Networking Qualifying Examination
Computer Sciences
Spring 2013

Please answer all six questions below.

A. Design principles

1. (a) Explain the principle of fate sharing.

   (b) Explain why stateful middleboxes such as firewalls violate fate sharing.

   (c) Is fate sharing an important principle today? Why or Why not? Explain briefly.

2. (a) The end-to-end principle results in a dumb network and smart hosts. List three pros and three cons of this.

   (b) Give an example where the end-to-end principle is violated today.

B. TCP on the Internet

TCP is the dominant protocol for data transfer on the Internet.
Let us consider two alternative ways of using TCP to send traffic across a N-hop Internet path: (i) There are N TCP flows, one between each hop on the path and traffic flows across them from source to destination and (ii) TCP is run end-to-end between the two endpoints of the path.

a) Which of the two alternatives achieve a higher end-to-end throughput and why?

b) Which of the two alternatives achieve a lower end-to-end latency and why?

c) The basic design of TCP Reno does not always perform well when there is one or more wireless hops in the end-to-end path. With an example, explain why this is so?

C. Multicast

The goal of multicast typically is to send the same content efficiently from a given source to multiple receivers. Multicast functionality on the Internet have been explored in at least two layers --- network layer and application layer.

a) What are the reasons for which a network layer multicast service has not gained significant popularity in the Internet?
b) Which of the above issues can be addressed by an application-layer multicast solution?
c) A digital fountain approach is considered a useful way to implement reliable multicast solutions. Is this technique equally efficient for unicast communication as well? Explain why or why not.

D. Availability
Consider an end-to-end Internet transaction between a smartphone and a server in the cloud.

a) Describe the various factors that could cause the transaction to fail.

b) What steps can the entity owning the server (e.g., the corresponding content provider) take to improve resilience of the transaction despite the fact that it cannot control many of the underlying factors causing failures?

E. Network Traffic Measurement
Understanding the behavior and characteristics of network traffic is of intrinsic importance to the design, implementation, deployment and management of new systems. However, gathering network traffic data and analyzing it thoroughly is fraught with challenges.

a) Provide a description of two basic methods for gathering data on network traffic behavior. Name two challenges for each of these methods and describe how those challenges be addressed toward the goal of compiling accurate and representative data.

b) Traffic from different applications (e.g., email or web) has been shown to exhibit a range of characteristics in different studies over the years. Describe how one might analyze application specific data toward the goal of improving the protocols or systems related to an application. Use one application as an example in your answer.

c) The Border Gateway Protocol (BGP) is singularly important in the Internet since it is used by all providers to establish inter-network paths. How would one measure the behavior of BGP and what are the pitfalls in such measurements?

F. Network Security
Over the past decade, there has been a gigantic increase in the quantity and diversity of Internet threats. Recently, there have been widely publicized reports on highly sophisticated next generation malware such as Stuxnet, which was alleged to have been developed by state-sponsored actors to disable Iran's nuclear facilities.

a) What are the basic objectives of a network security architects, what are the key components of a network security infrastructure and how are these components deployed and managed within a network infrastructure?

b) The current generation of malware that is typified by Stuxnet represents a multifaceted threat. Describe at least four different key characteristics of malware and how IT security professionals can design systems to detect and prevent the spread of such malware.

c) From the perspective of malware authorship, describe three ways in which you might write code that can overcome standard security deployments.