Lecture 26: Wrap-up

COMP 332, Spring 2024

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 Avi Kak's lecture 12 slides at https://engineering.purdue.edu/kak/compsec/

Today

1. Announcements
   - Homework 9 due Today at 11:59p
   - Office hours today: 2-3p
   - Office hours next week
     - Tues, May 14 from 1-2:30p
     - Wed, May 15 from 1-2:30p
   - CA review session
     - Thursday, May 16 from 1-3p in Exley 638
   - Final exam
     - Friday, May 17 from 9-12p in our normal classroom
     - Will post a practice final exam
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 really tested on midterm, so will probably 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 classes on, so will get multiple questions

Link layer

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

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

Security

- Confidentiality
  - Symmetric encryption
  - Public key encryption
- Authentication
  - Certificate authority
- Message integrity
  - Hash functions
- TLS
- IPsec (only a few things that I could ask you here)

… spent multiple classes on, so will get multiple questions

What will I definitely not ask you about?

- How to derive keys for public-key cryptography

What should you definitely review?

TCP finite state machine

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

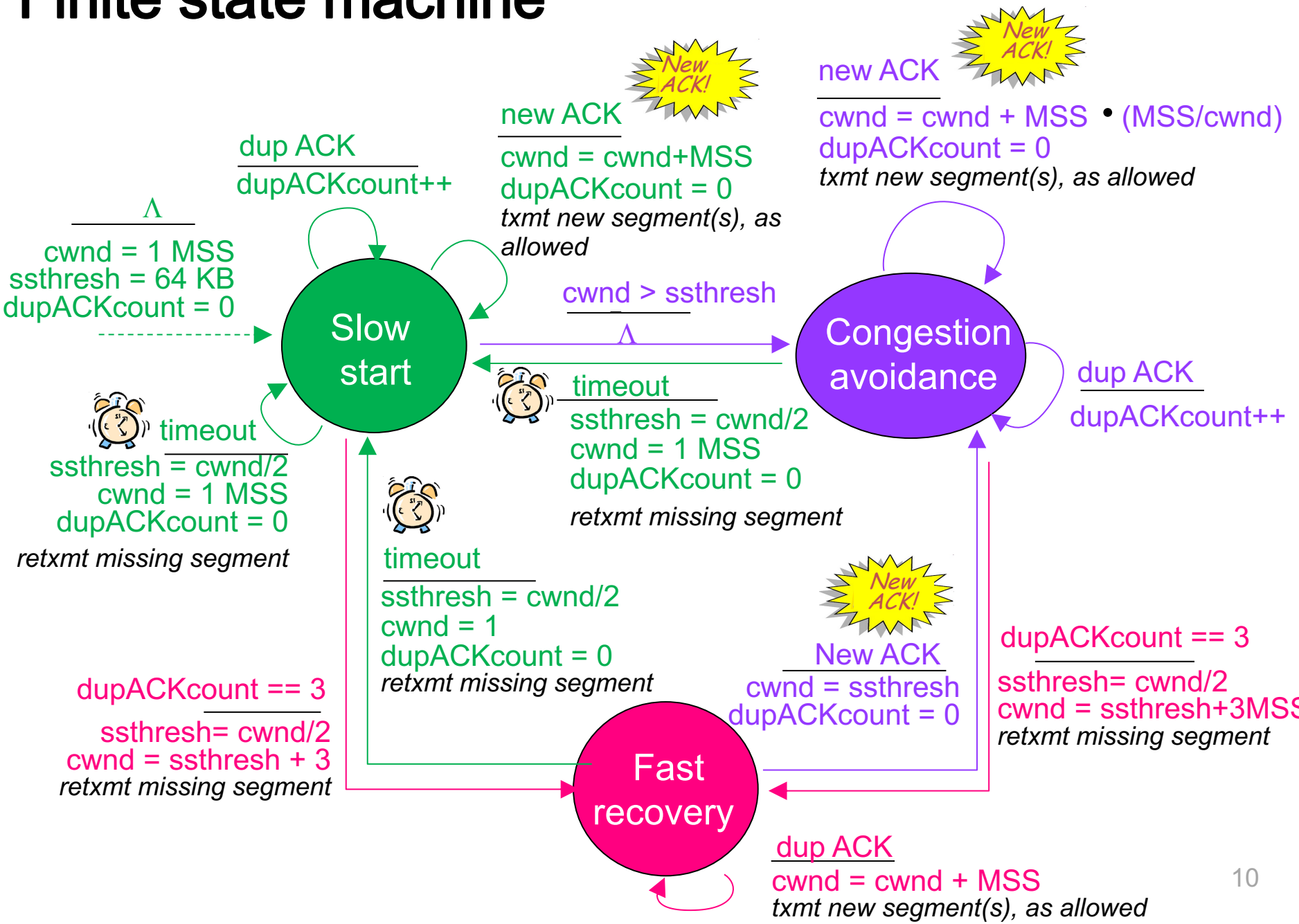
A day in the life of a web request

- can you fit all protocols we've covered into 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?
- think about number of RTTs incurred too

Network and link layer addressing

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

Finite state machine



Final

OVERVIEW

Final overview

In our normal classroom on Friday, May 17 from 9a-12p

- closed book, closed notes
- cumulative but covers primarily material since midterm

5 to 6 questions

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

Problem 1 to 3

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

Problem 4

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

Given scenario, design secure data transfer protocol

- e.g., suppose that Alice has a data file, d, that Bob needs.
  1. Alice and Bob want to make sure that if anyone intercepts the file during its transmission, then they cannot understand its content.
  2. Bob also wants to know whether or not whatever is transmitted from Alice to Bob has not been corrupted or altered in transit, and
  3. that the file was sent by Alice. Bob will only need to convince himself of that, no one else
  4. Bob and Alice are computationally limited, so their goal is to transfer the file while meeting criteria 1-4 above, but at the same time, be computationally efficient.

  You may assume:

  - 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

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 a 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

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

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

- True
- False