Wireless links, Wifi 802.11 wireless LAN cellular networks

CE 352, Computer Networks

Salem Al-Agtash

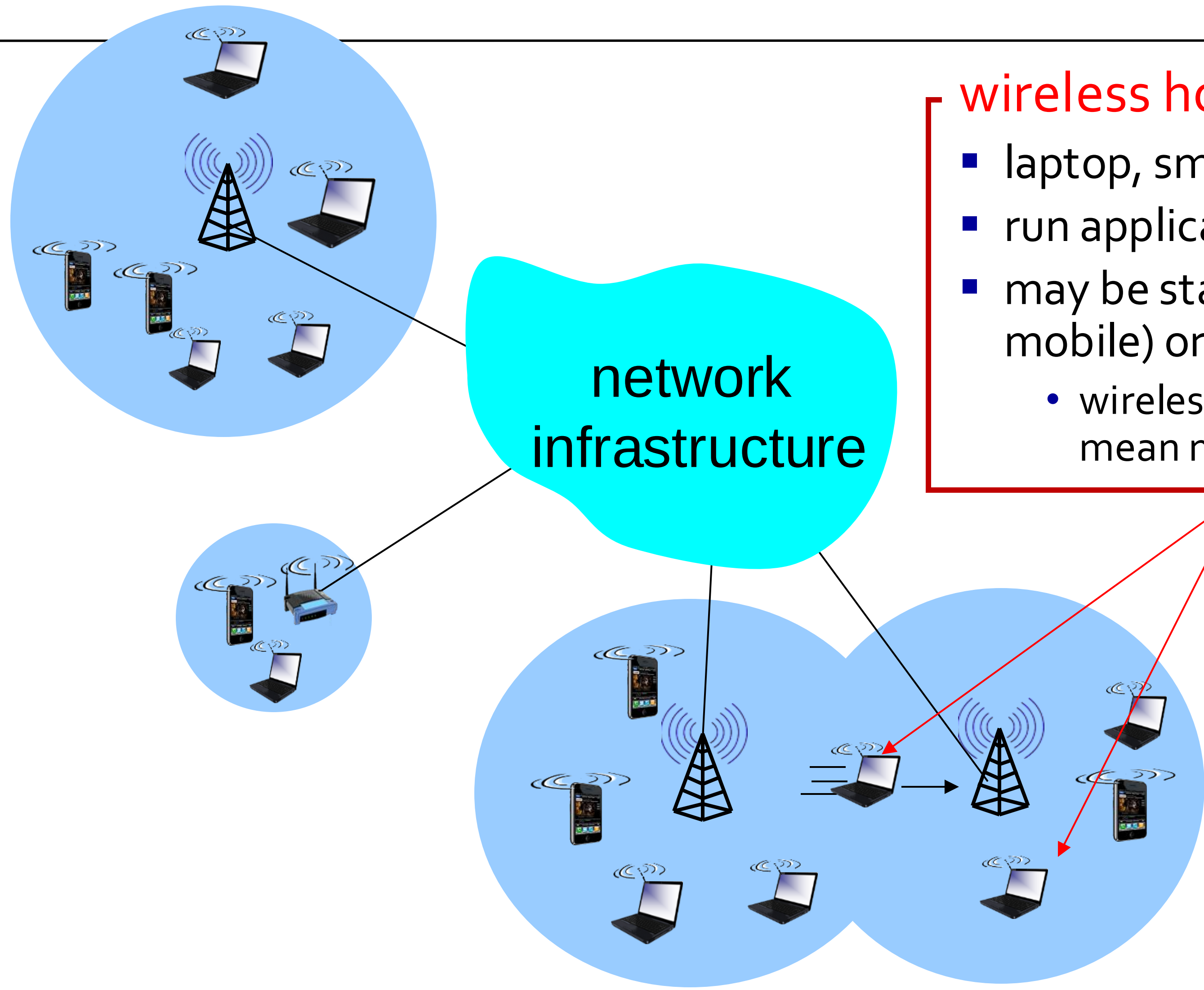
Lecture 23

Slides are adapted from Computer Networking: A Top Down Approach, 7th Edition © J.F Kurose and K.W. Ross

Wireless and Mobile Networks

- Over 7.5 billion wireless (mobile) phone users worldwide (2022)
- Wireless Internet-connected devices (Laptops, smartphones, cars, home security and appliances, watches, etc.) – [cellular and WiFi]
- two important aspects:
  - *wireless:* communication over wireless link
  - *mobility:* handling the mobile user who changes point of attachment to network
- Elements of wireless network:
  - Wireless hosts, base stations, wireless links
  - Hosts associated with a base station are operating in an infrastructure mode
  - In case host have no such infrastructure in which to connect, they connect together in an *add hoc network* mode (Bluetooth)

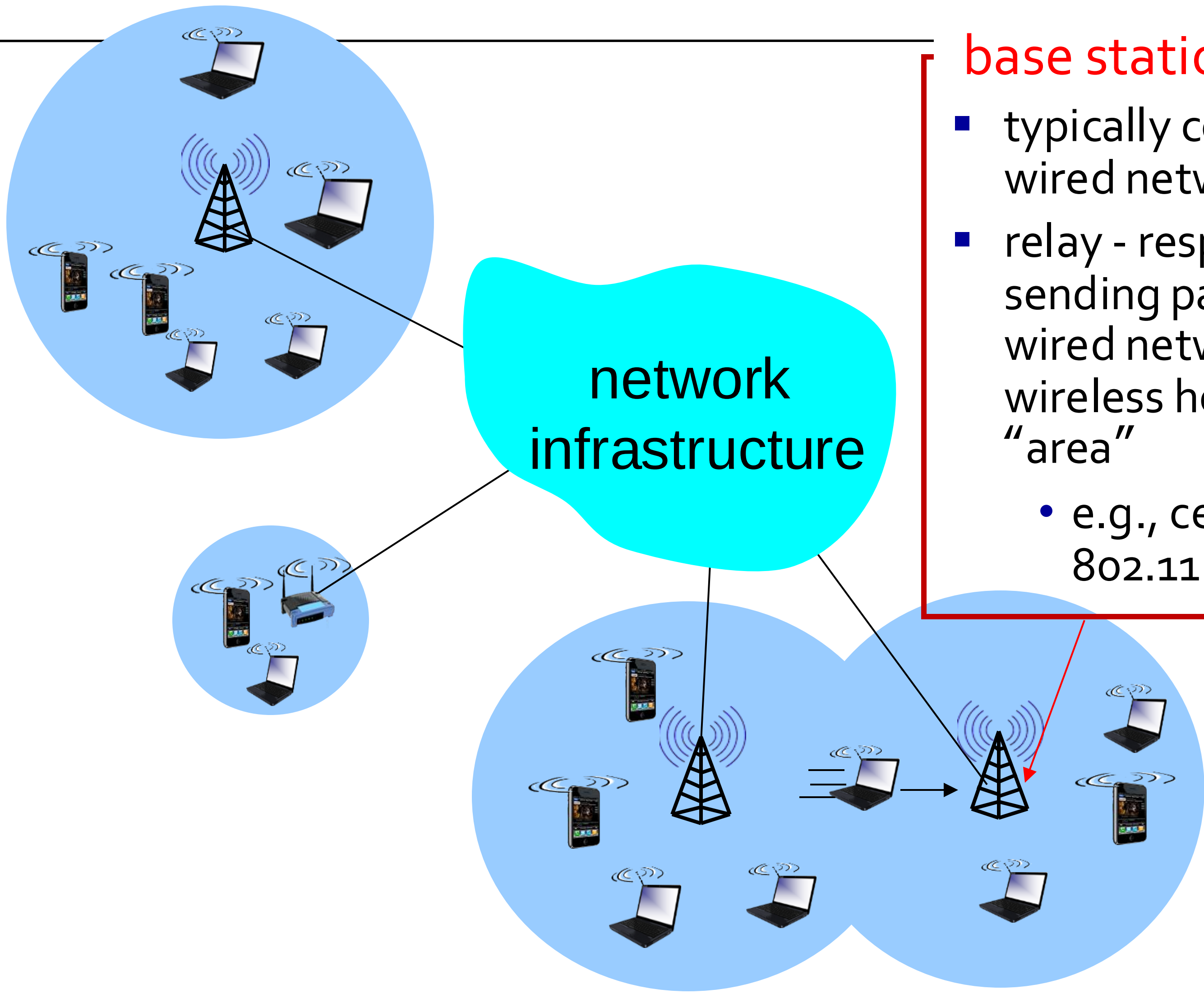
Wireless hosts



wireless hosts

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

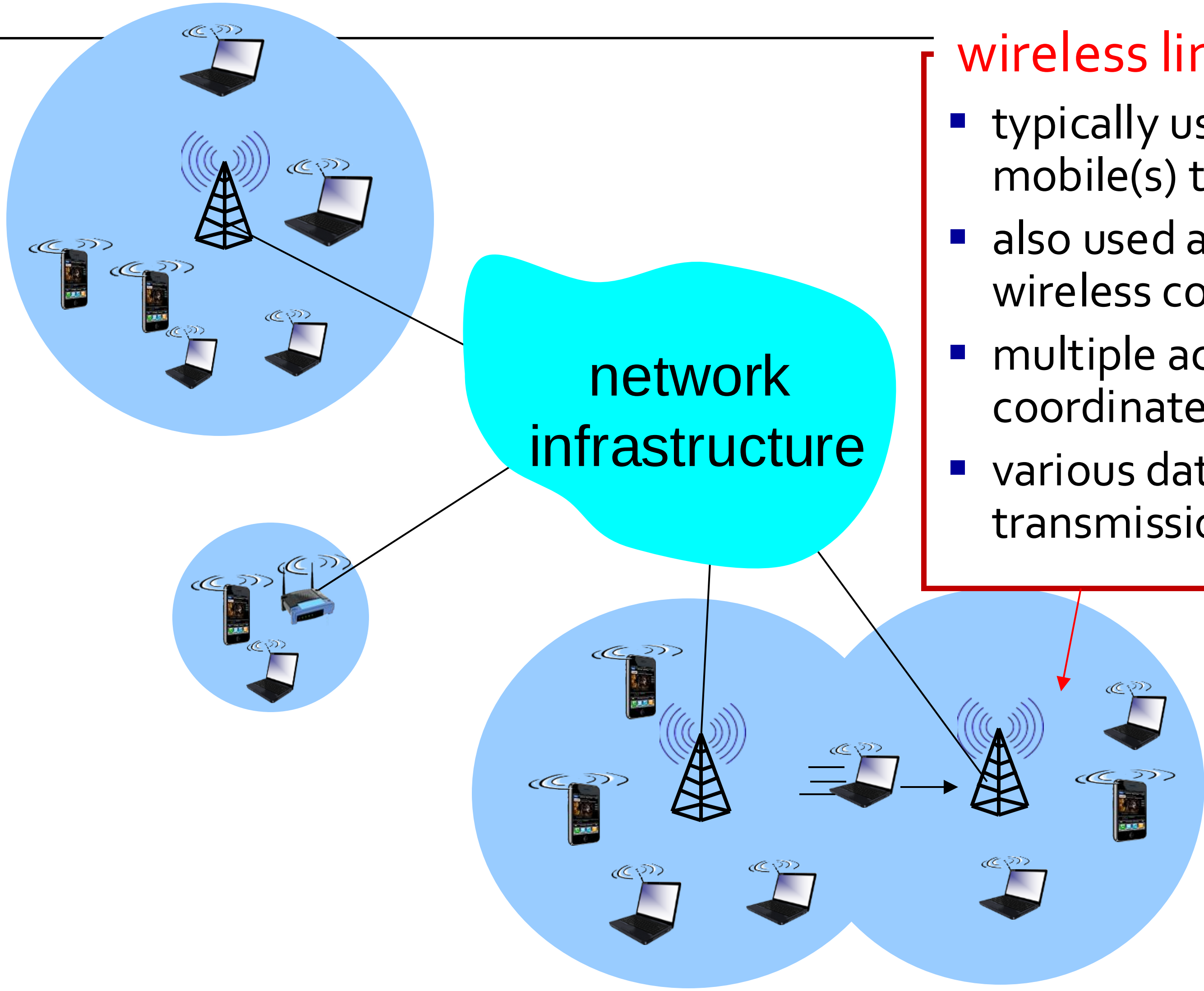
Base station



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

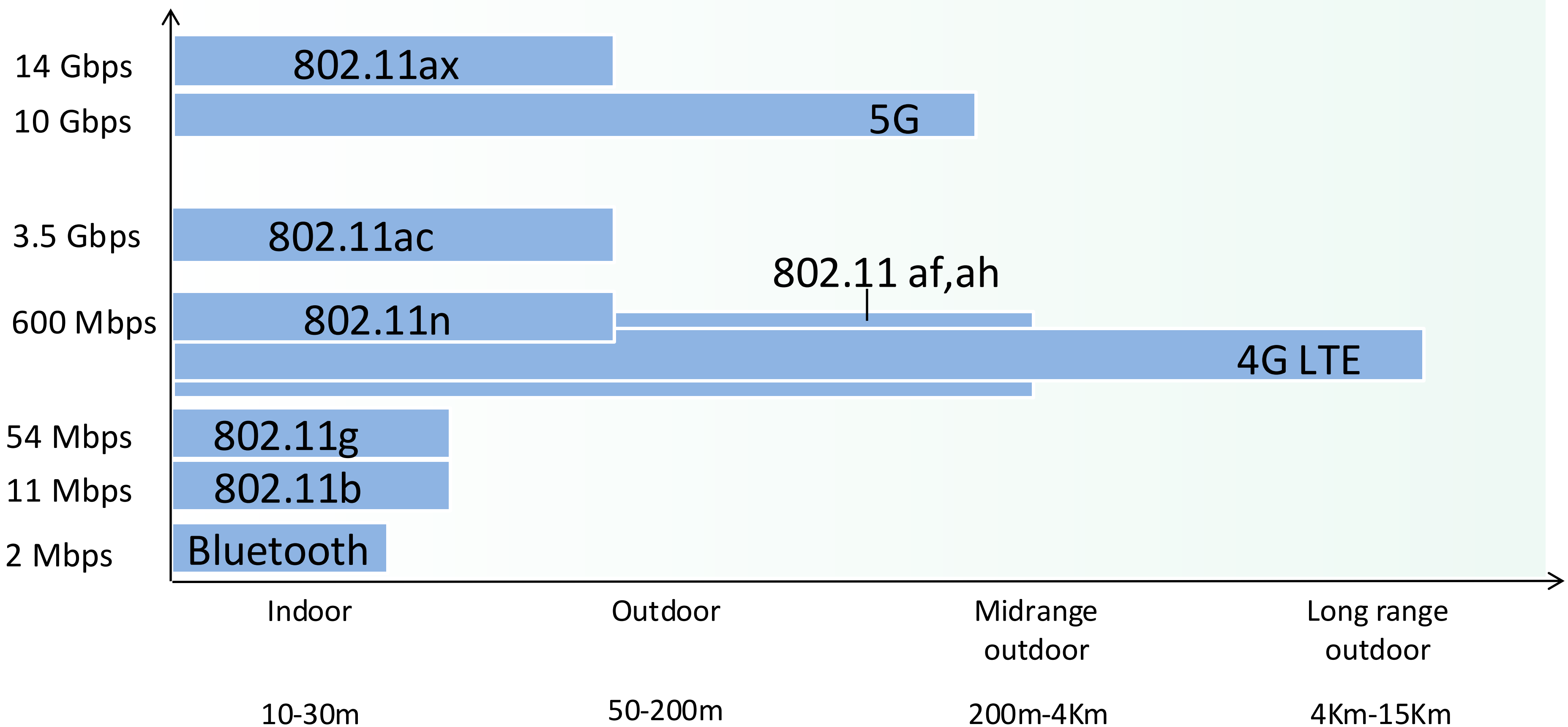
Wireless links



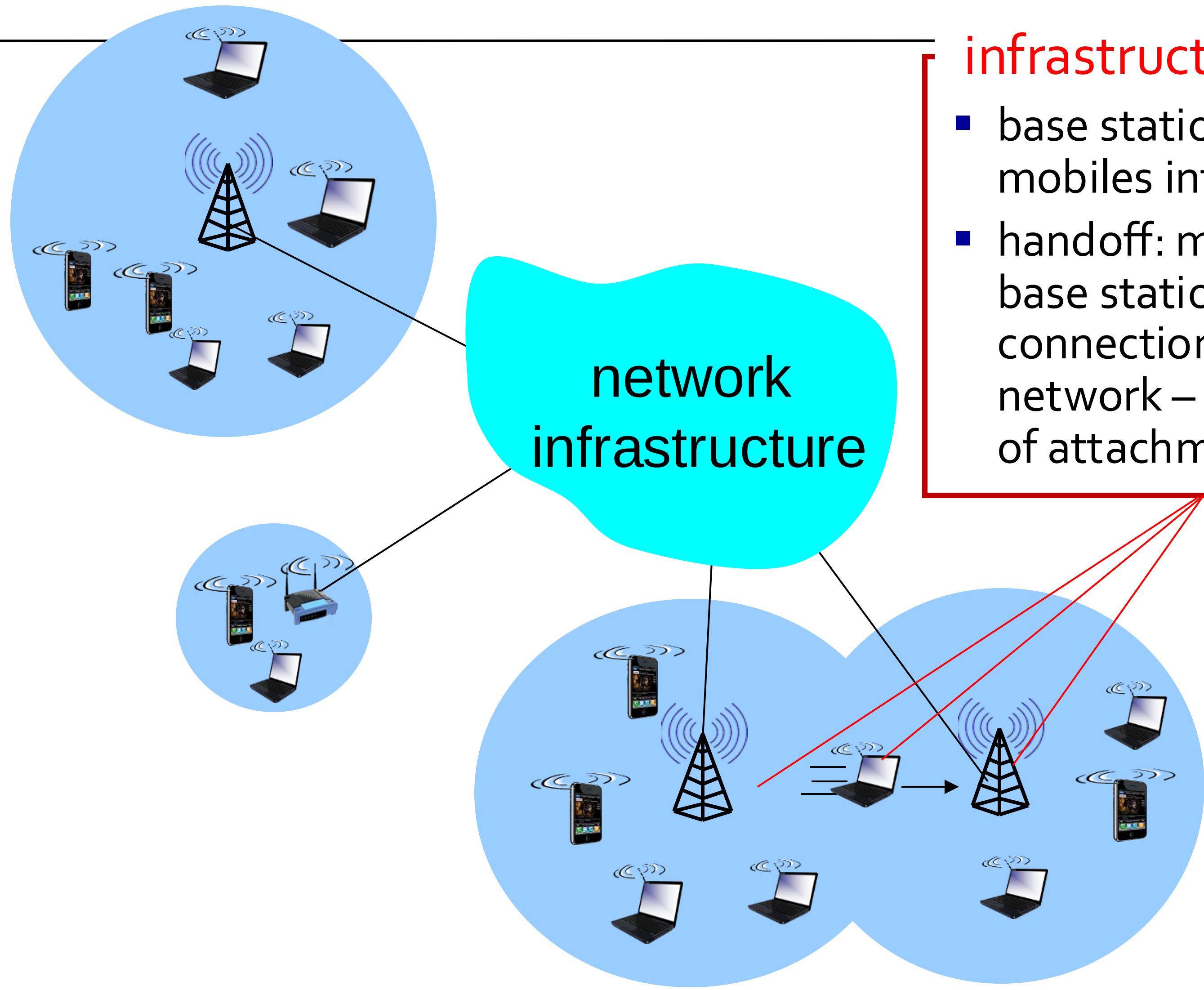
wireless link

- typically used to connect mobile(s) to base station
- also used as backbone wireless communication link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Characteristics of selected wireless links



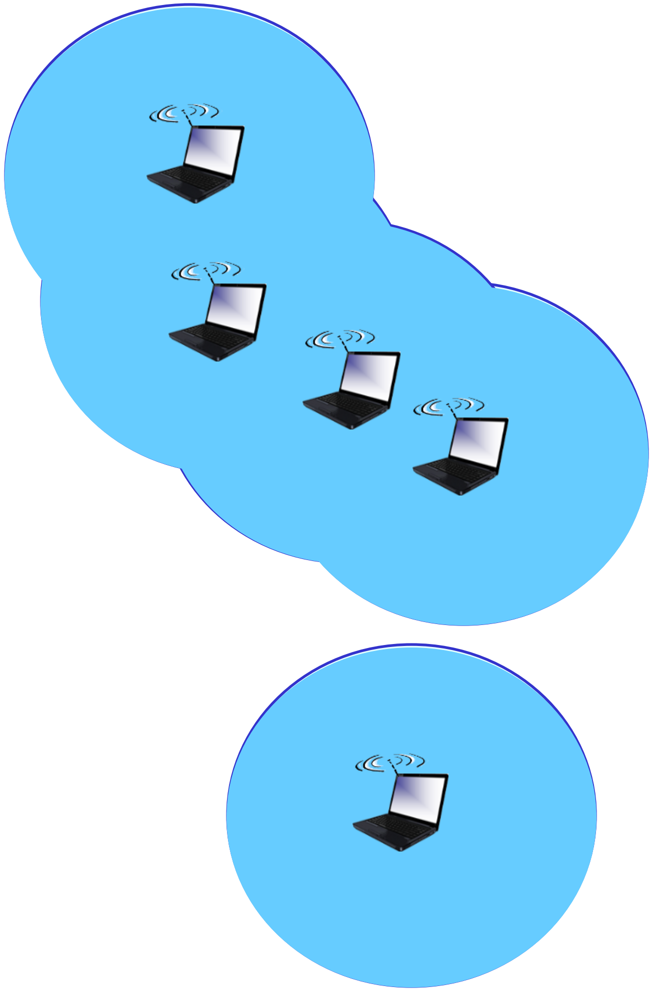
Infrastructure mode



infrastructure mode

- base station connects mobiles into wired network
- handoff: mobile changes base station providing connection into wired network – changes its point of attachment

ad hoc mode



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

Classification

	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*
no infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet, relay to reach other a given wireless node MANET (Metropolitan), VANET (vehicular)

Wireless Link differs from wired link

Wired Ethernet 802.1 vs. a wireless 802.11 network

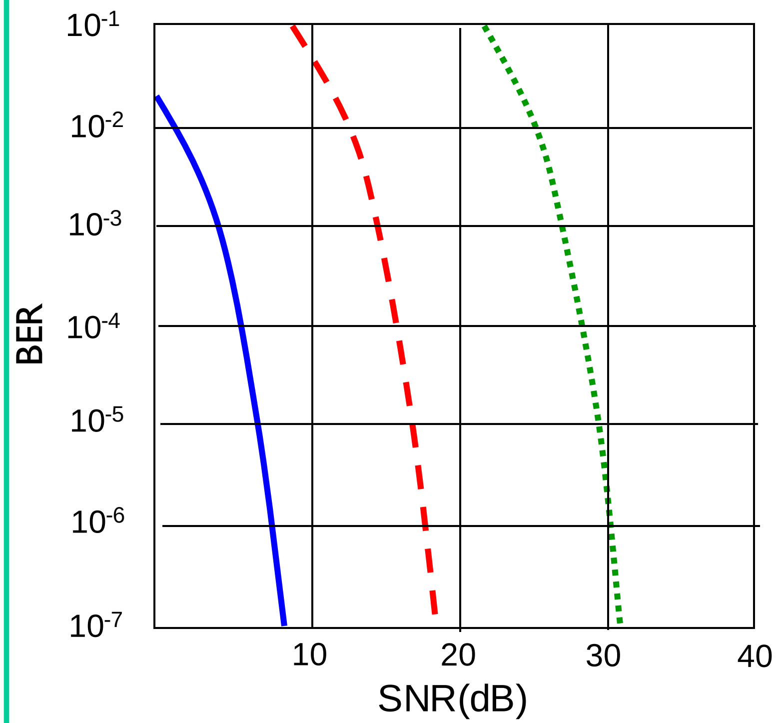
important differences from wired link ….

- *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

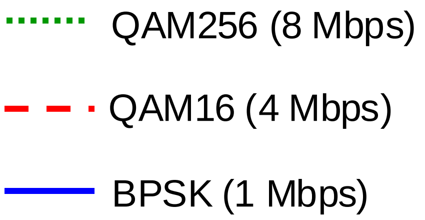
…. make communication across (even a point to point) wireless link much more "difficult"

SNR versus BER

- Bit errors (BER) more common
- SNR: signal-to-noise ratio (measure of strength of received signal) in dB (20log[S/N])
  - 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 thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)

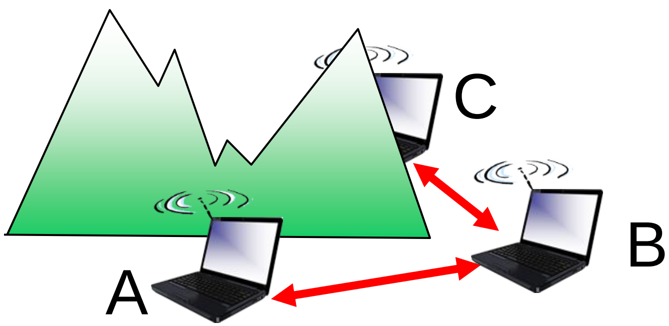


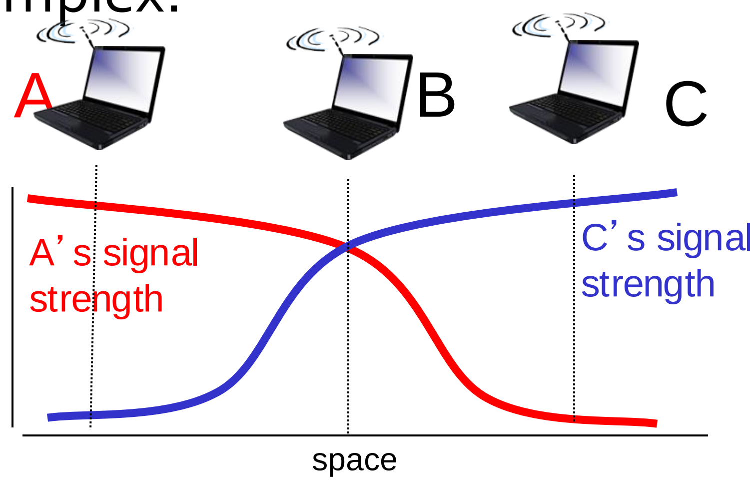
Modulation techniques:



Hidden terminal problem

Multiple wireless senders and receivers create additional problems (beyond multiple access and BER) – fading, makes multiple access in wireless network more complex:





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 (fading):

- 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")
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence

MAC protocols:

1. channel partitioning
- divide channel into smaller "pieces"
- allocate piece to node for exclusive use

(1.1 time slots, 1.2 frequency, 1.3 code)

2. random access
- channel not divided, allow collisions
- "recover" from collisions

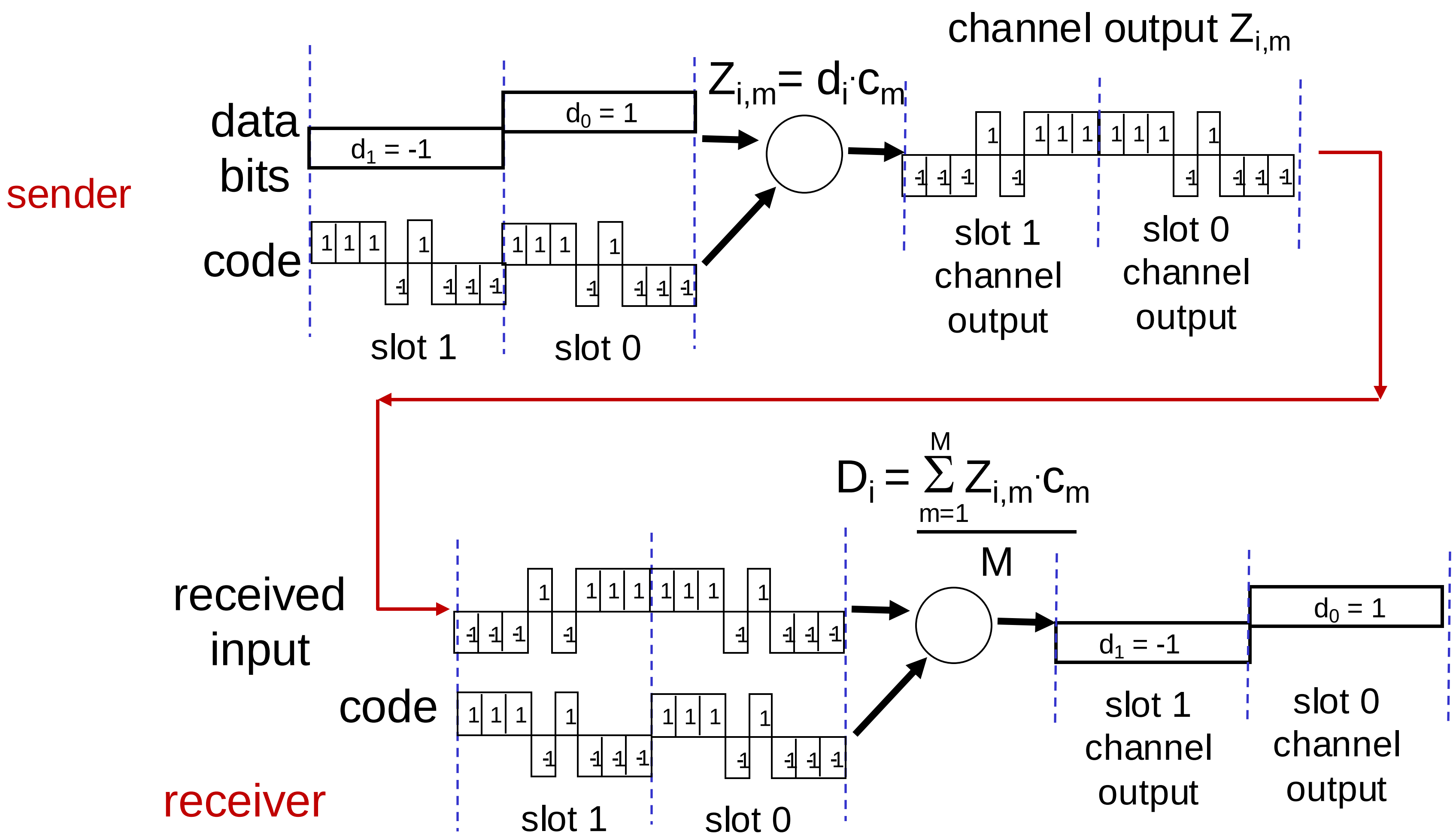
(2.1 Slotted ALOHA, 2.2 Pure ALOHA, 2.3 CSMA, CSMA/CD, CSMA/CA)

3. "taking turns"
- nodes take turns, but nodes with more to send can take longer turns

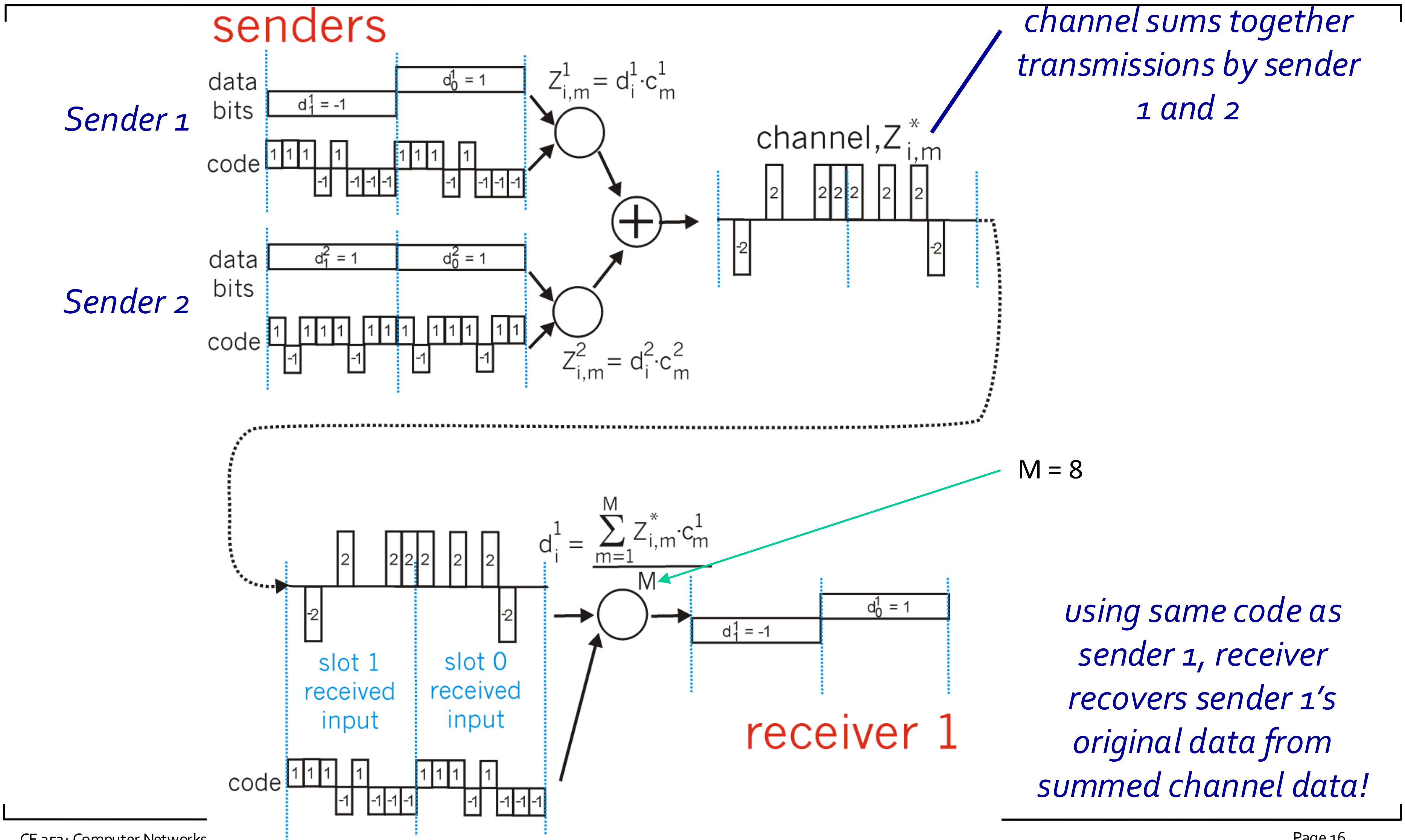
(3.1 Polling, 3.2 token passing)

COEN 146: Computer Networks Page 5

CDMA encode/decode



CDMA: two-sender interference



IEEE 802.11 Wireless LAN

WiFi, most important access network technologies in Café, airports, campuses, malls, …

direct sequence spread spectrum (DSSS) in physical layer

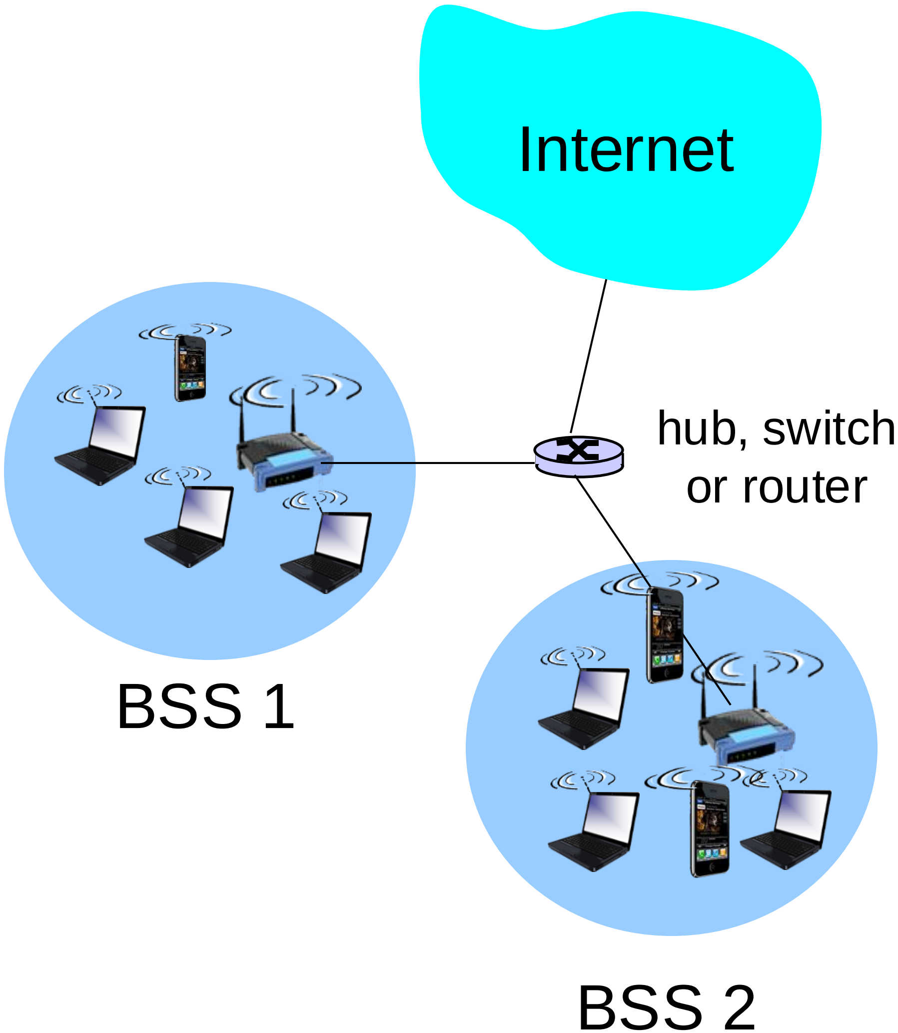
- all hosts use same chipping code

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

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

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

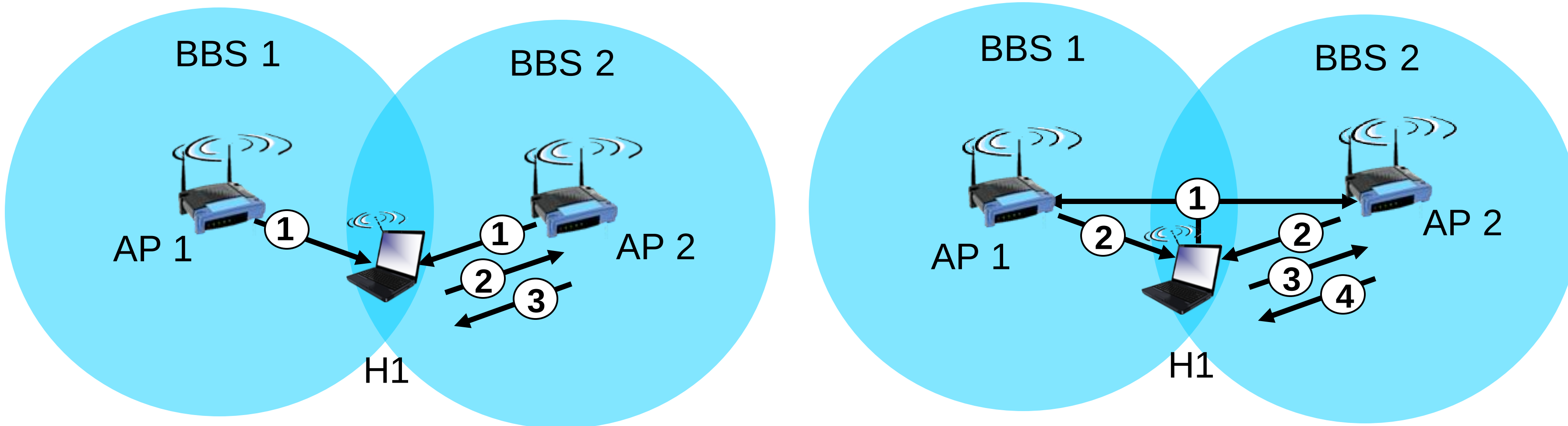
802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies within 85MHz band

- AP admin chooses frequency for AP
  - E.g. Admin installs 3 APs in same location, each assigned 1, 6, 11 channels
- interference possible: channel can be same as that chosen by neighboring AP! – WiFi jungle

host: must *associate* with an AP

- scans channels, listening for *beacon frames* containing AP's name (SSID - Service Set Identifier) and MAC address
- selects AP to associate with
- may perform authentication – Username/Password or MAC
  - RADIUS server
  - EDUROAM emerging
- will 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

wireless LANs do not use collision detection, transmits frame in its entirety

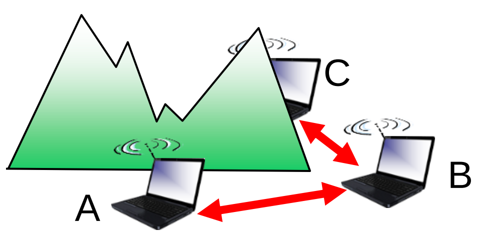
So needs to avoid collisions: 2^+ nodes transmitting at same time

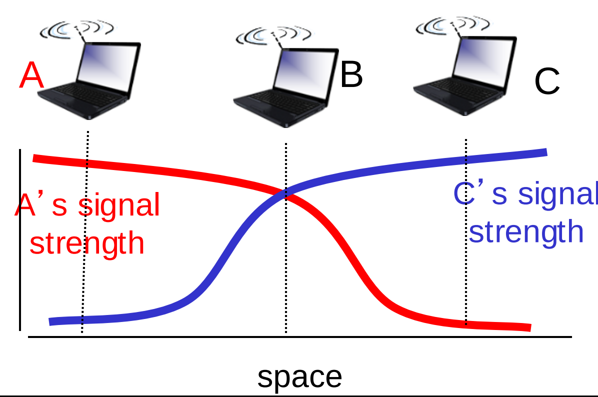
802.11: CSMA - sense before transmitting

- 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 MAC Protocol: CSMA/CA

802.11 sender

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

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

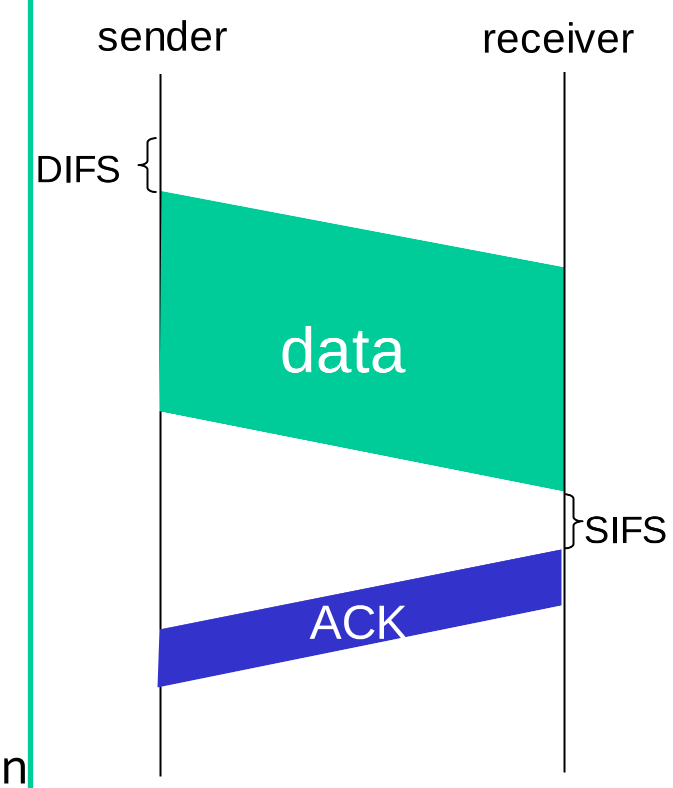
transmit when timer expires

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 (additional option in 802.11 MAC protocol): allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

sender first transmits *small* request-to-send (RTS) packets to BS using CSMA

- RTSs may still collide with each other (but they're short)

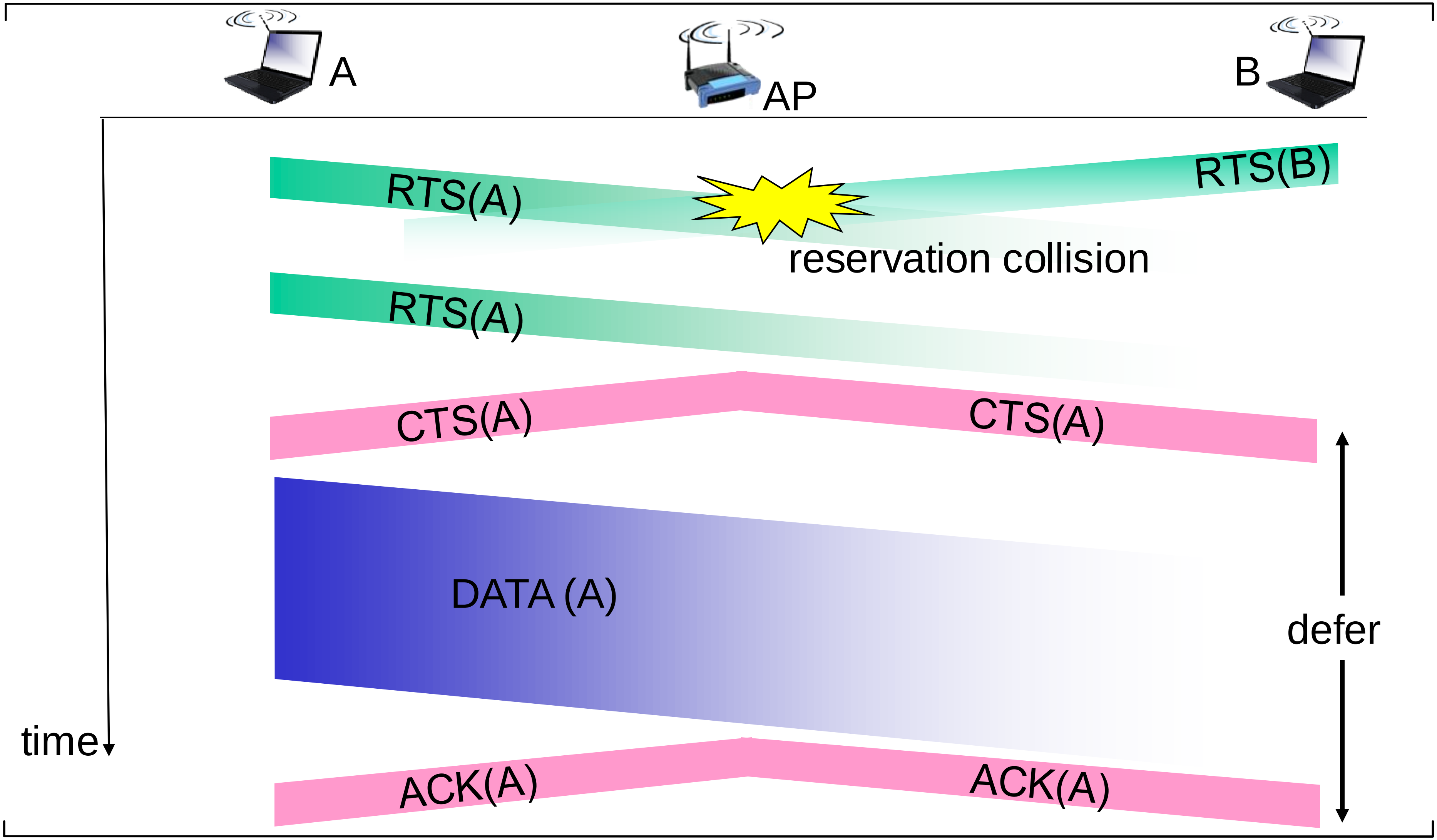
BS broadcasts clear-to-send CTS in response to RTS

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



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

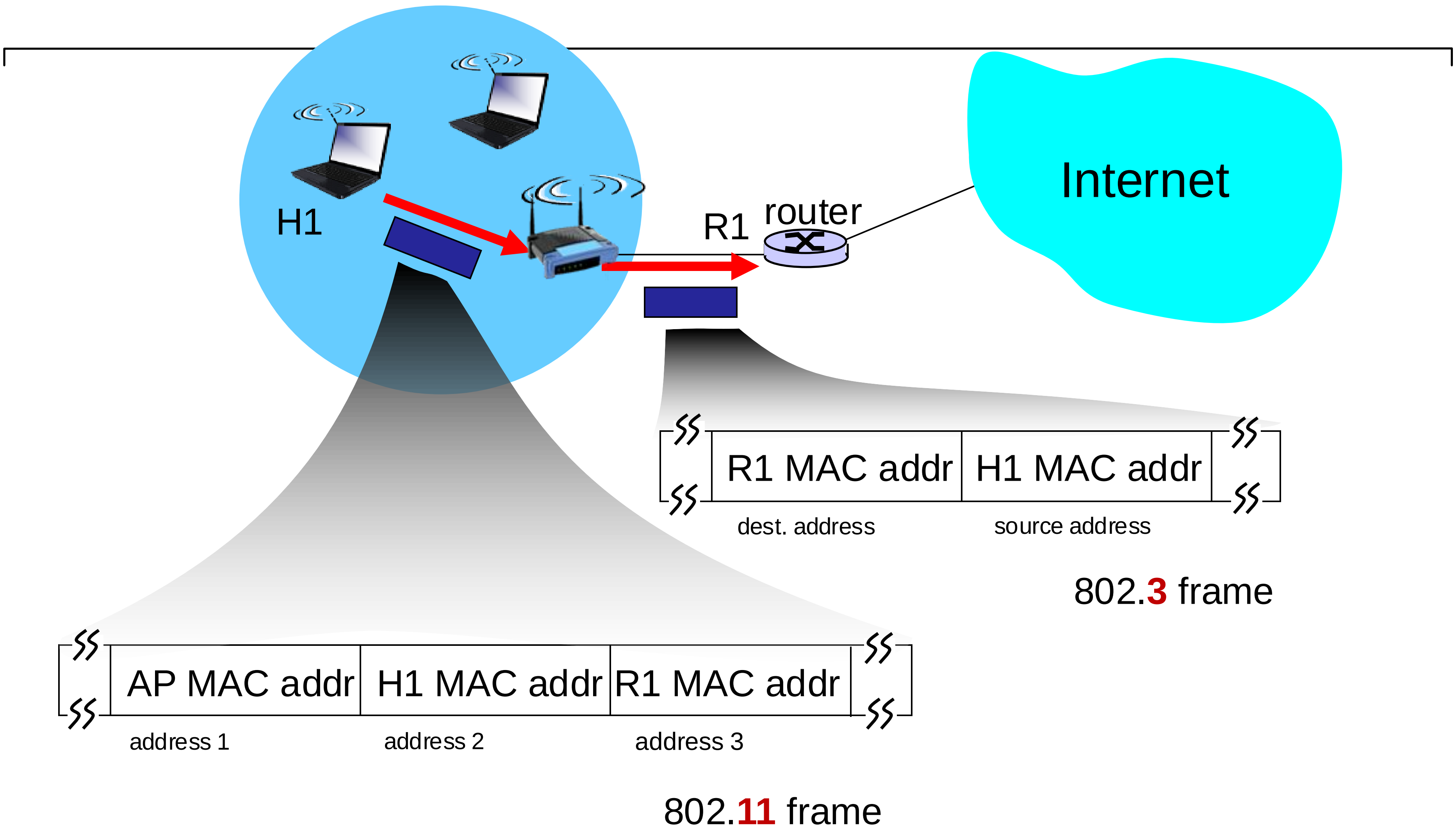
Address 4: used only in ad hoc mode

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

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

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

802.11 frame: addressing



802.11 frame: more

duration of reserved transmission time (RTS/CTS)

frame seq # (for RDT)

Bytes

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

Bits

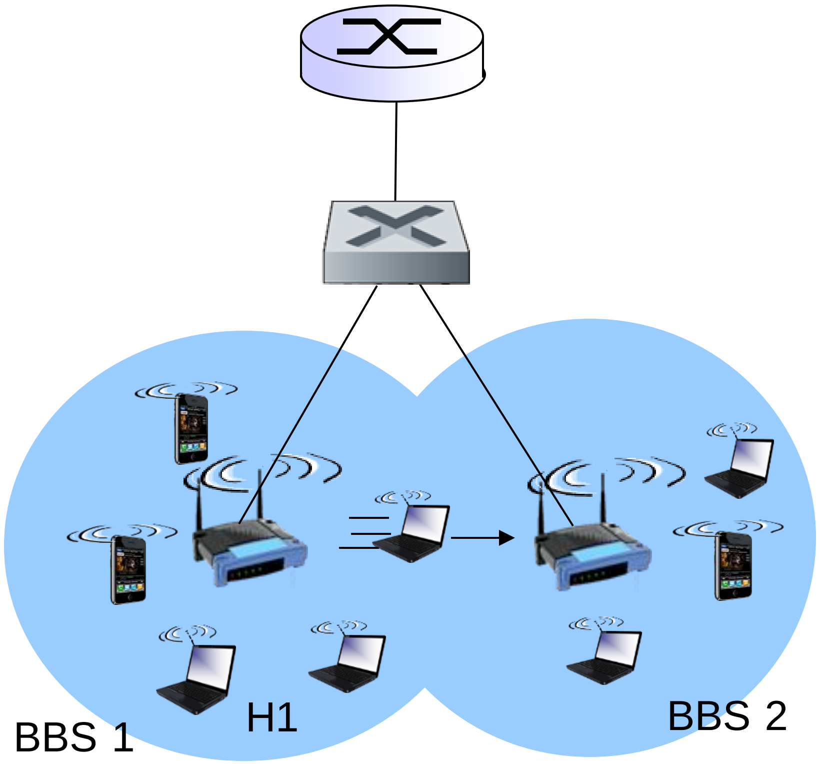
2	2	4	1	1	1	1	1	1	1	1
Protocol version	Type	Subtype	To AP	From AP	More frag	Retry	Power mgt	More data	WEP	Rsvd

frame type (RTS, CTS, ACK, data)

Wired Equivalent Privacy (**WEP**) is a security protocol for data confidentiality: indicates whether or not encryption is used

802.11: mobility within same subnet

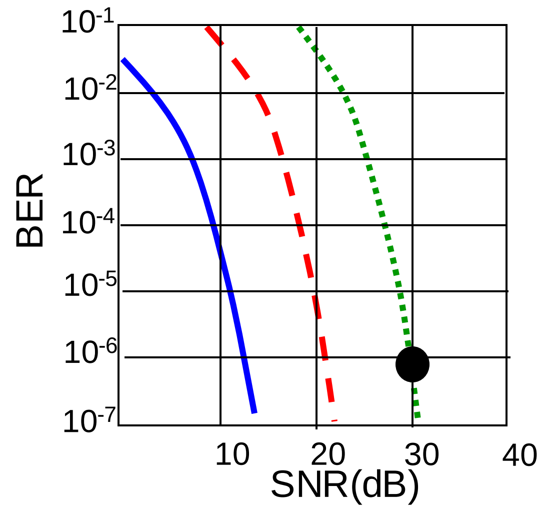
- H1 remains in same IP subnet: IP address can remain same
- APs have same SSID
- switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and “remember” which switch port can be used to reach H1
- Apply to VLAN connecting multiple LANs

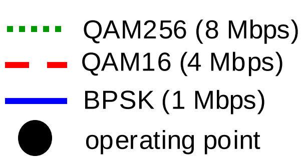


802.11: advanced capabilities

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

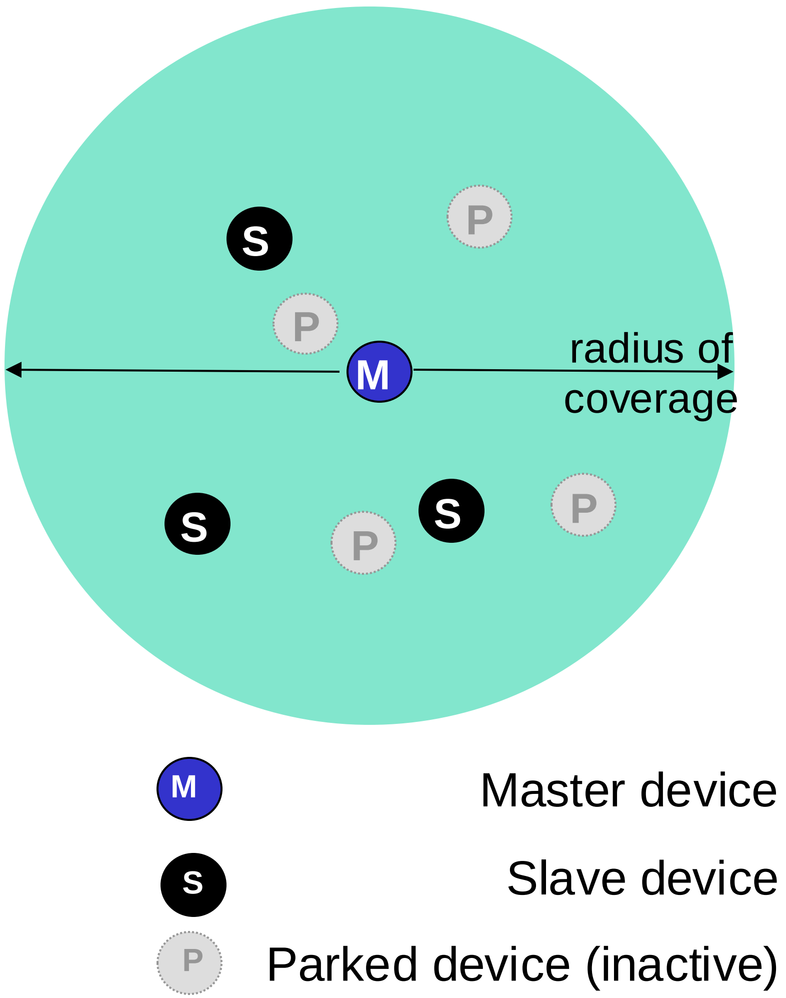
802.11: advanced capabilities

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

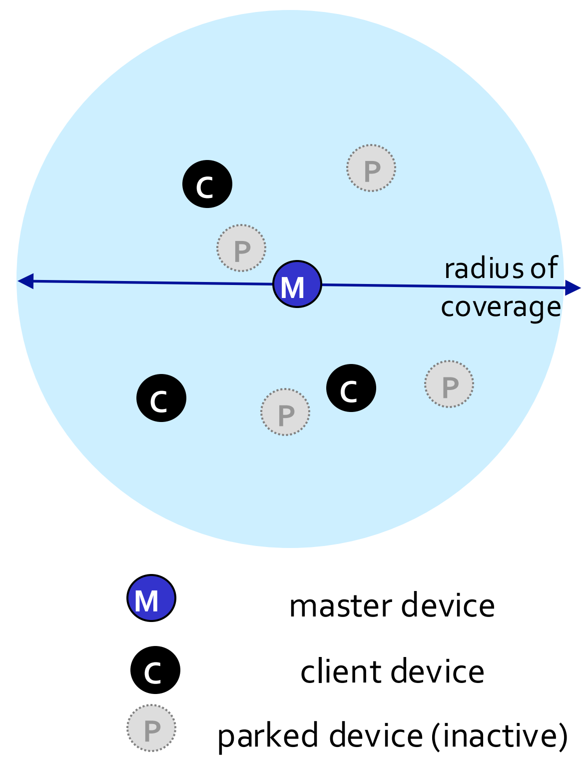
802.15: personal area network

- 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 3 Mbps
- 802.15.1 Bluetooth
- 802.15.4 Zigbee (lower powered, lower data rate)



Personal area networks: Bluetooth

- TDM, 625 msec sec. slot
- FDM: sender uses 79 frequency channels in known, pseudo-random order slot-to-slot (spread spectrum)
  - other devices/equipment not in piconet only interfere in some slots
- parked mode: clients can "go to sleep" (park) and later wakeup (to preserve battery)
- bootstrapping: nodes self-assemble (plug and play) into piconet



4G/5G cellular networks

- *the* solution for wide-area mobile Internet
- widespread deployment/use:
  - more mobile-broadband-connected devices than fixed-broadband-connected devices devices (5-1 in 2019)!
  - 4G availability: 97% of time in Korea (90% in US)
- transmission rates up to 100's Mbps
- technical standards: 3rd Generation Partnership Project (3GPP)
  - wwww.3gpp.org
  - 4G: Long-Term Evolution (LTE)standard

4G/5G cellular networks

similarities to wired Internet

- edge/core distinction, but both belong to same carrier
- global cellular network: a network of networks
- widespread use of protocols we've studied: HTTP, DNS, TCP, UDP, IP, NAT, separation of data/control planes, SDN, Ethernet, tunneling
- interconnected to wired Internet

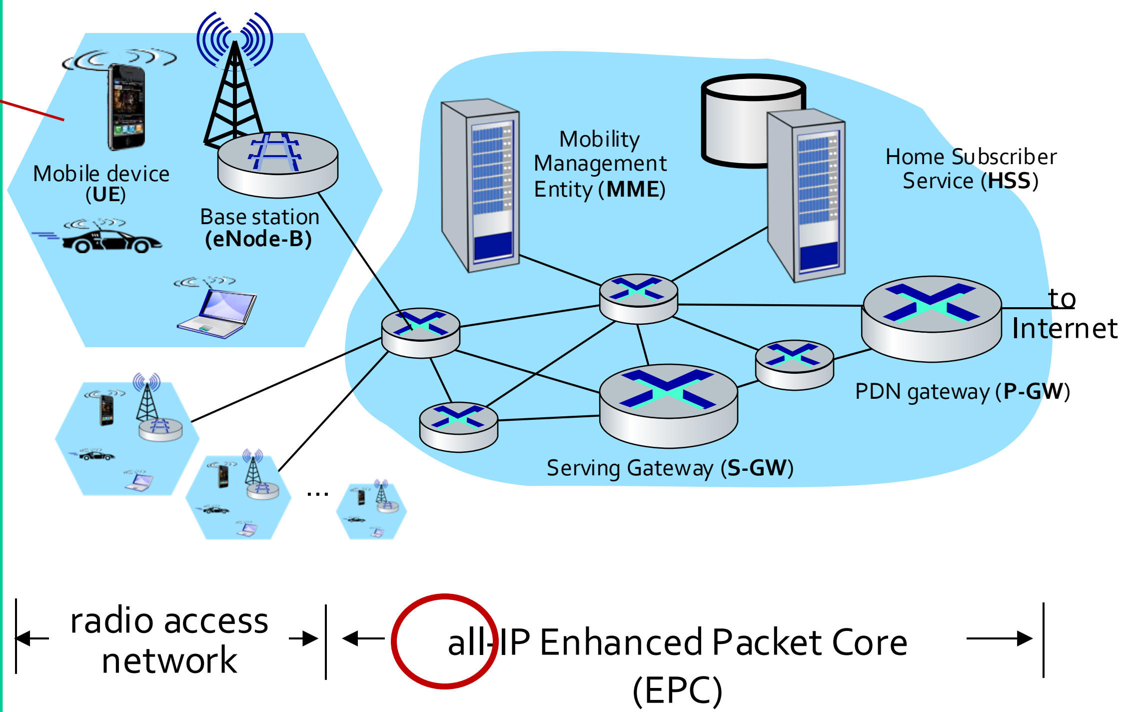
differences from wired Internet

- different wireless link layer
- mobility as a 1^{st} class service
- user "identity" (via SIM card)
- business model: users subscribe to a cellular provider
  - strong notion of "home network" versus roaming on visited nets
  - global access, with authentication infrastructure, and inter-carrier settlements

Elements of 4G LTE architecture

Mobile device:

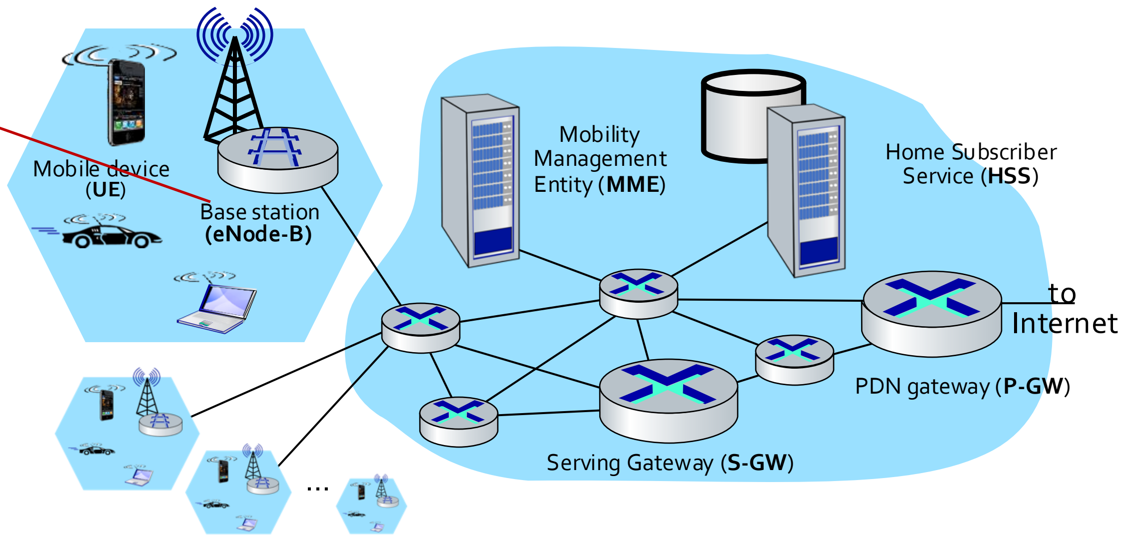
- smartphone, tablet, laptop, IoT, ... with 4G LTE radio
- 64-bit International Mobile Subscriber Identity (IMSI), stored on SIM (Subscriber Identity Module) card
- LTE jargon: User Equipment (UE)



Elements of 4G LTE architecture

Base station:

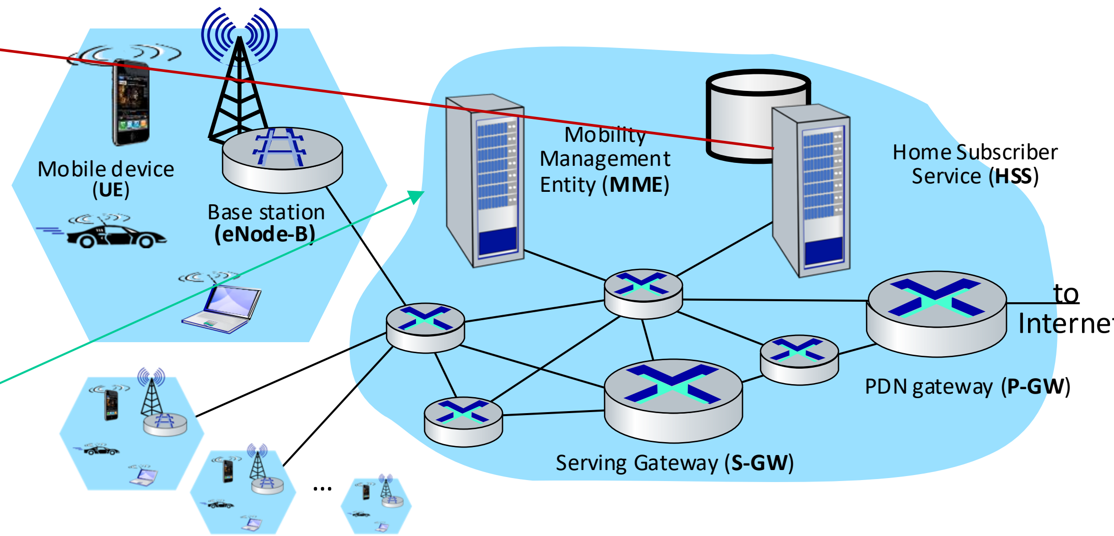
- at "edge" of carrier's network
- manages wireless radio resources, mobile devices in its coverage area ("cell")
- coordinates device authentication with other elements
- similar to WiFi AP but:
  - active role in user mobility
  - coordinates with nearly base stations to optimize radio use
- LTE jargon: eNode-B



Elements of 4G LTE architecture

Home Subscriber Service

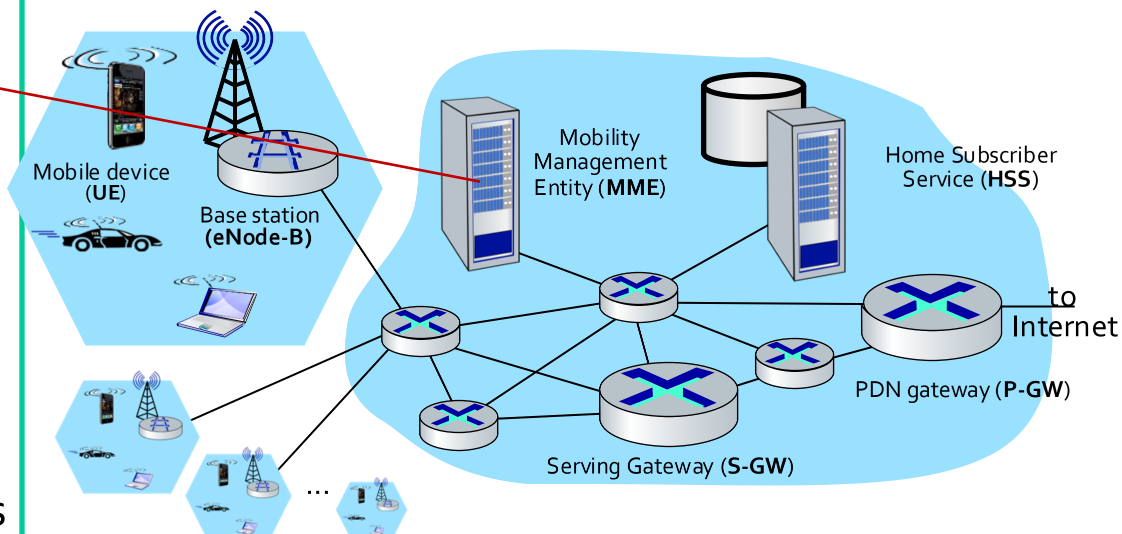
- stores info about mobile devices for which the HSS's network is their "home network"
- works with MME (Mobility Management Entity) in device authentication



Elements of 4G LTE architecture

Mobility Management Entity

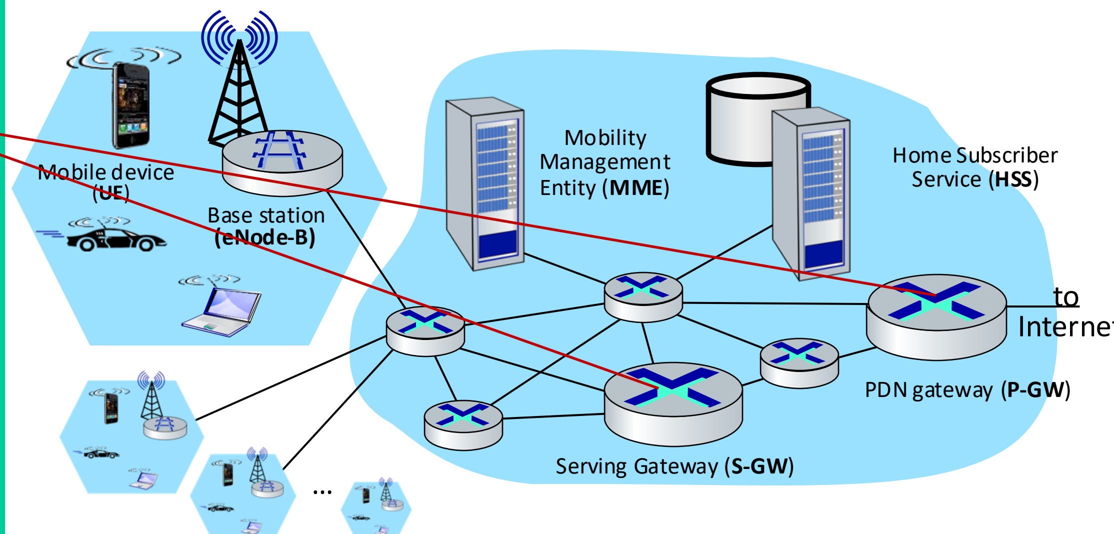
- device authentication (device-to-network, network-to-device) coordinated with mobile home network HSS
- mobile device management:
  - device handover between cells
  - tracking/paging device location
- path (tunneling) setup from mobile device to P-GW



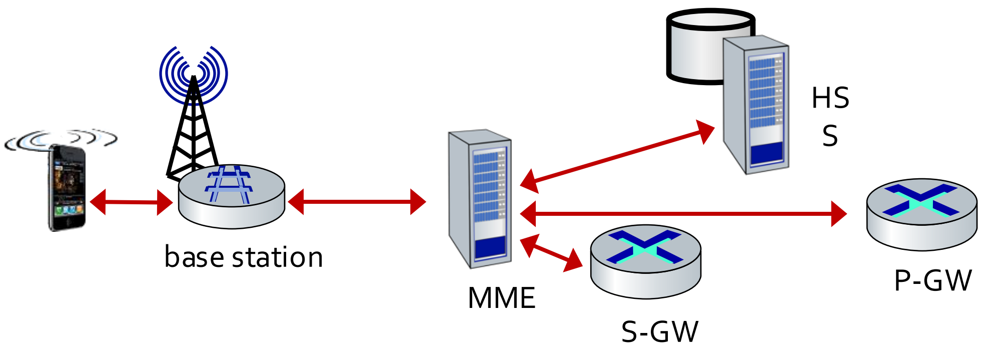
Elements of 4G LTE architecture

Serving Gateway (S-GW), PDN Gateway (P-GW)

- lie on data path from mobile to/from Internet
- P-GW
  - gateway to mobile cellular network
  - Looks like any other internet gateway router
  - provides NAT services
- other routers:
  - extensive use of tunneling

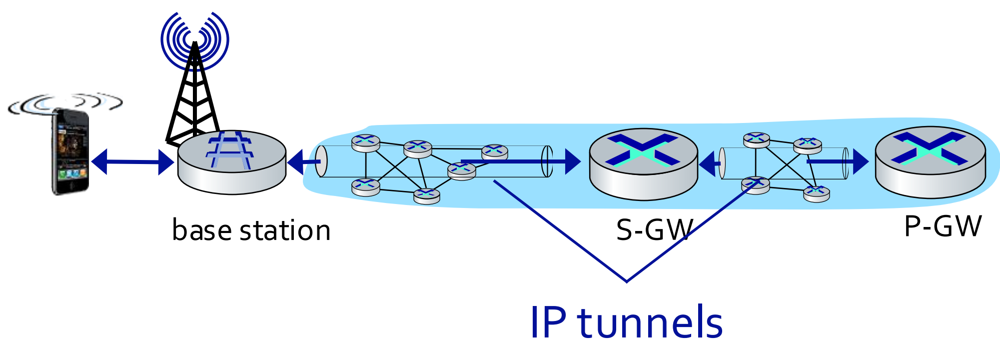


LTE: data plane control plane separation



control plane

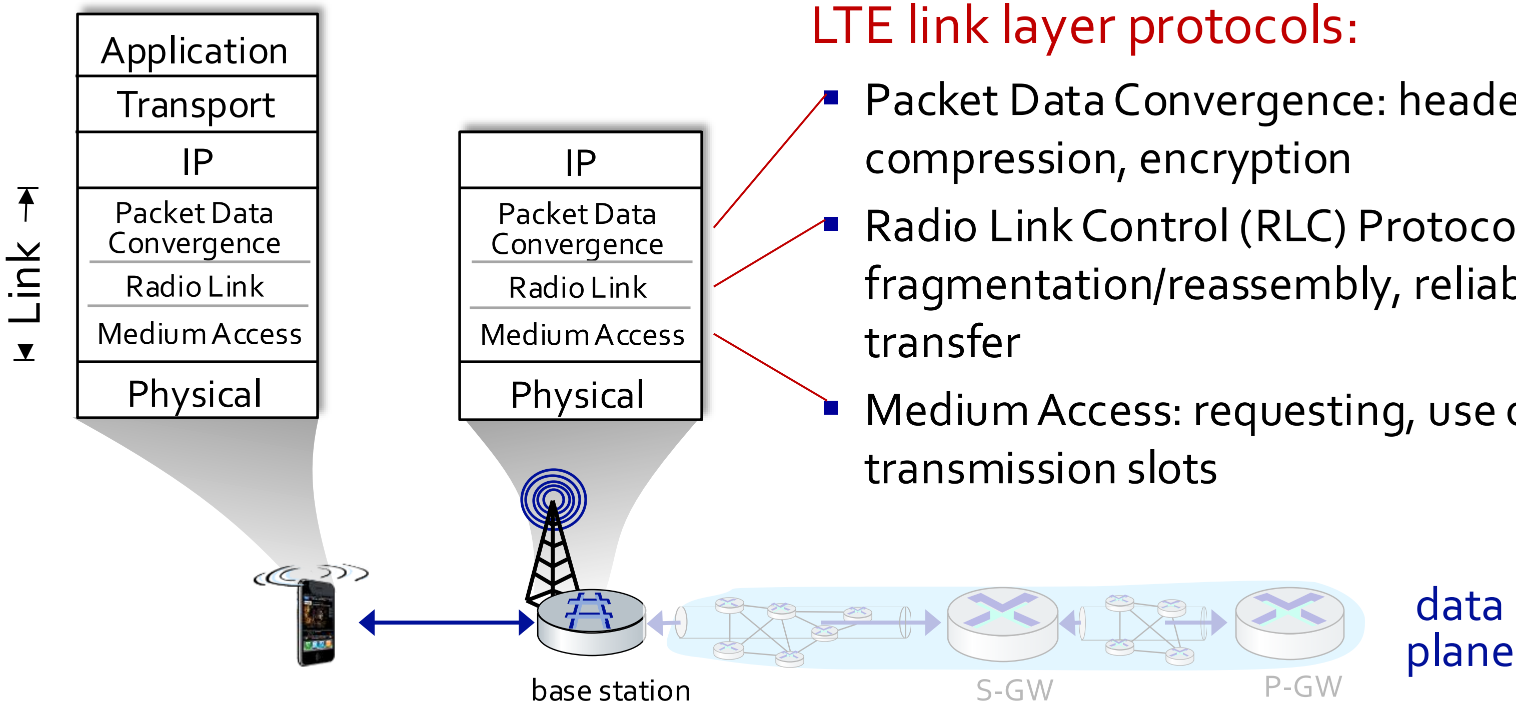
- new protocols for mobility management , security, authentication



data plane

- new protocols at link, physical layers
- extensive use of tunneling to facilitate mobility

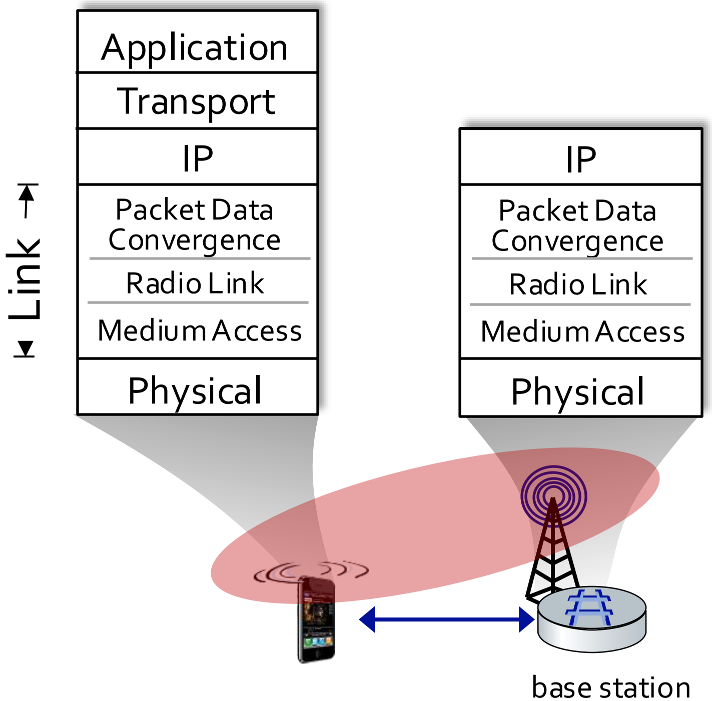
LTE data plane protocol stack: first hop



LTE link layer protocols:

- Packet Data Convergence: header compression, encryption
- Radio Link Control (RLC) Protocol: fragmentation/reassembly, reliable data transfer
- Medium Access: requesting, use of radio transmission slots

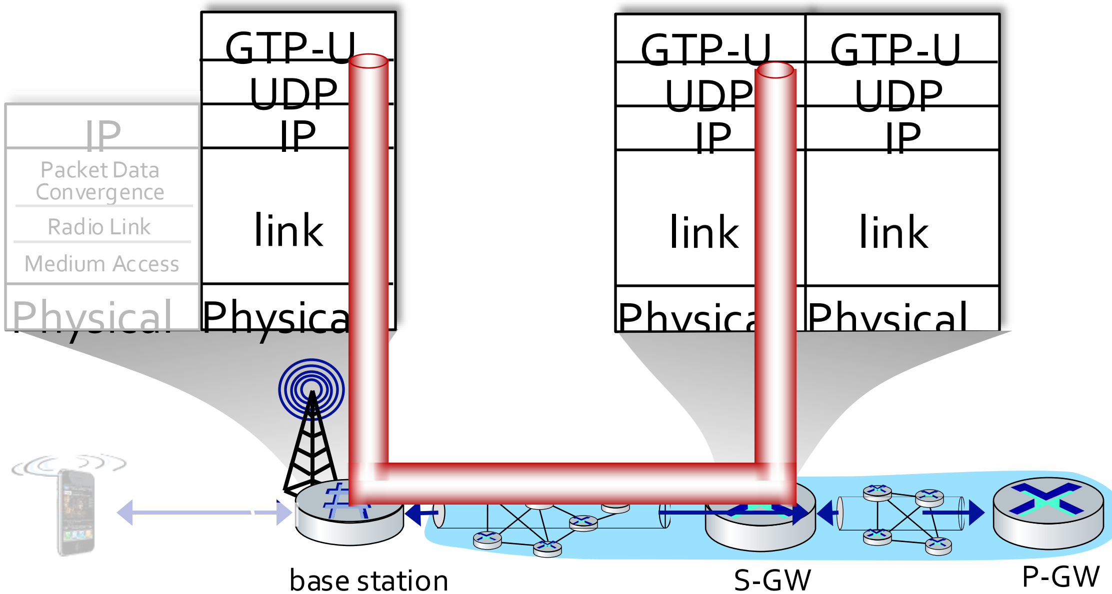
LTE data plane protocol stack: first hop



LTE radio access network:

- downstream channel: FDM, TDM within frequency channel (OFDM - orthogonal frequency division multiplexing)
  - "orthogonal": minimal interference between channels
  - upstream: FDM, TDM similar to OFDM
- each active mobile device allocated two or more 0.5 ms time slots over 12 frequencies
  - scheduling algorithm not standardized – up to operator
  - 100's Mbps per device possible

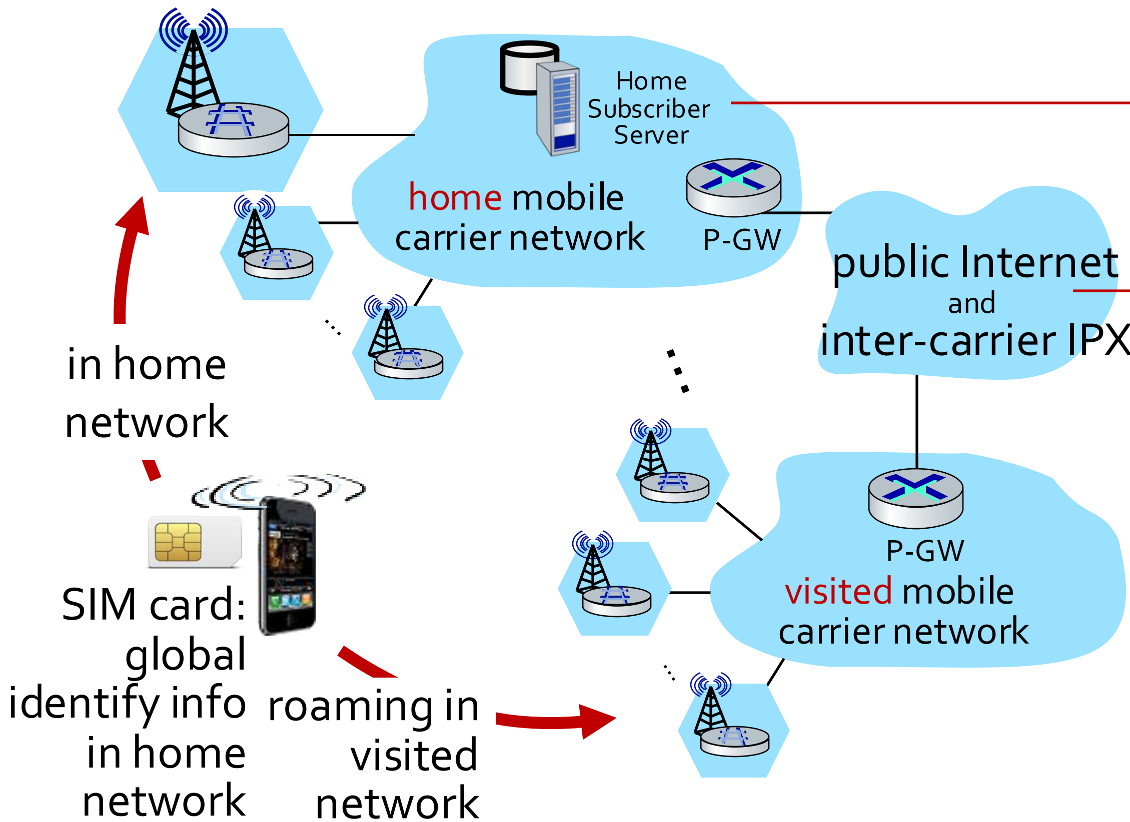
LTE data plane protocol stack: packet core



tunneling:

- mobile datagram encapsulated using GPRS Tunneling Protocol (GTP), sent inside UDP datagram to S-GW
- S-GW re-tunnels datagrams to P-GW
- supporting mobility: only tunneling endpoints change when mobile user moves

Global cellular network: a network of IP networks



home network HSS:

- identify & services info, while in home network and roaming

all IP:

- carriers interconnect with each other, and public internet at exchange points
- legacy 2G, 3G: not all IP, handled otherwise

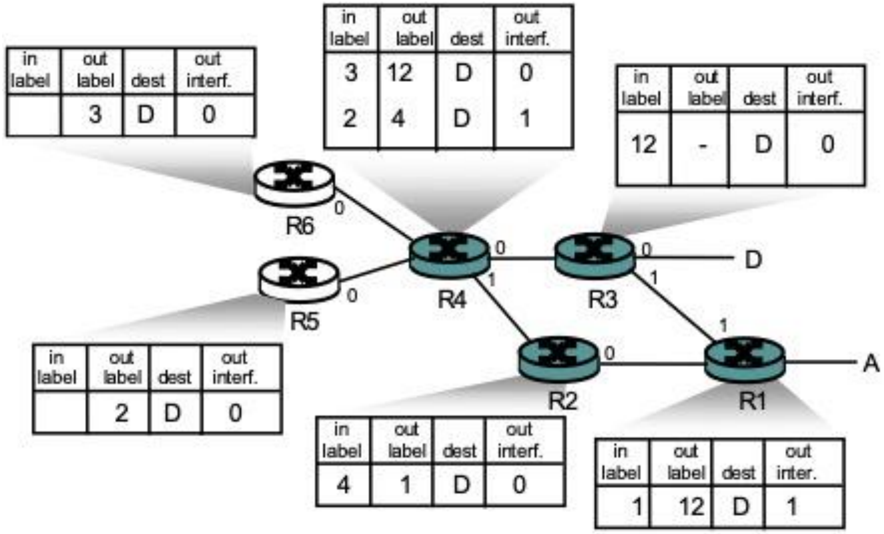
On to 5G!

- goal: 10x increase in peak bitrate, 10x decrease in latency, 100x increase in traffic capacity over 4G
- 5G NR (new radio):
  - two frequency bands: FR1 (450 MHz–6 GHz) and FR2 (24 GHz–52 GHz): millimeter wave frequencies
  - not backwards-compatible with 4G
  - MIMO: multiple directional antennae
- millimeter wave frequencies: much higher data rates, but over shorter distances
  - pico-cells: cells diameters: 10-100 m
  - massive, dense deployment of new base stations required

Review questions

Multiprotocol Label Switching (MPLS) evolved from a number of industry efforts in the mid-to-late 1990s to improve the forwarding speed of IP routers by adopting a key concept from the world of virtual-circuit networks: a fixed-length label. The goal was not to abandon the destination-based IP datagram-forwarding infrastructure for one based on fixed-length labels and virtual circuits, but to augment it by selectively labeling datagrams and allowing routers to forward datagrams based on fixed-length labels (rather than destination IP addresses) when possible. Consider below MPLS network with all routers R1 - R6 are MPLS enabled. In this case, the forwarding tables are MPLS-enhanced forwarding with no destination IP addresses. In this MPLS network example, each router has a forwarding table as indicated in the figure below.

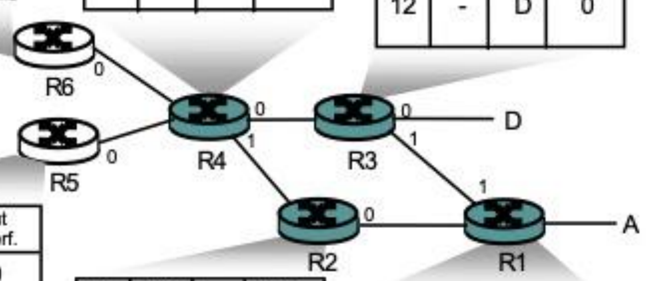
Suppose the packets from R5 are destined for D, in this case these packets will be switched via: R5 - .....



Review questions

Multiprotocol Label Switching (MPLS) evolved from a number of industry efforts in the mid-to-late 1990s to improve the forwarding speed of IP routers by adopting a key concept from the world of virtual-circuit networks: a fixed-length label. The goal was not to abandon the destination-based IP datagram-forwarding infrastructure for one based on fixed-length labels and virtual circuits, but to augment it by selectively labeling datagrams and allowing routers to forward datagrams based on fixed-length labels (rather than destination IP addresses) when possible. Consider below MPLS network with all routers R1 - R6 are MPLS enabled. In this case, the forwarding tables are MPLS-enhanced forwarding with no destination IP addresses. In this MPLS network example, each router has a forwarding table as indicated in the figure below.

Suppose the packets from R5 are destined for D packets will be switched via: R5 – R4 – R2 – R1 – R3



R6:

in label	out label	dest	out interf.
	3	D	0

R4:

in label	out label	dest	out interf.
3	12	D	0
2	4	D	1

R3:

in label	out label	dest	out interf.
12	-	D	0

R5:

in label	out label	dest	out interf.
	2	D	0

R2:

in label	out label	dest	out interf.
4	1	D	0

R1:

in label	out label	dest	out inter.
1	12	D	1

Quiz questions

- With the CSMA/CD protocol, the adapter waits K·512 bit times after a collision, where K is drawn randomly. For K=100 and a 100 Mbps broadcast channel that connects nodes with a distance of 50 Km and a propagation speed $3x10^8$ m/sec. Assume a frame is 1 MTU = 1500B. What is the channel efficiency?

- Suppose nodes A and B transmit over a 10 Mbps broadcast channel with a propagation delay between the nodes equals to 325s. Suppose CSMA/CD and Ethernet packets are used for this broadcast channel. If node A begins transmitting a frame and, before it finishes at time t = 576s (minimum timed frame 512+64), node B begins transmitting a frame. Can node A finish transmitting before it detects that node B has transmitted? *Hint: In the worst case, node B begins transmitting at time t = 324, which is the time right before the first bit of A's frame arrives at B.*

Quiz questions

- With the CSMA/CD protocol, the adapter waits K·512 bit times after a collision, where K is drawn randomly. For K=100 and a 100 Mbps broadcast channel that connects nodes with a distance of 50 Km and a propagation speed $3x10^8$ m/sec. Assume a frame is 1 MTU = 1500B. What is the channel efficiency?

Efficiency = $1/(1+5t_{prop}/t_{trans})$ → $t_{prop} = 50x10^3/3x10^8 = (50/3)x10^{-5}$ and $t_{trans} = 1500x8/100x10^6 = 120x10^{-6}$ → $1/(1+5[(50/3)\ x10^{-5}/(120x10^{-6})]) = 1/(1+(250/36)) = 12\%$

- Suppose nodes A and B transmit over a 10 Mbps broadcast channel with a propagation delay between the nodes equals to 325s. Suppose CSMA/CD and Ethernet packets are used for this broadcast channel. If node A begins transmitting a frame and, before it finishes at time t = 576s (minimum timed frame 512+64), node B begins transmitting a frame. Can node A finish transmitting before it detects that node B has transmitted? *Hint: In the worst case, node B begins transmitting at time t = 324, which is the time right before the first bit of A's frame arrives at B.*

t = 0 → A begins to transmit
t = 576 → A finishes transmitting
t = 324 → B begins to transmit
t = 324 + 325 (propagation delay from B to A) = 649 for B's first bit to arrive at A.
Because A finishes at t = 576 before it detects B's transmission at t = 649, then Yes finishes transmission before detection, and so with collision.

Review questions

- What is meant when we say that a network of devices is operating in "infrastructure mode"?
  - Devices communicate with each other and to the larger outside world via a base station (also known as an access point).
- What are the characteristics of wireless links:
  - The bit error rate (BER) of a wireless channel *decreases* as the signal-to-noise ratio (SNR) increases.
  - The "hidden terminal problem" happens when A sends to B over a wireless channel, and an observer, C (that can be even closer to A than B), does not detect/receive A's transmission because of physical obstacles in the path between A and C.
  - Multipath propagation occurs when portions of the electromagnetic wave reflect off objects and the ground taking paths of different lengths between the sender and a receiver, and thus arriving at the receiver at slightly different points in time.
  - Path loss refers to the decrease in the strength of a radio signal as it propagates through space.

Summary

Today:

- Wireless networks
  - Wireless hosts, base stations, and links
- SNR vs. BER
- CDMA/ CD and CA
- 802.11 LAN, channels, addressing, mobilities and capabilities
- Cellular networks, 2G, 3G, 5G, LTE

Canvas discussion:

- Reflection
- Exit ticket

Next time:

- read 8.1, 8.2 and 8.3 of K&R (security)
- follow on Canvas! material and announcements

Any questions?