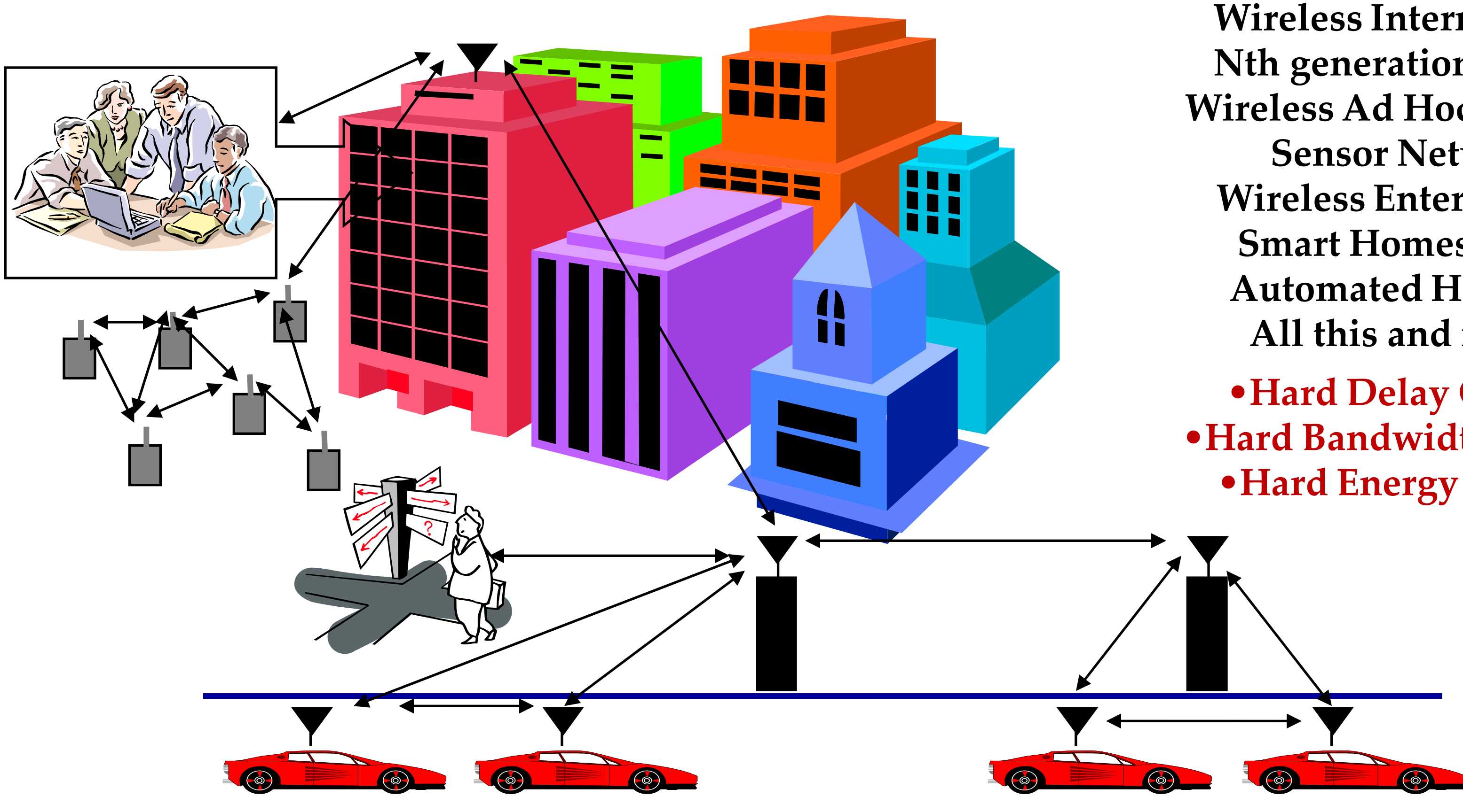
Introduction

HACETTEPE ÜNİVERSİTESİ
Daha İleriye... En İyiye...

Future Wireless Networks

Ubiquitous Communication Among <u>People</u> and <u>Devices</u>



Wireless Internet access
Nth generation Cellular
Wireless Ad Hoc Networks
Sensor Networks
Wireless Entertainment
Smart Homes/Spaces
Automated Highways
All this and more…

- **Hard Delay Constraints**
- **Hard Bandwidth Constraints**
- **Hard Energy Constraints**

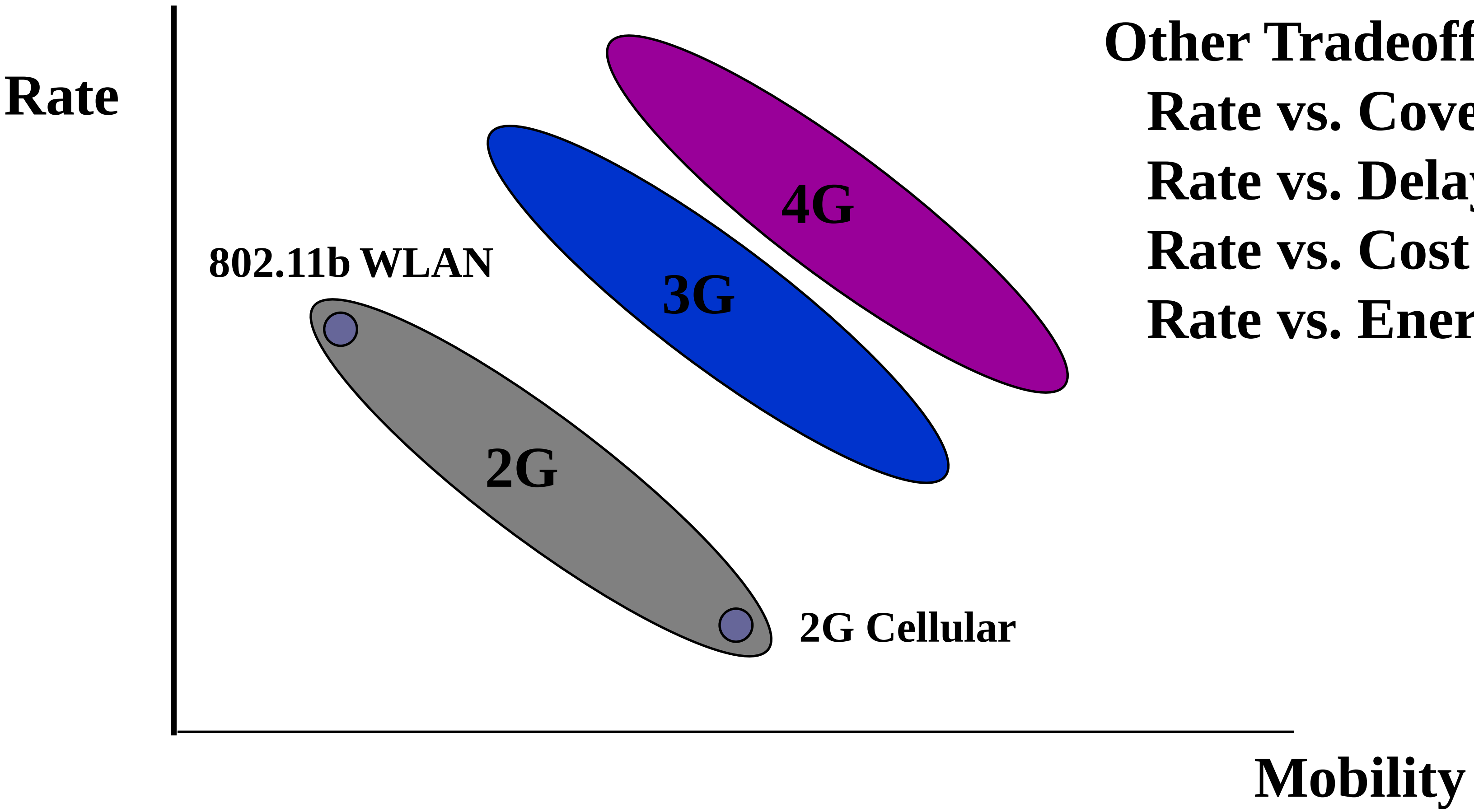
Exciting Developments for Wireless

- Internet and laptop use exploding
- 2G/3G wireless LANs growing rapidly
- Huge cell phone popularity worldwide
- Emerging systems such as Bluetooth, UWB, Zigbee, and WiMAX opening new doors
- Military and security wireless needs
- Important interdisciplinary applications

Design Challenges

- Wireless channels are a difficult and capacity-limited broadcast communications medium
- Traffic patterns, user locations, and network conditions are constantly changing
- Energy and delay constraints change design principles across all layers of the protocol stack

Future Generations



Other Tradeoffs:

- **Rate vs. Coverage**
- **Rate vs. Delay**
- **Rate vs. Cost**
- **Rate vs. Energy**

Fundamental Design Breakthroughs Needed

Wireless and Mobile Networks

Wireless but not mobile

e.g. wireless home or office networks with stationary workstations and large display.

Limited mobility do not require wireless links

e.g. a worker who uses a wired laptop at home, shut down the laptop, drives to work, and attaches the laptop to the company's wired network.

Both wireless and mobile

e.g. a mobile user sitting in the back seat of car which travels 160 km per hour.

Wireless and Mobile Networks

- At the intersection of wireless and mobility, we will find the most interesting technical challenges!

- The challenges posed by these networks are so different from traditional wired computer networks.

  (particularly at the data link and network layers)

Definitions I

Wireless hosts : the end-system run the applications.

a laptop, PDA, phone, computer, *etc.*

Wireless links :

- a host connects to a base station or to another wireless host through a wireless communication link.
- Different wireless link technologies have different transmission rates and can transmit over different distances.

Definitions II

Base station: a key part of the wireless network infrastructure.

If a wireless host is *associated with* a base station :

1. The host is within the wireless communication distance of the base station.
2. The host uses that base station to relay data between the host and the larger network.

e.g. Cell towers in cellular networks.
 Access points in 802.11 wireless LANs.

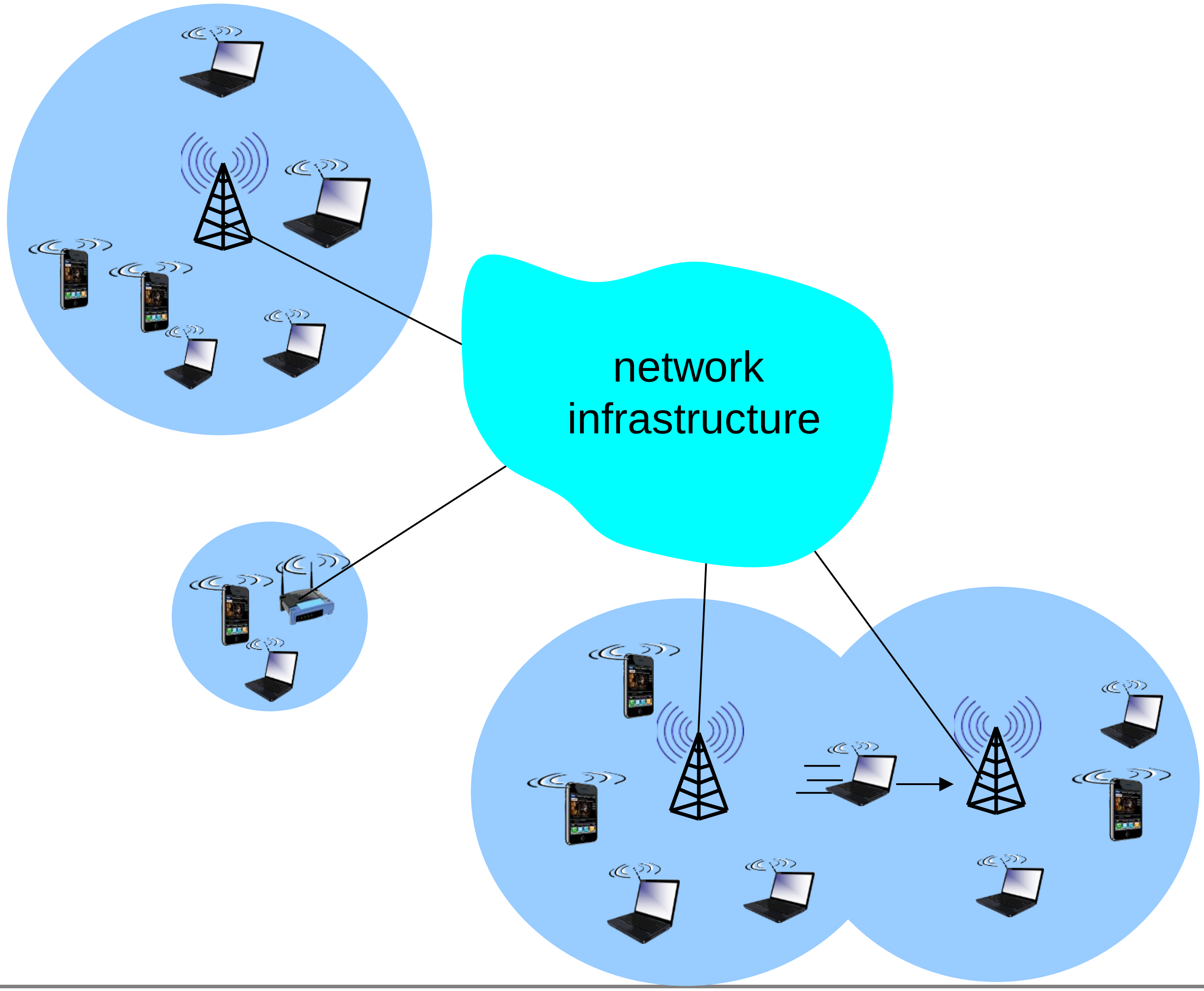
Definitions III

When a host associated with a base station are often referred to as operating in ***infrastructure mode***.

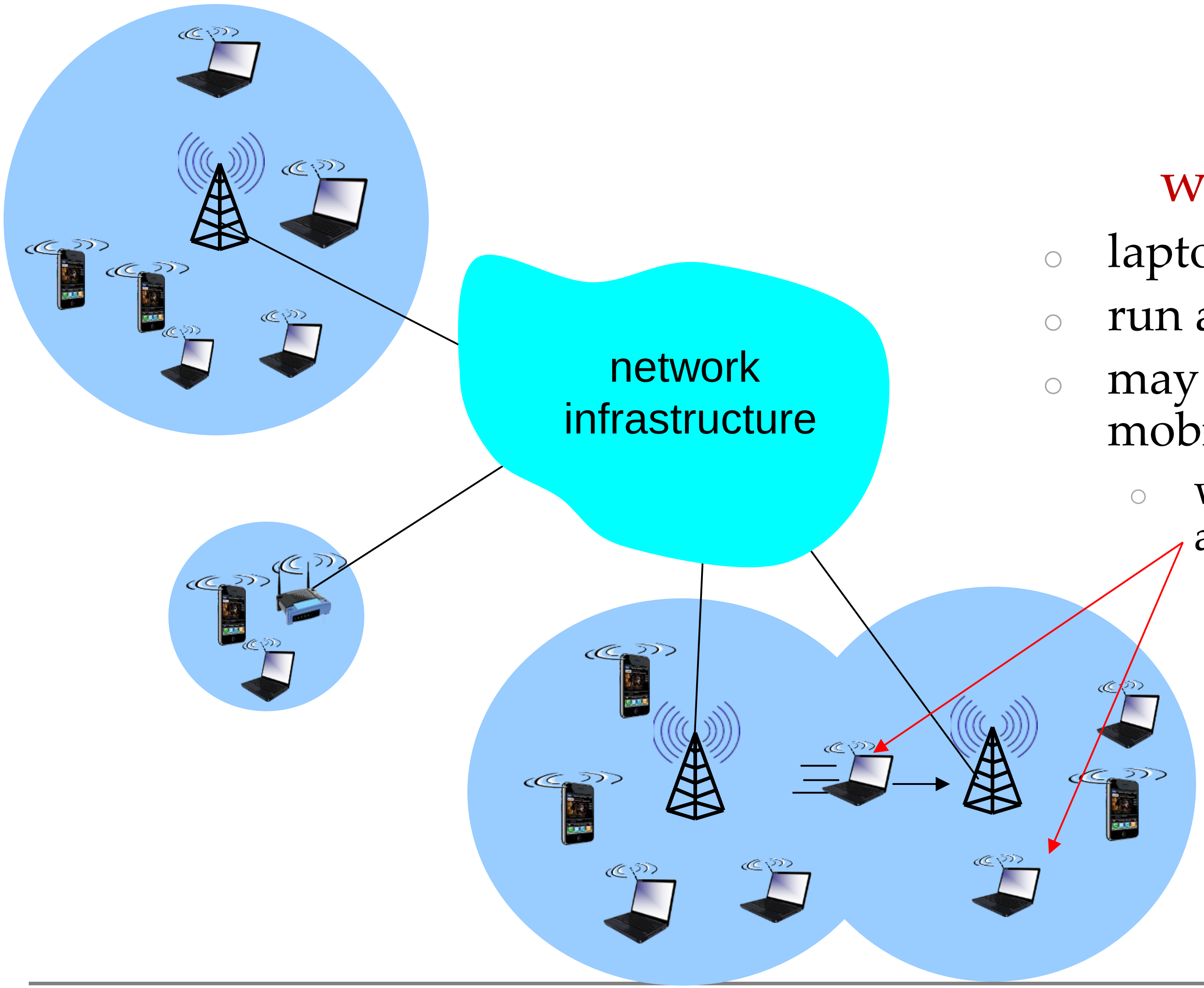
In ad hoc networks, wireless hosts have no such infrastructure with which to connect.

The host themselves must provide services such as routing, address assignment, DNS-like name translation, *etc*.

Elements of a Wireless Network



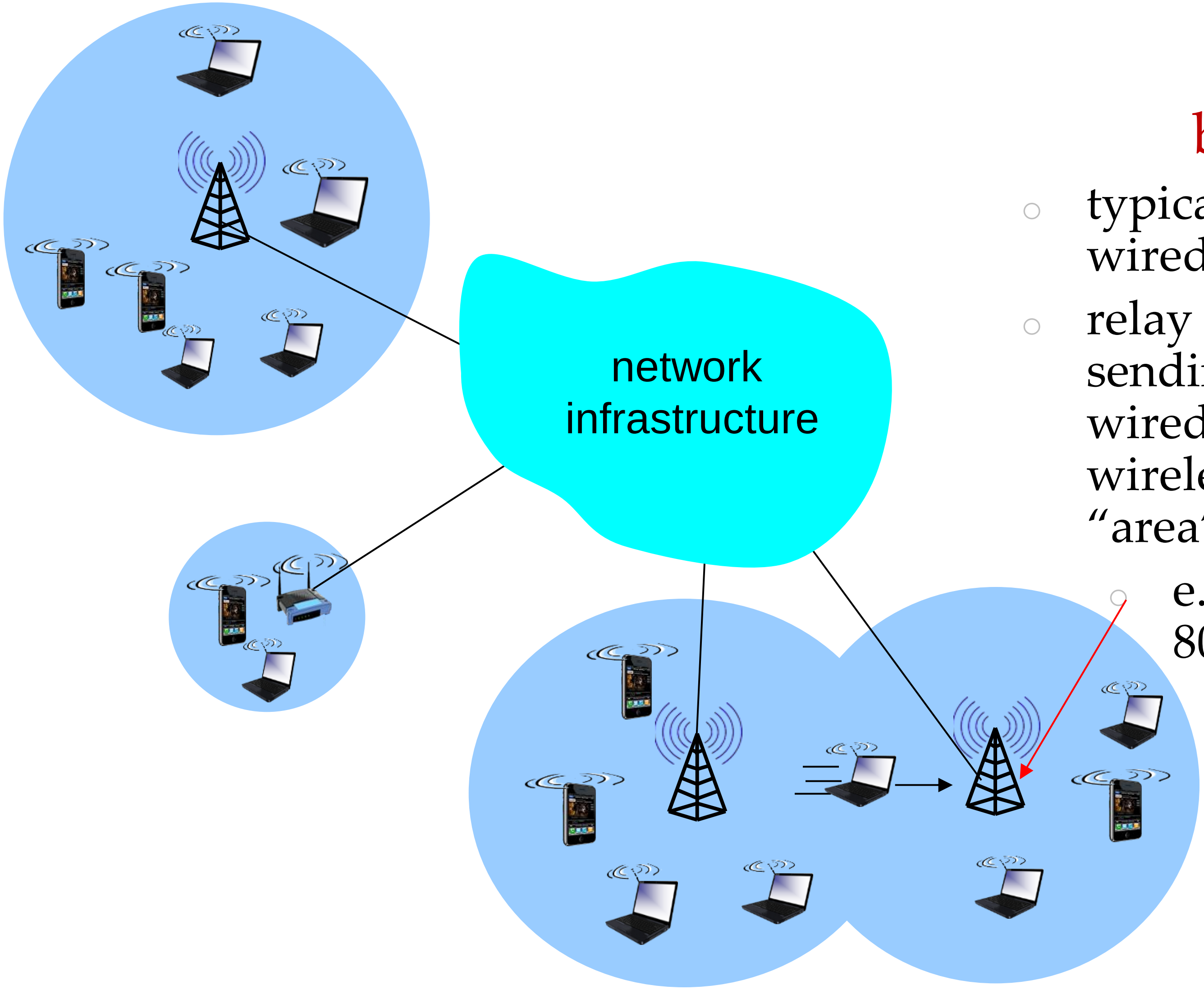
Elements of a Wireless Network



wireless hosts

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

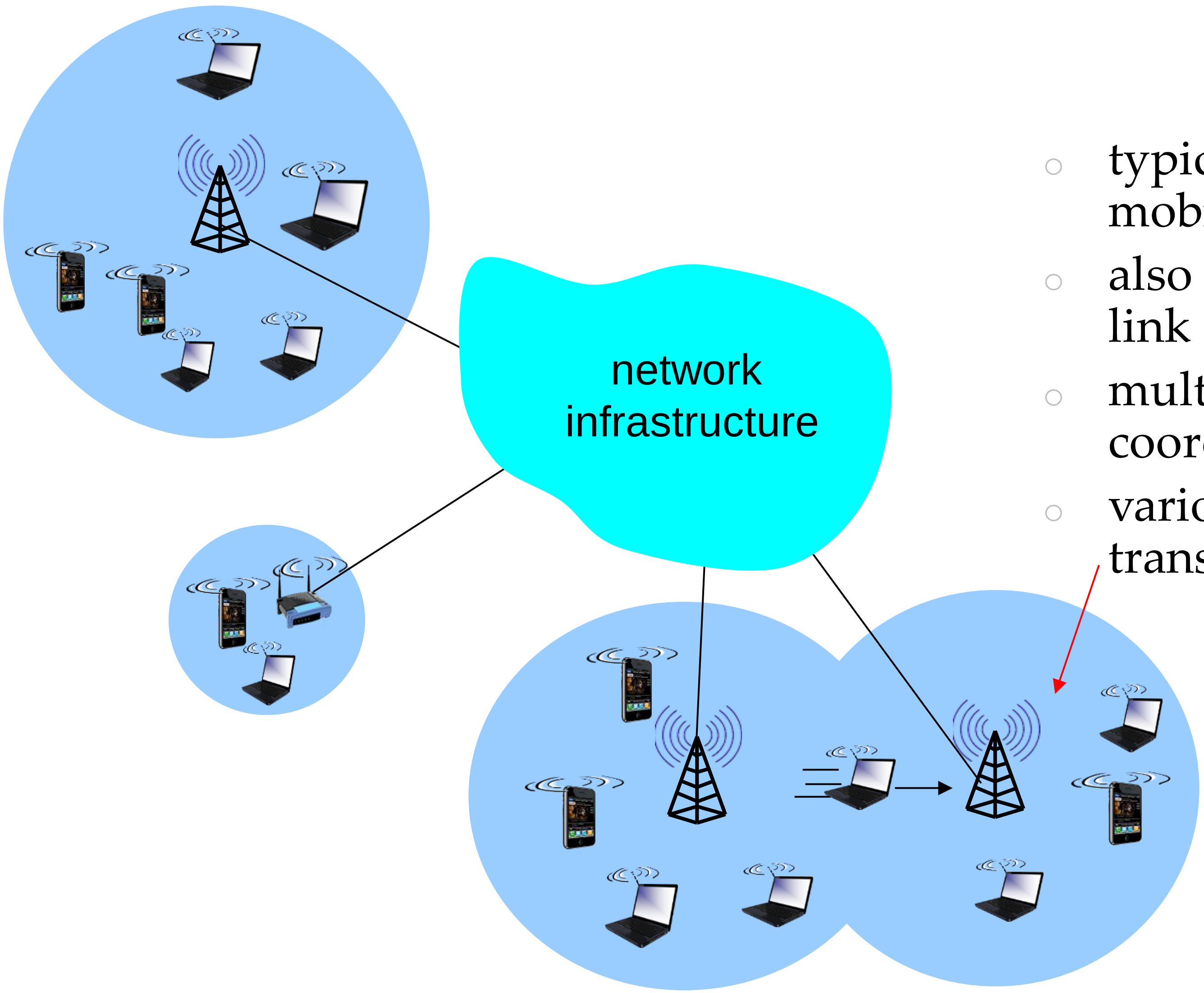
Elements of a Wireless Network



base station

- typically connected to wired network
- relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

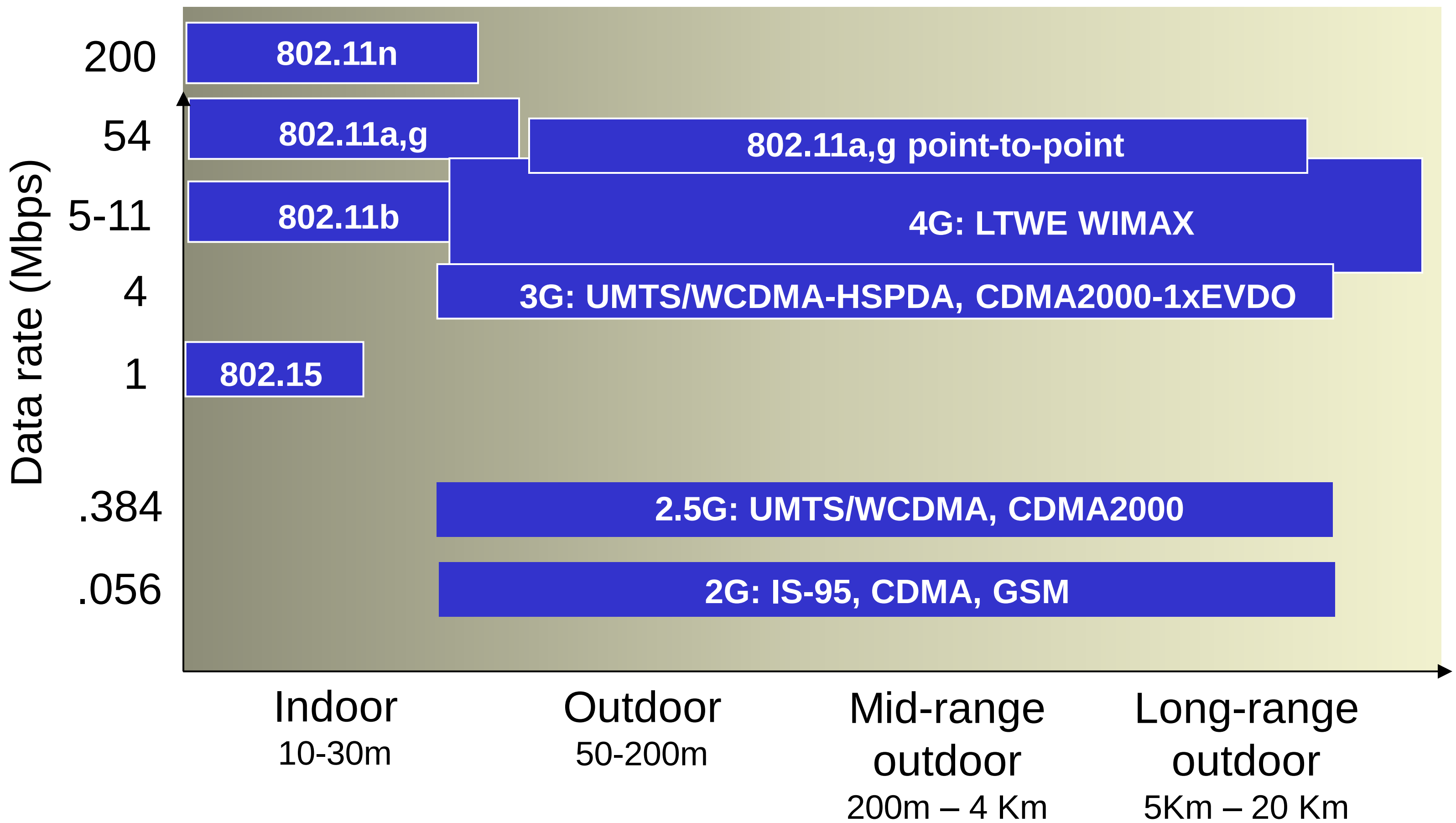
Elements of a Wireless Network



wireless link

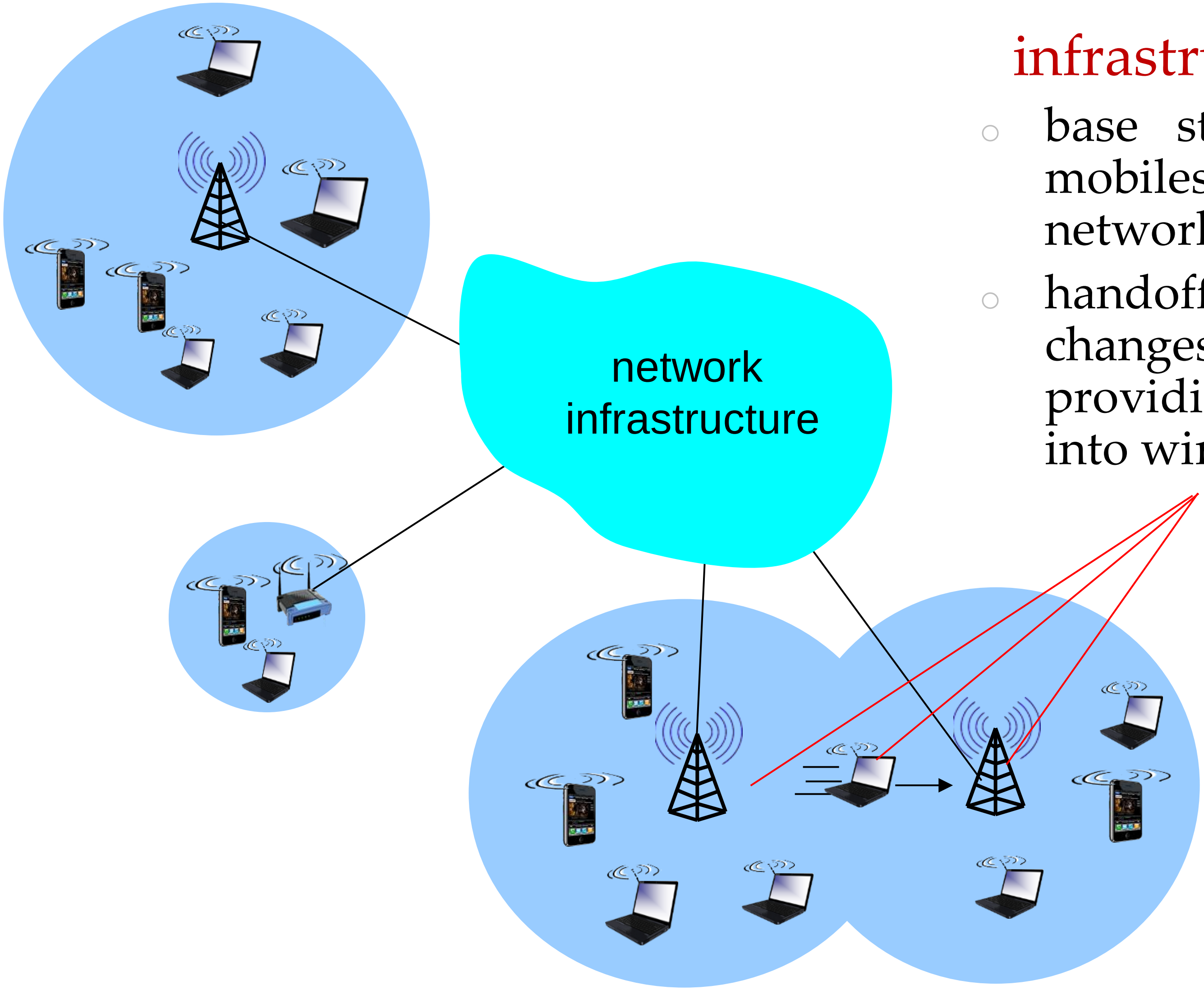
- typically used to connect mobile(s) to base station
- also used as backbone link
- multiple access protocol coordinates link access
- various data rates, transmission distance

Link Characteristics of Selected Wireless Network Standards



Link rate depends on distance, channel conditions, and the number of users in the wireless networks.

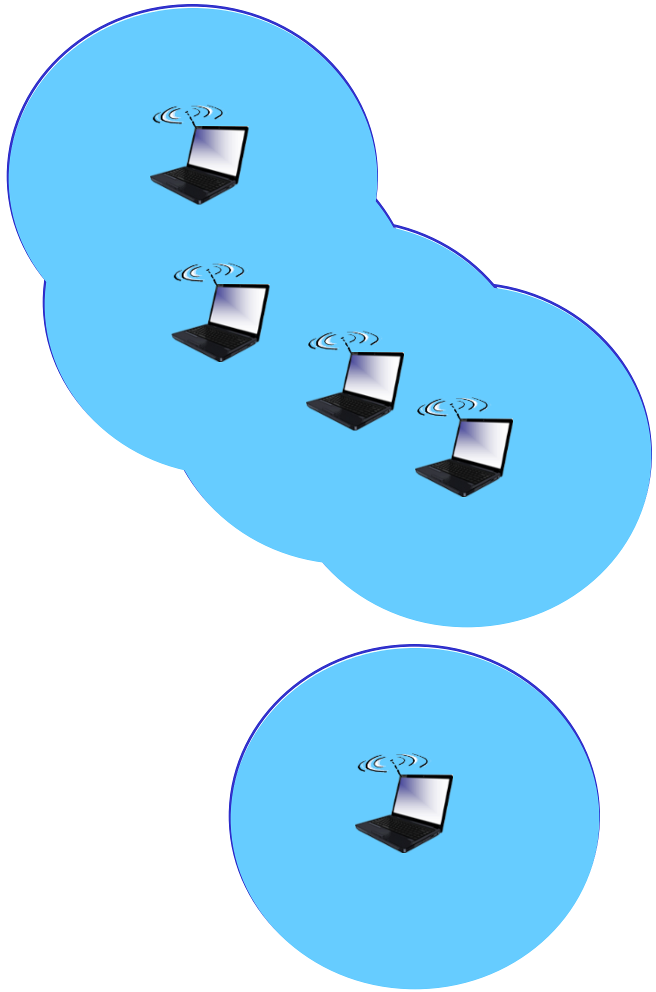
Elements of a Wireless Network



infrastructure mode

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

Elements of a Wireless Network



- ad hoc mode
- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Wireless Networks

Classification based on the number of hops and infrastructure :

1. Single hop, infrastructure-based.

   all communications between a host and the base station.

2. Single hop, infrastructure-less.

   no base station, one node may coordinate the transmissions of the other nodes. Bluetooh networks, 802.11 networks in ad hoc mode

3. Multi-hop, infrastructure-based.

   wireless mesh networks.

4. Multi-hop, infrastructure-less.

   mobile ad hoc networks (MANET)

   vehicular ad hoc networks (VANET)

	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. May have to relay to reach other a given wireless node MANET, VANET

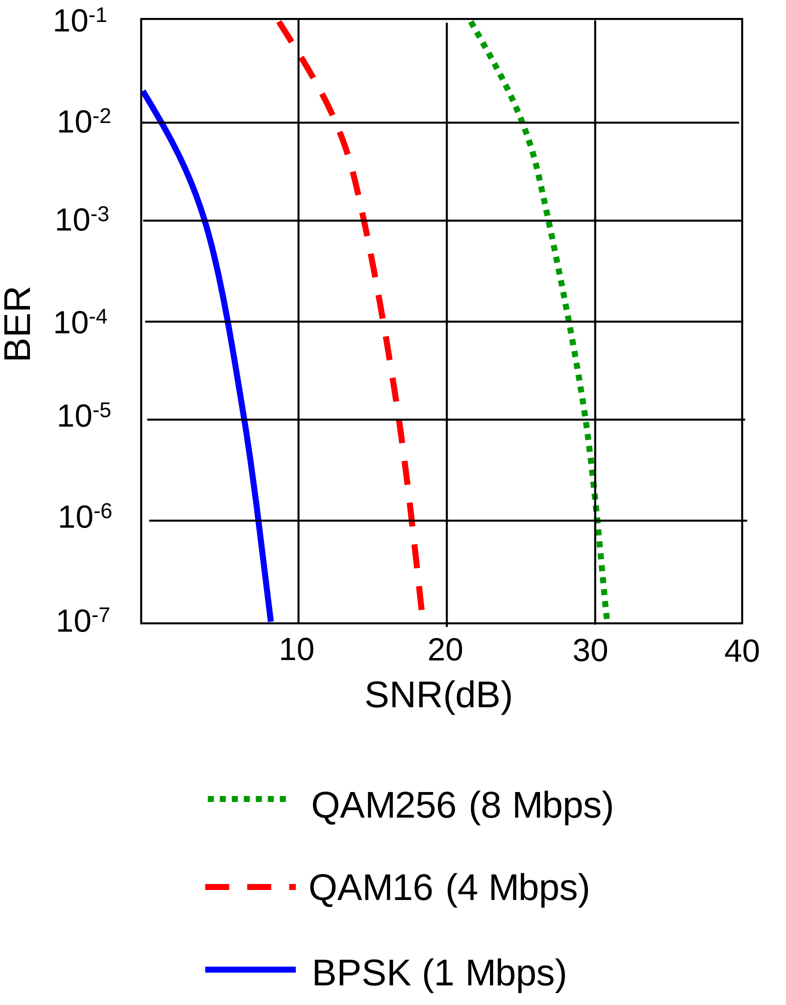
Wireless Link Characteristics

- Decreasing signal length
  - Electromagnetic radiation attenuates as it passes through matter (a wall, etc.).
  - The signal length decreases as the distance between sender and receiver increases (even in free spaces).
- Interference from other sources
  - Radio sources transmitting in the same frequency band will interfere with each other.
  - Electromagnetic noise in the environment.
- Multipath propogations
  - Radio signal reflets off objects ground, arriving destination at slightly different times.
  - Moving objects between the sender and receiver can cause multipath propogation to change over time.

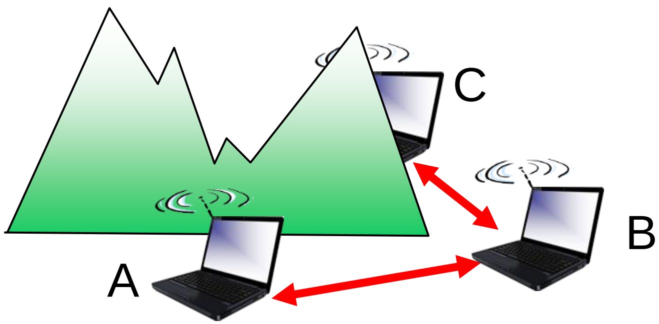
→bit errors will be more common in wireless links. (CRC, retransmissions)

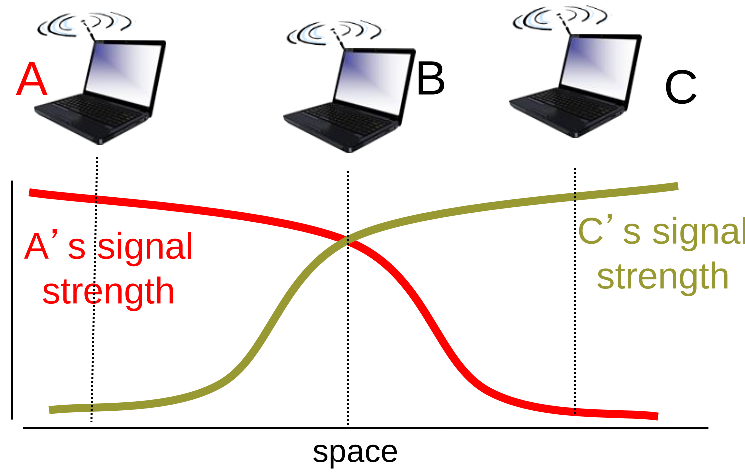
Wireless Link Characteristics (2)

- SNR: signal-to-noise ratio
  - 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 throughput
    - SNR may change with mobility/changes in the environment: dynamically adapt physical layer (modulation technique, rate)



Hidden Terminal Problem





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:

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

More Problems

Ambiguous collisions : Prevents A from overhearing transmissions from B.

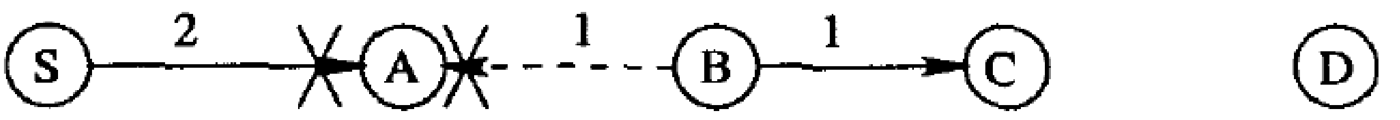


Figure 3: Node A does not hear B forward packet 1 to C, because B's transmission collides at A with packet 2 from the source S.

Receiver collisions : The node cannot tell the packet is received.

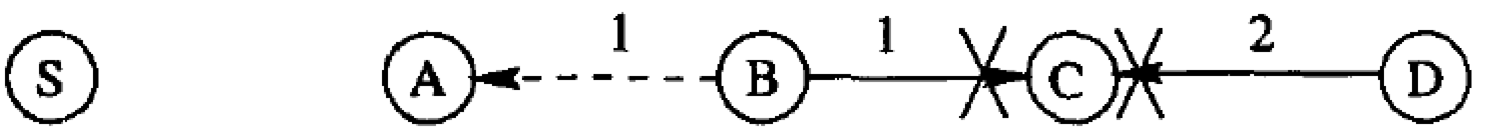
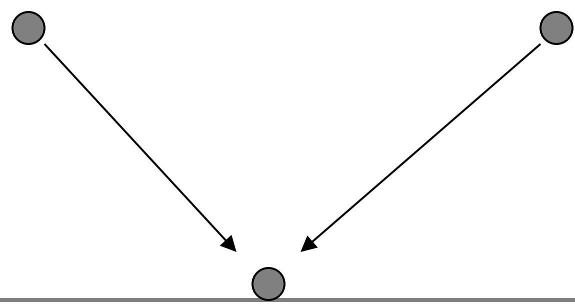


Figure 4: Node A believes that B has forwarded packet 1 on to C, though C never received the packet due to a collision with packet 2.

Multi-transmitter Interference Problem

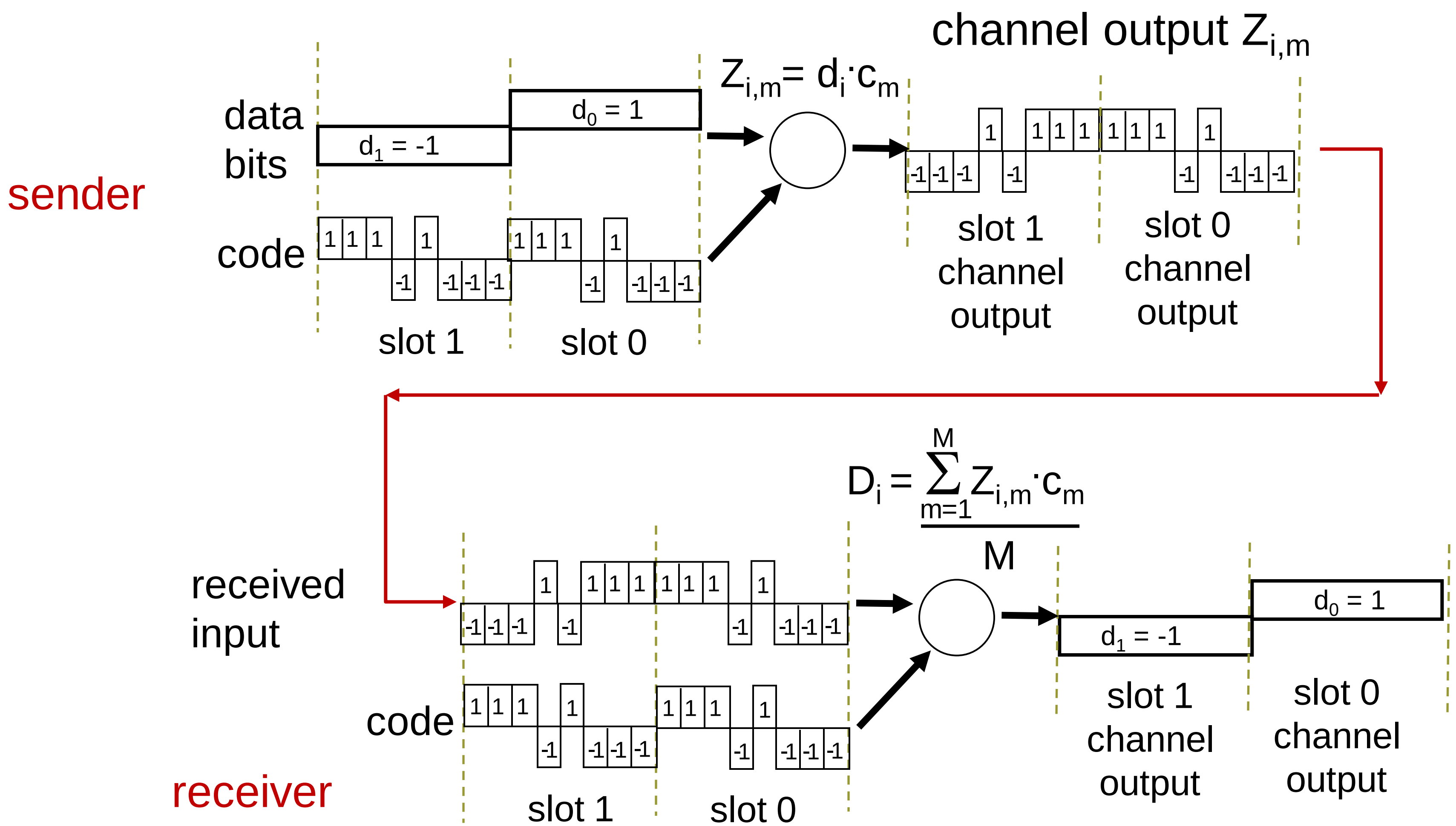
- Similar to multi-path or noise
- Two transmitting stations will constructively/destructively interfere with each other at the receiver
- Receiver will “hear” the sum of the two signals (which usually means garbage)



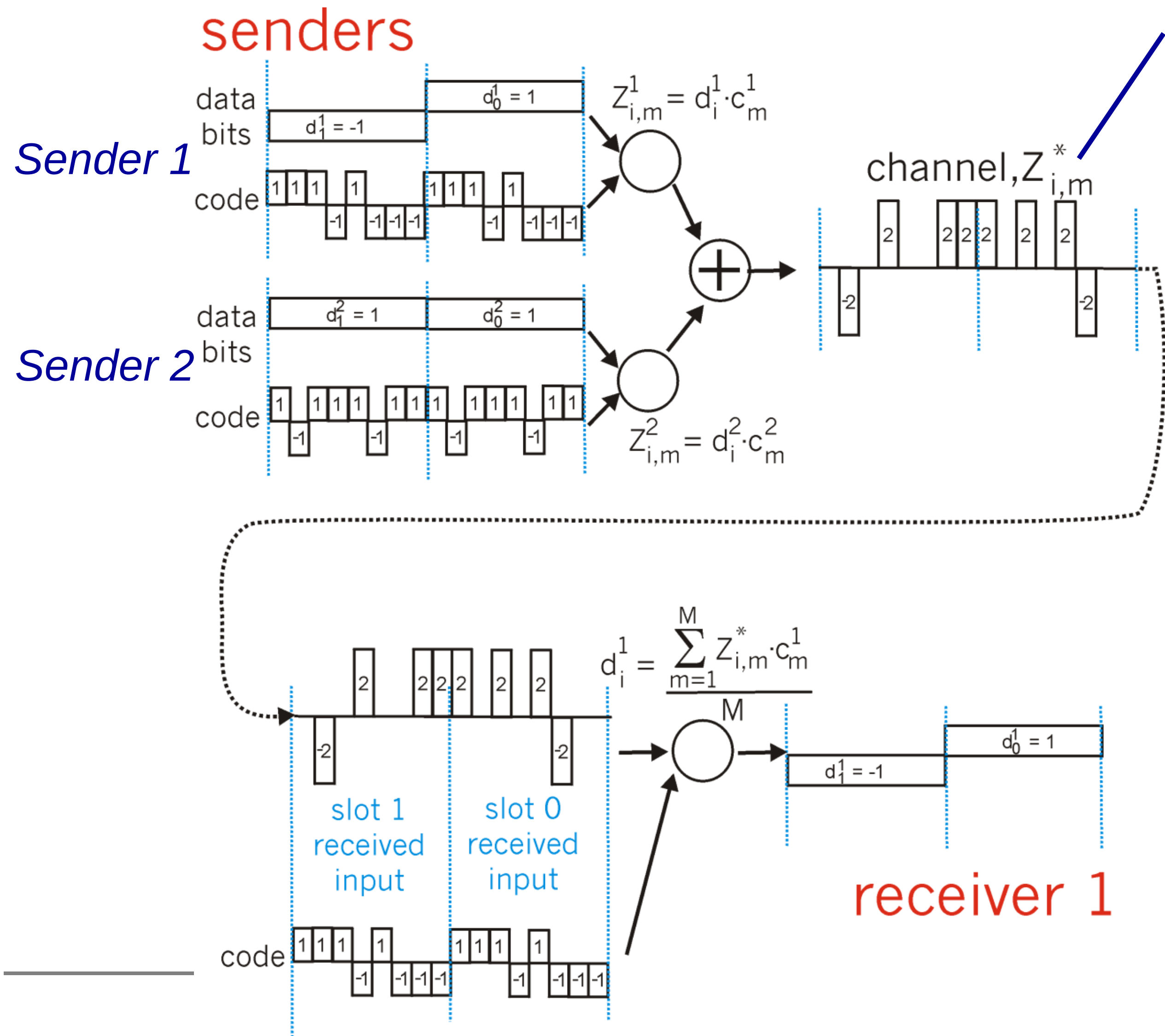
Code Division Multiple Access (CDMA)

- 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

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!

IEEE 802.11 Wireless LAN

802.11b
- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps
- direct sequence spread spectrum (DSSS) in physical layer
  - all hosts use same chipping code

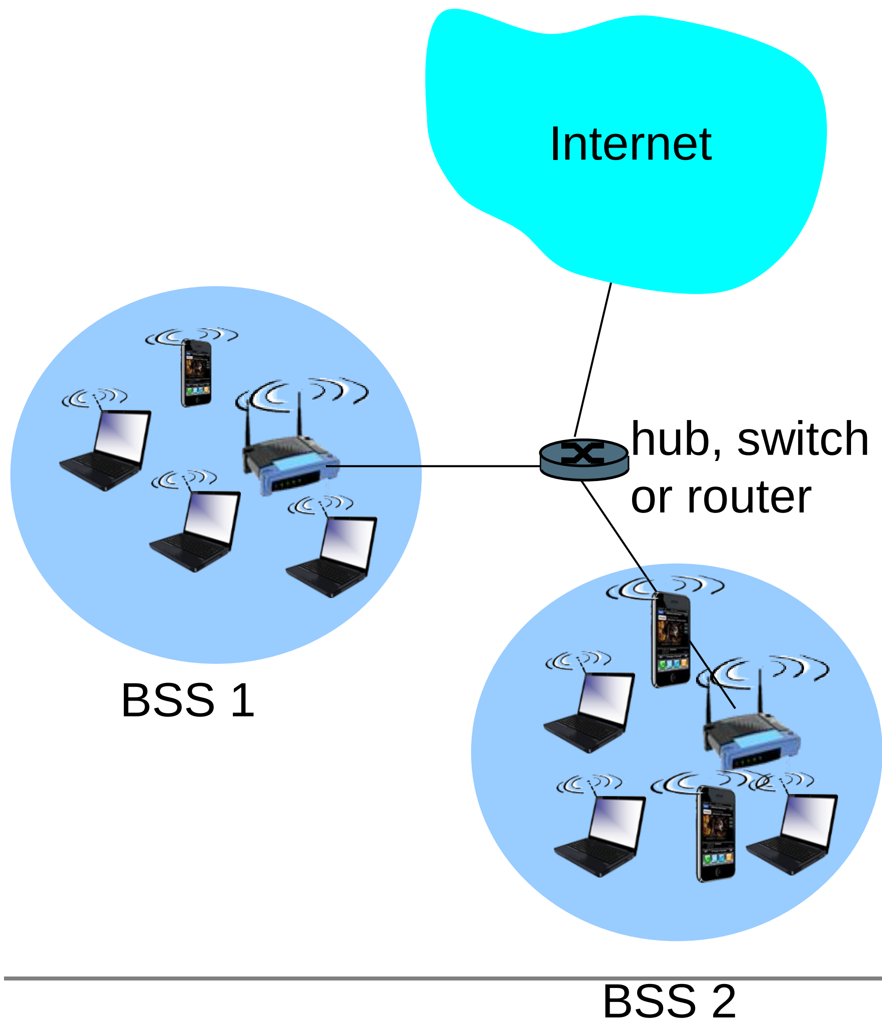
802.11a
- 5-6 GHz range (shorter transmission distance)
- up to 54 Mbps

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

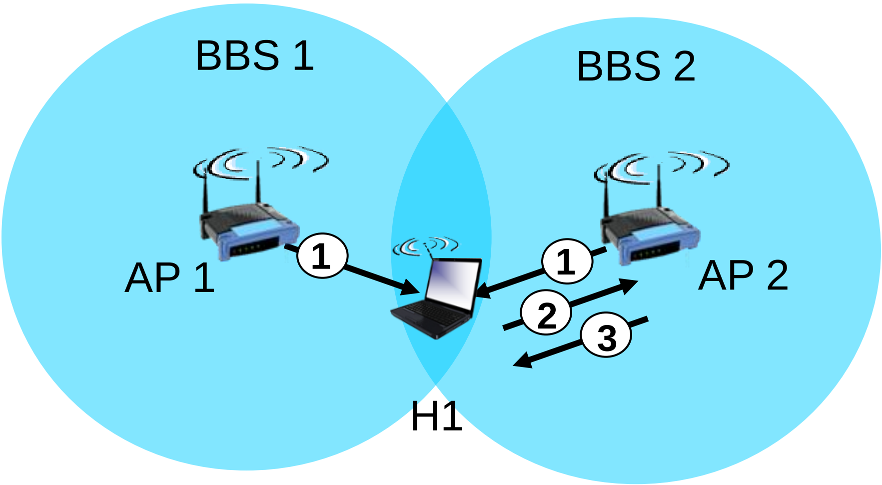


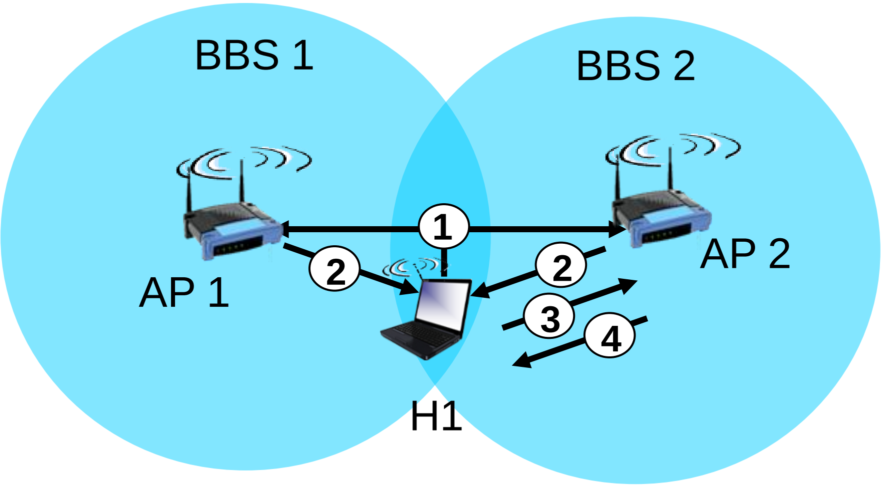
- wireless host communicates with base station
  - base station = access point (AP)
- Basic Service Set (BSS) (aka "cell") in infrastructure mode contains:
  - wireless hosts
  - access point (AP): base station
  - ad hoc mode: hosts only

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

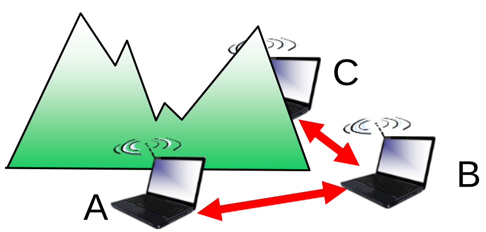
(2) Probe Response frames sent from APs

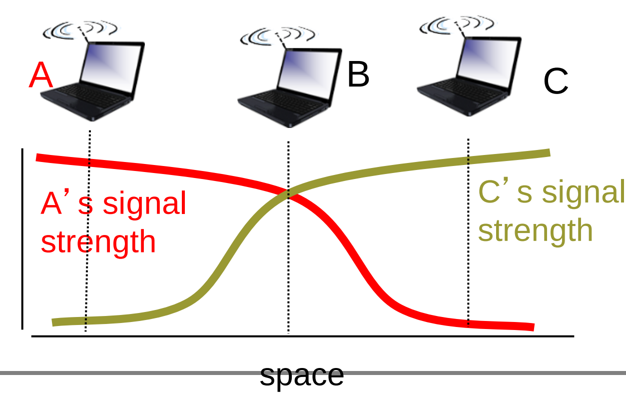
(3) Association Request frame sent: H1 to selected AP

(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: 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)





Carrier Sense Multiple Access (CSMA)

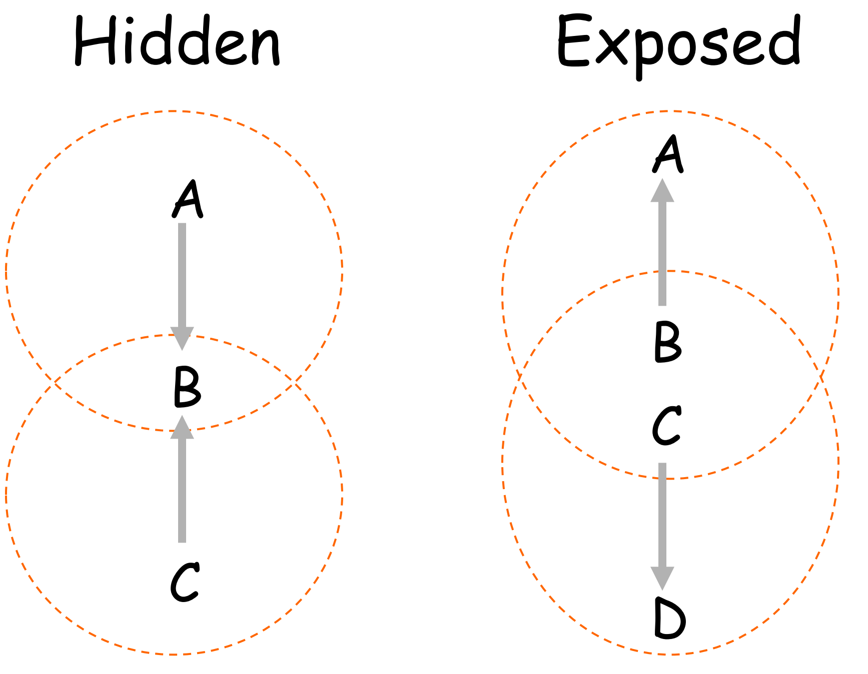
- Procedure
  - Listen to medium and wait until it is free (no one else is talking)
  - Wait a random back off time then start talking
- Advantages
  - Fairly simple to implement
  - Functional scheme that works
- Disadvantages
  - Can not recover from a collision
  - (inefficient waste of medium time)

Carrier Sense Multiple Access with Collision Detection (CSMA-CD)

- Procedure
  - Listen to medium and wait until it is free
  - Then start talking, but listen to see if someone else starts talking too
  - If a collision occurs, stop and then start talking after a random back off time
- This scheme is used for hub based Ethernet
- Advantages
  - More efficient than basic CSMA
- Disadvantages
  - Requires ability to detect collisions

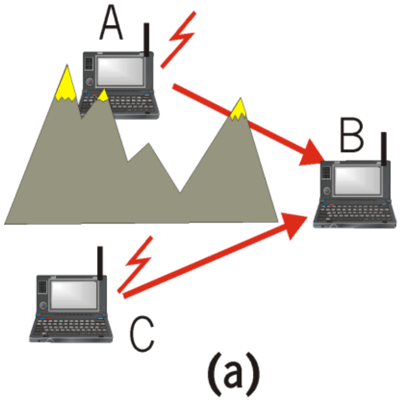
CSMA/CD Does Not Work

- Collision detection problems
  - Relevant contention at the receiver, not sender
    - Hidden terminal
    - Exposed terminal
  - Hard to build a radio that can transmit and receive at same time



Hidden Terminal Effect

- Hidden terminals: A, C cannot hear each other
  - Obstacles, signal attenuation
  - Collisions at B
  - Collision if 2 or more nodes transmit at same time
- CSMA makes sense:
  - Get all the bandwidth if you're the only one transmitting
  - Shouldn't cause a collision if you sense another transmission
- Collision detection doesn't work
- **CSMA/CA: CSMA with C**ollision **A**voidance



Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

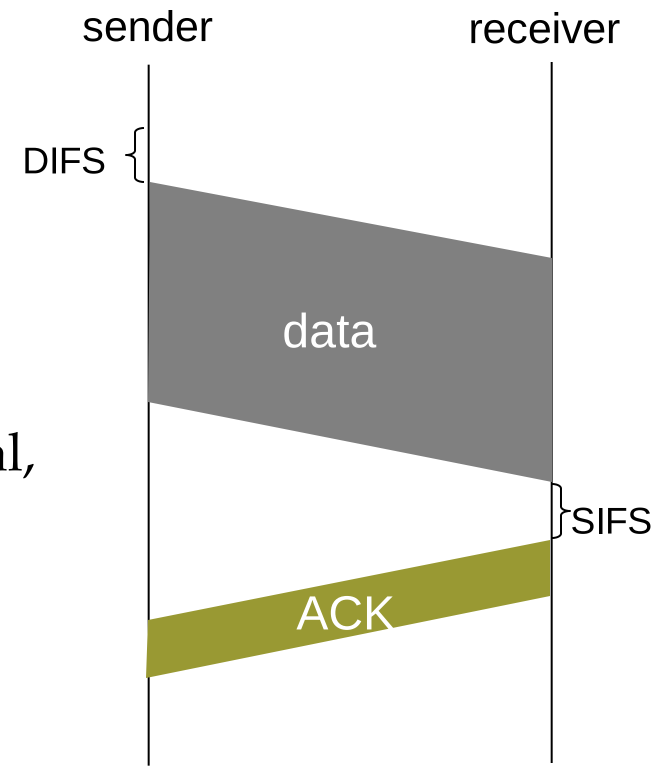
- Procedure
  - Similar to CSMA but instead of sending packets control frames are exchanged
  - RTS = request to send
  - CTS = clear to send
  - DATA = actual packet
  - ACK = acknowledgement

IEEE 802.11 MAC Protocol: 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 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)

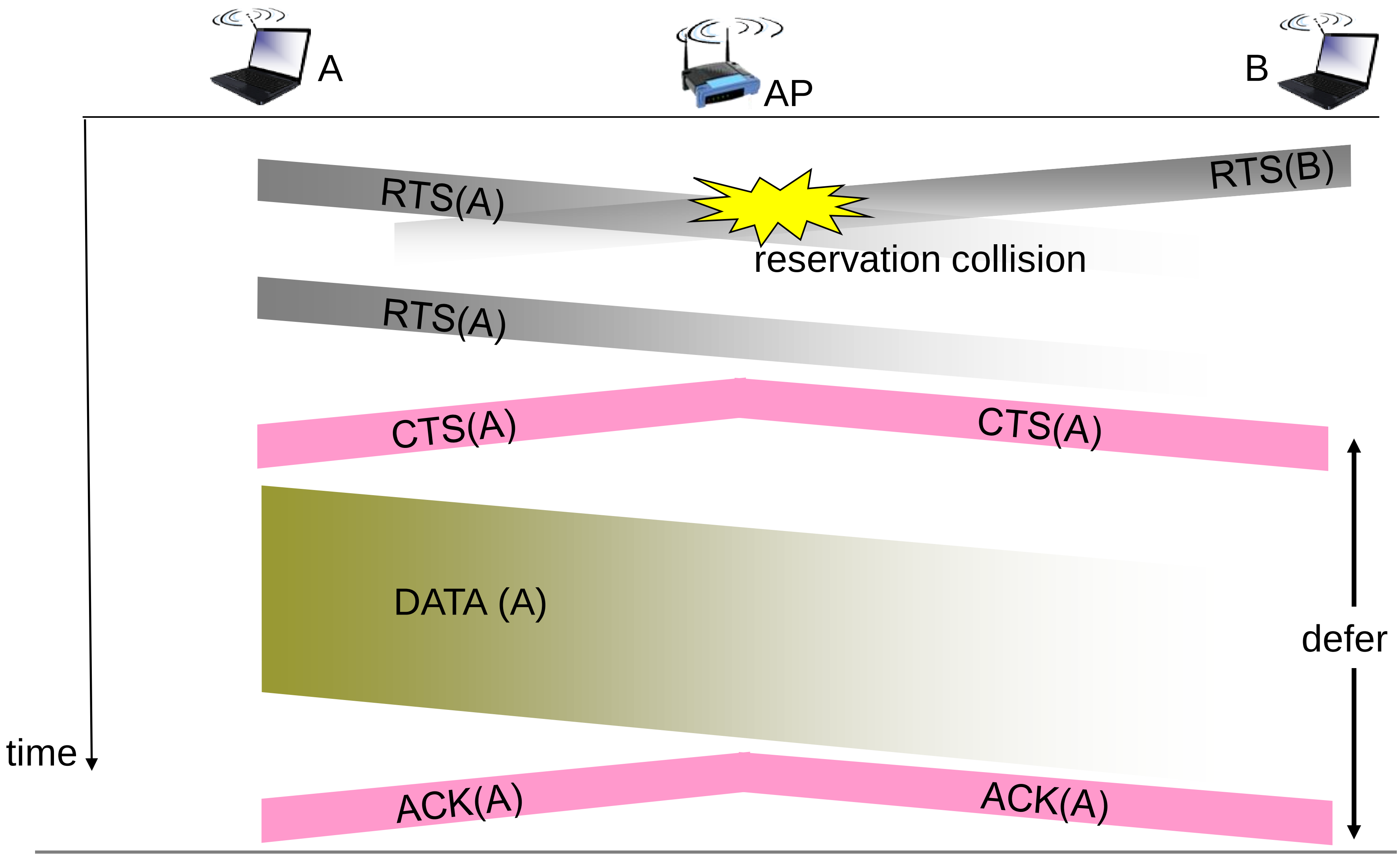
Avoiding collisions (more)

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

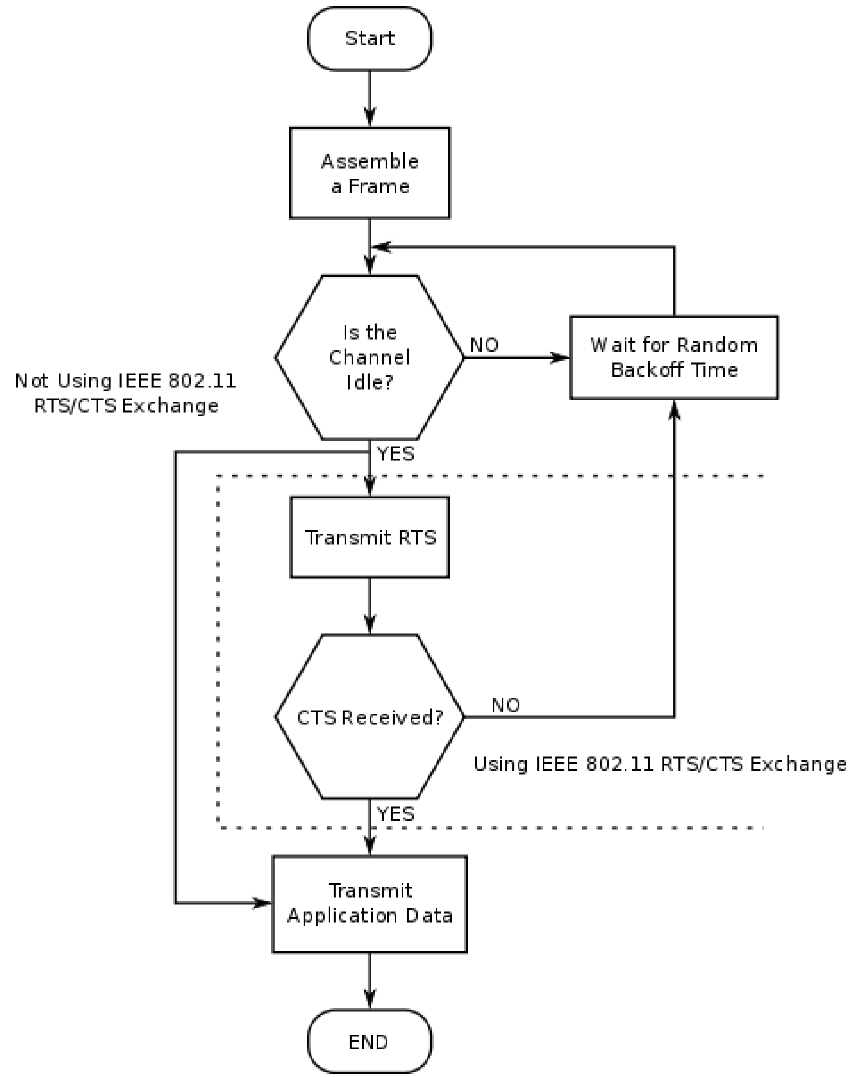
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely using small reservation packets!

Collision Avoidance: RTS-CTS exchange



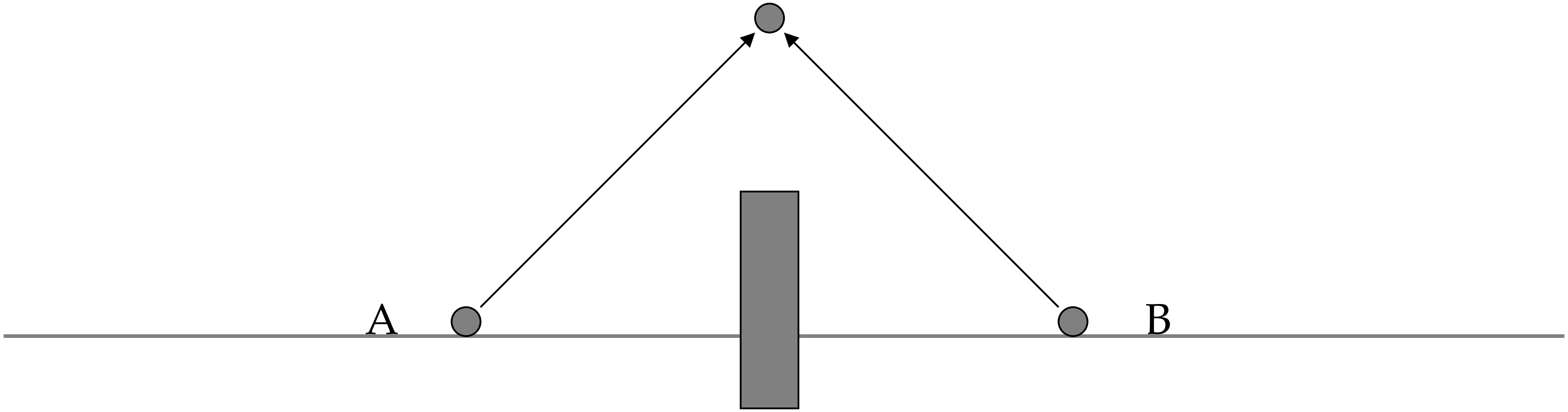
CSMA/CA



Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
Not Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit RTS
CTS Received?
NO
Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit Application Data
END

Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

- Advantages
  - Small control frames lessen the cost of collisions (when data is large)
  - RTS + CTS provide “virtual” carrier sense which protects against hidden terminal collisions (where A can’t hear B)

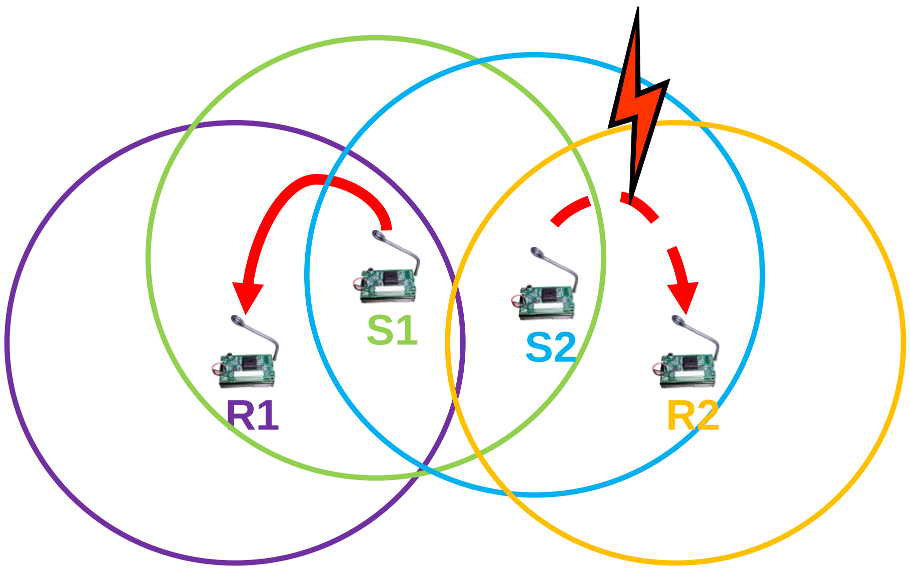


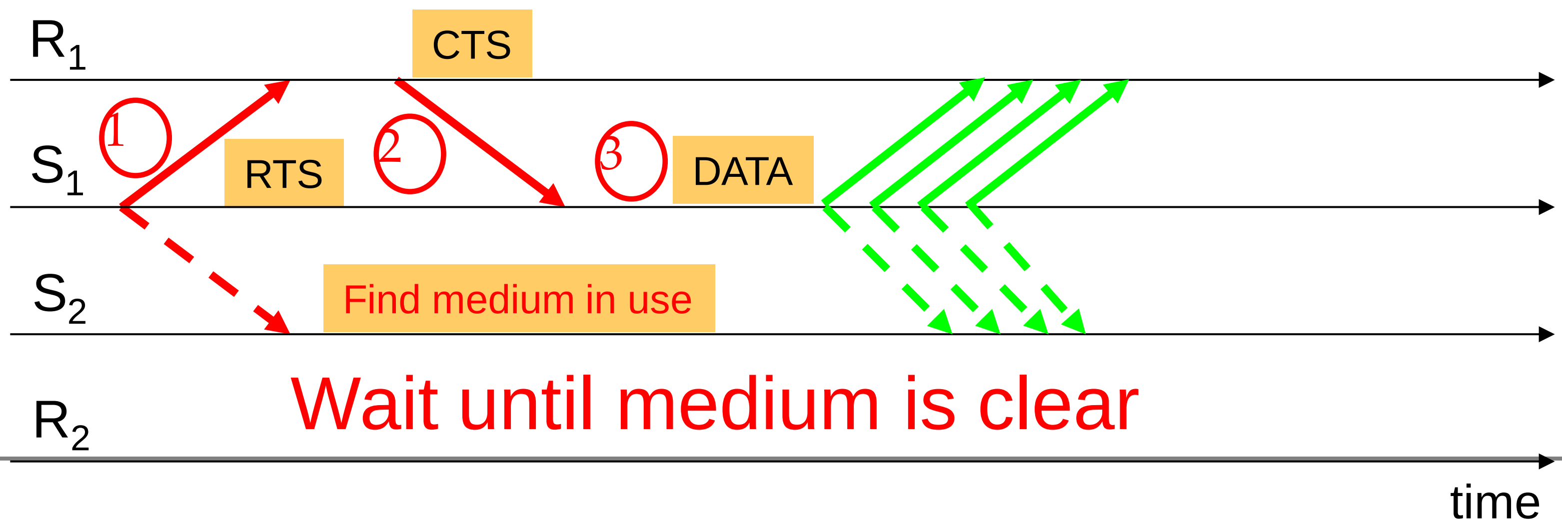
Carrier Sense Multiple Access with Collision Avoidance (CSMA-CA)

- Disadvantages
  - Not as efficient as CSMA-CD
  - Doesn’t solve all the problems of MAC in wireless networks

Exposed Terminal Problem

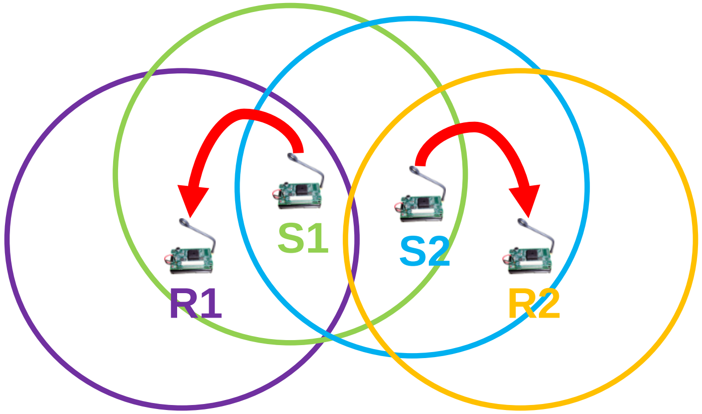
The sender mistakenly think the medium is in use, so that it unnecessarily defers the transmission.





Exposed Terminal Problem

- When a node hears an RTS from a neighboring node, but not the corresponding CTS, that node can deduce that it is an *exposed terminal* and is permitted to transmit to other neighboring nodes.



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

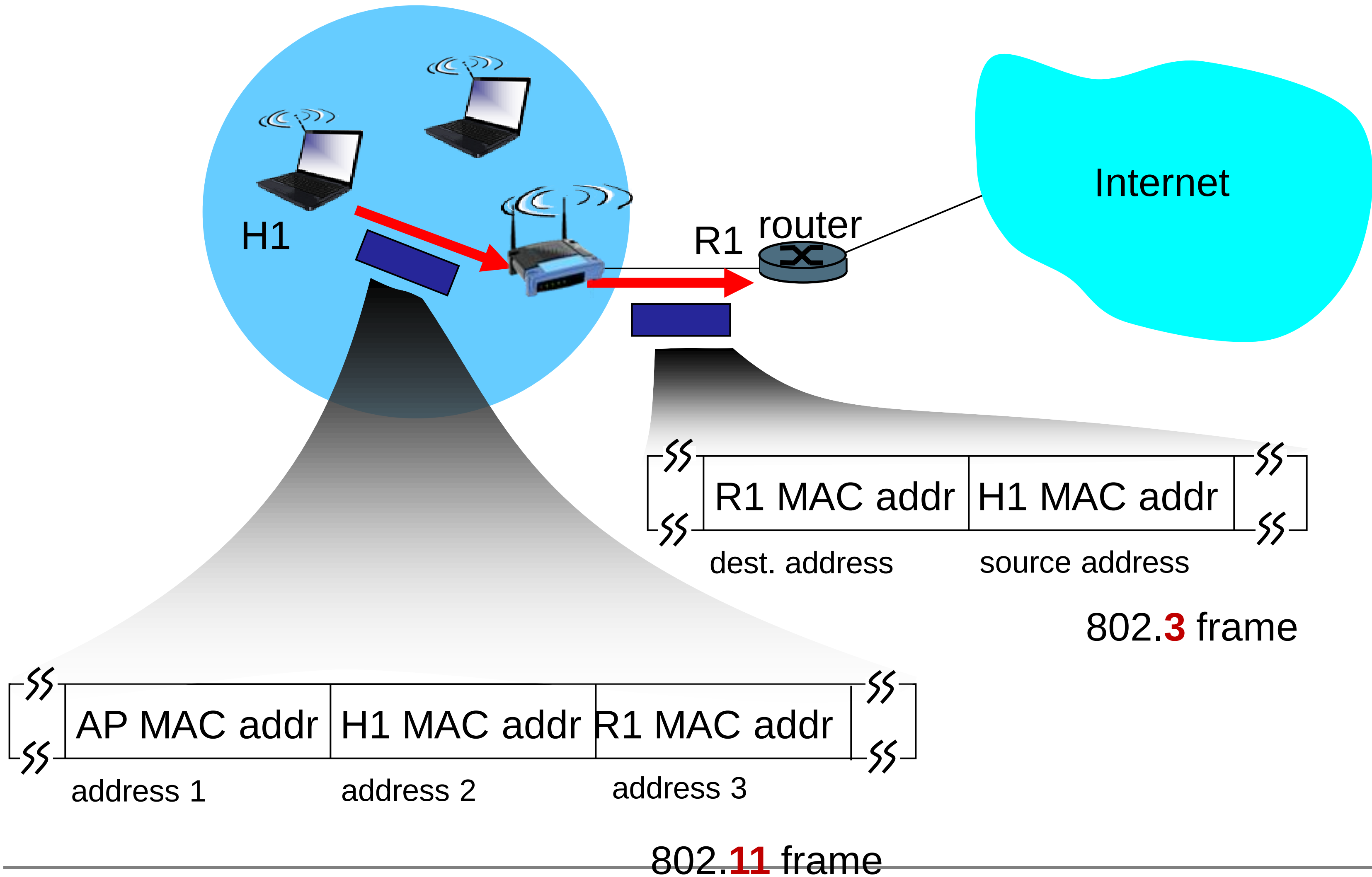
Address 1: MAC address of wireless host or AP to receive this frame

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

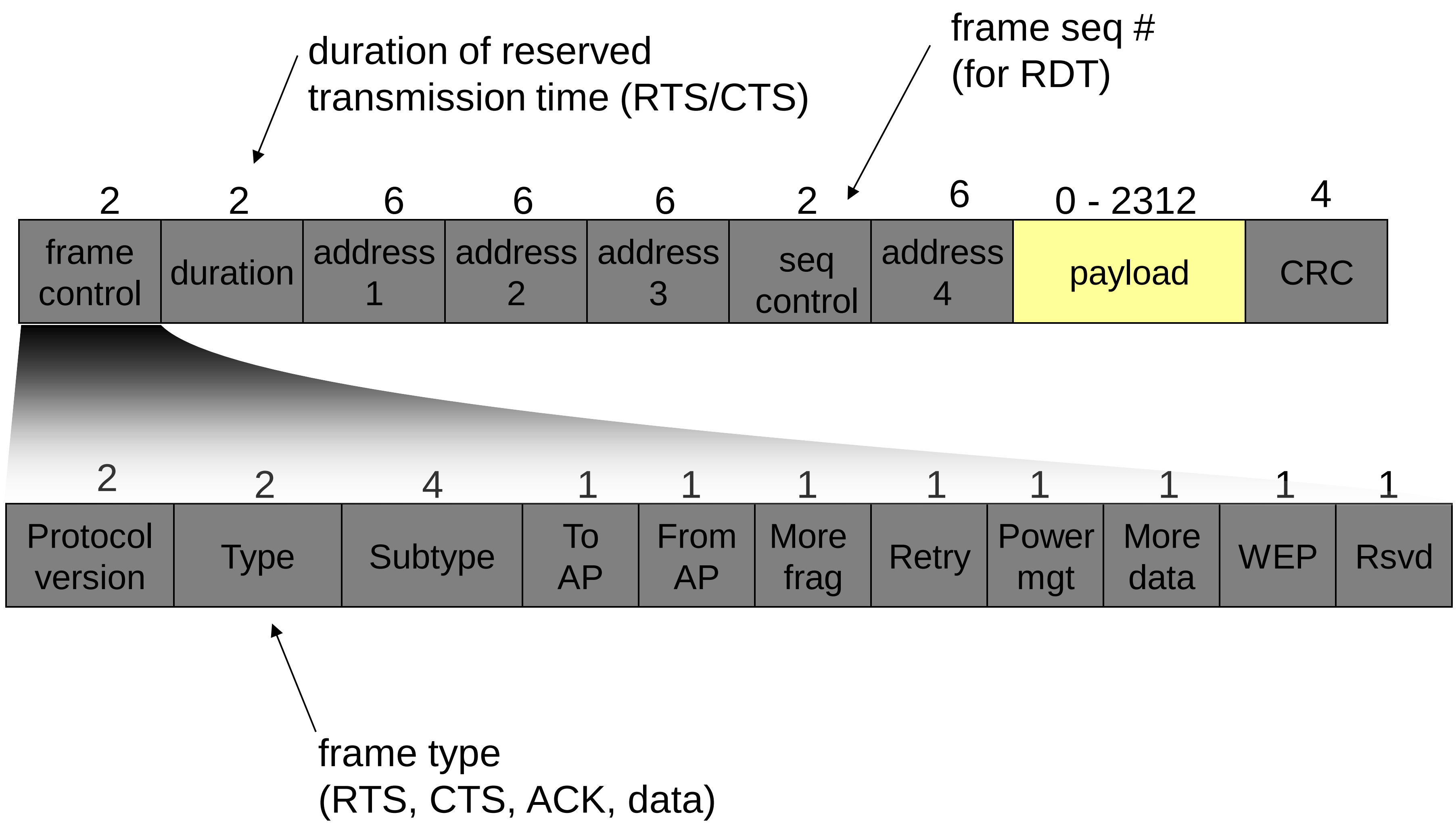
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

802.11 frame: addressing

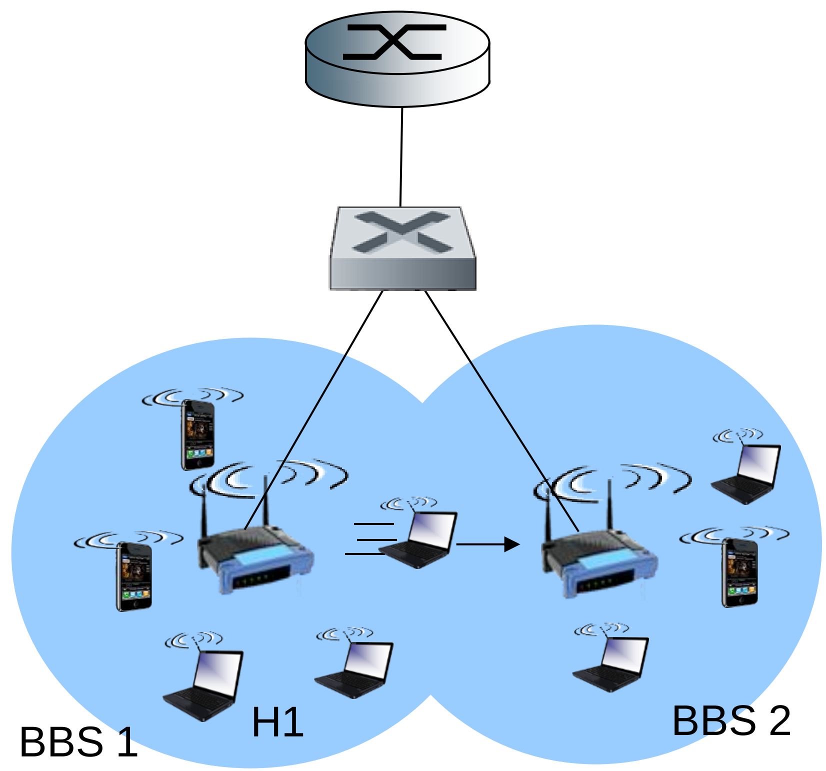


802.11 frame: more



802.11: mobility within same subnet

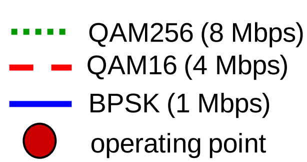
- H1 remains in same IP subnet: IP address can remain same
- switch: which AP is associated with H1?
  - self-learning : switch will see frame from H1 and "remember" which switch port can be used to reach H1

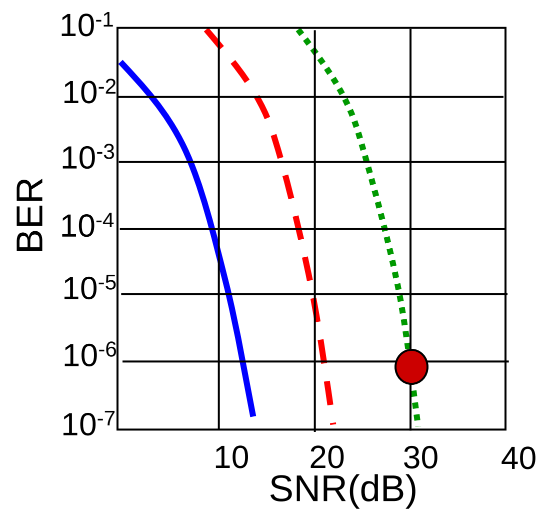


802.11: advanced capabilities

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

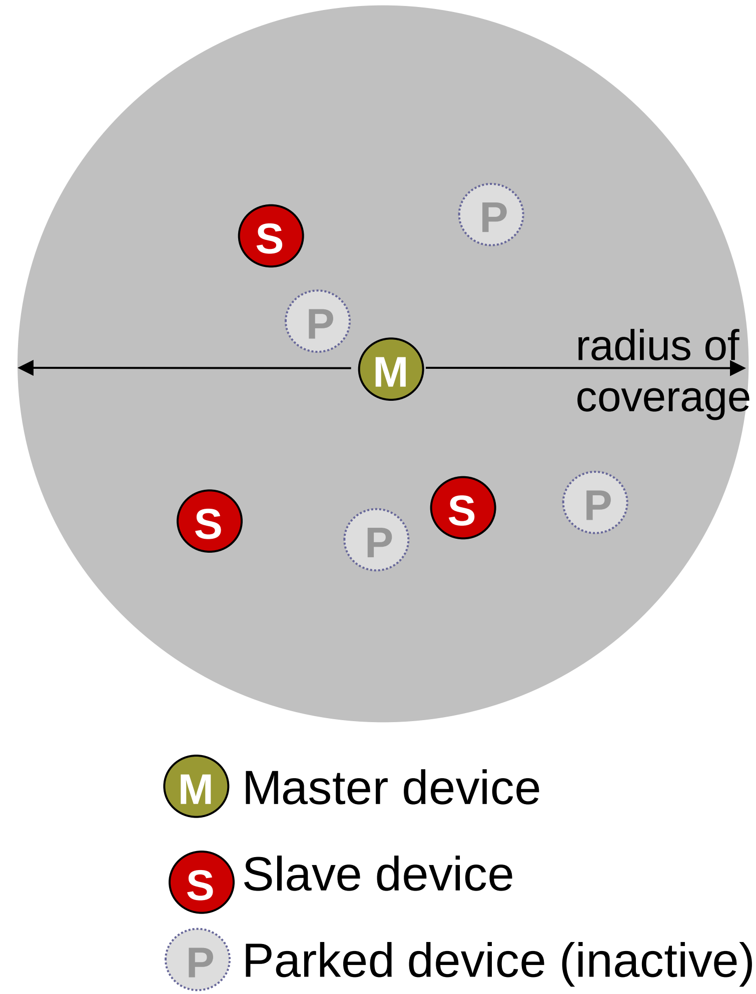
802.11: advanced capabilities

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

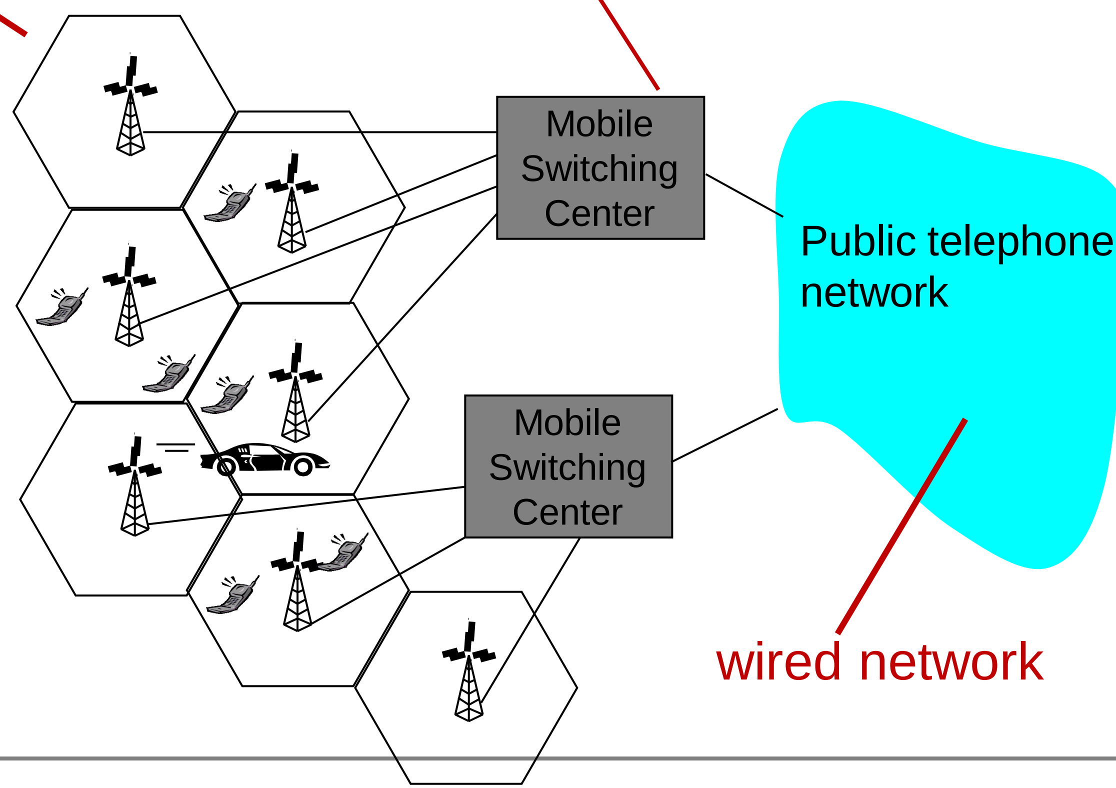
- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps



Components of cellular network architecture

MSC
- connects cells to wired tel. net.
- manages call setup (more later!)
- handles mobility (more later!)

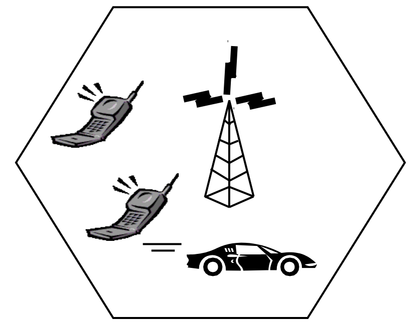
cell
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS

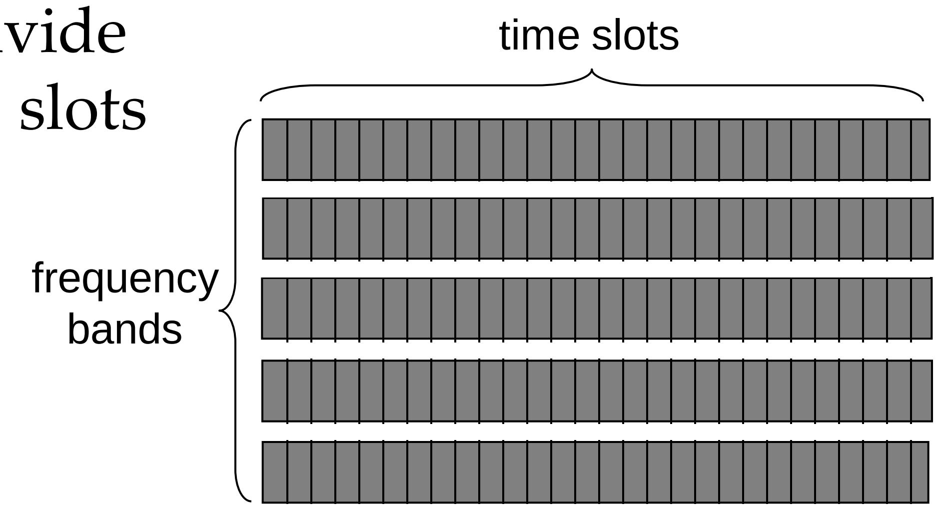


Cellular networks: the first hop

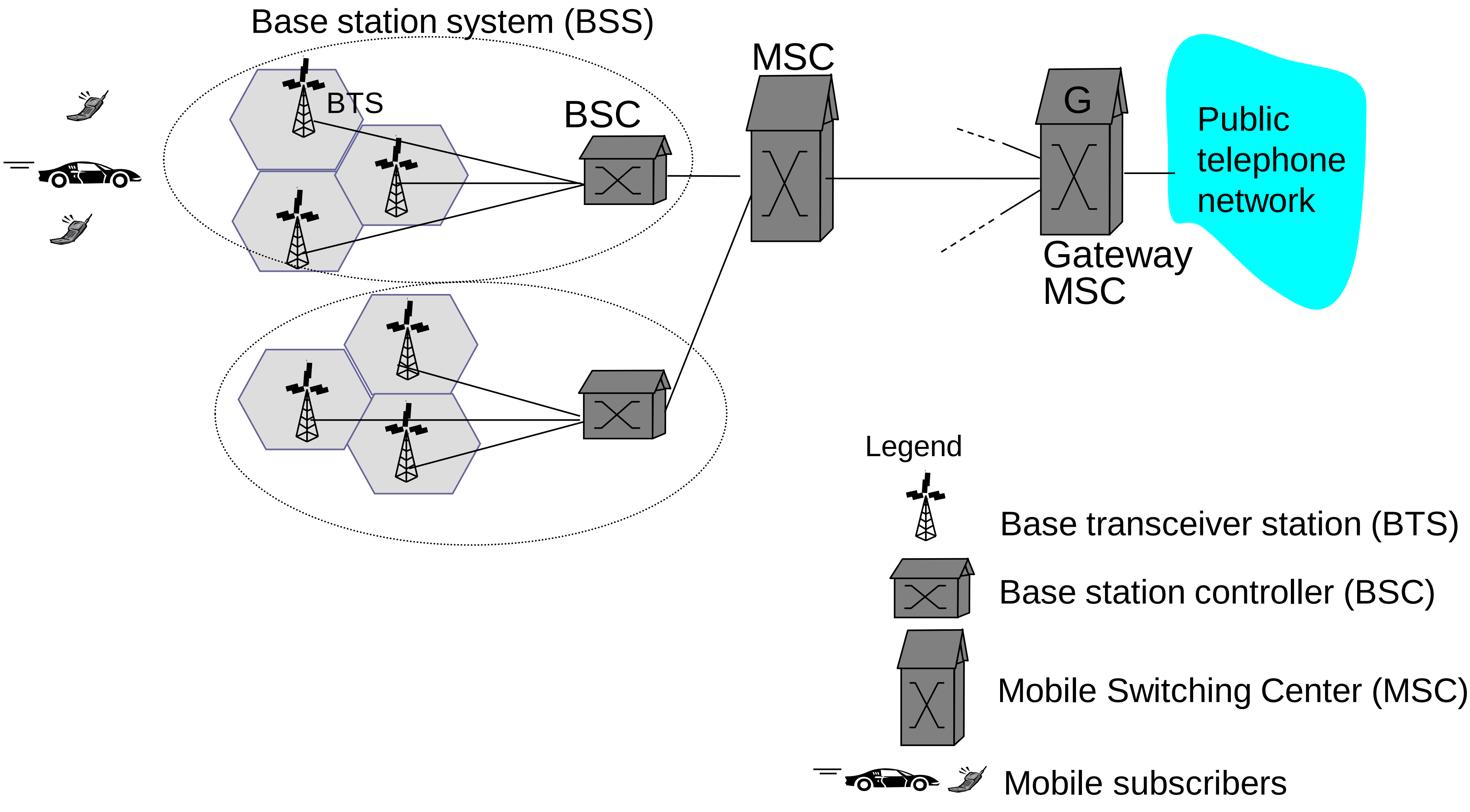
Two techniques for sharing mobile-to-BS radio spectrum

- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access

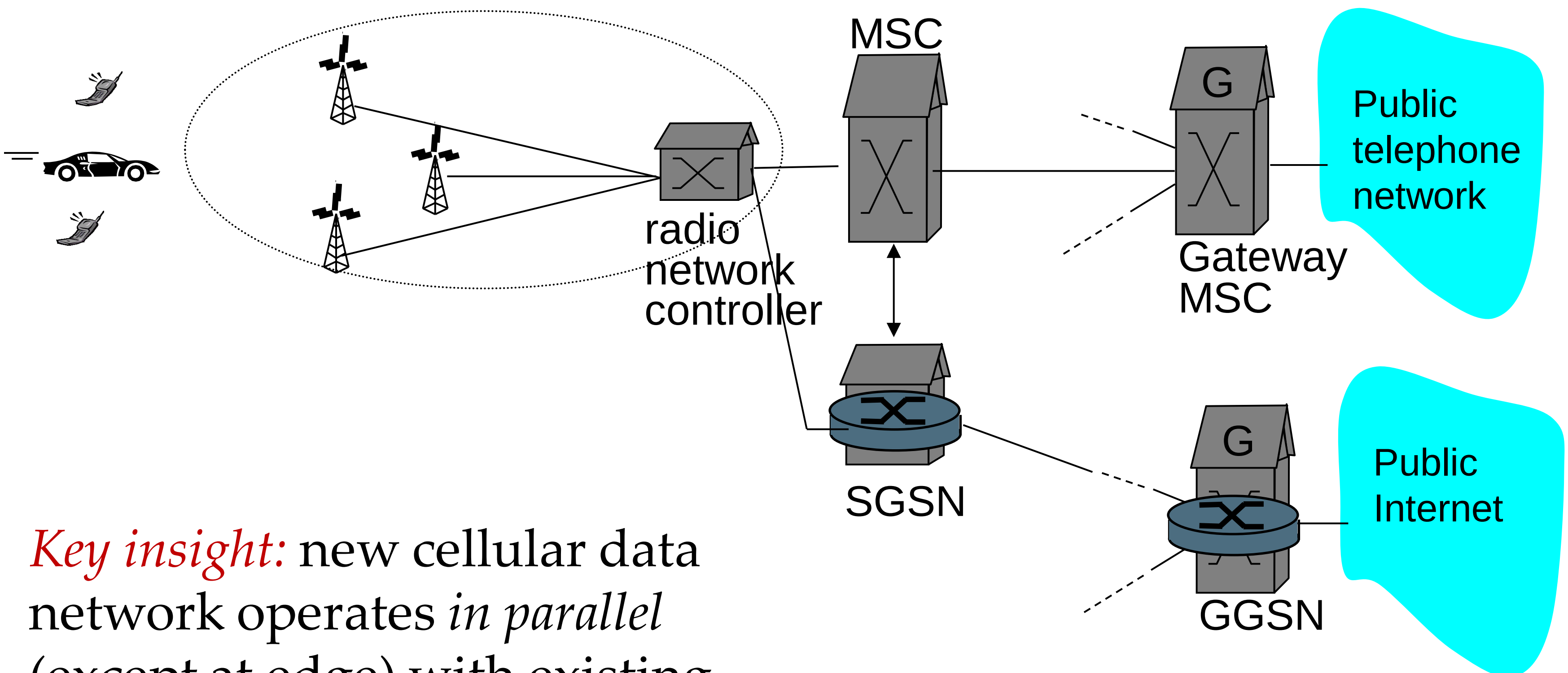




2G (voice) network architecture

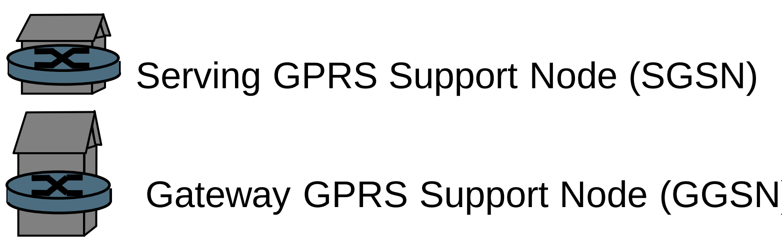


3G (voice+data) network architecture

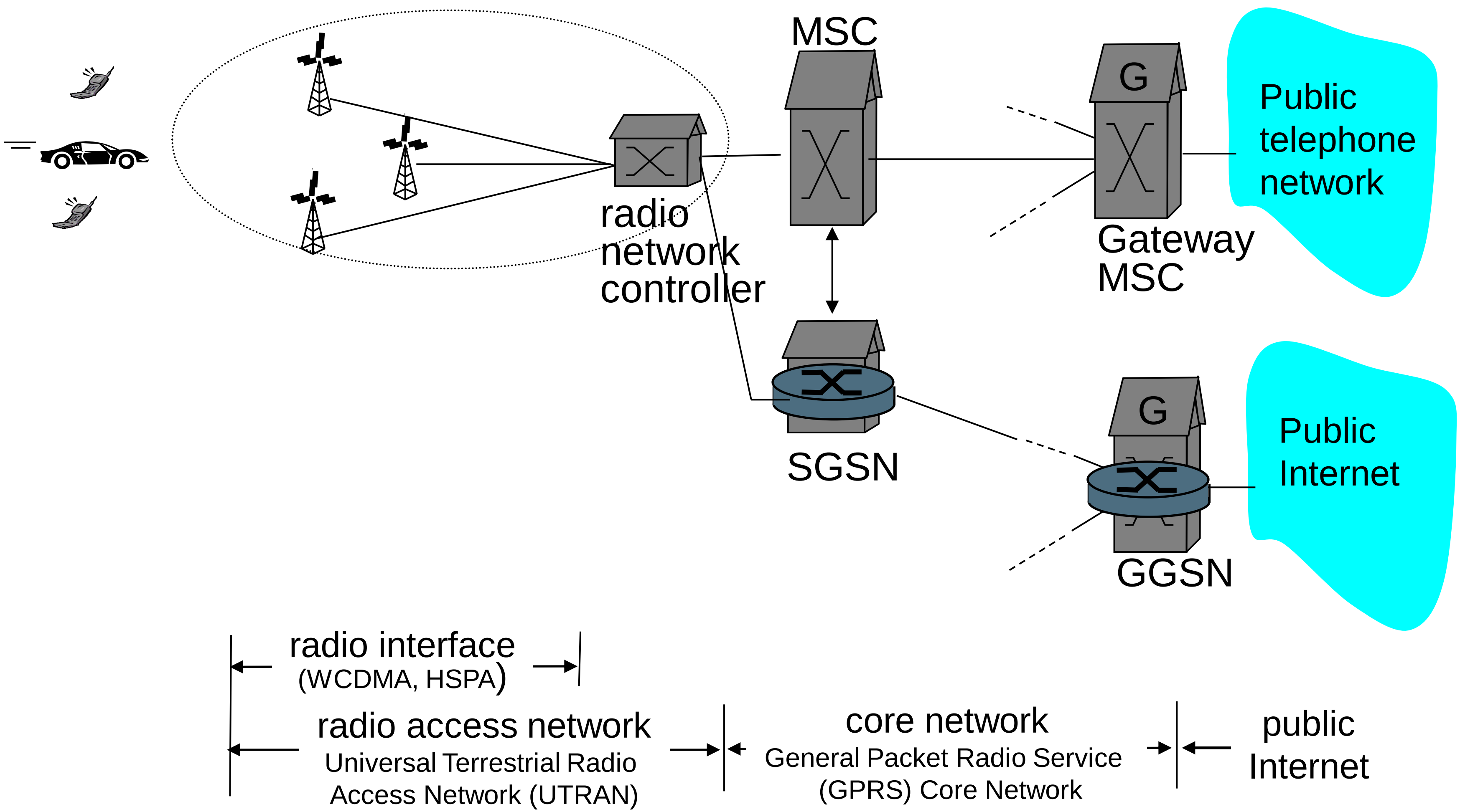


Key insight: new cellular data network operates *in parallel* (except at edge) with existing cellular voice network

- voice network unchanged in core
- data network operates in parallel

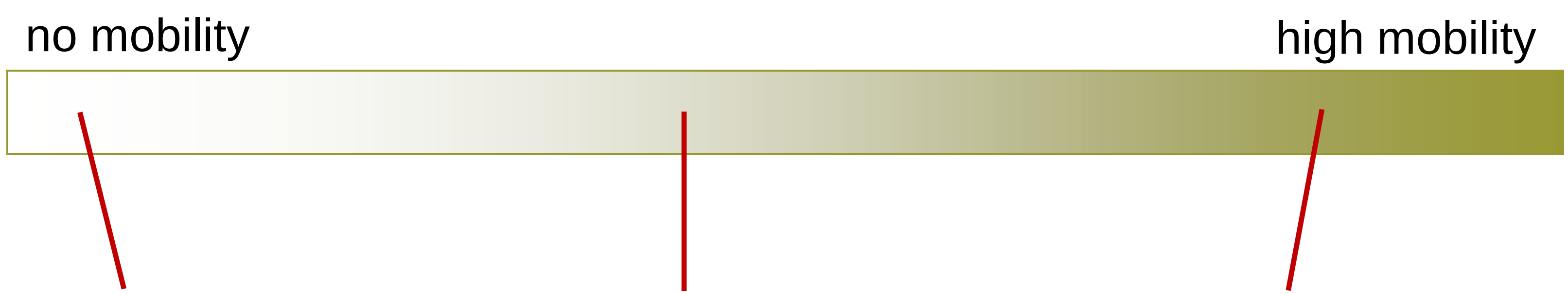


3G (voice+data) network architecture



What is mobility?

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



mobile wireless user, using same access point

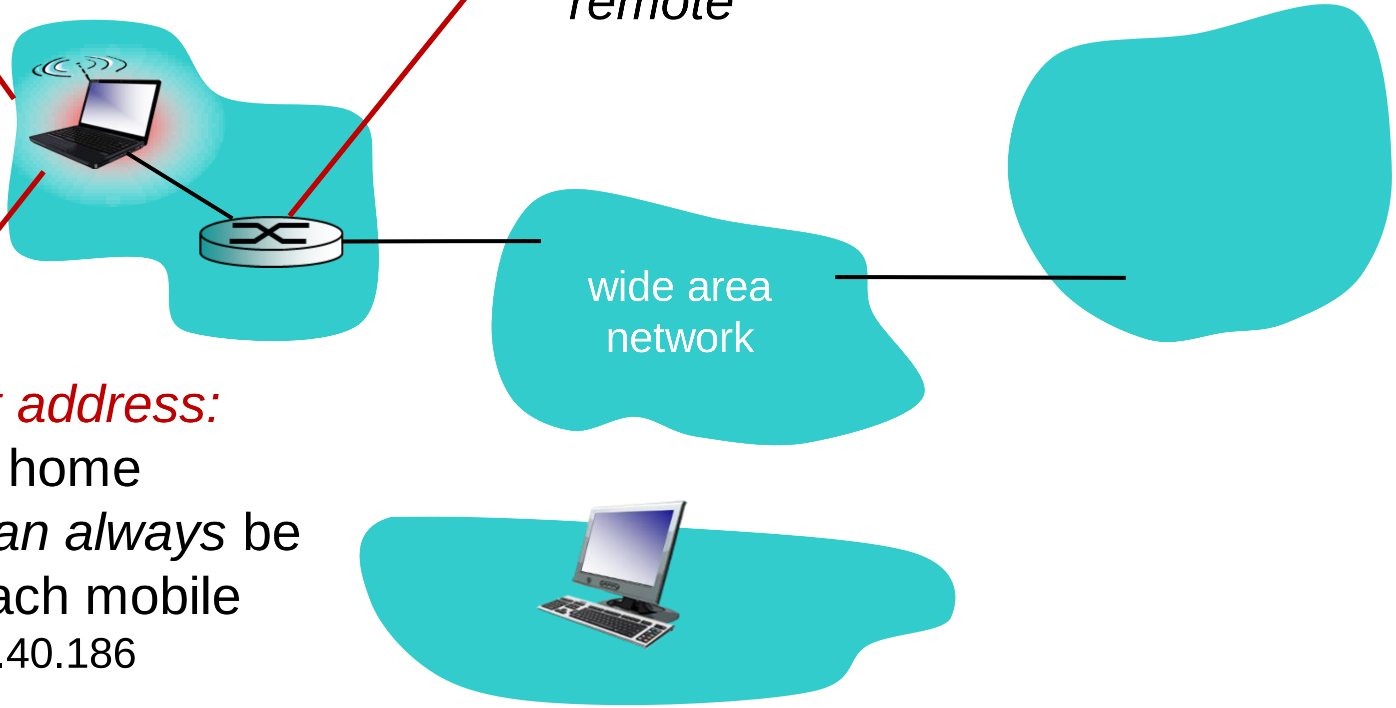
mobile user, connecting/ disconnecting from network using DHCP.

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

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



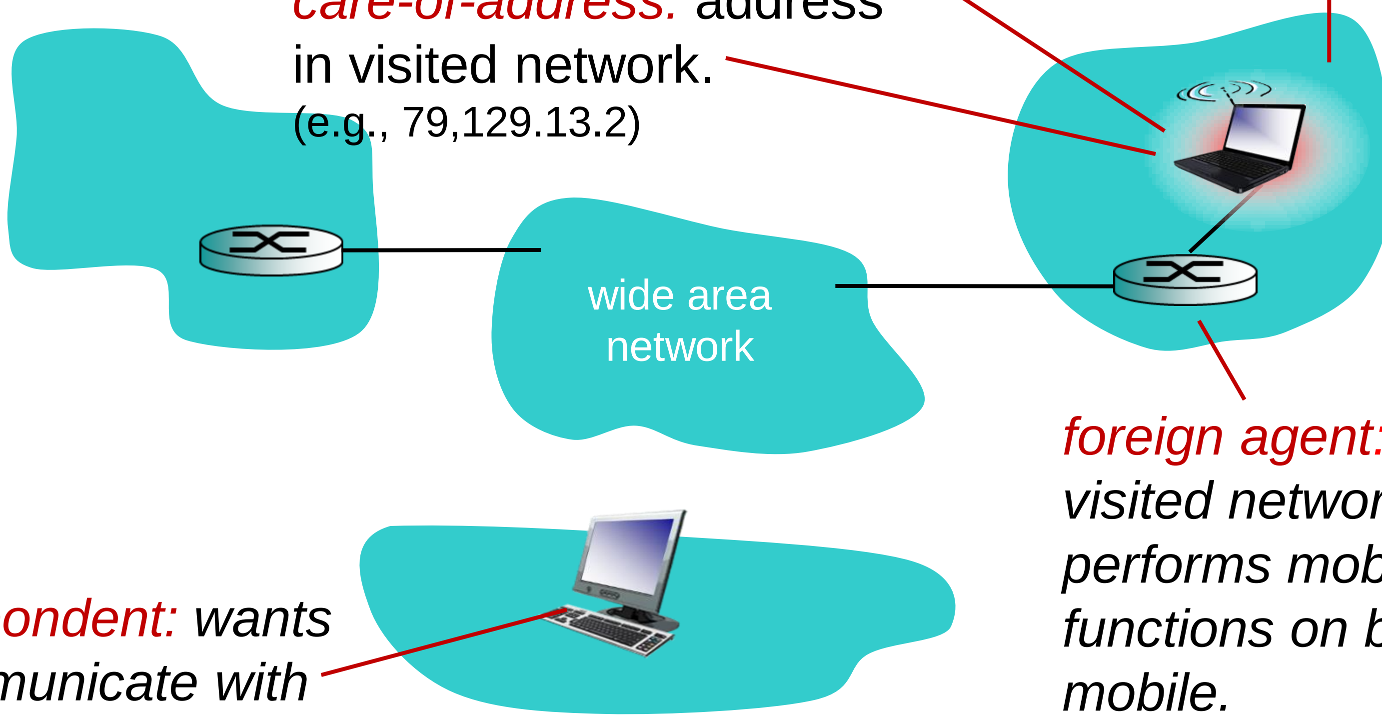
permanent address:
address in home network, *can always* be used to reach mobile
e.g., 128.119.40.186

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)



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

correspondent: wants to communicate with mobile

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

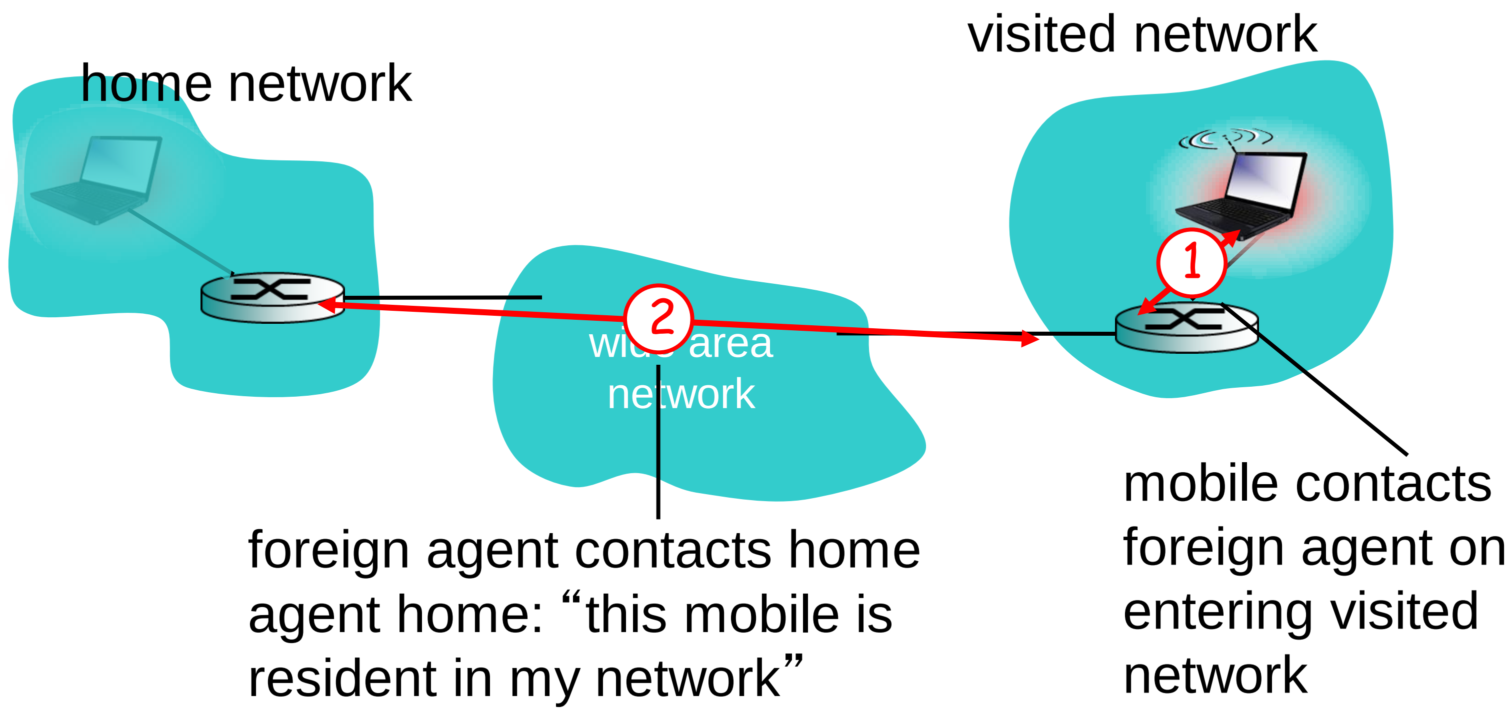
Mobility: approaches

- *let routing handle it:* routers advertise permanent address of mobile-nodes-in-r[illegible]e via usual routing table exchange.
  - routing table[illegible]ere each mobile located
  - no changes to [illegible]ns

not scalable to millions of mobiles

- *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

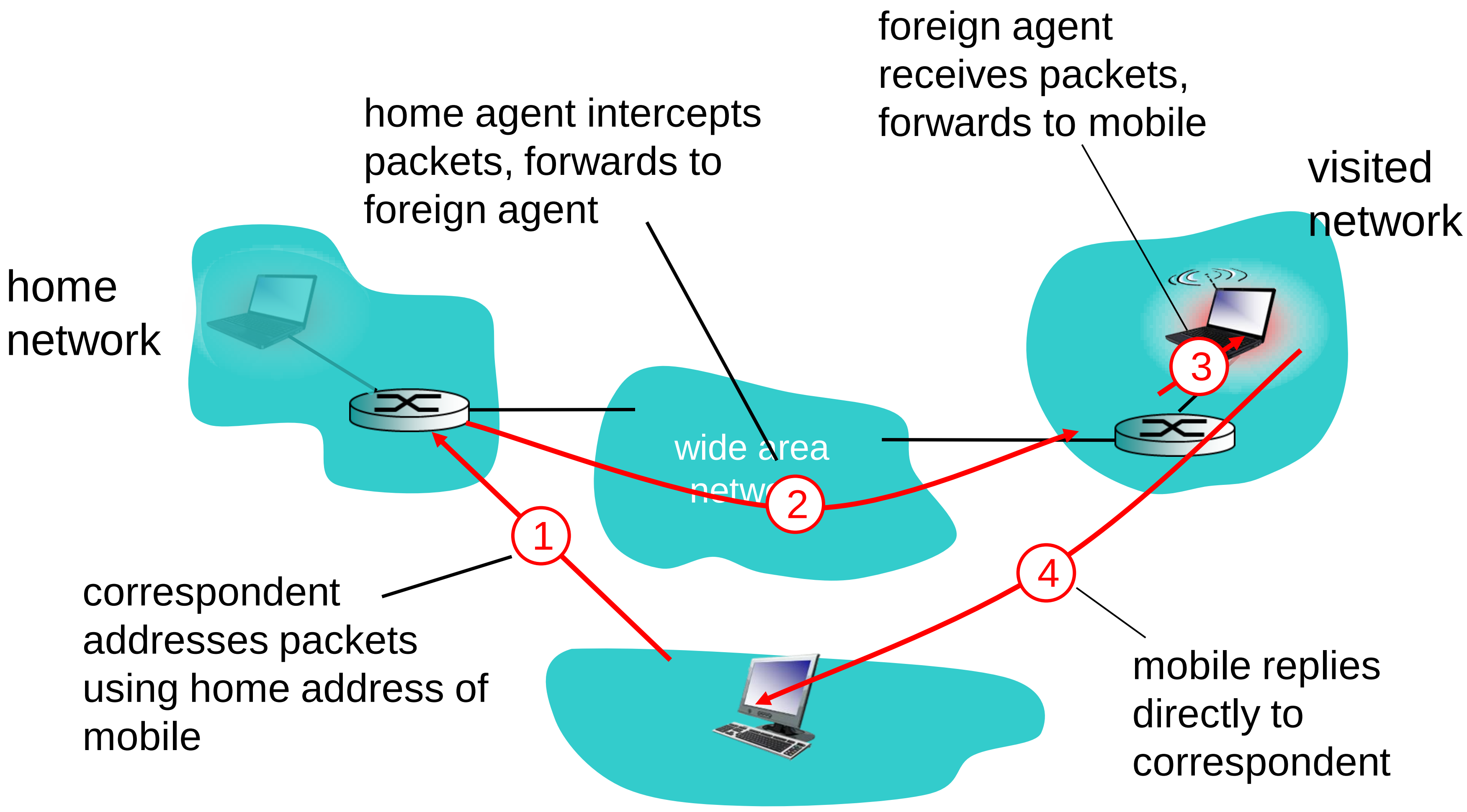
Mobility: registration



end result:

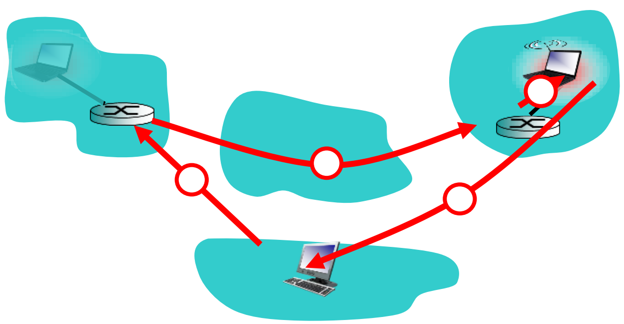
- foreign agent knows about mobile node
- home agent knows location of mobile node

Mobility via indirect routing



Indirect Routing: comments

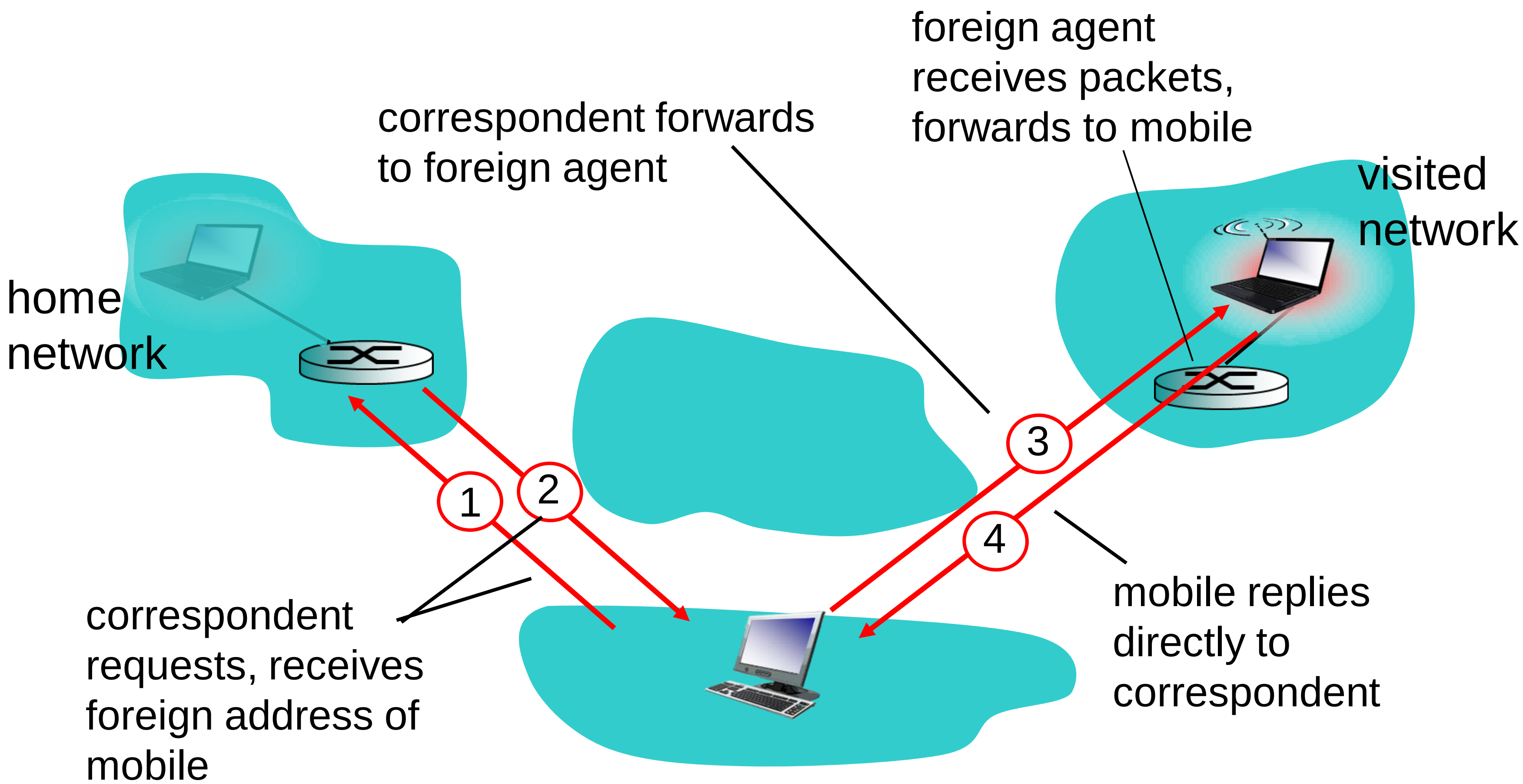
- mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile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



Indirect routing: moving between networks

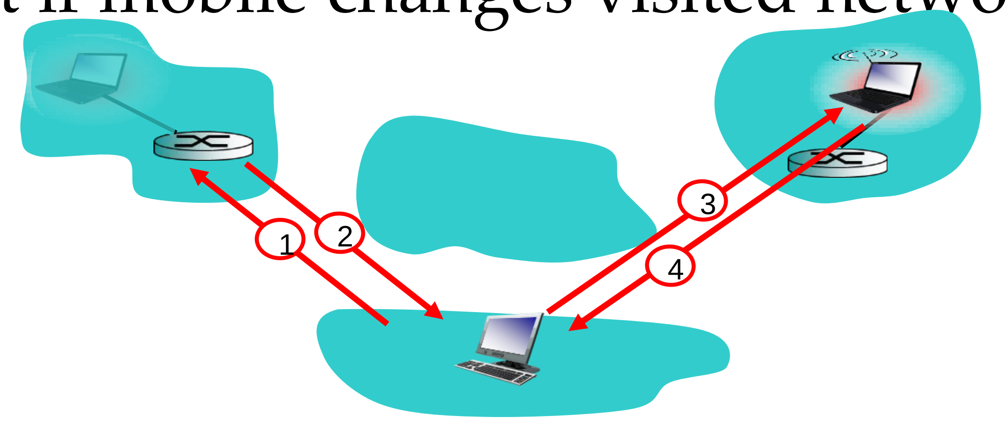
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: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

Mobility via direct routing



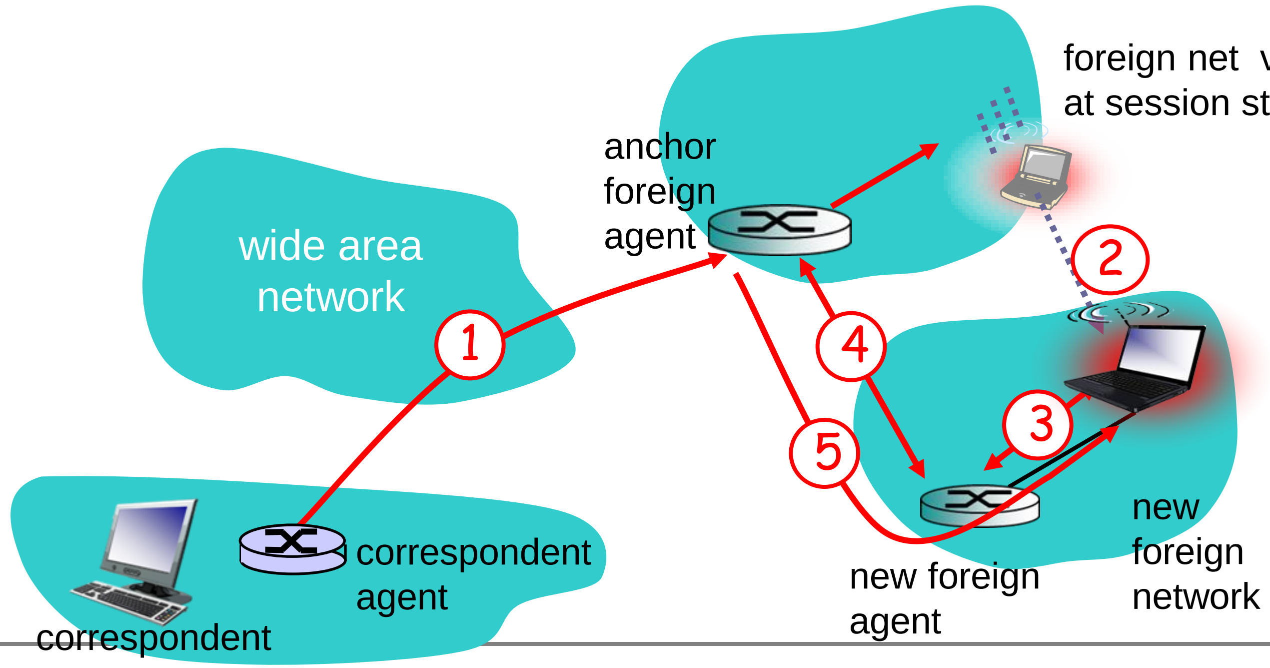
Mobility via direct routing: comments

- 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

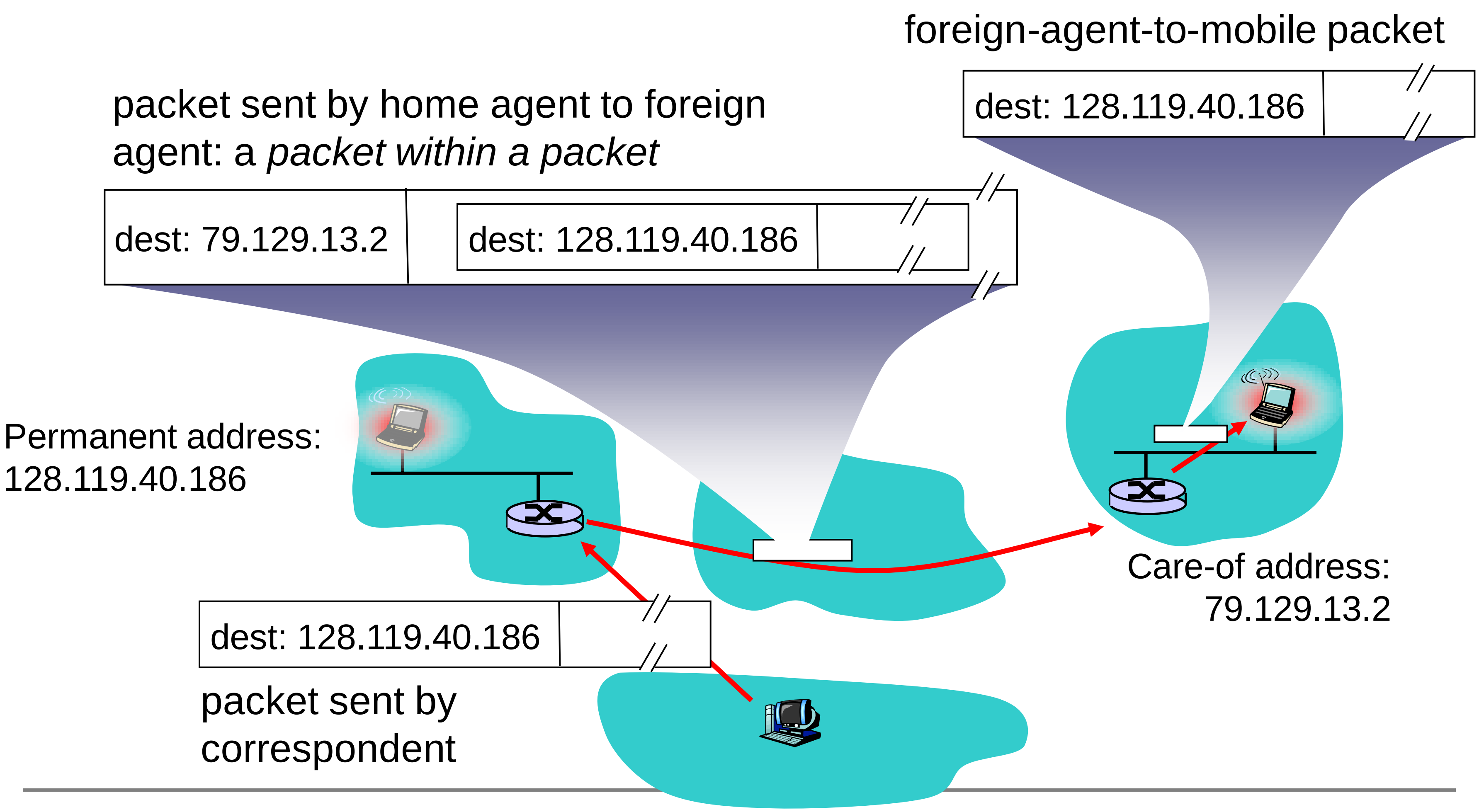
- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining)



Mobile IP

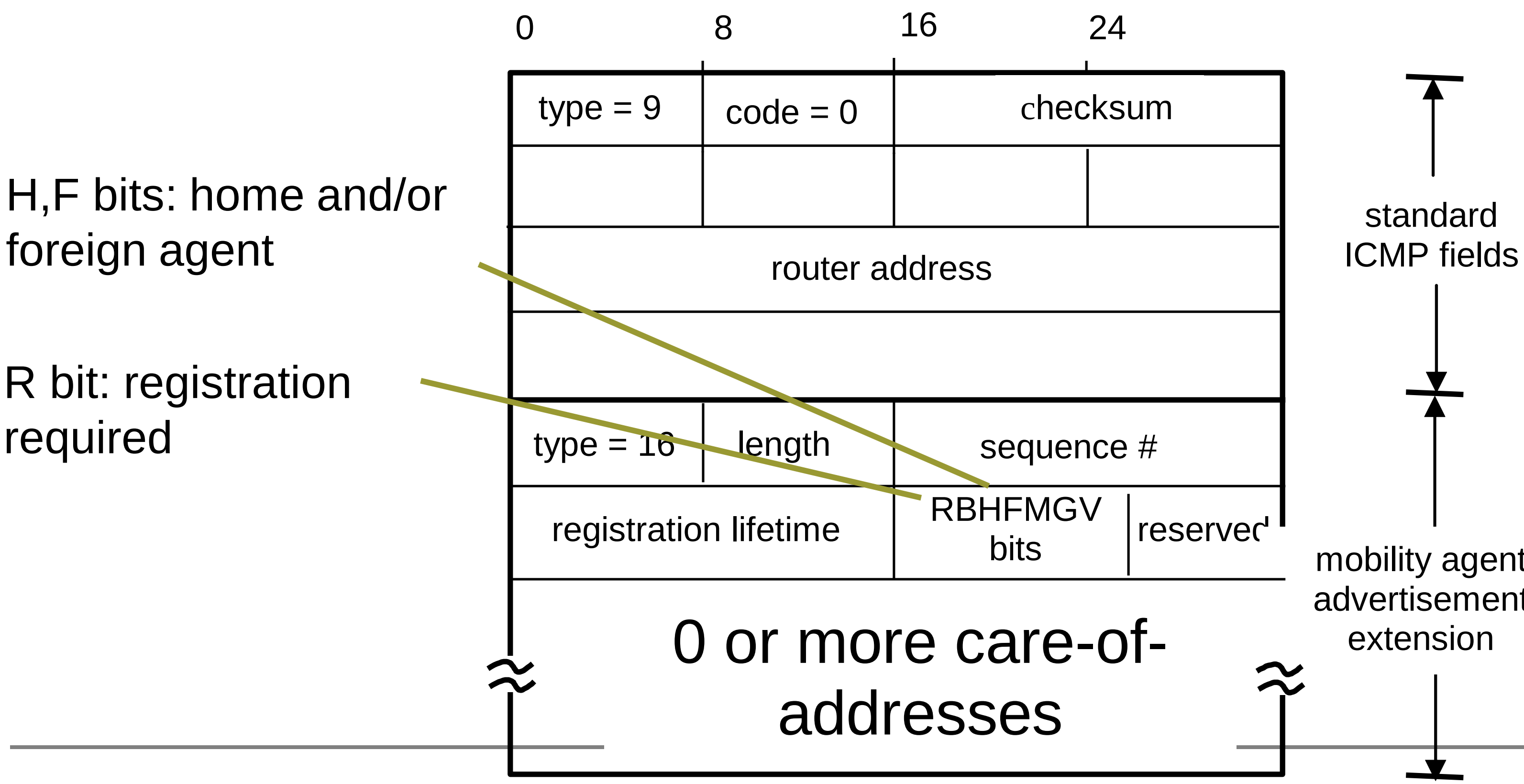
- RFC 3344
- has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent

Mobile IP: indirect routing

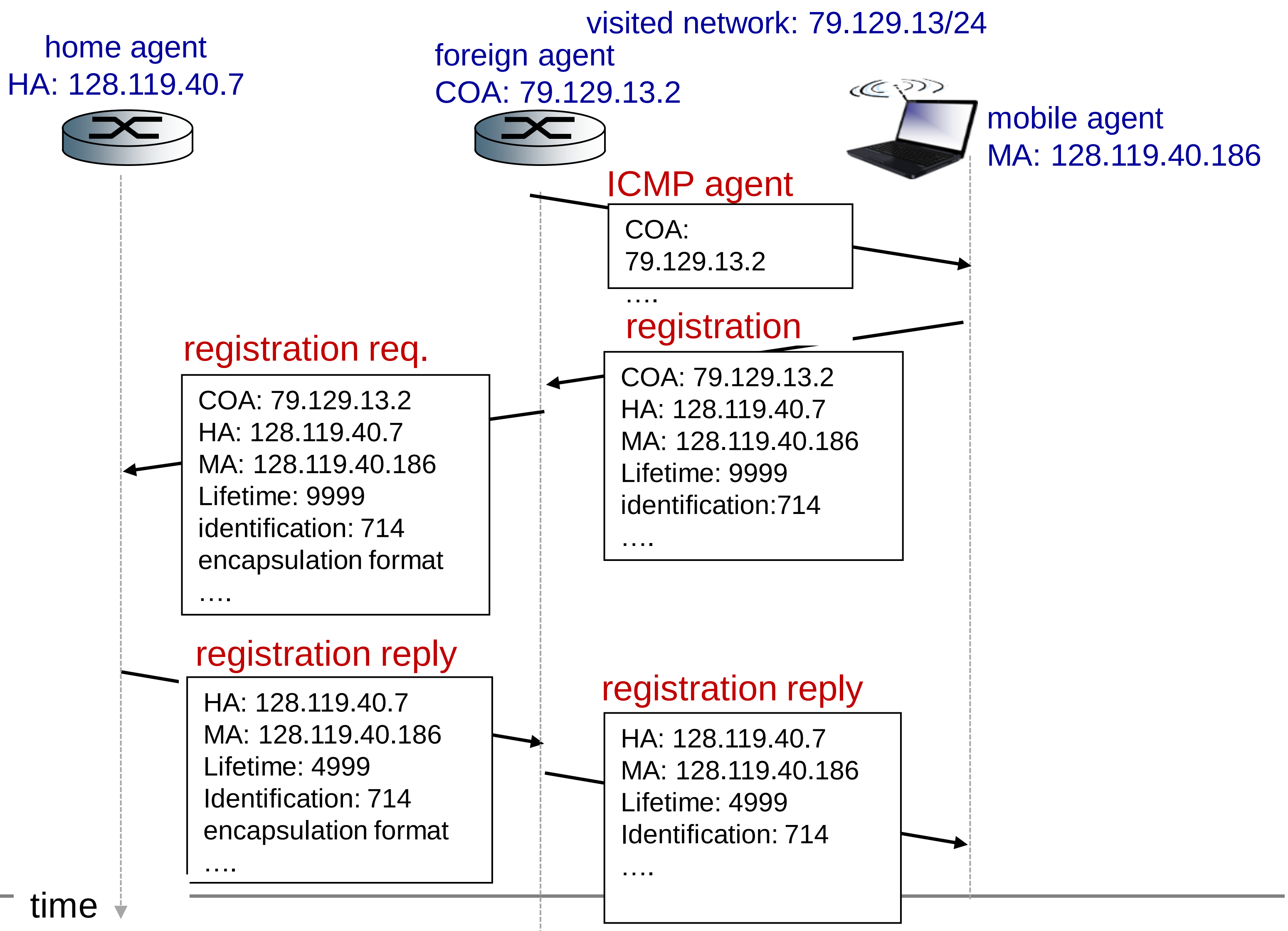


Mobile IP: agent discovery

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

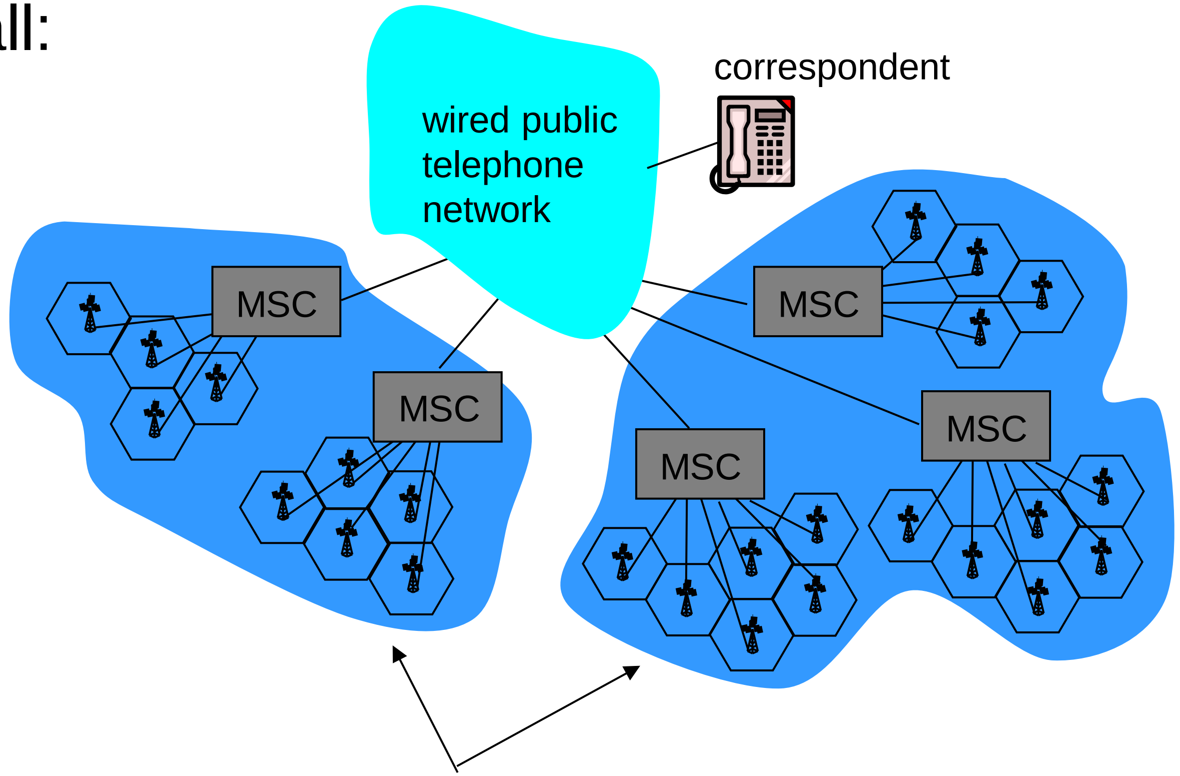


Mobile IP: registration example



Components of cellular network architectu

recall:

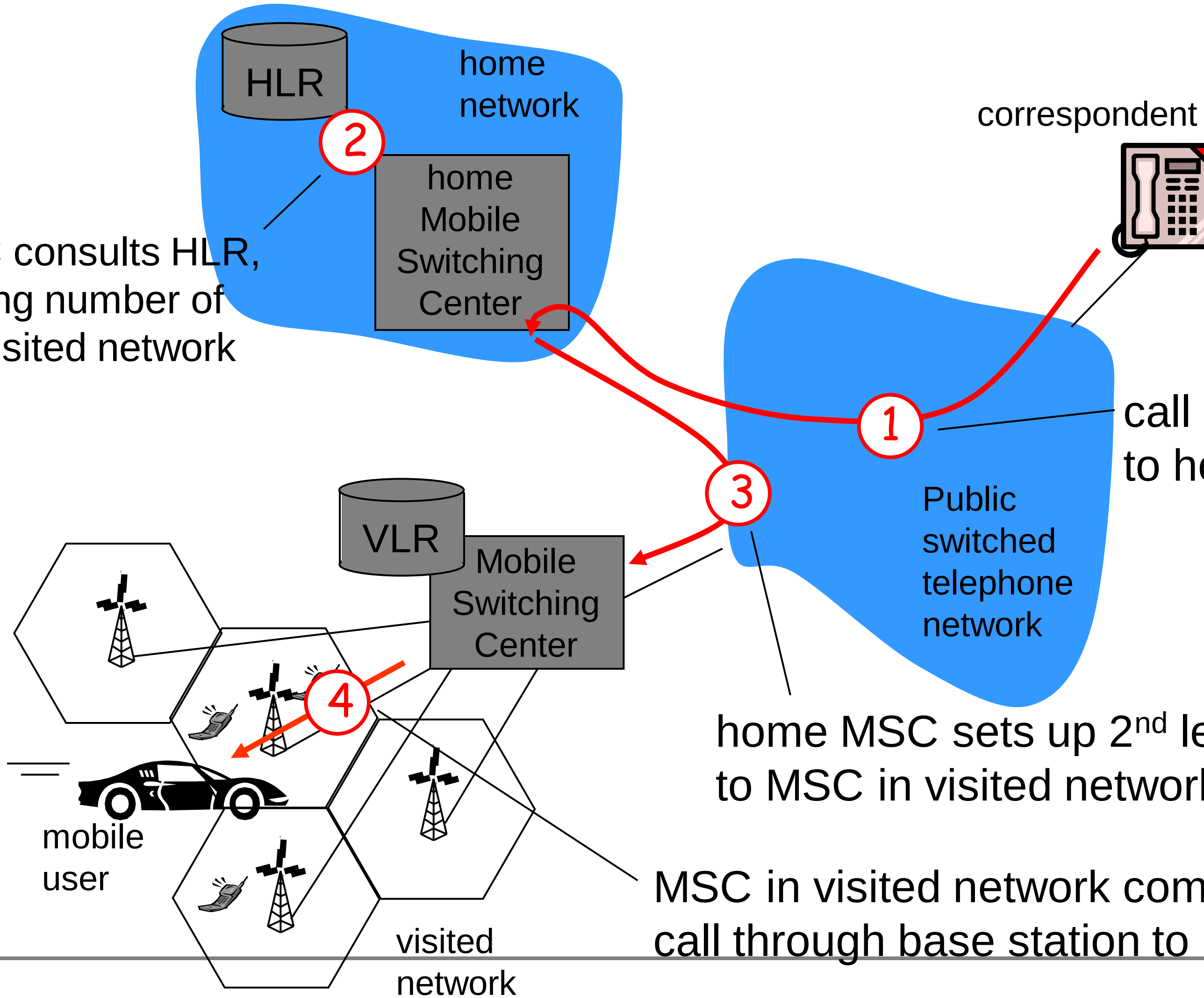


different cellular networks,
operated by different providers

Handling mobility in cellular networks

- *home network:* network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- *visited network:* network in which mobile currently resides
  - *visitor location register (VLR):* database with entry for each user currently in network
  - could be home network

GSM: indirect routing to mobile



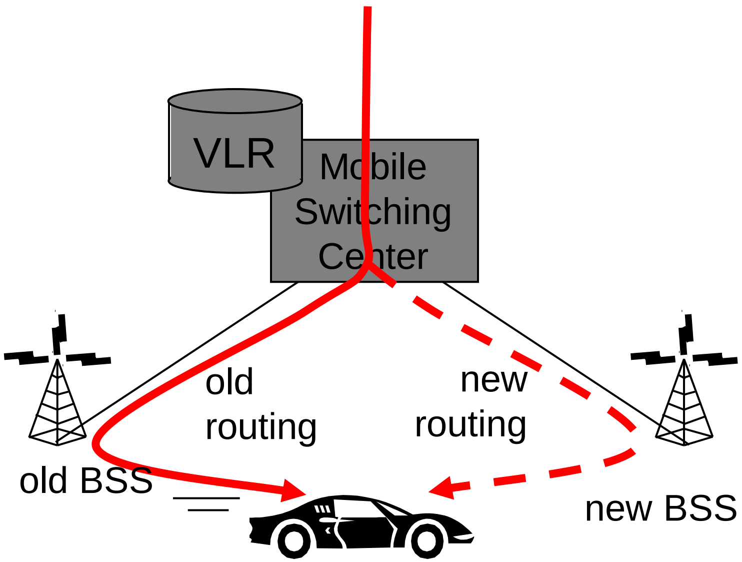
home MSC consults HLR, gets roaming number of mobile in visited network

call routed to home network

home MSC sets up 2nd leg of call to MSC in visited network

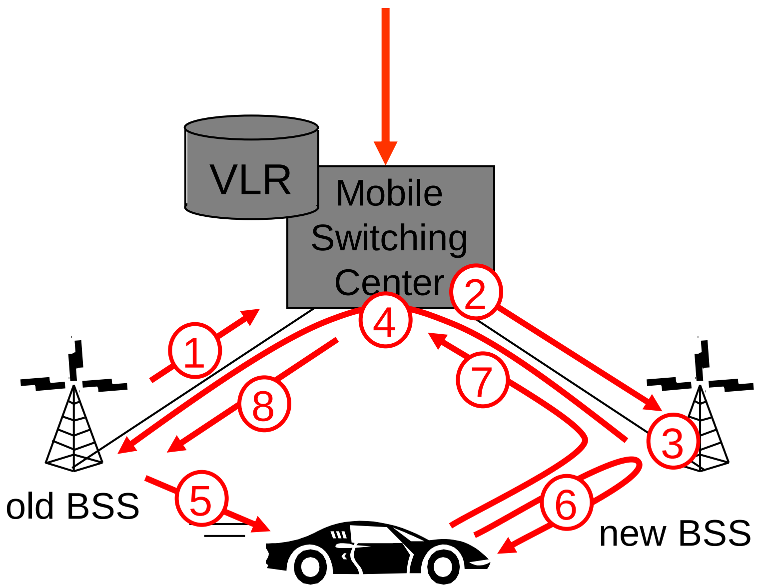
MSC in visited network completes call through base station to mobile

GSM: handoff with common MSC



- *handoff goal:* route call via new base station (without interruption)
- reasons for handoff:
  - stronger signal to/from new BSS (continuing connectivity, less battery drain)
  - load balance: free up channel in current BSS
  - GSM doesnt mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

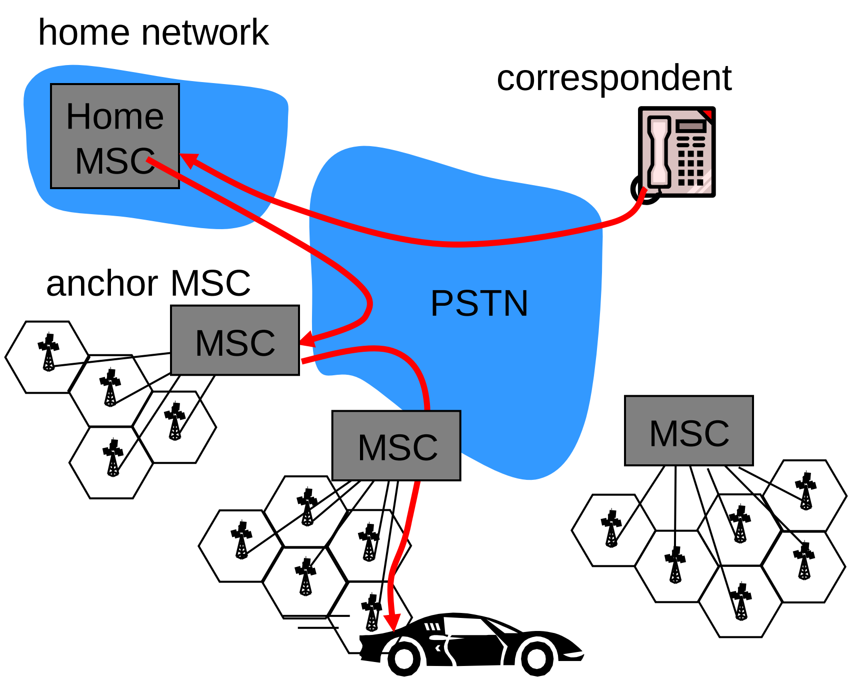
GSM: handoff with common MSC



1. old BSS informs MSC of impending handoff, provides list of 1^+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to activate new channel
7. mobile signals via new BSS to MSC: handoff complete. MSC reroutes call

8 MSC-old-BSS resources released

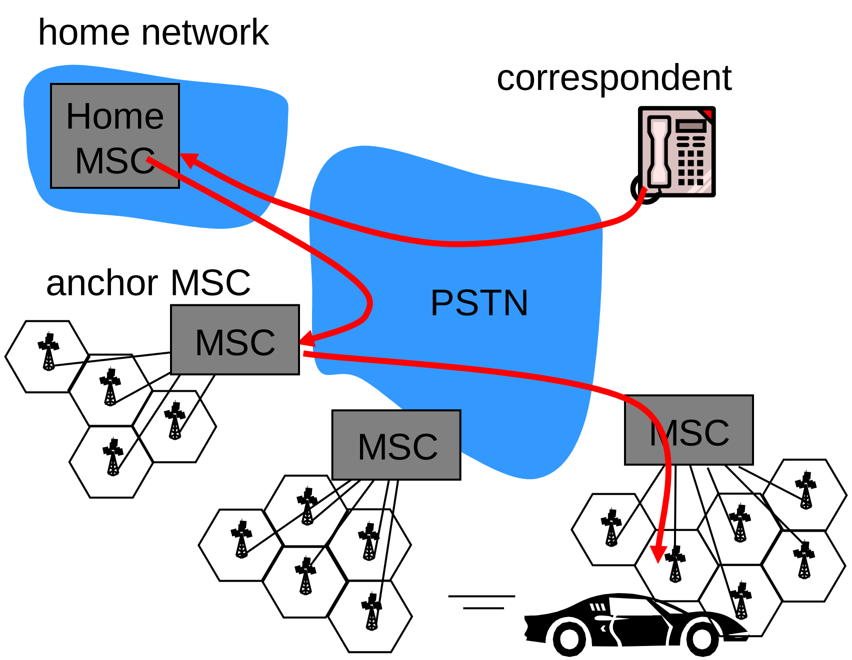
GSM: handoff between MSCs



(a) before handoff

- *anchor MSC:* first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

GSM: handoff between MSCs



(b) after handoff

- *anchor MSC:* first MSC visited during call
  - call remains routed through anchor MSC
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- optional path minimization step to shorten multi-MSC chain

Mobility: GSM versus Mobile IP

GSM element	Comment on GSM element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	**Home agent**
Visited System	Network other than home system where mobile user is currently residing	**Visited network**
Visited Mobile services Switching Center. Visitor Location Record (VLR)	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	**Foreign agent**
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	**Care-of-address**

Wireless, mobility: impact on higher layer protocols

- logically, impact *should* be minimal …
  - best effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- … but performance-wise:
  - packet loss/delay due to bit-errors (discarded packets, delays for link-layer retransmissions), and handoff
  - TCP interprets loss as congestion, will decrease congestion window un-necessarily
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links

Mobile & Wireless Networks

Ad hoc networks

- mobile ad hoc networks (MANETs)
- vehicular ad hoc networks (VANETs)

Wireless Sensor Networks (WSN)

Mobile Ad hoc Networks (MANETs)

Self configuring network of mobile nodes connected by wireless links

Provide communication in the absence of a fixed infrastructure

Dynamic topology due to mobility

Attractive for many applications
- disaster recovery operations
- military applications

Vehicular Ad hoc Networks (VANETs)

- Ad hoc network composed of vehicles
- Individual nodes different from traditional wireless nodes
  - No power constraint
  - Nodes mostly mobile
- Complements existing infrastructure
- Extends existing infrastructure

Applications

- Traffic control
  - Automatic speed limit enforcement
  - Rerouting in traffic congestion
- Safety
  - Notification of accident up ahead
  - Decentralized 911 service
  - Prioritized over non-safety applications
- Extended communication

- Will become the largest ad hoc network.

VANET

Two type of communication:

- V2V : vehicle to vehicle
- V2I : vehicle to infrastructure

Basic Components I

OBU : on-board unit

A device inside the vehicle

- Processes the data collected from various sensors fitted inside the vehicle and gives information about the condition of the vehicle

- Responsible for communication with the outside network (other vehicles, infrastructure)

Basic Components II

RSU : roadside unit

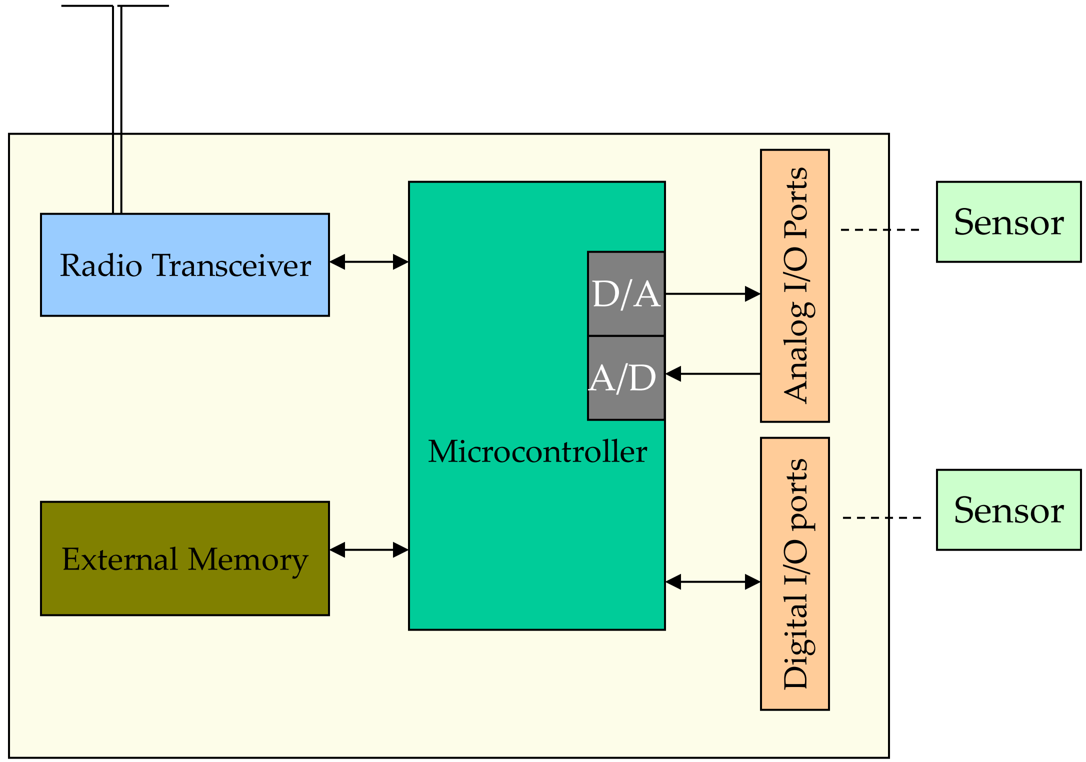
- RSU acts similar to a wireless LAN access point and can provide communications with infrastructure.

Wireless Sensor Network

*"A **wireless sensor network** (WSN) is a wireless network consisting of spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations."*

- Wikipedia

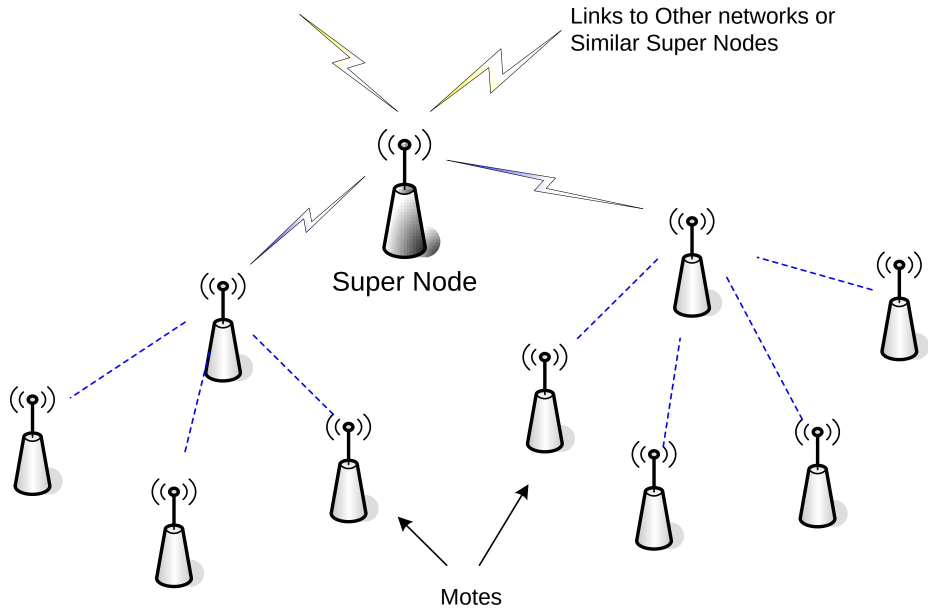
Mote



- A very low cost low power computer
- Monitors one or more sensors
- A Radio Link to the outside world
- Are the building blocks of Wireless Sensor Networks (WSN)

Wireless Sensor Networks

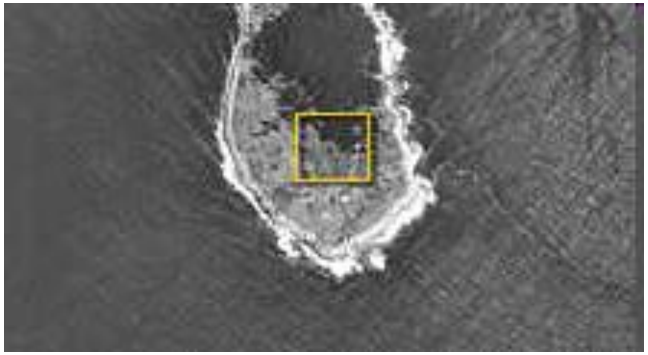
- Formed by hundreds or thousands of motes that communicate with each other and pass data along from one to another
- Research done in this area focus mostly on energy aware computing and distributed computing



WSN Applications

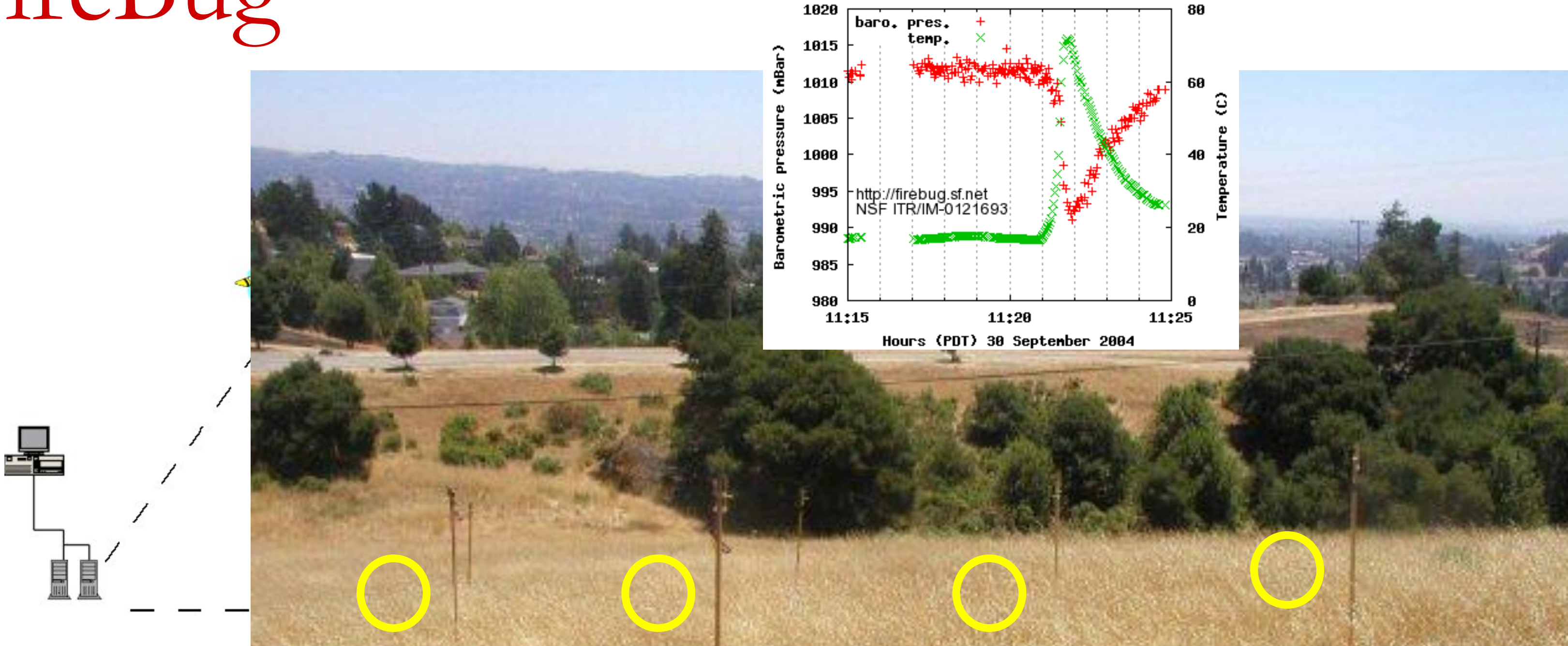
- Environmental/Habitat monitoring
- Acoustic detection
- Seismic Detection
- Military surveillance
- Inventory tracking
- Medical monitoring
- Smart spaces
- Process Monitoring

Habitat Monitoring on Great Duck Island



- http://www.greatduckisland.net/
- Intel Research Laboratory at Berkeley initiated a collaboration with the College of the Atlantic in Bar Harbor and the University of California at Berkeley to deploy wireless sensor networks on Great Duck Island, Maine (in 2002)
- Monitor the microclimates in and around nesting burrows used by the Leach's Storm Petrel
- Goal : habitat monitoring kit for researchers worldwide

FireBug



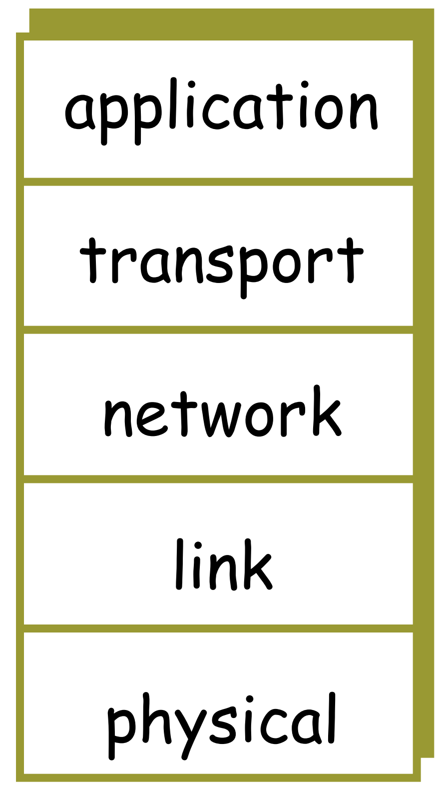
- Wildfire Instrumentation System Using Networked Sensors
- Allows predictive analysis of evolving fire behavior
- Firebugs: GPS-enabled, wireless thermal sensor motes based on TinyOS that self-organize into networks for collecting real time data in wild fire environments
- Software architecture: Several interacting layers (Sensors, Processing of sensor data, Command center)
- A project by University of California, Berkeley CA.

Preventive Maintenance on an Oil Tanker in the North Sea: The BP Experiment

- Collaboration of Intel & BP
- Use of sensor networks to support preventive maintenance on board an oil tanker in the North Sea.
- A sensor network deployment onboard the ship
- System gathered data reliably and recovered from errors when they occurred.
- The project was recognized by InfoWorld as one of the top 100 IT projects in 2004,

Internet protocol stack

- application: supporting network applications
  - FTP, SMTP
- transport: host-host data transfer
  - TCP, UDP
- network: routing of datagrams from source to destination
  - IP, routing protocols, mobile IP, DHCP
- link: data transfer between neighboring network elements
  - PPP, Ethernet, WLAN
- physical: bits "on the wire"



Reading

Chapter 5-6

‘Computer Networks: A top-down approach’, by Kurose and Ross, 6th Edition, Addison-Wesley