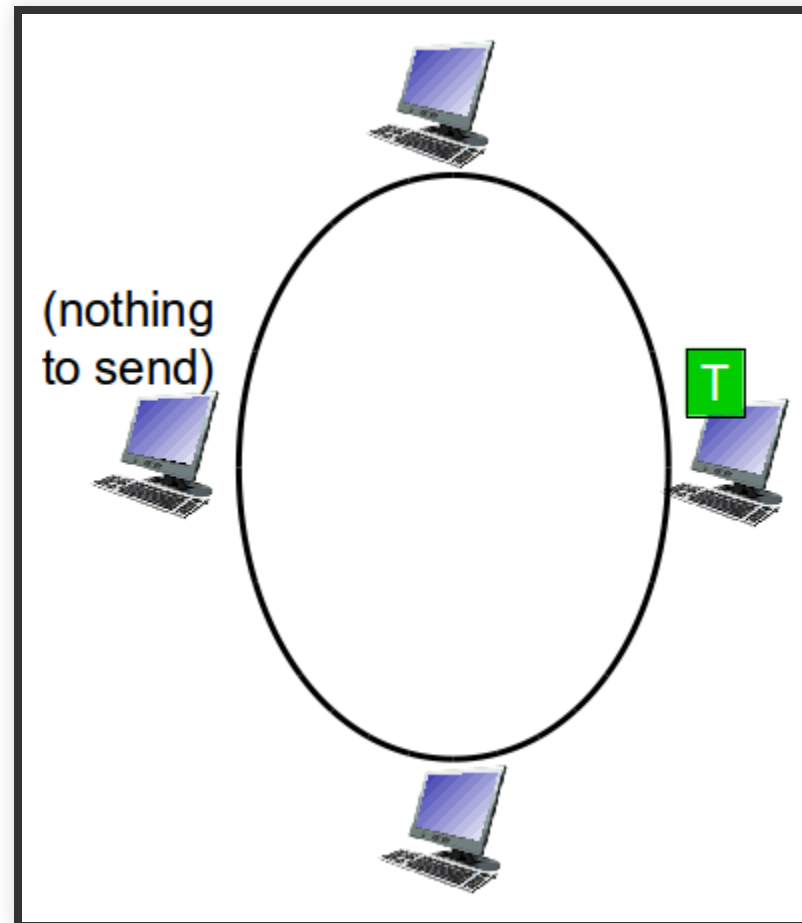
TOKEN PASSING



TOKEN PASSING



TOKEN PASSING



SUMMARY OF MAC PROTOCOLS

channel partitioning, by time, frequency or code

- Time Division, Frequency Division

SUMMARY OF MAC PROTOCOLS

random access (dynamic)

- ALOHA, S-ALOHA, CSMA, CSMA/CD
- carrier sensing: easy in some technologies (wire), hard in others (wireless)
- CSMA/CD used in Ethernet
- CSMA/CA used in 802.11

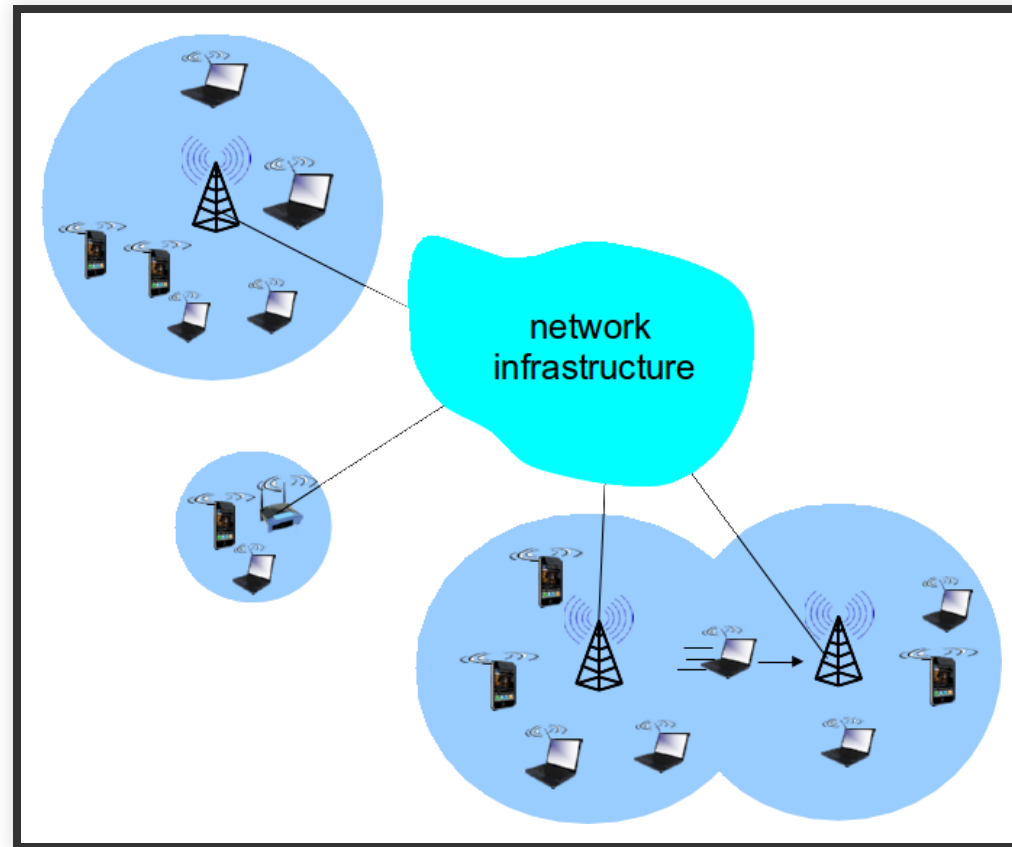
SUMMARY OF MAC PROTOCOLS

taking turns

- polling from central site, token passing
- bluetooth, FDDI, token ring

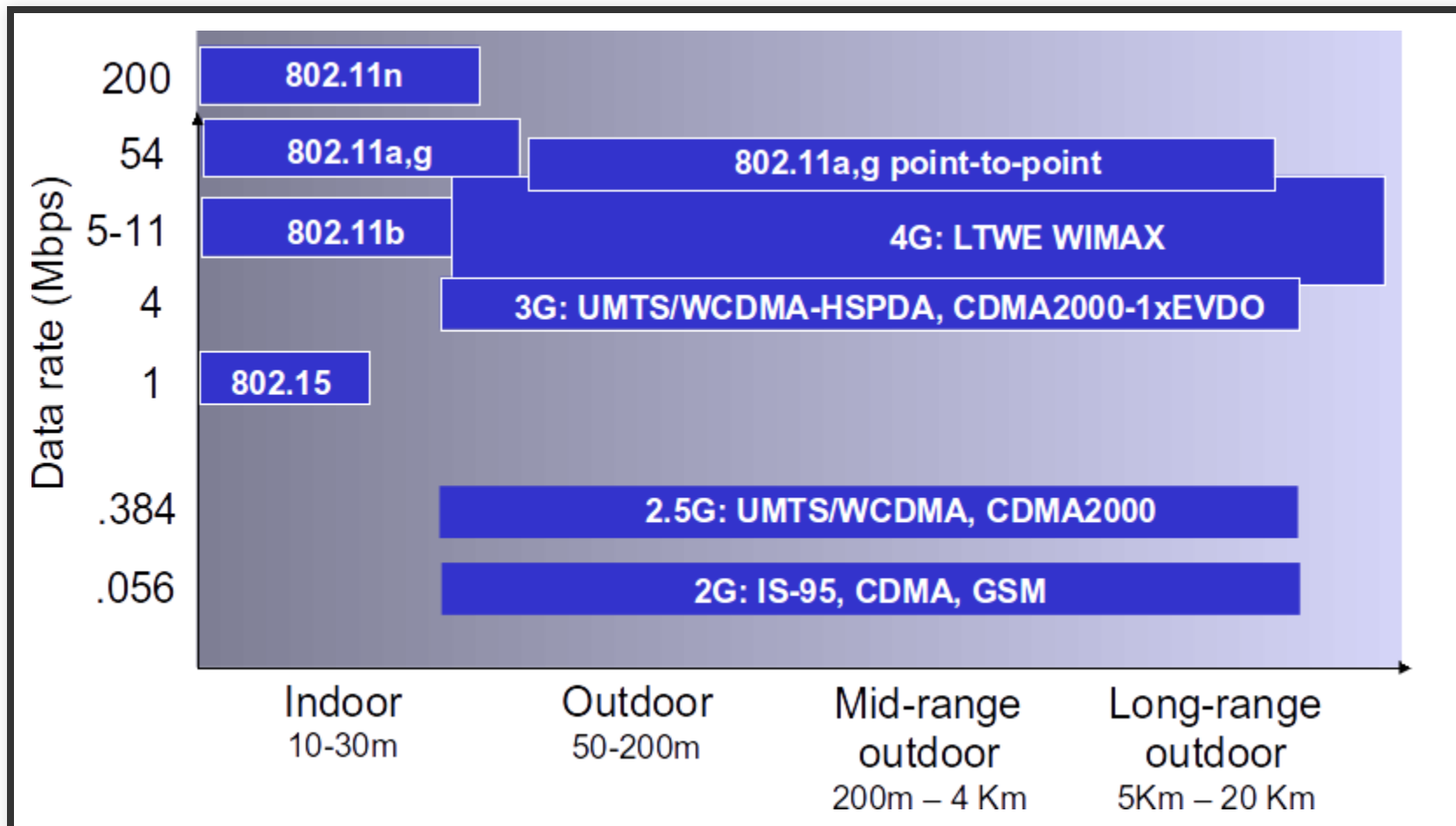
WIRELESS

ELEMENTS



- Wireless hosts
- Base station
- Wireless link

CHARACTERISTICS OF SELECTED WIRELESS LINKS



WIRELESS NETWORK TAXONOMY

single hop

multiple hops

infrastructure (e.g.,
APs)

host connects to
base station (WiFi,
WiMAX, cellular)
which connects to
larger Internet

host may have to
relay through
several wireless
nodes to connect to
larger Internet:
mesh net

WIRELESS LINKS

WIRELESS LINKS CHARACTERISTICS

important differences from wired link...

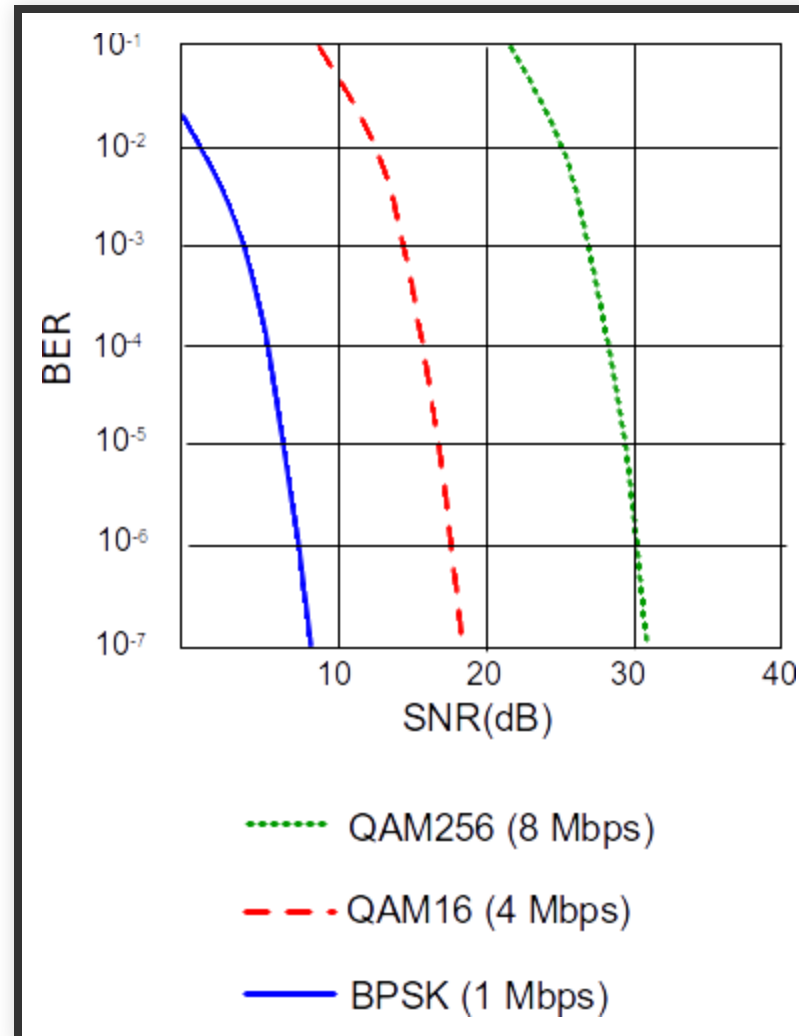
- **decreased signal strength:** radio signal attenuates as it propagates through matter (path loss)
- **interference from other sources:** standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well
- **multipath propagation:** radio signal reflects off objects ground, arriving at destination at slightly different times

Make communication across (even point to point) wireless link much more “difficult”

WIRELESS LINKS CHARACTERISTICS

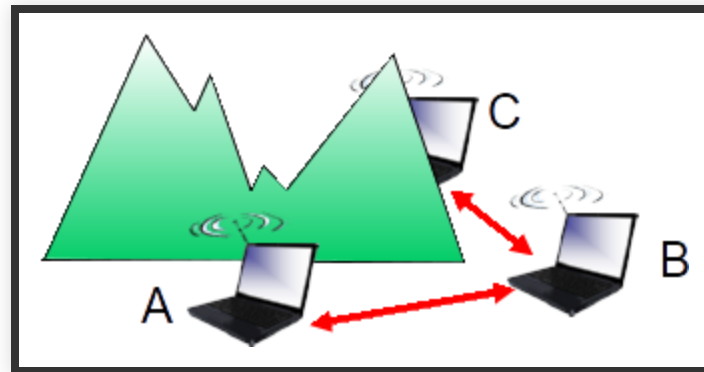
- **SNR:** signal-to-noise ratio
 - larger SNR – easier to extract signal from noise (a “good thing”)
- SNR versus BER tradeoffs
 - **given physical layer:** increase power → increase SNR → decrease BER
 - **given SNR:** choose physical layer that meets BER requirement, giving highest throughput
 - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

WIRELESS LINKS CHARACTERISTICS



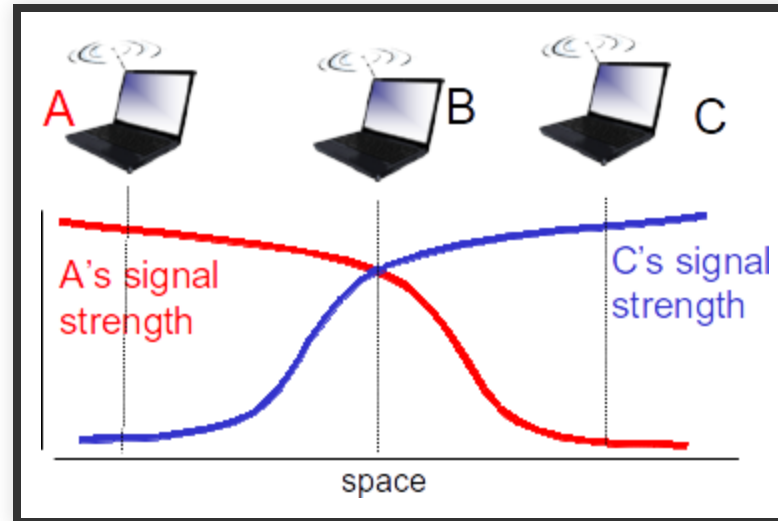
WIRELESS NETWORK CHARACTERISTICS

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

WIRELESS NETWORK CHARACTERISTICS



Signal attenuation/fading:

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

MULTIPLE ACCESS IN WIFI

More difficult due to

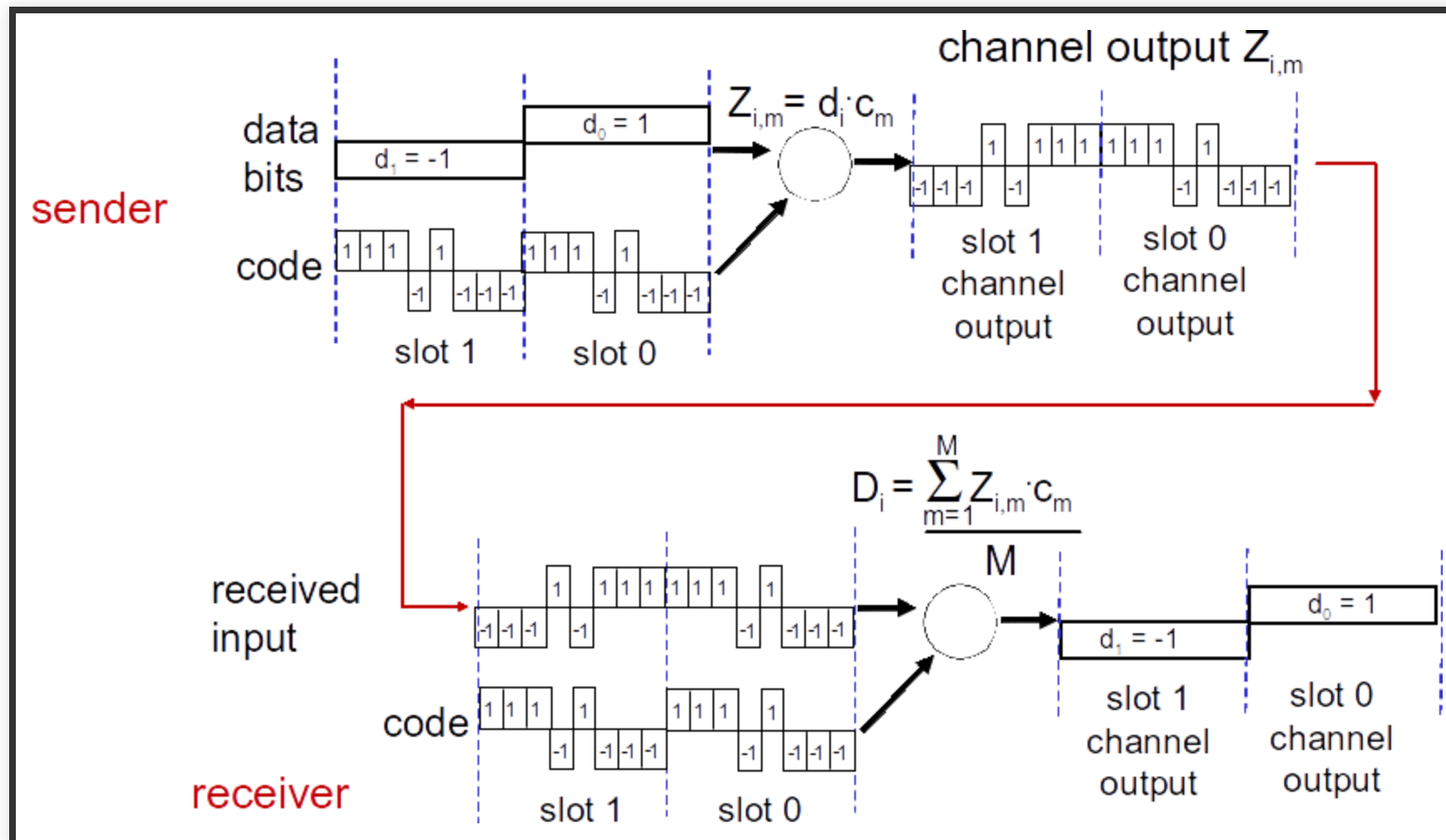
- Hidden terminal problem
- Fading

Lets see a different **channel partitioning** protocol CDMA, which is prevalent in wireless LAN

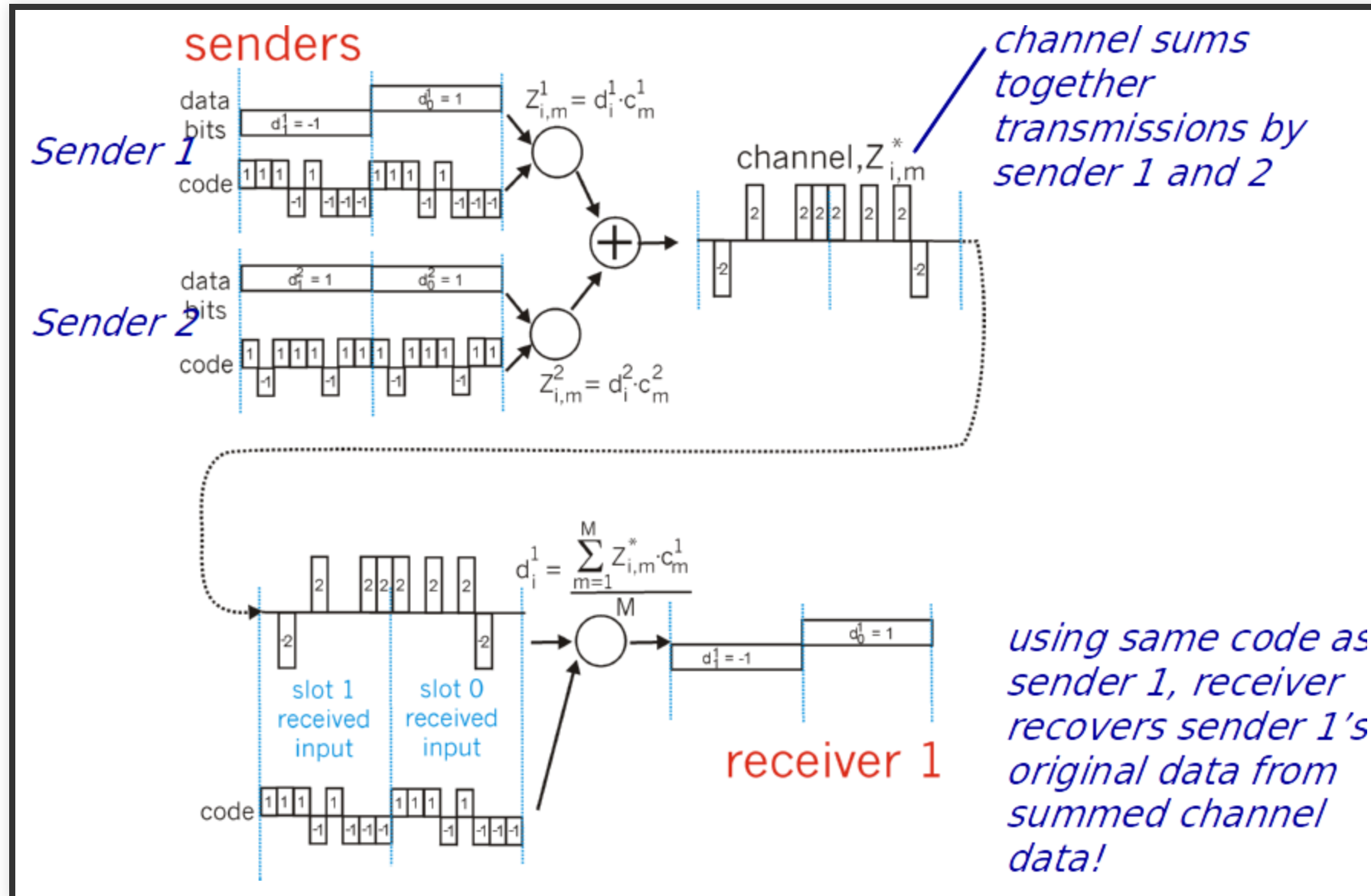
CODE DIVISION MULTIPLE ACCESS (CDMA)

- Unique "code" assigned to each user; i.e., code set partitioning
 - all users share same frequency, but each user has own "chipping" sequence (i.e., code) to encode data
 - allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")
- **Encoded signal** = (original data) * (chipping sequence)
- **Decoding:** inner-product of encoded signal and chipping sequence

CDMA ENCODE/DECODE



CDMA: TWO-SENDER INTERFERENCE



CDMA - NOTES

- Works under the assumption that signals are additive
 - Signal strength from different senders must be the same
- CDMA codes must be carefully chosen
- Think cocktail-party with multiple languages
 - Humans are quite skilled in filtering out the language that they understand - and skip the ones they don't

IEEE 802.11 WIRELESS LANS ("WI-FI")

IEEE 802.11 WIRELESS LAN

Multiple versions with similarities

- All share characteristics:
 - Medium access control: CSMA/CA
 - Same frame structure
 - Backwards compatible g can still talk to ac
 - Can reduce transmission rate to reach greater distance

 Very different in physical layer

IEEE 802.11 WIRELESS LAN

! 802.11a

- 5-6 GHz range - up to 54 Mbps

IEEE 802.11 WIRELESS LAN

! 802.11g

- 2.4-2.5 GHz range - up to 54 Mbps

IEEE 802.11 WIRELESS LAN

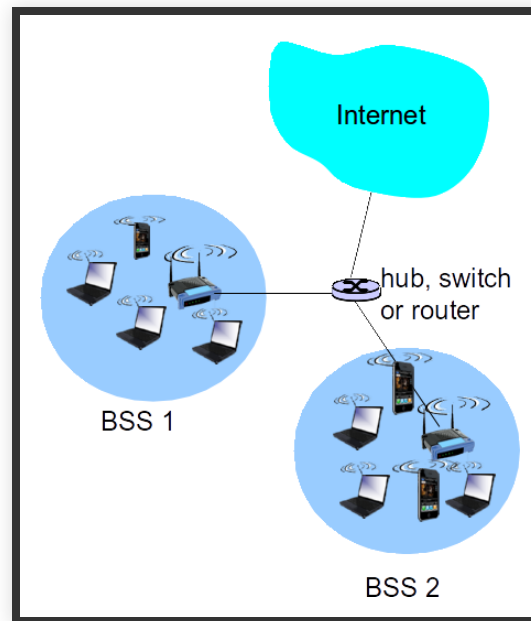
❗ 802.11n: multiple antennae

- 2.4-2.5 GHz range - up to 200 Mbps

IEEE 802.11 WIRELESS LAN

- ❗ 802.11ac: multiple antennae, wider bandwidth (up to 160MHz)
 - 5 GHz range
 - single-link throughput of at least 500 MBps
 - multi station throughput of at least 1 GBps
 - all use CSMA/CA for multiple access
 - all have base-station and ad-hoc network versions

IEEE 802.11 LAN ARCHITECTURE



- wireless host communicates with base station
 - base station = access point (AP)

IEEE 802.11 LAN ARCHITECTURE

Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:

- wireless hosts
- access point (AP): base station
- ad hoc mode: hosts only

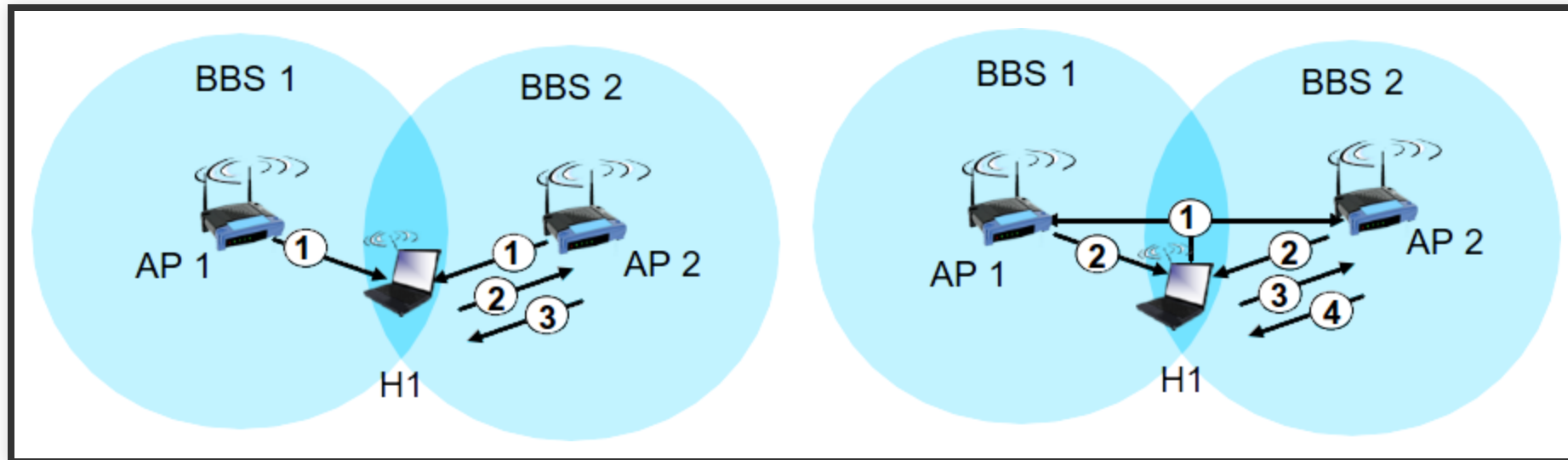
IEEE 802.11: CHANNELS, ASSOCIATION

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 (or 13 or 14) channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!

IEEE 802.11: CHANNELS, ASSOCIATION

- host: must associate with an AP
 - scans channels, listening for beacon frames containing AP's name (SSID) and MAC address
 - selects AP to associate with
 - may perform authentication [Chapter 8]
 - will typically run DHCP to get IP address in AP's subnet

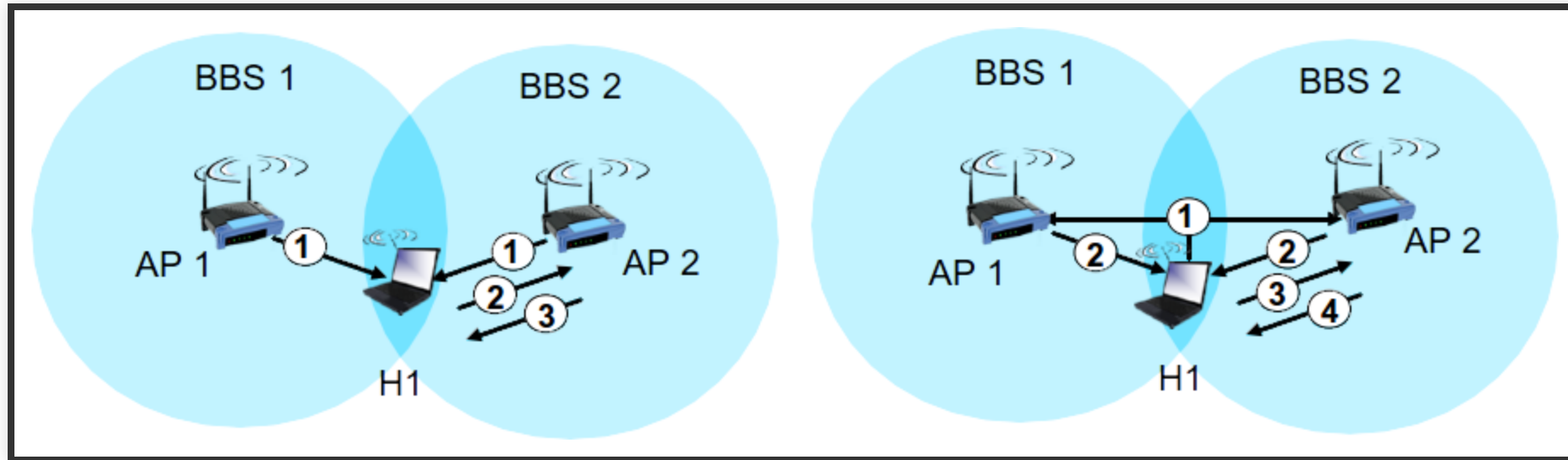
IEEE 802.11: PASSIVE/ACTIVE SCANNING



passive scanning:

- beacon frames sent from APs
- association Request frame sent: H1 to selected AP
- association Response frame sent from selected AP to H1

IEEE 802.11: PASSIVE/ACTIVE SCANNING



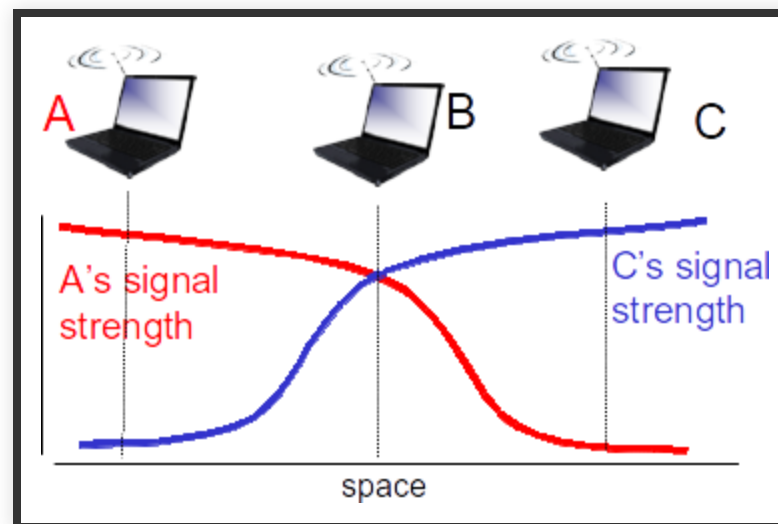
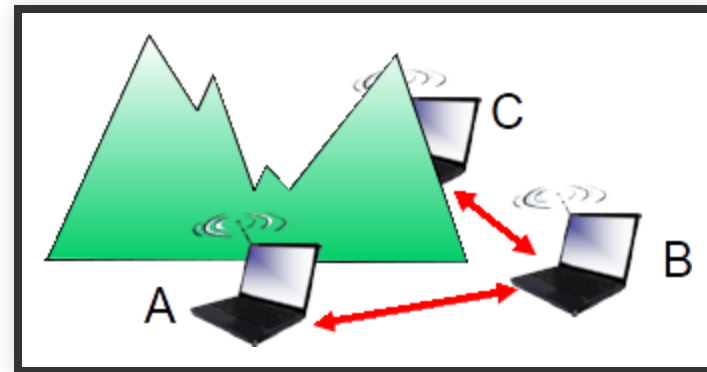
active scanning:

- Probe Request frame broadcast from H1
- Probe Response frames sent from APs
- Association Request frame sent: H1 to selected AP
- Association Response frame sent from selected AP to H1

IEEE 802.11: MULTIPLE ACCESS

- avoid collisions: 2+ nodes transmitting at same time
- 802.11: CSMA - sense before transmitting
 - don't collide with ongoing transmission by other node
- 802.11: no collision detection!
 - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
 - can't sense all collisions in any case: hidden terminal, fading
 - goal: **avoid collisions**: CSMA/C(ollision)A(voidance)

IEEE 802.11: MULTIPLE ACCESS



IEEE 802.11 MAC PROTOCOL: CSMA/CA

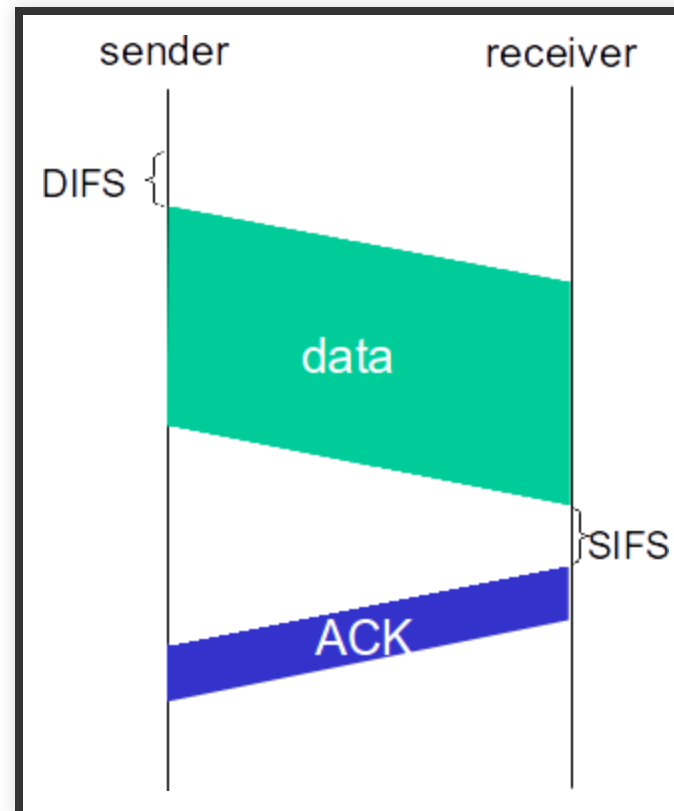
802.11 sender

1. if sense channel idle for short period of time (DIFS) then
 - transmit entire frame (no CD)
2. if sense channel busy then
 - start random backoff time
 - timer counts down while channel idle
3. when timer expires: transmit
4. if no ACK, increase random backoff interval, repeat from 2

IEEE 802.11 MAC PROTOCOL: CSMA/CA

802.11 receiver

- if frame received OK (passes CRC): return ACK after SIFS (ACK needed due to hidden terminal problem)




AVOIDING COLLISIONS

Dealing with hidden terminals

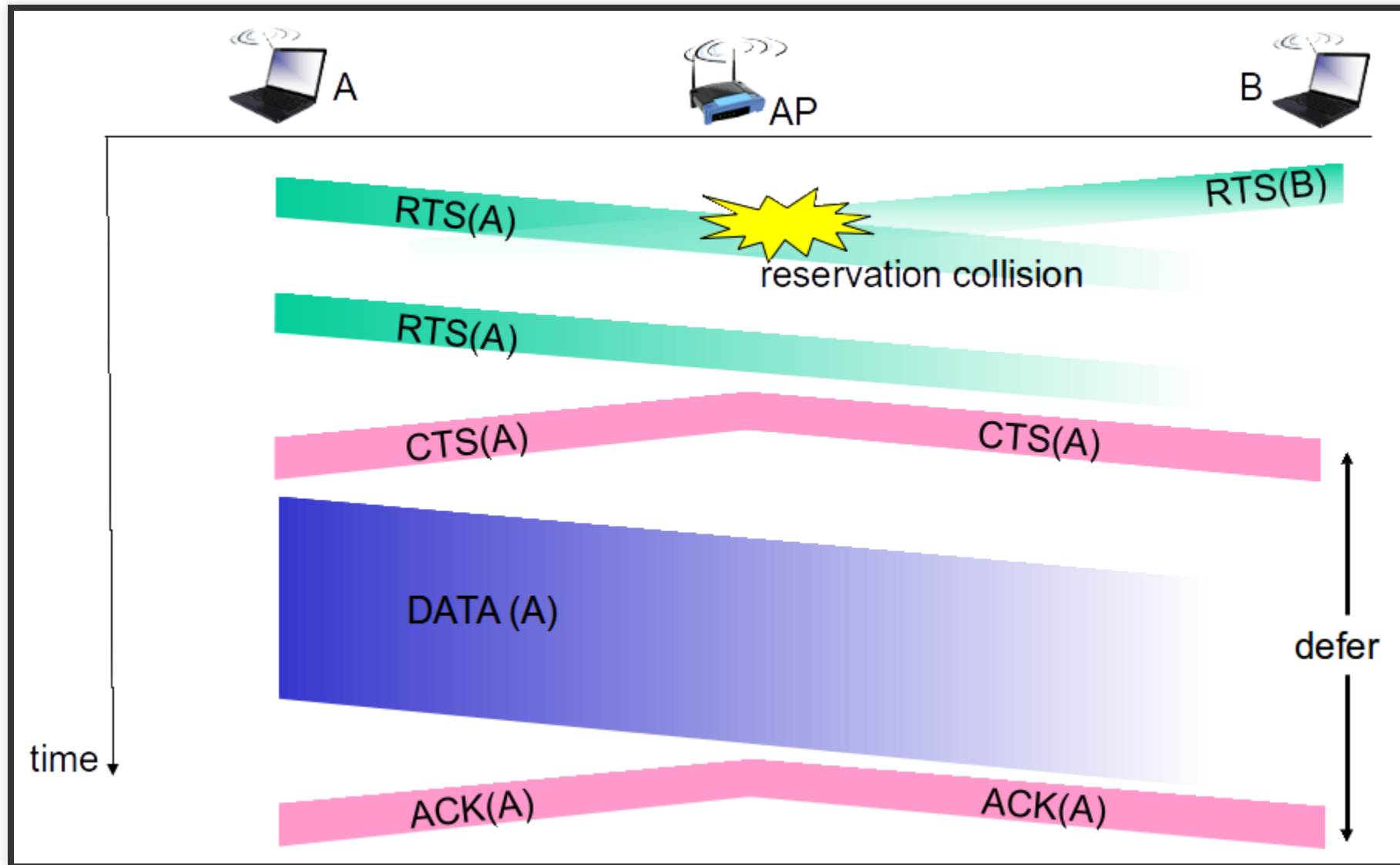
- ❗ **Idea:** allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

AVOIDING COLLISIONS

- sender first transmits small request-to-send (RTS) packets 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

 avoid data frame collisions completely using small reservation packets!

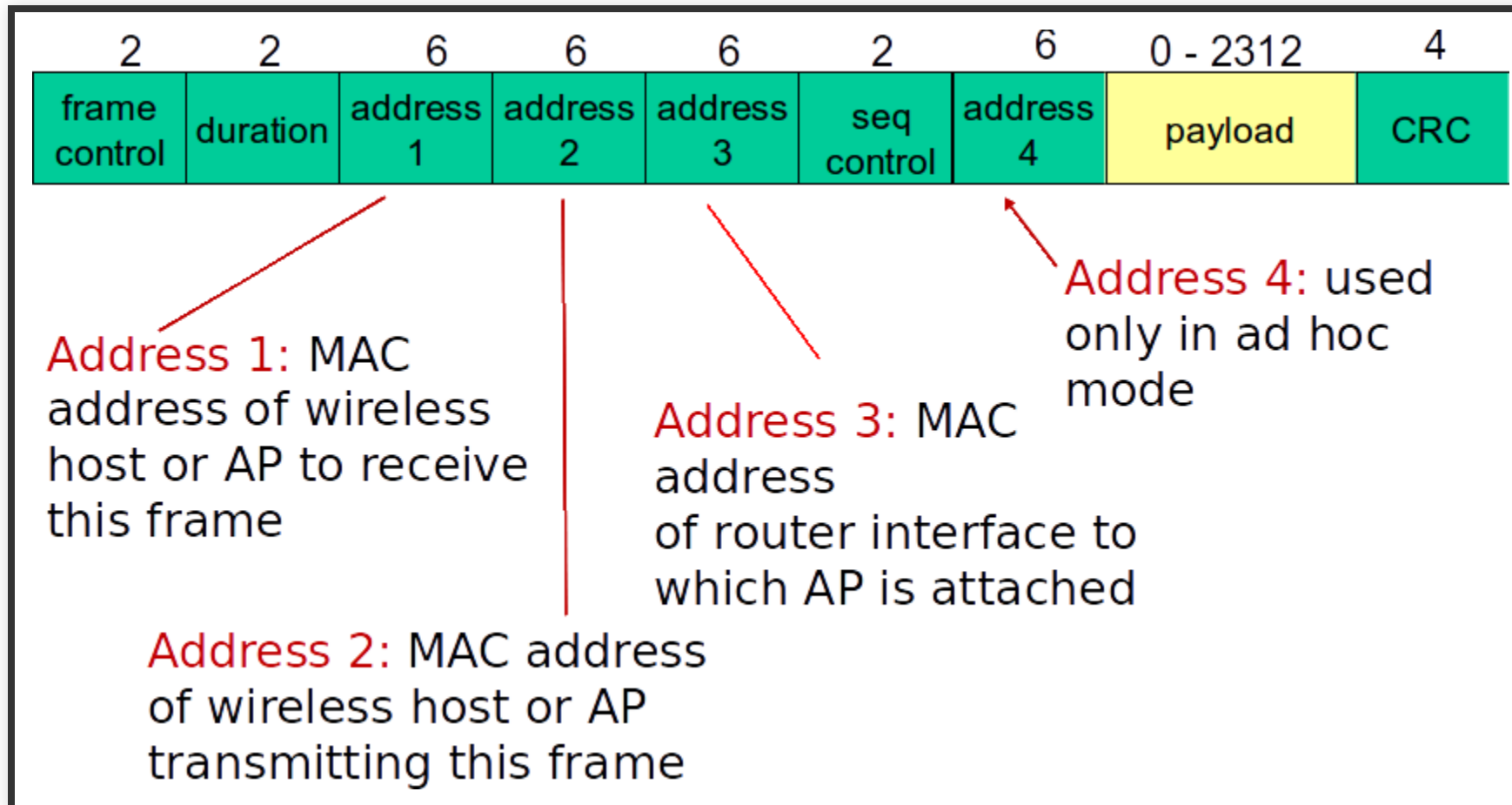
COLLISION AVOIDANCE: RTS-CTS EXCHANGE



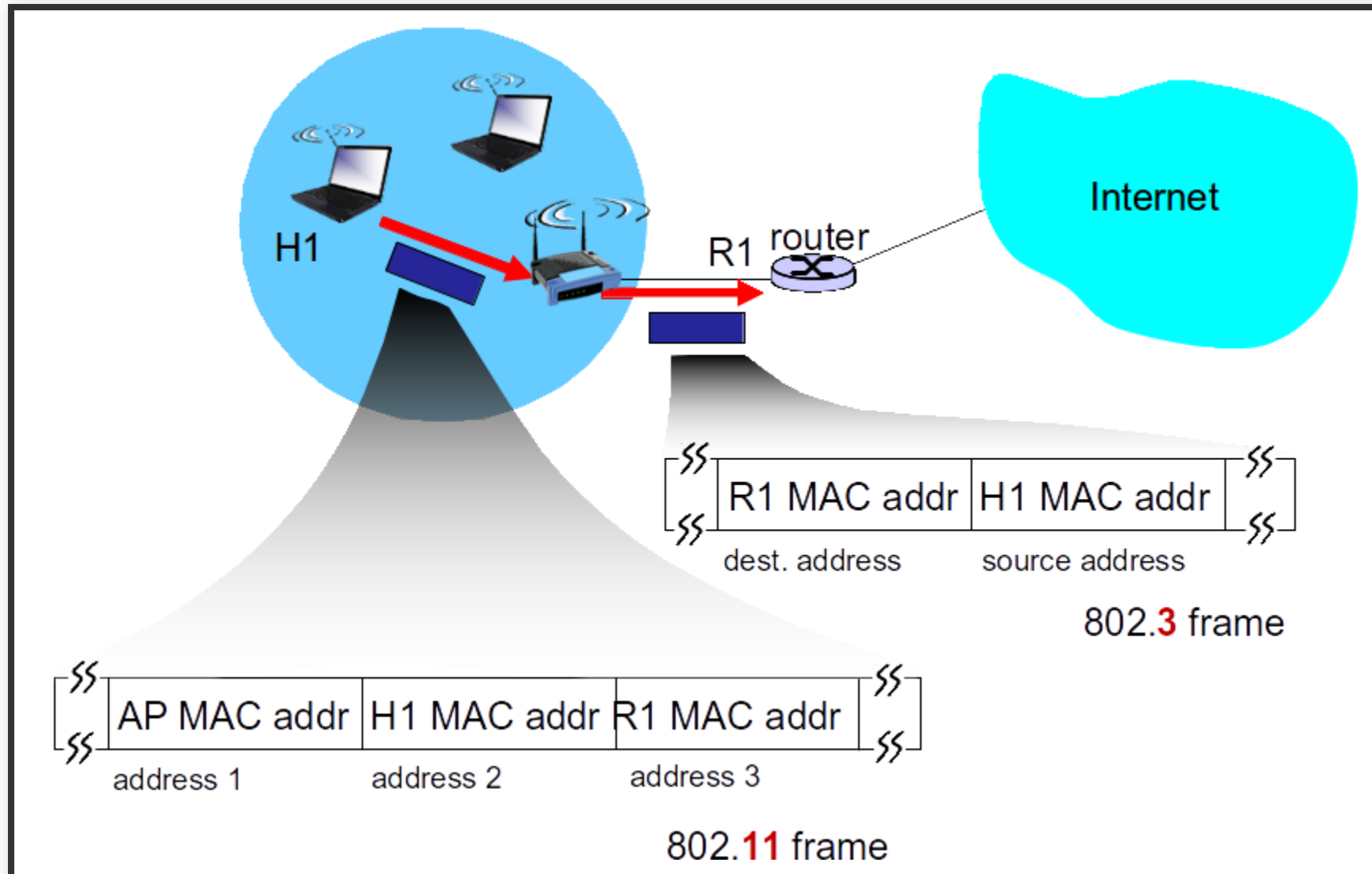
COLLISION AVOIDANCE: RTS-CTS

- Does introduce delay and consumes channel resources!
- Only used (if at all) for transmissions of long data frame
- Basestation can set RTS threshold so RTS/CTS only used if frame is larger than threshold
 - if RTS threshold $>$ max frame length \Rightarrow disable completely

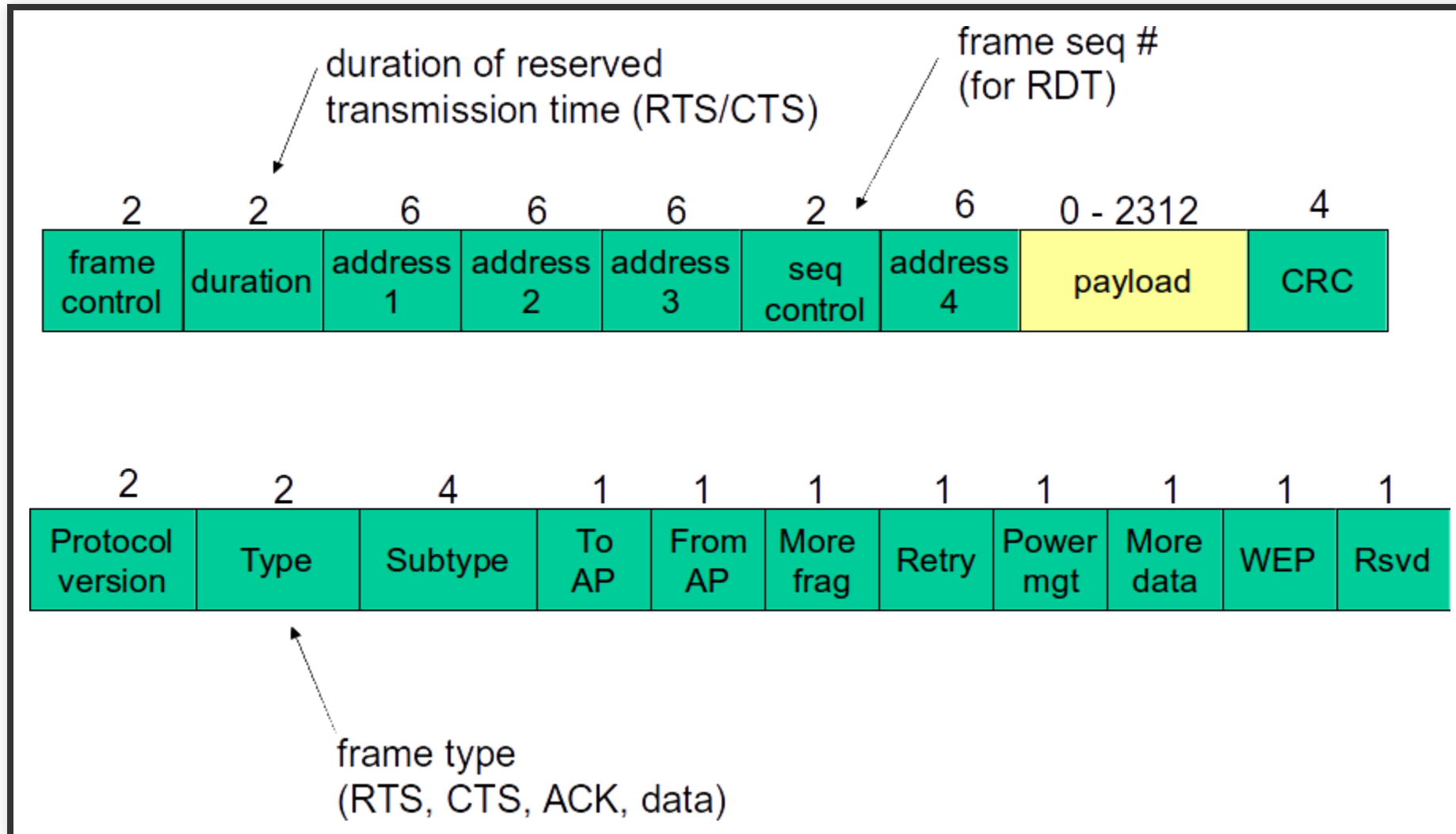
PROTOCOL 802.11 FRAME: ADDRESSING



PROTOCOL 802.11 FRAME: ADDRESSING



PROTOCOL 802.11 FRAME



PROTOCOL 802.11 FRAME

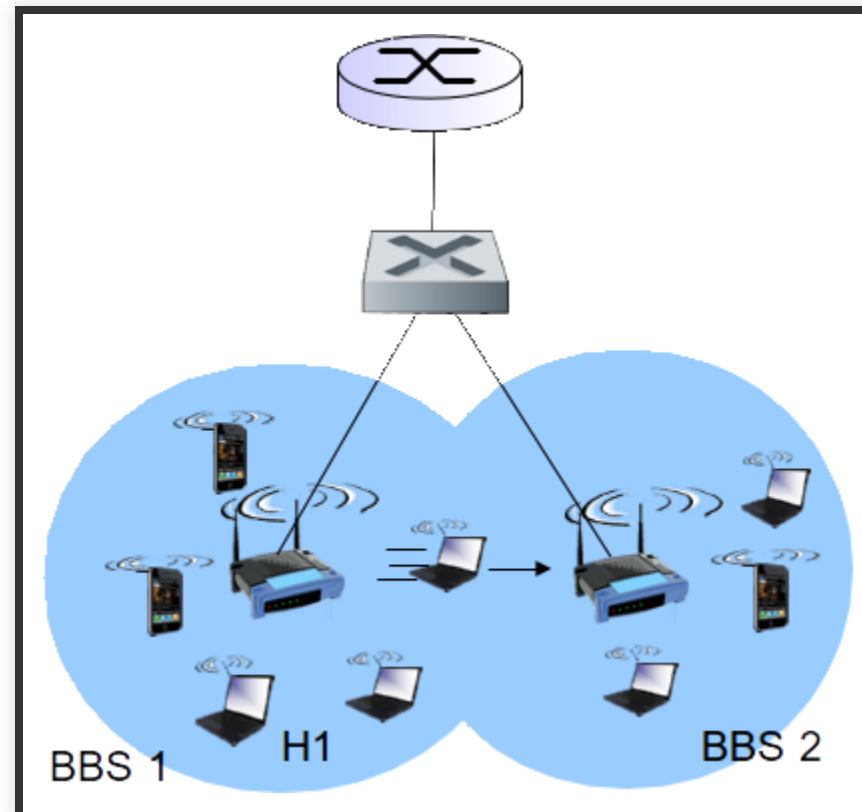
- **Payload:**
 - Contains an IP datagram or ARP packet
 - Allowed to be 2312 - often less than 1500
- **Seq no.:** Acks used - so need to know which is acked.
- **CRC:** Bit errors more frequent - so even more usefull here.
- **Duration:** Reserved time for RTS, CTS or data

PROTOCOL 802.11 FRAME: FRAME CONTROL

- **Type and subtype:** RTS, CTS, ACK, Data
- **To and From:** Define meaning of address fields (change with mode)
- **WEP:** Indicates if WEP encryption is used.

MOBILITY WITHIN SAME SUBNET

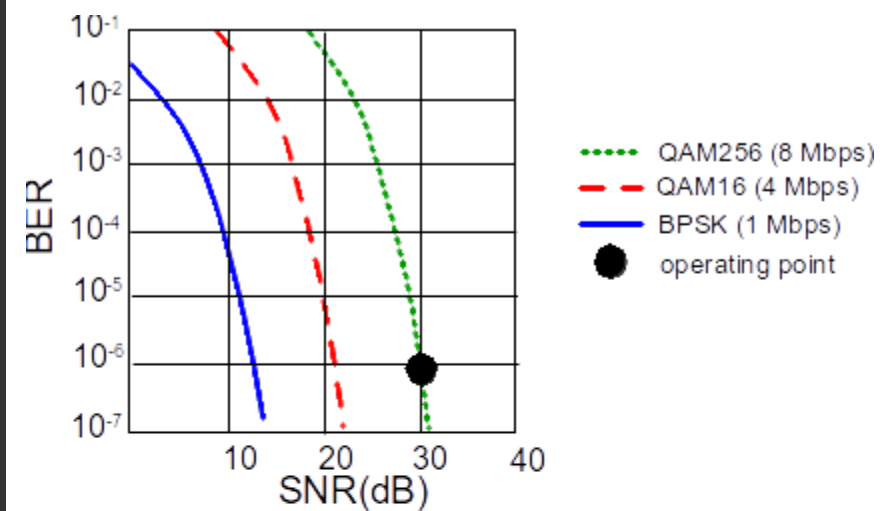
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
 - self-learning (Ch. 5): switch will see frame from H1 and "remember" which switch port can be used to reach H1



ADVANCED CAPABILITIES

Rate adaptation

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



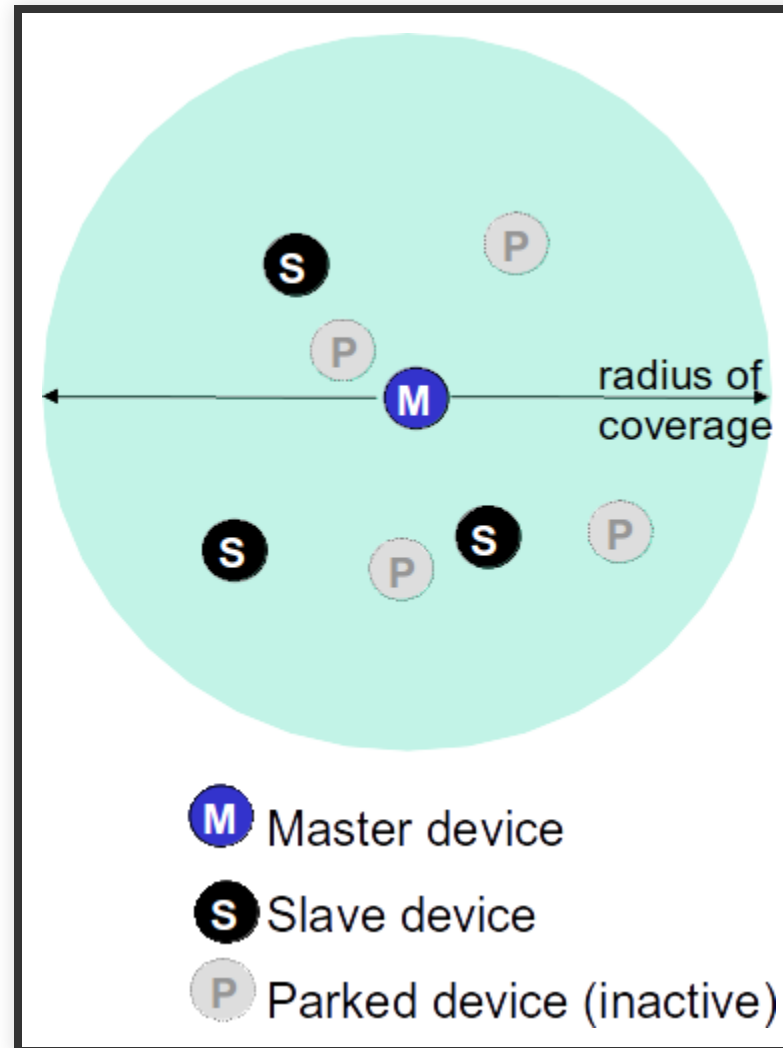
1. SNR decreases, BER increase as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but with lower BER

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

IEEE 802.15 - PERSONAL AREA NETWORK



Bluetooth piconet

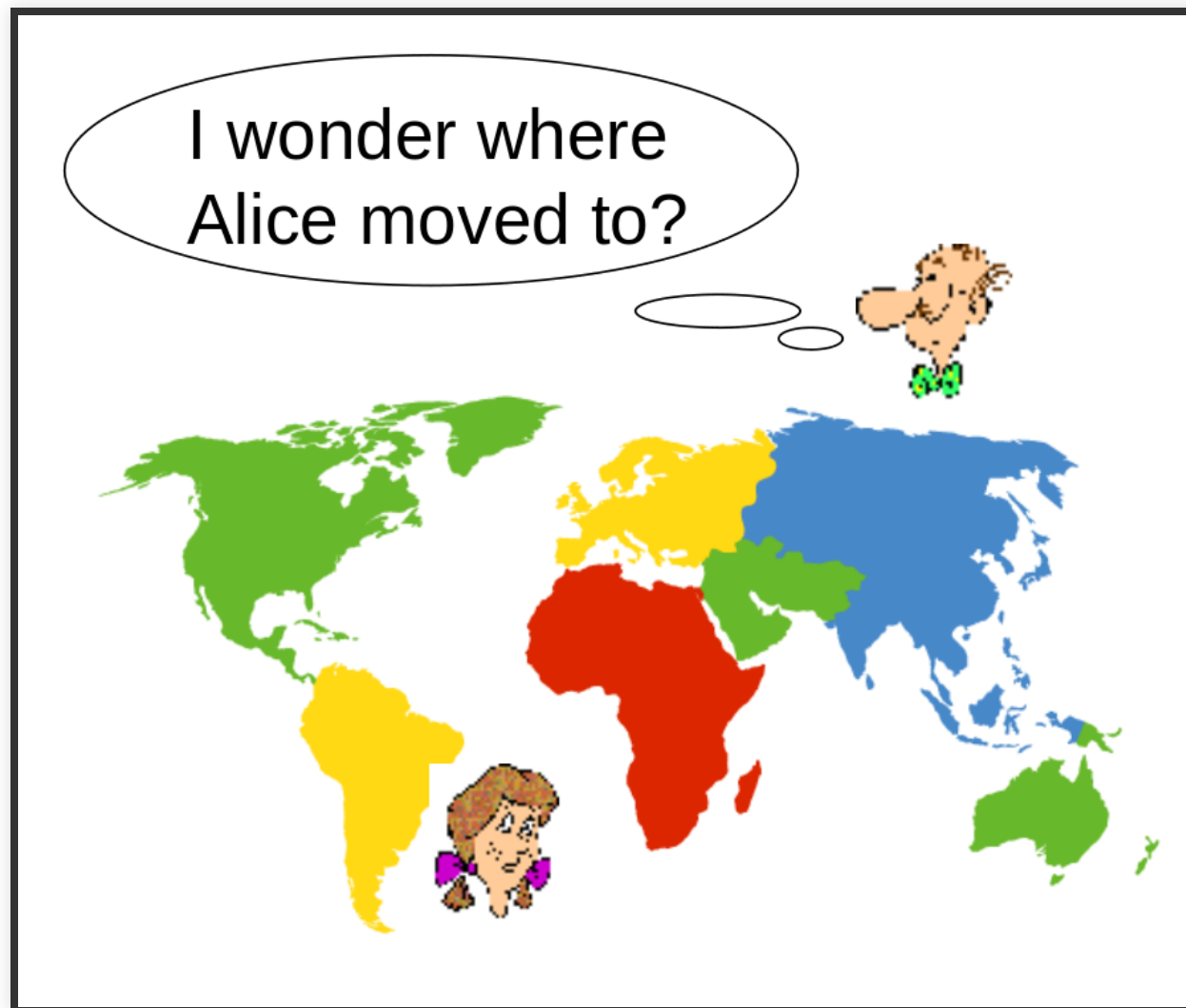
IEEE 802.15 - PERSONAL AREA NETWORK

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
 - slaves request permission to send (to master)
 - master grants requests
- 802.15: evolved from Bluetooth specification
 - 2.4-2.5 GHz radio band
 - up to 721 kbps

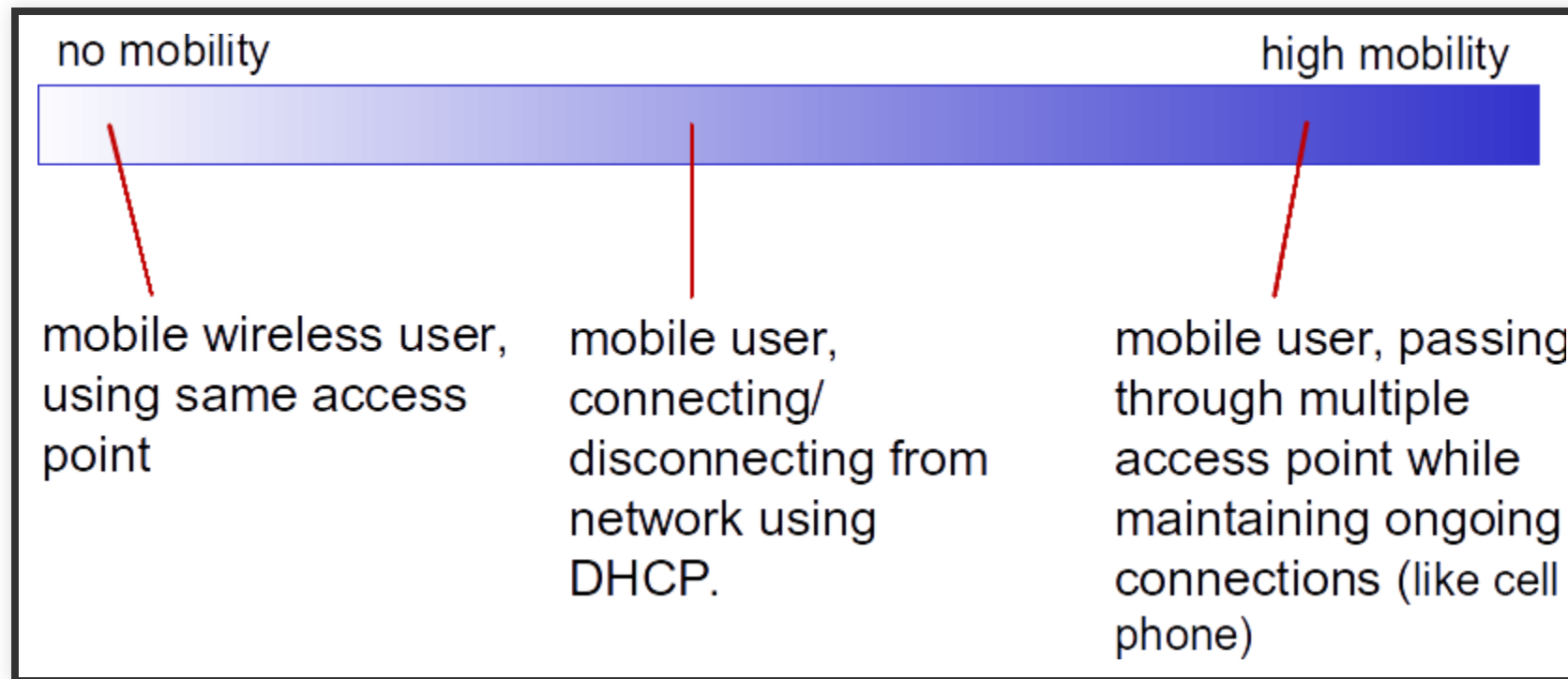
MOBILITY MANAGEMENT

MOBILE FRIEND

Consider friend frequently changing addresses, how do you find her?



MOBILITY



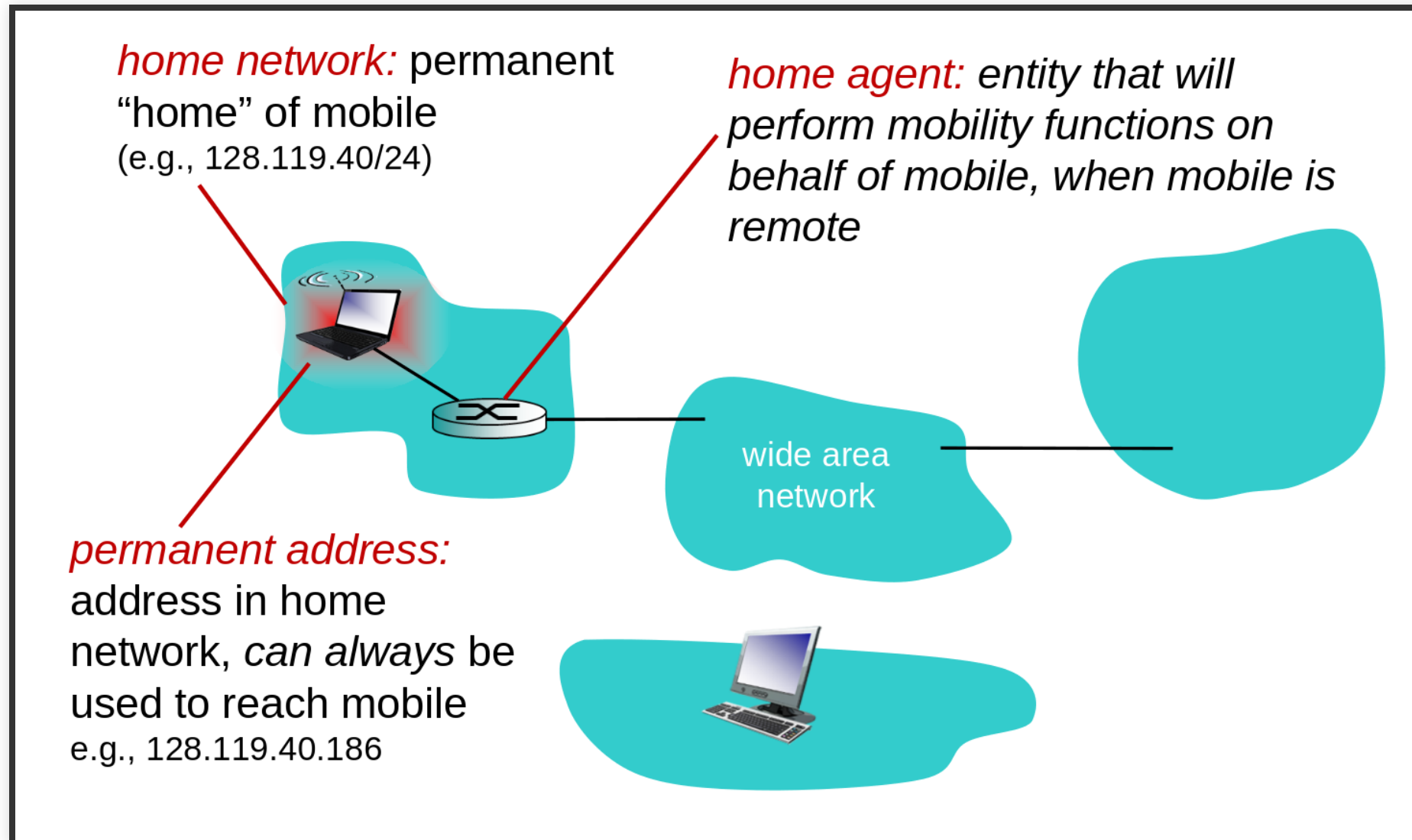
- **wireless:** communication over wireless link
- **mobility:** handling the mobile user who changes point of attachment to network

MOBILITY VIEWPOINT

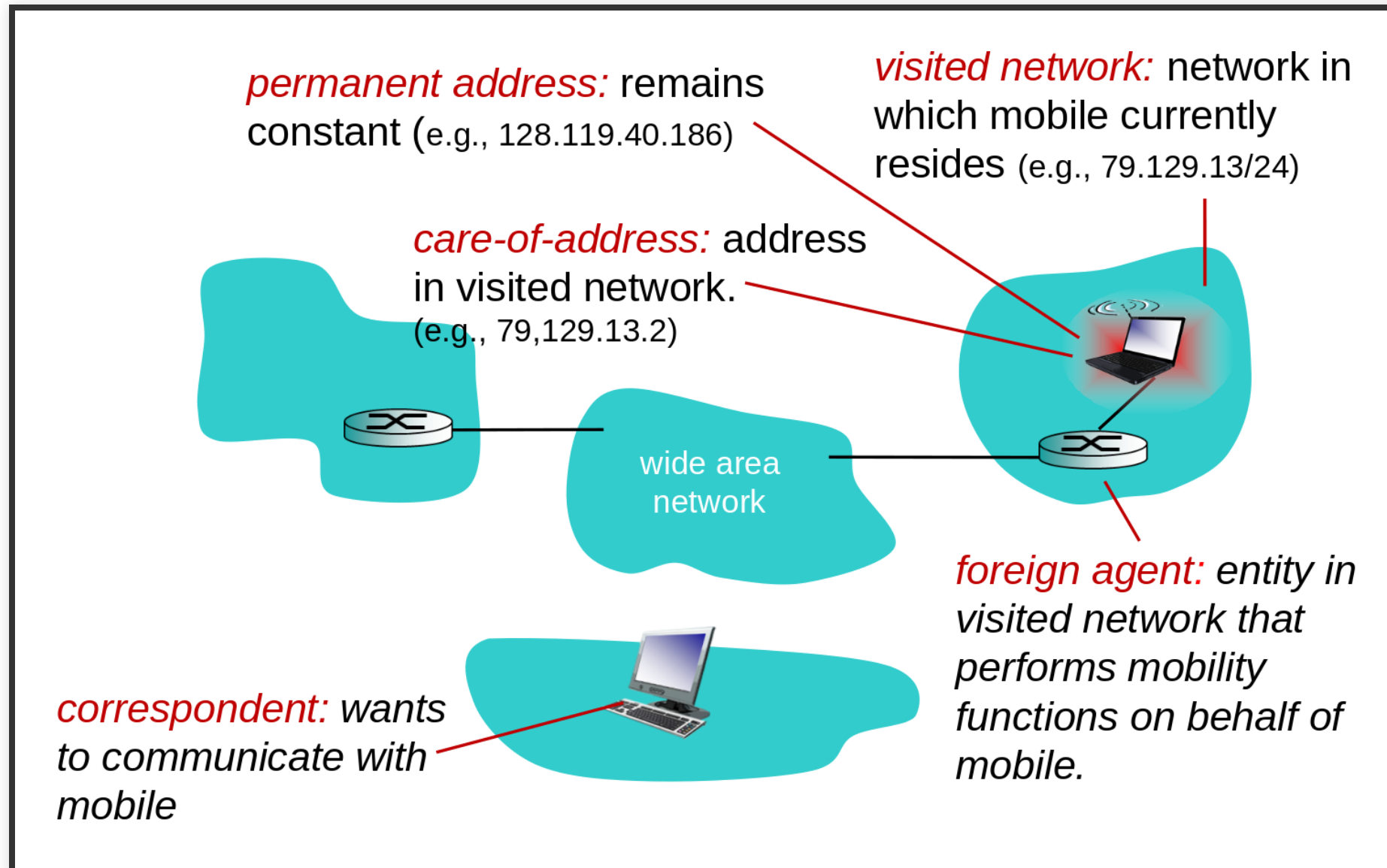
- Same access point, user just moving around at home - no change for link layer - not mobile
- Smartphone in car running 100km/h - highly mobile
- User with laptop, traveling. Receive new IP each place he turns on laptop.

Question: Must the device keep the same IP as it moves through IP networks?

MOBILITY VOCABULARY



MOBILITY VOCABULARY



ADDRESSING

Mobile node resident in foreign network → all traffic needs to be routed there

First plan: **Let routing handle it**

ADDRESSING

- Foreign network could advertise to all others
 - Existing intra- + inter-domain routing
 - Advertise to its neighbours a highly specific route to the permanent IP address
 - Neighbors would propagate routing information as part of normal procedure
- When node leaves network - repeat for new network
 - Old network would resign route

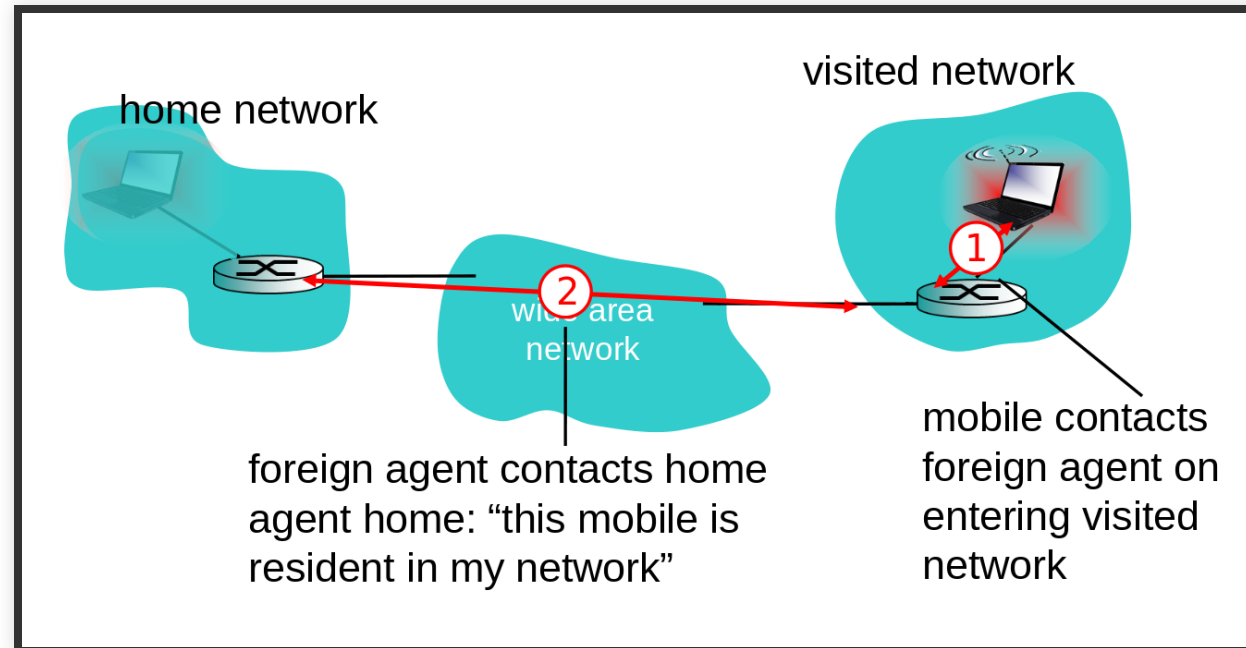
Q: Is this a good solution?

ADDRESSING - BETTER WAY

Push mobility functionality to network edge! (Like we have seen before Q: Where?)

Let end-systems handle it

ADDRESSING: REGISTRATION



end result:

- Foreign agent knows about mobile
- Home agent knows location of mobile

ADDRESSING: REGISTRATION

The foreign agent will create a **care-of-address (COA)** for the mobile node.

Now mobile node has 2 addresses

1. Permanent address
2. COA or Foreign Address

Mobile node could have done this by itself (using DHCP and contacting home network)

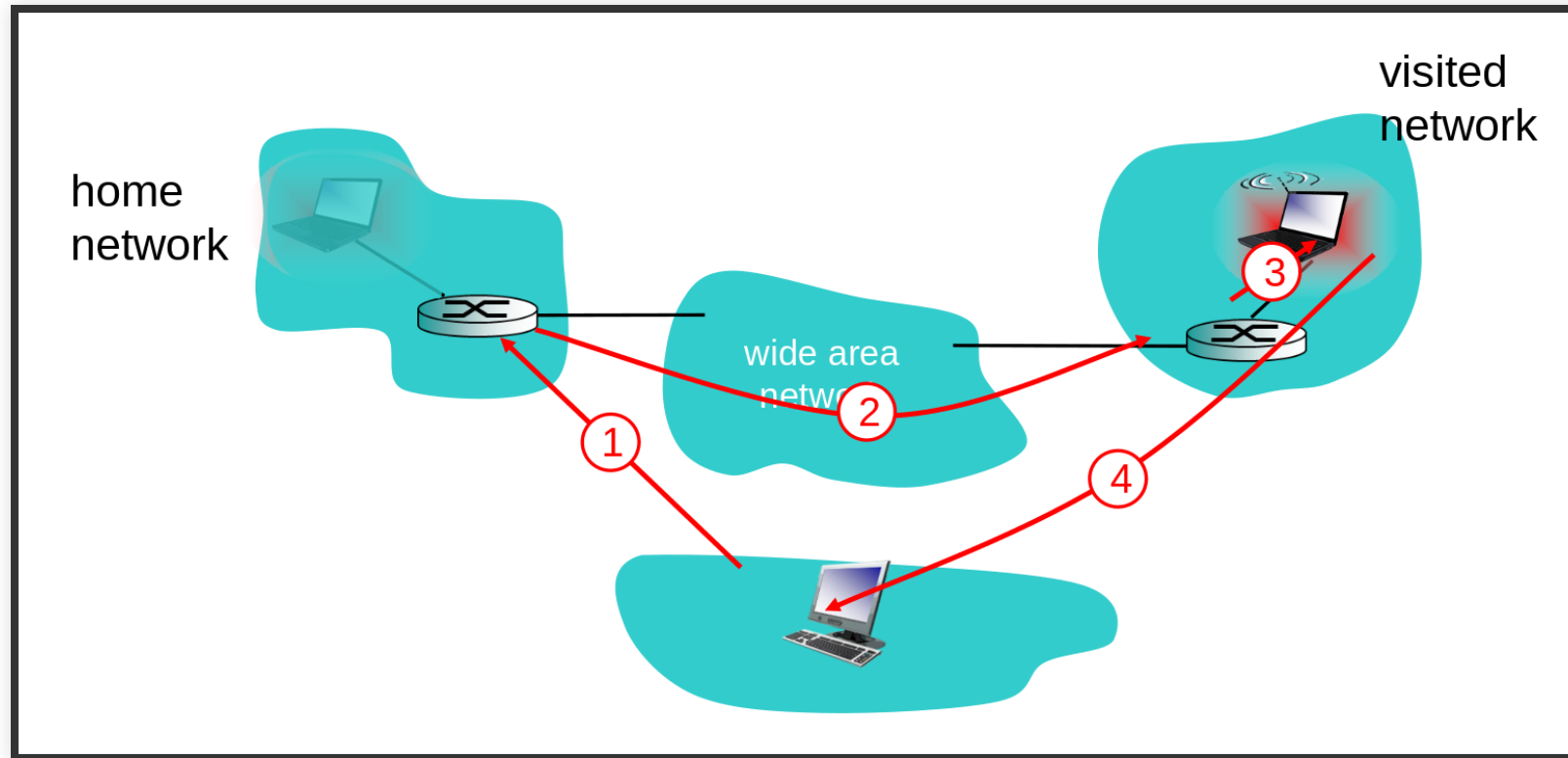
ADDRESSING: ROUTING

Mobile node with COA and home network knowing it only solves half the problem.

How should datagrams be addressed and forwarded to the mobile node?

Only home agent knows the location - not network wide!

ADDRESSING: INDIRECT ROUTING



communication from correspondent to mobile goes through home agent, then forwarded to remote

ADDRESSING: INDIRECT ROUTING

- Mobile uses two addresses:
 - **permanent address:** used by correspondent (hence mobile location is *transparent* to correspondent)
 - **care-of-address:** used by home agent to forward datagrams to mobile
- Foreign agent functions may be done by mobile itself
- Triangle routing: correspondent → home-network → mobile
inefficient when correspondent, mobile are in same network

INDIRECT ROUTING: MOVING BETWEEN NETWORKS

- Suppose mobile user moves to another network
 - registers with new foreign agent
 - new foreign agent registers with home agent
 - home agent update care-of-address for mobile
 - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: **on going connections can be maintained!**

INDIRECT ROUTING - SUMMARY

- Mobile-node-to-foreign-agent protocol
- Foreign-agent-to-home-agent registration protocol
- Home-agent datagram encapsulation protocol
- Foreign-agent decapsulation protocol



Suffers from triangle routing problem




Transparent to correspondent

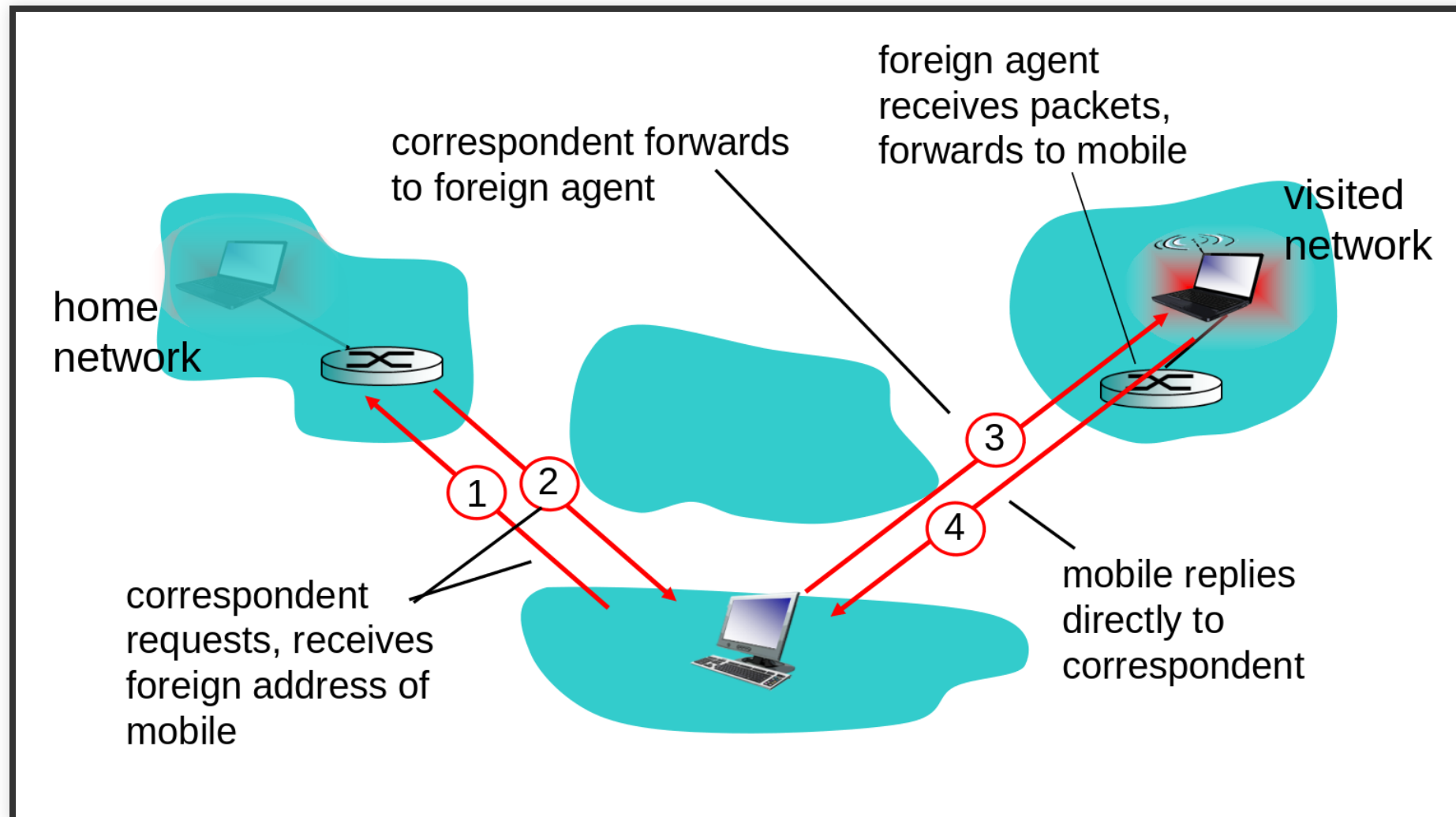
DIRECT ROUTING

Direct routing solved triangle routing problem - price: additional complexity

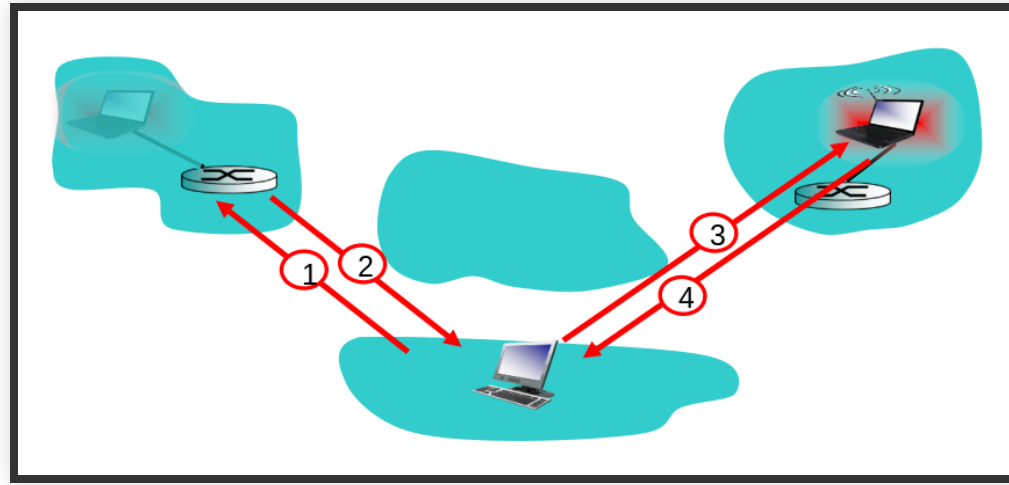
Correspondent gets foreign address of mobile, sends directly to mobile

 non-transparent to correspondent: correspondent must get care-of-address from home agent

DIRECT ROUTING



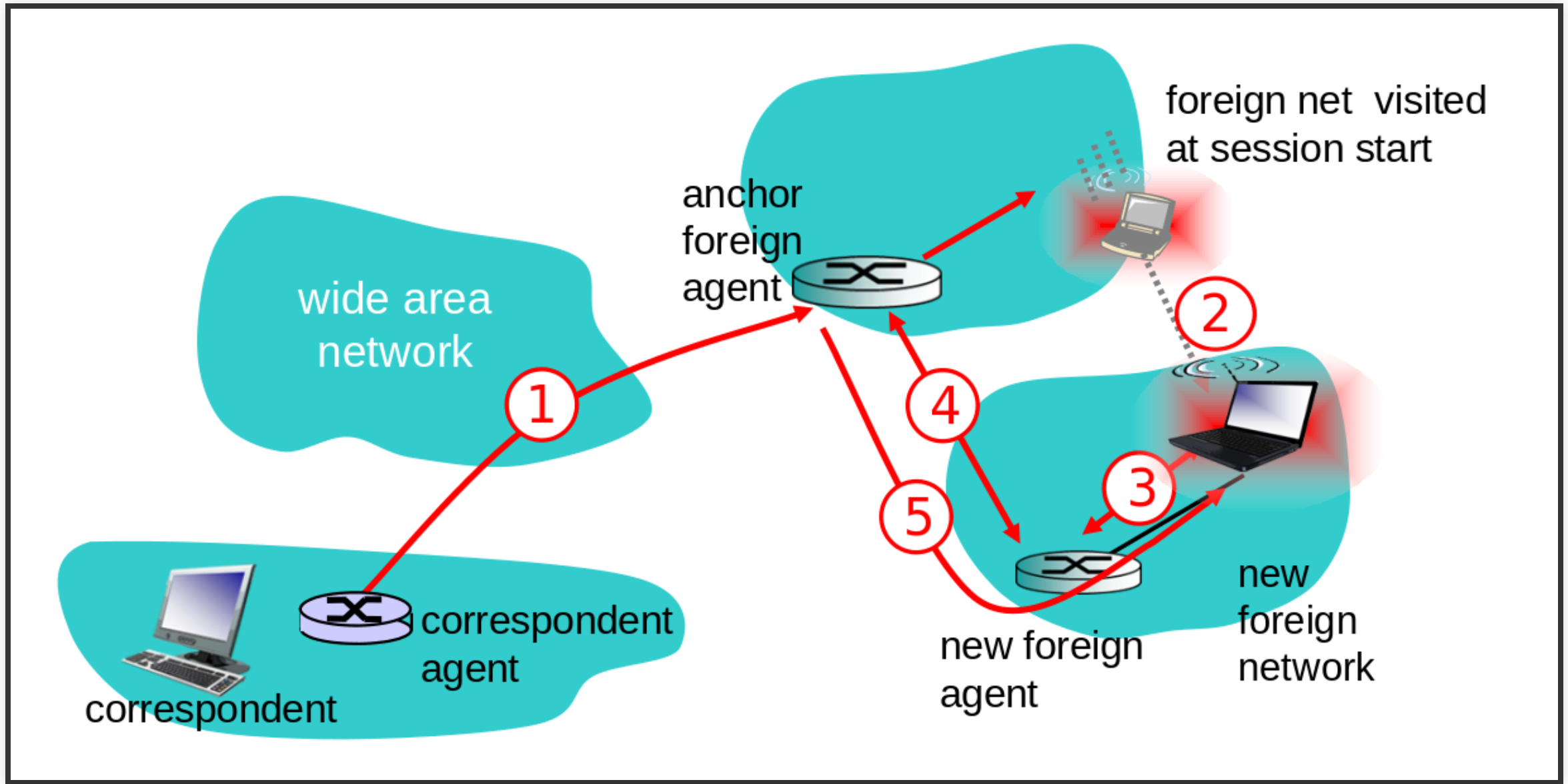
DIRECT ROUTING



Two new challenges

- Mobile-user location protocol (1+2)
- How can we handle mobile user switching to new network?
 - COA at home agent only queried at start of session

DIRECT ROUTING



MOBILE IP

MOBILE IP

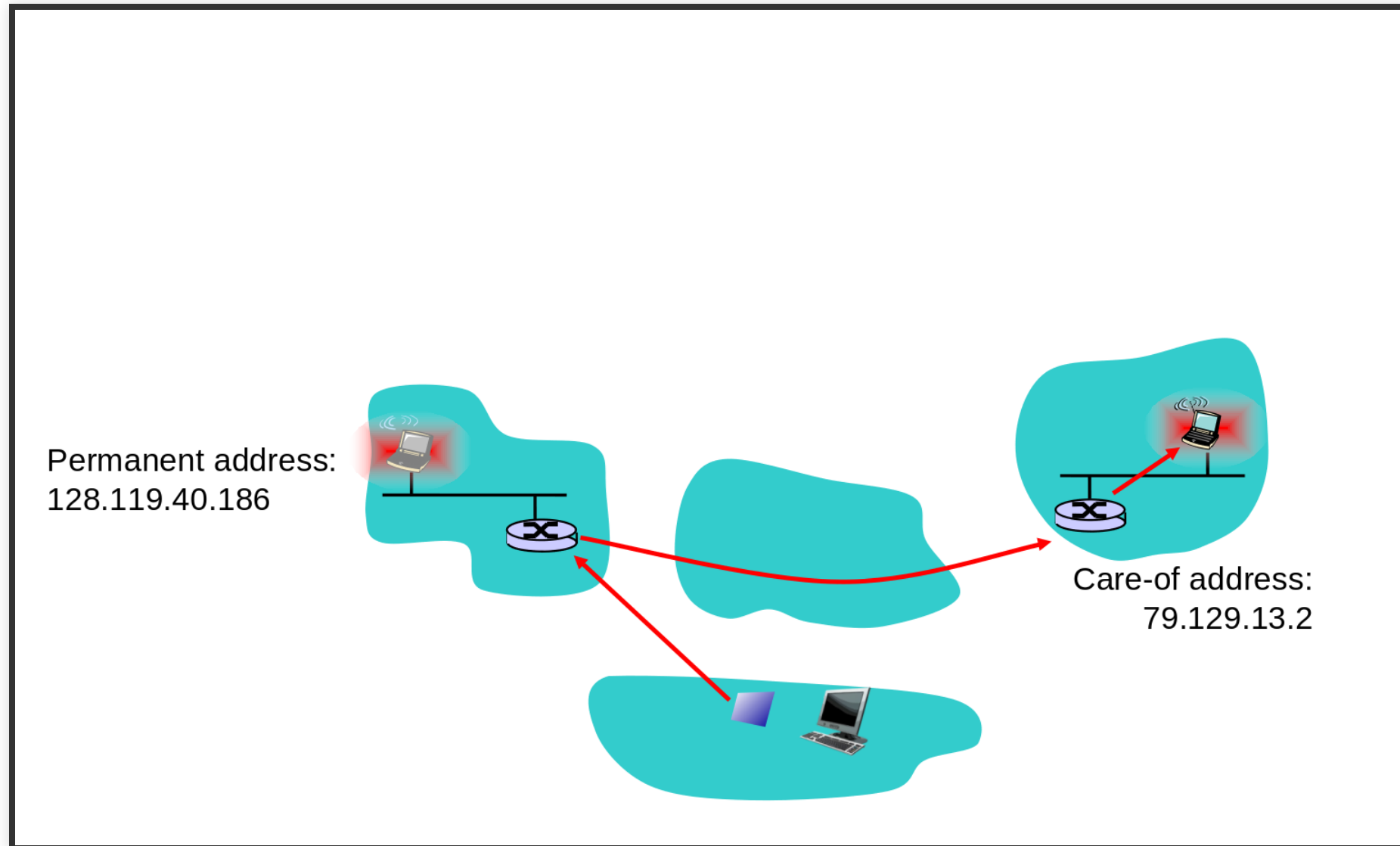
- RFC-3344
- Has many features we've seen:
 - home agents
 - foreign agents
 - foreign-agent registration
 - care-of-addresses
 - encapsulation (packet-within-a-packet)

MOBILE IP

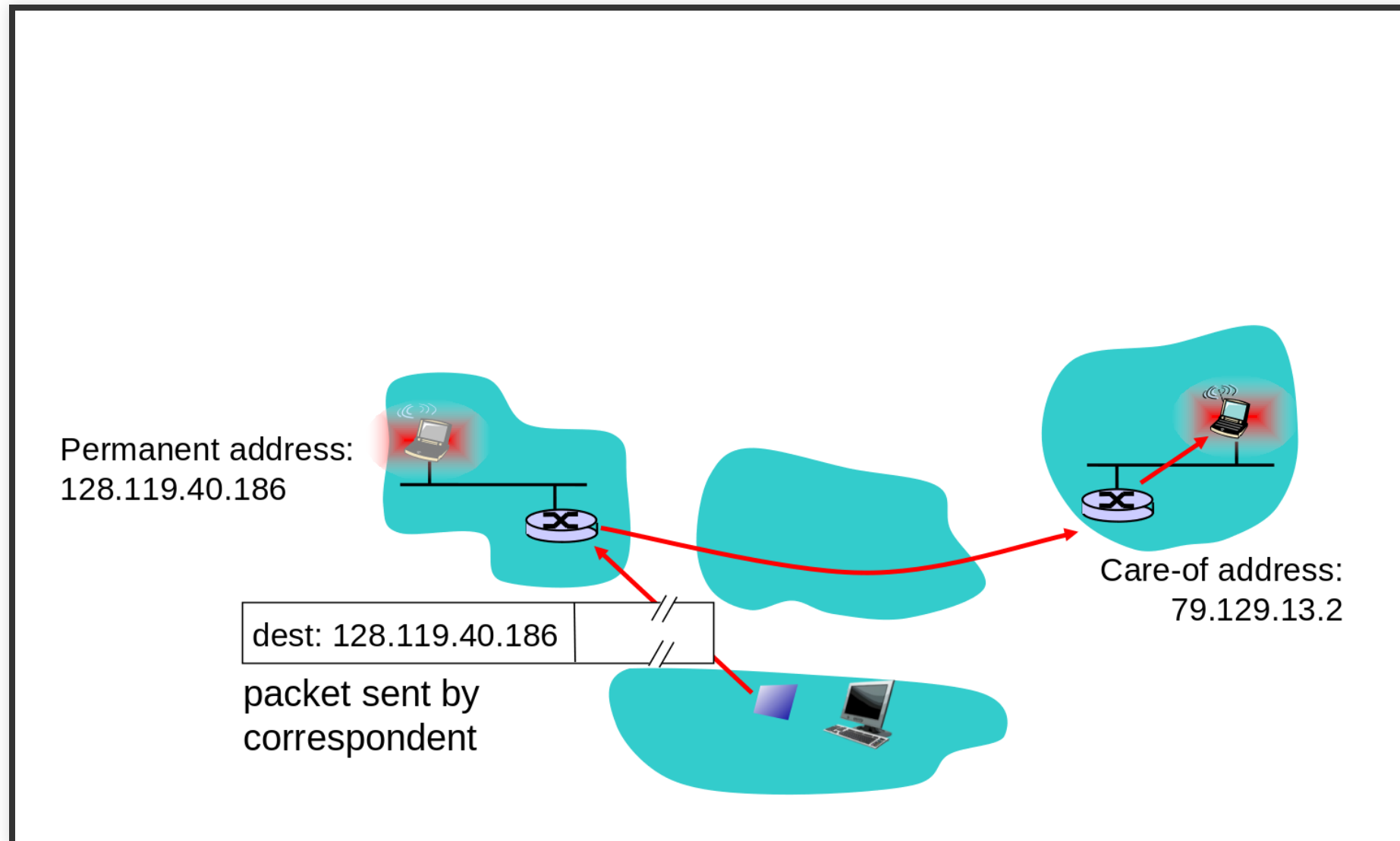
Three components of Mobile IP standard:

- Indirect routing of datagrams
- Agent discovery
- Registration with home agent

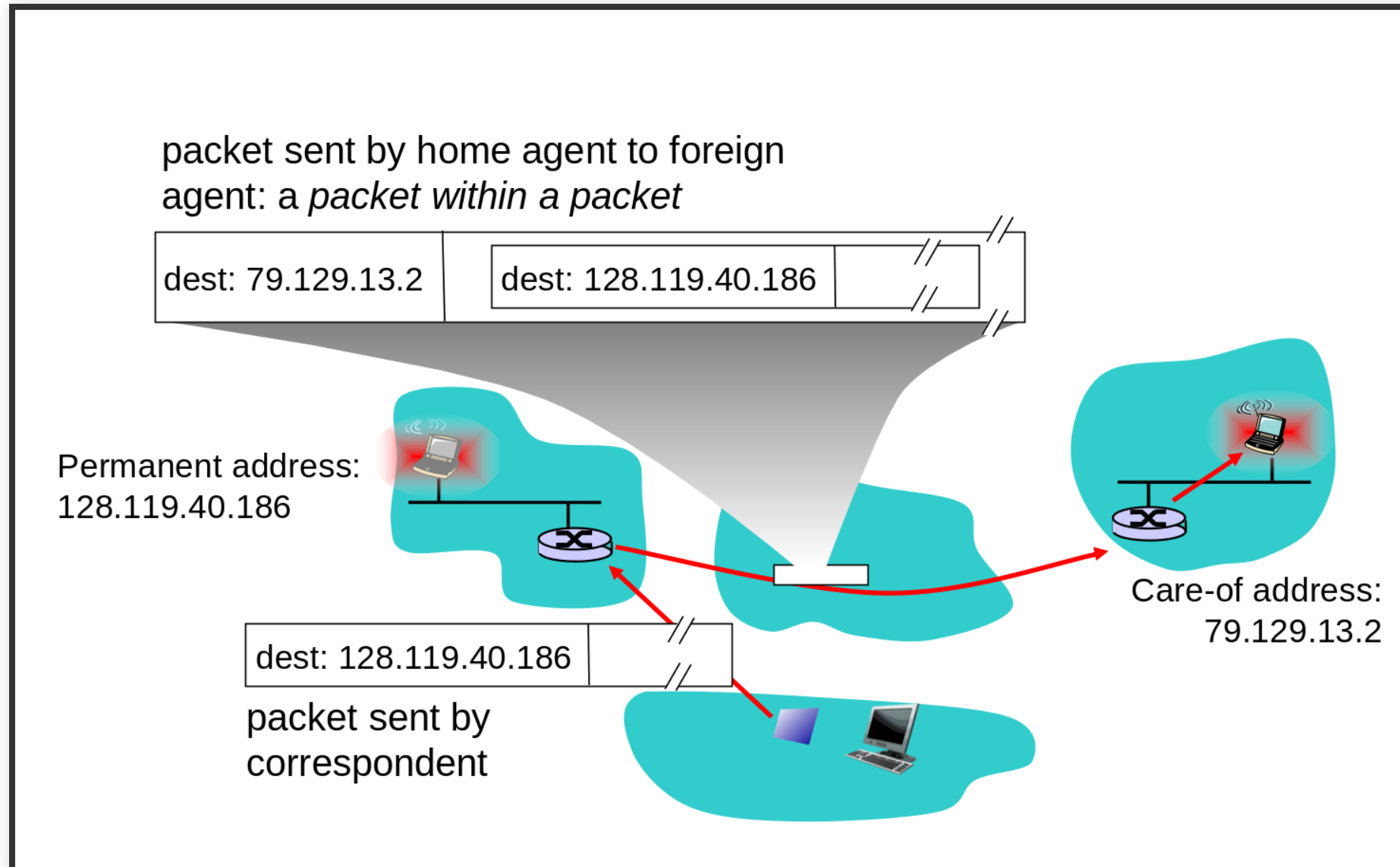
MOBILE IP - INDIRECT ROUTING



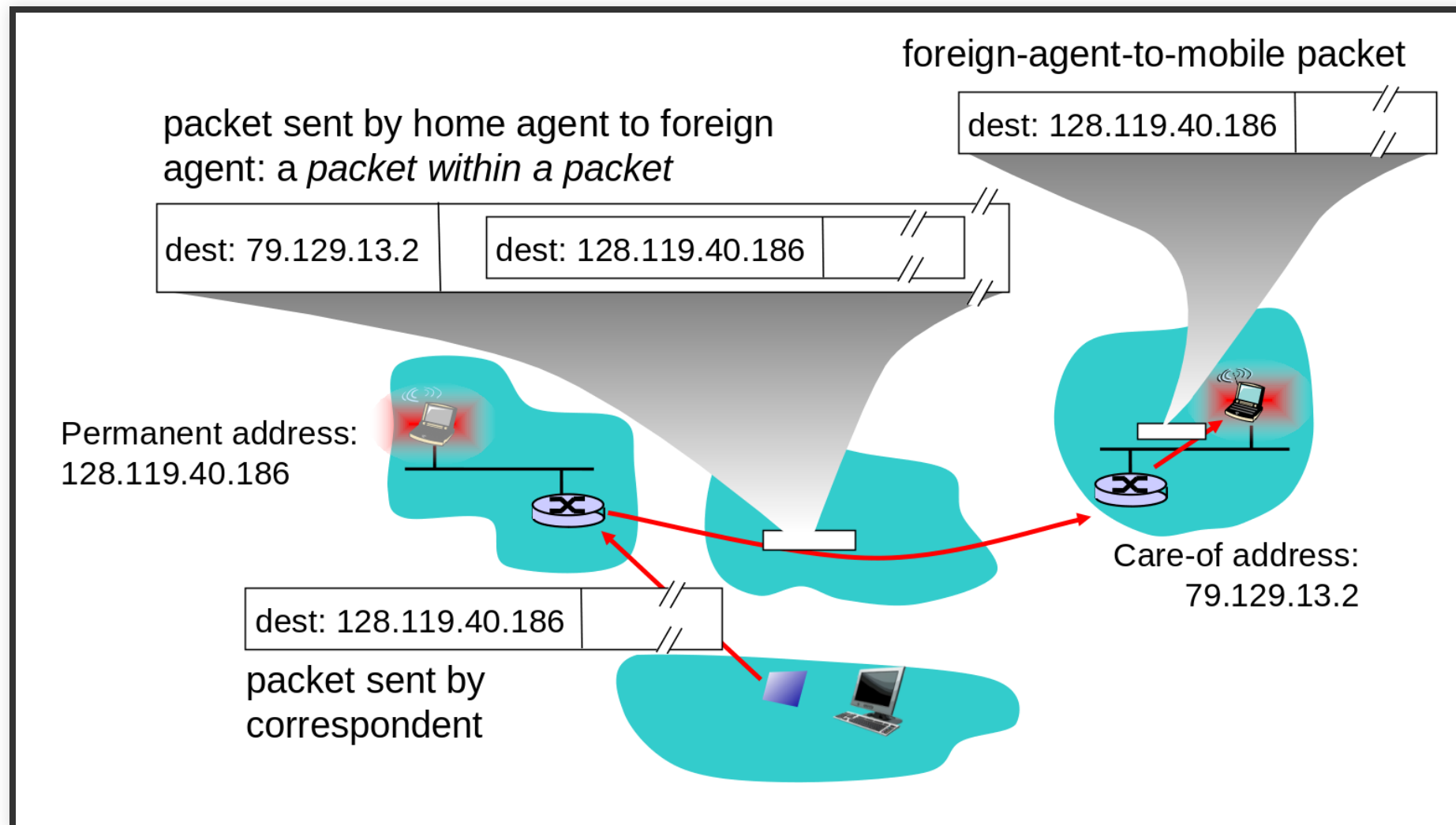
MOBILE IP - INDIRECT ROUTING



MOBILE IP - INDIRECT ROUTING



MOBILE IP - INDIRECT ROUTING



MOBILE IP AGENT DISCOVERY

Mobile node arriving to new network → must learn identity of corresponding foreign/home agent: **Agent discovery**

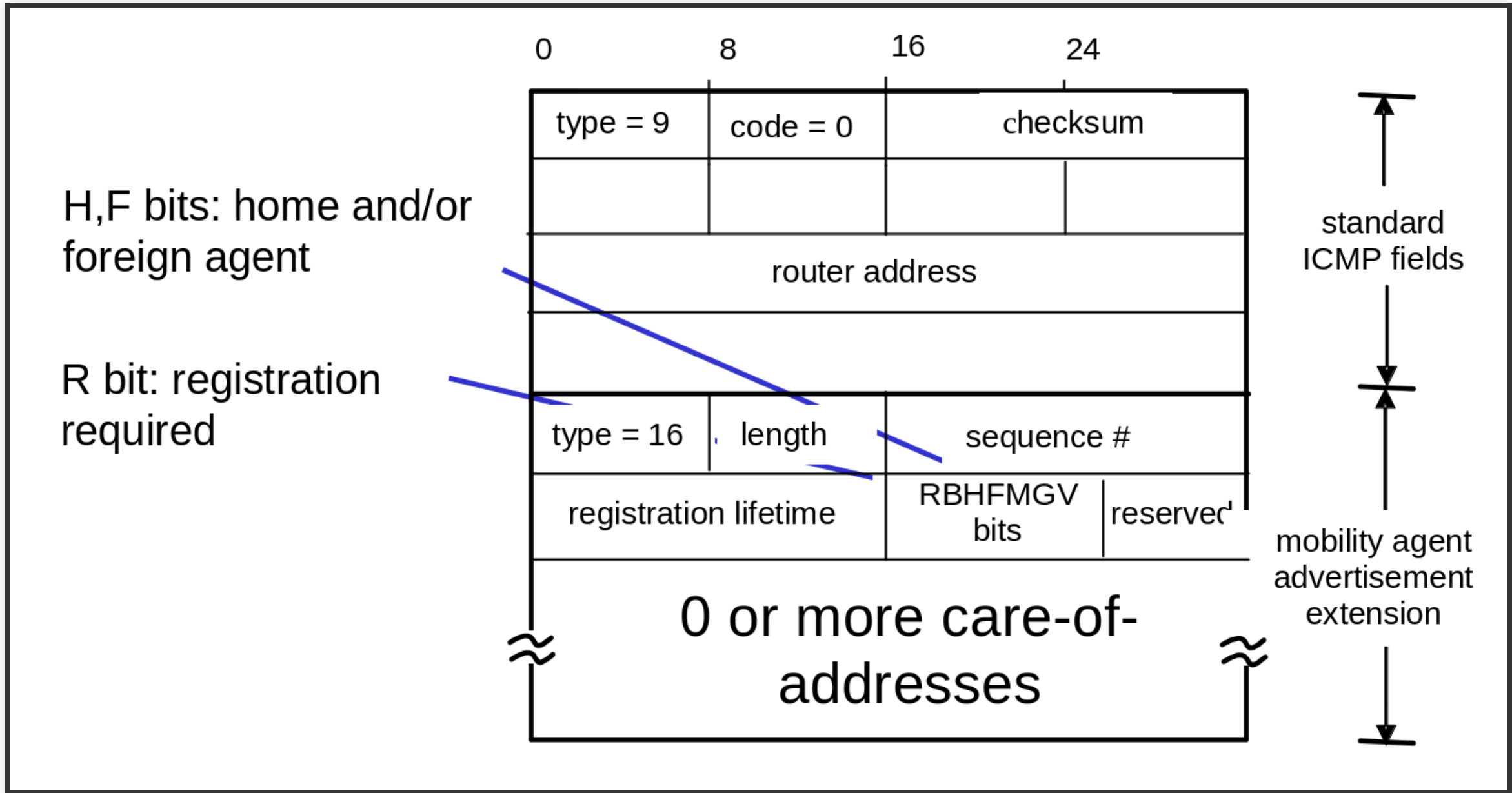
One of two ways

1. Agent advertisement
2. Agent solicitation

MOBILE IP AGENT ADVERTISEMENT

Agent advertisement: Foreign/home agents periodically advertise service by broadcasting ICMP messages (typefield = 9)

MOBILE IP AGENT ADVERTISEMENT



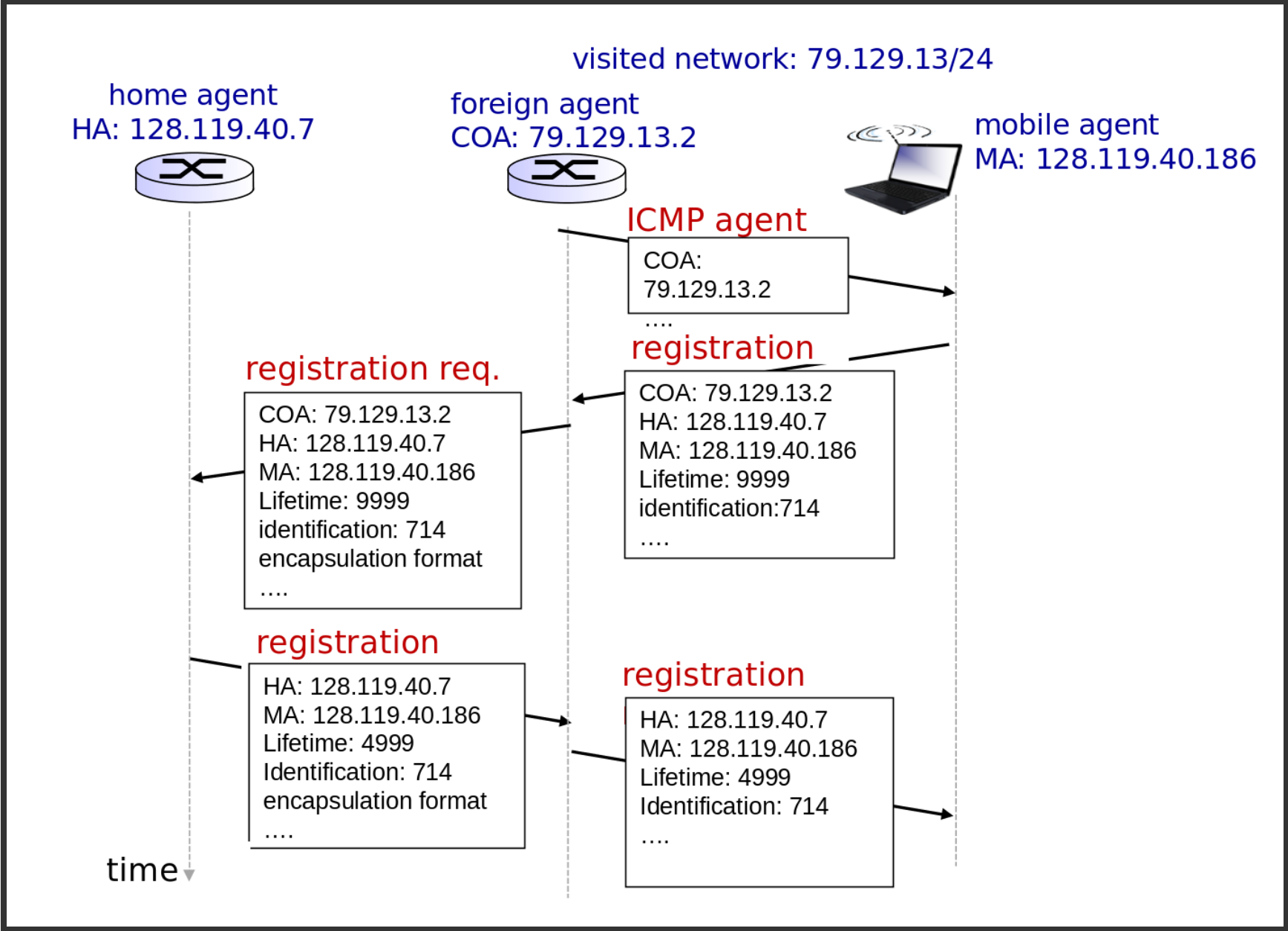
MOBILE IP AGENT SOLICITATION

If mobile user does not wish to way for advertisement: Broadcast
agent solicitation message.

This is a ICMP type 10 message.

Agent replies unicast → proceed as in advertisement.

AGENT ADVERTISEMENT AND REGISTRATION



SUMMARY

- Sharing a broadcast channel: multiple access
- Wireless links (capacity, distance)
- IEEE 802.11 ("Wi-Fi") incl CSMA/CA
- Mobility and addressing
- Mobile IP