

CS 3800: Computer Networks

Lecture 8: Link Layer (Wired & Wireless Networks)

Instructor: John Korah

Acknowledgement

- The following slides include material from author resources for:
 - KR Text book
 - “Data and computer communications,” William Stallings, Tenth edition

Learning Goals

- Understand the services provided by link layer
- Understand how packets are addressed and transmitted within the link layer.
- Link Layer mechanisms for wired and wireless networks
 - Understand protocols that allow medium sharing
 - Addressing in Link Layers
- Study key aspects of wireless communication

Topics

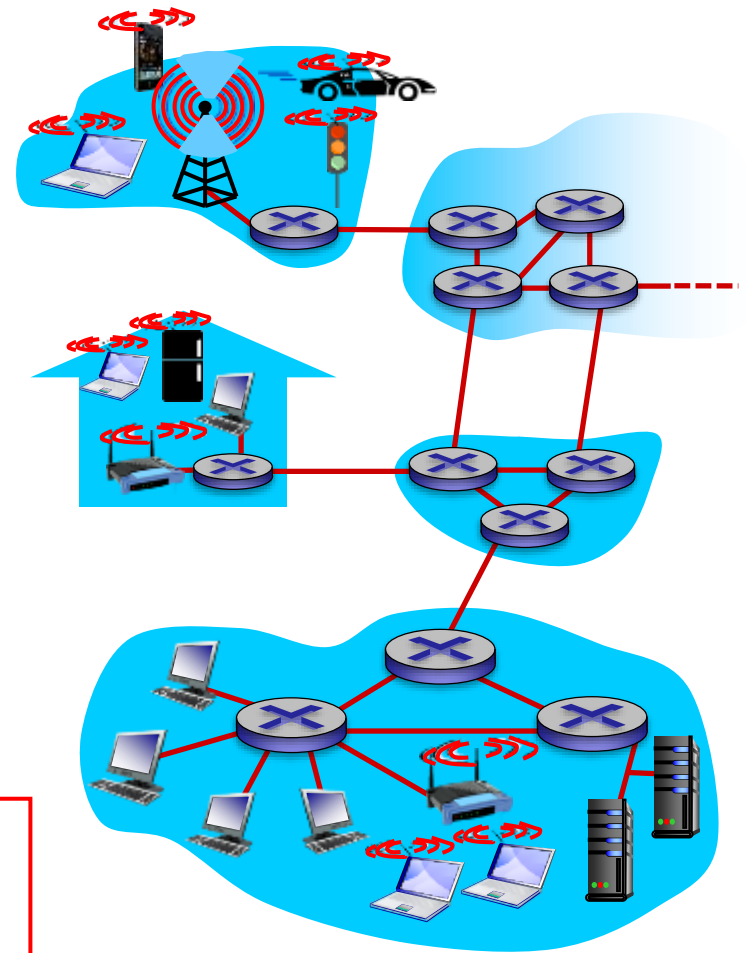
- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

Recall: Link layer

Recall:

- communication channels that connect adjacent nodes along communication path: **links**
 - wired links
 - wireless links
 - LANs
- layer-2 packet: **frame**, encapsulates datagram

data-link layer has responsibility of transferring datagram from one node to *physically adjacent* node over a link



Link layer services

- *framing, link access:*

- encapsulate datagram into frame, adding header, trailer
- channel access if shared medium
- Medium Access Control (MAC) addresses used in frame headers to identify source, destination
 - different from IP address!

- *flow control:*

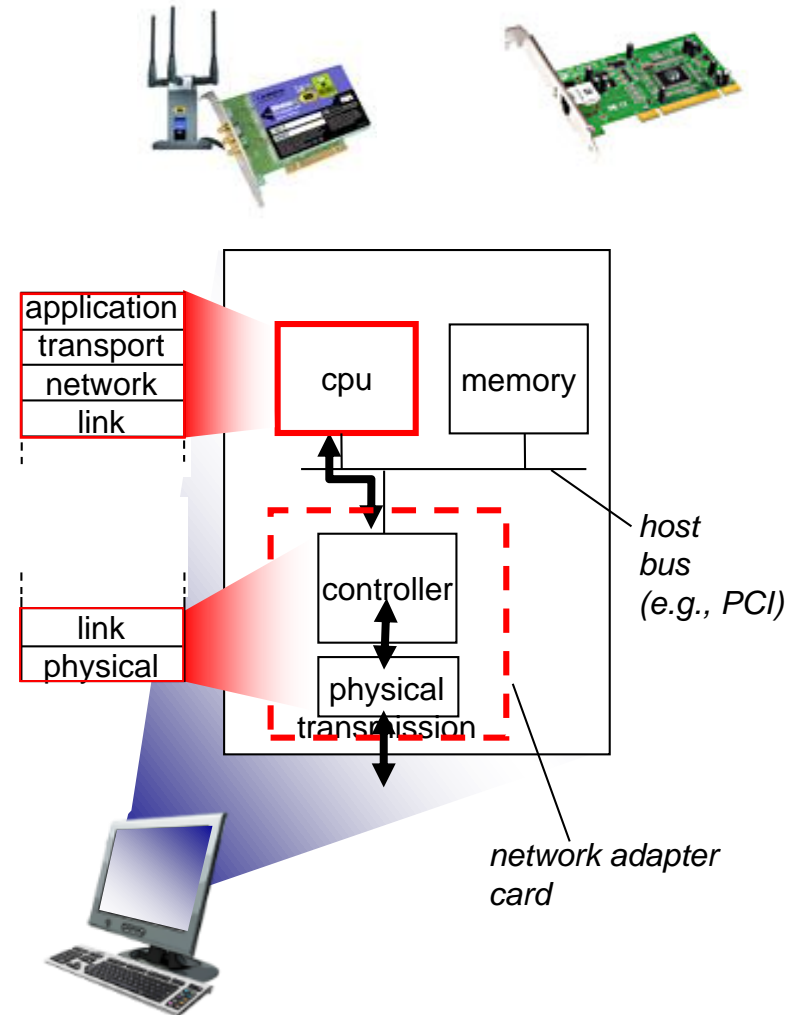
- pacing between adjacent sending and receiving nodes

Link layer services (more)

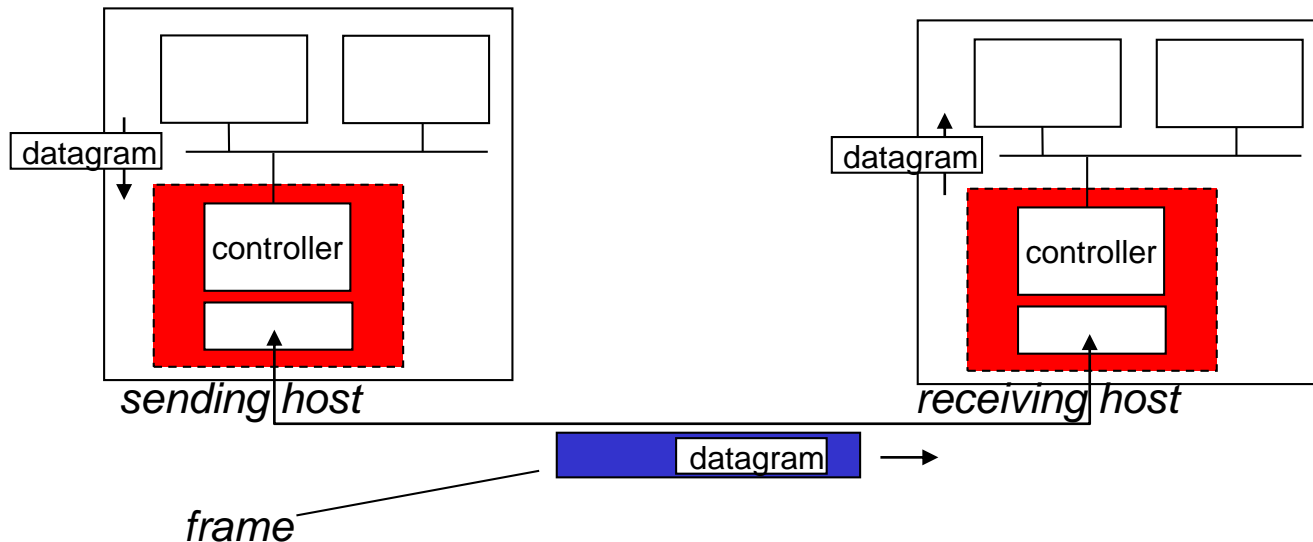
- *error detection:*
 - errors caused by signal attenuation, noise.
 - receiver detects presence of errors:
 - signals sender for retransmission or drops frame
- *error correction:*
 - receiver identifies *and corrects* bit error(s) without resorting to retransmission
- *half-duplex and full-duplex*
 - with half duplex, nodes at both ends of link can transmit, but not at same time

Where is the link layer implemented?

- In each and every host
- link layer implemented in “adaptor” (aka *network interface card* NIC) or on a chip
 - Ethernet card, Wireless (802.11) card
 - implements link, physical layer



Adaptors communicating



- sending side:
 - encapsulates datagram in frame
 - adds error checking bits, rdt, flow control, etc.
- receiving side
 - looks for errors, rdt, flow control, etc.
 - extracts datagram, passes to upper layer at receiving side

Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

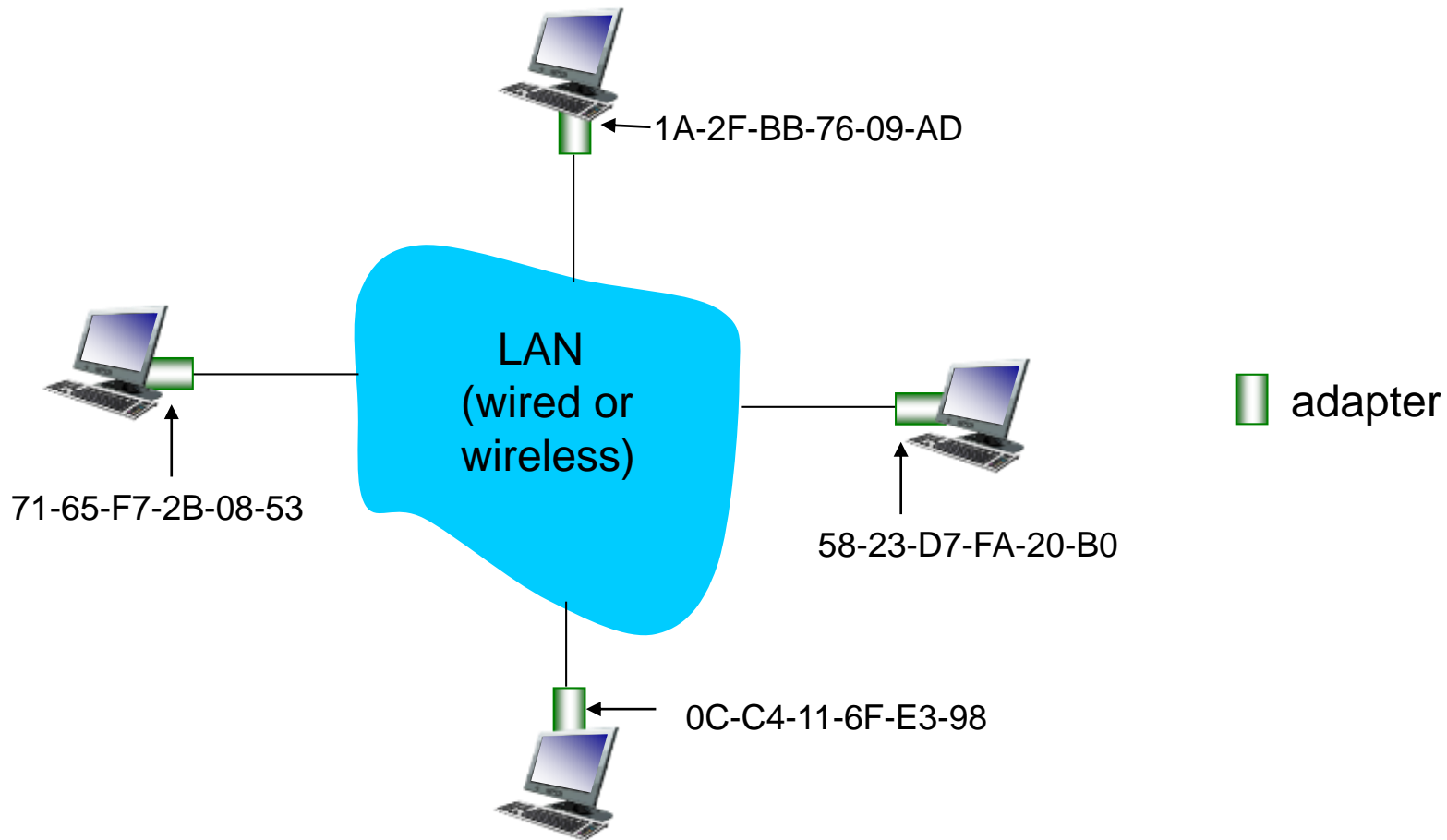
Medium Access Control (MAC) addresses

- 32-bit IP address:
 - *network-layer* address for interface
 - used for layer 3 (network layer) forwarding
- MAC (or LAN or physical or Ethernet) address:
 - function: *used ‘locally’ to get frame from one interface to another physically-connected interface (same network, in IP-addressing sense)*
 - 48 bit MAC address (for most LANs) burned in NIC ROM, also sometimes software settable
 - e.g.: 1A-2F-BB-76-09-AD

hexadecimal (base 16) notation
(each “numeral” represents 4 bits)

LAN addresses

each adapter on LAN has unique **LAN** address

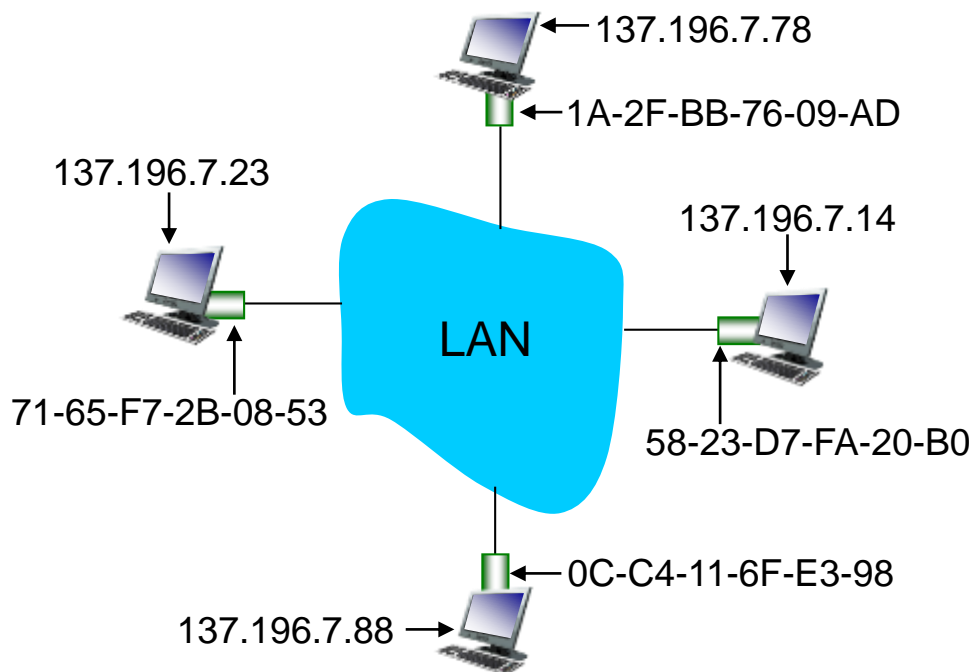


Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

Address Resolution Protocol (ARP)

Question: how to determine interface's MAC address, knowing its IP address?



ARP table: each IP node (host, router) on LAN has table

- IP/MAC address mappings for some LAN nodes:
< IP address; MAC address; TTL >
- TTL (Time To Live): time after which address mapping will be forgotten (typically 20 min)

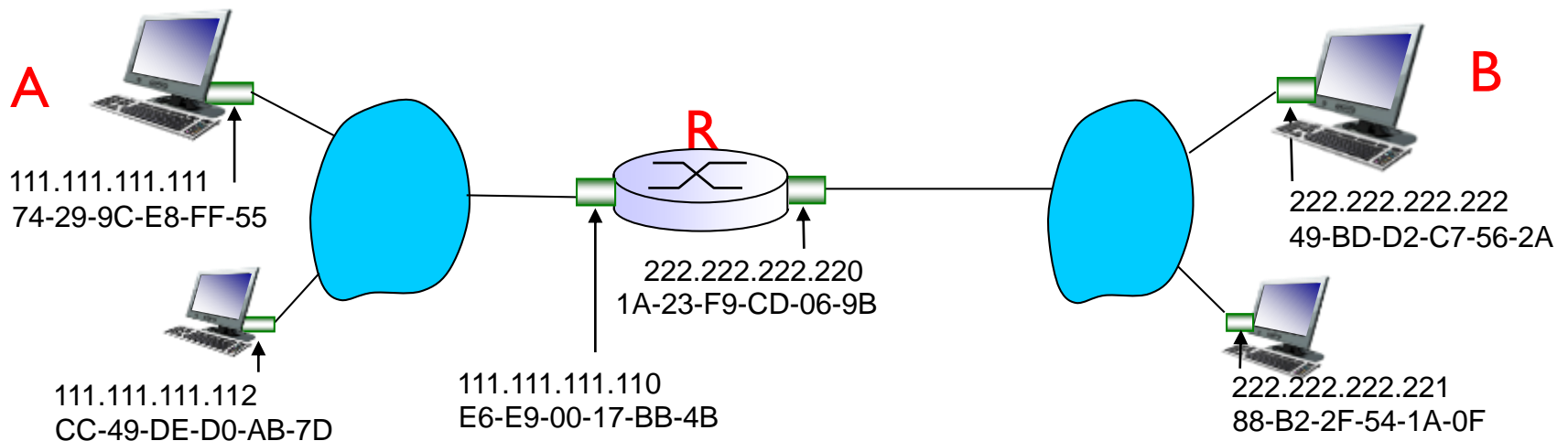
ARP protocol: same LAN

- A wants to send datagram to B
 - B's MAC address not in A's ARP table.
- A **broadcasts** ARP query packet, containing B's IP address
 - destination MAC address = FF-FF-FF-FF-FF-FF
 - all nodes on LAN receive ARP query
- B receives ARP packet, replies to A with its (B's) MAC address
 - frame sent to A's MAC address (unicast)
- A caches (saves) IP-to-MAC address pair in its ARP table until information becomes old (times out)
 - soft state: information that times out (goes away) unless refreshed
- ARP is “plug-and-play”:
 - nodes create their ARP tables *without intervention from net administrator*

Addressing: routing to another LAN

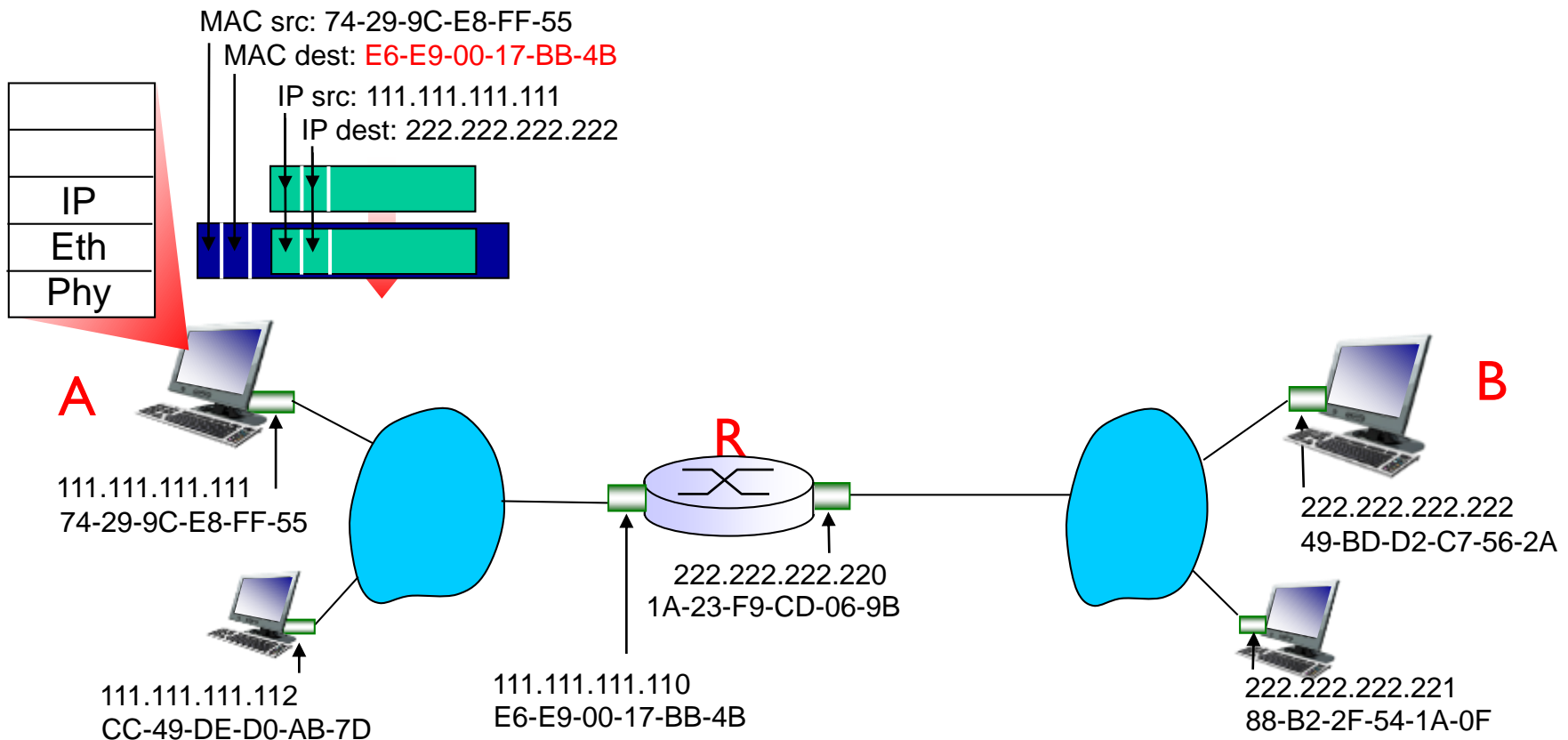
walkthrough: **send datagram from A to B via R**

- focus on addressing – at IP (datagram) and MAC layer (frame)
- assume A knows B's IP address
- assume A knows IP address of first hop router, R (how?)
- assume A knows R's MAC address (how?)



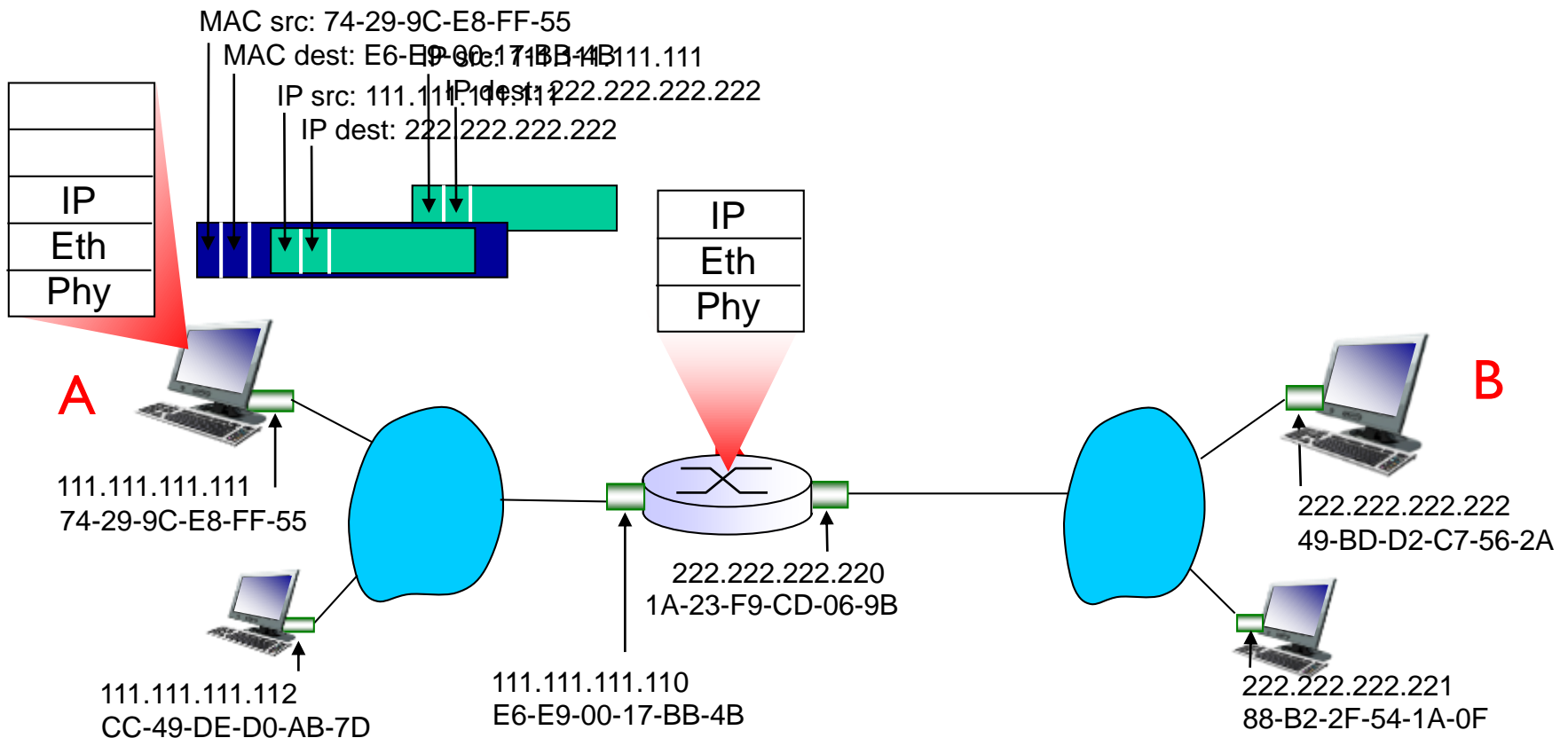
Addressing: routing to another LAN

- A creates IP datagram with IP source A, destination B
- A creates link-layer frame with R's MAC address as destination address, frame contains A-to-B IP datagram



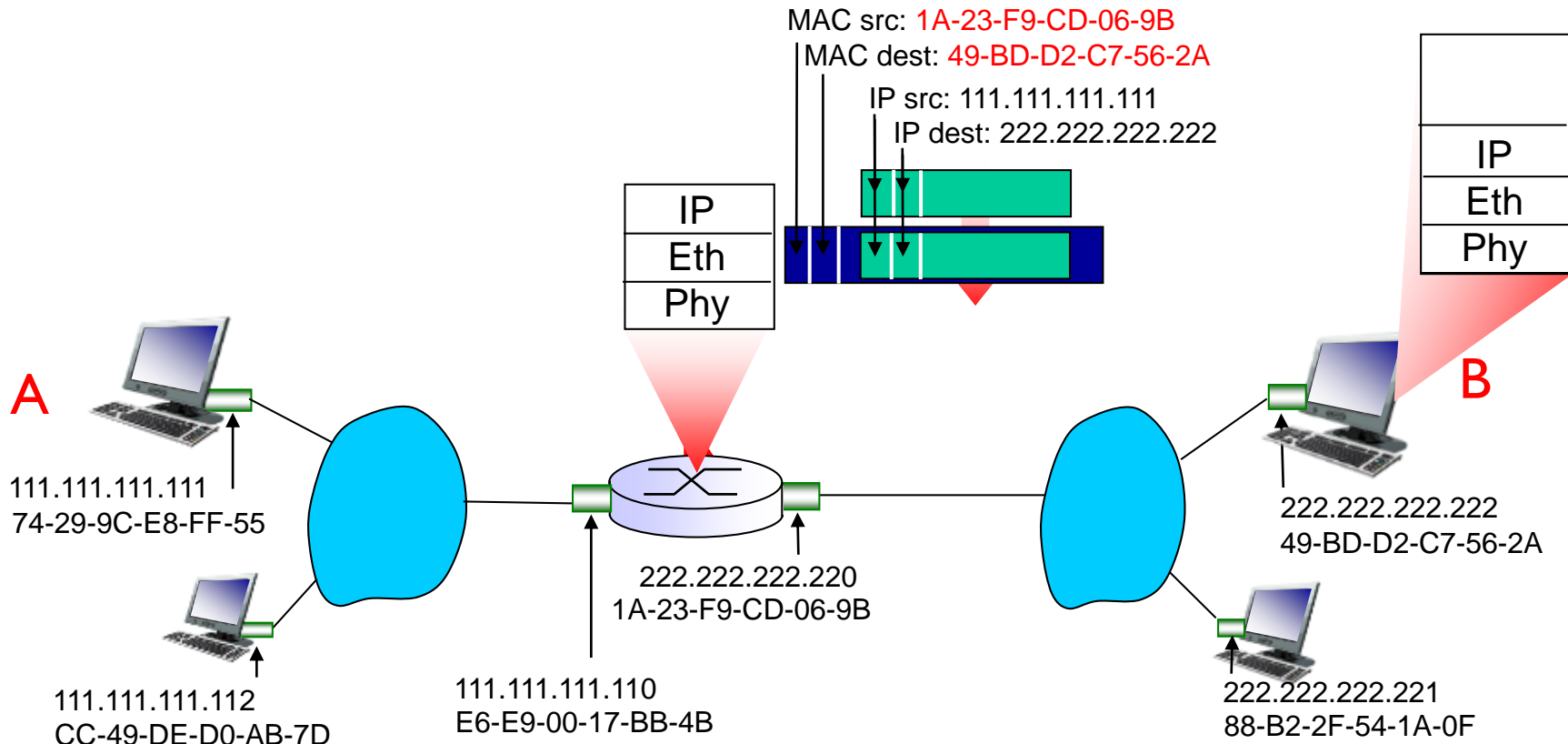
Addressing: routing to another LAN

- frame sent from A to R
- frame received at R, datagram removed, passed up to IP



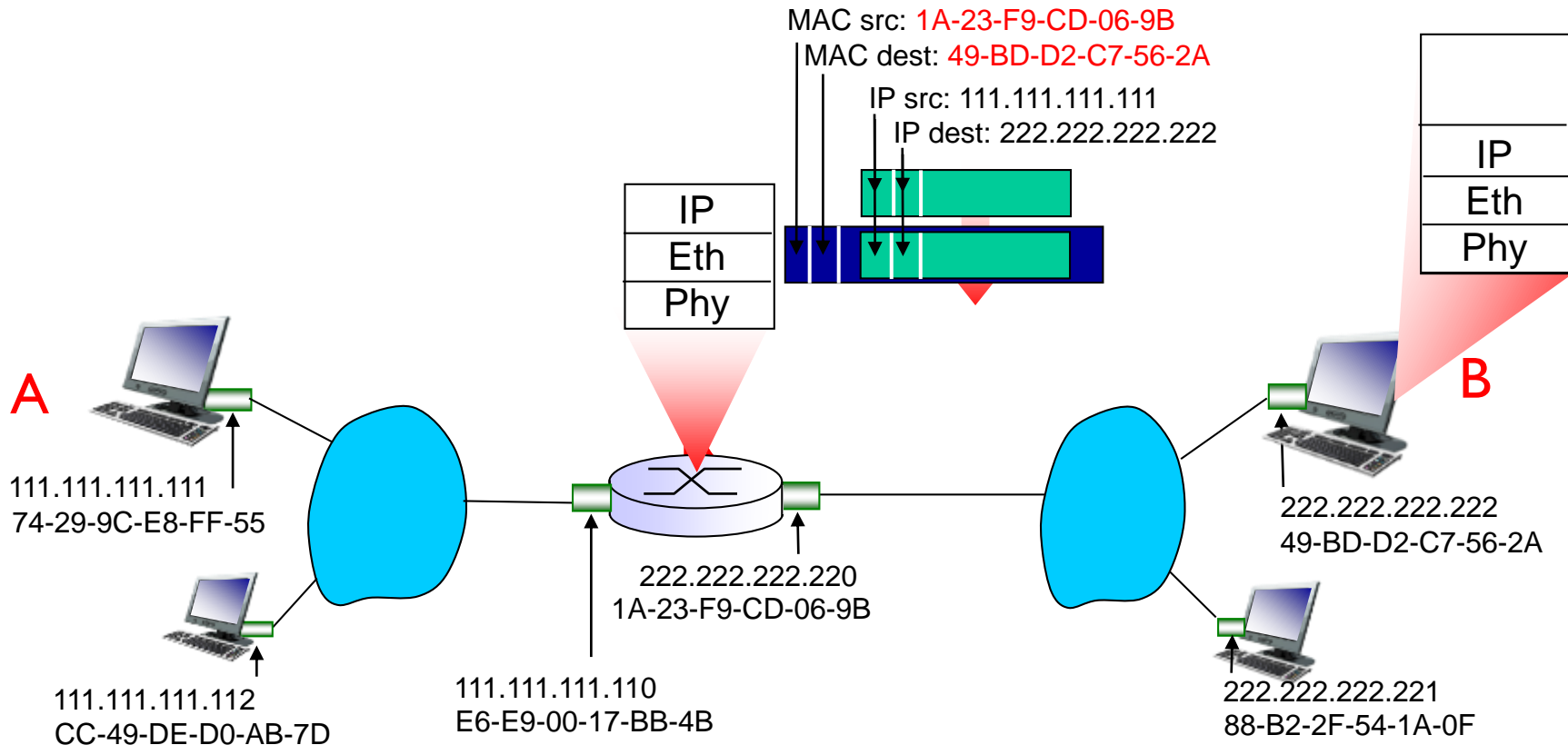
Addressing: routing to another LAN

- R forwards datagram with IP source A, destination B
- R creates link-layer frame with B's MAC address as destination address, frame contains A-to-B IP datagram



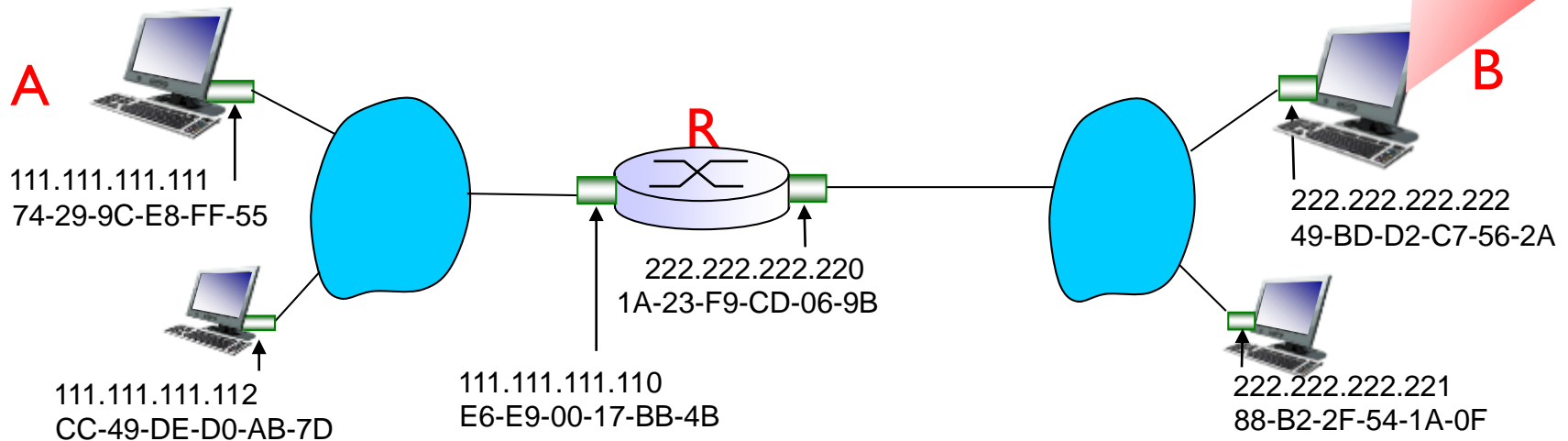
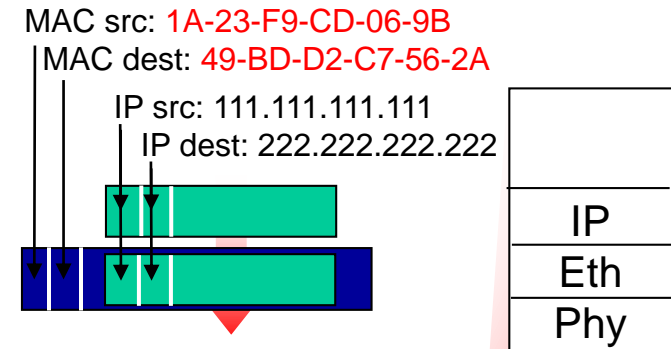
Addressing: routing to another LAN

- R forwards datagram with IP source A, destination B
- R creates link-layer frame with B's MAC address as destination address, frame contains A-to-B IP datagram



Addressing: routing to another LAN

- R forwards datagram with IP source A, destination B
- R creates link-layer frame with B's MAC address as dest, frame contains A-to-B IP datagram



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- **Wired Networks**
 - **Ethernet**
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

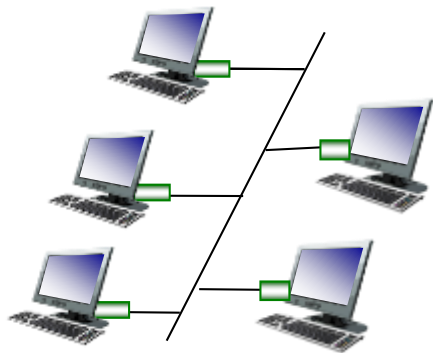
Ethernet

“dominant” wired LAN technology:

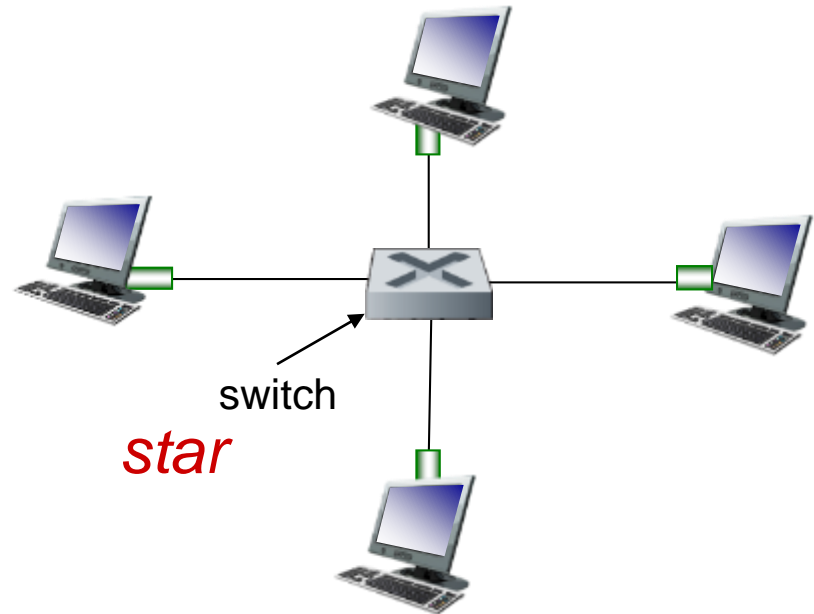
- simpler, cheap
- kept up with speed race: 10 Mbps – 10 Gbps

Ethernet: physical topology

- **bus:** popular through mid 90s
 - all nodes in same collision domain (can collide with each other)
- **star:** prevails today
 - active **switch** in center
 - each “spoke” runs a (separate) Ethernet protocol (nodes do not collide with each other)



bus: coaxial cable



Ethernet frame structure

sending adapter encapsulates IP datagram (or other network layer protocol packet) in **Ethernet frame**



preamble:

- 7 bytes with pattern 10101010 followed by one byte with pattern 10101011
- used to synchronize receiver, sender clock rates

Ethernet frame structure (more)

- **addresses:** 6 byte source, destination MAC addresses
 - if adapter receives frame with matching destination address, or with broadcast address (e.g. ARP packet), it passes data in frame to network layer protocol
 - otherwise, adapter discards frame
- **type:** indicates higher layer protocol
- **CRC:** cyclic redundancy check at receiver
 - error detected: frame is dropped

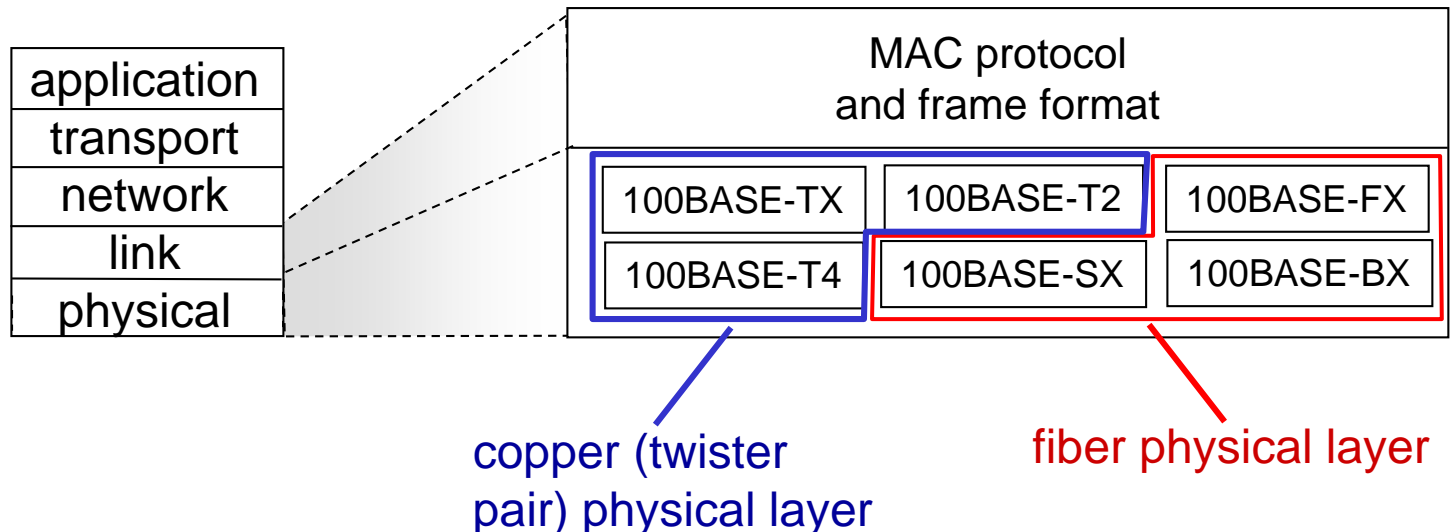


Ethernet: unreliable, connectionless

- **connectionless**: no handshaking between sending and receiving NICs
- **unreliable**: receiving NIC doesn't send acks or nacks to sending NIC
 - data in dropped frames recovered only if initial sender uses higher layer rdt (e.g., TCP), otherwise dropped data lost
- Ethernet's MAC protocol: **CSMA/CD**

802.3 Ethernet standards: link & physical layers

- *many* different Ethernet standards
 - common MAC protocol and frame format
 - different speeds: 2 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, 40 Gbps
 - different physical layer media: fiber, cable



Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

Multiple access links, protocols

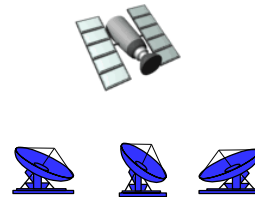
- *broadcast (shared wire or medium)*
 - old-fashioned Ethernet
 - 802.11 wireless LAN



shared wire (e.g.,
cabled Ethernet)



shared RF
(e.g., 802.11 WiFi)



shared RF
(satellite)



humans at a
cocktail party
(shared air, acoustical)

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 protocol

- distributed algorithm that determines how nodes share channel, i.e., determine when node can transmit

An ideal multiple access protocol

given: broadcast channel of rate R bps

Ideal protocol:

1. when one node wants to transmit, it can send at rate R .
2. when M nodes want to transmit, each can send at average rate R/M
3. fully decentralized:
 - no special node to coordinate transmissions
 - no synchronization of clocks, slots
4. simple

MAC protocols

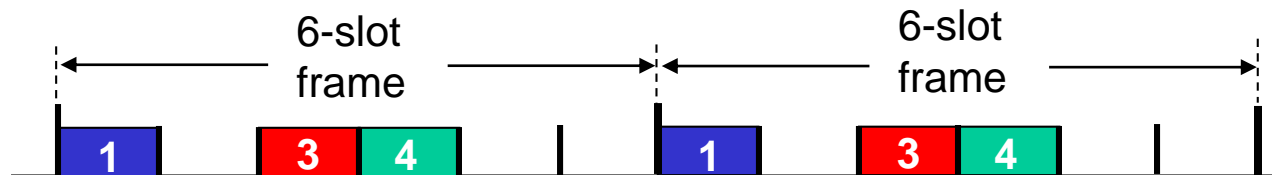
Three broad classes:

- *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”*
 - nodes take turns, but nodes with more to send can take longer turns

Channel partitioning MAC protocols: TDMA

TDMA: time division multiple access

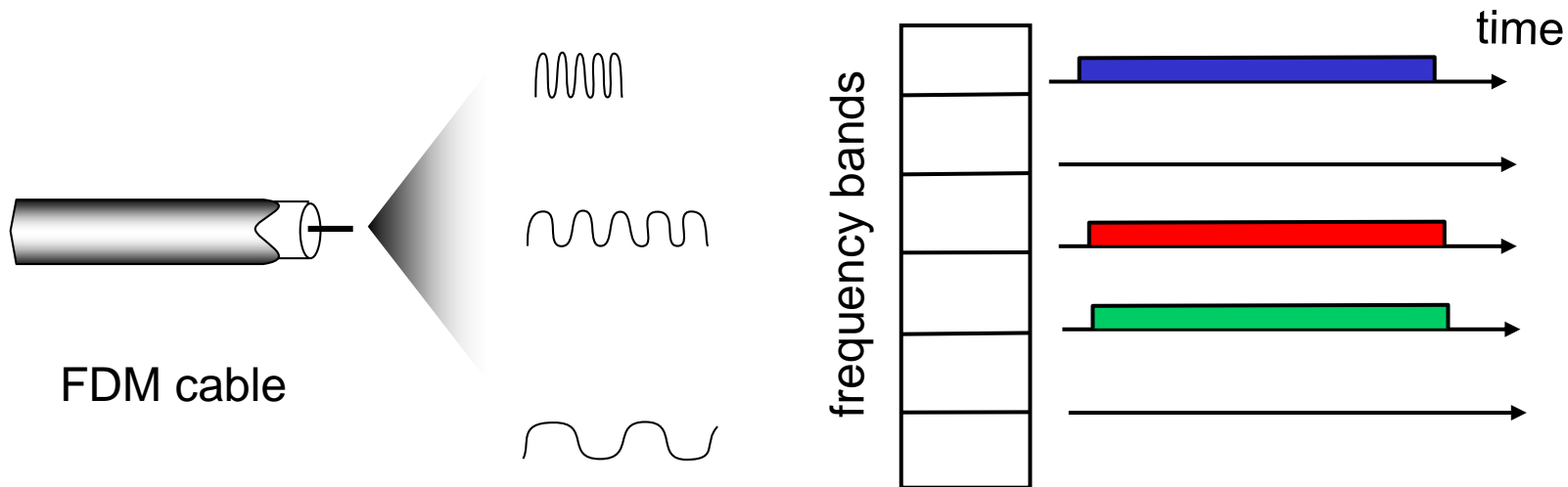
- access to channel in "rounds"
- each station gets fixed length slot (length = packet transmission time) in each round
- unused slots go idle
- example: 6-station LAN, 1,3,4 have packets to send, slots 2,5,6 idle



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 packet to send, 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)
- examples of random access MAC protocols:
 - CSMA, CSMA/CD, CSMA/CA

CSMA (carrier sense multiple access)

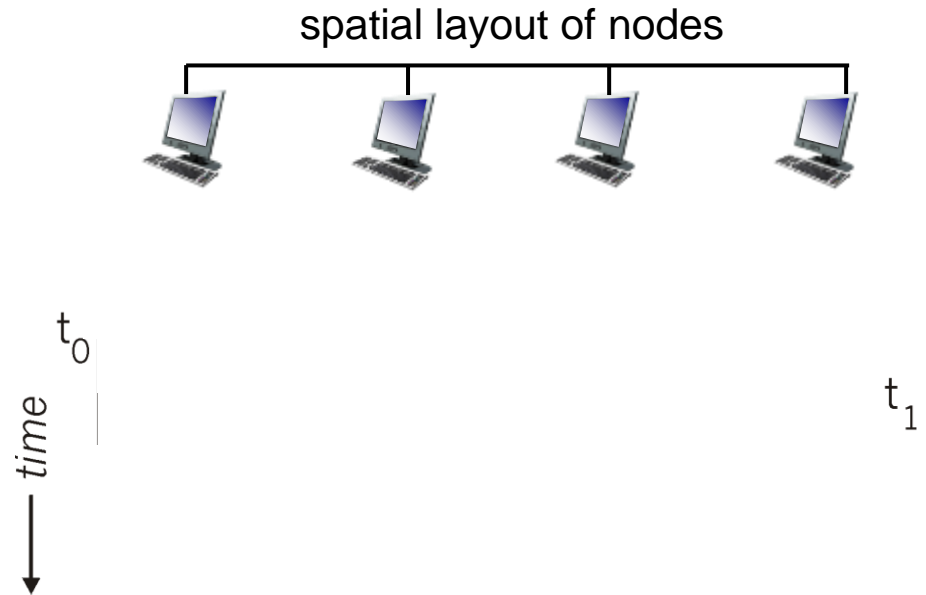
CSMA: listen before transmit:

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 &
propagation delay
play role in in
determining collision
probability

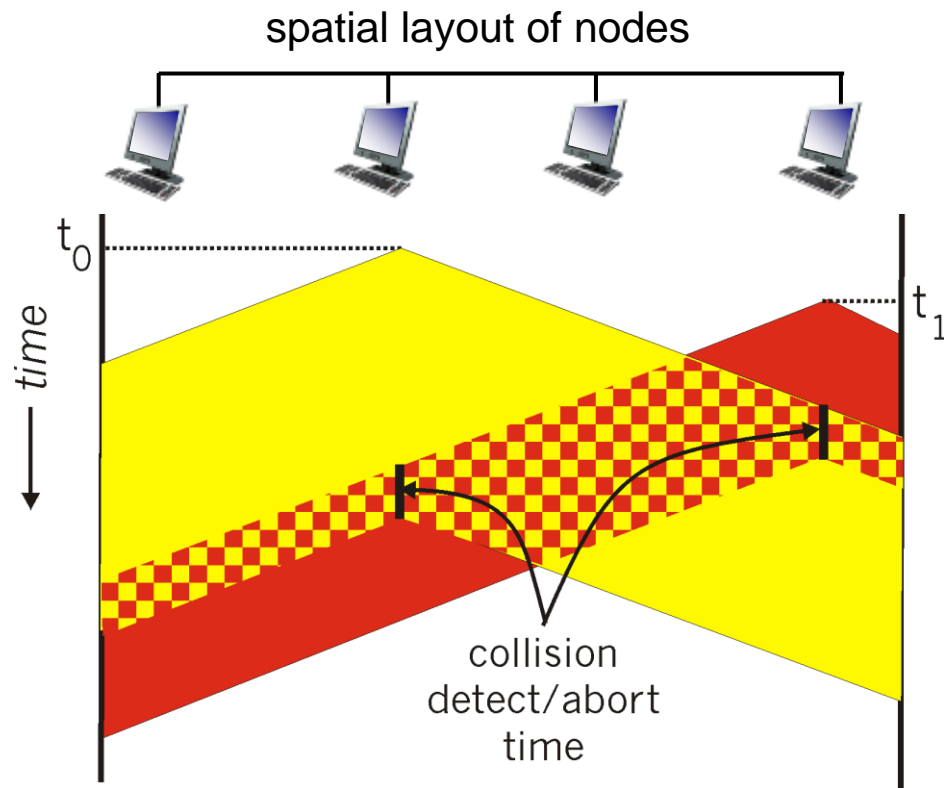


CSMA/CD (collision detection)

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)



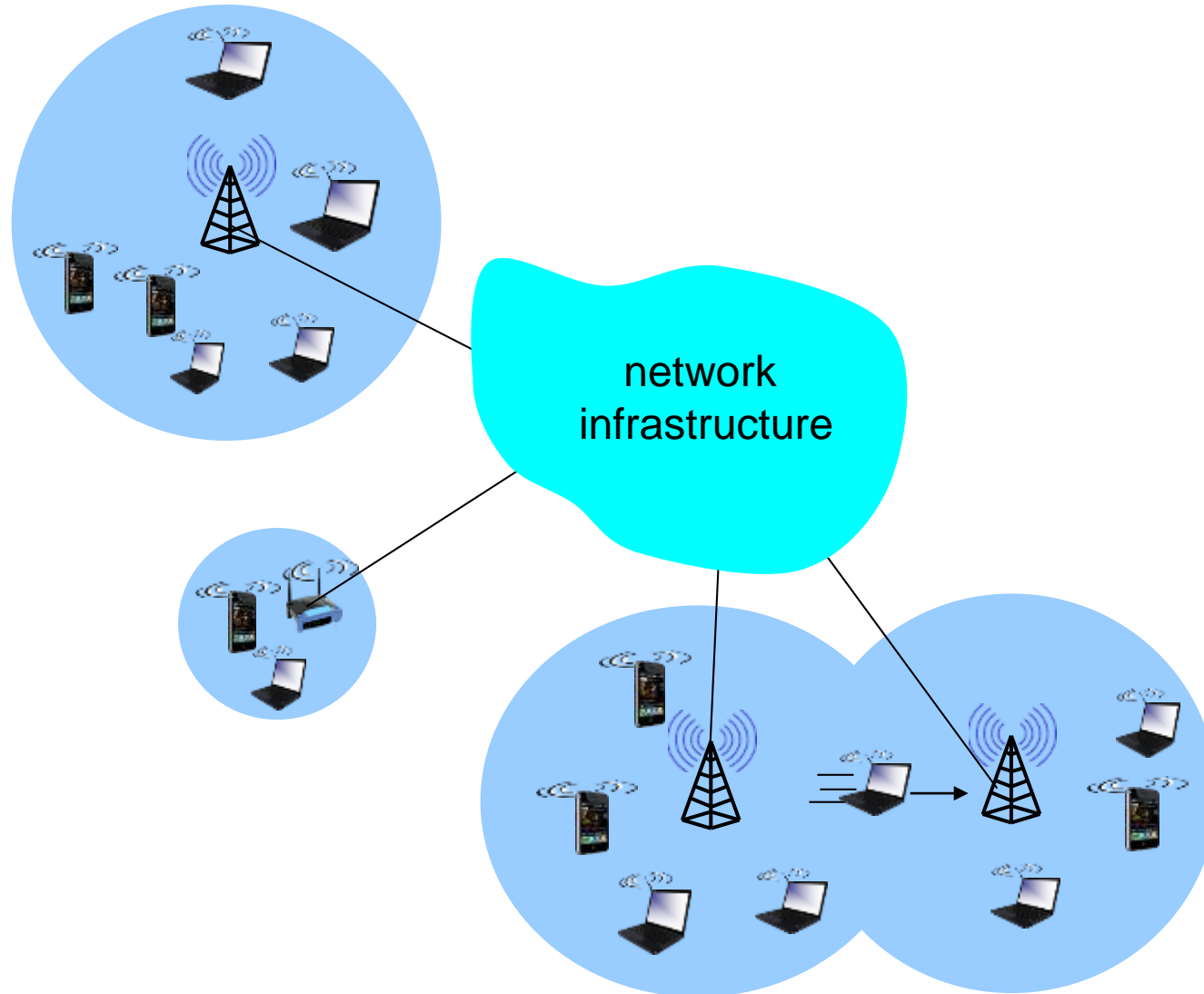
Ethernet CSMA/CD algorithm

1. NIC receives datagram from network layer, creates frame
2. If NIC senses channel idle, starts frame transmission. If NIC senses channel busy, waits until channel idle, then transmits.
3. If NIC transmits entire frame without detecting another transmission, NIC is done with frame !
4. If NIC detects another transmission while transmitting, aborts and sends jam signal
5. After aborting, NIC enters *binary (exponential) backoff*:
 - after m th collision, NIC chooses K at random from $\{0, 1, 2, \dots, 2^m - 1\}$. NIC waits $K \cdot 512$ bit times, returns to Step 2
 - longer backoff interval with more collisions

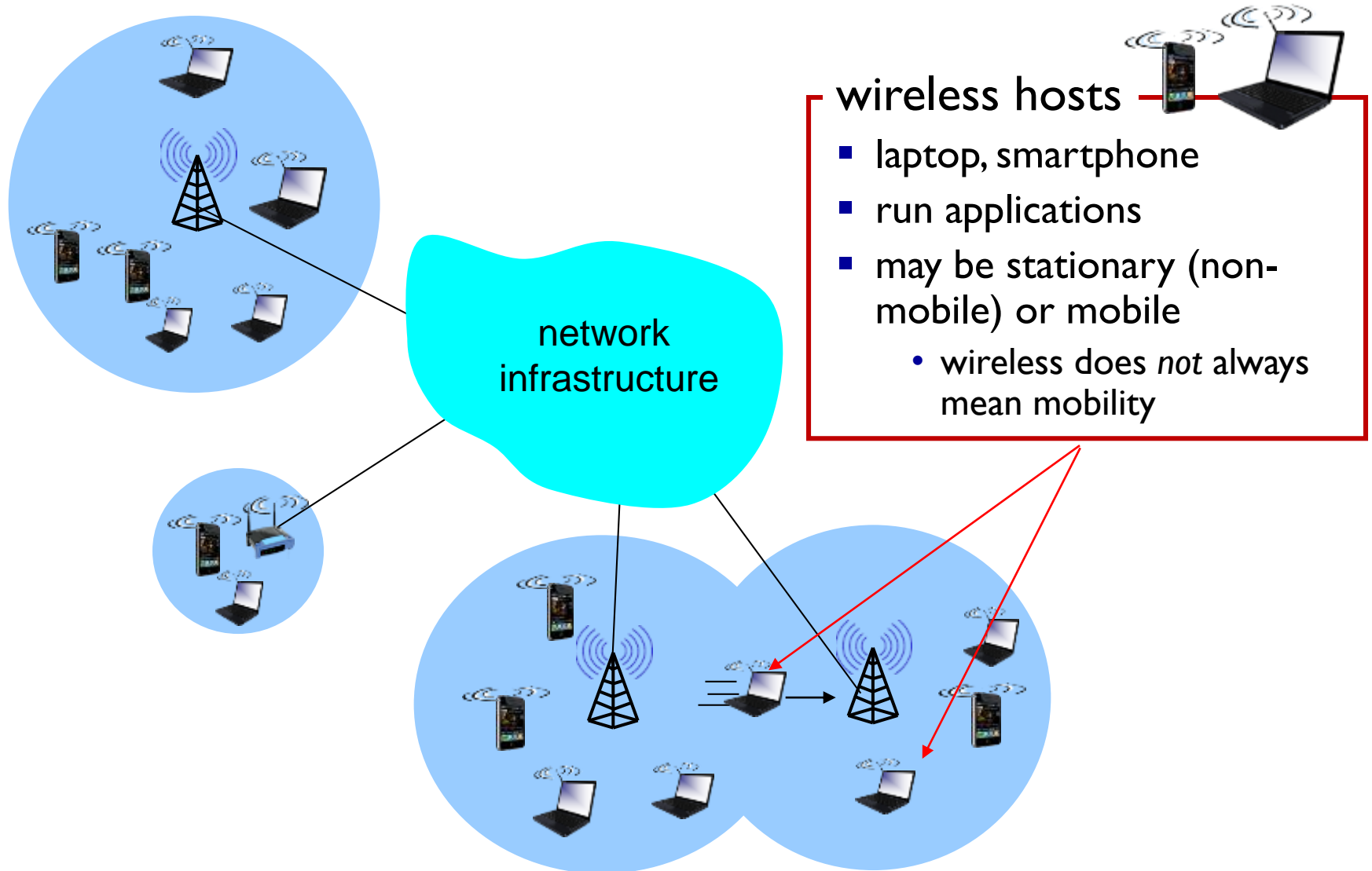
Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

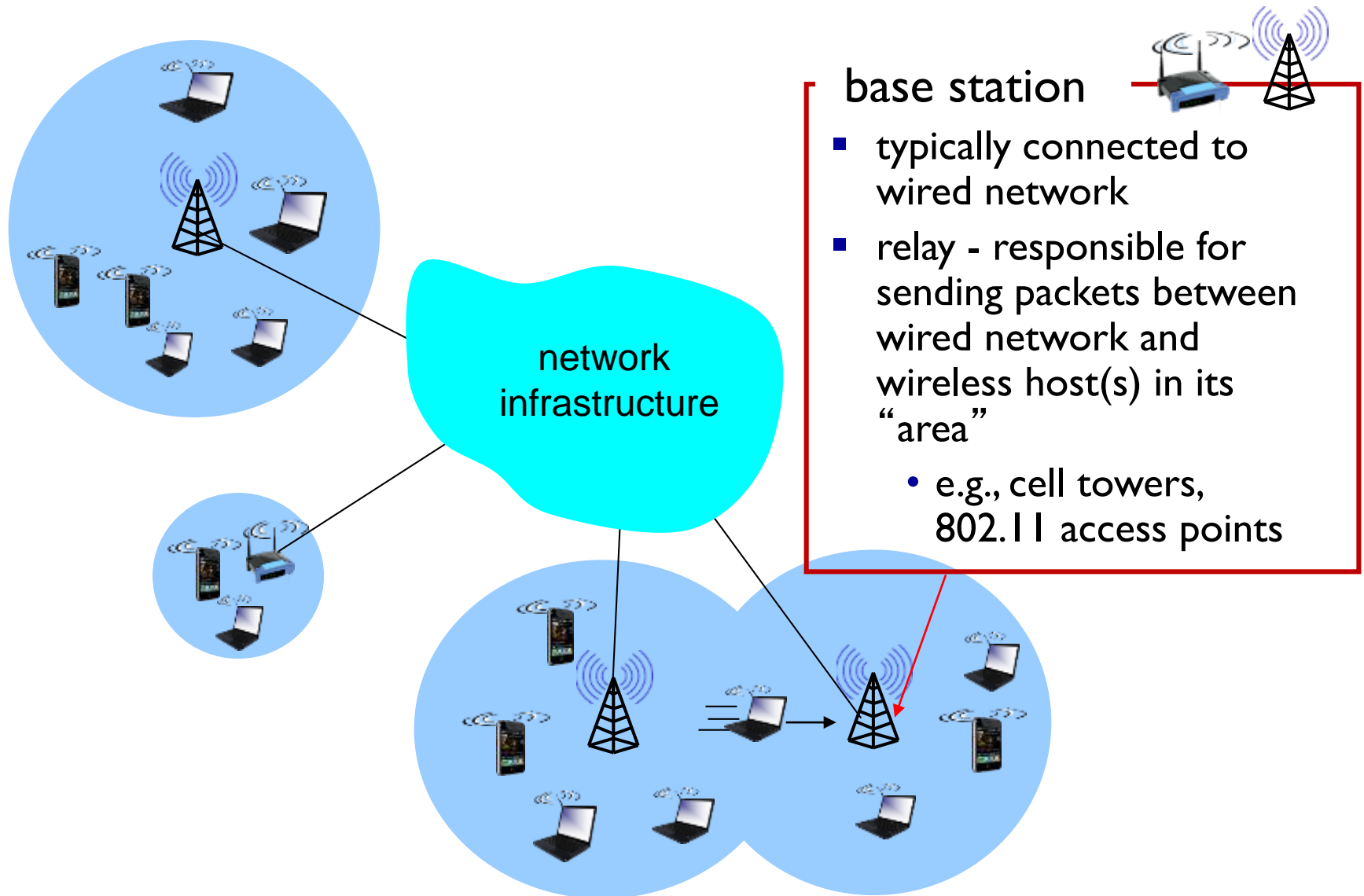
Elements of a wireless network



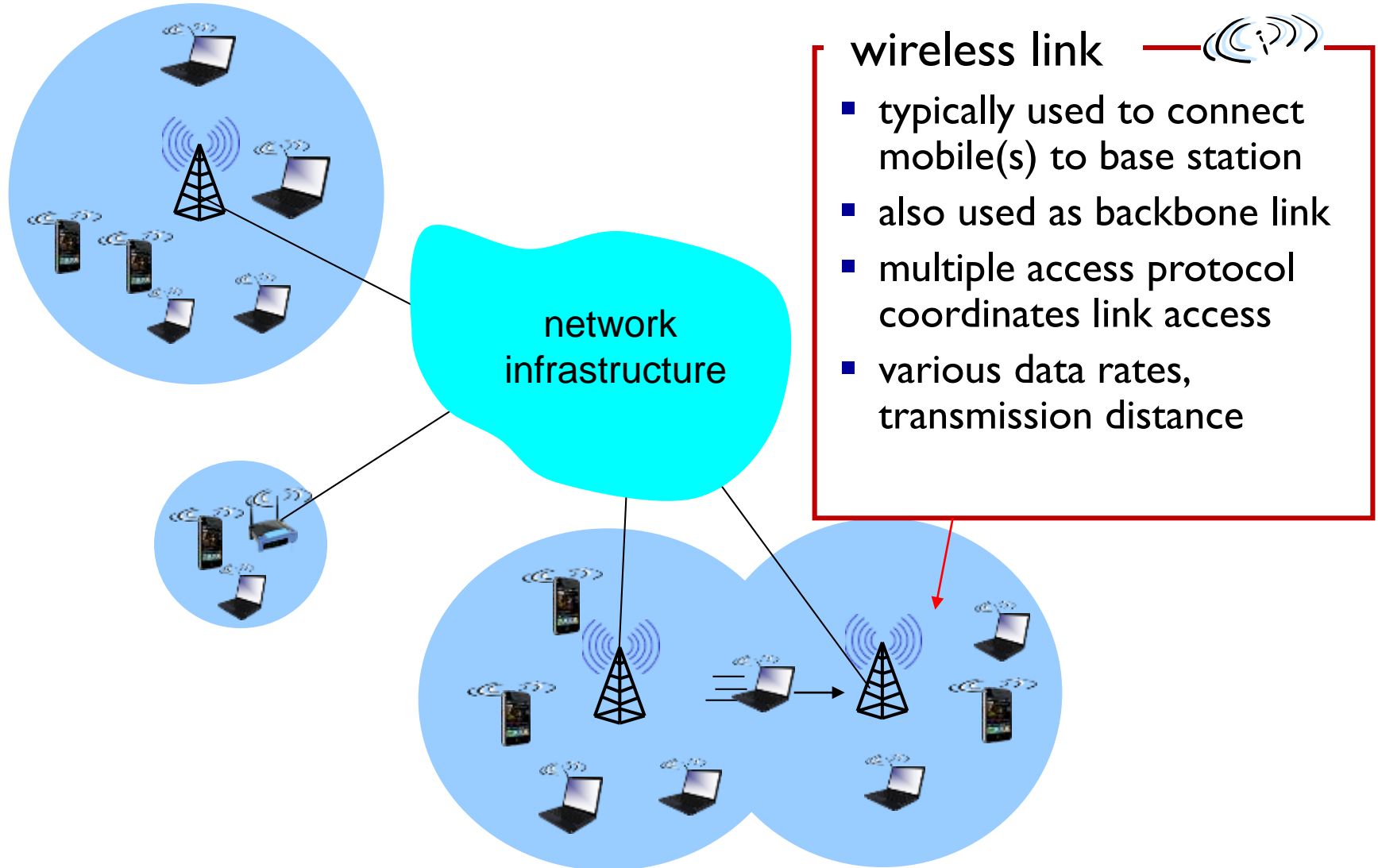
Elements of a wireless network



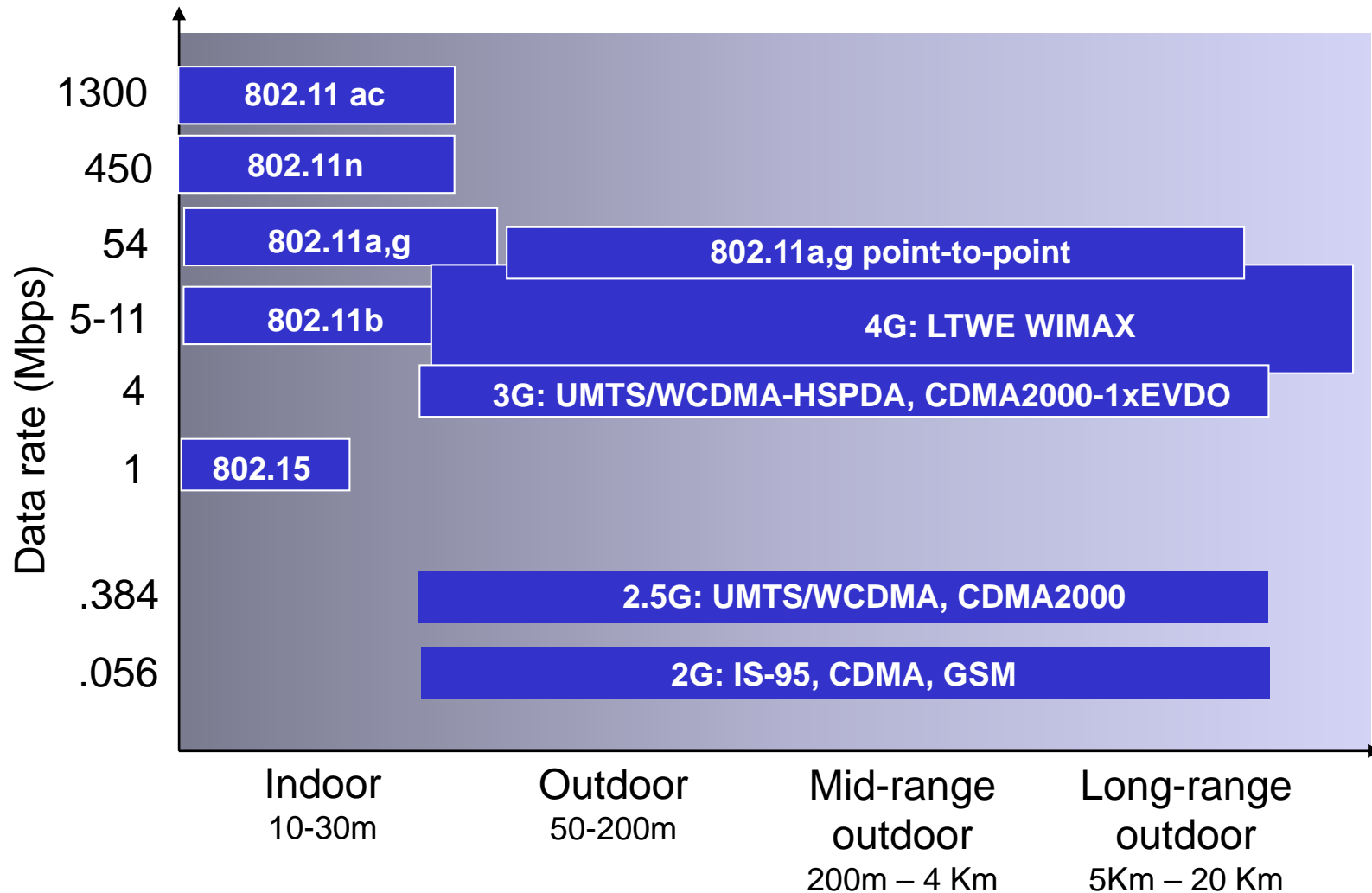
Elements of a wireless network



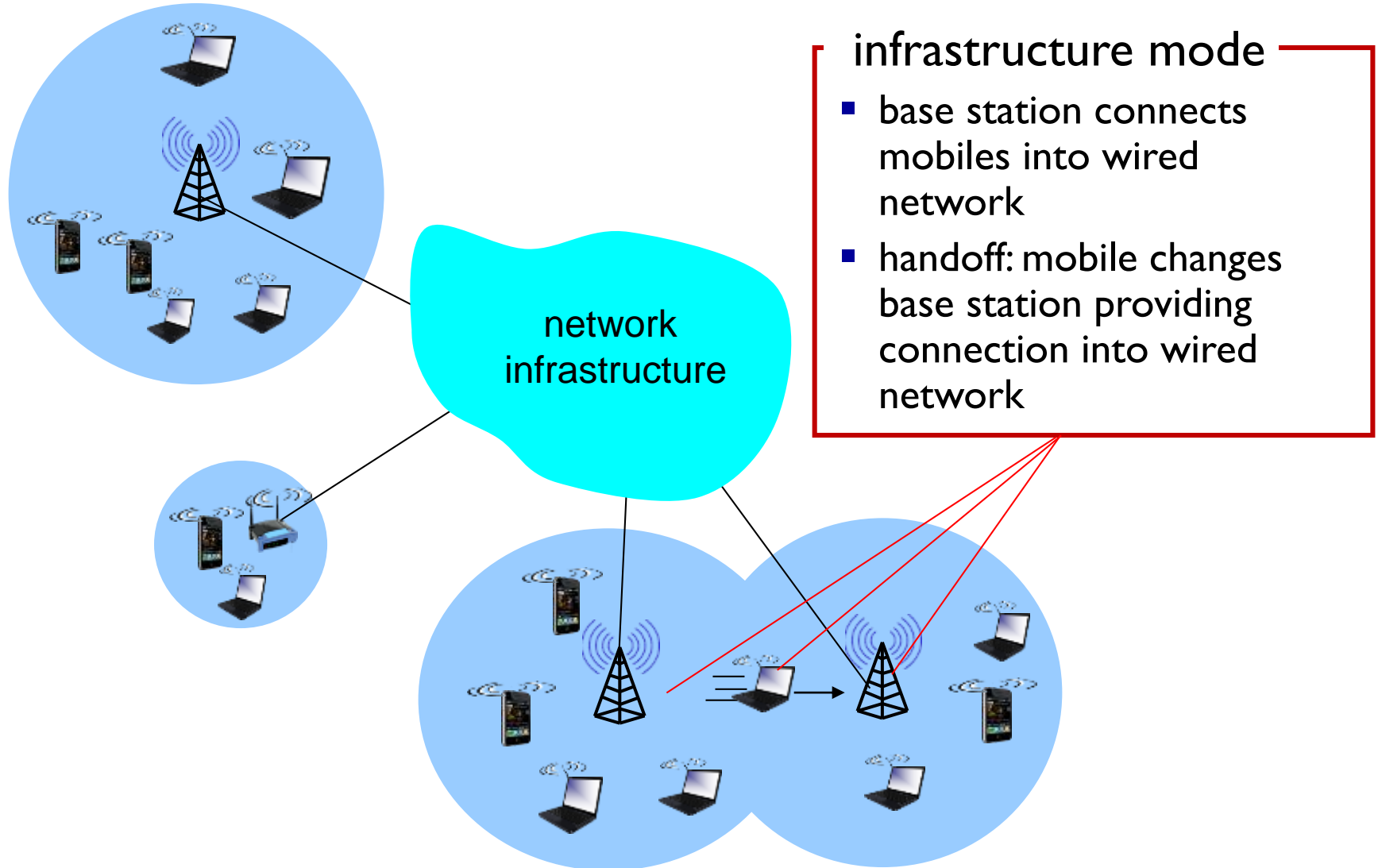
Elements of a wireless network



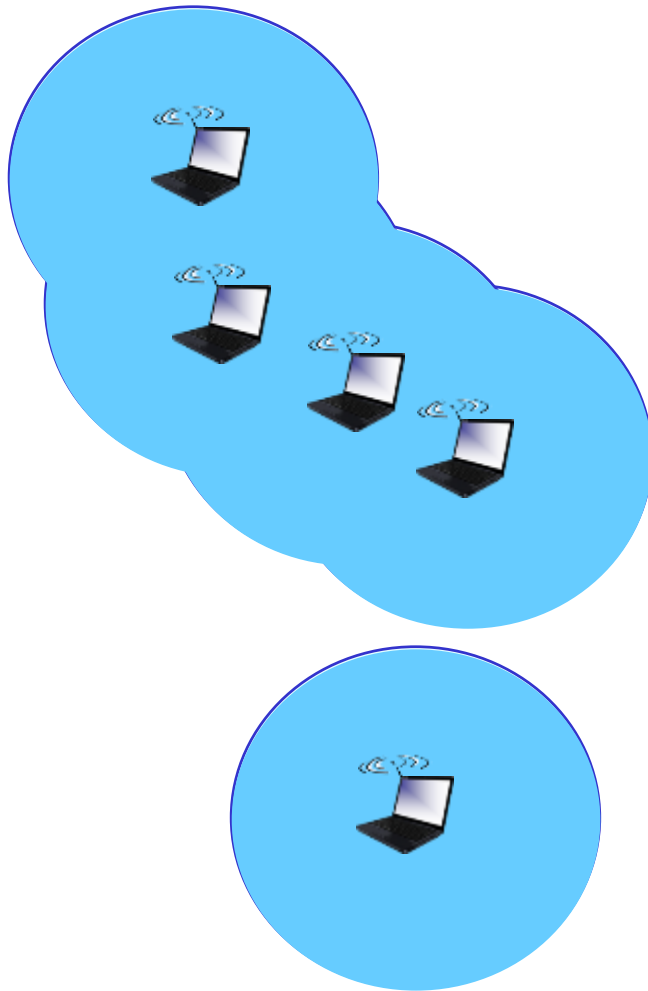
Characteristics of selected wireless links



Elements of a wireless 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

Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

IEEE 802.11 Wireless LAN

802.11b

- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps

802.11a

- 5-6 GHz range
- up to 54 Mbps

802.11g

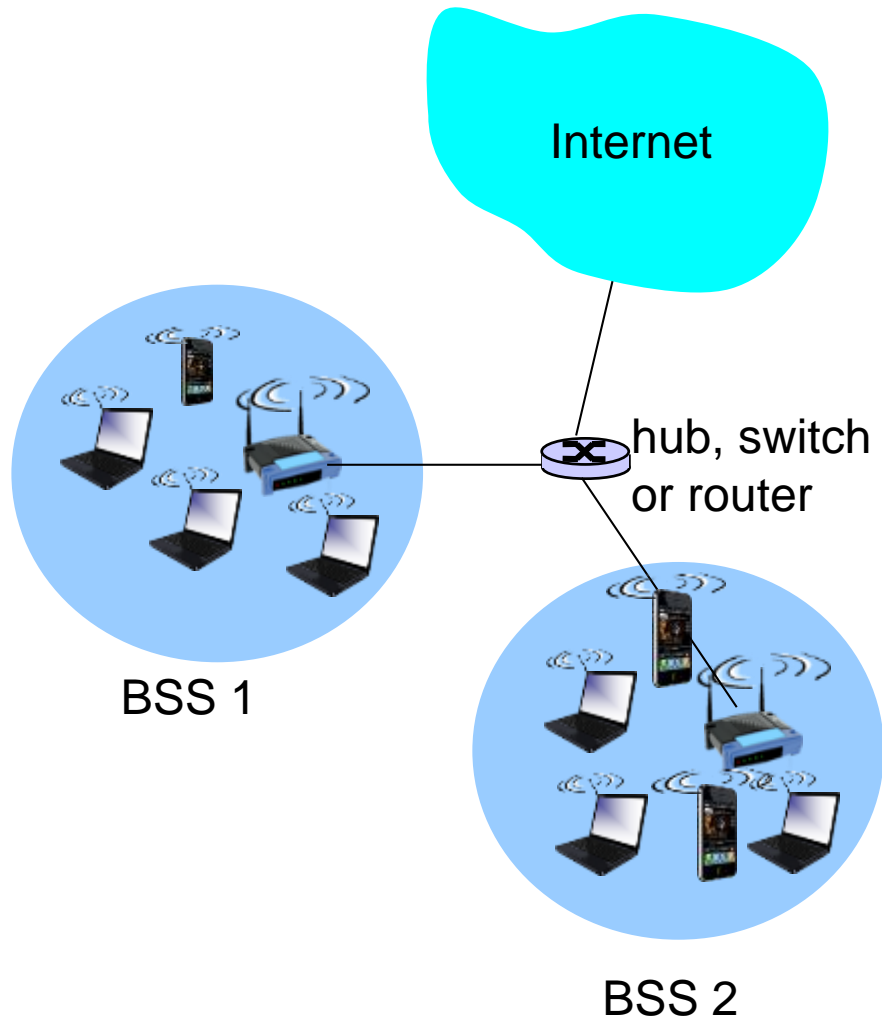
- 2.4-5 GHz range
- up to 54 Mbps

802.11n: multiple antennae

- 2.4-5 GHz range
- up to 200 Mbps

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

802.11 LAN architecture

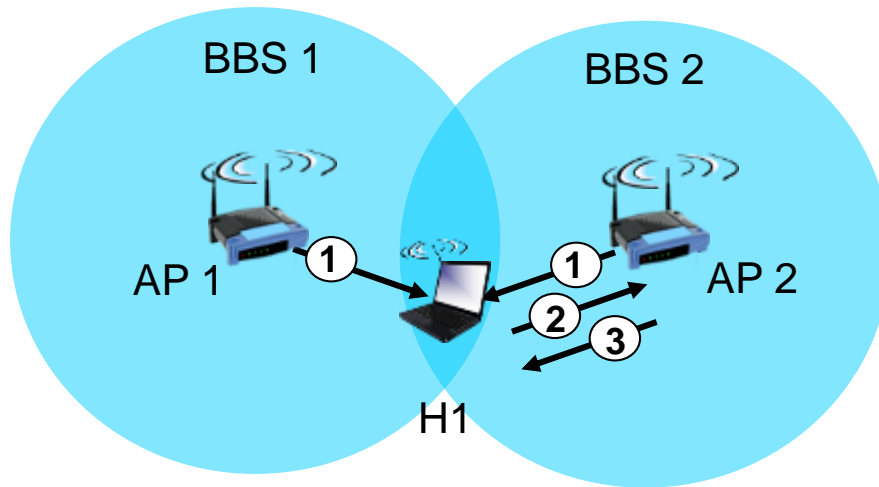


- wireless host communicates with base station
 - **base station = access point (AP)**
- **Basic Service Set (BSS)** (aka “cell”) in infrastructure mode contains:
 - wireless hosts
 - access point (AP): base station
 - ad hoc mode: hosts only

802.11: Channels, association

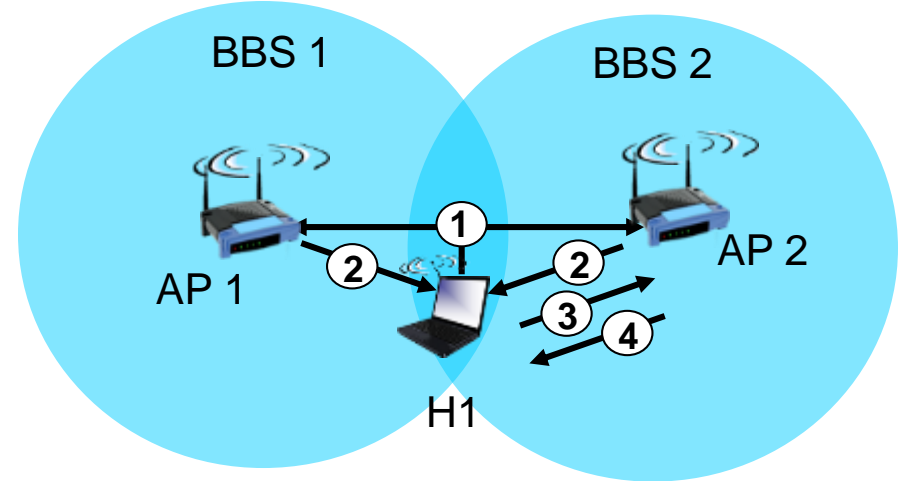
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
 - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
 - selects AP to associate with
 - may perform authentication
 - 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

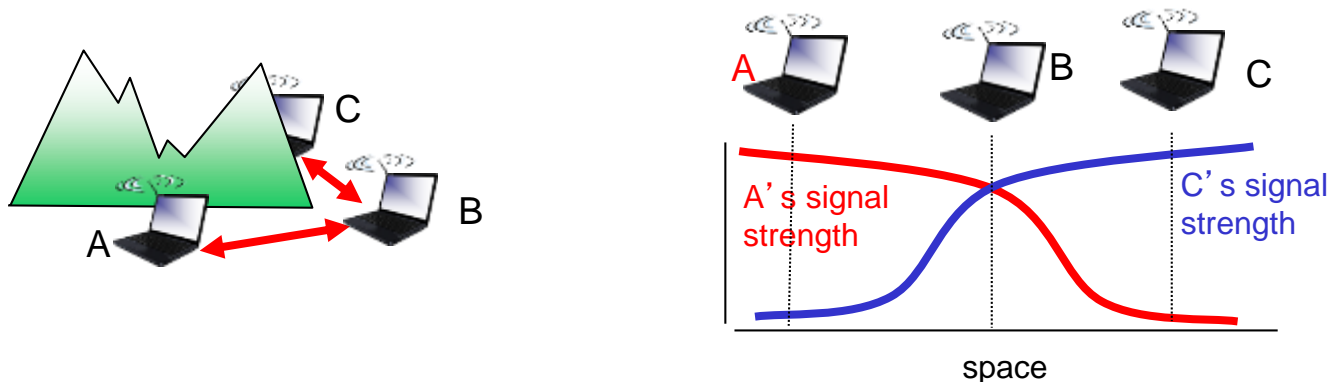


active scanning:

- (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

- avoid collisions: 2⁺ nodes transmitting at same time
- 802.11: Carrier Sense Multiple Access (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)



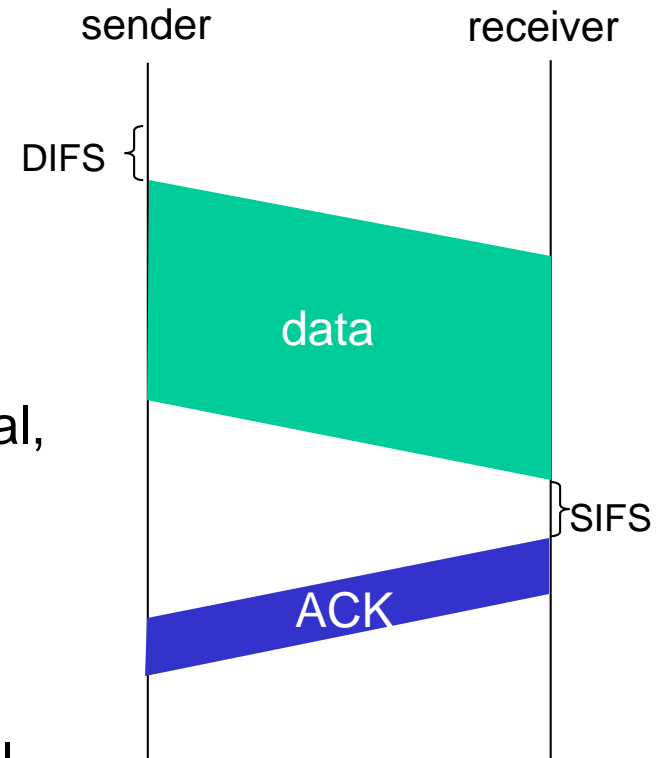
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

- 1 if sense channel idle for Distributed Inter-frame Space (**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 Short Inter-frame Spacing (**SIFS**) (ACK needed due to hidden terminal problem)



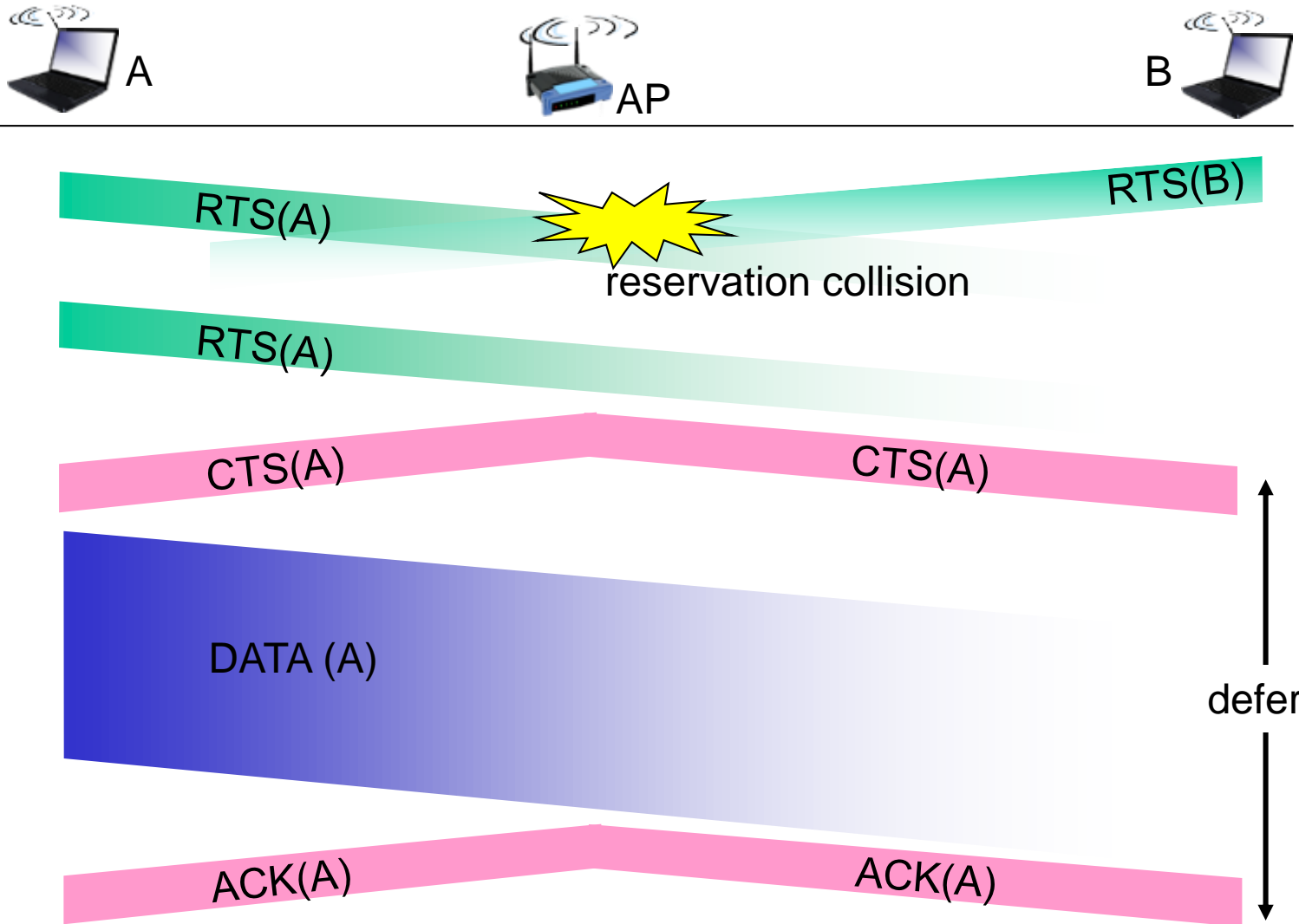
Avoiding collisions (more)

idea: allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

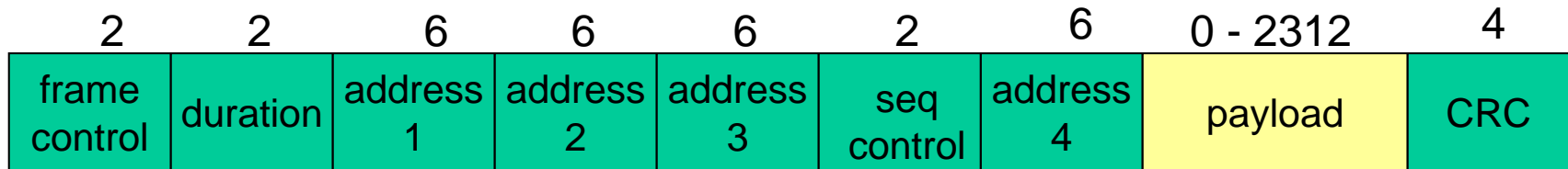
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
 - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
 - sender transmits data frame
 - other stations defer transmissions

*avoid data frame collisions completely
using small reservation packets!*

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



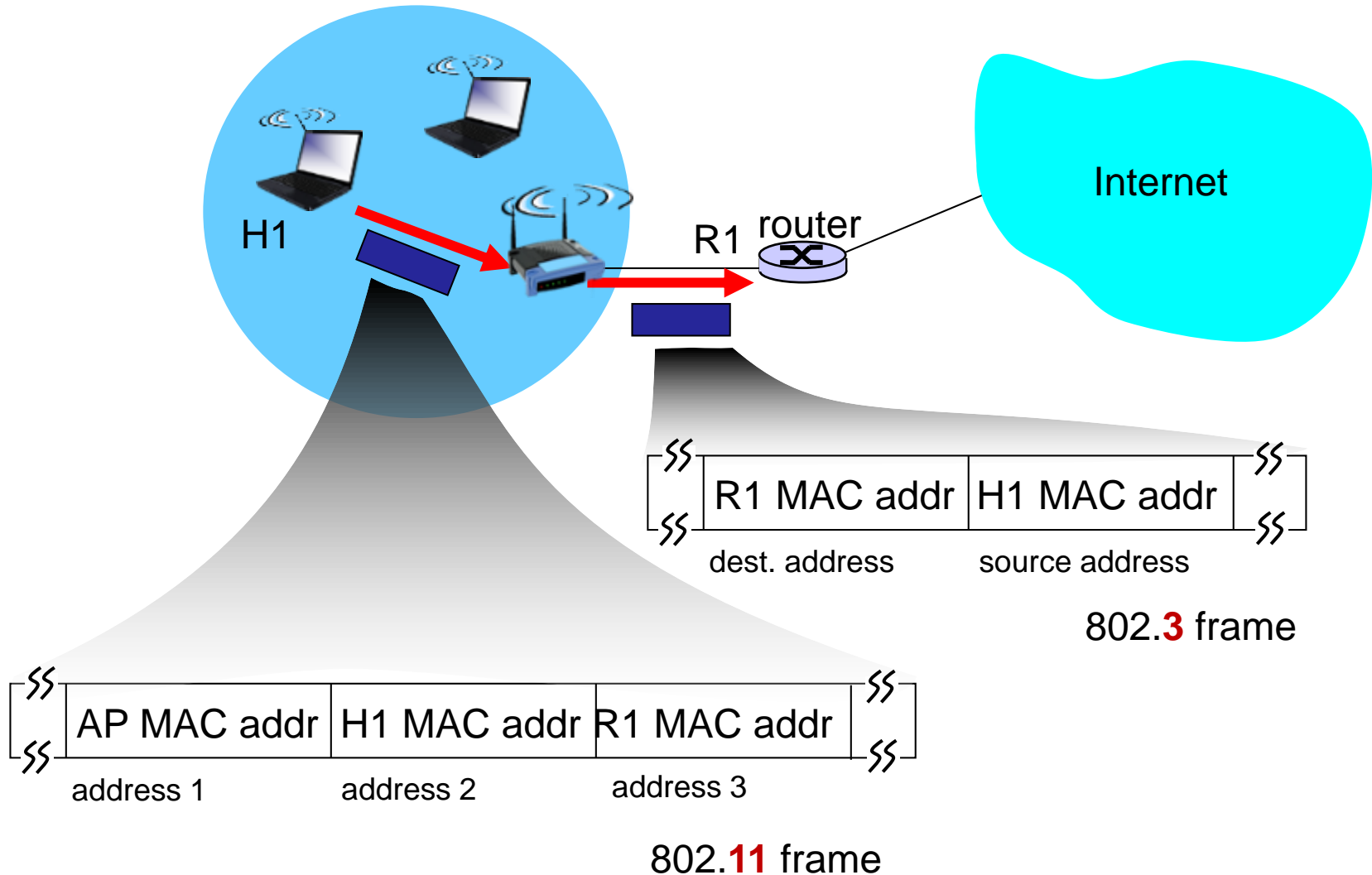
Address 1: MAC address of wireless host or AP to receive this frame

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

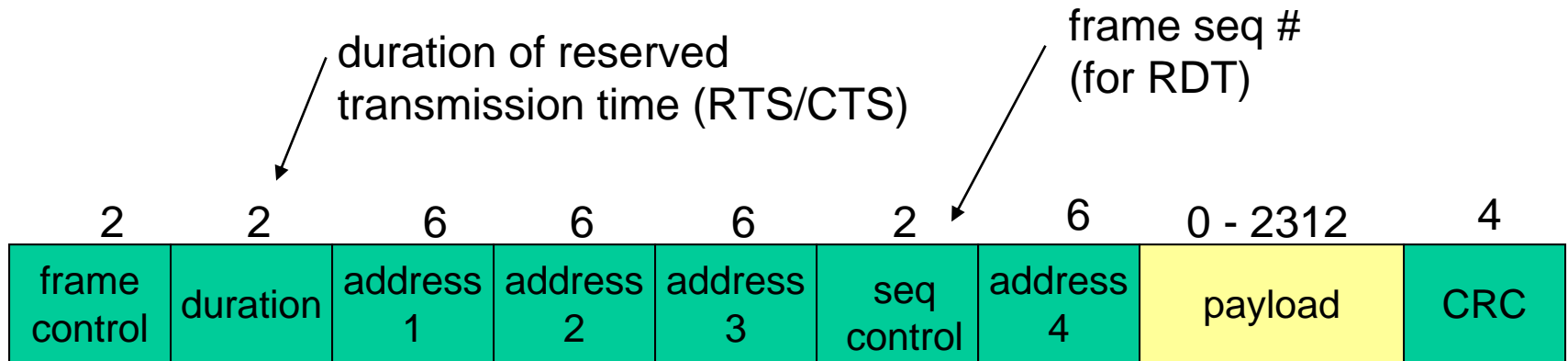
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing

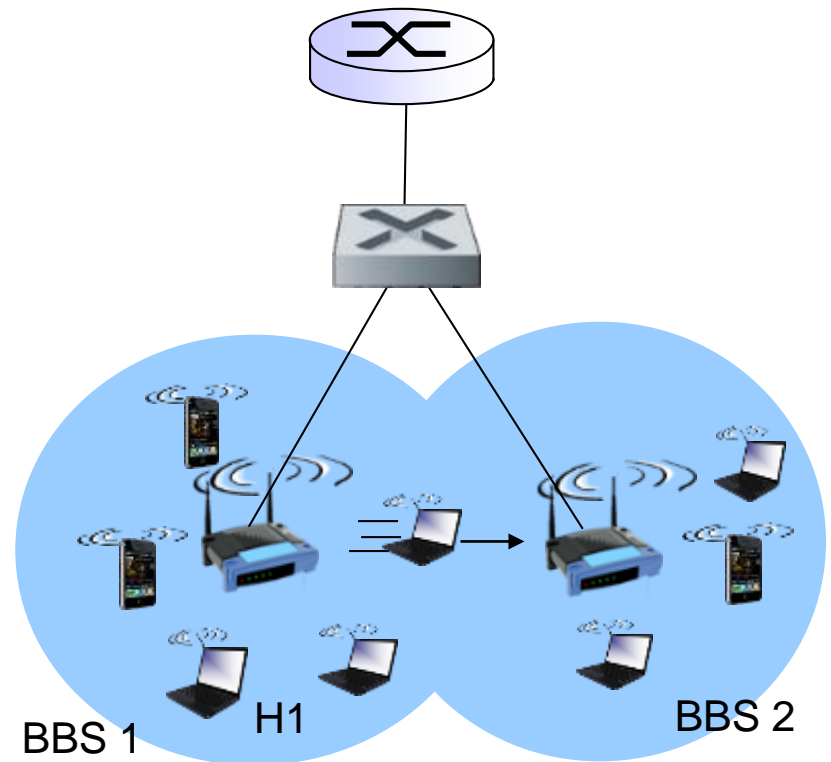


802.11 frame: more



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: switch will see frame from H1 and “remember” which switch port can be used to reach H1

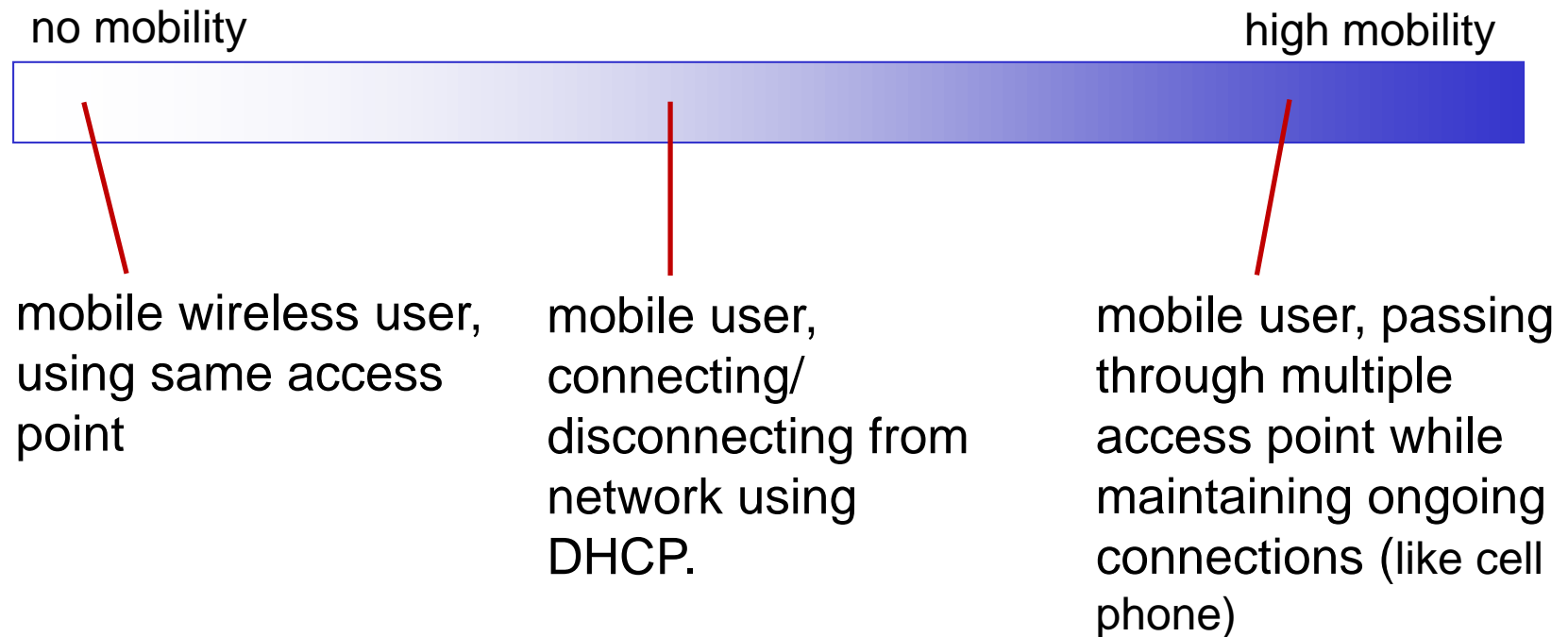


Topics

- Link Layer
 - Medium Access Control (MAC) Addresses
 - Address Resolution Protocol (ARP)
- Wired Networks
 - Ethernet
 - Multiple Access Protocols
- Wireless Networks
 - Elements of Wireless Networks
 - IEEE 802.11 Wireless LANs
 - Mobile IP

What is mobility?

- spectrum of mobility, from the *network* perspective:

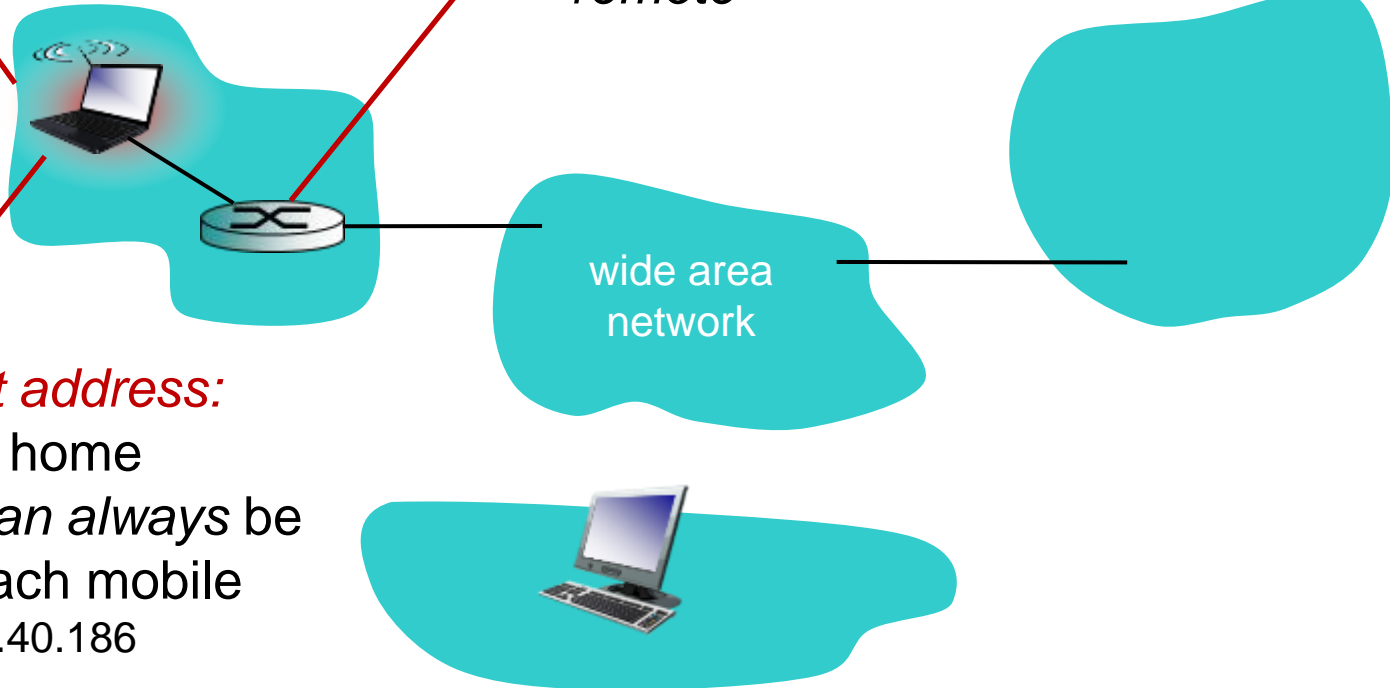


Mobility: vocabulary

home network: permanent
“home” of mobile
(e.g., 128.119.40/24)

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

permanent address:
address in home
network, *can always* be
used to reach mobile
e.g., 128.119.40.186



Mobility: more vocabulary

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

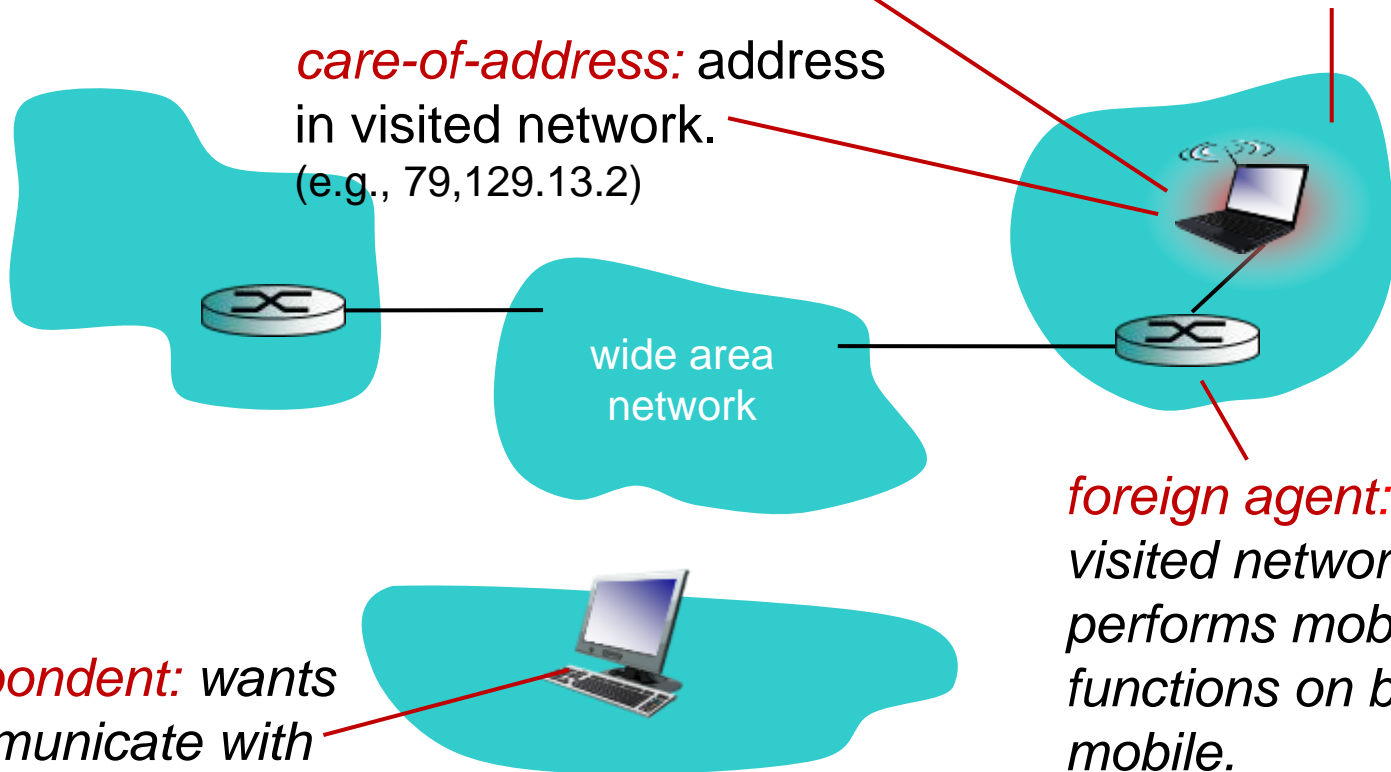
visited network: network in which mobile currently resides (e.g., 79.129.13/24)

care-of-address: address in visited network. (e.g., 79.129.13.2)

wide area network

foreign agent: entity in visited network that performs mobility functions on behalf of mobile.

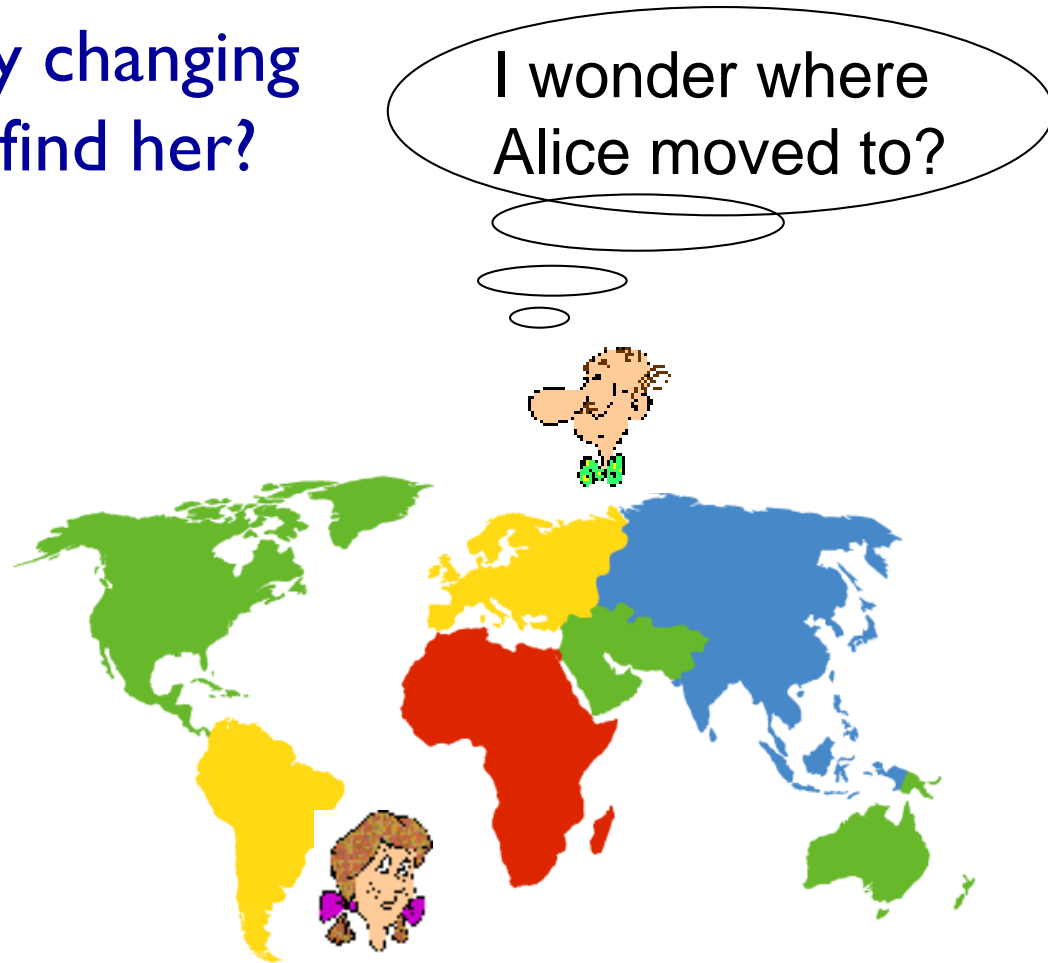
correspondent: wants to communicate with mobile



How do *you* contact a mobile friend:

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

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



Mobility: approaches

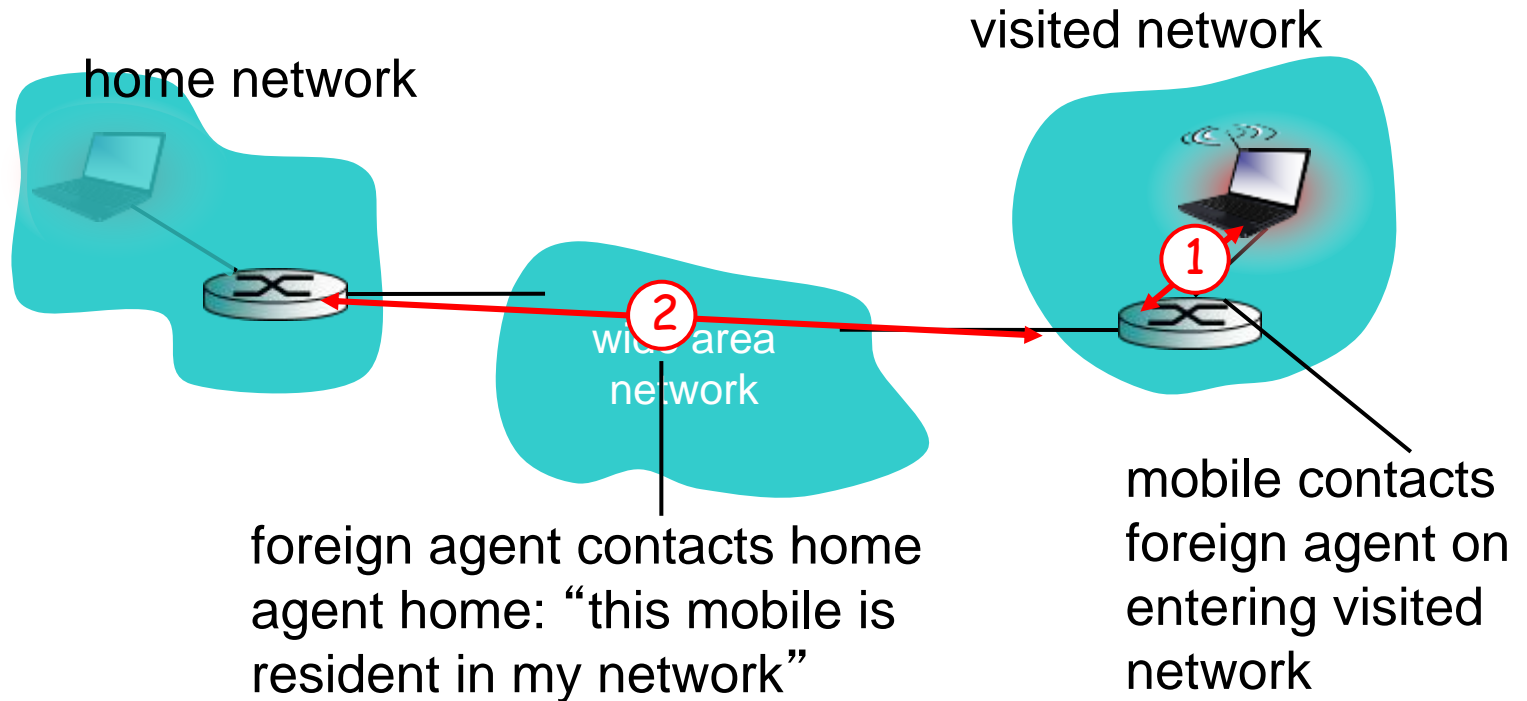
- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-residence via usual routing table exchange.
 - routing tables indicate where each mobile located
 - no changes to end-systems
- *let end-systems handle it:*
 - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
 - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Mobility: approaches

- *let routing handle it:* routers advertise permanent address of mobile, home residence via usual routing table exchange
 - routing table exchange where each mobile located
 - no changes to systems
- *let end-systems handle it:*
 - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
 - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

not
scalable
to millions of
mobiles

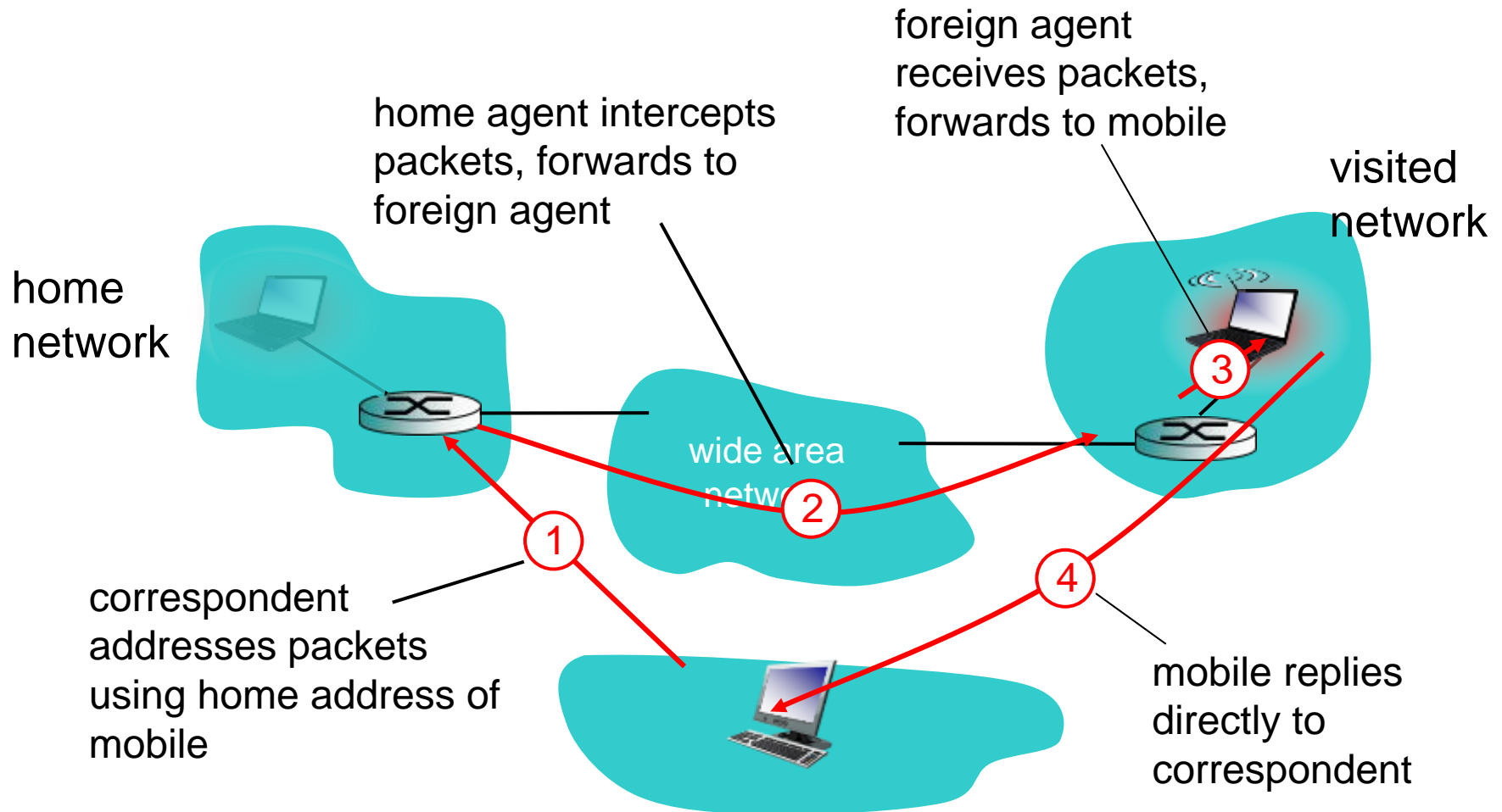
Mobility: registration



end result:

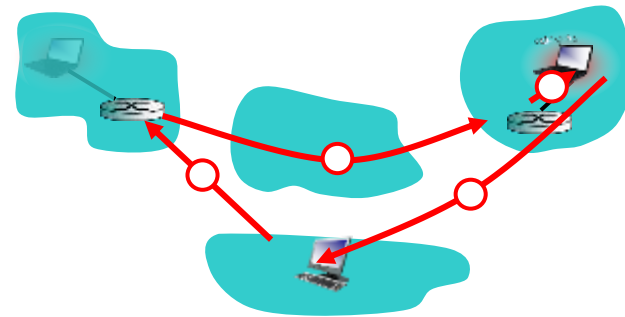
- foreign agent knows about mobile
- home agent knows location of mobile

Mobility via indirect routing



Indirect Routing: comments

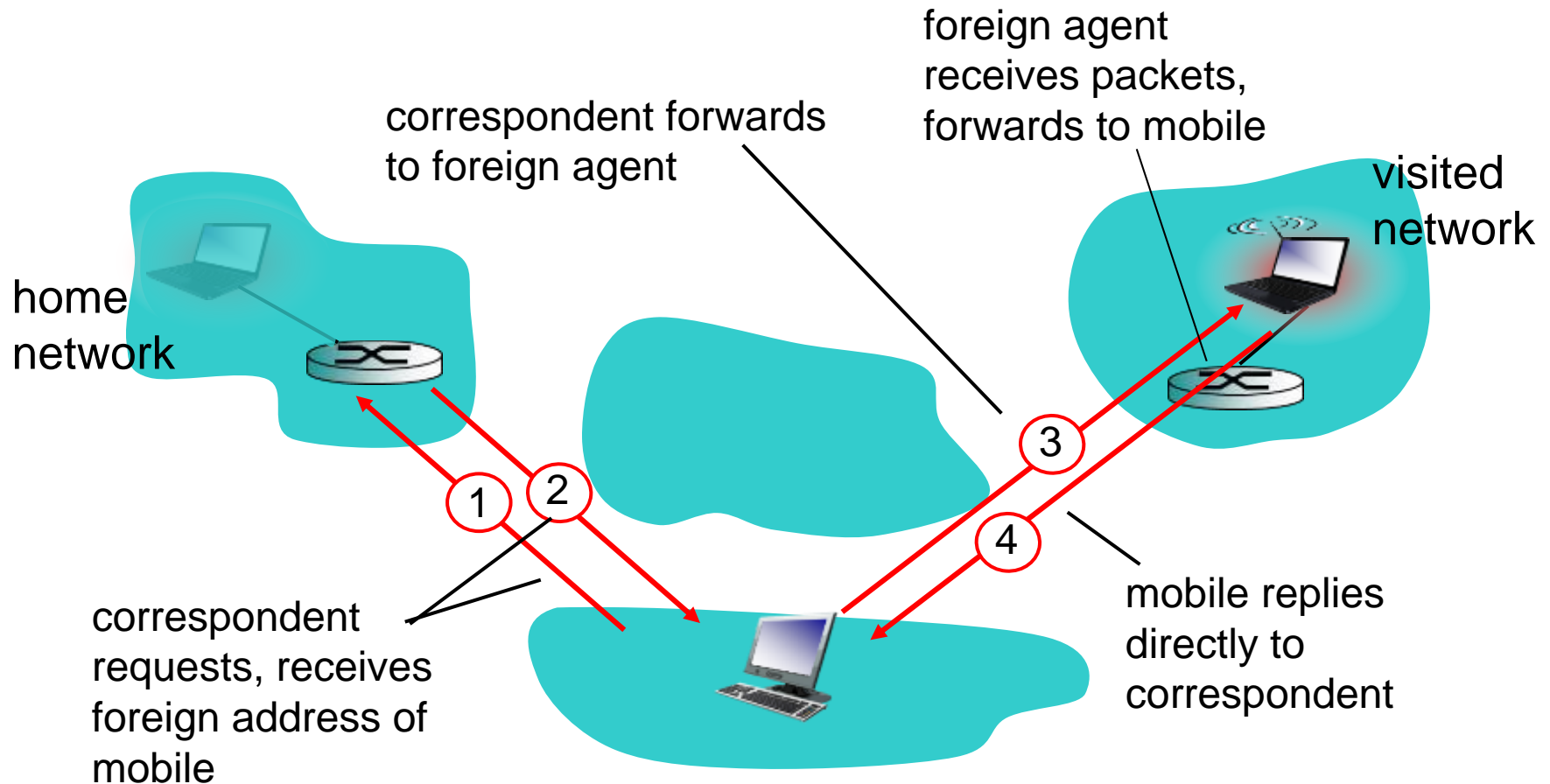
- mobile uses two addresses:
 - **permanent address**: used by correspondent (hence mobile location is *transparent* to correspondent)
 - **care-of-address**: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- **triangle routing**: correspondent-home-network-mobile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



Indirect routing: moving between networks

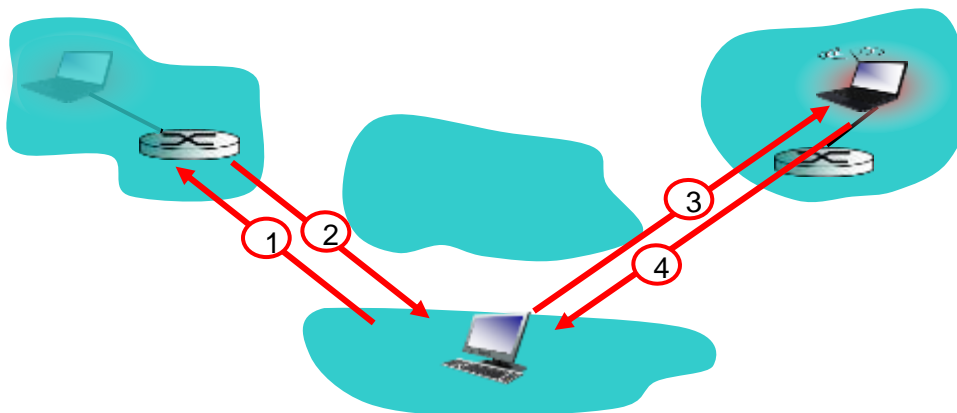
- suppose mobile user moves to another network
 - registers with new foreign agent
 - new foreign agent registers with home agent
 - home agent update care-of-address for mobile
 - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: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

Mobility via direct routing



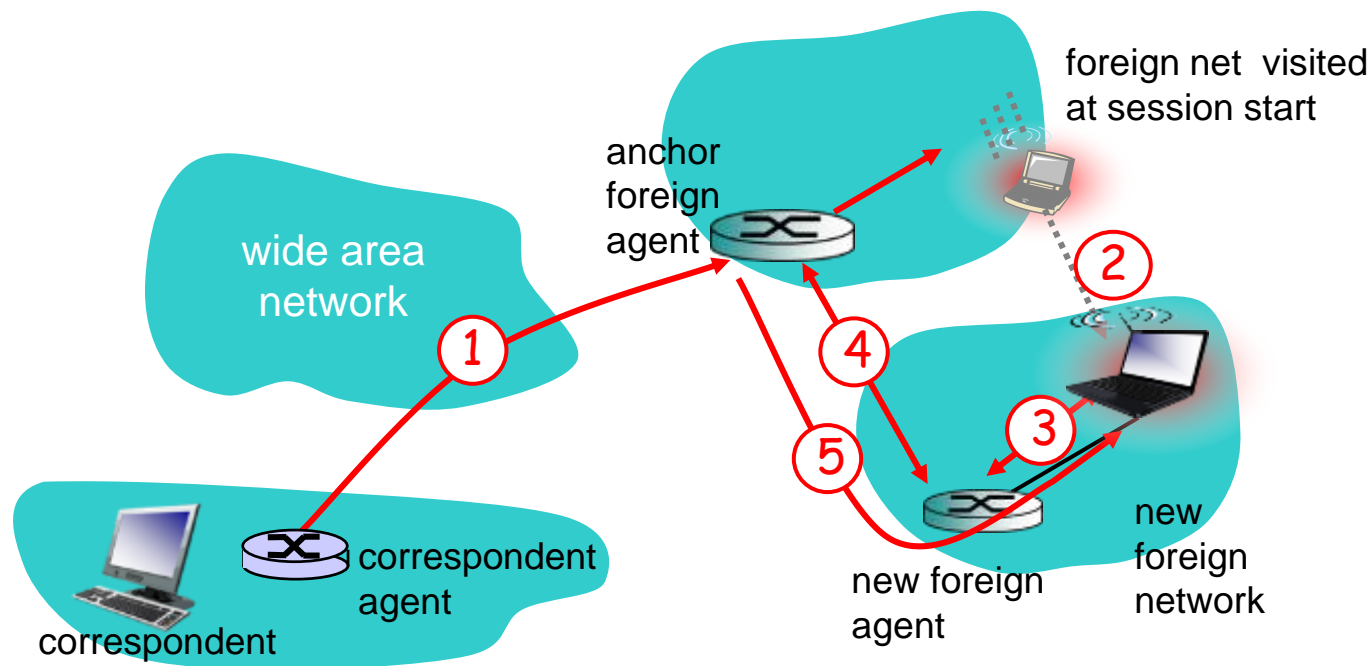
Mobility via direct routing: comments

- overcome triangle routing problem
- *non-transparent to correspondent*: correspondent must get care-of-address from home agent
 - what if mobile changes visited network?



Accommodating mobility with direct routing

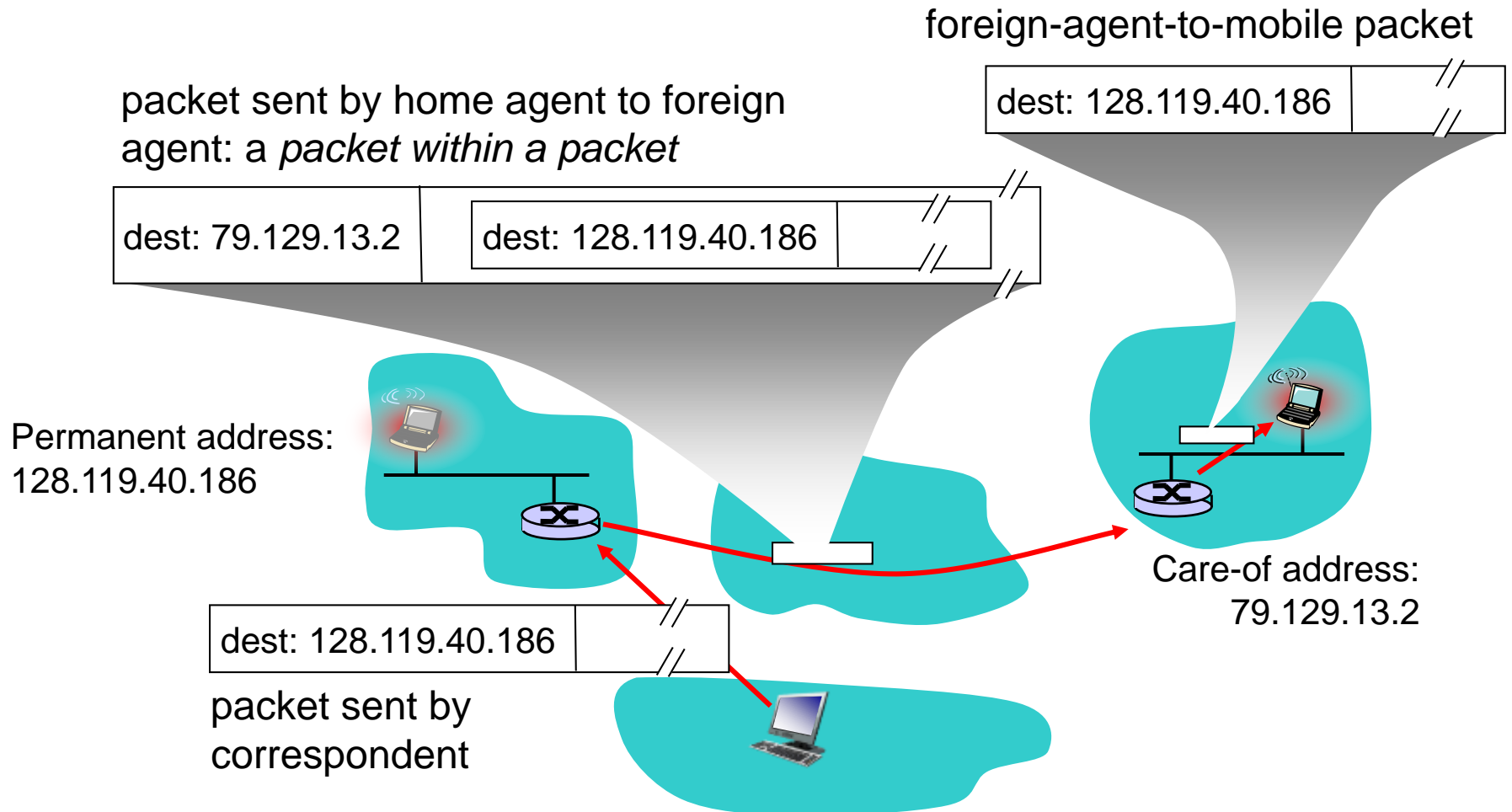
- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



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)
- three components to standard:
 - indirect routing of datagrams
 - agent discovery
 - registration with home agent

Mobile IP: indirect routing



Mobile IP: registration example

