Wireless and Mobile

To do ...

- Wireless concepts
- 802.11 and cell networks
- Mobility and its challenges

Slides partially based on J. Kurose and K. Ross, "Computer Networking: A Top Down Approach", 7Ed., 2016

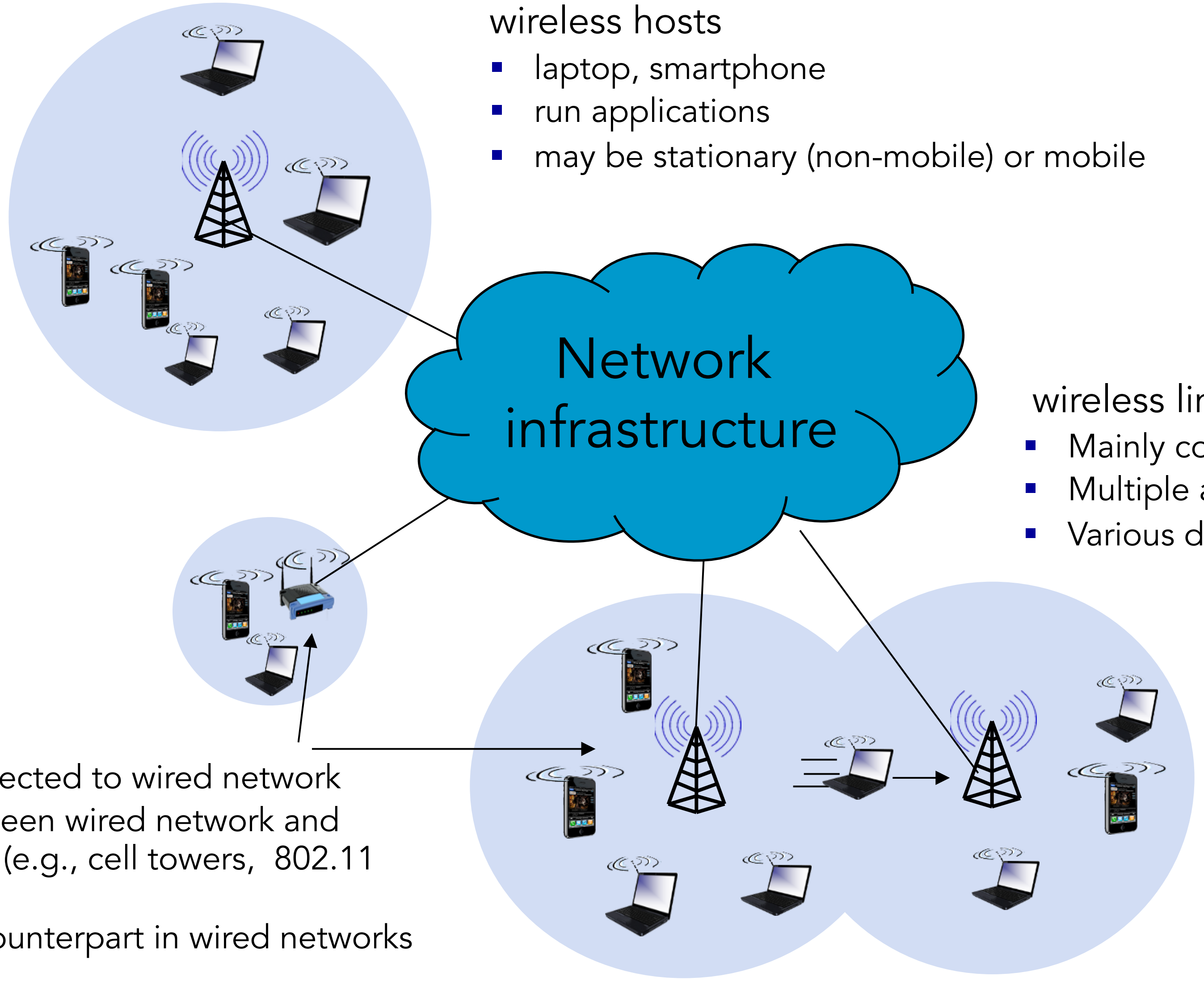
Northwestern

Wireless and mobile networks

- Number of wireless (mobile) phone subscribers now exceeds number wired phone subscribers
- Number of wireless Internet-connected devices >> than wireline Internet-connected devices*
  - Largest growth in M2M connections, followed by phones, TV/consoles
  - PCs continue to decline at ~3% rate
- By 2022, wireless will account for 71% of IP traffic (52% in 2017)*
- Two important (but different) challenges
  - Wireless: communication over wireless link
  - Mobility: handling the mobile user who changes point of attachment to network

*Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper

Elements of a wireless network



wireless hosts

- laptop, smartphone
- run applications
- may be stationary (non-mobile) or mobile

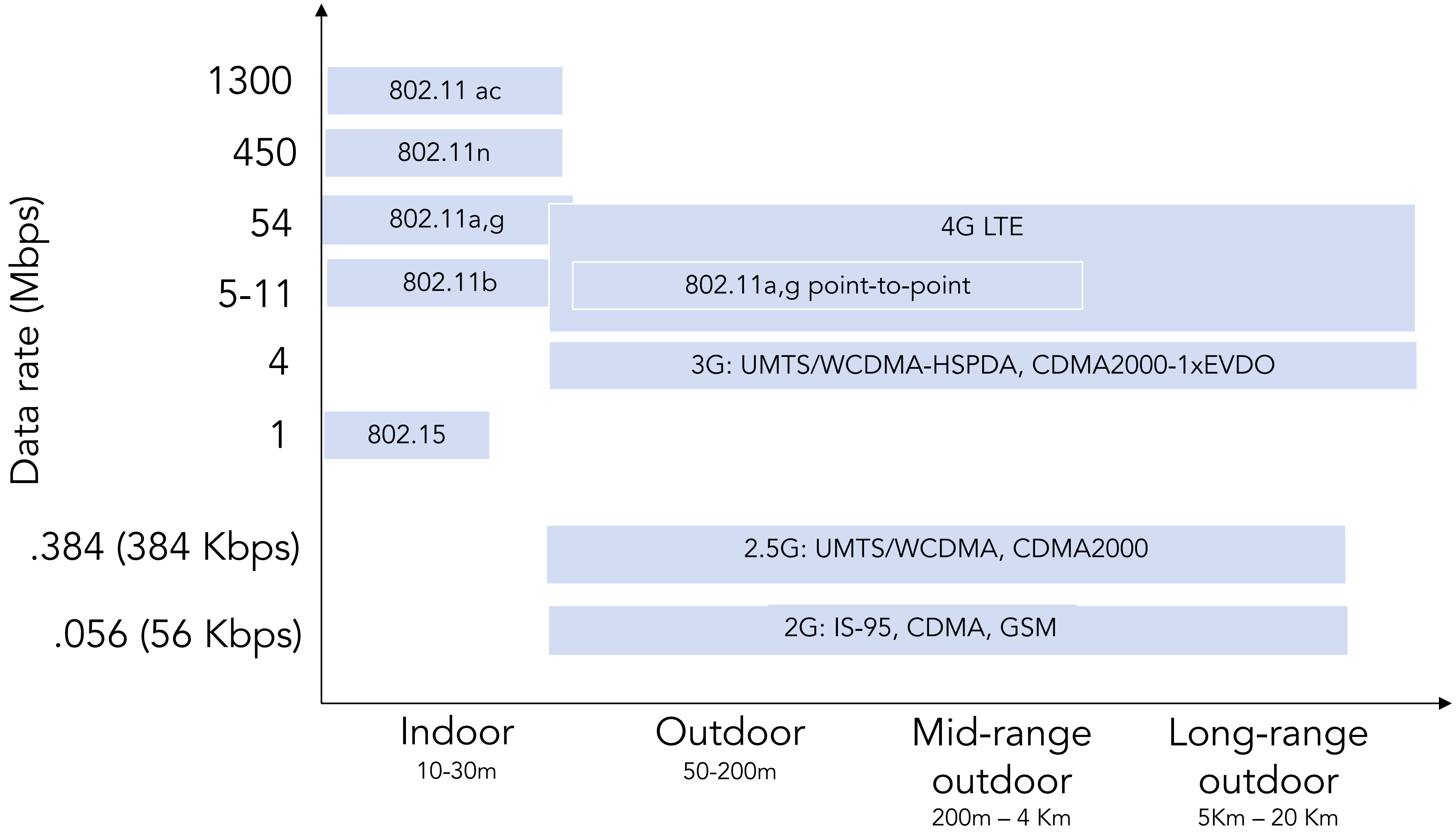
wireless link

- Mainly connecting mobile nodes to base station
- Multiple access protocol coordinates link access
- Various data rates, transmission distanc

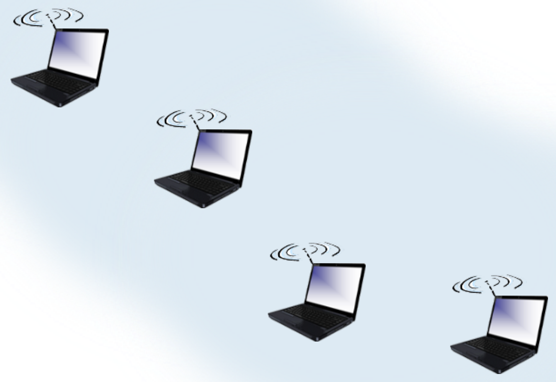
base station

- Typically connected to wired network
- Relaying between wired network and wireless hosts (e.g., cell towers, 802.11 access points)
- No obvious counterpart in wired networks

Characteristics of selected wireless links



Infrastructure and ad-hoc modes

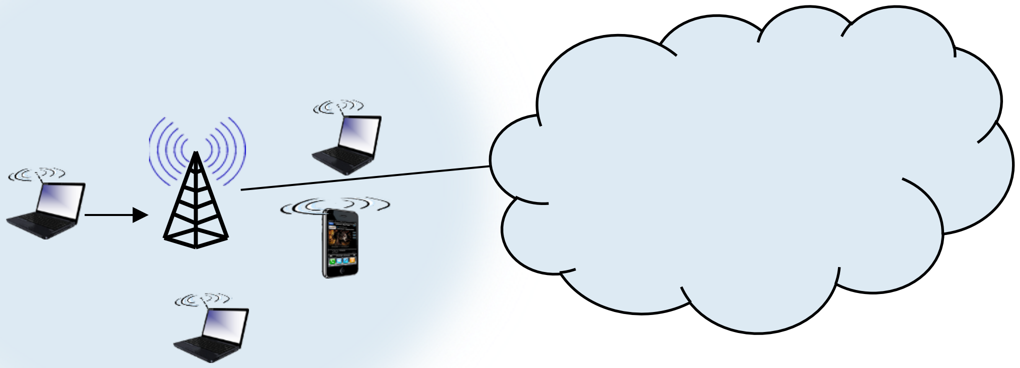


ad hoc mode

- no base stations
- nodes can only transmit to other within range
- must organize themselves into a network and route

infrastructure mode

- Base station connects mobiles into wired network
- Mobile devices changes base station (handoff) providing connection =



Combining the pieces – a taxonomy

	single hop	multiple hops
Infrastructure (e.g., APs)	Host connects to a base station (Access Point in WiFi) which connects to larger Internet – *802.11, 4G LTE*	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, one coordinator – *Bluetooth, 802.11 in ad hoc mode*	No base station, no connection to larger Internet. May have to relay to reach others, and all may be mobile – *MANET, VANET*

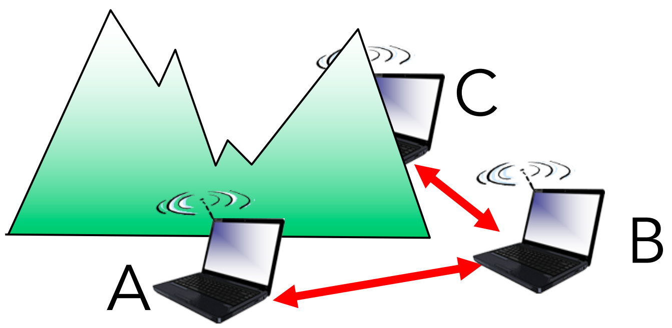
Wireless link characteristics

- Important differences from wired link ….
  - Decreased signal strength: It attenuates as it propagates through matter (path loss) – Lower Signal to Noise Ratio (SNR), harder to extract signal from noise
  - Interference from other sources: Standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices, other things (e.g., motors, TVs) interfere as well
  - Multipath propagation: Radio signal reflects off objects ground, arriving at destination at slightly different times (moving objects between senders and receivers can cause this to change over time)

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

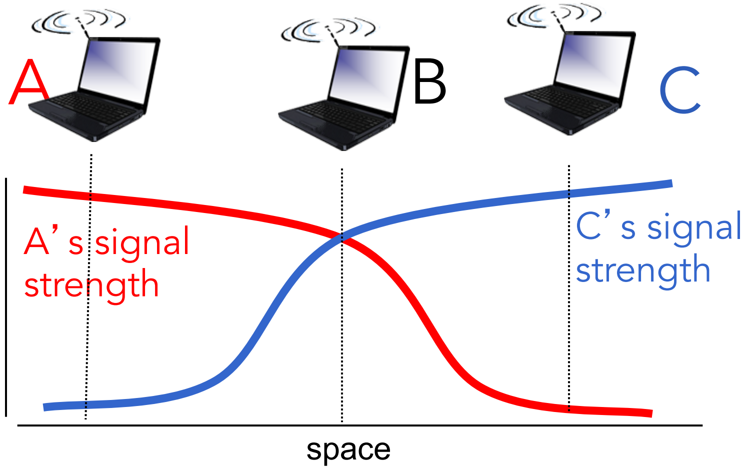
Wireless network characteristics

- 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 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

Code Division Multiple Access (CDMA)

- Space between nodes is a shared medium, we need a protocol to manage/limit interference – 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
  - Lets multiple users "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
- In the party analogy, each node is given a language to communicate in …

IEEE 802.11 Wireless LAN

- Many wireless LAN techs in the 90s – the winner 802.1, aka WiFi
- Many 802.11 standards

Standard	Frequency range	Data rate
802.11b	2.4 GHz	Up to 11 Mbps
802.11a	5 GHz	Up to 54 Mbps
80211.g	2.4 GHz	Up to 54 Mbps
802.11n	2.5 and 5 GHz	Up to 450 Mbps
802.11ac	5 GHz	Up to 1,300 Mbps

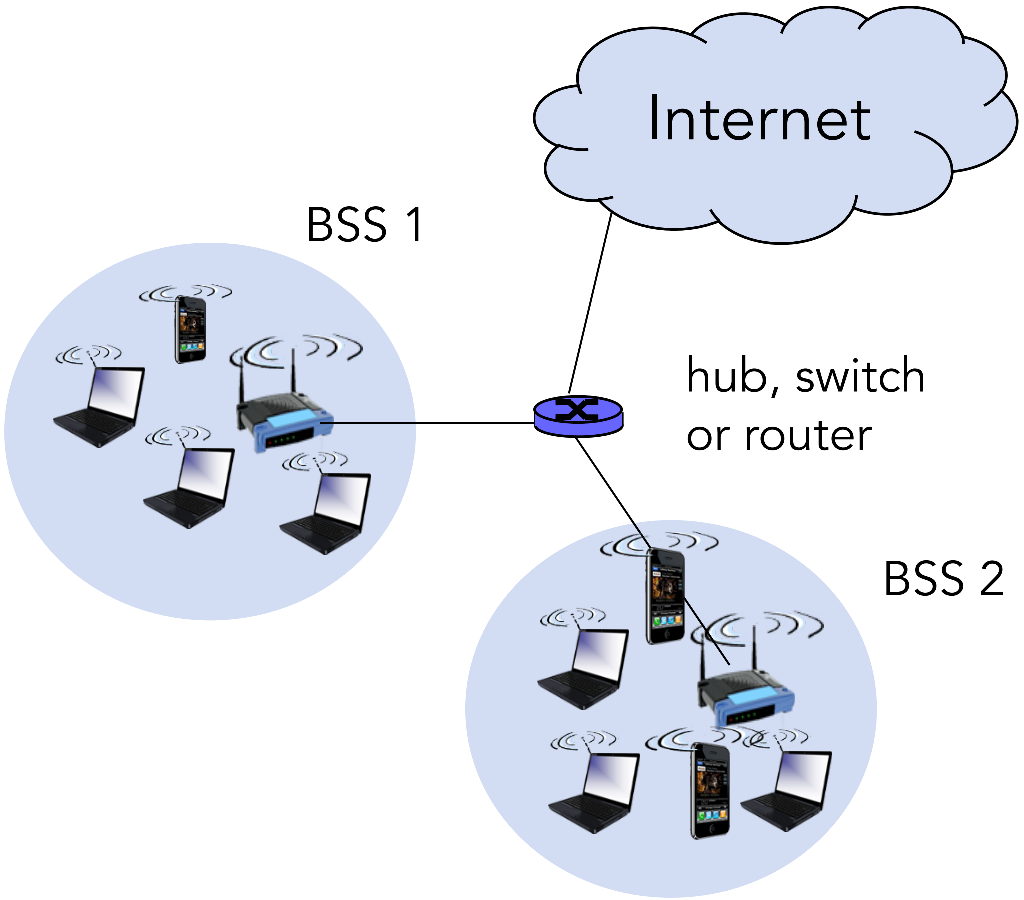
2.4 GHz is unlicensed (microwave oven!), 5 GHz has shorter transmission rate and suffers from multipath propagation

802.11n/ac use Multiple Input, Multiple Output antenna for < interference and > distances

- All use CSMA/CA for multiple access, same link-layer frame and are backward compatible

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

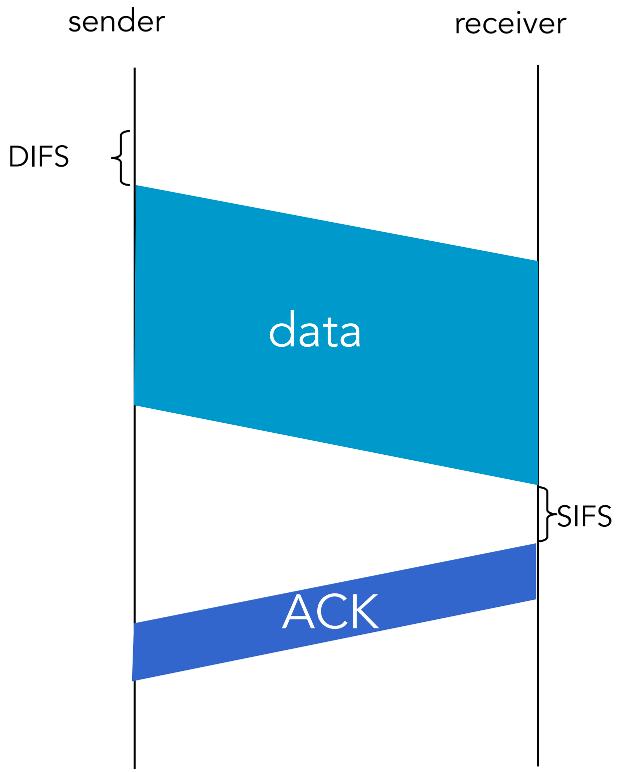
- When admin installs a 802.11b/g access point
  - Assign an SSID – Service Set Identifier
  - And a channel number from 11 partially overlapping ones
    - 2.4GHz-2.485GHz spectrum divided into 11 channels – any two channels are not overlapping if they are separated by four or more channels (so, max, 1, 6 and 11)
  - Possible interference – channel can be same as a neighboring AP!
- Host must associate with an AP
  - Scans channels, listening for beacon frames containing AP's name (SSID) and MAC address (passive, there's an active option)
  - Selects AP to associate with based on signal strength or load
  - May perform authentication using MAC address or user/password
  - And then run DHCP to get IP address in AP's subnet

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
- No collision detection!
  - Difficult to receive (sense collisions) when transmitting due to weak received signals (fading) – the strength of the transmitted signal is very strong compared to that of the received signal
  - Even if, can't sense all collisions in any case: hidden terminal, fading
  - Answer: Avoid collisions: CSMA/C(ollision)A(voidance)
- Before seeing CA, note 802.11 uses link-layer ACKs
  - Receiver gets a frame that passes CRC, waits for a short time (Short Inter-Frame Spacing, SIFS) and ACK

IEEE 802.11 MAC Protocol - CSMA/CA (avoid/detect)

- 802.11 sender
  - if sense channel idle for Distributed IFS then
    - Transmit entire frame (no Collision Detection)
  - (*) if sense channel busy then
    - start random backoff time (binary exponential backoff)
    - timer counts down while channel idle
    - transmit when timer expires
    - if no ACK, increase random backoff interval, goto *



- 802.11 receiver
  - if frame received OK
  - return ACK after SIFS (needs ACK because of 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 using small reservation packets!

802.11 frame

frame control	duration	address 1	address 2	address 3	seq control	address 4	payload	CRC
2 bytes	2	6	6	6	2	6	0 - 2312	4

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

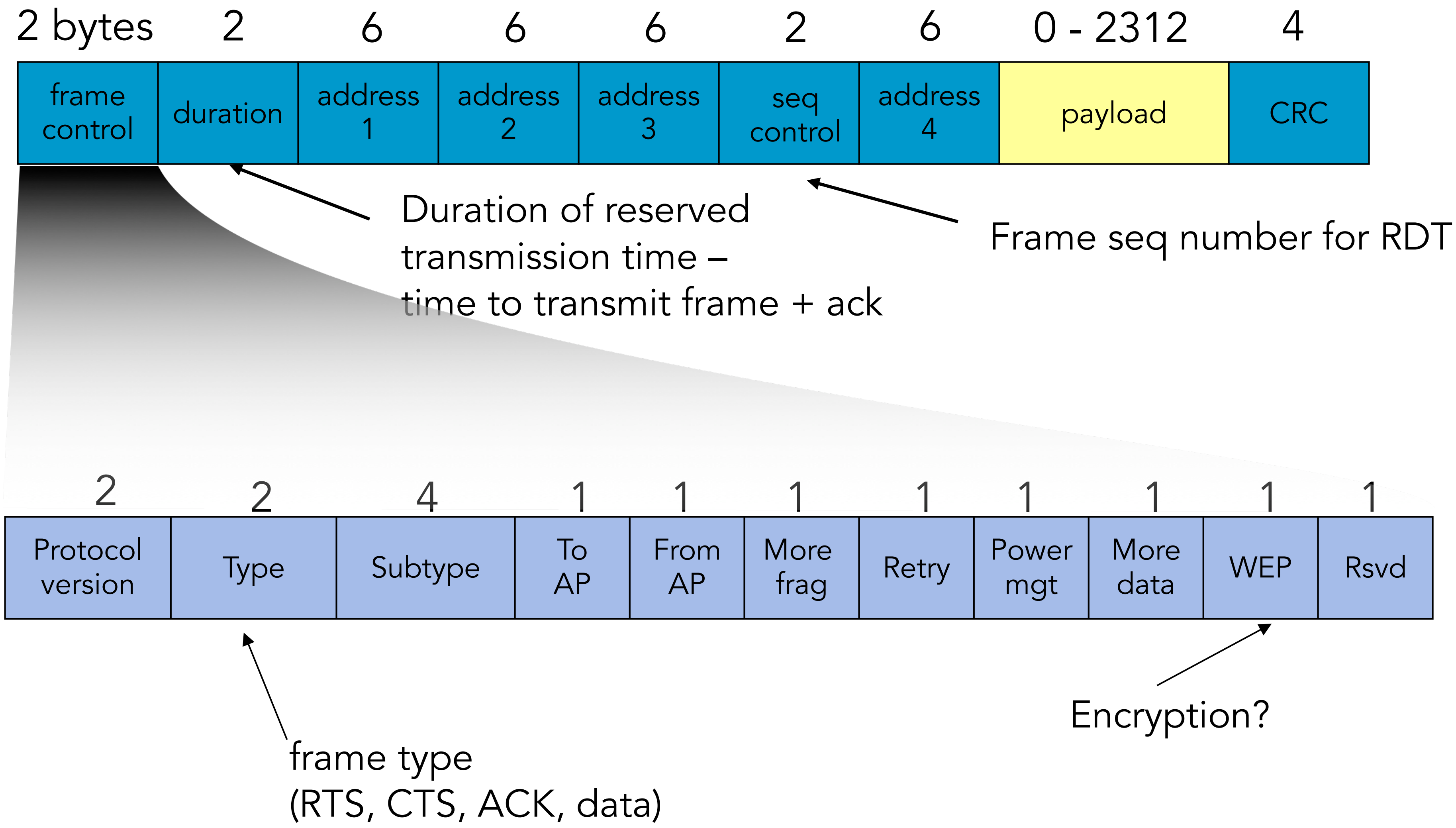
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

IP datagram or ARP packet; typically < 1,500B

- Remember an access point is a link-layer device, so no ide of IP
- Access point converts Ethernet frame to 802.11 frame, inserting its own MAC address in Address 2
- Removing its own address on the reverse path

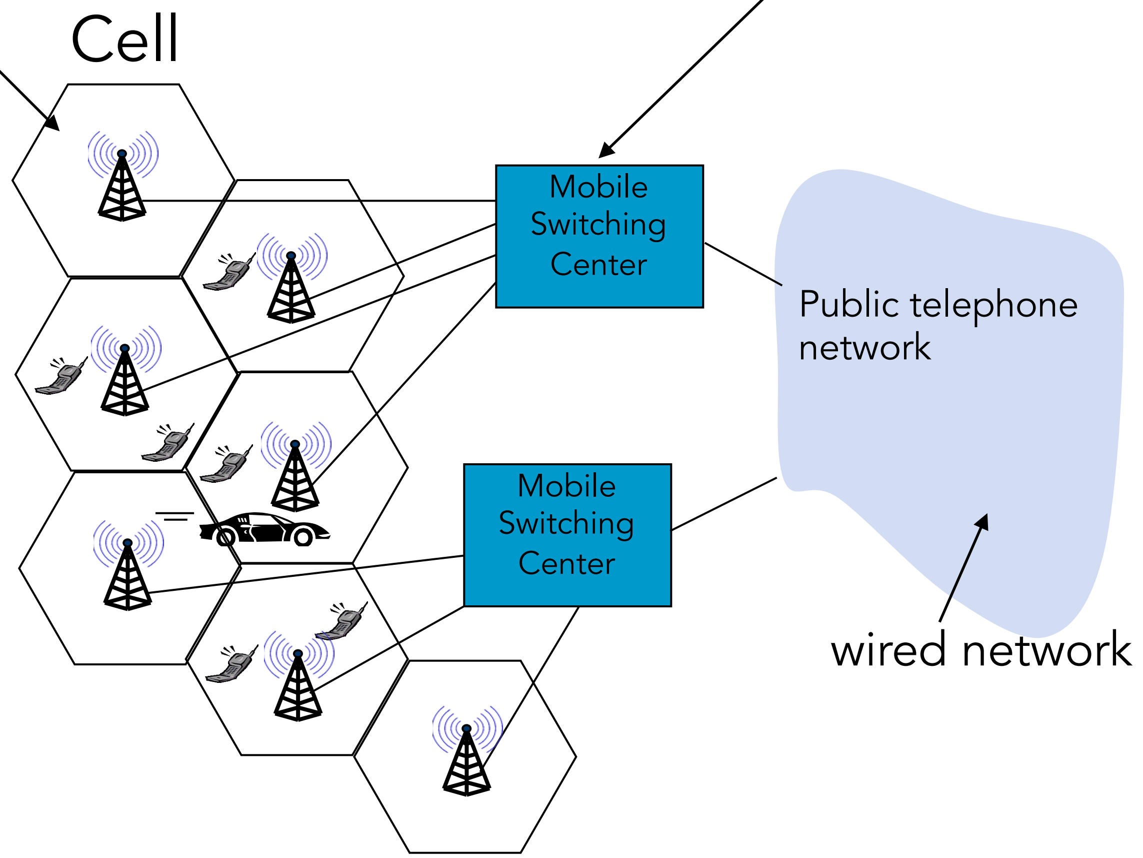
802.11 frame


2 bytes
2
6
6
6
2
6
0 - 2312
4
frame control
duration
address 1
address 2
address 3
seq control
address 4
payload
CRC
Duration of reserved transmission time – time to transmit frame + ack
Frame seq number for RDT
2
2
4
1
1
1
1
1
1
1
1
Protocol version
Type
Subtype
To AP
From AP
More frag
Retry
Power mgt
More data
WEP
Rsvd
frame type (RTS, CTS, ACK, data)
Encryption?

Components of cellular network architecture

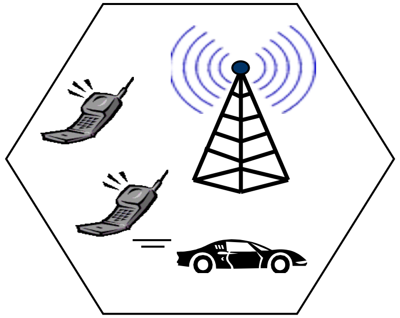
- Covered region partitioned into cells
- Each cell has a Base Transceiver Station
  BS ~ 802.11 AP
- Mobile users attach to network through BS

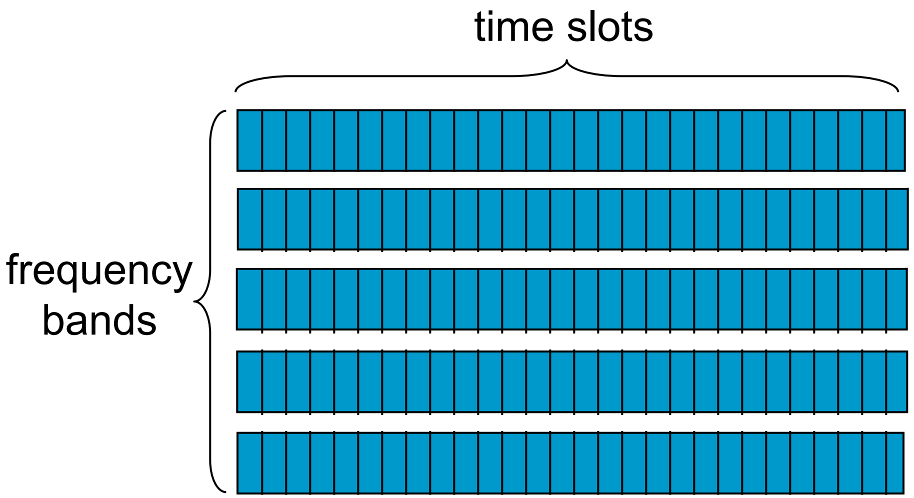
- Connects cells to wired telephone network
- Manages call setup
- Handles mobility



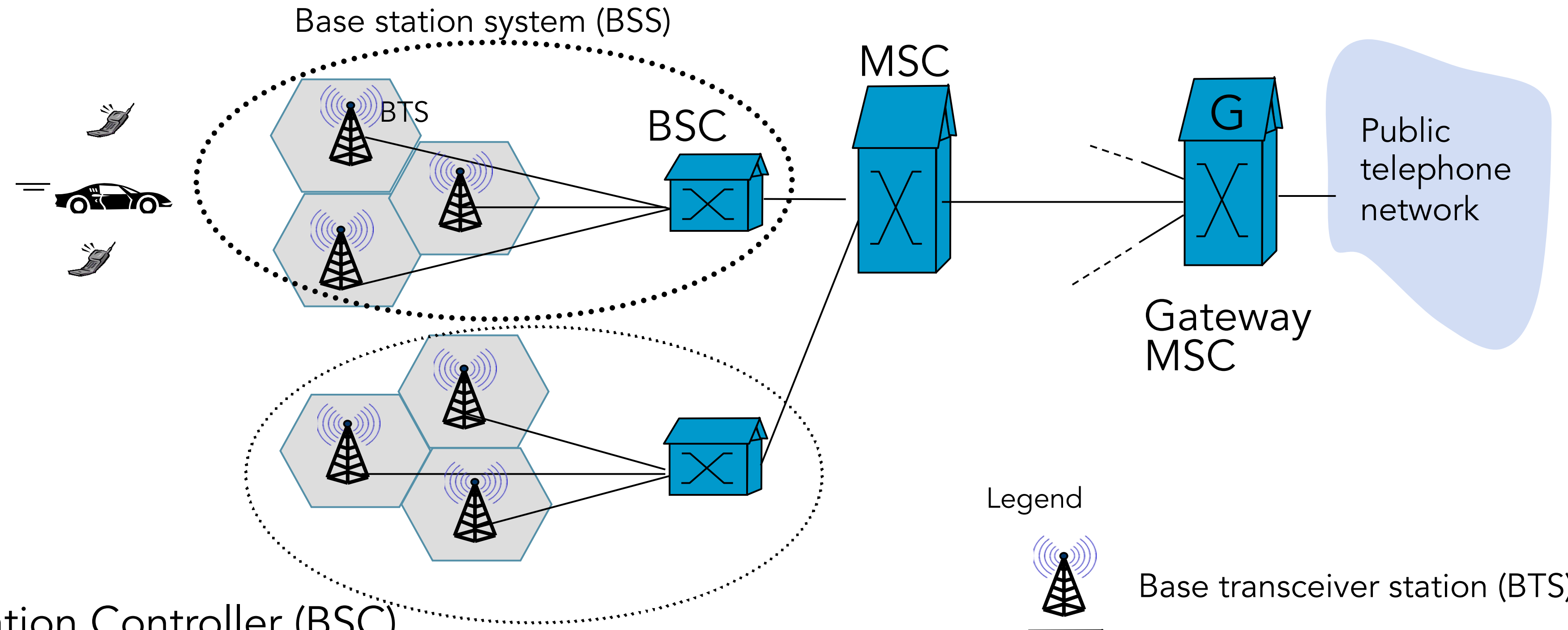
Cellular networks: the first hop

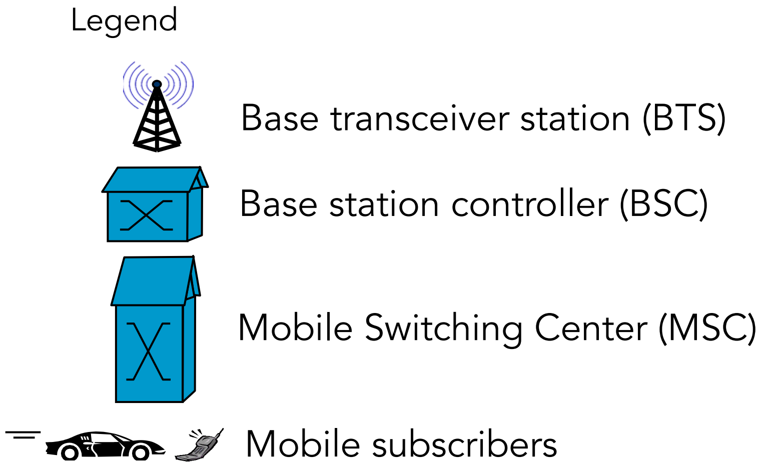
- Two techniques for sharing mobile-to-BS radio spectrum
  - Combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots (2G)
  - CDMA: code division multiple access
    - 3G - CDMA within TDMA slots available on multiple frequencies (FDMA)





2G (voice) network architecture



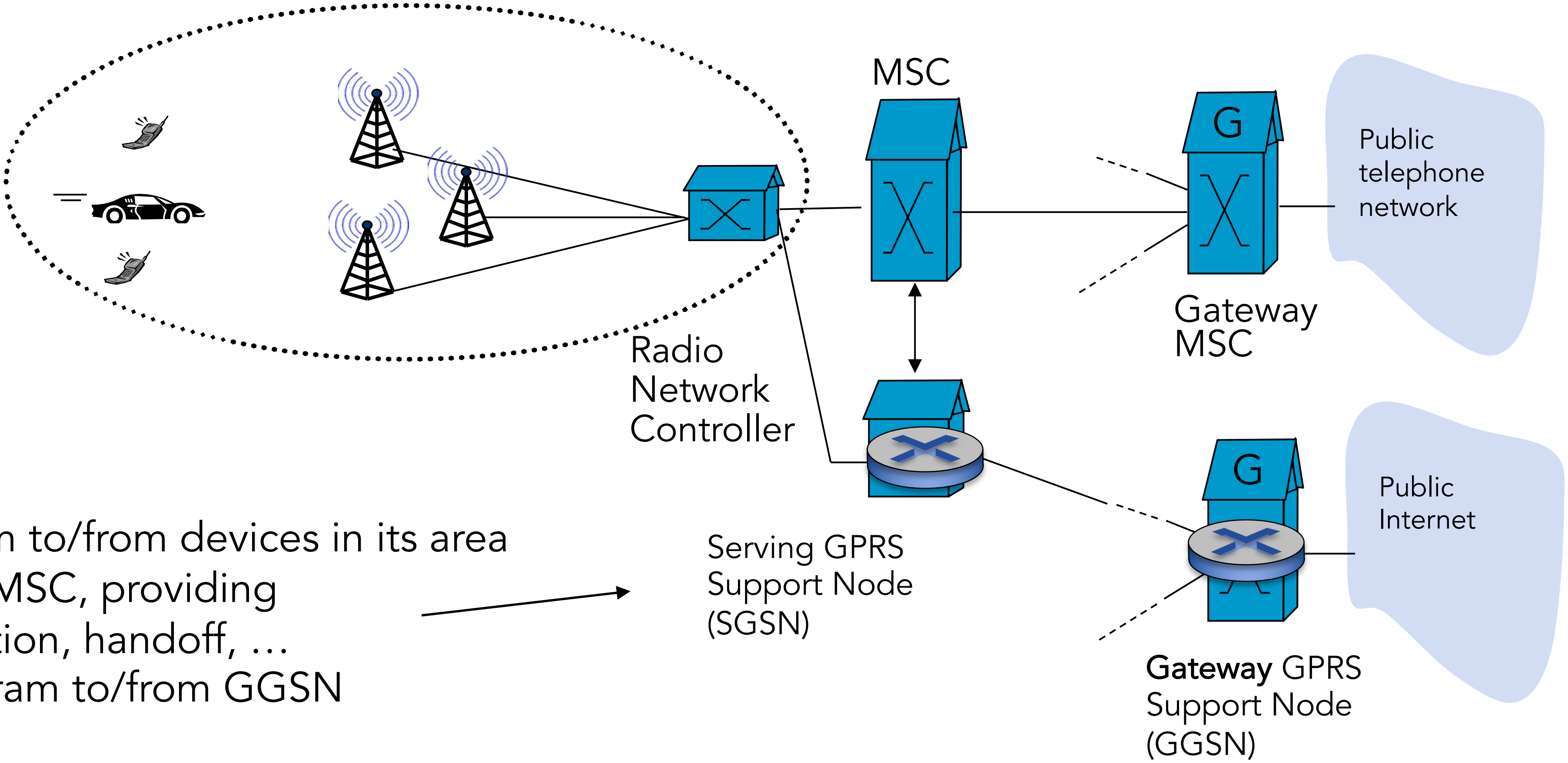


- A Base Station Controller (BSC) serves several Base Transceiver Stations (BTS), allocating BTS radio channels to subscribers, handoffs
- BSC and its BTSs form the Base Station Subsystem (BSS)

3G (voice+data) network architecture

Approach – New cell data network operates in parallel (except at edge) with existing cellular voice network

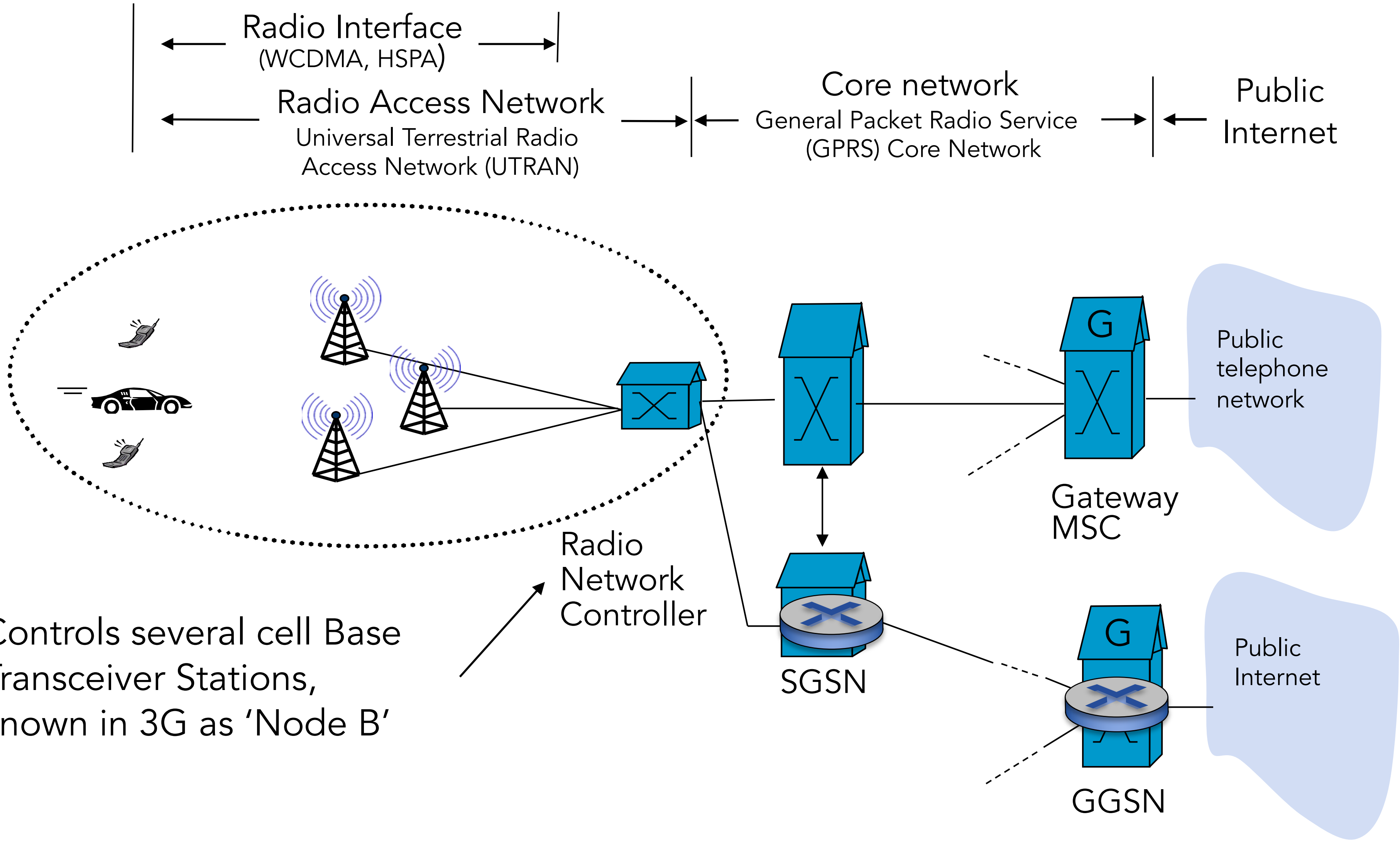
- Voice network unchanged in core
- Data network operates in parallel



Delivers datagram to/from devices in its area

- Interacts with MSC, providing user authorization, handoff, …
- Pass on datagram to/from GGSN

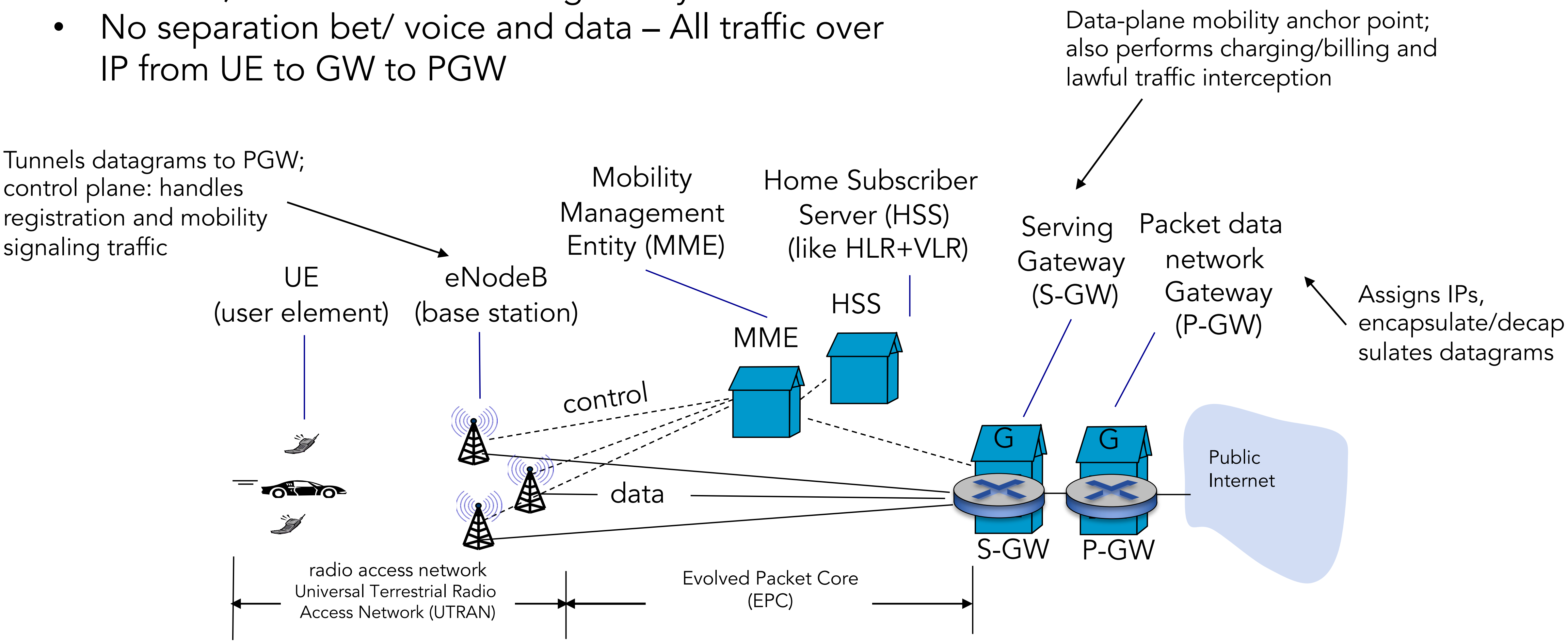
3G (voice+data) network architecture



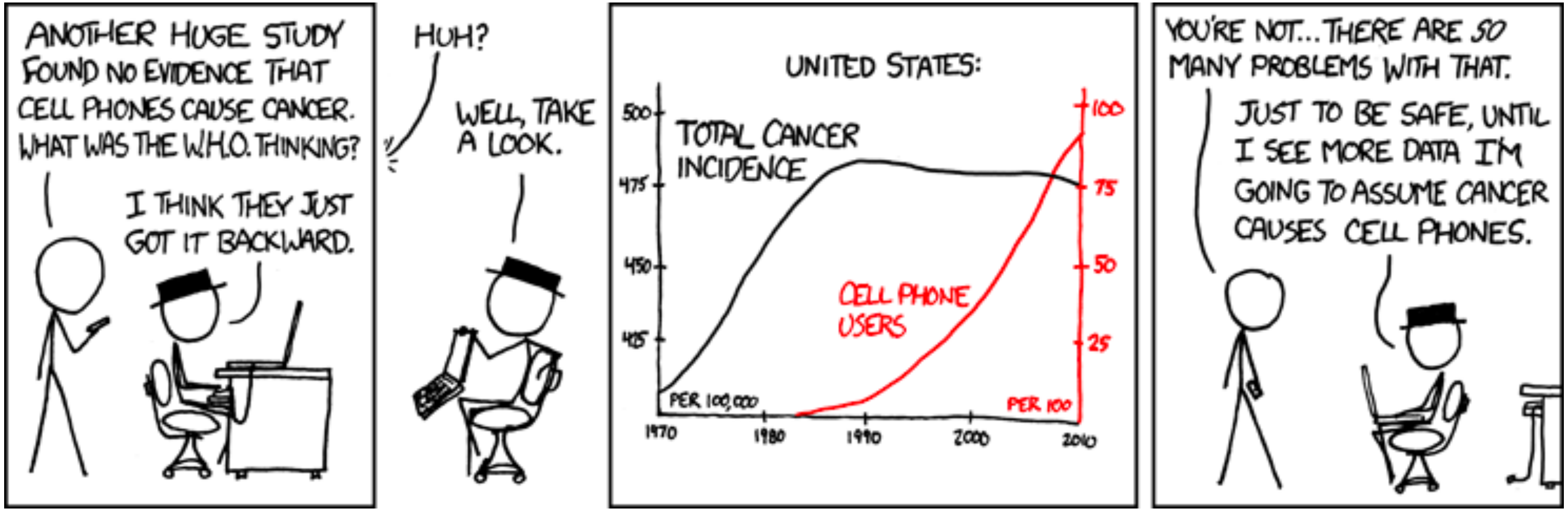
Controls several cell Base Transceiver Stations, known in 3G as 'Node B'

4G LTE overview

- All IP core: IP packets tunneled (through core IP network) from base station to gateway
- No separation bet/ voice and data – All traffic over IP from UE to GW to PGW



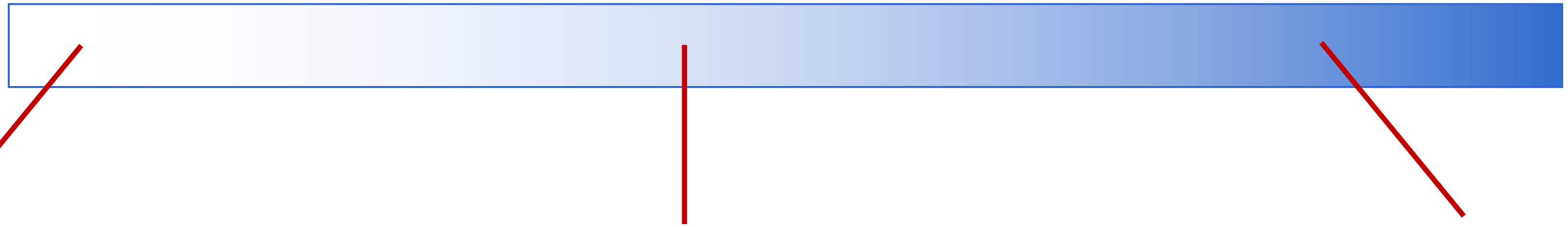
Go ahead, take 5’



Degrees of mobility

no mobility

high mobility



mobile wireless user, using same access point or moving within a building

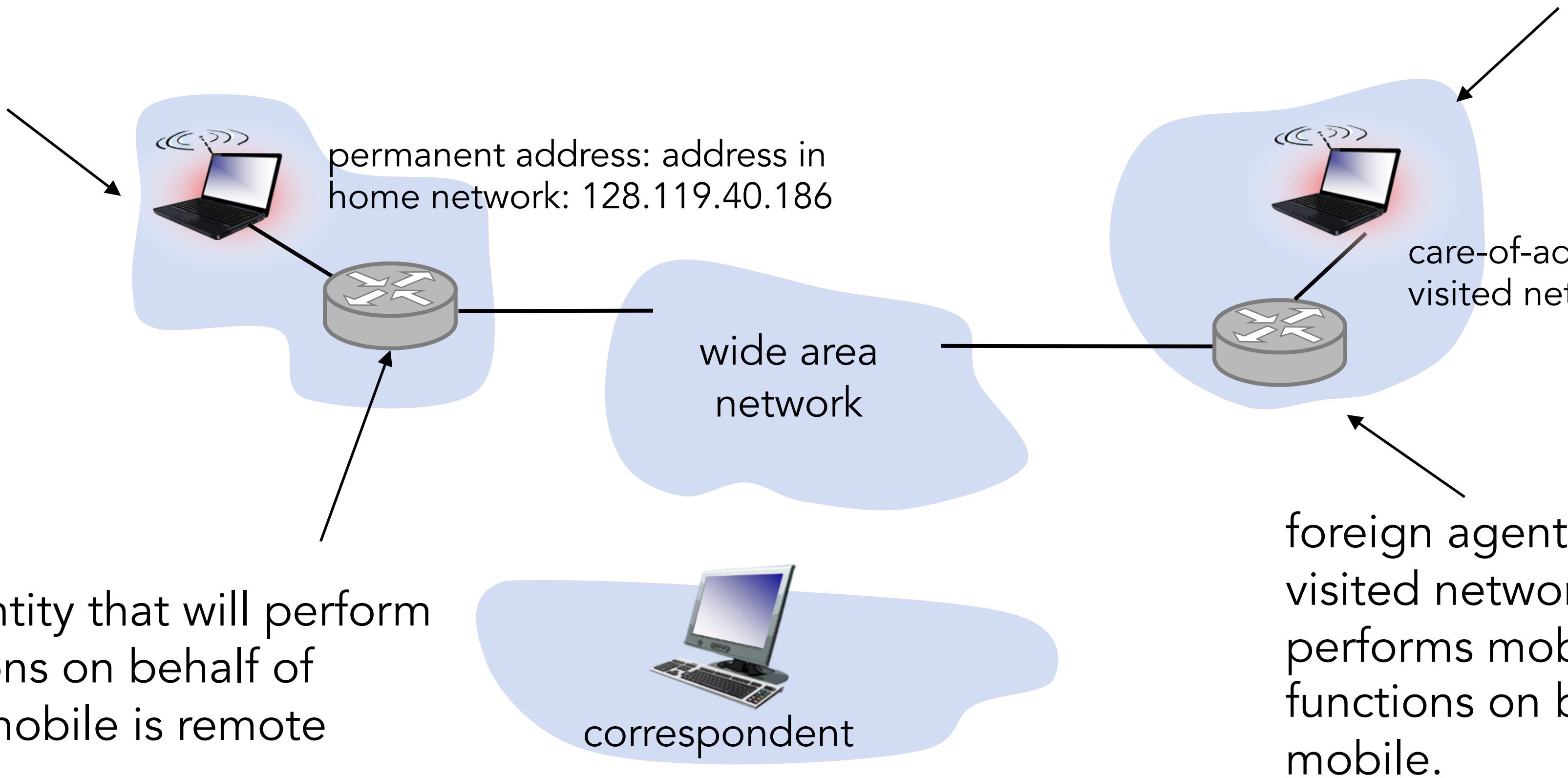
mobile user, connecting/ disconnecting from network using DHCP

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

Mobility vocabulary

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

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

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

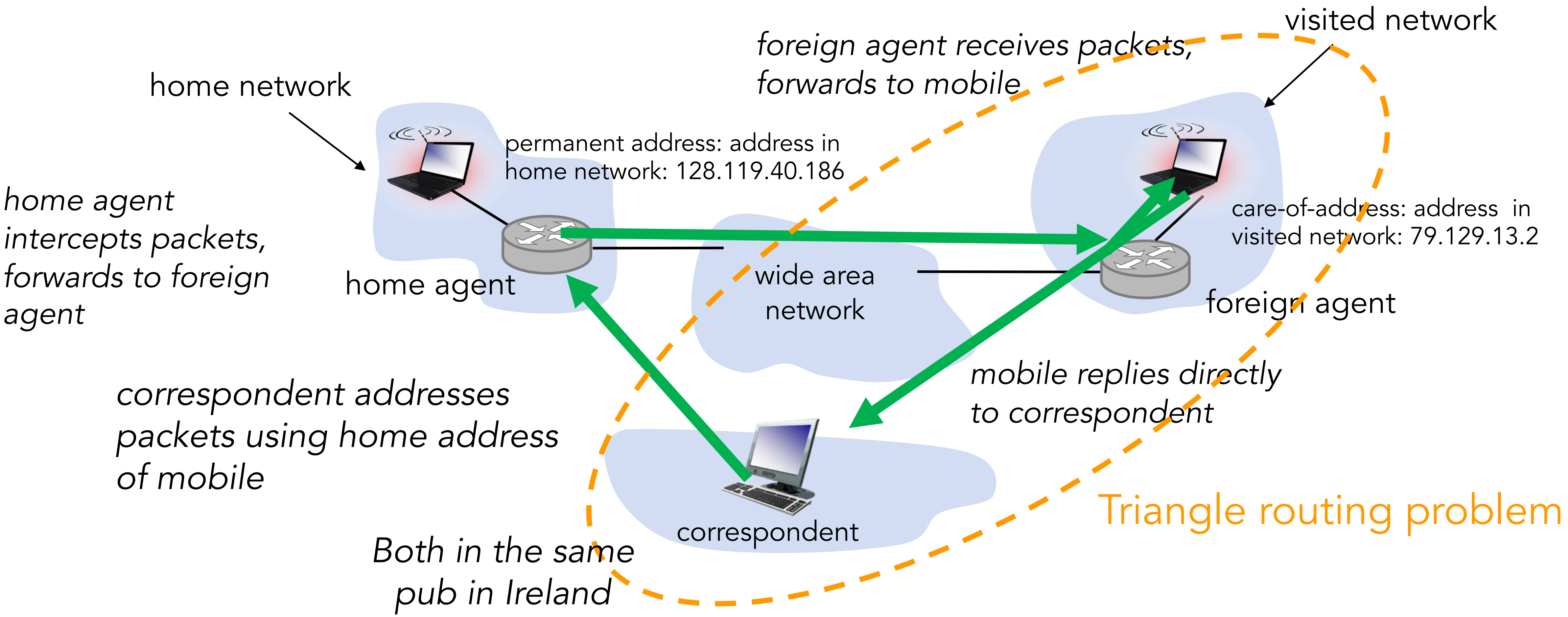
Mobility approaches

- 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
  - *Hard to scale to millions!*

- 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

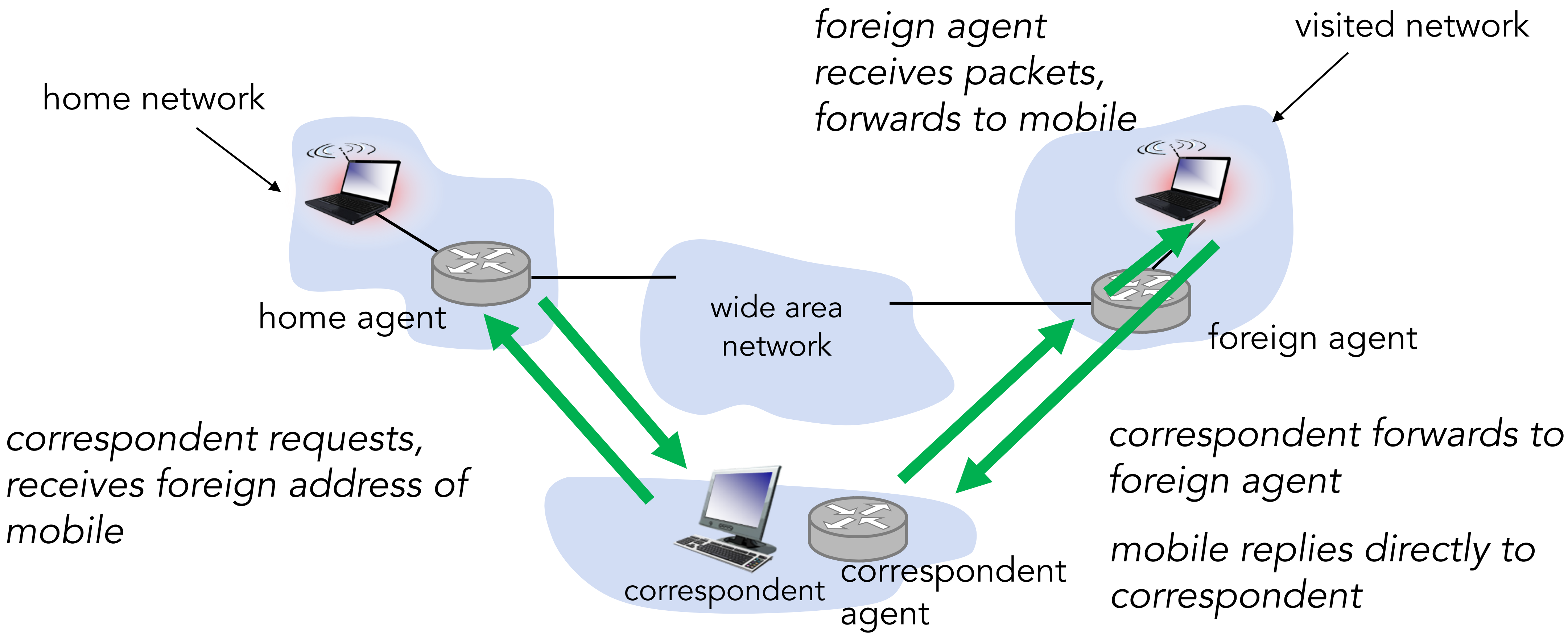
Indirect routing

- Mobile contacts foreign agent on entering visited network
- Foreign agent informs home agent home



Direct routing

- Solving the triangle routing problem
- What to do when the device moves? Anchor on first foreign network visited



In practice – IP mobility

- Within the same subnet
  - Device detects a weak signal from AP, scans for other APs and switches
  - Not a router but a switch connecting the APs, IP address can remain
  - Self-learning – Switch will see frame from the moved device and "remember" which switch port can be used to reach it

- Mobile IP [RFC 3344] – Indirect routing
  - Has many features we've seen: Home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
  - Agent discovery is done using ICMP with an 'agent advertisement' or 'agent solicitation' mode

In practice – Cell mobility

- Handoffs – a devices changes its association from one BS to another
  - Within the same MSC, the MSC handles it in cooperation with the old and new BSs
  - Across Mobile Switch Centers – Direct routing with anchor
- Across networks – Indirect routing
  - User registers in a visiting network with Visitor Location Register (VLR) who informs user's Home Location Register of user's new place
  - When correspondent initiates, contacts user's home network MSC, who asks HLR who has the user's Mobile Station Roaming Number (~CoA, invisible to the user) or the VLR contact info
  - MSC sets up the second leg of the call

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
  - *So no impact on applications?*
- … but performance-wise
  - packet loss/delay due to bit-errors (dropped packets, delays for link-layer retransmissions), and handoff
  - TCP interprets loss as congestion, decreases cwnd un-necessarily
    - Some options: local recovery (i.e., 802.11 ARQ or FEC), TCP sender awareness of wireless link, split TCP
  - delay impairments for real-time traffic
  - limited bandwidth of wireless links