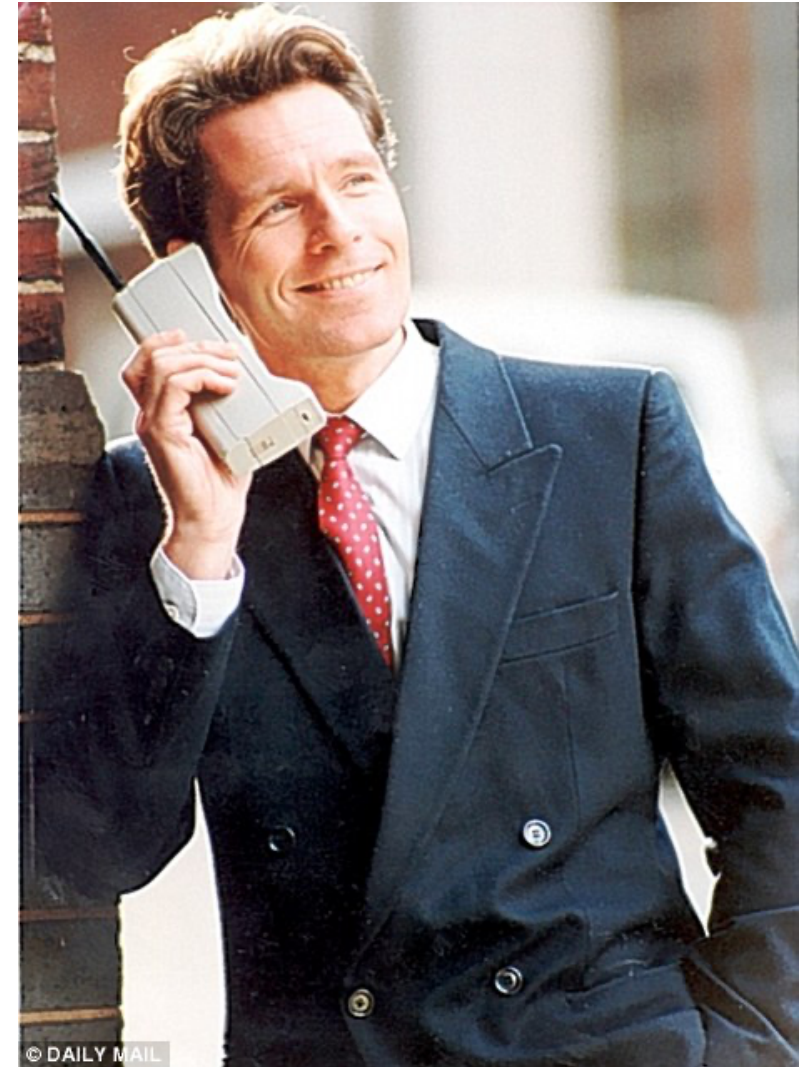


CS-340 Introduction to Computer Networking

Lecture 17: Mobility

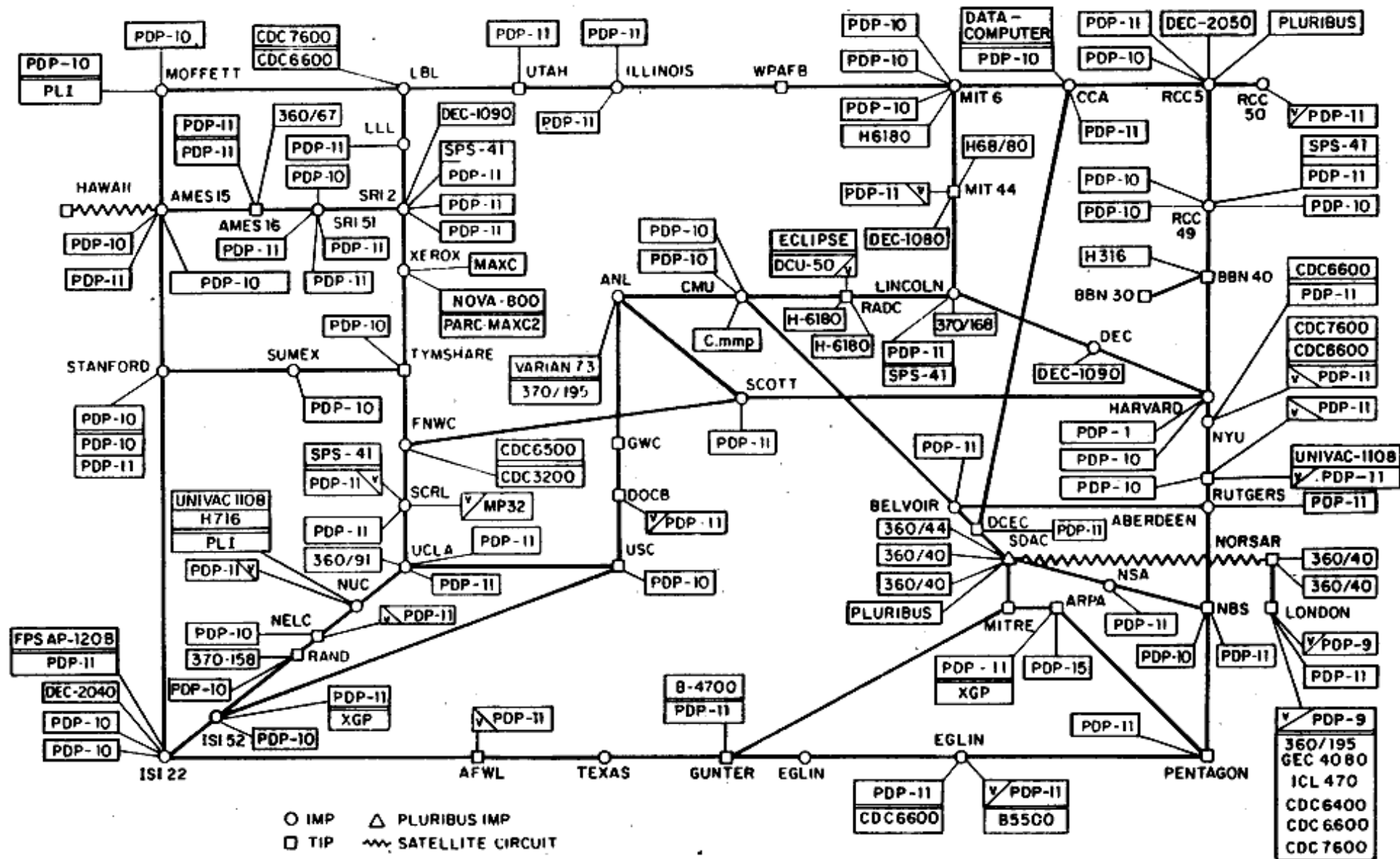
Steve Tarzia



Last Lecture: Authentication

- **Digital signatures** are special bit sequences attached to documents that can only be computed by the holder of a private key.
 - Signatures are used to establish **transitive trust** and verify new public keys, thus preventing **Man In The Middle** and other attacks.
 - **Certificate authorities** verify public keys with digitally signed certificates.
 - MITM with root authority's private key can forge arbitrary certificates.
- **Cryptographic hash** functions are irreversible and unpredictable.
 - Used to create a small summary of a document than can be signed with RSA.
 - Also used in **Message Authenticate Codes** (HMAC) to verify that sender has a shared secret: $MAC = \text{hash}(\text{message} + \text{key})$
- **Transport Layer Security (TLS)** encrypts a TCP stream.
 - Details are complex, to allow many different systems to interoperate and to mitigate a variety of attacks: Eg., packet replay, connection replay.

ARPANET LOGICAL MAP, MARCH 1977



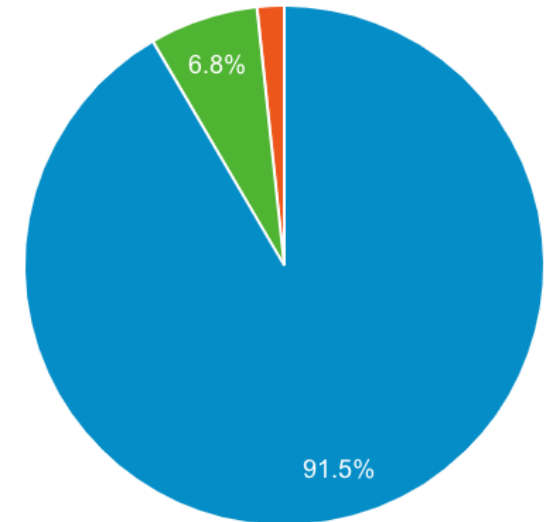
(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Mobility

- Internet protocols were designed assuming that hosts are fixed.
 - Wireless radios + battery-powered computers = *mobile computing*
 - *Smartphones* are now more common than wired hosts.
- February 2020 unique users on gunmemorial.org website:

	697,251	697,251
	% of Total: 100.00% (697,251)	% of Total: 100.00% (697,251)
1. ■ mobile	637,915	91.55%
2. ■ desktop	47,179	6.77%
3. ■ tablet	11,738	1.68%




Types of mobility

- Wireless enables mobility, but it's not the same thing

no mobility

high mobility



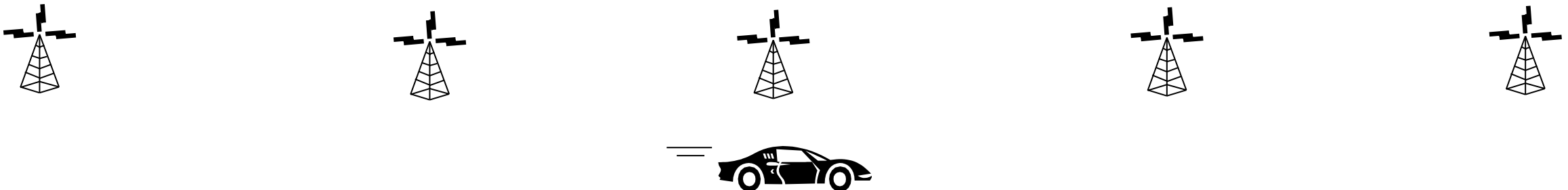
Wireless user always using same access point.
(eg., ALOHA)

Your **laptop**, connecting to different networks using DHCP.

Smartphone passing through various base stations while maintaining a connection.

IP addresses and mobility

- Applications use sockets to connect to \langle IP address, port \rangle .
- IP address cannot change during connection.
- Eg., consider a mobile user watching a YouTube video.
- Service is designed to use a single TCP connection to send all data.
- Changing IP address would require requesting the video again.
- Laptop users experience application interruptions when moving between networks. Somehow, cellular data continues smoothly.



Why not use BGP for mobility?



- BGP allows routes to change.
- Theoretically, it could be used to let your one IP address roam between different parts of the Internet, even through different AS's.
- But this would add a lot of load to BGP and would be too slow.
- Core routers would need hundreds of millions of extra /32 routes as smartphones moved between networks.
 - We would lose the benefits of route aggregation (due to blocks of addresses being in one place).
 - Core routers are already a bottleneck for the Internet's speed.
- Solution: do some kind of routing/redirection at the network edge.

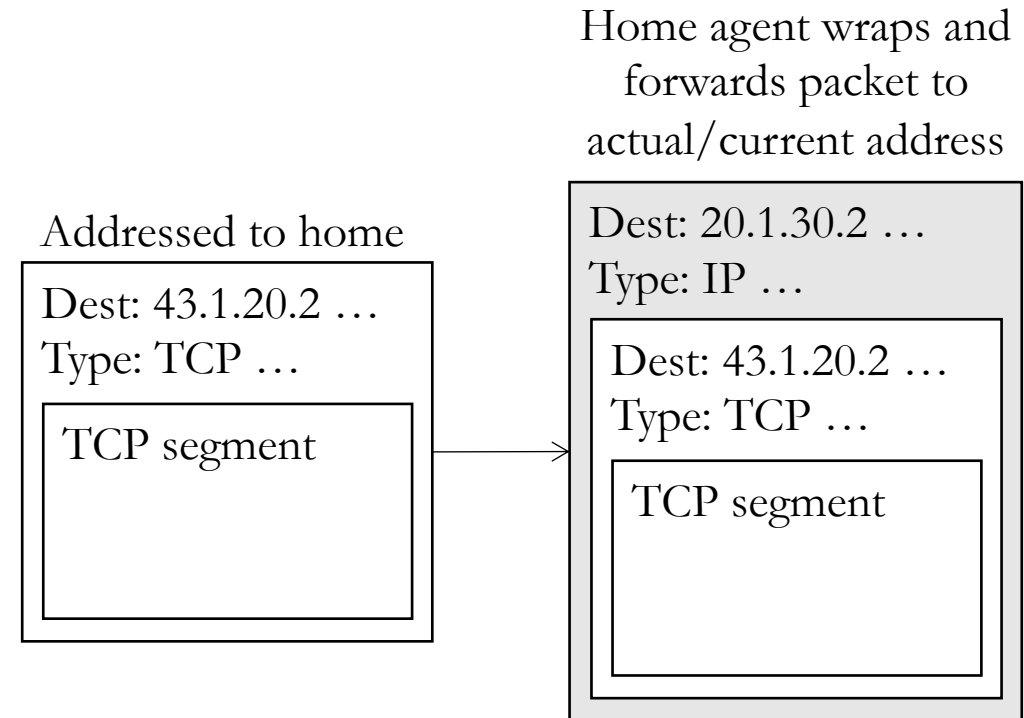
Transient youth analogy

- Young adults' mailing addresses are very “mobile”
 - Various dorm rooms, sublets, internships, first few jobs, ...
- Also true for active-duty military.
- How can we send a package or letter to a friend whose last-known address may be out of date?
 - Use some other permanent connection to request address (SMS/Facebook).
 - Send package to parent's house.
 - Ask parent for child's address.
 - Send package to Army Post Office (APO) or Fleet Post Office (FPO).
- We need to contact some **permanent address**.



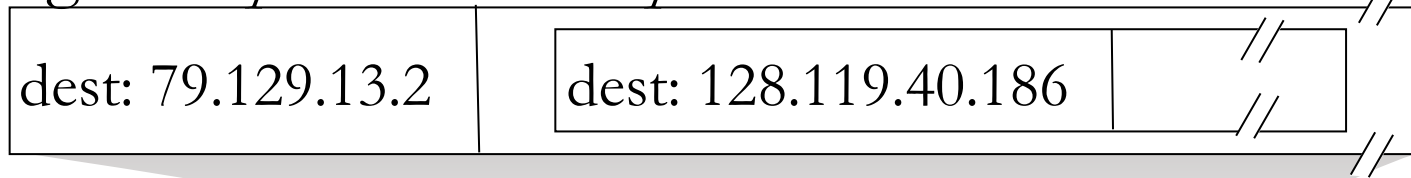
IP Tunnel

- Remember how we sent IPv6 packets through old routers by wrapping them in IPv4 packets? That's an example of IP tunneling.
- Also use **IP tunnel** for mobile IP.
- Mobile client registers its temporary address to **home agent**.
- Home agent is the router responsible for home address' subnet.
- Packets are addressed to home address, received by home agent, and encapsulated in packet addressed to temporary address and forwarded.

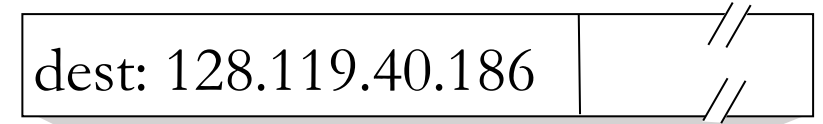


Indirect Routing

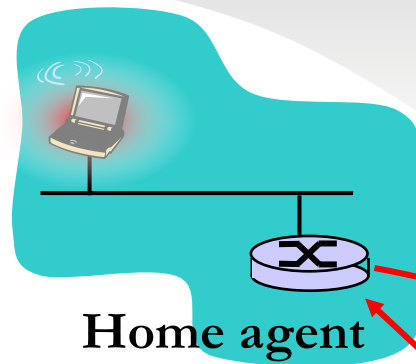
packet sent by home agent to foreign agent: a *packet within a packet*



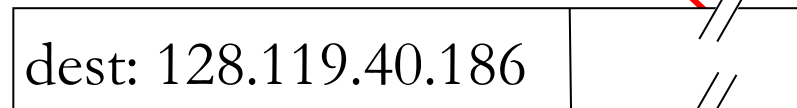
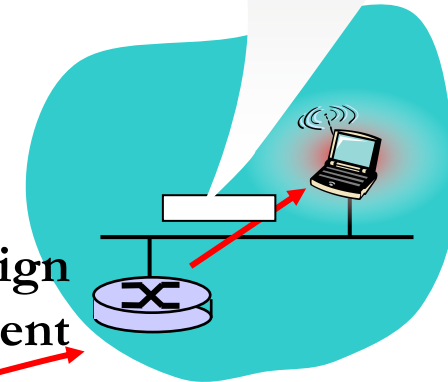
foreign-agent-to-mobile packet



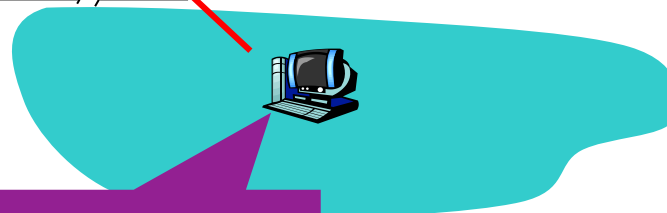
Permanent address:
128.119.40.186
(*virtual* location)



Foreign agent



packet sent by correspondent



Message source

Mobile IP details (RFCs [3344](#), [5944](#))

- **Home agent** is router that receives packets addressed to **home address**.
- **Foreign agent** is router that delivers packets at final hop.
 - Its address is the **care-of address**.

Setup:

1. Mobile host uses a protocol similar to DHCP to find Foreign Agt.
2. Mobile host *registers* Home Agt and home address with Foreign Agt.
3. Foreign Agt relays registration to Home Agt.

Operation:

1. Home Agt receives packets addressed to home address
2. Home Agt *encapsulates* packet, addressing it to care-of address
3. Foreign Agt receives encapsulated packet, and *unpacks* it.
4. Foreign Agt sends packet to mobile host (using MAC address)

Smartphone Push Notifications

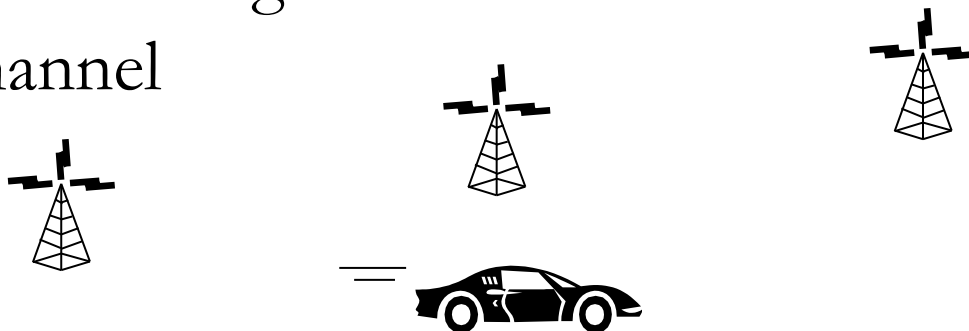
- *Location registration* is also used for iOS and Android push notifications.
- Whenever phone gets a new IP address, the OS registers that address with a central push notification server. It gets: $\langle \text{user id, IP address} \rangle$
- Smartphone apps like WhatsApp or Snapchat send user notifications to the iOS/Android push notification server: $\langle \text{user id, message} \rangle$
 - The push notification server relays the message to the user's current IP addr.
- On iOS, to protect users' privacy, different apps have different user ids (called device tokens).
- How to deal with NAT?
 - *OS sends keepalive msgs.*
 - *Just one active TCP socket is needed for all apps.*



Link-Layer Handoff

- Generally speaking, **handoff** is the act of transferring an ongoing connection from one channel to another.
- Basic handoff steps:
 1. Notice that first channel is weak or crowded
 2. Find a superior second channel
 3. Join the second channel
(now we are using both channels)
 4. Tell “router” that second channel should be used
 5. Notice that data is arriving on second channel
 6. Close the first channel

In WiFi, alternative “channels” correspond to different base stations advertising the same network id (ssid). Probably on a different frequency.

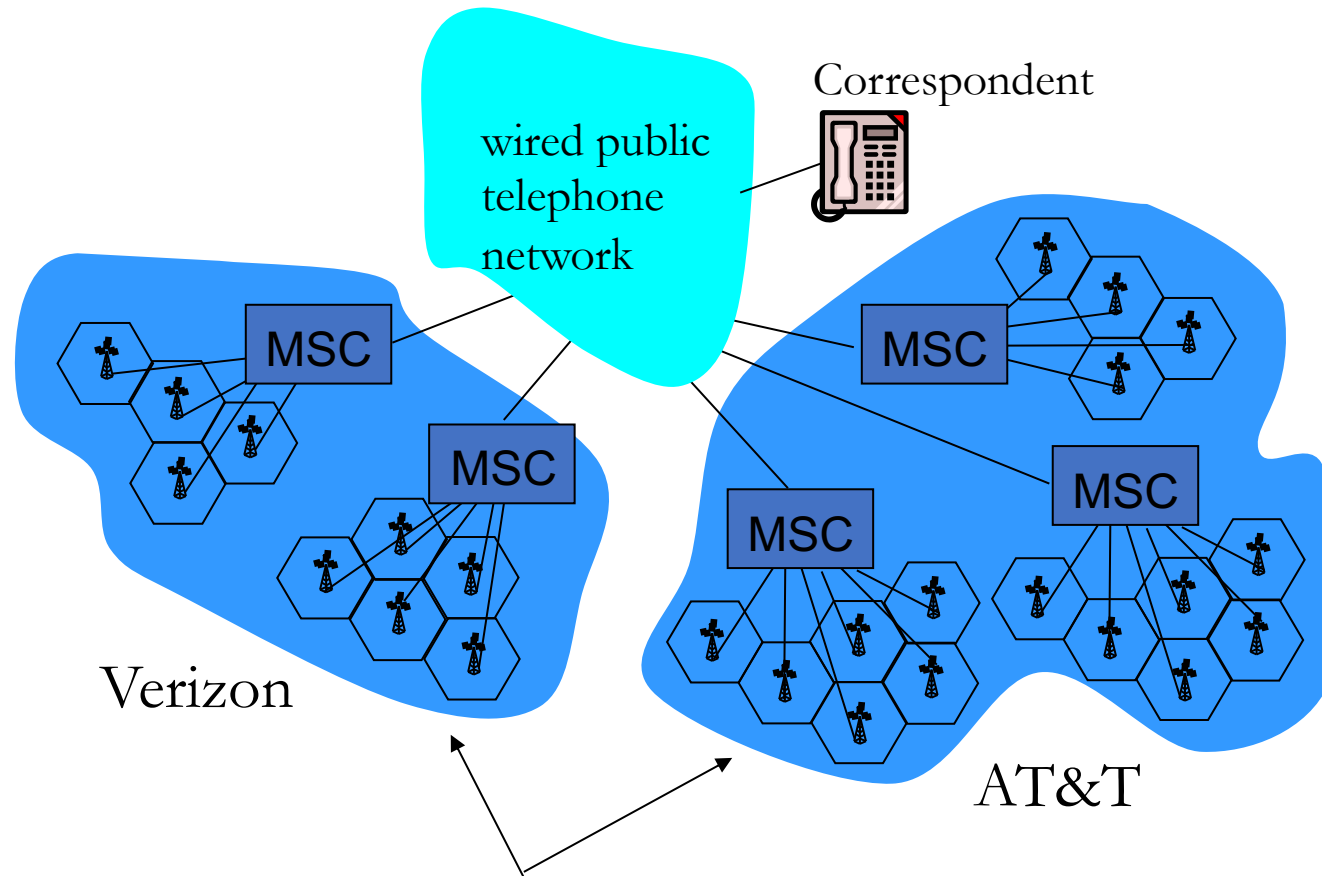


TCP behavior on mobile wireless

- Recall that TCP assumes that packet loss is due to congestion.
- However *wireless noise* and *handoff* can cause temporary packet loss.
- Congestion window may be reduced unnecessarily.
- In other words, TCP was design with the assumption that hosts are stationary.
- Mobile-aware TCP is an active area of research.

GSM cellular connections

- Basic idea is same as mobile IP, but it operates at the Link Layer.



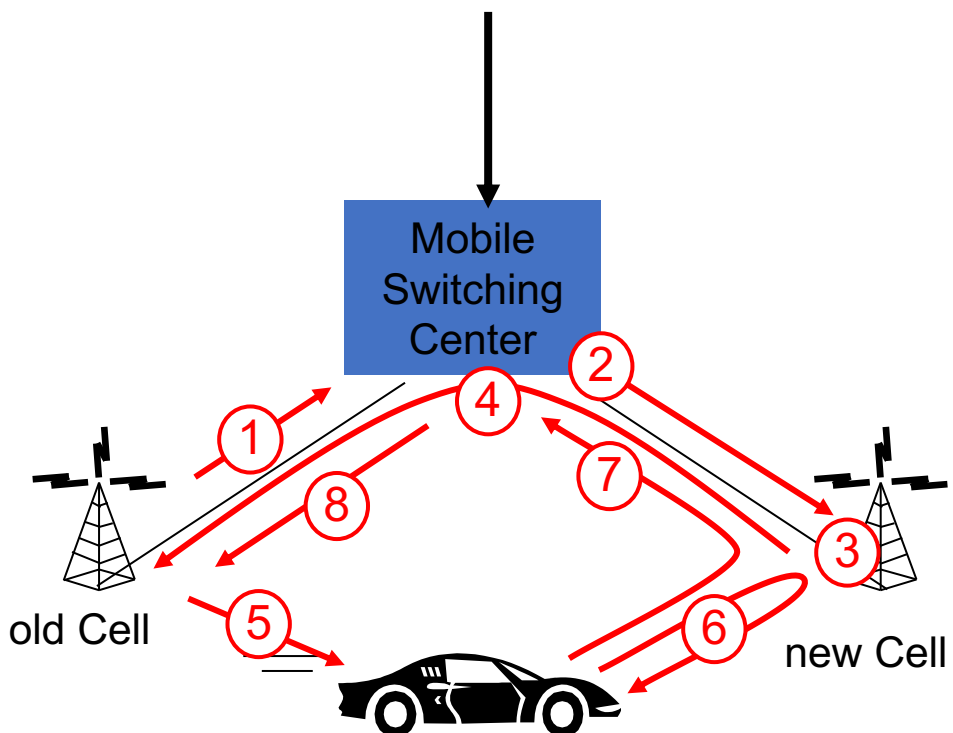
Verizon

AT&T

Different cellular networks,
operated by different providers

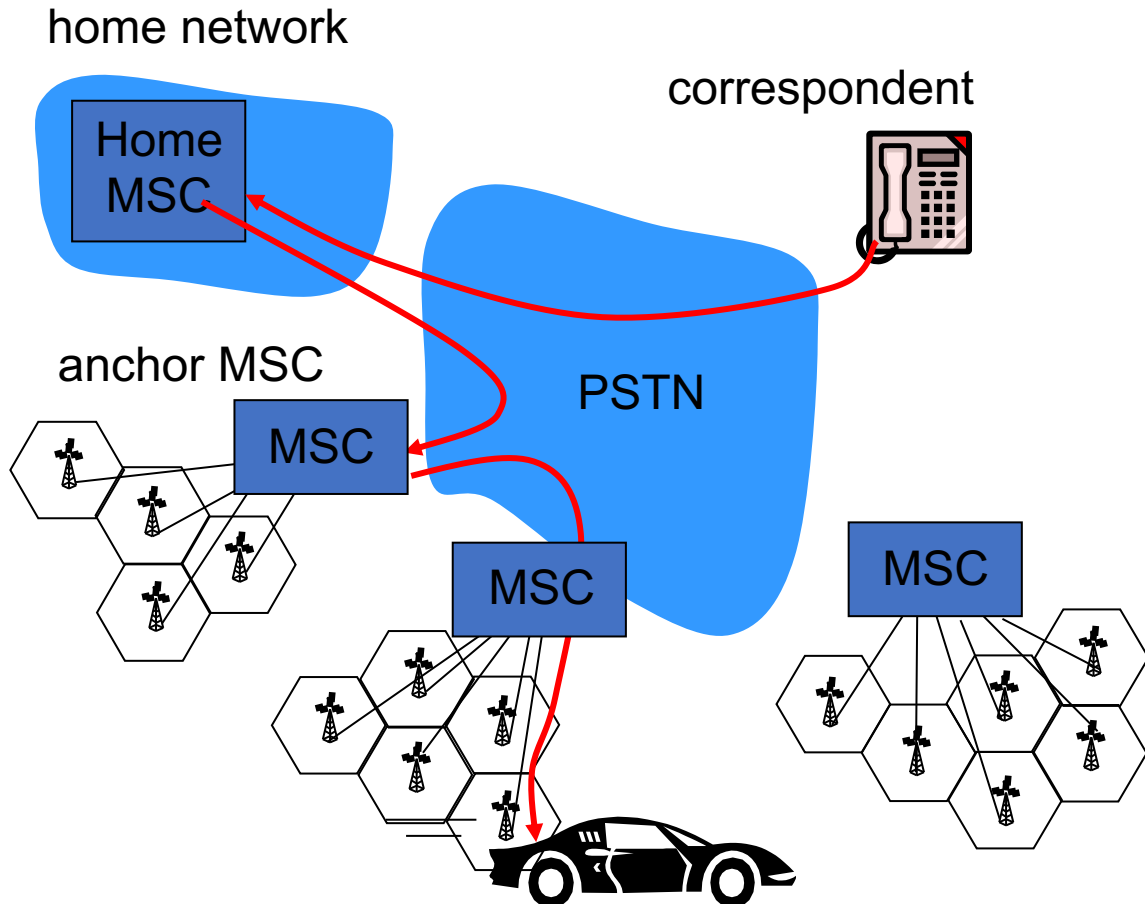
MSC: *Mobile Switching Center* routes traffic to/from multiple “cells.” MSC is the equivalent of an edge router.

Handoff within a Mobile Switching Center



1. Old Cell informs MSC of impending handoff, provides list of new Cells
2. MSC sets up path (allocates resources) to new Cell
3. New Cell allocates radio channel for use by mobile.
4. New Cell signals MSC, old Cell: ready
5. Old Cell tells mobile: handoff to new Cell
6. Mobile & new Cell activate new channel
7. Mobile signals via new Cell to MSC: handoff complete. MSC reroutes call
8. MSC-old-Cell resources released

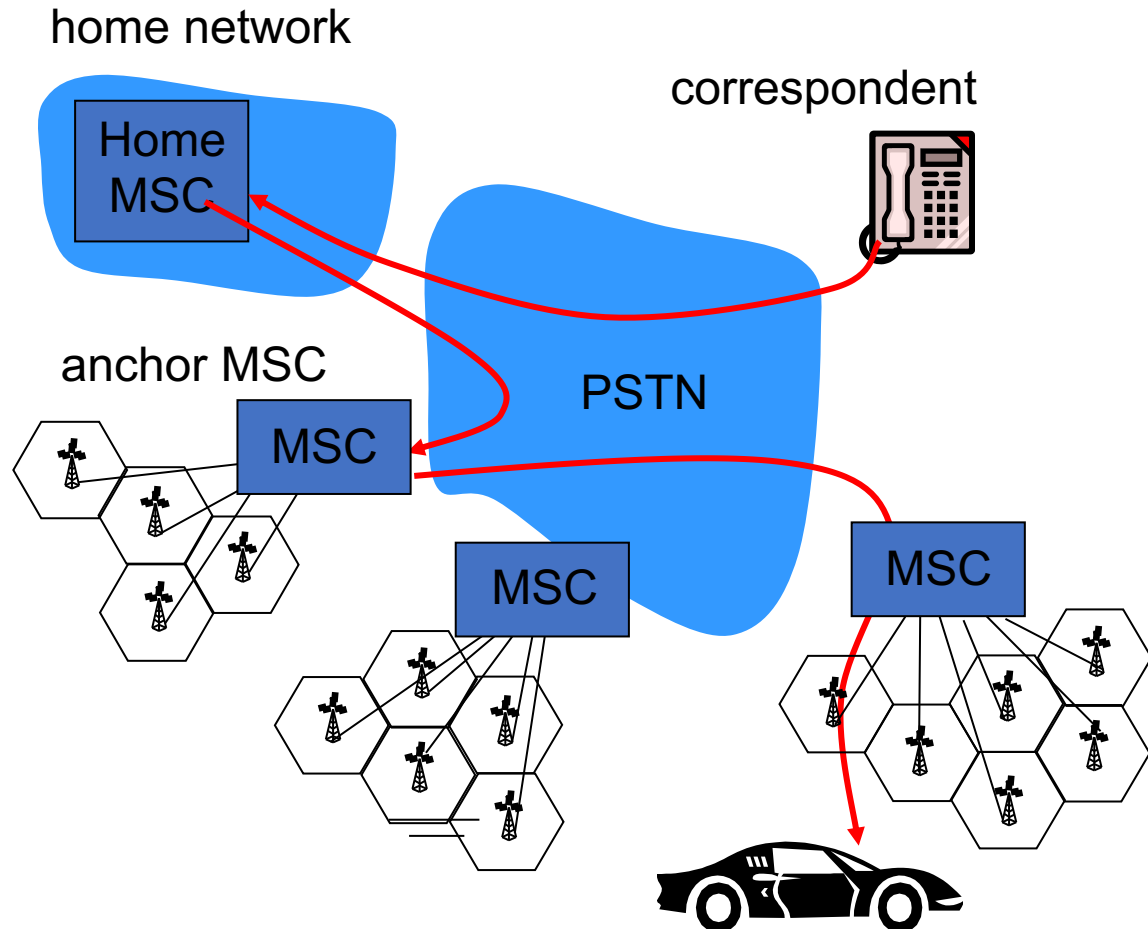
Handoff between MSCs



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.
- Optionally bypass intermediate MSCs to shorten the multi-MSC chain.

Handoff between MSCs



b) After handoff & chain shortening

- **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.
- Optionally bypass intermediate MSCs to shorten the multi-MSC chain.

Recap

- IP addressing was designed for a static world.
- **Mobile IP** gives host a permanent **home address**.
 - Registers with **Foreign Agent** which registers with **Home Agent**.
 - Home agent encapsulates received traffic in **IP tunnel**, forwards traffic to foreign agent at **care-of address**.
- Smartphone push notifications also use **location registration**.
- **Handoff**: set up the 2nd channel, transfer connection, then close 1st.