This lecture is being recorded

18-452/18-750
Wireless Networks and Applications
Lecture 18: Wireless and the Internet

Peter Steenkiste

Spring Semester 2022

http://www.cs.cmu.edu/~prs/wirelessF22/

Announcements

- Midterm solutions will be posted on Wednesday
  - » Please use office hours for questions
  - » Regrade requests should be posted on gradescope (not office hours!)
- Homework 3 will also be posted later this week
- Project 2: I have given feedback on all proposals
  - » We have an interesting set of projects!
  - » However, many proposals were very vague about equipment
    - – "We were thinking about using this device"
  - » The equipment for teams that submitted proposals early has arrived – I will e-mail details

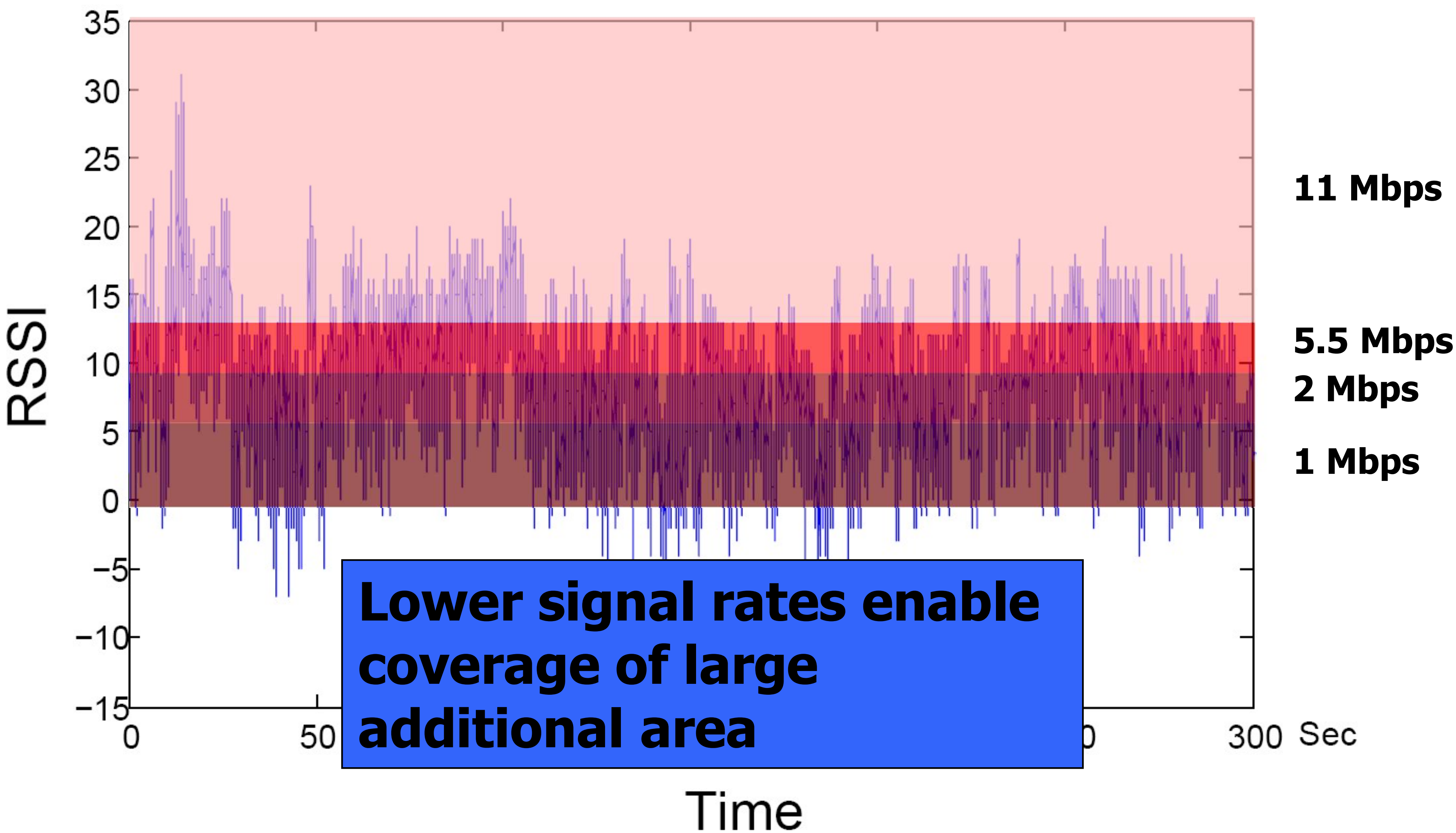
Outline

- WiFi deployments
  - » Planning
  - » Channel selection
  - » Rate adaptation
- The Internet 102
- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Disconnected operation
- Disruption tolerant networks

Bit Rate Adaptation

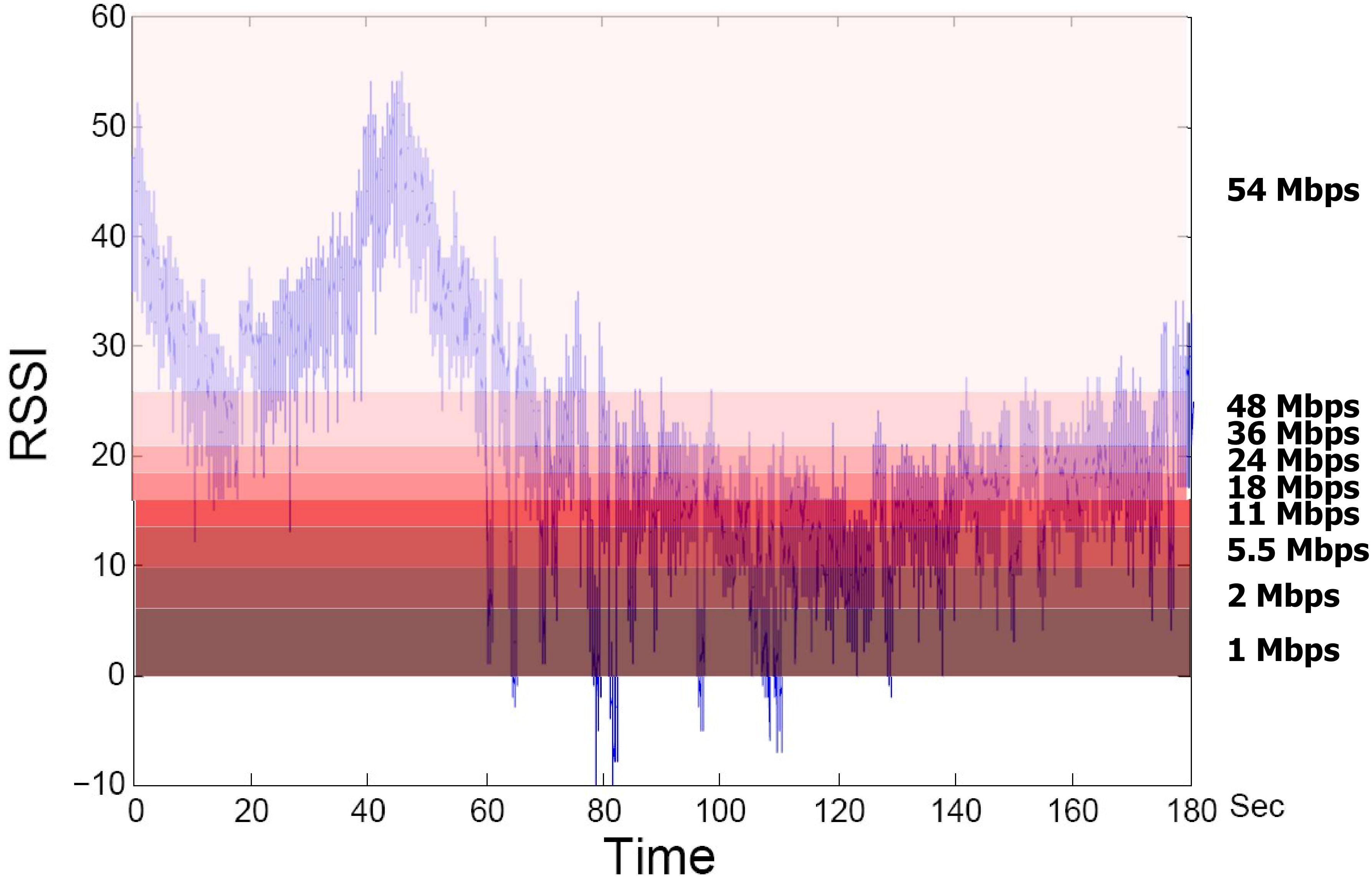
- All modern WiFi standards are multi bit rate
  - 802.11b has 4 rates, more recent standards have 10s
  - Vendors can have custom rates!
- Many factors influence packet delivery:
  - Fast and slow fading: nature depends strongly on the environment, e.g., vehicular versus walking
  - Interference versus WiFi contention: response to collisions is different
  - Random packet losses: can confuse “smart” algorithms
  - Hidden terminals: decreasing the rate increases the chance of collisions
- Transmit rate adaptation: how does the sender pick?

"Static" Channel



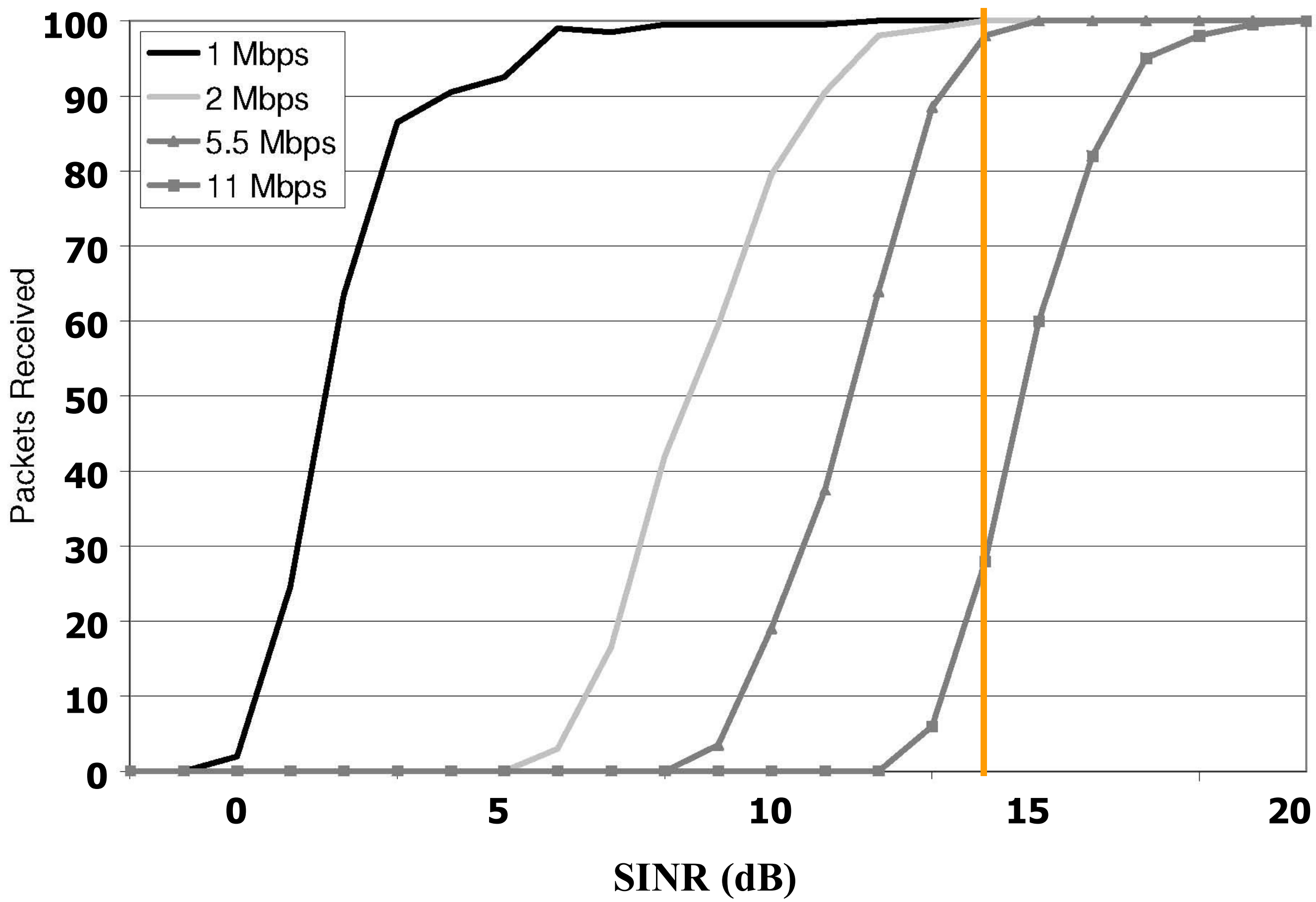
Lower signal rates enable coverage of large additional area

Mobile Channel – Pedestrian



Transmit Rate Selection

- **Goal: pick rate that provides best throughput**
  - **E.g. SINR 14 dB → 5.5 Mbps**
  - **Needs to be adaptive**



High Level Designs

- "Trial and Error": senders use past packet success or failures to adjust transmit rate
  - » Sequence of x successes: increase rate
  - » Sequence of y failures: reduce rate
  - » Hard to get x and y right
  - » Random losses can confuse the algorithm
- Senders use channel state information to pick transmit rate
  - » Early days: SNR …. Today: channel state matrix
  - » Assumes a relationship between PDR and channel state
    - – Need to recover if this fails, e.g., hidden terminals
- Today: need to consider other factors
  - » Different transmission modes, traffic load, …

CHARM

- **Channel-aware rate selection algorithm**
- **Transmitter passively determines SINR at receiver by leveraging channel reciprocity**
  - » **Determines SINR without the overhead of active probing (RTS/CTS)**
- **Select best transmission rate using rate table**
  - » **Table is updated (slowly) based on history**
  - » **Needed to accommodate diversity in hardware and special conditions, e.g., hidden terminals**
- **Jointly considers problem of transmit antenna selection**

SINR: Noise and Interference

$$\text{SINR} = \frac{\text{RSS}}{\text{Noise} + \sum \text{Interference}}$$

- Noise
  - » Thermal background radiation
  - » Device inherent
    - – Dominated by low noise amplifier noise figure
  - » ~Constant
- Interference
  - » Mitigated by CSMA/CA
  - » Reported as "noise" by NIC

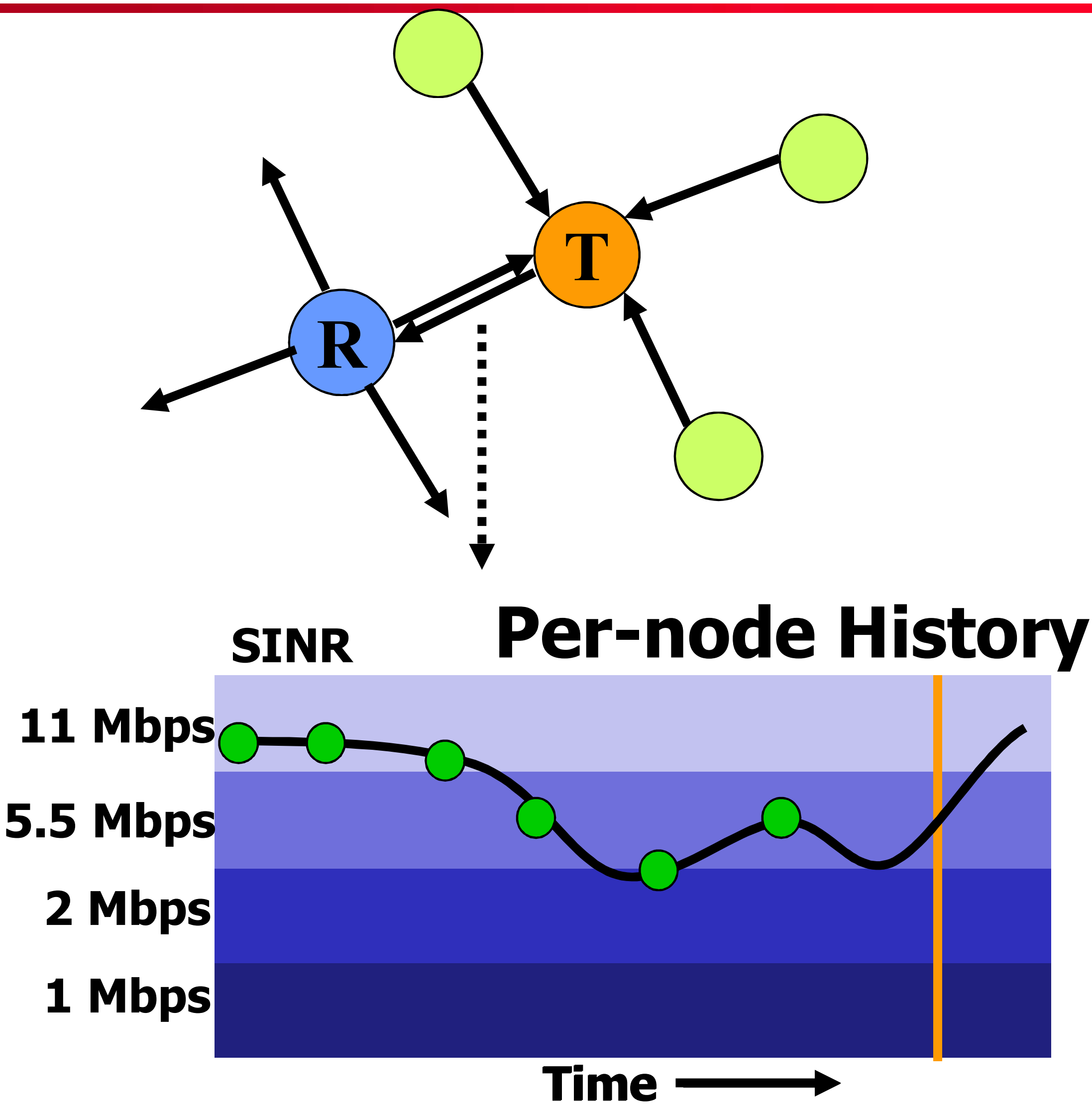
SINR: RSS

$$RSS = P_{tx} + G_{tx} - PL + G_{rx} \qquad (1)$$

$$PL = P_{tx} + G_{tx} + G_{rx} - RSS \qquad (2)$$

- **By the reciprocity theorem, at a given instant of time**
  - » $PL_{A \rightarrow B} = PL_{B \rightarrow A}$
- **A overhears packets from B and records RSS (1)**
- **Node B records P_{tx} and card-reported noise level in beacons and probes, so A has access to them**
- **A can then calculate path-loss (2) and estimate RSS and SINR at B**

CHARM: Channel-aware Rate Selection

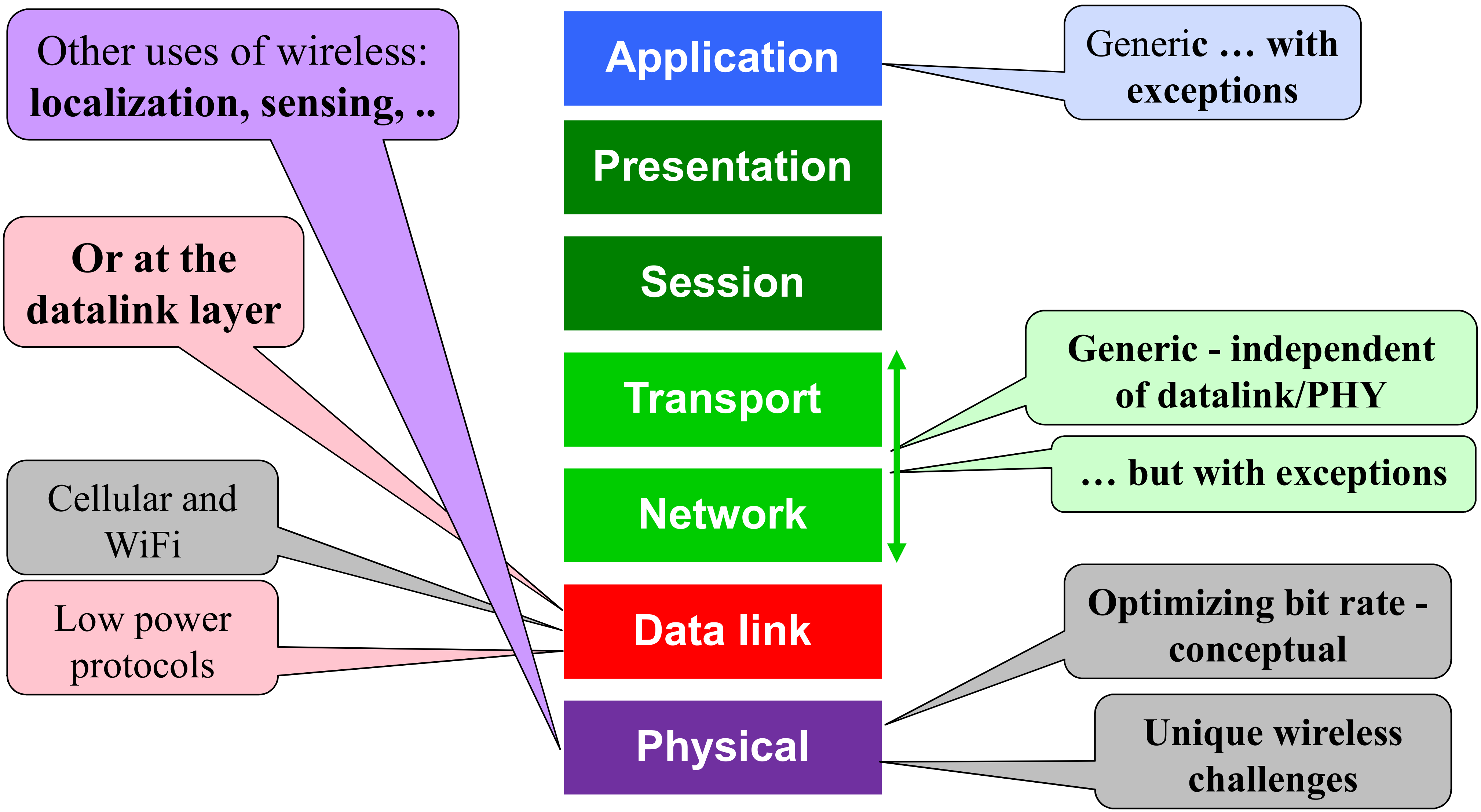


- Leverage reciprocity to obtain path loss
  - » Compute path loss for each host: P_{tx} - RSSI
- On transmit:
  - » Predict path loss based on history
  - » Select rate & antenna
  - » Update rate thresholds
- Today's algorithms use CSI but are much more sophisticated
  - » E.g., have to deal with more many more rates, MIMO, etc.

Outline

- Wireless and the Internet
- Mobility: Mobile IP
- TCP and wireless
- Applications and wireless
- Disruption tolerant networks

Course Overview



Wireless and the Internet Challenges

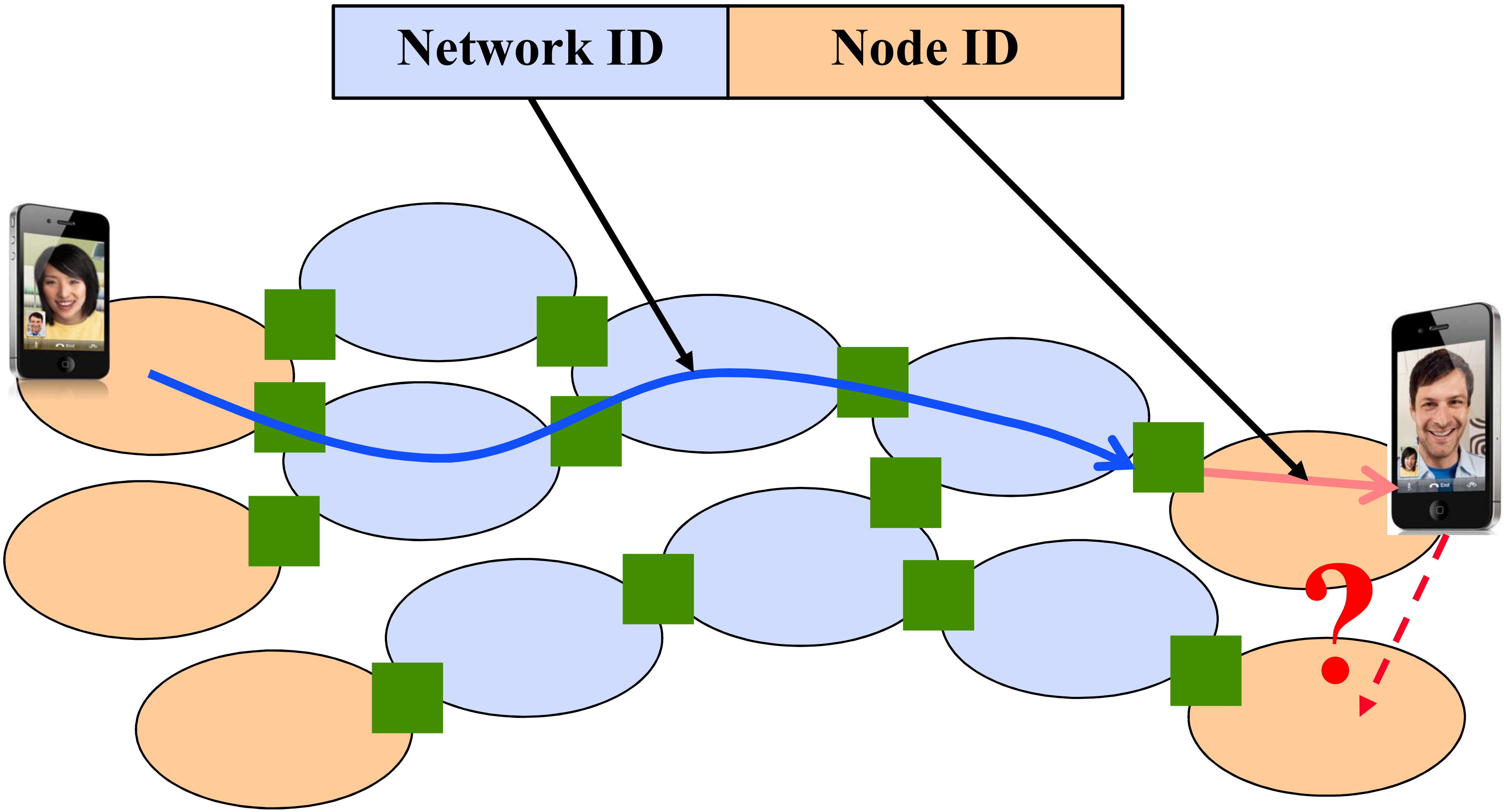
- Mobile hosts are hard to find
  - » Their address does not match the network they are in
- IP addresses are used both to forward packets to a host and to identify the host
  - » Active session break when a host moves
- TCP congestion control interprets packet losses as a sign of congestion
  - » Assumes links are reliable, so packet loss = full queue
- TCP is also very sensitive to latency!
  - » Wireless networks tend to have higher latencies
- Applications can no longer assume they are always connected to the Internet
  - » Mobile apps must support "disconnected" operations!

IP Address Structure

Network ID	Node ID

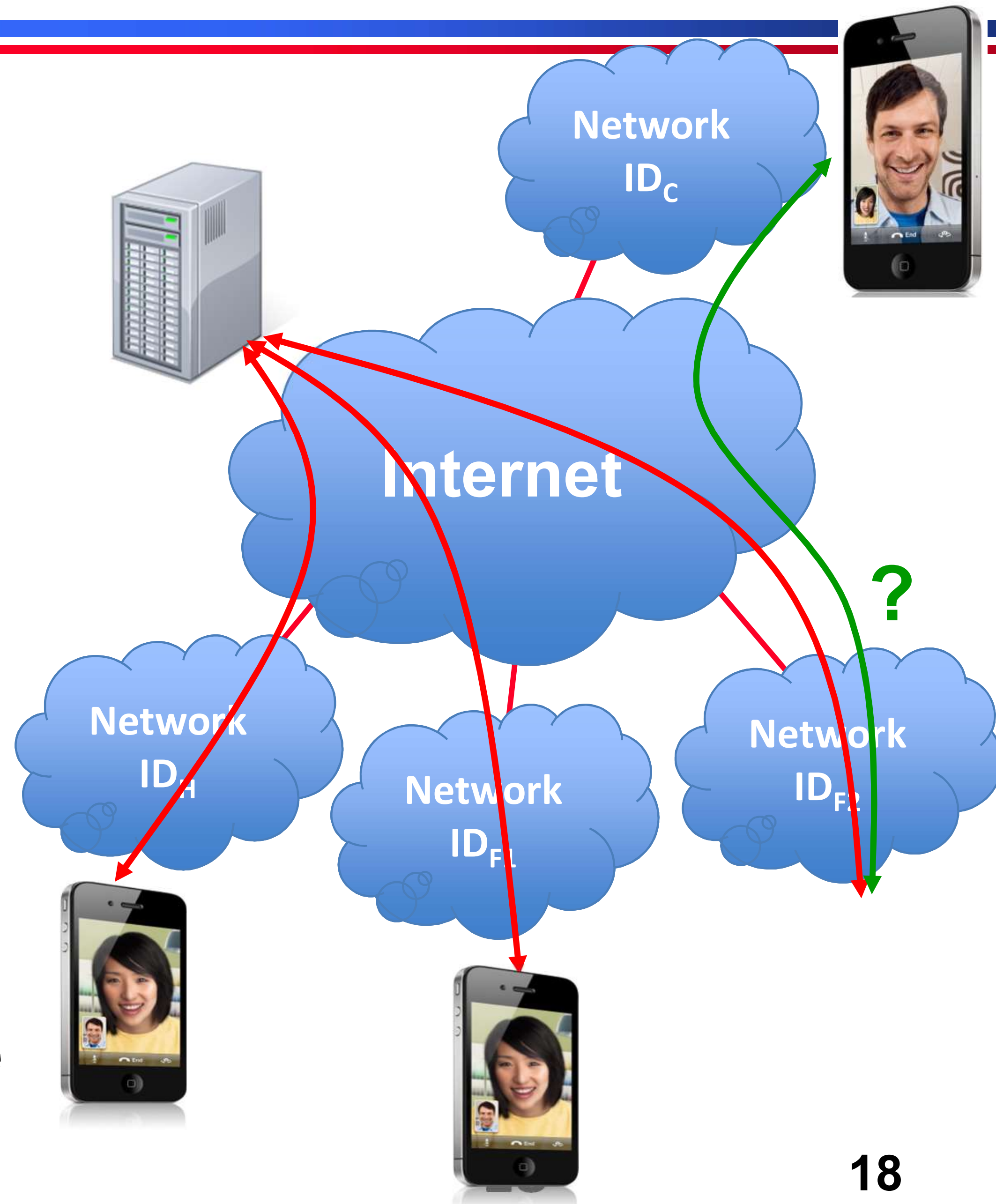
- Network ID identifies the network
  - » CMU = 128.2
- Node ID identifies node within a network
  - » Node IDs can be reused in different networks
  - » Can be assigned independently by local administrator
- Size of Network and Node IDs are variable
  - » Originally Network IDs came in three sizes only
  - » Variable sized Network IDs are often called a prefix
- Great, but what does this have to do with mobility?

Routing and Forwarding in the Internet



Mobility Challenges

- When a host moves to a new network, it gets a new IP address
- How do other hosts connect to it?
  » Assume you provide services
  » They have old IP address
- How do peers know you are the same host?
  » IP address identifies host
  » Associated with the socket of any active sessions
- What assumption is made here?



Communicating with Mobile Hosts: Requirements

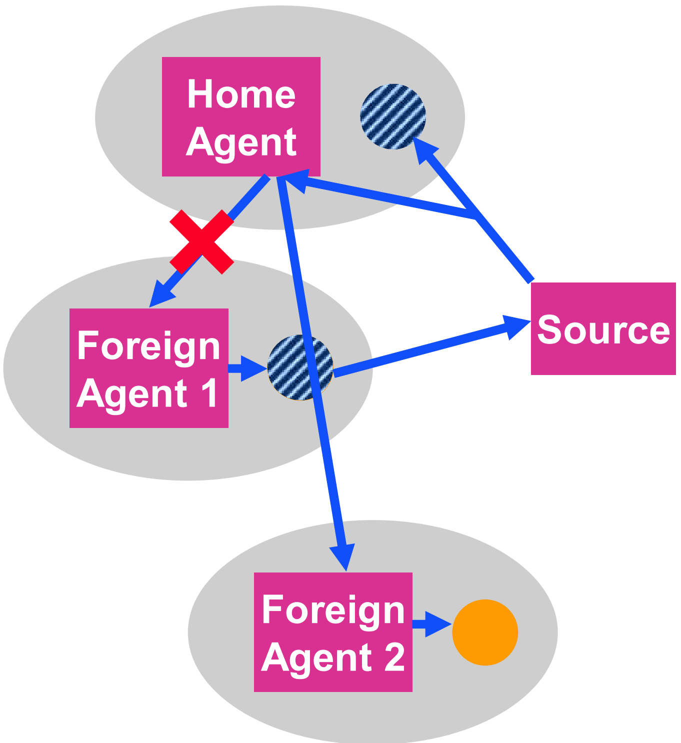
- Communicate with mobile hosts using their "home" IP address
- Mobility should be transparent to applications and higher level protocols
  - » No need to modify the software
- Minimize changes to host and router software
  - » No changes to communicating host
- Security should not get worse
- Challenge: Internet routing will delivery to the wrong (home) network
- Need a new solution: mobile IP!

Finding Mobile Hosts: Mobile IP

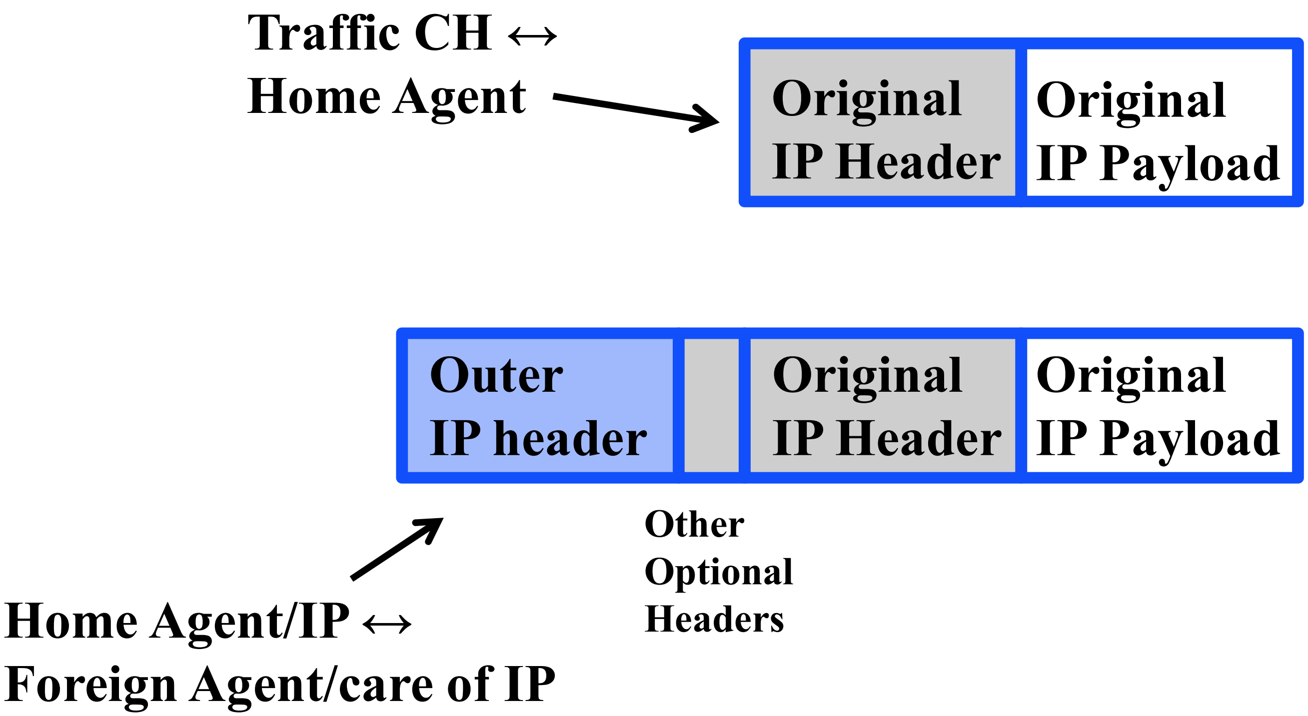
- Any host can contact mobile host using its usual "home" IP address
  - » Target is "nomadic" devices: do not move while communicating, i.e., laptop
- Home network has a home agent that is responsible for intercepting packets and forwarding them to the mobile host.
  - » E.g., router at the edge of the home network
  - » Forwarding is done using tunneling
- Remote network has a foreign agent that manages communication with mobile host.
  - » Module that runs on mobile and the point of contact for the mobile host
- Binding ties home IP address of mobile host to a "care of" address in the foreign network.
  - » binding = (home IP address, foreign IP addess)

Mobile IP Operation

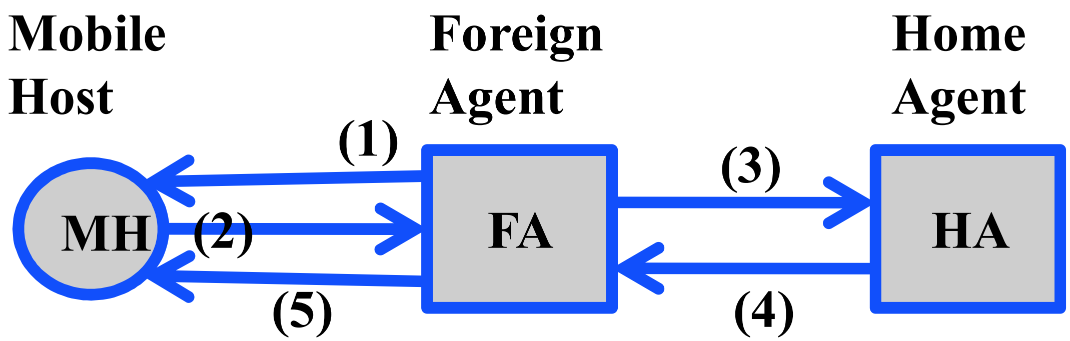
- **Registration process: mobile host registers with home agent.**
  - » **Home agents needs to know that it should intercept packet and forward them**
- **In foreign network, foreign agent gets local "care of" address and notifies home agent**
  - » **Home agent knows where to forward packets**
- **Tunneling**
  - » **Home agent forward packets to foreign agent**
  - » **Return packets are tunneled in the reverse direction**
- **Supporting mobility**
  - » **Update binding in home and foreign agents.**



Tunneling
IP-in-IP Encapsulation

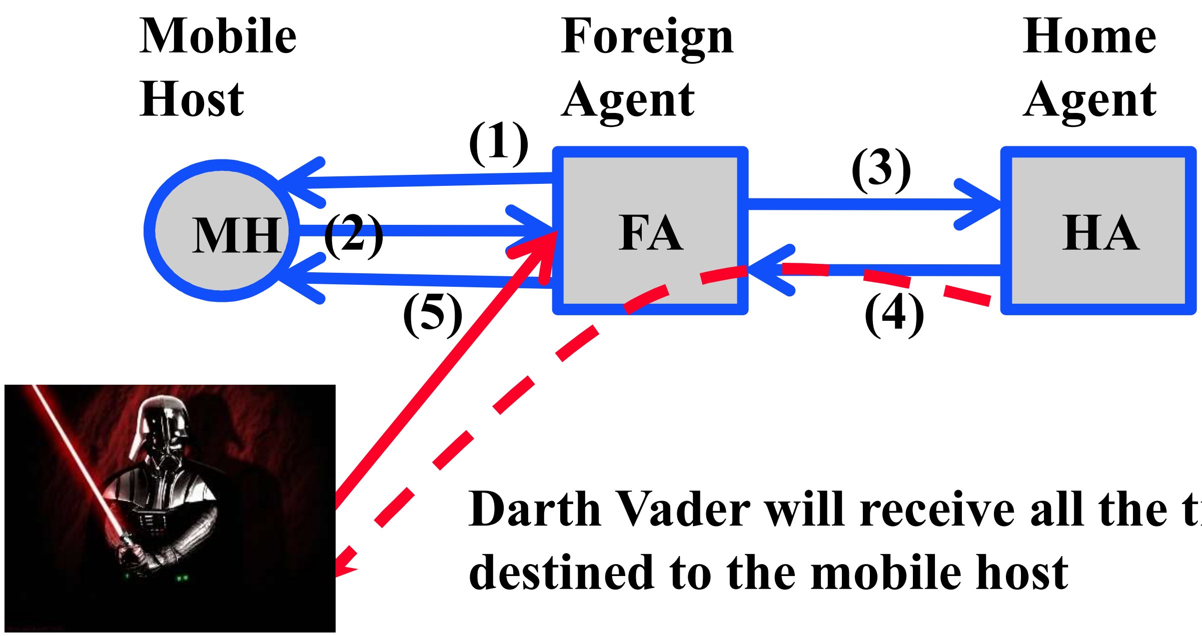


Registration via Foreign Agent



1. FA advertizes service
2. MH requests service
3. FA relays request to HA
4. HA accepts (or denies) request and replies
5. FA relays reply to MH

Authentication



Darth Vader will receive all the traffic destined to the mobile host

Solution: Registration messages between a mobile host and its home agent must be authenticated

Mobile IP Discussion

- Mobile IP not used in practice
- Mobile devices are typically clients, not servers, i.e., they initiate connections
  - » The problem Mobile IP solves rare in practice
- Mobile IP is not designed for truly mobile users
  - » Designed for nomadic users, e.g. visitors to a remote site
- IETF defined several solutions that are more efficient
  - » Also more heavy weight: creates overlay with tunnels and special “routers”, but they rely on “relays” similar to mobile IP

- Reality: maintaining your “home” address while being mobile is not particularly useful
- Practical solution: when you connect to new network, you obtain a “local” IP address and use that for communication

More Practical Way to Support Mobility

- Host gets new IP address in new “foreign” network
  - » Simple: use Dynamic Host Configuration (DHCP)
  - » No impact on Internet routing
- Raises two challenges:
  1. Finding the host: Host does not have constant address → how do other devices contact the host?
     - Sometimes needed for server notifications
     - Simple solutions: client periodically checks with server instead of the server contacting the client
  2. Maintaining a TCP connection while mobile → TCP session is tied to the src/dst IP addresses

How to Handle Active Connections for Mobile Nodes?

- **Hosts use a 4 tuple to identify a TCP connection**
  - » <Src Addr, Src port, Dst addr, Dst port>
  - » Changing either IP address breaks the connection
- **Best approach: add a level of indirection!**
  - » An “identifier”: identifies the connection on the end-point
  - » A “locator”: the current IP address of the end-point
  - » Host does a mapping
- **Practical challenge: how to update securely state when IP addresses change**
  - » Generally not supported for TCP, but
  - » Google’s QUIC transport protocol does support mobility