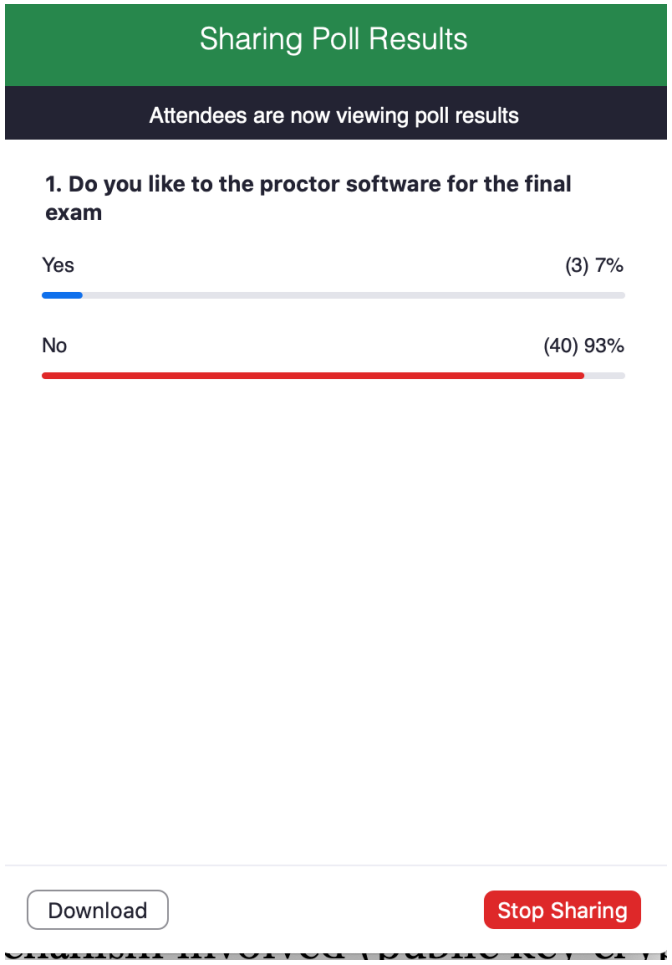
Final Review

The final exam

- Open notes, open book
- Will be on Avenue, set up as a quiz
- McMaster standard Casio FX-991 or MS Plus calculator allowed
- Types of questions:
  - True or False
  - Fill in black
- All-in-one slides will be posted on Avenue
- Office hrs:
  - Monday 4:30 – 5:30pm or by appointment
  - Will answer questions on Piazza
- Please resolve all grading (assignments, quizzes) related issues by April 23rd



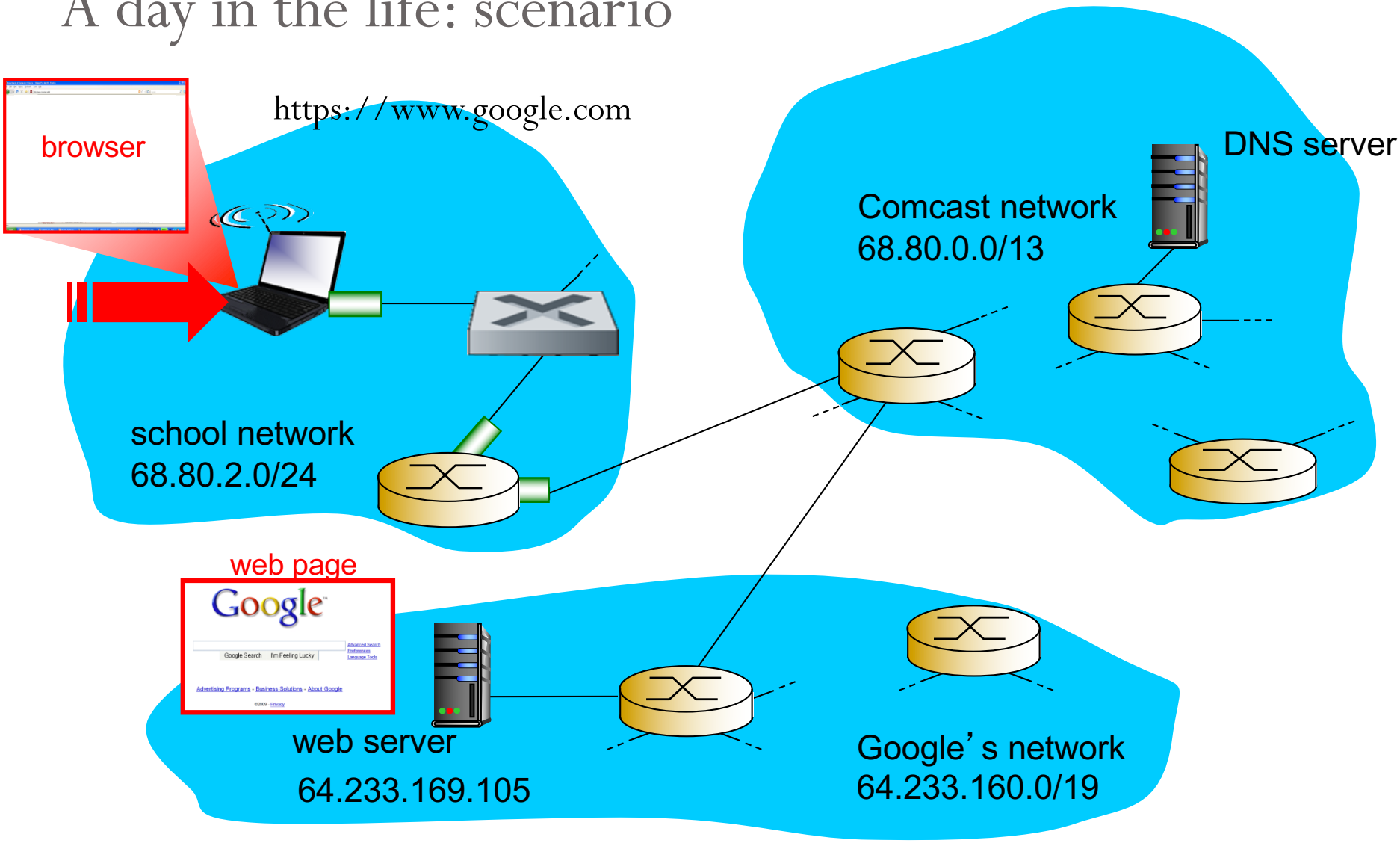
In-class polling result

No proctor software will Be used!

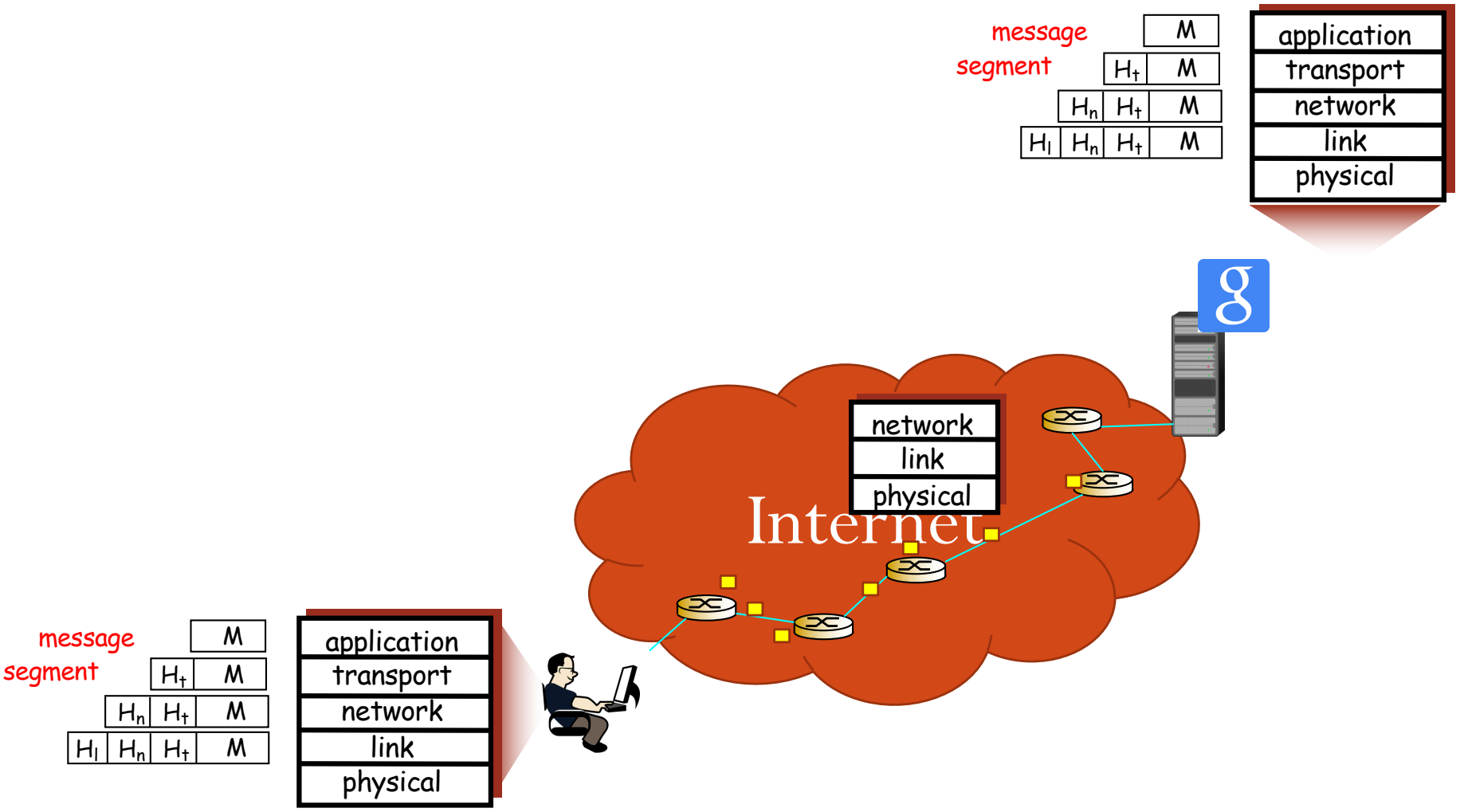
Review Tips

- Go over the "A day in the life of a web request" walkthrough → extend it to "A day in the life of a web request over HTTPs via MacWiFi (enterprise WPA2)"
  - Make sure you understand the protocols and network elements involved
- Make sure you understand all the quiz solutions

A day in the life: scenario



Coverage


message segment
M
H_t M
H_n H_t M
H_l H_n H_t M
application
transport
network
link
physical
network
link
physical
Internet
message segment
M
H_t M
H_n H_t M
H_l H_n H_t M
application
transport
network
link
physical

Application layer

- HTTP
  - Persistent vs non-persistent
  - HTTP request and response headers
  - Cookies
- DNS
  - DNS server hierarchy
  - Recursive and iterated DNS query
  - DNS query/response format

Transport Layer

- Error detection: Internet checksum
- Reliability:
  - Use of ACK, sequence number, timeout, retransmission
  - Bandwidth-delay-product: BW x RTT
  - Delay on each hop: transmission delay + propagation delay + processing delay + queuing delay
- TCP
  - Connection setup and tear down
  - TCP header format
  - TCP congestion control and flow control
- UDP
  - header format

Network layer

- Protocols
  - IP v4 header format
  - IP v4 address dot decimal representation, subnet mask & subnet address (a.b.c.d/x)
  - DHCP: what does it do?
  - NAT: how does it work?
  - ICMP: which ICMP messages are used in traceroute?
  - Intra-domain: RIP, OSPF
- Algorithms
  - Dijkstra's algorithm
  - Distance vector algorithm
  - Configuration of forwarding table entries based on intra-domain

Data link layer

- Protocol
  - Functions of data link layer
  - MAC address, ARP
  - Ethernet, 802.11 frame format, 802.11 frame types
  - Contention and broadcast domains
  - CSMA/CD, CSMA/CA
    - When will collisions occur? Why exponential backoff?
    - Inter-frame spacing
  - Difference between hubs & switches
  - Composition of WLAN
  - Self-learning algorithm

Security

- Symmetric key vs public key cryptography
  - Needs for KDC and CA

$$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$$

- Digital signature using pubic key cryptography
- Message integrity using hash function or digest
- Authentication using symmetric key and public key cryptography
  - Why do the naïve ones fail?
- Security attacks & counter-measures
  - Mapping, IP spoofing, packet sniffering, DOS
  - Ingress filter, firewall, ARP, IP traceback
- SSL: how is authentication done and how is session key set up
- IPSec: AH vs. ESP, tunnel model vs. transport mode, SAs
- 802.11i: crypto mechanism involved (public key crypto, symmetric key crypto, nonce)
- Different types of firewalls