



Wireless and Mobile Networks

Reading: Sections 2.8 and 4.2.5

COS 461: Computer Networks
Spring 2010 (MW 3:00-4:20 in COS 105)

Mike Freedman

<http://www.cs.princeton.edu/courses/archive/spring10/cos461/>

Goals of Today's Lecture

- **Wireless links:** unique channel characteristics
 - High, time-varying bit-error rate
 - Broadcast where some nodes can't hear each other
- **Ad-hoc routing:** no fixed infrastructure
- **Mobile hosts:** addressing and routing challenges
 - Keeping track of host's changing attachment point
 - Maintaining a data transfer as the host moves
- **Some specific examples**
 - Wireless: 802.11 wireless LAN (aka "WiFi")
 - Ad-hoc routing: DSR and AODV
 - Mobility: Boeing Connexion and Mobile IP

Widespread Deployment

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

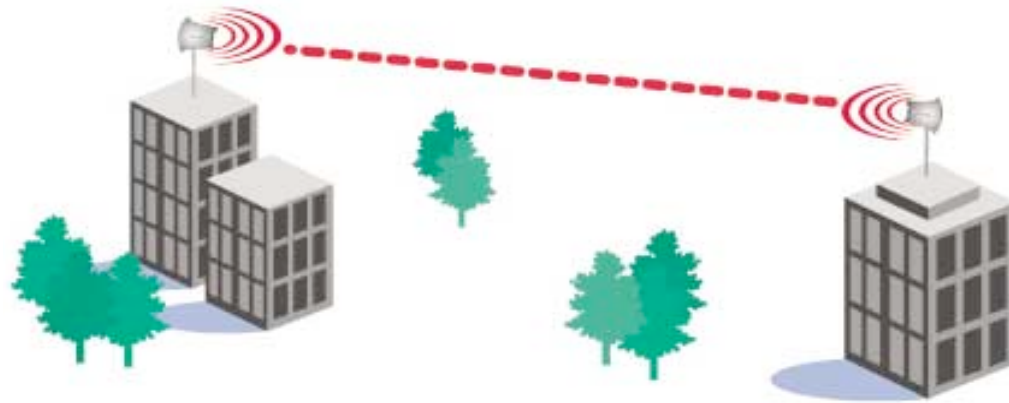


- **Wireless local area networks**
 - Wireless adapters built in to most laptops, and even PDAs
 - More than 220,000 known WiFi locations in 134 countries
 - Probably many, many more (e.g., home networks, corporate networks, ...)

Wireless Links and Wireless Networks

Wireless Links: High Bit Error Rate

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



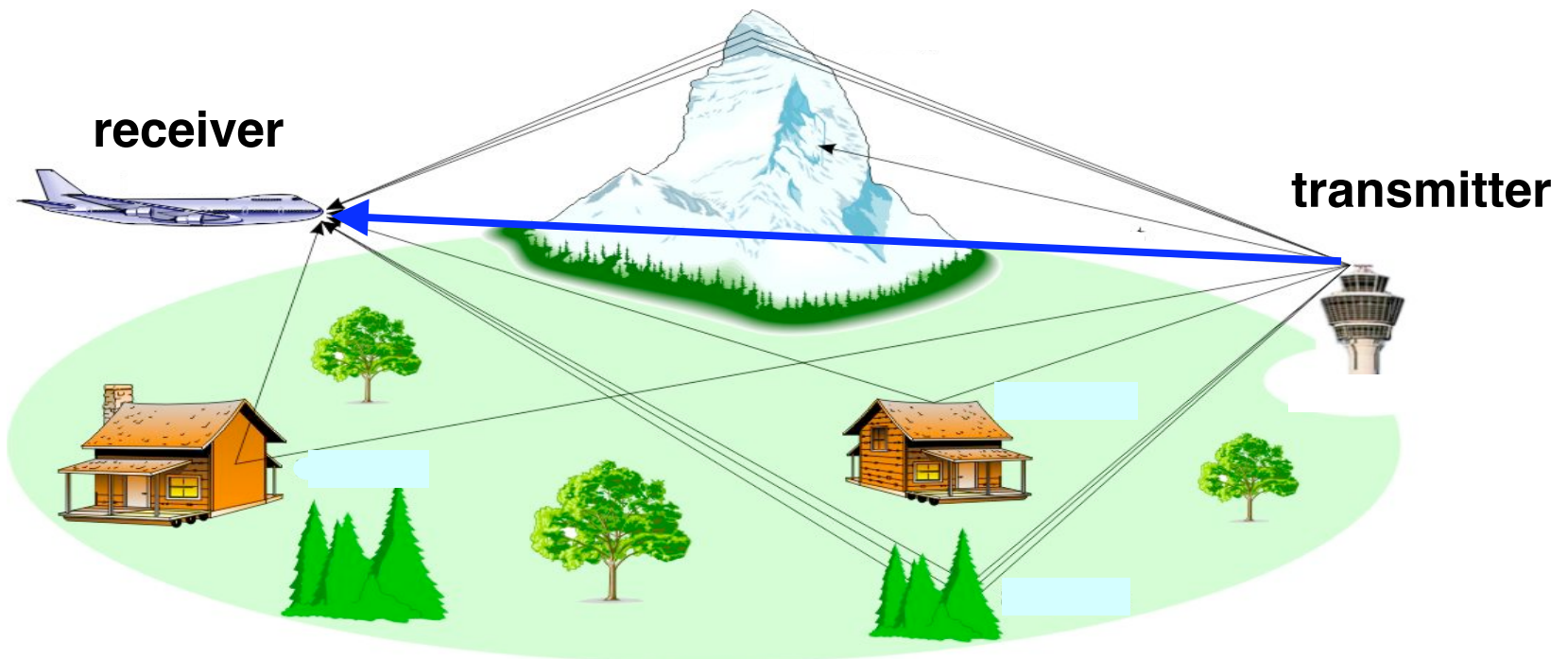
Wireless Links: High Bit Error Rate

- **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



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
- **(Many research proposals for TCP alternatives / extensions for wireless)**

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**

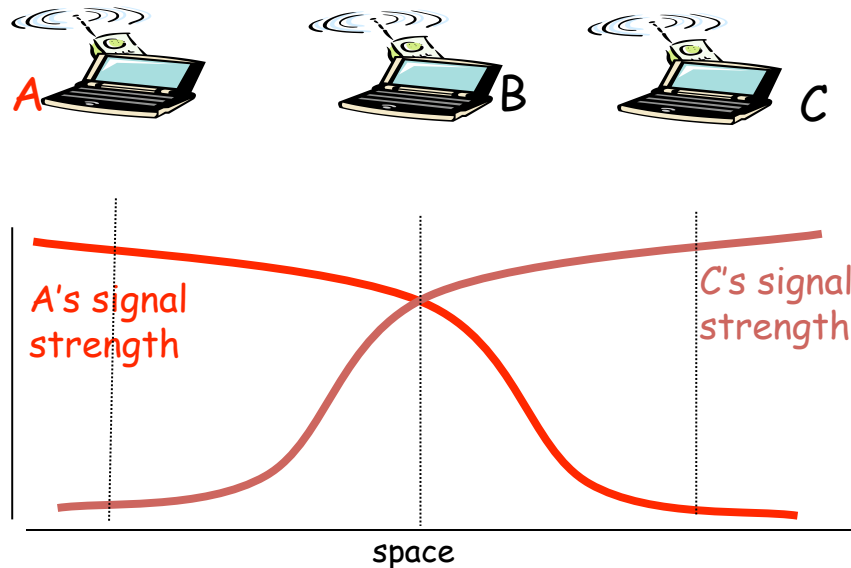


- A and B hear each other
- B and C hear each other
- **But, A and C do not**

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**



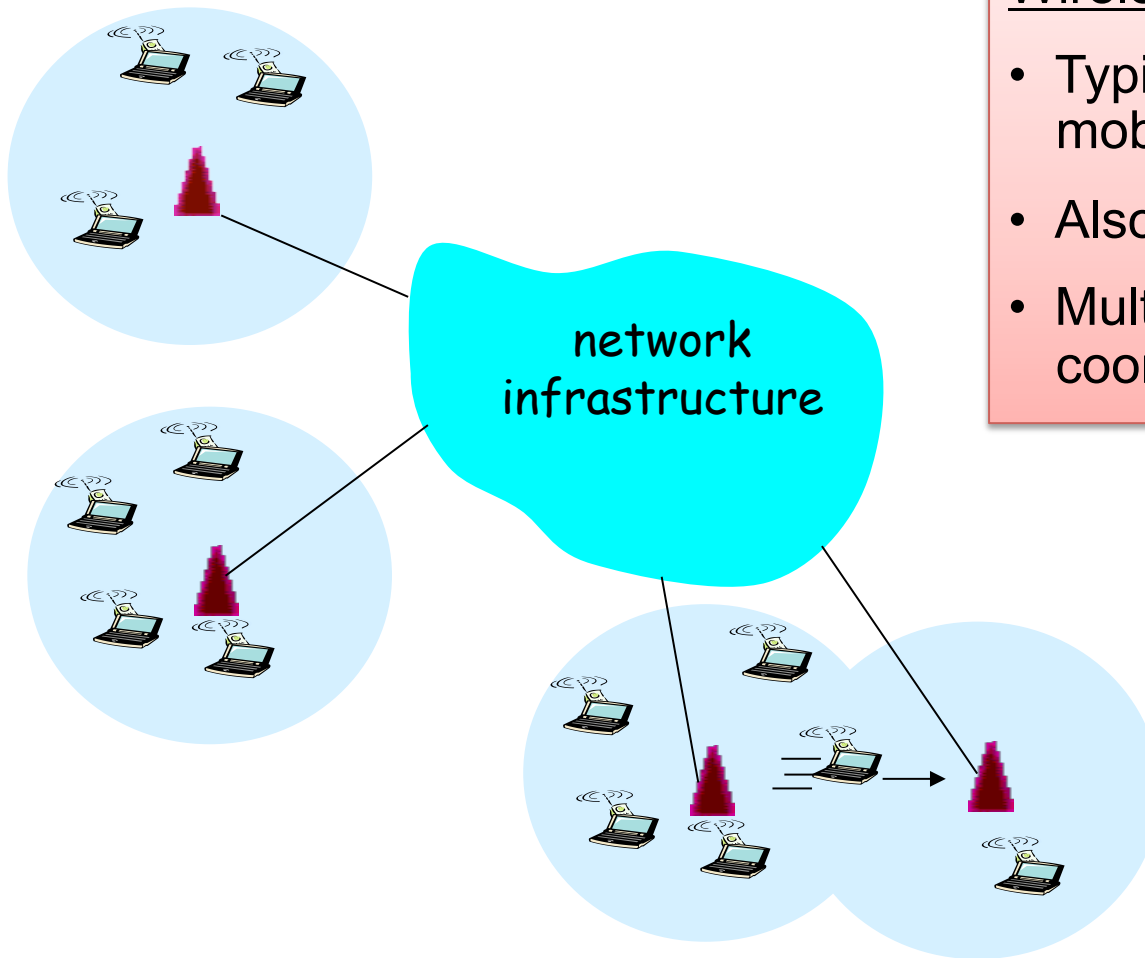
- A and B hear each other
- B and C hear each other
- **But, A and C do not**

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

Example Wireless Link Technologies

- **Data networks**
 - Indoor (10-30 meters)
 - 802.11n: 200 Mbps
 - 802.11a and g: 54 Mbps
 - 802.11b: 5-11 Mbps
 - 802.15.1: 1 Mbps
 - Outdoor (50 meters to 20 kmeters)
 - 802.11a and g point-to-point: 54 Mbps
 - WiMax: 5-11 Mbps
- **Cellular networks, outdoors**
 - 3G enhanced: 4 Mbps
 - 3G: 384 Kbps
 - 2G: 56 Kbps

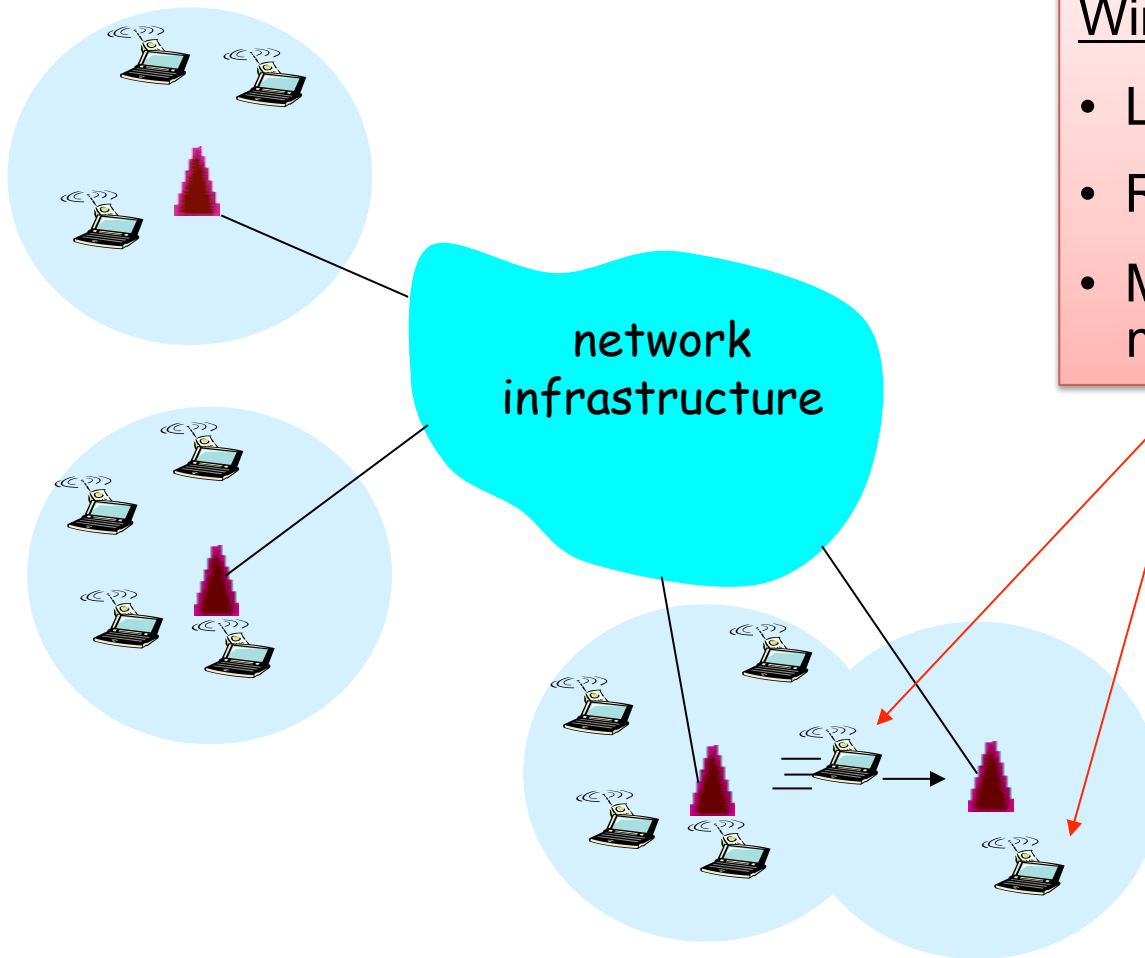
Wireless Network: Wireless Link



Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access

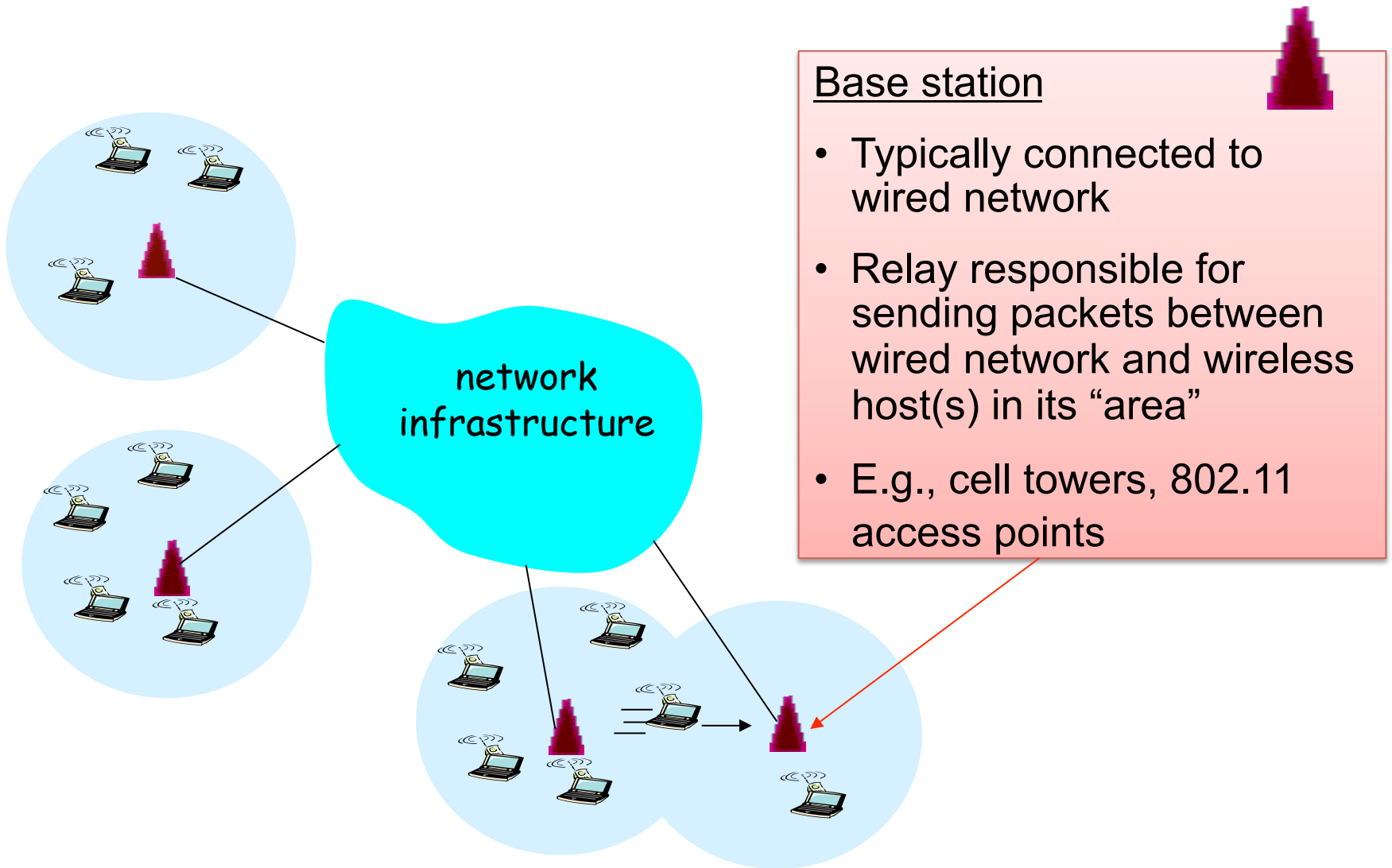
Wireless Network: Wireless Hosts



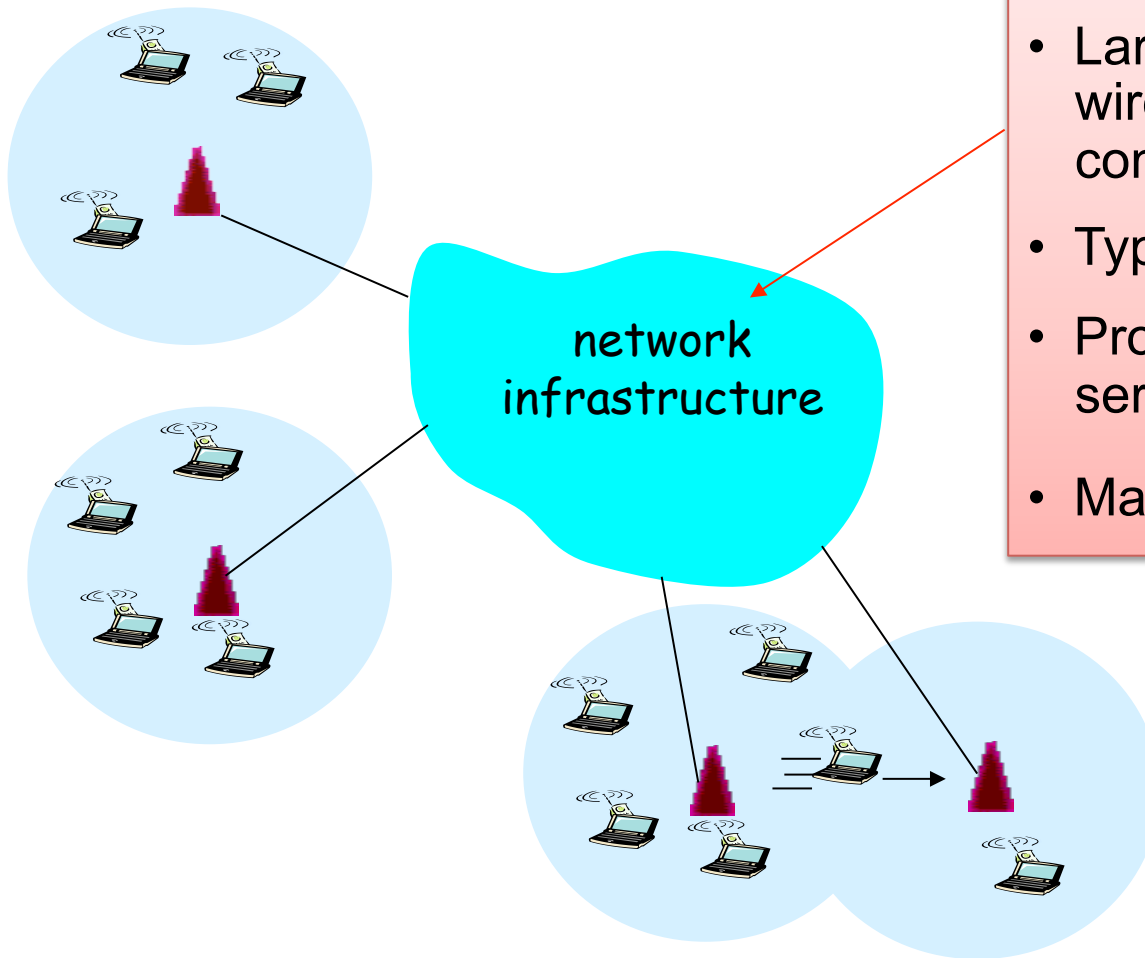
Wireless host

- Laptop, PDA, IP phone
- Run applications
- May be stationary (non-mobile) or mobile

Wireless Network: Base Station



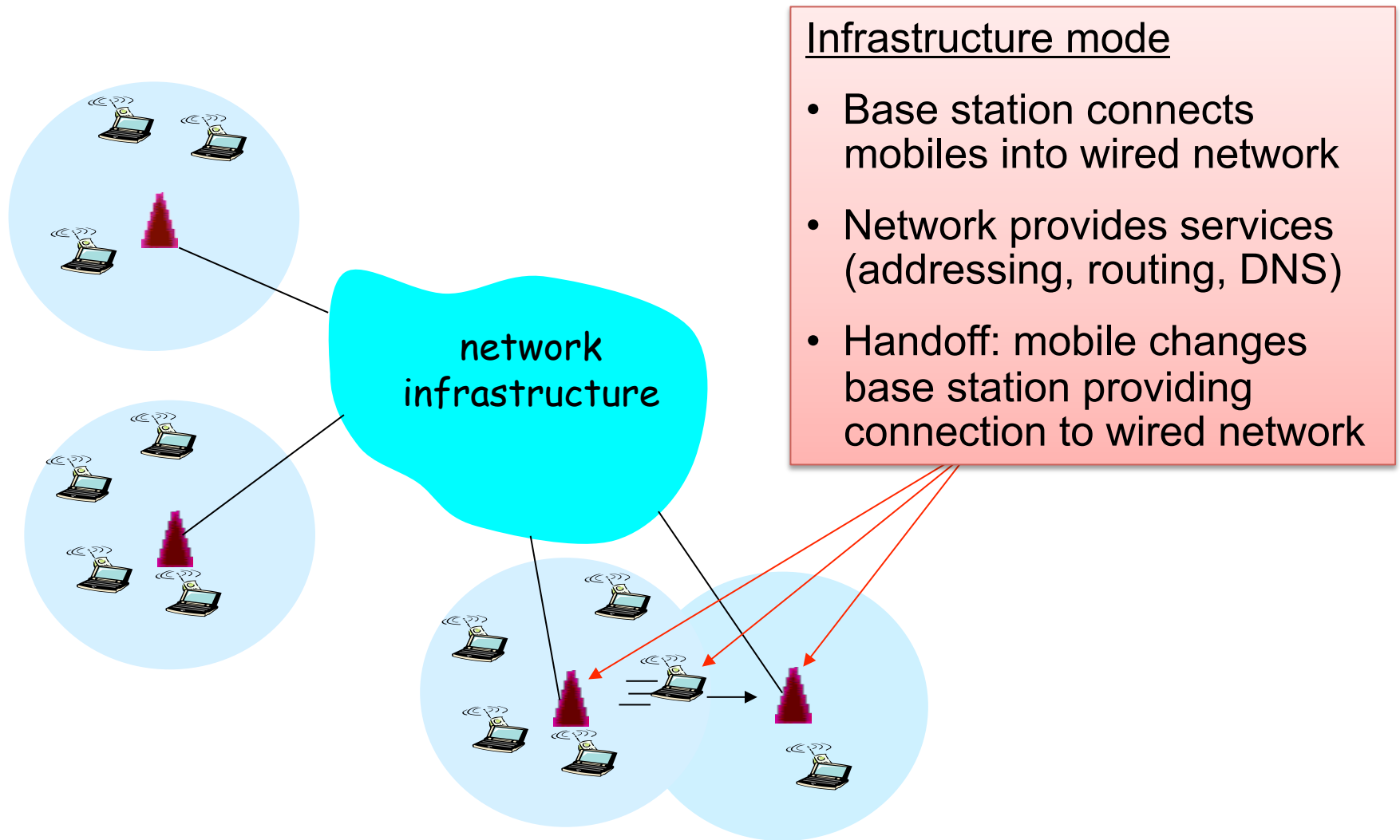
Wireless Network: Infrastructure



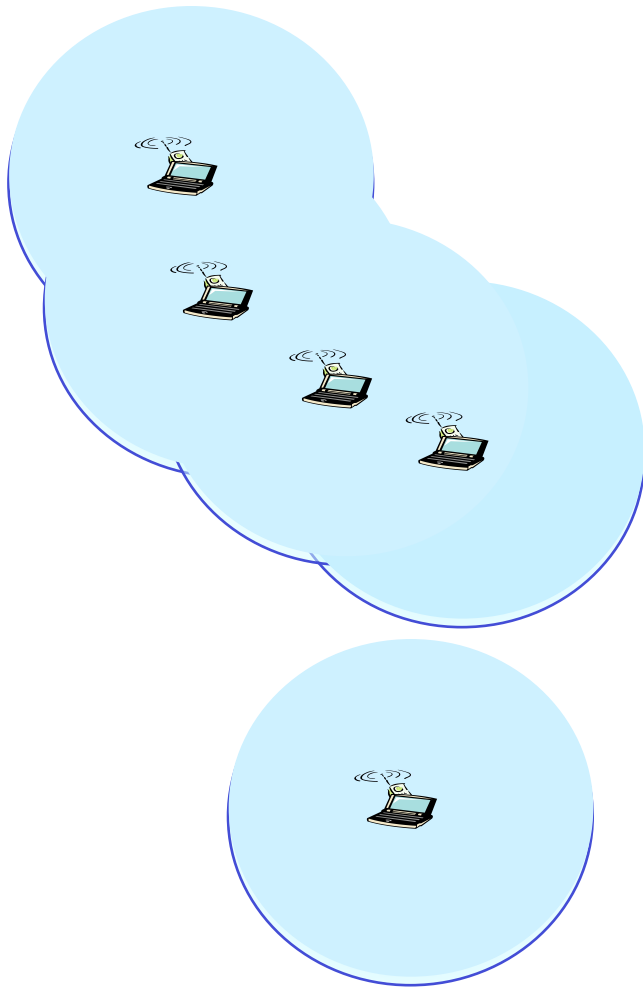
Network infrastructure

- Larger network with which a wireless host wants to communicate
- Typically a wired network
- Provides traditional network services
- May not always exist

Scenario #1: Infrastructure Mode



Scenario #2: Ad-Hoc Networks



Ad hoc mode

- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes self-organize and route among themselves

Infrastructure vs. Ad Hoc

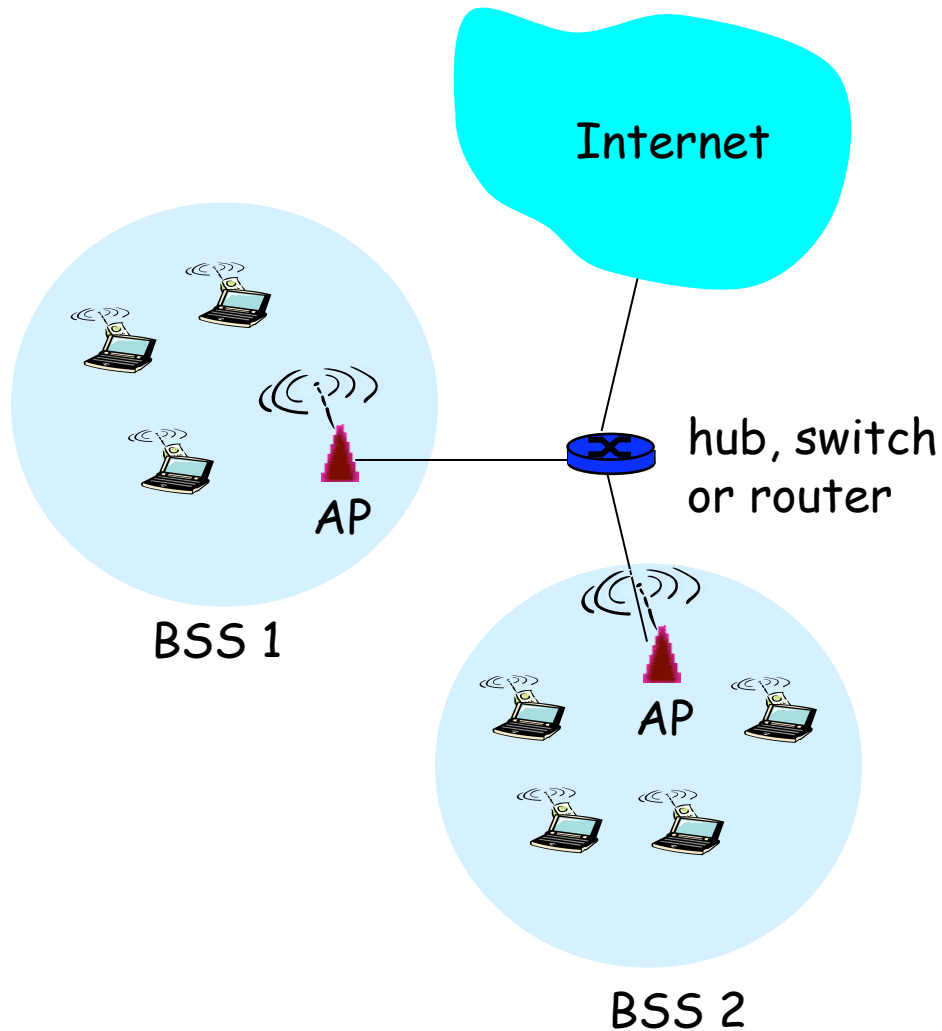
- **Infrastructure mode**
 - Wireless hosts are associated with a base station
 - Traditional services provided by the connected network
 - E.g., address assignment, routing, and DNS resolution
- **Ad hoc networks**
 - Wireless hosts have no infrastructure to connect to
 - Hosts themselves must provide network services
- **Similar in spirit to the difference between**
 - Client-server communication
 - Peer-to-peer communication

Different Types of Wireless Networks

	Infrastructure-based	Infrastructure-less
Single-hop	Base station connected to larger wired network (e.g., WiFi wireless LAN, and cellular telephony networks)	No wired network; one node coordinates the transmissions of the others (e.g., Bluetooth, and ad hoc 802.11)
Multi-hop	Base station exists, but some nodes must relay through other nodes (e.g., wireless sensor networks, and wireless mesh networks)	No base station exists, and some nodes must relay through others (e.g., mobile ad hoc networks, like vehicular ad hoc networks)

WiFi: 802.11 Wireless LANs

802.11 LAN Architecture

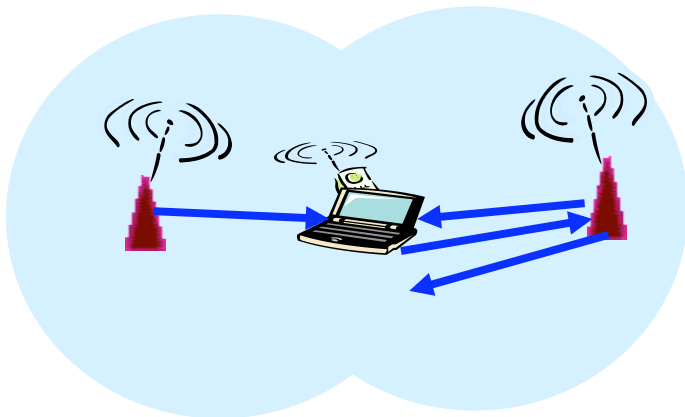


- Access Point (AP)
 - Base station that communicates with the wireless hosts
- Basic Service Set (BSS)
 - Coverage of one AP
 - AP acts as the master
 - Identified by an “network name” known as an SSID

SSID: Service Set Identifier

Channels and Association

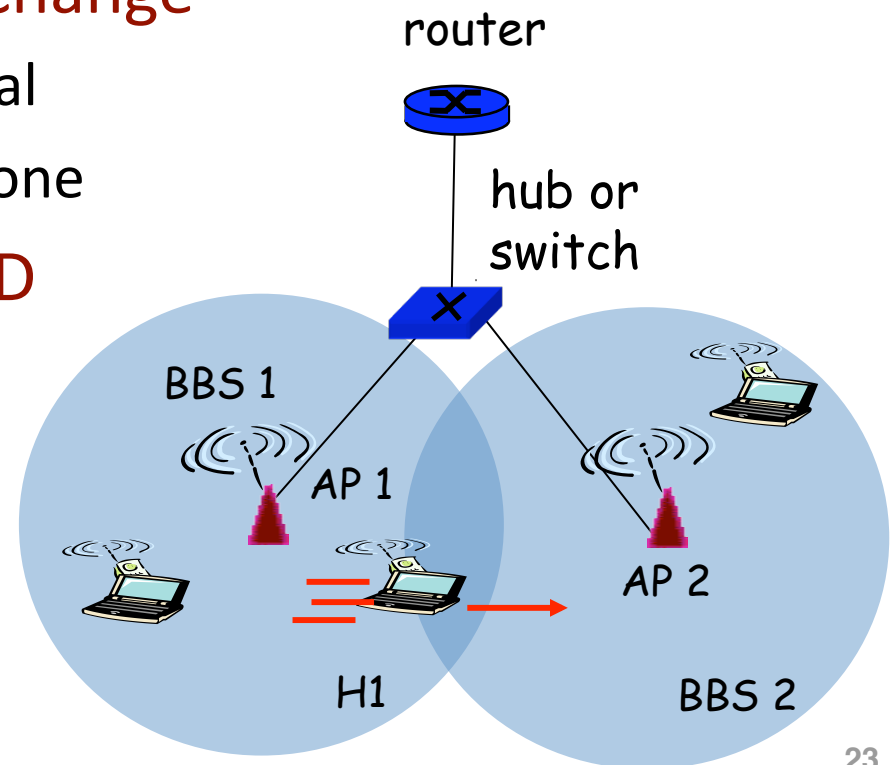
- Multiple channels at different frequencies
 - Network administrator chooses frequency for AP
 - Interference if channel is same as neighboring AP
- Access points send periodic beacon frames
 - Containing AP's name (SSID) and MAC address
 - Host scans channels, listening for beacon frames
 - Host selects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



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

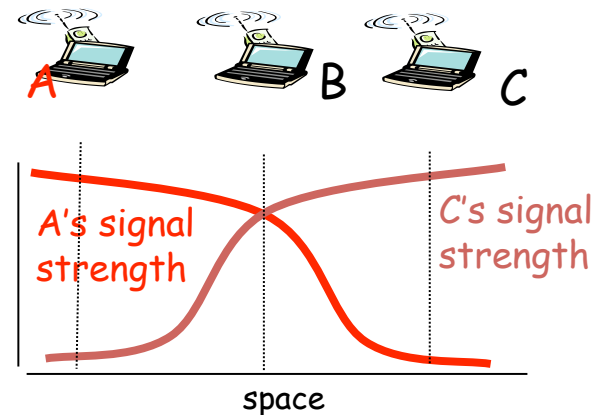
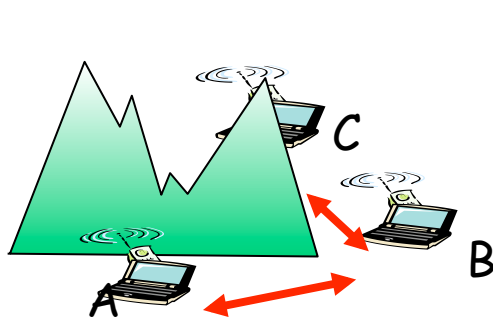
Mobility Within the Same Subnet

- **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



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

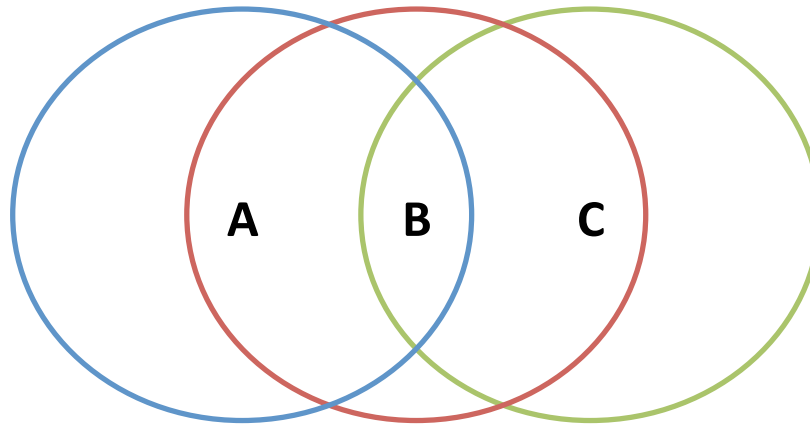
CA: Collision Avoidance, Not Detection

- 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 *not* do collision detection

Medium Access Control in 802.11

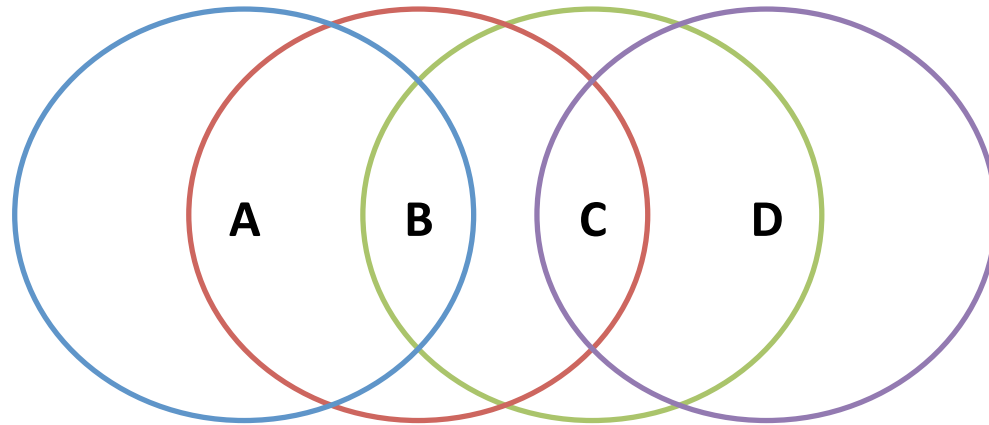
- Collision avoidance, not detection
 - First exchange control frames before transmitting data
 - Sender issues “Request to Send” (RTS), including length of data
 - Receiver responds with “Clear to Send” (CTS)
 - If sender sees CTS, transmits data (of specified length)
 - If other node sees CTS, will idle for specified period
 - If other node sees RTS but not CTS, free to send
- Link-layer acknowledgment and retransmission
 - CRC to detect errors
 - Receiving station sends an acknowledgment
 - Sending station retransmits if no ACK is received
 - Giving up after a few failed transmissions

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



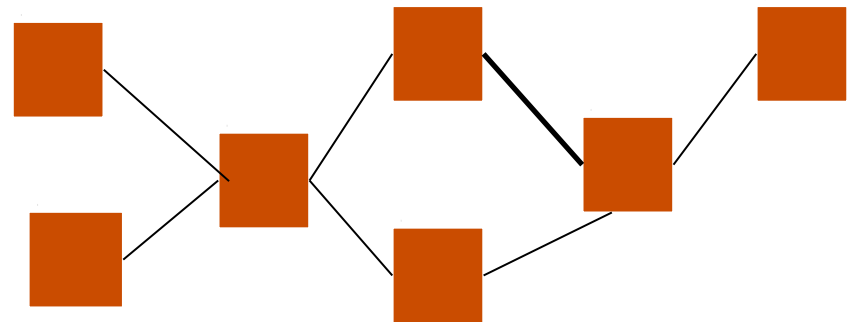
- B sending to A, C wants to send to D
- As C receives B's packets, carrier sense would prevent it from sending to D, even though wouldn't interfere
- RTS/CTS can help
 - C hears RTS from B, but not CTS from A
 - C knows it's transmission will not interfere with A
 - C is safe to transmit to D

Ad-hoc routing protocols

Traditional Routing vs Ad Hoc

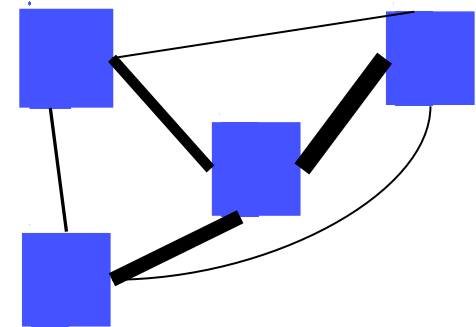
- Traditional network:

- Well-structured
- $\sim O(N)$ nodes & links
- All links work $\sim$ well



- Ad Hoc network

- N^2 links - but many bad!
- Topology may be really weird
 - Reflections & multipath cause strange interference
- Change is frequent



Problems using DV or LS

- DV loops are very expensive
 - Wireless bandwidth $\ll$ fiber bandwidth...
- LS protocols have high overhead
- N^2 links cause very high cost
- Periodic updates waste power
- Need fast, frequent convergence

Proposed protocols

- **Basic Taxonomy:**
 - Reactive (on-demand)
 - Proactive (table driven)
 - Source routing
 - Hop-by-hop routing
- Destination-Sequenced Distance Vector (DSDV)
- Dynamic Source Routing (DSR)
- Ad Hoc On-Demand Distance Vector (AODV)

Dynamic Source Routing

- Source routing
 - Intermediate nodes can be out of date
- On-demand route discovery
 - Don't need periodic route advertisements
- (Design point: on-demand may be better or worse depending on traffic patterns...)

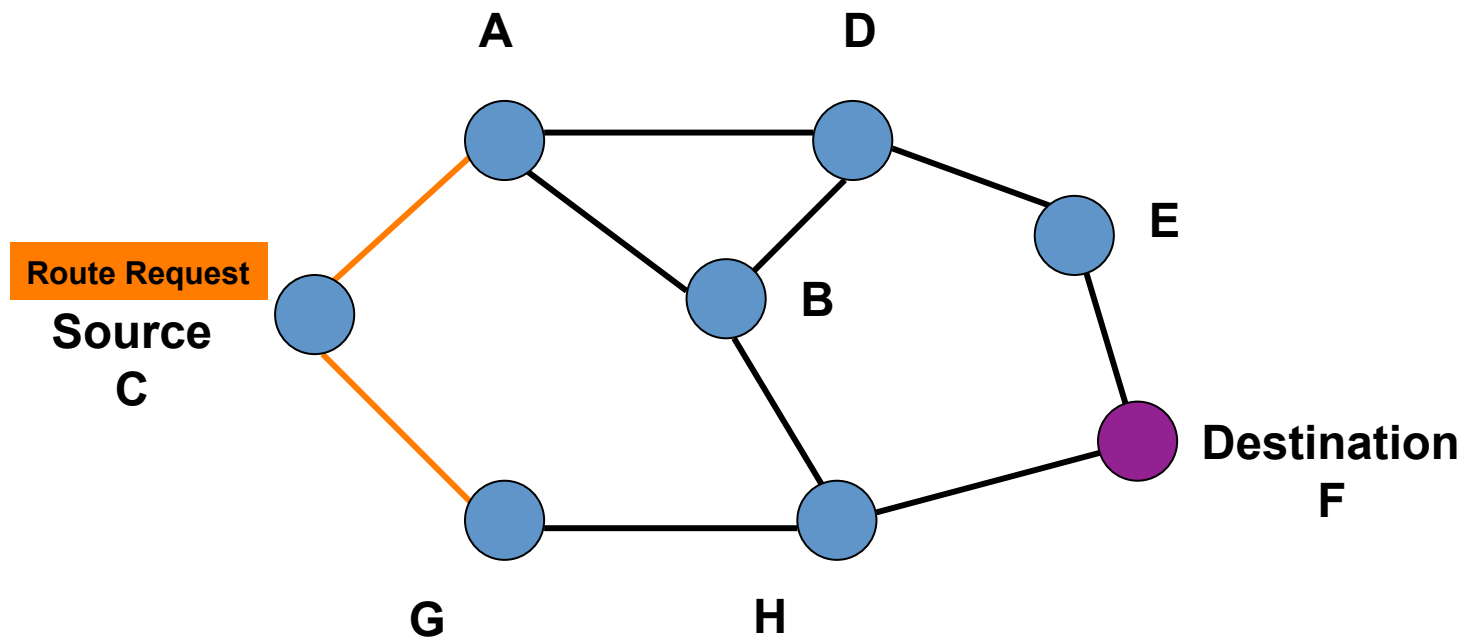
DSR Components

- **Route discovery**
 - The mechanism by which a sending node obtains a route to destination
- **Route maintenance**
 - The mechanism by which a sending node detects that the network topology has changed and its route to destination is no longer valid

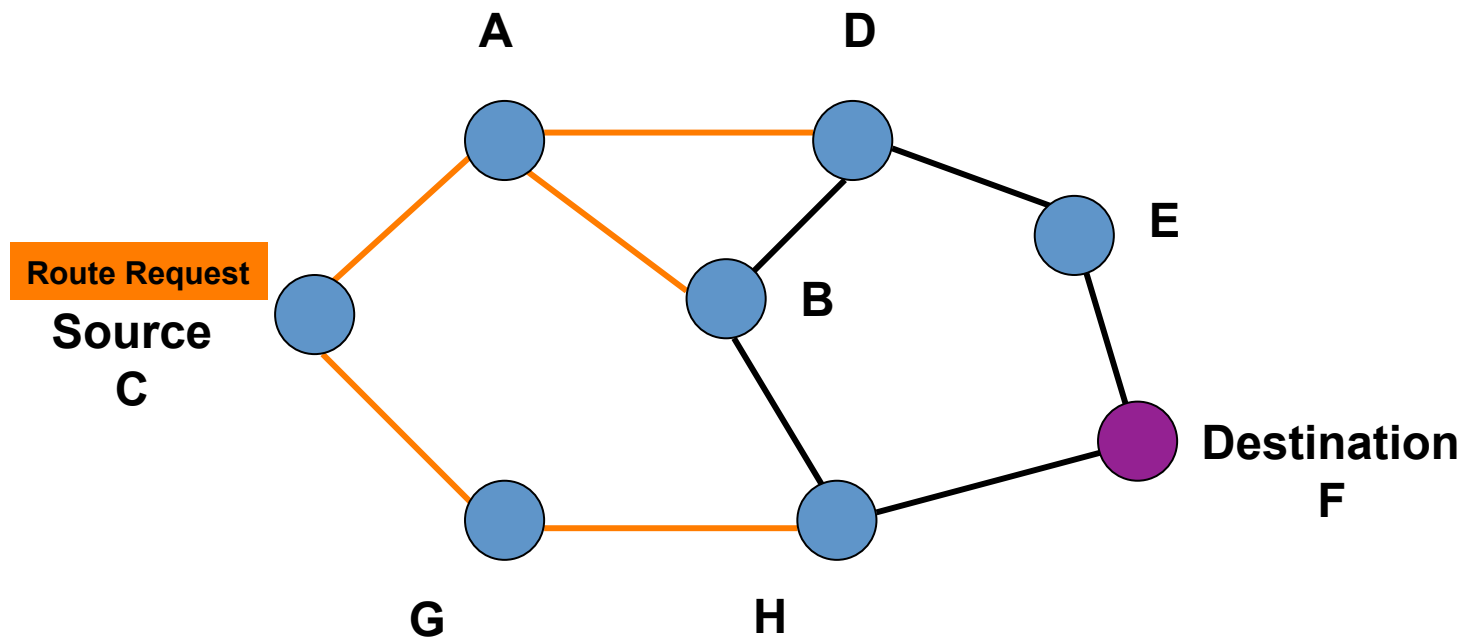
DSR Route Discovery

- Route discovery - basic idea
 - **Source** broadcasts route-request to **Destination**
 - Each node forwards request by adding own address and re-broadcasting
 - Requests propagate outward until:
 - Target is found, or
 - A node that has a route to Destination is found

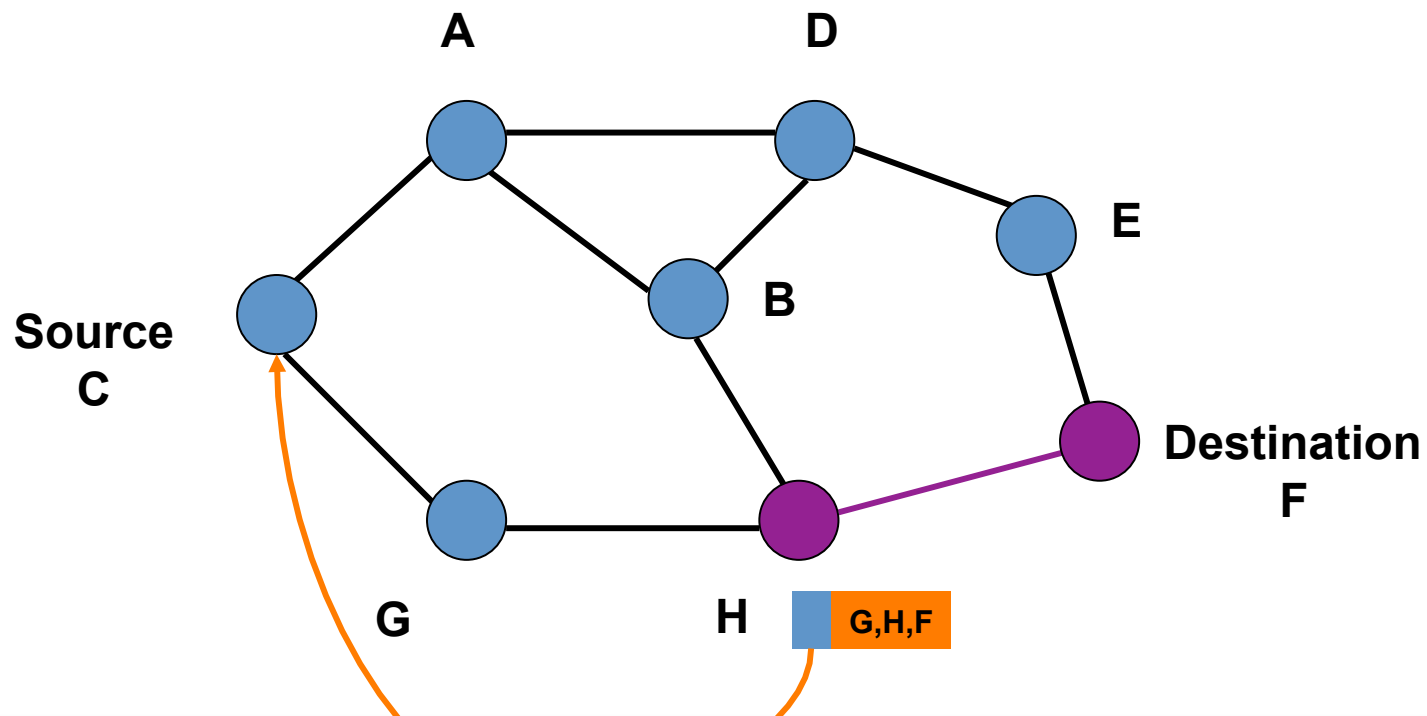
C Broadcasts Route Request to F



C Broadcasts Route Request to F

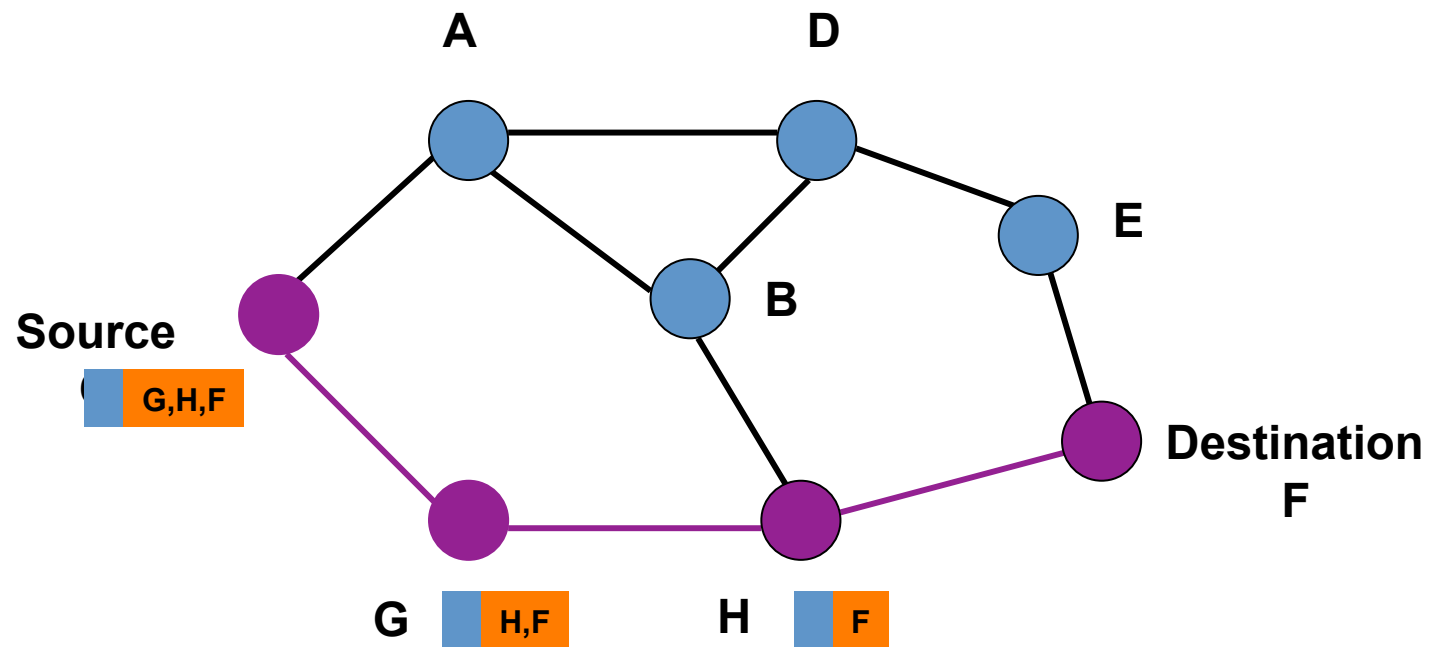


H Responds to Route Request



- Using reversed path if links bidirectional (802.11)
- Using own route discovery if links unidirectional

C Transmits a Packet to F



Forwarding Route Requests

- A request is forwarded if:
 - Node is not the destination
 - Node not already listed in recorded source route
 - Node has not seen request with same sequence number
 - Node doesn't already have cached answer
 - IP TTL field may be used to limit scope
- Destination copies route into a Route-reply packet and sends it back to **Source**

Route Cache

- All source routes learned by a node are kept in Route Cache (reduces cost of discovery)
- If intermediate node receives RR for destination and has entry cached, it responds to RR and does not propagate RR further
- Nodes overhearing RR/RP may insert routes in cache (remember it's a broadcast channel)

Sending Data

- Check cache for route to destination
- If route exists then
 - If reachable in one hop
 - Send packet
 - Else insert routing header to destination and send
- If route does not exist, buffer packet and initiate route discovery

Discussion

- Source routing is good for on demand routes instead of a priori distribution
- But, high packet overhead ← **Why esp important?**
- Route discovery protocol used to obtain routes on demand
 - Caching used to minimize use of discovery
- No Periodic messages
- But, need to buffer packets

Ad Hoc On-Demand Distance Vector

- On-demand protocol
- Table-driven, distance-vector routing
- Similar to DSR in finding routes, but
 - Uses sequence numbers on route updates
 - Has an idea of freshness of a route
- RouteREQuest includes normal stuff plus
 - src-seq, dest-seq, broadcast-seq, hop-count

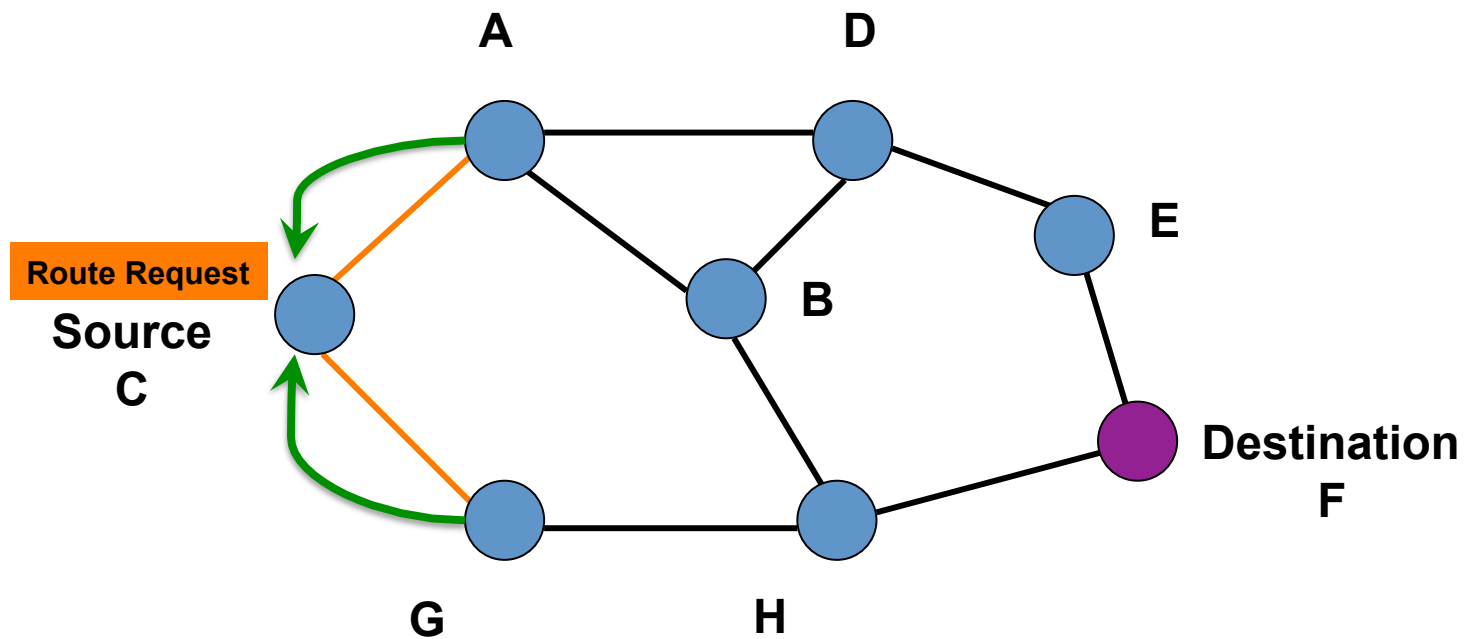
Route Requests

- On RREQ
 - REPLY
If my dest-seq $\geq$ received dest-seq OR
I am destination
 - DISCARD
If src-adr & broadcast-seq were seen
 - Re-broadcast
otherwise

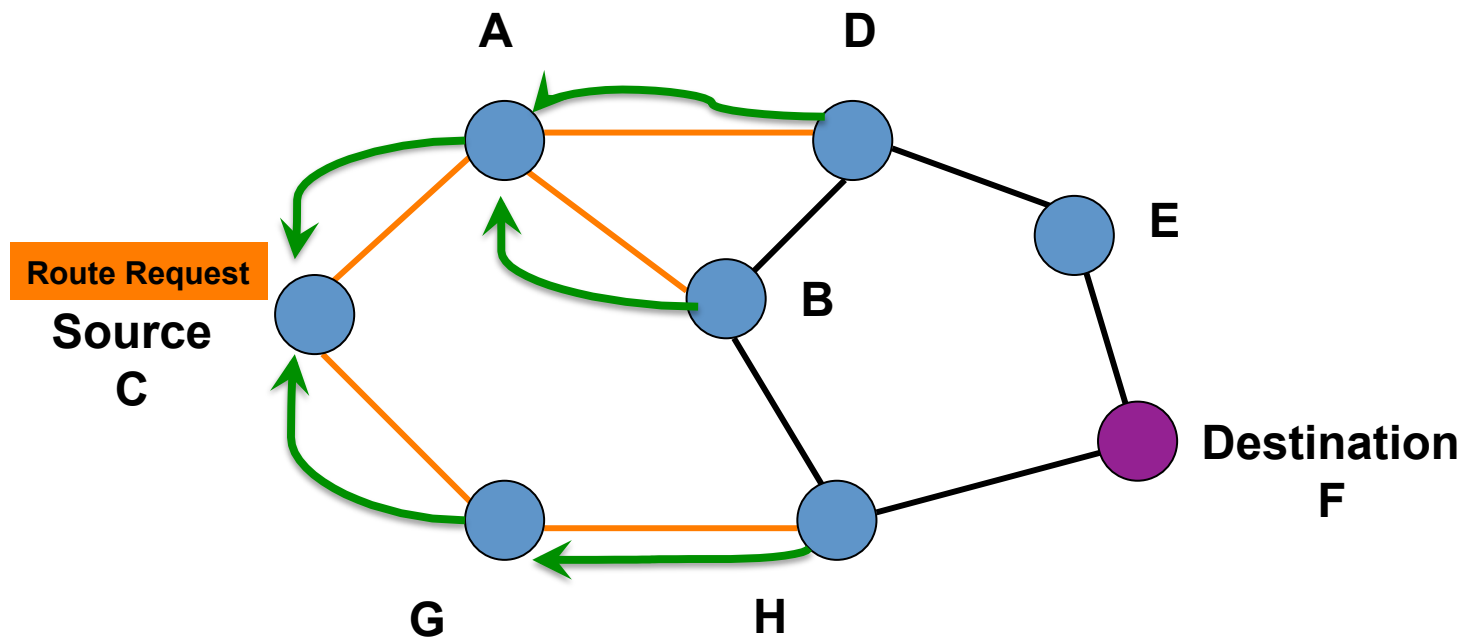
Route Maintenance

- Update routing table when receive information that improves on the routing metric:
 - No previous route known
 - Smaller hop-count with same dst-seq number
 - Larger dst-seq number (fresher)

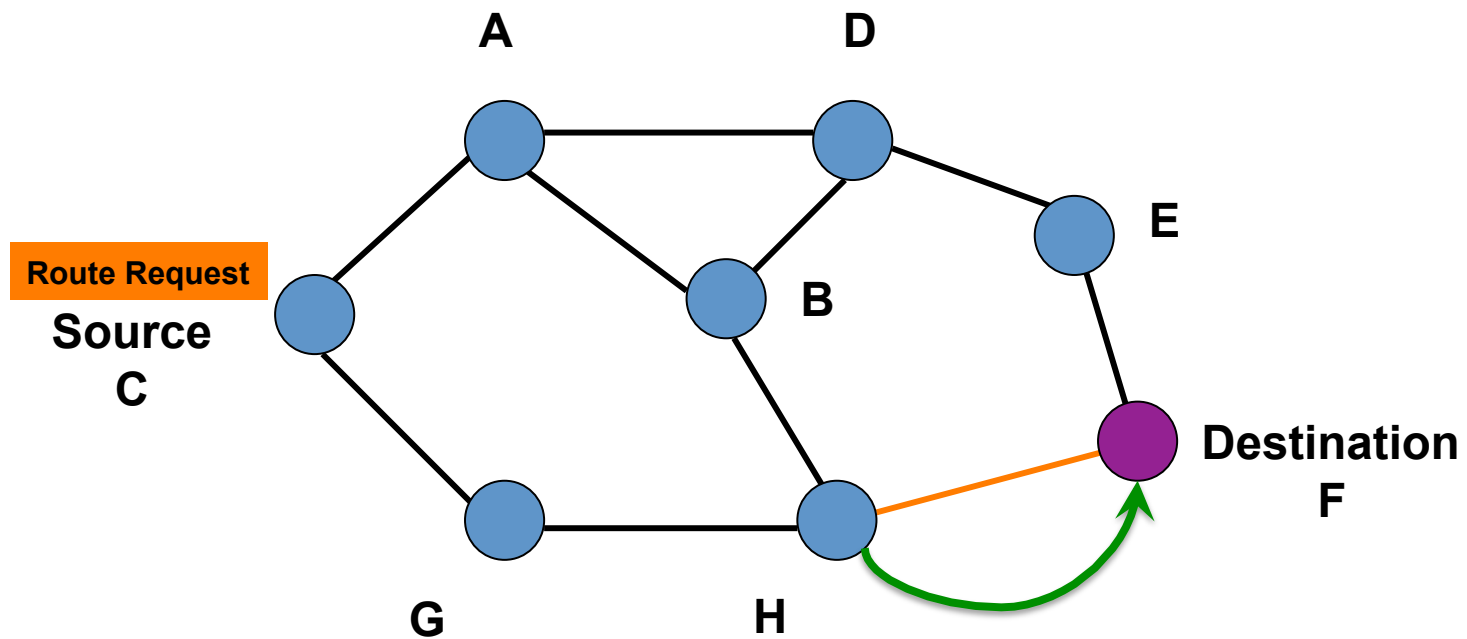
C Broadcasts Route Request to F



C Broadcasts Route Request to F



F unicasts RREP to C



Route Maintenance

- Update routing table when receive information that improves on the routing metric:
 - No previous route known
 - Smaller hop-count with same dst-seq number
 - Larger dst-seq number (fresher)
- Eavesdrop
- Periodic hellos (unlike DSR)
 - Higher network overhead vs. smaller connection setup time

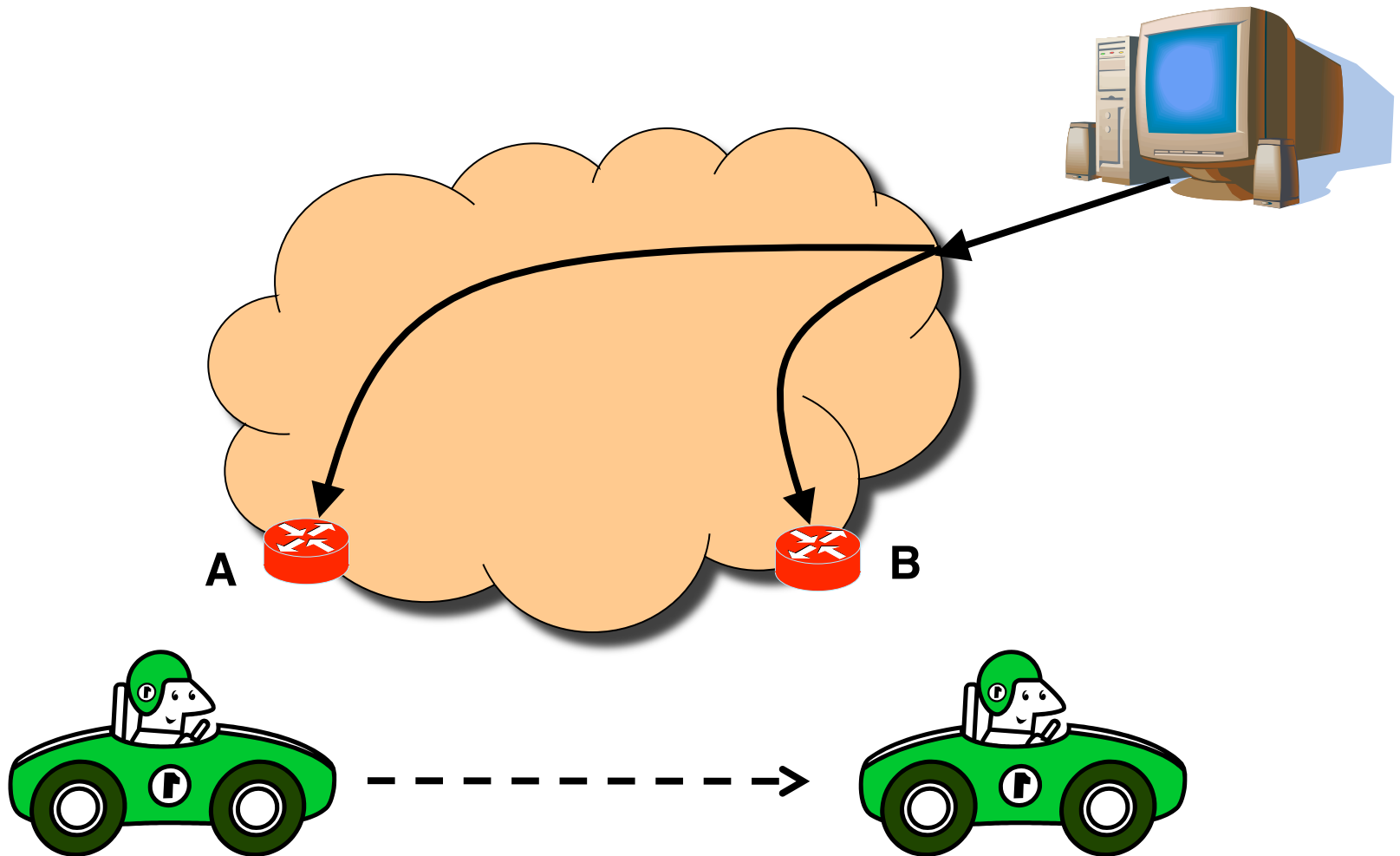
Host Mobility

Varying Degrees of User Mobility

- Moves only within same access network
 - Single access point: mobility is irrelevant
 - Multiple access points: only link-link layer changes
 - Either way, users is not mobile at the network layer
- Shuts down between changes access networks
 - Host gets new IP address at the new access network
 - No need to support any ongoing transfers
 - Applications have become good at supporting this
- Maintains connections while changing networks
 - Surfing the 'net while driving in a car or flying a plane
 - Need to ensure traffic continues to reach the host

Maintaining Ongoing Transfers

- Seamless transmission to a mobile host



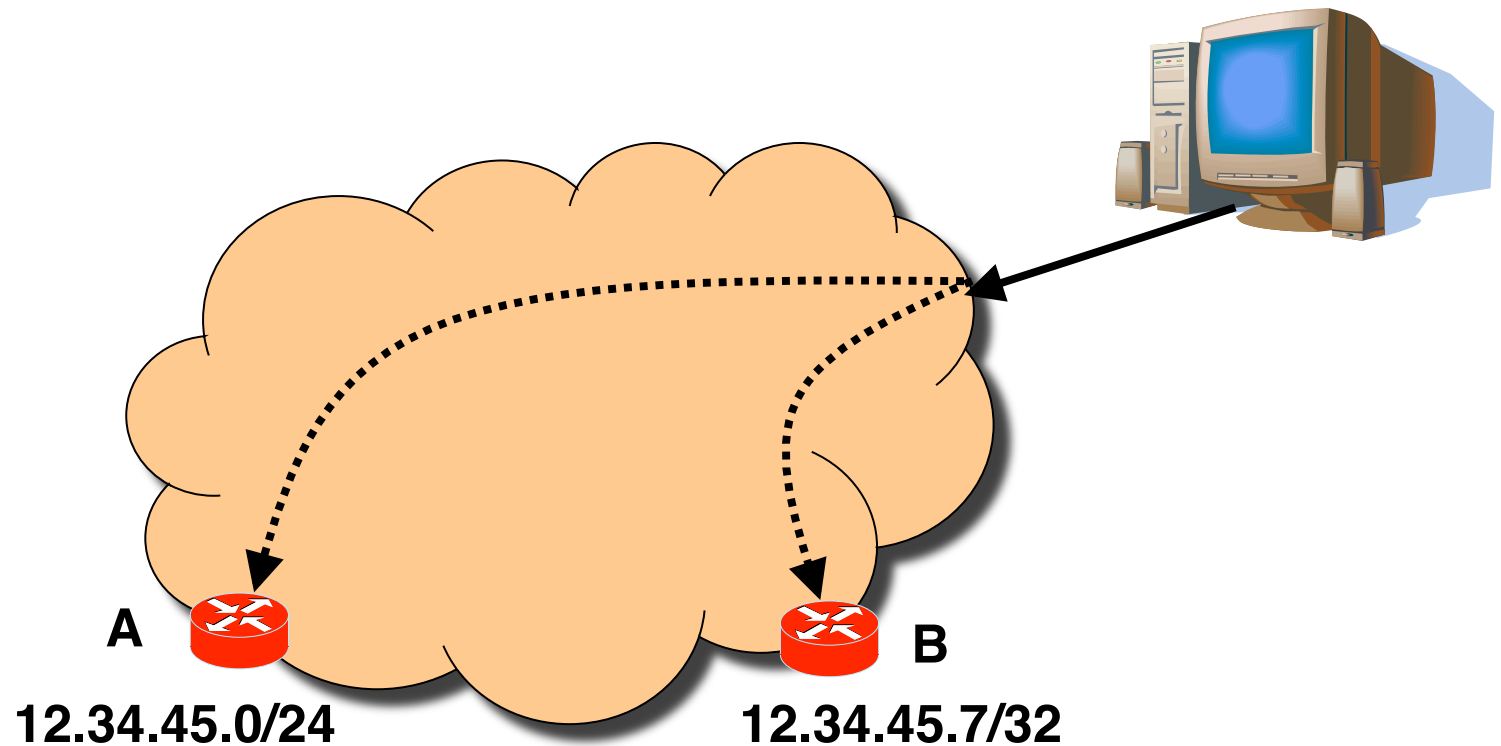
E.g., Keep Track of Friends on the Move

- Sending a letter to a friend who moves often
 - How do you know where to reach him?
- Option #1: have him update you
 - Friend contacts you on each move
 - So you can mail him directly
 - E.g., Boeing Connexion service
- Option #2: ask his parents when needed
 - Parents serve as “permanent address”
 - So they can forward your letter to him
 - E.g., Mobile IP



Option #1: Let Routing Protocol Handle It

- Mobile node has a single, persistent address
- Address injected into routing protocol (e.g., OSPF)



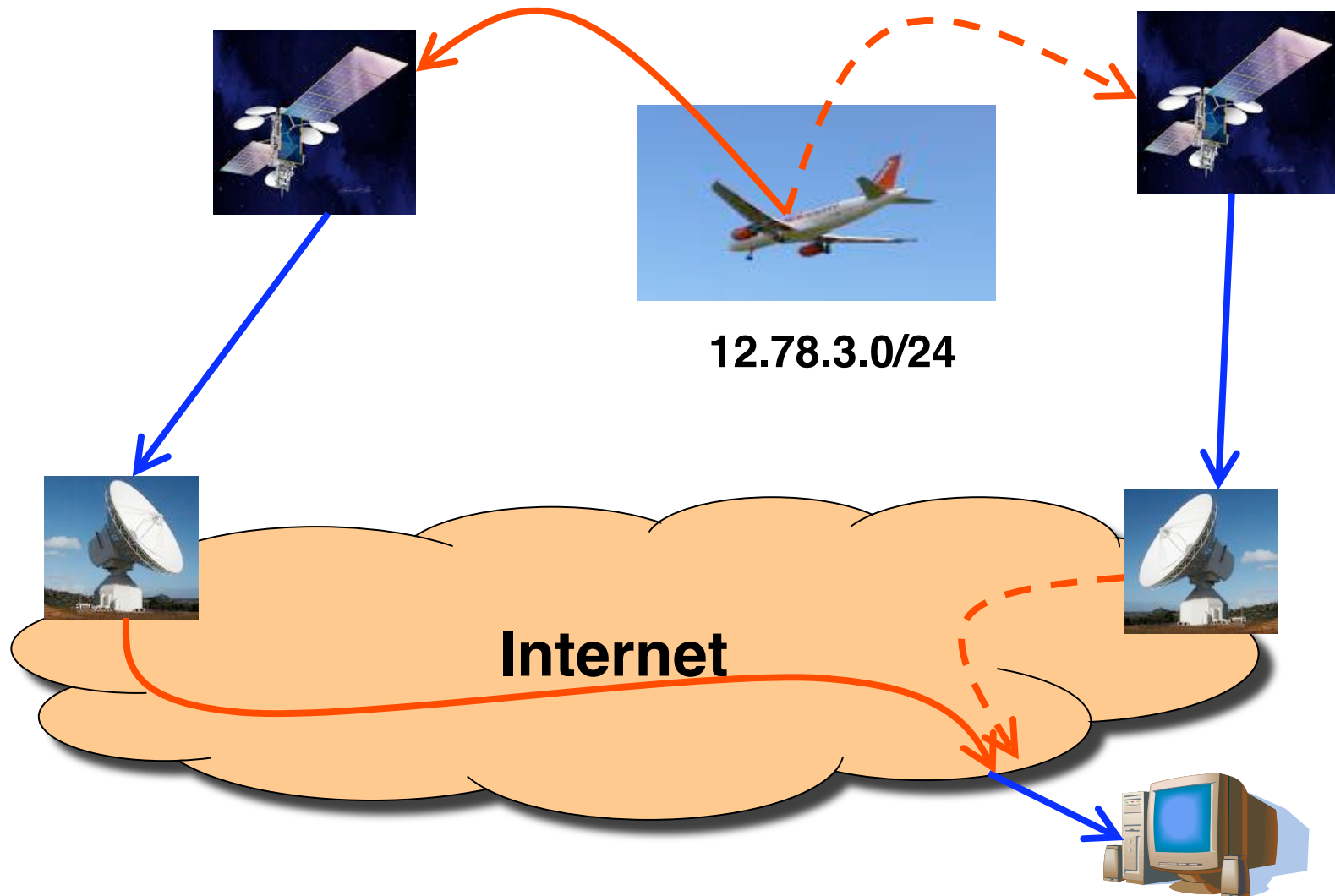
Mobile host with IP address 12.34.45.7

Example: Boeing Connexion Service



- **Boeing Connexion service**
 - Mobile Internet access provider
 - WiFi “hot spot” at 35,000 feet moving 600 mph
 - Went out of business in December 2006... ☹
- **Communication technology**
 - Antenna on the plane to leased satellite transponders
 - Ground stations serve as Internet gateways
- **Using BGP for mobility**
 - IP address block per airplane
 - Ground station advertises into BGP
 - <http://www.nanog.org/mtg-0405/abarbanel.html>

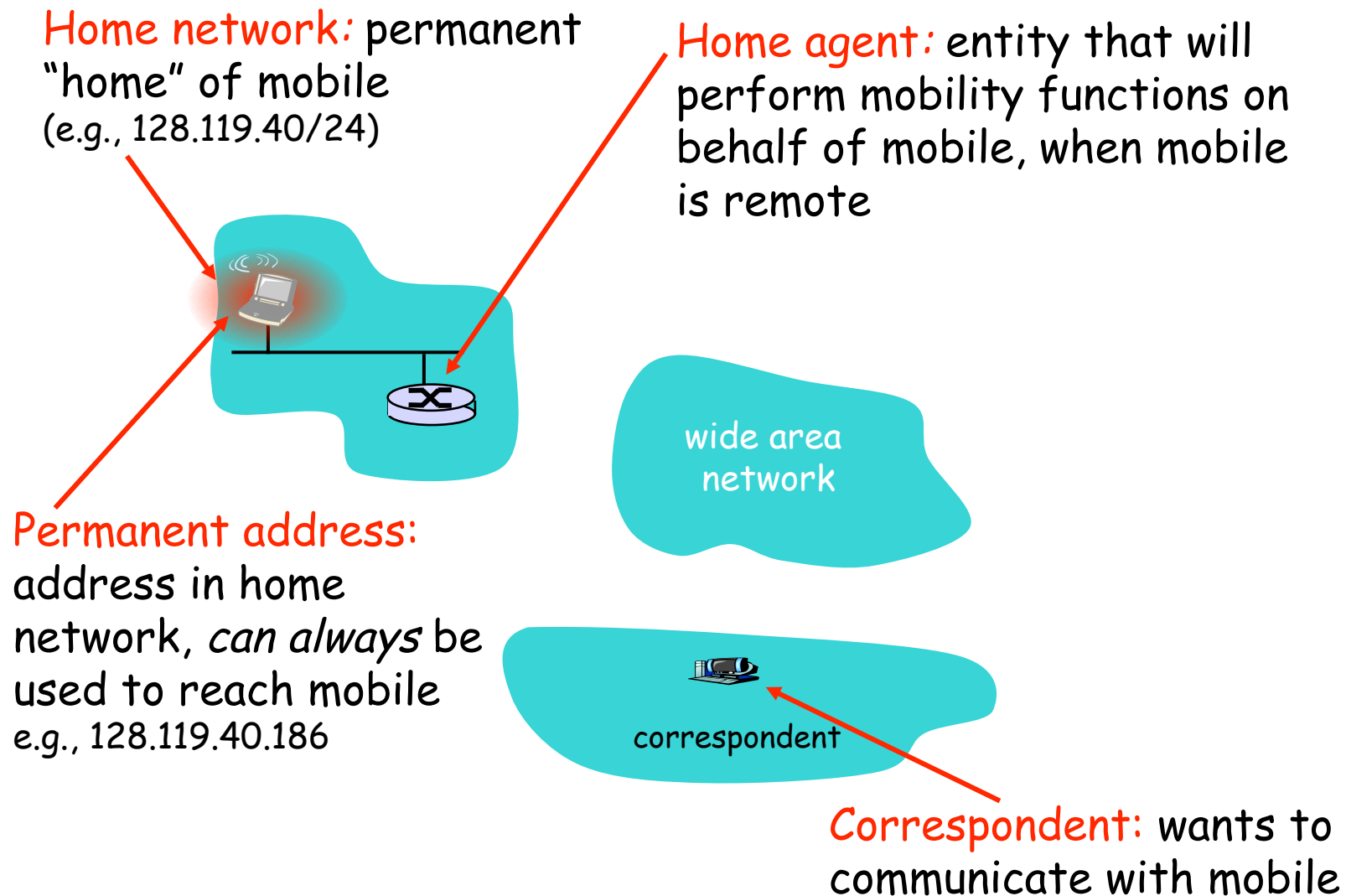
Example: Boeing Connexion Service



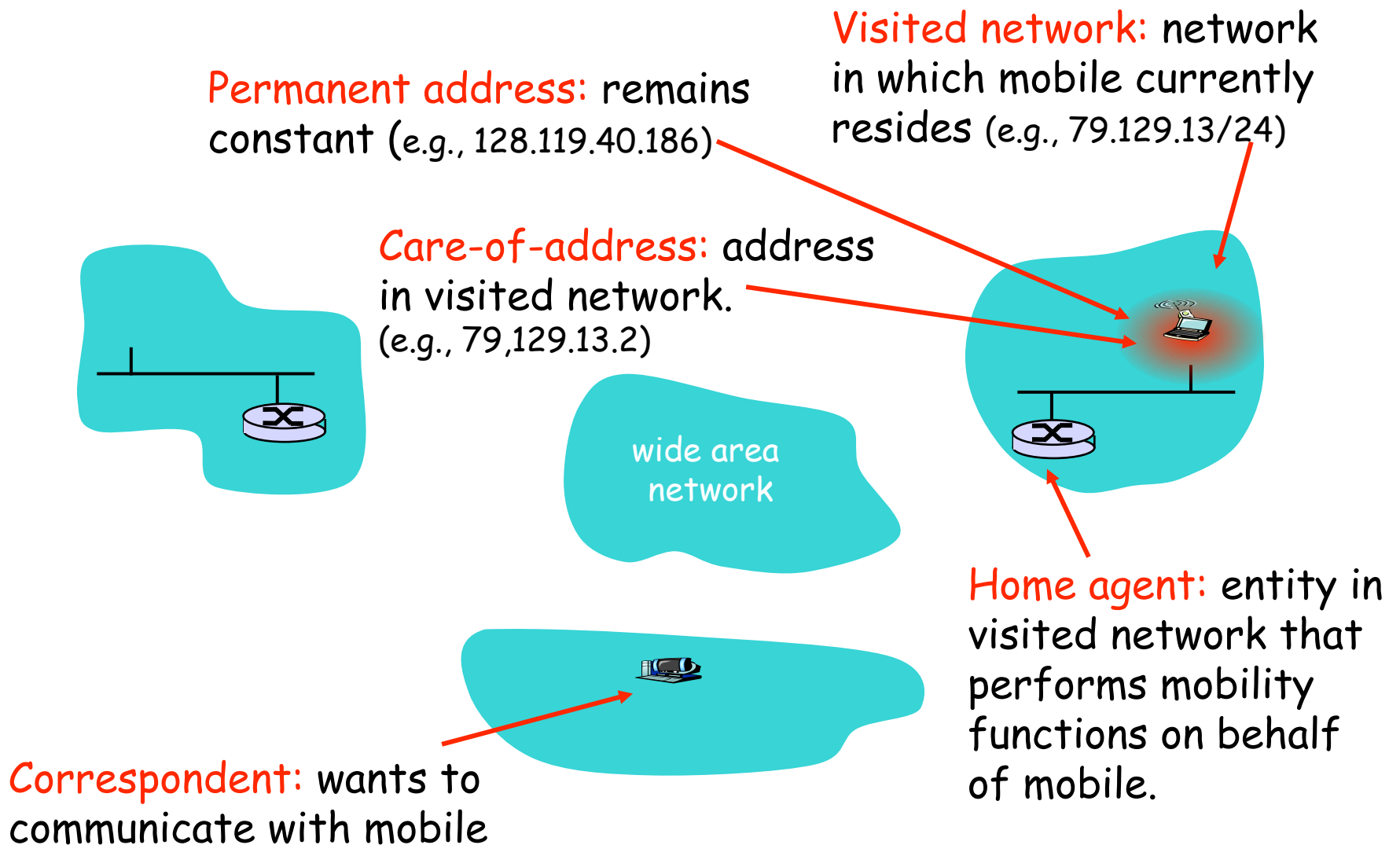
Summary: Letting Routing Handle It

- **Advantages**
 - No changes to the end host
 - Traffic follows an efficient path to new location
- **Disadvantages**
 - Does not scale to large number of mobile hosts
 - Large number of routing-protocol messages
 - Larger routing tables to store smaller address blocks
- **Alternative**
 - Mobile IP

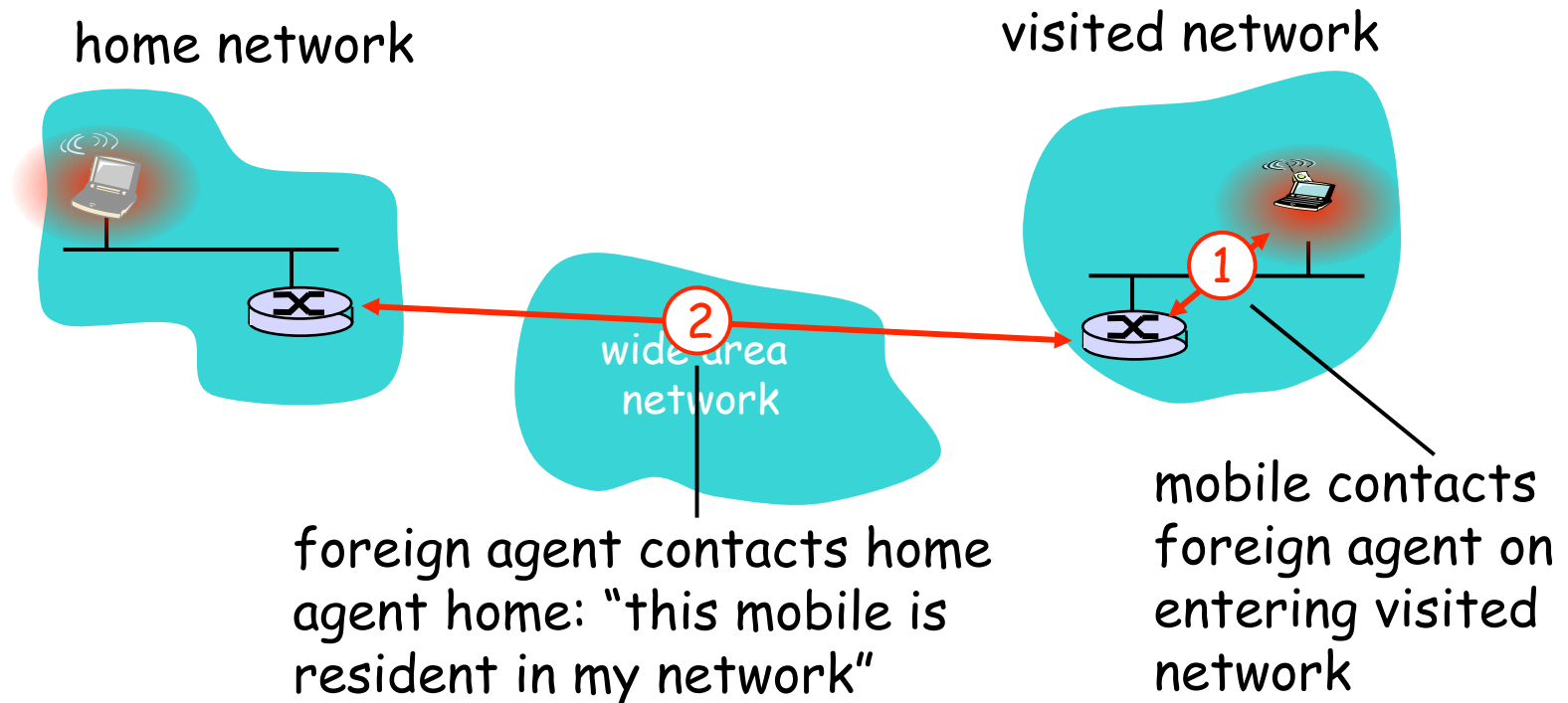
Option #2: Home Network and Home Agent



Visited Network and Care-of Address

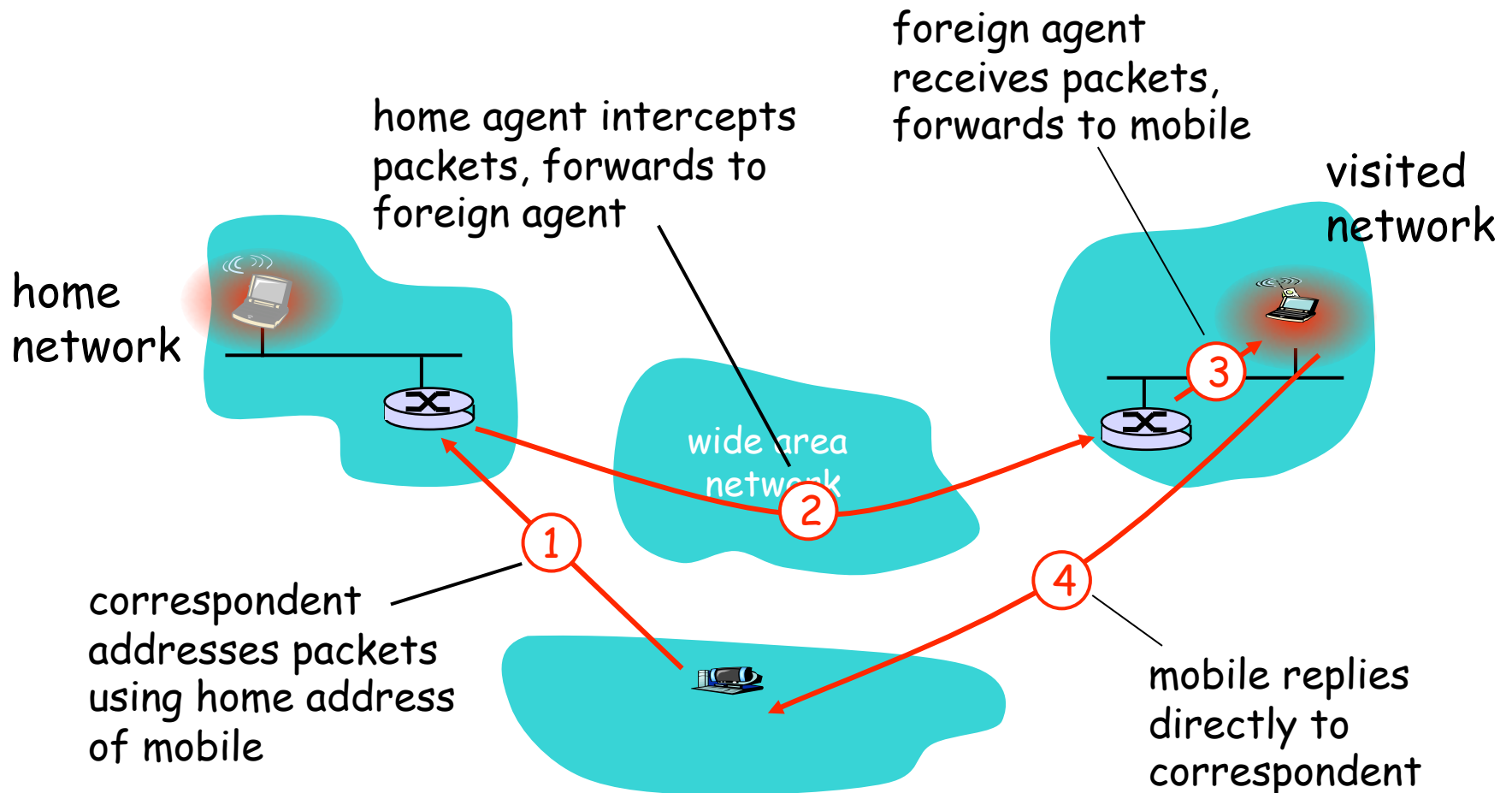


Mobility: Registration



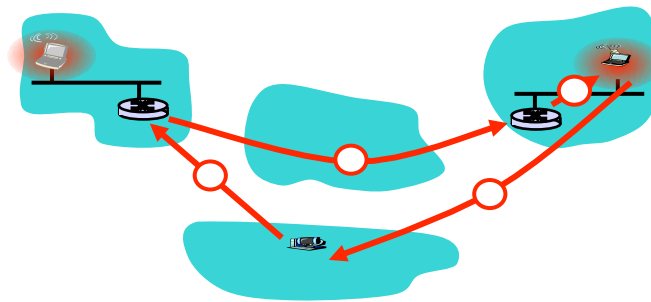
- Foreign agent knows about mobile
- Home agent knows location of mobile

Mobility via Indirect Routing

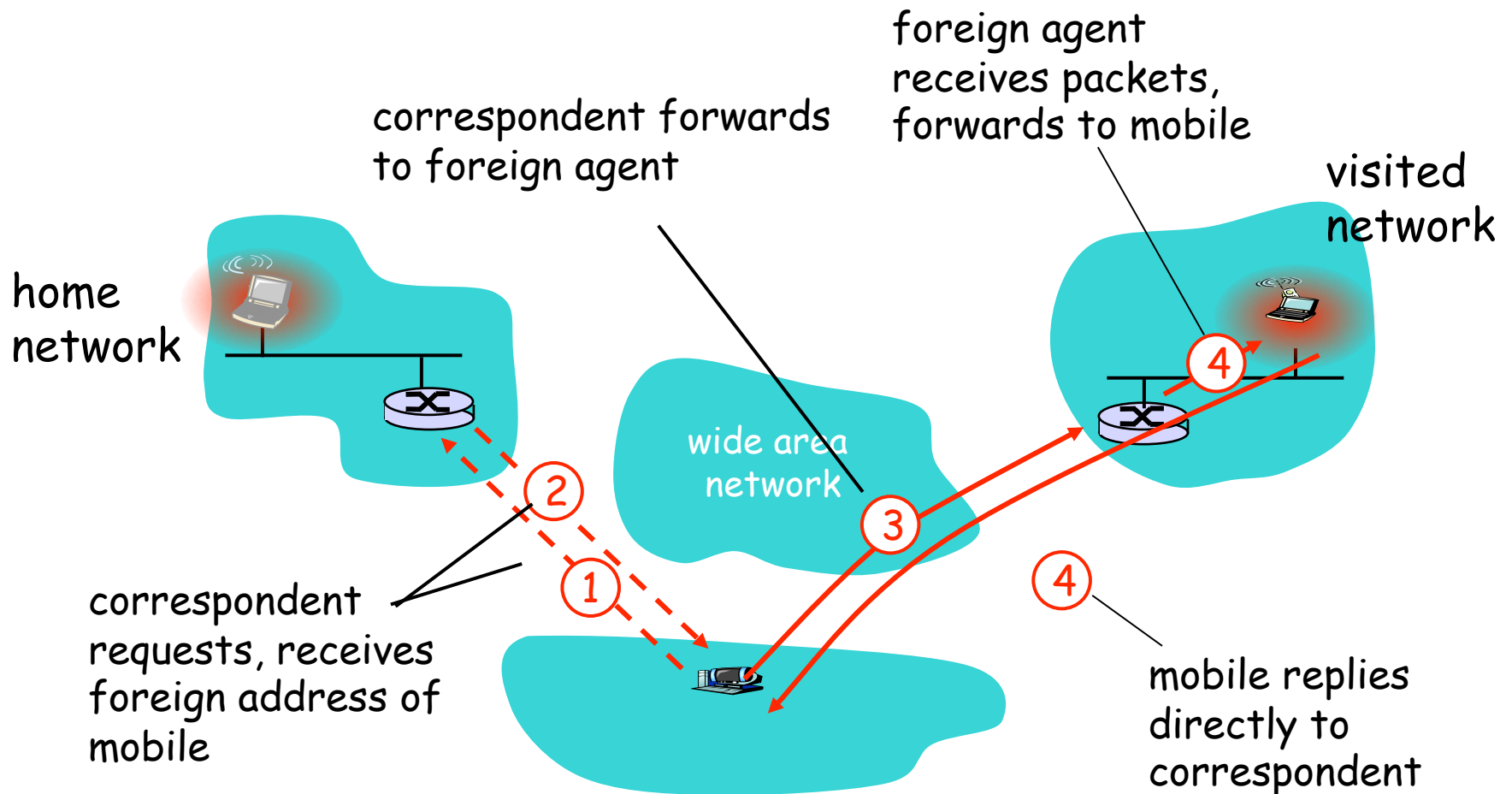


Indirect Routing: Efficiency Issues

- Mobile uses two addresses
 - Permanent address: used by correspondent (making mobile's location is transparent to correspondent)
 - Care-of-address: used by the home agent to forward datagrams to the mobile
- Mobile may perform the foreign agent functions
- Triangle routing is inefficient
 - E.g., correspondent and mobile in the same network



Mobility via Direct Routing



No longer transparent to the correspondent

Mobility Today

- Limited support for mobility
 - E.g., among base stations on a campus
- Applications increasingly robust under mobility
 - Robust to changes in IP address, and disconnections
 - E.g., e-mail client contacting the e-mail server
 - ... and allowing reading/writing while disconnected
 - New Google Gears for offline Web applications
- Increasing demand for seamless IP mobility
 - E.g., continue a VoIP call while on the train
- Increasing integration of WiFi and cellular
 - E.g., dual-mode cell phones that can use both networks
 - Called Unlicensed Mobile Access (UMA)

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**
 - 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