CS118 Discussion 1B, Week 10

Boyan Ding

Outline

- Security
- Wireless: 802.11
- Mobile IP
- Cellular Networks: LTE
- A day in the network

Quiz 3 - logistics

- Time: 11:30am-10pm (PDT), Friday, June 11
    - Choose 2.5h within to finish the exam
- Covered material: All remaining chapters after quiz 2 (Refer to the study guide on CCLE for details)
- Format: similar to quiz 1 & 2

Security

- Attacks:
  - Spoofing attach
  - Playback/Replay attack
  - Man in the middle attack
- Defenses:
  - Digital signature
  - Nonce
  - Certificate authorities

Security solutions

- Solutions at different layers:
    - Network layer security: IPsec
        - Example: VPN
    - Transport layer security: SSL
- Other solutions:
    - Firewalls
        - Limitation: vulnerable to IP spoofing
    - IDS (intrusion detection system)

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

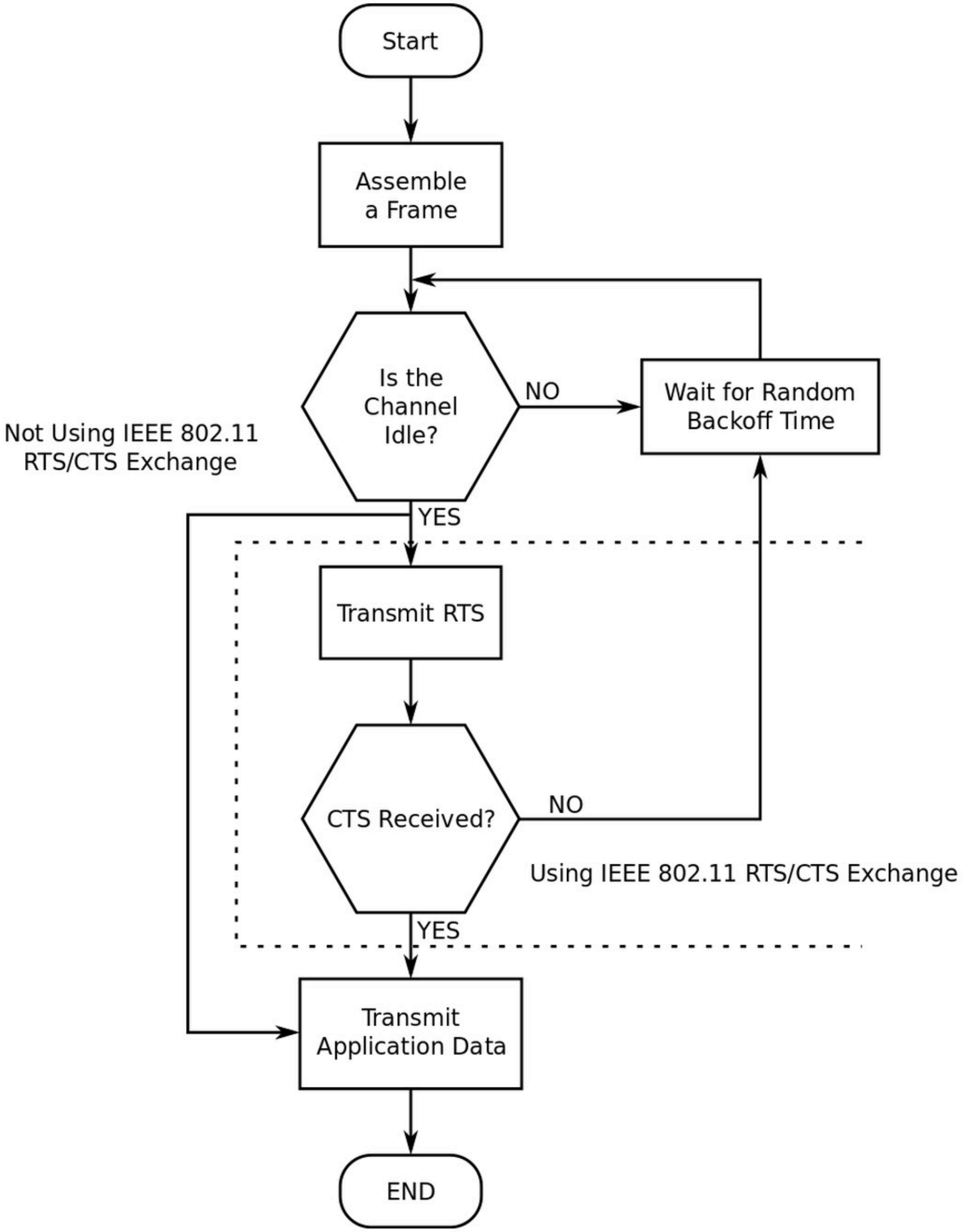
802.11: CSMA/CA

- 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


Start
Assemble a Frame
Is the Channel Idle?
NO
Wait for Random Backoff Time
Not Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit RTS
CTS Received?
NO
Using IEEE 802.11 RTS/CTS Exchange
YES
Transmit Application Data
END

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

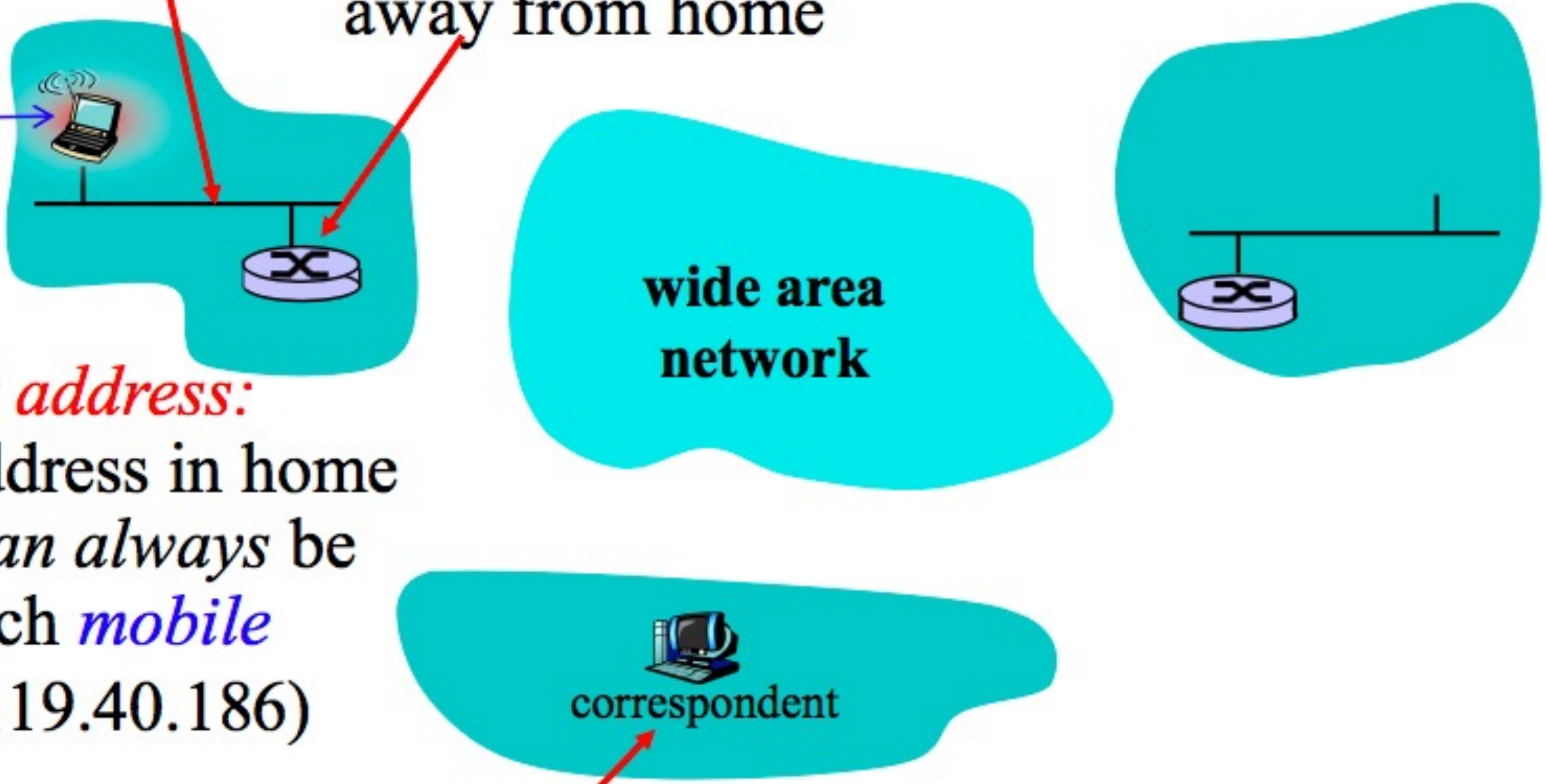
Mobile IP

- 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)

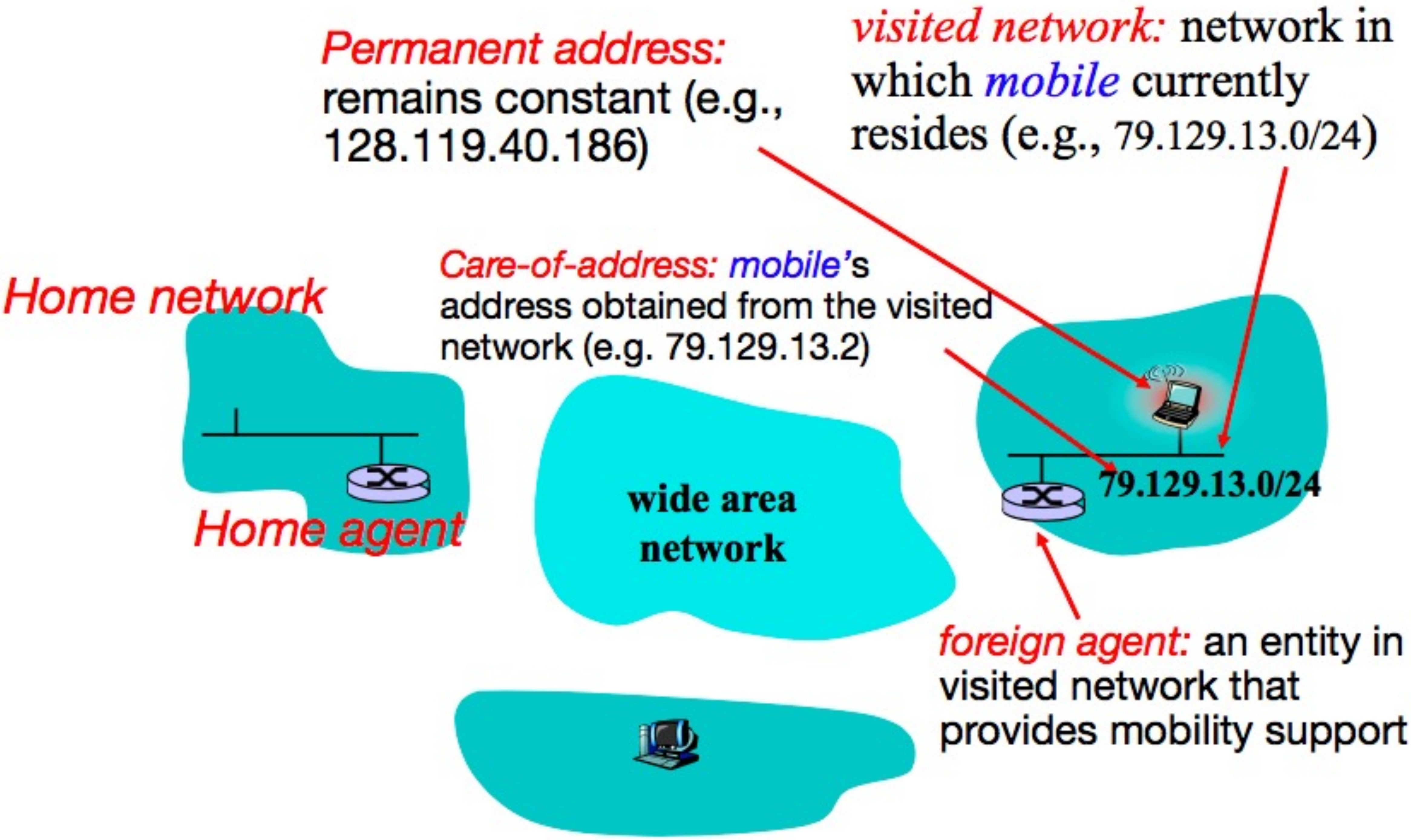
home agent: entity that will perform mobility functions on behalf of *mobile* when *mobile* is away from home



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)



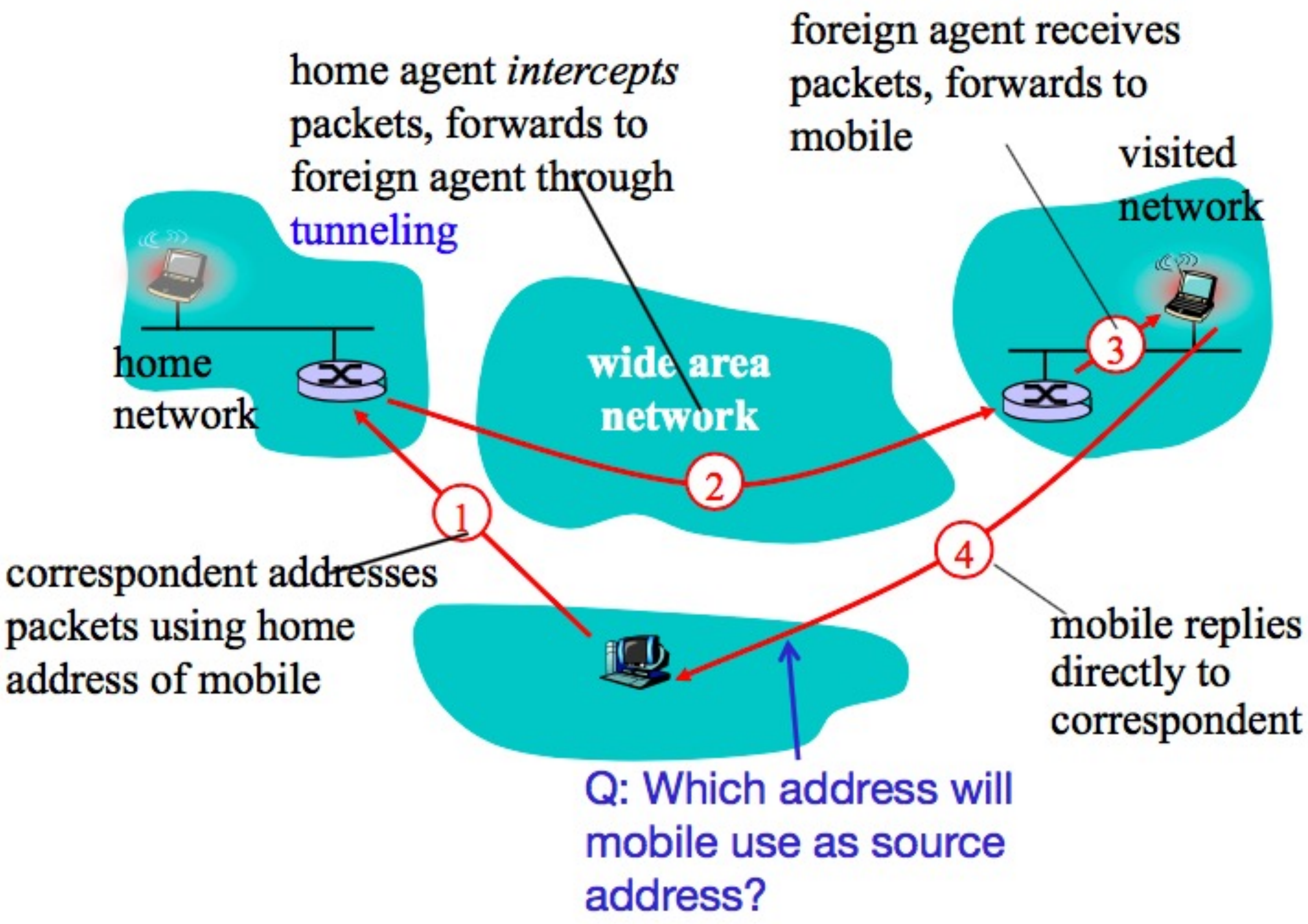
Permanent address: remains constant (e.g., 128.119.40.186)

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

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)



home agent *intercepts* packets, forwards to foreign agent through tunneling

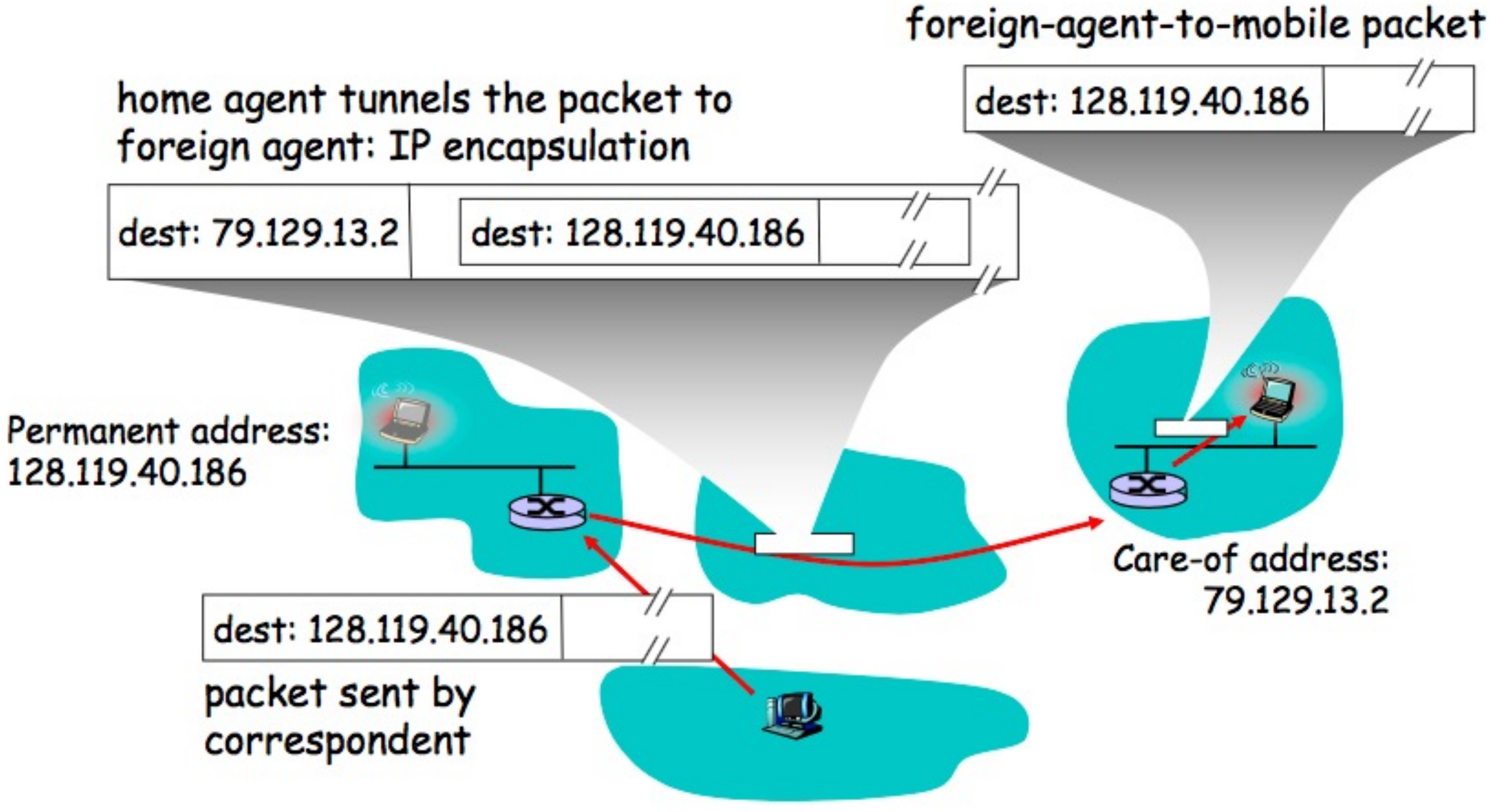
foreign agent receives packets, forwards to mobile

correspondent addresses packets using home address of mobile

mobile replies directly to correspondent

Q: Which address will mobile use as source address?

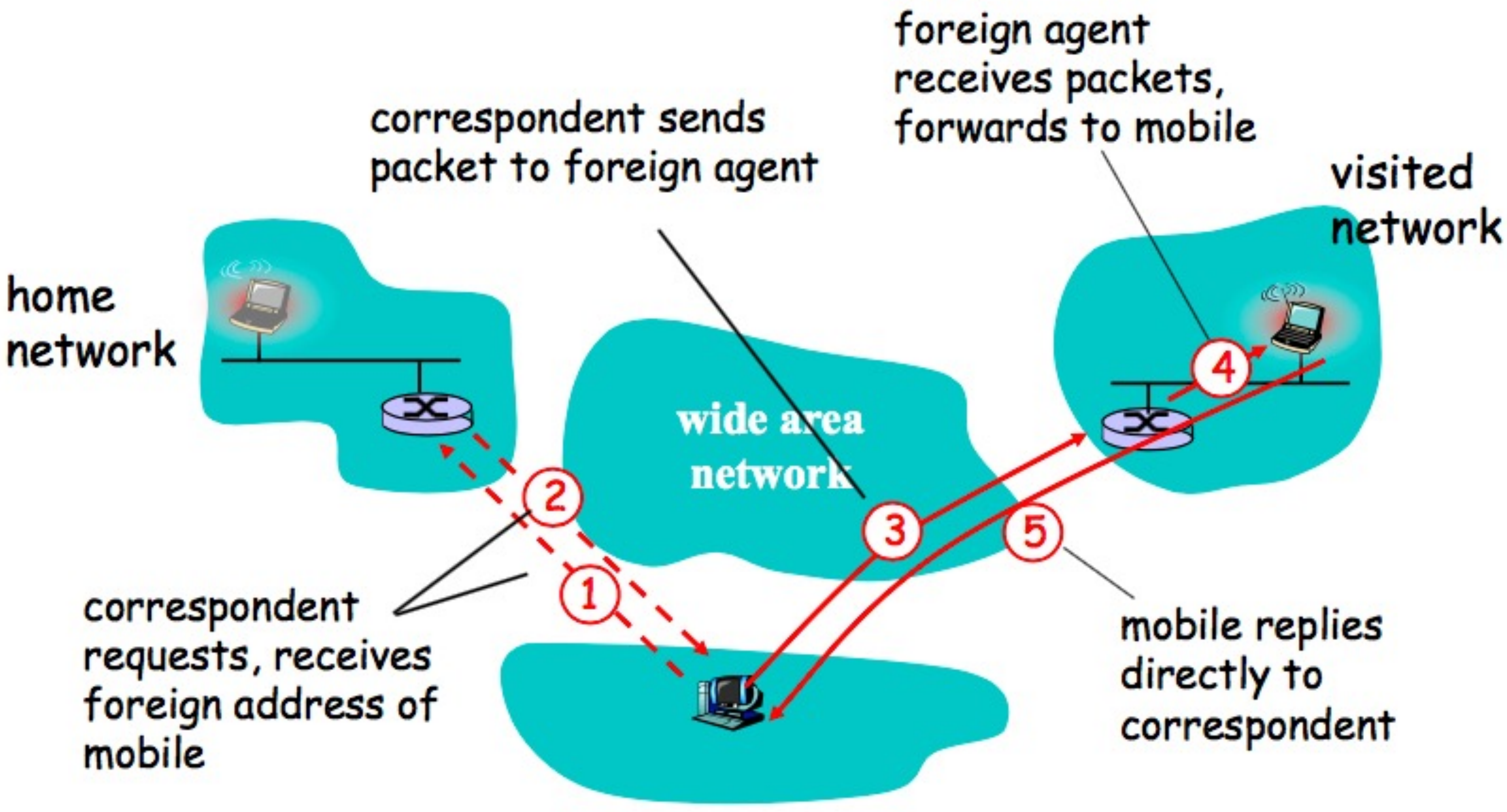
Mobile IP: Indirect Routing (II)


foreign-agent-to-mobile packet
dest: 128.119.40.186
home agent tunnels the packet to foreign agent: IP encapsulation
dest: 79.129.13.2
dest: 128.119.40.186
Permanent address: 128.119.40.186
Care-of address: 79.129.13.2
dest: 128.119.40.186
packet sent by correspondent

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
- Supports mobile movement transparently
  - No change to transport protocols
  - Cost: triangle routing

Mobile IP: Direct Routing


foreign agent receives packets, forwards to mobile
correspondent sends packet to foreign agent
visited network
home network
wide area network
4
2
3
5
1
correspondent requests, receives foreign address of mobile
mobile replies directly to correspondent

Good: Eliminate triangle routing problem

Bad:

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

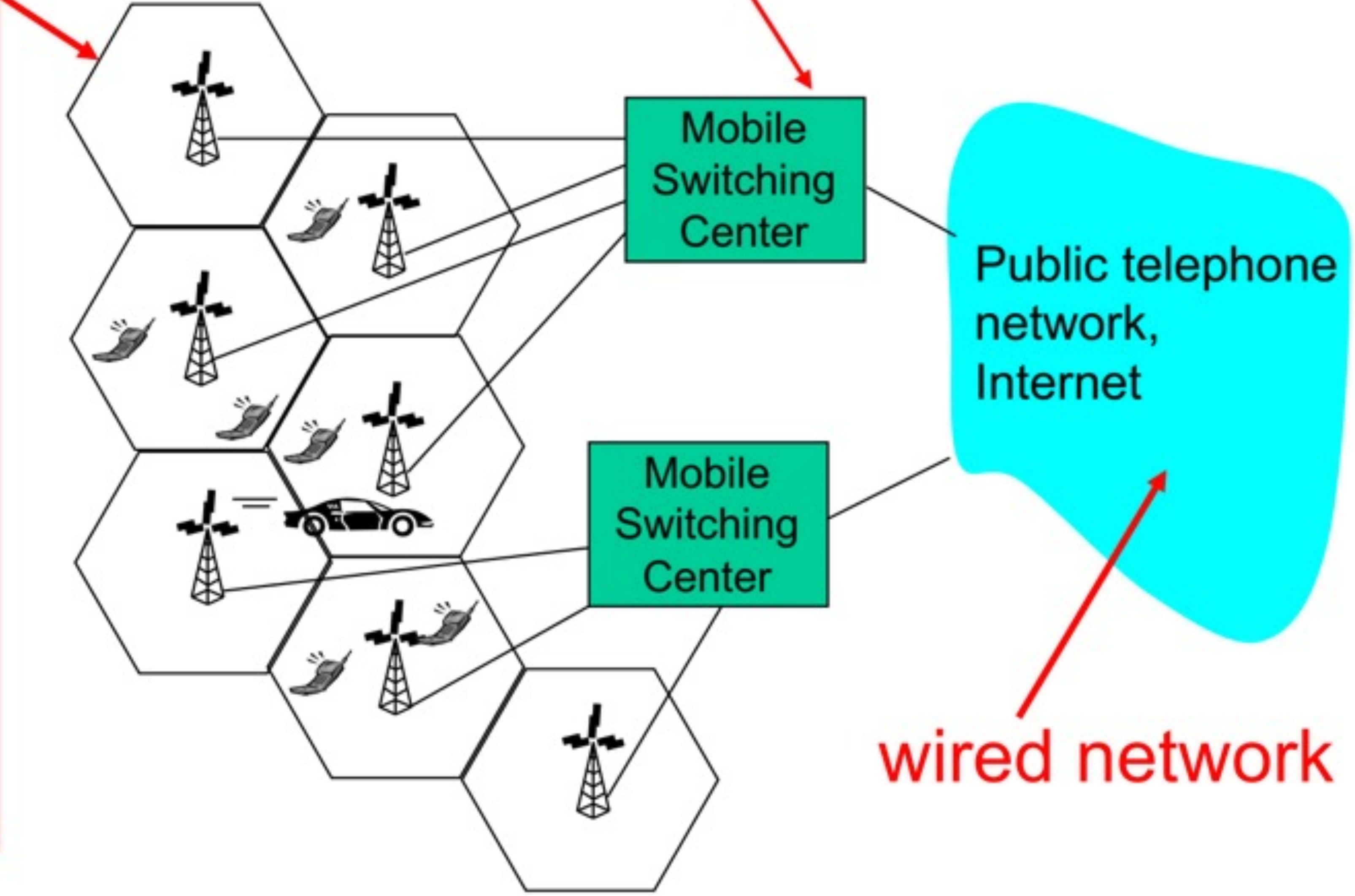
Cellular Network: Basic Components

MSC

- connects cells to wide area net
- manages call setup (more later!)
- handles mobility (more later!)

cell

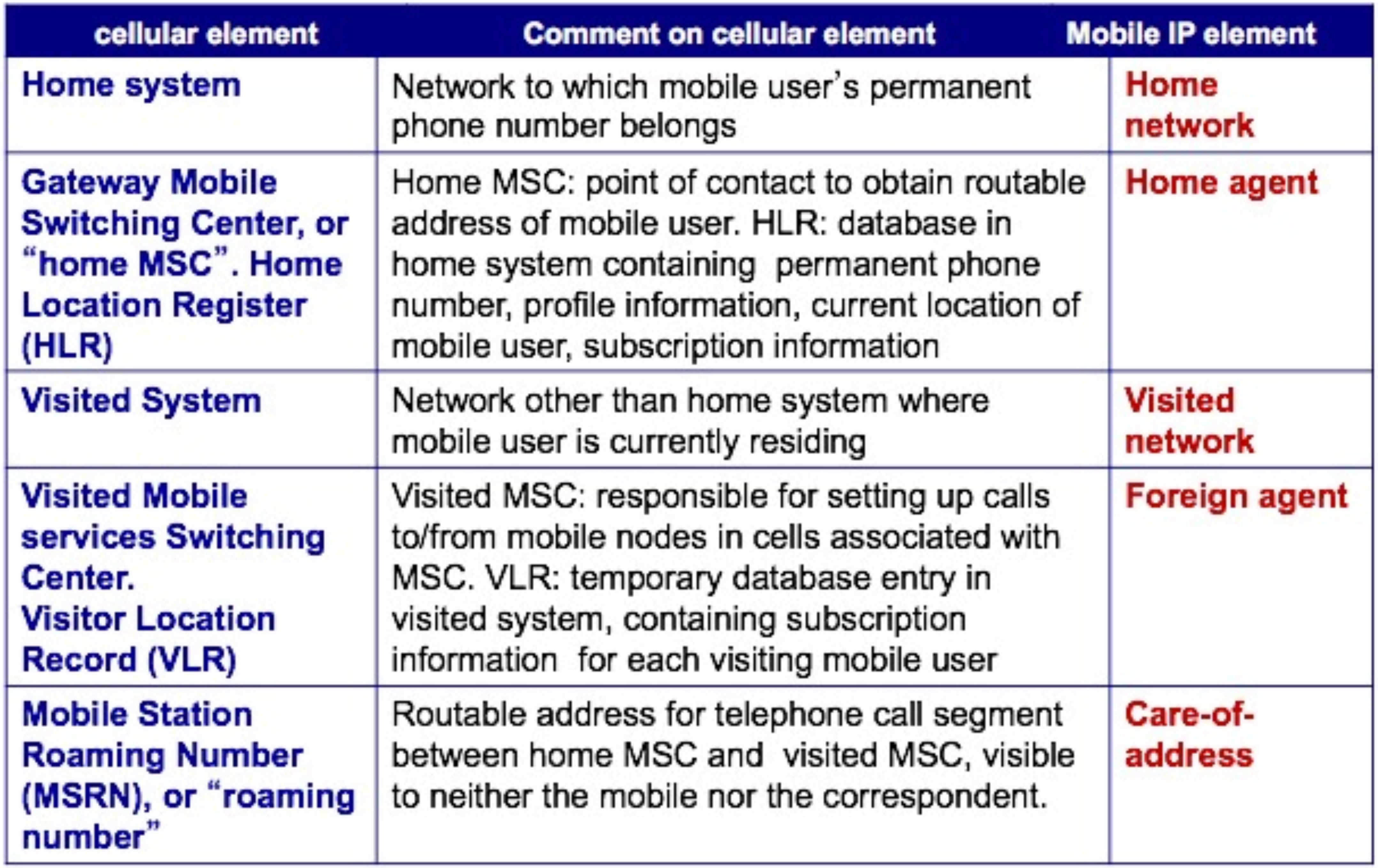
- covers geographical region
- *base station* (BS) analogous to 802.11 AP
- *mobile users* attach to network through BS
- *air-interface:* physical and link layer protocol between mobile and BS



Cellular Network and Mobility

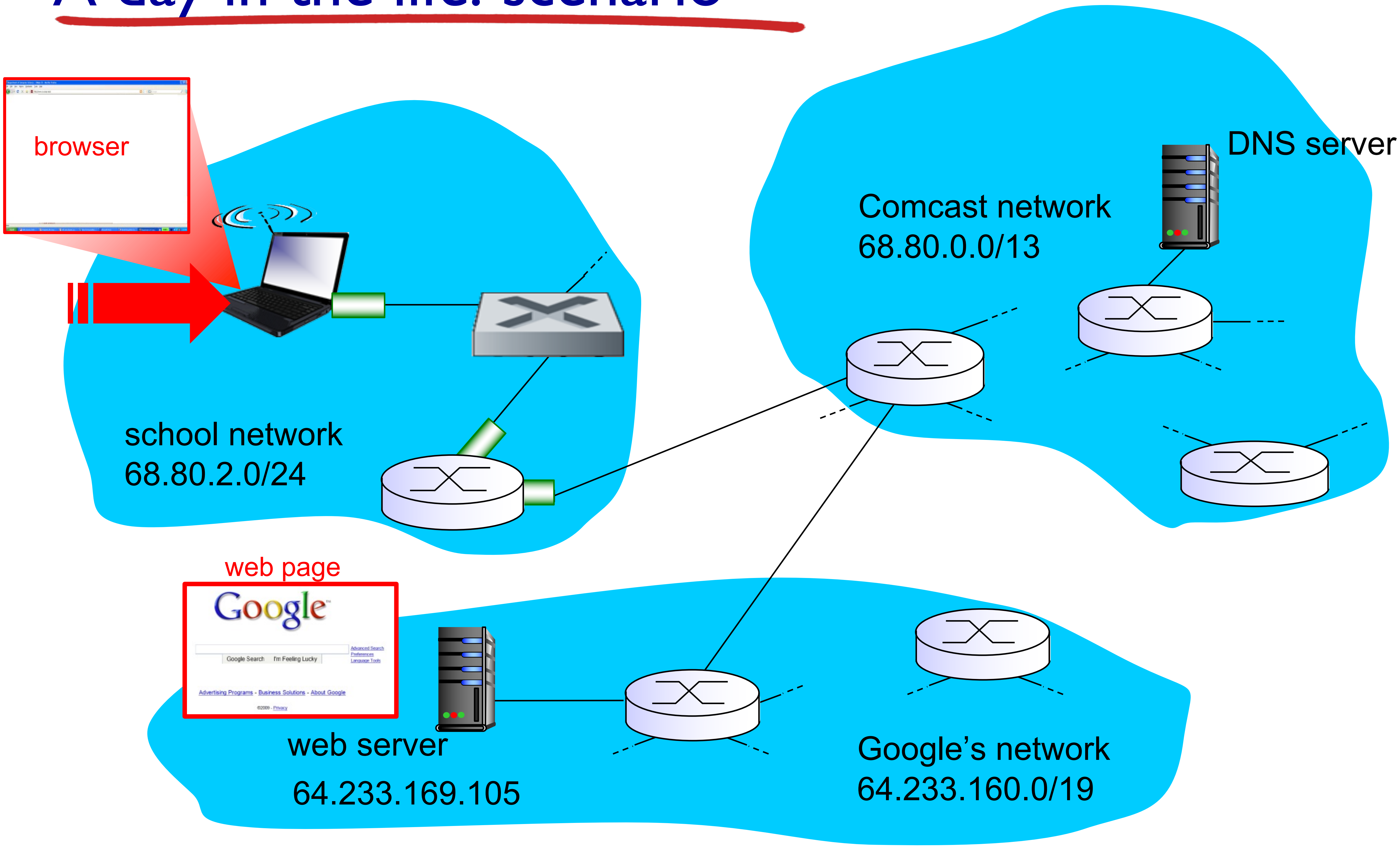
- Home network: network of cellular provider you subscribe to (e.g., Sprint PCS, Verizon)
  - home location register (HLR): database in home network containing permanent cell phone #, profile information (services, preferences, billing), information about current location (could be in another network)
- 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

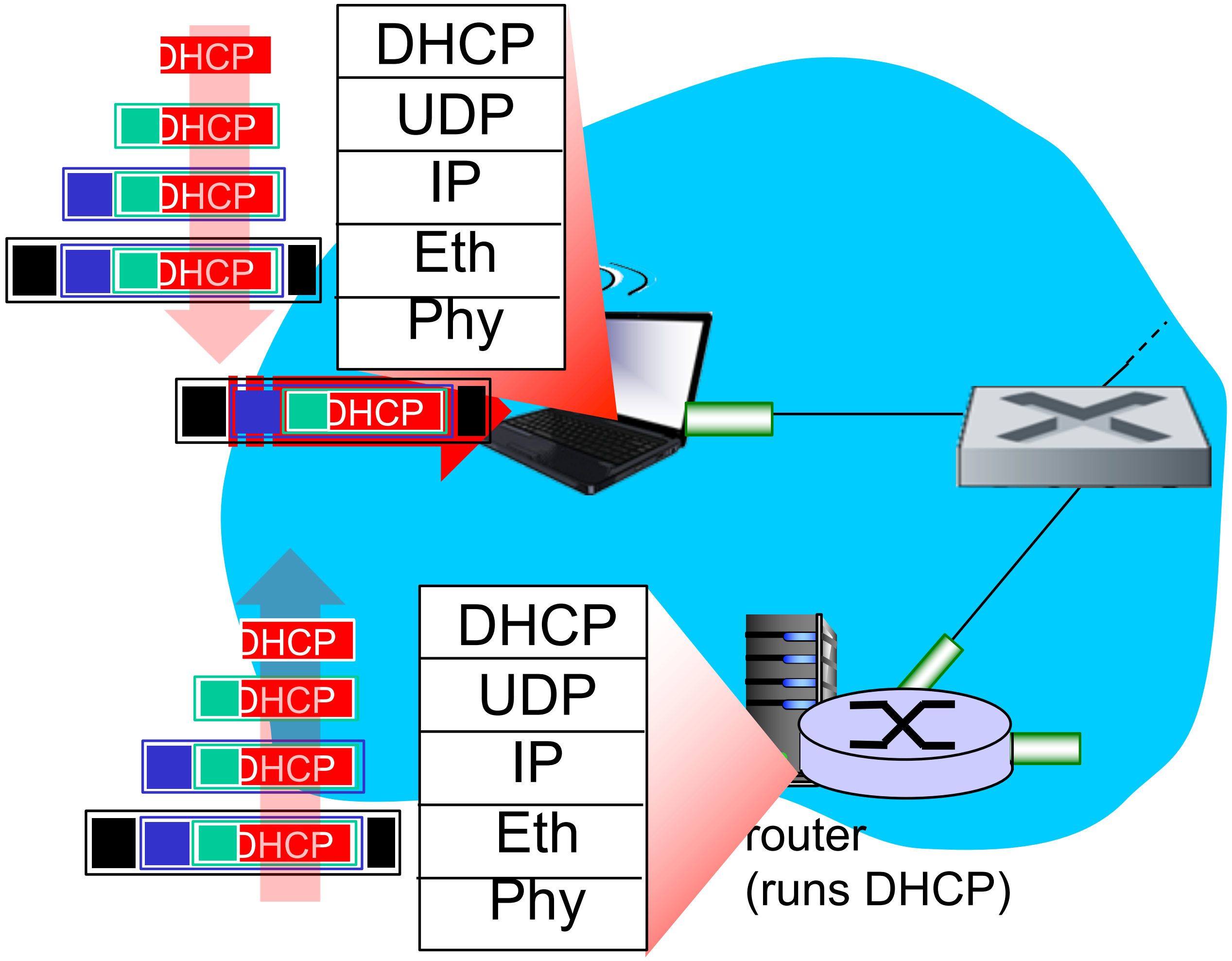


cellular element	Comment on cellular element	Mobile IP element
Home system	Network to which mobile user's permanent phone number belongs	**Home network**
Gateway Mobile Switching Center, or "home MSC". Home Location Register (HLR)	Home MSC: point of contact to obtain routable address of mobile user. 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**

A day in the life: scenario



A day in the life… connecting to the Internet

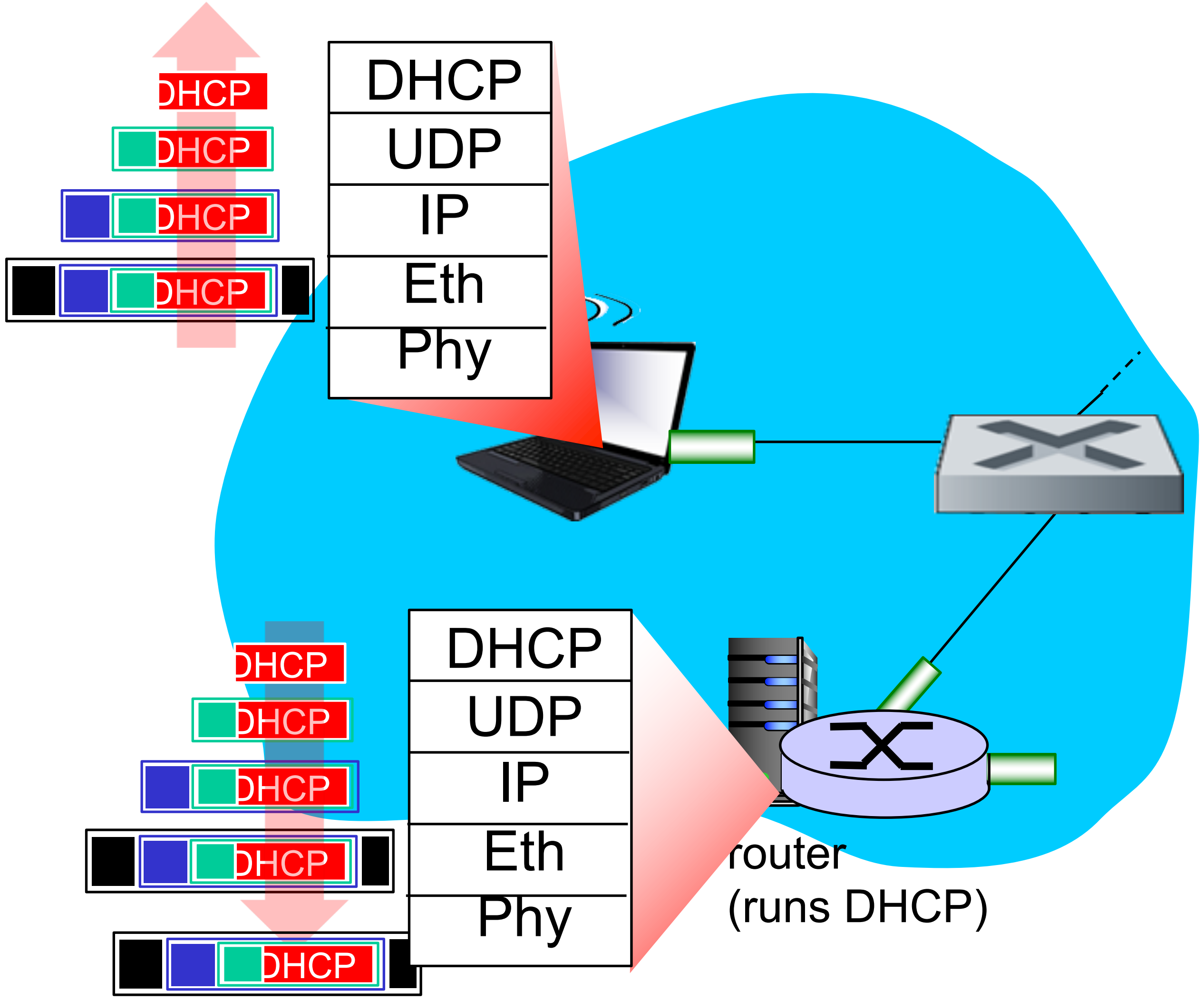


- connecting laptop needs to get its own IP address, addr of first-hop router, addr of DNS server: use *DHCP*

- DHCP request encapsulated in UDP, encapsulated in IP, encapsulated in 802.3 Ethernet (ip.src = 0.0.0.0; ip.dst = 255.255.255.255)
- Ethernet frame broadcast (dest: FFFFFFFFFFFF) on LAN, received at router running DHCP server

- Ethernet demuxed to IP demuxed, UDP demuxed to DHCP

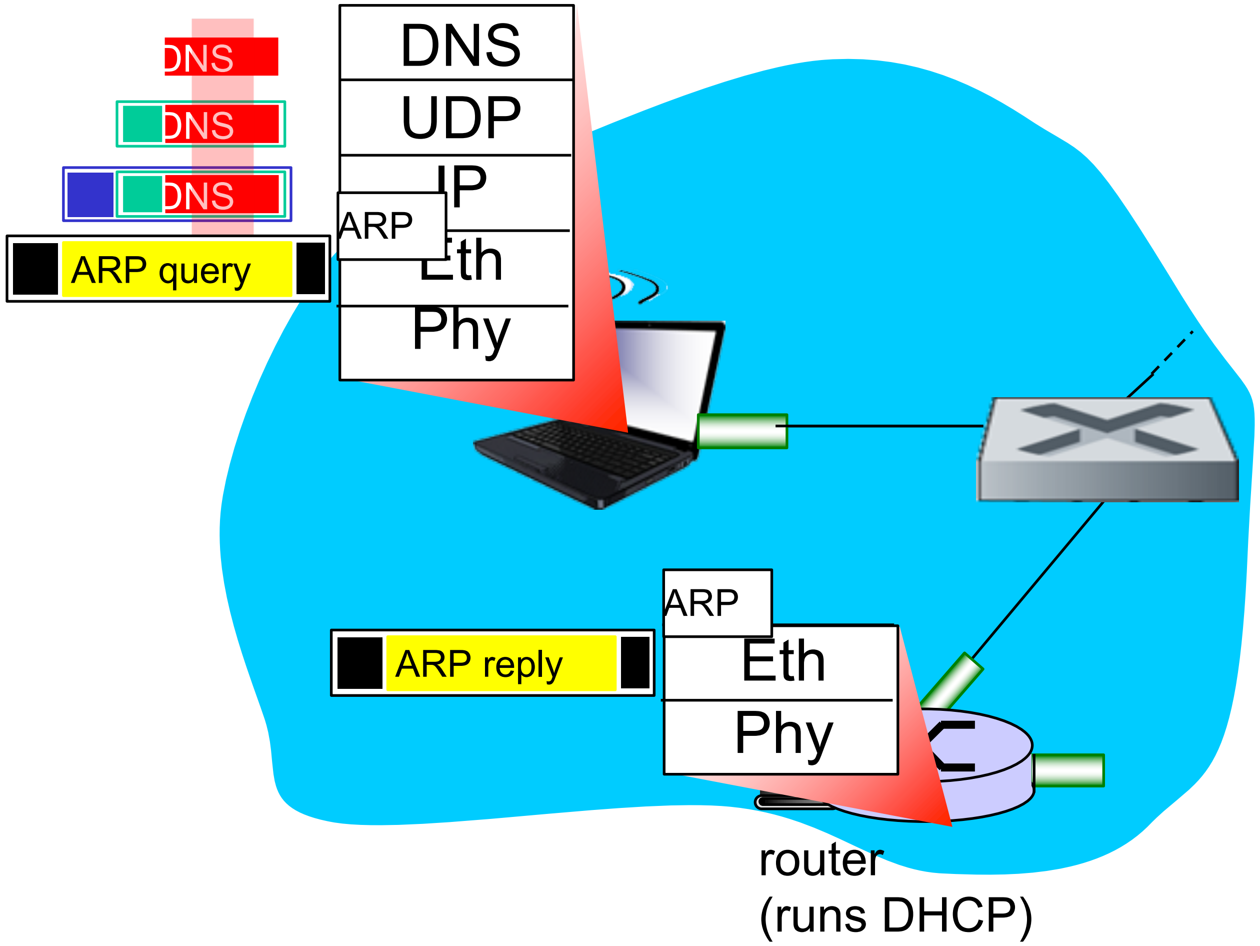
A day in the life… connecting to the Internet



- DHCP server formulates *DHCP ACK* containing client's IP address, IP address of first-hop router for client, name & IP address of DNS server
- encapsulation at DHCP server, frame forwarded (switch learning) through LAN, demultiplexing at client
- DHCP client receives DHCP ACK reply

Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

A day in the life… ARP (before DNS, before HTTP)



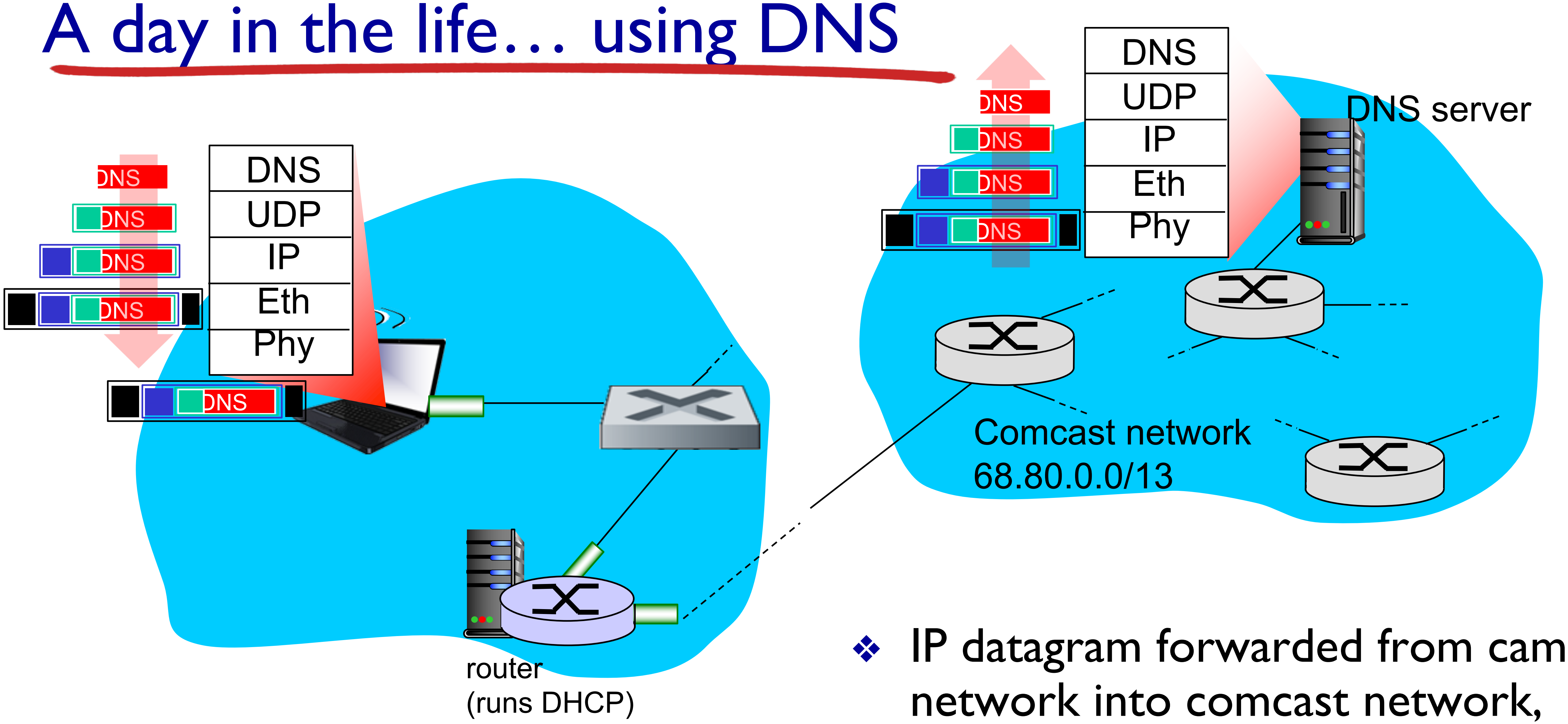
- before sending *HTTP* request, need IP address of www.google.com: *DNS*

- DNS query created, encapsulated in UDP, encapsulated in IP, encapsulated in Eth. To send frame to router, need MAC address of router interface: ARP

- ARP query broadcast, received by router, which replies with ARP reply giving MAC address of router interface

- client now knows MAC address of first hop router, so can now send frame containing DNS query

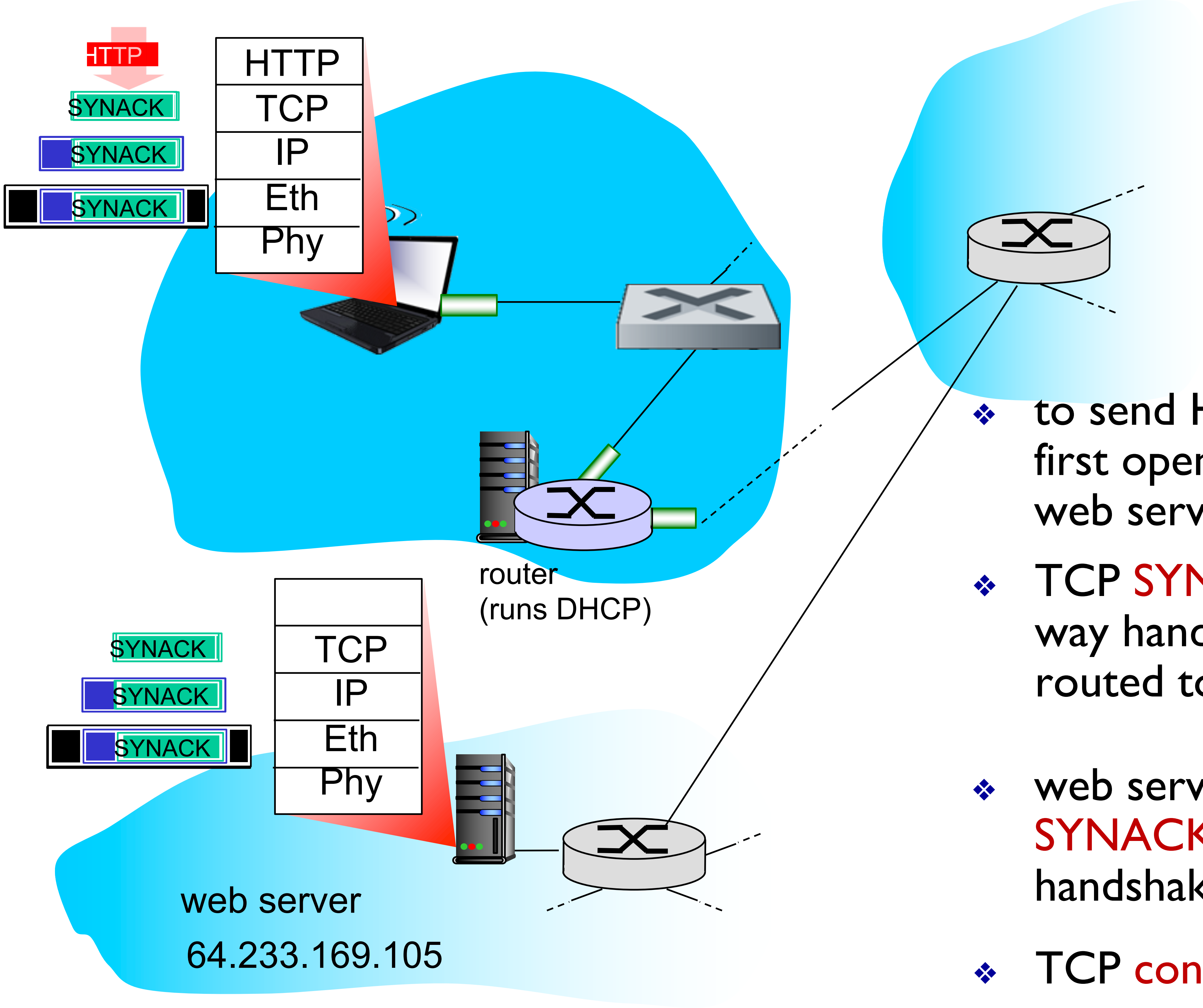
A day in the life… using DNS



- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router

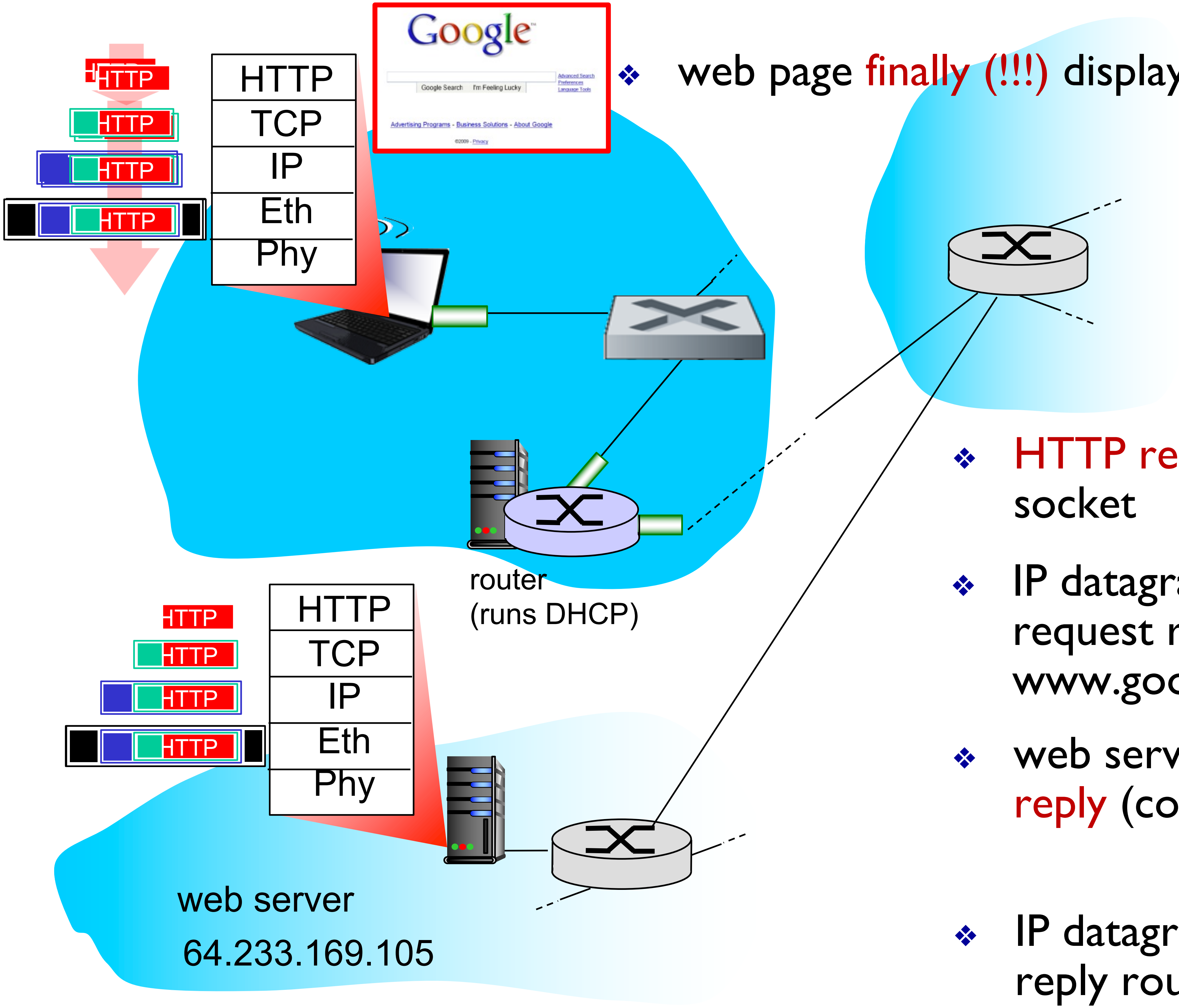
- IP datagram forwarded from campus network into comcast network, routed (tables created by RIP, OSPF, IS-IS and/or BGP routing protocols) to DNS server
- demux'ed to DNS server
- DNS server replies to client with IP address of www.google.com

A day in the life…TCP connection carrying HTTP



- to send HTTP request, client first opens TCP socket to web server
- TCP SYN segment (step 1 in 3-way handshake) inter-domain routed to web server
- web server responds with TCP SYNACK (step 2 in 3-way handshake)
- TCP connection established!

A day in the life… HTTP request/reply



- web page finally (!!!) displayed

- HTTP request sent into TCP socket
- IP datagram containing HTTP request routed to www.google.com
- web server responds with HTTP reply (containing web page)
- IP datagram containing HTTP reply routed back to client