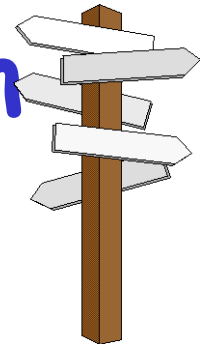
Evolving Internet: Architectural Challenges and solutions

Chadi BARAKAT

INRIA Sophia Antipolis, France
Diana Research Group

Email: Chadi.Barakat@inria.fr
WEB: http://team.inria.fr/diana/chadi/

Course schedule and evaluation



Four lectures (my part)

Friday, September 13 – Internet Mobility

Friday, September 20 – Routing in Mobile Wireless Networks (HW1)

Friday, October 11 – Routing in Mobile Disconnected Networks

Friday, October 18 – Transport and congestion control (HW2)

Three lectures by Walid Dabbous

Fridays Sep 27, Oct 4 and Oct 25 – Intra and inter domain routing (HW3)

Continuous evaluation of class work and home work (HW1, HW2 and HW3)

Written exam on November 8, 2024 (50% of final mark)

Internet and Wireless Mobility

Chadi BARAKAT

INRIA Sophia Antipolis, France
DIANA group

Email: Chadi.Barakat@inria.fr
WEB: http://team.inria.fr/diana/chadi/

References - Sources

- Slides of Prof. Jennifer Rexford, Princeton Univ.
- Slides of Prof. Jim Kurose, Umass Univ at Amherst.
- "Computer Networking book" by Jim Kurose and Keith Ross
- Lecture "Mobile Networks: IP Routing and MANET Routing Algorithms" by Intel Education

Internet is more and more mobile

- More than 2 billion cellular subscribers
- Widespread deployment of wireless local area networks
- Widespread usage of laptops and PDAs over work stations

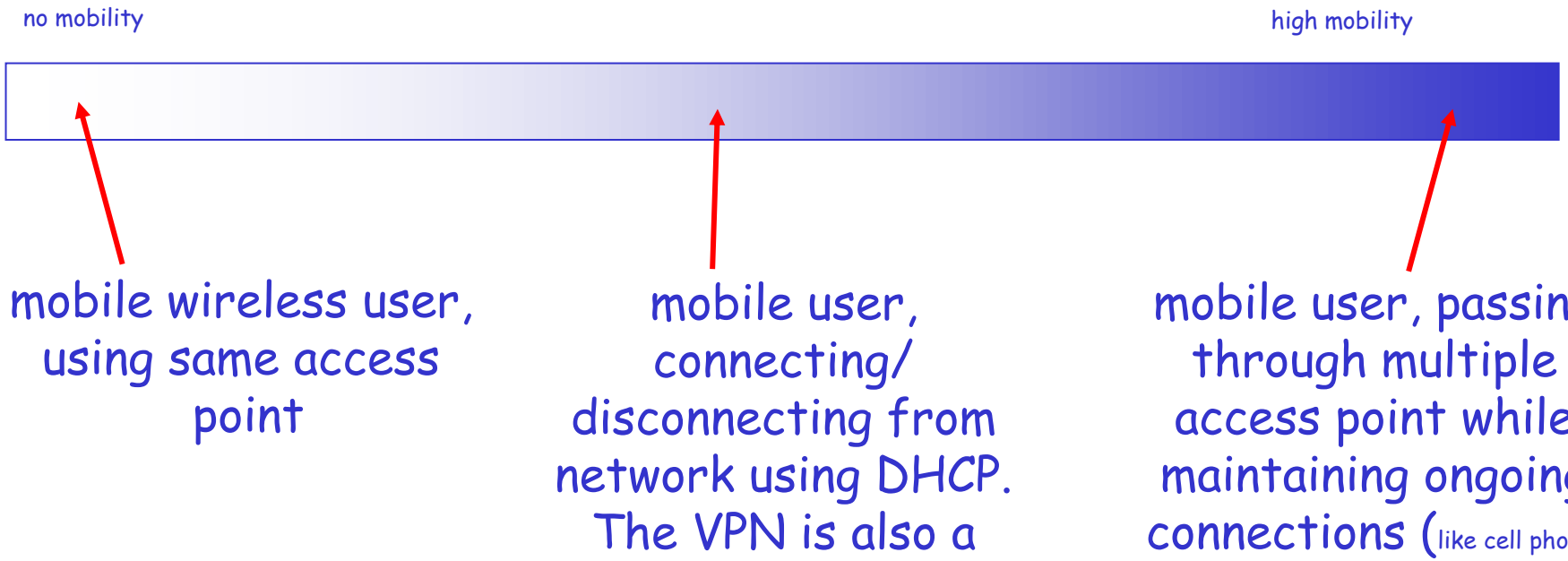
- Even routers are becoming mobile:
  - Internet in the plane, in the train, satellites as routers, etc.
- VPN and Tunnels

Wireless Internet vs. Cellular networks

- You can do Internet in cellular networks …
  - You connect to a dial up server in your home network or any other network and you stay connected with it while you move
  - Cellular network is a kind of logical link layer 2
  - Mobility is transparent to IP
- A wireless Internet is a one that understands IP
  - MSC are routers having IP addresses
  - Base stations can also have their own IP addresses
  - Routers can be all wireless (case of mesh networks)
  - And all this can move
  - The well known norm is 802.11 with its two modes access point and infrastructure
  - WiMax is also coming

Spectrum of mobility

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



Spectrum of mobility (ctd)

- Moves only within same access network
  - Single access point: mobility is irrelevant
  - Multiple access points: only 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

Main problems with mobility

- How to find someone ?
  - IP address is a locator not an identifier
  - Name of a machine could be a identifier
  - DNS works today
    - Solves the (name, locator) question
  - Does not scale to frequent updates
- How to maintain the connections ?
  - No session layer in the Internet
  - Connections use IP address as ID ☹
    - TCP and UDP
    - Think about sockets
  - They break when IP changes (your msn disconnects you)
- Internet applications designed for static machines

Goals of Today's Lecture

- Host Mobility at the wireless link level (below IP)
  - IP address does not change.
  - Mobility in GSM as an example. Handled by layer 2.

- Host Mobility at the IP level / Fixed Network
  - addressing and routing challenges
  - Keeping track of the host's changing attachment point
  - Maintaining a data transfer as the host moves

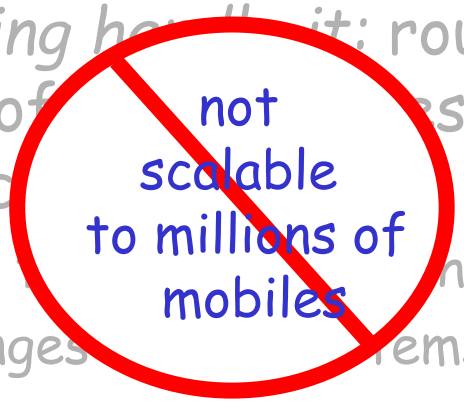
- Host Mobility at the IP level / Mobile Network
  - routing in MANETs and DTNs

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 address of mobile-nodes-in-residence via usual routing table exchange.
  - routing scalability where each router must include an entry for every mobile in the world
  - no changes to end-systems



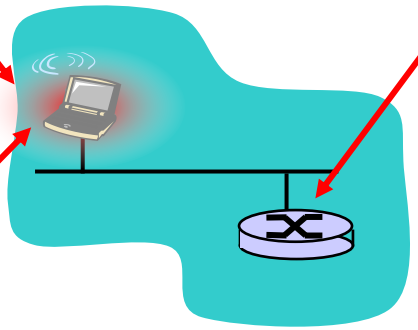
- *let end-systems handle it:*
  - *indirect routing:* communication from correspondent to mobile goes through home agent, then forwarded to remote
  - *direct routing:* correspondent gets foreign address of mobile, sends directly to mobile

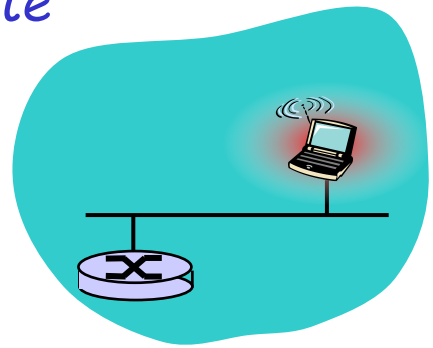
- First the end-system approach, then the routing one.

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*





wide area network

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

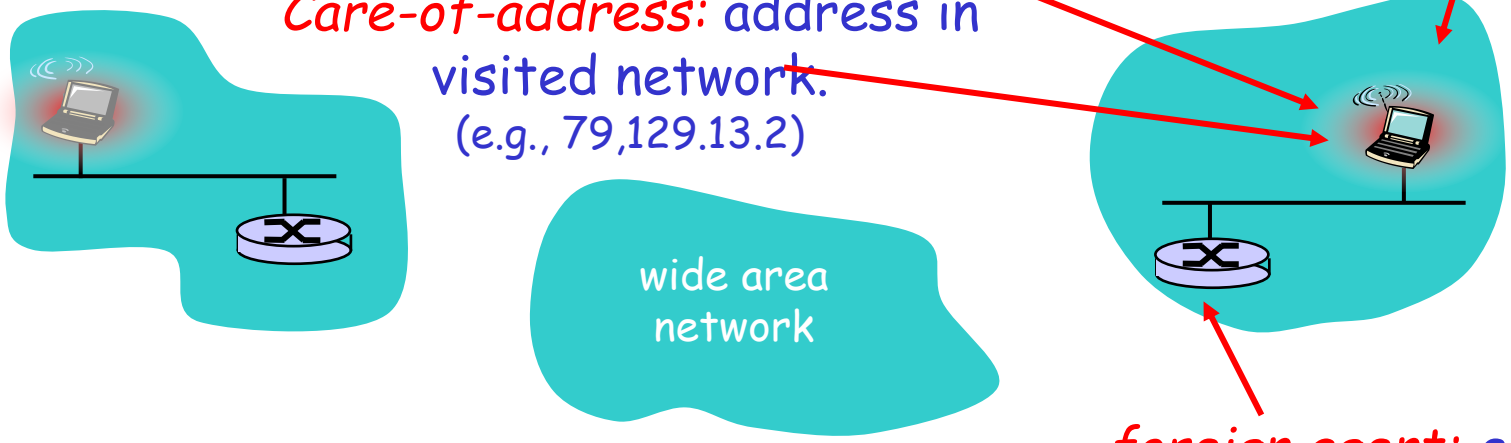
correspondent

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)

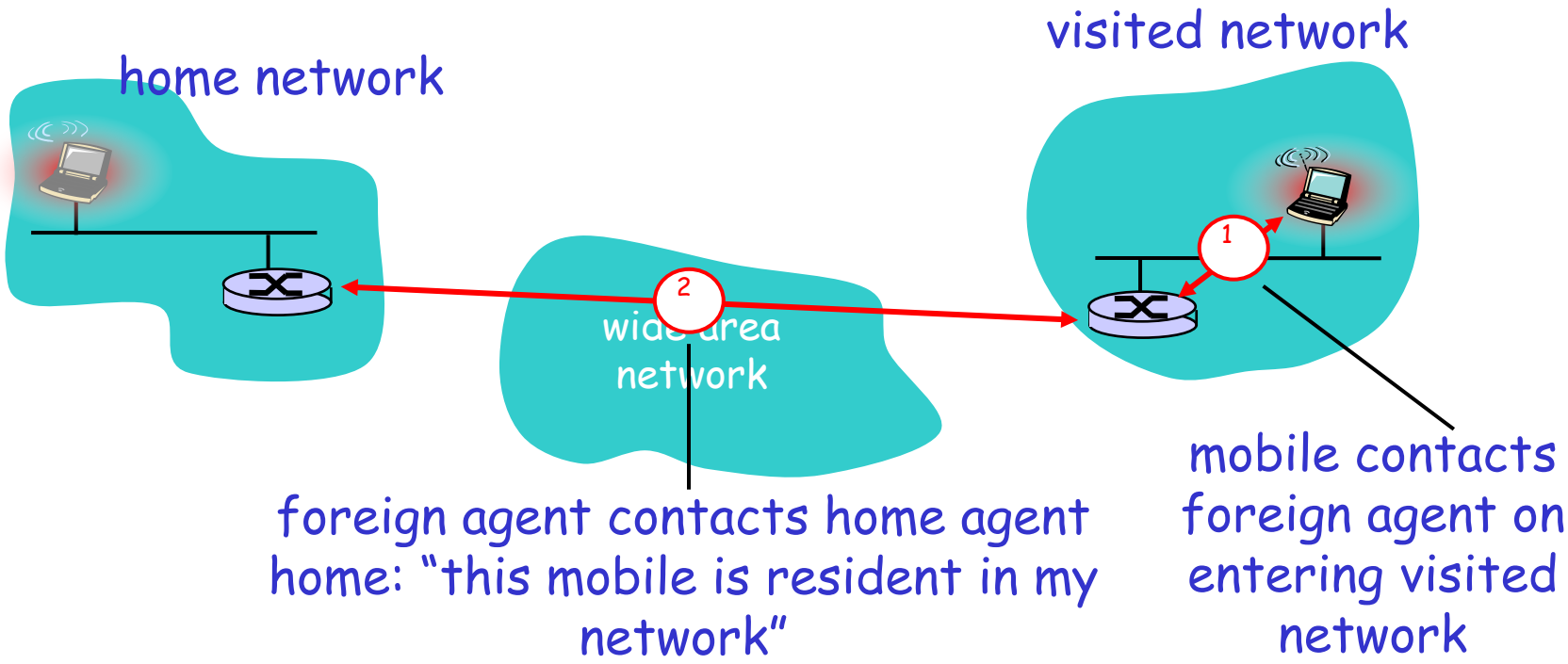
Care-of-address: address in visited network. (e.g., 79,129.13.2)



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

correspondent: wants to communicate with mobile

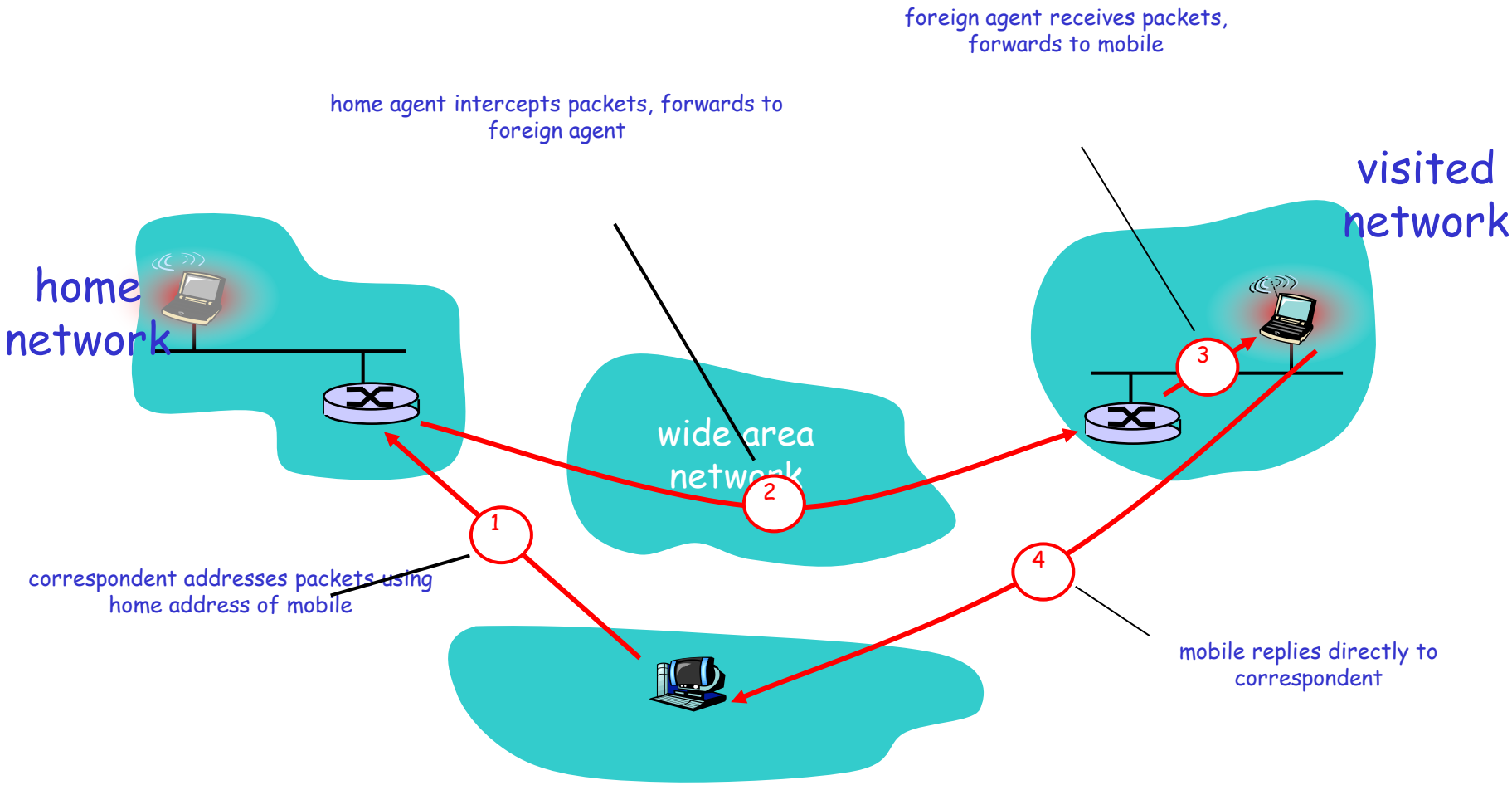
Mobility: registration



End result:

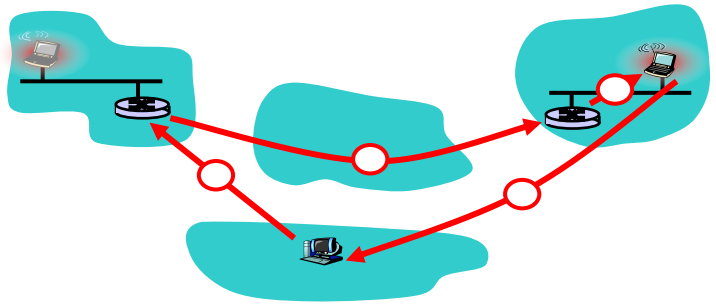
- Foreign agent knows about mobile
- Home agent knows location of mobile

Mobility via Indirect Routing



Indirect Routing: comments

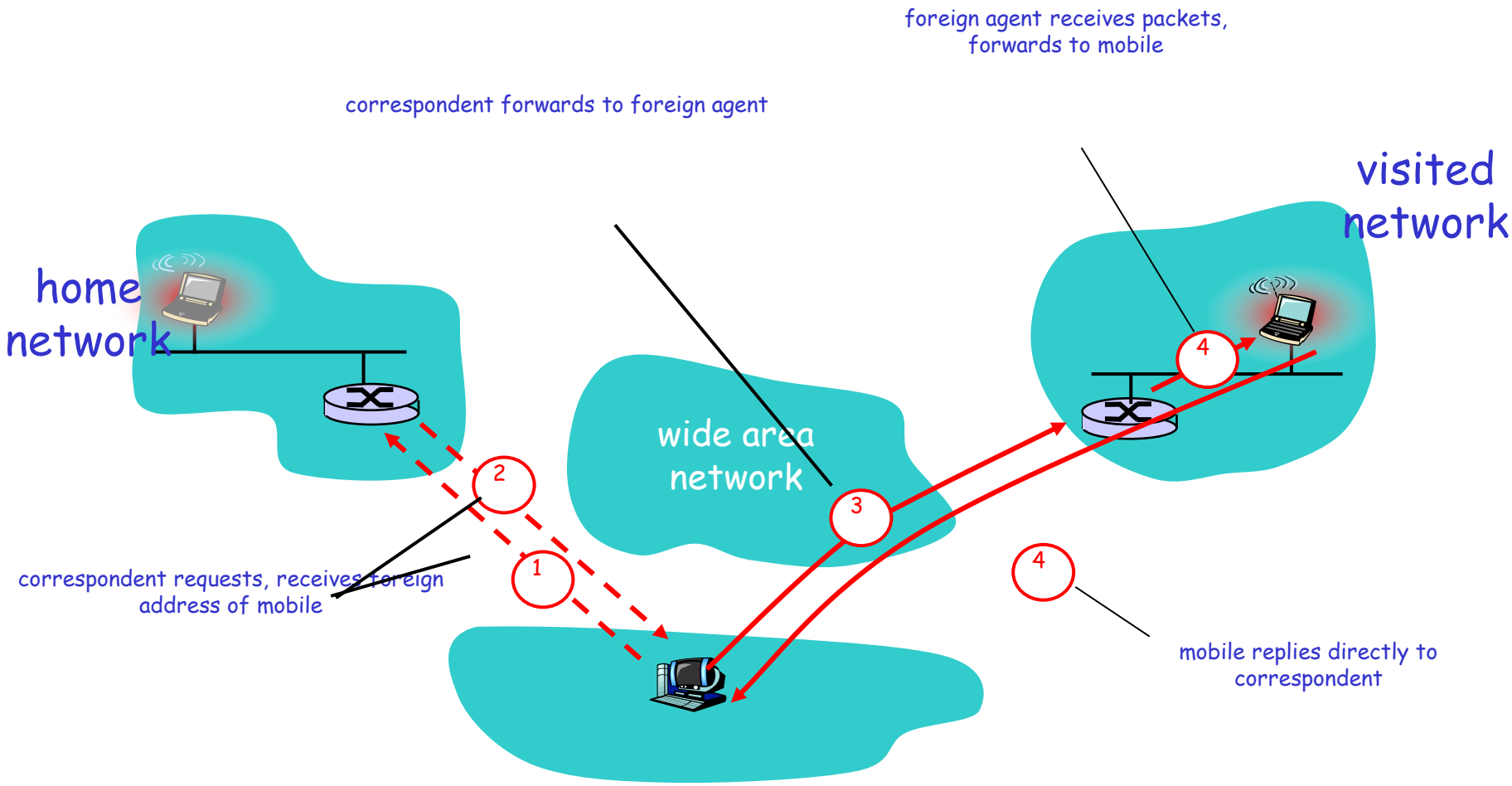
- Mobile uses two addresses:
  - permanent address: used by correspondent (hence mobile location is *transparent* to correspondent)
  - care-of-address: used by home agent to forward datagrams to mobile
- Connections established with permanent address.
  - They don't stop during movement.
- foreign agent functions may be done by mobile itself
- triangle routing: correspondent-home-network-mobile
  - Inefficient when correspondent and mobile are in same network (unnecessary long delay)



Indirect Routing: moving between networks

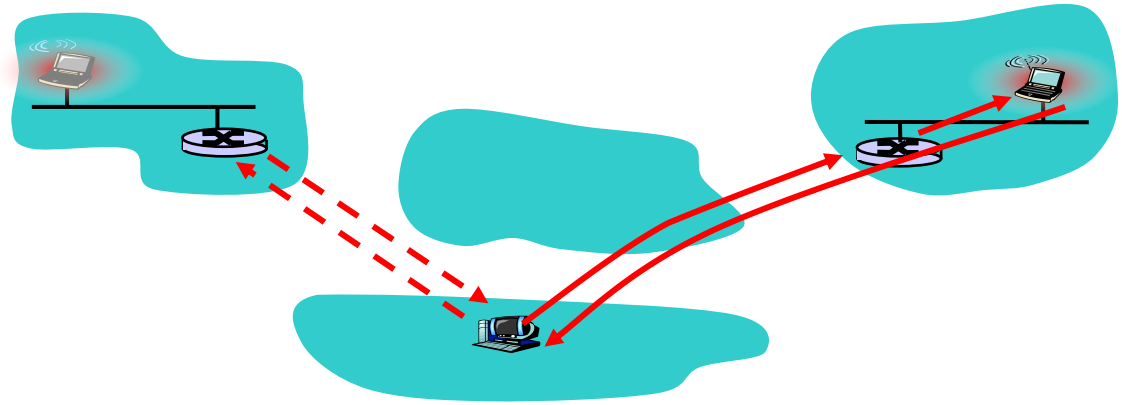
- suppose mobile user moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - packets continue to be forwarded to mobile (but with new care-of-address)
- mobility, changing foreign networks transparent: *on going connections can be maintained!*
- Think about packets in transit
  - Duty of old foreign agent to forward them to new foreign agent
  - Otherwise they are lost and have to be retransmitted

Mobility via Direct Routing



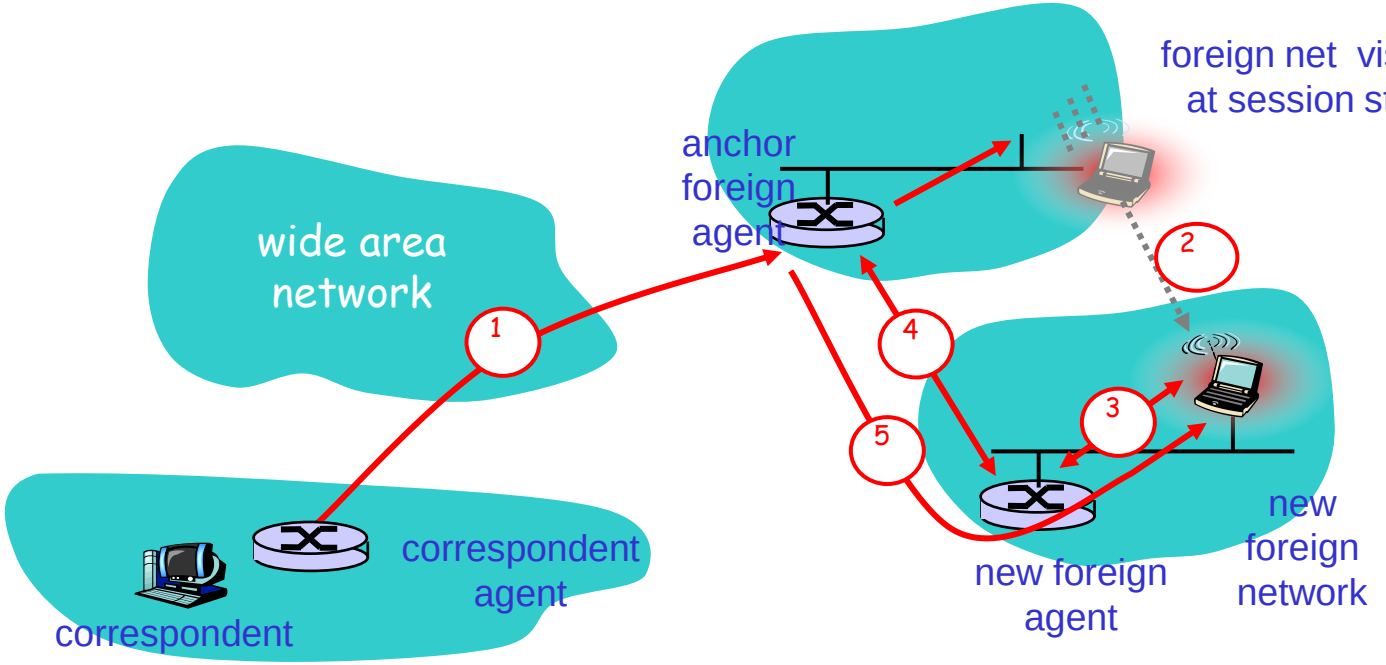
Mobility via Direct Routing: comments

- overcome triangle routing problem
  - Reduces routing delay.
- non-transparent to correspondent: correspondent must get care-of-address from home agent
  - what if mobile changes visited network during the communication?
  - The mobile only updates its home agent.
    Who updates the correspondant?



Accommodating mobility with direct routing

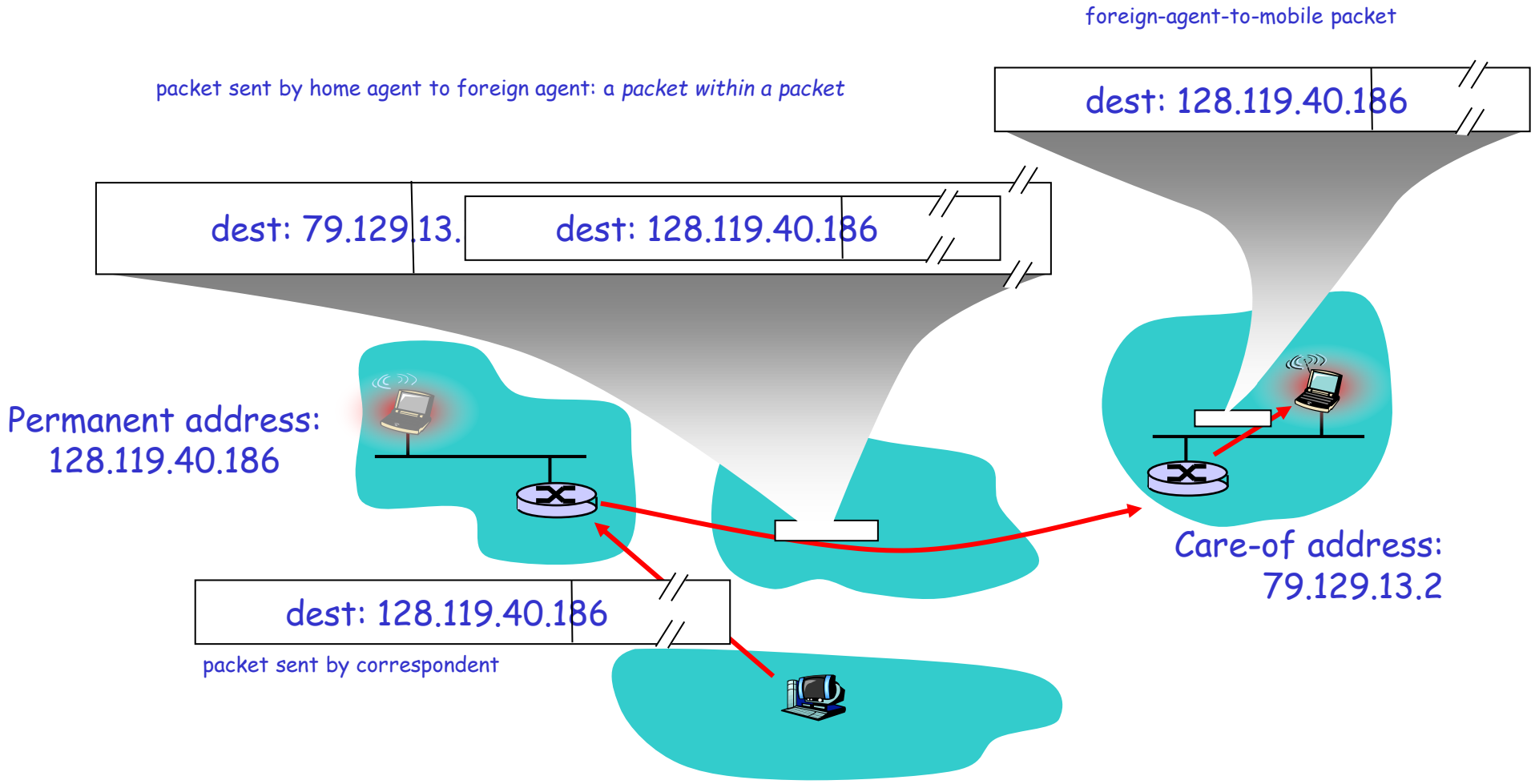
- anchor foreign agent: FA in first visited network
- data always routed first to anchor FA
- when mobile moves: new FA arranges to have data forwarded from old FA (chaining).
  - Longer and longer chain as mobile moves until communication ends.



Mobile IP

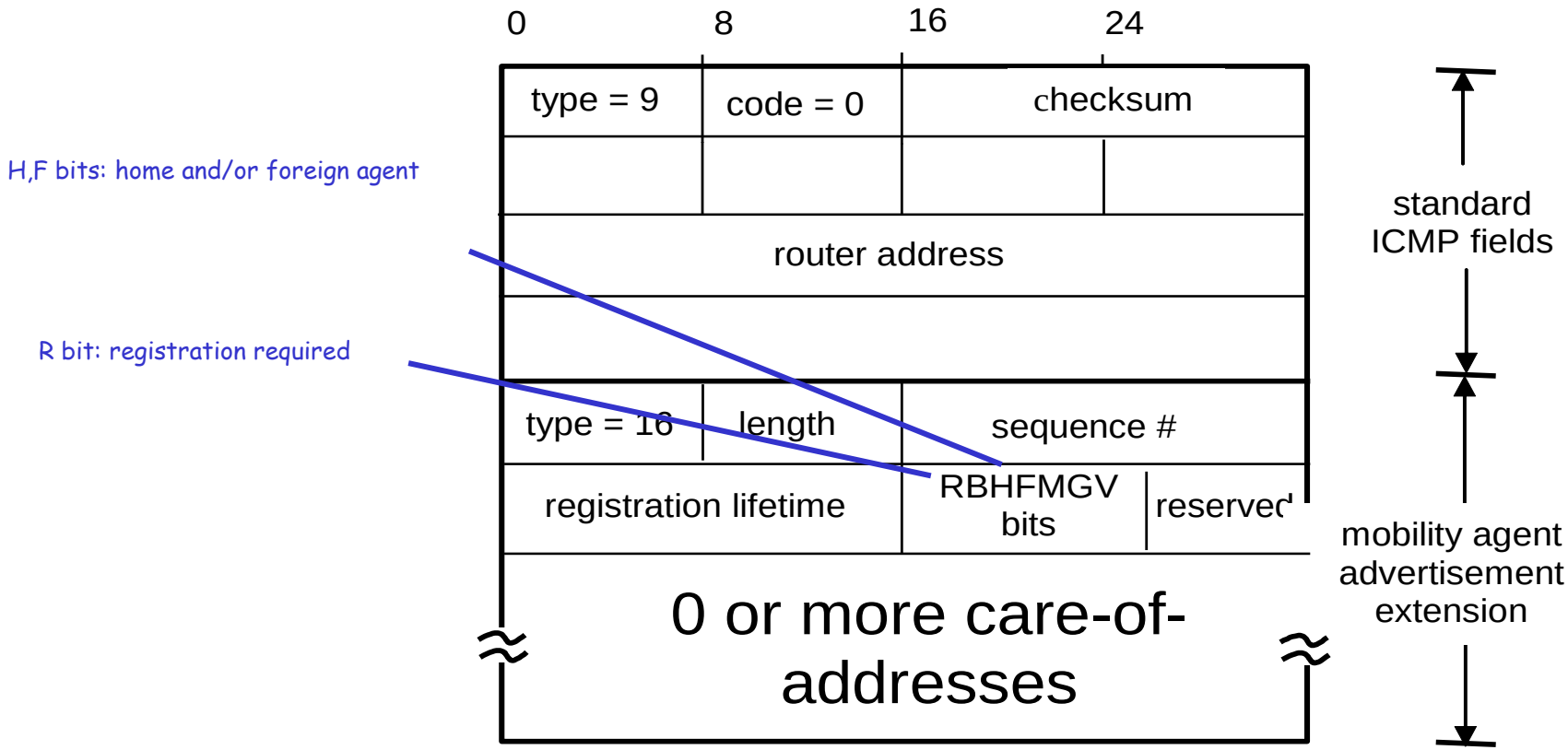
- RFC 3220
- Has many features we've seen:
  - home agents, foreign agents, foreign-agent registration, care-of-addresses, encapsulation (packet-within-a-packet)
- Three components to standard:
  - indirect routing of datagrams
  - agent discovery
  - registration with home agent
- Direct routing support will come with Mobile IPv6.

Mobile IP: indirect routing

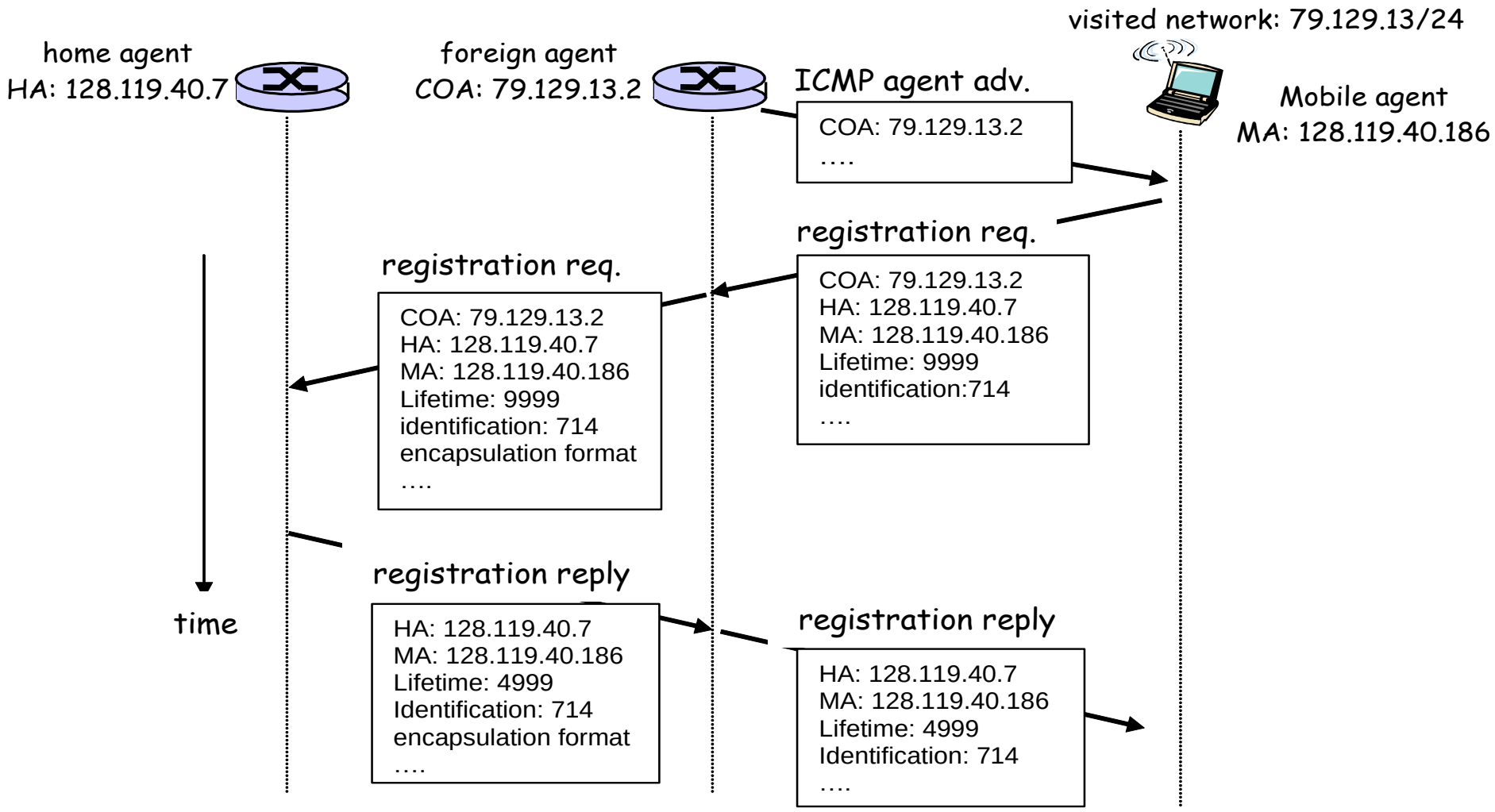


Mobile IP: agent discovery

- agent advertisement: foreign/home agents advertise service by broadcasting ICMP messages (typefield = 9)



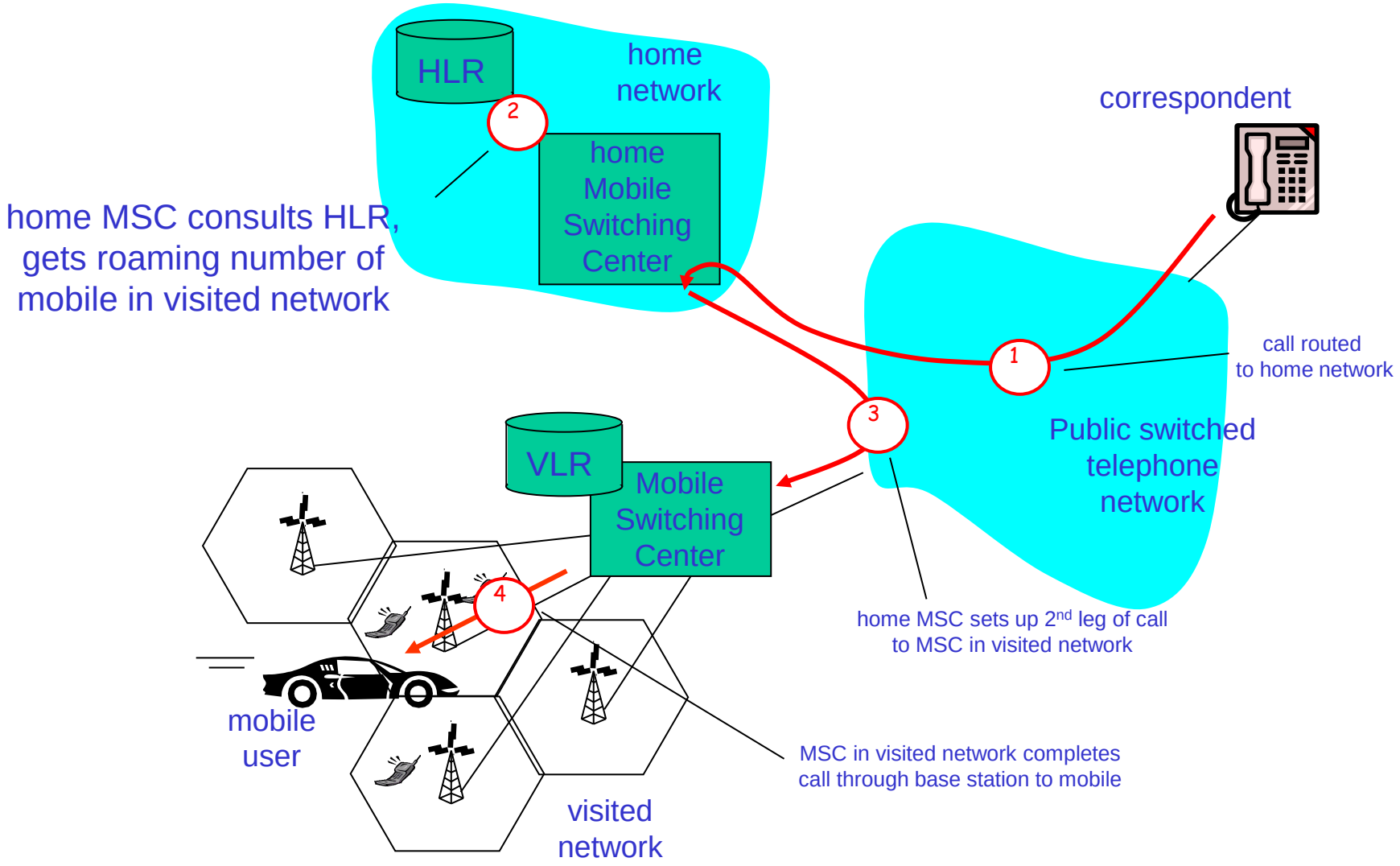
Mobile IP: registration example



Handling mobility in cellular networks (almost the same story)

- *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

Indirect routing to mobile (GSM)



Impact on Internet design

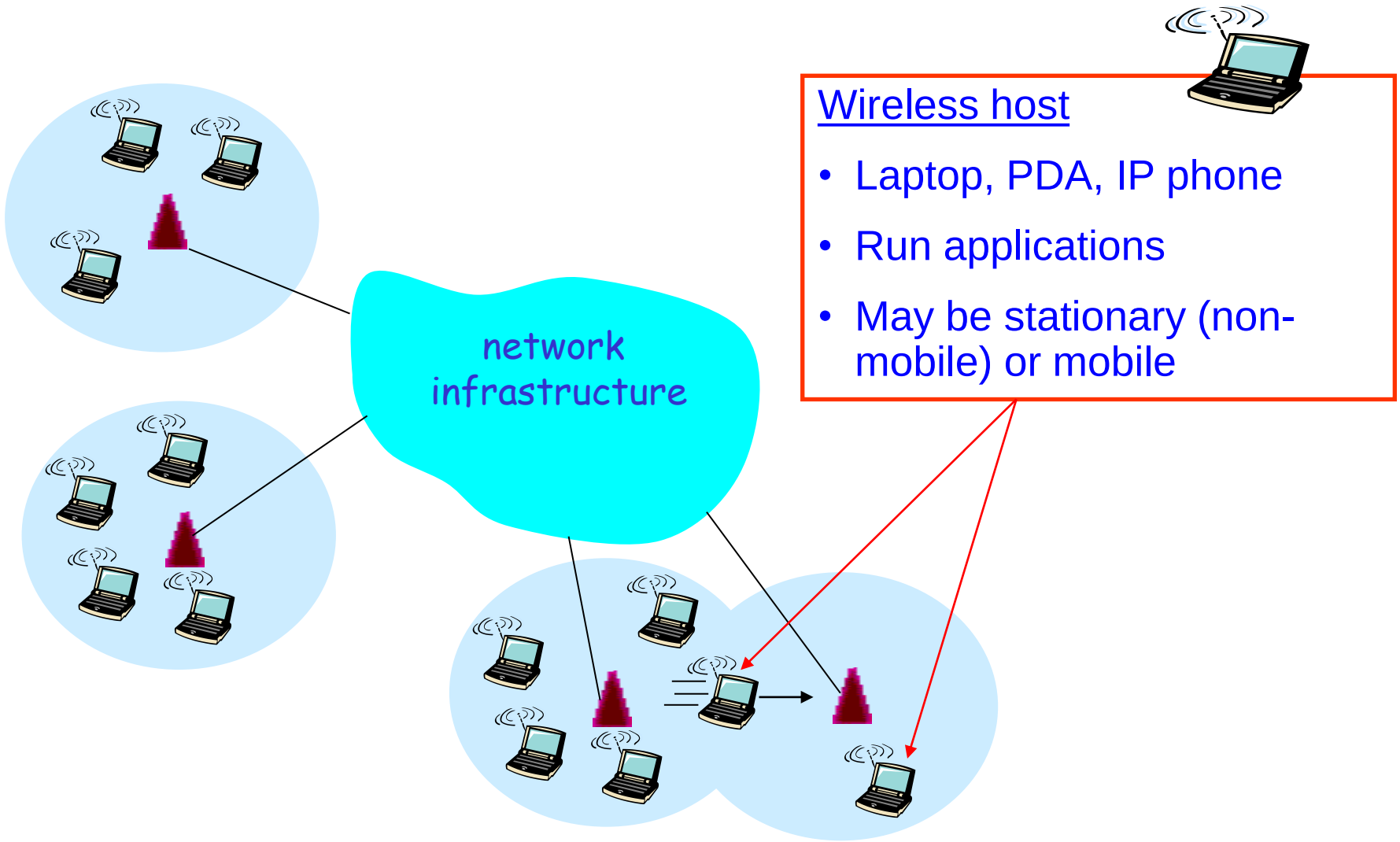
- Mobility breaks association of address (or ID) and location
  - When you move you change address. This can no longer be your ID
  - TCP (UDP) connections and many applications are lost when the IP address change (more and more applications resist by reopening the connection)
  - This cannot continue if we want seamless mobility
- Different options
  - Layer 3 solution a la mobile IP and shim6:
    - Same IP socket, same applications, IP changes hidden at the network layer
  - Layer 3 solution a la HIP, but that requires new socket definition
    - IP changes hidden at the network layer, but a new socket is needed to account for a new identity (e.g. public key), other than the IP address
  - Layer 4 solution a la SCTP: exploit all existing IP addresses
    - Mostly one transport connection per pair of IP addresses
  - Application level solutions
- Always a need for a home agent like approach for localization

Mobility Today

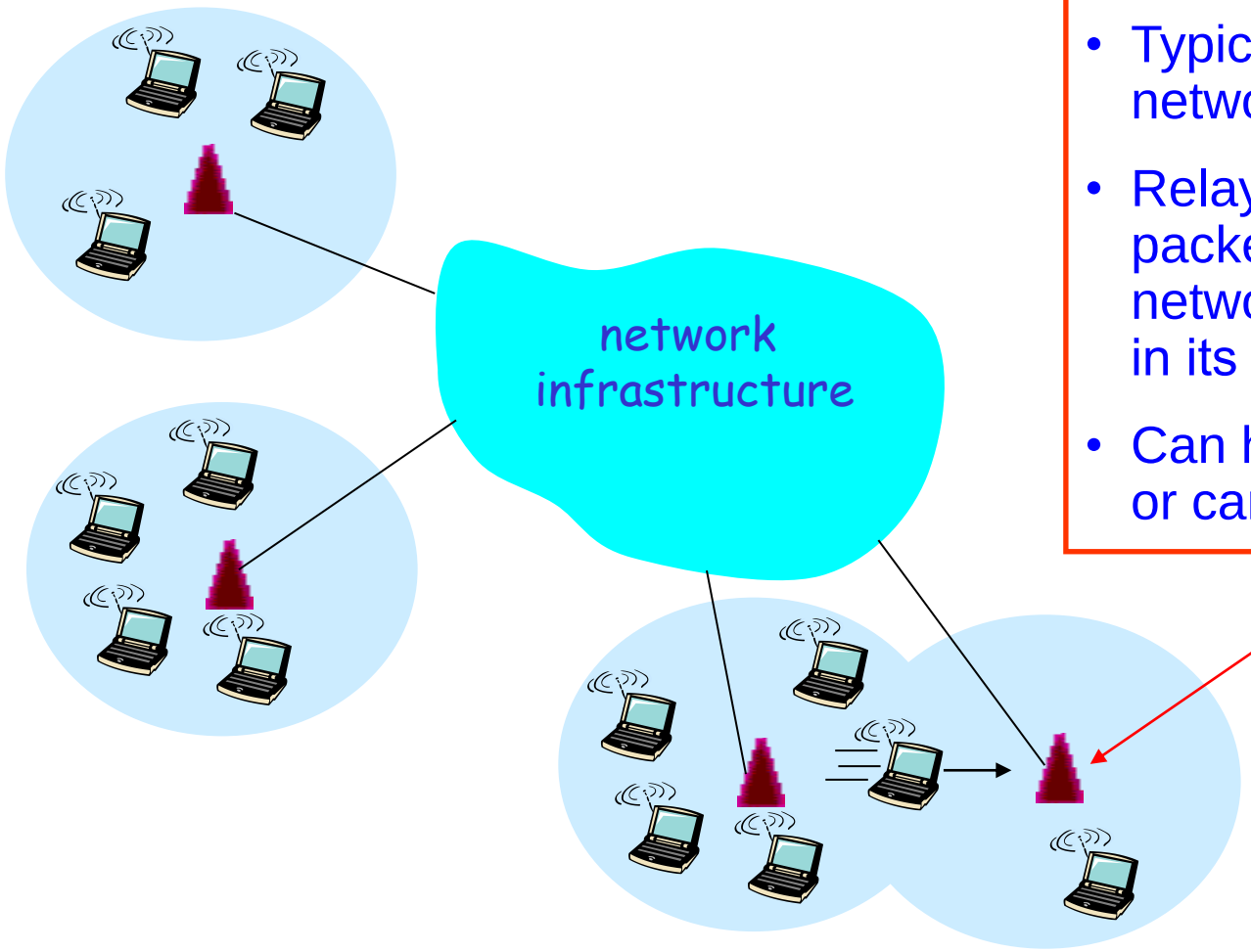
- Limited support for mobility, waiting for mobile IPv6
  - E.g., among base stations on a campus (same IP address)
- Applications increasingly robust under mobility
  - Robust to changes in IP address, and disconnections
    - E.g., e-mail client allowing reading/writing while disconnected
    - New Google Gears for offline Web applications
  - Localization ensured by per-service databases (msn, skype)
  - They replace sometimes the need for mobile IP
- Increasing number of interfaces per device
  - WiFi, 3G/4G, bluetooth, even cables on laptops
  - Known as multi-homing. Very beneficial for backup and load balancing
    - A problem for ongoing connections even in case of no mobility
    - Can be seen as a specific case of mobility
    - Active research area: SCTP then multipath TCP and iOS7

Wireless Networking

A Wireless Network



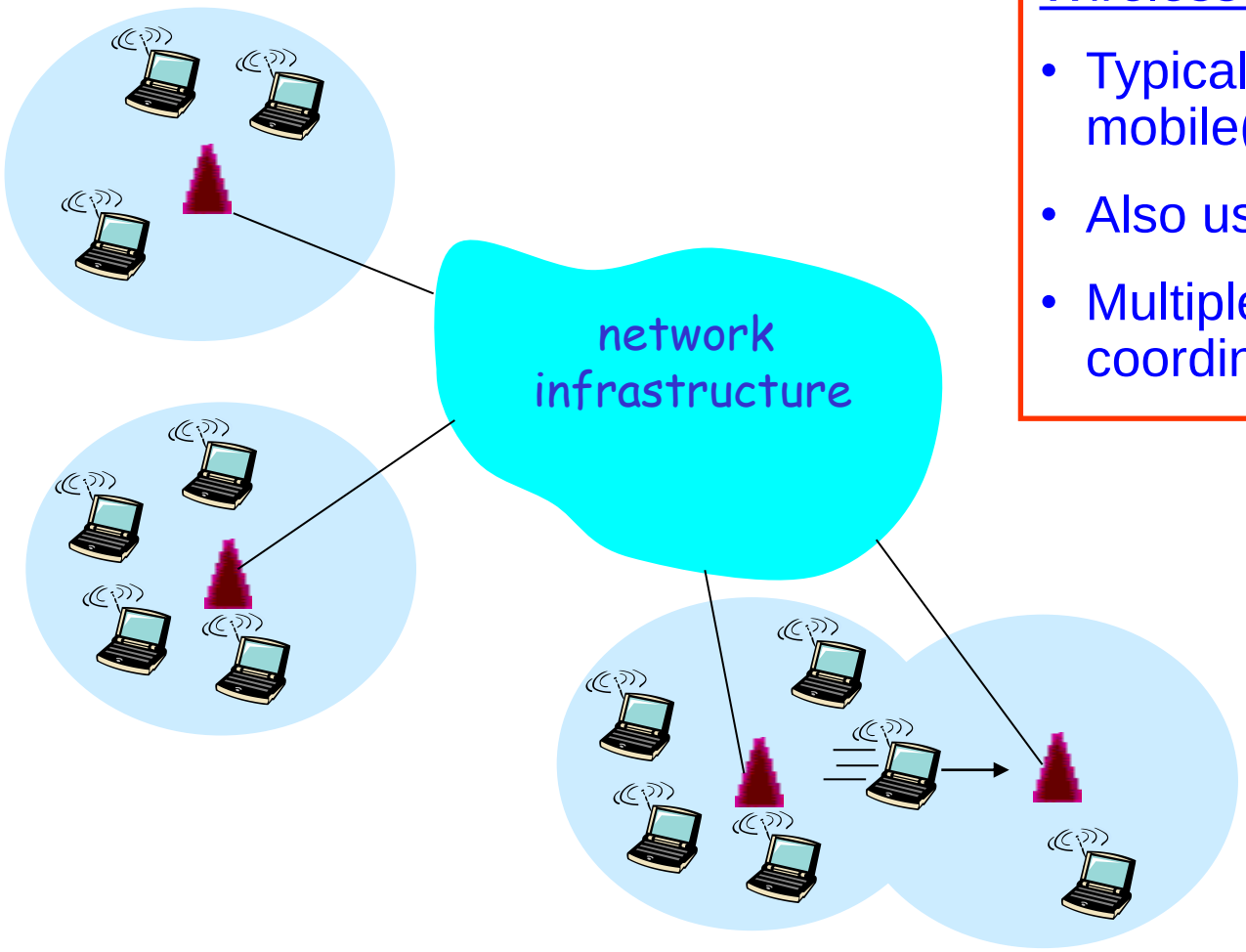
Wireless Network: Base Station



Base station

- Typically connected to wired network
- Relay responsible for sending packets between wired network and wireless host(s) in its “area”
- Can have its own IP address or can be at level 2 (bridge)

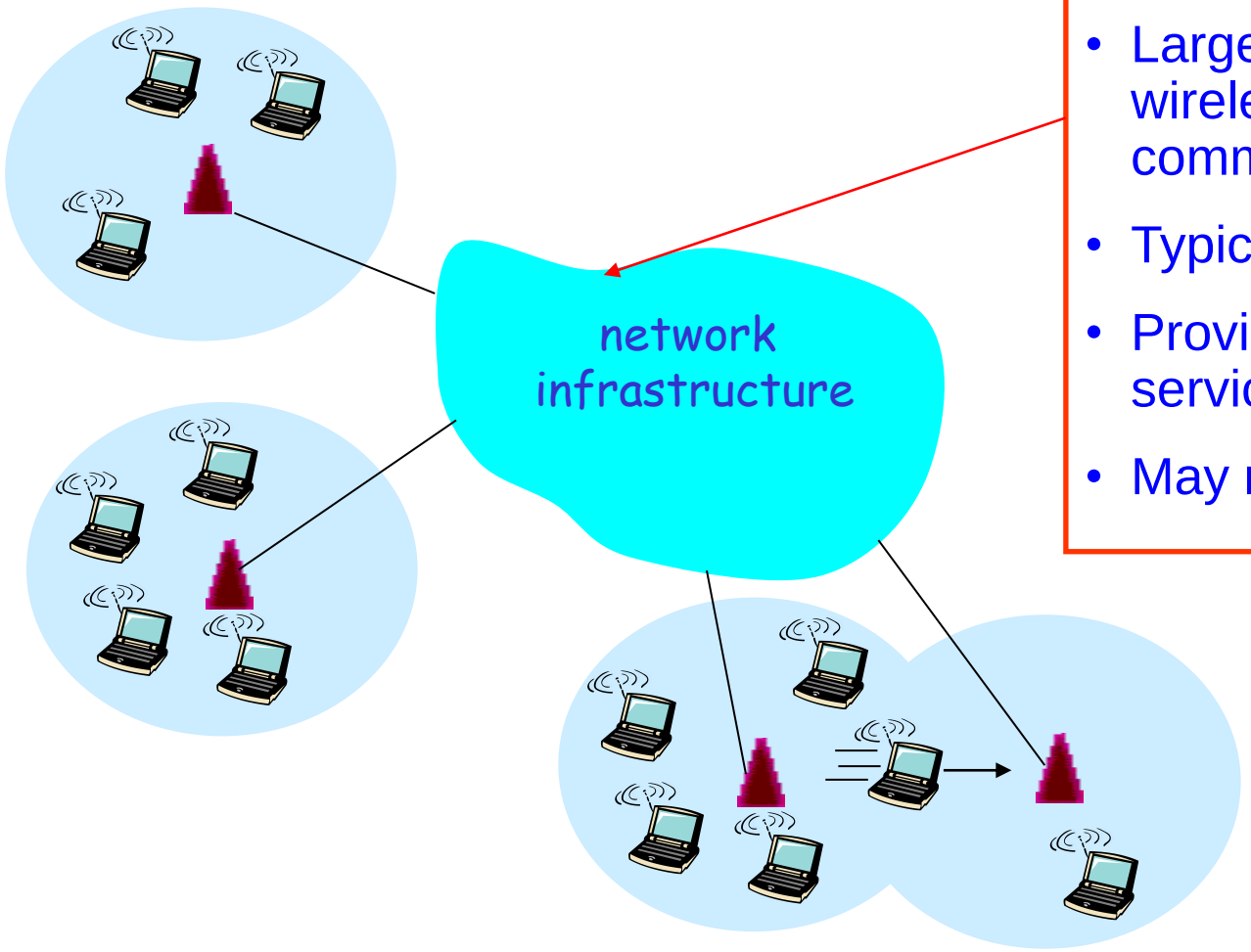
A Wireless Network



Wireless link

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

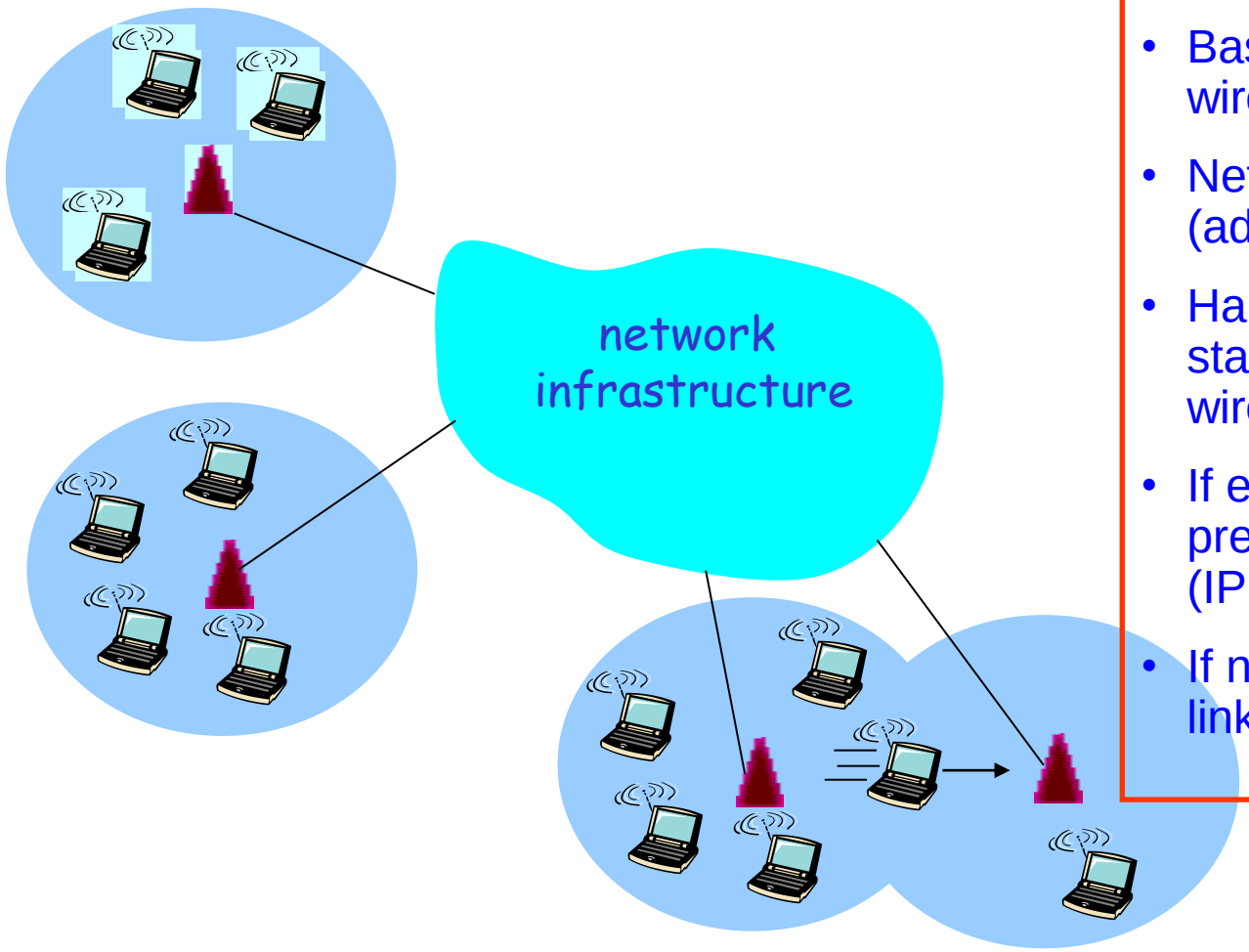
Wireless Network: Infrastructure



Network infrastructure

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

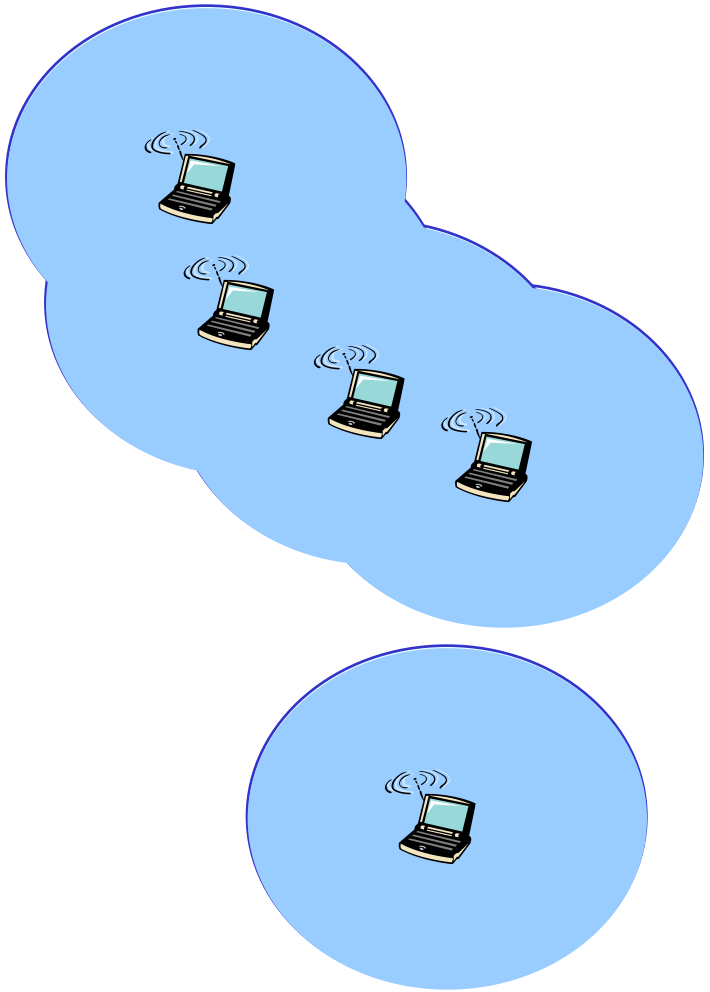
Scenario #1: Infrastructure Mode



Infrastructure mode

- Base station connects mobiles into wired network
- Network provides services (addressing, routing, DNS)
- Handoff: mobile changes base station providing connection to wired network
- If each AP has its own network prefix, mobile IP is to be used to (IP address to be changed)
- If not it is a simple handoff at the link level (a BS looks as a bridge)

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
- Routing to be dynamic to adapt to mobility of nodes
- This is what we call MANETs
- Mobility handled by IP routing in this case (remember the option 1, slides Mobility: Approaches)

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)

Wireless Network Characteristics

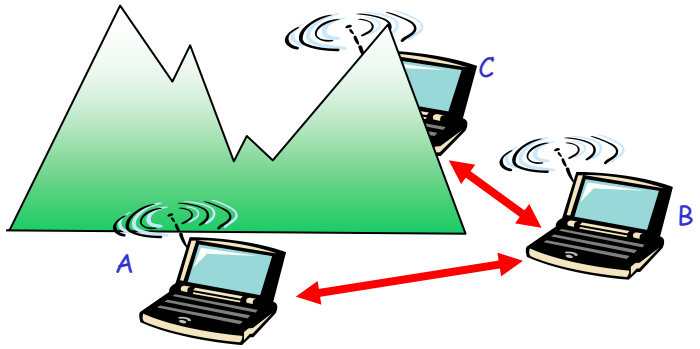
Differences from wired link ….

- decreased signal strength: radio signal attenuates as it propagates through matter (path loss)
- interference from other sources: standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., phone); devices (motors) interfere as well. Need for a MAC address.
- multipath propagation: radio signal reflects off objects ground, arriving ad destination at slightly different times

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

Wireless network characteristics

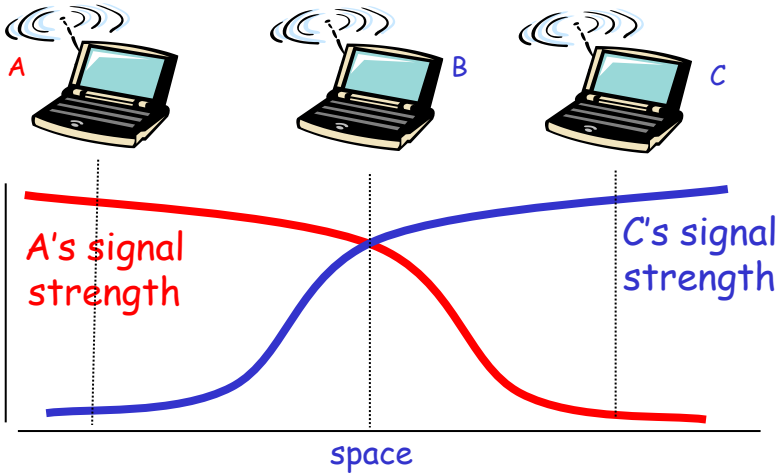
Multiple wireless senders and receivers create additional problems (beyond multiple access):



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 fading:

- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

IEEE 802.11 Wireless LAN

- 802.11b
  - 2.4-5 GHz unlicensed spectrum
  - up to 11 Mbps
  - direct sequence spread spectrum (DSSS) in physical layer
    - all hosts use same chipping code
- 802.11a
  - 5-6 GHz range
  - up to 54 Mbps
- 802.11g
  - 2.4-5 GHz range
  - up to 54 Mbps
- 802.11n: multiple antennae
  - 2.4-5 GHz range
  - up to 200 Mbps

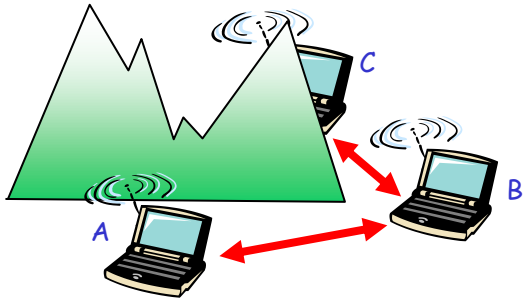
- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

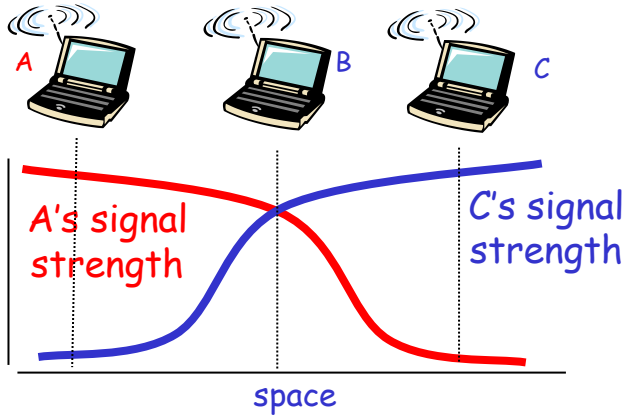
802.11: Channels, association

- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
  - AP admin chooses frequency for AP
  - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
  - scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
  - selects AP to associate with
  - may perform authentication
  - will typically 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
- 802.11: *no* collision detection!
  - difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
  - can't sense all collisions in any case: hidden terminal, fading
  - goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender

1 if sense channel idle for **DIFS** then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

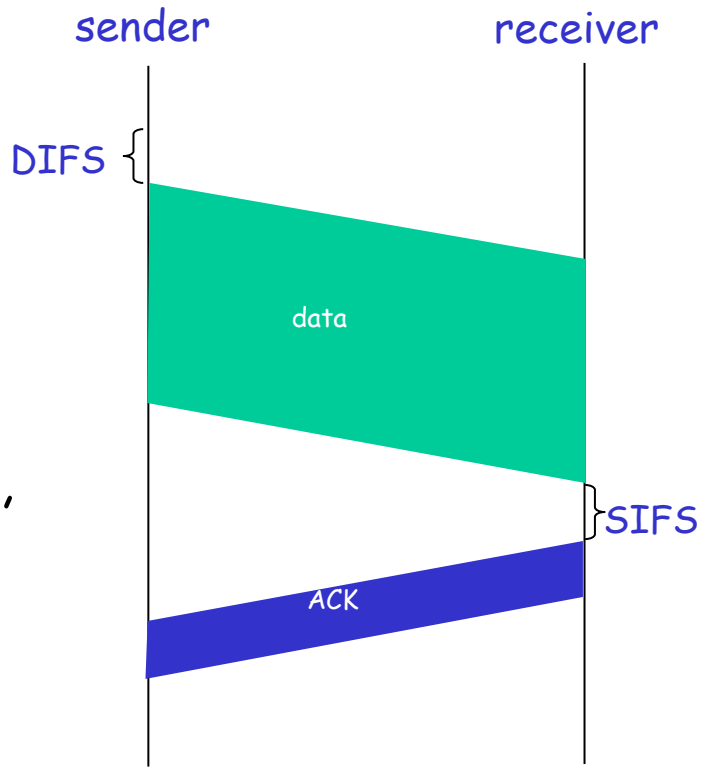
transmit when timer expires

if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK

return ACK after **SIFS** (ACK needed due to hidden terminal problem)



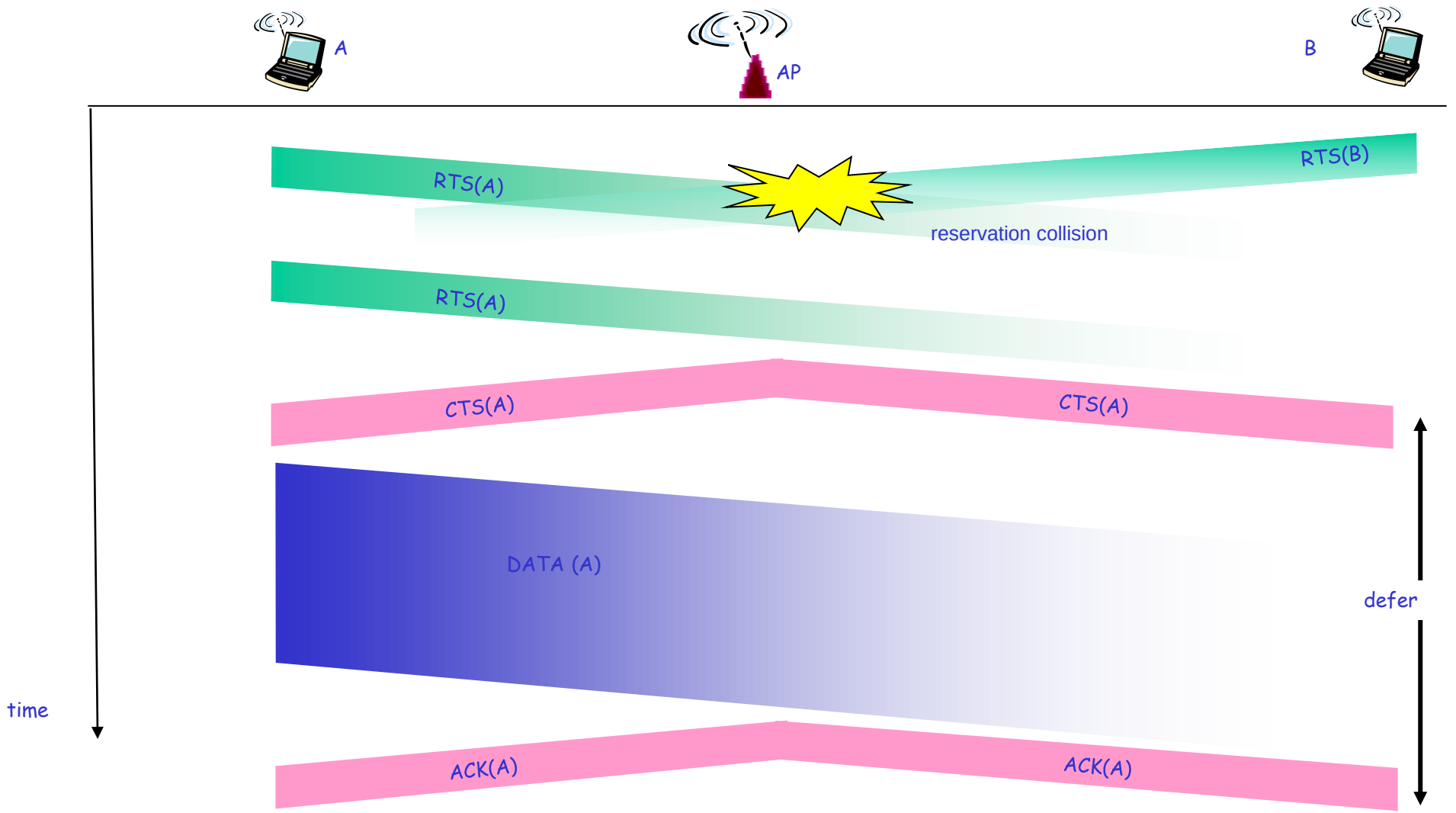
Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

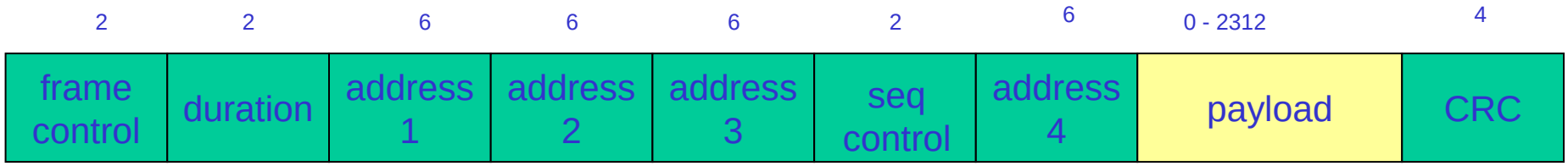
- sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTSs may still collide with each other (but they're short)
- BS broadcasts clear-to-send CTS in response to RTS
- RTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

Avoid data frame collisions completely using small reservation packets!

Collision Avoidance: RTS-CTS exchange



802.11 frame: addressing



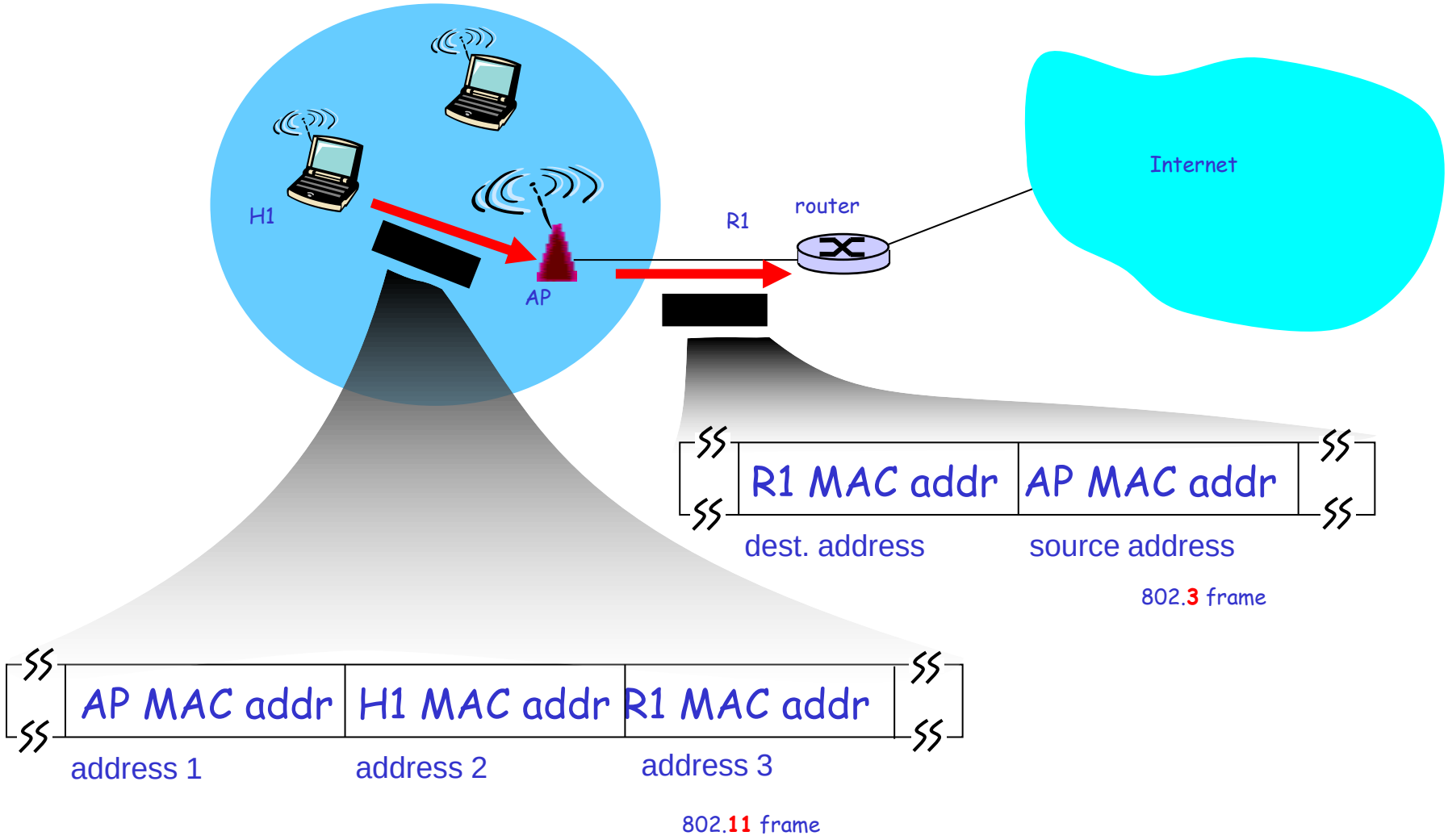
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

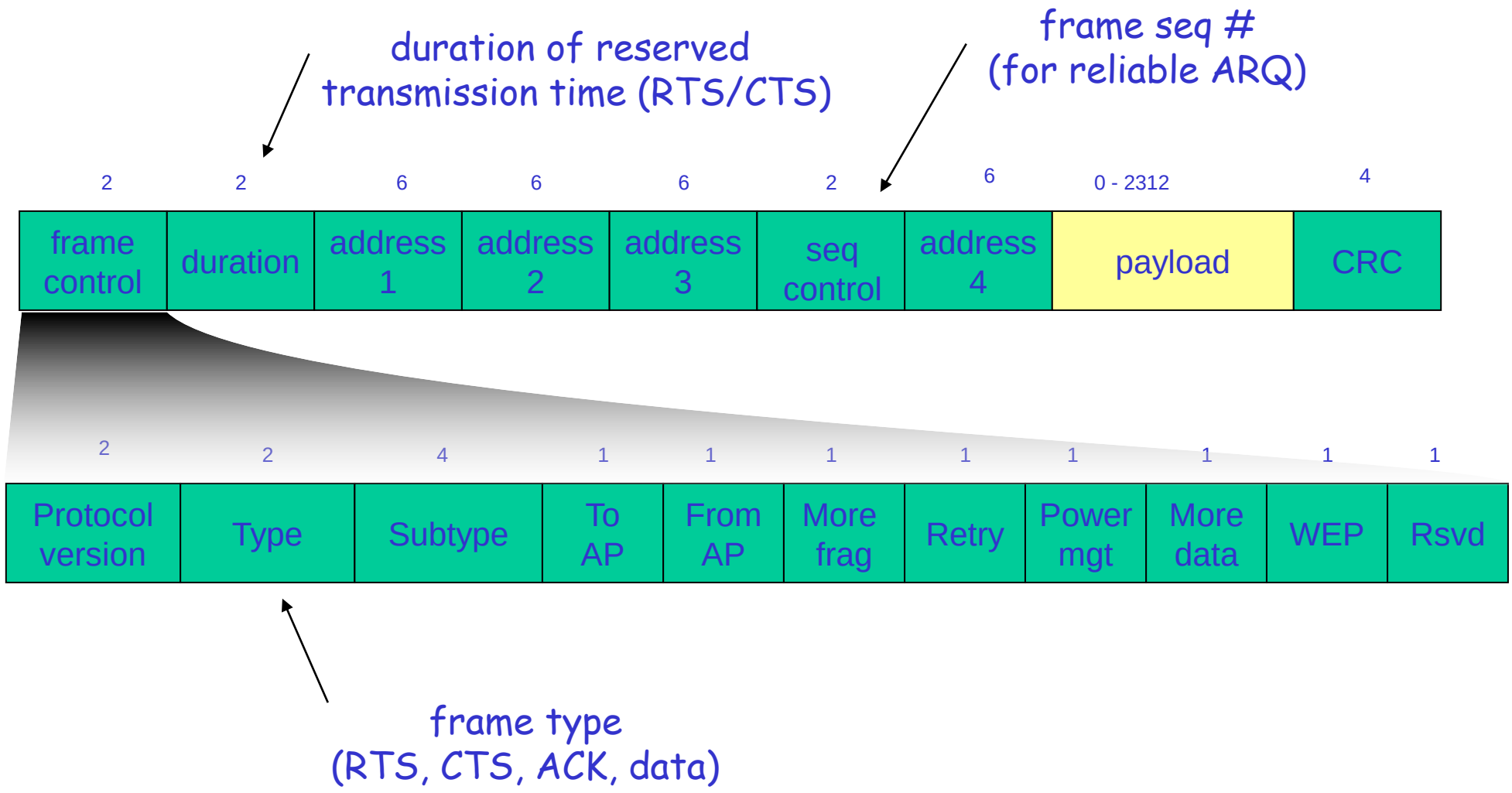
Address 3: MAC address of router interface to which AP is attached.
In case of Mobile-to-Mobile communication, MAC address of AP

Address 4: used when communication between mobiles of different APs

802.11 frame: addressing



802.11 frame: more



Address fields: 4 cases

From AP	To AP	Add 1	Add 2	Add 3	Add 4
0	0	Dst M	Src M	AP	0
1	0	Dst M	AP	Src R	0
0	1	AP	Src M	Dst R	0
1	1	Dst AP	Src AP	Dst M	Src M

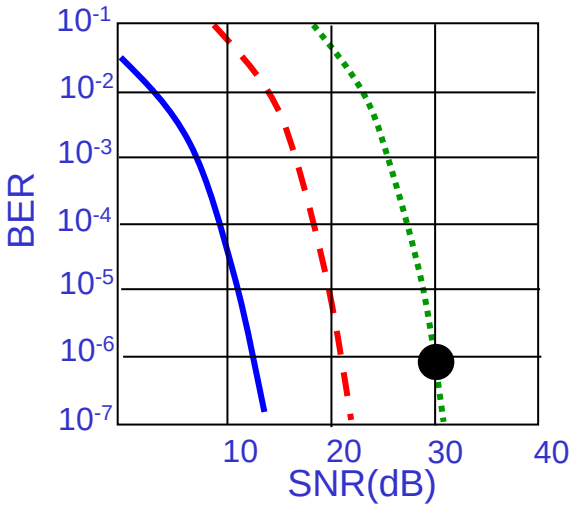
MAC of AP = BSSID

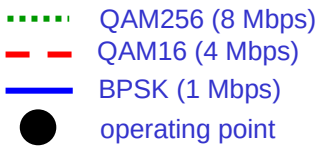
Fourth case is for packets transmitted between AP over the air

802.11: advanced capabilities

Rate Adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies





1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

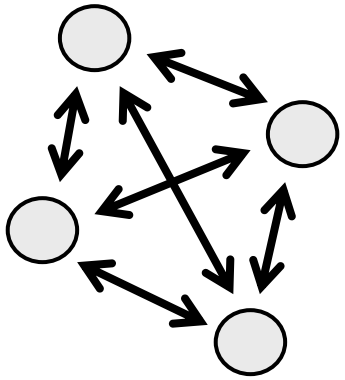
802.11 MAC fairness problem

- All station access the medium with same rate
  - As long as they see the same frame error rate
- Same throughput in frames / second
- What if frames are of different size?
  - Thrp 1 / Thrp 2 ~ FrameSize 1 / FrameSize2
- What if frames are of equal size but bit rates different?
  - Thrp 1 = Thrp 2 even if BitRate 1 ≠ BirRate 2
  - Too much fair …
  - And too little total link throughput
    - How much? Think about two competing stations at 11Mbps and 1Mbps
  - One desirable behavior Thrp 1 / Thrp 2 ~ BitRate 1 / BitRate 2
  - How to reach ? What about total throughput?

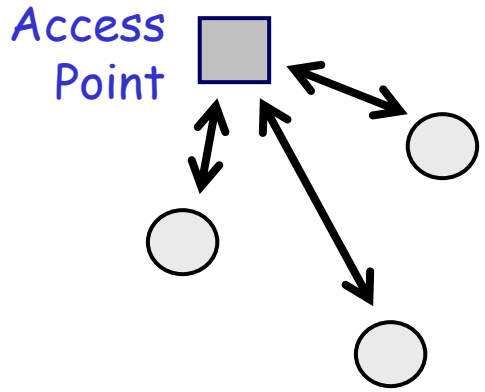
Routing in MANETs
Mobile Ad Hoc Networks

So far…

- Before MANETs: Nodes in a 802.11 basic service are directly connected to each other
- There is no need for routing and IP (layer 3) provides essentially no functionality



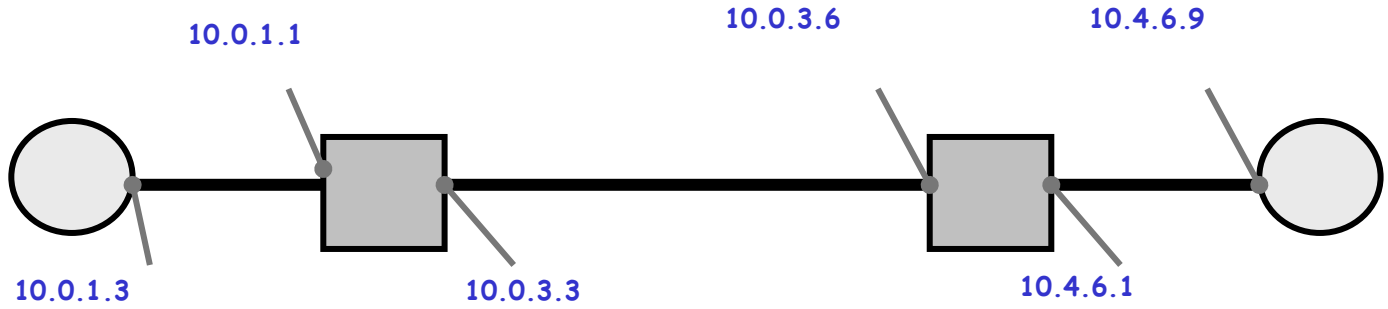
Ad Hoc Mode



Infrastructure Mode
AP can be the default IP gateway
or even a bridge at Layer 2
(passage by the bridge mandatory)

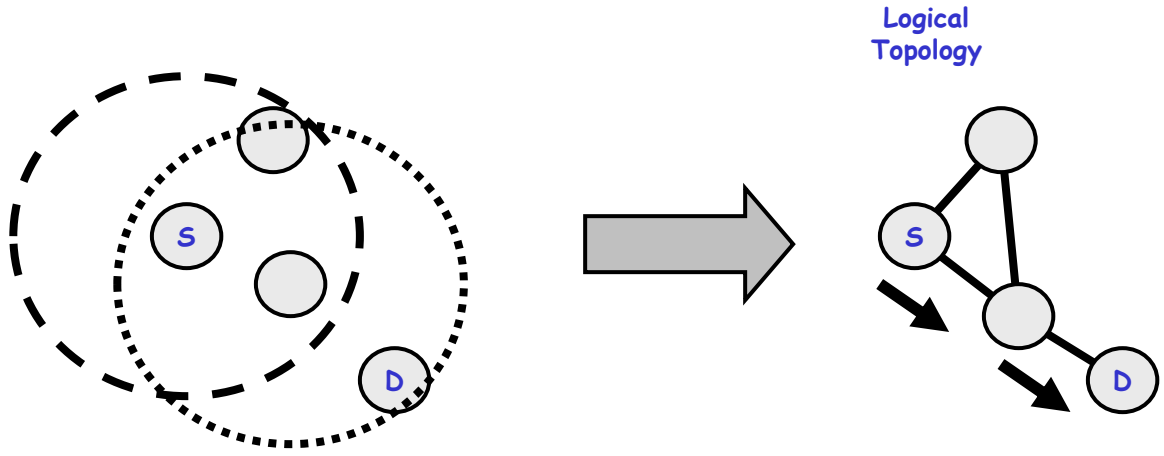
Need for Layer 3 Routing

- Of course, nodes may not be connected via Layer 2
  - Nodes that are in a different IP subnet, i.e., the destination IP network is different than the local IP network
  - Nodes that are out of radio range in an ad hoc wireless network
- Layer 3, or IP, routing is needed in this case



MANETs

- A mobile ad hoc network (MANET) is characterized by…
  - Multi-hop routing so that nodes not directly connected at Layer 2 can communicate through Layer 3 routing
  - A node is a laptop, a PDA, etc
  - Wireless links between wireless nodes
  - Mobile nodes serve as sources, destinations and ROUTERS (relays)



MANET vs. Traditional Routing

- Every node is potentially a router in a MANET, while most nodes in traditional wired networks do not route packets
  - Nodes transmit and receive their own packets and, also, forward packets for other nodes
- Topologies are dynamic in MANETs due to mobile nodes, but are relatively static in traditional networks
  - More frequent updates and more overhead.
- Both assume the existence of a path between two hosts otherwise there is no communication.
  - The end-to-end paradigm can still apply.
  - Path stability of the order of end-to-end delay.
  - Otherwise it is what we call a DTN or a PSN (next course).

MANET vs. Traditional Routing

- MANET topologies tend to have many more redundant links than traditional networks
  - And more interference
- A MANET "router" typically has a single interface, while a traditional router has an interface for each network to which it connects
- Power efficiency is an issue in MANETs, while it is normally not an issue in traditional networks
- MANETs may have gateways to fixed network, but are typically "stub networks," while traditional networks can be stub networks or transit networks

MANET Routing

- Nodes must determine how to forward packets
  - Source routing: Routing decision is made at the sender
  - Hop-by-hop routing: Routing decision is made at each intermediate node
- Difficult to achieve good performance
  - Routes change over time due to node mobility
  - Best to avoid long delays when first sending packets
  - Best to reduce overhead of route discovery and maintenance
  - Want to involve as many nodes as possible – to find better paths and reduce likelihood of partitions

Common Features

- MANET routing protocols must…
  - Discover a path from source to destination
  - Maintain that path (e.g., if an intermediate node moves and breaks the path)
  - Define mechanisms to exchange routing information
- Reactive protocols
  - Discover a path when a packet needs to be transmitted and no known path exists
  - Attempt to alter the path when a routing failure occurs
- Proactive protocols
  - Find paths, in advance, for all source-pair destinations
  - Periodically exchange routing information to maintain paths

IETF MANET Working Group

http://www.ietf.org/html.charters/manet-charter.html

"The purpose of this working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies. The fundamental design issues are that the wireless link interfaces have some unique routing interface characteristics and that node topologies within a wireless routing region may experience increased dynamics, due to motion or other factors."

IETF MANET Working Group

- Currently trying to move four proposed MANET routing protocols to Experimental RFC status
  - Optimized Link State Routing (OLSR) protocol
  - Ad Hoc On Demand Distance Vector (AODV) protocol
  - Dynamic Source Routing (DSR) protocol
    - Like AODV but source routing (no routing tables)
  - Topology Broadcast based on Reverse-Path Forwarding (TBRPF) protocol
    - Like OSPF but routing trees are exchanged instead of full topology
- URLs
  - http://www.ietf.org/html.charters/manet-charter.html
  - http://protean.itd.nrl.navy.mil/manet/manet_home.html

OLSR

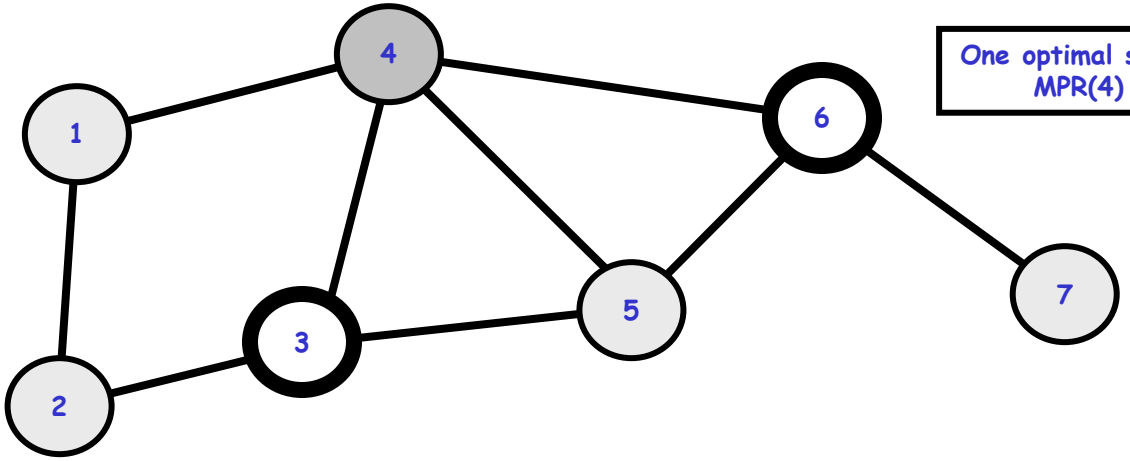
- Optimized Link State Routing (OLSR) protocol
  - IETF Experimental RFC number 3626
  - Developed by the Hipercom group at INRIA Rocquencourt
- Proactive (table-driven) routing protocol
  - A route is available immediately when needed
- Based on the link-state algorithm
  - Nodes advertise information only about links with neighbors who are in its multipoint relay selector set
  - Reduces size of control packets
- Reduces flooding by using only multipoint relay nodes to send information in the network
  - Reduces number of control packets by reducing duplicate transmissions

OLSR (2)

- Does not require reliable transfer, since updates are sent periodically
- Does not need in-order delivery, since sequence numbers are used to prevent out-of-date information from being misinterpreted
- Uses hop-by-hop routing
  - Routes are based on dynamic table entries maintained at intermediate nodes

Multipoint Relays

- Each node *N* in the network selects a set of neighbor nodes as multipoint relays, *MPR*(*N*), that retransmit control packets from *N*
  - Neighbors not in *MPR*(*N*) process control packets from *N*, but they do not forward the packets
- *MPR*(*N*) is selected such that all two-hop neighbors of *N* are covered by (one-hop neighbors) of *MPR*(*N*)

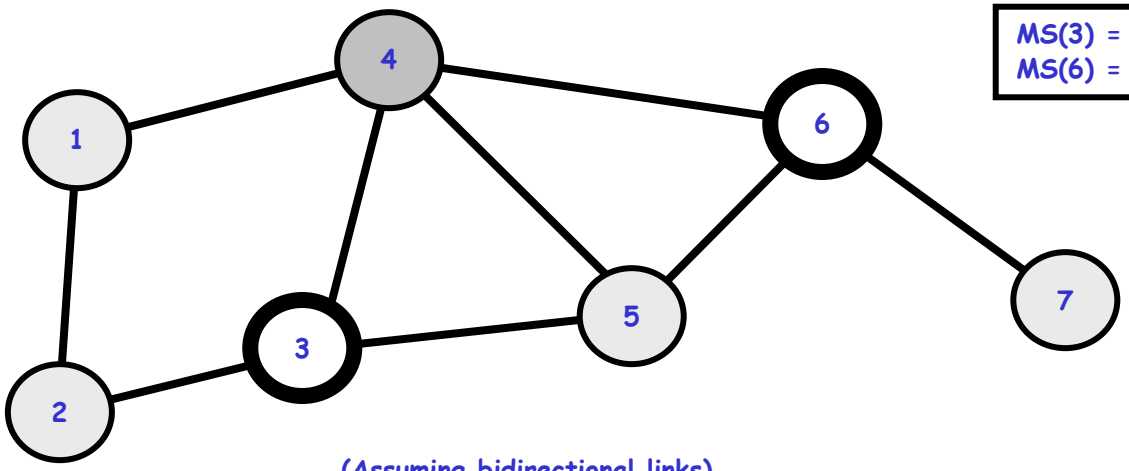


One optimal set for Node 4:
MPR(4) = { 3, 6 }

Is there another optimal MPR(4)?

Multipoint Relay Selector Set

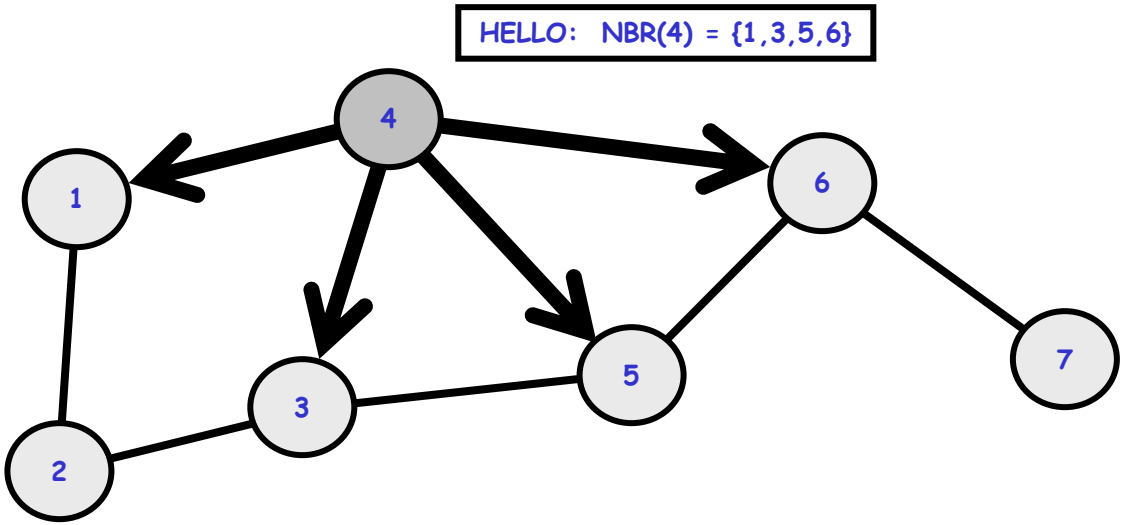
- The multipoint relay selector set for Node *N*, *MS*(*N*), is the set of nodes that choose Node *N* in their multipoint relay set
  - Only links *N*-*M*, for all *M* such that $N \in MS(M)$ will be advertised in control messages
  - Globally advertise links to neighbors that send you updates



(Assuming bidirectional links)

HELLO Messages (1)

- Each node uses HELLO messages to determine its MPR set
- All nodes periodically broadcast HELLO messages to their one-hop neighbors (bidirectional links)
- HELLO messages are not forwarded

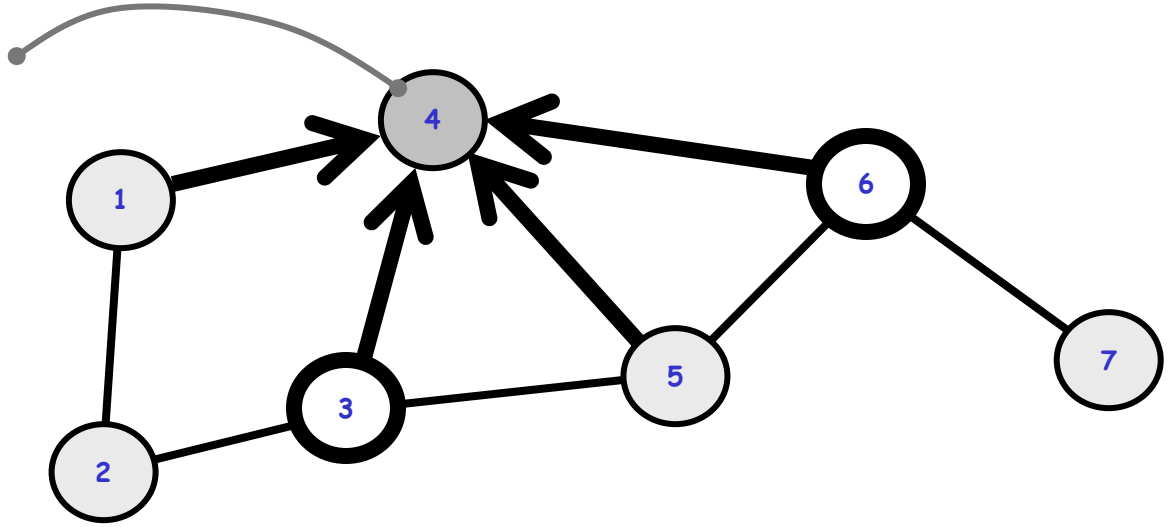


HELLO Messages (2)

- Using the neighbor list in received HELLO messages, nodes can determine their two-hop neighborhood and an optimal (or near-optimal) MPR set
- A sequence number is associated with this MPR set
  - Sequence number is incremented each time a new set is calculated

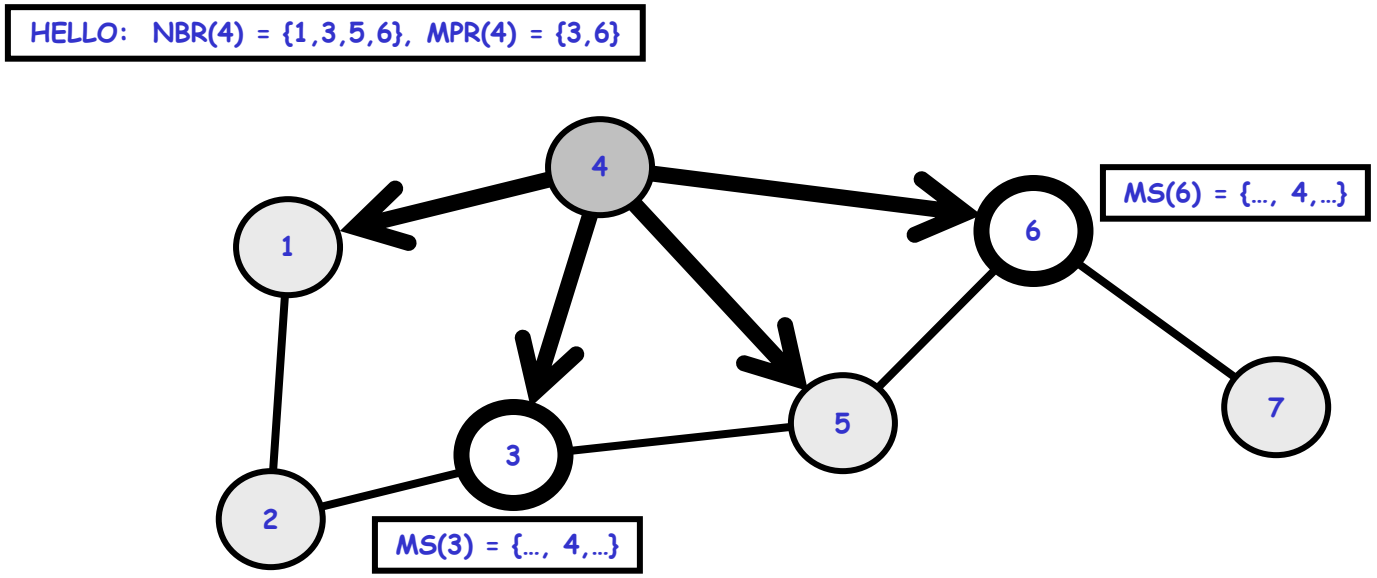
At Node 4:
NBR(1) = {2}
NBR(3) = {2,5}
NBR(5) = {3,6}
NBR(6) = {5,7}

MPR(4) = {3,6}



HELLO Messages (3)

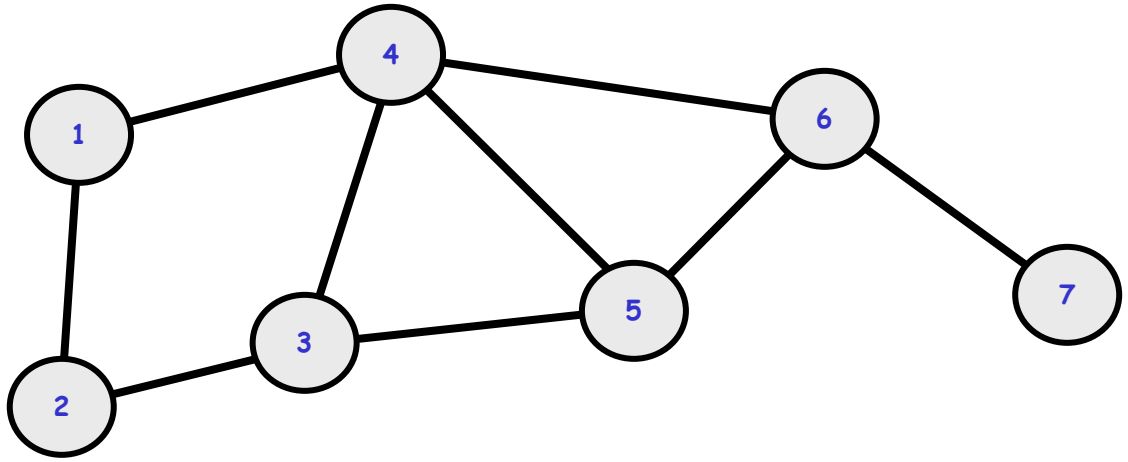
- Subsequent HELLO messages also indicate neighbors that are in the node's MPR set
- MPR set is recalculated when a change in the one-hop or two-hop neighborhood is detected



TC Messages

- Nodes send topology information in Topology Control (TC) messages
  - List of advertised neighbors (link information)
  - Sequence number (to prevent use of stale information)
- A node generates TC messages only for those neighbors in its MS set
  - Only MPR nodes generate TC messages
  - Not all links are advertised
- A nodes processes all received TC messages, but only forwards TC messages if the sender is in its MS set
  - Only MPR nodes propagate TC messages

OLSR Example (1)

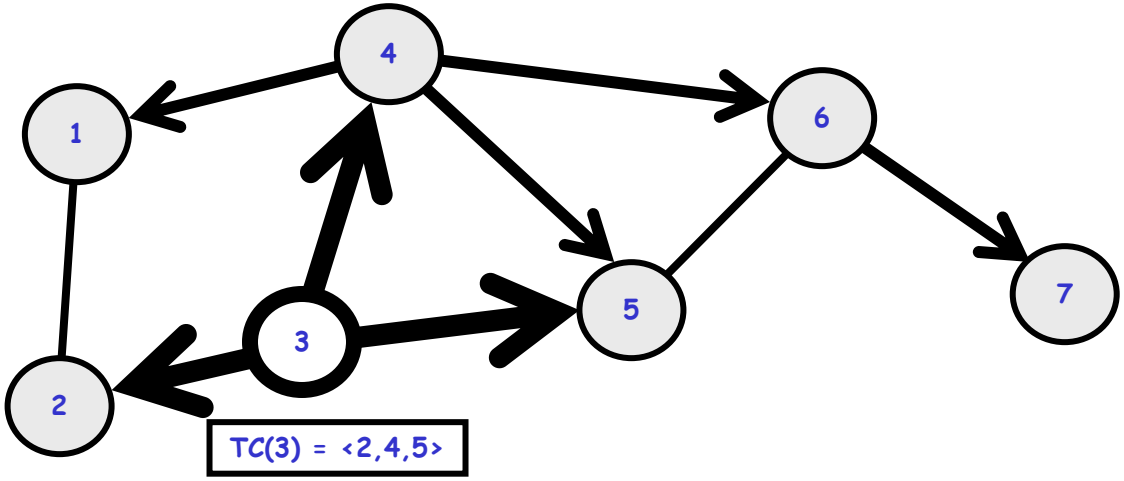


MPR(1) = { 4 }
MPR(2) = { 3 }
MPR(3) = { 4 }
MPR(4) = { 3, 6 }
MPR(5) = { 3, 4, 6 }
MPR(6) = { 4 }
MPR(7) = { 6 }

MS(1) = { }
MS(2) = { }
MS(3) = { 2, 4, 5 }
MS(4) = { 1, 3, 5, 6 }
MS(5) = { }
MS(6) = { 4, 5, 7 }
MS(7) = { }

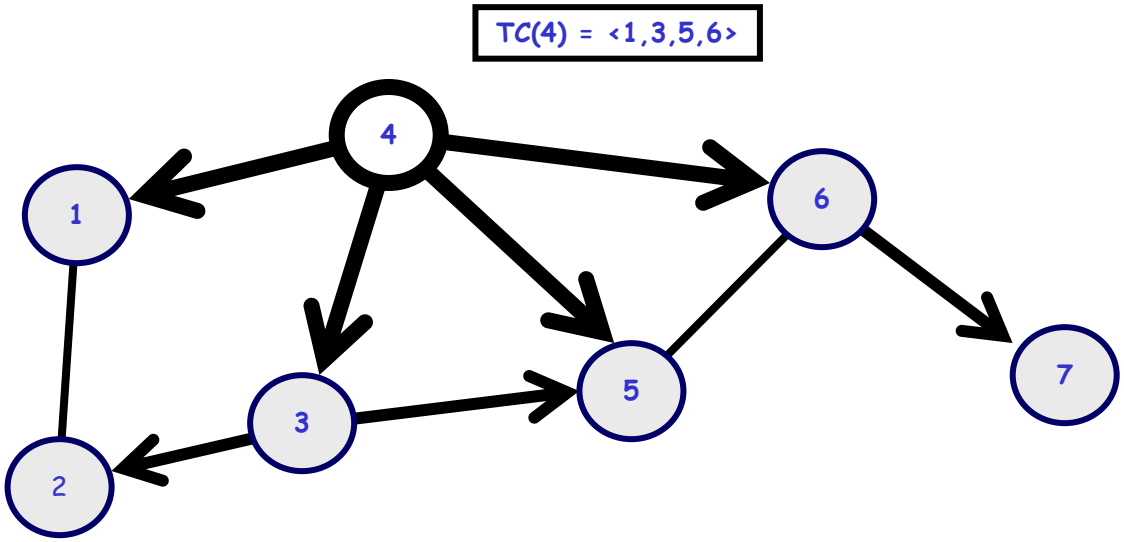
- Only nodes 3, 4, 6 are MPR and so they generate TC msgs

OLSR Example (2)



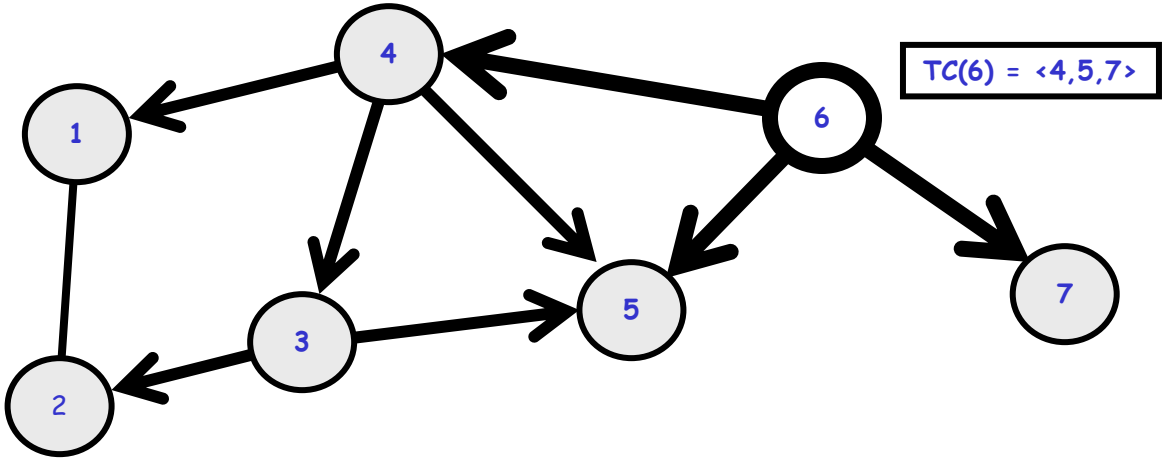
- Node 3 generates a TC message advertising nodes in MS(3) = {2, 4, 5}
- Node 4 forwards Node 3's TC message since Node 3 ∈ MS(4) = {1, 3, 5, 6}
- Node 6 forwards TC(3) since Node 4 ∈ MS(6)

OLSR Example (3)



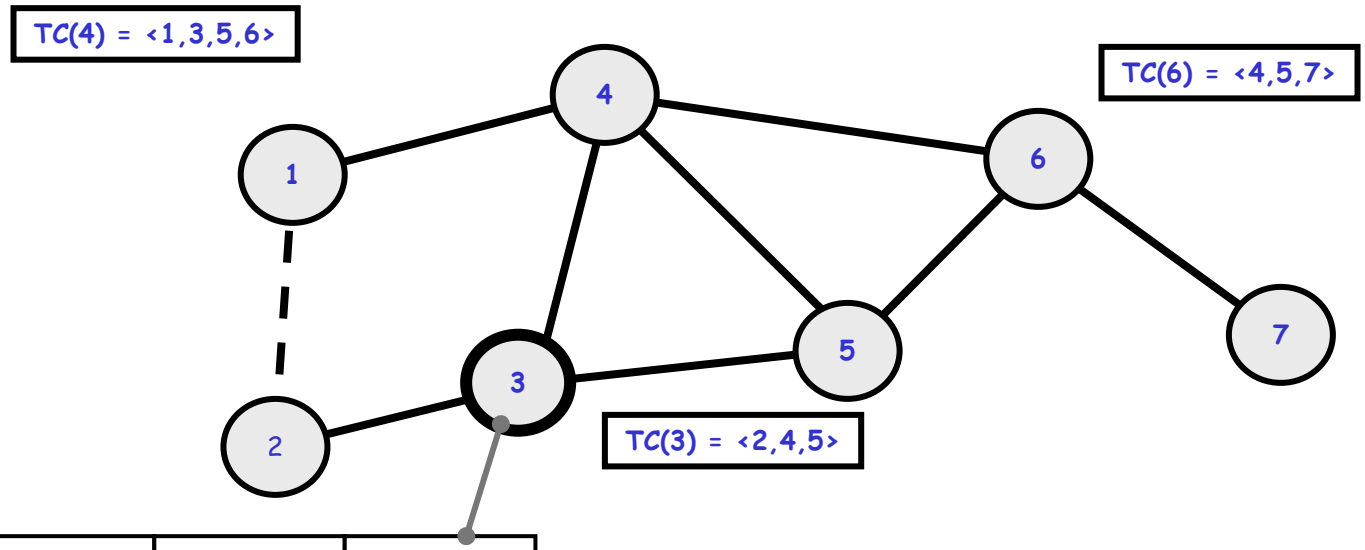
- Node 4 generates a TC message advertising nodes in MS(4) = {1, 3, 5, 6}
- Nodes 3 and 6 forward TC(4) since Node 4 $\in$ MS(3) and Node 4 $\in$ MS(6)

OLSR Example (4)



- Node 6 generates a TC message advertising nodes in MS(6) = {4, 5, 7}
- Node 4 forwards TC(6) from Node 6 and Node 3 forwards TC(6) from Node 4
- After Nodes 3, 4, and 6 have generated TC messages, all nodes have link-state information to route to any node

OLSR Example (5)



Dest	Next	Hops
1	4	2
2	2	1
4	4	1
5	5	1
6	4 (5)	2
7	4 (5)	3

- Given TC information, each node forms a topology table
- A routing table is calculated from the topology table
- Note that Link 1-2 is not visible except to Nodes 2 and 1.

AODV

- AODV: Ad hoc On-demand Distance Vector routing protocol
  - ITEF Experimental RFC number 3561
- Pure on-demand routing protocol
  - A node does not perform route discovery or maintenance until it needs a route to another node or it offers its services as an intermediate node
  - Nodes that are not on active paths do not maintain routing information and do not participate in routing table exchanges
- Uses a broadcast route discovery mechanism
- Uses hop-by-hop routing
  - Routes are based on dynamic table entries maintained at intermediate nodes
  - Similar to Dynamic Source Routing (DSR), but DSR uses source routing

AODV (2)

- Local HELLO messages are used to determine local connectivity
  - Can reduce response time to routing requests
  - Can trigger updates when necessary
- Sequence numbers are assigned to routes and routing table entries
  - Used to supersede stale cached routing entries
- Every node maintains two counters
  - Node sequence number
  - Broadcast ID

AODV Route Request (1)

- Initiated when a node wants to communicate with another node, but does not have a route to that node
- Source node broadcasts a route request (RREQ) packet to its neighbors

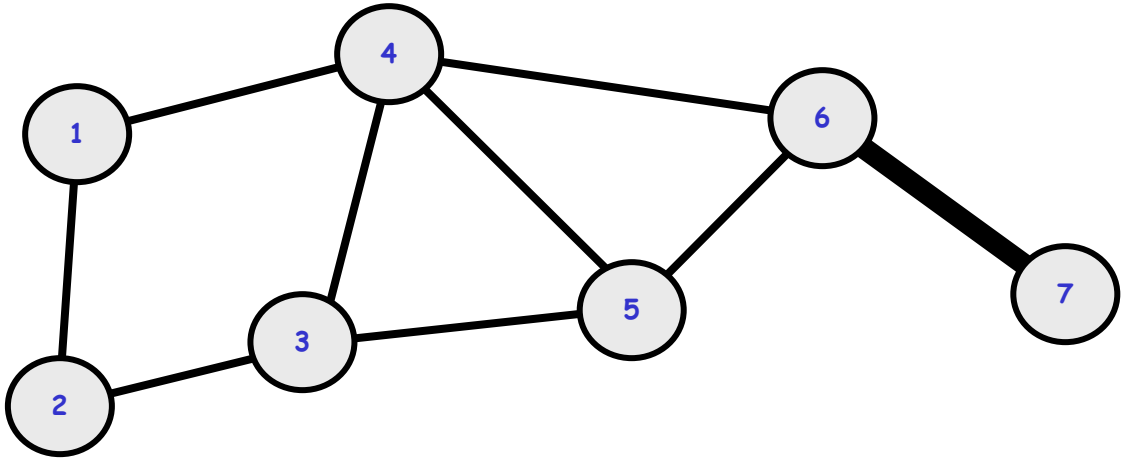
AODV Route Request (2)

- Sequence numbers
  - Source sequence indicates "freshness" of reverse route to the source
  - Destination sequence number indicates freshness of route to the destination
- Every neighbor receives the RREQ and either …
  - Returns a route reply (RREP) packet, or
  - Forwards the RREQ to its neighbors
- (source_addr, broadcast_id) uniquely identifies the RREQ
  - broadcast_id is incremented for every RREQ packet sent
  - Receivers can identify and discard duplicate RREQ packets

AODV Route Request (3)

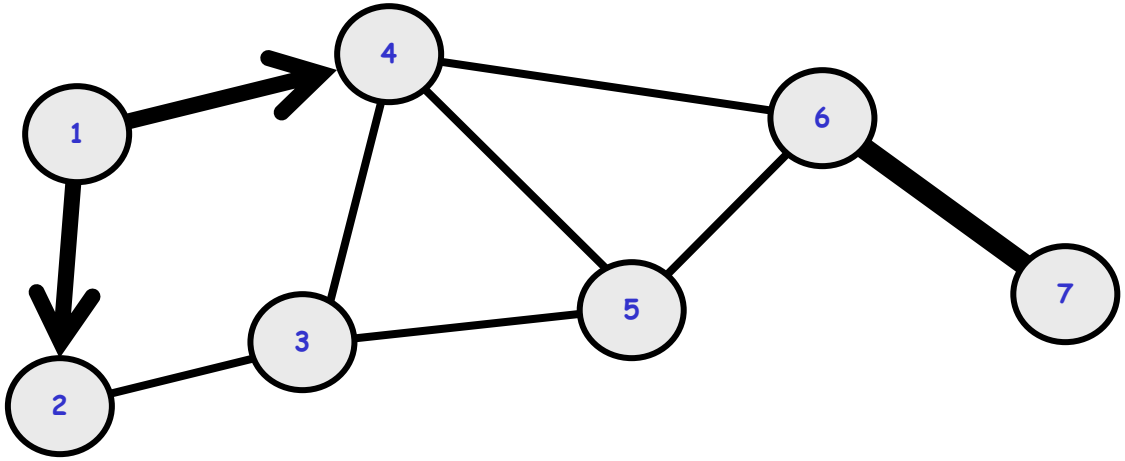
- If a node *cannot* respond to the RREQ
  - The node increments the hop count
  - The node saves information to implement a reverse path set up (AODV assumes symmetrical links)
    - Neighbor that sent this RREQ packet
    - Destination IP address
    - Source IP address
    - Broadcast ID
    - Source node's sequence number
    - Expiration time for reverse path entry (to enable garbage collection)

AODV Example (1)



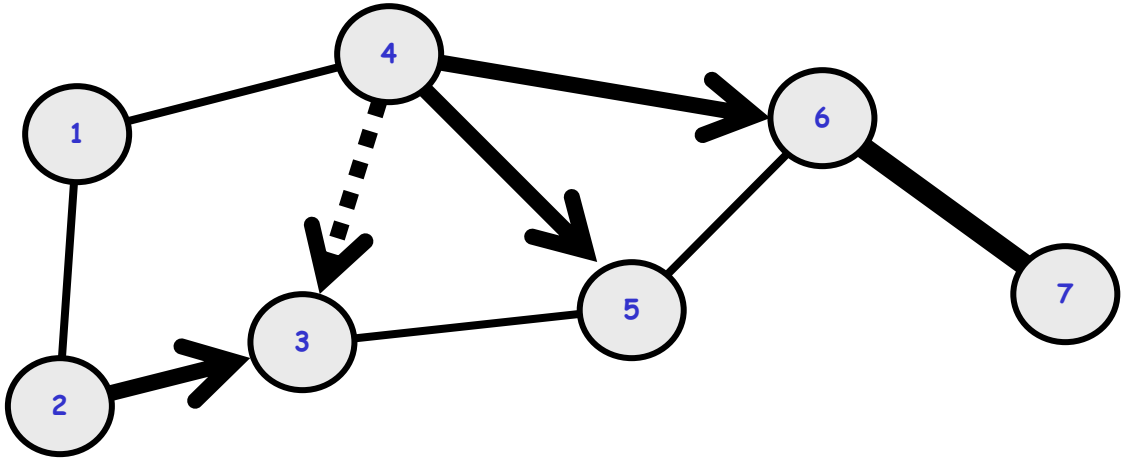
- Node 1 needs to send a data packet to Node 7
- Assume Node 6 knows a current route to Node 7
- Assume that no other route information exists in the network (related to Node 7)

AODV Example (2)



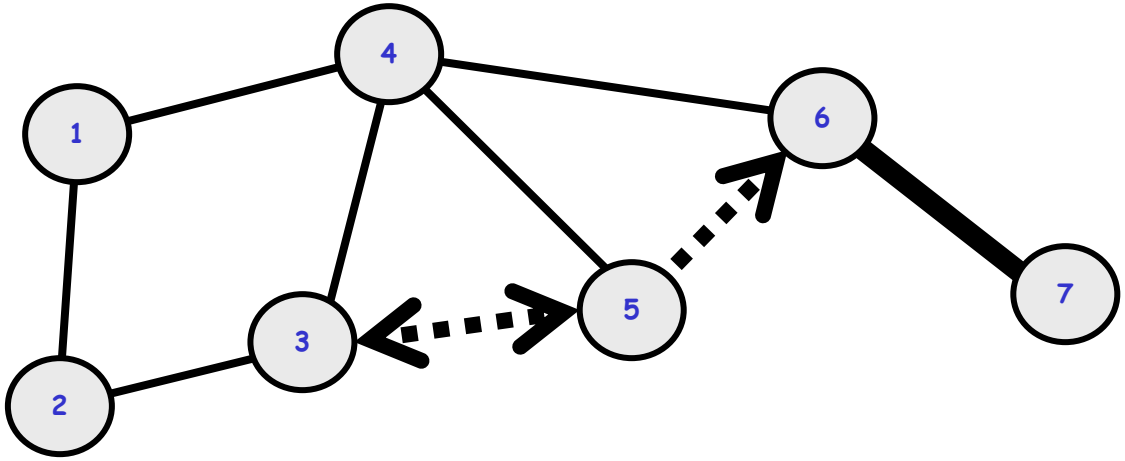
- Node 1 sends a RREQ packet to its neighbors
  - source_addr = 1
  - dest_addr = 7
  - broadcast_id = broadcast_id + 1
  - source_sequence_# = source_sequence_# + 1
  - dest_sequence_# = last dest_sequence_# for Node 7

AODV Example (3)



- Nodes 2 and 4 verify that this is a new RREQ and that the source_sequence_# is not stale with respect to the reverse route to Node 1
- Nodes 2 and 4 forward the RREQ
  - Update source_sequence_# for Node 1
  - Increment hop_cnt in the RREQ packet

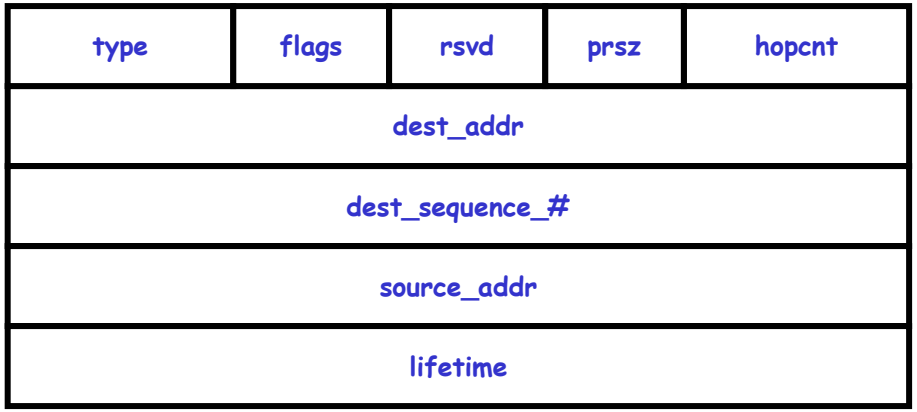
AODV Example (4)



- RREQ reaches Node 6, which knows a route to 7
  - Node 6 must verify that the destination sequence number is less than or equal to the destination sequence number it has recorded for Node 7 (otherwise link to 7 has changed and is to be checked)
- Nodes 3 and 5 will forward the RREQ packet, but the receivers recognize the packets as duplicates

AODV Route Reply (1)

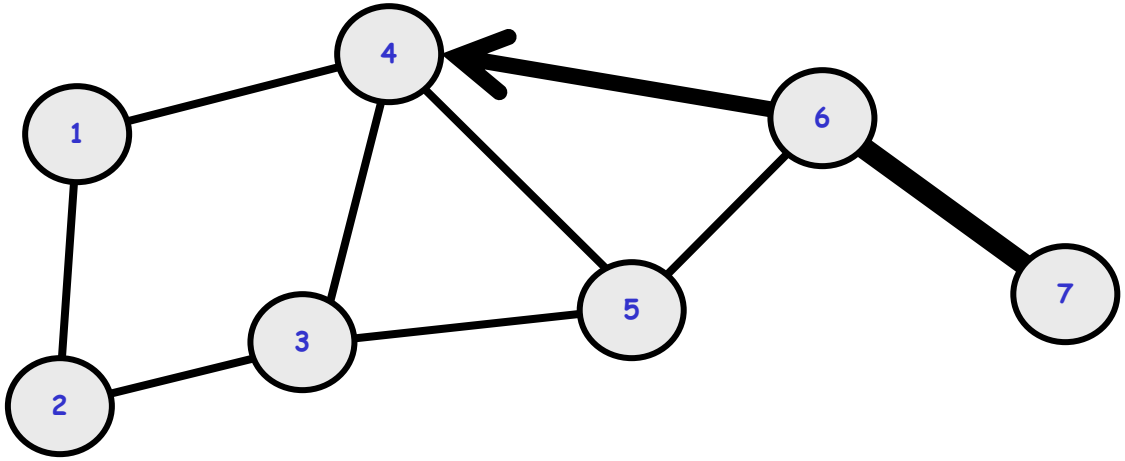
- If a node receives an RREQ packet and it has a current route to the target destination, then it unicasts a route reply packet (RREP) to the neighbor that sent the RREQ packet



AODV Route Reply (2)

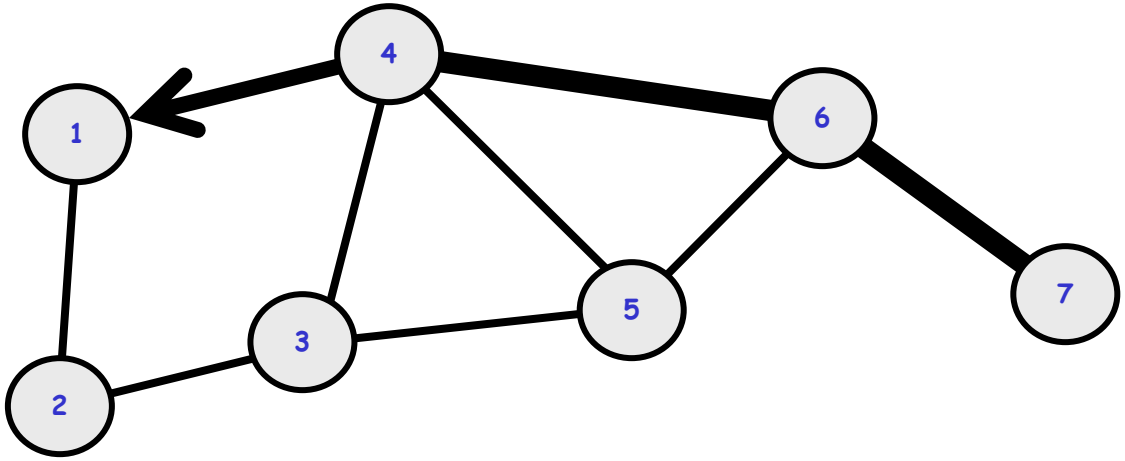
- Intermediate nodes propagate the first RREP for the source towards the source using cached reverse route entries
- Other RREP packets are discarded unless…
  - dest_sequence_# number is higher than the previous, or
  - destination_sequence_# is the same, but hop_cnt is smaller (i.e., there's a better path)
- RREP eventually makes it to the source, which can use the neighbor sending the RREP as its next hop for sending to the destination
- Cached reverse routes will timeout in nodes not seeing a RREP packet

AODV Example (5)



- Node 6 knows a route to Node 7 and sends an RREP to Node 4
  - source_addr = 1
  - dest_addr = 7
  - dest_sequence_# = maximum(own sequence number, dest_sequence_# in RREQ)
  - hop_cnt = 1

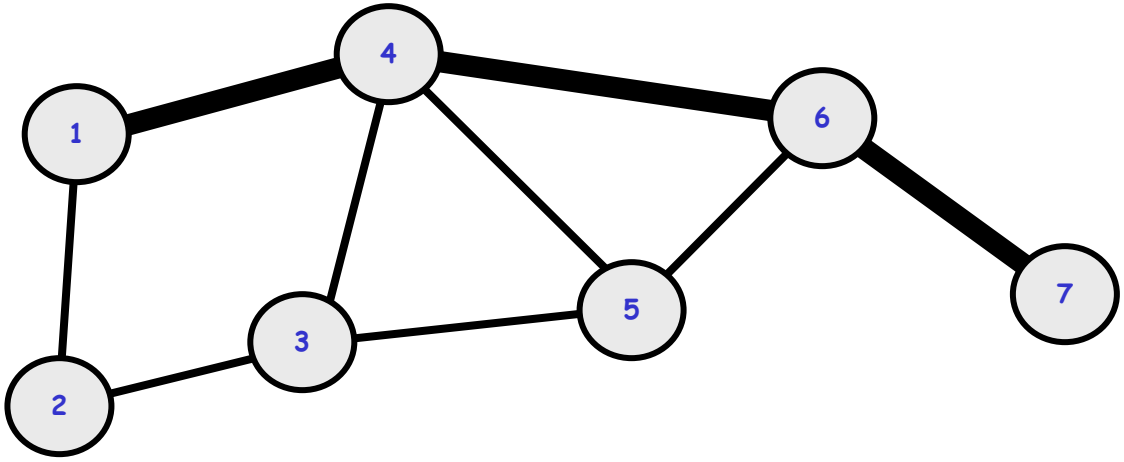
AODV Example (6)



- Node 4 verifies that this is a new route reply (the case here) or one that has a lower hop count and, if so, propagates the RREP packet to Node 1
  - Increments hop_cnt in the RREP packet

AODV Example (7)

Dest	Next	Hops
7	4	3

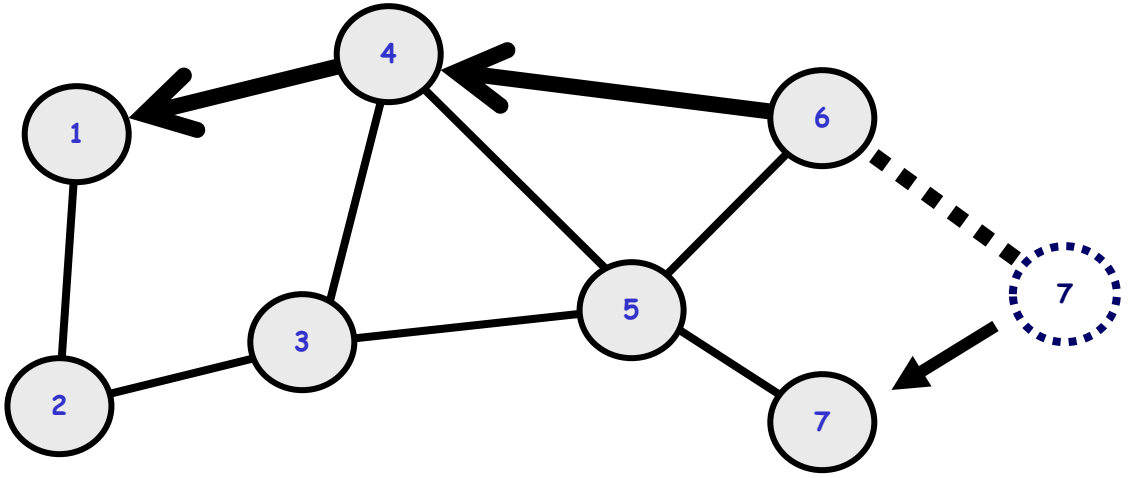


- Node 1 now has a route to Node 7 in three hops and can use it immediately to send data packets
- Note that the first data packet that prompted path discovery has been delayed until the first RREP was returned

AODV Route Maintenance

- Route changes can be detected by…
  - Failure of periodic HELLO packets
  - Failure or disconnect indication from the link level
  - Failure of transmission of a packet to the next hop (can detect by listening for the retransmission if it is not the final destination)
- The upstream (toward the source) node detecting a failure propagates a route error (RERR) packet with a new destination sequence number and a hop count of infinity (unreachable)
- The source (or another node on the path) can rebuild a path by sending a RREQ packet

AODV Example (8)



- Assume that Node 7 moves and link 6-7 breaks
- Node 6 issues an RERR packet indicating the broken path
- The RERR propagates back to Node 1
- Node 1 can discover a new route

Conclusions and open issues

- Layer 3 routing is needed to extend wireless mobile networks beyond local area networks of directly connected nodes
- Mobile ad hoc networks use multi-hop routing to enable communications in dynamic topologies
- MANET routing is hard to do well – it experiences the problems of both wireless and mobility
- A number of reactive and proactive MANET routing protocols have been proposed
- MANETs are still a niche application and they are relatively immature

Conclusions and open issues

- Among the hot issues in MANETs:
  - Power control
    - Your power decides one how much you interfere with others
    - and how far you can send packets
  - Portioning
    - Very likely
    - Ad-hoc routing suppose the existing of a route
    - But what if the route is not there ? Change the end-to-end principle ?
  - Load Balancing
    - Harder than in wired Internet because of Interference
  - Some people still convinced that routing should be done at layer 2. MANETs become a LAN in this case.
  - Performance of upper layer protocols as TCP, P2P, etc
    - Locality in P2P? Look at BitHoc@Inria. Large TCP window size? How much?

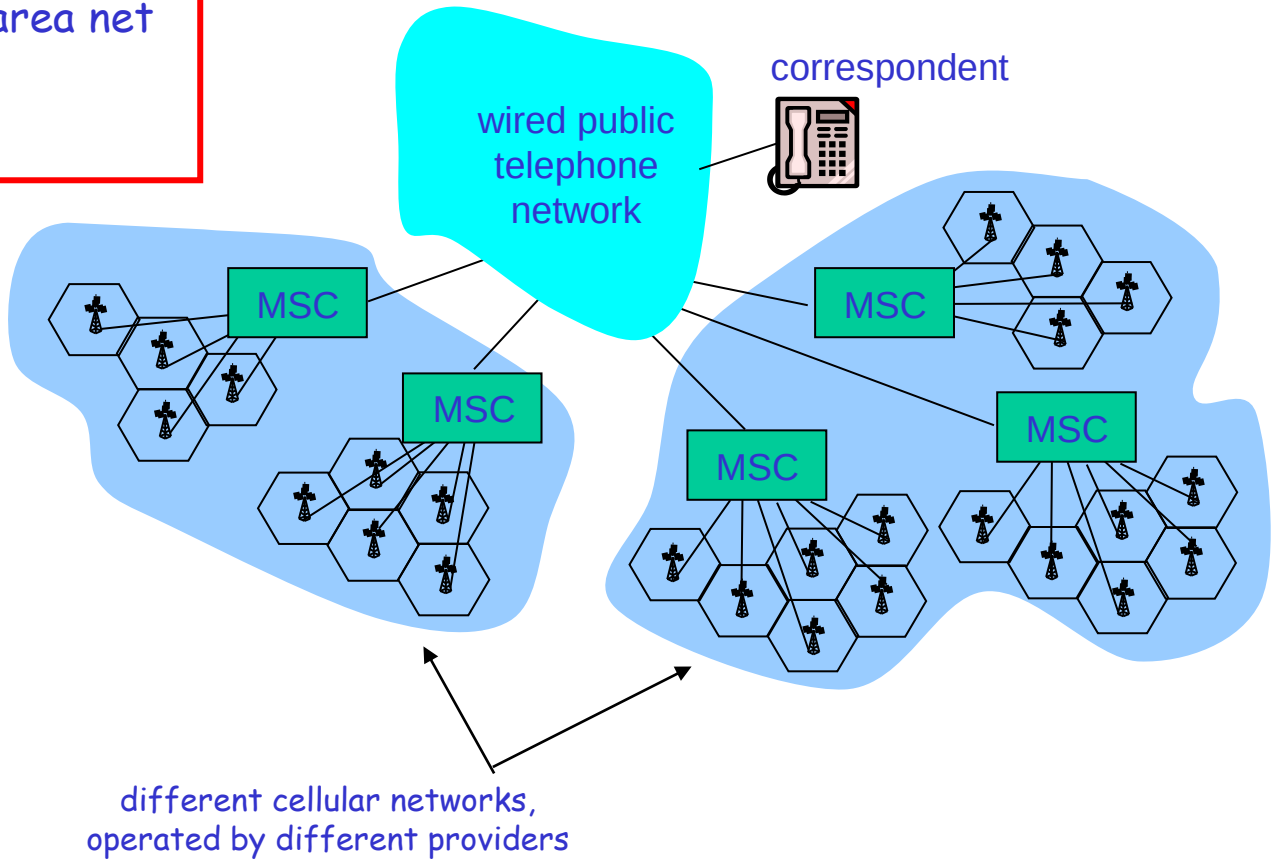
Additional slides

- For further information and details
- Not included in the course

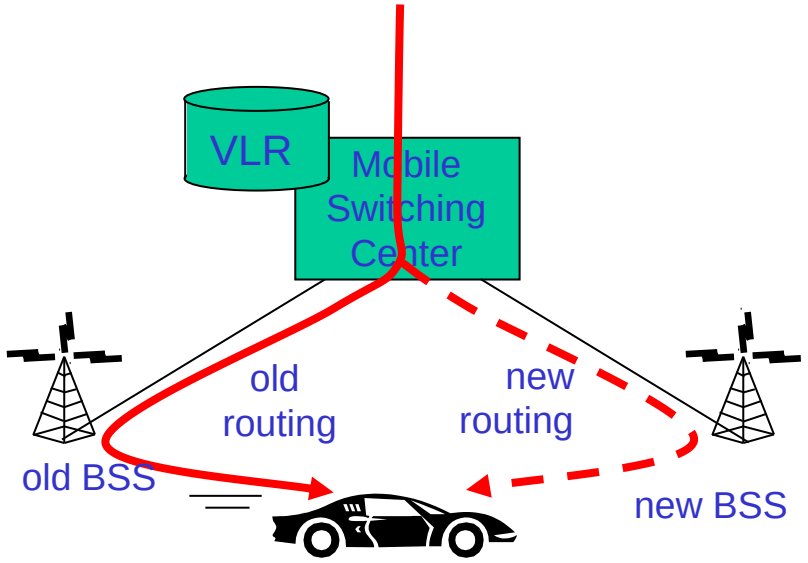
Mobility in cellular networks: Transparent to IP

Mobile Switching Center

- connects cells to wide area net
- manages call setup
- handles mobility

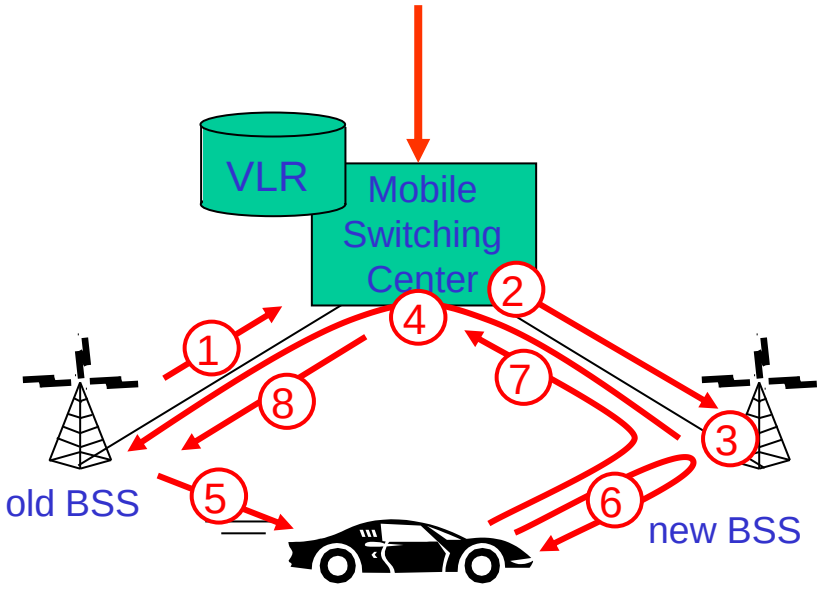


Handoff with common MSC (micro-mobility)



- 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)

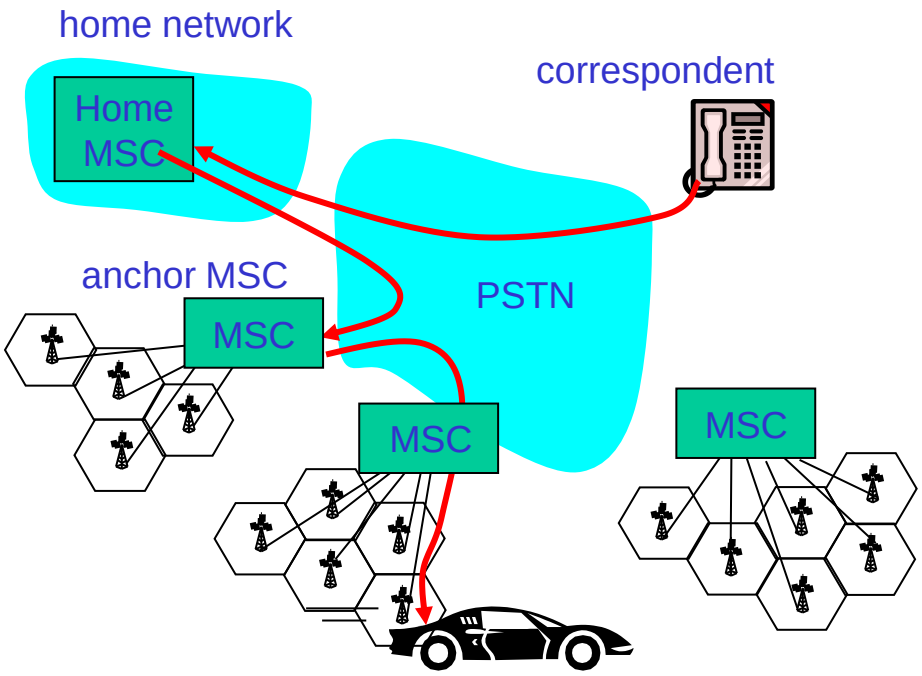
GSM: handoff with common MSC



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

GSM: handoff between MSCs

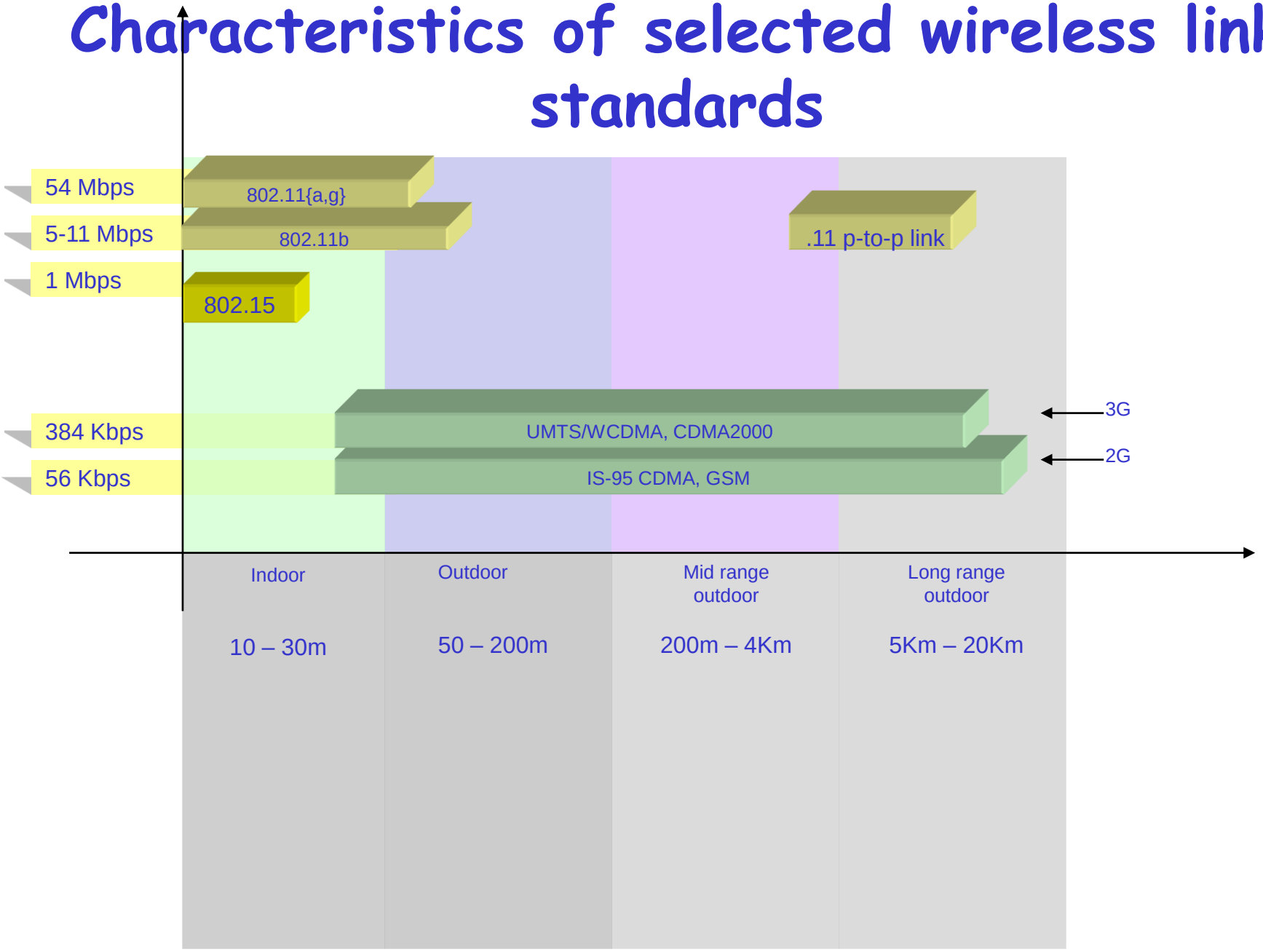


- *anchor MSC:* first MSC visited during cal
  - call remains routed through anchor MSC
  - This avoids establishing a new call.
- new MSCs add on to end of MSC chain as mobile moves to new MSC
- Correspondent pays to home network
- Mobile pays the rest (the two communications)

SCTP : Stream Control Transport Protocol

- A kind of combination of both TCP and UDP
  - UDP not reliable but it is message oriented.
  - TCP is reliable, offers congestion control, but it is byte oriented.
- STCP is a kind of TCP with the message oriented feature of UDP
- Plus the notion of multiple streams inside the same connection
  - A stream can be for example an HTTP object.
  - Or a connection over some specific interface.
  - A stream does not wait for the retransmission of a packet from other streams
- Originally proposed to carry audio signaling protocols that require reliability, the notion of streams and a message-oriented service.
- Reliability in SCTP can be controlled.

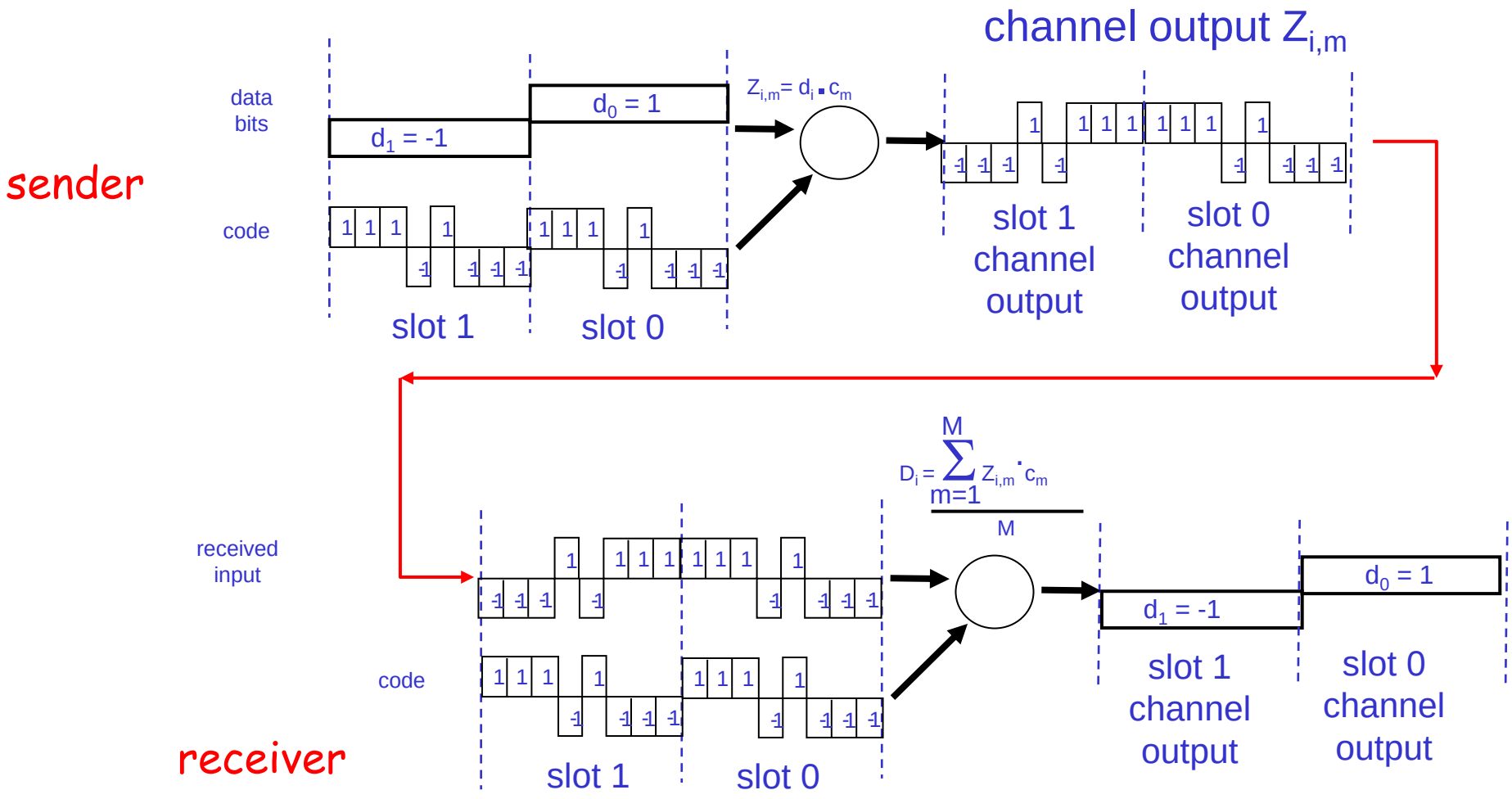
Characteristics of selected wireless link standards



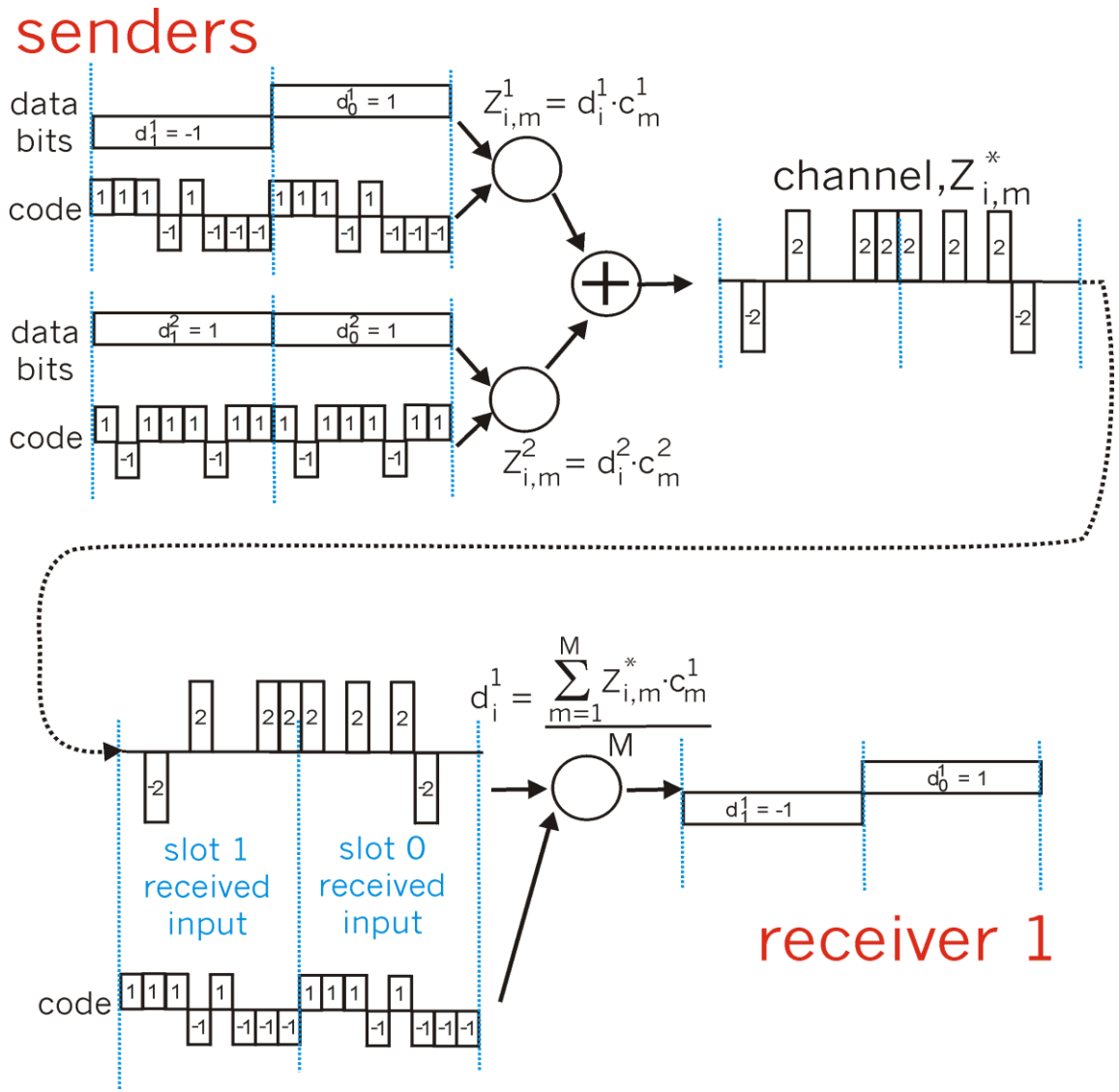
Code Division Multiple Access (CDMA)

- used in several wireless broadcast channels (cellular, satellite, etc) standards
- 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
- *encoded signal* = (original data) X (chipping sequence)
- *decoding:* inner-product of encoded signal and chipping sequence
- allows multiple users to "coexist" and transmit simultaneously with minimal interference (if codes are "orthogonal")

CDMA Encode/Decode

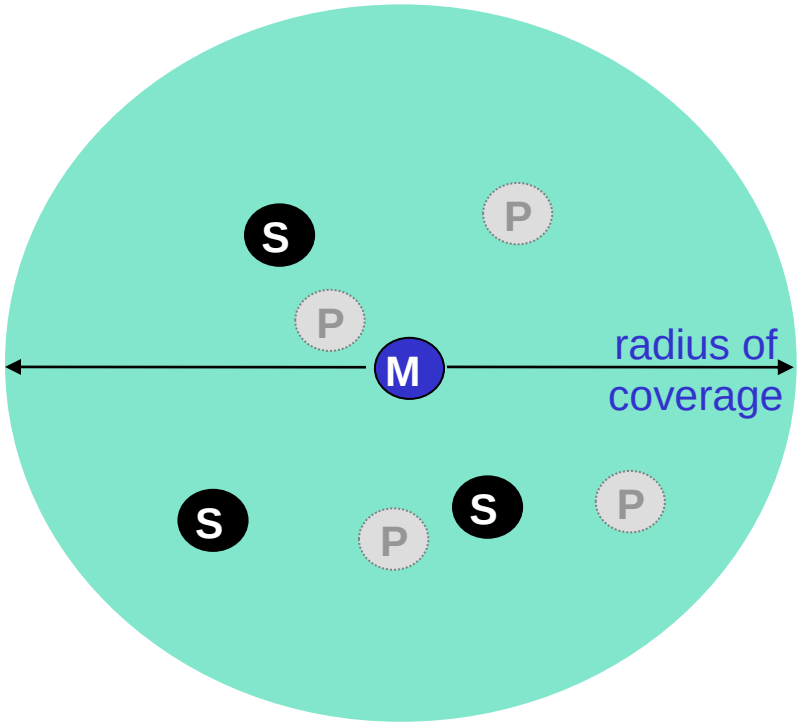


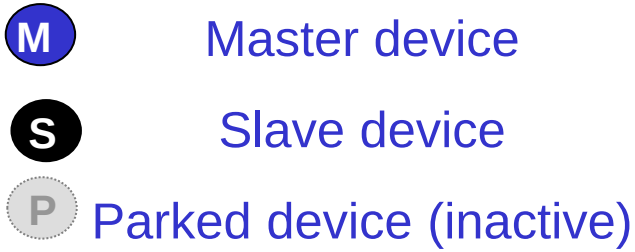
CDMA: two-sender interference



802.15: personal area network

- less than 10 m diameter
- replacement for cables (mouse, keyboard, headphones)
- ad hoc: no infrastructure
- master/slaves:
  - slaves request permission to send (to master)
  - master grants requests
- 802.15: evolved from Bluetooth specification
  - 2.4-2.5 GHz radio band
  - up to 721 kbps

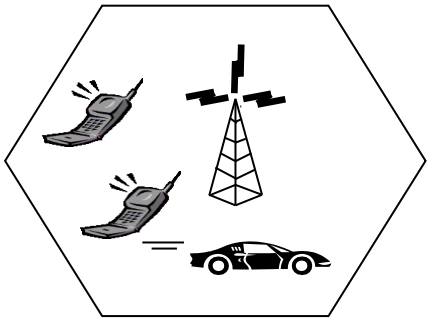


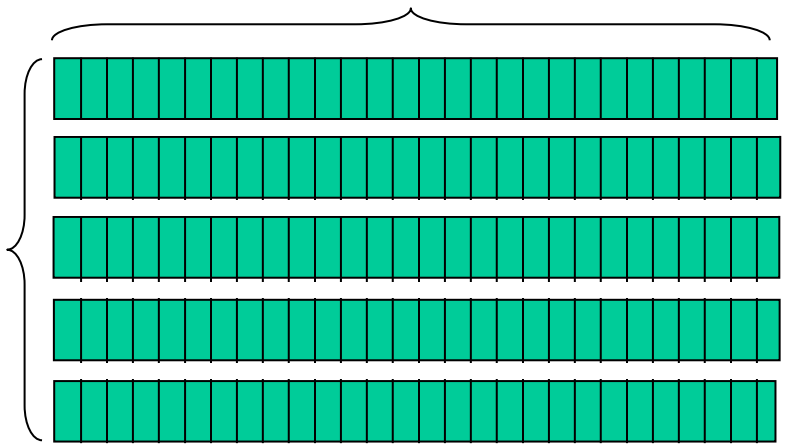


Cellular networks: the first hop

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

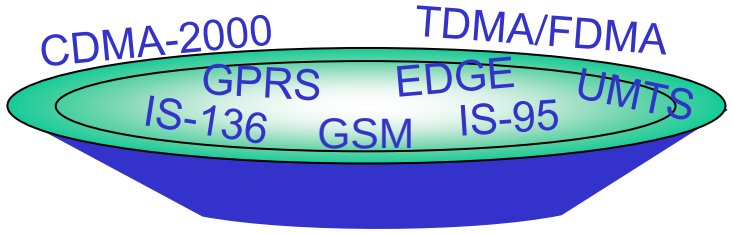




Cellular standards: brief survey

2G systems: voice channels

- IS-136 TDMA: combined FDMA/TDMA (north america)
- GSM (global system for mobile communications): combined FDMA/TDMA
  - most widely deployed
- IS-95 CDMA: code division multiple access



Don't drown in a bowl of alphabet soup: use this for reference only

Cellular standards: brief survey

2.5 G systems: voice and data channels

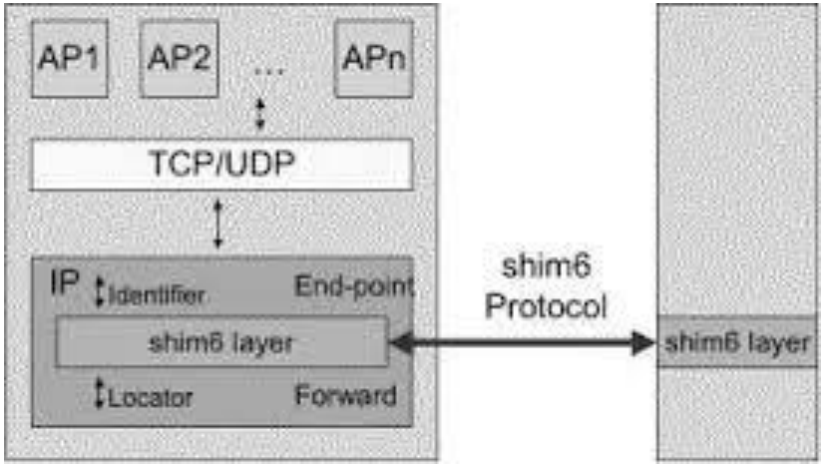
- for those who can't wait for 3G service: 2G extensions
- general packet radio service (GPRS)
  - evolved from GSM
  - data sent on multiple channels (if available)
- enhanced data rates for global evolution (EDGE)
  - also evolved from GSM, using enhanced modulation
  - Date rates up to 384K

3G systems: voice/data

- Universal Mobile Telecommunications Service (UMTS)
  - GSM next step, but using CDMA
- CDMA-2000

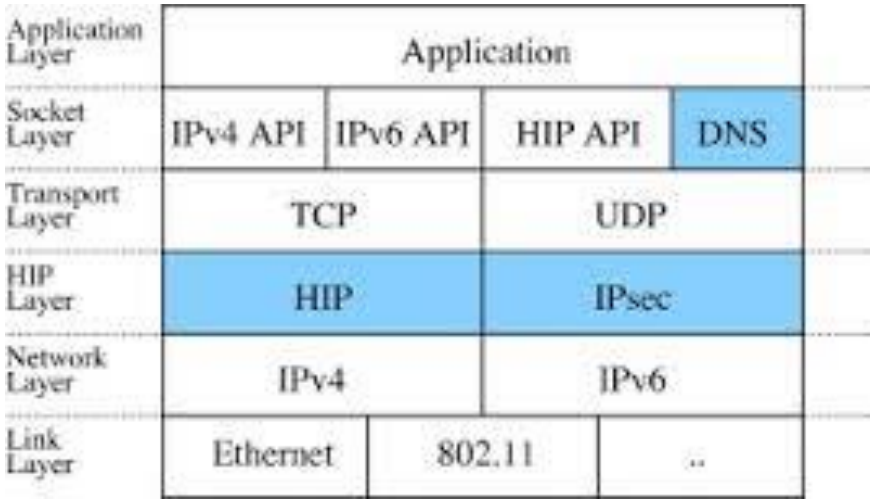
Shim6 (for IPv6)

- Shim6: Site Multihoming by IPv6 Intermediation
  - Specific to IPv6
  - A layer 3.5 solution (between 3 and 4)
  - One IP address is chosen as ID of the machine
  - Other IP addresses are chosen as locators
  - Sockets built with the ID of the machine
  - Packets leave the machine with the address of the interface
    - IP address rewriting
  - Shim6 maintains an updated list of locators for the peer machine



HIP

- HIP: Host Identity Protocol
  - A Layer 3.5 solution (between 3 and 4)
  - IP addresses are no longer identifiers
    - A public key can be for example an identifier
    - Or the canonial name of the machine
  - HIP maps identifiers to locators as in shim6
  - Requires redefining sockets to accomodate new identifiers at transport and application layer
    - Hence rewriting applications
    - DNS can be used to find locators



Hierarchical Algorithms (1)

- Scalability – MANET protocols often do not perform well for large networks (especially if not dense)
  - Global topology is based on the connectivity of each mobile node
- Clusters can be used to provide scalability
  - Clusters are formed (dynamically, of course) to provide hierarchy
  - Global routing is done to clusters
  - Local routing is done to nodes within a cluster
  - Clusters of clusters (super-clusters) can be formed to extend hierarchy
  - Similar in principle to IP subnets

Hierarchical Algorithms (2)

- A special node, called the *cluster-head*, is designated in each cluster
  - Responsible for routing data to or from other clusters
  - May be a special node, or may be designated through a clustering algorithm
- Algorithms
  - Clustering -- form clusters
  - Cluster-head identification -- may be an integral part of the clustering algorithm
  - Routing -- some routing algorithm is still needed
    - Applied at each level of the hierarchy

Hierarchical Algorithm Example