Lecture 26: Review and Overview of Final Exam

COMP 332, Spring 2018

Victoria Manfredi

WESLEYAN UNIVERSITY

Acknowledgements: materials adapted from Computer Networking: A Top Down Approach 7th edition: ©1996-2016, J.F Kurose and K.W. Ross, All Rights Reserved as well as from slides by Abraham Matta at Boston University, and some material from Computer Networks by Tannenbaum and Wetherall.

Today

1. Announcements
   - hw10 written due fFriday at 11:59p
   - office hours Thursday from 4-5:30p
   - office hours as usual next week
   - should have at least one help session next week
2. What have we covered?
3. Final exam overview

What have we covered?

… SINCE THE MIDTERM

Transport layer

- Congestion control
- Flow control
- Seq #s and ACKs

… not tested on midterm, so will definitely ask about

Network layer

- Router functions
- Internet Protocol
- Addressing
- Link-state vs. distance vector routing
- Intra-domain routing protocols
  - OSPF
- Inter-domain routing protocols
  - BGP

… spent multiple weeks on, so will get multiple questions on this material

Link layer

- ARP
- Ethernet and frames
- Switches (vs. Routers)

… spent 1 class on. Will definitely get a question on, but only so much that I can ask about link layer

Security

- Confidentiality
  - symmetric encryption
  - public key encryption
- Authentication
- Message integrity
- TLS
- IPsec
- Tor
- Decoy routing

… spent multiple weeks on, so will get multiple questions on this material

What will I definitely not ask you about?

- How to derive keys for public-key cryptography
- IPsec
- Decoy routing

What should you definitely review?

TCP finite state machine

- when/why state transitions occur
- what information is important to keep track of

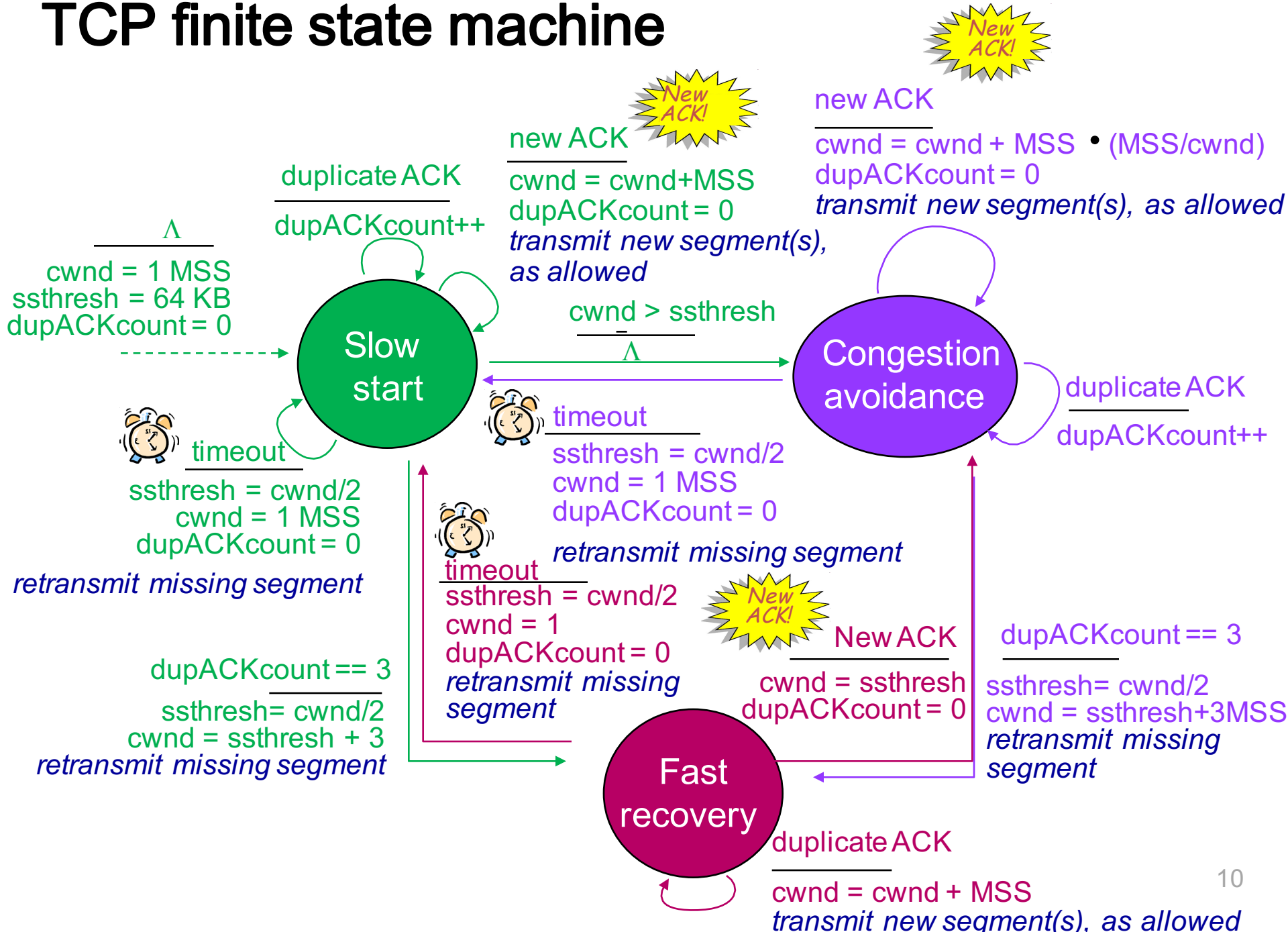
A day in the life of a web request

- can you fit all protocols we've covered in to this?
  - including TLS, BGP, OSPF, …
  - what lower layer protocols do upper layer protocols run over?
  - what protocols need to execute depending on what info is available?

Network and link layer addressing

- when, why both?
- how is each used?

TCP finite state machine



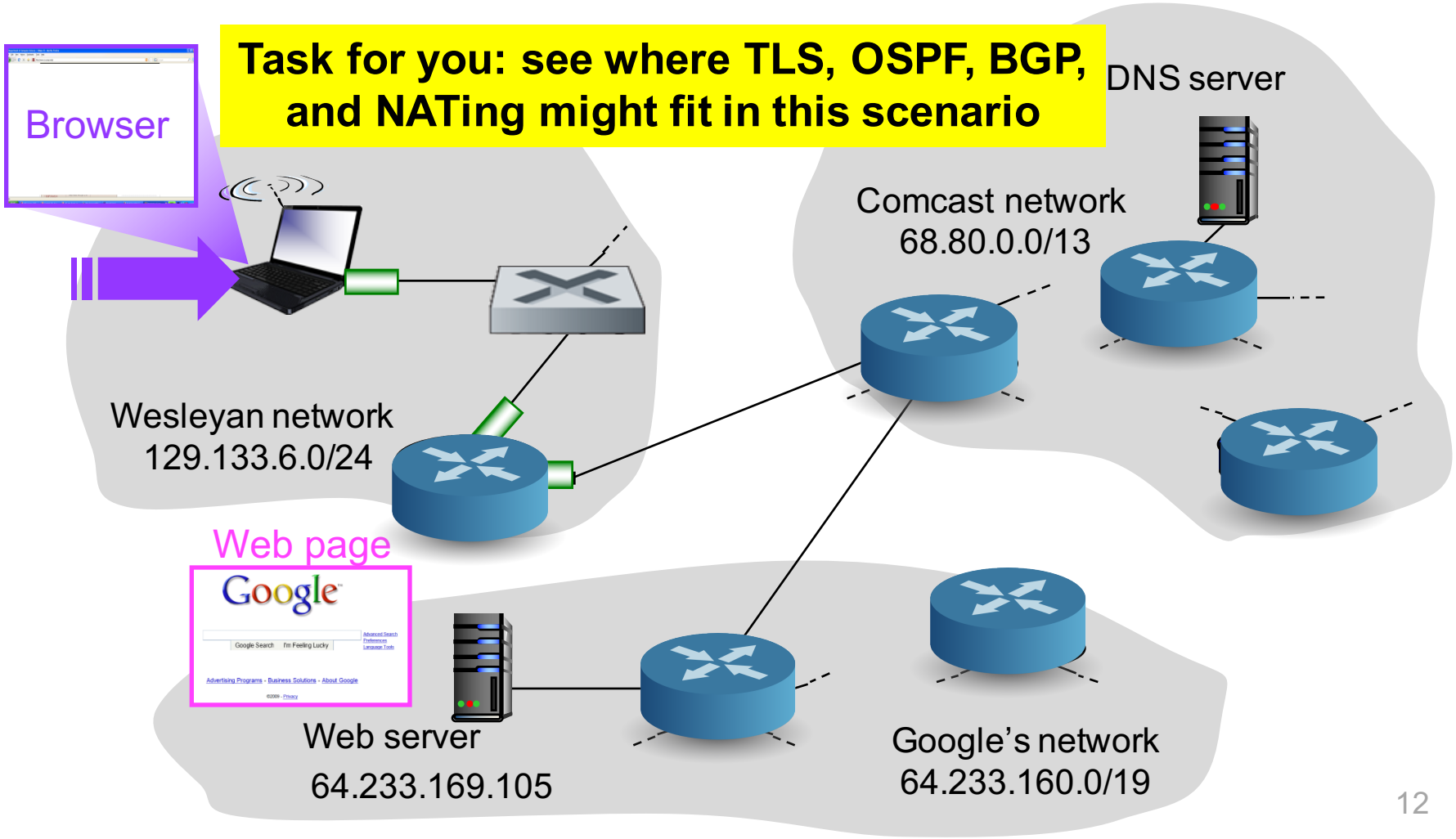
Summarizing Example

A DAY IN THE LIFE OF A WEB REQUEST USING HTTPS

What really happens when you enter URL?

Scenario: student attaches laptop to campus network

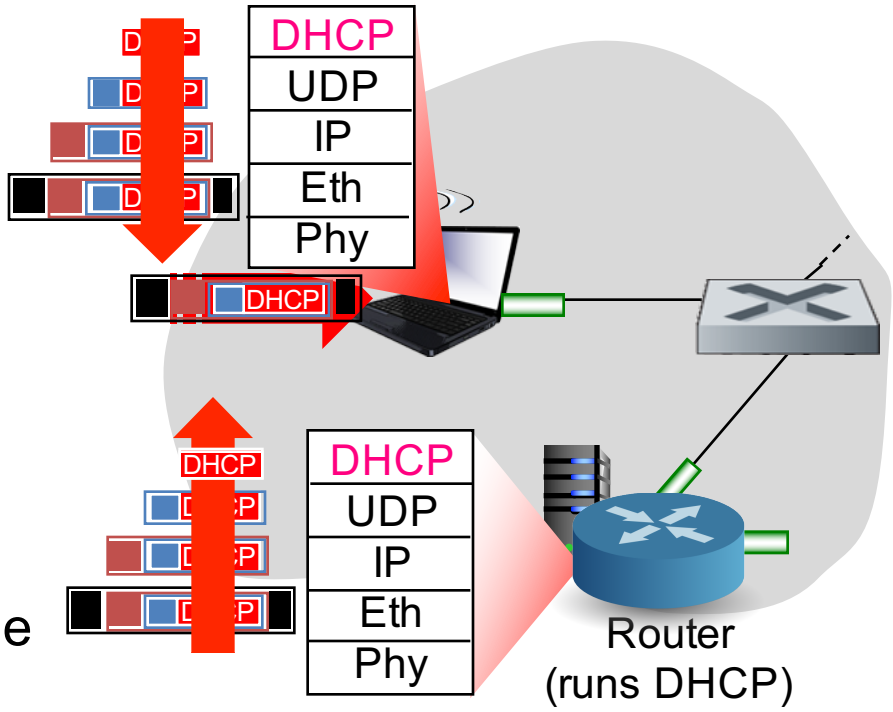
– requests/receives www.google.com



How does client connect to Internet?

Client needs

- its own IP addr on network
- IP addr of first-hop router
- IP addr of DNS server



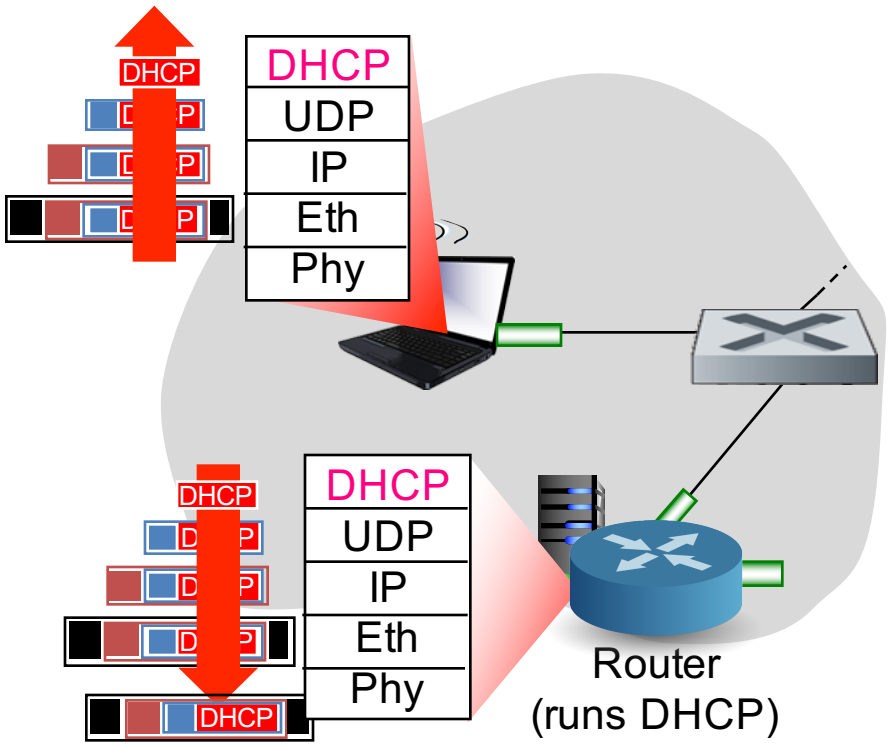
How? DHCP request

- encapsulated in UDP
- encapsulated in IP
- encapsulated in Ethernet frame
- broadcast on LAN
  - dst: FF-FF-FF-FF-FF-FF

Router running DHCP server receives DHCP request

- Ethernet demuxed to IP demuxed to UDP demuxed to DHCP

How does client connect to Internet?



DHCP server sends DHCP ACK

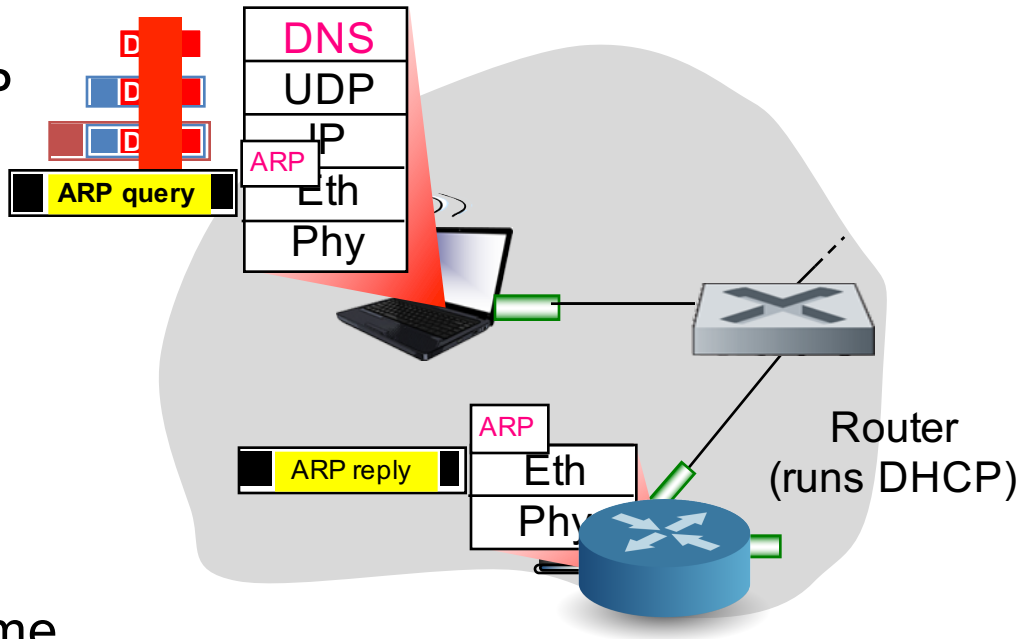
- contains
  - IP addr assigned to client
  - IP addr of 1st-hop router
  - name & IP addr of DNS server
- encapsulate
  - in UDP, then IP, then Ethernet frame
- forward to client
  - through LAN via switch

Client receives DHCP ACK, now has its **own IP addr**, knows name & IP addr of **DNS server**, IP addr of its **1st-hop router**

Client now needs IP addr of www.google.com

DNS query created

- encapsulated in UDP
- encapsulated in IP
- encapsulated in Ethernet



Client needs MAC addr of router

- to send Ethernet frame
- broadcasts ARP query

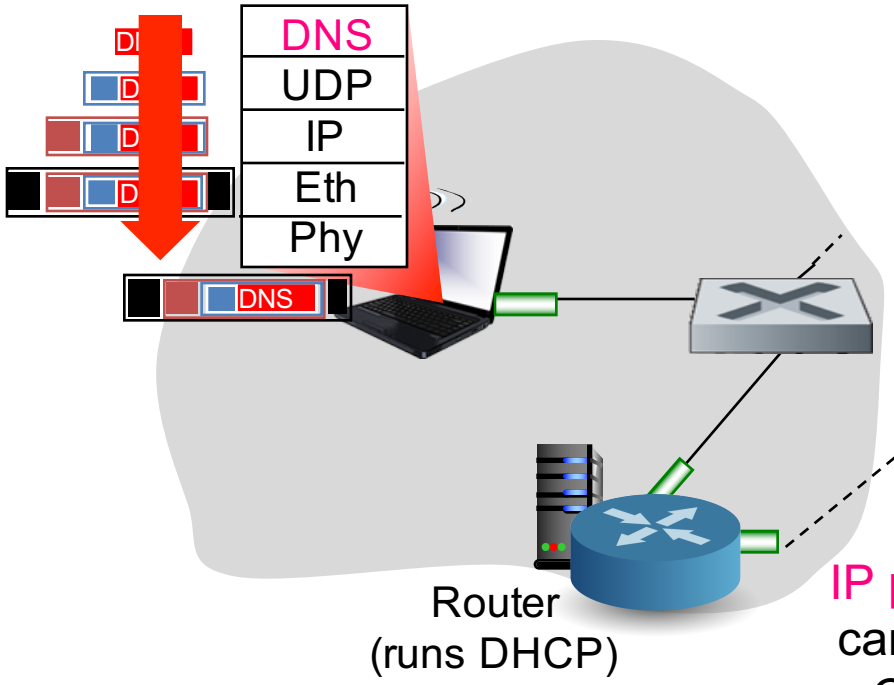
Router receives ARP query

- sends ARP reply with MAC addr of router interface

Client now has its **MAC addr of 1st-hop router**, can now send frame containing DNS query

Client now needs IP addr of www.google.com

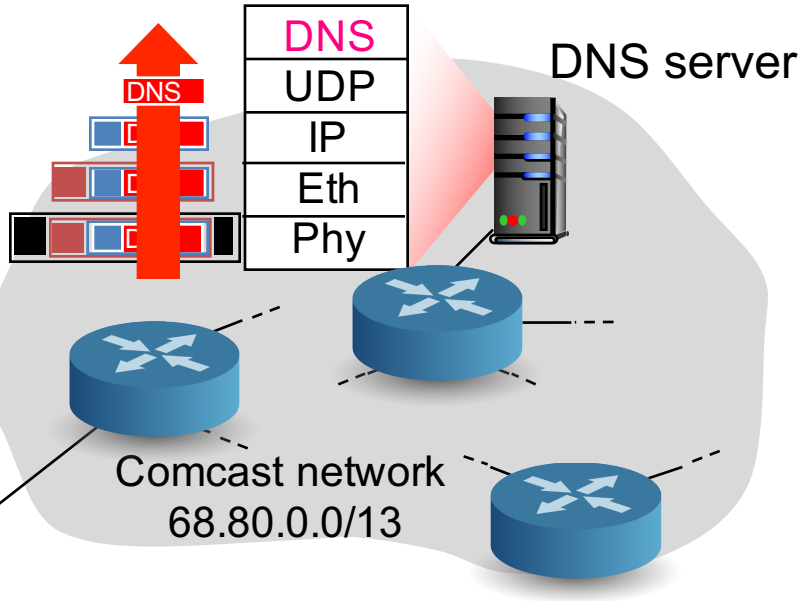
IP pkt containing DNS query forwarded via LAN switch from client to 1st hop router



Router (runs DHCP)

IP pkt forwarded from campus network into Comcast network

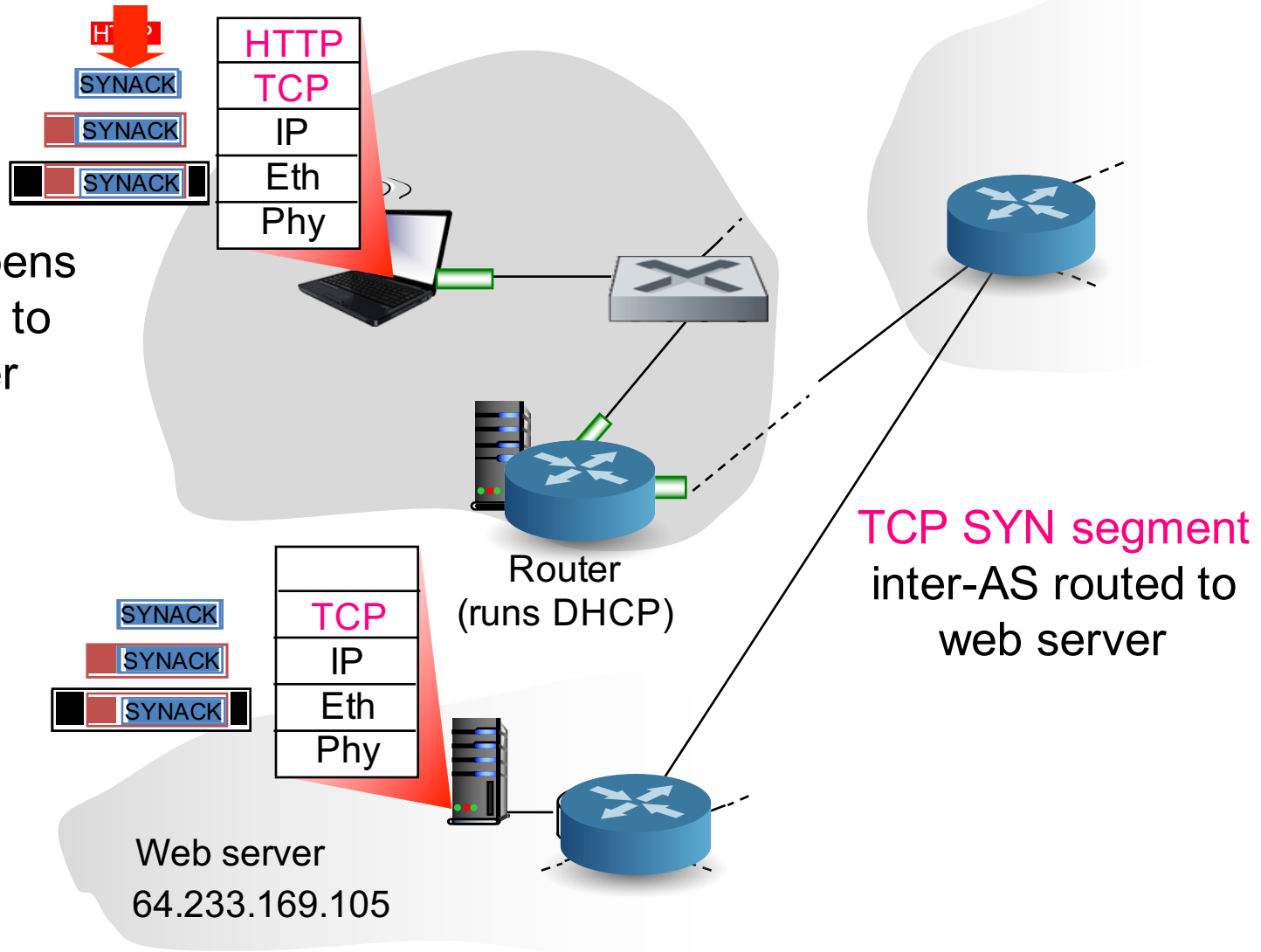
DNS server replies to client with IP addr of www.google.com



Routed to DNS server using tables created by e.g., OSPF and BGP

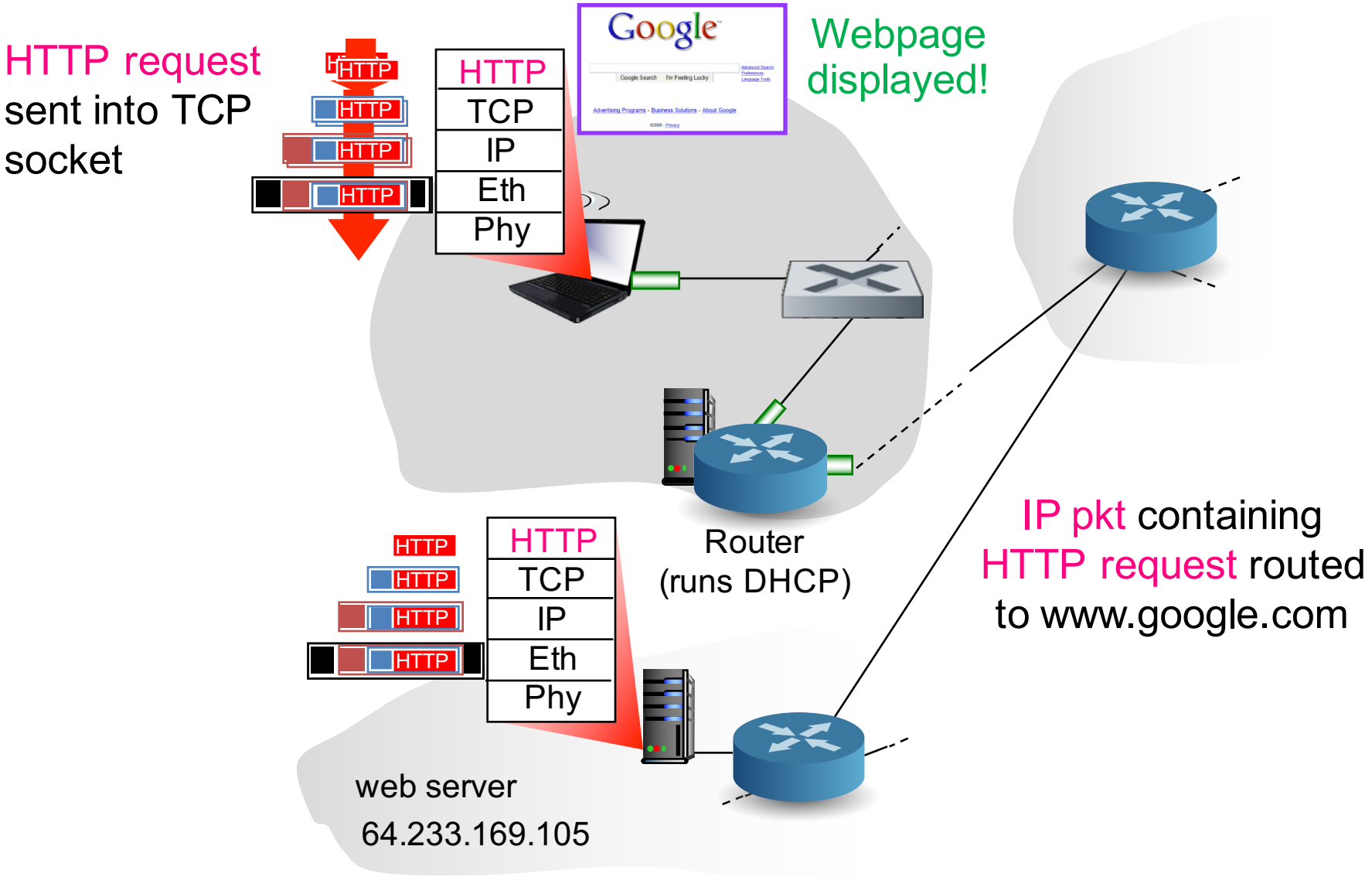
Client now has **IP addr of www.google.com**, can now open TCP conn to send HTTP request

Client opens TCP connection to carry HTTP



Web server responds with TCP SYNACK and client replies with TCP ACK. Connection established!

Client sends HTTP request and receives reply



Web server responds with IP pkt containing HTTP reply (containing webpage) routed back to client

Final

OVERVIEW

Final overview

In our normal classroom on Wed., May 16 from 9a-12p

- closed book, closed notes
- covers primarily material in lectures 13 to 25

5-6 questions

- transport layer short questions
- network and link layer short questions
- security short questions
- given a network, answer questions about it
- design a secure communication protocol
- challenge question

Problem 1 to 3 – 10 points each

Similar to review questions in book, should only need to write a few sentences to answer

Problem 1: transport layer short questions

- 3 in total

Problem 2: network and link layer short questions

- 5 in total

Problem 3: security short questions

- 3 in total

Problems 4 – 10 points

Given network answer questions

- what protocols are used and where?
  - TLS, ARP, DNS, BGP, …
- how is addressing done?
  - network-layer
  - link-layer
- what if NAT is in use?

Problem 5 – 10 points

Given scenario, design a secure data transfer protocol

- E.g., suppose that Alice has a data file, d, that Bob needs.
  - Alice and Bob want to make sure (i) that if anyone intercepts the file during its transmission, then they cannot understand its content.
  - Bob also wants to know (ii) whether or not whatever is transmitted from Alice to Bob has not been corrupted or altered in transit, and
  - (iii) that the file was sent by Alice
    - Bob will only need to convince himself of that, no one else
  - Finally, (iv) Bob and Alice are computationally limited, so their goal is to transfer the file while meeting criteria (i) to (iii) above, but at the same time, being computationally efficient.
  - You may assume that:
    - Symmetric key. Alice and Bob share a secret symmetric key that no one else knows, and Bob and Alice both know that no one else knows it.
    - Public keys. There is a public key infrastructure available (e.g., a CA that has Bob and Alice's public keys, and that the public key of the CA is known to Bob and Alice).

Problem 6 – 5 points

Something to challenge you …

- haven't yet decided if/what this question will be

More questions

TEST YOURSELF

True or False?

Each network adapter has a unique MAC address

- do switches use these MAC addresses when forwarding frames?

For Ethernet, if an network adapter determines that a frame it has just received is addressed to a different adapter

- it discards the frame without sending an error message to the network layer
- it discards the frame and sends an error message to the network layer
- it delivers the frame to the network layer, and lets the network layer decide what to do
- it sends a NACK (not acknowledged frame) to the sending host

True or False?

In a distance-vector routing algorithm, each node has a map of the entire network and determines the shortest path from itself to all other nodes in the network.

The network portion of an IP address is the same for all the hosts on the same IP network.

… choose one

The link-state algorithm has the following properties:

- it requires the source node to know the costs between every pair of adjacent nodes in the graph
- it determines the shortest path from the source node to all other nodes
- after the kth iteration, the least-cost paths are known to k nodes
- all of the above

The ARP protocol

- runs on top of TCP
- runs on top of UDP
- runs directly on top of IP
- none of the above

… choose one

As part of hierarchical routing, hot-potato routing does the following

- Labels suspicious packets as “hot”.
- Chooses the gateway (border router) that has the smallest cost.
- Determines the number of ASes in the shortest AS path from router to destination.
- Provides information to a router about the existence of external networks.

Every autonomous system must use the same intra-autonomous system (domain) routing algorithm.

- True
- False

… choose one

In routing among ASs, which of the following issues dominates:

- geographical distance between ASs
- policy
- number of ASs traversed
- current congestion levels in the ASs

In the BGP routing algorithm, each AS advertises to its neighbors its estimates of the shortest distances from the AS to all possible destination ASs.

- True
- False