Logistics

- Final Exam: Monday, 6/12 6:30pm – 9:30pm in ROLFE1200
  - Roughly 1/3 problems before midterm, 2/3 after midterm
  - Closed book & notes, allow up to 1 double sided cheat sheet

Chapter 6: Wireless and Mobile Networks

6.1 Introduction

6.2 Wireless links characteristics

- CDMA

6.3 IEEE 802.11 wireless LANs (“wi-fi”)

6.4 Cellular Internet Access

Wireless: communication over wireless channel

6.5 Principles: addressing and routing to mobile users

6.6 Mobile IP

6.7 Handling mobility in cellular networks

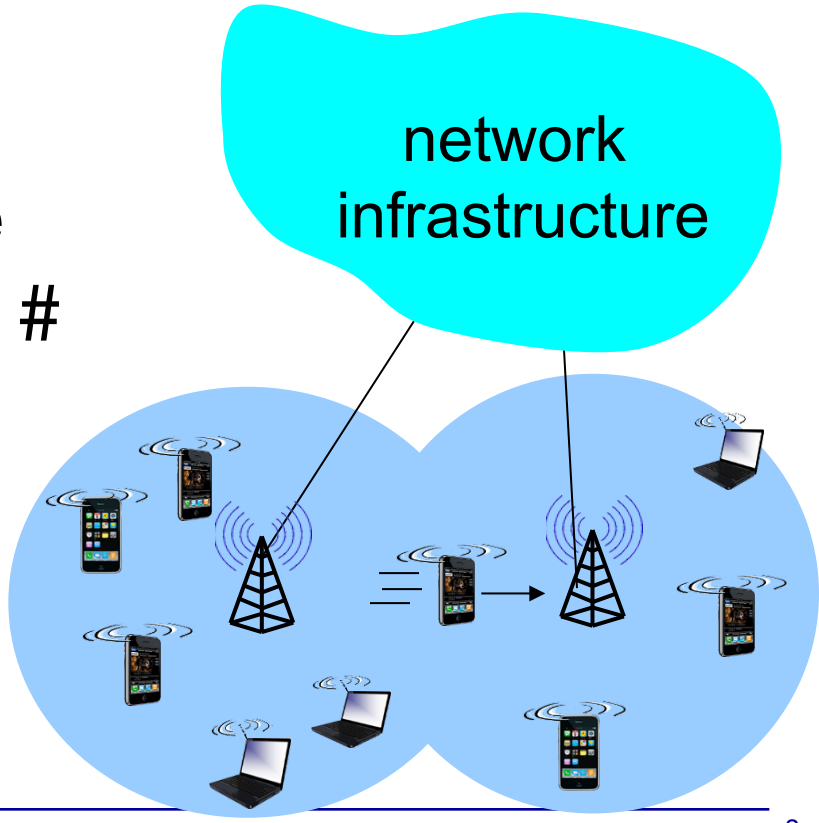
6.8 Mobility and higher-layer protocols

6.9 Summary

Mobility: hosts that change attachment point to the network

Two important (but different) challenges

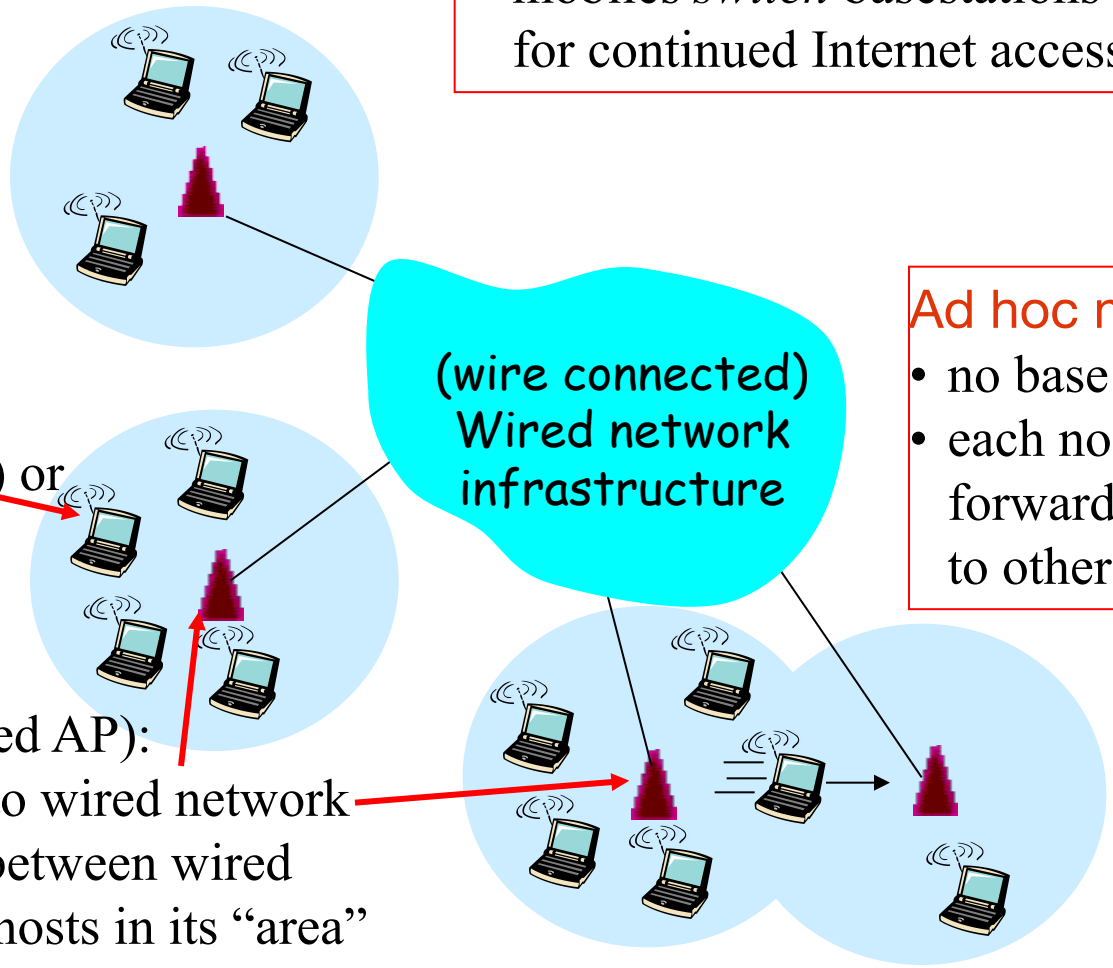
- wireless: communication over wireless link
- mobility: handling the mobile user who changes point of attachment to network
- # of wireless (mobile) phone subscribers far exceeds the # of wired phone subscribers
- Smart phones → anytime untethered Internet access



Elements of a wireless network

wireless link
- connecting mobile(s) to base station
- multiaccess protocol: coordinates link access

Infrastructure mode:
- basestations connect mobiles to wired networks
- mobiles *switch* basestations after move for continued Internet access (handoff)

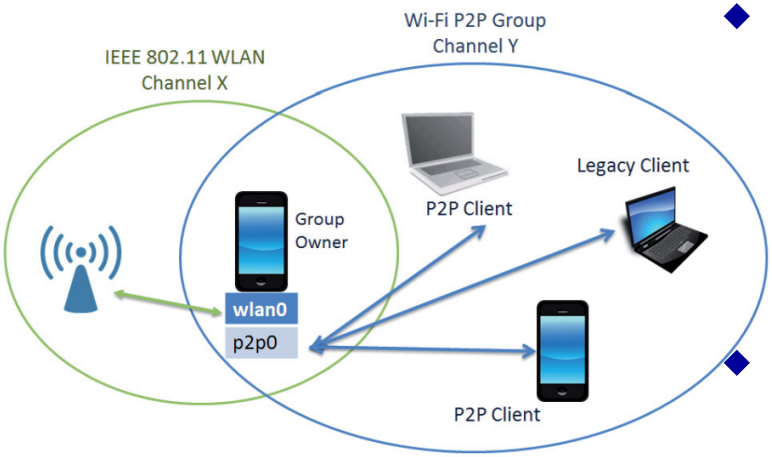


Wireless host: may be stationary (non-mobile) or mobile

Ad hoc mode:
- no base stations;
- each node helps forward packets to other nodes

Base station (also called AP):
- typically connected to wired network
- forwarding packets between wired network and wireless hosts in its "area"

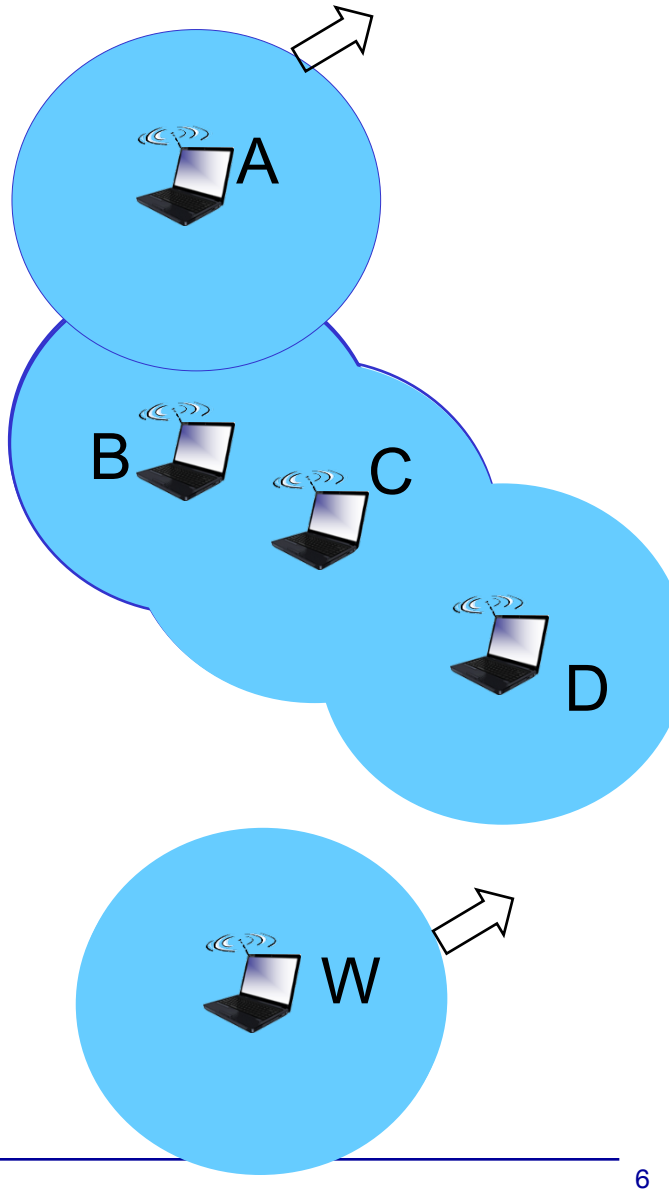
Wi-Fi Direct (aka AirDrop)



- A mechanism that allows for PCs, Phones & Devices to connect & communicate directly with each other
- Does not the devices to be connected to the same or any network
- Provides a high bandwidth transport for bi-directional data exchange
- Not just 1:1, can support multiple devices

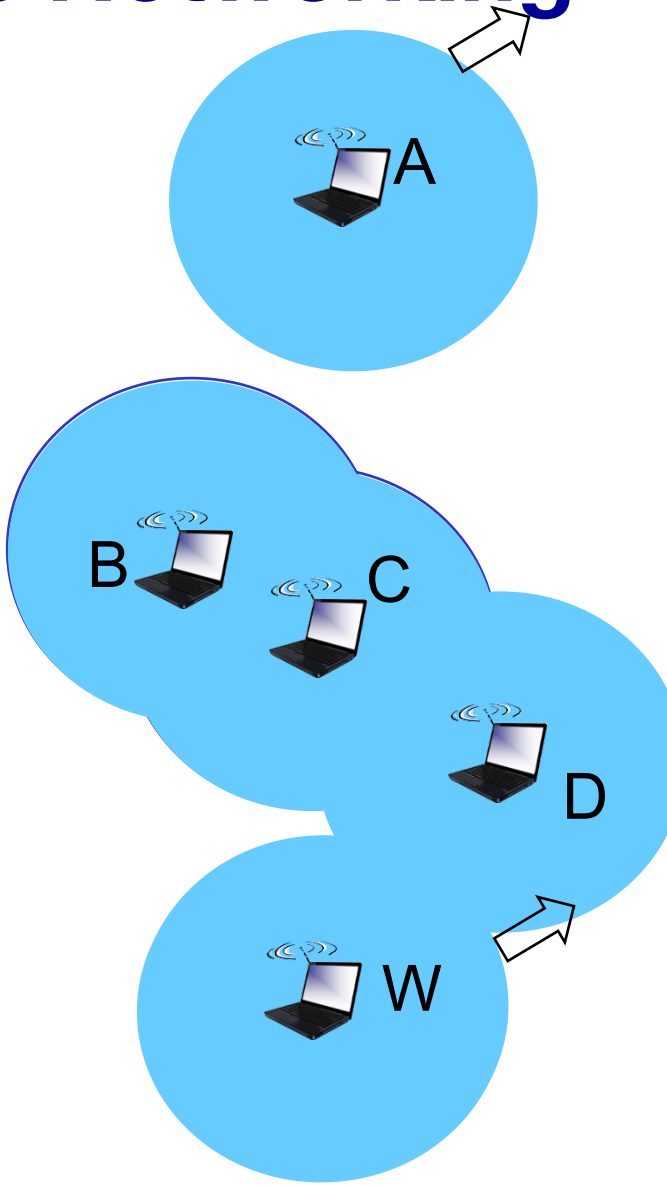
Ad Hoc Model of Wireless Networking

- no base station
- nodes can only transmit to other nodes within link coverage



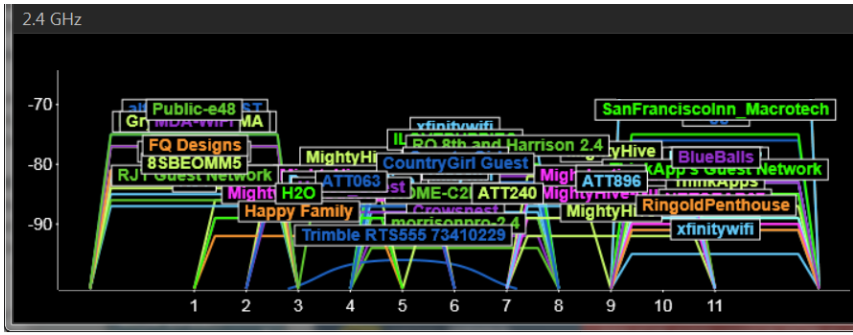
Ad Hoc Model of Wireless Networking

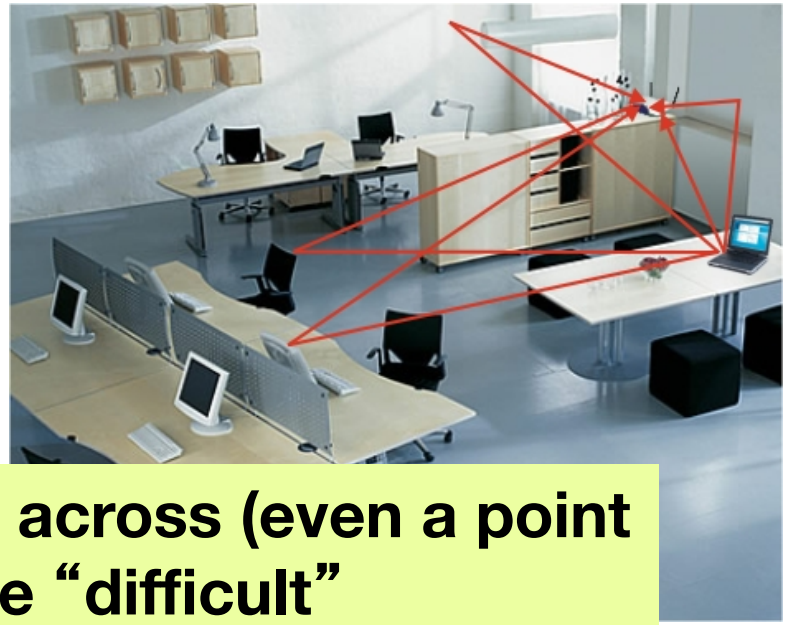
- no base station
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network
  - exchange information about who can reach whom
  - Both distance-vector and link-state approaches have been tried



Wireless Link Characteristics

- Decreased signal strength: radio signal attenuates as it propagates through matter (different frequencies have different penetration properties)
- Interference signals from other sources
  - standardized wireless network frequencies (e.g., 2.4 GHz) shared by other devices (e.g., microwave oven, cordless phone)
- Multipath propagation: radio signal reflects off objects around (e.g. walls), arriving at destination at slightly different times

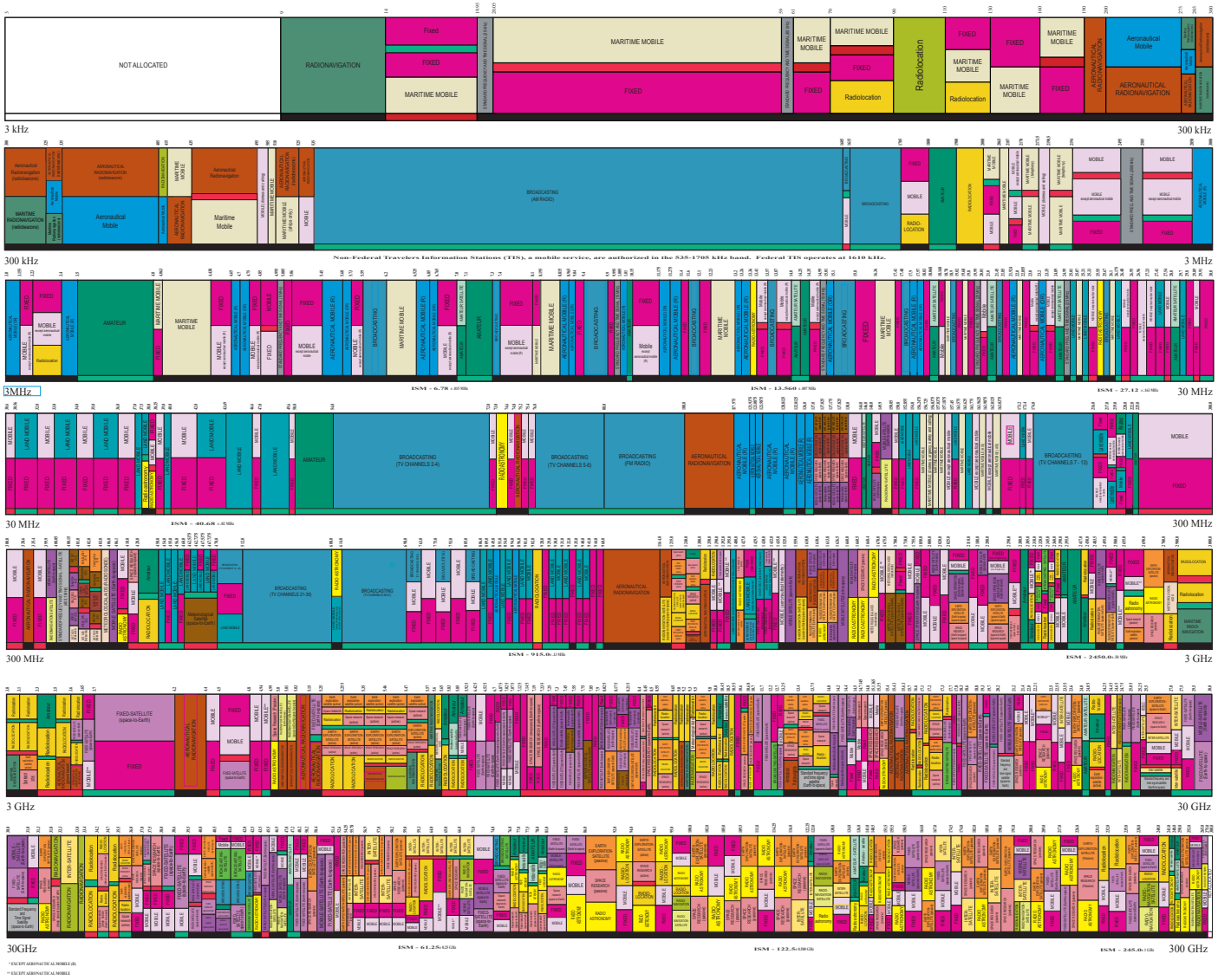




the above make communication across (even a point to point) wireless link much more "difficult"

UNITED STATES FREQUENCY ALLOCATIONS

THE RADIO SPECTRUM

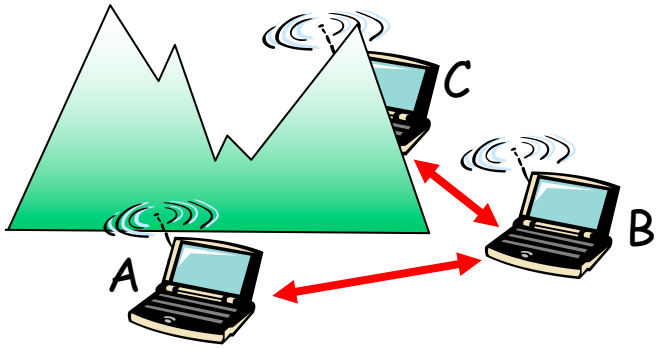


https://en.wikipedia.org/wiki/Spectrum_management

Besides multiple access: other problems

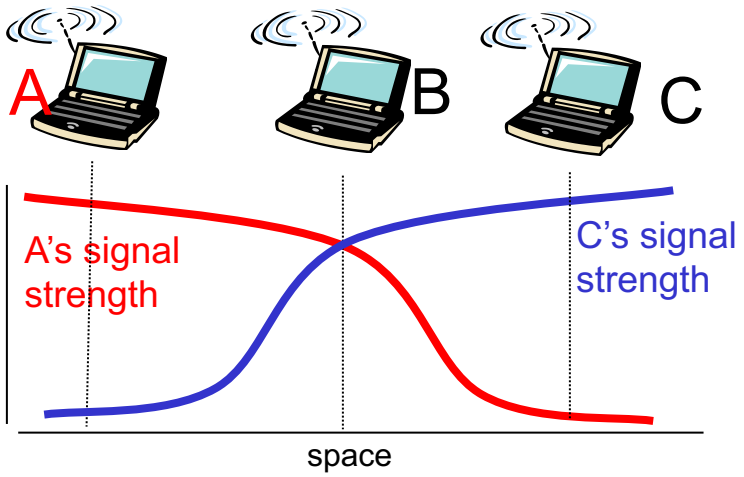
Hidden terminal

- B, A hear each other
- B, C hear each other
- A, C can't hear each other
- A, C may send to B at the same time!



Signal attenuation

- B, A hear each other
- B, C hear each other
- A, C cannot hear each other → interference at B



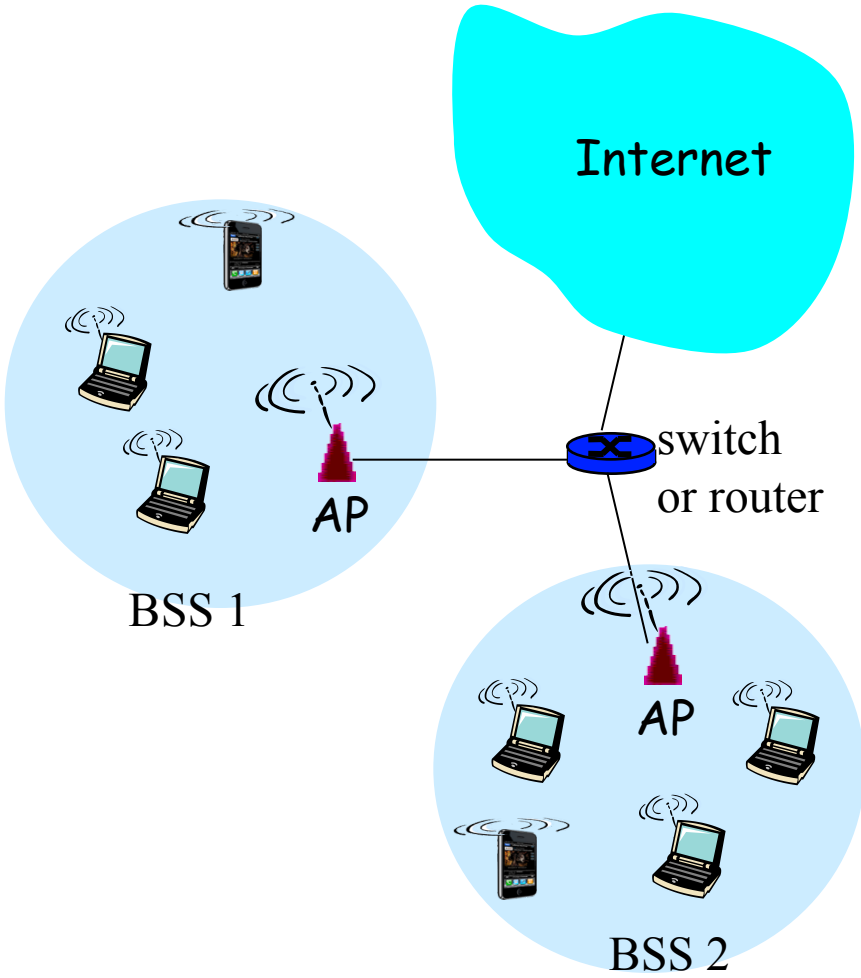
IEEE 802.11 Wireless LAN (WiFi)

FYI

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

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

802.11 LAN architecture

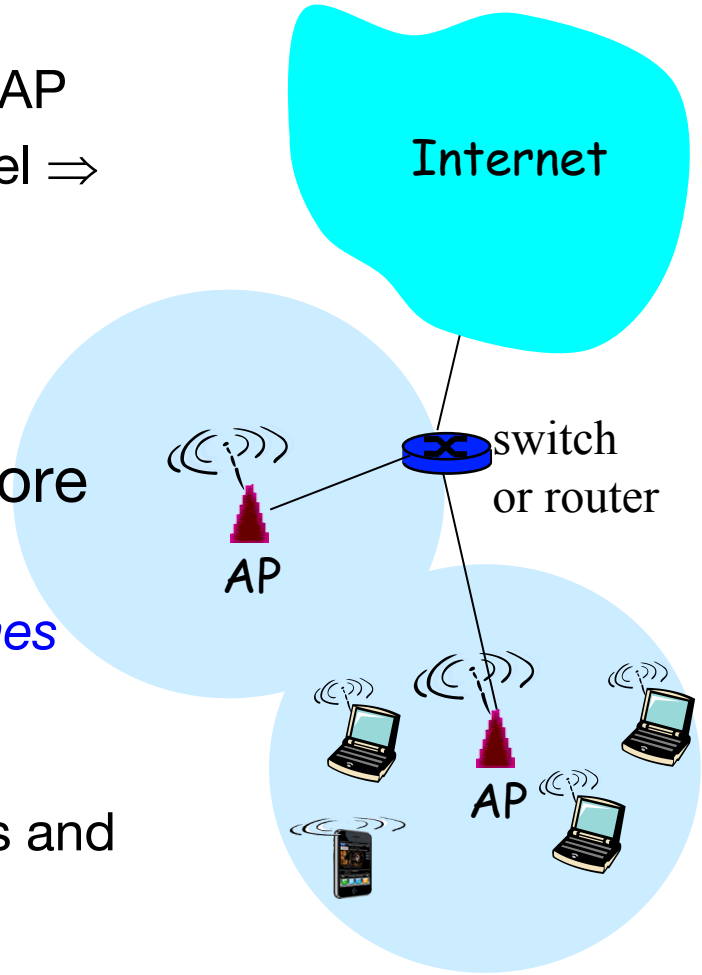


- wireless host communicates with base station
  - AP: access point (i.e. basestation)
- Basic Service Set (BSS) contains:
  - wireless hosts
  - access point (AP): base station

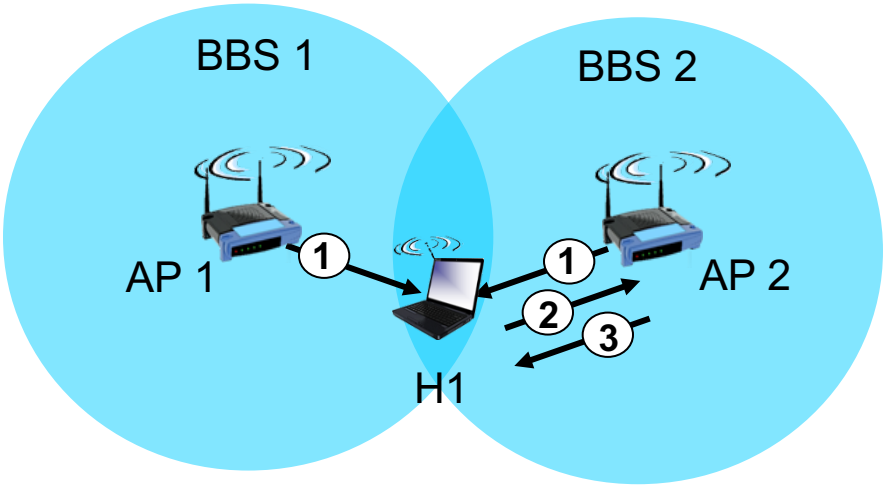
BSS: Basic Service Set (aka “cell”)
SSID: Service Set Identifier

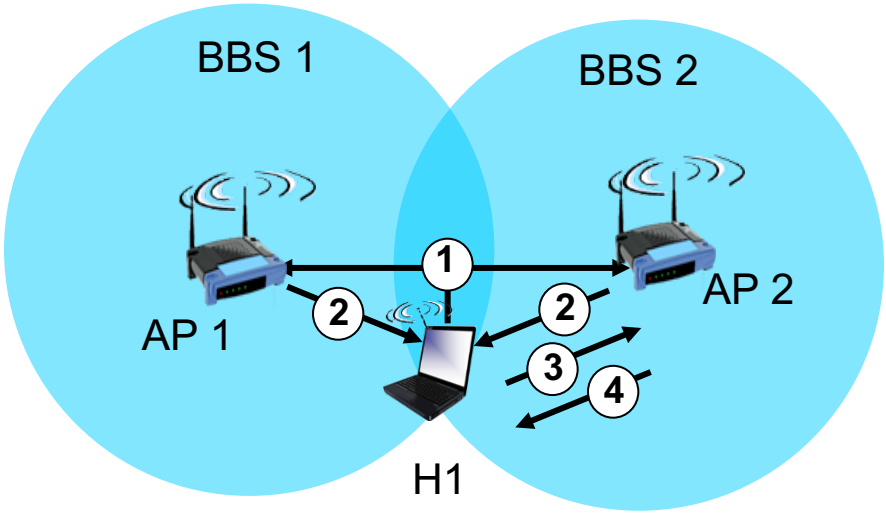
802.11 LAN architecture

- 802.11b: divides 2.4--2.485GHz spectrum into 11 channels at different frequencies
  - (802.11n effectively have only 3 channels, as it uses wider frequency band)
  - Administrator chooses frequency for an AP
  - If neighbor APs use same default channel ⇒ interference
- AP sends *beacon frame* periodically
  - Contain SSID, its own MAC address
- Host: must associate with an AP before transmitting data
  - scan channels, listening for *beacon frames*
  - Select AP to associate with by initiating association protocol
  - Typically use DHCP to get an IP address and other information in the AP's subnet



802.11: passive/active scanning





passive scanning:

(1)beacon frames sent **from APs**

(2)association Request frame sent: H1 to selected AP

(3)association Response frame sent from selected AP to H1

active scanning:

(1)Probe Request frame broadcast **from H1**

(2)Probe Response frames sent from APs

(3)Association Request frame sent: H1 to selected AP

(4)Association Response frame sent from selected AP to H1

IEEE 802.11: multiple access

- Like Ethernet, uses CSMA: sense the channel before transmitting
  - don't collide with ongoing transmission
- Unlike Ethernet:
  - *no collision detection* – once start, transmit all frames to completion
  - *Receiver sends acknowledgment* – sender finds out whether the transmission collided or succeeded
- Why no collision detection?
  - weak received signals (fading) → difficult to receive (sense collisions) when transmitting
  - can't sense all collisions, e.g. hidden terminal case
- Solution: CSMA / C(ollision)A(voidance)

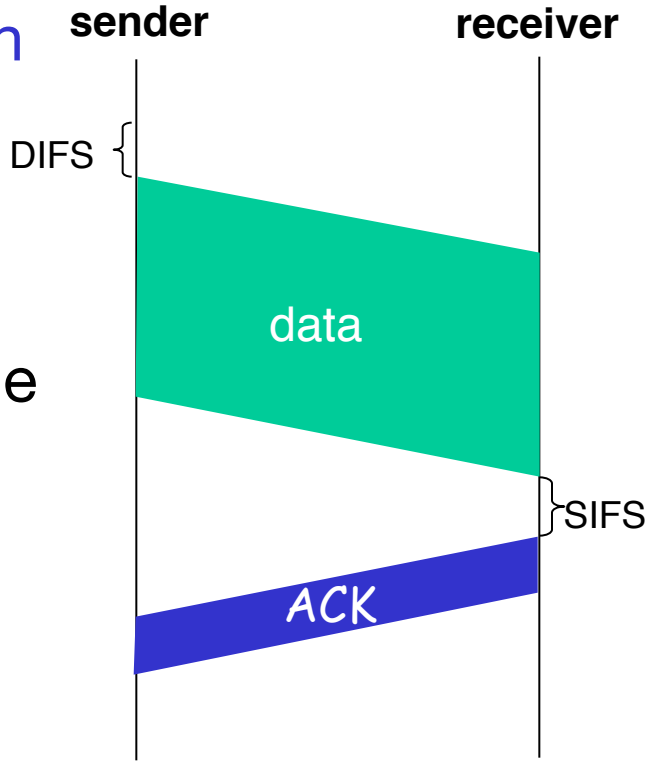
IEEE 802.11 MAC Protocol: CSMA/CA

802.11 sender: channel sensing

If sense channel idle for **DIFS** period then
transmit *entire* frame

Else if sense channel busy then

- start random backoff timer
- timer counts down while channel idle
- transmit when timer expires
- if no ACK, increase random backoff interval, repeat



802.11 receiver

if frame received OK then
return ACK after **SIFS**

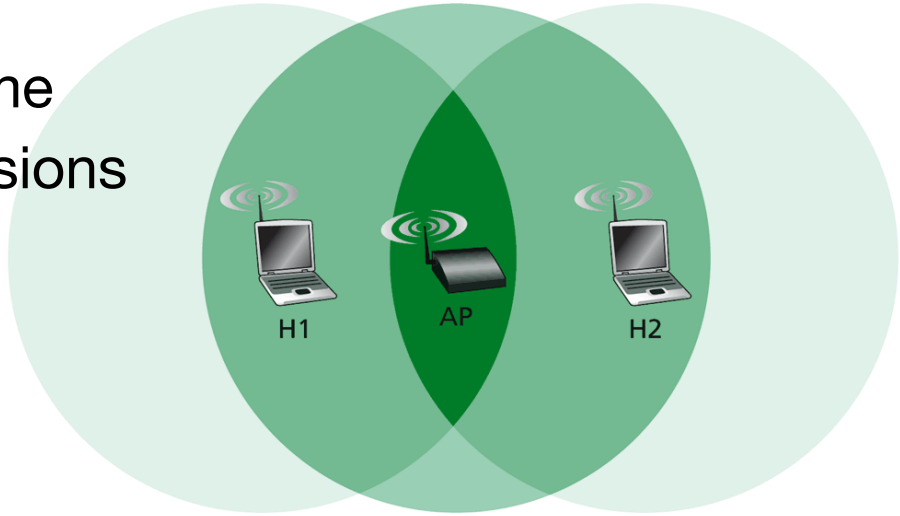
DIFS: Distributed Inter-Frame Spacing
SIFS: Short Inter-Frame Spacing

Optional Collision Reduction

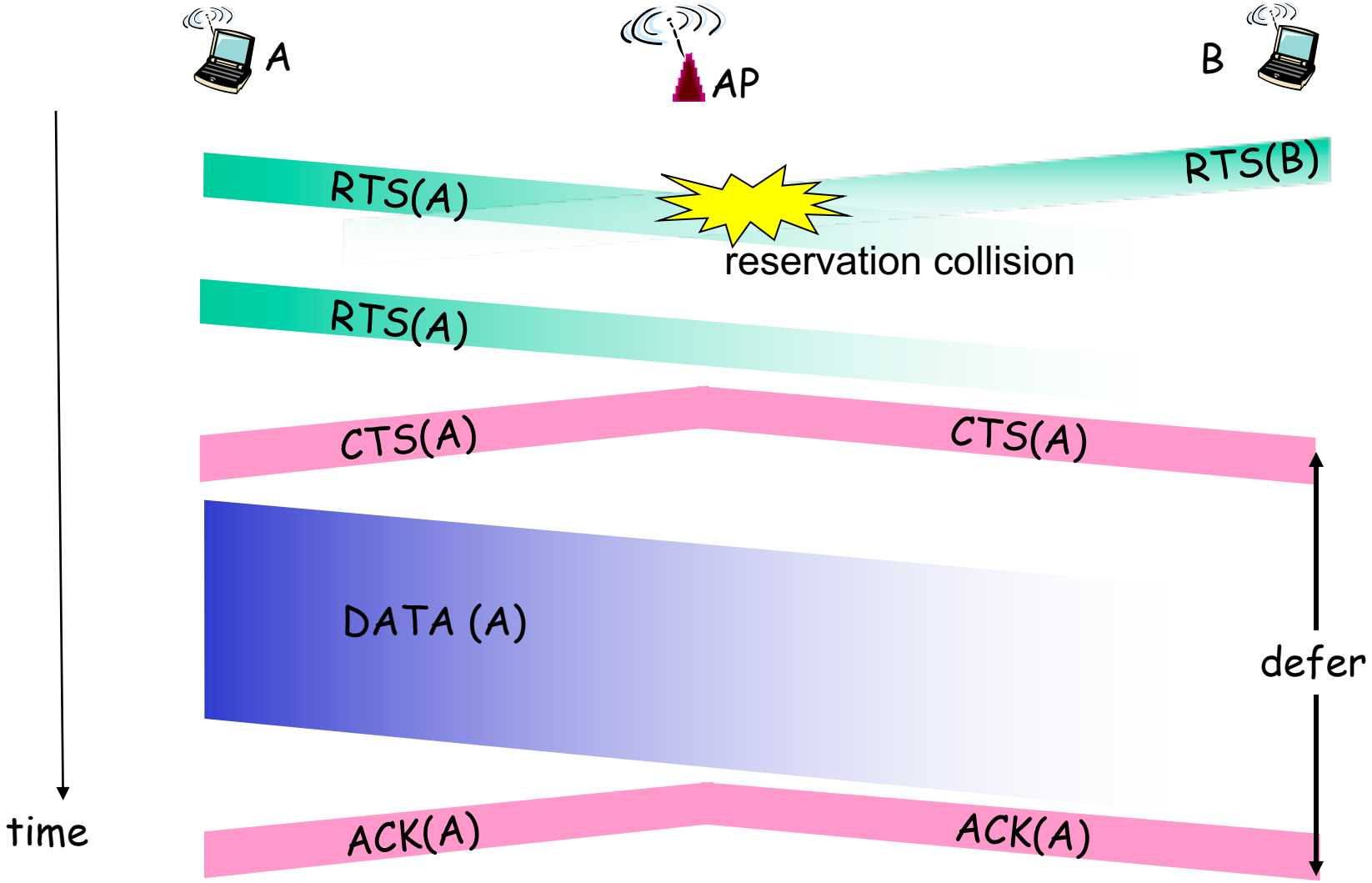
- idea: allow sender to "reserve" channel: avoid collisions of long data frames

1. sender first transmits a small request-to-send (RTS) packet to AP using CSMA
   - RTSs may still collide with each other (but they're short)
2. AP broadcasts clear-to-send (CTS) in response to RTS
3. CTS heard by all nodes within AP's range
   - sender transmits its data frame
   - other stations defer transmissions

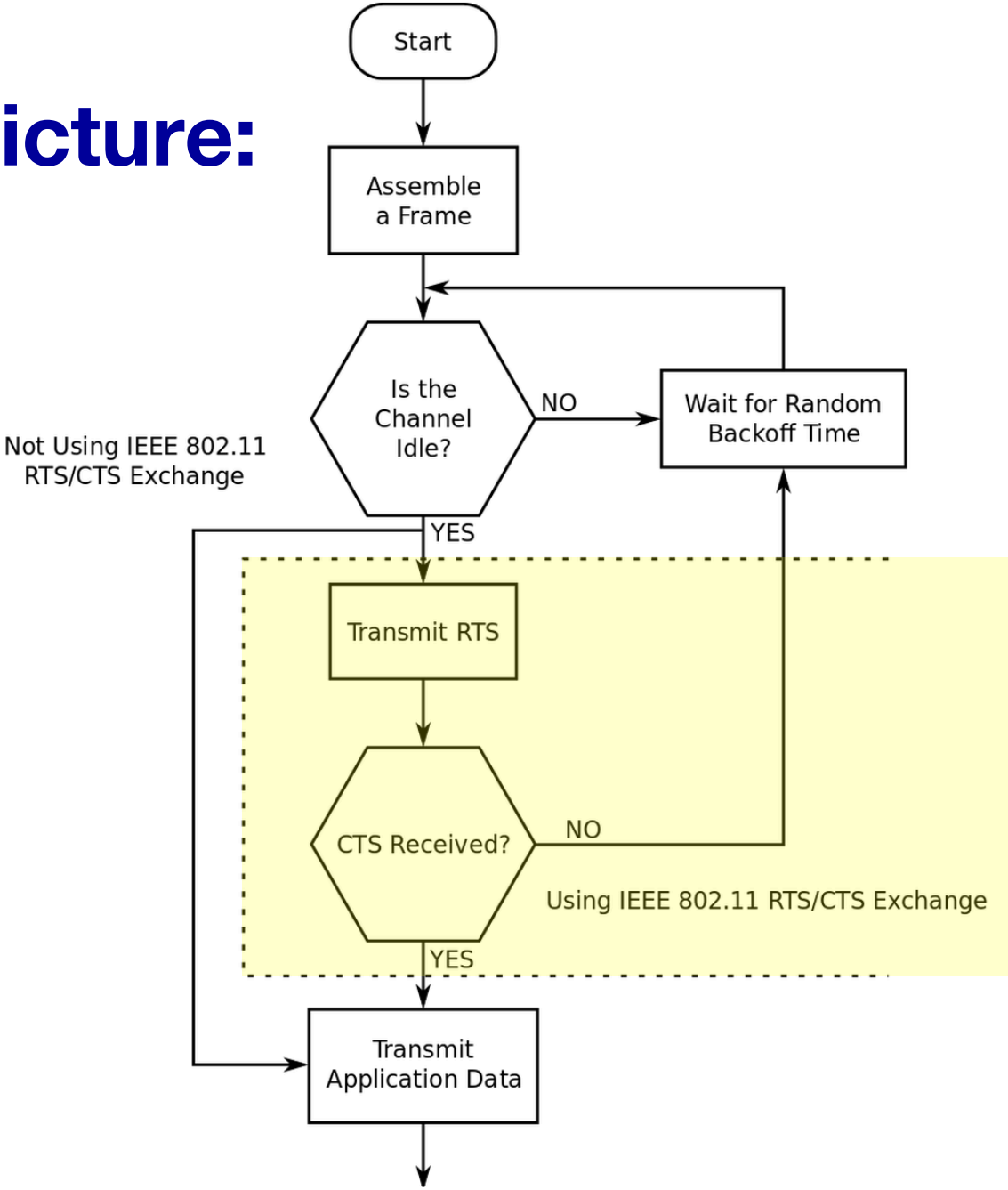
Use small packet exchanges to avoid data frame collision



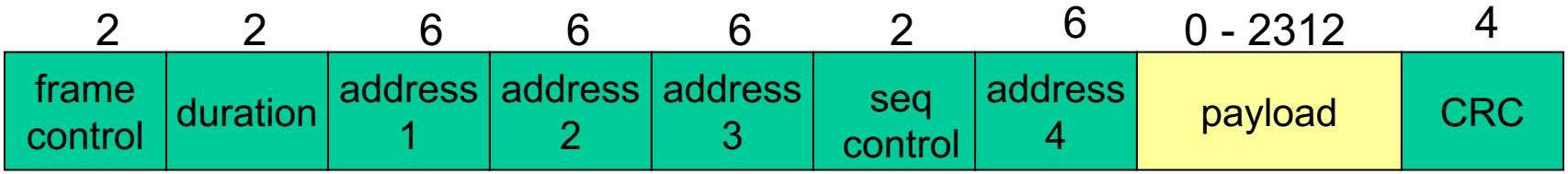
Collision Avoidance: RTS-CTS exchange



The combined picture:



802.11 frame: addressing



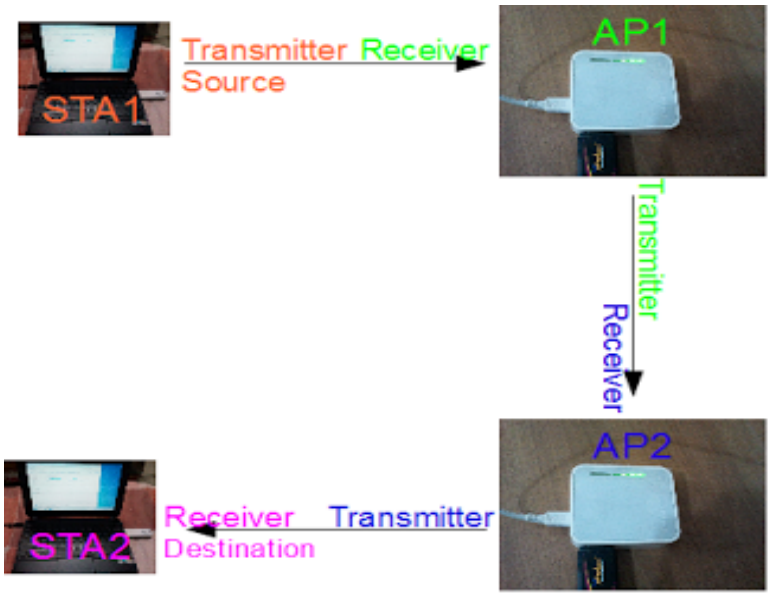
Address 1: MAC address of wireless host or AP to receive this frame

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

Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

- http://80211notes.blogspot.com/2013/09/understanding-address-fields-in-80211.html



•SA(Source Address): Source of the data (MSDU) --> STA1
•TA(Transmitter Address) : STA that transmitted the frame --> STA1, AP1, AP2
•RA(Receiver Address) : Immediate recipient of the frame --> AP1, AP2, STA2
•DA(Destination Address) : Final recipient of the data (MSDU) --> STA2
•BSSID (Basic Service Set IDentifier) : Unique identifier of the BSS, e.g, the MAC address of the AP in an infrastructure network --> AP1, AP2

Hint For Project 3

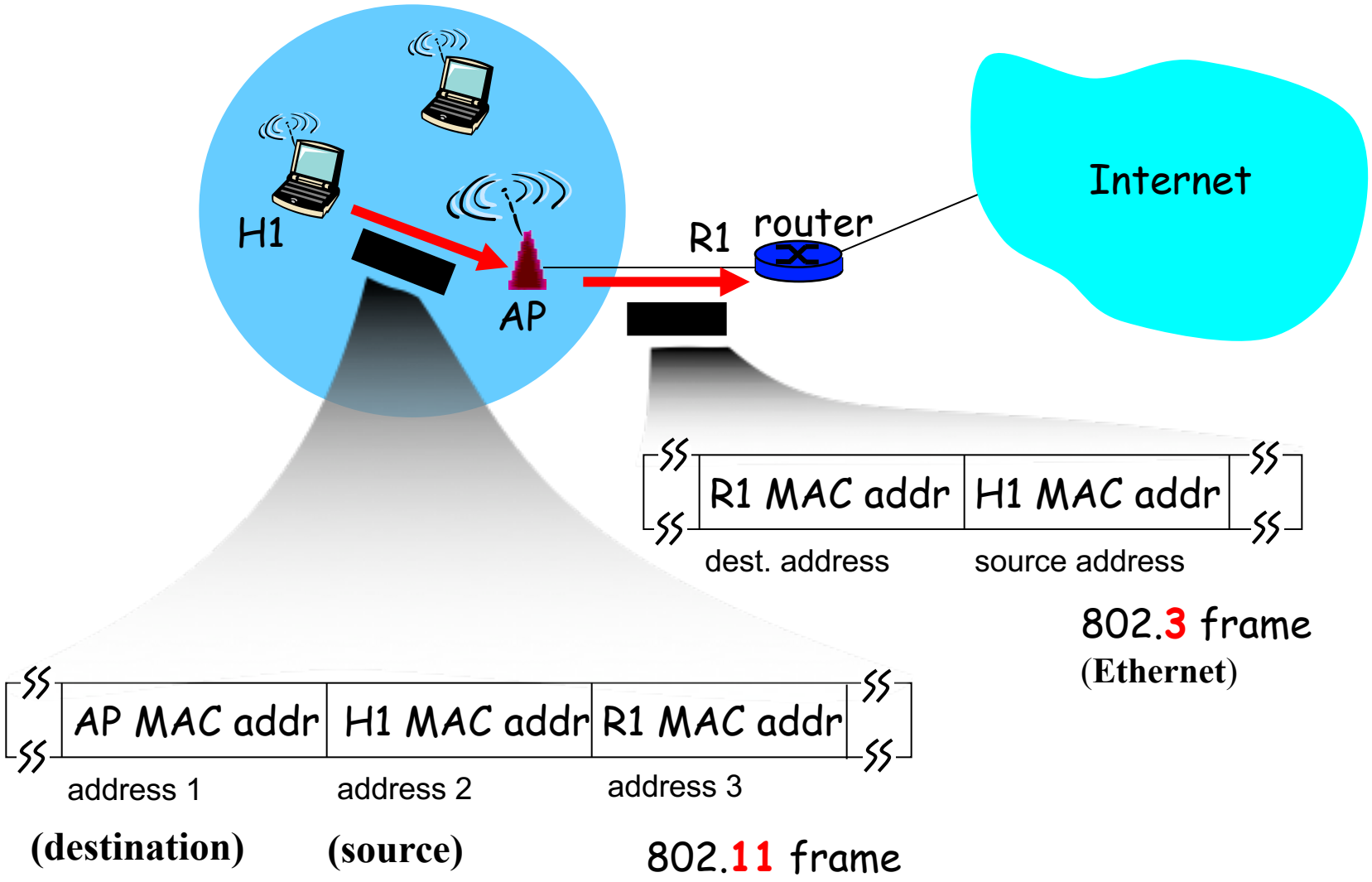
- man nc

Addresses in 802.11 Frame

- Not all used all the time
- Only Address1 is mandatory. For e.g, CTS frame only has Address1. The remaining fields are filled based on the the frame

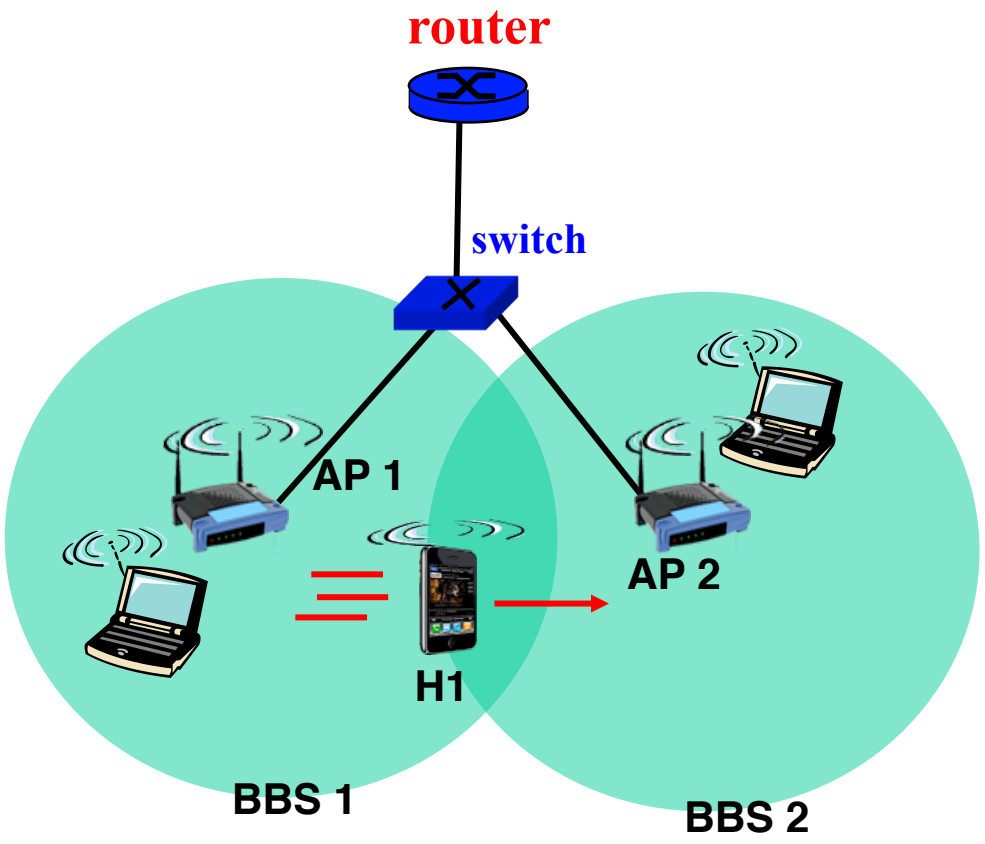
	Control Frames	Management Frames	Data Frames
Address 1	RA	RA	RA
Address 2	TA(not all)	TA	TA
Address 3	Not used	BSSID	BSSID or SA or DA
Address 4	Not used	Not used	BSSID or SA

802.11 frame: addressing



802.11: mobility within same subnet

- H1 detects weakening signal from AP1, scans and finds AP2 to attach to
- H1 remains in same IP subnet: IP address can remain same
- Switch: which AP is associated with H1?
  - self-learning: switch will see frame from H1 and "remember" which interface can be used to reach H1



Wi-Fi Security Techniques

- At the moment
  - Wired Equivalent Privacy (WEP)
  - 802.1X Access Control
  - Wireless Protected Access (WPA)

- In the future
  - 802.11i

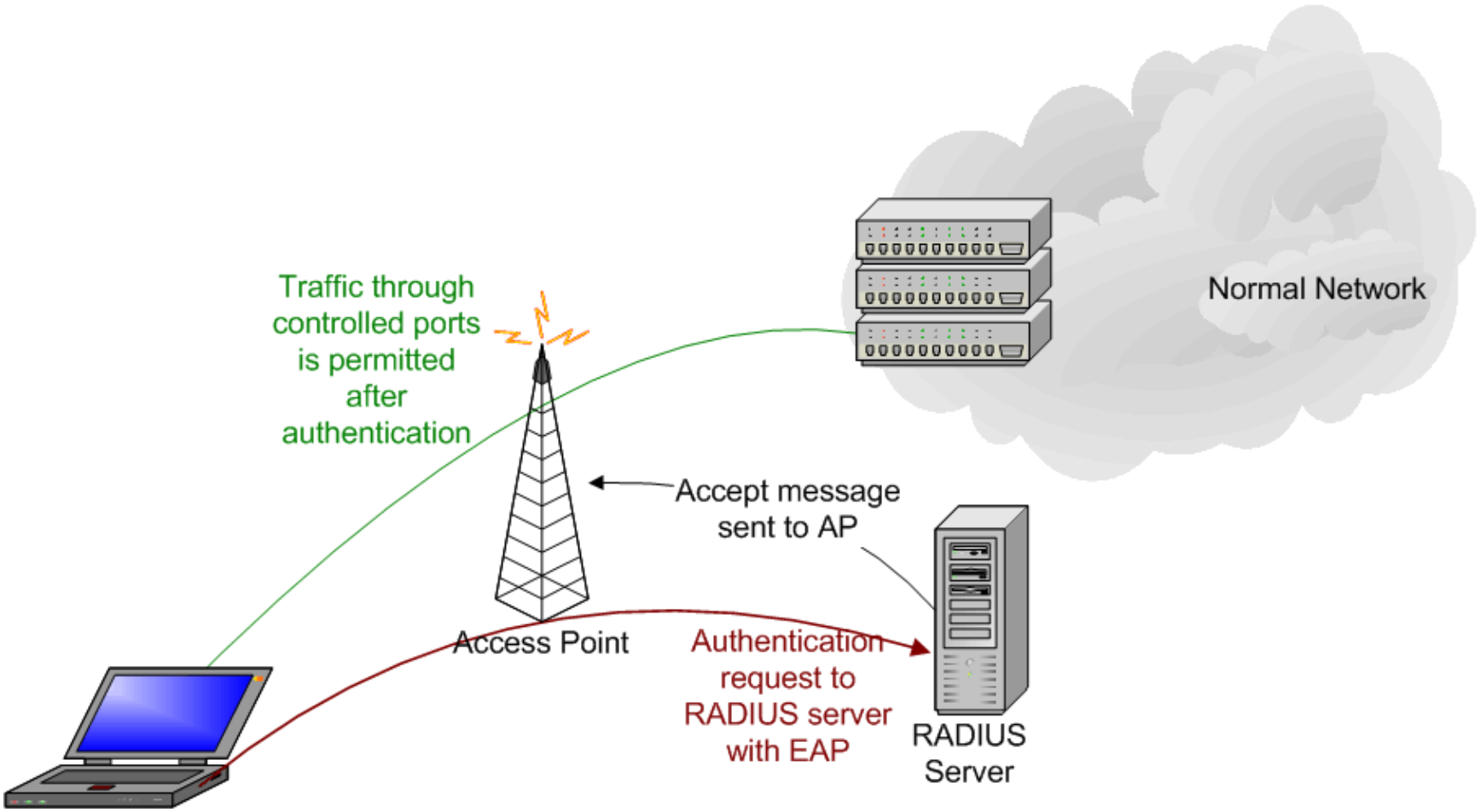
Wired Equivalent Privacy (WEP)

- Original security solution offered by the IEEE 802.11 standard
- Uses RC4 encryption with pre-shared keys and 24 bit initialization vectors
- Flawed design, easily broken
  - IV reuse causes problems
  - Tools to break WEP available on the internet
- Offers very little security at all

802.1x Access Control

- Designed as a general purpose network access control mechanism
  - Not Wi-Fi specific
- Access to network is controlled by switches (Access points in the Wi-Fi domain)
- User management with RADIUS
  - Extensible Authentication Protocol (EAP) used in authentication process
  - Authentication is done with the RADIUS server, which ”tells” the access point whether access to controlled ports should be allowed or not
- Doesn’t affect data transmissions, only authentication messages are encrypted if used EAP method is encrypting

802.1x Access Control



Wireless Protected Access (WPA)

- 802.1x Access Control
  - Pre-shared key setup available for SOHO environments
- TKIP (Temporal Key Integrity Protocol) encryption
  - RC4, dynamic encryption keys (session based)
    - 48 bit IV, key mixing function
  - Fixes all issues found from WEP
- Uses Message Integrity Code (MIC) Michael
  - Ensures data integrity
- Old hardware should be upgradeable to WPA

WPA and Security Threats

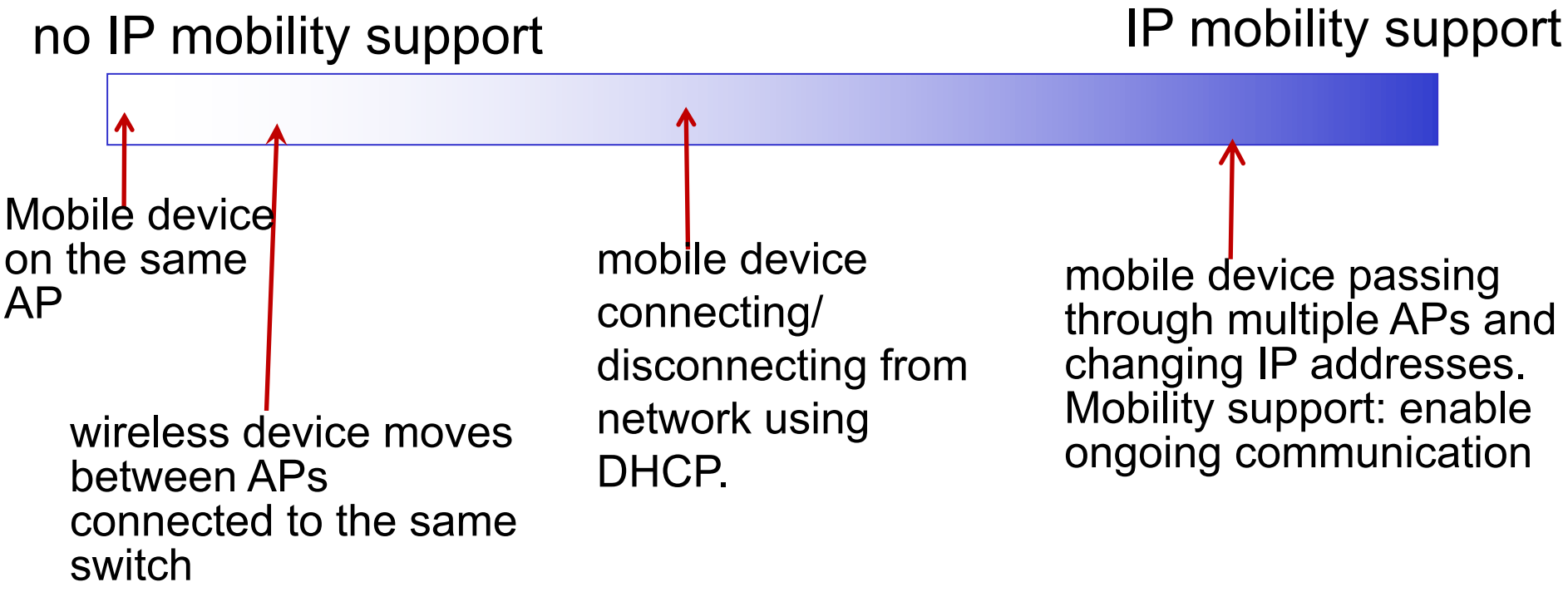
- Data is encrypted
  - Protection against eavesdropping and man-in-the-middle attacks
- Denial of Service
  - As a security precaution, if WPA equipment sees two packets with invalid MICs within a second, it disassociates all its clients, and stops all activity for a minute
  - Only two packets a minute enough to completely stop a wireless network

IP Mobilty

spectrum of mobility support

from the *network* perspective

- Does the moving lead to IP address change?
- Must the communication continue while a host's IP address changes?



How do *you* contact a mobile friend?

Consider a friend who frequently changes addresses, how do you find her?

- search all phone books?
- expect her to let you know where she is?
- call her parents?

Mobility: approaches

- *Let routing handle it*: routers advertise IP address of mobile-nodes-in-residen usual routing table exchange.
  - routing tables indicate where each mobi ed
  - no change to hosts needed
- *Let end-systems handle it*:
  - Each mobile host keeps “home” updated on its whereabouts

IP Mobility: Basic Concept

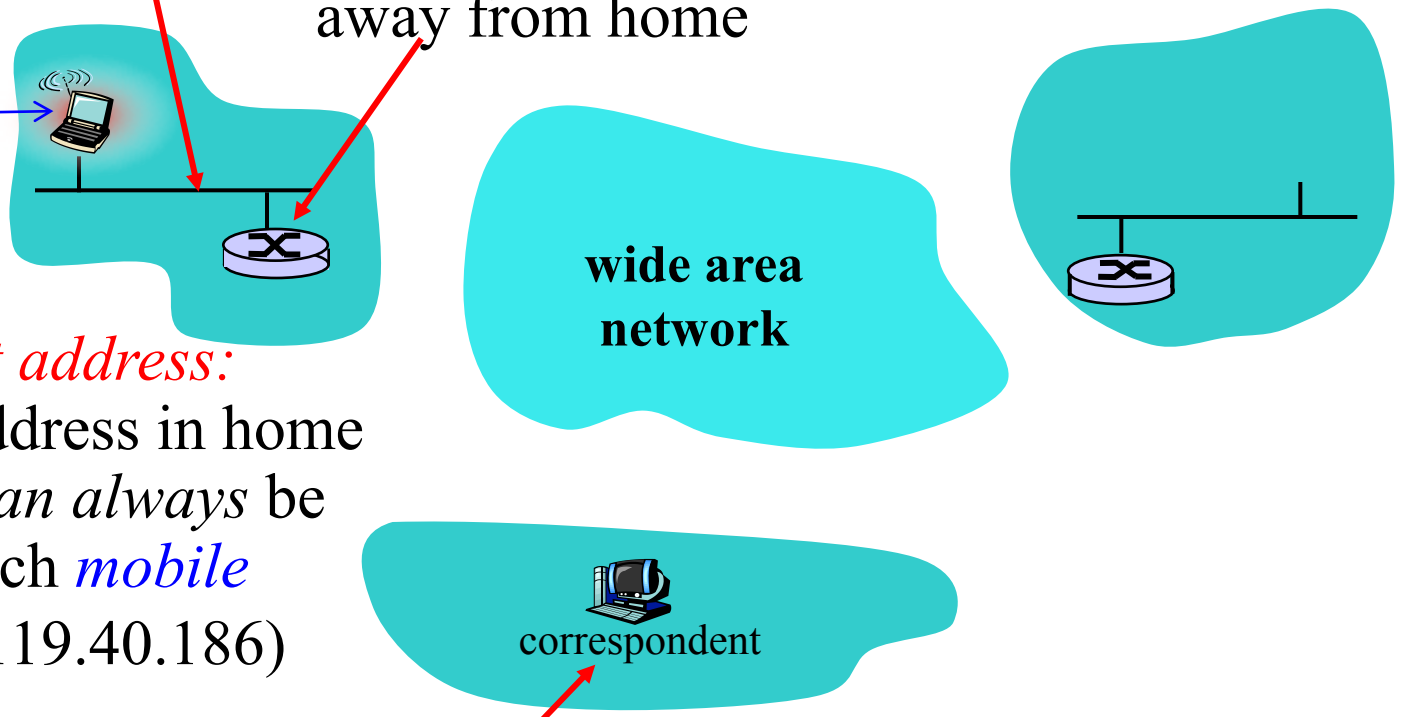
- Every host has a home
  - Stationary host: always home
  - Mobile host: may move away from home, have a home agent
- When a mobile moves outside home
  - Get a foreign IP address (care-of-address)
  - Connect to a foreign agent
  - Foreign agent notifies the home agent
- Other hosts can contact the mobile's home agent to learn where the mobile is
  - *indirect routing*: others send packets to mobile's home agent, which forwards to mobile
  - *direct routing*: others learn mobile's foreign address, directly send packets to the mobile

https://tools.ietf.org/html/rfc6301

IP Mobility: Vocabulary (I)

home network: permanent "home" of *mobile* (e.g., 128.119.40.0/24)

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



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

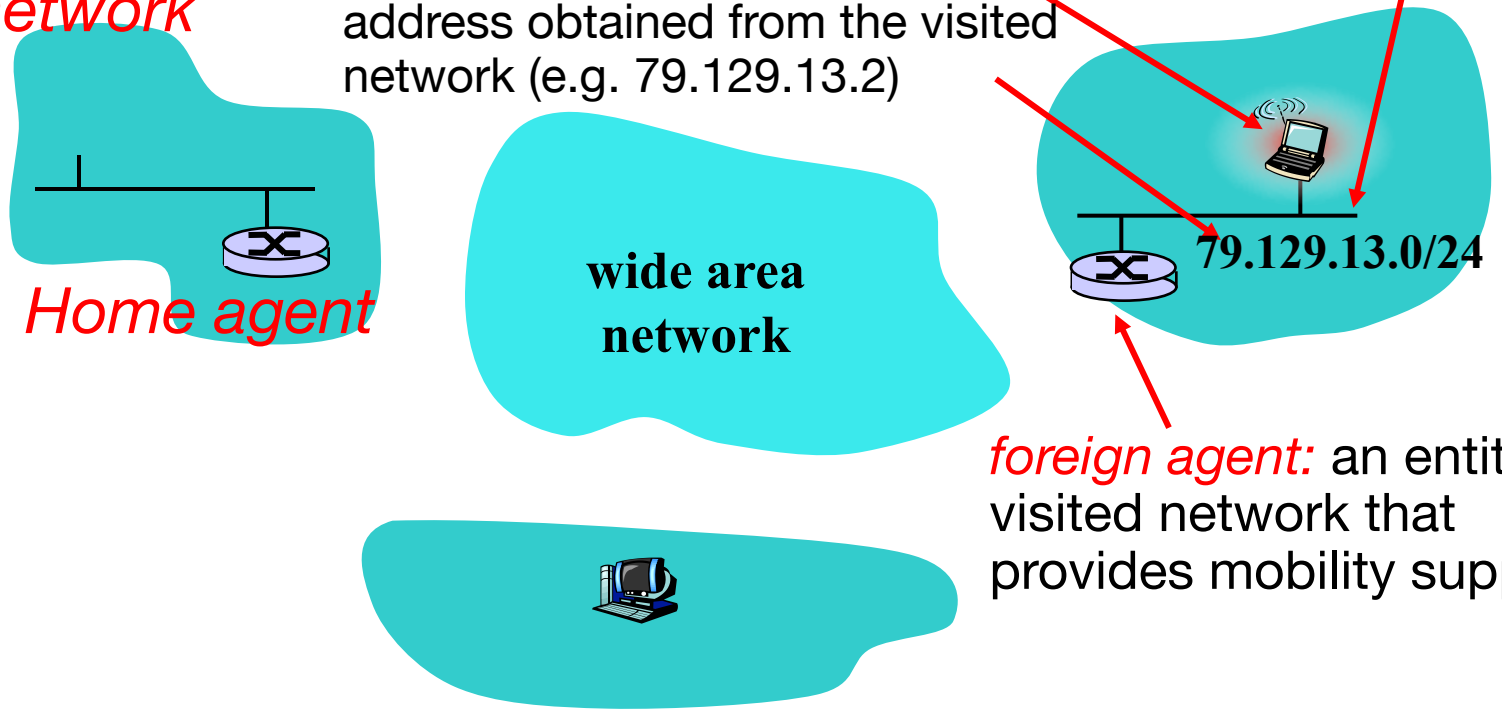
Correspondent: a computer that wants to communicate with *mobile*

Vocabulary (II): when away from home

Permanent address: remains constant (e.g., 128.119.40.186)

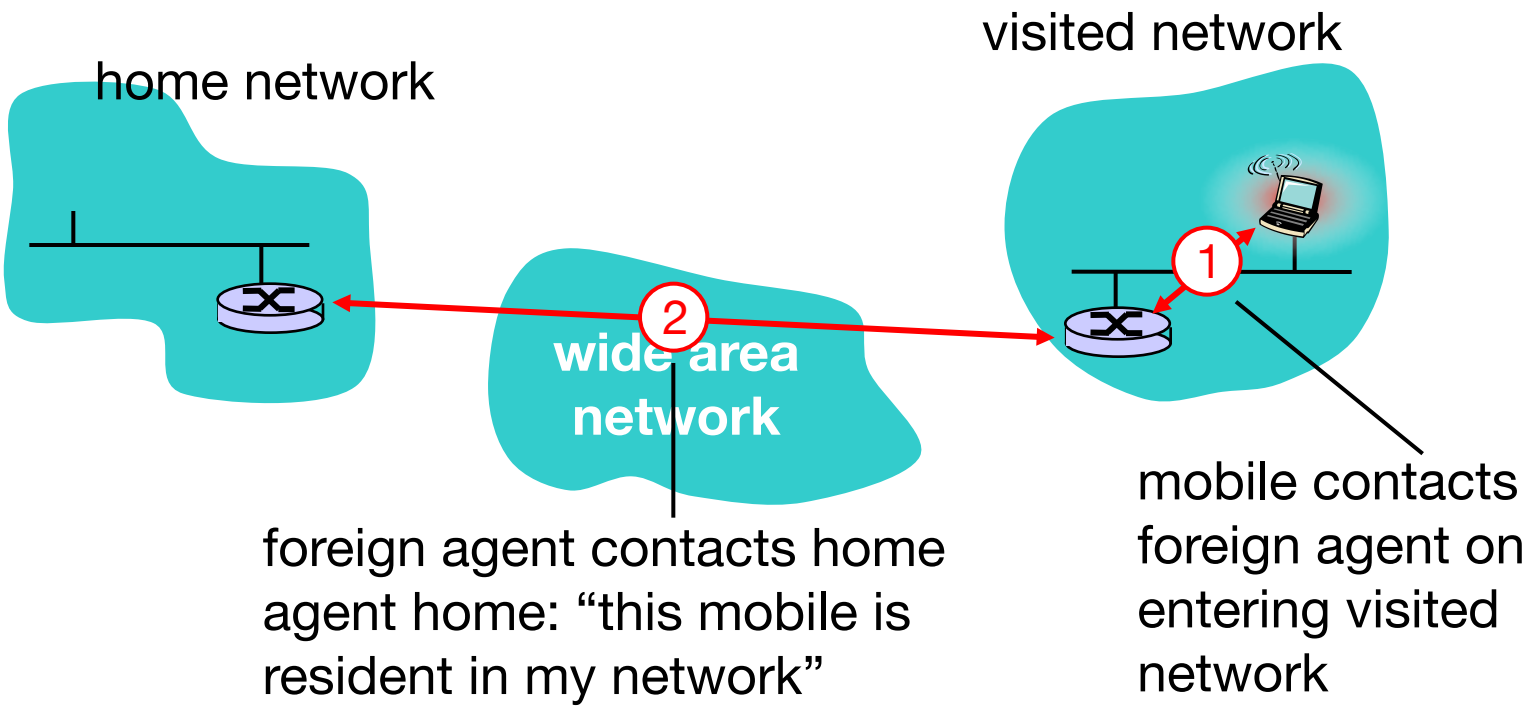
visited network: network in which *mobile* currently resides (e.g., 79.129.13.0/24)

Care-of-address: mobile's address obtained from the visited network (e.g. 79.129.13.2)



foreign agent: an entity in visited network that provides mobility support

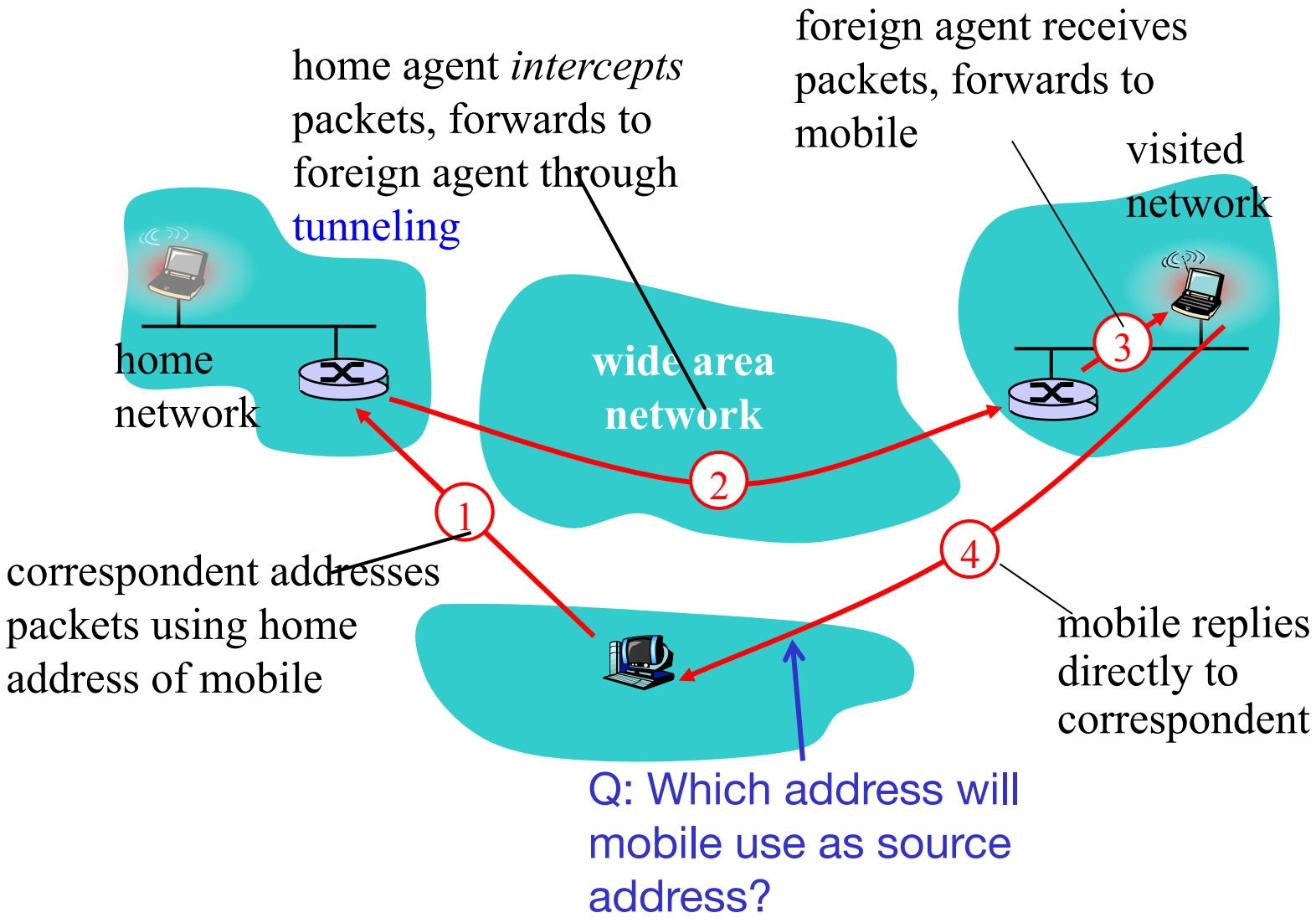
Mobility: registration



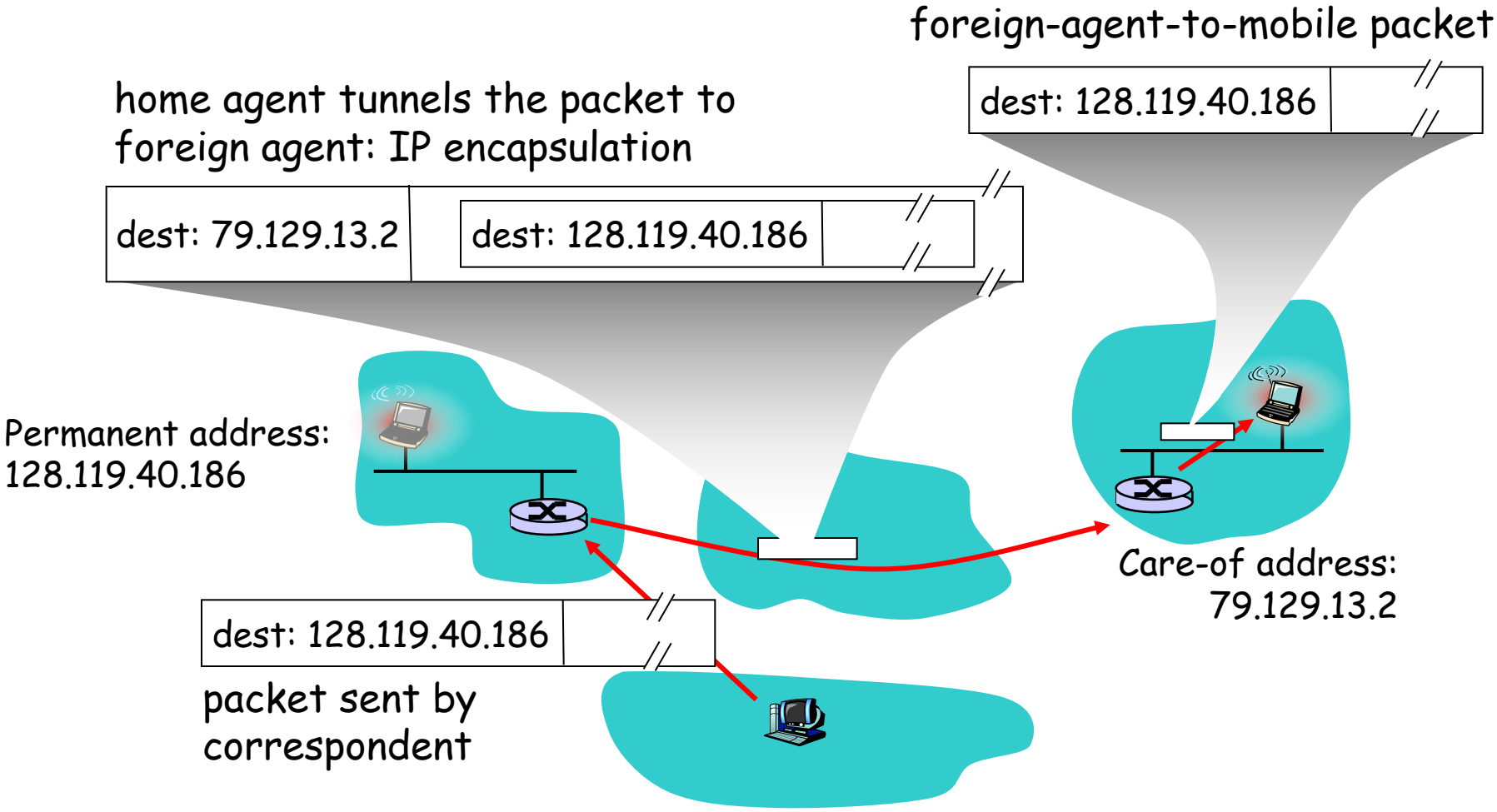
End result:

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

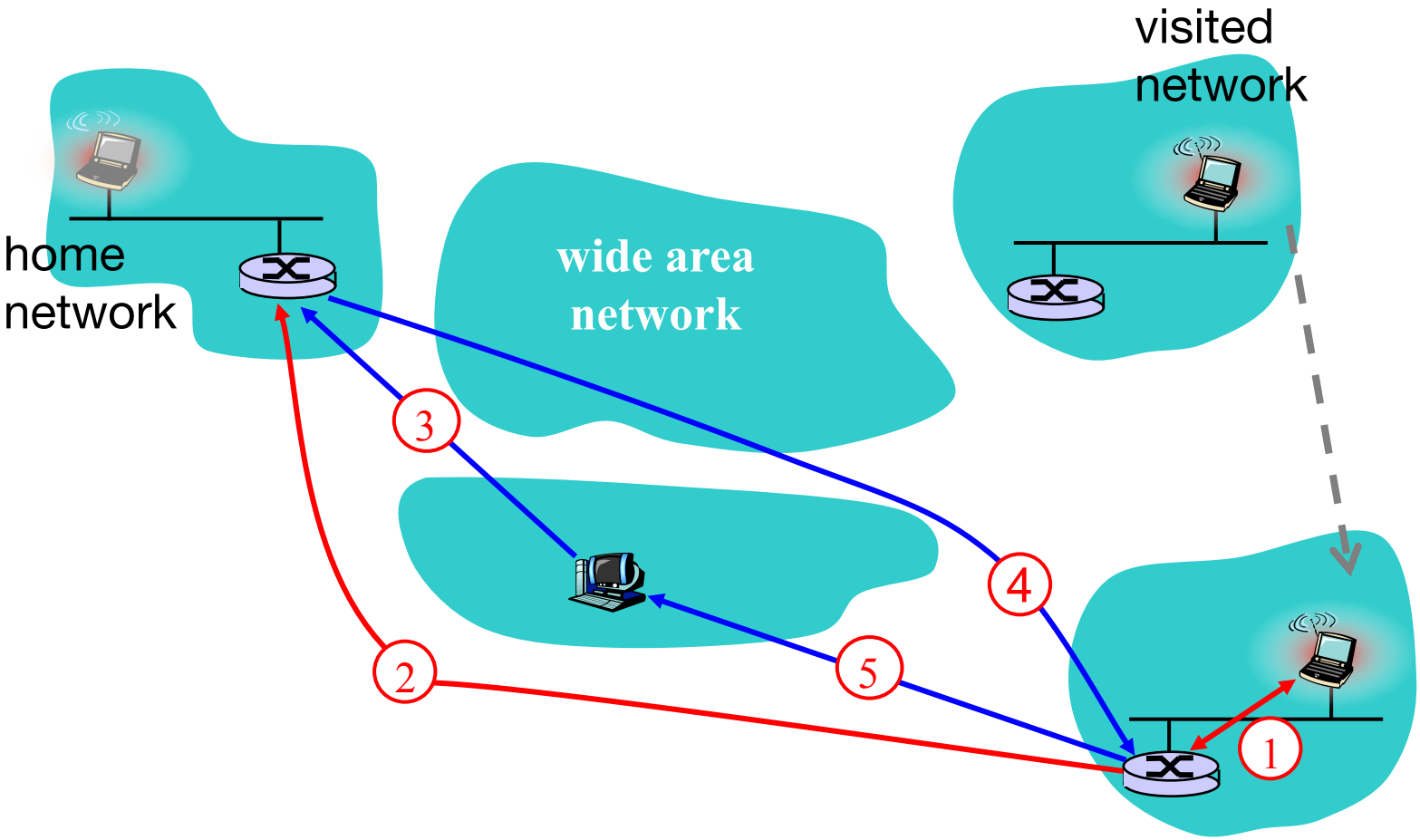
Supporting Mobility via Indirect Routing



Mobile IP: indirect routing



Indirect Routing: handling further movement



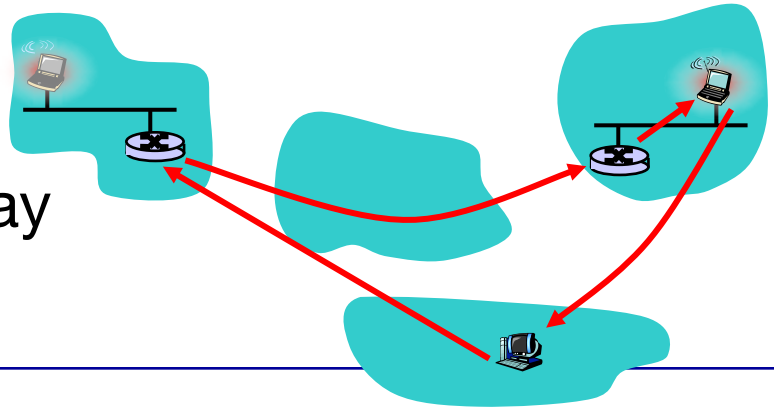
Q: Will the correspondence be aware of mobile's move?

Indirect Routing: moving between networks

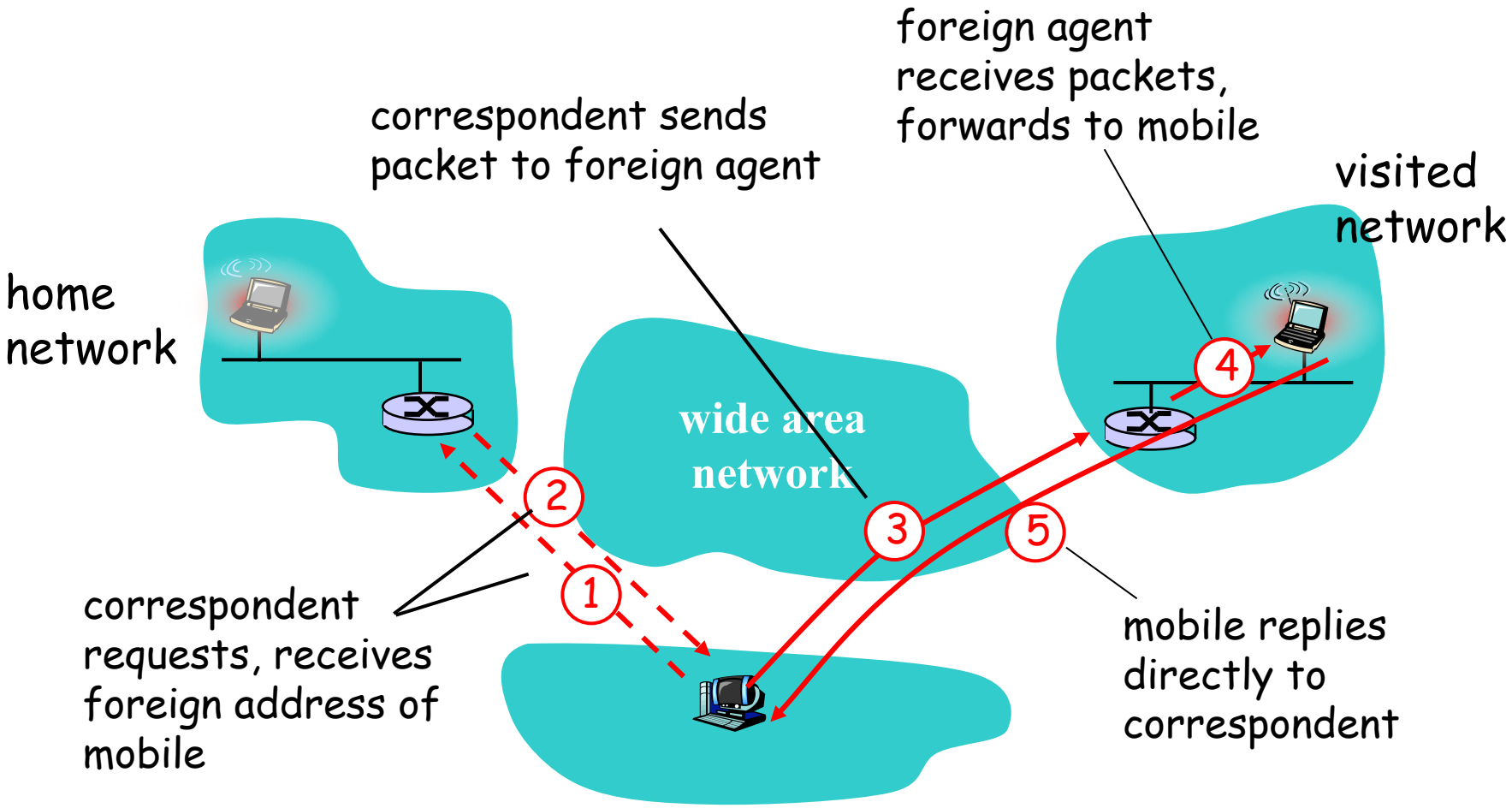
- When mobile moves to another network
  - registers with new foreign agent
  - new foreign agent registers with home agent
  - home agent update care-of-address for mobile
  - Home agent continue to forward packets to mobile through IP-in-IP tunnel (to the new care-of-address)
- Mobility is transparent to correspondent
- mobility is transparent to TCP/any transport protocol
  - TCP connection uses mobile's home address, *ongoing connections can be maintained* while mobile moves

Summary of Indirect Routing

- Mobile uses two addresses:
  - permanent address: used by correspondent to send packet to mobile
  - care-of-address: used by home agent to forward packet to mobile
- Mobile can perform foreign agent function itself
  - Just get a care-of address from foreign DHCP server
- Mobility is transparent to correspondent
- May result in triangle routing: correspondent→home-network→mobile
  - Inefficient, especially when correspondent & mobile are close but home agent is far away

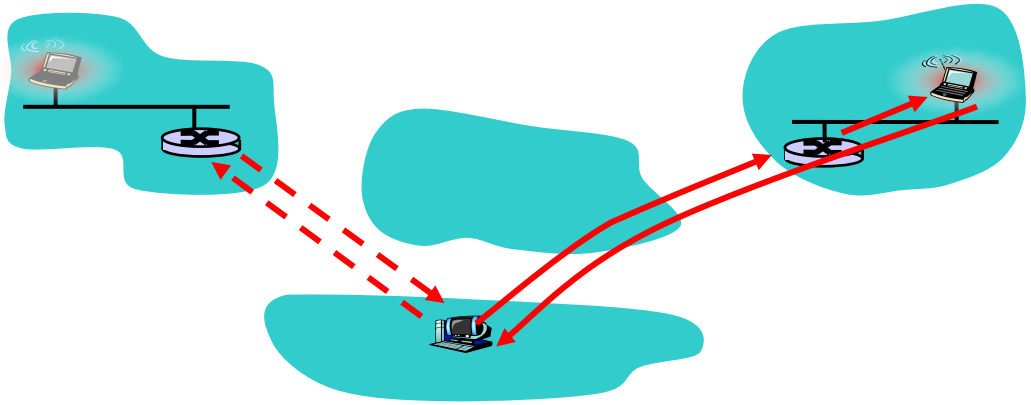


Mobility via Direct Routing



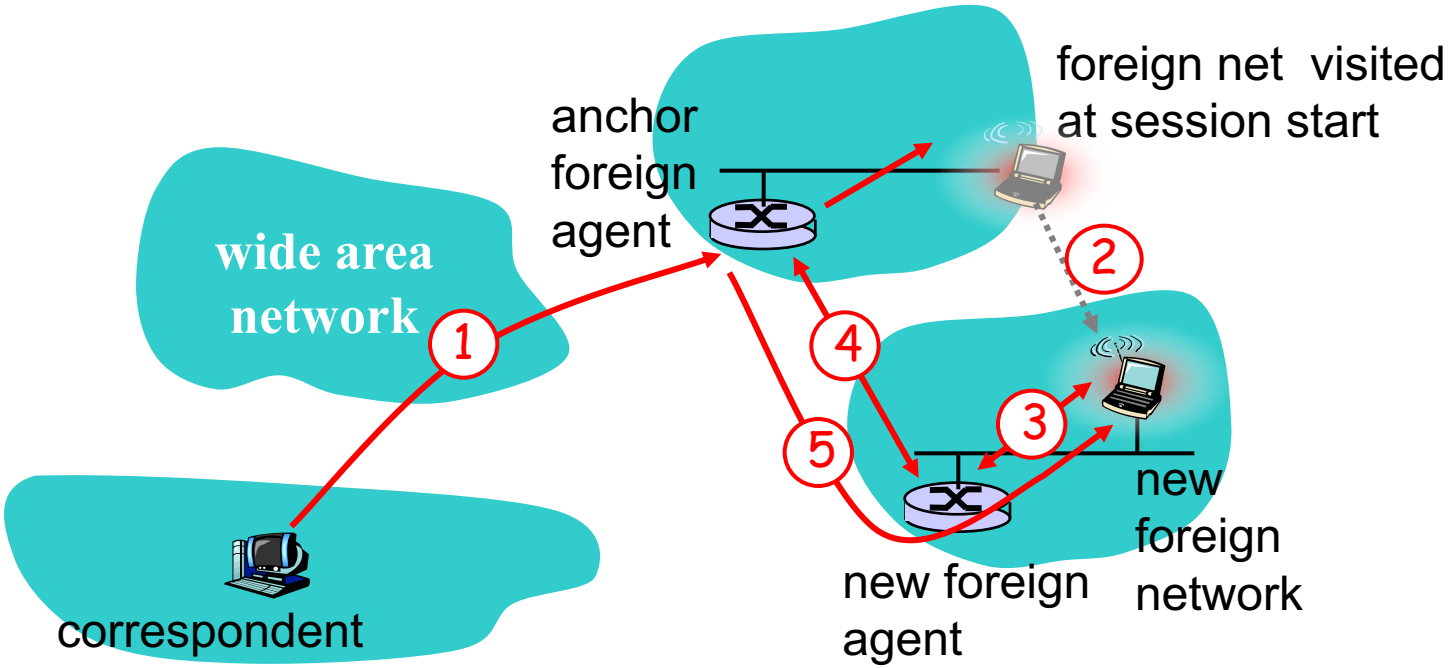
Mobility via Direct Routing: comments

- Good: Eliminate triangle routing problem
- bad:
  - Correspondent must be aware of mobility support
  - what if mobile moves from network to network?



Accommodating mobility with direct routing

- anchor foreign agent: FA in the first visited network
- data always routed first to anchor FA
- when mobile moves: new FA notifies the old FA to have data forwarded from old FA (chaining)



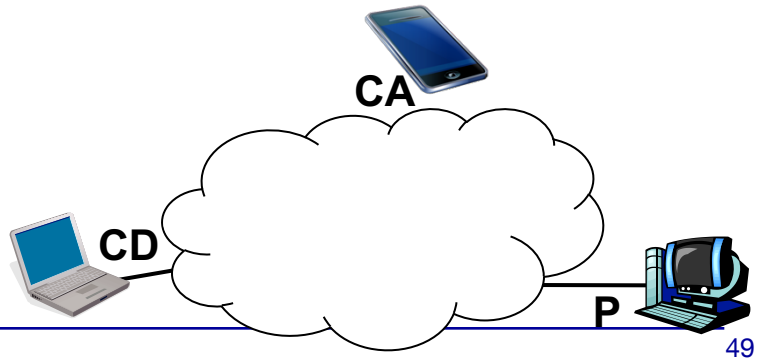
IP mobility: summary

- A mobile has
  - a home-agent, and
  - a permanent home IP address
- When a mobile moves to a new location,
  - Obtain a new care-of address
  - Informing its home agent of its new IP address
- Indirect routing: A correspondent sends data to a mobile's home address, the home-agent forward data to the mobile's care-of address
- Direct routing: correspondent obtains mobile's care-of address, sends packet to mobile directly

Mobility via indirect routing

- correspondent sends data to the mobile's home agent
  - Source = CD; destination = P (mobile's permanent address)
- Home agent tunnels data to mobile
  - Outer IP header: Source = P; destination = CA
  - Inner IP header: source = CD; destination = P
- Mobile tunnels data to correspondent
  - Outer header: Source = CA; destination = CD
  - Inner header: source = P; destination = CD
- Supports mobile movement transparently
  - No change to transport protocols
  - Cost: triangle routing

P = mobile's Permanent home address
CA = Care-of Address
CD = CorresponDent address



Security Threats

- Wireless technology doesn't remove any old security issues, but introduces new ones
  - Viruses, Trojans and stuff like that are still there
  - Eavesdropping
  - Man-in-the-middle attacks
  - Denial of Service

Eavesdropping

- Easy to perform, almost impossible to detect
- By default, everything is transmitted in clear text
  - Usernames, passwords, content ...
  - No security offered by the transmission medium
- Different tools available on the internet
  - Network sniffers, protocol analysers . . .
  - Password collectors
- With the right equipment, it's possible to eavesdrop traffic from few kilometers away

Man in the middle attacks

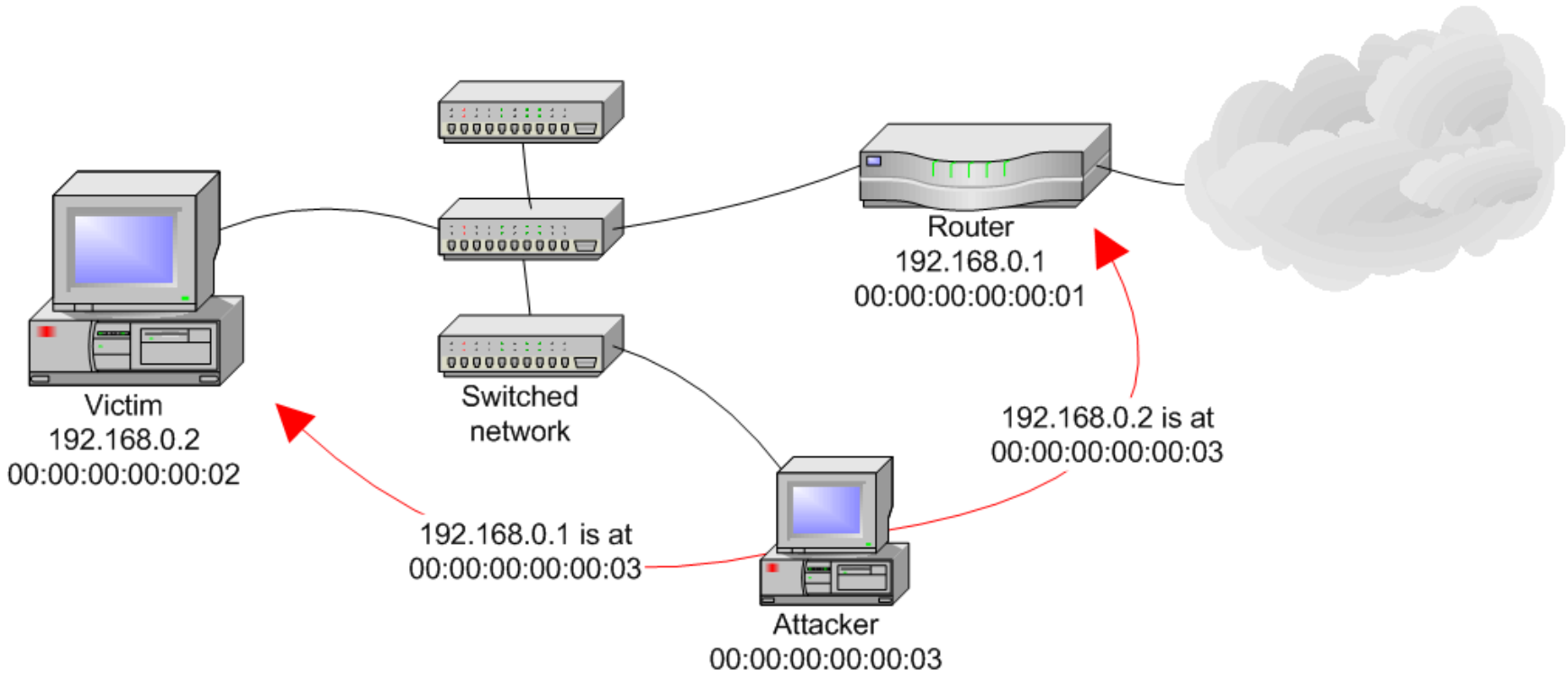
- In a MITM attack, the attacker funnels victim's traffic through a point controlled by the attacker

- Allows data analysis and manipulation
  - Tools available on the internet

- Can target secure higher level protocols

- MITM attacks are also possible in wired networks

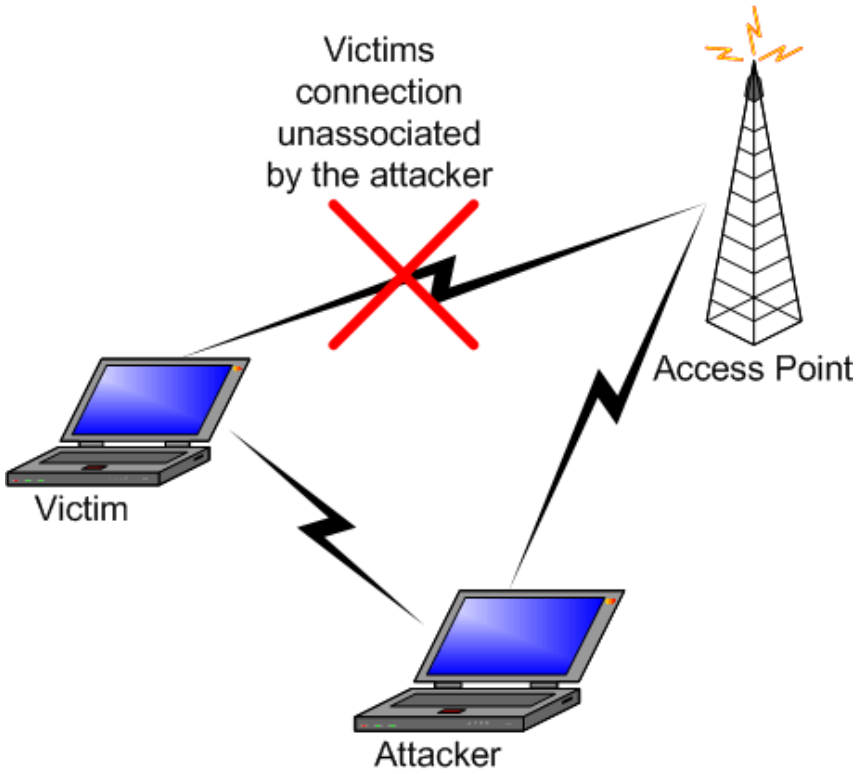
Man in the middle attacks



The attacker can terminate victim's SSL/TSL session at her host and reconnect
to the actual site. This allows the attacker to see everything in clear text

Wireless MITM Attack

1. Attacker spoofes a disassociate message from the victim
2. The victim starts to look for a new access point, and the attacker advertises his own AP on a different channel, using the real AP's MAC address
3. The attacker connects to the real AP using victim's MAC address



Denial of Service

- Frequency jamming
  - Not very technical, but works
- Spoofed deauthentication / disassociation messages
  - can target one specific user
- Attacks on higher levels
  - SYN Flooding
  - Ping of death
  - ...

End !!!

802.11 frame: more detail

FYI