CS118 Discussion 1B, Week 10

Zhehui Zhang
HAINES A2 / Friday / 12:00pm-1:50pm

Logistics

- Final Exam: Monday 6:30pm-9:30pm
  - Roughly 20% before midterm, 80% after midterm
  - Closed book & notes, allow up to 2 double-sided cheat sheets
- Sign up for Project 2 demo!!
- ***Please complete course evaluation on MyUCLA, thanks!***

Wireless and Mobile Network

- Wireless access: WIFI
  - CSMA/CA VS. CSMA/CD
  - RTS/CTS mechanism
- Mobility: MobileIP
  - Home network, visited network
  - Permanent address VS. care-of-address
  - Indirect (triangle) routing VS. direct routing
- Wireless and mobility are not necessarily correlated
  - Wireless without mobility?
  - Mobility without wireless?

Wireless network

- Infrastructure mode vs. ad-hoc mode
- Problems:
  - multiple access
  - hidden terminal
  - signal attenuation

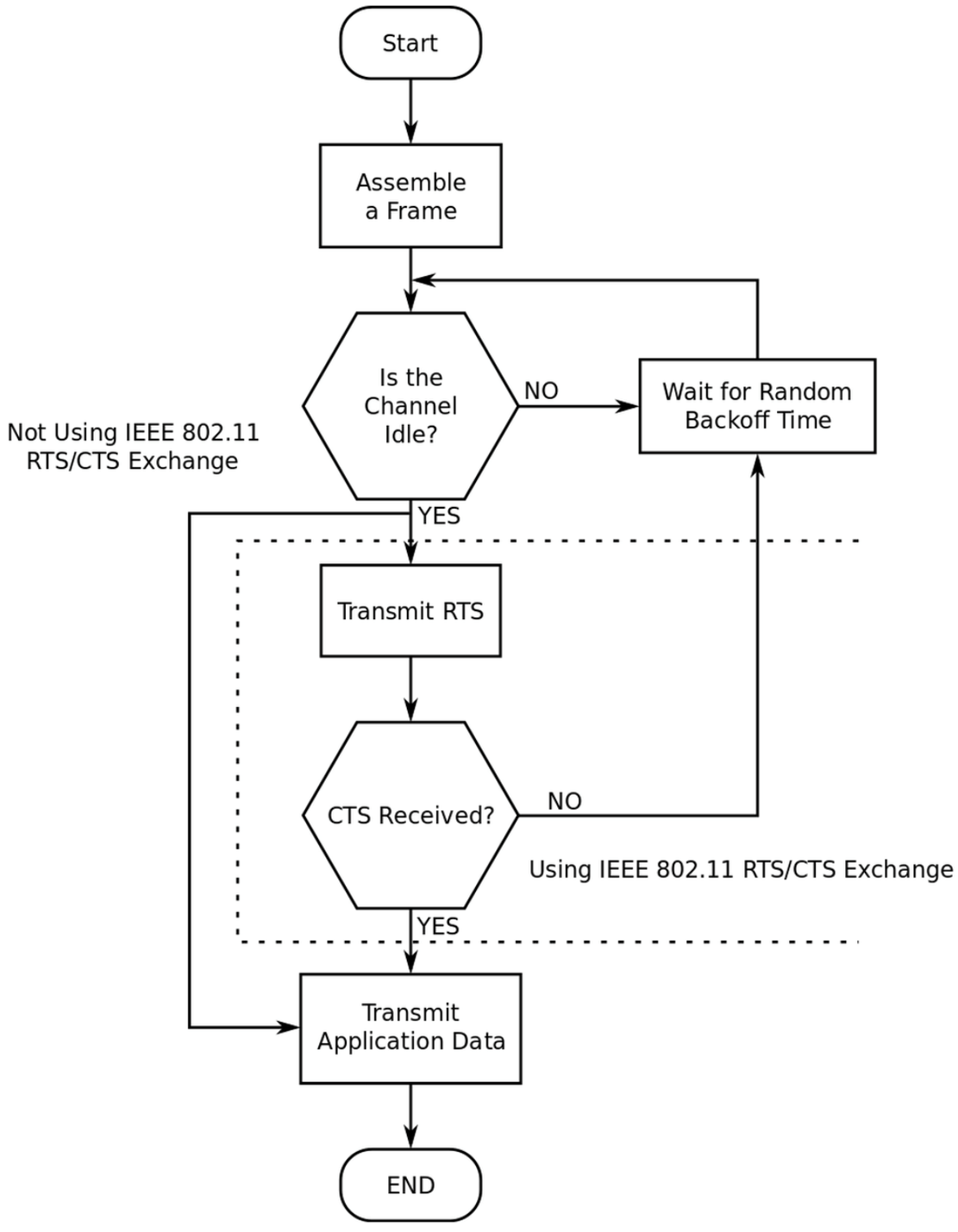
802.11: CSMA/CA

- 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**

802.11: CSMA/CA

- Allow sender to “reserve” channel: avoid collisions of long data frames
- 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)
- AP broadcasts clear-to-send (CTS) in response to RTS
- CTS heard by all nodes within AP's range
  - sender transmits its data frame
  - other stations defer transmissions

802.11: CSMA/CA



802.11: mobility, security

- Mobility: within same subnet (under the same switch)
- Security:
  - Wired Equivalent Privacy (WEP)
    - weak-n-flawed, not usable
  - 802.1X Access Control
  - Wireless Protected Access (WPA), WPA2

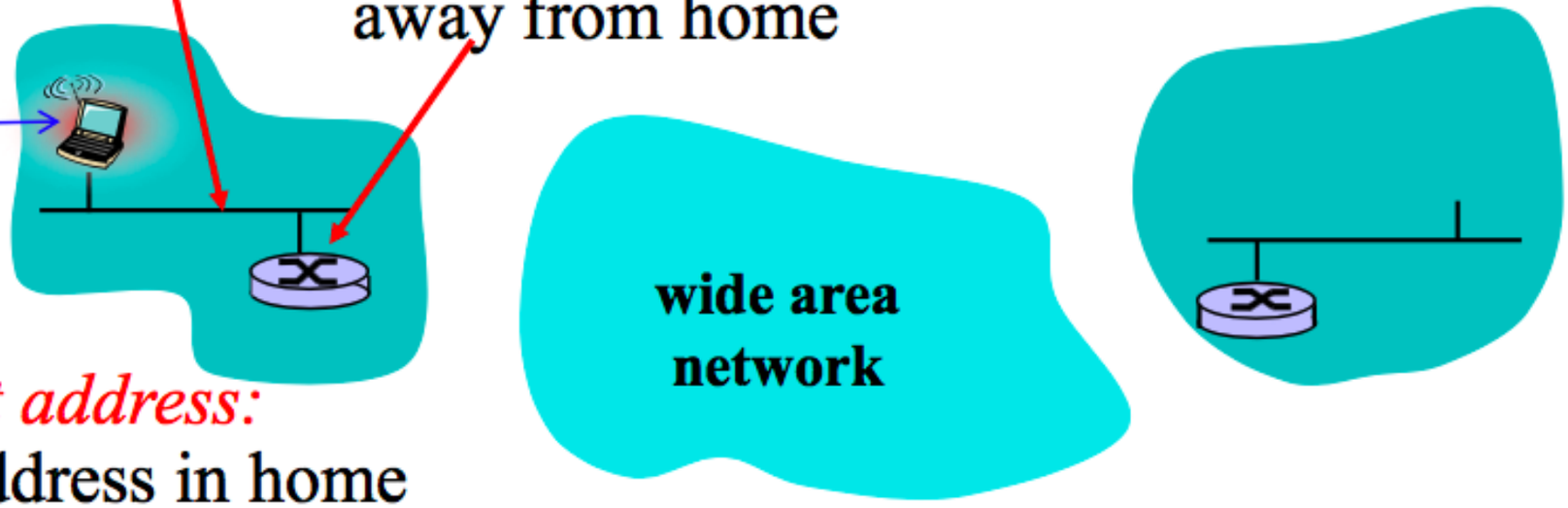
Mobile IP

- Home network, visited network
- Permanent address vs. care-of-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 vs. direct routing
  - 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

Mobile IP: Vocabulary (I)

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

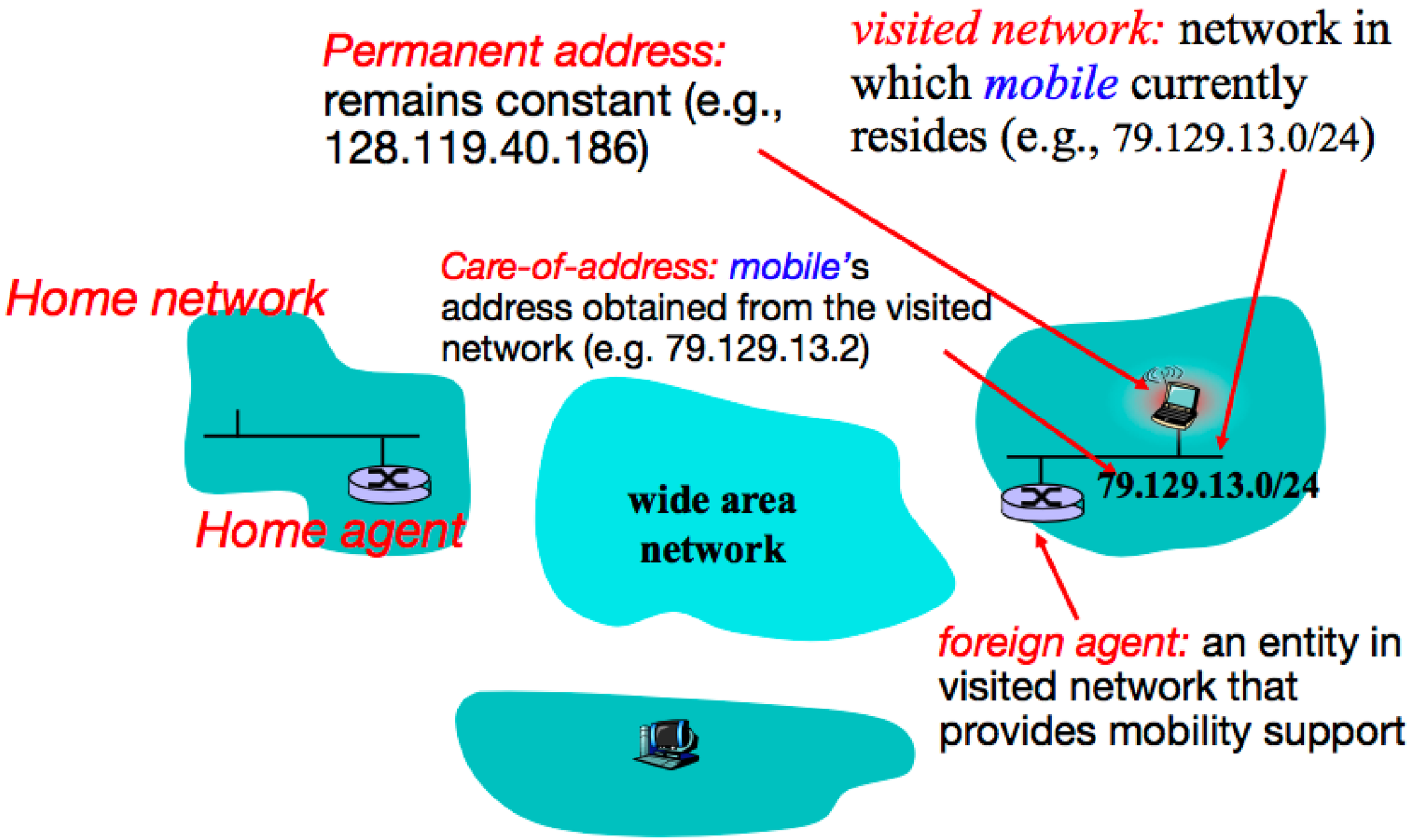
home agent: entity that will perform mobility functions on behalf of *mobile* when *mobile* is away from home



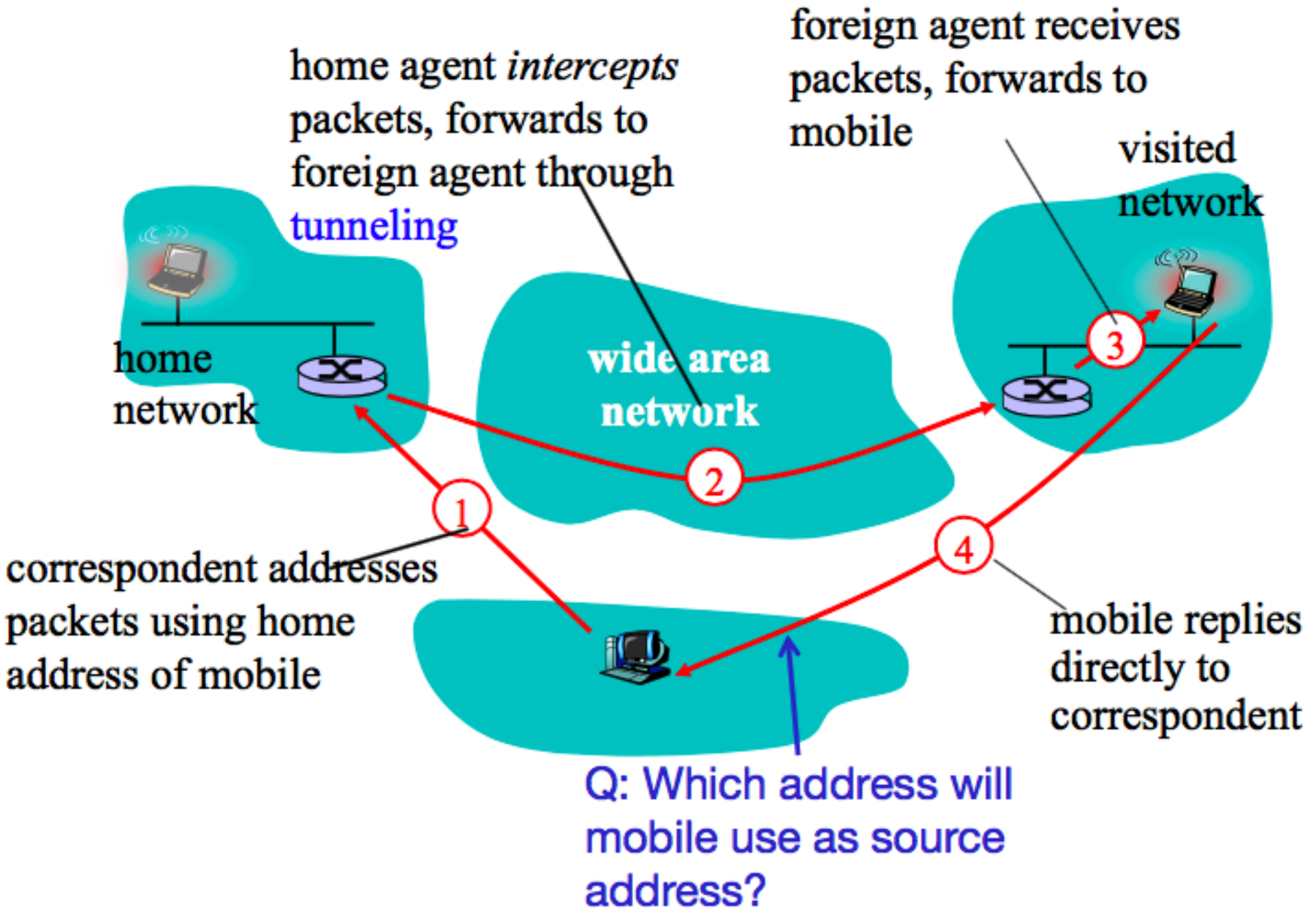
Permanent address: *mobile*'s address in home network, *can always* be used to reach *mobile* (e.g., 128.119.40.186)

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

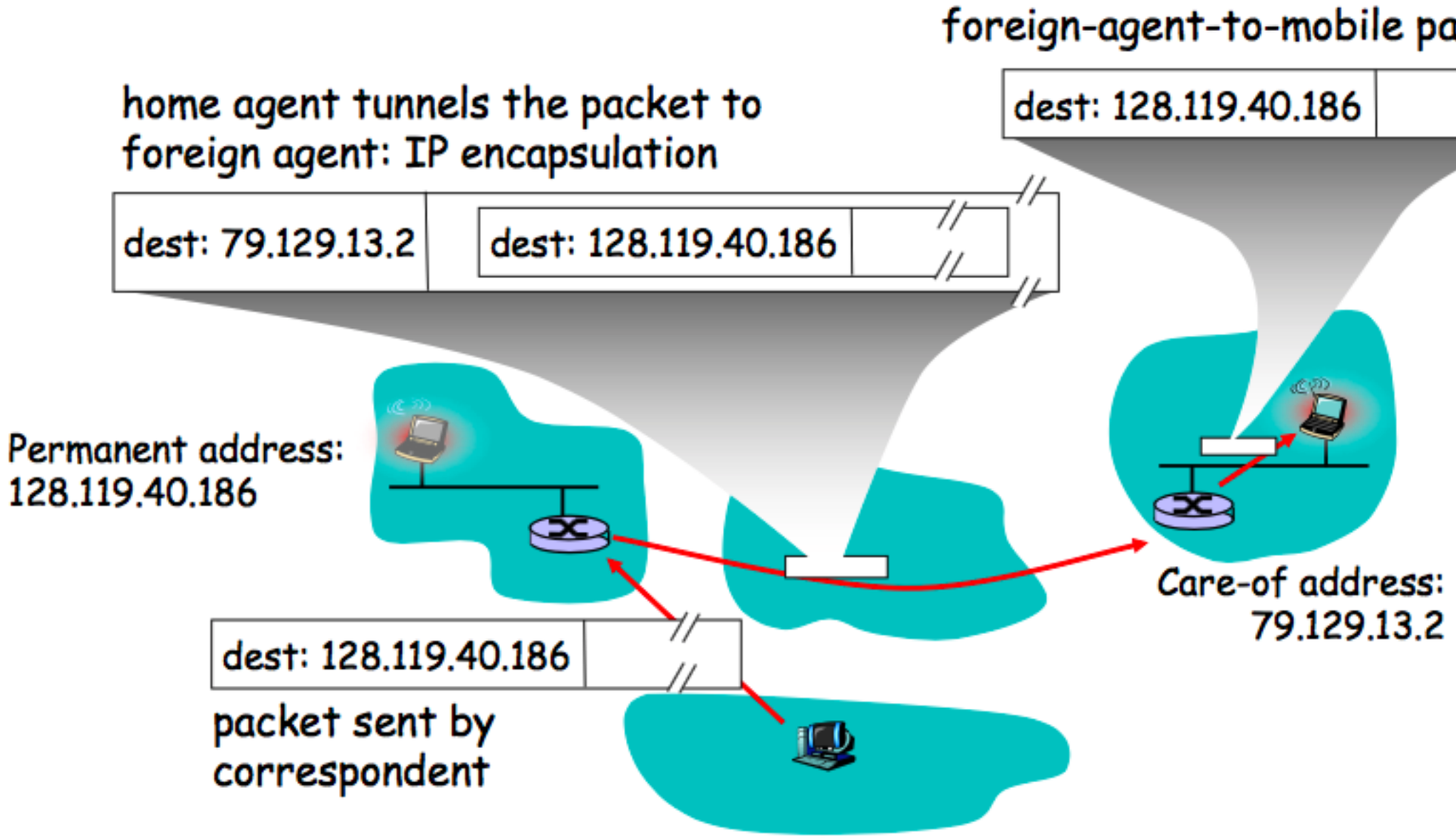
Mobile IP: Vocabulary (II)



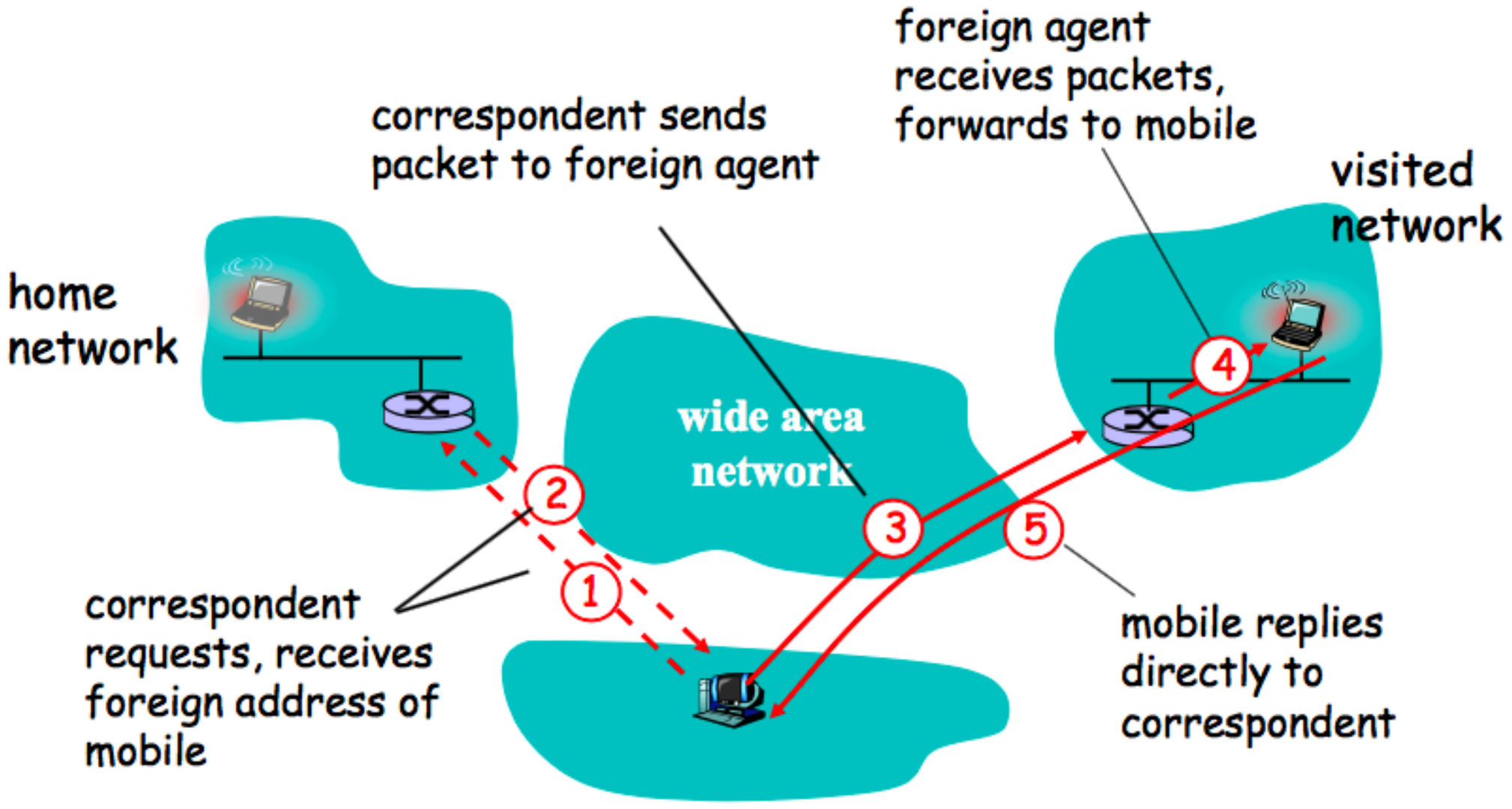
Mobile IP: Indirect Routing (I)



Mobile IP: Indirect Routing (II)



Mobile IP: Direct Routing



Good: Eliminate triangle routing problem

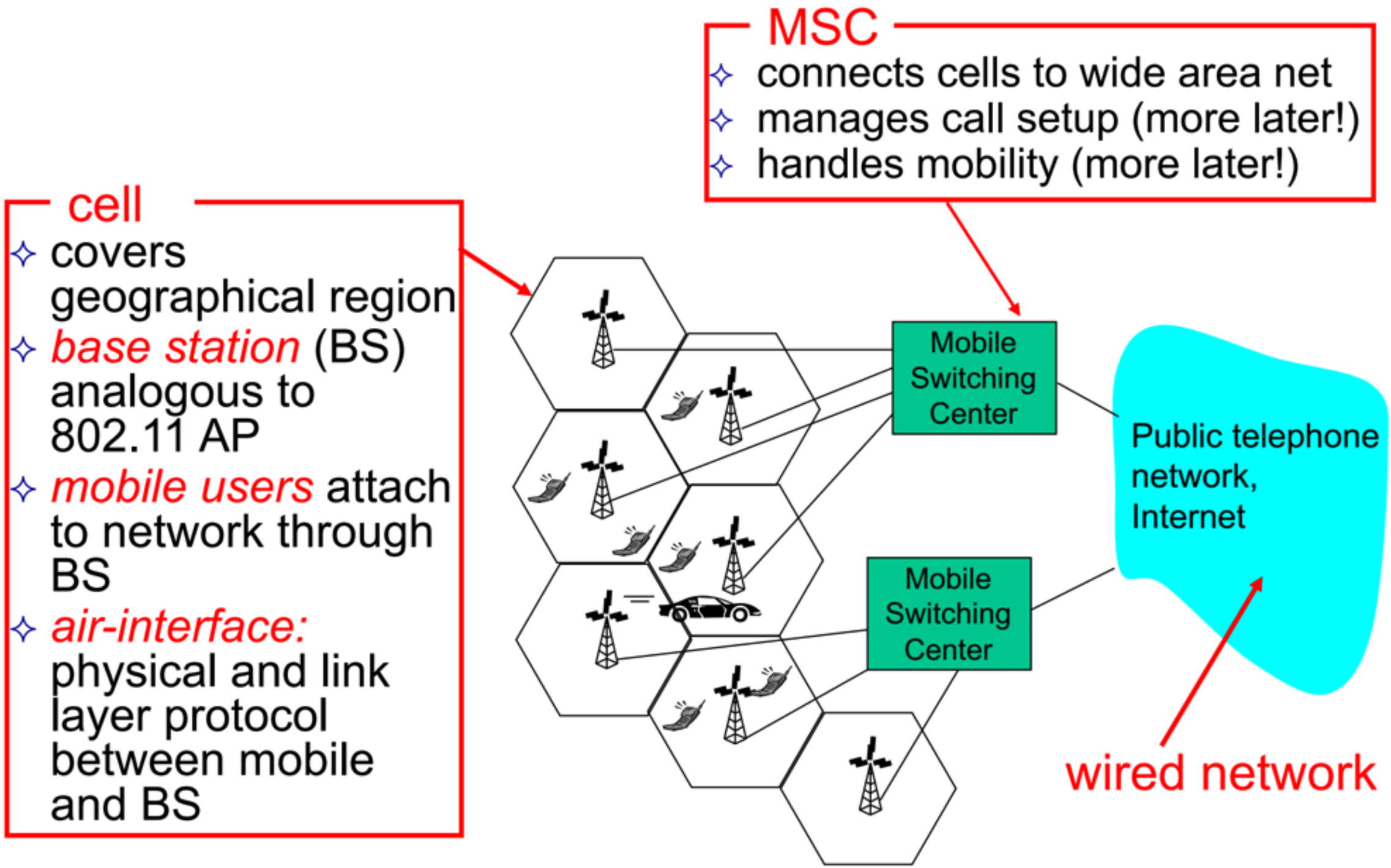
Bad:

- Correspondent must be aware of mobility support
- what if mobile moves from network to network?

Mobile IP: Indirect Routing Summary

- 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

Cellular Network: Basic Components



Cellular Network and Mobility

- 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

Mobility: Cellular v.s. MobileIP

cellular element	Comment on cellular element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. HLR: database in home system containing permanent phone number, profile information, current location of mobile user, subscription information	**Home agent**
Visited System	Network other than home system where mobile user is currently residing	**Visited network**
Visited Mobile services Switching Center. Visitor Location Record (VLR)	Visited MSC: responsible for setting up calls to/from mobile nodes in cells associated with MSC. VLR: temporary database entry in visited system, containing subscription information for each visiting mobile user	**Foreign agent**
Mobile Station Roaming Number (MSRN), or "roaming number"	Routable address for telephone call segment between home MSC and visited MSC, visible to neither the mobile nor the correspondent.	**Care-of-address**

Network security principles

- Confidentiality
- Authentication
- Integrity
- Access and availability

Corresponding security threats

- Eavesdropping
- Impersonation
- Hijacking/MITM Attack (Man-in-the-middle attacks)
- DoS (Denial of Service)

Courtesy: Alex Afanasyev

Key-based cryptography

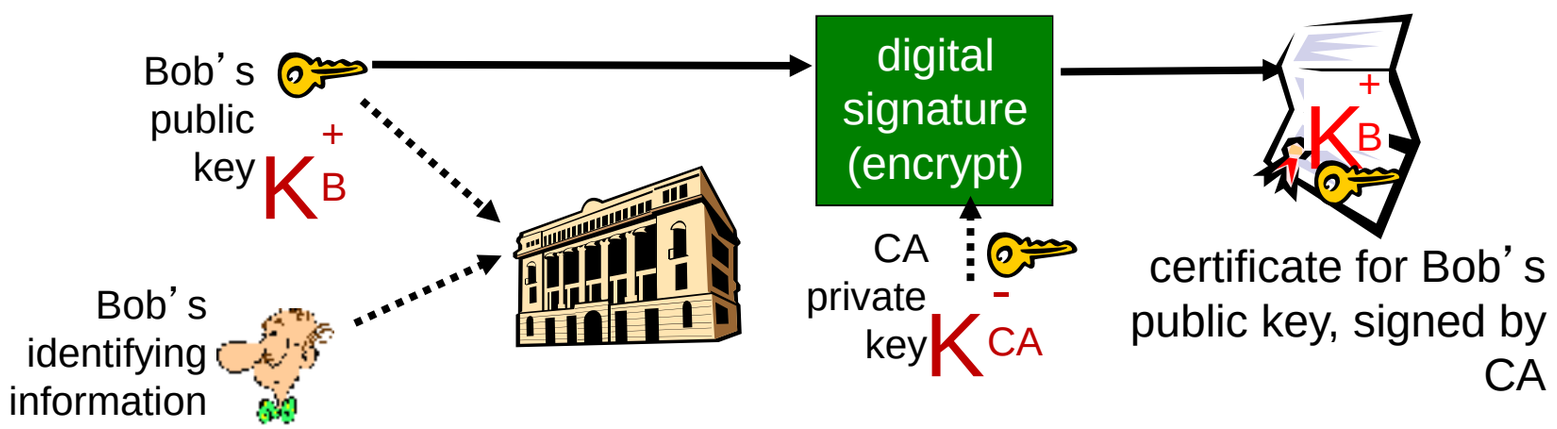
- Symmetric key crypto: DES, AES
- Asymmetric key crypto:
  - Diffie-Hellman [2015 Turing Award], RSA [2002 Turing Award]
  - pubkey, private key

Authentication: digital signatures

- Verifiable, non-forgeable
- Hash functions:
  - MD5
  - SHA-1
- Digital signature: ***signed*** message digest
- CA (certificate authority)

How CA works

- Certification authority (CA): binds public key to particular entity, E.
  - E (person, router) registers its public key with CA.
  - E provides “proof of identity” to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E’s public key digitally signed by CA – CA says “this is E’s public key”



More things to know

- IPSec (network layer), VPN, Firewall, IDS …
- How to achieve:
  - Encryption
  - Authentication
  - Digital signature
  - Message integrity

Exercise

- What are the security mechanisms to defend against the following network attacks?
  - Data sniffing & interception
  - IP address spoofing
  - Replay attack
  - Man in the middle attack
  - Email spam
  - Illegal access to UCLA campus network