Computer Sciences Department
Networking Qualifying Exam
Fall 2013
All parts of all six questions must be answered.

1. **Congestion Control**

   Multiple techniques for effective congestion control have been proposed in the literature. Two alternatives that have been considered are end-host based mechanisms and router-based mechanisms.

   a) Describe briefly one end-host based congestion control mechanism and a router-based mechanism. Compare the advantages and disadvantages of each approach.

   b) Pick any one of the router-based congestion control mechanisms and explain if and why it is a better queueing discipline than the standard drop tail mechanism?

   c) Explain the "Fast Retransmit" technique in TCP and why it's necessity.

2. **Wireless Systems**

   a) Two alternative approaches to handle link layer losses in the wireless medium are the Snoop protocol and the Split TCP approach. Explain the advantages and disadvantages of each.

   b) Should static wireless mesh networks use reactive routing protocols such as AODV or DSR. Explain why or why not?

   c) RTS-CTS messages are rarely used by most WiFi devices today. Explain why.

3. **Border Gateway Protocol**

   Suppose two Autonomous Systems (ASes) A and B want to communicate with each other over the wide-area Internet using BGP. Which of the following two security properties can the ASes ensure for their routes? In each case describe what mechanisms would they need to use to ensure these properties.

   (a) when a server in AS A sends traffic to a server in AS B, it actually reaches the intended destination server in B and not to a malicious server
   (b) a malicious adversary C cannot intercept and sniff the above traffic between the servers in these two ASes, A and B

4. **Network Architecture and Multicast**

   a) State the end-to-end principle.

b) If one were to strictly follow this principle, where would it would be best to implement:

(i) Intra-domain multicast? In the network, or within end-points
(ii) Internet-wide multicast? In the network, or within end-points

Give a clear explanation of how adhering to the end-to-end principle leads to your answer.

5. **Network Measurement and Service Level Agreements**

Service Level Agreements (SLAs) are contracts between a network service provider and its customers. One of the central components of an SLA is the performance guarantees that are made to customers. Since network conditions are dynamic and violations of SLA can lead to penalties for the network provider it is critical that they measure and monitor their infrastructures to ensure they meet the specified guarantees.

a) Name three different performance metrics that are important to monitor in order to ensure that service level agreements are met.

b) Describe how these SLA metrics can be measured in provider networks and the challenges in making these measurements.

c) Describe the support infrastructure that is required for making the measurement of SLA metrics.

6. **The Evolving Web**

The World Wide Web continues to be one of the dominant applications on the Internet. However, to talk about the Web as a monolithic infrastructure is inaccurate since it has evolved and diversified so much over the years, and is likely to continue to evolve in the future.

a) Describe the basic protocols and system components that make up the Web and role that they play in a simple Web use scenario.

b) The evolving needs of web applications have led to the development of a variety of specialized infrastructures that support scalability, robustness and high performance. Give two examples of such infrastructures and describe how they interoperate with basic web components.

c) As e-commerce sites have grown, the web in general and those sites in particular have become high value targets for malicious activity. Give two examples of threats that have emerged and the security methods that have been developed to address these threats. Are these security measures effective?