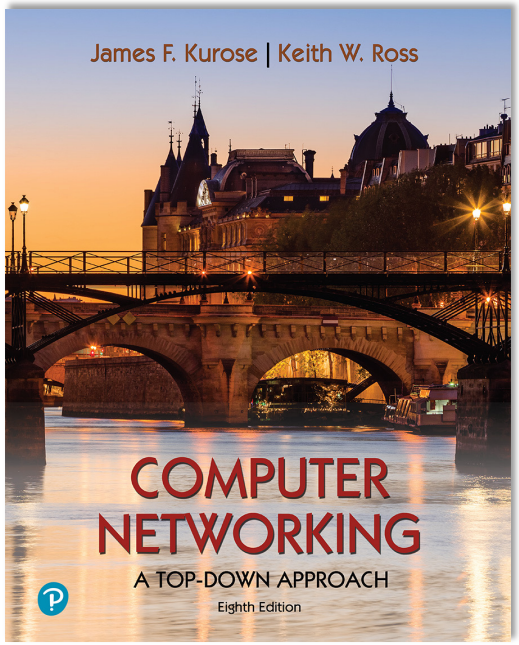
Chapter 7
Wireless (and Mobile) Networks

A note on the use of these PowerPoint slides:
We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Adapted, pmc, 2025.



Computer Networking: A Top-Down Approach
8th edition
Jim Kurose, Keith Ross
Pearson, 2020

Chapter 7 outline

- Introduction

Wireless

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

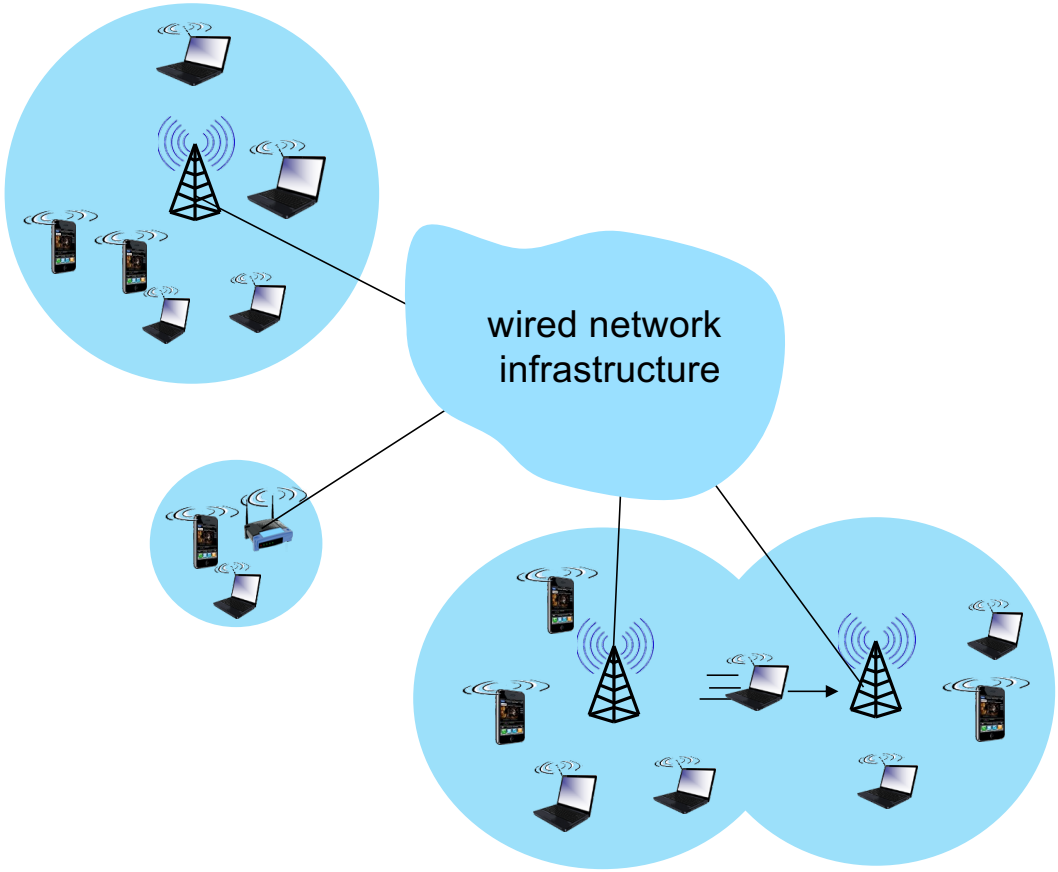
(not covered in RC)

- Cellular networks: 4G and 5G

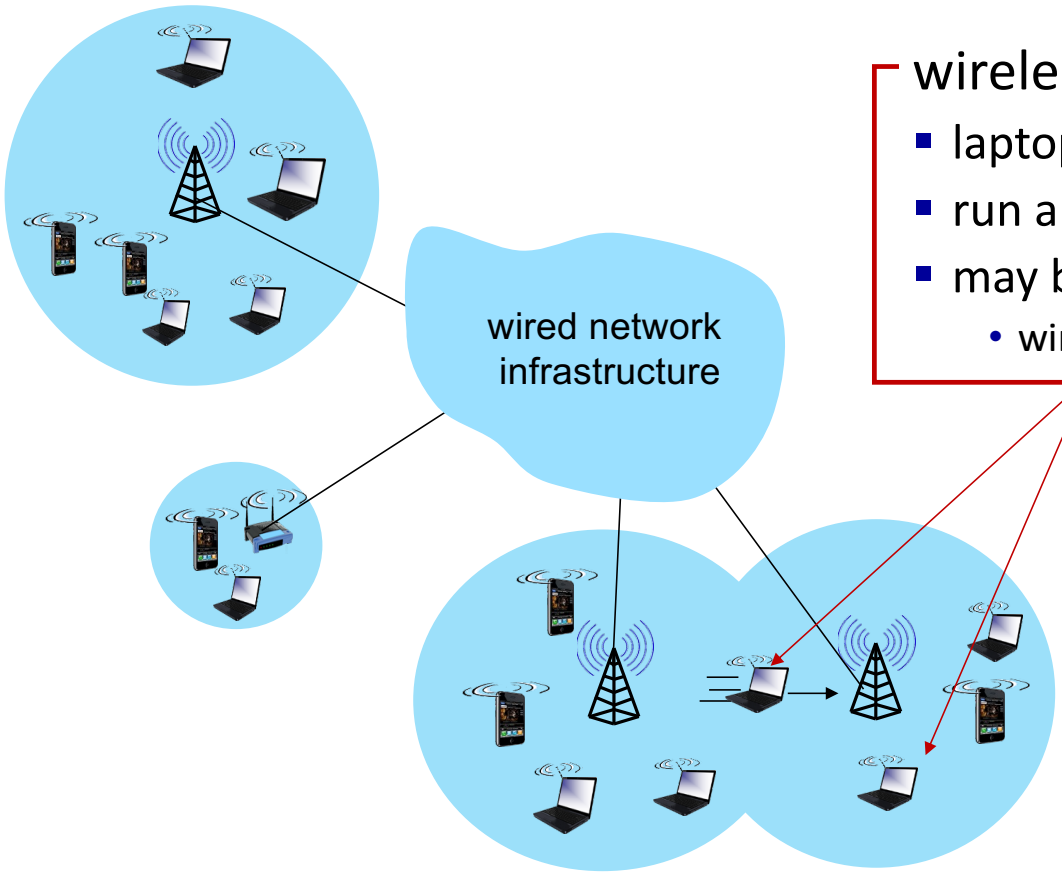
Mobility

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

Elements of a wireless network



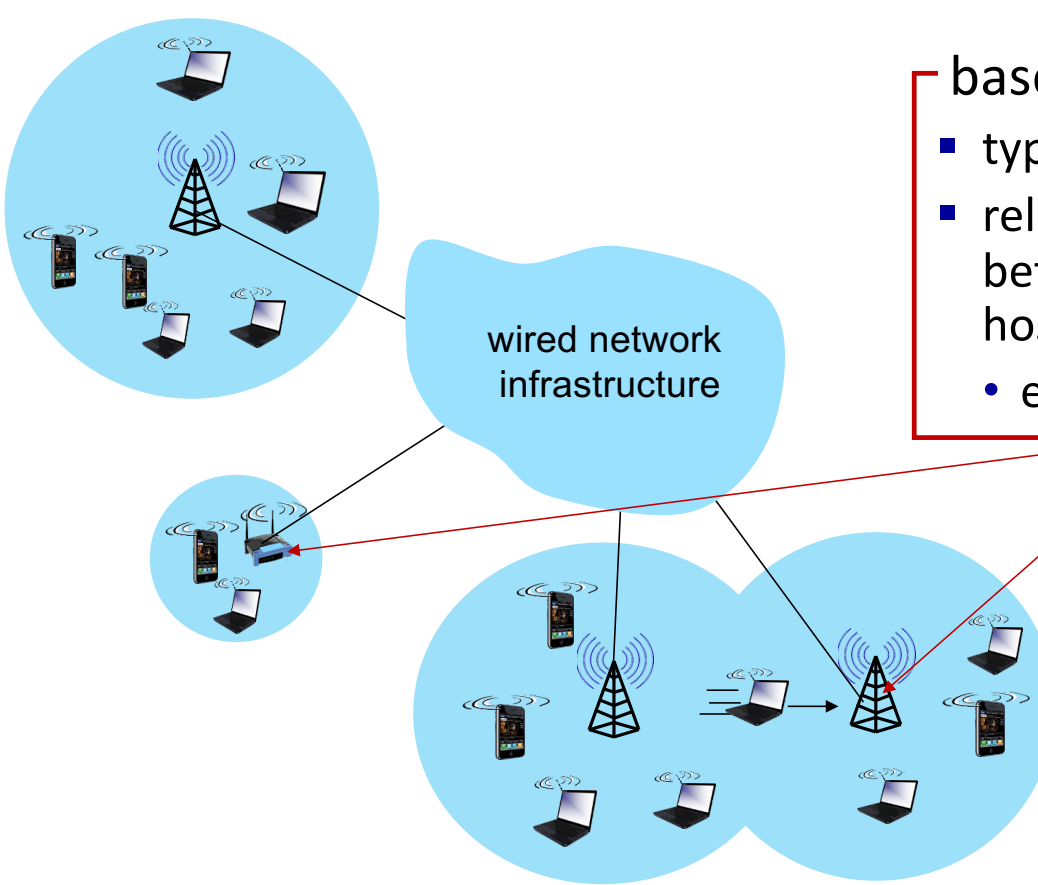
Elements of a wireless network



wireless hosts

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

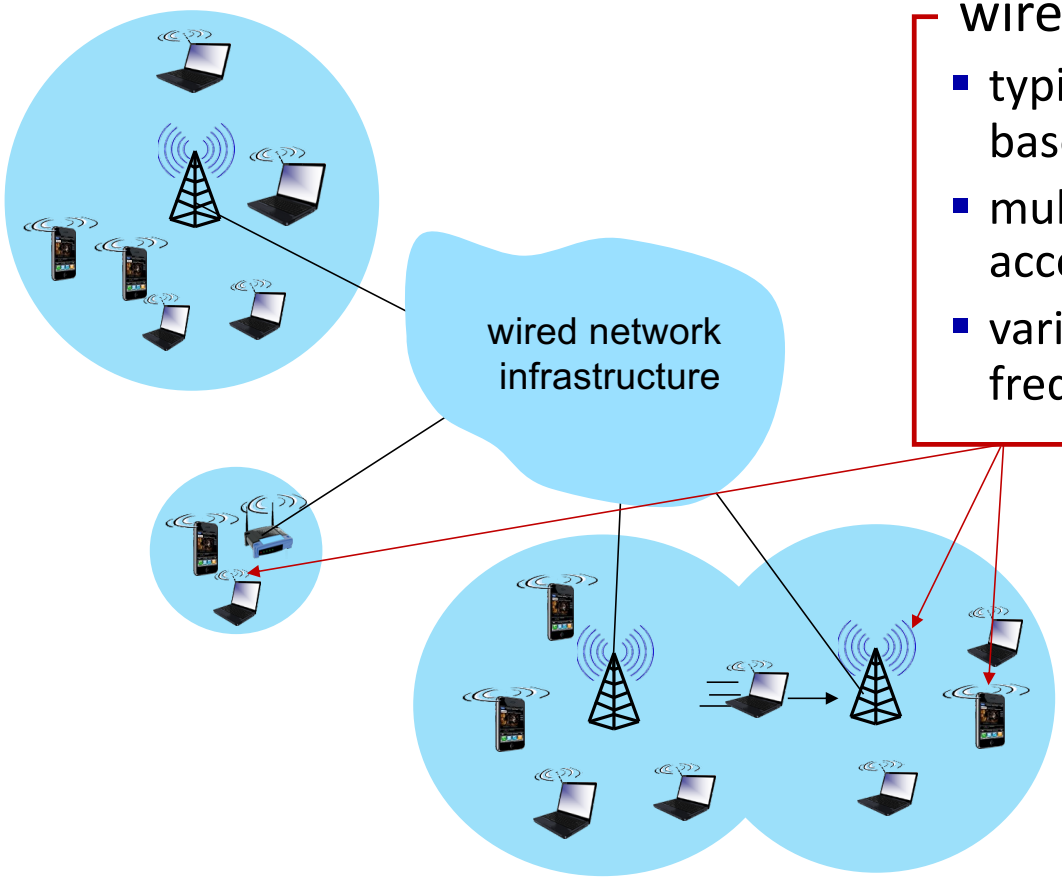
Elements of a wireless network



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

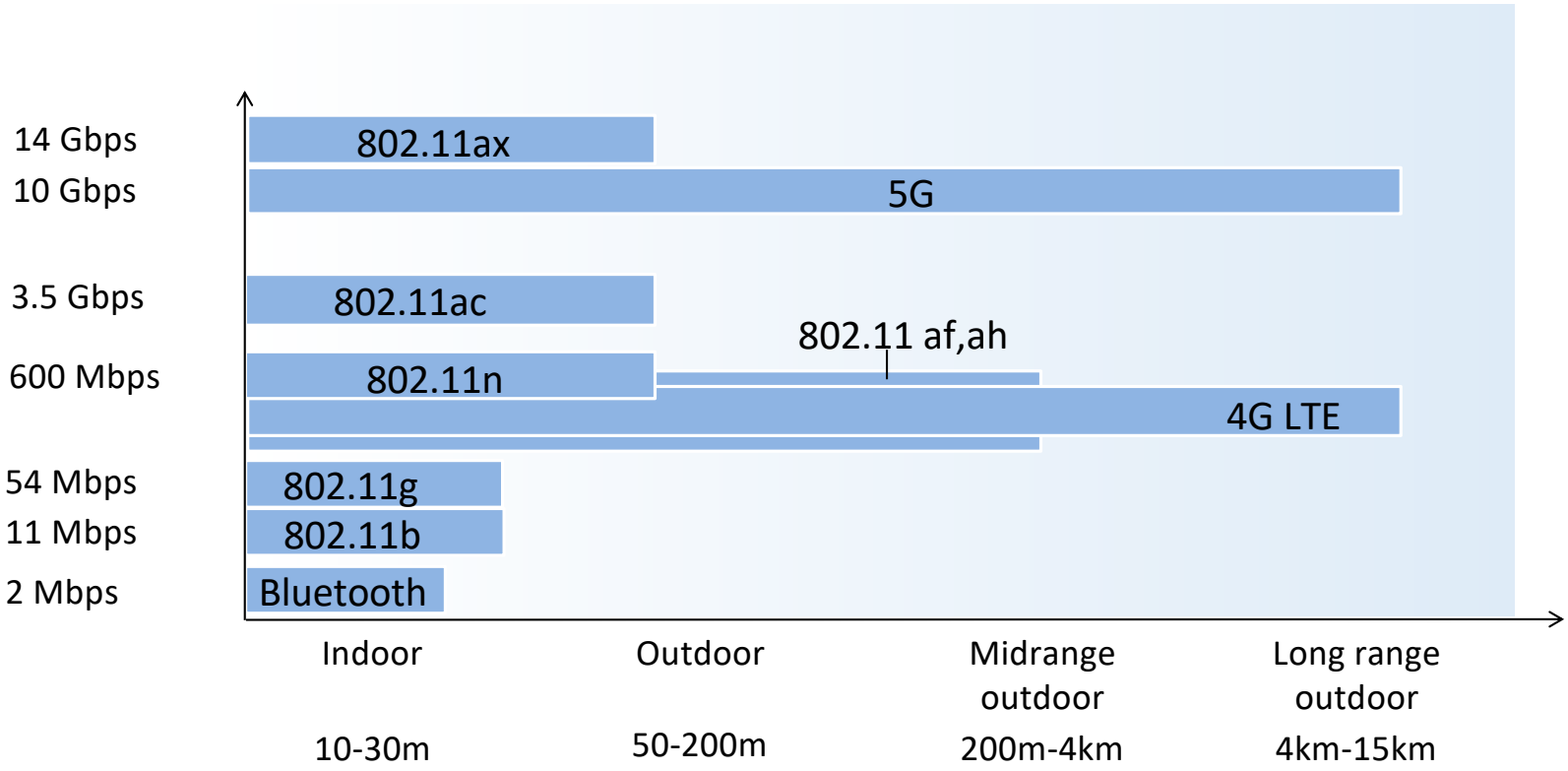
Elements of a wireless network



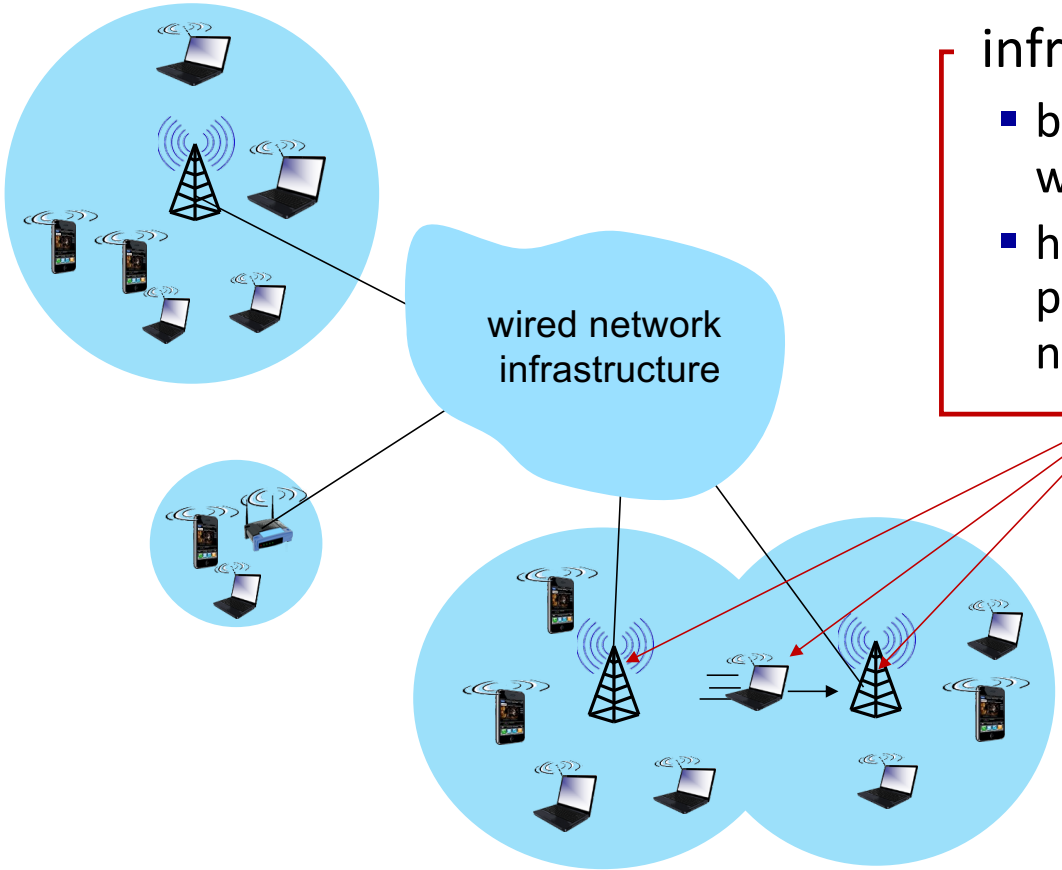
wireless link

- 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



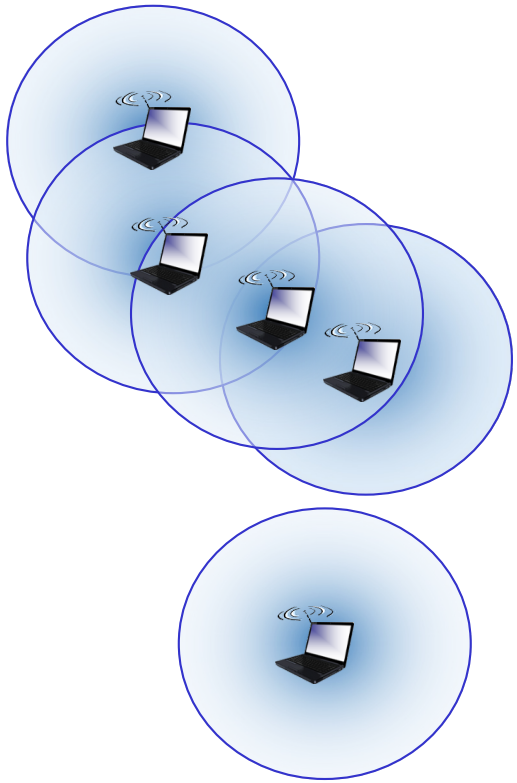
Elements of a wireless network



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 a given wireless node (MANET, VANET)

Chapter 7 outline

- Introduction

Wireless

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

Mobility

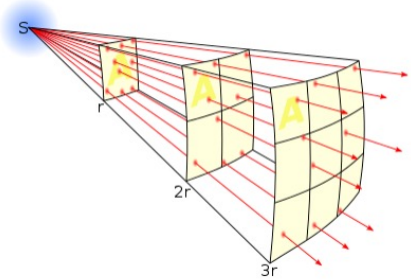
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

Wireless link characteristics: fading (attenuation)

Wireless radio signal attenuates (loses power) as it propagates (free space "path loss")

Free space path loss ~ $(fd)^2$

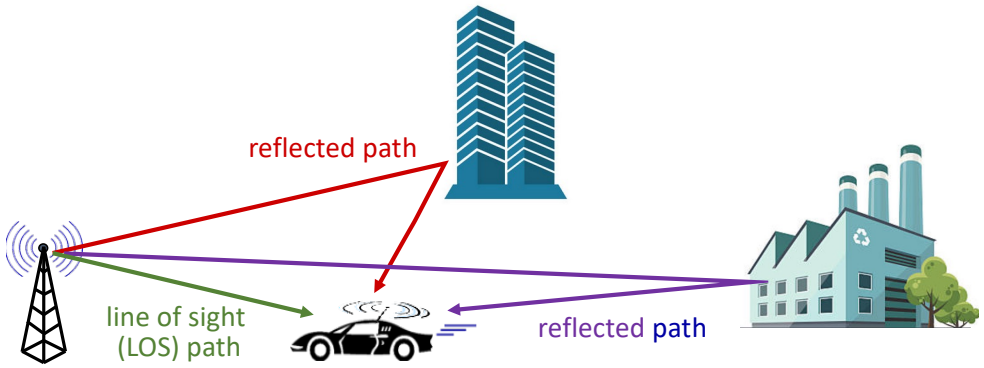
f: frequency
d: distance



higher frequency or longer distance → larger free space path loss

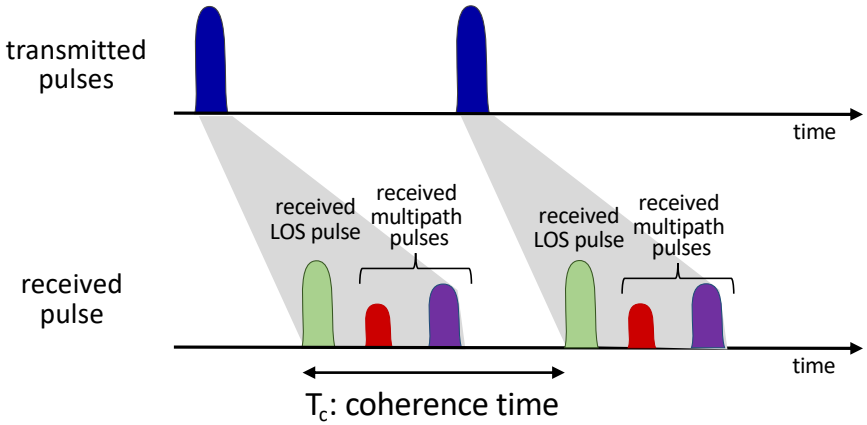
Wireless link characteristics: multipath

multipath propagation: radio signal reflects off objects ground, built environment, arriving at destination at slightly different times



Wireless link characteristics: multipath

multipath propagation: radio signal reflects off objects ground, built environment, arriving at destination at slightly different times

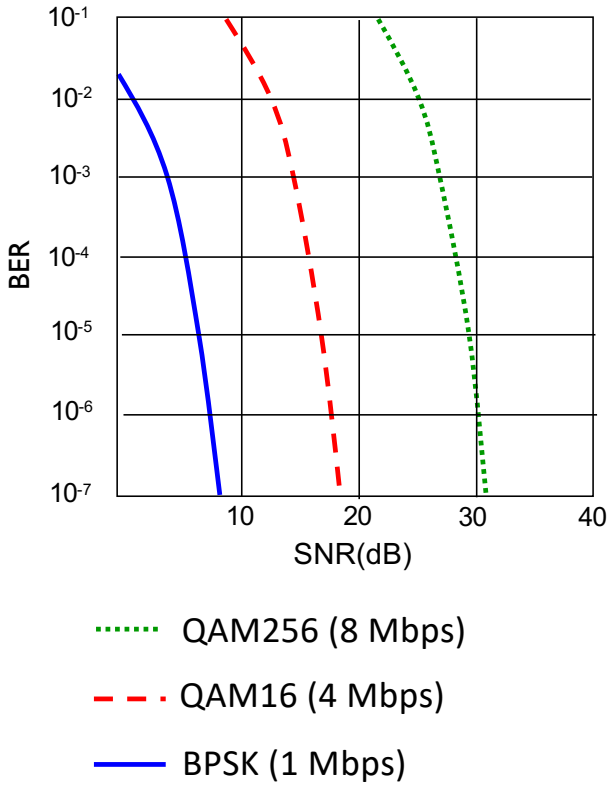


Coherence time:

- amount of time bit is present in channel to be received
- influences maximum possible transmission rate, since coherence times cannot overlap
- inversely proportional to
  - frequency
  - receiver velocity

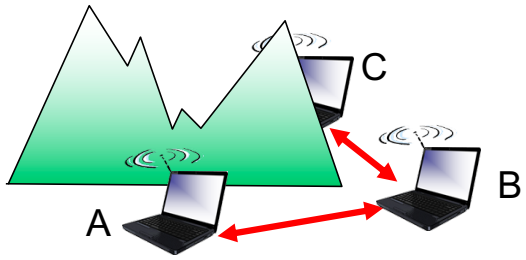
Wireless link characteristics: noise

- interference from other sources on wireless network frequencies: motors, appliances
- SNR: signal-to-noise ratio
  - larger SNR – easier to extract signal from noise (a “good thing”)
- SNR versus BER tradeoff
  - *given physical layer:* increase power -> increase SNR->decrease BER
  - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



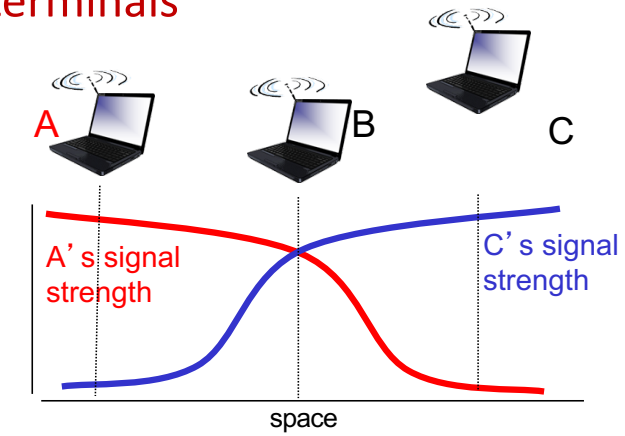
Wireless link characteristics: hidden terminals

Hidden terminal problem



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

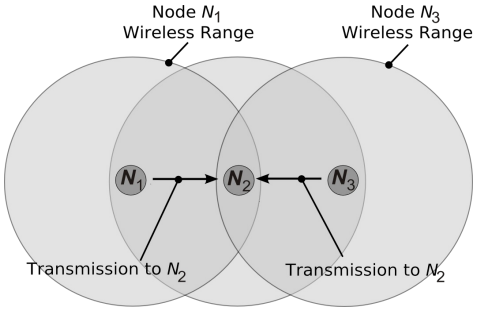
Attenuation also causes "hidden terminals"



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

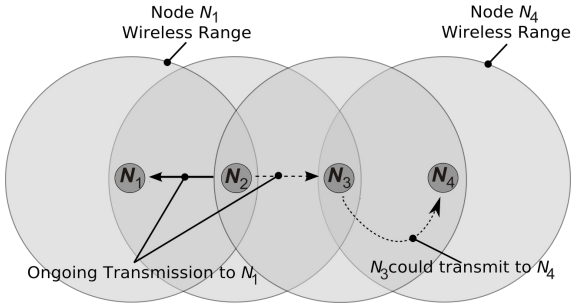
Wireless link characteristics: hidden terminals

Feeling the channel at the transmitter does not give information about the channel (signal strength, quality, etc.) at the receiver.



Hidden node problem / Fading

N1 and N3 do not hear each other due to obstacles or attenuation resulting in potential collision in N2



Exposed node problem

N1 and N4 could be simultaneous receptors from N2 and N3, respectively, but as these senders are within range, simultaneous transmission is not possible

Less problematic
→ only reduced channel utilization

Main problems

Chapter 7 outline

- Introduction

Wireless

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

Mobility

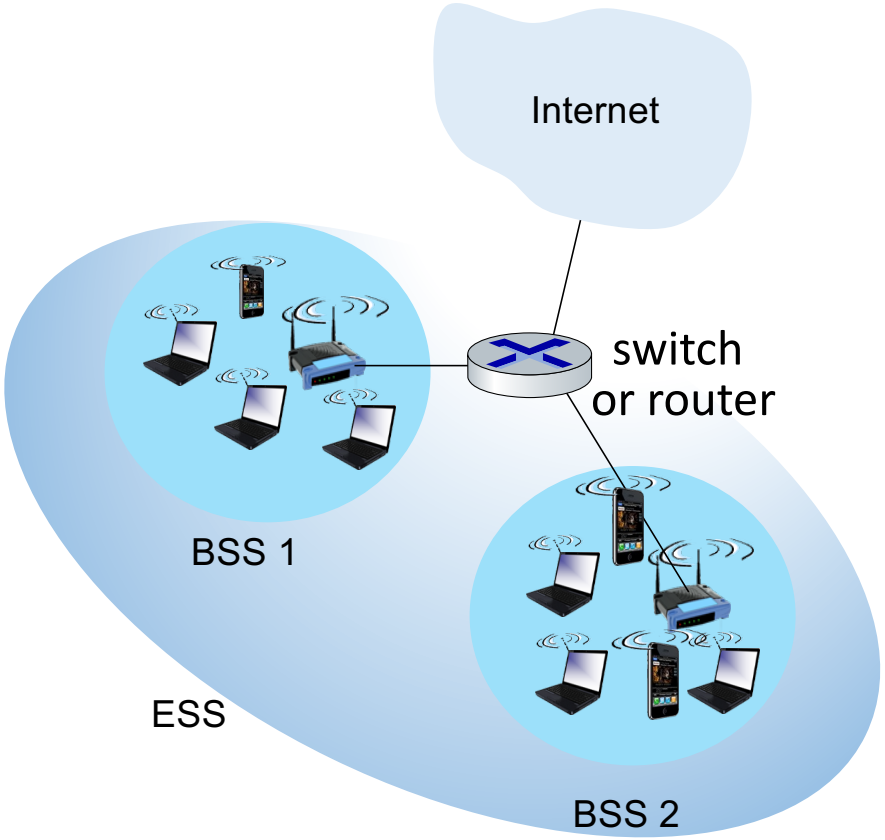
- Mobility management: principles
- Mobility management: practice
  - 4G/5G networks
  - Mobile IP
- Mobility: impact on higher-layer protocols

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	30 m	2.4 GHz
802.11n (WiFi 4)	2009	600 Mbps	70 m	2.4, 5 GHz
802.11ac (WiFi 5)	2013	3.47 Gbps	70 m	5 GHz
802.11ax (WiFi 6)	2020	14 Gbps	70 m	2.4, 5 GHz
802.11af	2014	35 – 560 Mbps	1 km	unused TV bands (54-790 MHz)
802.11ah	2017	347 Mbps	1 km	900 Mhz

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

802.11 LAN architecture

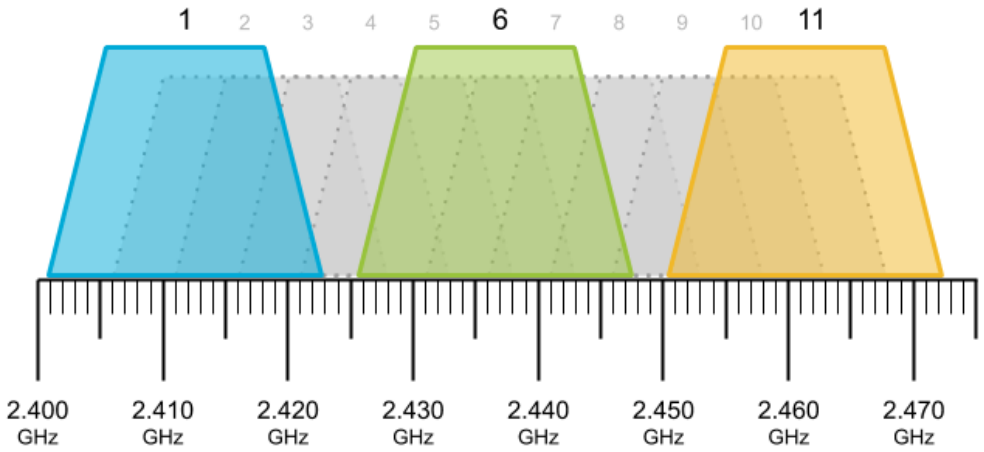


- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only
- Extended Service Set (ESS) includes one or more BSSs

802.11: Channels

- 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!

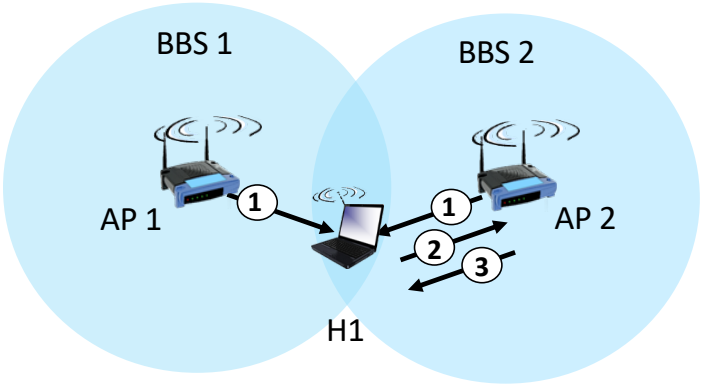
Example: 2.4 GHz

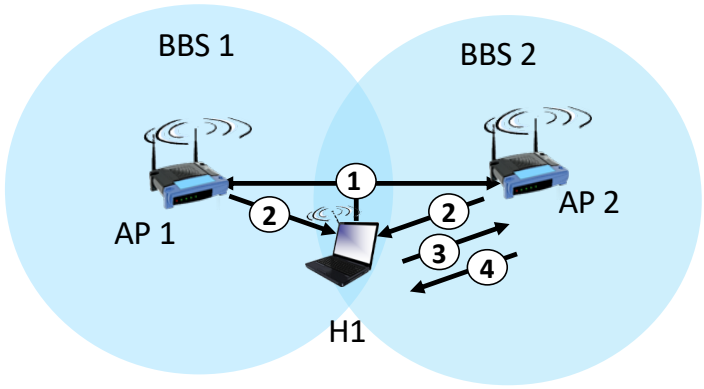


802.11: Association

- 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 before association
  - then typically run DHCP to get IP address in AP's subnet

802.11: passive/active scanning





passive scanning:

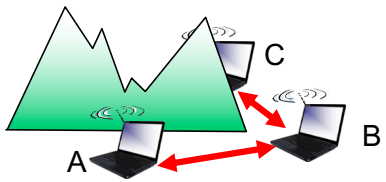
(1) Beacon frames sent from APs
(2) Association Request frame sent: H1 to selected AP
(3) Association Response frame sent from selected AP to H1

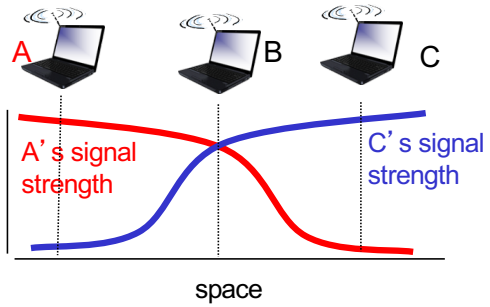
active scanning:

(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/CollisionAvoidance



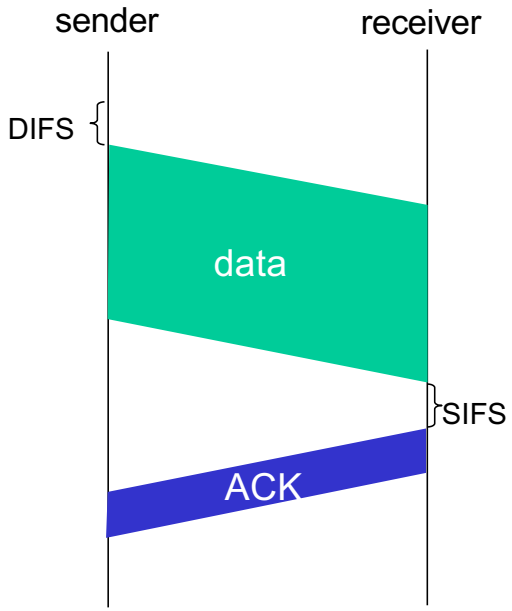


IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then
- transmit entire frame (no CD)
- if no ACK within t, increase random backoff interval
  - otherwise transmission successful

2 if sense channel busy then
- start random backoff time
- timer counts down while channel idle
- when timer expires senses channel again



802.11 receiver

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

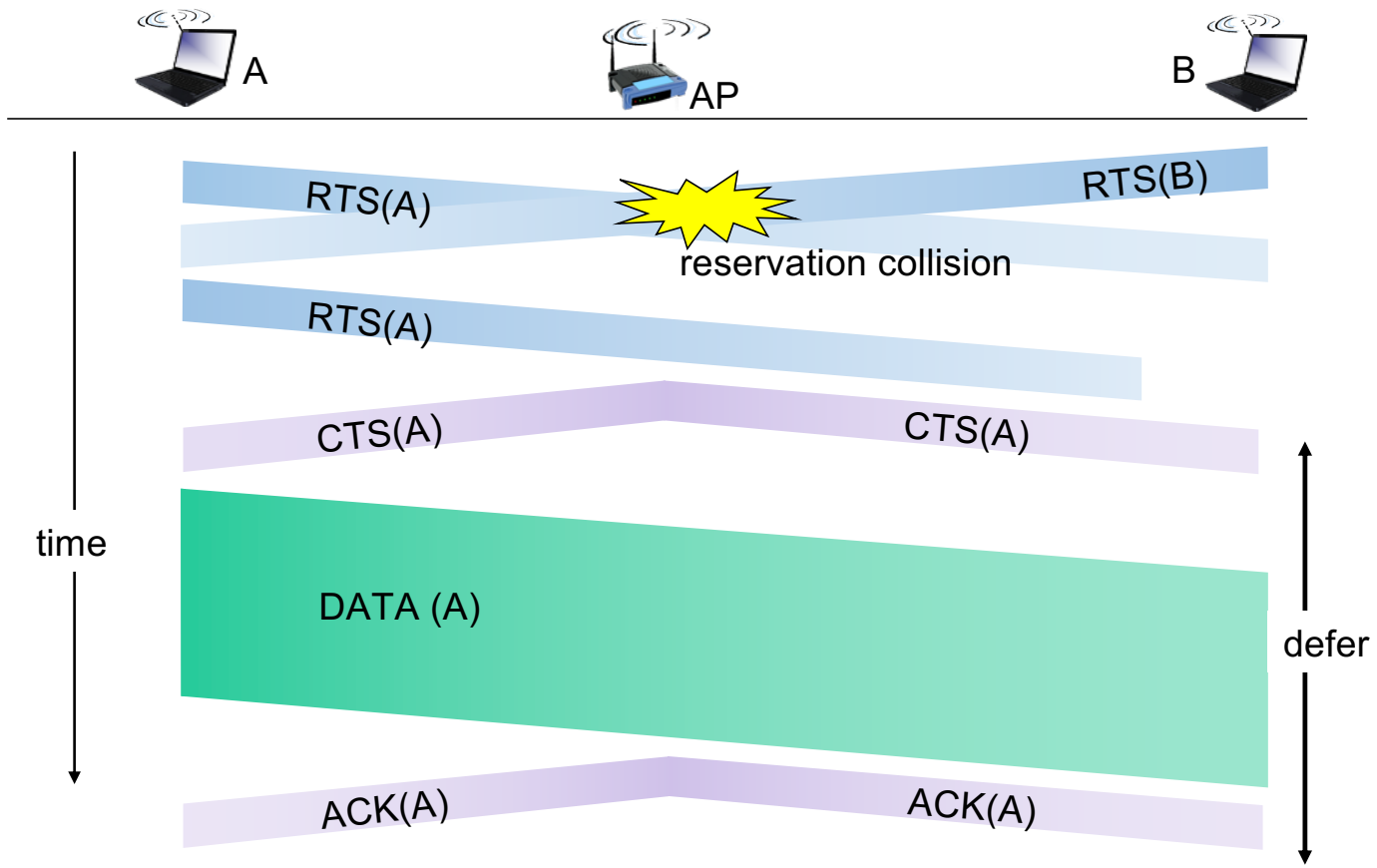
DIFS – DCF (Distributed Coordinated Function) Interframe Space (standard-dep, from 28 to 50 μs)
SIFS – Short Interframe Space (standard-dependent, usually from 10 to 16 μs)

Avoiding collisions (more)

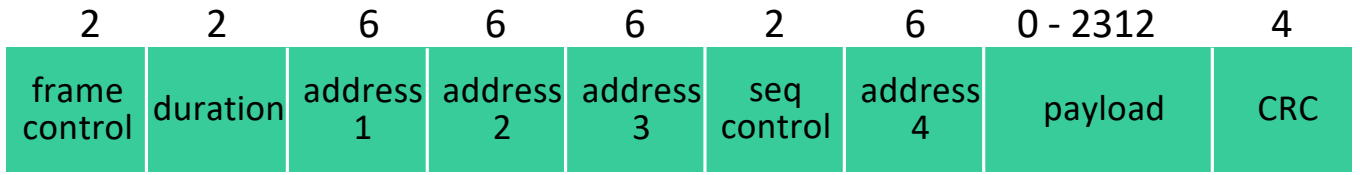
idea: sender "reserves" channel use for data frames using small reservation packets

- 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



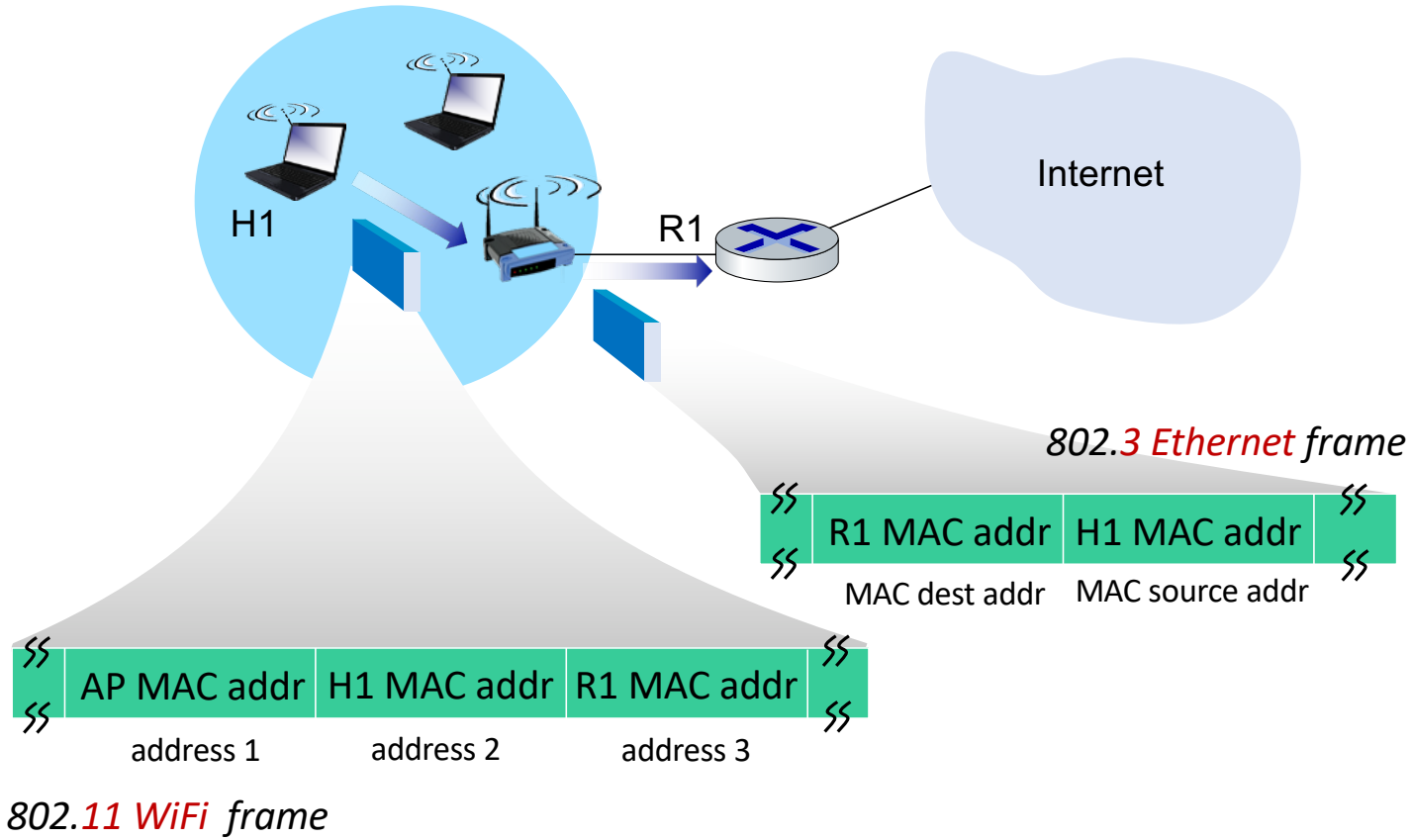
Address 1: MAC address of wireless host or AP to receive this frame

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

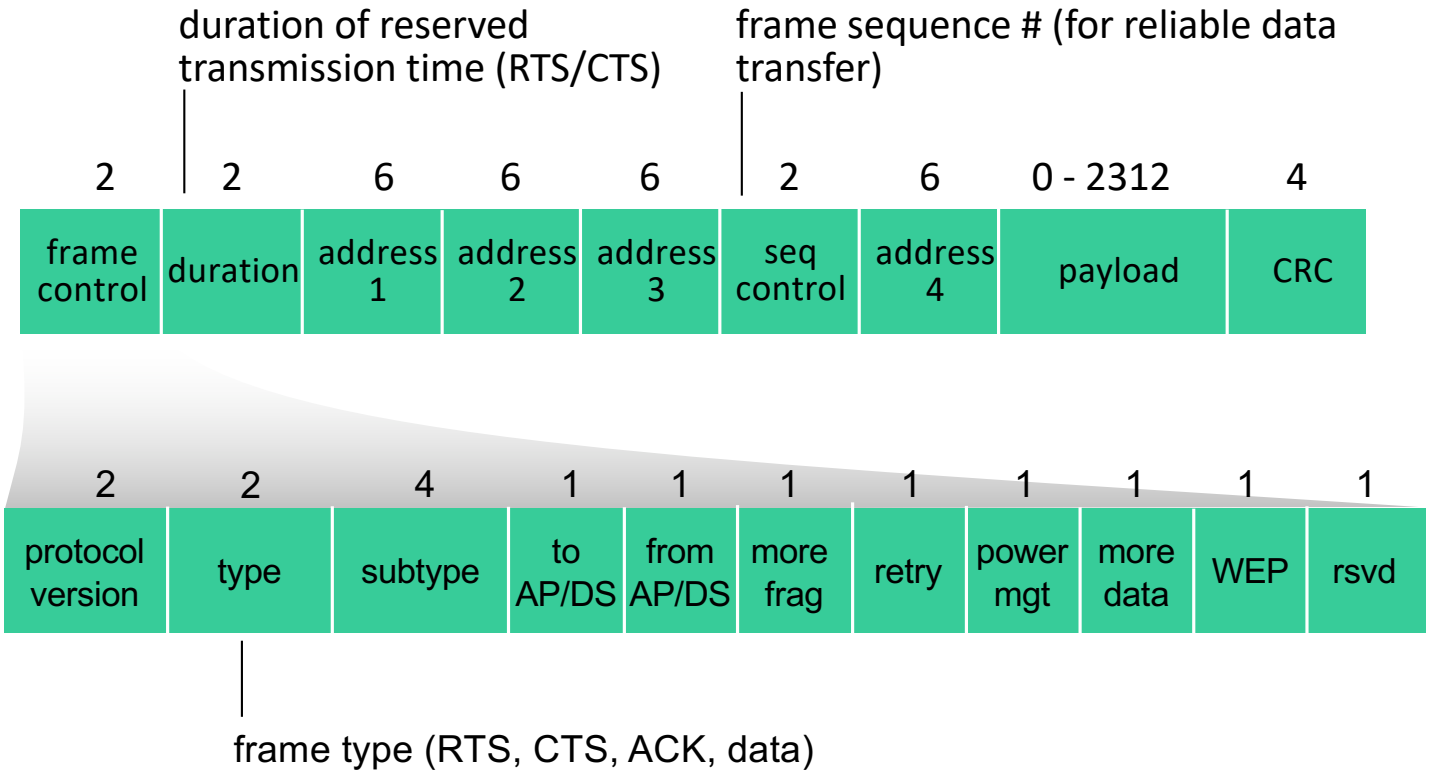
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

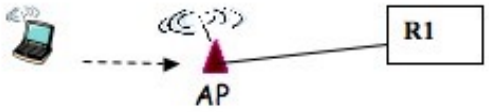
802.11 frame: addressing



802.11 frame: addressing



802.11 frame: addressing

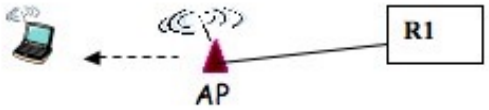


toDS=1, fromDS=0

A1 (RA) = BSSID = MAC AP
A2 (TA) = SA = MAC STA
A3 (DA) = MAC R1

toDS=1, fromDS=1

A1 (RA) = MAC AP2
A2 (TA) = MAC AP1
A3 (DA) = MAC R2
A4 (SA) = MAC R1



toDS=0, fromDS=1

A1 (RA) = DA = MAC STA
A2 (TA) = BSSID = MAC AP
A3 (SA) = MAC R1

DA - Destination Address - receptor final
SA - Source Address - origem da transmissão
RA - Receiver Address - estação wireless que deve processar a trama
wireless STA -> RA=DA
wired node -> RA=MAC AP; DA=router
TA - Transmitter Address - interface wireless que transmitiu a trama
BSSID - MAC da interface wireless do AP (Infrastructured networks); aleatório BSSID (Ad-hoc networks)

802.11 frame types

Management frames – used to perform *supervisory functions* such as joining and leaving wireless networks and moving associations from AP to AP.

Control frames - used in conjunction with data frames to perform *control operations* such as channel acquisition and carrier-sensing maintenance functions, and positive acknowledgment of received data. Control frames allow to deliver data reliably from STA to STA.

Data frames - used to send data from STA to STA. Several different data frame may occur, depending on the network.

802.11 frame types and subtypes

Type 00 – Management frames
e.g. Beacon, Association request, Probe request, etc.

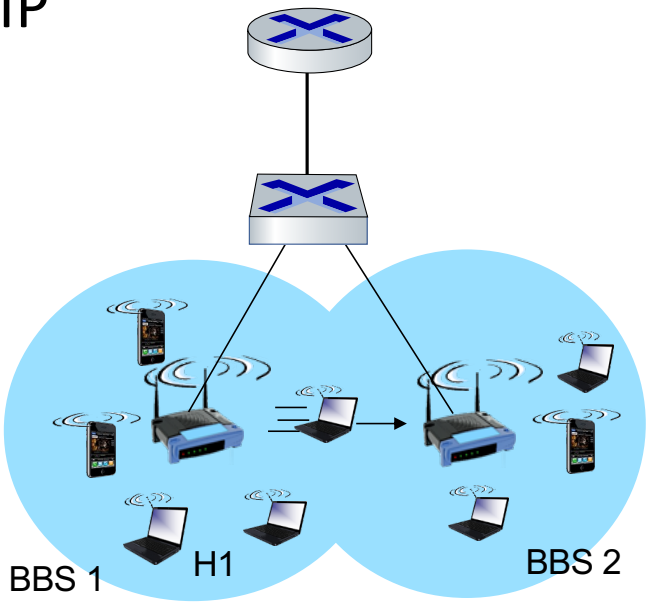
Type 01 – Control frames
e.g. RTS, CTS, ACK, etc.

Type 10 – Data frames
e.g. Data

Type value	Type Description	Subtype Value	Subtype description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	0110-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101	Action
00	Management	1110-1111	Reserved
01	Control	0000-0111	Reserved
01	Control	1000	Block Ack Request
01	Control	1001	Block Ack
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1111	CF-END
10	Data	0000	Data
10	Data	0001	Data + CF-Ack
10	Data	0010	Data + CF-Ack + CF-Poll
10	Data	0100	Null (no data)
10	Data	0101	CF-Ack (no data)
10	Data	0110	CF-Poll (no data)
10	Data	0111	CF-Ack + CF-Poll (no data)
10	Data	1000	QoS Data
10	Data	1001	QoS Data + CF-Ack
10	Data	1010	QoS Data + CF-Poll
10	Data	1011	QoS Data + CF-Poll + CF-Ack
10	Data	1100	QoS Null (no data)
10	Data	1101	Reserved
10	Data	1110	QoS CF-Poll (no data)
10	Data	1111	QoS CF-Ack + CF-Poll (no data)
11	Reserved	0000-1111	Reserved

802.11: 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. 6): switch will see frame from H1 and "remember" which switch port can be used to reach H1



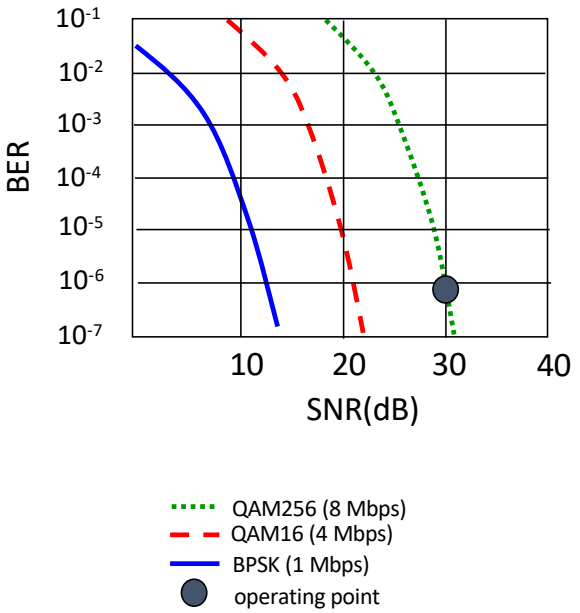
802.11: advanced capabilities

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 but with lower BER



802.11: advanced capabilities

power management

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