Wireless Networks

Note: The slides are adapted from the materials from Prof. Richard Han at CU Boulder and Profs. Jennifer Rexford and Mike Freedman at Princeton University, and the networking book (Computer Networking: A Top Down Approach) from Kurose and Ross.

Wireless Links

Widespread Deployment

- Worldwide cellular subscribers
  - 1993: 34 million
  - 2005: more than 2 billion
  - 2009: more than 4 billion

    > landline subscribers

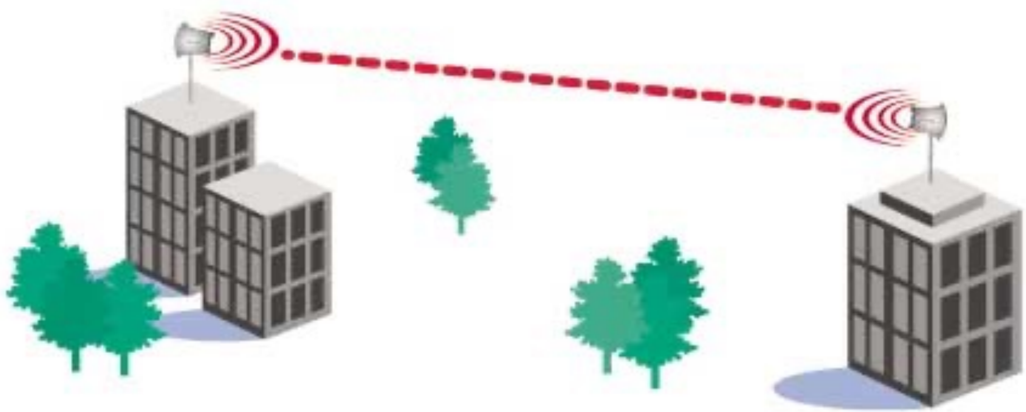
- Wireless local area networks
  - Wireless adapters built in to most laptops, and even PDAs
  - More than 220,000 known WiFi locations in 134 countries
  - Probably many, many more (e.g., home networks, corporate networks, …)

Wireless Properties

- Interference / bit errors
  - More sources of corruption compared to wired
- Multipath propagation
  - Signal does not travel in a straight line
- Broadcast medium
  - All traffic to everyone
- Power trade-offs
  - Important for power constrained devices

Wireless Links: High Bit Error Rate

- Decreasing signal strength
  - Disperses as it travels greater distance
  - Attenuates as it passes through matter

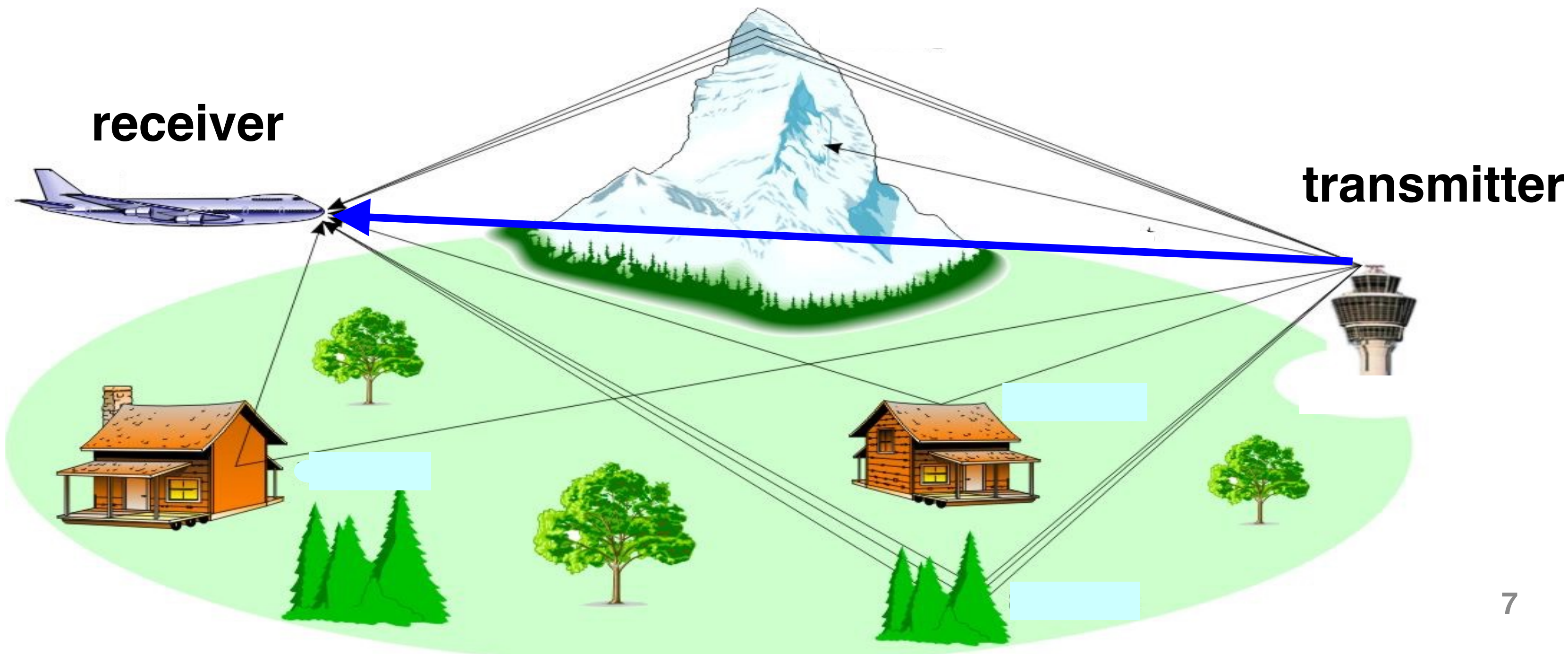


Wireless Links: High Bit Error Rate

- Interference from other sources
  - Radio sources in same frequency band
  - E.g., 2.4 GHz wireless phone interferes with 802.11b wireless LAN
  - Electromagnetic noise (e.g., microwave oven)

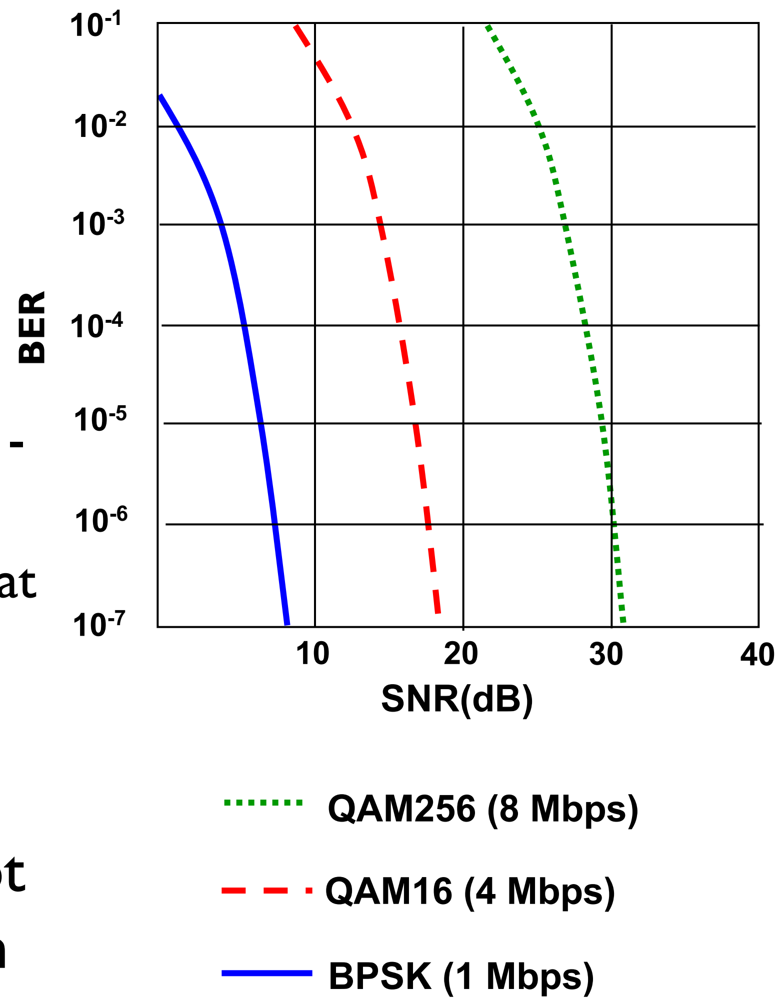
Wireless Links: High Bit Error Rate

- Multi-path propagation
  - Electromagnetic waves reflect off objects
  - Taking many paths of different lengths
  - Causing blurring of signal at the receiver



Wireless Link Characteristics

- 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 thruput
    - SNR may change with mobility: dynamically adapt physical layer (modulation technique, rate)



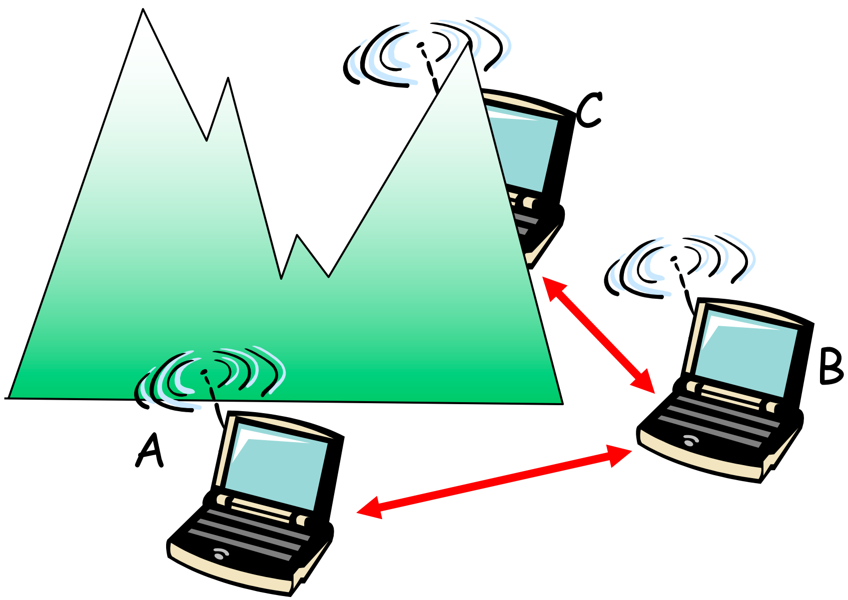
Dealing With Bit Errors

- Wireless vs. wired links
  - Wired: most loss is due to congestion
  - Wireless: higher, time-varying bit-error rate

- Dealing with high bit-error rates
  - Sender could increase transmission power
    - Requires more energy (bad for battery-powered hosts)
    - Creates more interference with other senders
  - Stronger error detection and recovery
    - More powerful error detection/correction codes
    - Link-layer retransmission of corrupted frames

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: hidden terminal problem

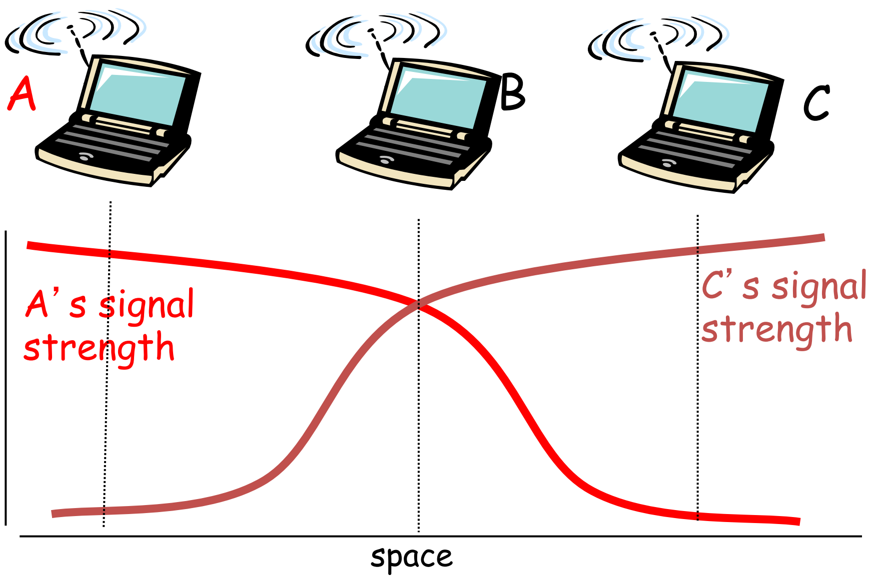


- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

So, A and C are unaware of their interference at B

Wireless Links: Broadcast Limitations

- Wired broadcast links
  - E.g., Ethernet bridging, in wired LANs
  - All nodes receive transmissions from all other nodes
- Wireless broadcast: fading over distance



- **A and B hear each other**
- **B and C hear each other**
- **But, A and C do not**

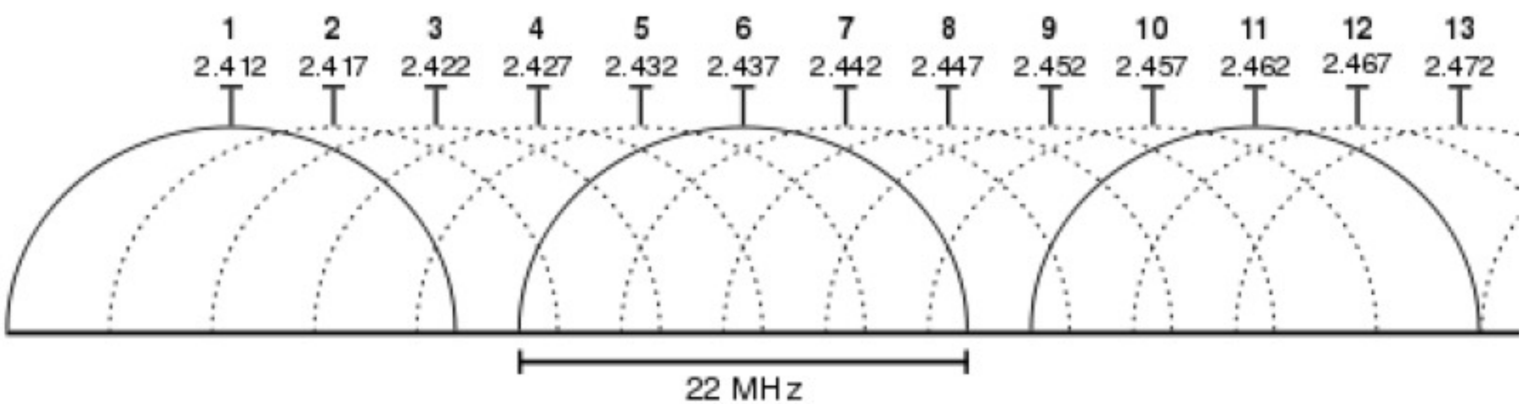
So, A and C are unaware of their interference at B

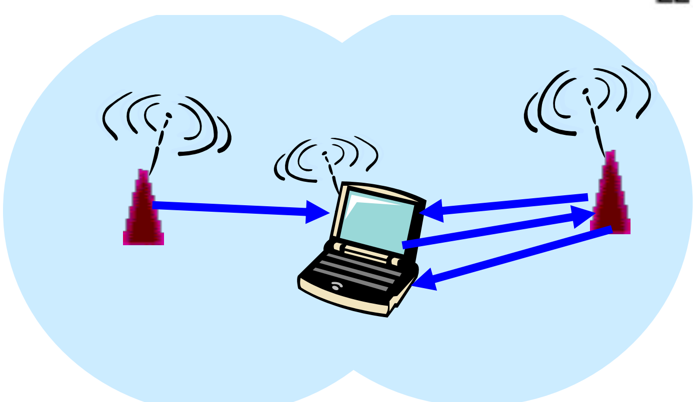
Example Wireless Link Technologies

- Data networks
  - 802.15.1 (Bluetooth): 2.1 Mbps – 10 m
  - 802.11b (WiFi): 5-11 Mbps – 100 m
  - 802.11a and g (WiFi): 54 Mbps – 100 m
  - 802.11n (WiFi): 200 Mbps – 100 m
  - 802.16 (WiMax): 70 Mbps – 10 km
- Cellular networks, outdoors
  - 2G: 56 Kbps
  - 3G: 384 Kbps
  - 3G enhanced: 4 Mbps
  - 4G LTE: 100Mbps
  - LTE Advanced: 1Gbps

Channels and Association

- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP

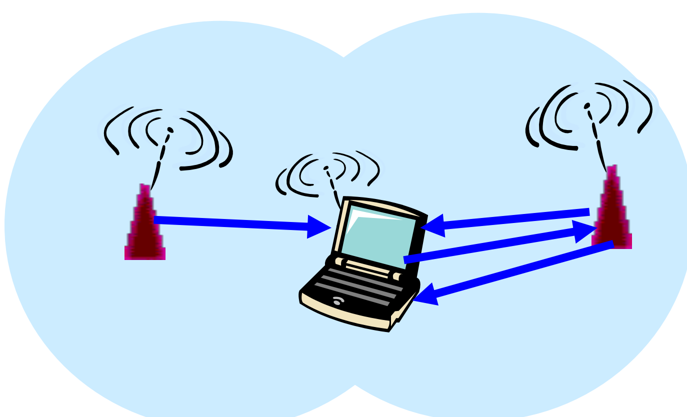




- Beacon frames from APs
- Associate request from host
- Association response from AP

Channels and Association

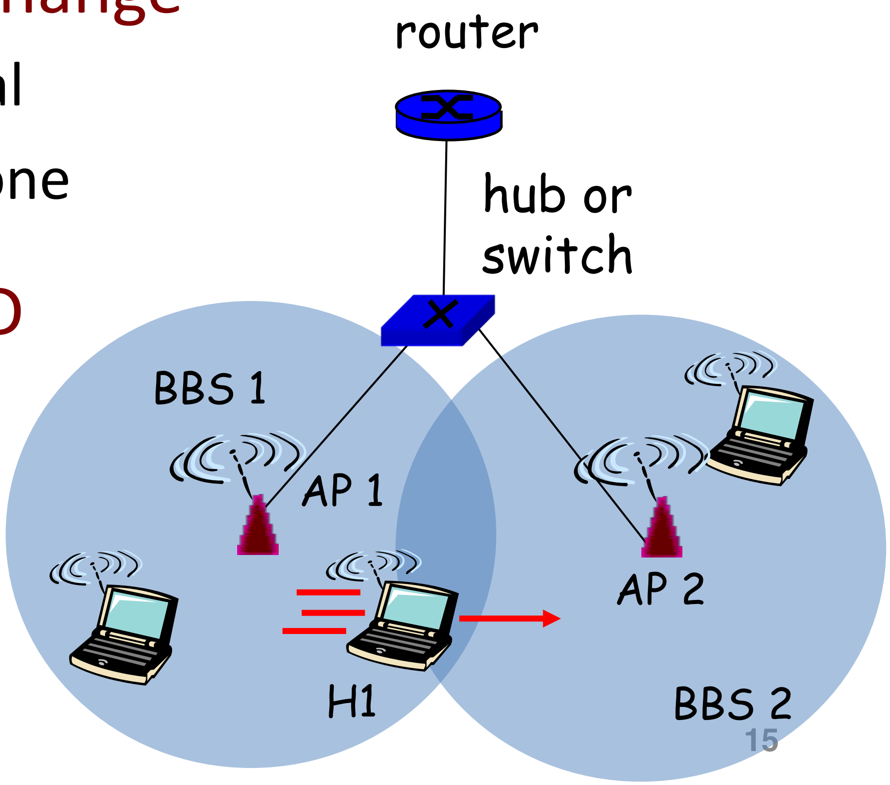
- Multiple channels at different frequencies
  - Network administrator chooses frequency for AP
  - Interference if channel is same as neighboring AP
- Access points send periodic beacon frames
  - Containing AP's name (SSID) and MAC address
  - Host scans channels, listening for beacon frames
  - Host selects an access point to associate with



- Beacon frames from APs
- Associate request from host
- Association response from AP

Mobility Within the Same Subnet

- H1 remains in same IP subnet
  - IP address of the host can remain same
  - Ongoing data transfers can continue uninterrupted
- H1 recognizes the need to change
  - H1 detects a weakening signal
  - Starts scanning for stronger one
- Changes APs with same SSID
  - H1 disassociates from one
  - And associates with other
- Switch learns new location
  - Self-learning mechanism



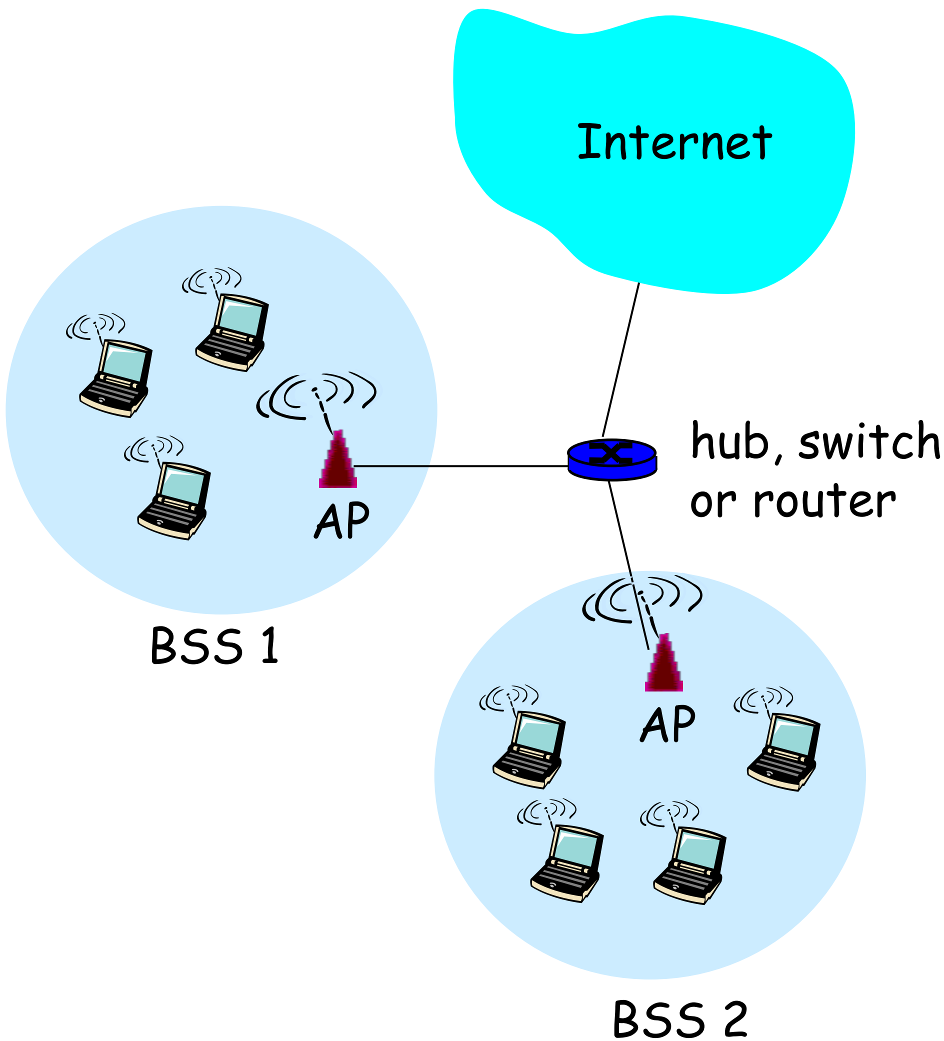
Questions

- Loss is primary caused by bit errors
  (A) Ethernet (Wired)
  (B) 802.11 (Wireless)
  (C) Both
  (D) Neither

- All hosts on subnet see all communication
  (A) Ethernet (Wired)
  (B) 802.11 (Wireless)
  (C) Both
  (D) Neither

WiFi: 802.11 Wireless LANs

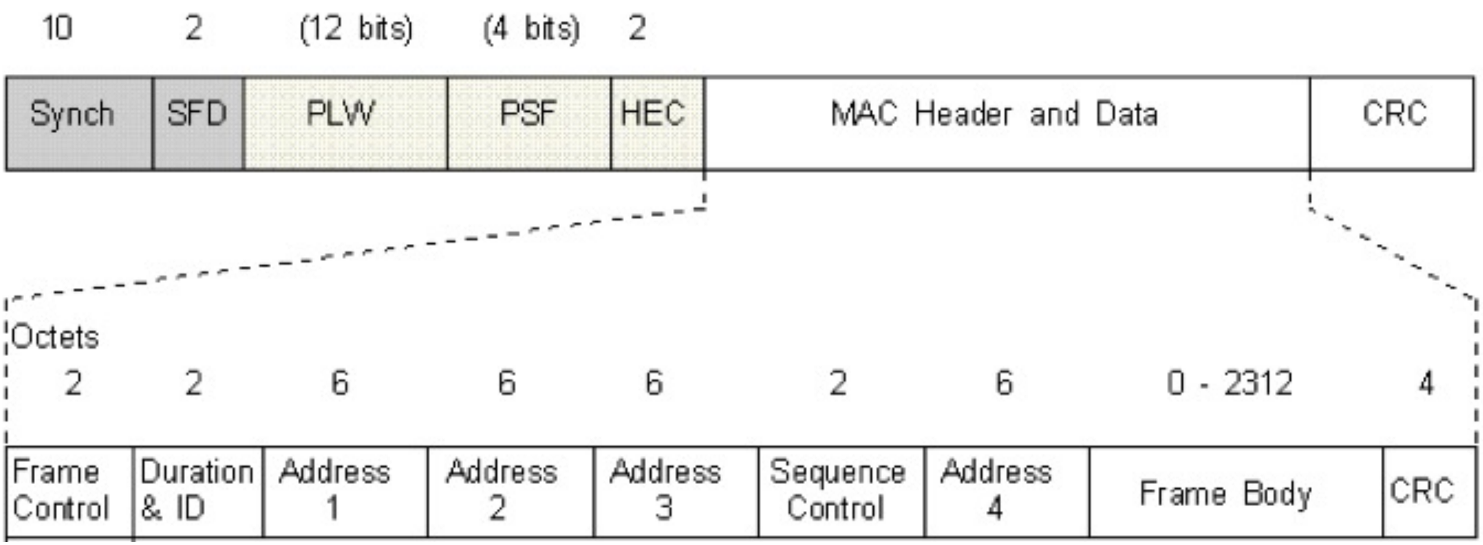
802.11 LAN Architecture



- Access Point (AP)
  - Base station that communicates with the wireless hosts
- Basic Service Set (BSS)
  - Coverage of one AP
  - AP acts as the master
  - Identified by an "network name" known as an SSID

SSID: Service Set Identifier

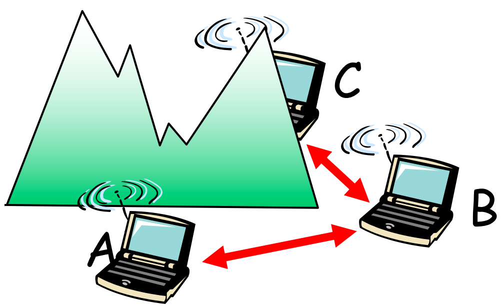
Wireless LAN addressing and bridging

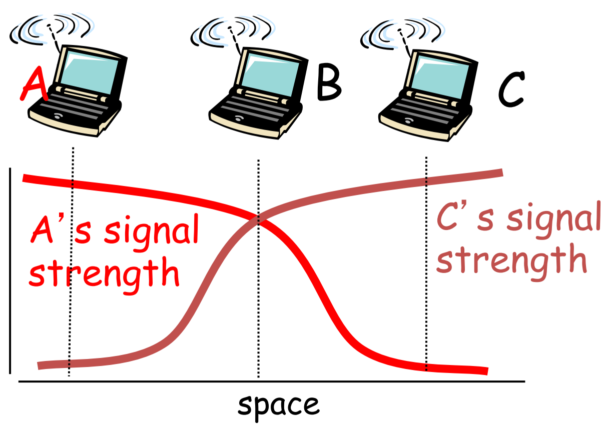


Function	Addr 1 (Receiver)	Addr 2 (Transmitter)	Addr 3	Addr 4
Intra-BSS	Dest	Source		
To AP	BSS ID	Source	Dest	
From AP	Dest	BSS ID	Source	
Bridged APs	Reciever	Transmitter	Dest	Source

CSMA: Carrier Sense, Multiple Access

- Multiple access: channel is shared medium
  - Station: wireless host or access point
  - Multiple stations may want to transmit at same time
- Carrier sense: sense channel before sending
  - Station doesn't send when channel is busy
  - To prevent collisions with ongoing transfers
  - But, detecting ongoing transfers isn't always possible

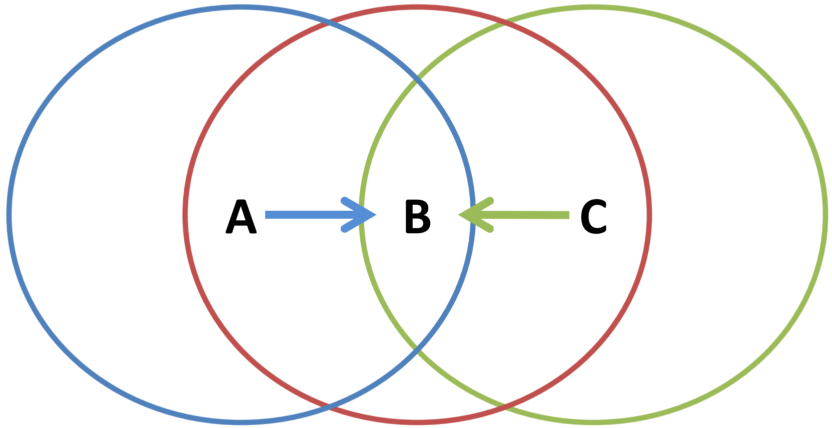




CA: Collision Avoidance, Not Detection

- Collision detection in wired Ethernet
  - Station listens while transmitting
  - Detects collision with other transmission
  - Aborts transmission and tries sending again
- Problem #1: cannot detect all collisions
  - Hidden terminal problem
  - Fading
- Problem #2: listening while sending
  - Strength of received signal is much smaller
  - Expensive to build hardware that detects collisions
- So, 802.11 does collision avoidance, not detection

Hidden Terminal Problem



- A and C can't see each other, both send to B
- Occurs b/c 802.11 relies on physical carrier sensing, which is susceptible to hidden terminal problem

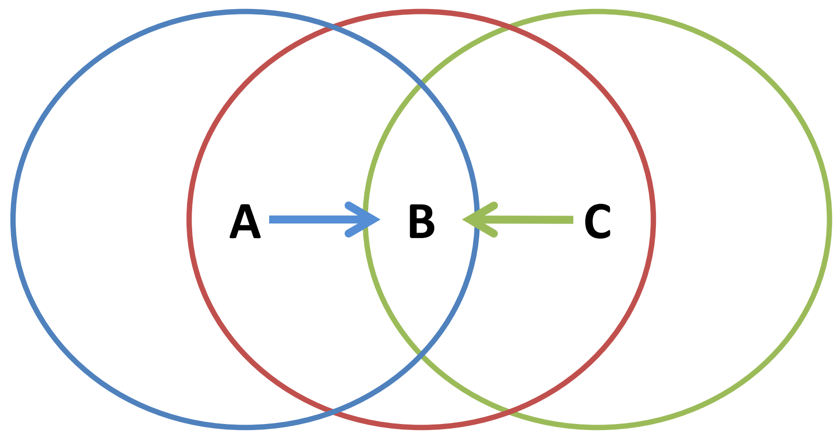
Virtual carrier sensing

- First exchange control frames before transmitting data
  - Sender issues "Request to Send" (RTS), incl. length of data
  - Receiver responds with "Clear to Send" (CTS)
- If sender sees CTS, transmits data (of specified length)
- If other node sees CTS, will idle for specified period
- If other node sees RTS but not CTS, free to send

When to Resume Sending?

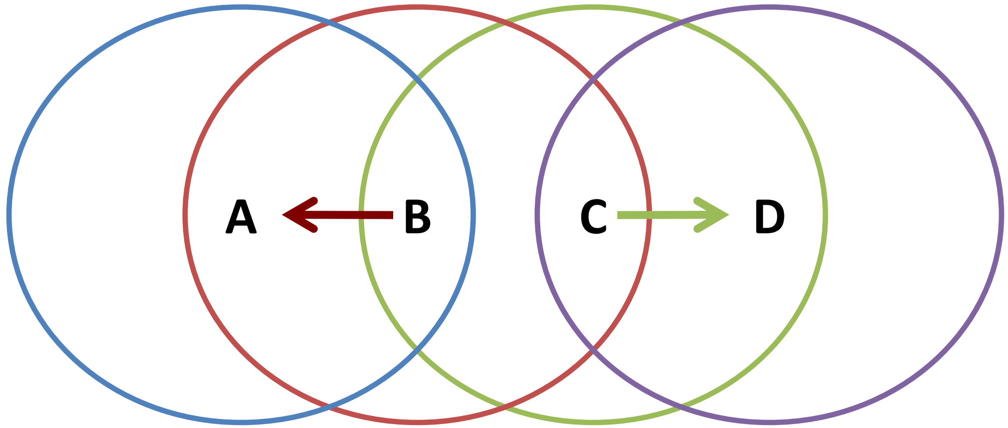
- How does host C know when to resume sending?
  - RTS & CTS both include a Network Allocation Vector (NAV) indicating the length of their upcoming transmission
  - Data frame also contains a “NAV” to indicate the length of transmission
  - After Host A has finished sending its data, Host B sends an ACK; Host C hears B’s ACK and knows the data transmission is over

Hidden Terminal Problem



- A and C can’t see each other, both send to B
- RTS/CTS can help
  - Both A and C would send RTS that B would see first
  - B only responds with one CTS (say, echo’ing A’s RTS)
  - C detects that CTS doesn’t match and won’t send

Exposed Terminal Problem



- B sending to A, C wants to send to D
- As C receives B's packets, carrier sense would prevent it from sending to D, even though wouldn't interfere
- RTS/CTS can help
  – C hears RTS from B, but not CTS from A
  – C knows it's transmission will not interfere with A
  – C is safe to transmit to D

Cellular Network Architecture

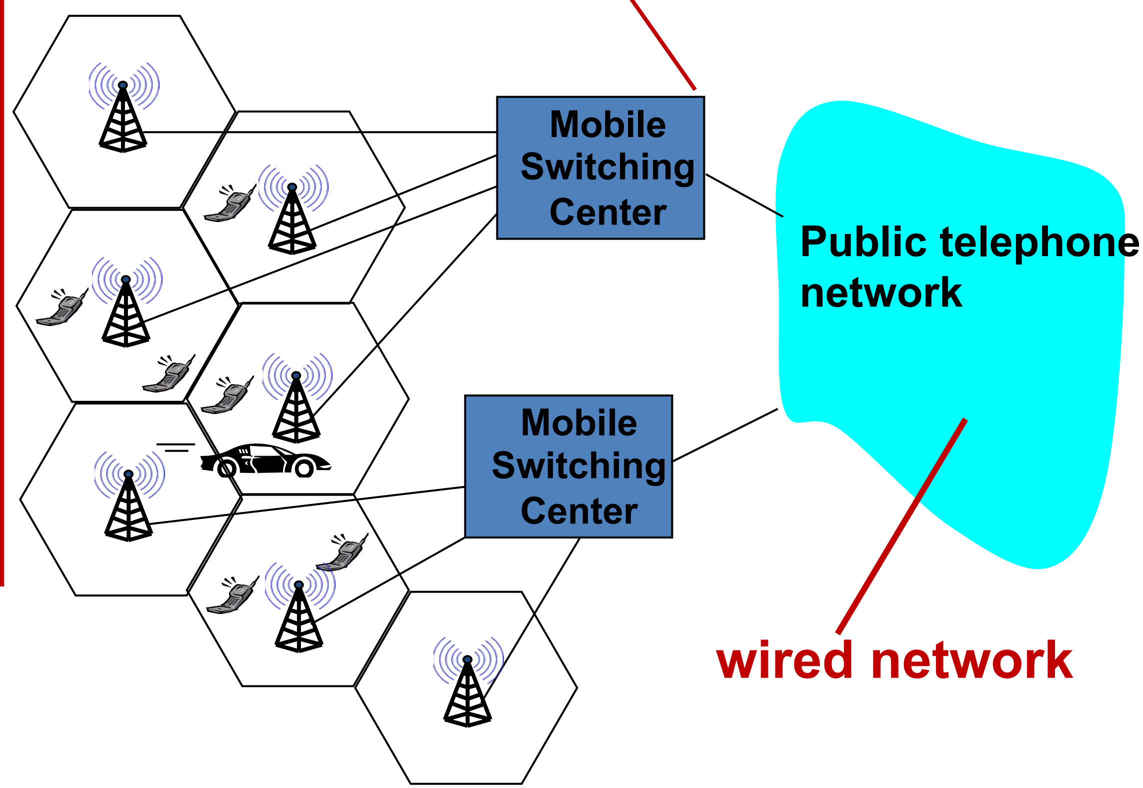
Components of cellular network architecture

MSC

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

cell

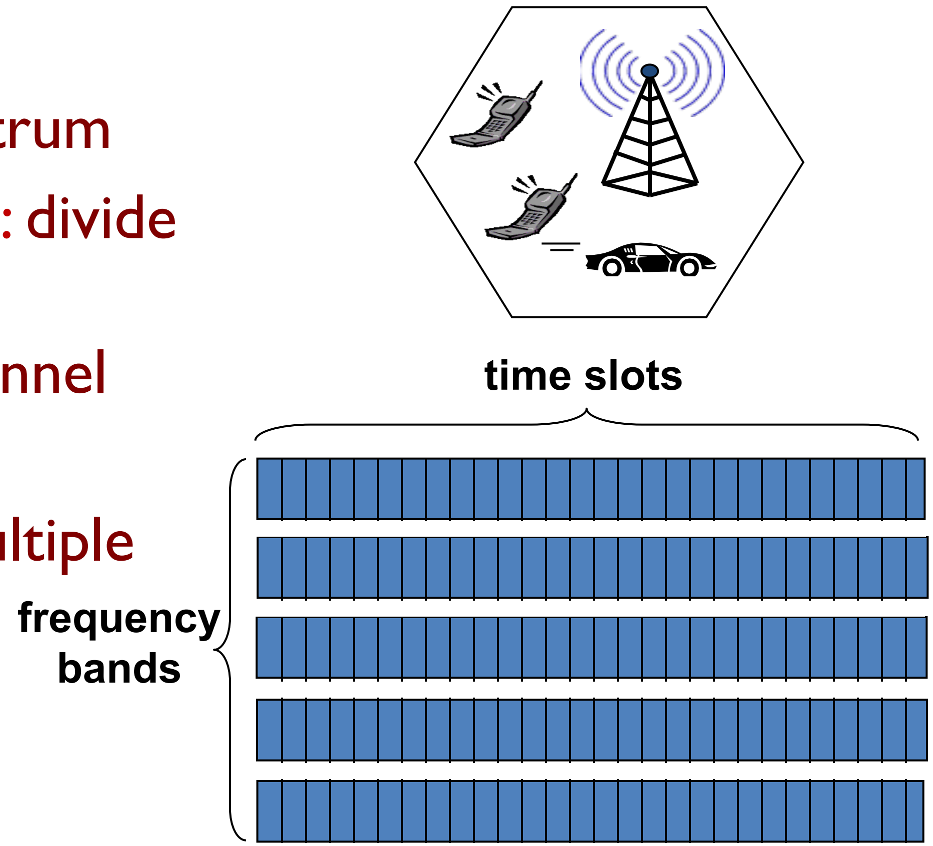
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS



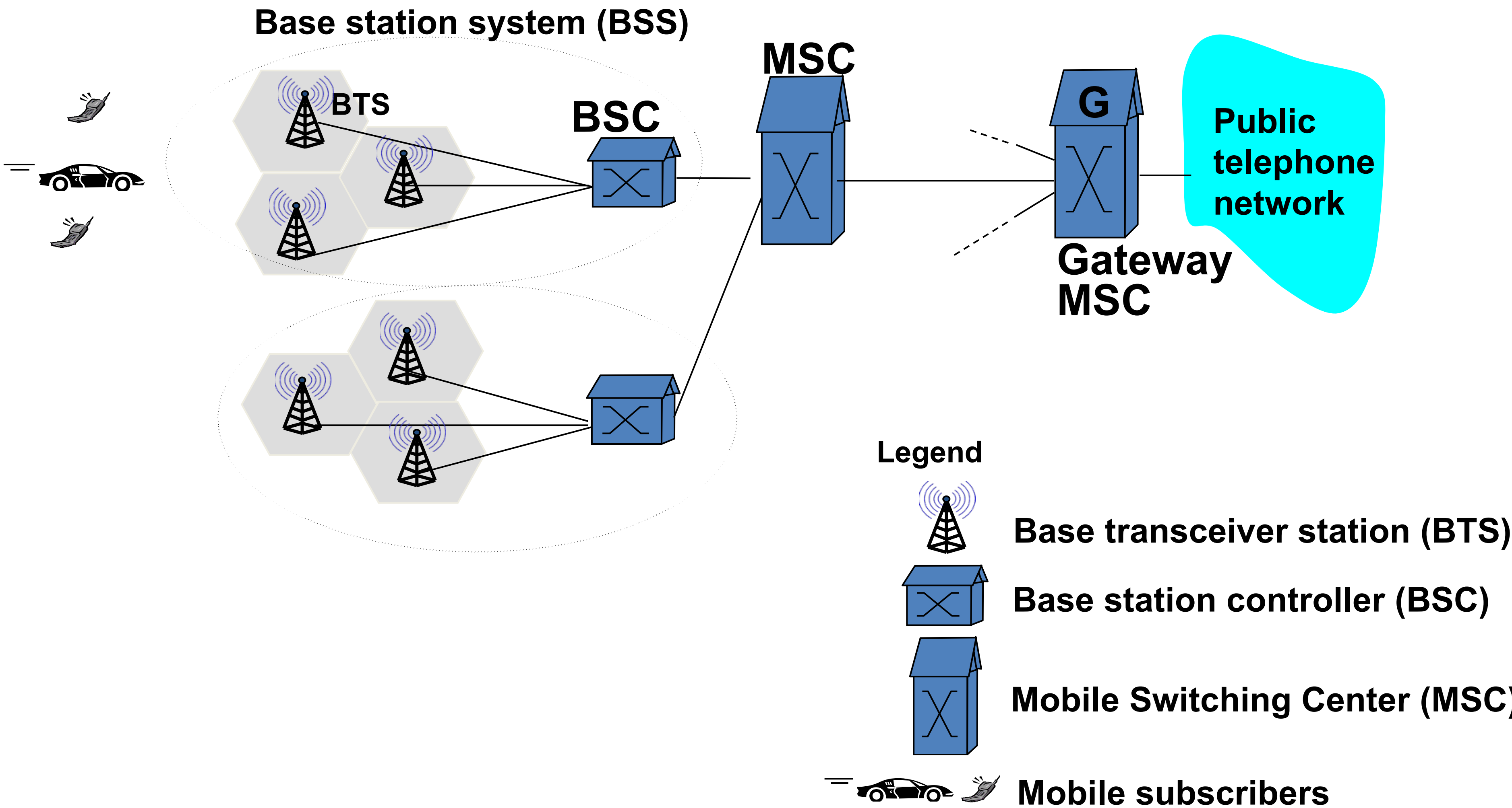
Cellular networks: the first hop

Two techniques for sharing mobile-to-BS radio spectrum

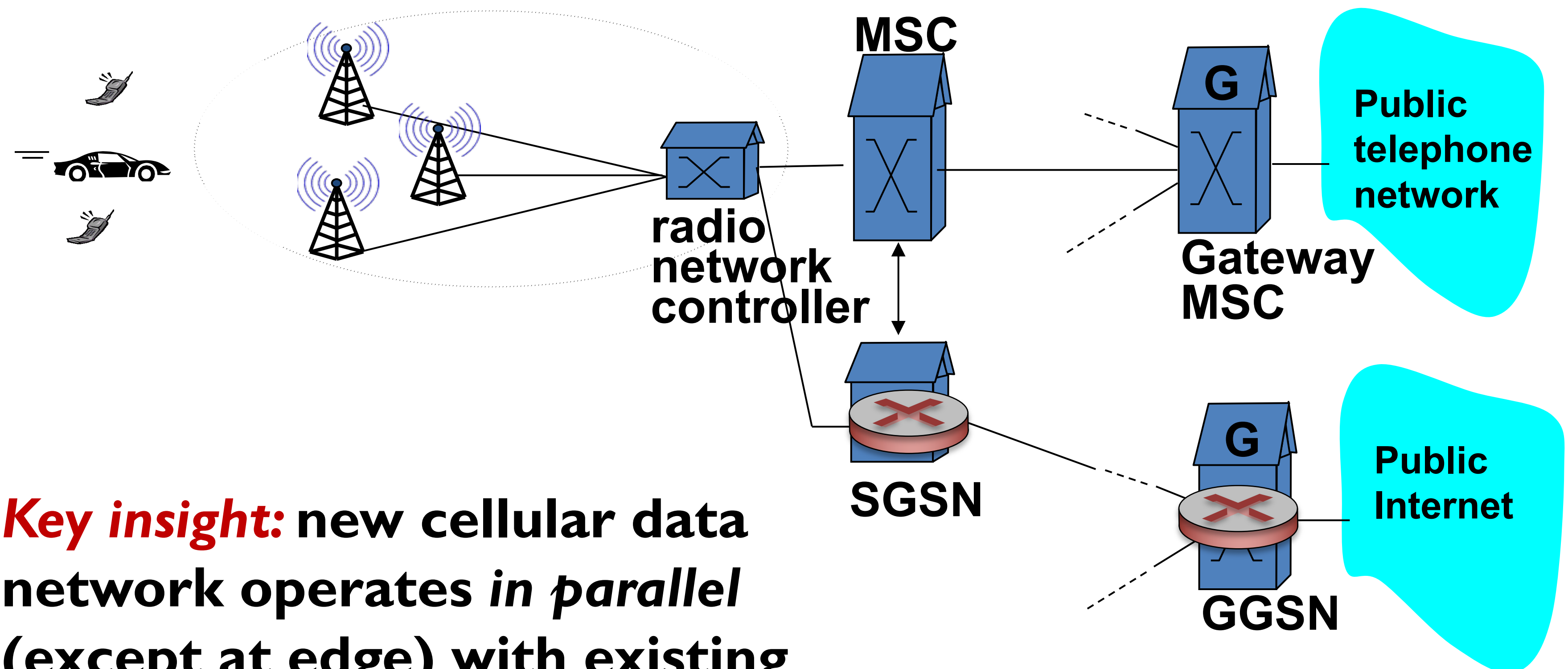
- combined FDMA/TDMA: divide spectrum in frequency channels, divide each channel into time slots
- CDMA: code division multiple access



2G (voice) network architecture

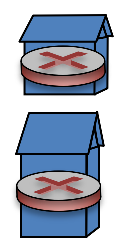


3G (voice+data) network architectur



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

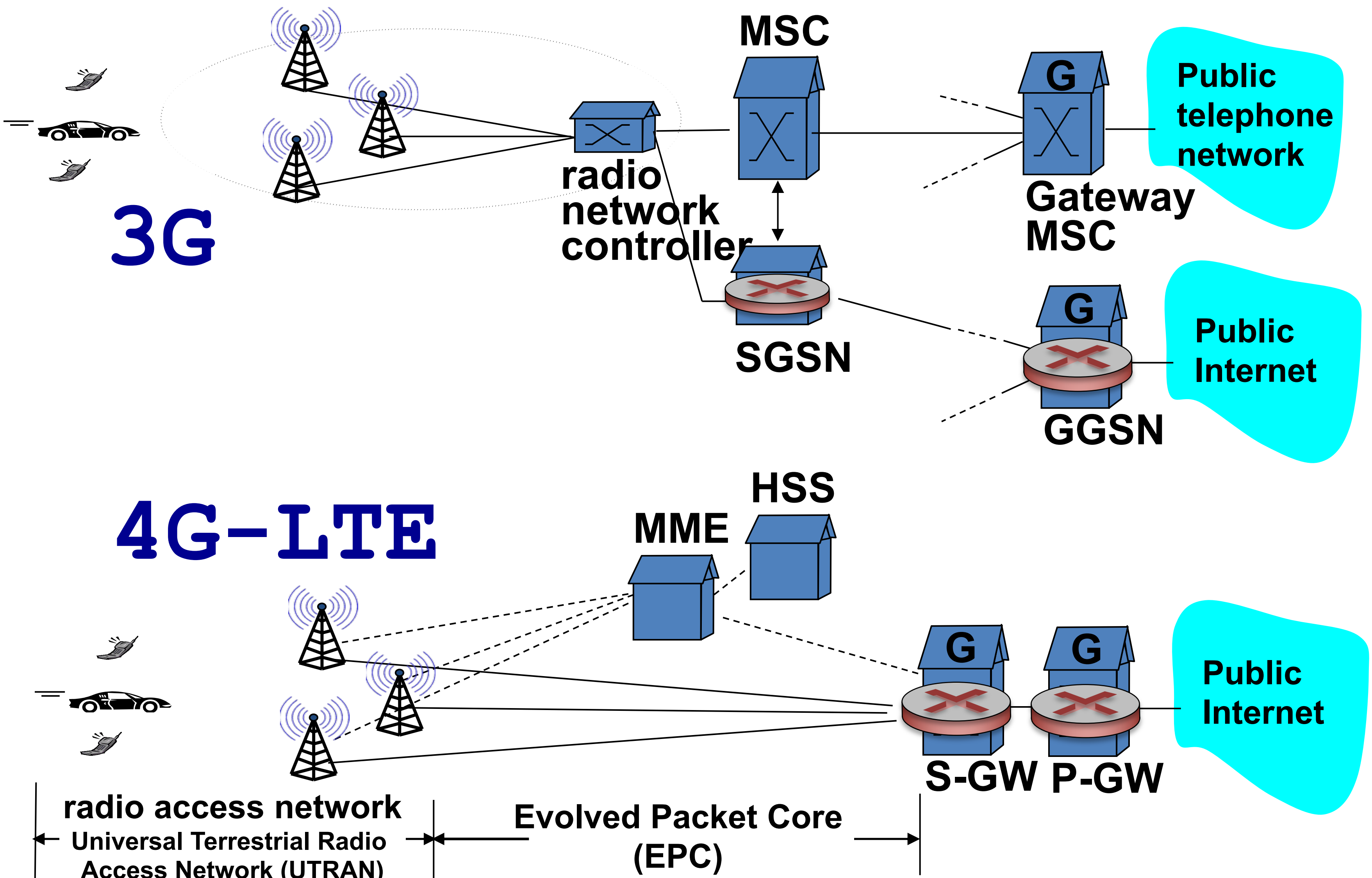
- voice network ***unchanged*** in core
- data network operates in parallel



Serving GPRS Support Node (SGSN)

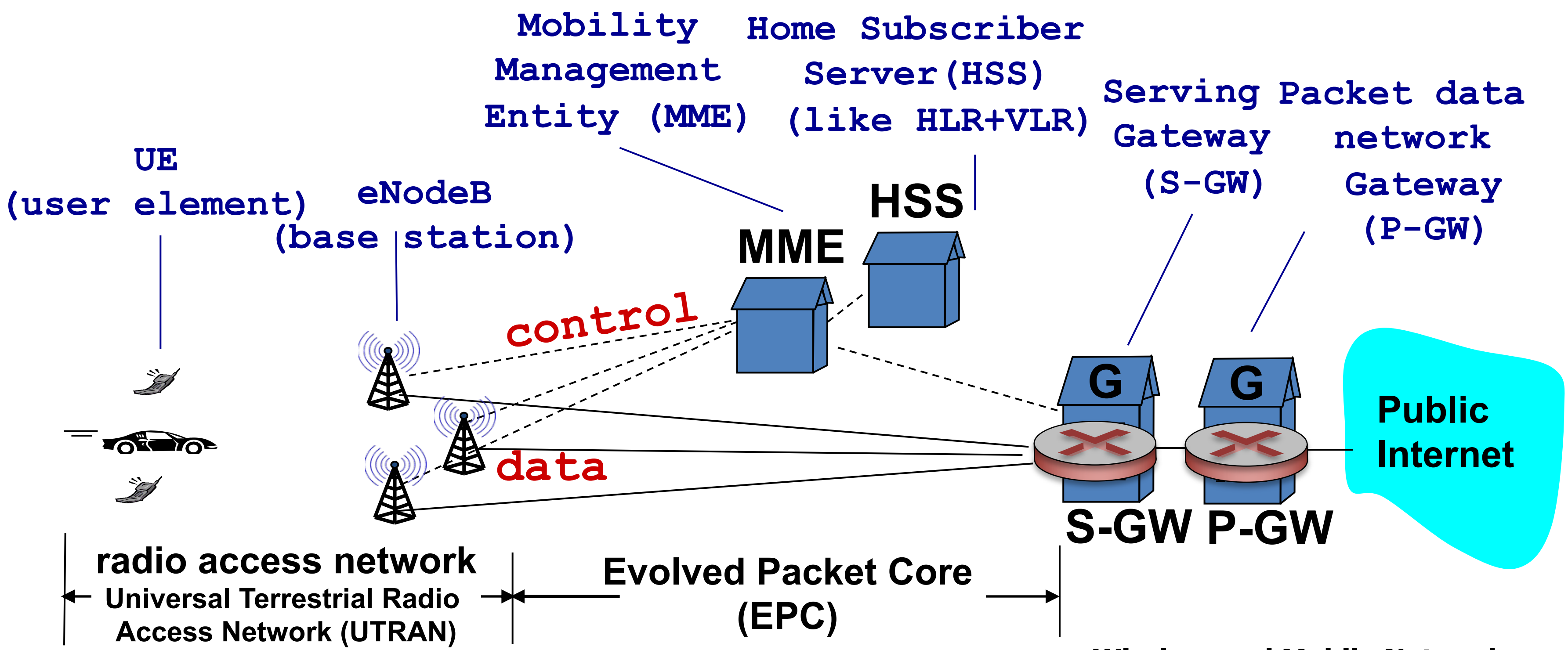
Gateway GPRS Support Node (GGSN)

3G versus 4G LTE network architecture



4G: differences from 3G

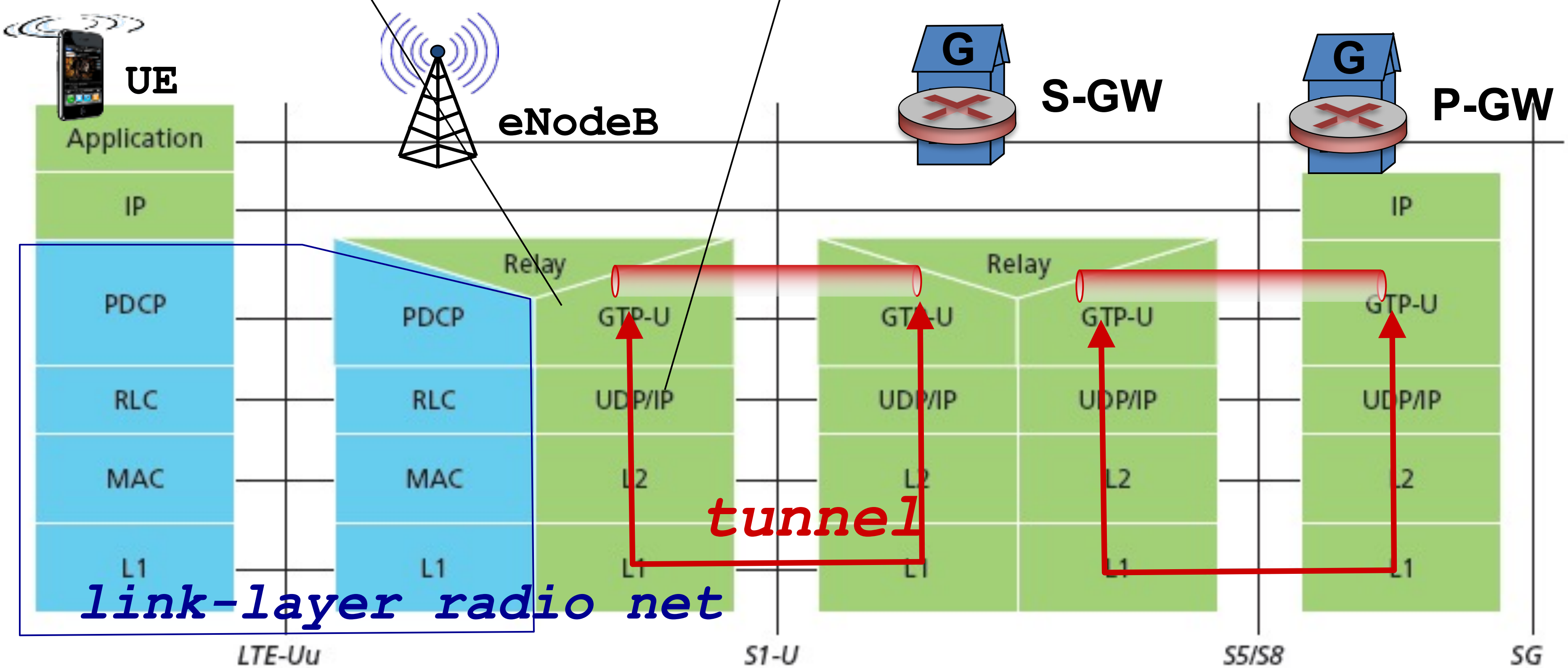
- all IP core: IP packets tunneled (through core IP network) from base station to gateway
- no separation between voice and data – all traffic carried over IP core to gateway



Radio+Tunneling: UE – eNodeB – PGW

IP packet from UE encapsulated in GPRS Tunneling Protocol (GTP) message at ENodeB

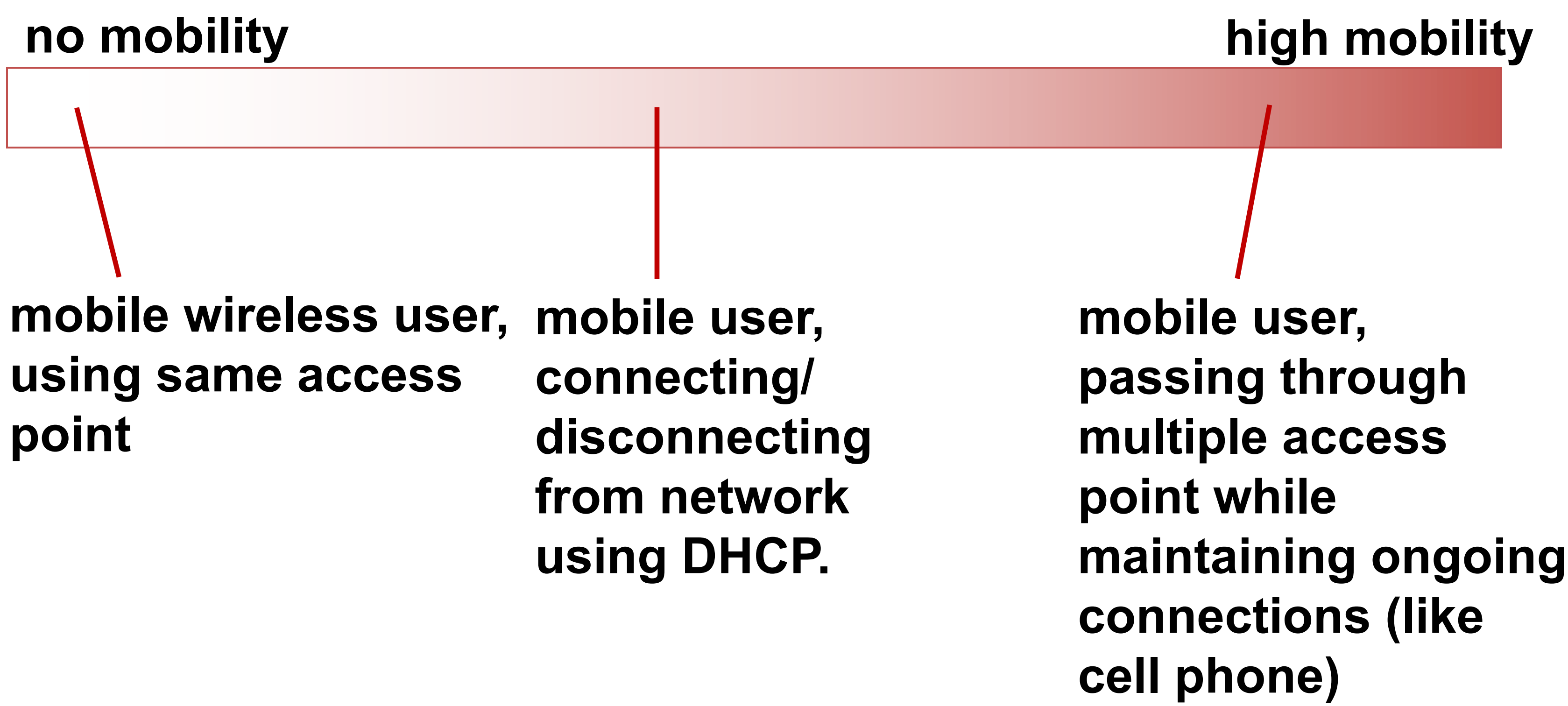
GTP message encapsulated in UDP, then encapsulated in IP. large IP packet addressed to SGW



Mobility

What is mobility?

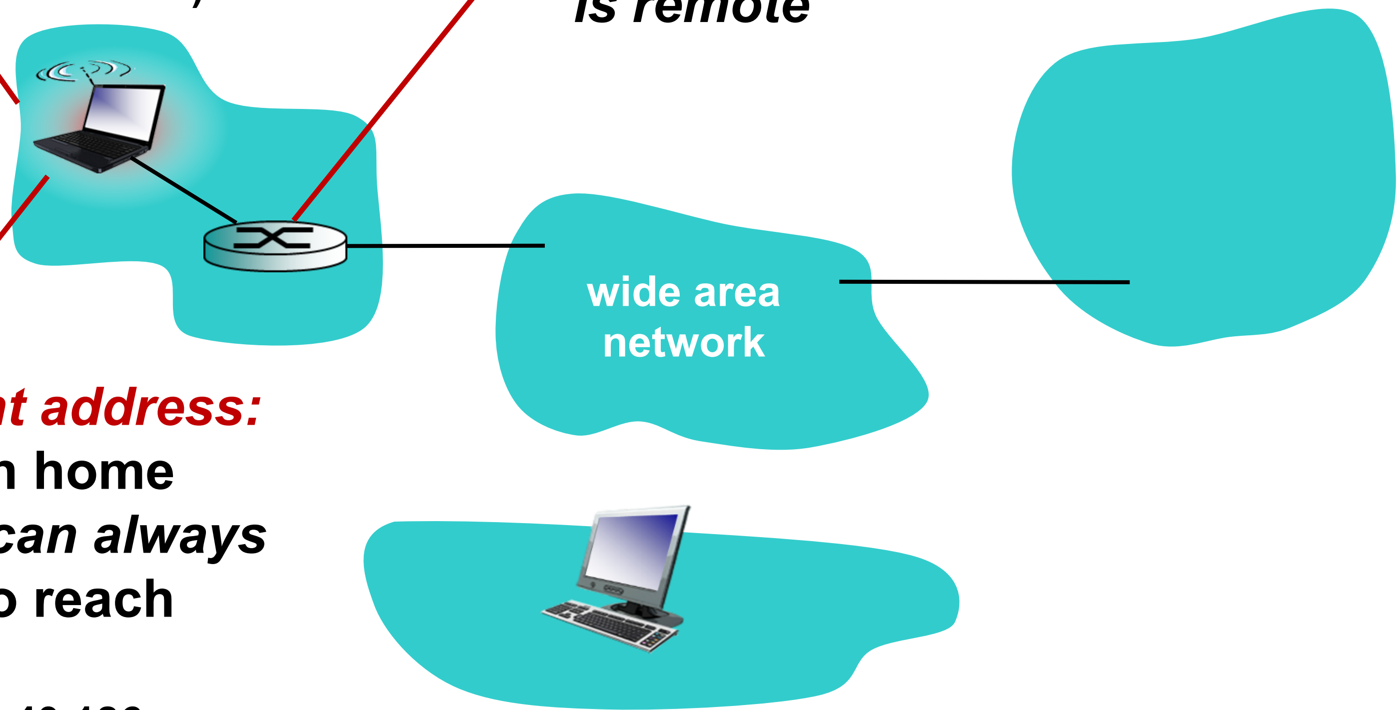
- spectrum of mobility, from the *network* perspective:



Mobility: vocabulary

home network: **permanent "home" of mobile**
(e.g., 128.119.40/24)

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



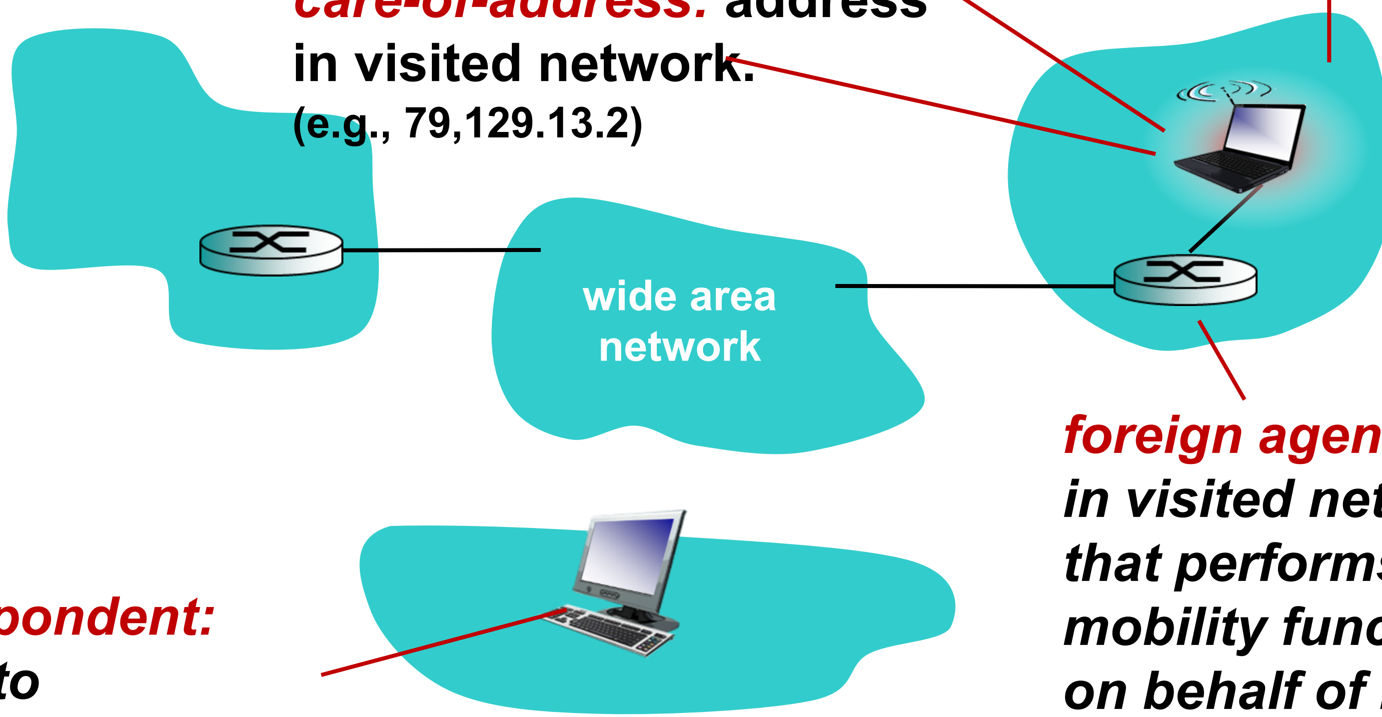
permanent address: **address in home network, *can always* be used to reach mobile**
e.g., 128.119.40.186

Mobility: more vocabulary

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

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

care-of-address: **address in visited network. (e.g., 79,129.13.2)**



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 ad… obile-nodes-in-residence via … g table exchange.
  - routing tables i… where each mobile located
  - no changes to end-systems

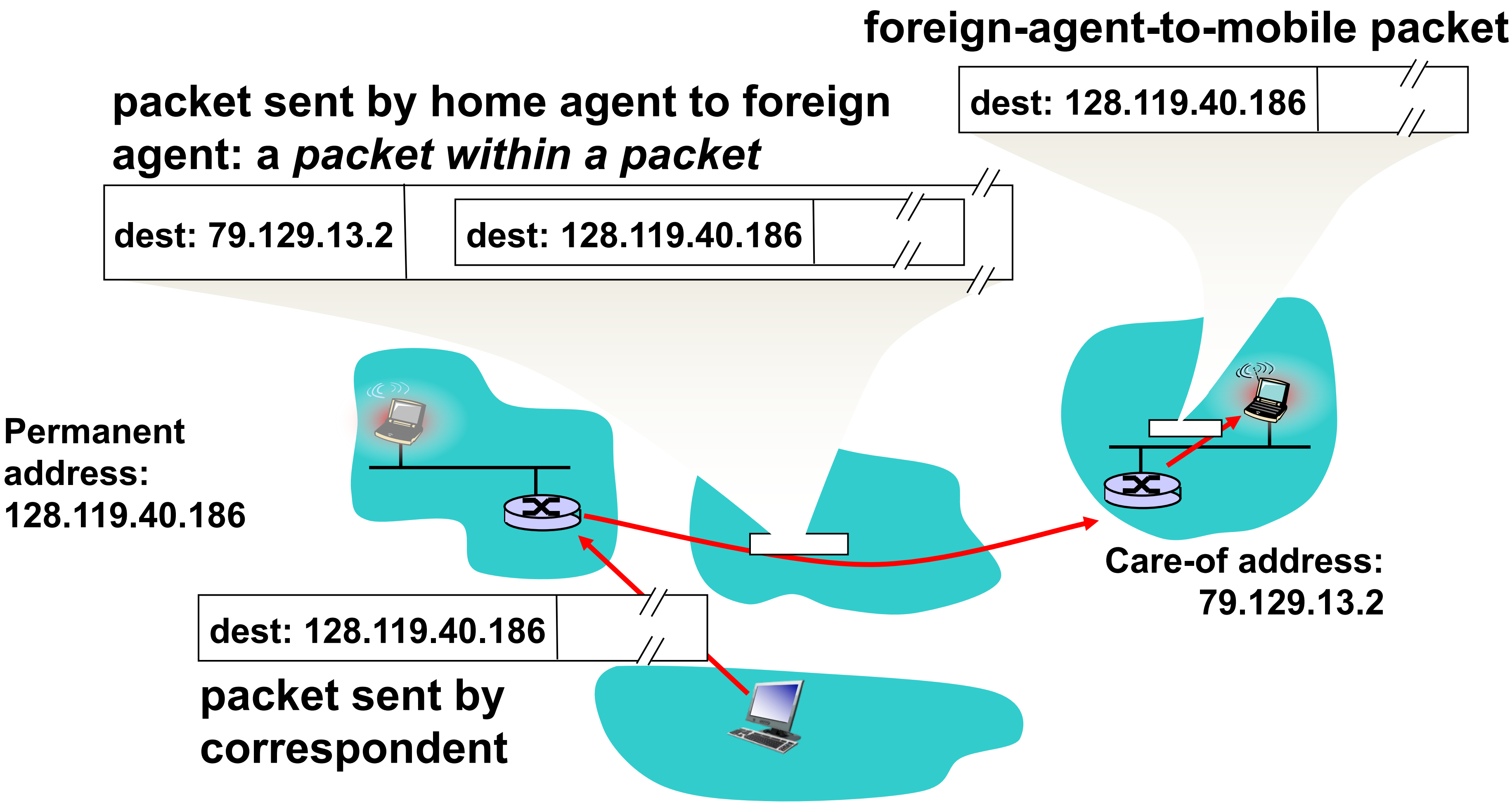
not
scalable
to millions of
mobiles

- *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

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

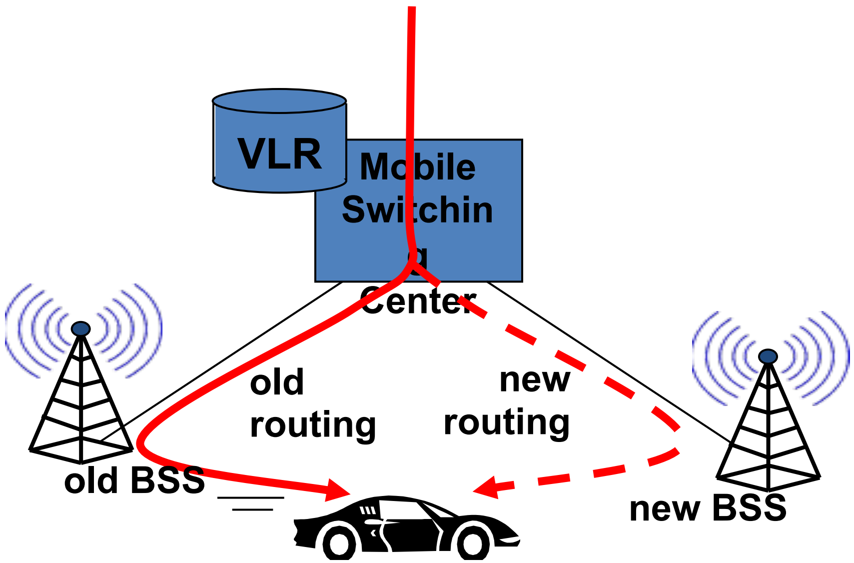
Mobile IP: indirect routing



Handling mobility in cellular networks

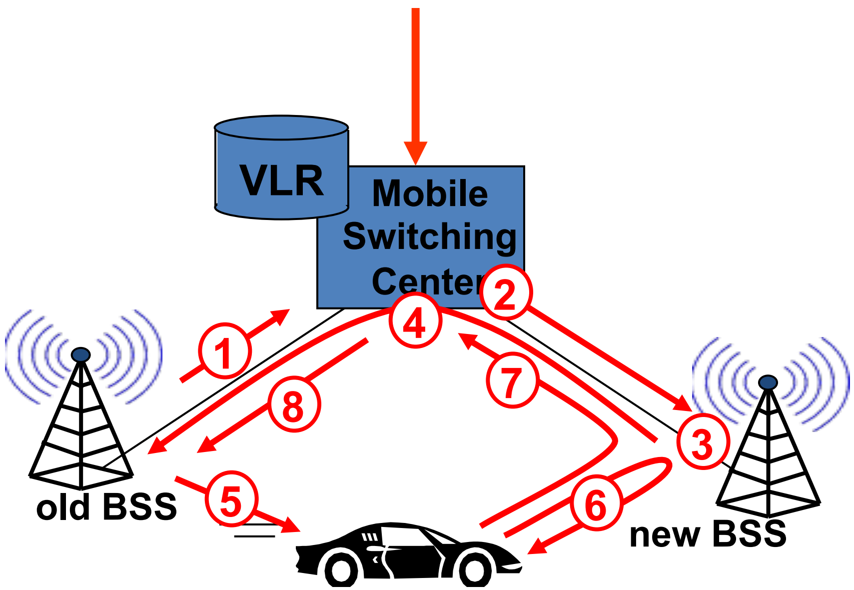
- *home network:* network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - *home location register (HLR):* database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- *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: 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 doesn't mandate why to perform handoff (policy), only how (mechanism)
- handoff initiated by old BSS

GSM: handoff with common MSC

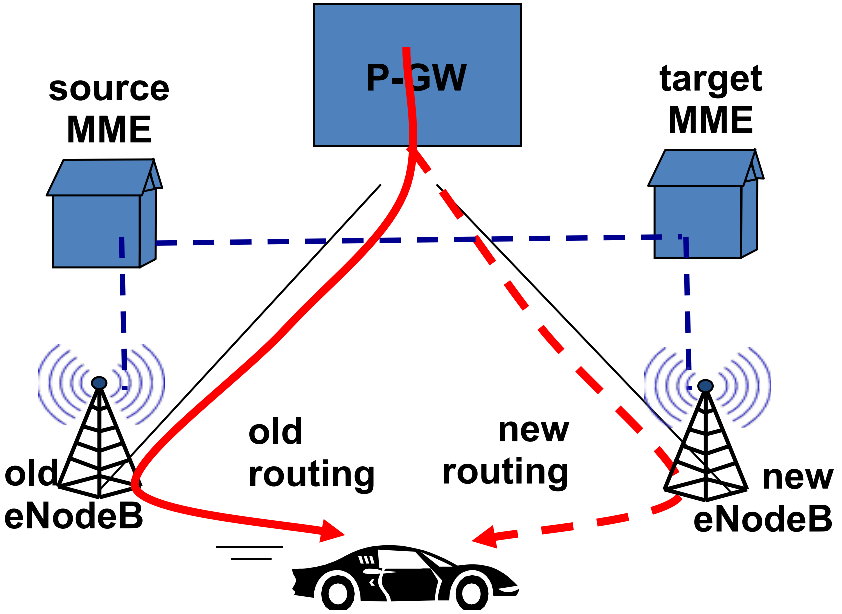


1. old BSS informs MSC of impending handoff, provides list of 1^+ new BSSs
2. MSC sets up path (allocates resources) to new BSS
3. new BSS allocates radio channel for use by mobile
4. new BSS signals MSC, old BSS: ready
5. old BSS tells mobile: perform handoff to new BSS
6. mobile, new BSS signal to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

8 MSC-old-BSS resources released

Handling Mobility in LTE

- Paging: idle UE may move from cell to cell: network does not know where the idle UE is resident
  - paging message from MME broadcast by all eNodeB to locate UE
- **handoff: similar to 3G:**
  - **preparation phase**
  - **execution phase**
  - **completion phase**



Impact on Higher-Layer Protocols

- Wireless and mobility change path properties
  - Wireless: higher packet loss, not from congestion
  - Mobility: transient disruptions, and changes in RTT
- Logically, impact should be minimal …
  - Best-effort service model remains unchanged
  - TCP and UDP can (and do) run over wireless, mobile
- But, performance definitely *is* affected
  - TCP treats packet loss as a sign of congestion
  - TCP tries to estimate the RTT to drive retransmissions
  - TCP does not perform well under out-of-order packets
- Internet not designed with these issues in mind

Conclusions

- Wireless
  - Already a major way people connect to the Internet
  - Gradually becoming more than just an access network
- Mobility (not discussed)
  - Today's users tolerate disruptions as they move
  - … and applications try to hide the effects
  - Tomorrow's users expect seamless mobility
- Challenges the design of network protocols
  - Wireless breaks the abstraction of a link, and the assumption that packet loss implies congestion
  - Mobility breaks association of address and location
  - Higher-layer protocols don't perform as well