

# Wireless networking

- Very popular!
  - more wireless (cell) phone users than wired phone users
  - almost all incoming Dartmouth students have wireless laptops
- Untethered (wireless) Internet access very appealing
  - hence popularity of wireless LANs in the home
- Two primary challenges
  - communicating over a wireless link
  - *mobility*: handling mobile users who change their point of attachment to the network
- We'll concentrate on 802.11 WLANs
  - as used at many campuses and homes

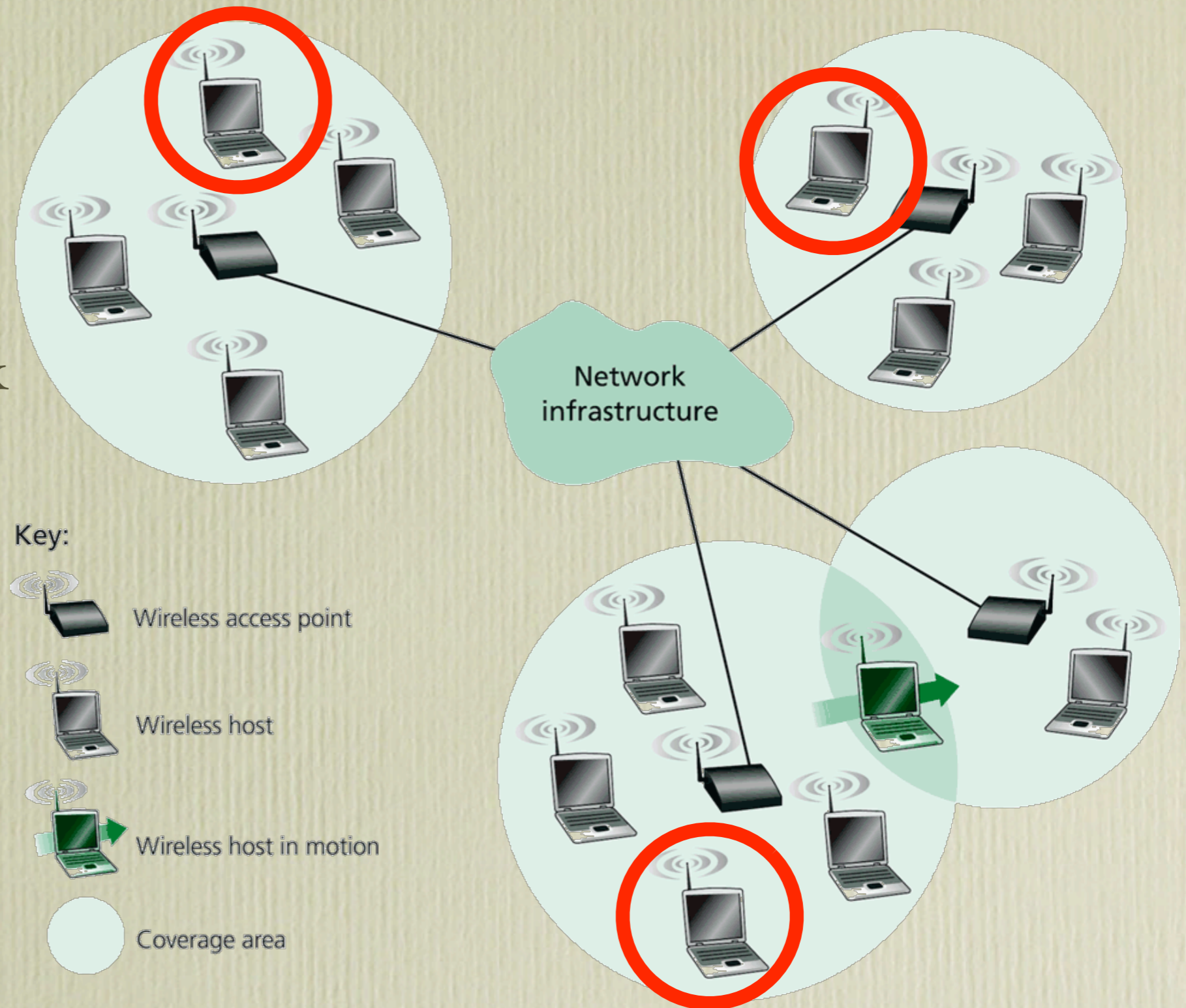
# Radio

“You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat.”

Albert Einstein

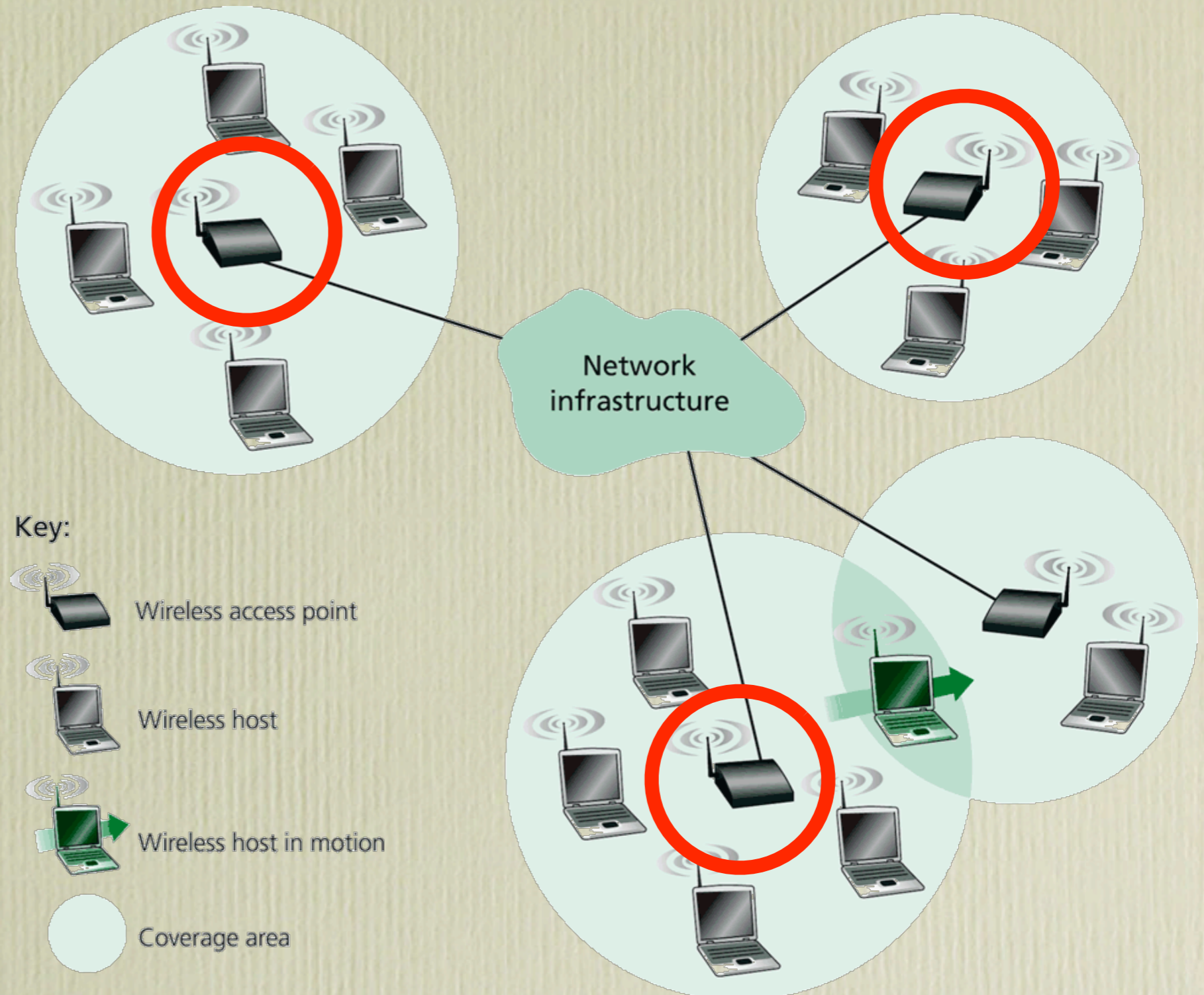
# Elements of a wireless network

- hosts (mobile stations) can be laptops, PDAs, phones, Vocera badges
- hosts run network applications
- hosts may be mobile or non-mobile
  - wireless != mobility
  - e.g., desktops with wireless NICs



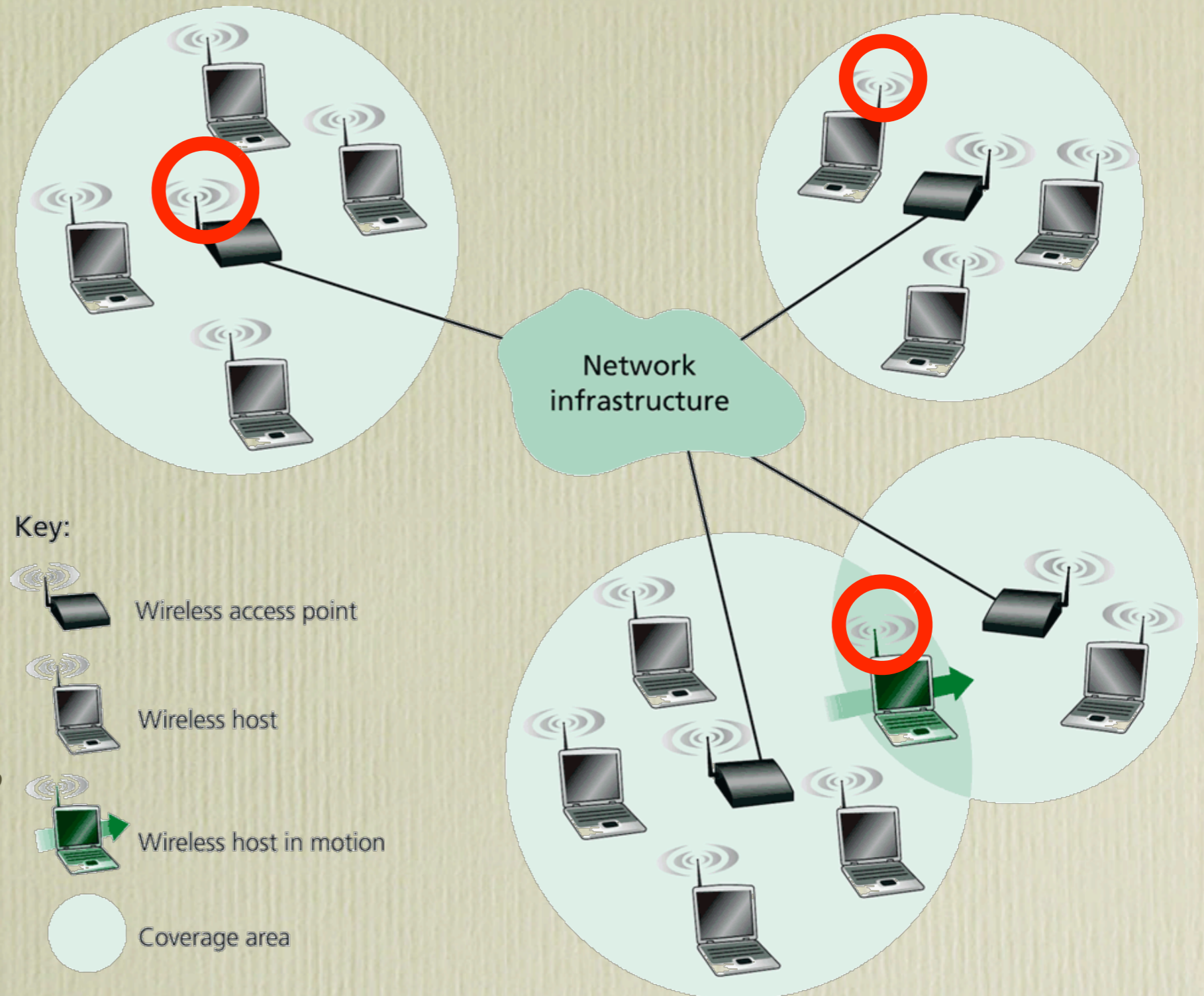
# Elements of a wireless network

- base stations
- typically connected to wired network
- responsible for relaying packets between wired and wireless network in its coverage area
- e.g., cell towers, 802.11 access points



# Elements of a wireless network

- wireless link
- used to connect mobiles to base station
- also used as backbone link
- MAC protocol coordinates link access
- varying data rates, transmission distances

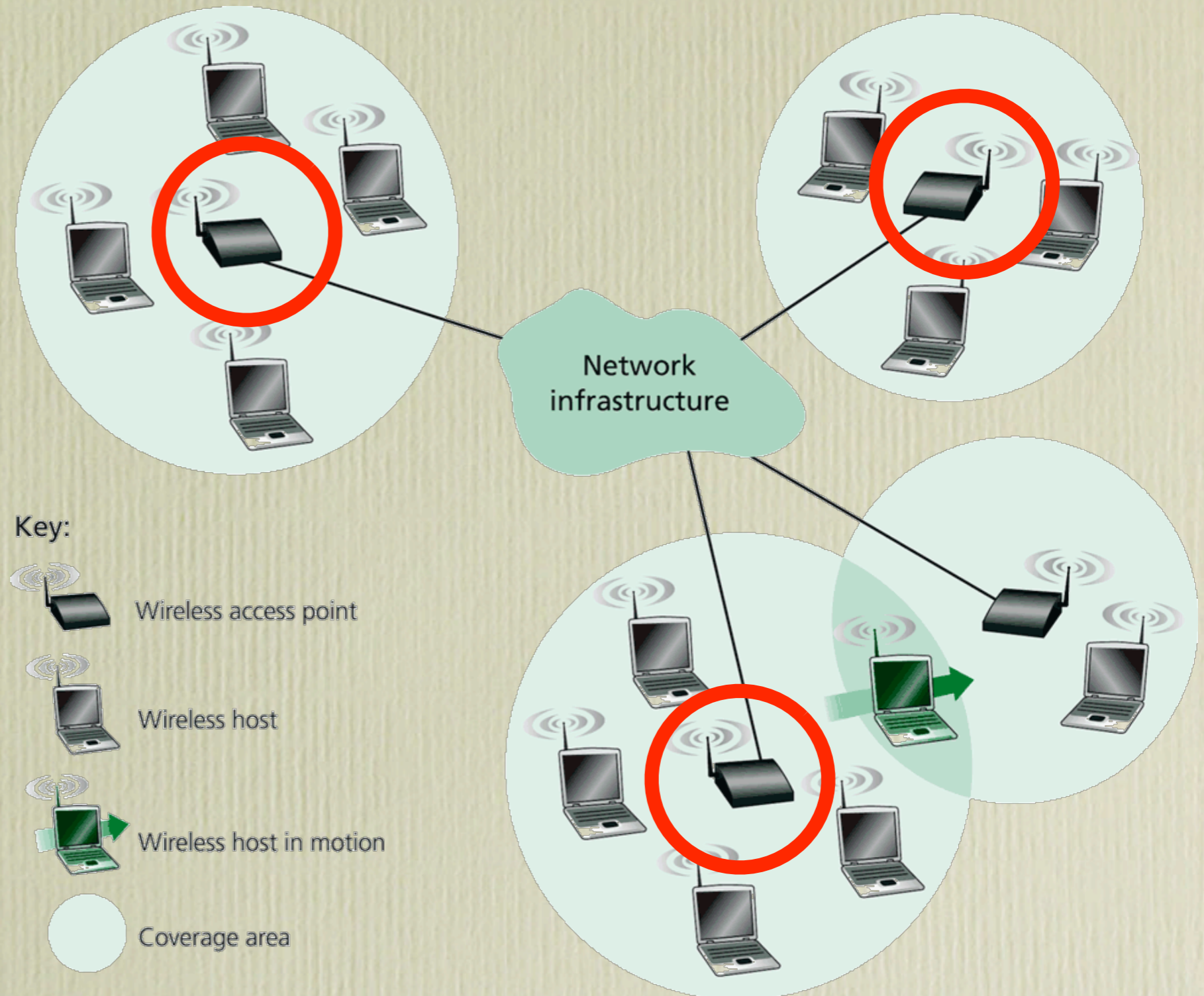


# Characteristics of wireless links

100Mbps	802.11n (WiFi)			
70Mbps				802.16 (WiMAX)
54Mbps	802.11a/g (WiFi)			
5-11Mbps	802.11b (WiFi)			
1Mbps	802.15 (WPAN)			
384Kbps	UMTS/WCDMA, CDMA2000 (3G)			
56Kbps	IS-95 CDMA, GSM (2G), GPRS/EDGE (2.5G)			
	Indoor 10-30m	Outdoor 50-200m	Mid-range outdoor 200m-4km	Long-range outdoor 5km-50km

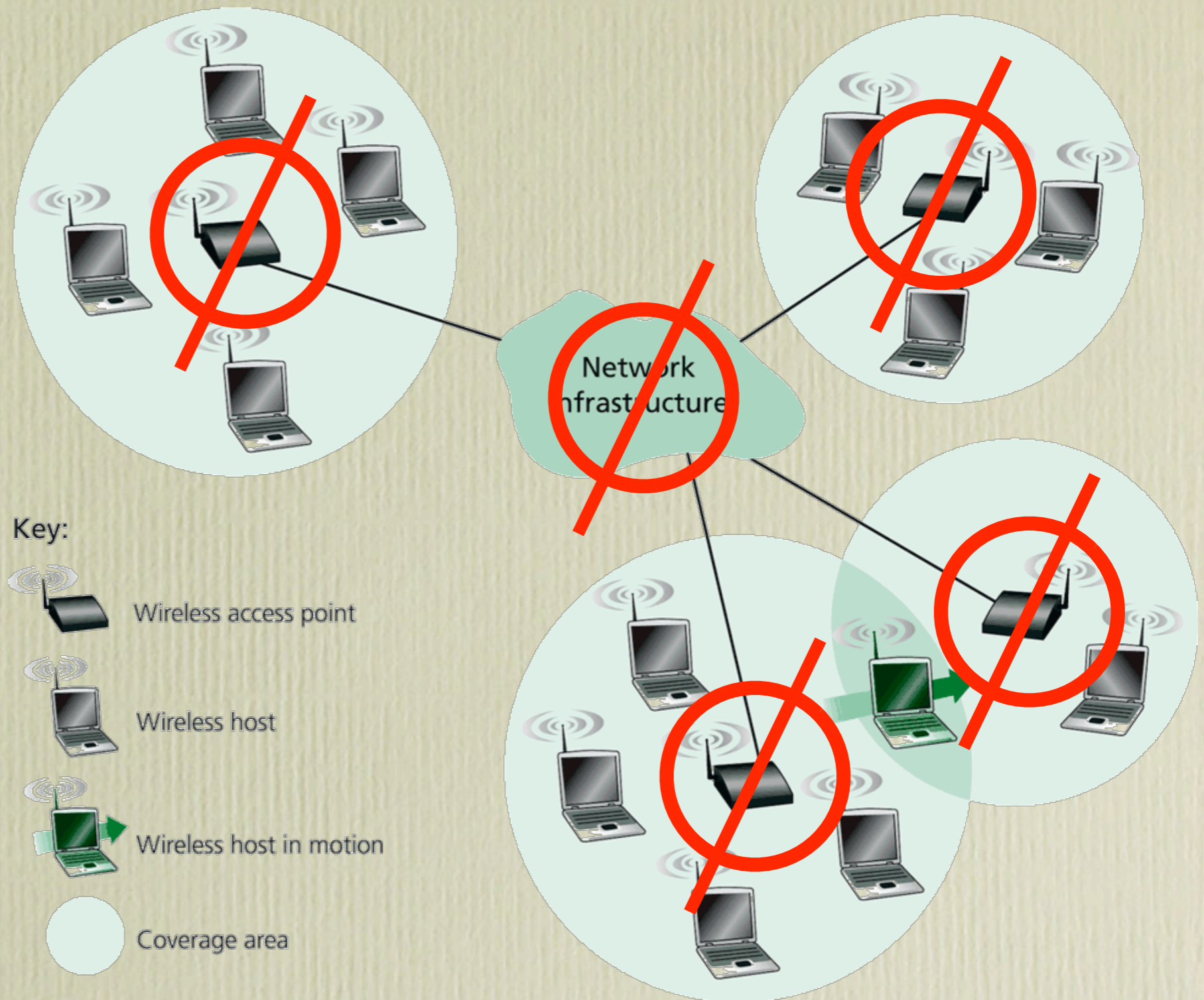
# Elements of a wireless network

- *infrastructure* mode
- base station connects mobile to wired network
- handoff: mobile changes the base station that is providing its connection to wired network



# Elements of a wireless network

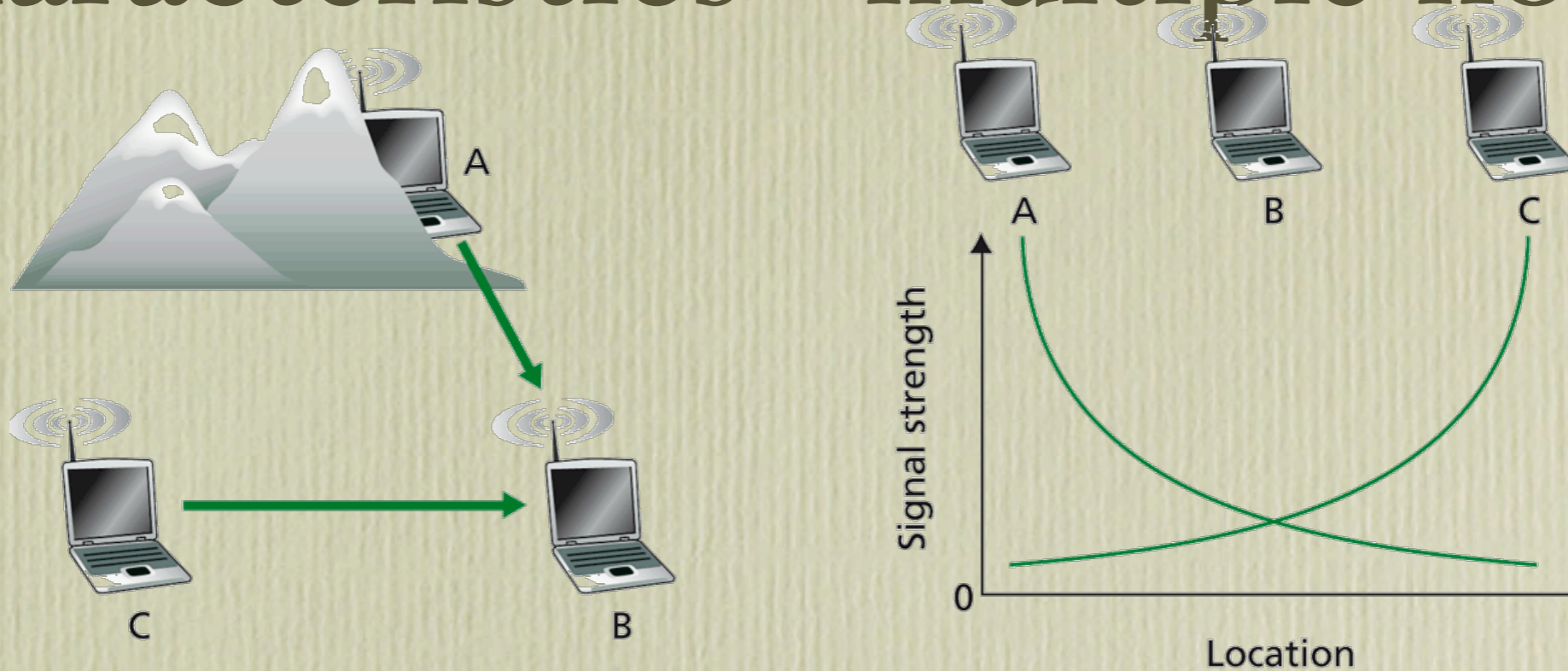
- *ad hoc* mode
- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organise into a network
  - route amongst themselves
  - i.e., nodes run routing algorithms
- Sony PSP uses ad hoc 802.11.b



# Characteristics of wireless links

- Different from wired link!
- *varying signal strength*
  - radio link attenuates as it propagates through matter
- *interference*
  - frequencies may be shared (e.g., 2.4GHz ISM bands used by phones)
  - other devices may interfere (microwave ovens)
- *multipath propagation*
  - radio signal reflects off objects, frames arrive at destination at different times

# Characteristics - multiple nodes

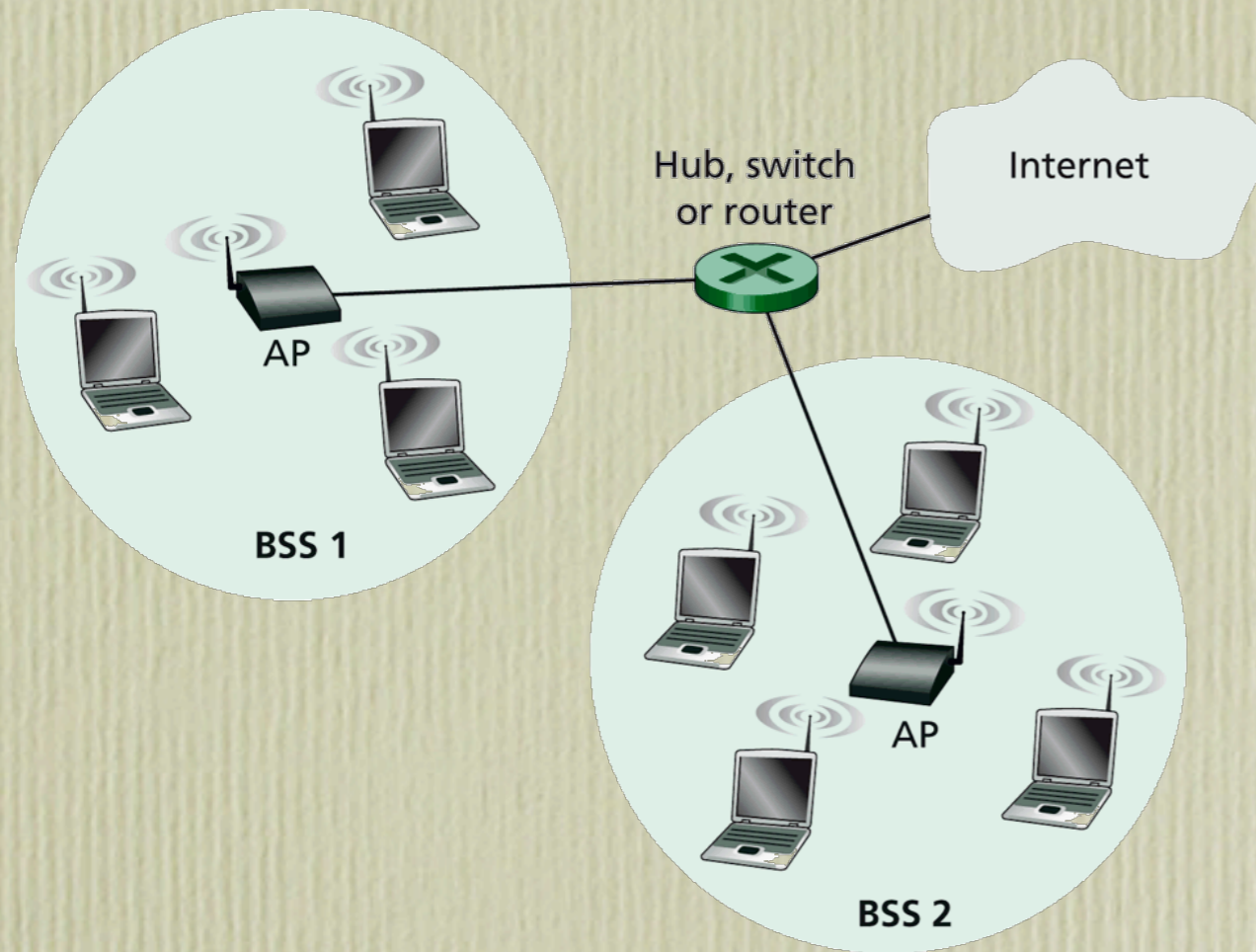


- Shared channel, so standard MAC problem, and more!
- *hidden terminal*: B and A hear each other, B and C hear each other, but A and C cannot hear each other
  - A and C may transmit to B simultaneously
- *signal fading*: A and C cannot hear each other interfering at B

# IEEE 802.11 Wireless LAN (WiFi)

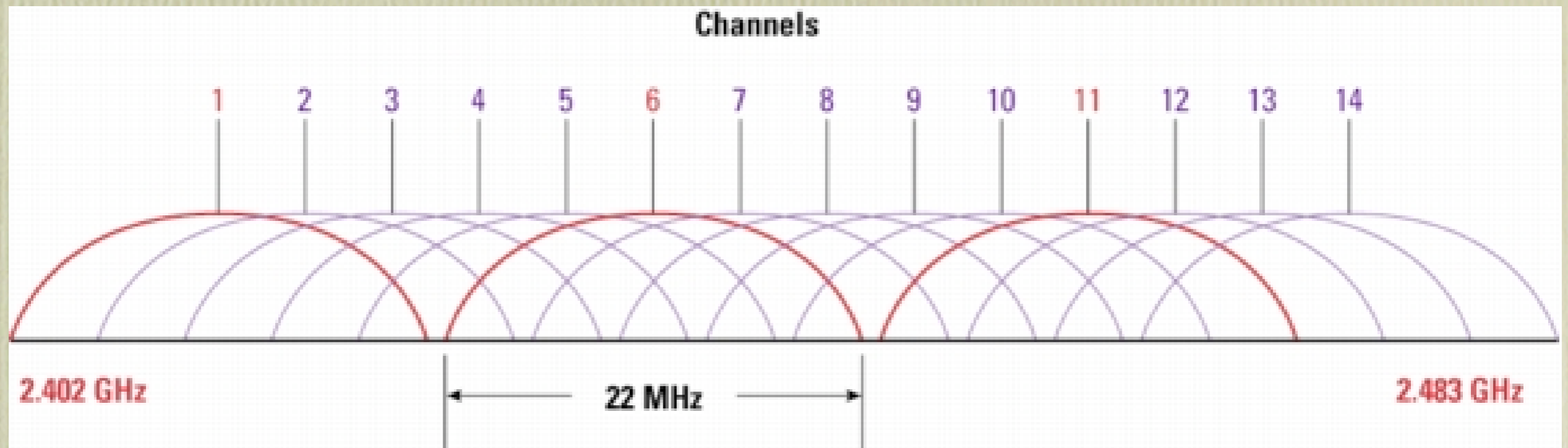
- 802.11b
  - 2.4GHz unlicensed (ISM) spectrum
  - up to 11Mbps
  - direct sequence spread spectrum physical layer
    - handles signal carrier, modulation
    - similar to CDMA
    - older 802.11 used frequency-hopping
- 802.11g
  - 2.4GHz
  - up to 54Mbps (different symbol encoding)
  - backwards-compatible with 802.11b (but slows data rate)
- 802.11a
  - 5.1-5.2 and 5.8GHz spectrum
  - up to 54Mbps
- 802.11n
  - $\geq 100$ Mbps
  - MIMO (multiple antennas)
  - 2.4 or 5GHz spectrum
  - interoperable with 802.11a/b/g
  - still in development
- All use CSMA/CA MAC
- All have infrastructure and ad hoc versions

# 802.11 architecture



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

# 802.11 channels



- 802.11b/g: 2.4-2.485GHz spectrum divided into 14 channels
  - AP admin chooses channel for AP
  - interference: channel may overlap/equal that of neighbouring AP
    - 11b/g has only 3 non-overlapping channels! Makes deploying a campus-wide network difficult (or installing a single AP in a crowded apartment block)
    - 802.11a has 16 channels (8 non-overlapping)
- Channel allocations differ by country
  - US only uses 1-11
  - only 10 and 11 are usable worldwide

# 802.11: association

- host must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP name (SSID) and MAC address (BSSID)
    - AP periodically broadcasts beacons (remember radio is broadcast)
      - active scanning - send *Probe Request*, APs send *Probe Response*
    - SSID (Service Set ID), e.g., “Kiewit Wireless”
      - can span multiple BSSIDs
  - selects an AP with which to associate
    - e.g., highest RSSI (Received Signal Strength Indicator)
    - or by using list of preferred SSIDs
  - may authenticate if required (WEP/WPA)
  - typically then runs DHCP to get IP address in AP’s subnet
- when finished, host may *disassociate*
  - not required (laptop may be closed, or may roam)

# 802.11: MAC

- MAC protocol wants to avoid collisions
  - two nodes transmitting at the same time
- CSMA - sense before transmitting
  - don't collide with other nodes' ongoing transmissions
- *No* collision detection!
  - difficult in wireless environment
    - cannot receive while transmitting
    - signal fading
    - hidden terminal
  - CSMA/CA
    - Collision *Avoidance*

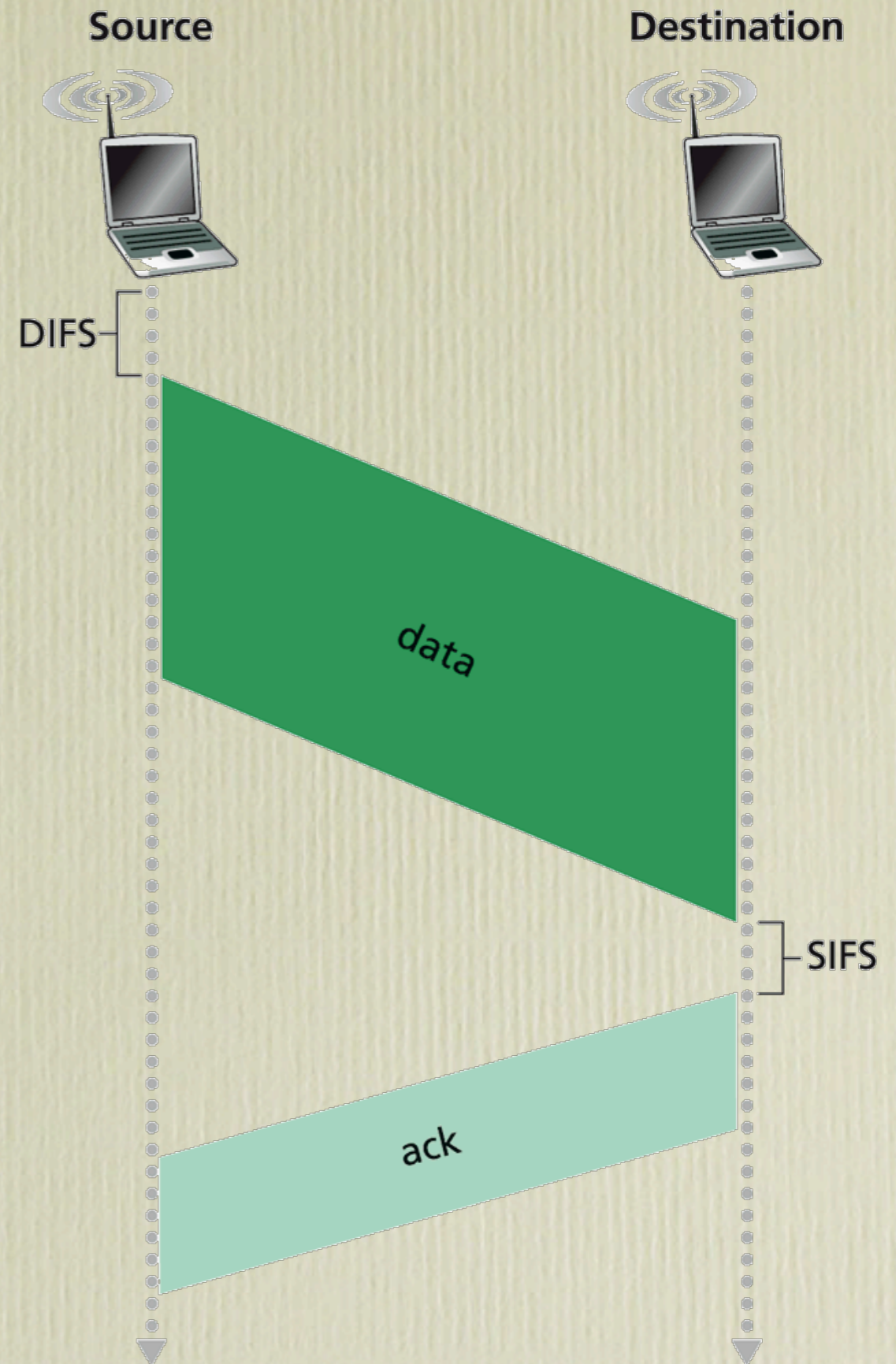
# CSMA/CA

## Sender

- if sense channel idle for DIFS (Distributed Inter-frame Space) then transmit *entire* frame (no CD)
- 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 timer

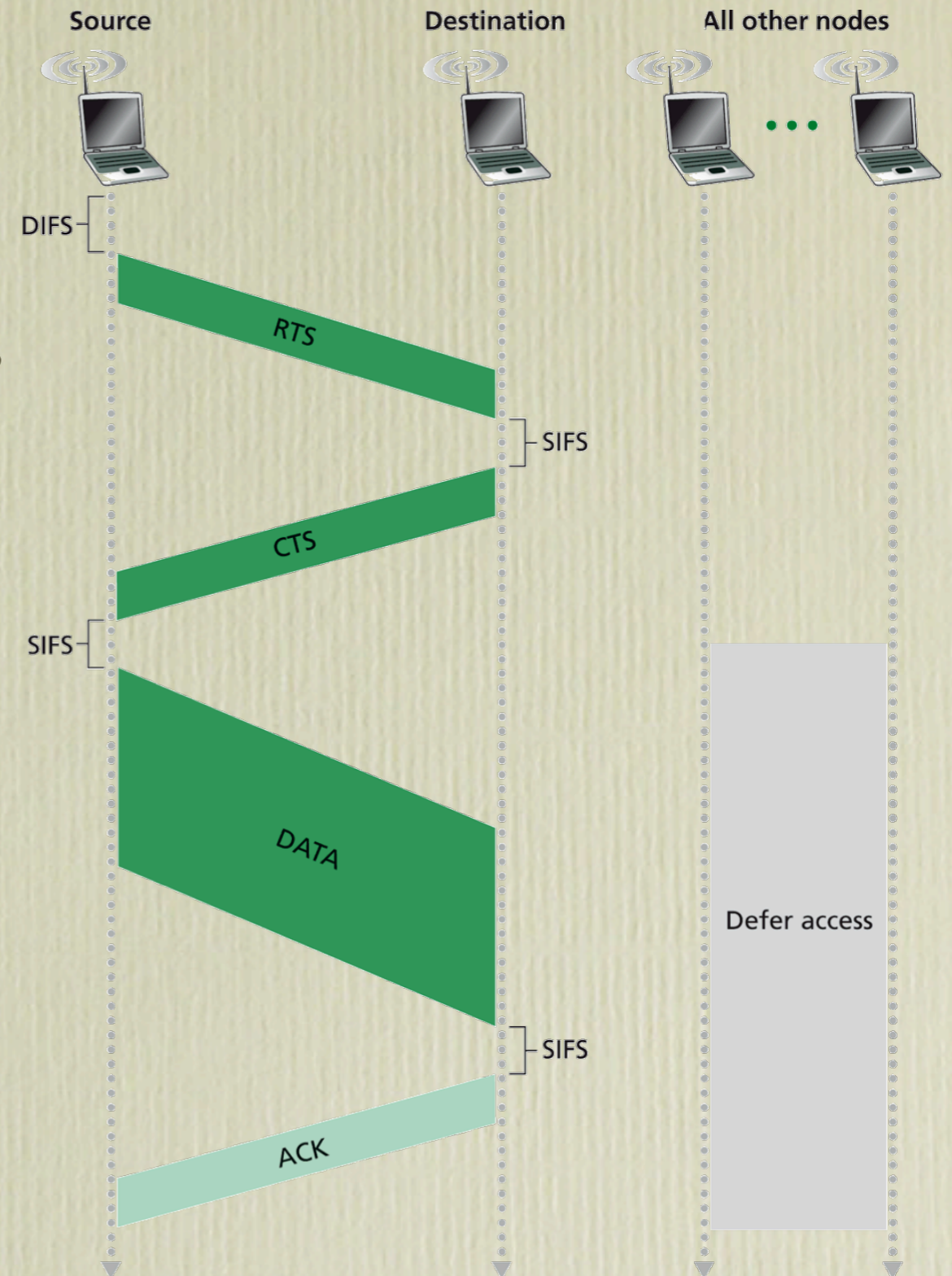
## Receiver

- if frame received OK then
  - return ACK after SIFS (Short Inter-frame Spacing)
  - ACK needed because of hidden terminal problem
  - SIFS, DIFS, PIFS for priority

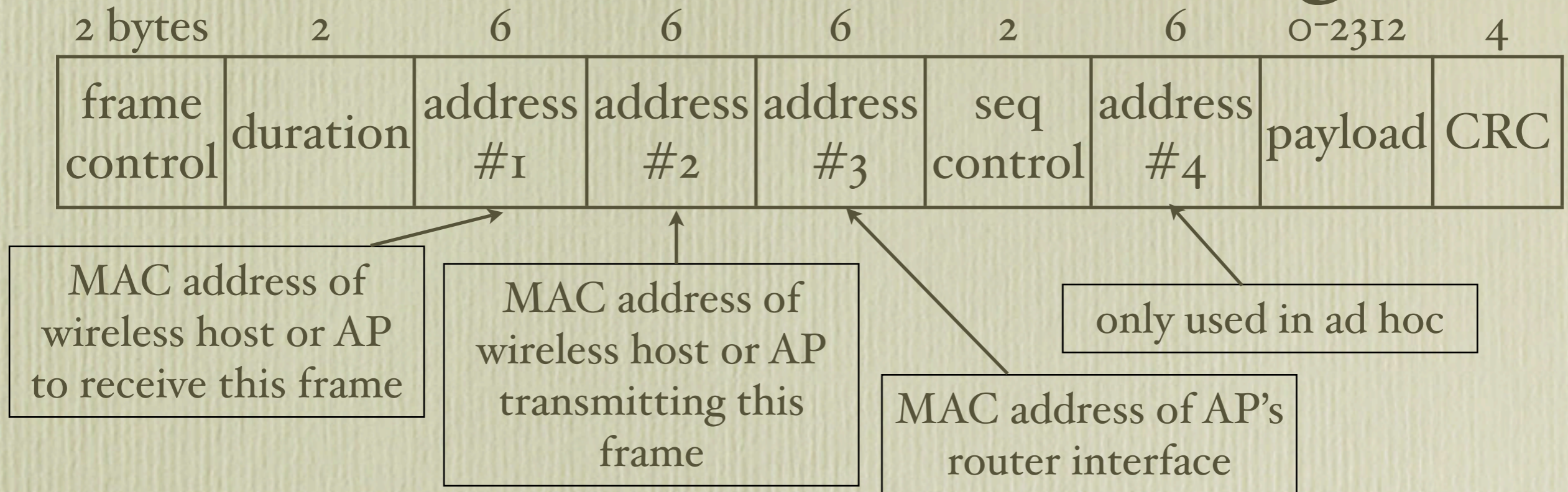


# RTS/CTS

- goal: allow sender to “reserve” channel rather than random access of data frames
- avoid collisions of long data frames
- sender first transmits small RTS (Request-To-Send) frame to AP using CSMA
- RTS frames may collide with each other (but they are short)
- AP broadcasts CTS (Clear-To-Send) in response to RTS
- CTS heard by all nodes (including hidden terminals)
- other stations defer transmission for the time specified in the CTS

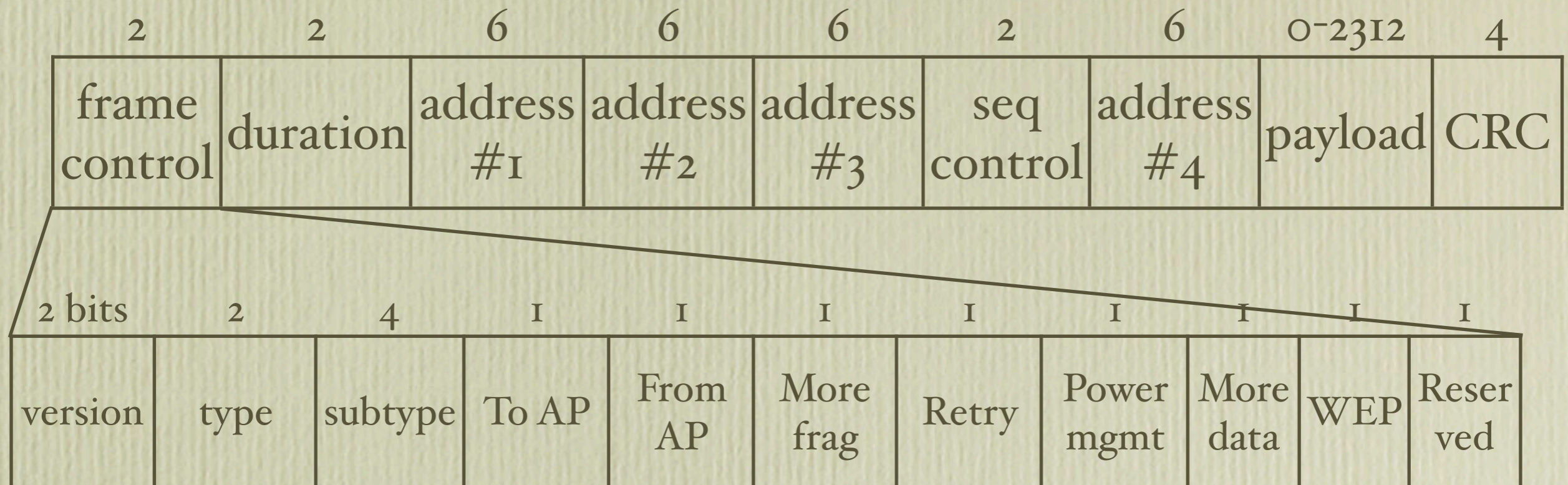


# 802.11 frame: addressing



- AP *bridges* 802.11 to 802.3 (Ethernet)
  - “wireless Ethernet”
  - AP is transparent to routers - they just see hosts
- AP removes 802.11 header and adds 802.3 header with AP router MAC as source (or dest)

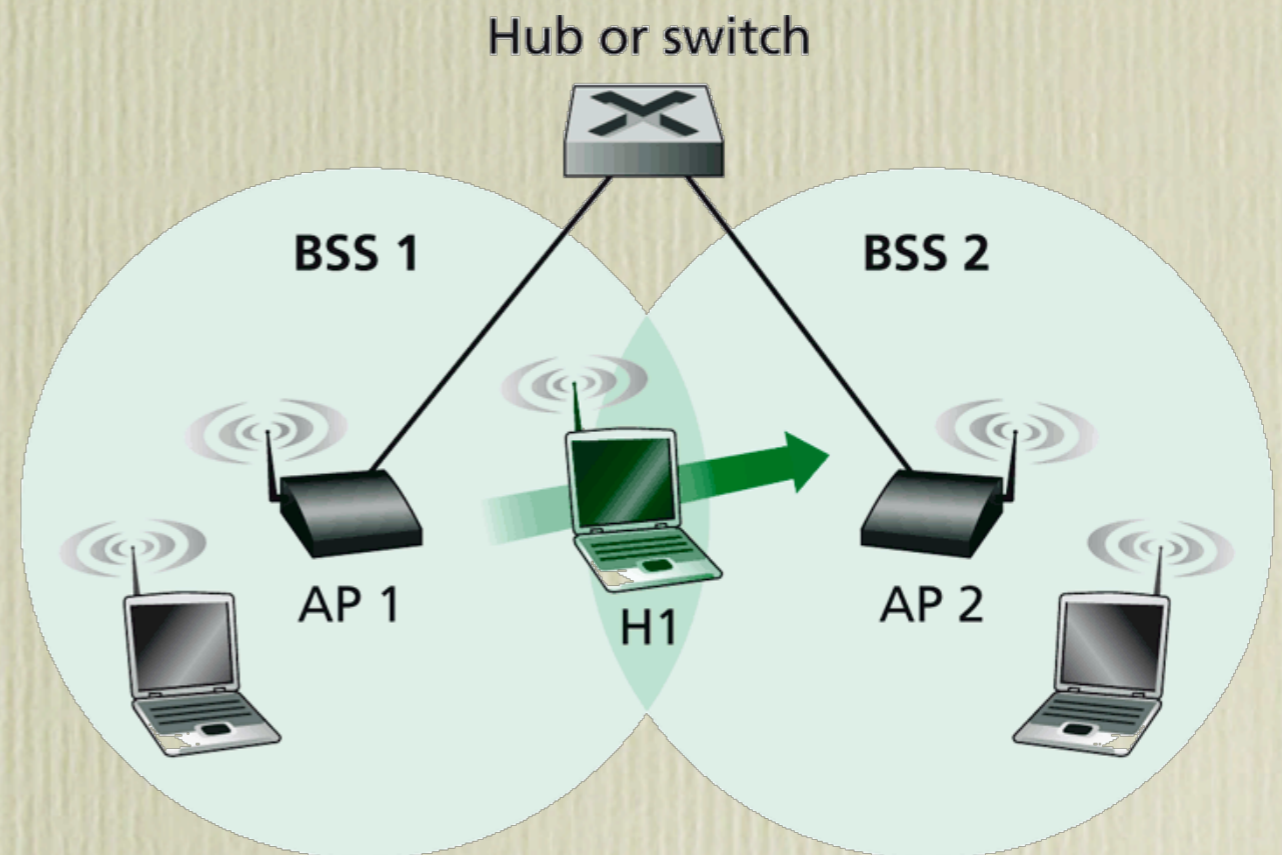
# 802.11 frame: other fields



- frame control: lots of fields
  - type (beacons, RTS/CTS, data, ACKs etc.)
  - To & From affect address fields
- duration: channel reservation time
- seq control: sequence number
  - needed for retransmits (remember rdt2.1)

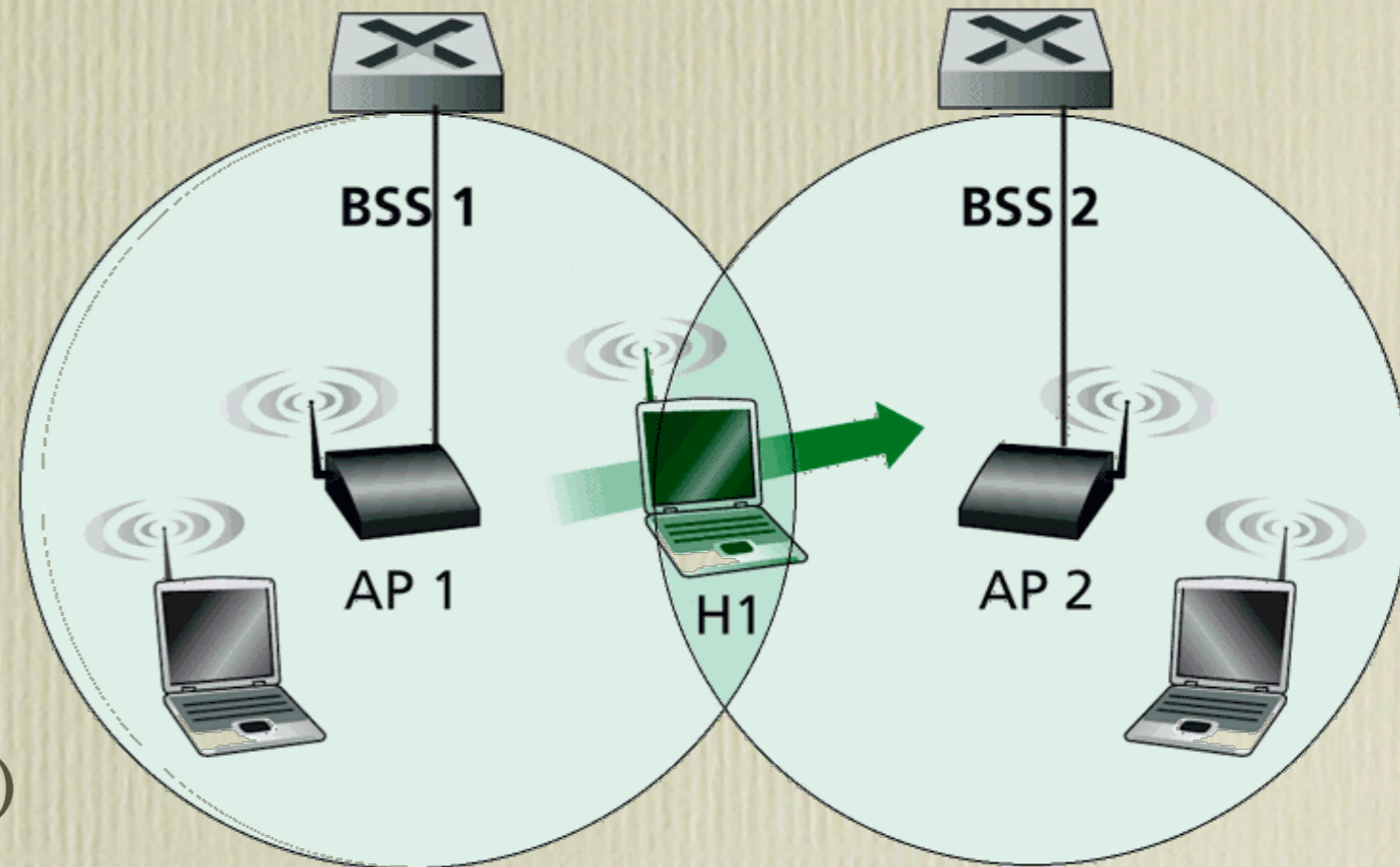
# Mobility within same subnet

- H<sub>I</sub> stays in same subnet
  - IP address remains same
  - H<sub>I</sub> *disassociates* from AP<sub>1</sub>, *roams* and *associates* with AP<sub>2</sub>
- switch 'learns' which AP H<sub>I</sub> is associated with
  - when it sees a frame from H<sub>I</sub> it remembers port
- some APs may buffer frames and forward them to new AP

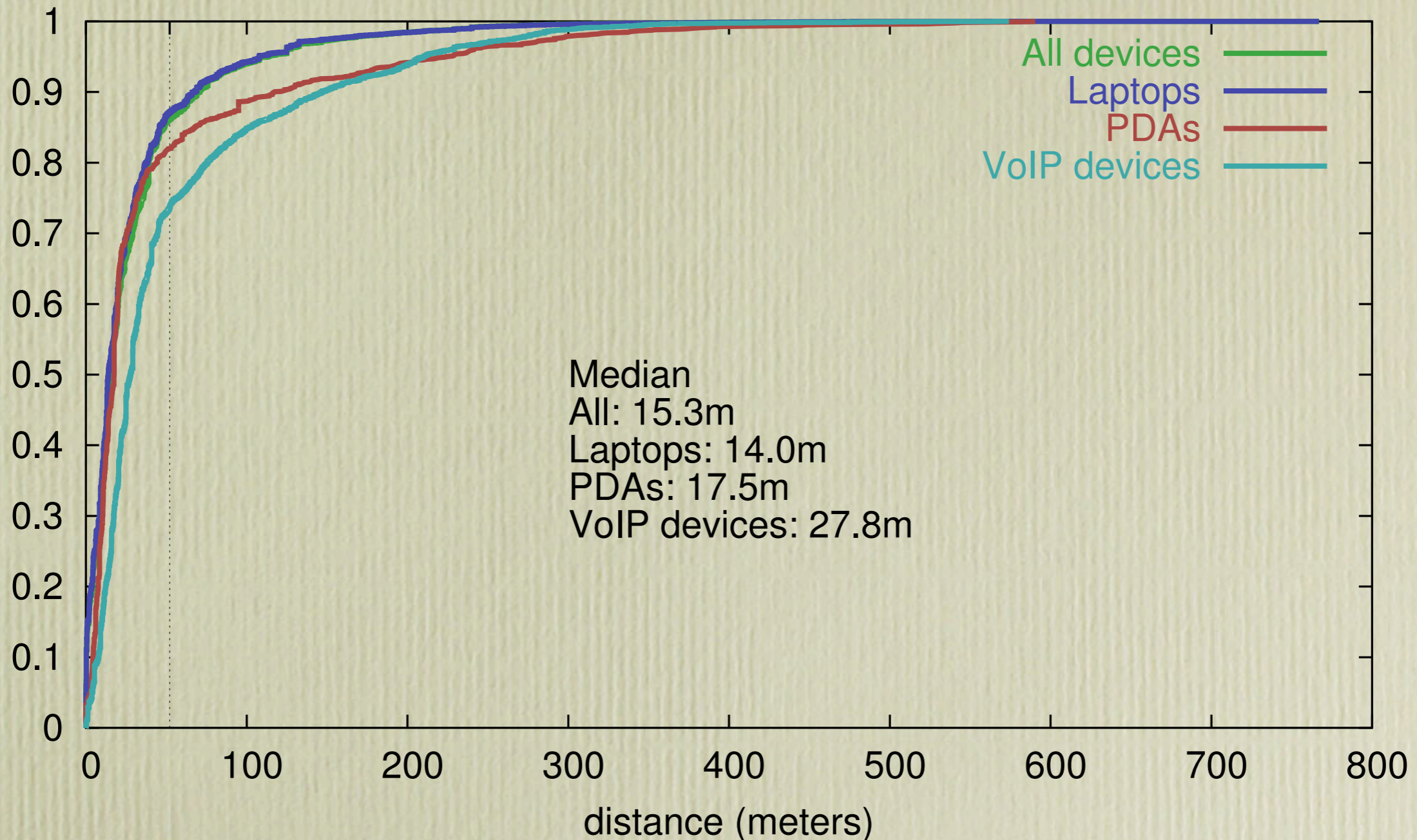


# Mobility between subnets

- H<sub>I</sub> crosses subnets
  - IP address changes!
  - What happens to TCP connections?
  - H<sub>I</sub> *disassociates* from AP<sub>I</sub>, *roams* and *associates* with AP<sub>2</sub>
  - common at Dartmouth
  - new Aruba system helps (see David Bourque's talk)
- *ping-pong* effect
  - H<sub>I</sub> may associate and *reassociate* with AP<sub>I</sub>, then AP<sub>2</sub>, then AP<sub>I</sub>, etc...
    - varying RSSI



# Mobility at Dartmouth



- Most laptops aren't mobile
- But what about VoIP devices?

# Impact of mobility

- logically, should be no problem
  - TCP, UDP can run over wireless and mobile links
- in practice, performance impacted
  - loss/delay due to bit errors (discarded packets, delays for link-layer retransmissions) and handoff
  - TCP interprets loss as congestion and backs off
  - means delay impaired (think real-time traffic e.g., VoIP)
  - restricts the already-limited bandwidth of wireless links
  - different APs may have different numbers of users

# Power management

- Perhaps the biggest problem in wireless networks
  - radio is a big power drain
- Mobile station can choose to sleep
  - *Listen Interval* in association request, *Power Management* bit in frames
  - AP will buffer frames and send in intervals
  - beacons can tell stations to wake up if they have frames waiting
- Choose AP with strongest RSSI
- Mobile station might reduce power levels
- In ad hoc networks, power-aware routing
  - e.g., forward to closer nodes
  - don't forward if battery level is low

# 802.11 data rates

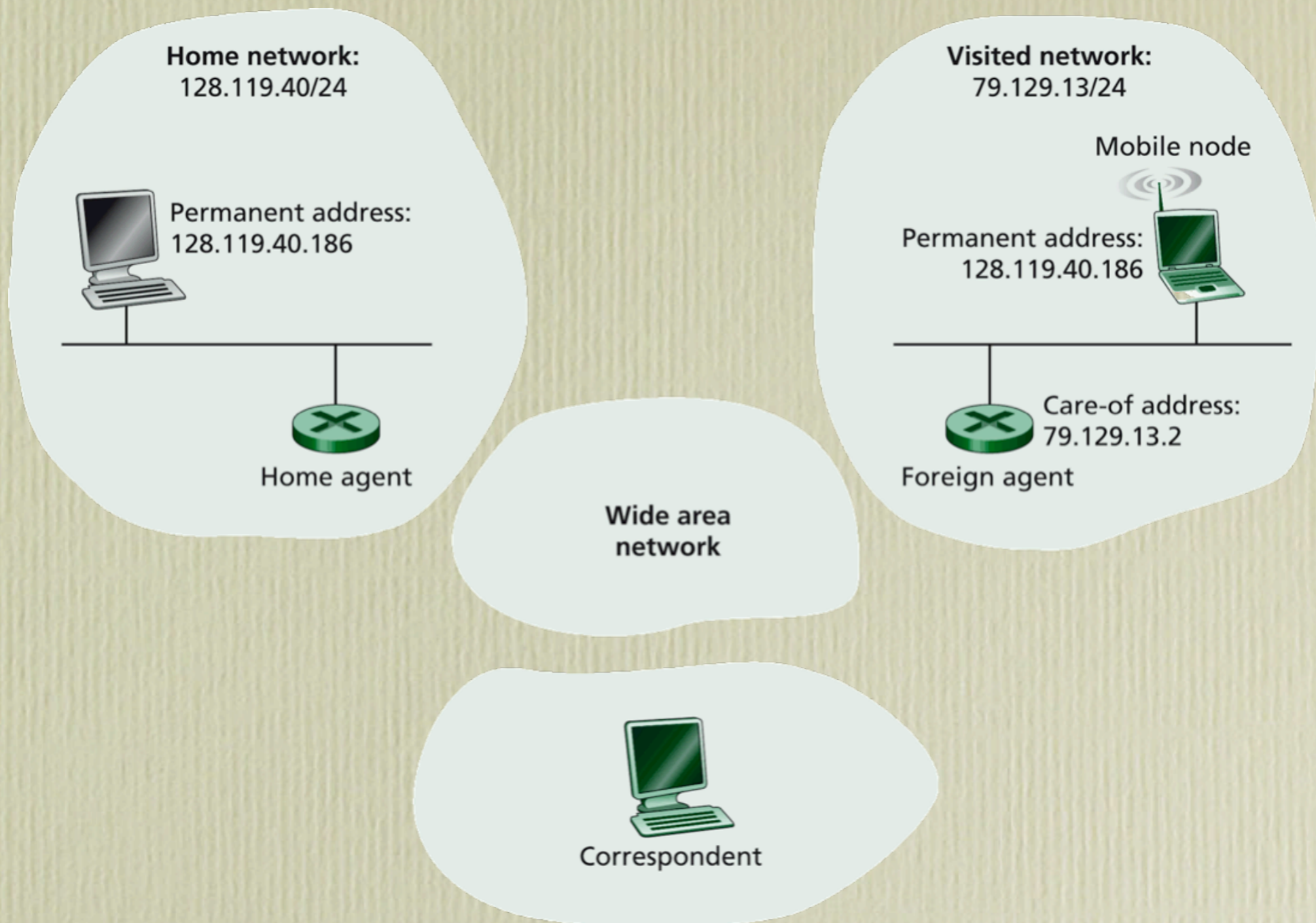
- 802.11b is 11Mbps. What does this mean?
  - 11Mbps link-layer rate
  - 802.11 headers, ACKs, DIFS, SIFS, etc included
  - typically get 5-6 Mbps at best
- different data rates depending on S/N
  - e.g., 802.11b: 1, 2, 5.5, 11Mbps
  - AP and stations will advertise supported rates
  - station will choose lower rate if low S/N
    - higher noise, lower Shannon limit, so lower rate - use different encoding
  - AP might choose not to allow clients with low S/N
    - force them on to other APs (load-balancing)

# Fat versus thin access points

- Fat APs (Cisco)
  - transparent to network
    - AP turns 802.11 frame into 802.3 frame
  - easy to physically deploy (just plug into Ethernet)
  - hard to manage
  - hard to do mobility, without creating huge subnets
- Thin APs (Aruba)
  - can create virtual LANs (virtual subnets that span links)
  - can deal with intra-subnet mobility, security, radio calibration
  - can be cheaper (APs are cheaper, but require expensive switch)
  - requires *encapsulation* of frames
    - 802.11 frames sent to switch, which acts accordingly
  - cross-layer solution ☹

# Mobile networking

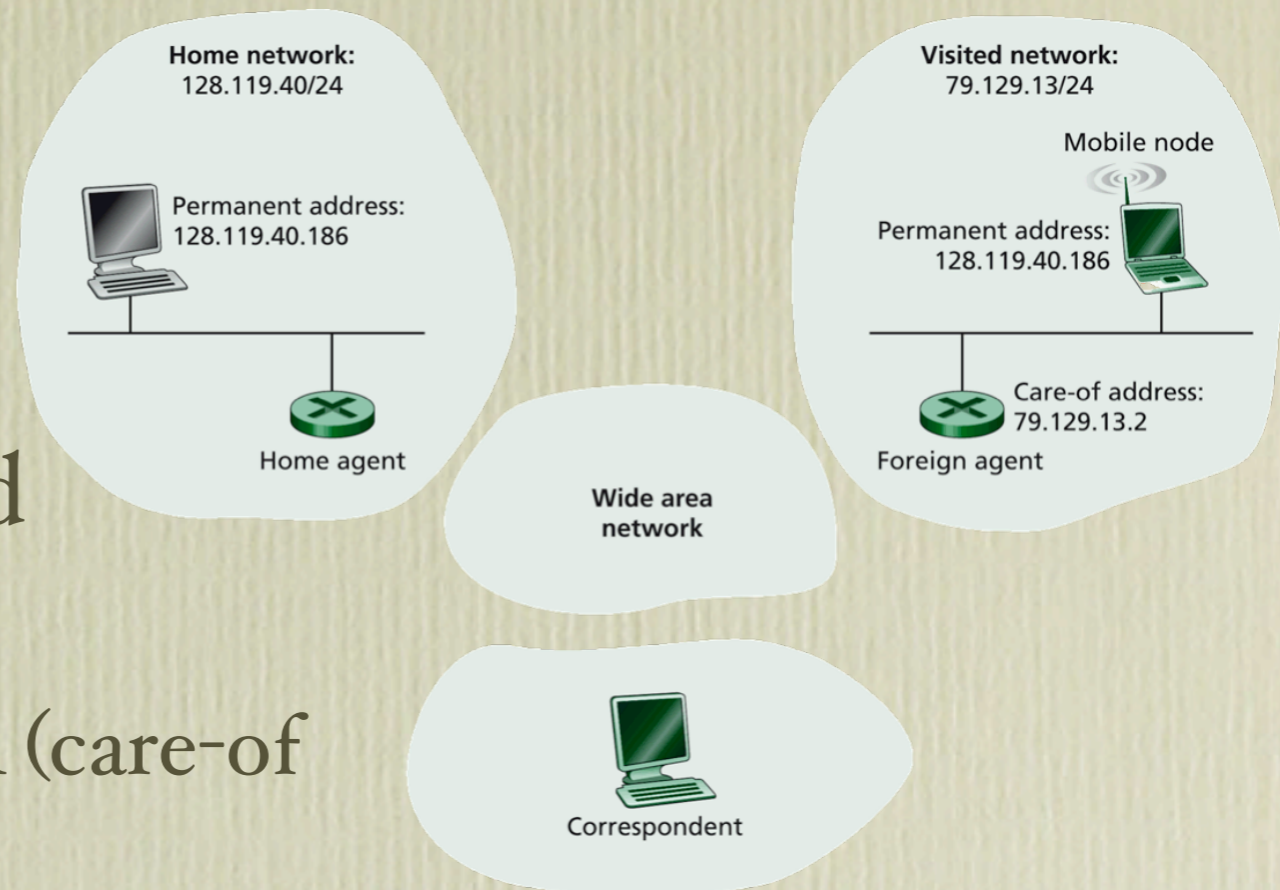
- Goal: allow mobile station to maintain ongoing connections while moving between networks (not just subnets)
  - useful for lots of mobile applications
- Cellphones can roam between base stations and networks, so why not VoIP phones?
- Cellphones keep same phone number, so should mobile nodes keep same IP address?
  - useful for servers, maintaining TCP connections
  - but not for *all* users - some are happy with DHCP and DSL at home



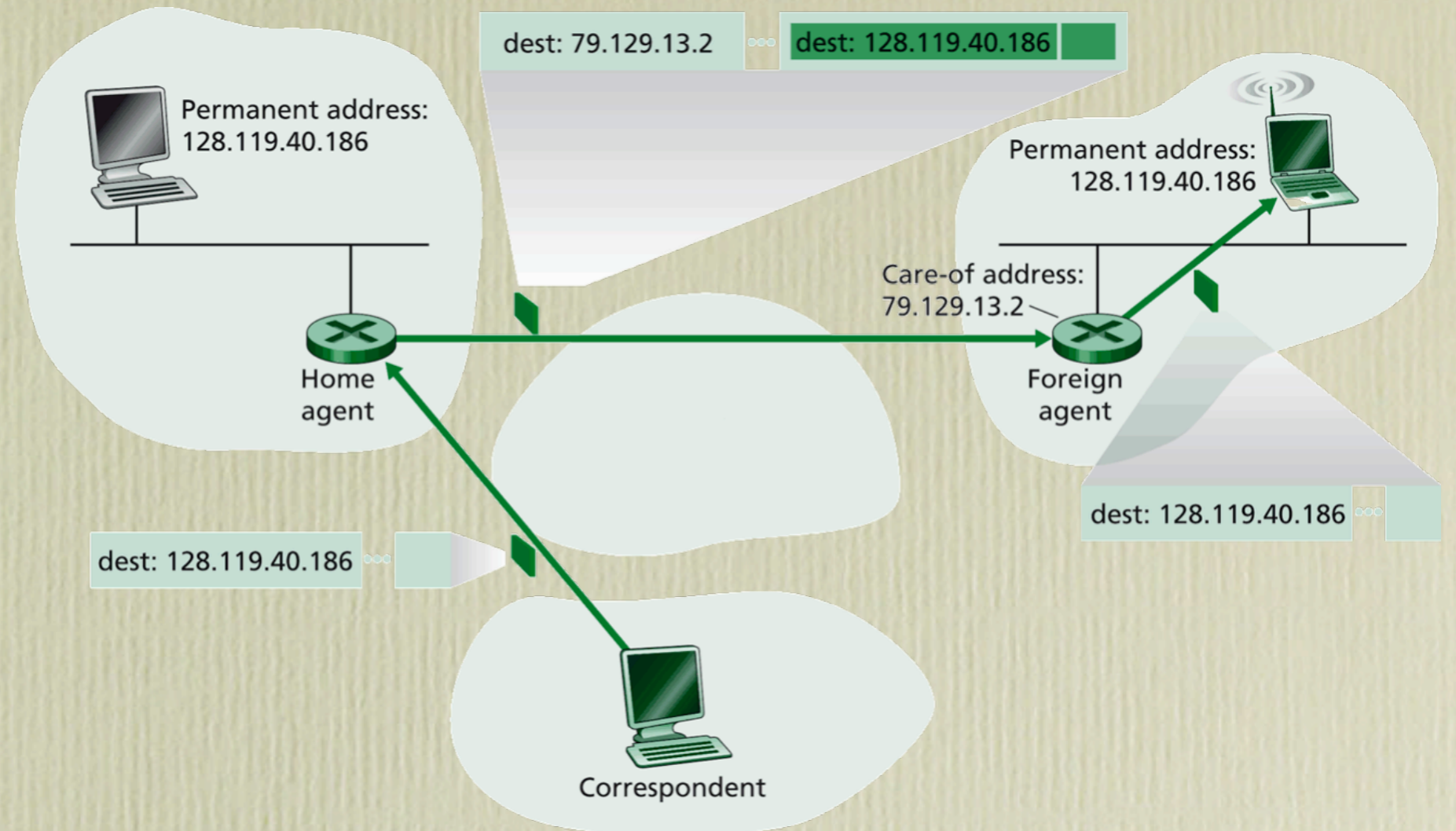
- We want *correspondent* to be able to communicate with *mobile node* even when they are on *visited network*
- *Home agent* and *foreign agent* take care of mobility management

# Addressing

- Node has *permanent address*
  - IP address
- Node *registers* when in visited network:
  - foreign agent gives node a COA (care-of address) in that network's range
  - foreign agent tells home agent that the node is resident in visited network, and node's COA
- Foreign agent can reside on node
  - but home agent needs to be separate

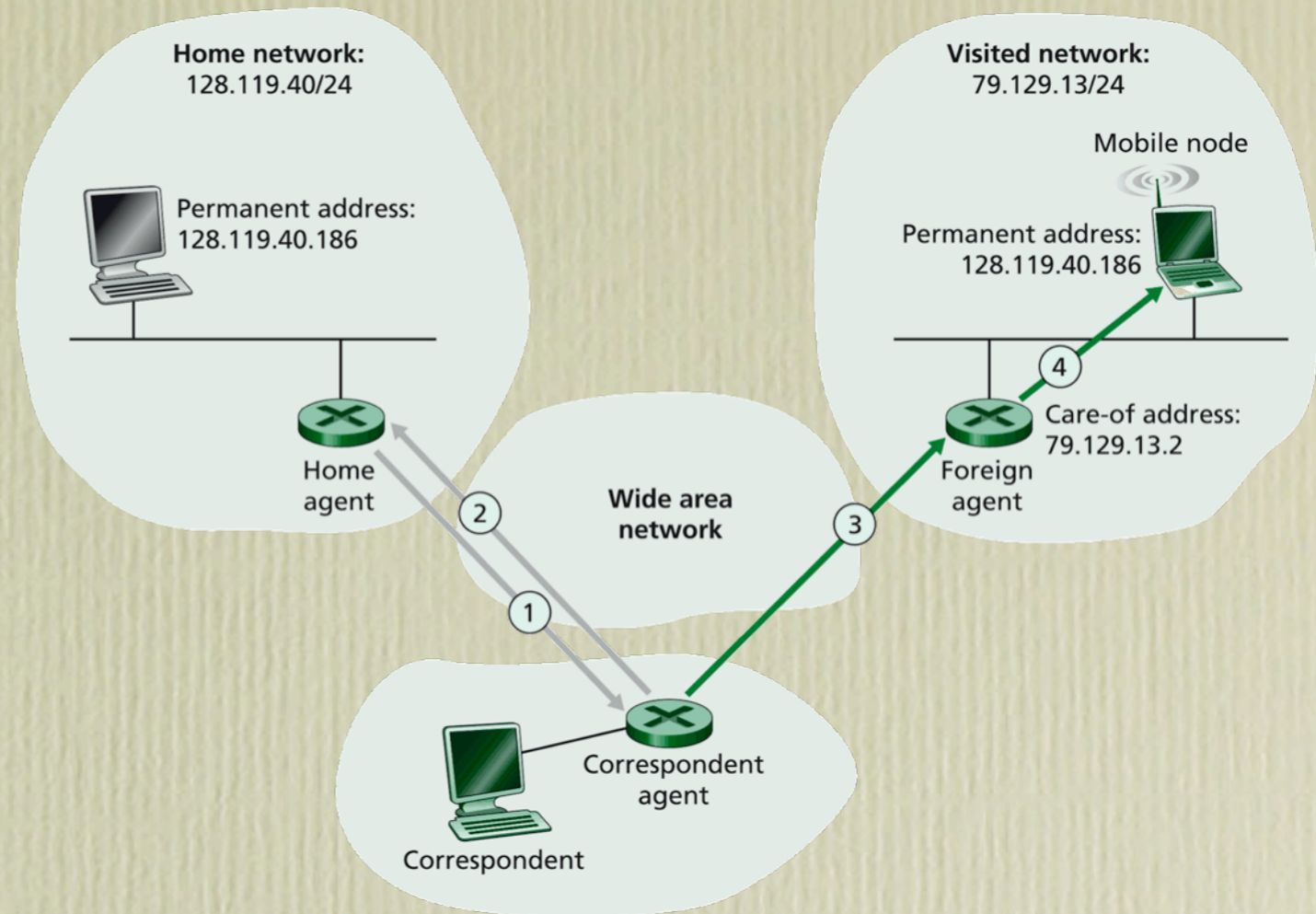


# Routing



- Indirect routing:
  - datagrams get routed from correspondent back to home agent
  - home agent then encapsulates and forwards datagrams to foreign agent (tunneling), who deencapsulates and forwards to COA
  - return datagrams go directly to correspondent
- Triangle routing: inefficient
  - what if correspondent and mobile node on same network?

# Routing



- Direct routing
- Correspondent agent in correspondent's network learns COA from home agent
  - requires mobile-user *location protocol*
- What if mobile node moves to another visited network?
  - another protocol needed to tell correspondent agent new COA
  - or original foreign agent can act as "anchor"
    - forward to subsequent foreign agents
    - this is how GSM cellphones work

# Mobile IP (RFC 3220)

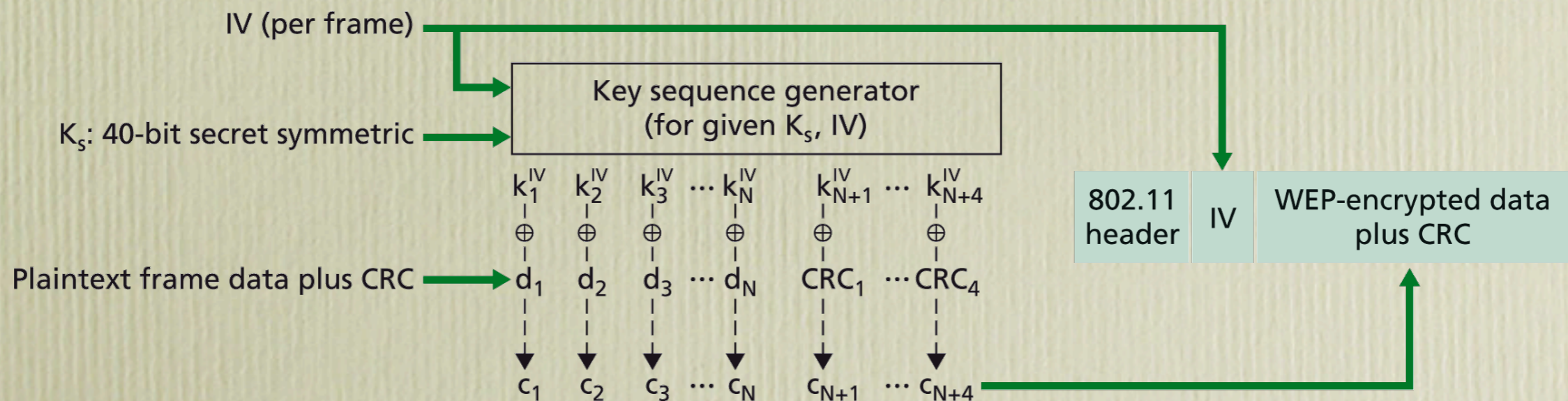
- Agent discovery
  - foreign/home agents advertise service by broadcasting ICMP
- Registration with home agent
  - node sends registration message (UDP, port 434) to foreign agent
  - foreign agent records node's permanent address and sends registration message containing COA to home agent
  - home agent checks registration address binds permanent address to COA, and replies to foreign agent
  - foreign agent checks reply and forwards to node
- Indirect routing
  - home agent encapsulates datagrams and sends to COA

# Wireless security

- Wireless is a *broadcast* channel
  - any node can see any other node's datagrams
- Some sort of link-layer security might be desirable
  - can't expect all users to use application-layer security (can we?)
  - very few home users turn on security features in their APs
- Initial 802.11 security protocol = WEP (Wired Equivalent Privacy)
  - still used in lots of CPU-bound devices (Vocera, PSP)
- Newer protocol - 802.11i, WPA (WiFi Protected Access)
  - won't cover this in class - too complex
  - but many of the threats/principles are still valid

# WEP

- symmetric shared key
  - somehow negotiated out-of-band (*key distribution*)
- when station authenticates with AP
  - AP sends *nonce* (one-time value) to station
  - station encrypts nonce using shared key
  - AP decrypts nonce
    - if match, then station is authenticated



# WEP

- 40-bit key + 24-bit IV (Initialisation Vector)
  - IV can (should) change with *every* frame
  - otherwise attacker can determine content by comparing lots of encrypted frames
- data + 4-byte CRC encrypted using RC4 stream cipher
  - RC4 creates a *stream* of key values to encrypt (XOR) each byte
  - RC4 is cheap (think CPU-bound devices)
- IV included in *plaintext* after 802.11 header
  - encrypted data appended after header and IV
- receiver uses 40-bit shared key + IV retrieved from frame to decrypt

# Problems with WEP

- Key management is complicated
  - how to conveniently distribute these 40-bit keys?
- 40-bit key length is very short
- stream ciphers vulnerable if keystream reused
  - 24-bit IV means  $2^{24}$  keys
  - so IV repeated every 17 million frames (not uncommon in busy network)
- infrequent rekeying enables *decryption dictionaries*
  - collect lots of frames over time
  - messy key management means WEP keys rarely changed
- turns out first byte in every payload is known (0xAA)
  - first byte of SNAP header (LLC)
  - leads to attacks on weak WEP keys

# Other wireless security 'features'

- Hidden SSID
  - “Kiewit Wireless” used to do this
  - Don't broadcast SSID in beacons, only respond to Probe Requests containing specific SSID
  - attacks: ask a student, Google
- MAC authentication
  - AP maintains table of permitted source MAC addresses
  - doesn't scale
    - each AP at Dartmouth would have table of >10,000 MACs
      - this problem reduced with thin APs
    - every time someone buys a new NIC they need to tell Kiewit
  - easy to spoof MAC address
    - just sniff the air, look for a permitted MAC address

# Other attacks

- Signal jammer
  - transmit white noise at high-power in ISM bands
  - not a lot we can do in the network
  - need to physically locate the jammer and dismantle it
- Spoofing
  - control traffic is insecure
  - can send deauthenticate/disassociate frames to clients
- 'Rogue' APs
  - set up APs on same channel and/or same SSID
  - *man in the middle* attacks
  - may be legitimate, e.g., student installs AP in their dorm
  - Aruba system detects rogue APs and sends deauthenticate frames to associated clients (spoofing!)

# What is acceptable security?

- Can we rely on app-layer security (ssh, SSL)?
  - can still observe IP addresses
- Even if frame is encrypted, location might still be known
  - can still see link-layer headers (i.e., MAC addresses)
  - could work out who is in whose dorm late at night
  - security, but not *privacy*
- Hard problems!
- Be careful when using wireless networks
  - especially 'free' hotspots...

# IEEE 802.15: WPANs

- low power, low rate (721 kbps) short range (10m)
- PHY: frequency-hopping spread spectrum in 2.4GHz
  - TDM, hop between 79 channels in known pseudo-random manner
- *piconets* of up to 8 devices: ad hoc networks
  - one device acts as master - synchronises clocks
- ZigBee: provides “application profiles” for devices
  - e.g., headset profile supported by two devices → interoperable
- Bluetooth: earlier WPAN (basis for 802.15 link/PHY)
- can interoperate with 802.11
  - if 802.11 and 802.15 interface on same host, *collaborative interoperability*: MAC protocols will both backoff before frames leave the NIC

# IEEE 802.16: WiMAX

- Worldwide Interoperability for Microwave Access
  - 30 mile range, 70Mbps (in theory), 2-11GHz spectrum
  - designed for wireless backhaul links, fixed broadband access
    - some propose WiMAX mobile stations, but power drain and NLOS (non-line of sight) are problems
    - can work in conjunction with 802.11 - T-Mobile train in UK
- European rival: HIPERMAN
- WiMAX standards process has been *very* slow
  - might get overtaken by a mix of other standards
  - e.g., for clients, 802.11 is getting faster
  - e.g., Dartmouth is testing another ~71-95GHz system instead - see <http://www.gigabeam.com>