Networks

Wireless and Mobile Networks - Introduction

Adopted from material in “Computer Networking: A Top Down Approach” by Kurose and Ross and slides developed by William Conner

Wireless and Mobile Networks - Introduction

Section 7.1

Overview

- Wireless
  - Characteristics
  - Code Division Multiple Access (CDMA)
  - Collision avoidance (CSMA/CA)
  - 802.11 Wi-Fi
- Cellular networks
- Mobility
  - Indirect vs. direct mobile routing
  - Mobile IP

Wireless Networks

- Communication “through the air” (unguided media)

- Examples of wireless networks
  - Cellular networks
  - 802.11 Wi-Fi
  - Sensor networks
  - Satellite communications

Wireless Devices

- Laptops
- Tablets
- Smart phones
- Internet of Things (IoT)

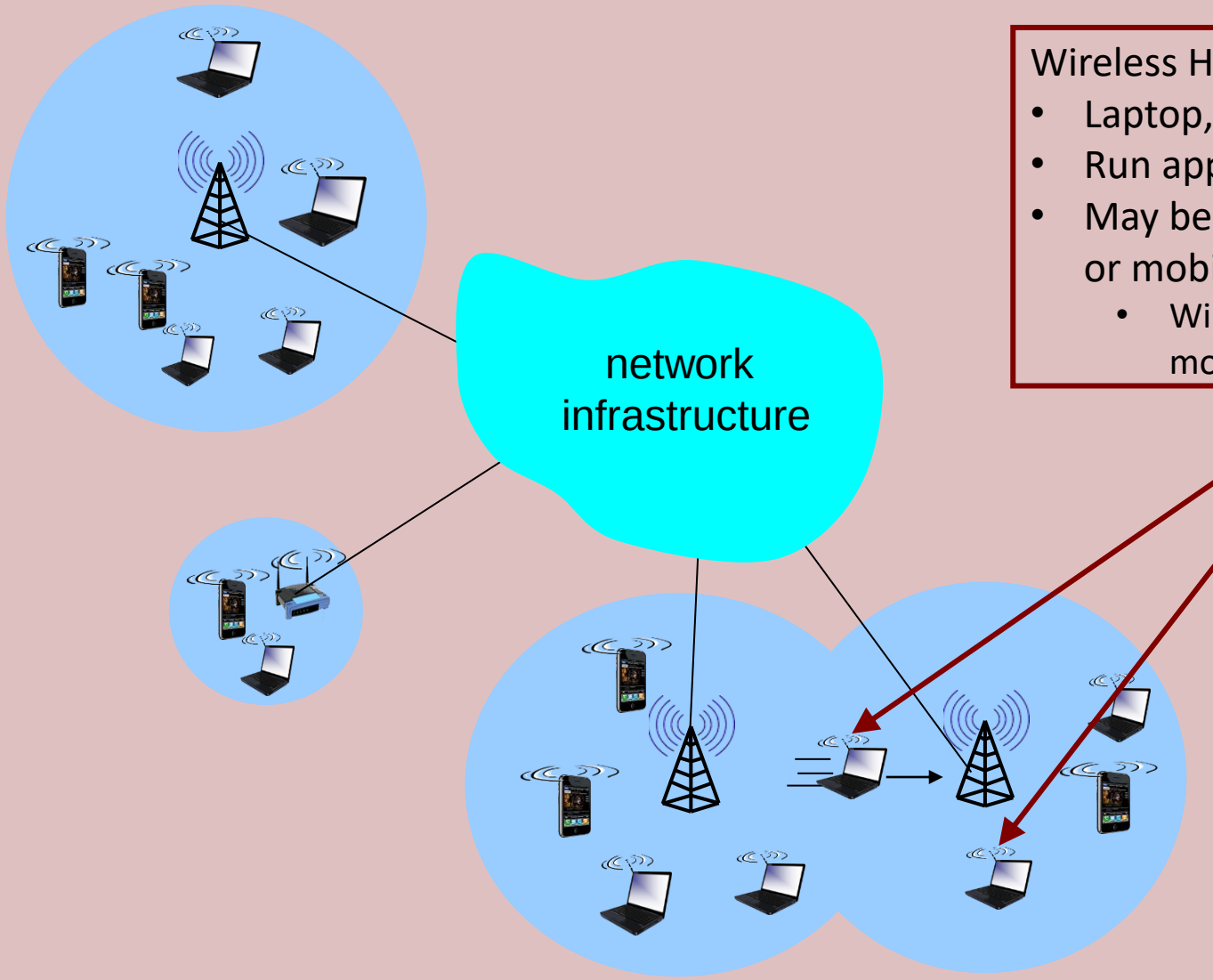
Cellular vs. Landline Phones

- Cell phone subscriptions outnumber landlines by more than 3-to-1 in the United States (2019)
  - 405 million cell phone subscriptions
  - 107 million landlines

- Cell phone subscriptions are growing and landlines are declining

Source: https://data.worldbank.org

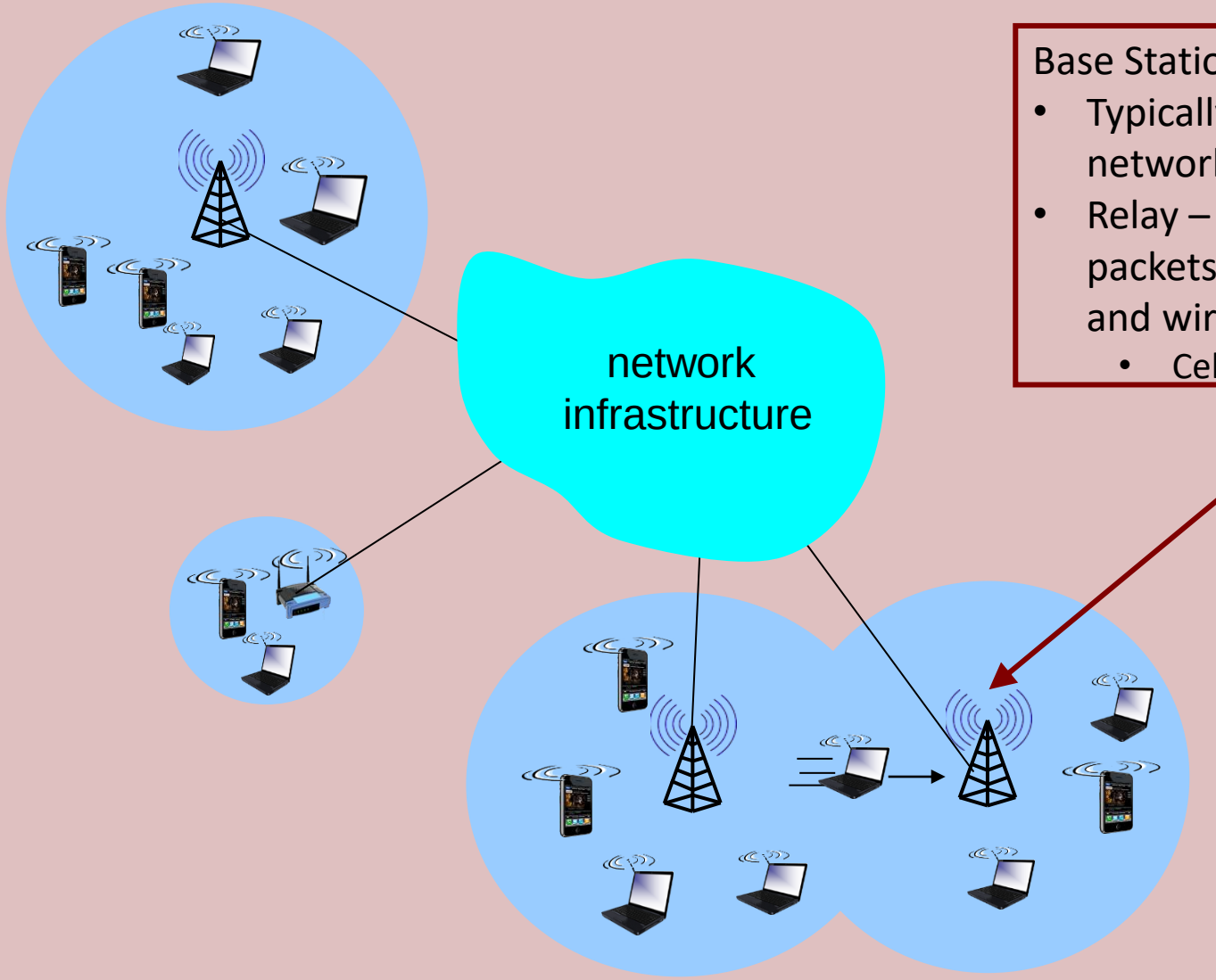
Wireless Network



Wireless Hosts:

- Laptop, smartphone
- Run applications
- May be stationary (non-mobile) or mobile
  - Wireless does *not* always mean mobility

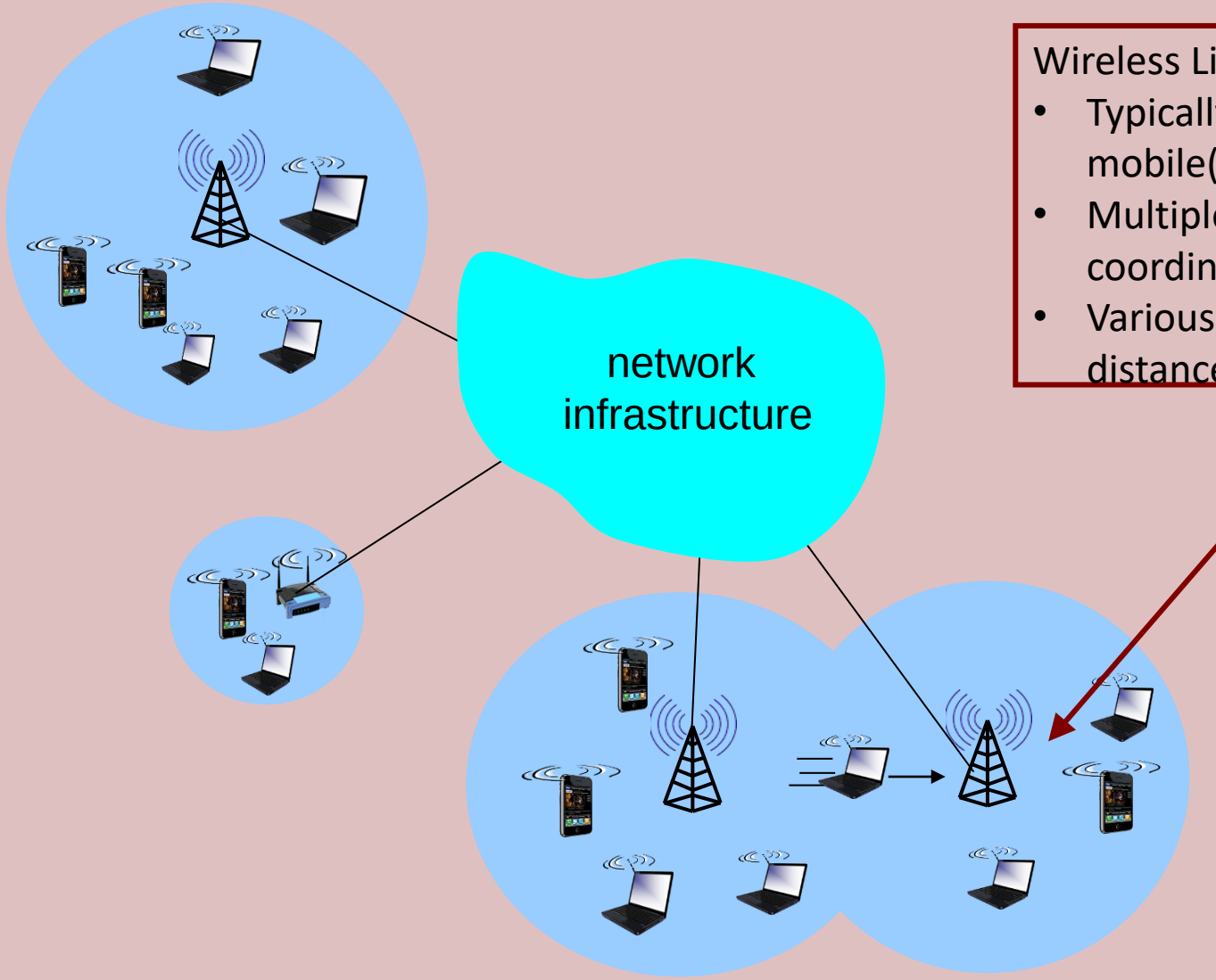
Wireless Network



Base Station:

- Typically connected to wired network
- Relay – responsible for sending packets between wired network and wireless host(s) in its “area”
  - Cell towers, 802.11 access points

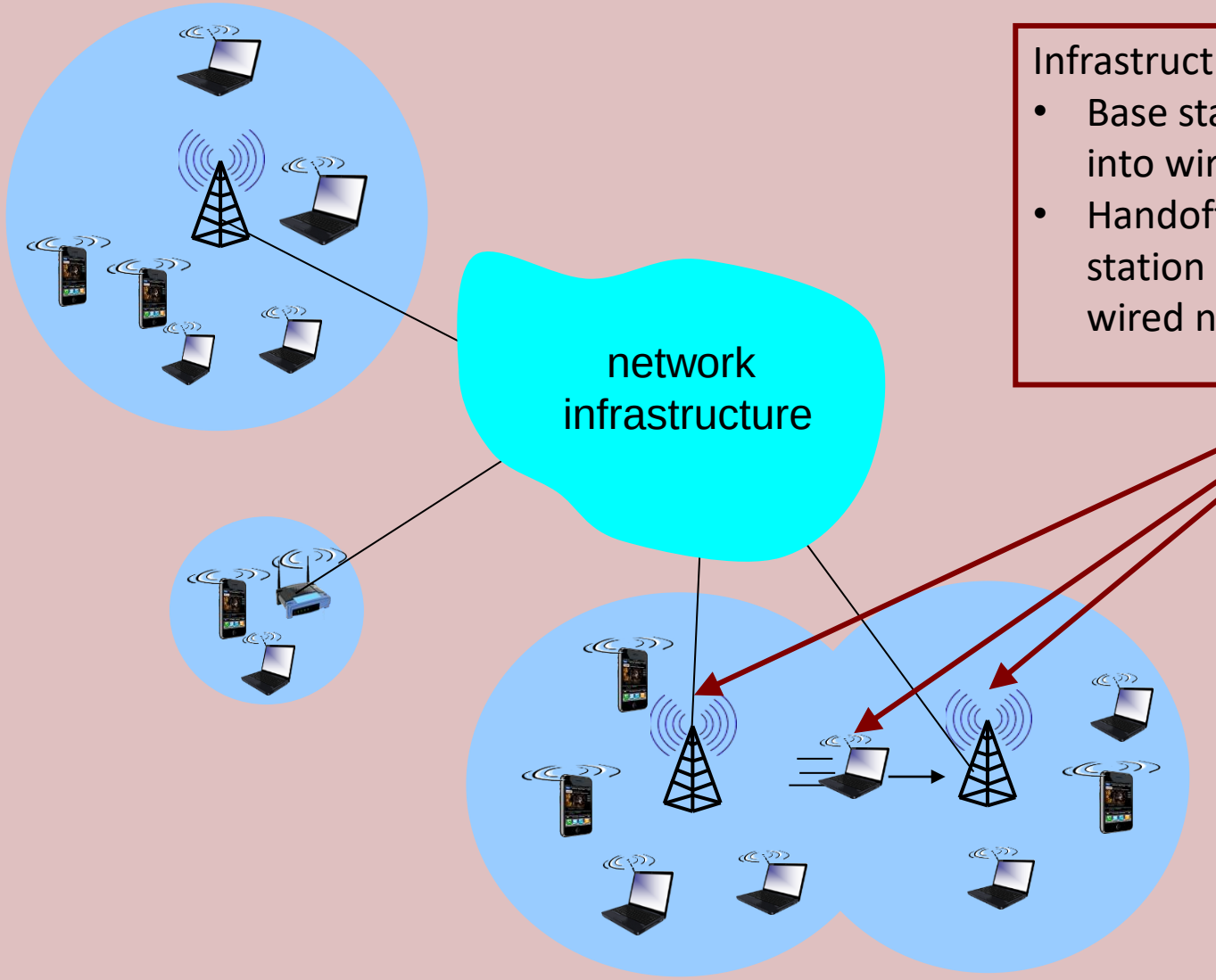
Wireless Network



Wireless Link:

- Typically used to connect mobile(s) to base station
- Multiple access protocol coordinates link access
- Various data rates, transmission distance

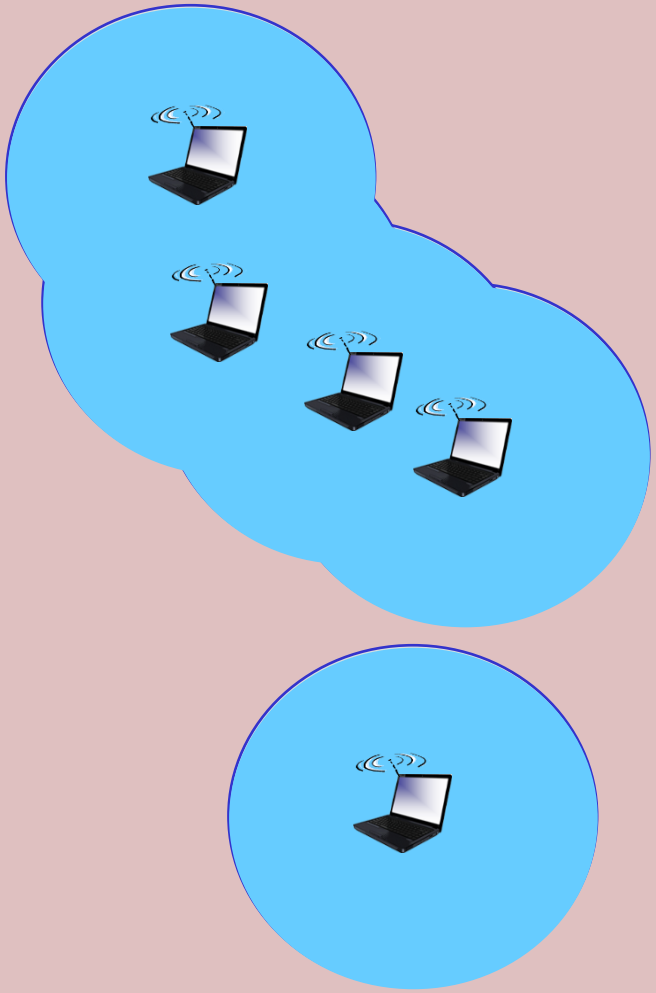
Wireless Network



Infrastructure Mode:

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

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 Characteristics

Protocol	Data Rate	Range
802.15	1 Mbps	Indoor (up to 10 m)
802.11b	11 Mbps	Indoor (up to 30 m)
802.11a,g	54 Mbps	Indoor (up to 30 m)
802.11a,g point-to-point	54 Mbps	Long range (up to 20 km)
802.11n	200 Mbps	Indoor (up to 30 m)
802.11ac	1.3 Gbps	Indoor (up to 30 m)
2G	56 Kbps	Long range (up to 20 km)
3G	4 Mbps	Long range (up to 20 km)
4G	11 Mbps	Long range (up to 20 km)

Directional Antenna

- Enables long range point-to-point wireless transmissions
- Concentrates signal in one intended direction
- Base station could use multiple directional antennae, rather than a single omnidirectional antenna

Wireless Network Taxonomy

	Single Hop	Multiple Hops
Infrastructure (e.g., APs)	Host connects to base station (Wi-Fi, 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

Thank You!

Networks

Wireless Links and Network Characteristics

Adopted from material in “Computer Networking: A Top Down Approach” by Kurose and Ross and slides developed by William Conner

Wireless Links and Network Characteristics

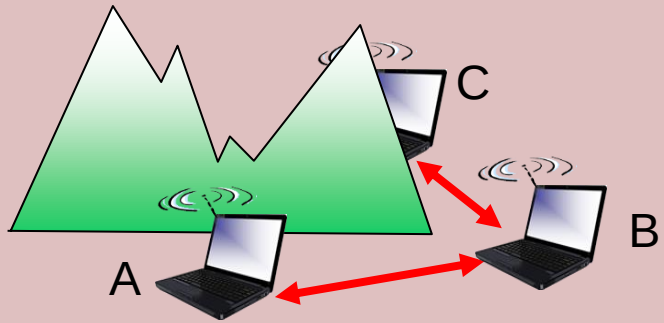
Section 7.2

Wireless Link Challenges

- Decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- Interference from other sources: standardized wireless frequencies shared by other devices
- Multipath propagation: radio signal reflects off of objects and the ground, arriving at the destination at slightly different times

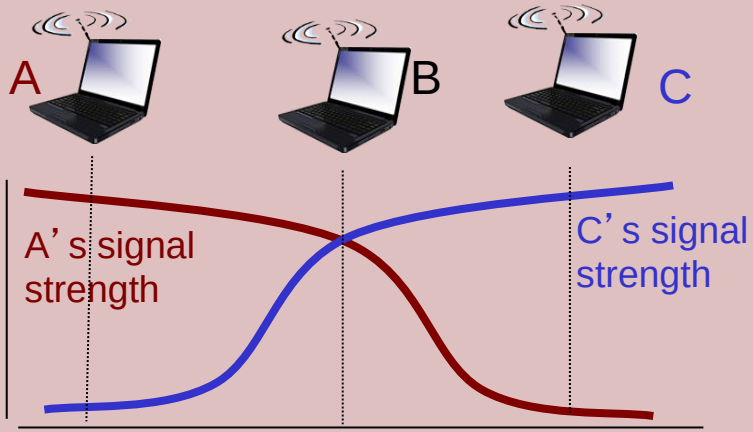
Wireless Network Challenges

Multiple wireless senders and receivers create additional problems (beyond multiple access):



Hidden Terminal Problem

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



Signal Attenuation:

- B, A hear each other
- B, C hear each other
- A, C cannot 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 the same frequency, but each user has their own “chipping” sequence (i.e., code) to encode data
- Allows multiple users to “coexist” and transmit simultaneously with minimal interference (if codes are “orthogonal”)
- Human analogy: conversations at a party are had in different languages; most participants “tune in” and hear the language they are listening for

Code Division Multiple Access (CDMA)

Encoded signal = (original data) x (chipping sequence)

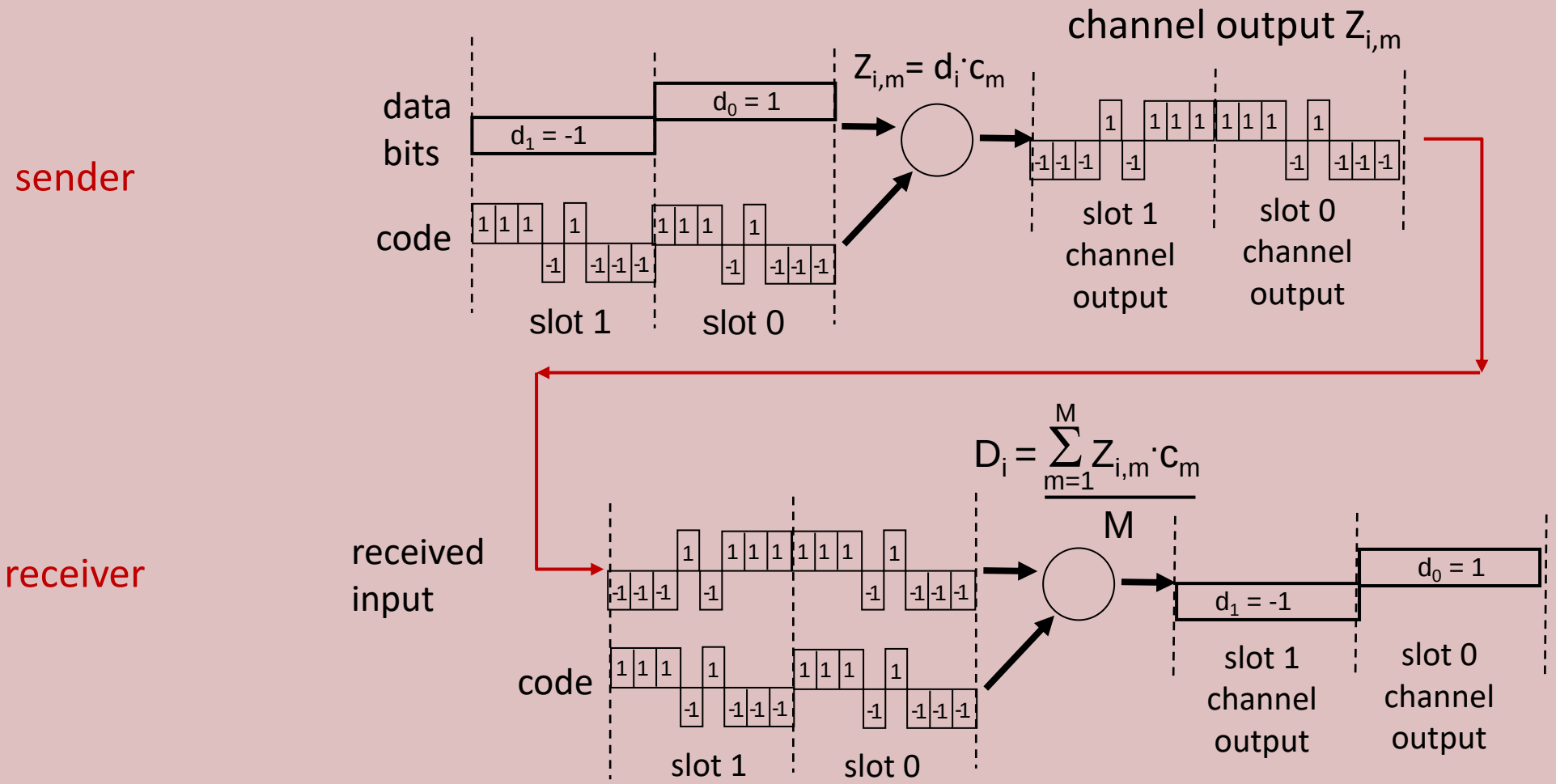
Decoding: normalized inner product of encoded signal and chipping sequence

Bandwidth requirement: increases by a factor equal to the length of the chipping sequence

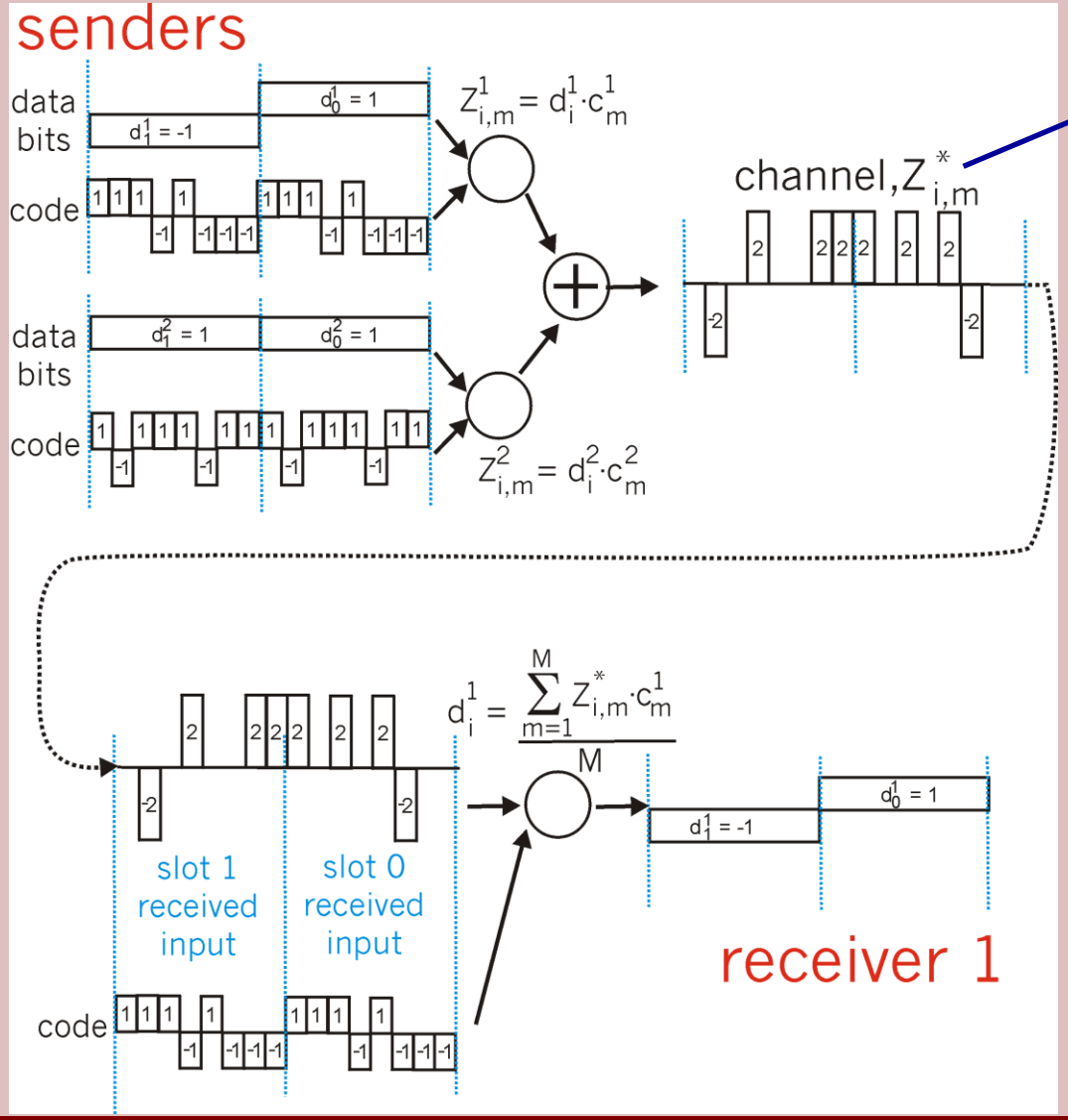
Orthogonal Codes

- Normalized inner product of any two distinct chipping sequences must be zero
- Walsh codes are used to generate orthogonal chipping sequences
- Generation details are beyond the scope of this course (coding theory)

CDMA Encode/Decode



CDMA: Two-Sender Interference



channel sums together transmissions by sender 1 and 2

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

*-Division Multiple Access

- TDMA divides into time slots
- FDMA divides into frequency bands
- What does CDMA divide?

Thank You!

Networks

Wireless LANs

Adopted from material in “Computer Networking: A Top Down Approach” by Kurose and Ross and slides developed by William Conner

Wireless LANs

Section 7.3

IEEE 802.11 Wireless LAN

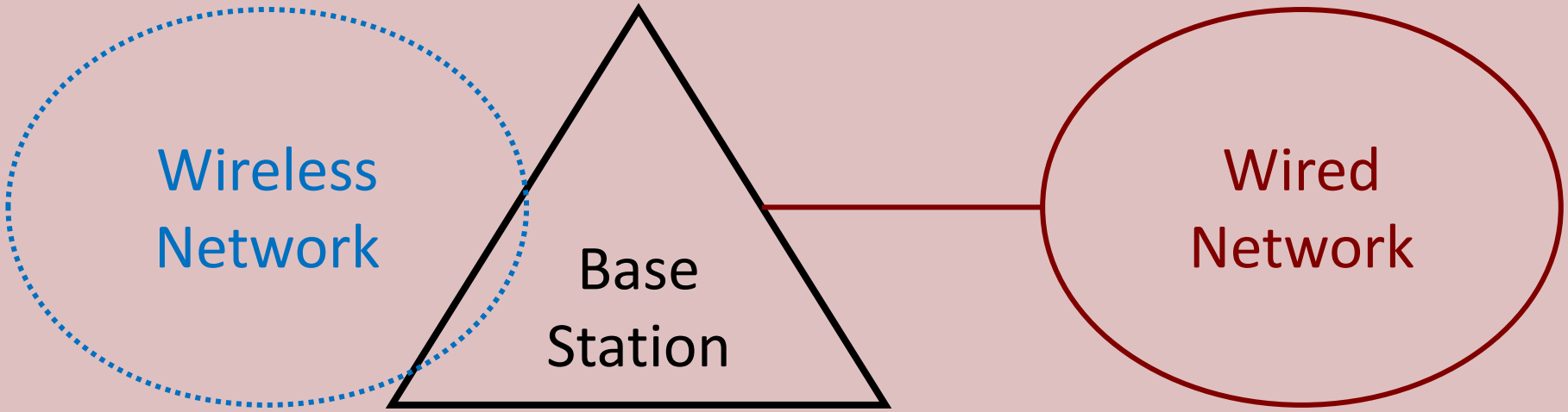
- CSMA/CA for multiple access
- Base station and ad hoc variants

Standard	Rate
802.11a	Up to 54 Mbps
802.11b	Up to 11 Mbps
802.11g	Up to 54 Mbps
802.11n	Up to 200 Mbps

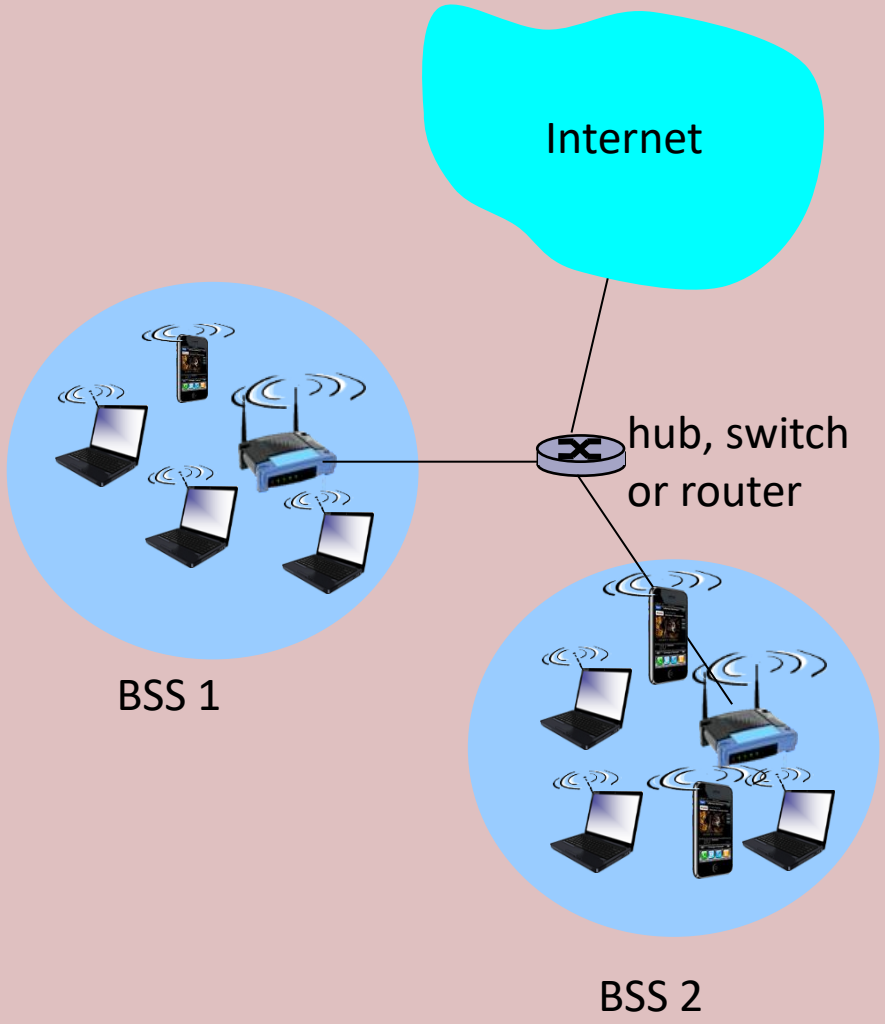
Base Station

- Also referred to as an access point (AP)

- Connects hosts on a wireless network to a wired network (infrastructure mode)



802.11 LAN Architecture



Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:

- Wireless hosts
- Base station
- Hosts communicate with base station

Ad hoc mode: hosts only

802.11: Channels, Association

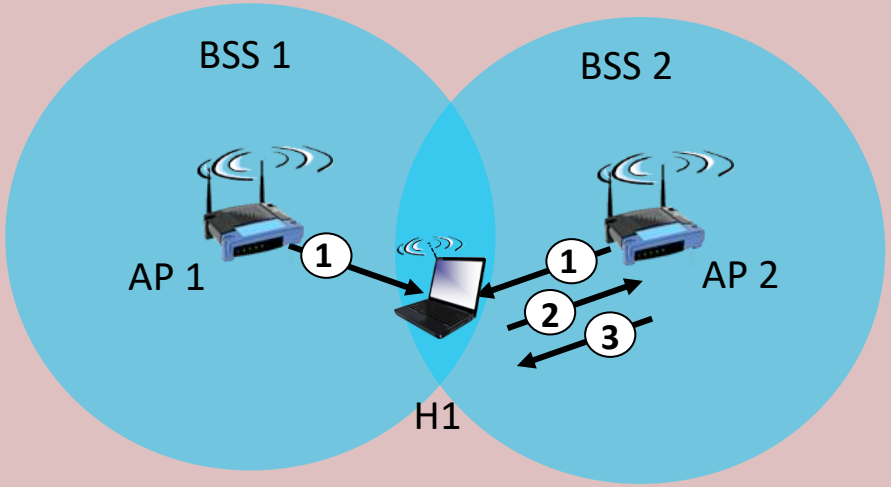
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - Admin chooses frequency for AP
  - Interference possible: channel can be same as that chosen by neighboring AP!

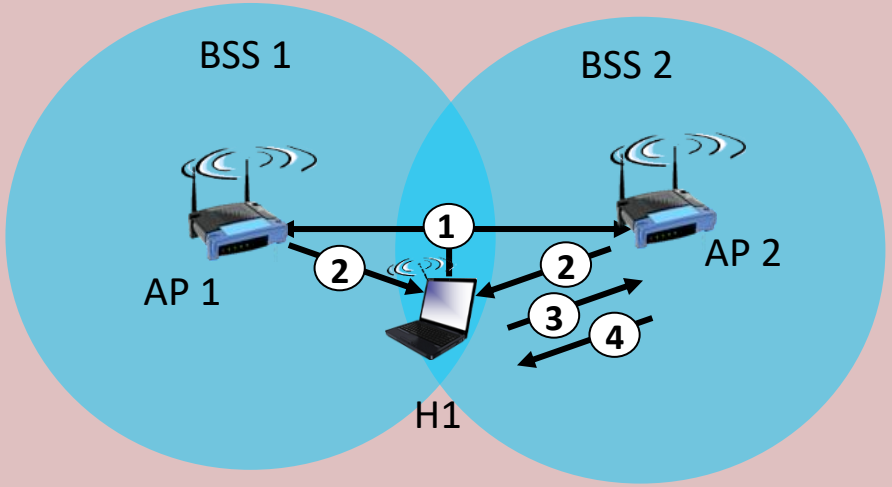
Optimal channel assignment if you have three APs?

(Hint: channels must be at least 4 apart)

- 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 send from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent from selected AP to H1

Review: CSMA

- Listen before transmit
- If channel sensed idle, transmit entire frame
- If channel sensed busy, defer transmission

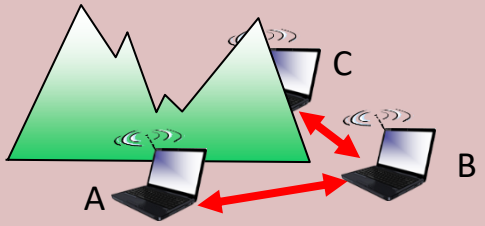
Review: CSMA/CD

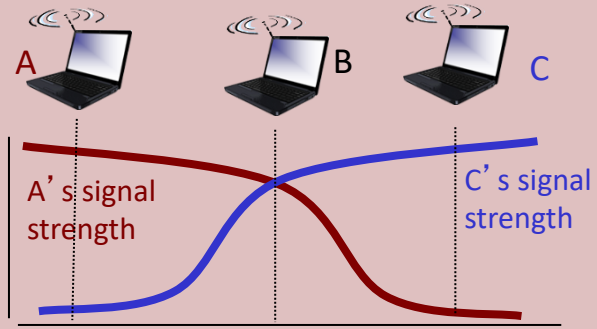
- Carrier sensing, deferral as in CSMA
  - Collisions *detected* within short time
  - Colliding transmissions aborted, reducing channel wastage

- 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

802.11: Multiple Access

- Avoid collisions: 2+ nodes transmitting at the same time
- 802.11: CSMA – sense before transmitting
  - Don't collide with ongoing transmission by another 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)





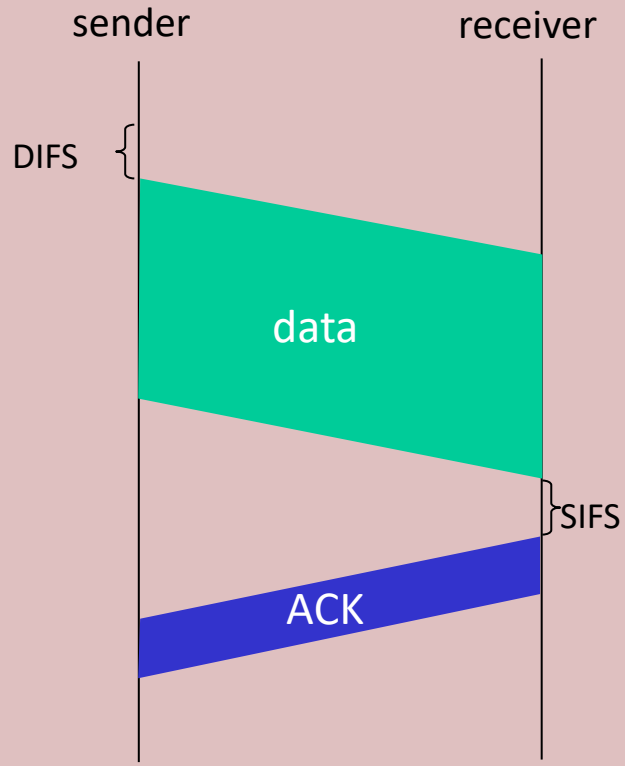
802.11: CSMA/CA

802.11 Sender

1. If sense channel idle for **DIFS** then
   transmit entire frame (no CD)
2. If sense channel busy then
   start random backoff timer
   timer counts down while channel idle
   transmit when timer expires
   if no ACK, increase random backoff interval, repeat 2

802.11 Receiver

1. If frame received OK
   return ACK after SIFS



Why does 802.11 use ACK (802.3 did not use ACK)?

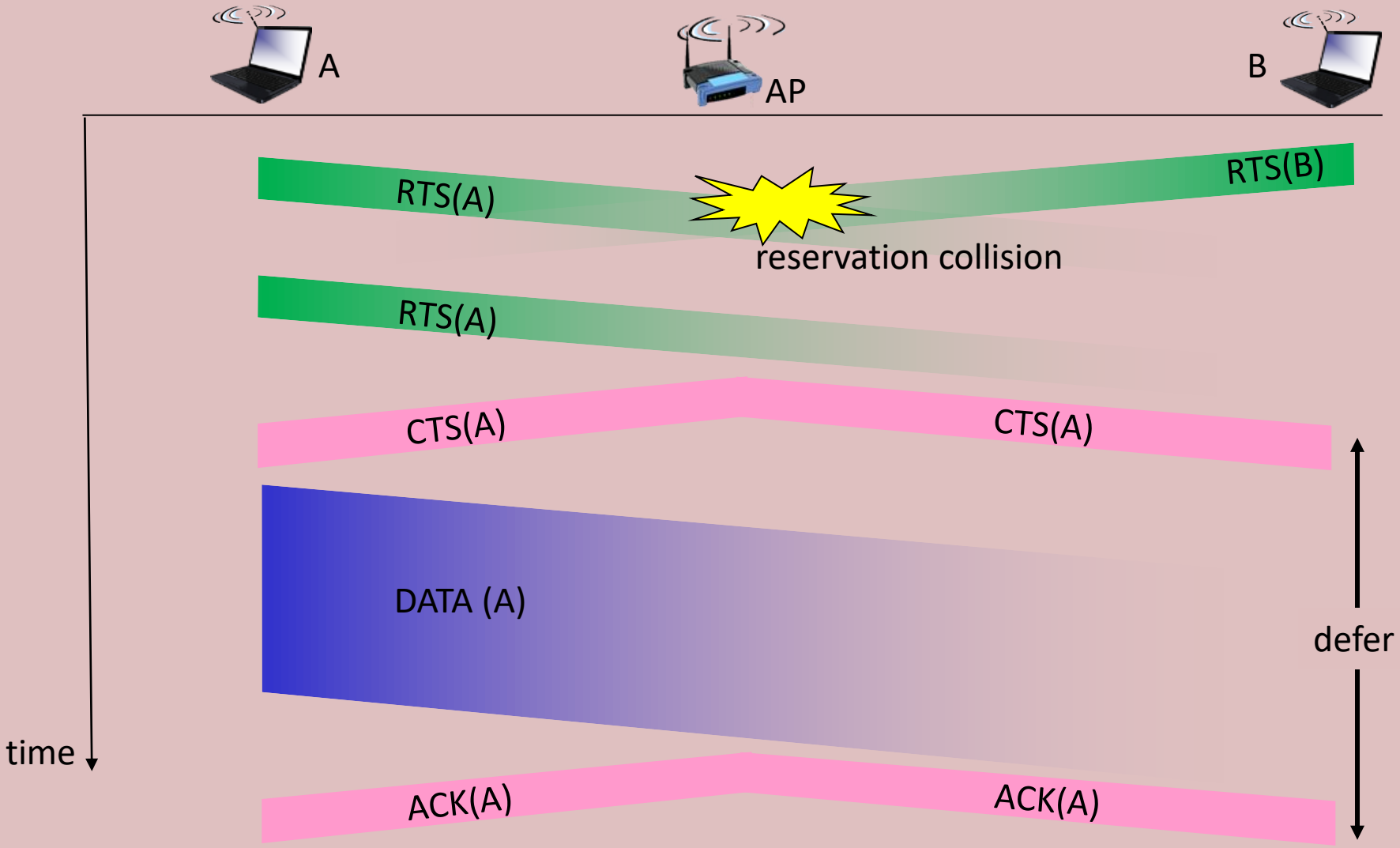
DIFS and SIFS

- Distributed Interframe Spacing (DIFS): duration that channel must be continuously idle prior to transmitting a DATA frame or reserving the channel
- Short Interframe Spacing (SIFS): duration to process received frame and send response
- SIFS < DIFS, so responses to received frames have priority over new transmissions

Collision Avoidance

- Sender reserves channel with small frame before sending large frame
- Sends small request-to-send (RTS) to base station (small frame could collide)
- Base station replies with clear-to-send (CTS) heard by all nodes
- Sender can now send large DATA frame (large frame should not collide)

Collision Avoidance



NOTE: DIFS and SIFS not shown above

802.11 Frame

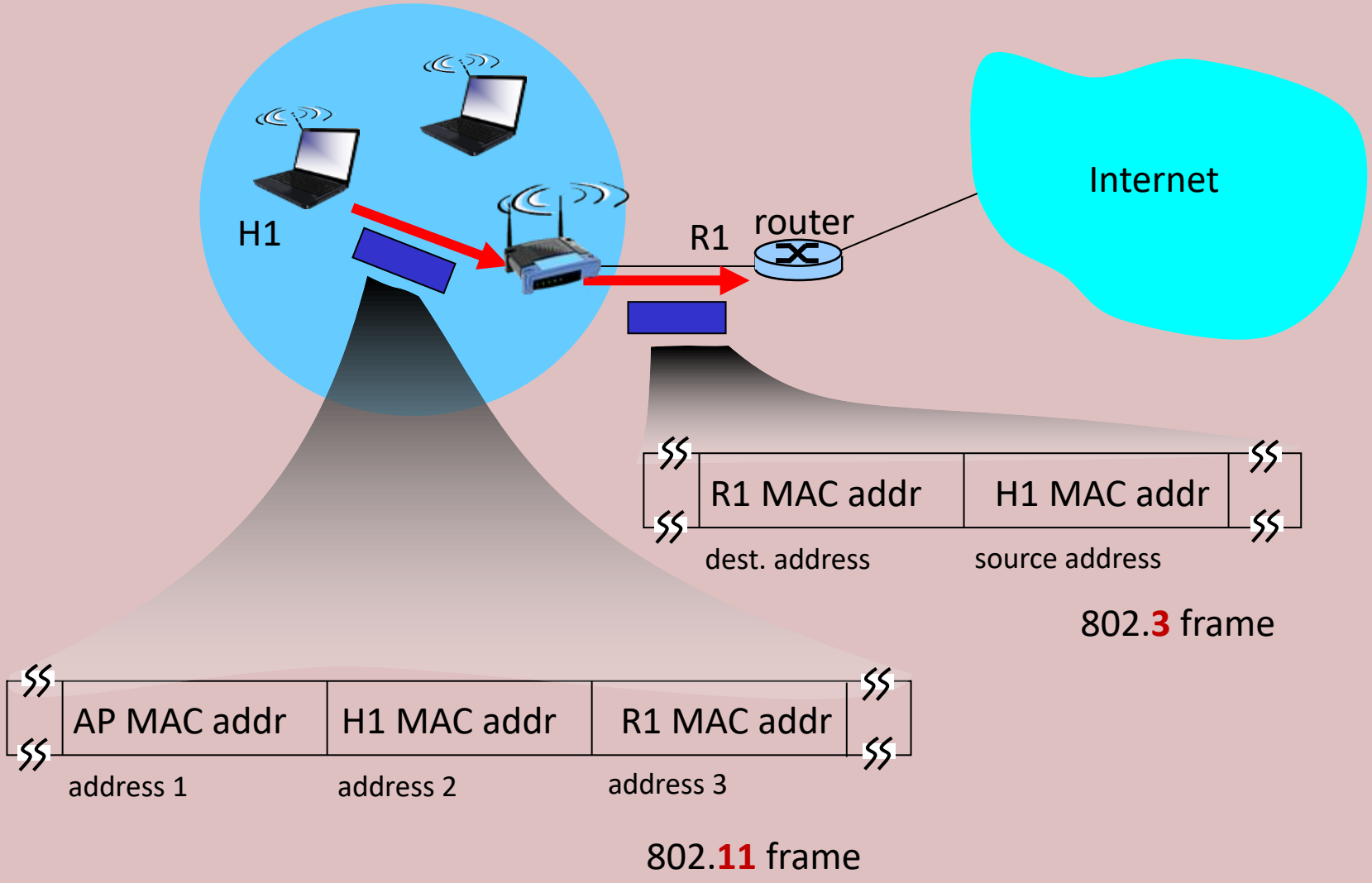
Address 1: MAC address of wireless host or AP to receive this frame

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

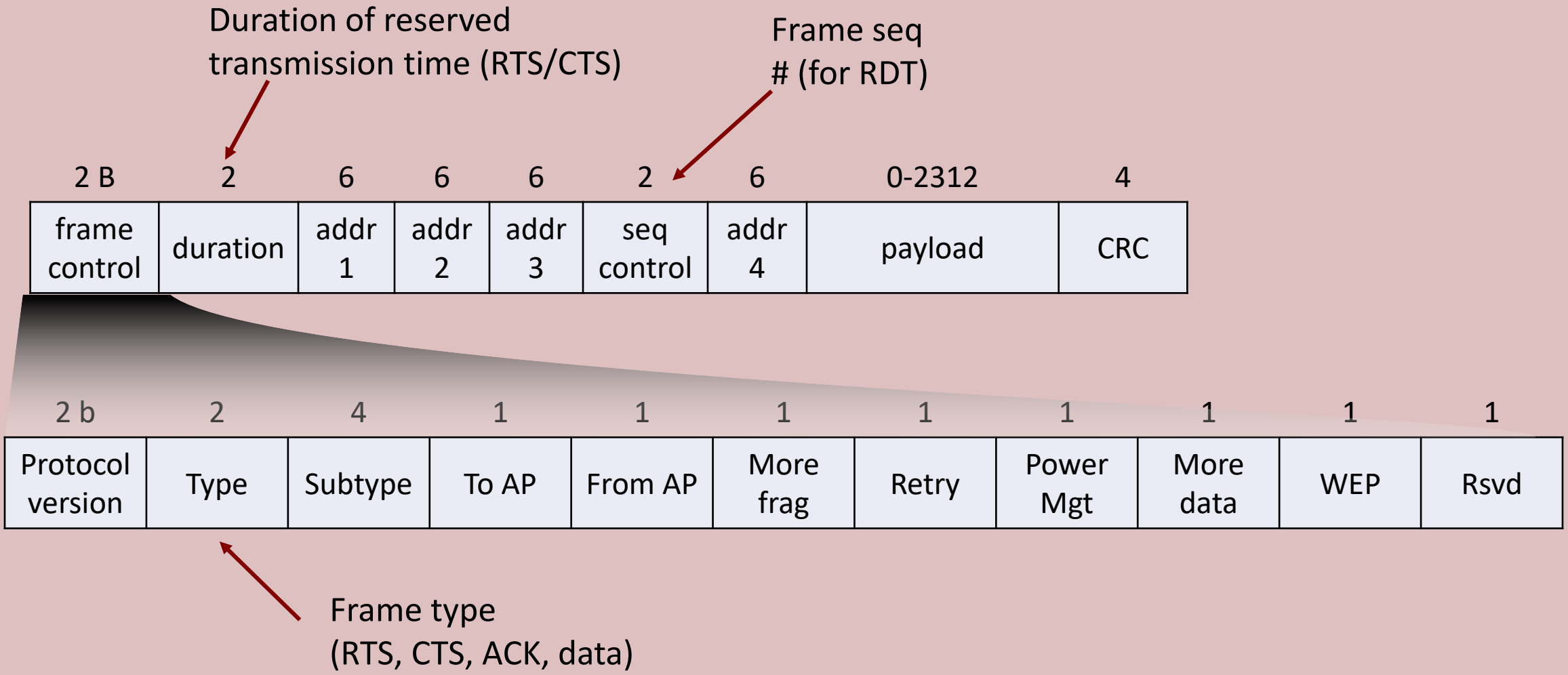
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 Frame

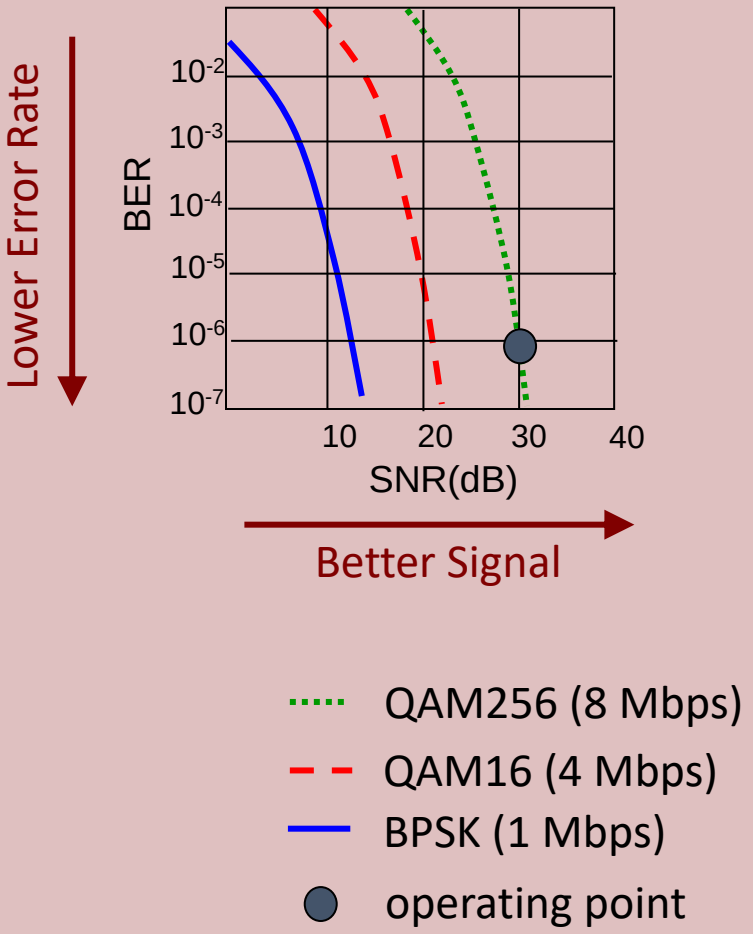

H1
R1
router
Internet
R1 MAC addr
H1 MAC addr
dest. address
source address
802.3 frame
AP MAC addr
H1 MAC addr
R1 MAC addr
address 1
address 2
address 3
802.11 frame

802.11 Frame


Duration of reserved transmission time (RTS/CTS)
Frame seq # (for RDT)
2 B
2
6
6
6
2
6
0-2312
4
frame control
duration
addr 1
addr 2
addr 3
seq control
addr 4
payload
CRC
2 b
2
4
1
1
1
1
1
1
1
1
Protocol version
Type
Subtype
To AP
From AP
More frag
Retry
Power Mgt
More data
WEP
Rsvd
Frame type (RTS, CTS, ACK, data)

802.11 Rate Adaptation

- Base station, mobile, dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies



1. SNR decreases, BER increases as node moves away from base station
2. When BER becomes too high, switch to lower transmission rate but lower BER

802.11 Power Management

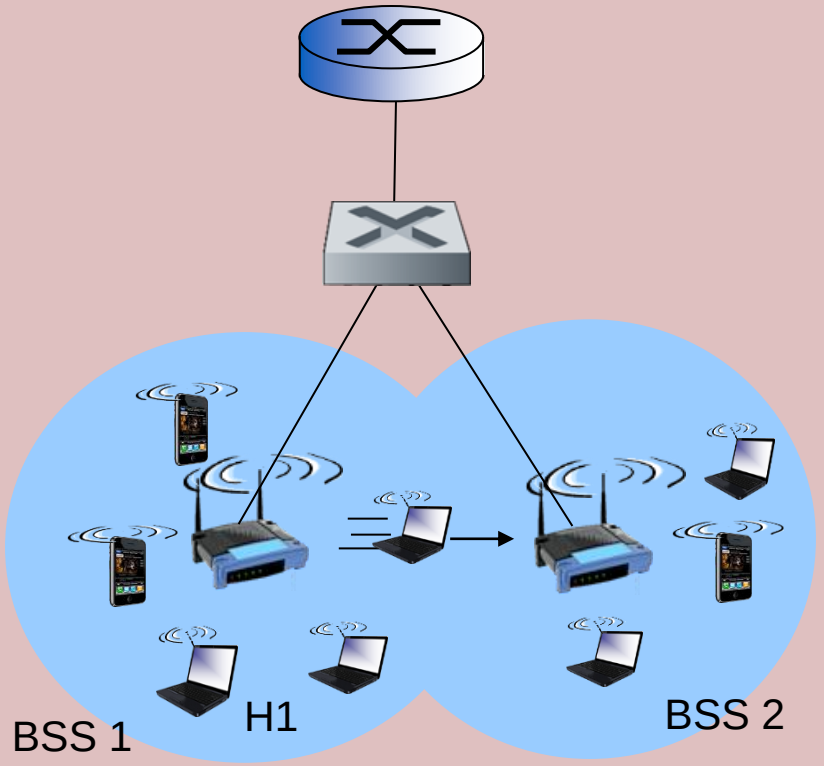
- Node-to-AP: “I am going to sleep until next beacon frame”
  - AP knows not to transmit frames to this node
  - Node wakes up before next beacon frame

- 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

802.11 Mobility

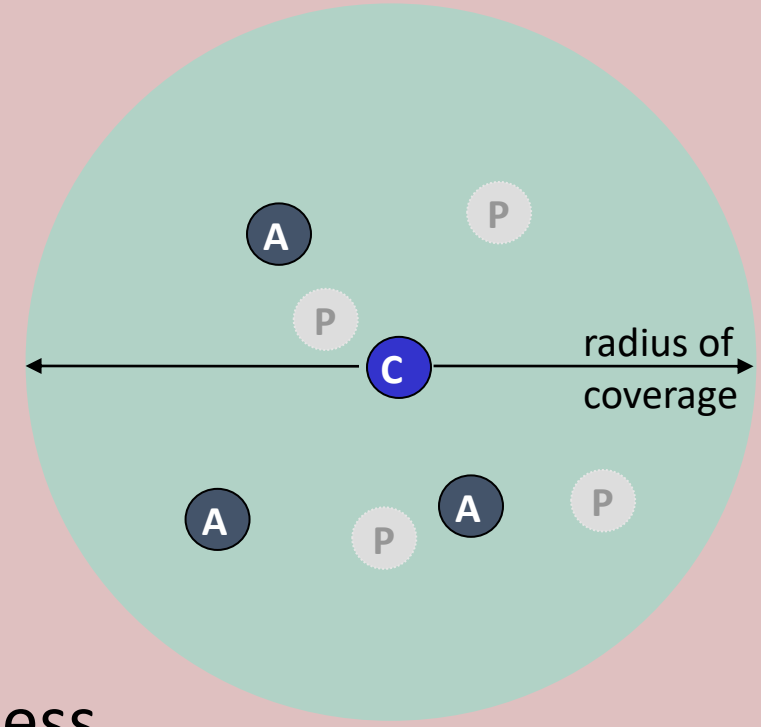
- H1 remains in same IP subnet: IP address can remain the same

- 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



802.15 Personal Area Network

- Less than 10m diameter
- Replacement for cables (mouse, keyboard, headphones)
- Ad hoc: no infrastructure
- Coordinated access, rather than random access
- 802.15 evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - Up to 721 kbps



Thank You!

Networks

Cellular Internet

Adopted from material in “Computer Networking: A Top Down Approach” by Kurose and Ross and slides developed by William Conner

Cellular Internet

Section 7.4

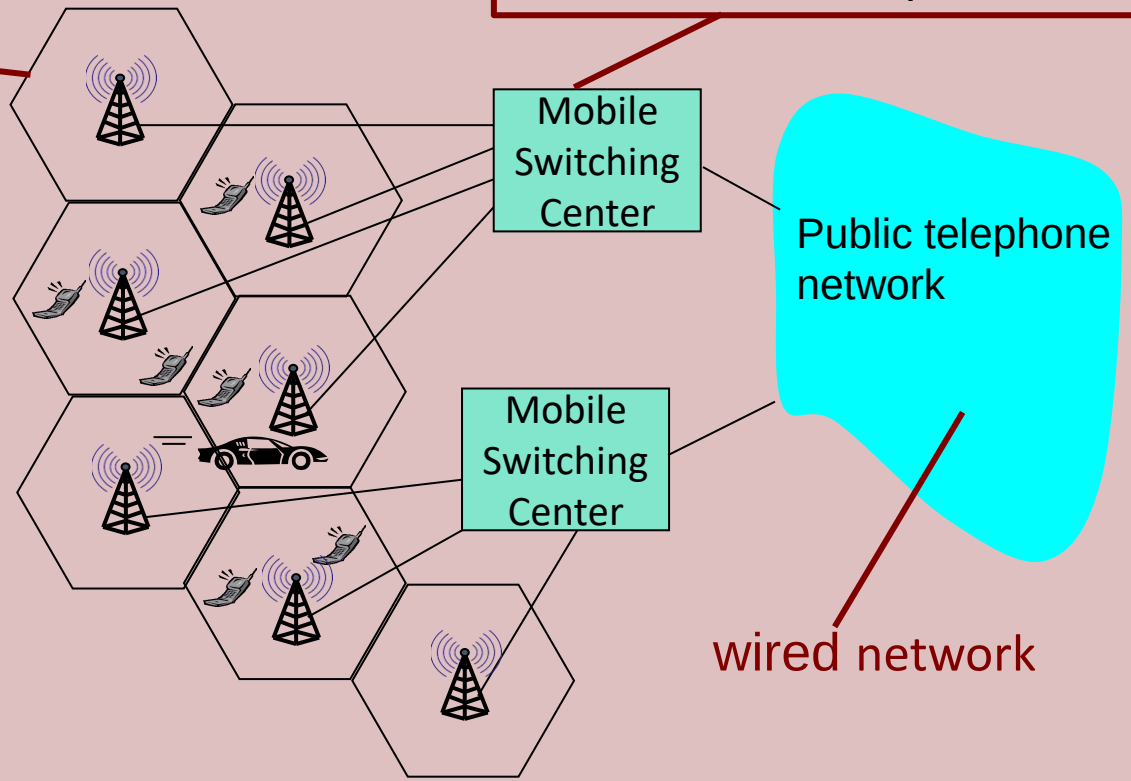
Mobile Phone Networks

MSC:

- Connects cells to wired telephone network
- Manages call setup
- Handles mobility

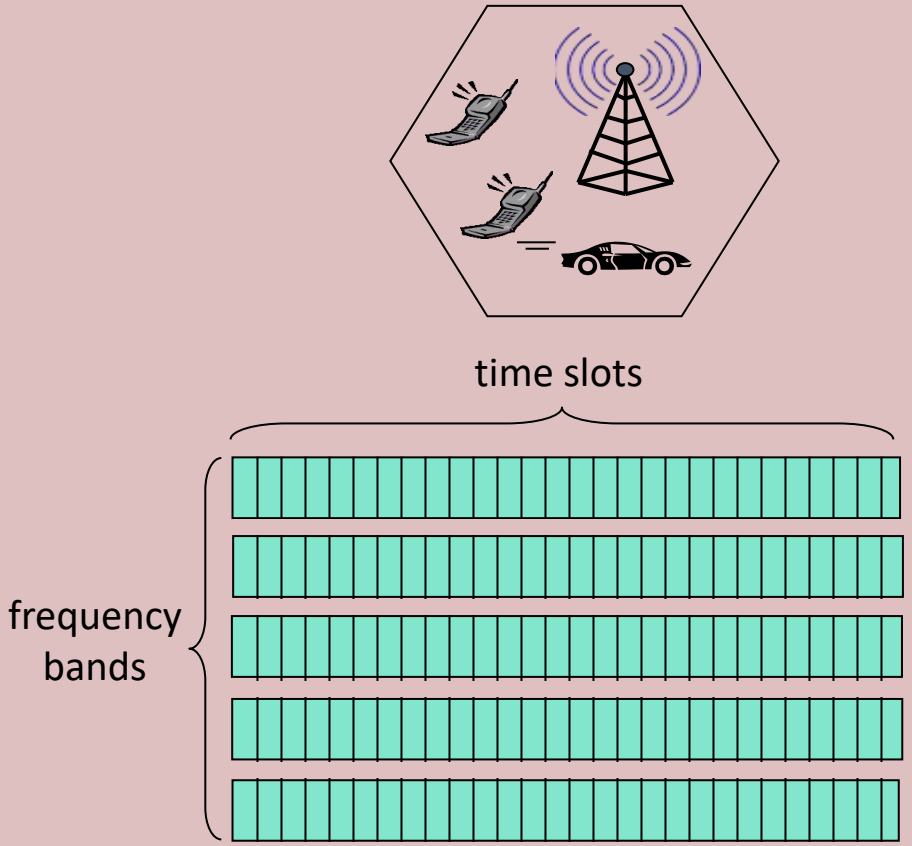
Cell:

- Covers geographical region
- Base station (BS) analogous to 802.11 AP
- Mobile users attach to network through BS
- Air-interface: physical and link layer protocol between mobile and BS



Cellular Network Multiple Access

- Two protocols used for multiple access:
  - CDMA: code division multiple access (3G and later)
  - Combined TDMA/FDMA: divide channel into frequency bands *and* time slots (2G)



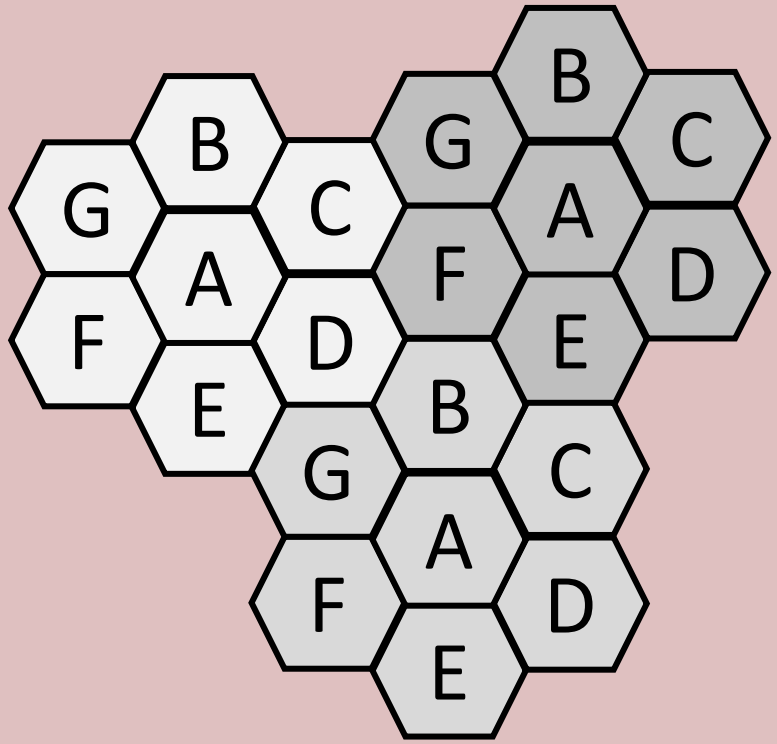
Pre-1G Networks

- Deployed in several cities in the 1950s
- Large transmitter on top of tall building with single channel for sending and receiving
- Push-to-talk system: push button to enable sending and disable receiving
- Used by CB radios, taxis, and police vehicles

1G (Analog Voice) Networks

- Advanced Mobile Phone System (AMPS): invented by Bell Labs and deployed in 1982
- Cells were 10-20 km in diameter and could support up to 100 full duplex calls
- Adjacent cells could not reuse same frequencies
- FDMA used to separate channels

Frequency Reuse



Assume that frequencies do not overlap for distinct letters

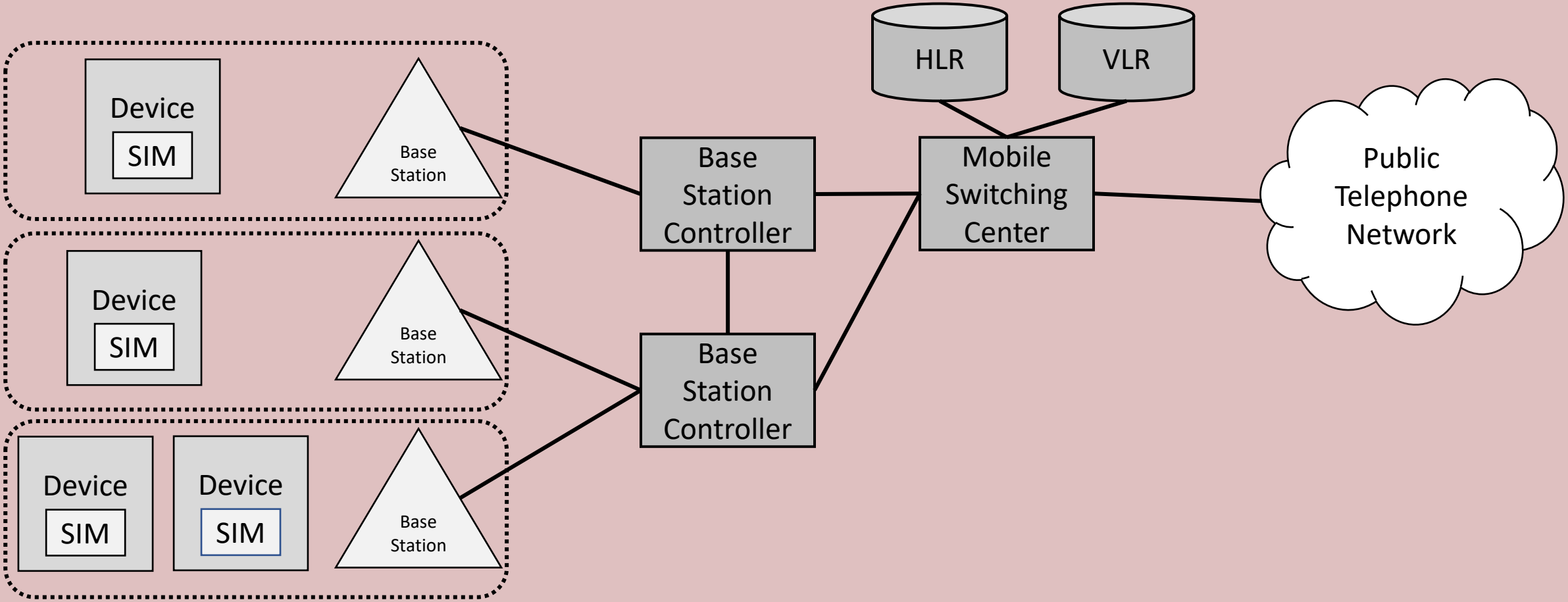
2G (Digital Voice) Networks

- Switched from analog to digital, which enabled compression and encryption
- Global System for Mobile Communications (GSM): developed in Europe in the 1980s and deployed in 1991
- Subscriber Identity Module (SIM) card: removable chip with subscriber and account information

2G (Digital Voice) Networks

- Public Switched Telephone Network (PSTN): traditional phone network
- Base Station Controller (BSC): manages cell, including handoffs
- Mobile Switching Controller (MSC): connect base stations to PSTN
- Home Location Register (HLR): database of last-known location for each device; used to route calls
- Visitor Location Register (VLR): database of mobiles associated with cells managed by an MSC

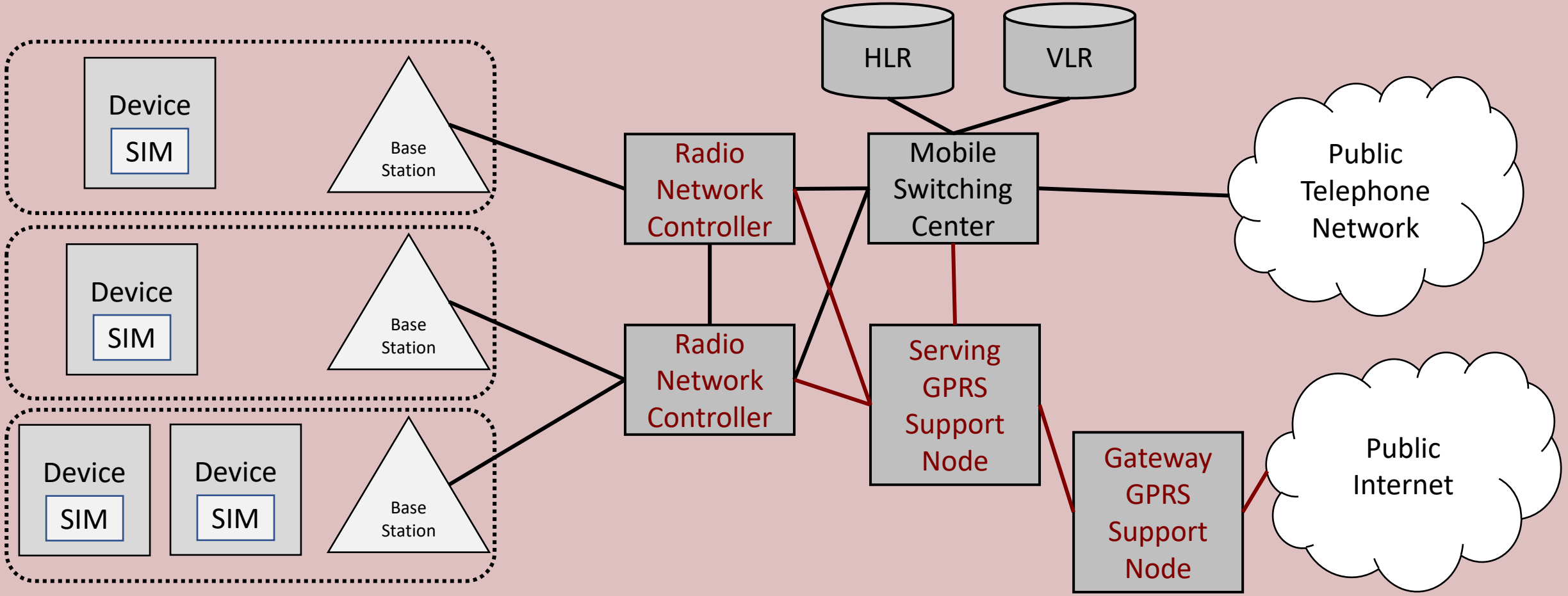
2G (Digital Voice) Networks



3G (Voice + Data) Networks

- Network targeted for smart phones
- Radio network connected to two separate networks
  - 2G network infrastructure for voice
  - New network infrastructure for data
- Introduction of CDMA

3G (Voice + Data) Networks



New cellular network operates *in parallel* with existing (unchanged) cellular voice network

4G LTE Networks

- Long term evolution (LTE)
- Higher bandwidth for richer smartphone applications
- Single IP core network for voice and data between base stations and gateway MSC (i.e., no longer using separate paths for voice and data)

Thank You!

Networks

Mobility Principles

Adopted from material in “Computer Networking: A Top Down Approach” by Kurose and Ross and slides developed by William Conner

Mobility Principles

Section 7.5

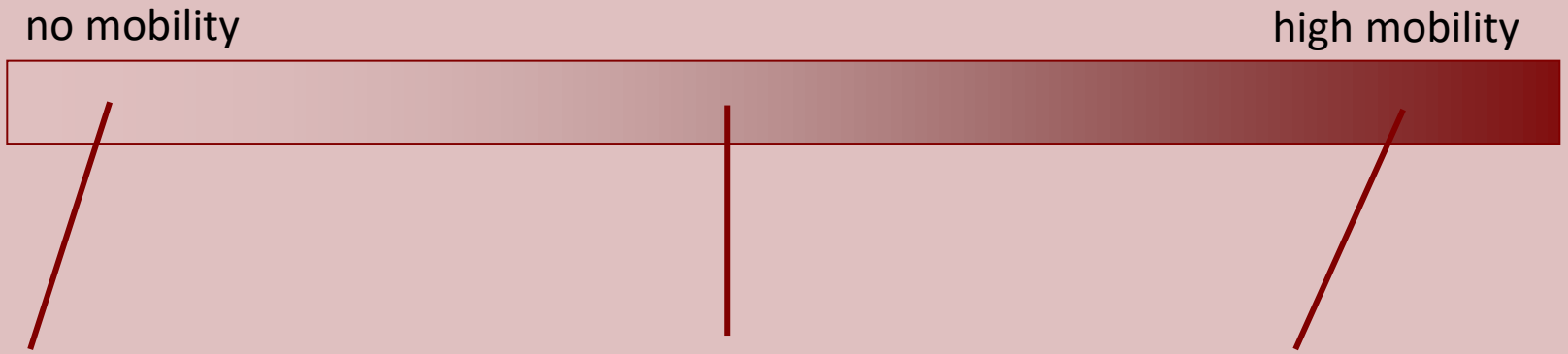
Wireless vs. Mobile

- Wireless: communication over wireless link (e.g., cellular networks, 802.11)
  - Unguided media
  - “Through the air”

- Mobility: handling the mobile user who changes point of attachment to network

- Wireless and mobility are related, but also cover distinct concepts (why?)

Mobility Spectrum



(im)mobile wireless user, using same access point

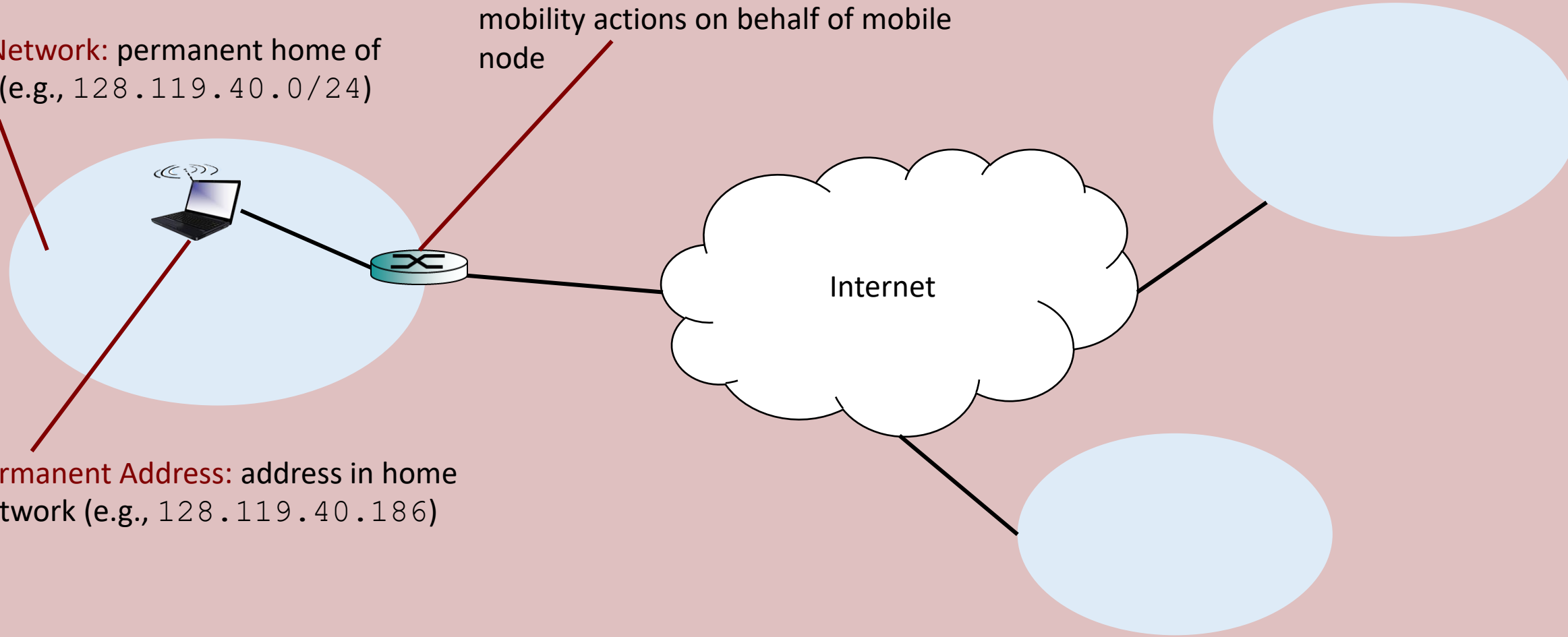
mobile user, connecting/ disconnecting from network using DHCP

mobile user, passing through multiple access points while maintaining ongoing connections (like cell phone)

Mobile Terminology

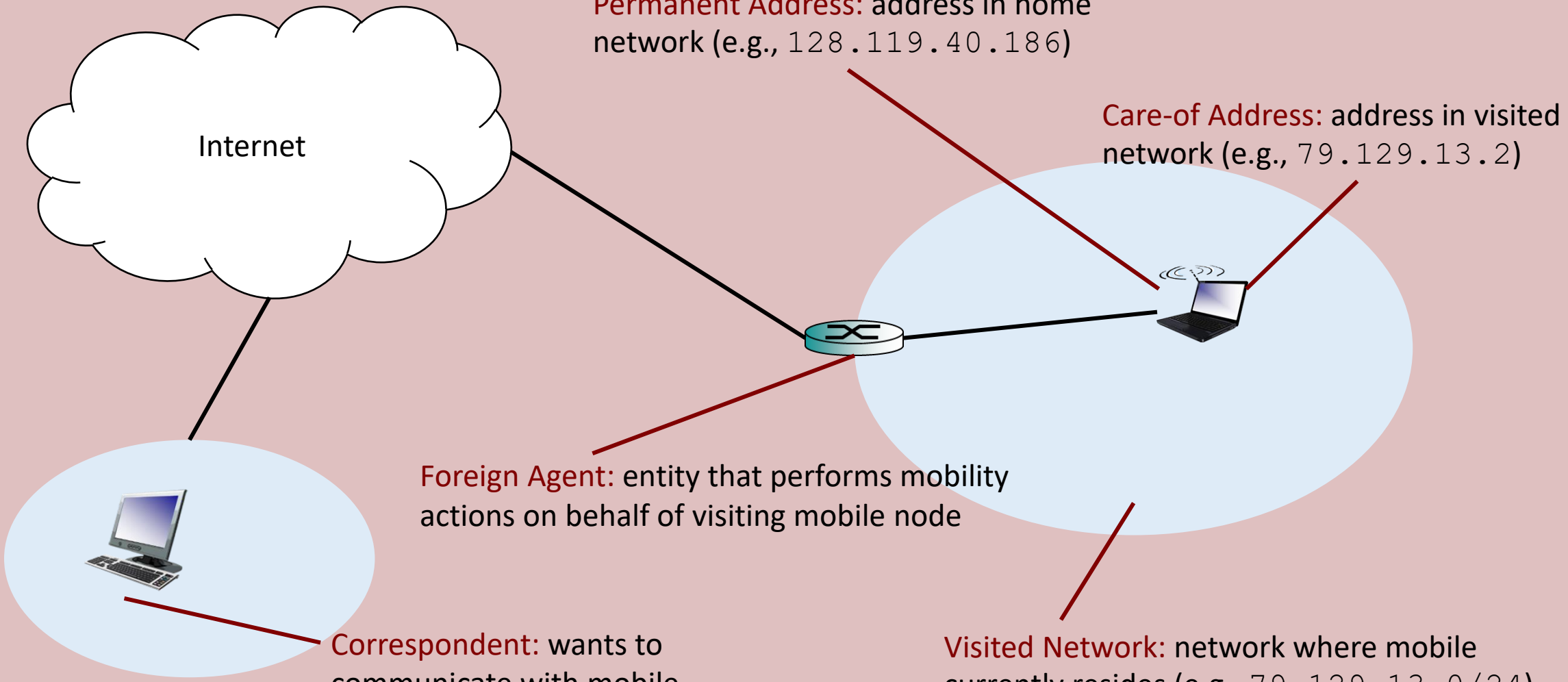
Home Agent: entity that performs mobility actions on behalf of mobile node

Home Network: permanent home of mobile (e.g., `128.119.40.0/24`)



Permanent Address: address in home network (e.g., `128.119.40.186`)

Mobile Terminology



Care-of Address (CoA)

- Foreign agent CoA: IP address of foreign agent
  - Same CoA reused for all visitors in network
  - Packets forwarded via foreign agent

- Co-located CoA: IP address of visitor
  - Individual CoA assigned to each visitor
  - Packets directly forwarded to visitor
  - Foreign agent or DHCP can assign CoA

Real-Life Mobility

Consider your friend who frequently changes addresses; how do you find her?

- Search all phone books?
- Call her parents?
- Expect her to let you know where he/she is?
- Facebook!

Approaches to Mobility

- *Let routing handle it:* routers advertise permanent addresses of mobile-nodes-in-residence via usual routing table exchange
  - Routing tables indicate where each mobile is located
  - No changes to end-systems

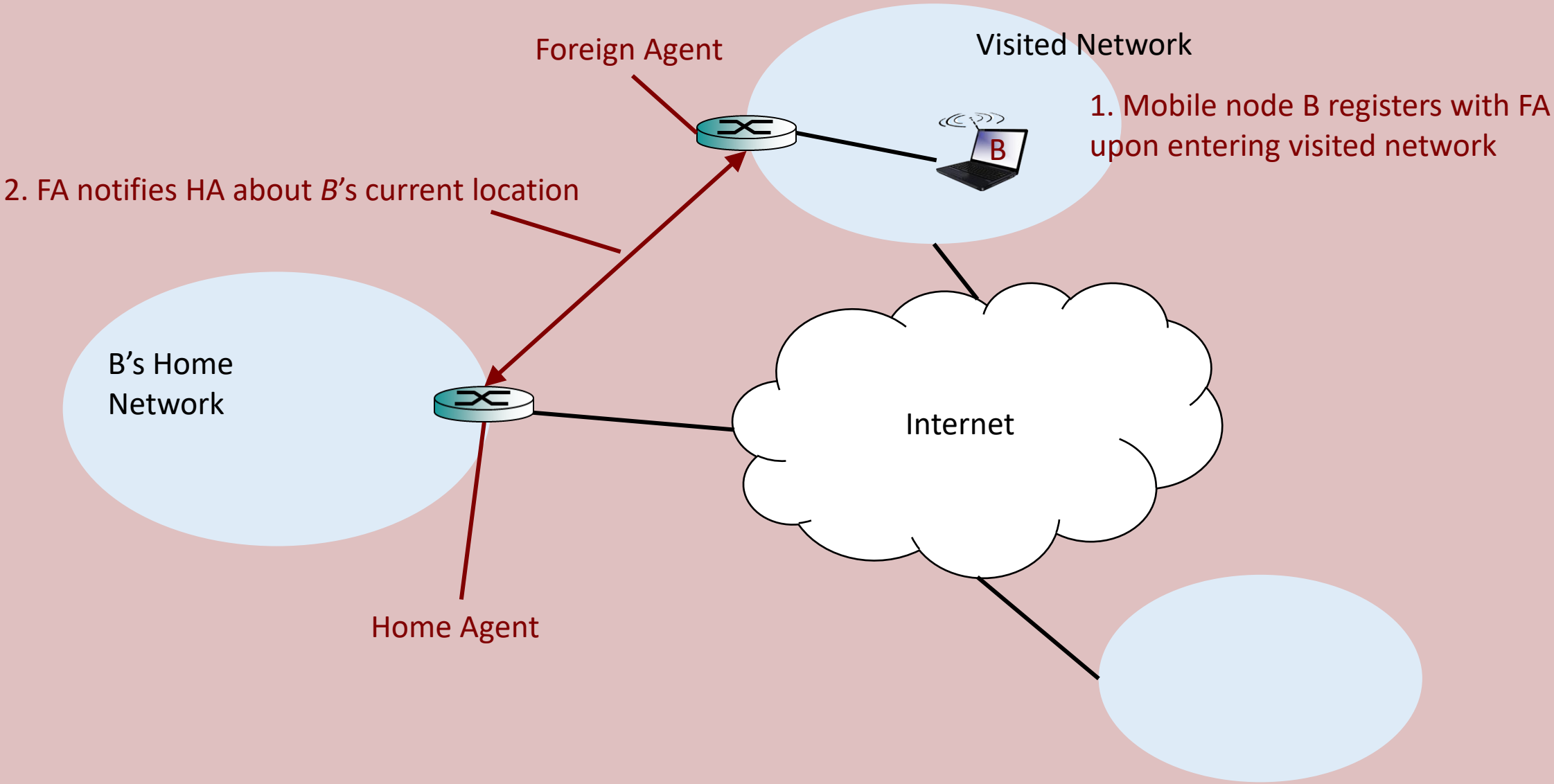
- *Let end-systems handle it:*
  - *Indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *Direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

Approaches to Mobility

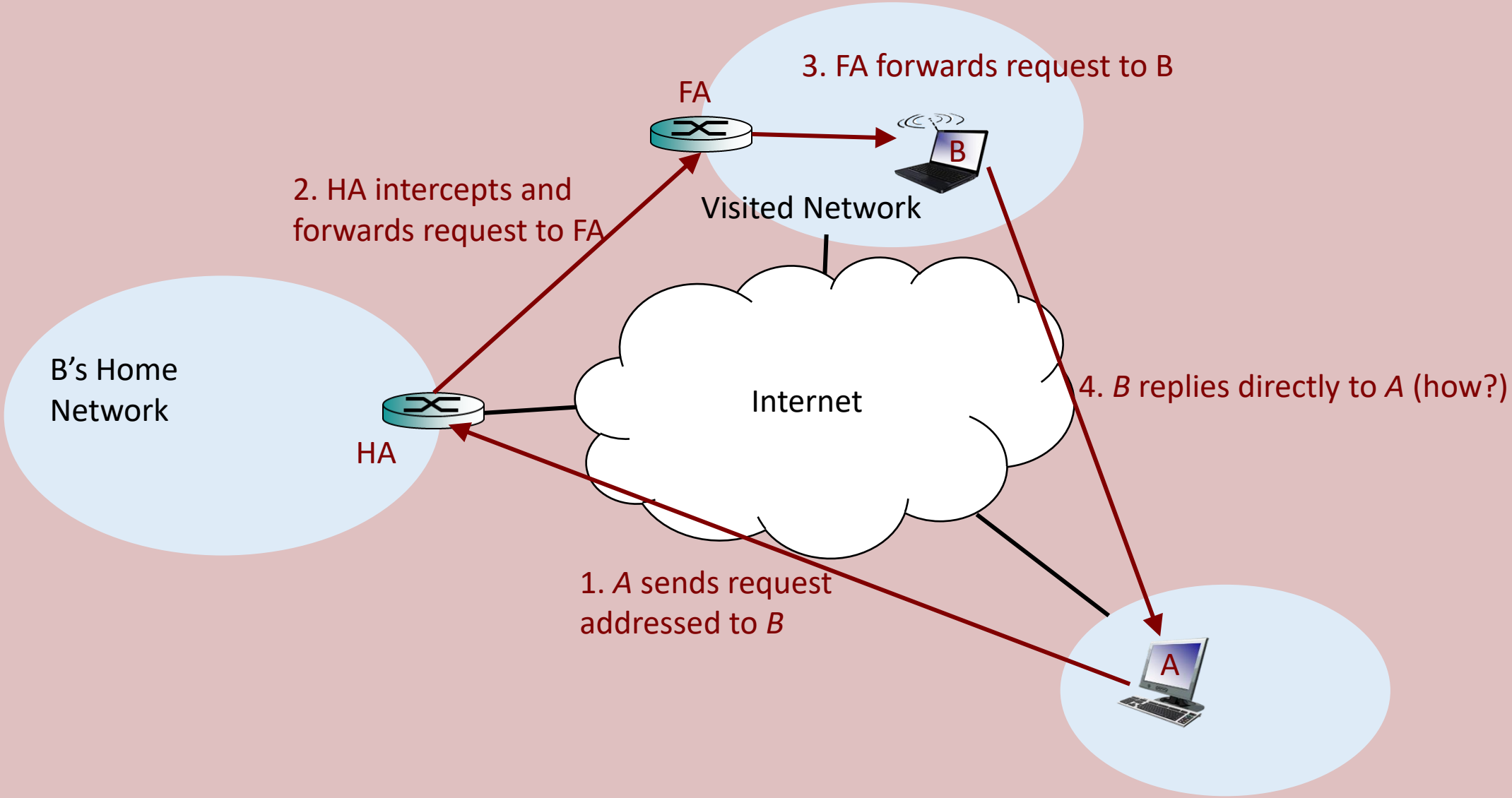
- *Let routing handle it:* rou rtise permanent addresses of mobile-nodes-in-reside routing table exchange
  - Routing tables indicate obile is located
  - No changes to end-syste

- *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 Registration



Indirect Mobile Routing



Gratuitous ARP

- Method for quickly updating ARP mappings as mobile station comes and goes from home network
- Home agent (or mobile node) *sends itself* an ARP query that it answers to update IP-to-MAC mapping
- Enables (or disables) interception by home agent

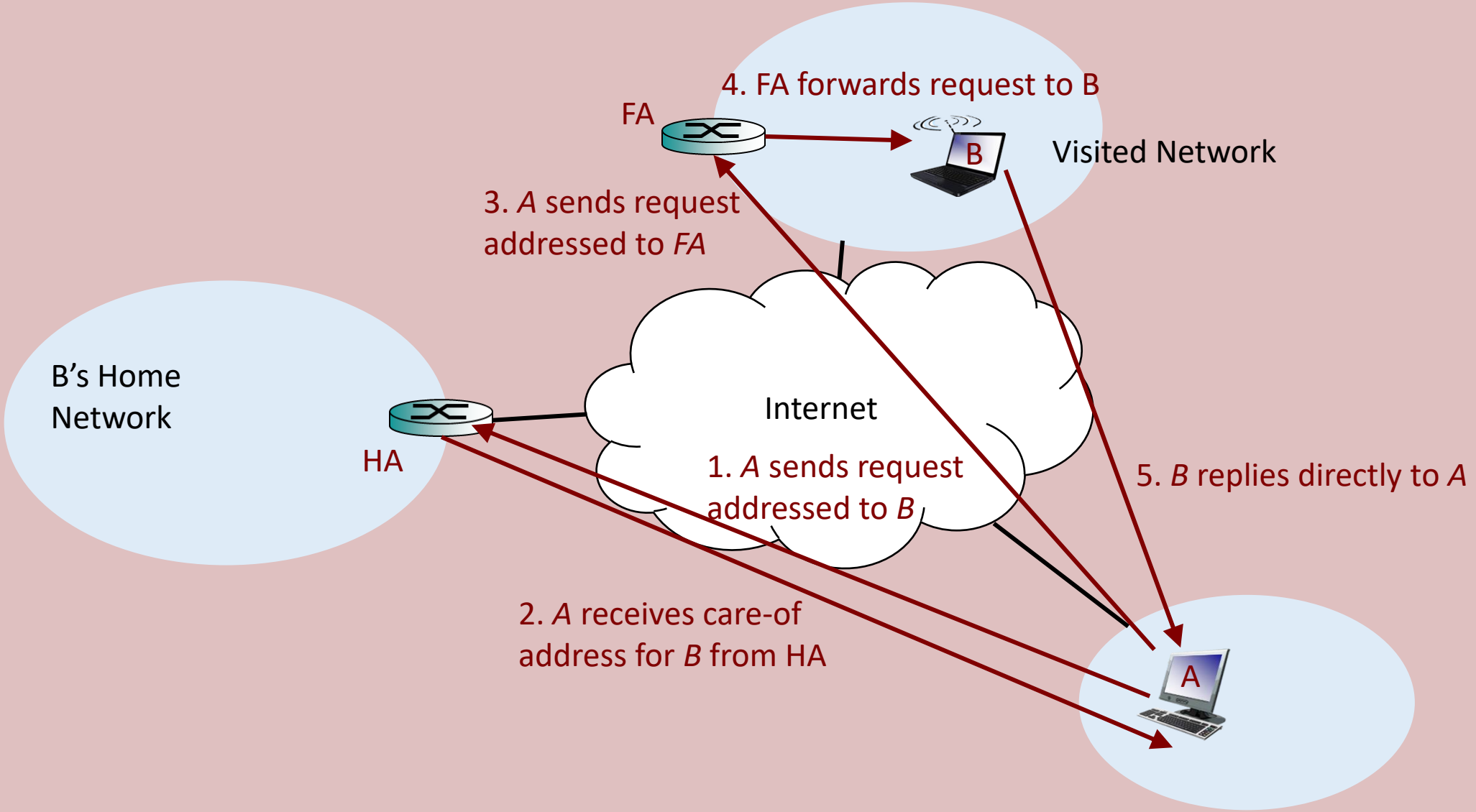
Indirect Mobile Routing

- Correspondent sends message to permanent address
- Home agent forwards to care-of address
- Mobile node can act as its own foreign agent (if necessary)
- Triangle routing: very inefficient if correspondent and mobile node are in the same network

Indirect Mobile Routing

- Mobile node registers with new foreign agent upon visiting new network
- Foreign agent notifies home agent and home agent updates care-of address
- Packets continue to be forwarded to mobile node without breaking connection (changing networks is transparent)

Direct Mobile Routing

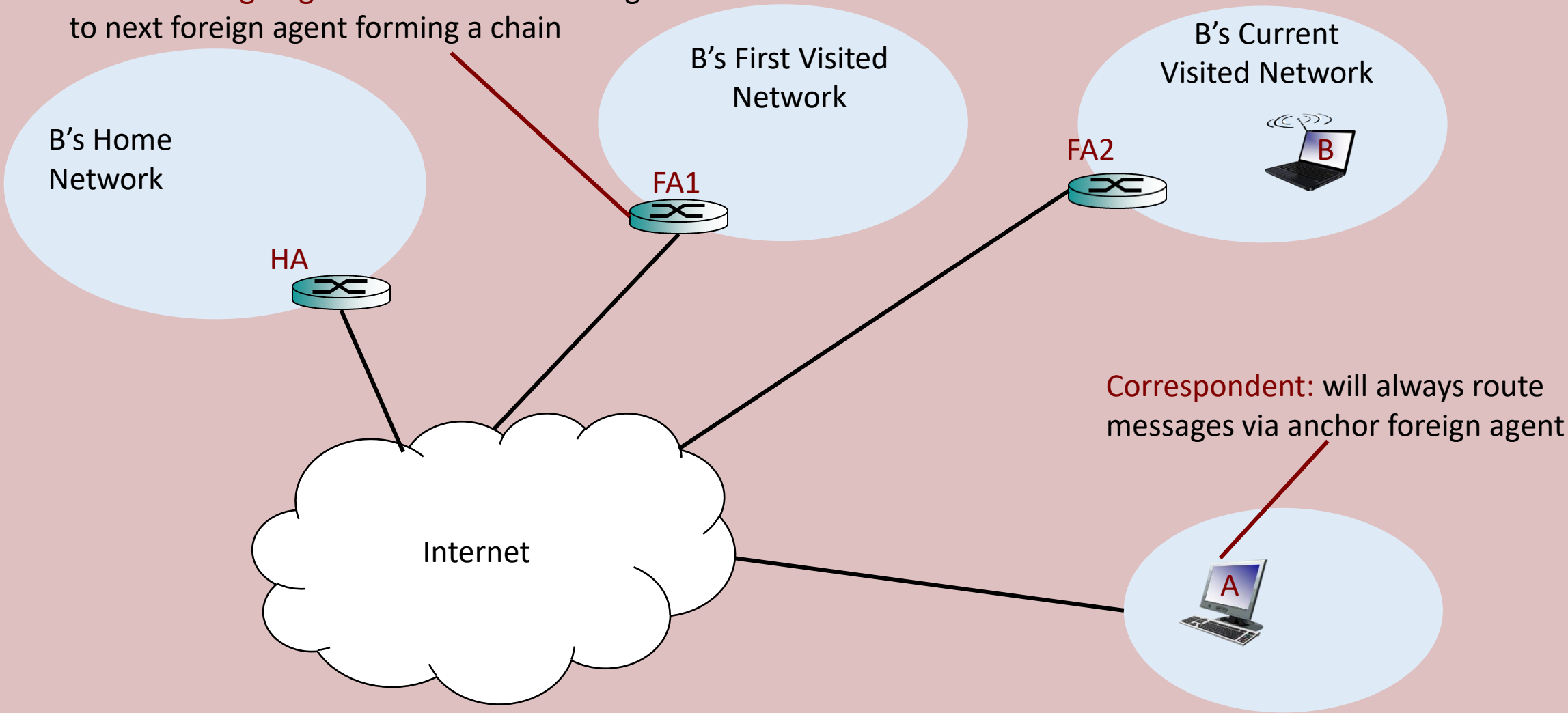


Direct Mobile Routing

- Solves inefficiencies of triangle routing
- Mobile routing is no longer transparent to correspondent (why?)
- Complicates visiting multiple networks during single connection (why?)

Direct Mobile Routing

Anchor Foreign Agent: will forward messages to next foreign agent forming a chain



Correspondent: will always route messages via anchor foreign agent

Thank You!

Networks

Mobile IP

Adopted from material in “Computer Networking: A Top Down Approach” by Kurose and Ross and slides developed by William Conner

Mobile IP

Sections 7.6, 7.8

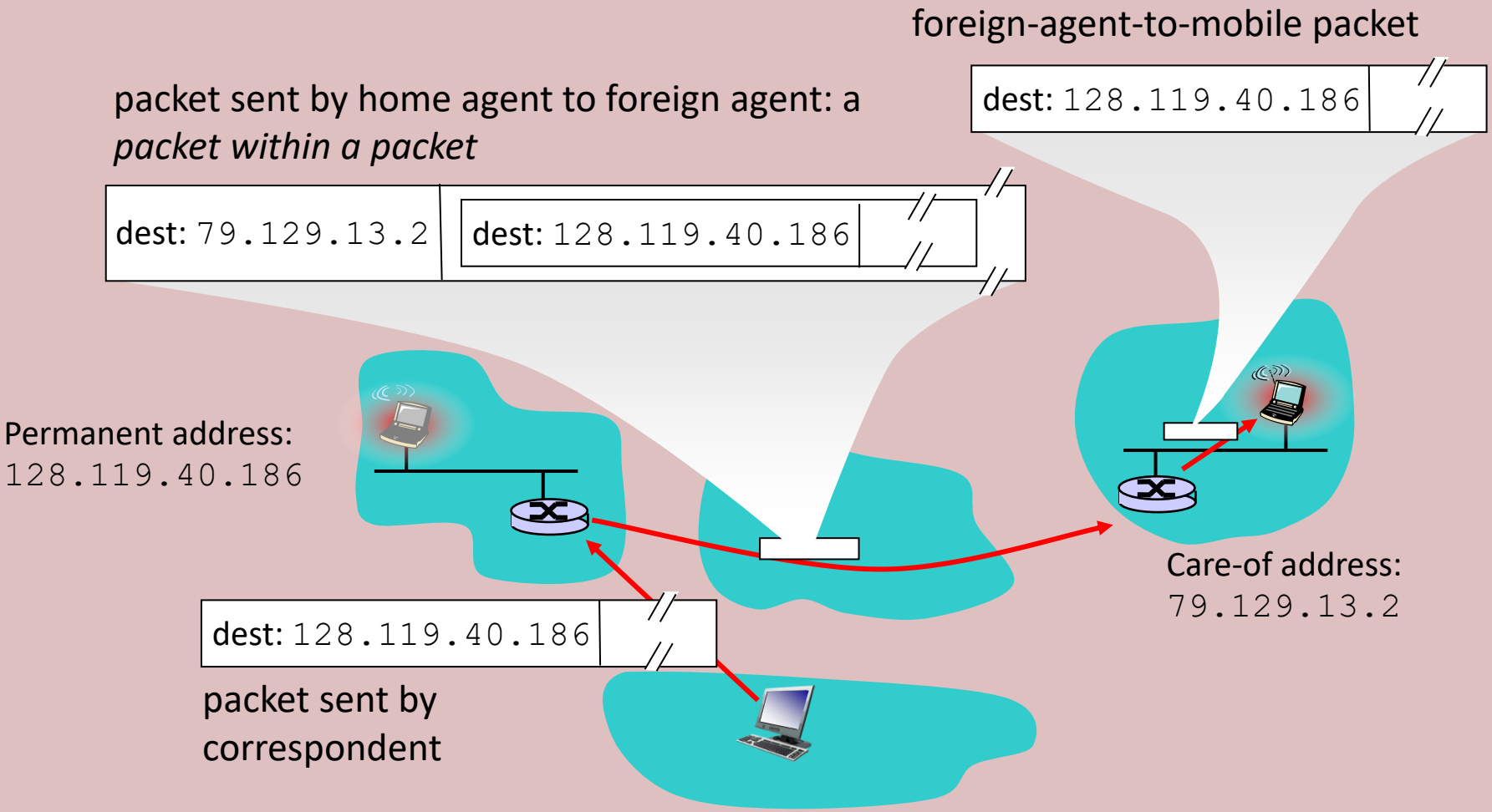
Mobile IP

- RFC 3344

- Has many features we've seen:
  - Home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)

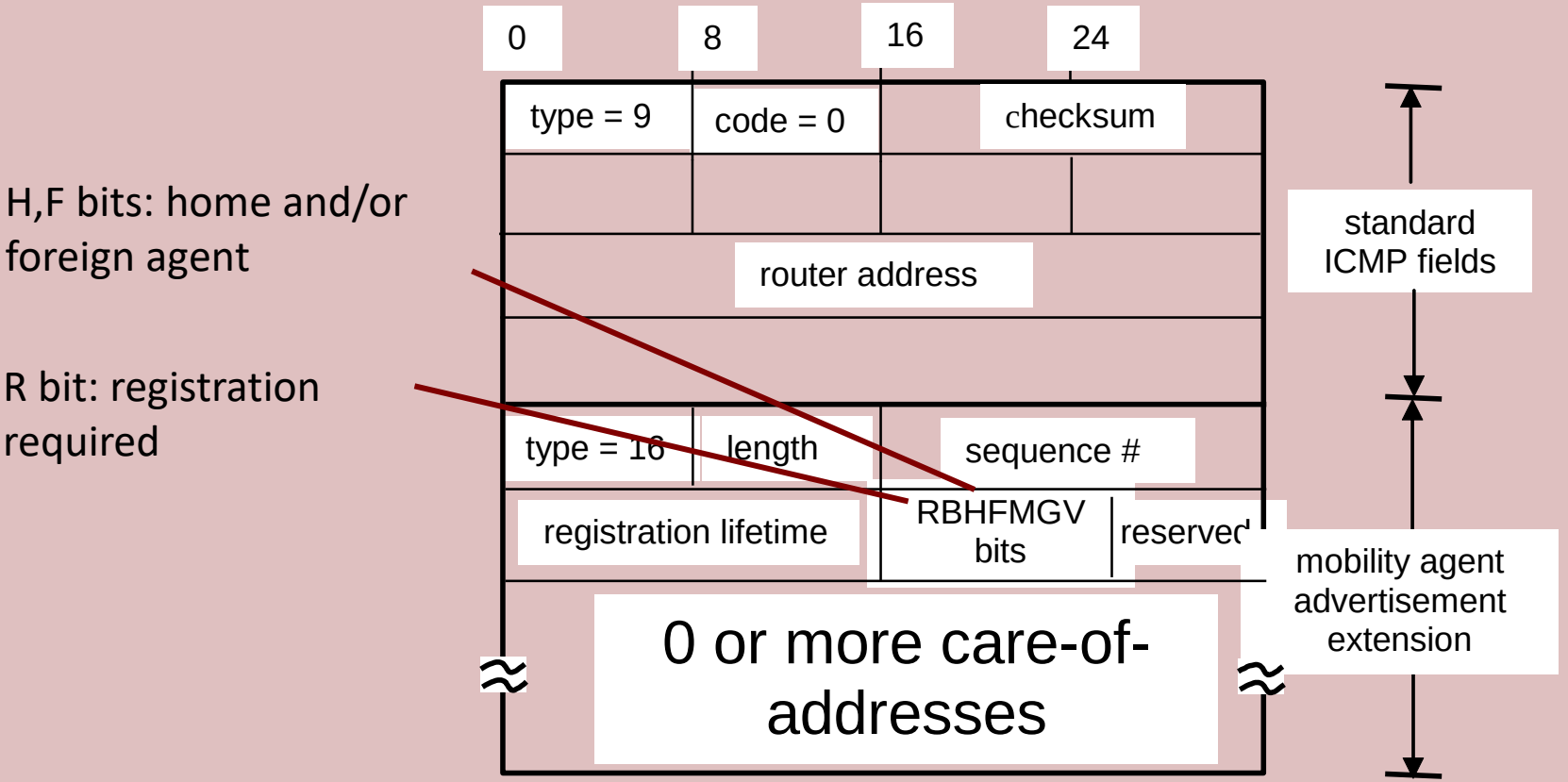
- Three components to the standard:
  - Indirect routing of datagrams
  - Agent discovery
  - Registration with home agent

Mobile IP: Indirect Routing

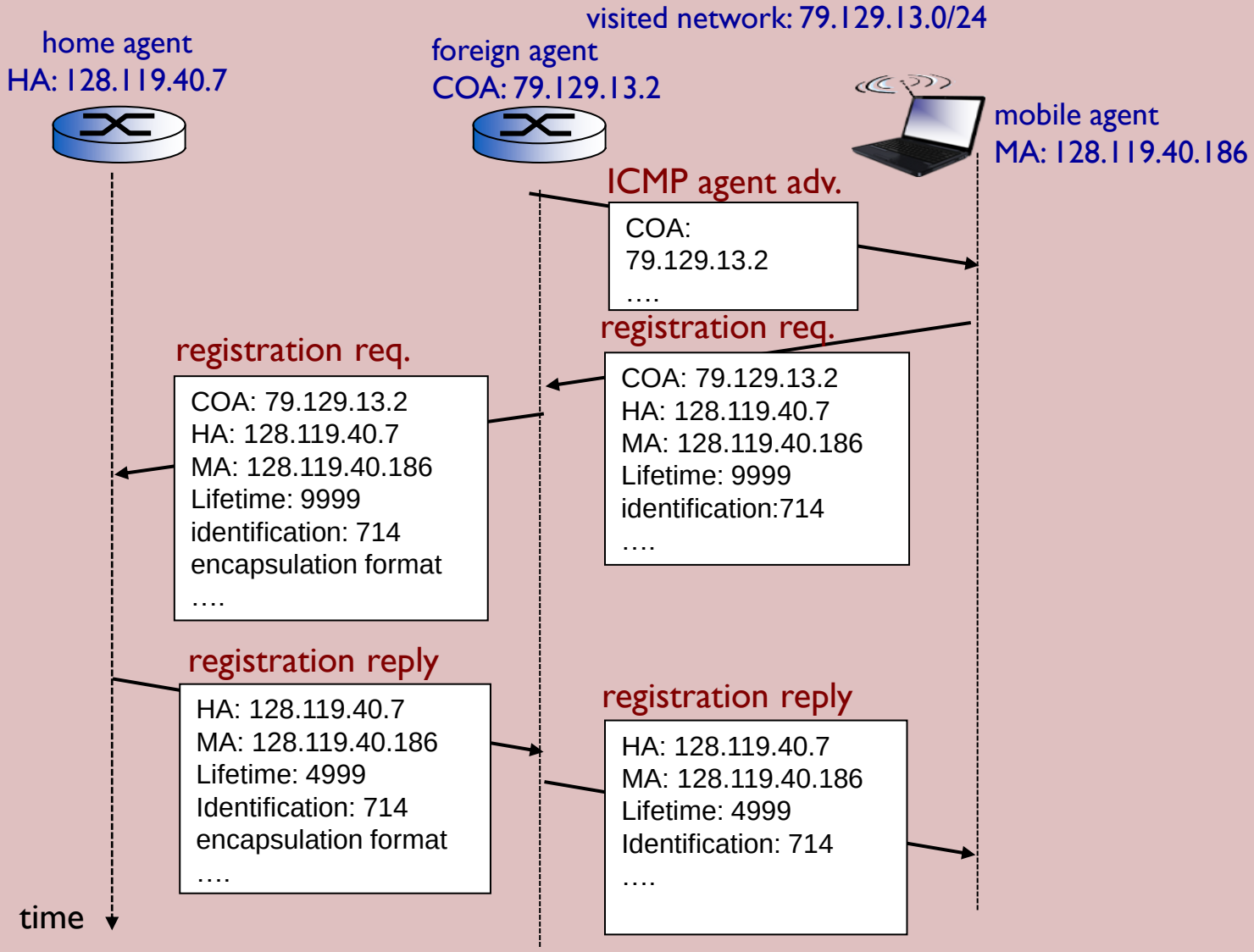


Mobile IP: Agent Discovery

Agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)



Mobile IP: Registration



Reverse Tunneling

- Some ISPs filter traffic with source IP addresses that don't match (why?)
- Visiting host might have outgoing traffic discarded when replying to correspondent
- Solution: use care-of address as source IP address and forward outgoing traffic via home agent (downside?)

Mobile IP Security

- Problem: attacker might submit fake registration with their IP address to intercept traffic

- Solution: registration messages are authenticated

Mobile IP Security

- Problem: attacker might *replay* previously seen registration to trick home network into thinking node is in visiting network

- Solution: registration messages have identifier field so that replayed messages can be detected

Mobility/Wireless Impact on Higher Layers

- No logical impact because TCP and UDP still work for wireless/mobile hosts

- Performance impact
  - Higher packet loss/delay due to bit errors and handoffs (why handoffs?)
  - TCP will misinterpret packet loss on last wireless hop as network congestion
  - Less bandwidth and additional delays for applications

Thank You!