

CSC358 Week 11

Note: all lecture activities will be recorded and the recording will be made available on the CSC358 Quercus.

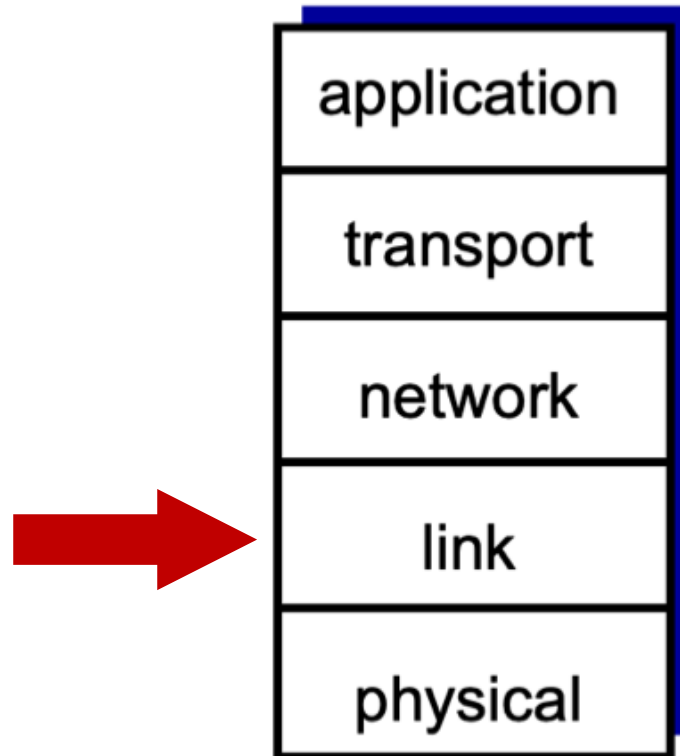
Logistics

- Exam
 - online exam (Quercus Quiz) at the originally scheduled time (Apr 13, 9 am – 12 pm EST)
 - We will provide detailed exam instructions beforehand as well as a mock practice exam
 - more details in next week's lecture
- Next week's lecture:
 - finishing up topics
 - exam review
- There are tutorials this and next week.

Communication Protocol

- All students' audio is muted by default.
- You may ask questions using Chat. Chat messages will be anonymized in the recording.
- If you'd like to ask a question by speaking, click on "raise your hand", the instruction may assign you at a presenter, then your audio will be heard by the class.
- The instructor may miss your raised hand from time to time when they stare at their presentation. Apologies ahead.

We are here



Link layer, LANs: outline

6.1 introduction, services

6.2 error detection,
correction

6.3 multiple access
protocols

6.4 LANs

- addressing, ARP
- Ethernet
- **switches**
- **VLANS**

Ethernet switch

- *link-layer device: takes an active role*
 - store, forward Ethernet frames
 - examine incoming frame's MAC address, *selectively* forward frame to one-or-more outgoing links when frame is to be forwarded on segment, uses CSMA/CD to access segment
 - compared to traditional *hubs* that simply transmit the bits at the physical layer.
- *transparent*
 - hosts are unaware of presence of switches
- *plug-and-play, self-learning*
 - switches do not need to be configured

splitter

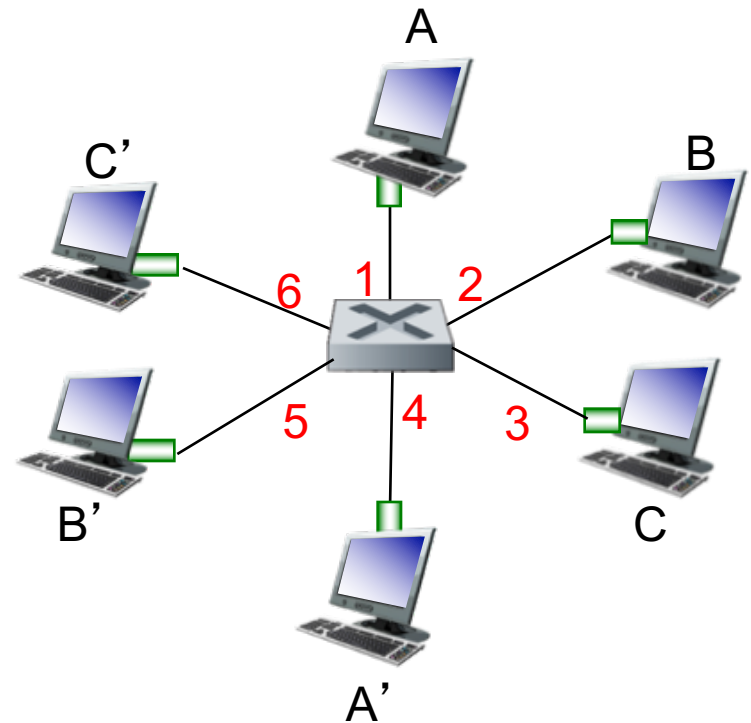
switch

hub



Switch: *multiple* simultaneous transmissions

- hosts have dedicated, direct connection to switch
- switches buffer packets
- Ethernet protocol used on *each* incoming link, but no collisions; full duplex
 - each link is its own collision domain
- **switching:** A-to-A' and B-to-B' can transmit simultaneously, without collisions



*switch with six interfaces
(1,2,3,4,5,6)*

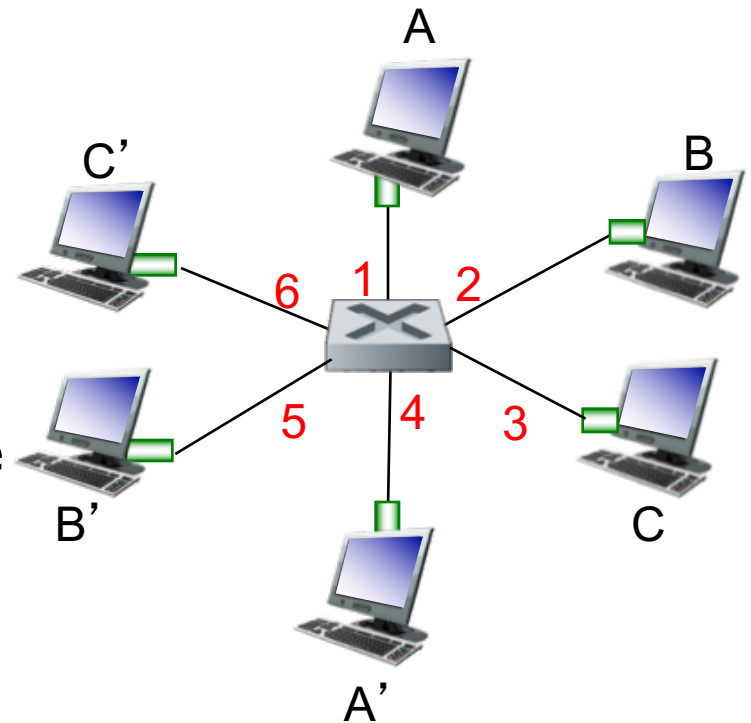
Switch forwarding table

Q: how does switch know A' reachable via interface 4, B' reachable via interface 5?

- **A:** each switch has a **switch table**, each entry:
 - (MAC address of host, interface to reach host, time stamp)
 - looks like a routing table!

Q: how are entries created, maintained in switch table?

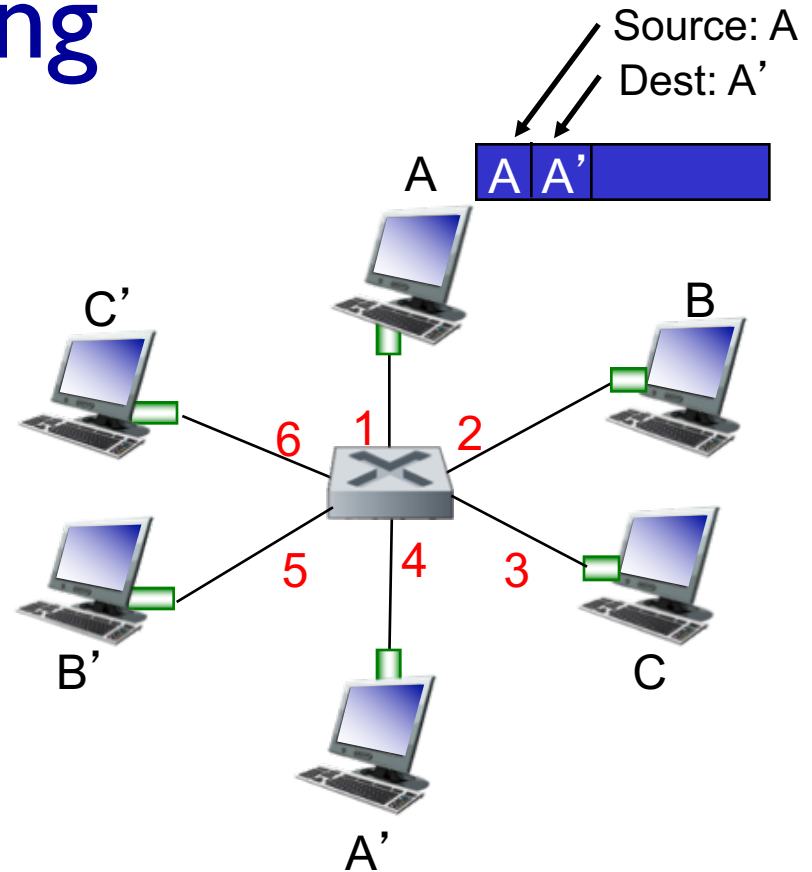
- something like a routing protocol?



*switch with six interfaces
(1,2,3,4,5,6)*

Switch: self-learning

- switch *learns* which hosts can be reached through which interfaces
 - when frame received, switch “learns” location of sender: incoming LAN segment
 - records sender/location pair in switch table



MAC addr	interface	TTL
A	1	60

*Switch table
(initially empty)*

Switch: frame filtering/forwarding

when frame received at switch:

1. record incoming link, MAC address of sending host
2. index switch table using MAC destination address

3. if entry found for destination

then {

if destination on segment from which frame arrived
then drop frame

else forward frame on interface indicated by entry

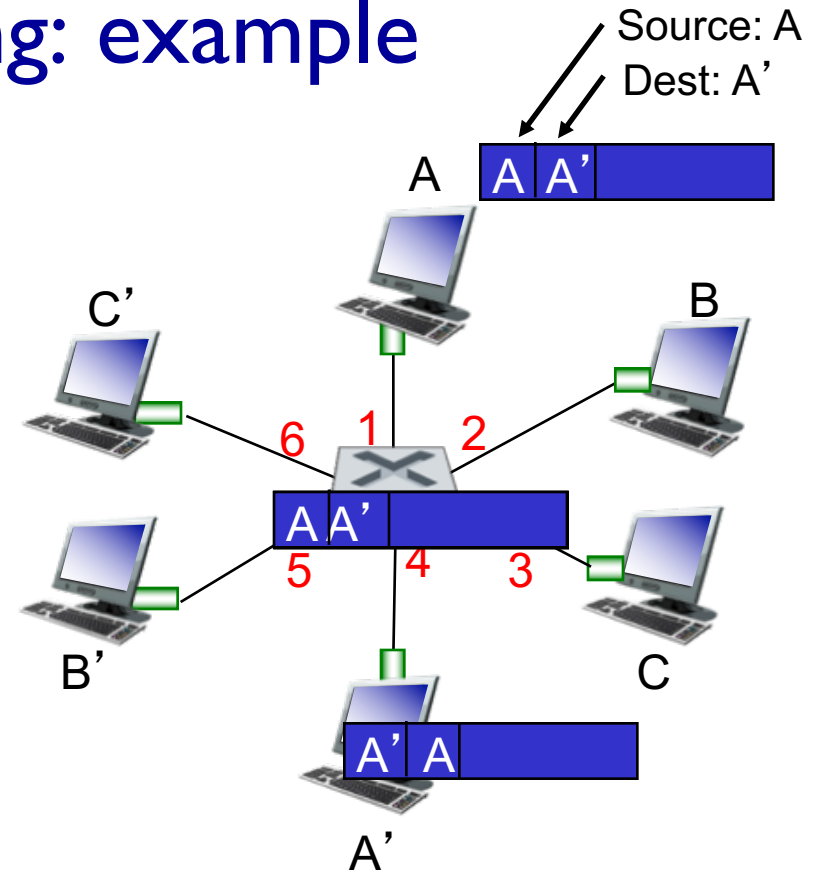
}

else

flood /* forward on all interfaces except arriving
interface */

Self-learning, forwarding: example

- frame destination, A', location unknown: *flood*
- destination A location known: *selectively send on just one link*

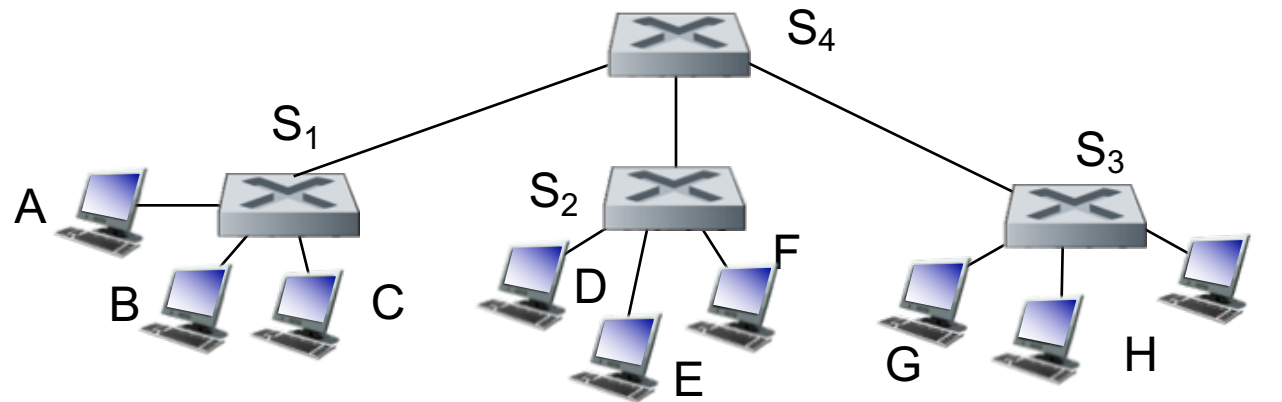


MAC addr	interface	TTL
A	1	60
A'	4	60

*switch table
(initially empty)*

Interconnecting switches

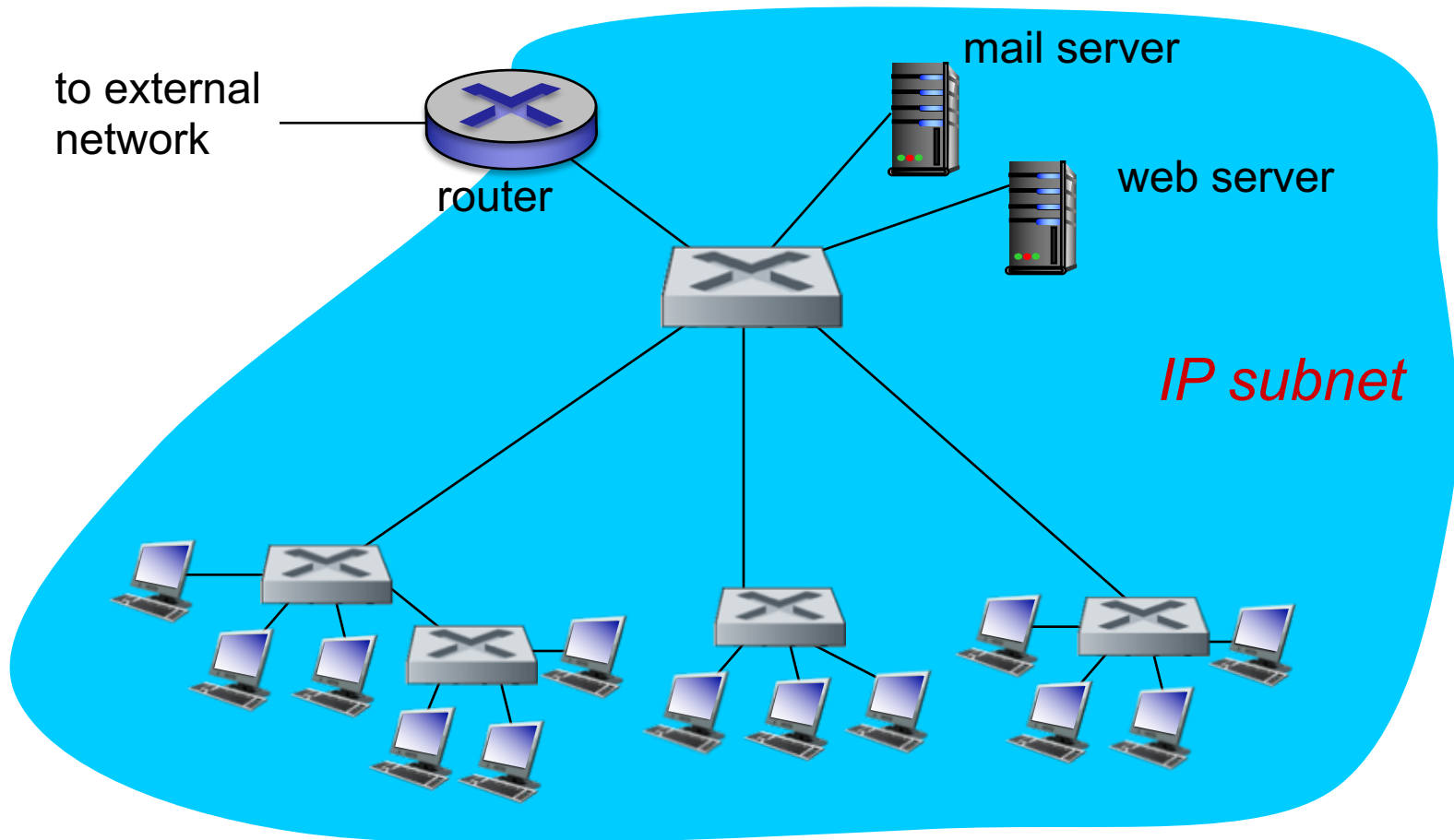
self-learning switches can be connected together:



Q: sending from A to G - how does S₁ know to forward frame destined to G via S₄ and S₃?

- **A:** self learning! (works exactly the same as in single-switch case!)

Institutional network



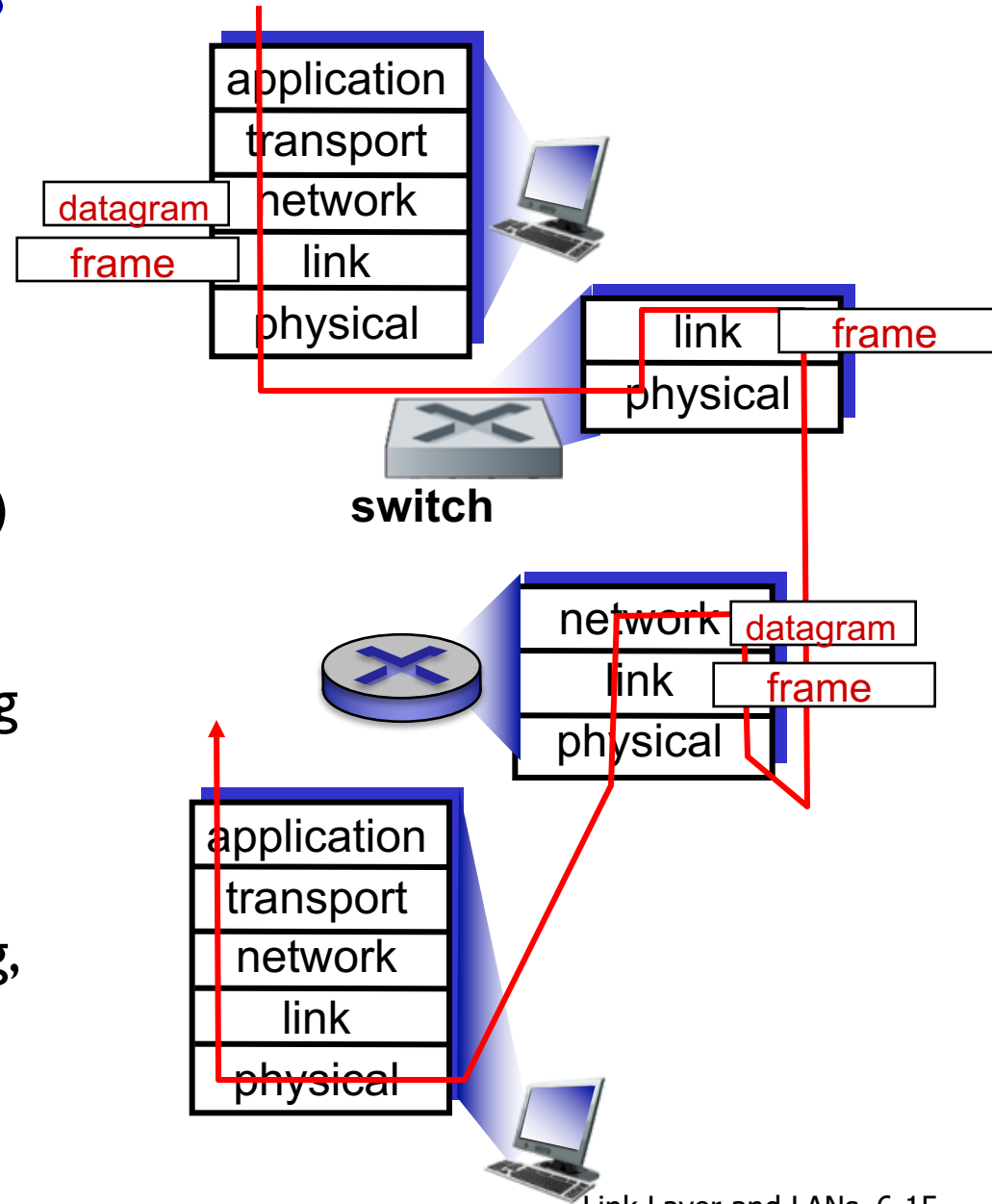
Switches vs. routers

both are store-and-forward:

- **routers:** network-layer devices (examine network-layer headers)
- **switches:** link-layer devices (examine link-layer headers)

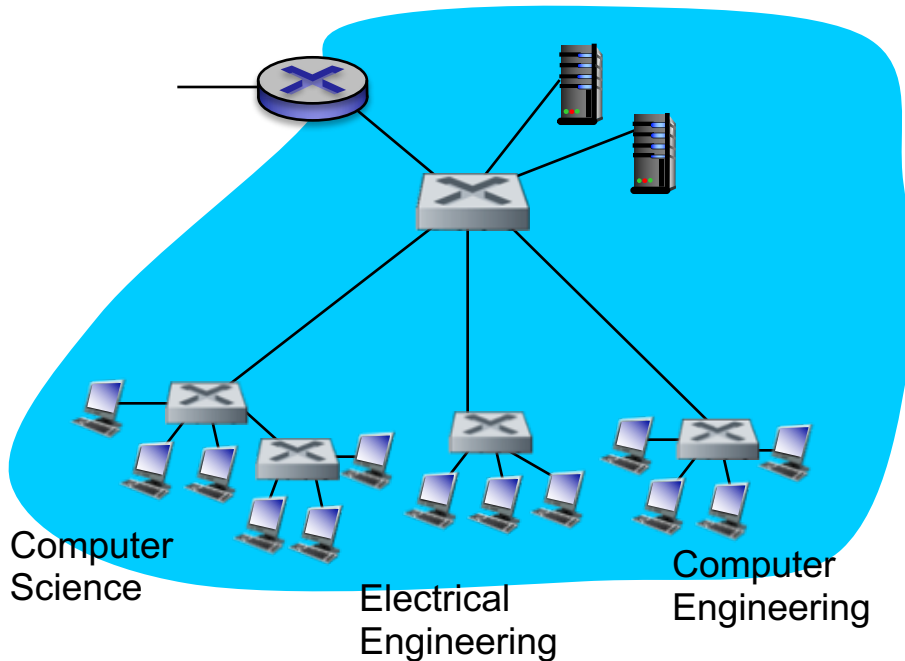
both have forwarding tables:

- **routers:** compute tables using routing algorithms, IP addresses
- **switches:** learn forwarding table using flooding, learning, MAC addresses



VLAN

VLANs: motivation



consider:

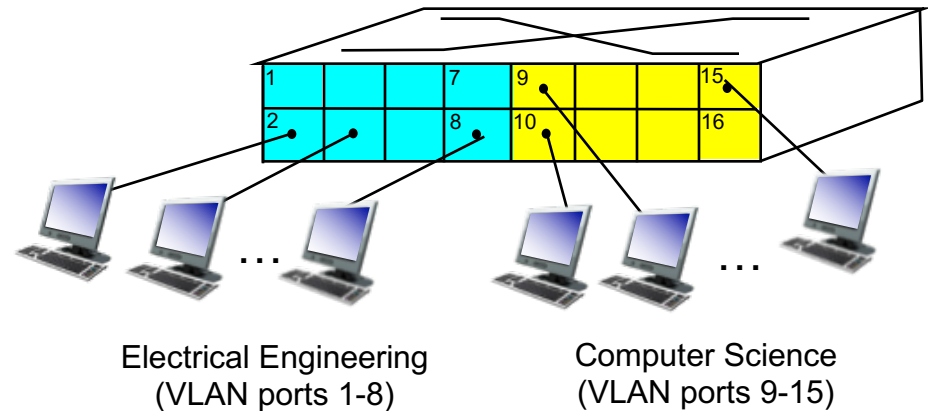
- CS user moves office to EE, but wants connect to CS switch?
- single broadcast domain:
 - all layer-2 broadcast traffic (ARP, DHCP, unknown location of destination MAC address) must cross entire LAN
 - security/privacy, efficiency issues

VLANs

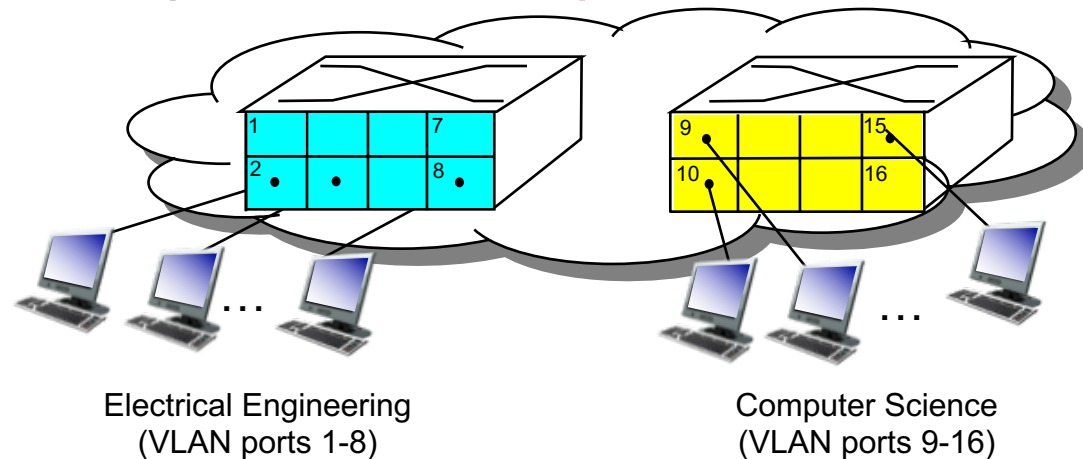
Virtual Local Area Network

switch(es) supporting VLAN capabilities can be configured to define multiple **virtual** LANs over single physical LAN infrastructure.

port-based VLAN: switch ports grouped (by switch management software) so that **single** physical switch

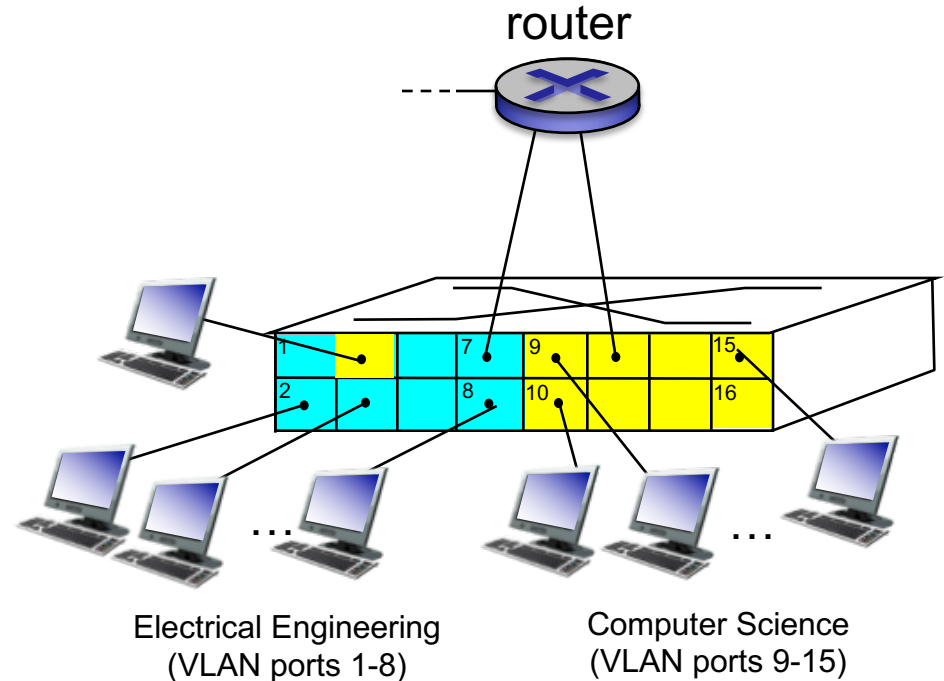


... operates as **multiple** virtual switches



Port-based VLAN

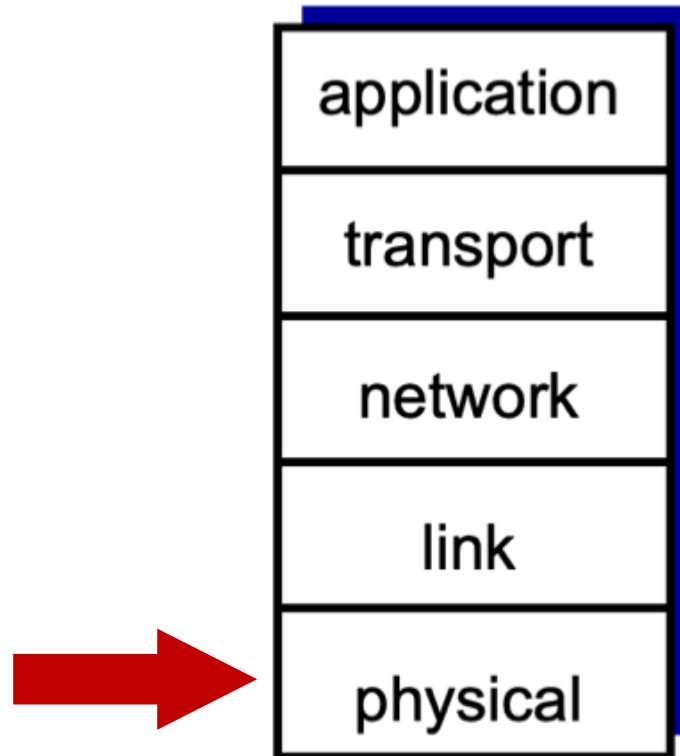
- **traffic isolation:** frames to/from ports 1-8 can *only* reach ports 1-8
 - can also define VLAN based on MAC addresses of endpoints, rather than switch port
- **dynamic membership:** ports can be dynamically assigned among VLANs
- **forwarding between VLANs:** done via routing (just as with separate switches)
 - in practice vendors sell combined switches plus routers



Link Layer Summary

- principles behind data link layer services:
 - error detection, correction
 - sharing a broadcast channel: multiple access
 - link layer addressing
- instantiation and implementation of various link layer technologies
 - Ethernet
 - switched LANS, VLANs

Going deeper: Physical Layer!!



Physical Layer Outline

1. Network Interface Card

- Circuit Theory

2. Twisted pair

- Electromagnetism
 - The Maxwell equations
- Signal processing
- Fourier transform; Laplace transform

3. Optics

- Optics
- Optics
- Material science: fluoride glass, phosphate glass, chalcogenide glass

4. USB

- connectors
- cabling
- power

4. Wireless

- Radio theory
- Antenna
- Modulation
- Resonance

5. Bluetooth

- Link manager

Too many things going on at the physical layer, so we'll skip most of these.

- GSM, GPRS, 3G, LTE, 5G

7. Information Theory

- Shannon's theorem
- Entropy

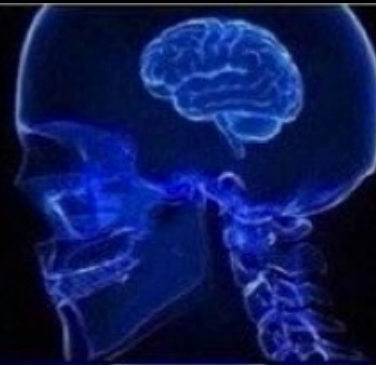
8. Quantum communication

- Quantum mechanics
- Quantum information theory
- Quantum teleportation

Synthesis:

A Day in the Life of a Web Request

**OPEN BROWSER,
ENTER URL,
BROWSE INTERNET**



CSC358...



**MORE
CSC358...**



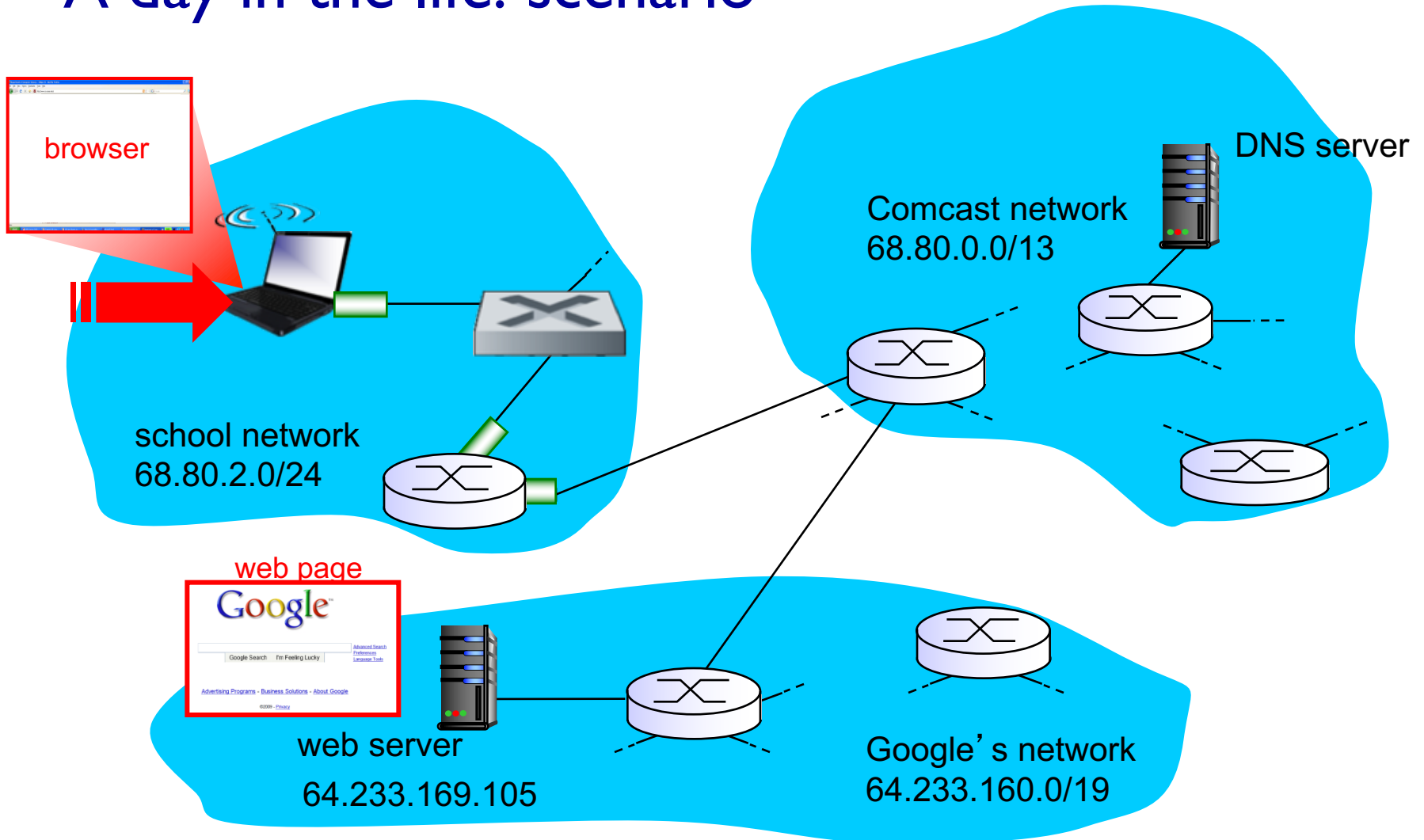
**HTTP, TCP, UDP, IP,
ETHERNET, DNS, DHCP, ARP,
BGP, OSPF, ICMP, MAC,
CSMA, MPLS, ROUTER, SWITCH,
DELAY, AIMD, RDT, SEGMENT,
DATAGRAM, FRAME, BITS ...**



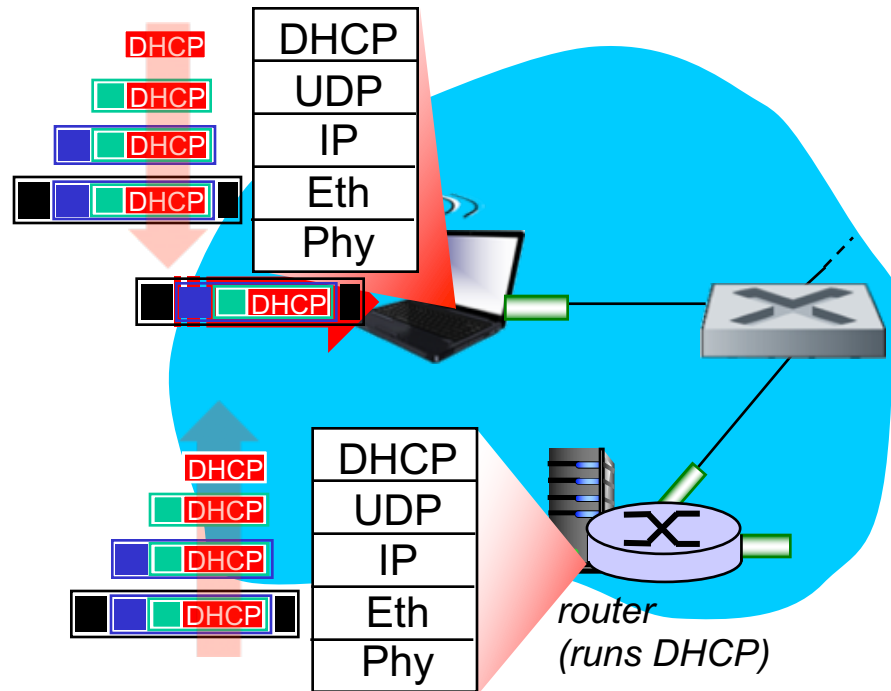
Synthesis: a day in the life of a web request

- journey down protocol stack complete!
 - application, transport, network, link
- putting-it-all-together: synthesis!
 - *goal*: identify, review, understand protocols (at all layers) involved in seemingly simple scenario: requesting www page
 - *scenario*: student attaches laptop to campus network, requests/receives www.google.com

A day in the life: scenario

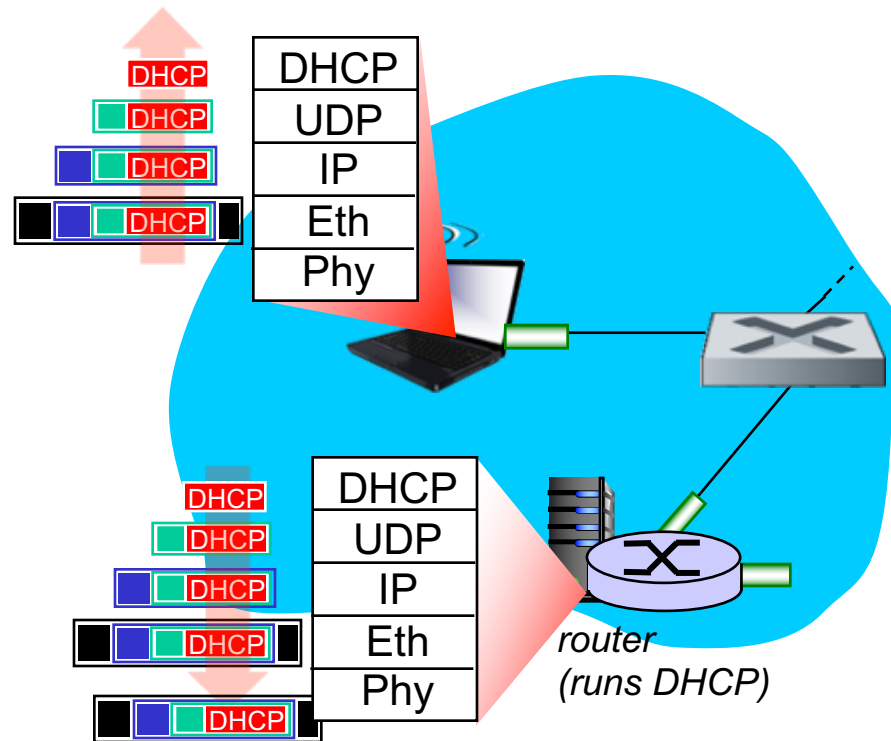


A day in the life... connecting to the Internet



- 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
- Ethernet frame **broadcast** (dest: FFFFFFFFFFFFFFFF) on LAN, received at router running **DHCP** server
- Ethernet **demuxed** to IP demuxed, UDP demuxed to DHCP

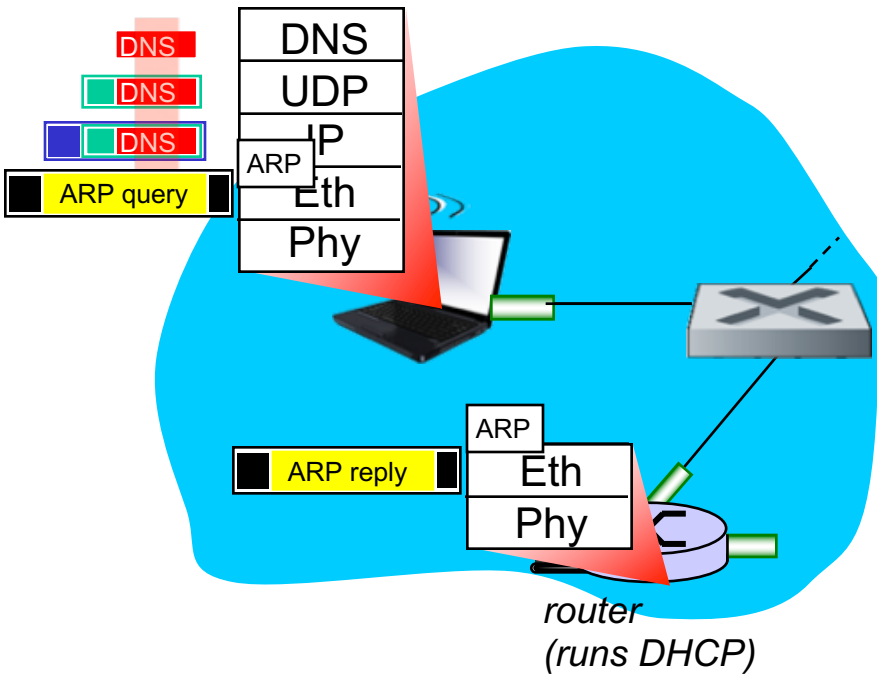
A day in the life... connecting to the Internet



- 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

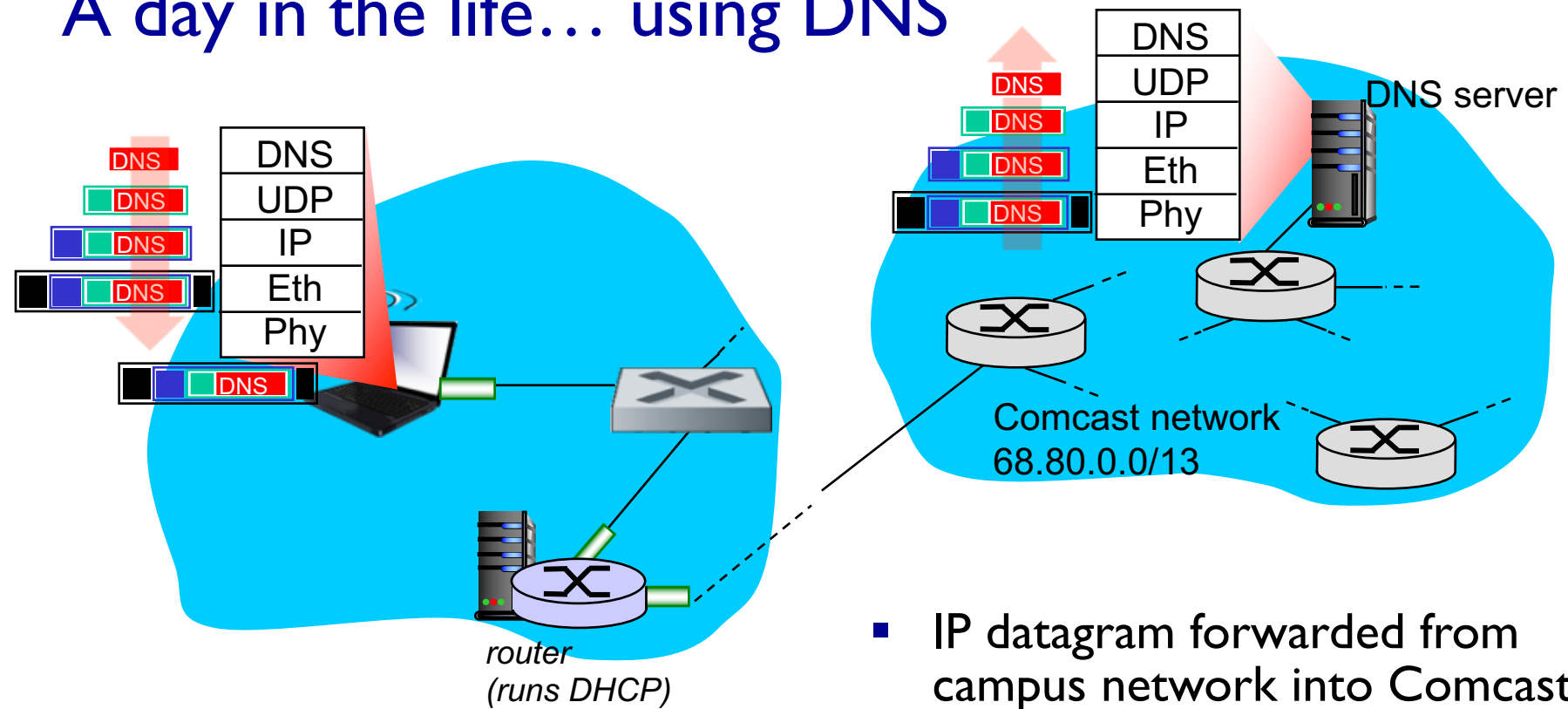
Client now has IP address, knows name & addr of DNS server, IP address of its first-hop router

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

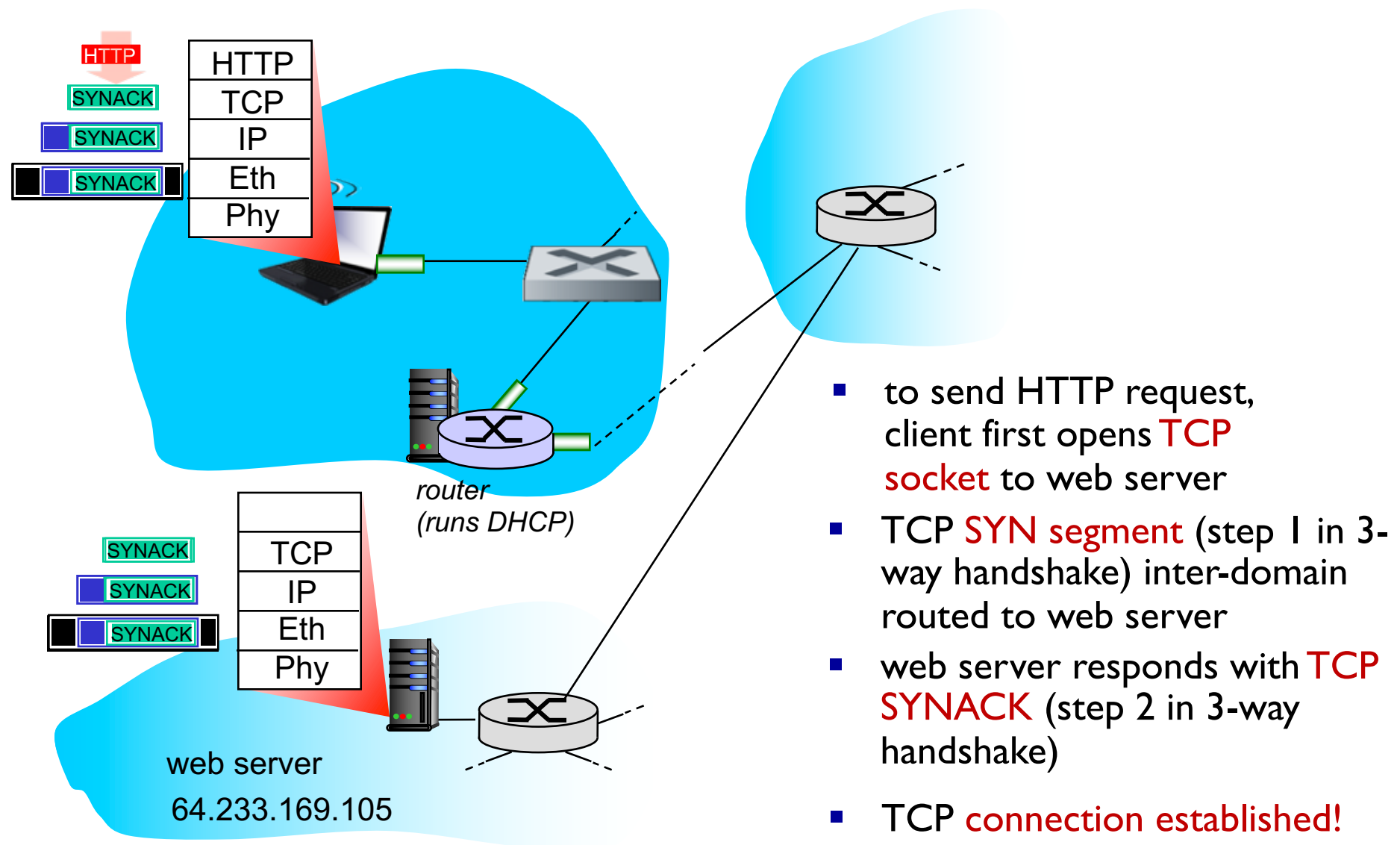
A day in the life... using DNS



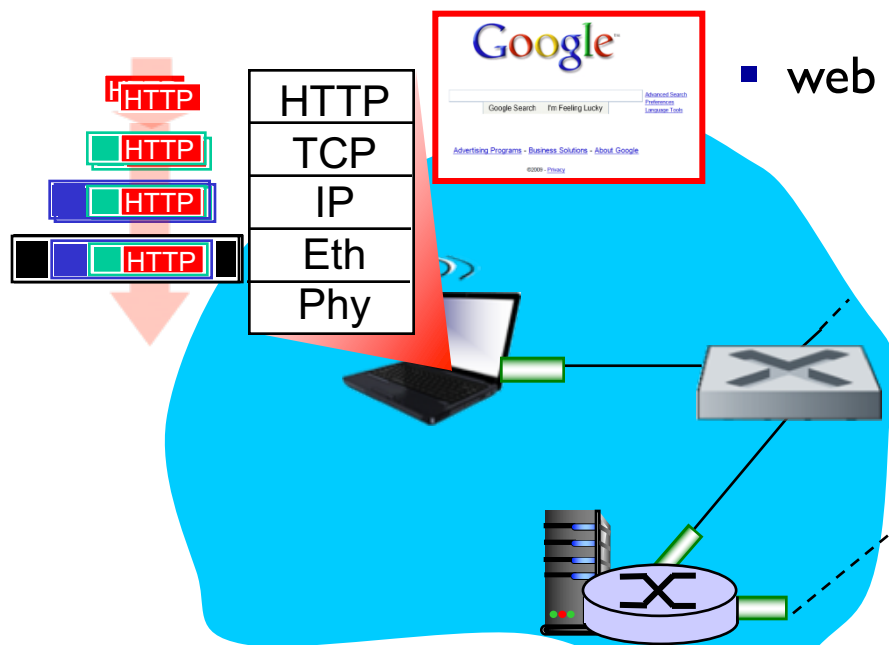
- IP datagram containing DNS query forwarded via LAN switch from client to 1st hop router

- 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
- demuxed to DNS server
- DNS server replies to client with IP address of **www.google.com**

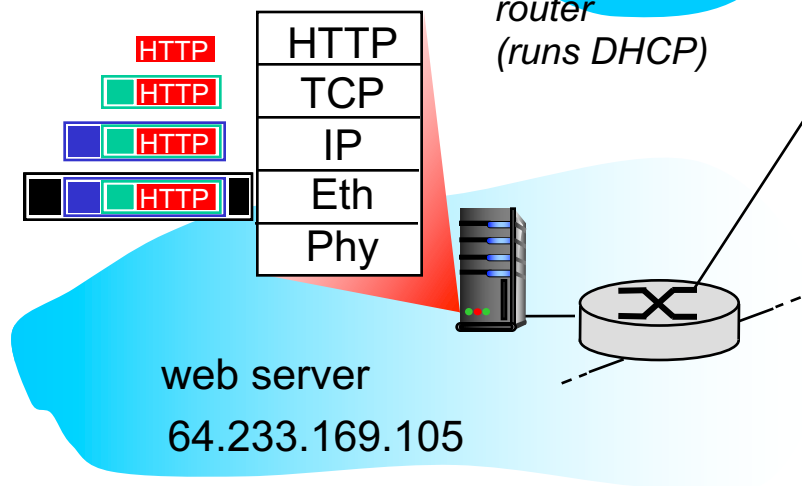
A day in the life...TCP connection carrying HTTP



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

Next Topic

One more thing:

Wireless and Mobile Network

Wireless and Mobile Networks

Background:

- # wireless (mobile) phone subscribers now exceeds # wired phone subscribers (5-to-1)!
- # wireless Internet-connected devices equals # wireline Internet-connected devices
 - laptops, Internet-enabled phones promise anytime untethered Internet access
- two important (but different) challenges
 - *wireless*: communication over wireless link
 - *mobility*: handling the mobile user who changes point of attachment to network

Outline

7.1 Introduction

Wireless

7.2 Wireless links,
characteristics

6.73 IEEE 802.11 wireless
LANs (“Wi-Fi”)

67.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

Mobility

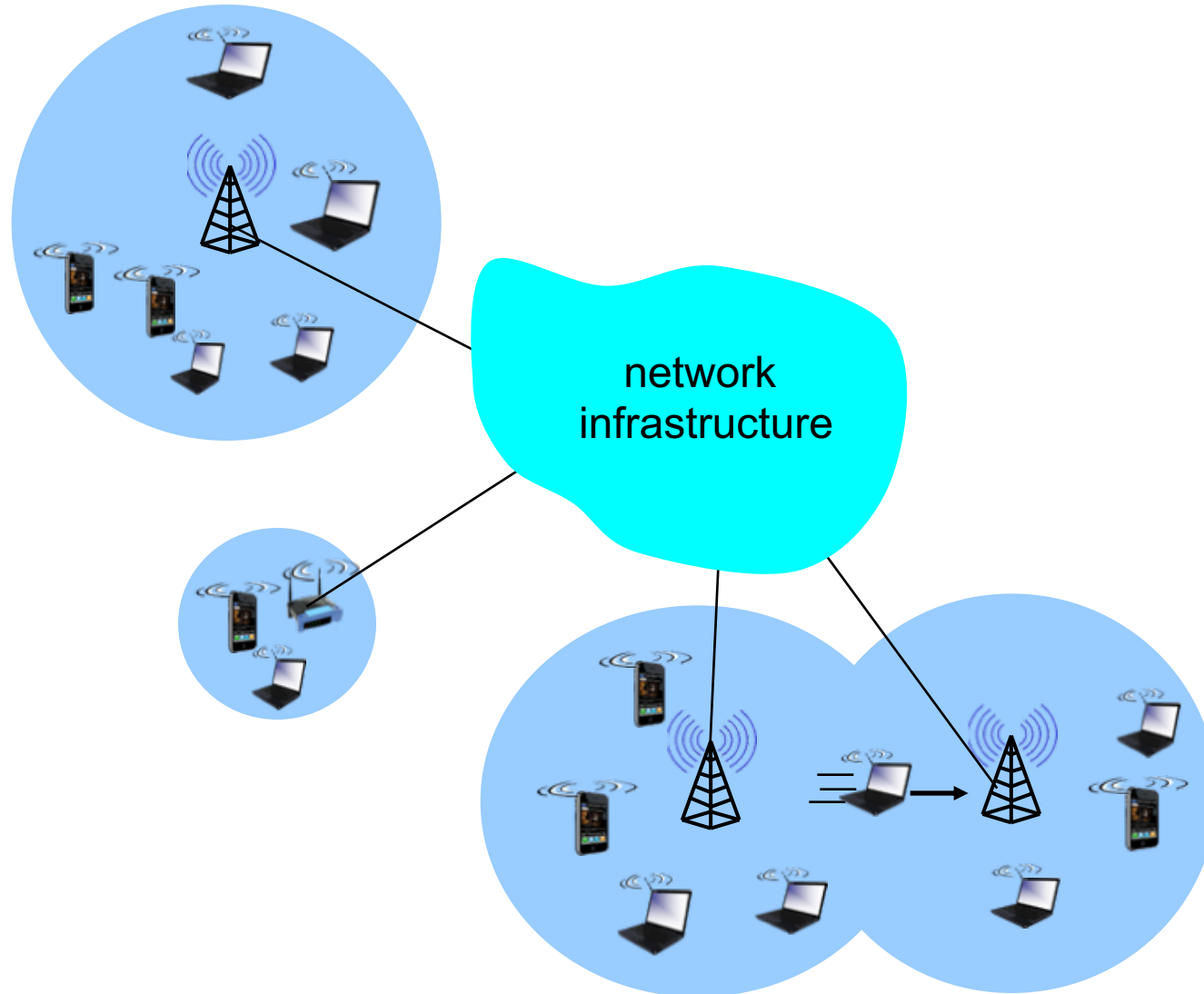
7.5 Principles: addressing and
routing to mobile users

7.6 Mobile IP

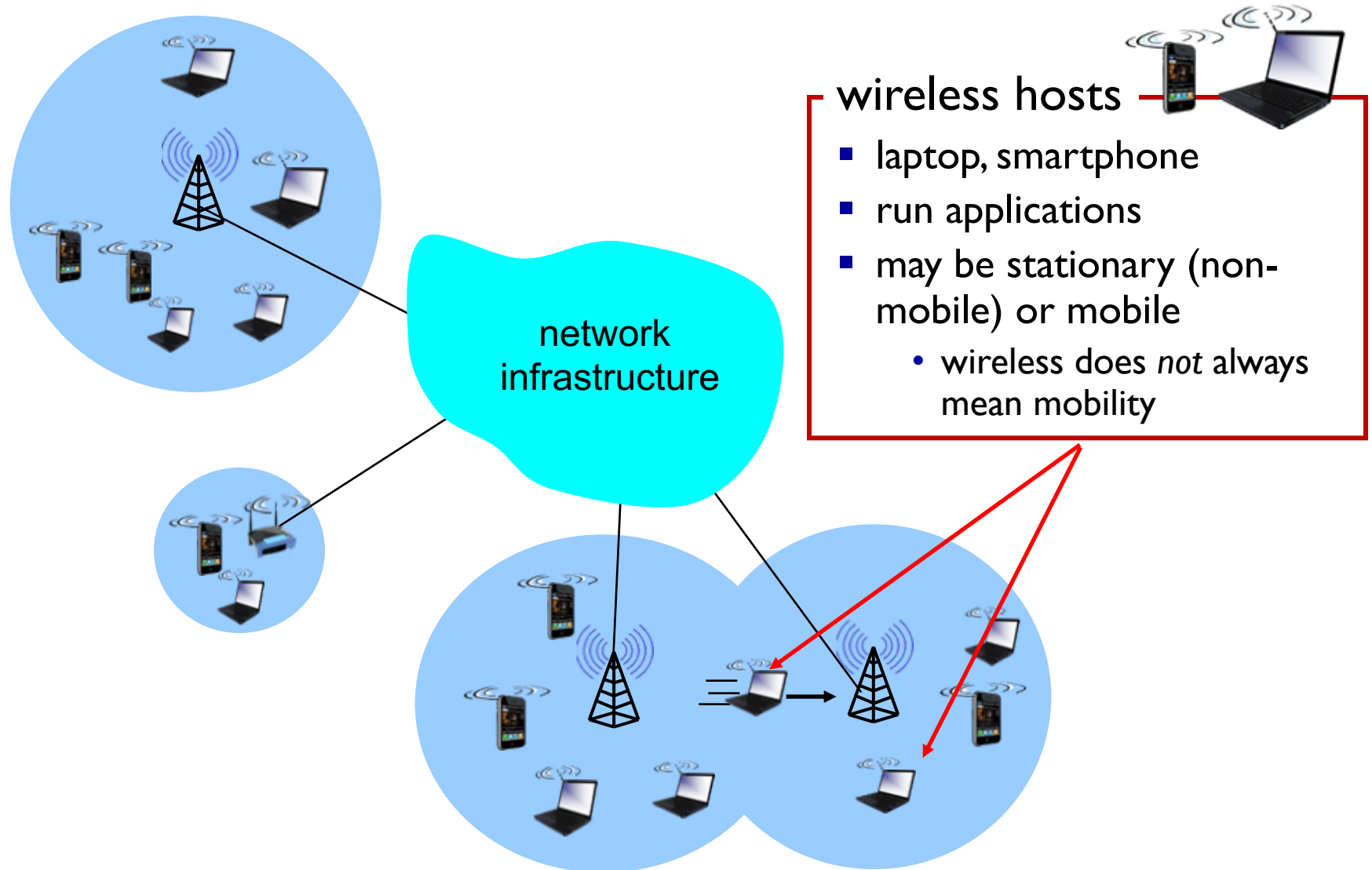
7.7 Handling mobility in
cellular networks

7.8 Mobility and higher-layer
protocols

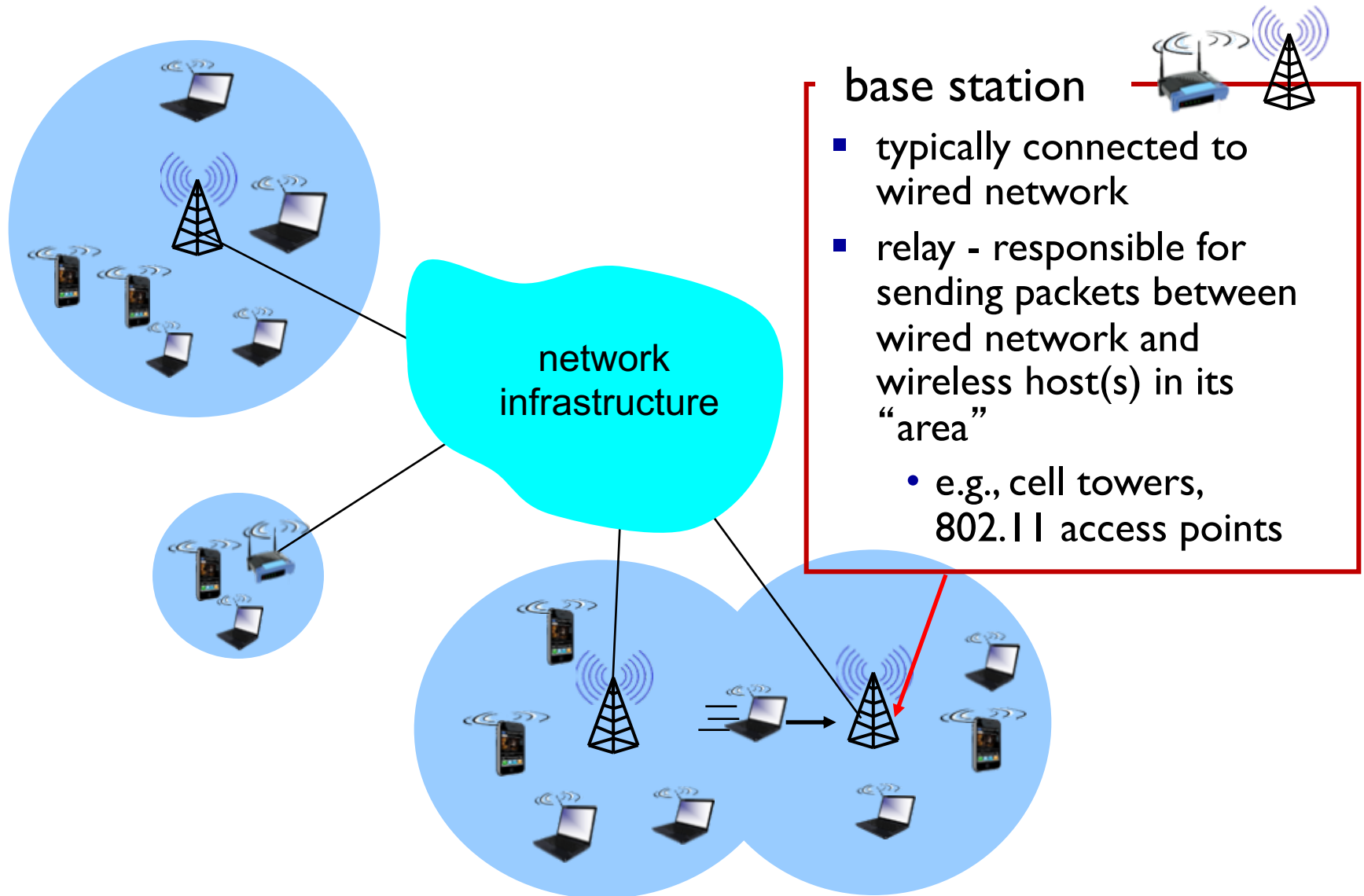
Elements of a wireless network



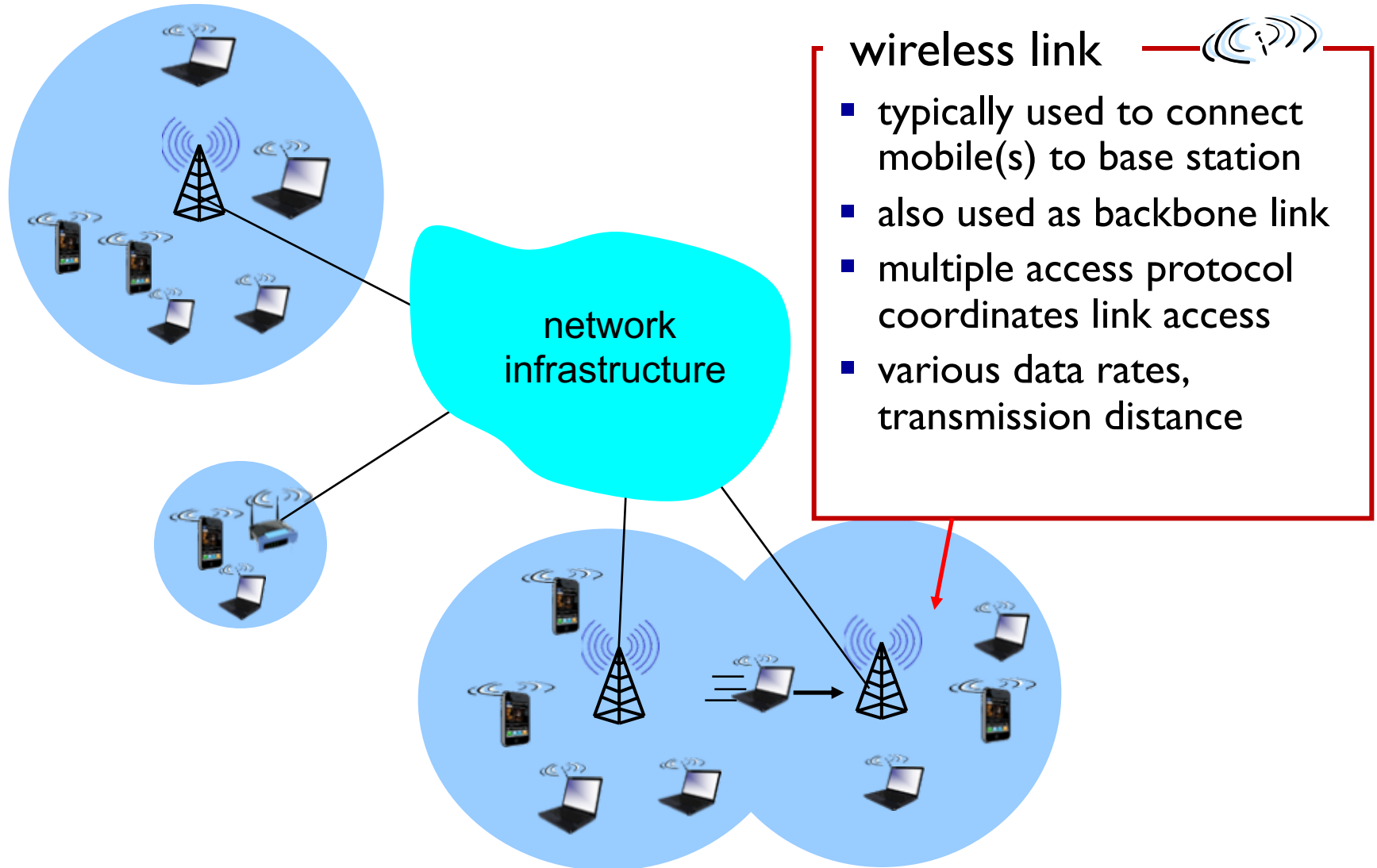
Elements of a wireless network



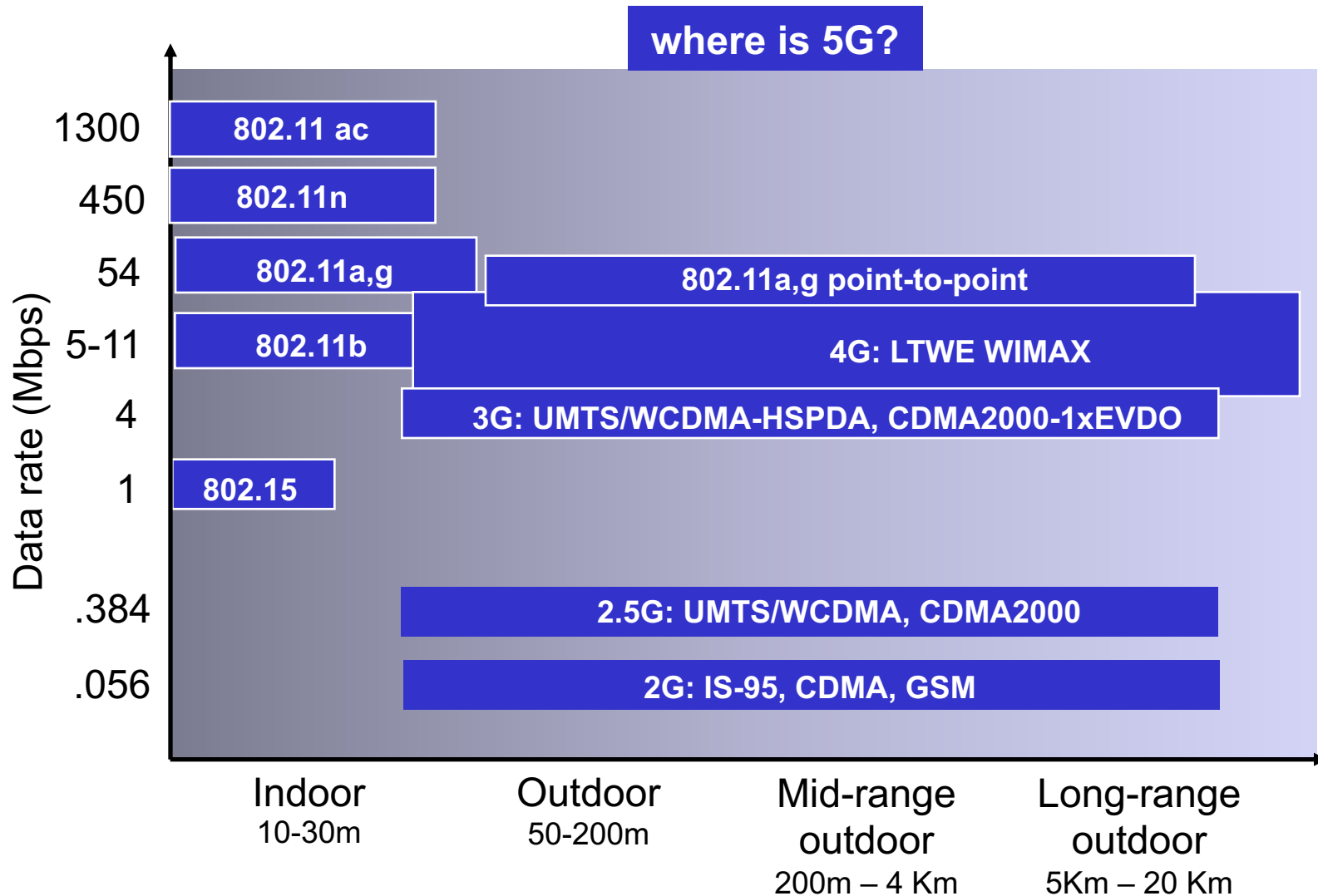
Elements of a wireless network



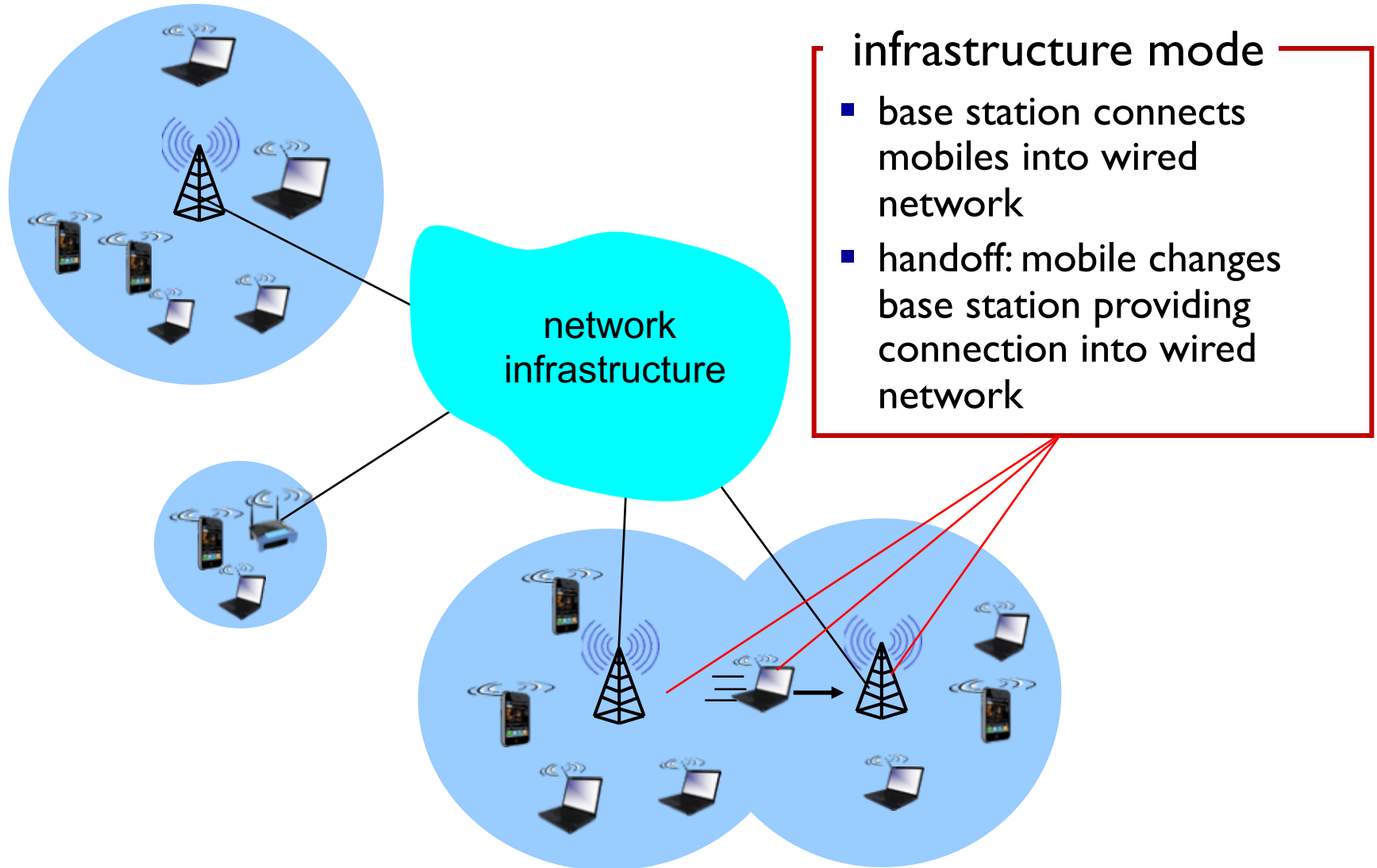
Elements of a wireless network



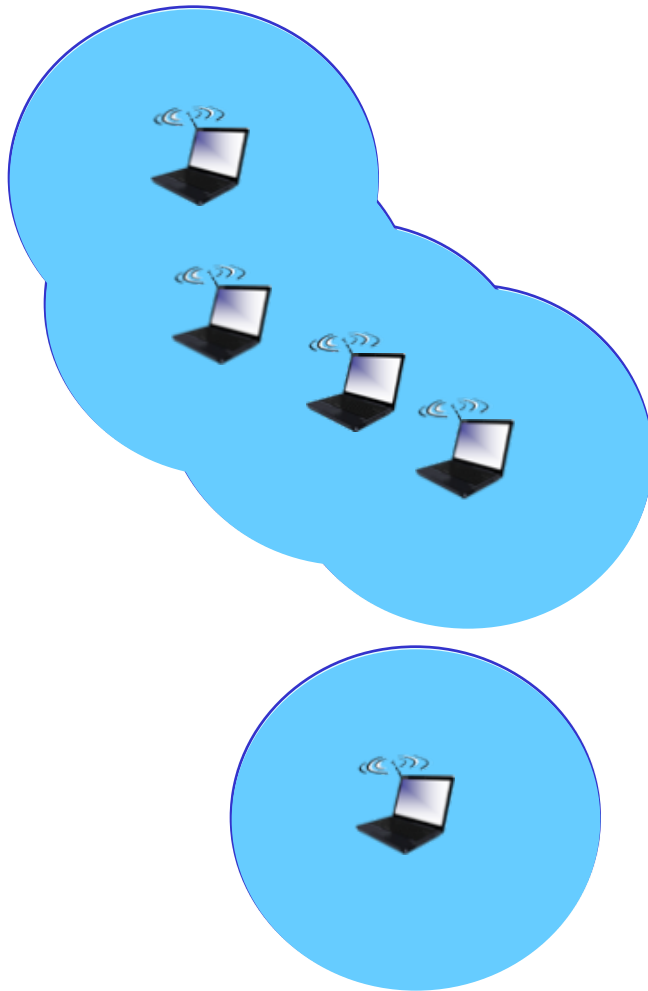
Characteristics of selected wireless links



Elements of a wireless network



Elements of a wireless network



ad hoc mode

- no base stations
- nodes can only transmit to other nodes within link coverage
- nodes organize themselves into a network: route among themselves

Outline

7.1 Introduction

Wireless

7.2 Wireless links, characteristics

- CDMA

7.3 IEEE 802.11 wireless LANs (“Wi-Fi”)

7.4 Cellular Internet Access

- architecture
- standards (e.g., 3G, LTE)

Mobility

7.5 Principles: addressing and routing to mobile users

7.6 Mobile IP

7.7 Handling mobility in cellular networks

IEEE 802.11 Wireless LAN

802.11b

- 2.4-5 GHz unlicensed spectrum
- up to 11 Mbps

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

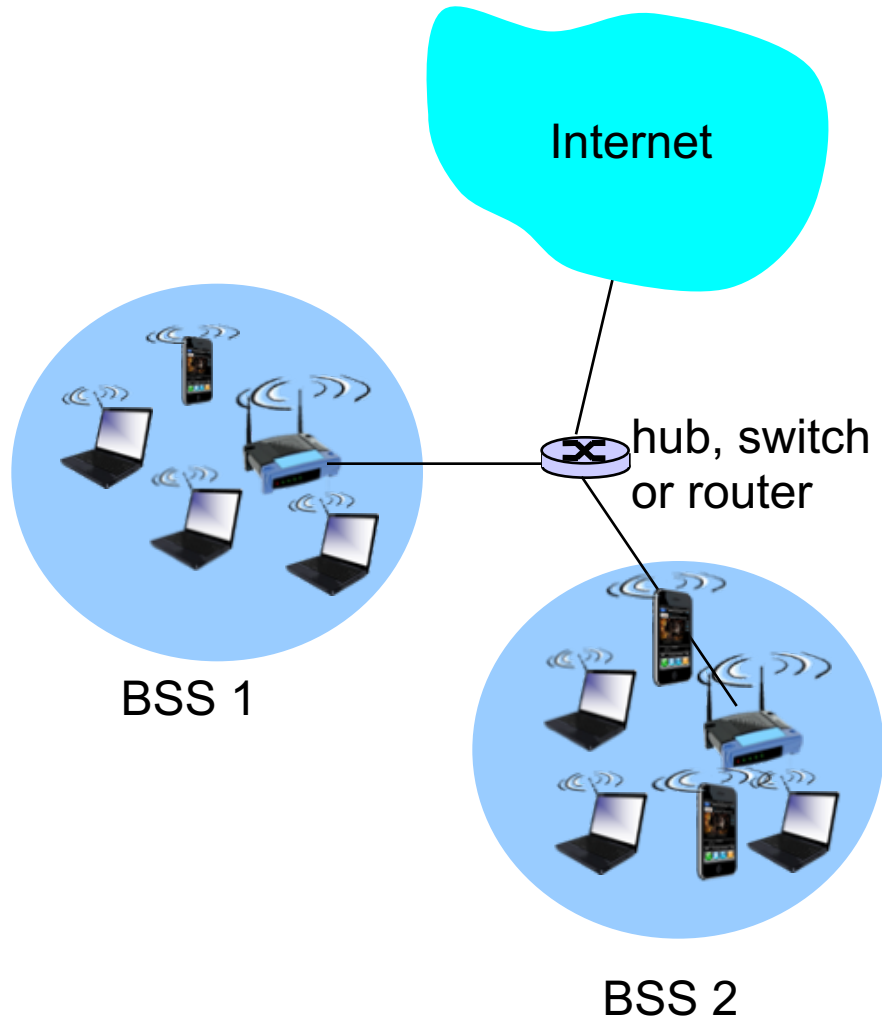
- 2.4-5 GHz range
- up to 600 Mbps

802.11ac: multiple antennae

- 2.4-5 GHz range
- up to 1300 Mbps

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

802.11 LAN architecture

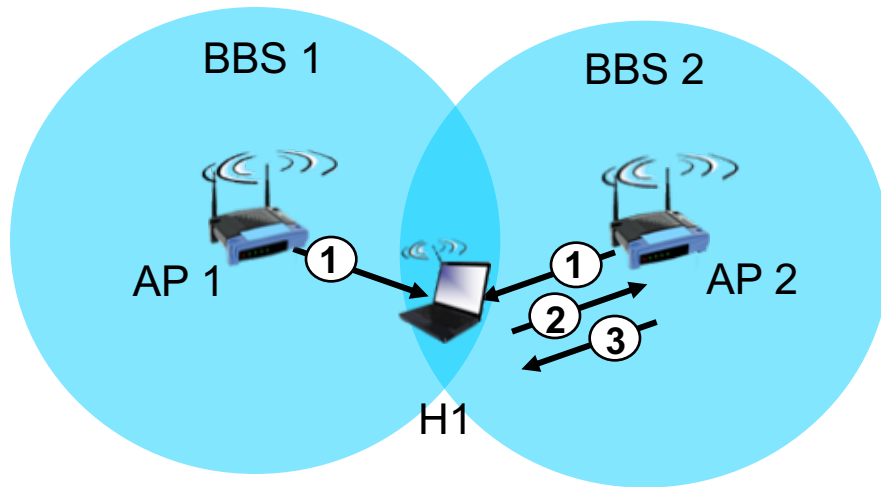


- wireless host communicates with base station
 - **base station = access point (AP)**
- **Basic Service Set (BSS)** (aka “cell”) in infrastructure mode contains:
 - wireless hosts
 - access point (AP): base station

802.11: Channels, association

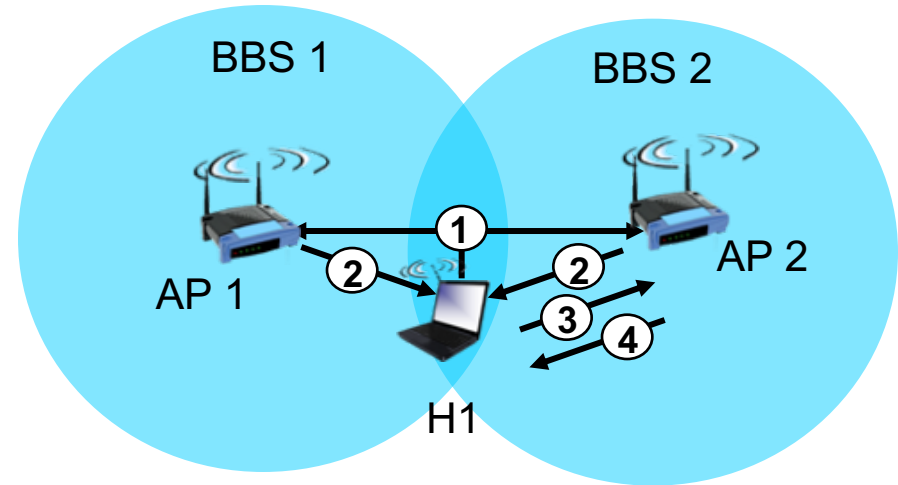
- 802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies
 - AP admin chooses frequency for AP
 - interference possible: channel can be same as that chosen by neighboring AP!
- host: must *associate* with an AP
 - scans channels, listening for *beacon frames* containing AP's 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

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

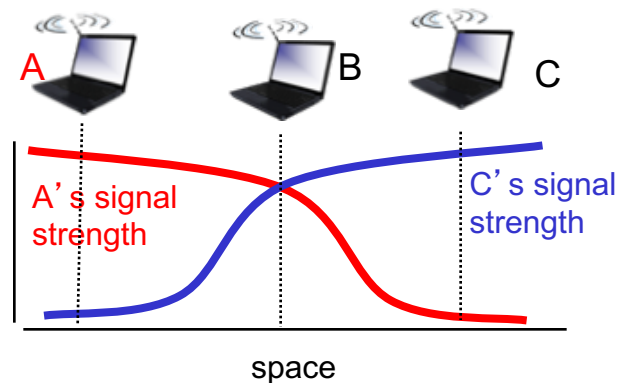
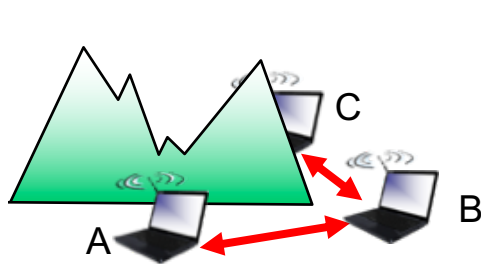


active scanning:

- (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

- 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!
 - can't sense all collisions: hidden terminal, fading
 - goal: *avoid collisions*: CSMA/CA (Collision Avoidance)



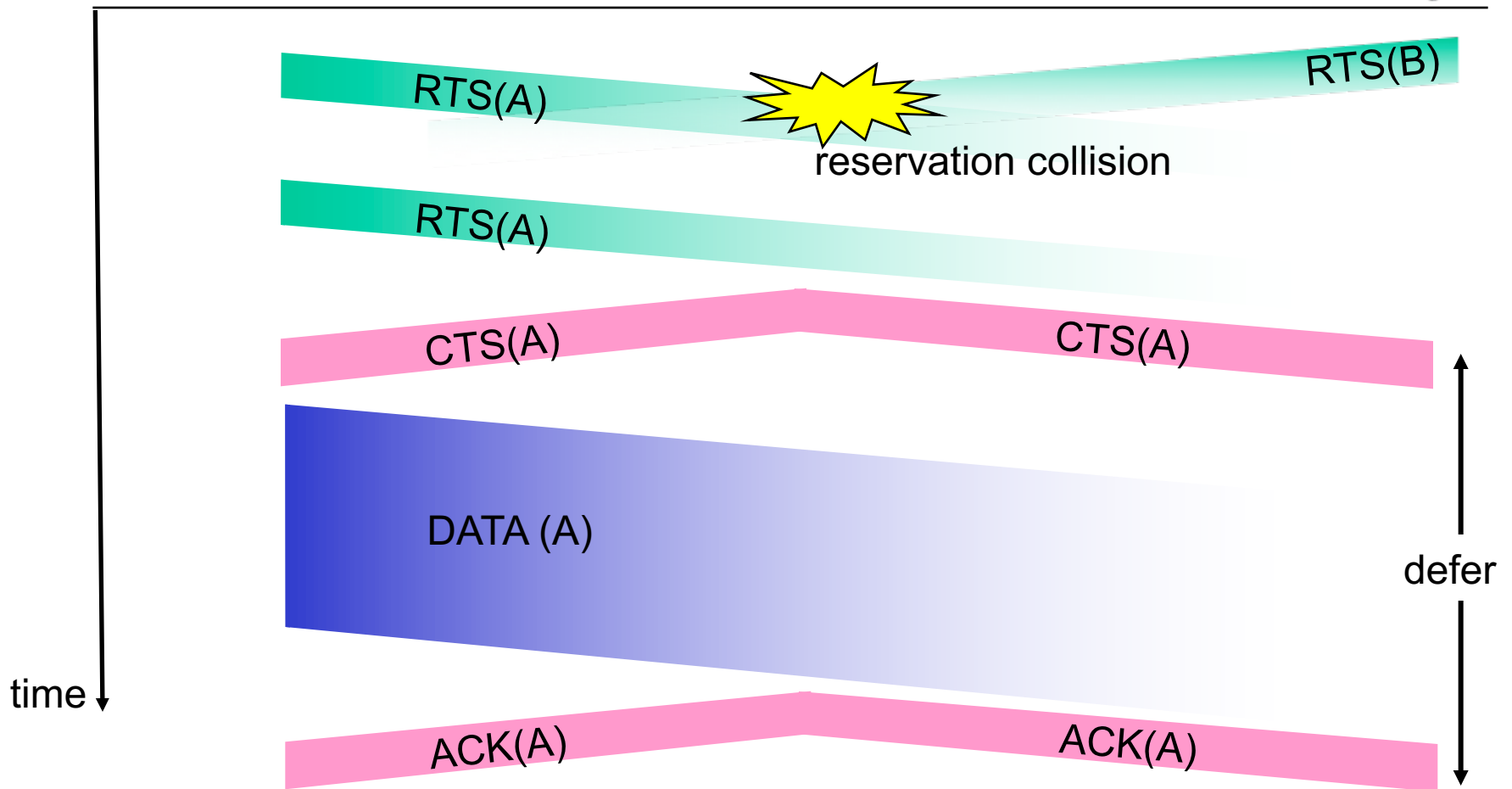
Avoiding collisions

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
- CTS (with sender’s ID) 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



Next Week

- Cellular network
- Exam review