CS118 Discussion 1C, Week 10

Zengwen Yuan

Bunche Hall 3156, Friday 2:00—3:50 p.m.

Logistics

- Final Exam: Monday, 6/10, 6:30 pm – 9:30 pm in Franz Hall 1260
    - Roughly 20% before midterm, 80% after midterm — refer to study guide for detailed chapters
    - 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: Wi-Fi
  - CSMA/CA vs. CSMA/CD
  - RTS/CTS mechanism
- Mobility: MobileIP
  - Home network, visited network
  - Permanent address, care-of-address
  - Indirect (triangle) routing, direct routing
- Wireless and mobility are not necessarily correlated
  - Wireless without mobility?
  - Mobility without wireless?

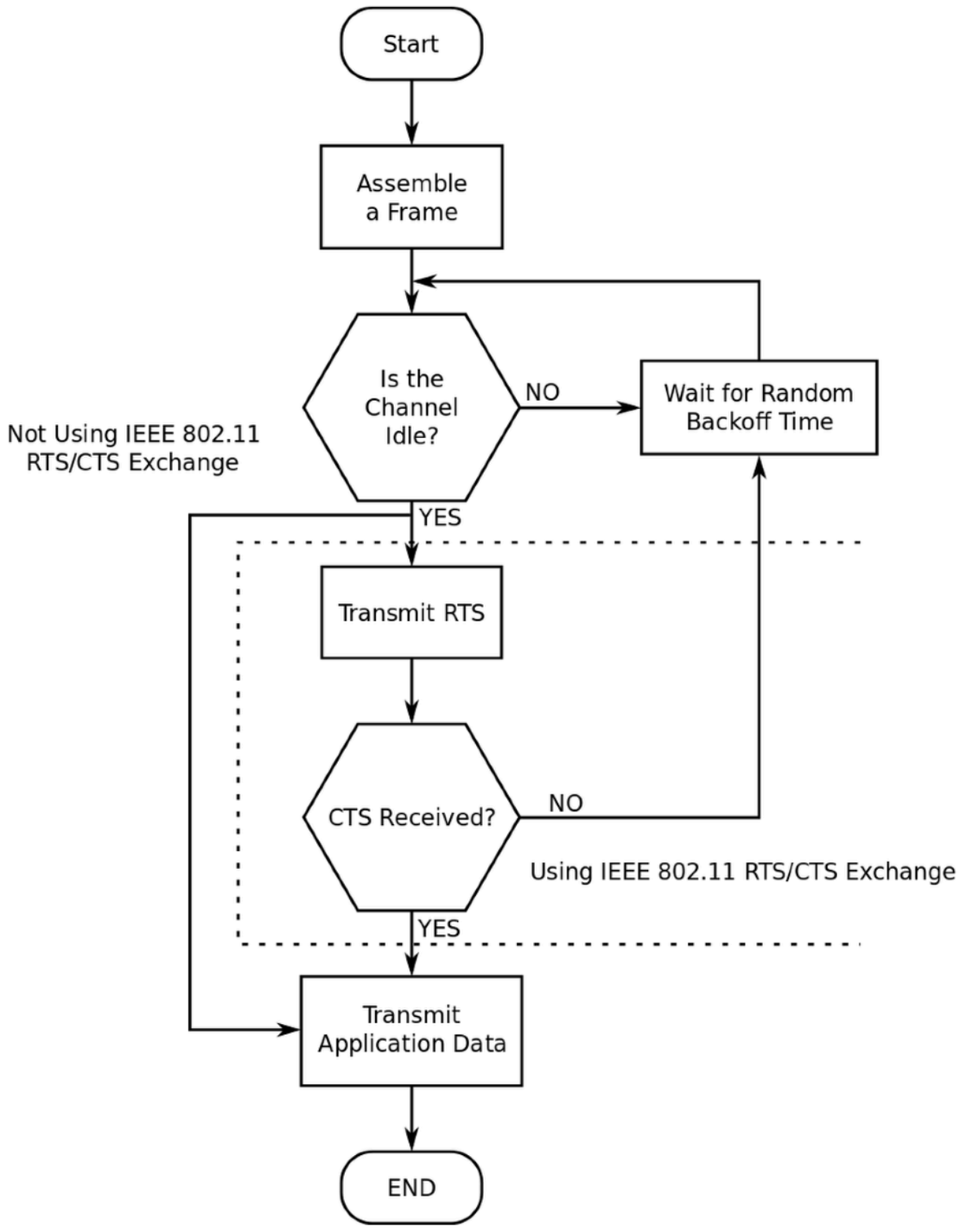
Wireless network

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

802.11: CSMA/CA

- 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

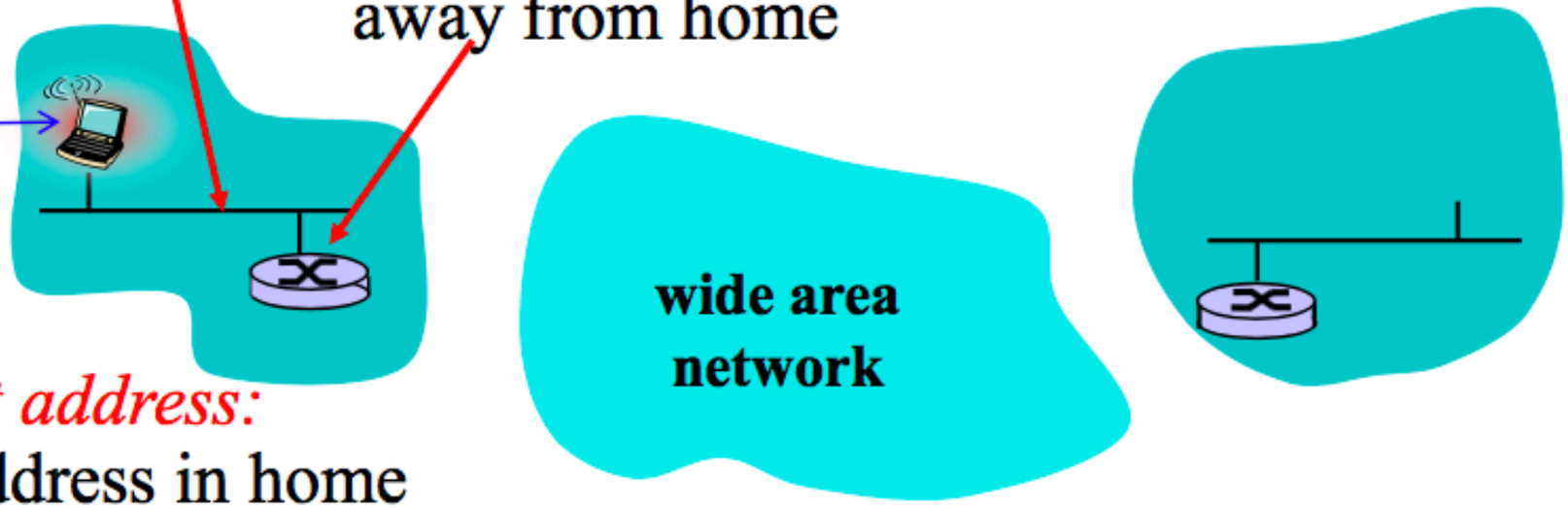
Mobile IP

- 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*

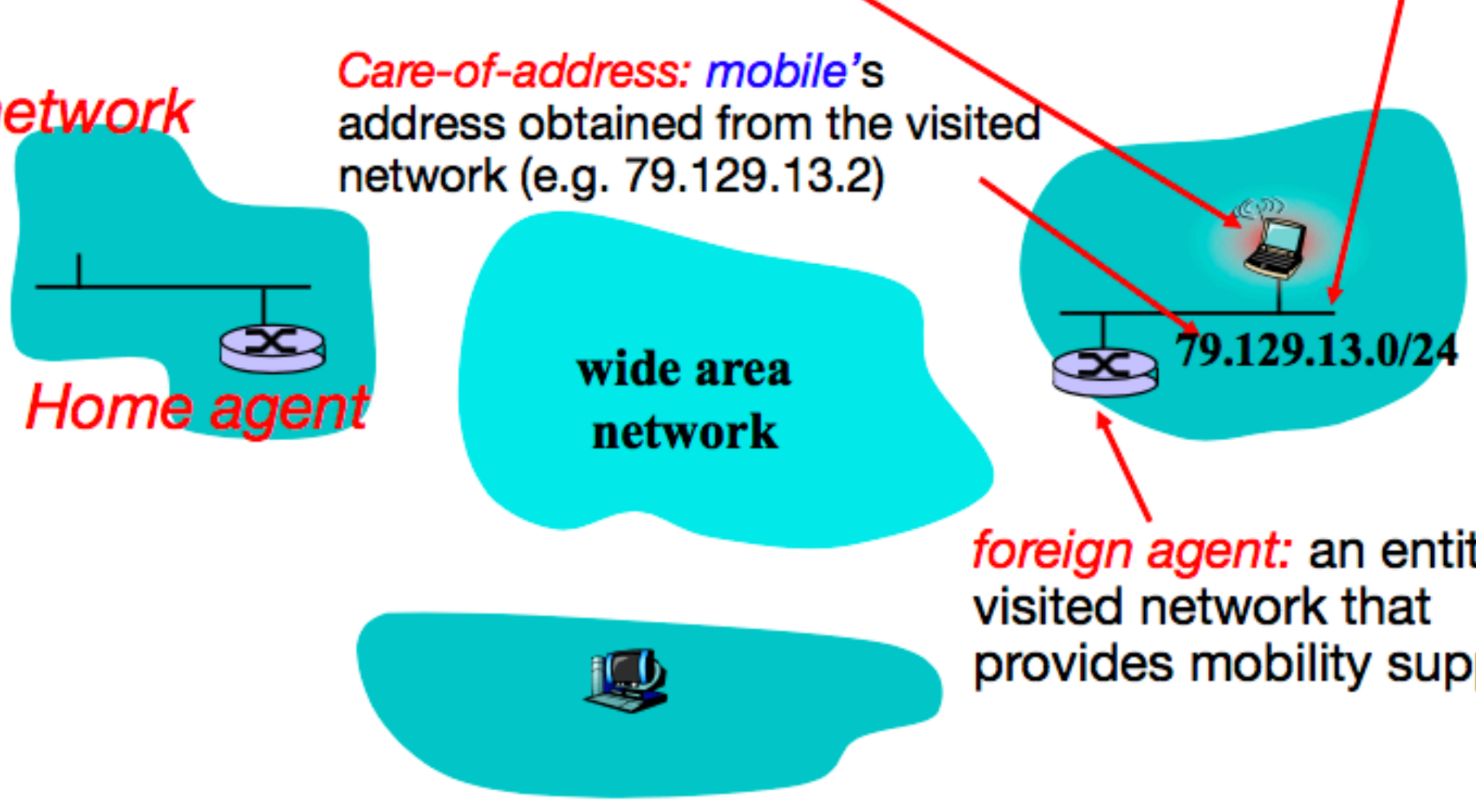
Mobile IP: Vocabulary (II)

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)

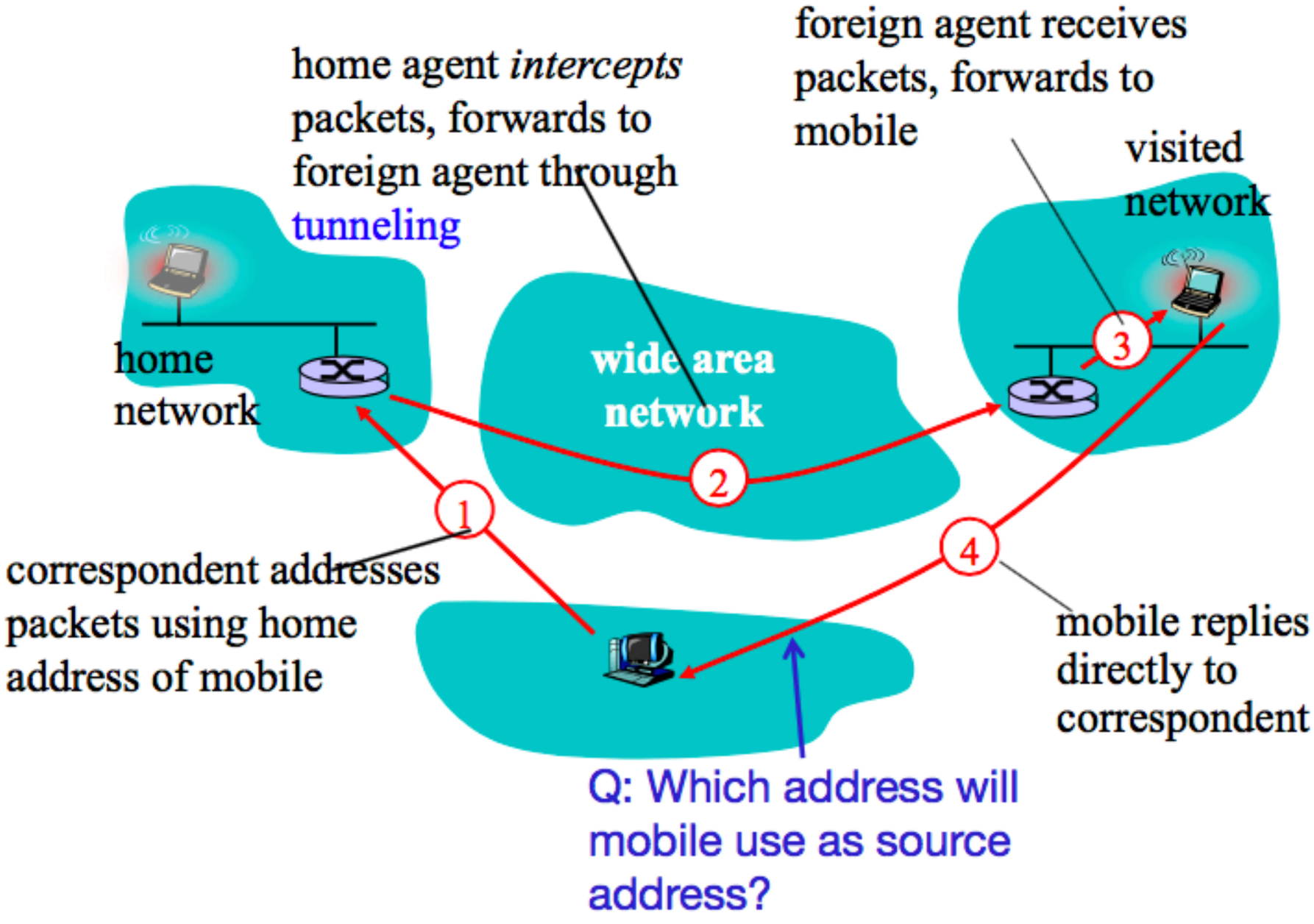
Home network

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

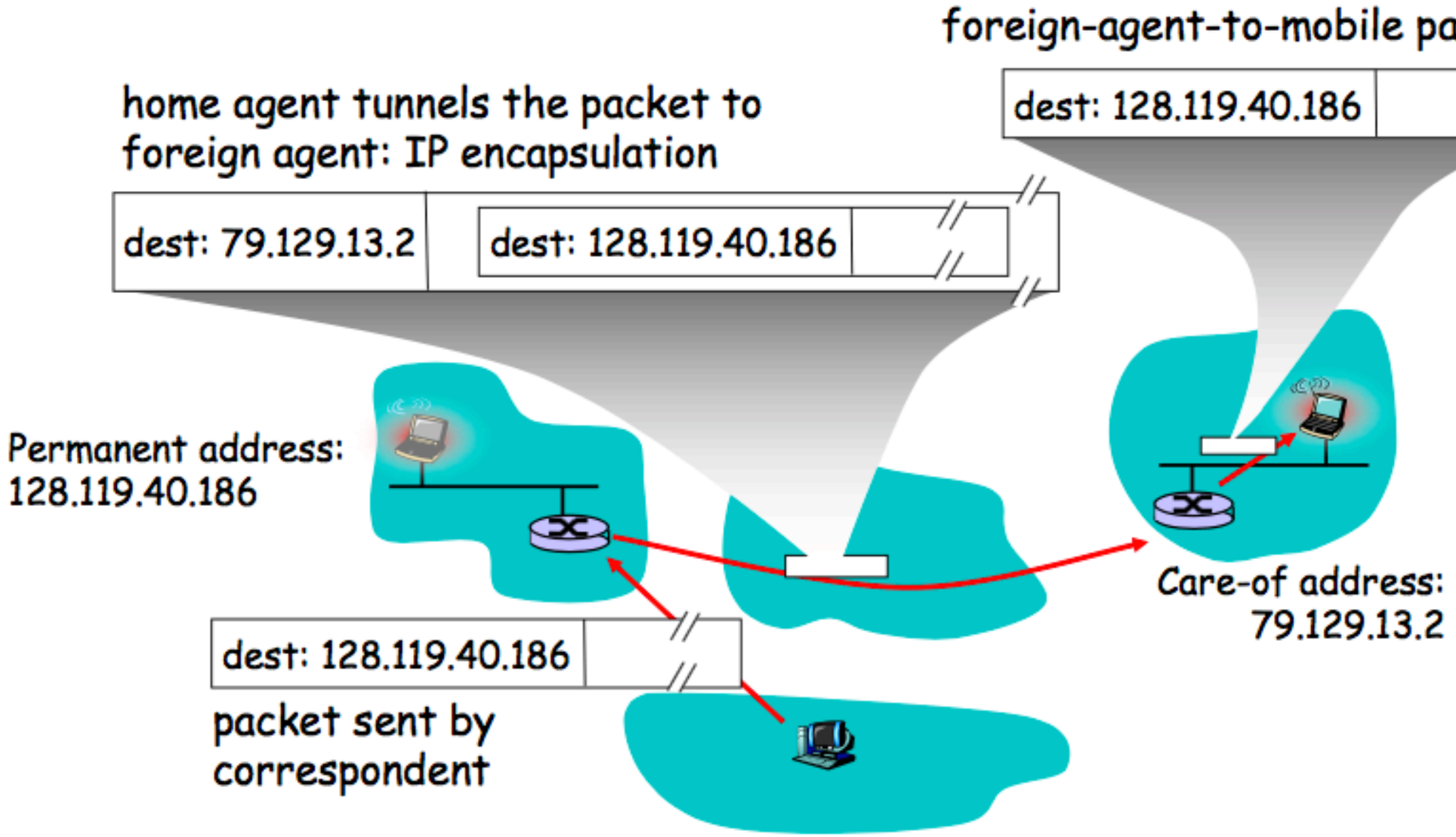


foreign agent: an entity in visited network that provides mobility support

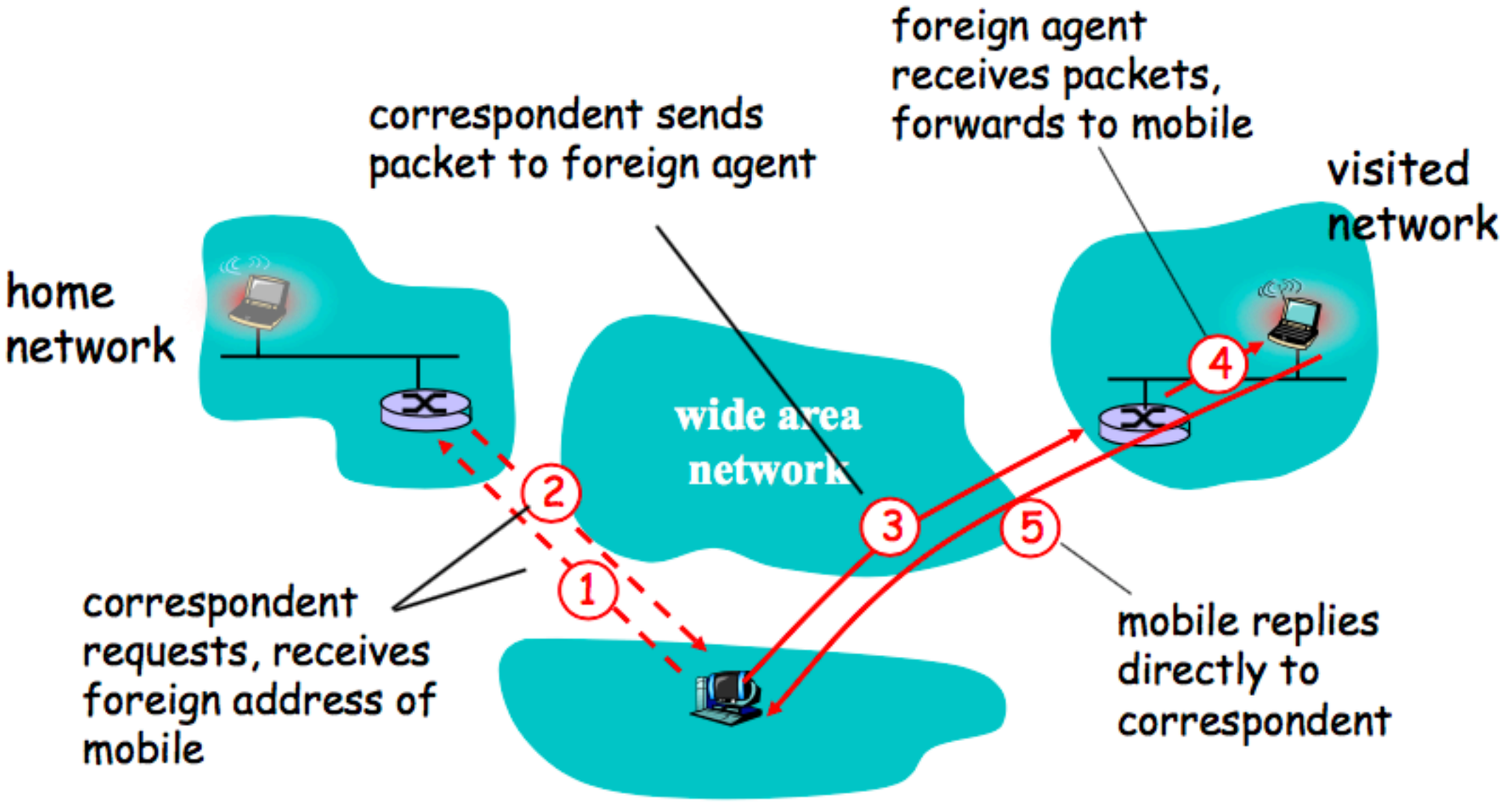
Mobile IP: Indirect Routing (I)



Mobile IP: Indirect Routing (II)



Mobile IP: Direct Routing



Good: Eliminate triangle routing problem

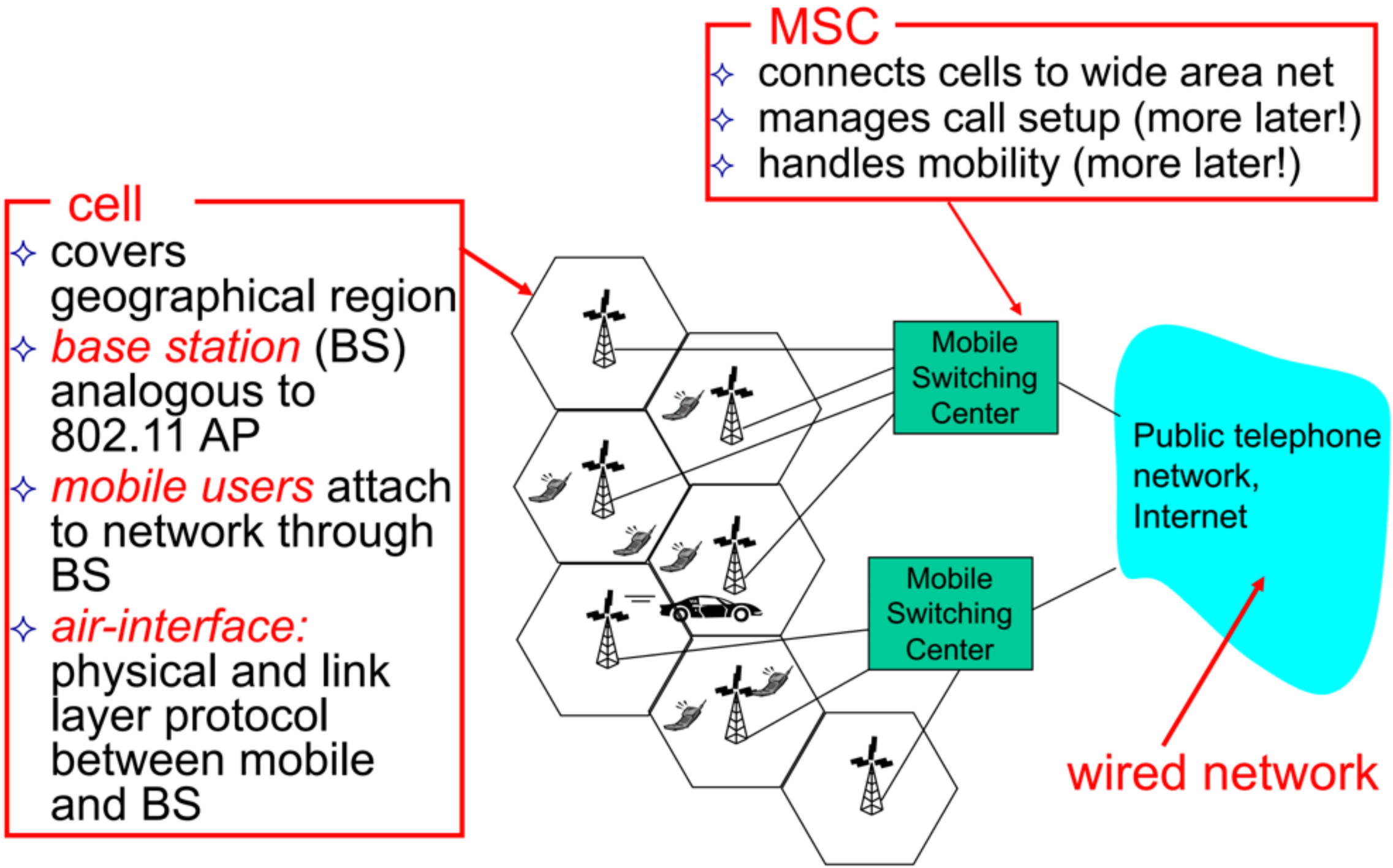
Bad:

- 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

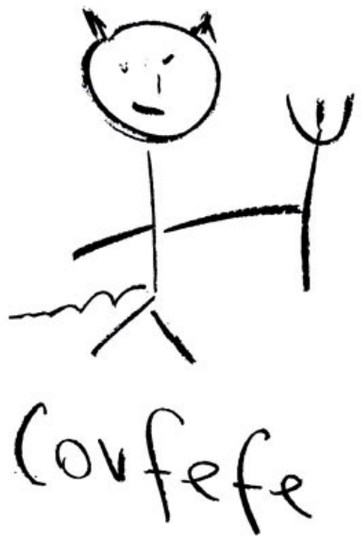


Network security principles

- 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)

SSL: Secure Sockets Layer

- A transport layer protocol (it sits between TCP and Application)
  - variation: TLS protocol
- Benefit: confidentiality, integrity, authentication
- Main steps
  - handshake
  - key derivation
  - data transfer
  - connection closure

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
  - (Distributed) denial of service attack
  - Email spam
  - Illegal access to UCLA networks
  - Network virus

Study guide & Project 2

Week 1

- Big Picture - Different Layers
    - Application
    - Transport
    - Network
    - Link
    - Physical
- Application layer architectures
    - Client-Server
    - P2P
- Socket Programming
- HTTP
    - Headers
    - Request
    - Response

Week 2

- HTTP
    - Persistent vs Non Persistent
    - Pipelining
    - Parallel Connections
    - Stateful and Stateless protocols
    - Cookies
    - Web Caching - CDN
- Email
    - SMTP
    - Securing Email - PGP / GPG
    - Mail Access protocols: POP, IMAP, HTTP

Week 3

- DNS
  - Architecture
  - Records
  - Query/Reply
  - Dig - Example in homework
- CDN - Akamai
- Client-Server vs P2P architecture: Pros and Cons
- Bit-Torrent
- Internet Video
  - Rate Control
  - Error Control

Week 4

- Transport Layer
    - TCP
    - UDP
    - Multiplexing and Demultiplexing
- UDP
    - Headers
    - Checksum
- Reliable Data Transfer
    - Sequence #
    - Acknowledgement
    - Retransmission timer
- TCP
    - Header
    - Handshake and teardown
    - Flow control

Week 5

- Setting TCP Retransmission timer
  - SampleRTT, SRTT, DevRTT, RTO
  - Karn’s Algorithm
- Fast Transmit
- Congestion Control
  - Slow Start
  - Congestion Avoidance
- TCP Throughput

Week 6

- Network Layer
- Routing and Forwarding
- VC and Datagram
- IP Datagram format
- IP Fragmentation
- Subnet
- Special Addresses
- Longest prefix Matching
- NAT - Network Address Translation
- DHCP

Week 7

- IPv6 vs IPv4
- Tunneling
- ICMP
- Traceroute
- Routing Algorithms
  - Link State
  - Distance Vector
- Count to Infinity
- OSPF Protocol
- Hierarchical architecture - Autonomous Systems
- BGP: i-BGP, e-BGP

Week 8

- Named Data Networking (NDN) - Not in exam
- Link Layer: Unicast, Broadcast, Multicast
- Where is LL implemented
- Byte Stuffing — HDLC, PPP, COBS
- Multiple Access Protocols
  - Channel Partitioning — FDM, TDM, CDMA
  - Random Access — Aloha, Slotted Aloha, CSMA
  - Taking Turns — token ring
- Efficiency of Aloha, Slotted Aloha
- Binary Exponential backoff
- 1-persistent, p-persistent, non-persistent CSMA

Week 9

- Ethernet - Bus and Star Topology
- MAC Address
- Ethernet frame structure
- ARP: IP Address to MAC Address
- Plug and Play
- Soft State
- Difference between hub, switch, router
- Switches - Forwarding Table
- Self Learning
- Advantages and Disadvantages of Routers and Switches

Week 10

- Wireless and mobile
- Infrastructure and ad-hoc mode
- Hidden Terminal and Fading
- 802.11 LAN Architecture
- Passive and Active Scanning
- CSMA/CA
- Mobility within subnet
- Indirect and direct routing
- Security Threats
- Cellular Networks
- IPSec
- VPNs