Networks (2IRR20)

Wireless and Mobile (07)

Dr. Tanir Ozcelebi

TU/e Computer Science
Interconnected Resource-aware Intelligent Systems (IRIS)

Slides adapted from the textbook:
Computer Networking: A Top-Down Approach
8th edition, Global Edition by Jim Kurose, Keith Ross

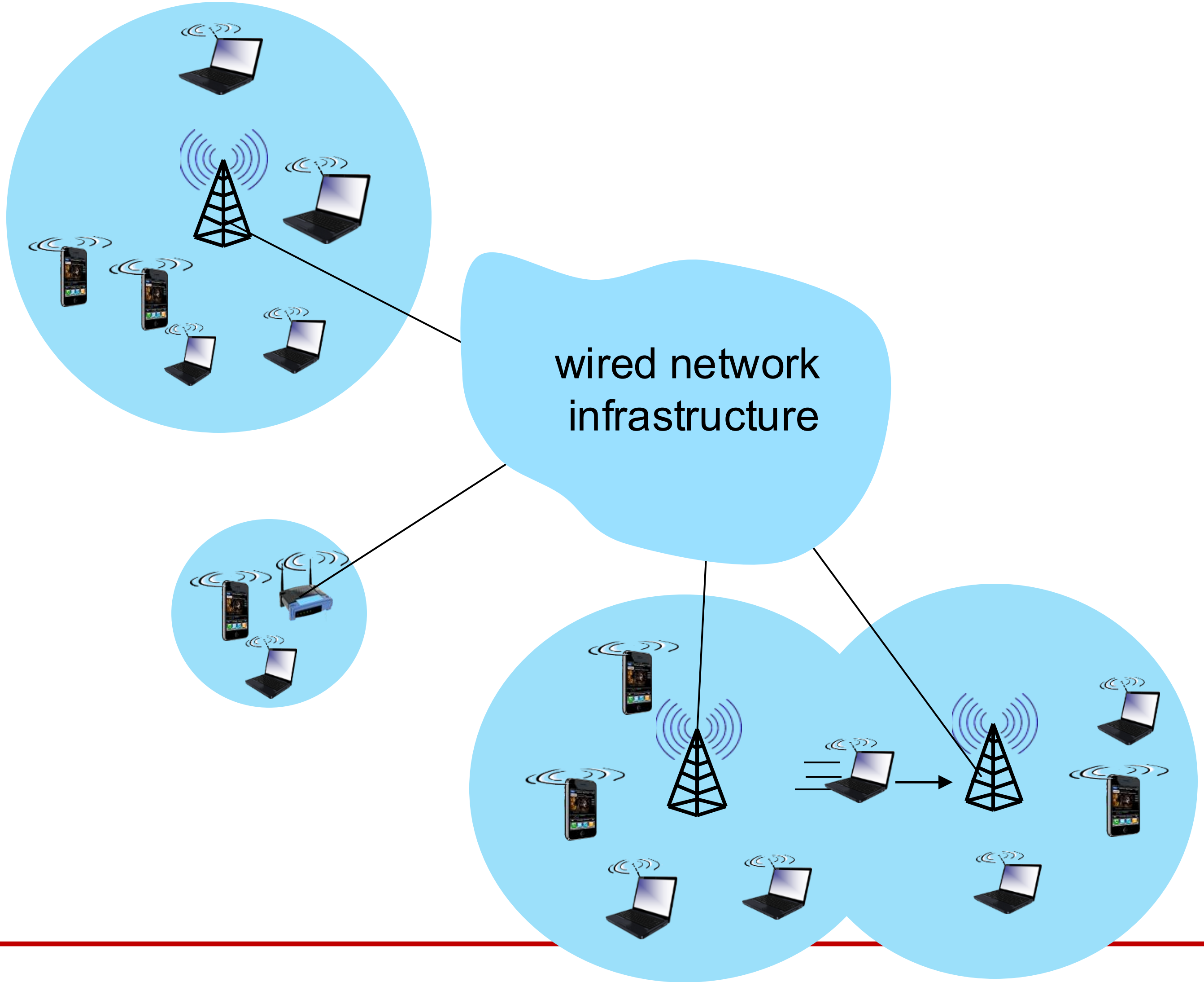
This slide set

- Wireless
  - Wireless Links and network characteristics
  - WiFi: 802.11 wireless LANs

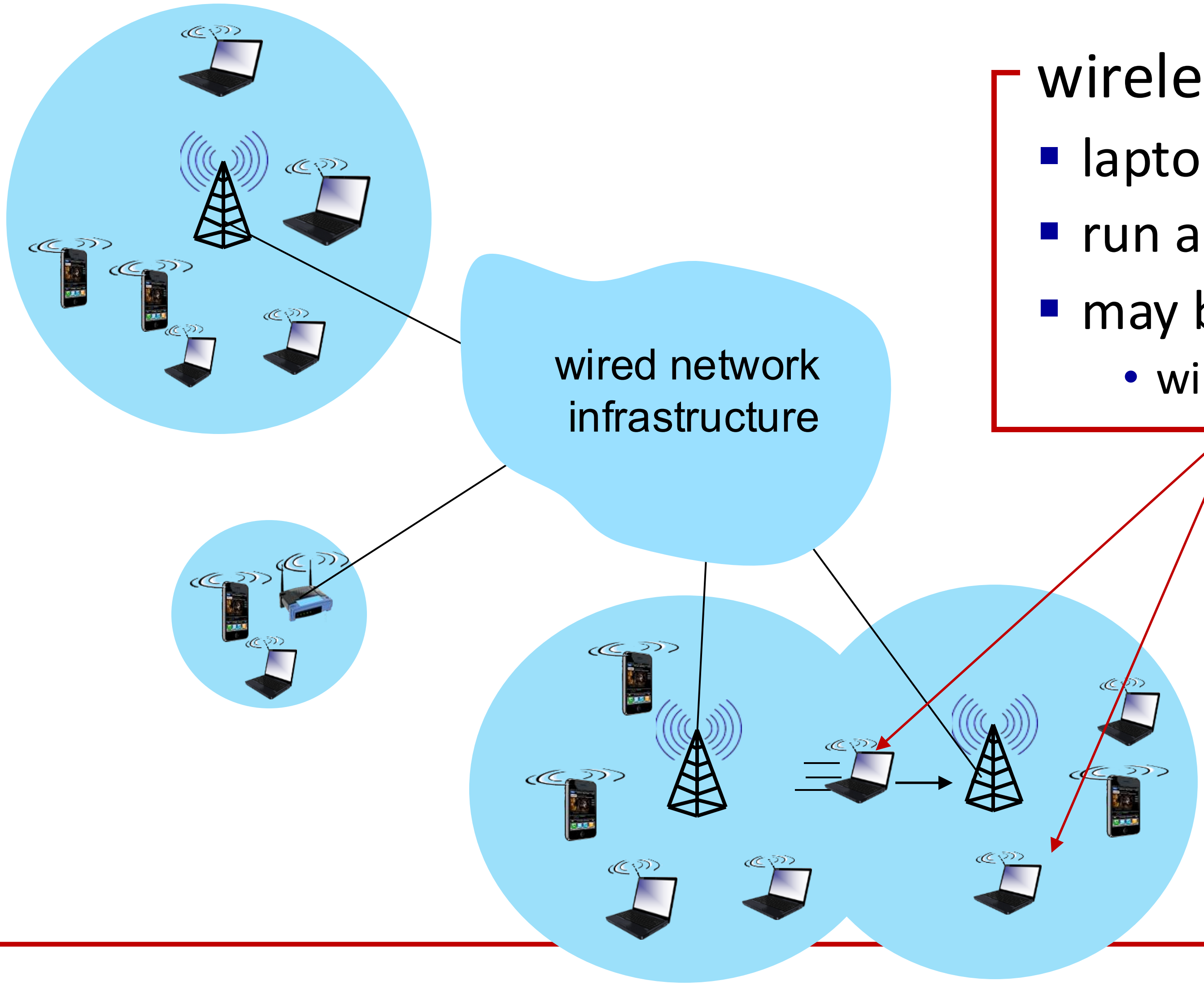
- Mobile
  - Mobility management
  - Mobile IP
  - Mobility: impact on higher-layer protocols

Introduction

Elements of a wireless network



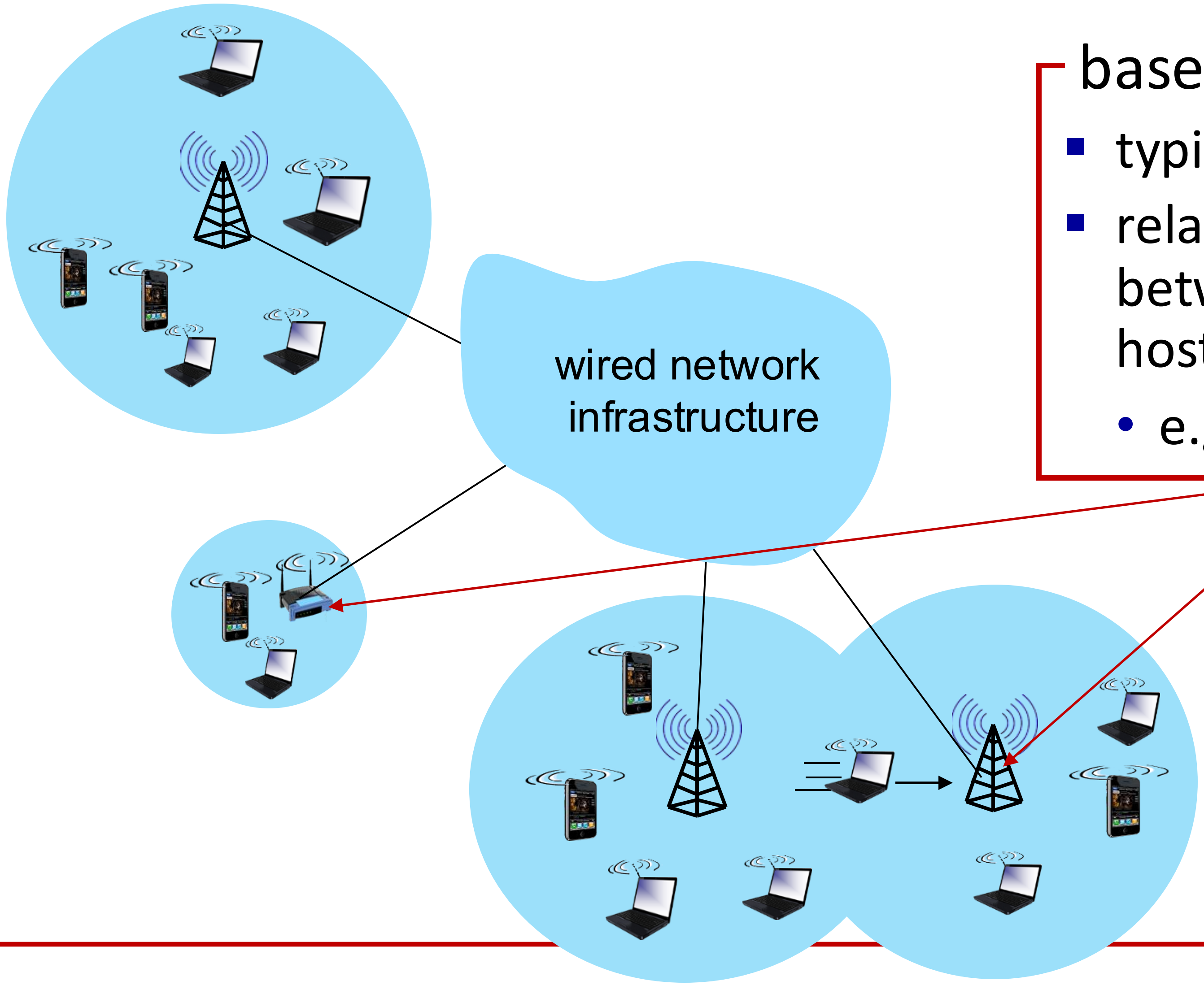
Elements of a wireless network



wireless hosts

- laptop, smartphone, IoT
- run applications
- may be stationary (non-mobile) or mobile
  - wireless does *not* always mean mobility!

Elements of a wireless network

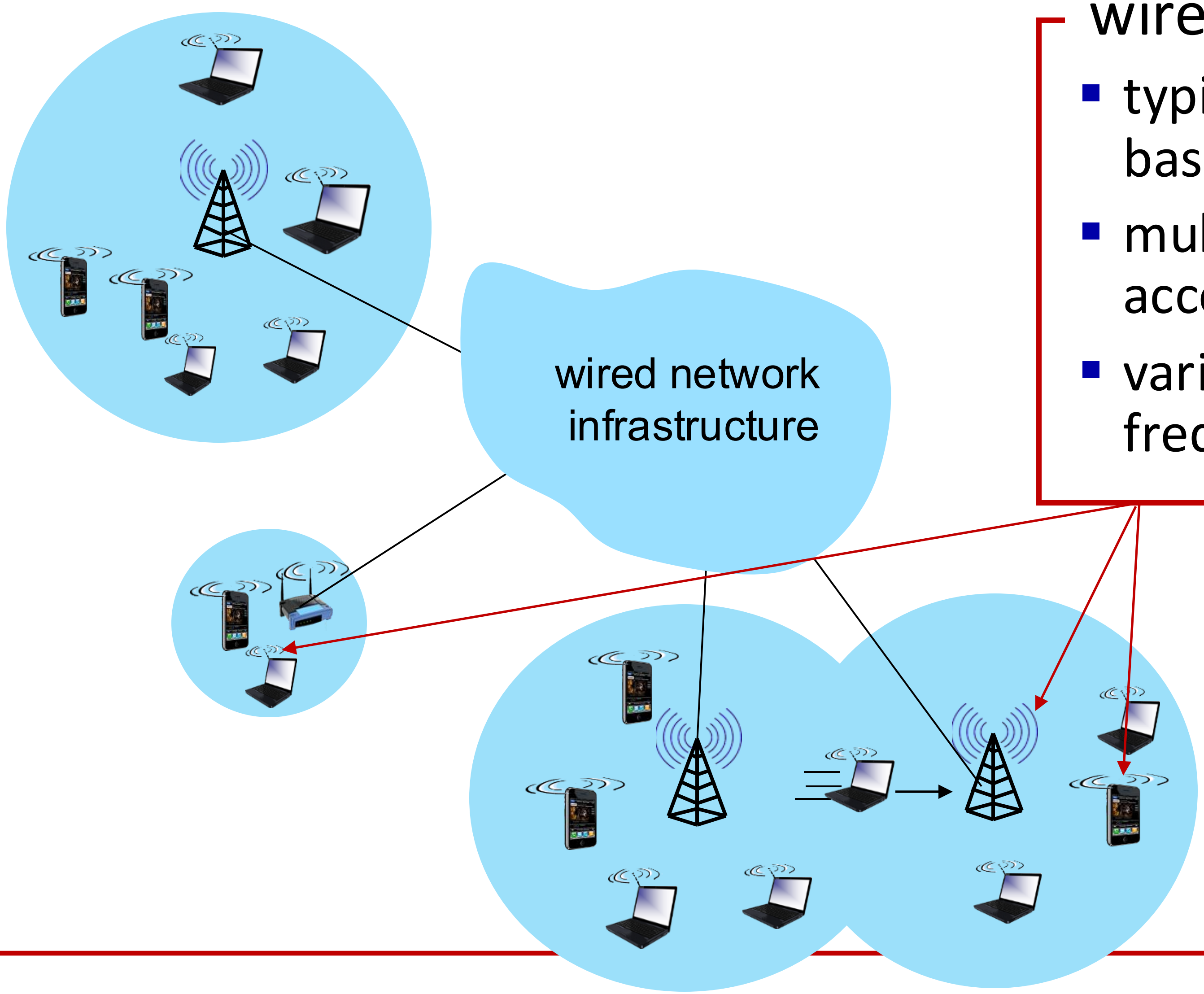


base station 

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its “area”
  - e.g., cell towers, 802.11 access points

Dr. Tanir Ozcelebi (t.ozcelebi@tue.nl)

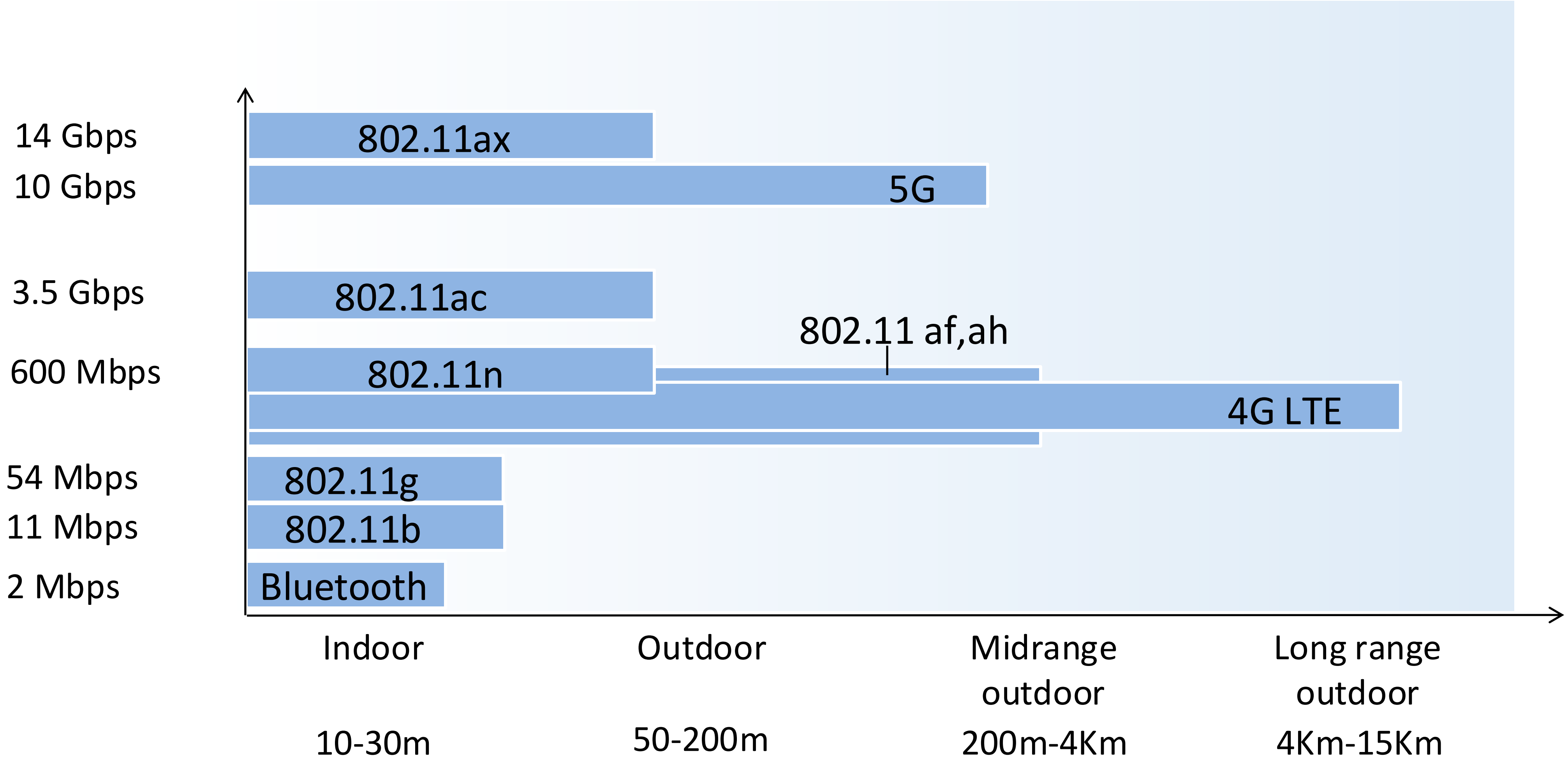
Elements of a wireless network



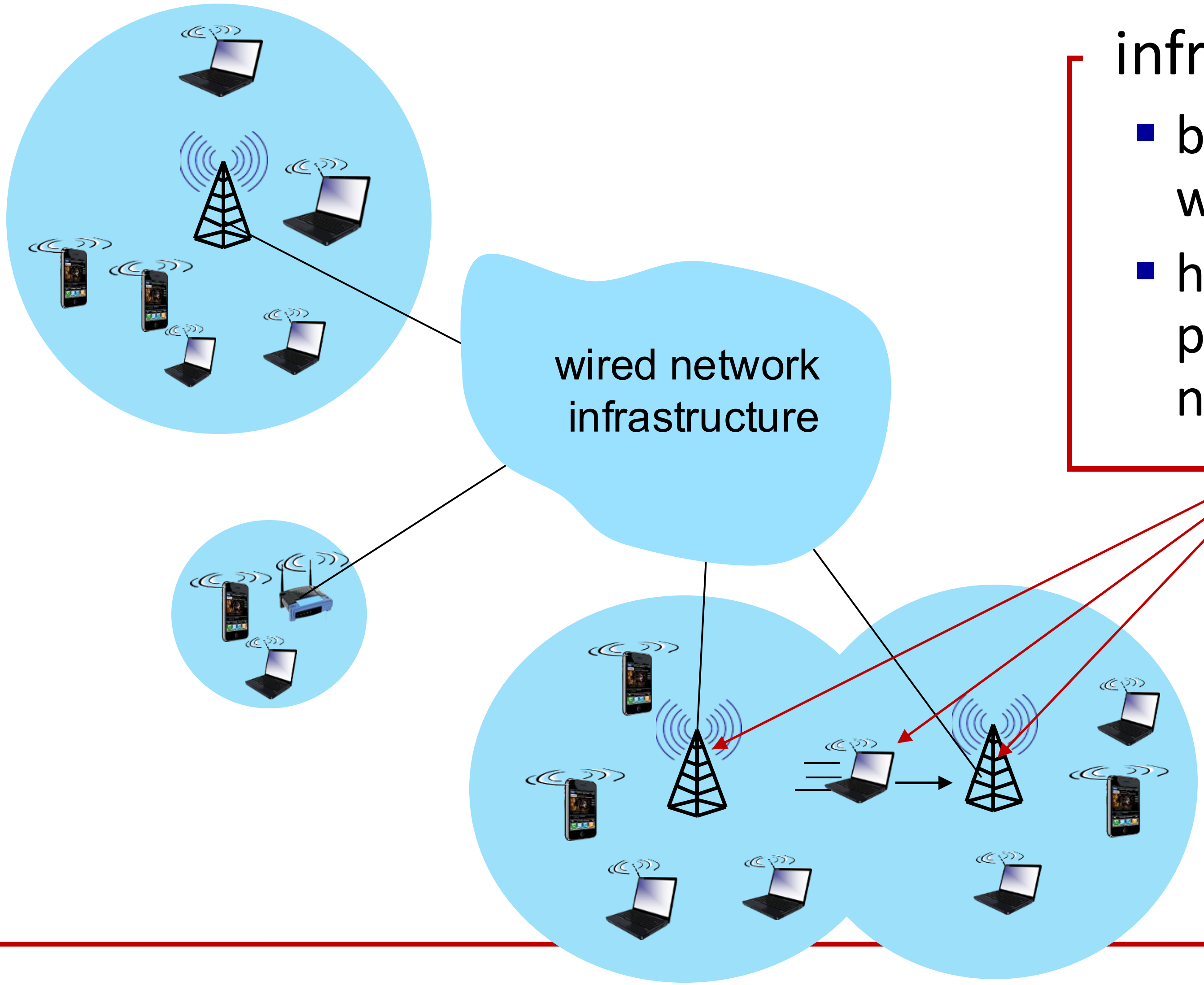
wireless link

- typically used to connect mobile(s) to base station, also used as backbone link
- multiple access protocol coordinates link access
- various transmission rates and distances, frequency bands

Characteristics of selected wireless links



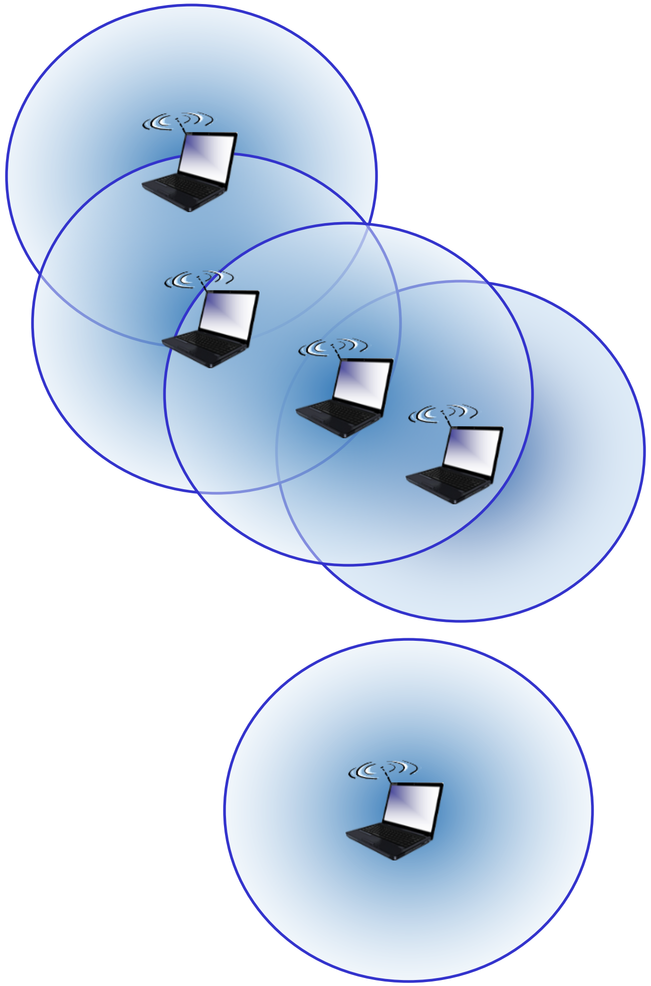
Elements of a wireless network



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network

Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless network taxonomy

	single hop	multiple hops
infrastructure (e.g., APs)	host connects to base station (WiFi, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: *mesh net*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Wireless links and network characteristics

Wireless link characteristics (1)

important differences from wired link ….

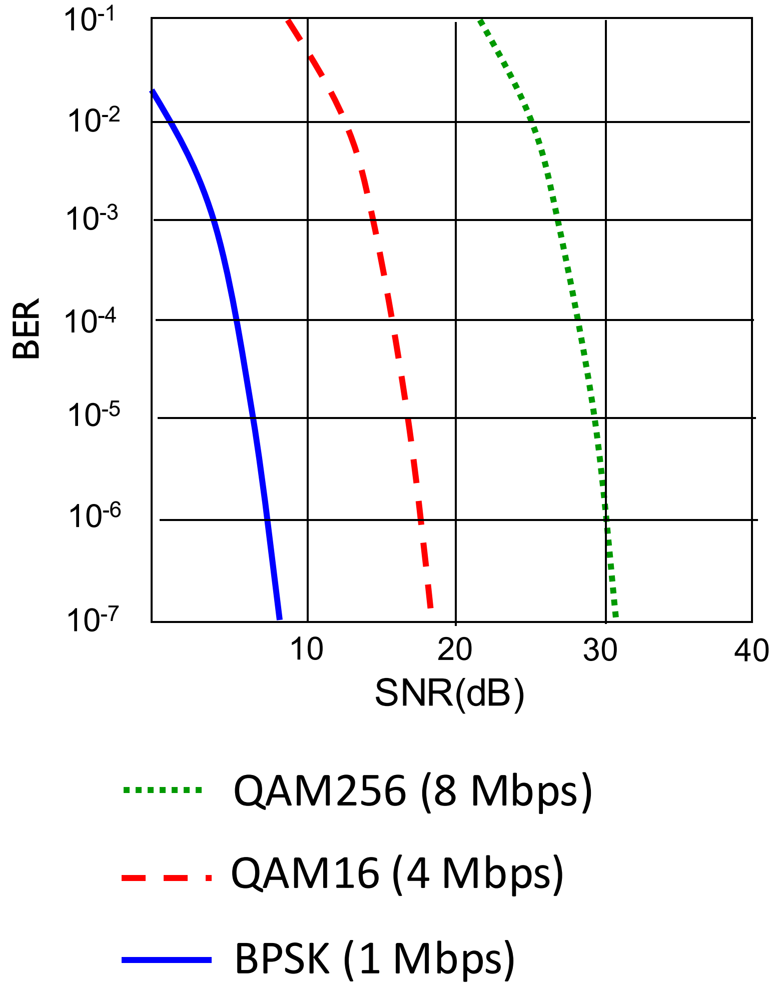
- decreased signal strength*:* radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: wireless network frequencies (e.g., 2.4 GHz) shared by many devices (e.g., WiFi, cellular, motors): interference
- multipath propagation: radio signal reflects off objects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

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

Wireless link characteristics (2)

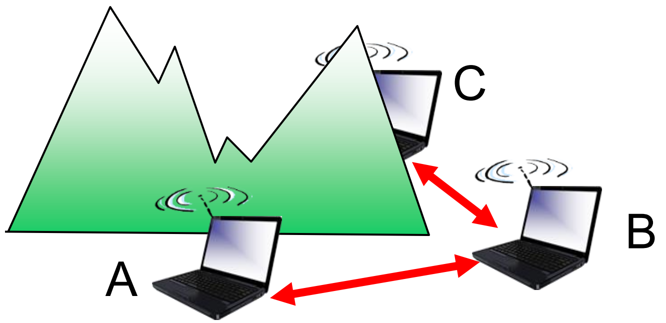
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a "good thing")

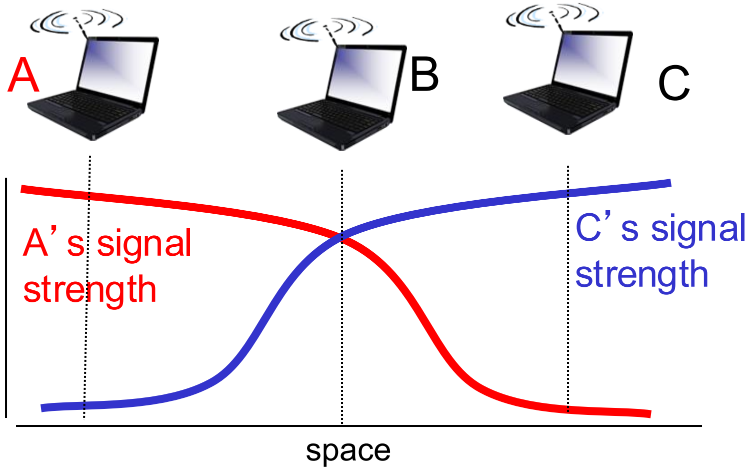
- SNR versus BER tradeoffs
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - *given SNR:* choose physical layer that meets BER requirement, giving highest throughput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



Wireless link characteristics (3)

Multiple wireless senders, 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

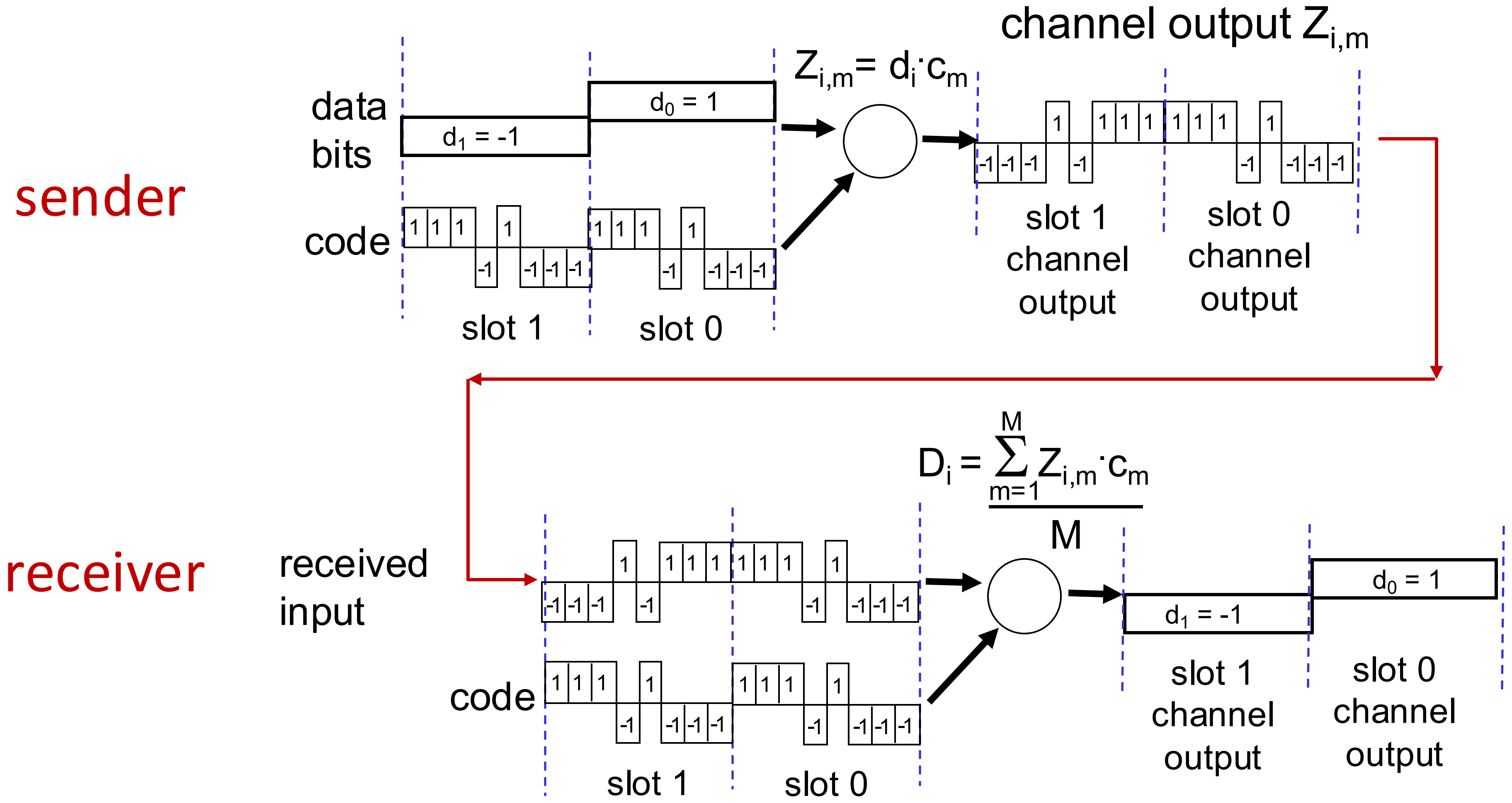
Signal attenuation:

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

Code Division Multiple Access (CDMA)

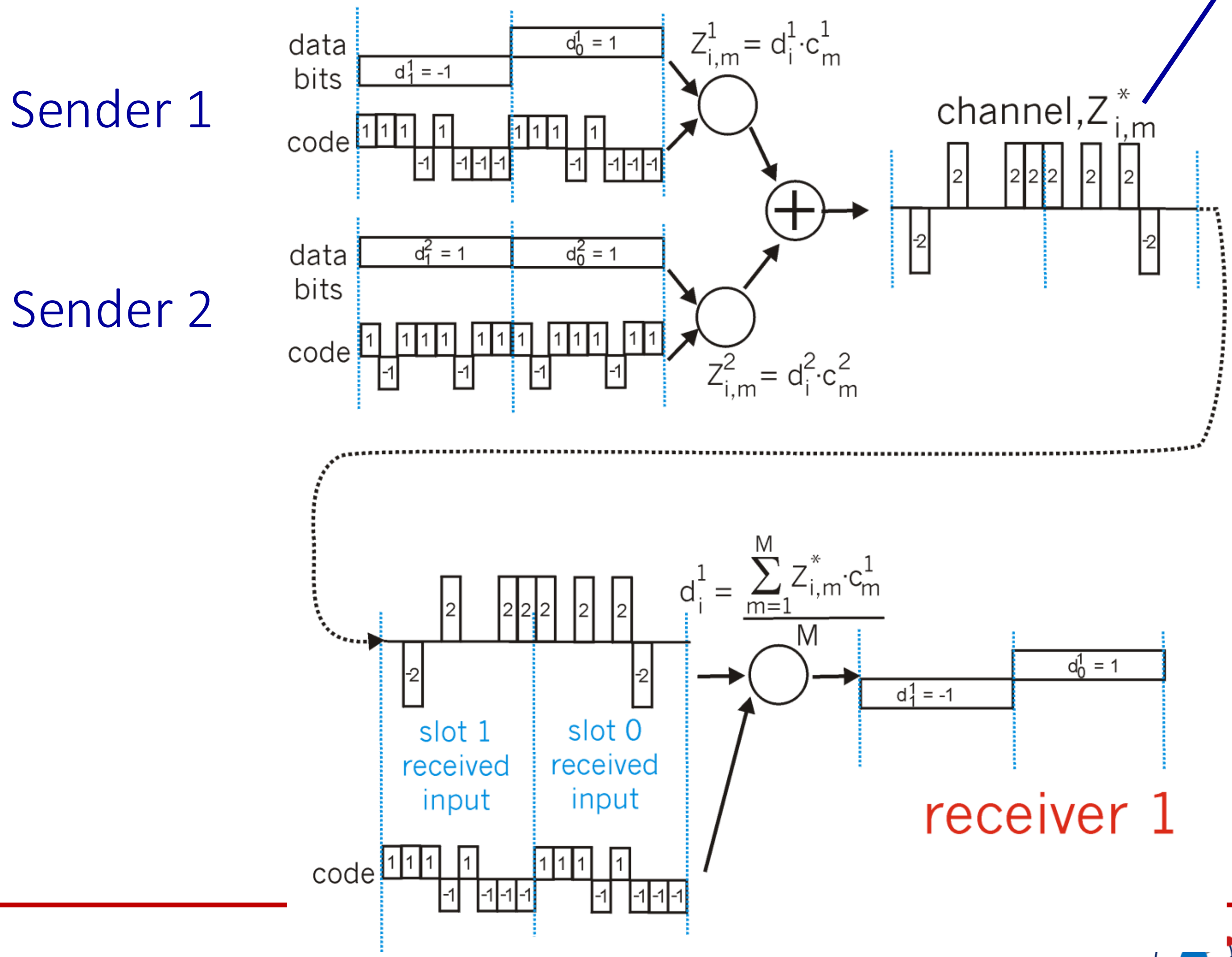
- unique “code” assigned to each user; i.e., code set partitioning
  - all users share same frequency, but each user has own “chipping” sequence (i.e., code) to encode data
  - allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)
- encoding: inner product: (original data) X (chipping sequence)
- decoding: summed inner-product: (encoded data) X (chipping sequence)

CDMA encode/decode



... but this isn't really useful yet!

CDMA: two-sender interference



channel sums together transmissions by sender 1 and 2

using same code as sender 1, receiver recovers sender 1's original data from summed channel data!

… now *that's* useful!

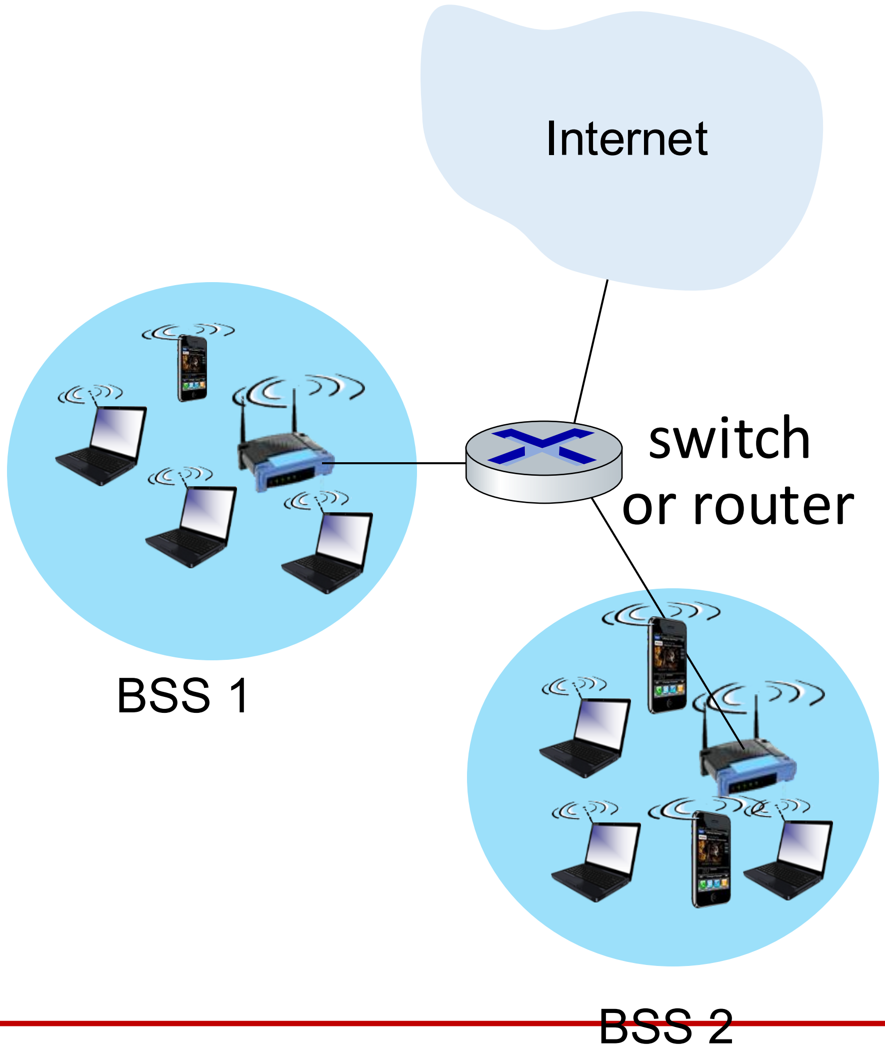
WiFi: 802.11 wireless LANs

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
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz
802.11ax (WiFi 6)	2020	14 Gbps	70m	2.4, 5 Ghz
802.11be (Wifi 7)	2024 (exp)	23 Gbps	70m	2.4, 5 , 6 Ghz
802.11bn (Wifi 8)	2028 (exp)	100 Gbps	70m	2.4, 5, 6 Ghz

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

802.11 LAN architecture



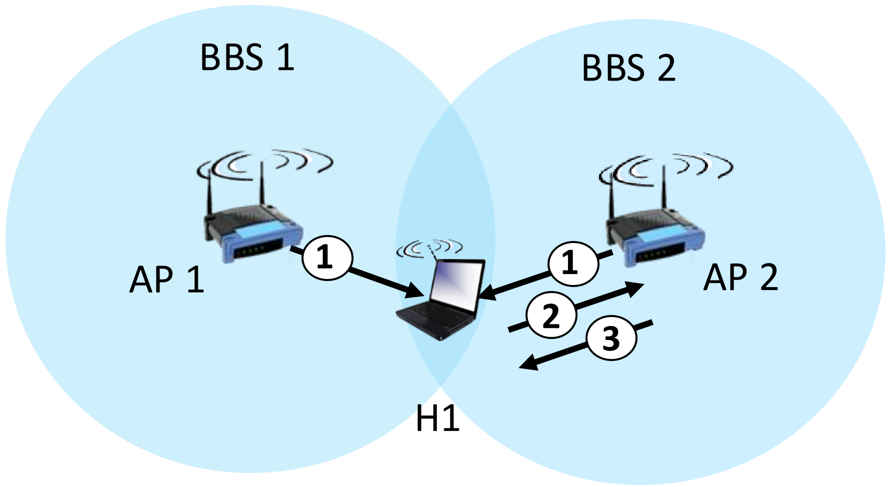
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

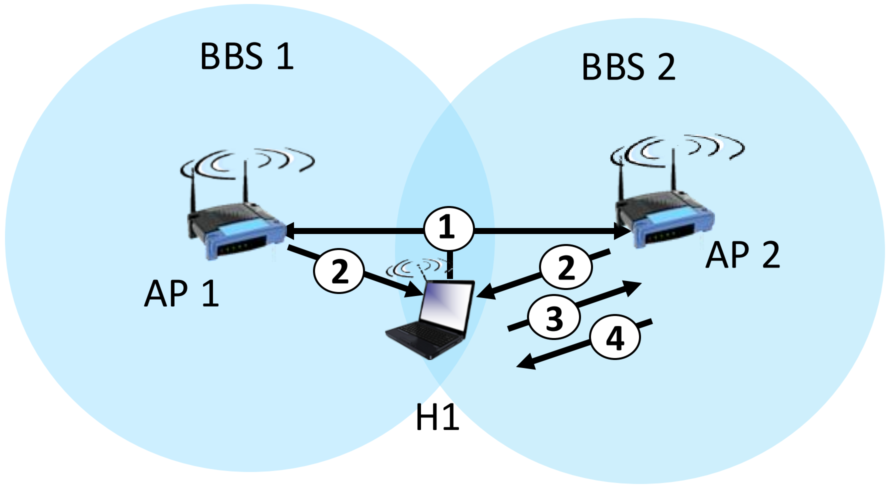
802.11: Channels, association

- 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 AP's name (SSID) and MAC address
  - selects AP to associate with
  - then may perform authentication [Chapter 8]
  - then typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning





passive scanning:

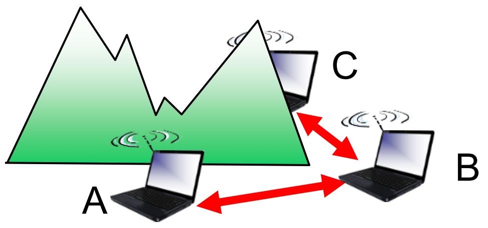
(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

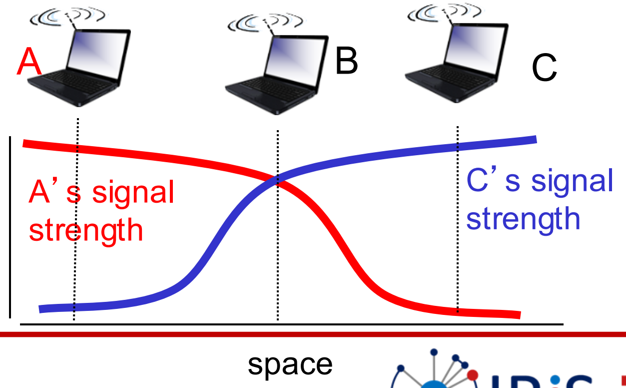
active scanning:

(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: 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/<u>C</u>ollision<u>A</u>voidance



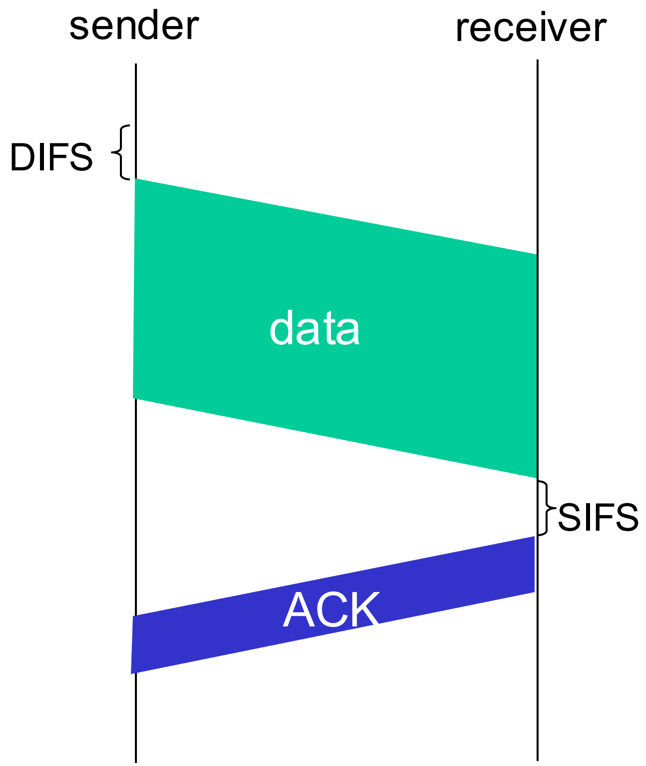


IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

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

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



802.11 receiver

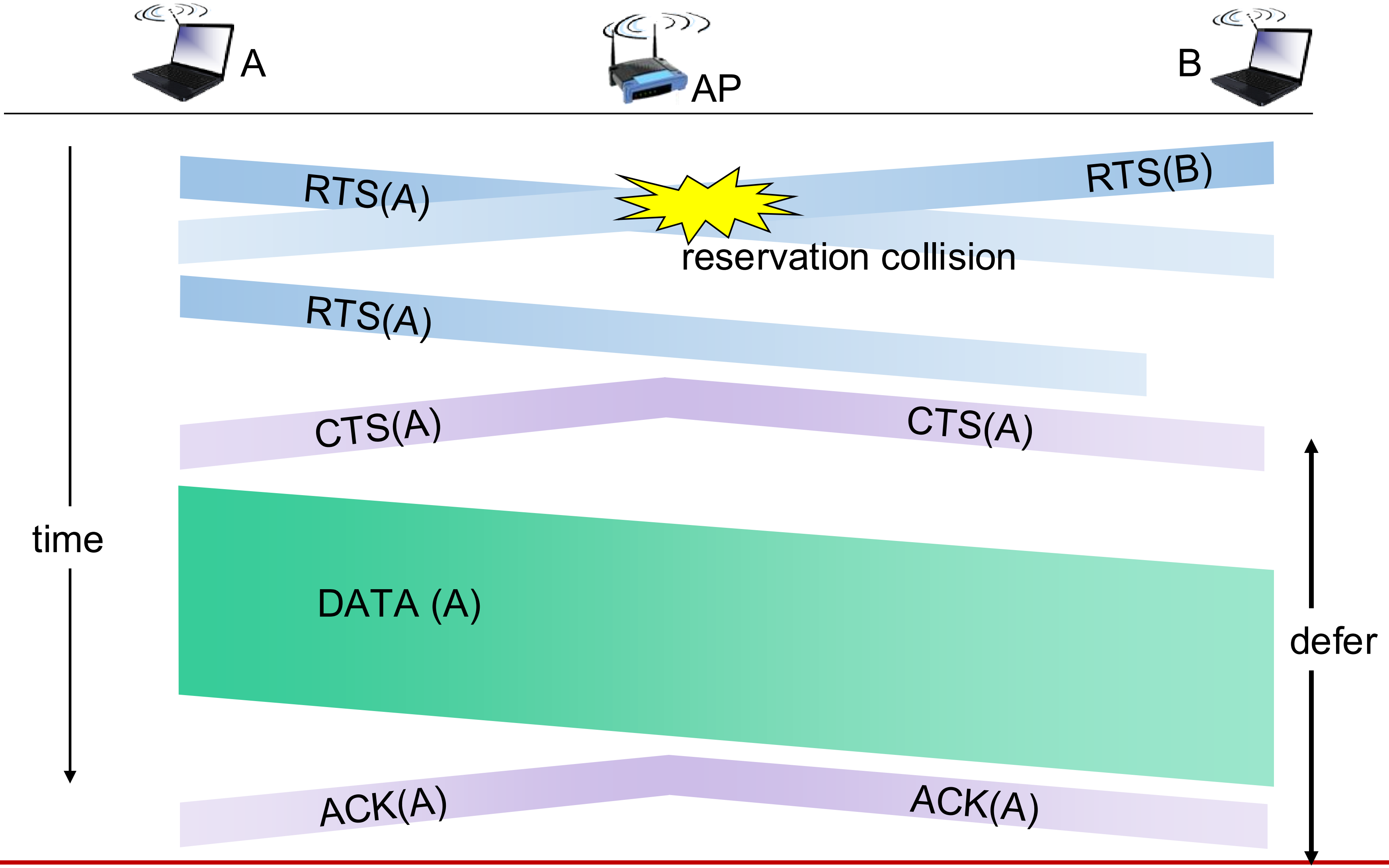
if frame received OK
  return ACK after **SIFS** (ACK needed due to hidden terminal problem)

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 frame: addressing

2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

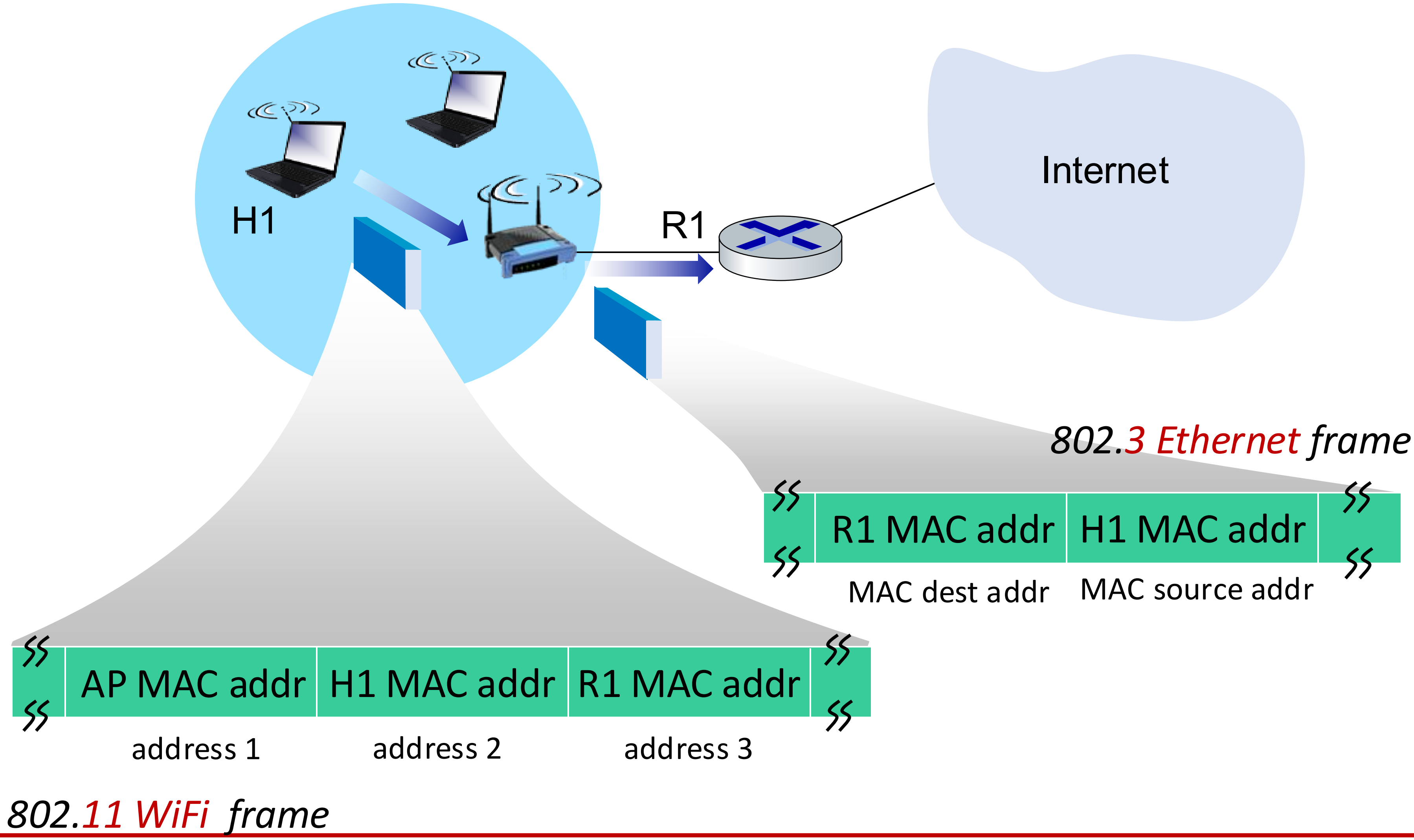
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing



802.11 frame: addressing

duration of reserved transmission time (RTS/CTS)

frame sequence # (for reliable data transfer)

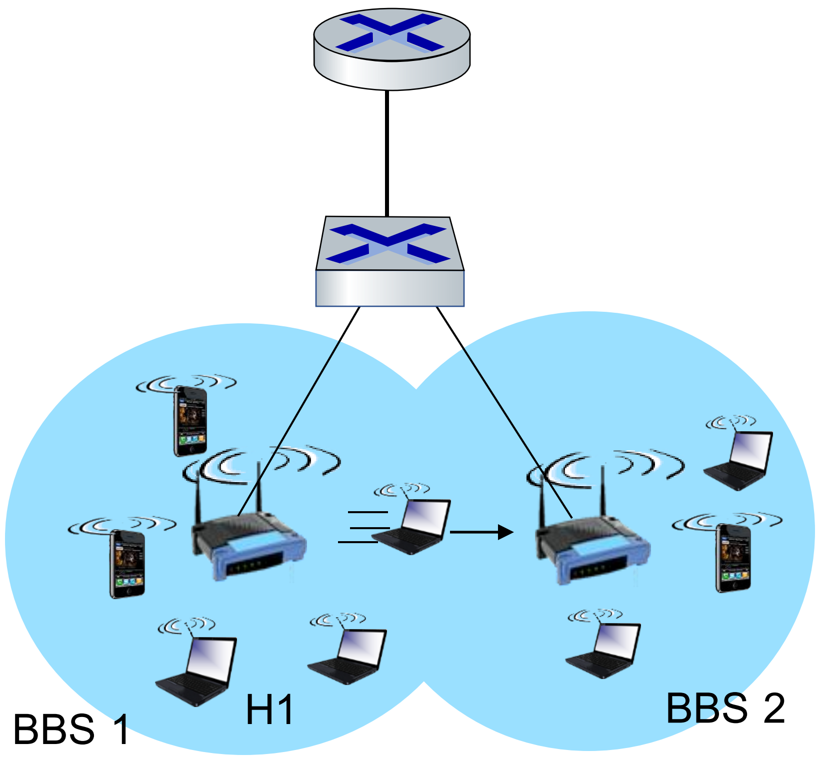
2	2	6	6	6	2	6	0 - 2312	4
frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC

2	2	4	1	1	1	1	1	1	1	1
protocol version	type	subtype	to AP	from AP	more frag	retry	power mgt	more data	WEP	rsvd

frame type (RTS, CTS, ACK, data)

802.11: mobility within same subnet

- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - Low mobility: Self-learning will do the job → switch will see frame from H1 and "learn again" which switch port can be used to reach H1.
  - High mobility: We need more → New AP could broadcast a frame with source address MAC_{H1}.



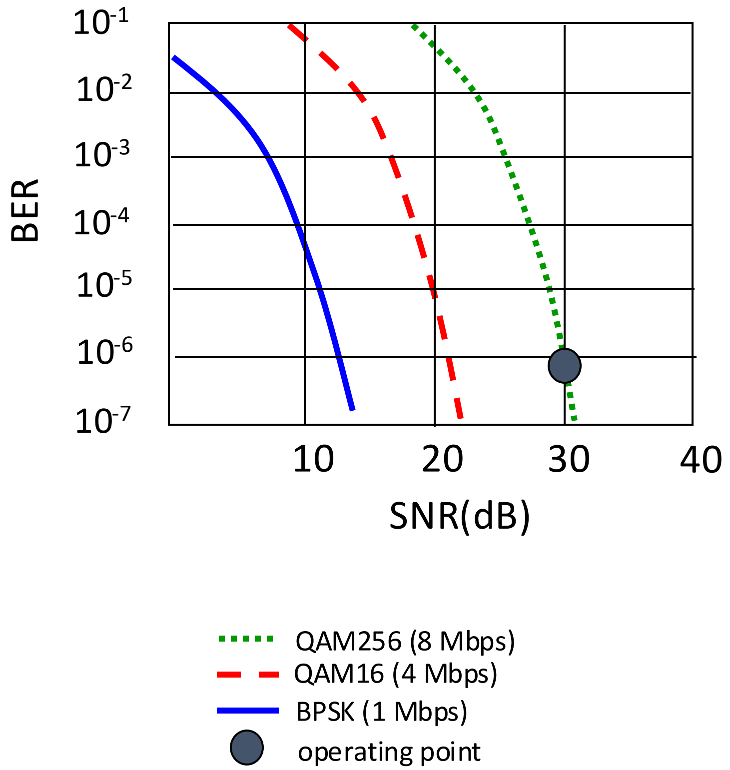
802.11: advanced capabilities

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 lower transmission rate to reduce BER



802.11: advanced capabilities

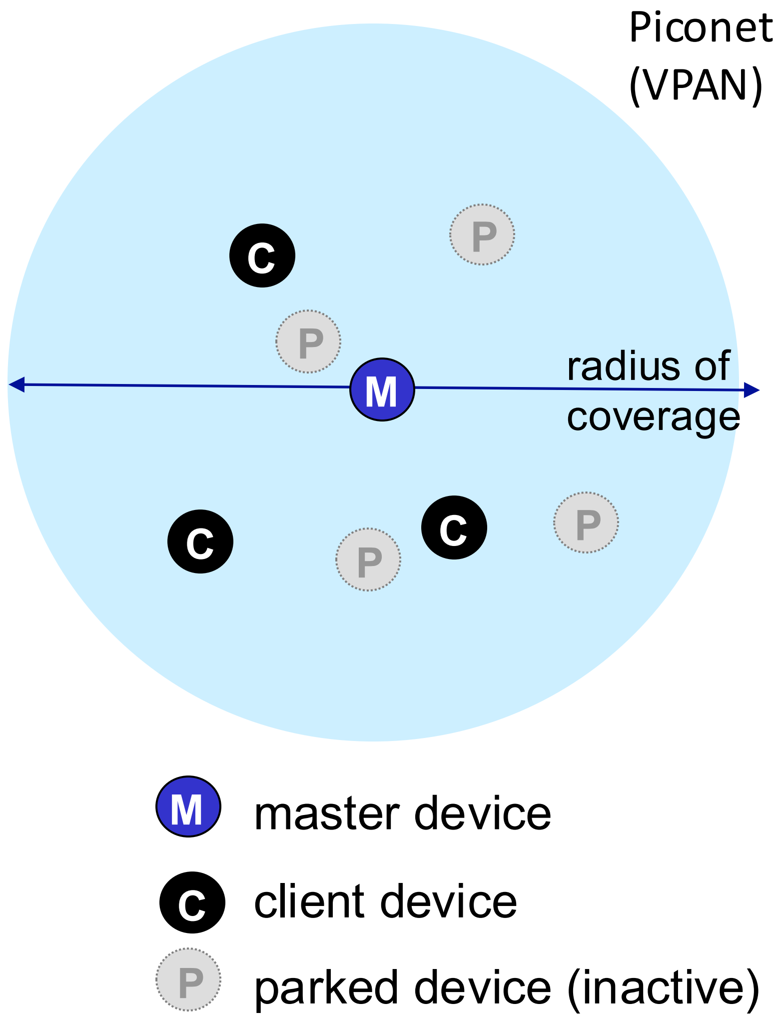
power management

- 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** (~every 100ms)

- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames are to be sent; otherwise sleep again until next beacon frame (asleep 99% of the time!)

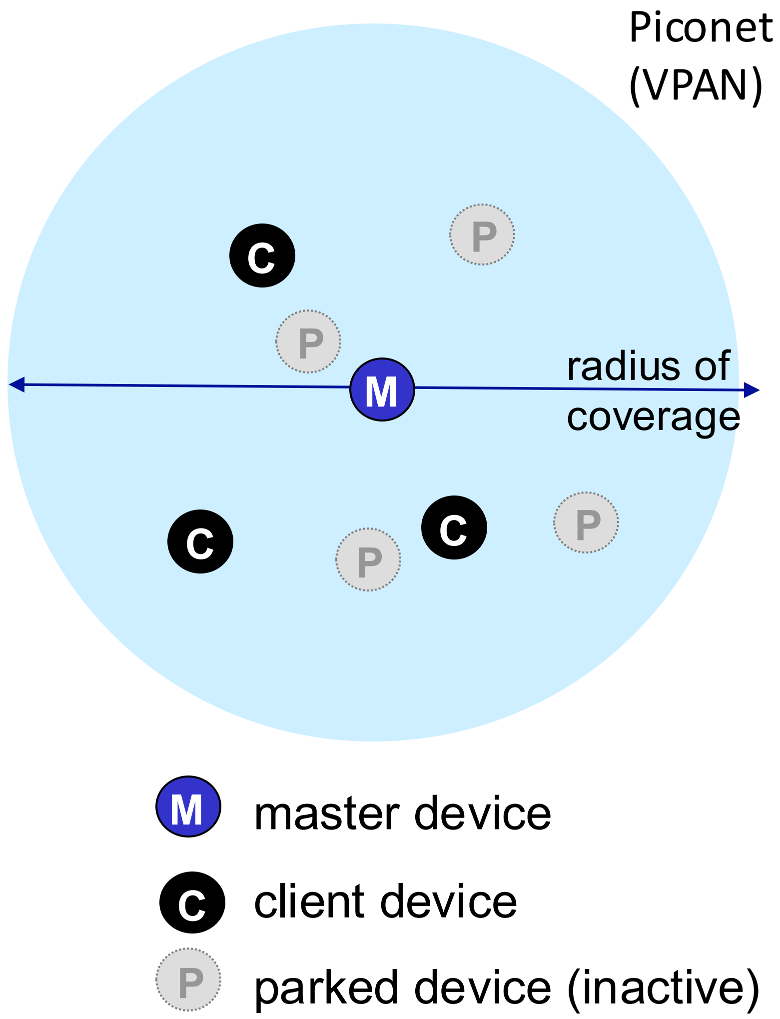
Personal area networks: Bluetooth

- less than 10 m diameter
  - max 8 active nodes
    plus some “parked” (sleeping) ones
- 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
  - master determines which nodes are active, their clocks, the frequency sequence to use etc etc.



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 (VPAN) only interfere in some slots
- parked mode: clients can "go to sleep" (park) and later wakeup (to preserve battery) → master determines



Mobility management

What is mobility?

- spectrum of mobility, from the network perspective:

no mobility — high mobility

device moves between networks, but powers down while moving

device moves within same AP in one provider network

device moves among APs in one provider network

device moves among multiple provider networks, while maintaining ongoing connections

We're interested in these!

Mobility approaches

- let network (routers) handle it:
  - routers advertise well-known name, address (e.g., permanent 32-bit IP address), or number (e.g., cell #) of visiting mobile node via usual routing table exchange.
  - Internet routing could do this already *with no* changes! Routing tables can indicate where each mobile is located via longest prefix match!

Mobility approaches

- let network (routers) handle it:
  - routers advertise well-known … ess (e.g., permanent 32-bit IP address), or number (e.g., ce… mobile node via usual routing table exchange
  - Internet routing could do thi… *no* changes! Routing tables can indicate where each mobile is lo… a longest prefix match!

not scalable to billions of mobiles

- let end-systems handle it: functionality at the "edge"
  - *indirect routing:* communication from correspondent to mobile goes through mobile's home network, then forwarded to remote mobile
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Contacting a mobile friend:

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

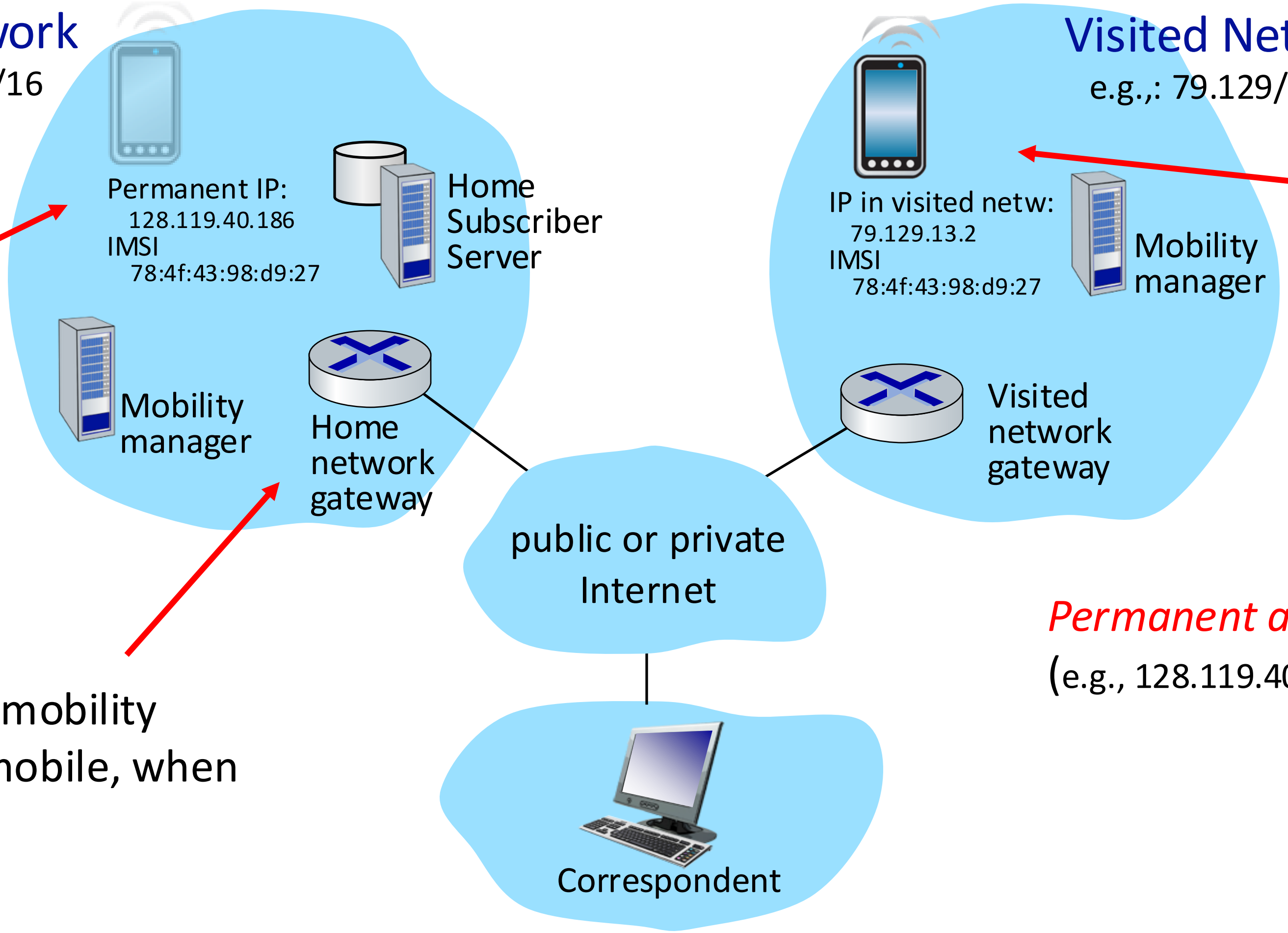
- search all phone books?
- expect her to let you know where he/she is?
- call his/her parents?
- social media!

The importance of having a "home":

- a definitive source of information about you
- a place where people can find out where you are

Home network, visited network: general IP

[permanent "home" of mobile]



Permanent address: address in home network, *can always* be used to reach mobile.

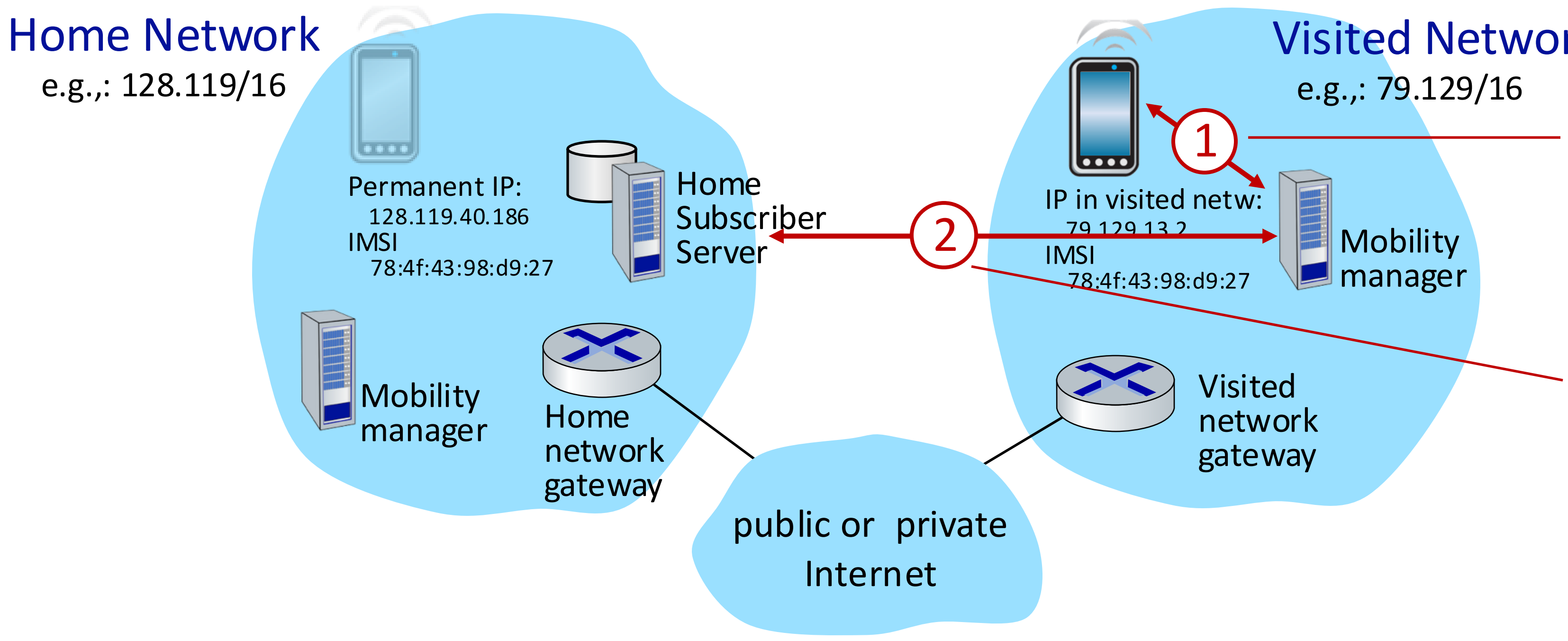
entity that will perform mobility functions on behalf of mobile, when mobile is remote

Address in visited network.
(e.g., 79.129.13.2)

Known as care-of-address (CoA) in mobile IP.

Permanent address: remains constant
(e.g., 128.119.40.186)

Registration: home needs to know where you are!



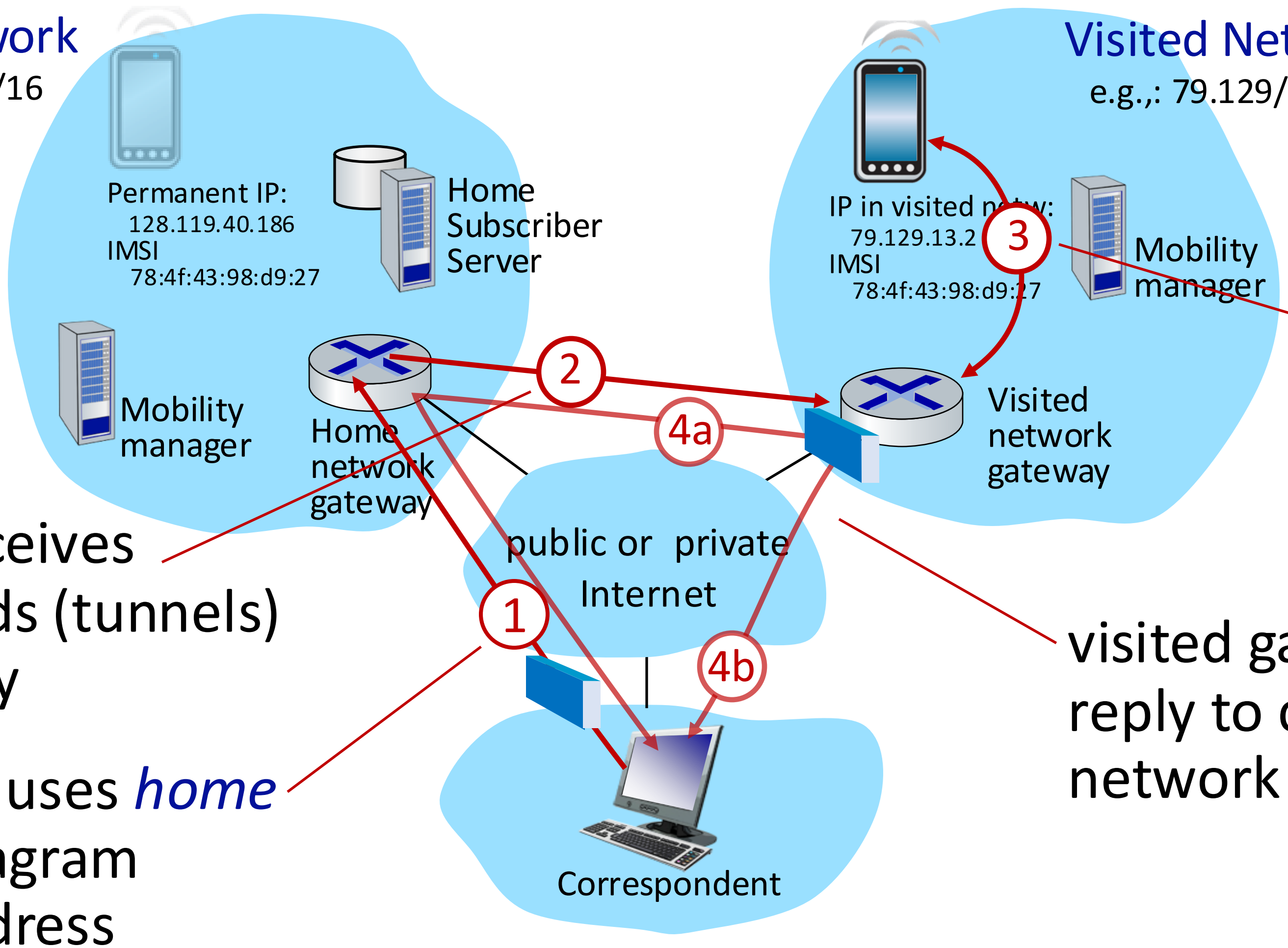
mobile *associates* with visited mobility manager

visited mobility manager *registers* mobile's location with home HSS

end result:

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

Mobility with indirect routing



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

correspondent uses *home* address as datagram destination address

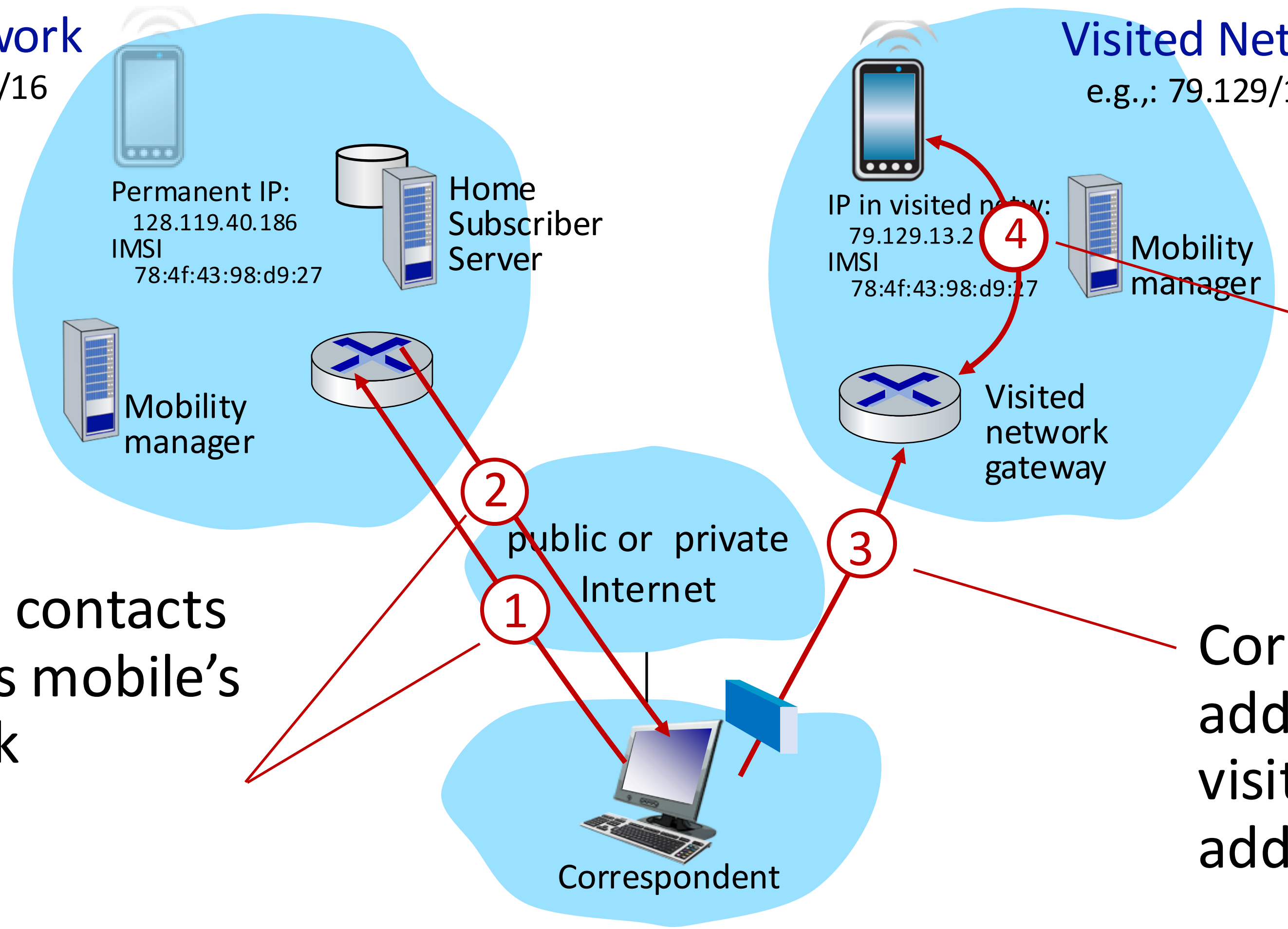
visited gateway router forwards to mobile

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

Mobility with indirect routing: comments

- triangle routing:
  - inefficient when correspondent and mobile are in same network
- mobile moves among visited networks: transparent to correspondent!
  - registers in new visited network
  - new visited network registers with home HSS
  - datagrams continue to be forwarded from home network to mobile in new network
  - *on-going (e.g., TCP) connections between correspondent and mobile can be maintained!*

Mobility with direct routing



visited gateway router forwards to mobile

correspondent contacts *home* HSS, gets mobile's visited network

Correspondent addresses datagram to visited network address

Mobility with direct routing: comments

- overcomes triangle routing inefficiencies
- *non-transparent to correspondent:* correspondent must get care-of-address from home agent
- what if mobile changes visited network?
  - can be handled, but with additional complexity

Mobile IP

- mobile IP architecture standardized ~20 years ago [RFC 5944]
  - did not see wide deployment/use
  - perhaps WiFi for Internet, and 2G/3G phones for voice were "good enough" at the time

- mobile IP architecture:
  - indirect routing to node (via home network) using tunnels
  - mobile IP home agent: combined roles of 4G HSS and home P-GW
  - mobile IP foreign agent: combined roles of 4G MME and S-GW
  - protocols for agent discovery in visited network, registration of visited location in home network via ICMP extensions

Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- … but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handover loss
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - bandwidth a scare resource for wireless links