

# Spring 2016 Computer Networking PhD Qualifying Exam

## 1. Managing Congestion in the Internet

Network congestion occurs when demand for resources exceeds capacity. The result is a degradation of performance, which can be severe if not addressed directly. Over the years, a wide variety of mechanisms have been developed to address congestion and it is still an active area of research.

- a) Describe the basic mechanisms implemented in the Reno version of TCP to address network congestion. Why have there been so many new versions of TCP since Reno?
- b) Several end-to-end mechanisms have been proposed to *avoid* congestion. Name one of these mechanisms and describe the basic algorithm for avoiding congestion. Have these mechanisms proved to be popular - why or why not?
- c) In contrast to end-to-end congestion avoidance, mechanisms for managing congestion *within* the network have also been developed. Give the name of one of these mechanisms and explain the basic algorithm. Have these mechanisms proved to be popular - why or why not?

## 2. Measuring Network Properties

Understanding the Internet from an empirical perspective can serve as a foundation for developing new protocols and systems, and for managing a network effectively.

- a) Describe two basic methods for gathering data from the Internet. Compare and contrast these methods by providing three strengths and three weaknesses of each.
- b) Network traffic measurement is a fundamental task, which has implications in both research and operations. Describe how traffic measurement is typically done within an administrative domain, and how this process can be tuned to shed light on events in traffic streams that would be of interest to network operators.
- c) Describe a method that can be used to measure a service provider's topological structure. What are the challenges in this approach to network topology analysis and how might they be overcome?

## 3. Wireless medium access

- a) A hidden terminal is considered a classic problem in random access wireless environments. How does 802.11 based systems attempt to solve this problem?
- b) Does the 802.11 standard solve the exposed terminal problem? If yes, explain how it solves the problem. If no, explain how exposed terminals are prevented from simultaneous communication.
- c) In the Opportunistic Auto Rate adaptation protocol, if the achievable data rates of two backlogged clients, A and B, are 11 Mbps and 1 Mbps respectively, what is the actual data throughputs achieved by each client when they are the only active wireless transmitters in the system. Make any necessary simplifying assumptions. Why is this an improvement over the basic 802.11 standard.

## 4. Multicast

The original IP multicast scheme from Cheriton and Deering was proposed for an intra-domain setting. Several attempts were made to extend IP multicast to the wide-area/inter-domain settings.

- i) Describe two reasons why the vision of inter-domain IP multicast was never realized.
- ii) Overlay-based multicast systems have been proposed to realize inter-domain multicast. Describe two downsides to realizing multicast using purely end host-based mechanisms.
- iii) In reliable multicast, any data transmitted by a source should be delivered to all group members reliably. Which of the two schemes, native IP multicast or end-host multicast, is more amenable to implementing reliability semantics? Why?

## 5. Overlay Routing

Overlay networks can help overcome the limitations imposed by the Internet's wide-area routing protocols (BGP and various interior gateway protocols). Consider an example where an overlay provider is offering routing service to users. The provider has overlay nodes deployed across various ISPs within the Internet.

(a) While using overlay networking is beneficial, it can create significant issues. Explain these issues in the context of:

- (i) An Internet Service Provider where overlay nodes are hosted
- (ii) The overlay service provider

(b) Using the example of an application and a corresponding performance metric, describe a situation where leveraging overlay routing can result in worse performance for the application than using traditional BGP paths.

## 6. Caching, DHTs, and Security

a) The automated worm fingerprinting paper advocates deploying custom algorithms on Internet routers to detect worms.

- (i) Explain the benefits of detecting worms in the core of the Internet.
- (ii) In-network worm detection as suggested by this paper is no longer effective. Provide three reasons why this is the case.

(b) The performance of Web caching can be improved by using multiple caches, essentially implementing a distributed cache. Consider an enterprise network that has deployed a family of caches  $F$  to improve Web access performance its employees experience.

(i) Describe how a distributed hash table such as Chord can be used to build an efficient distributed cache across the family of caches  $F$ .

(ii) When does your DHT-based distributed cache offer worse performance, even when content experiences a "hit", than using a single cache?

(iii) How can you improve your DHT-based cache to overcome the performance issues identified in (ii) above?