Networking Qualifying Examination Computer Sciences

Fall 2011

Please answer all six questions below.

1) **Invariant Properties in Internet Packet Traffic**

Studying the Internet as an engineering artifact is based on careful instrumentation and measurement of the infrastructure. Over the years, an important objective of measurement-based study is identifying characteristics that are persistent over time or *invariant*.

a) Name and define the invariant property that characterizes network packet traffic in terms of an arrival process at a node in the Internet (hint: think about correlation structure). Provide a both a pictorial representation of this characteristic and a closed form mathematical expression.

b) Why was this property considered controversial when it was originally identified?

c) What is the standard explanation for the cause of this invariant property in packet traffic?

d) Are there any other invariant properties of Internet packet traffic?

2) **The Domain Name System**

The domain name system provides an invaluable mapping capability between alphanumeric names and IP addresses. Because of its importance, DNS has evolved in both scale and capacity to accommodate the on-going needs of Internet users.

a) Describe the basic components of the domain name system and how they interoperate.

b) How can DNS affect performance and how has the system has been enhanced to provide better performance?

c) How can the DNS be compromised by malicious parties and how has the system been enhanced to address these threats?

3) **Wireless networking**

The 802.11-based protocol has multiple mechanisms to deal with losses on the wireless medium. They include PHY rate adaptation and transmit power control.

a) On detecting a packet loss in the wireless channel, when should a transmitter use the PHY rate adaptation approach and when should it use the transmit power control approach, and why?

b) The Opportunistic Auto Rate (OAR) paper explains a method by which multiple 802.11 links can achieve time-based fairness. What mechanism does the OAR paper use to achieve this time-based fairness between multiple transmitters. Give a compelling example to explain.

c) Does the 802.11 standard solve the exposed terminal problem. If yes, explain how. If no, explain why not.

4) **Congestion control**

TCP is a transport layer solution for implementating congestion control in the Internet. Random Early Detection (RED) is a network layer based solution for implementing this functionality.

a) What are the advantages and disadvantages of each approach? You should consider an end-to-end TCP mechanism with no RED discipline in the path against no TCP-like congestion mechanism but RED implemented in routers in the path.

b) Compare the fairness properties of RED and TCP. In particular, consider two flows, one currently occupying more share of the bandwidth than the other. Like in a) you should consider an end-to-end TCP mechanism with no RED discipline in the path against no TCP-like congestion mechanism but RED implemented in routersin the path.

c) How much state does RED need to maintain per flow for its operation?

d) The RED approach, with its probabilistic packet drops is usually better for TCP flows when compared to a Drop Tail queueing discipline. Why?

5) **BGP Security**

BGP is the de-facto wide-area protocol that strings together multiple different points in the Internet and enables end-to-end reachability. However, BGP has several fundamental security problems.

a) Problems: BGP is susceptible to *(i)* prefix hijack/interception and *(ii)* malicious blackholing (without hijacking/intercepting the prefix). Describe using examples how each of these two attacks can be created.

b) Some solutions: *(i)* Explain how you can modify BGP to solve the route hijack/interception problem. *(ii)* Explain how you can modify BGP to solve the malicious blackholing problem. *(iii)* Both approaches are not adoptable today, and hence, ultimately ineffective at stemming the attacks. Explain why.

c) Suppose, as a stub network, your goal was to ensure that: *(i)* your traffic is protected from malicious interception and *(ii)* you can always be reached despite the potential for blackholing. Describe an easy-to-adopt, and backward compatible approach that you can use to meet your goals without relying on BGP modifications or other network support.

6) **Multicast and the end-to-end principle**

This question is about Internet-wide, multi-ISP-spanning multicast.

A classic argument that undercut most of the early design discussions of Internet-wide multicast functionality relates to the end-to-end principle: should mutlicast functions be implemented within the network, or "outside" of it? There are a variety of multicast functions spanning from group creating and management to sequencing and reliable delivery.

a) Start by first providing a list of functions that make up a multicast session. Then, describe which of these *must* be implemented in the end-host, and which *can* be implemented in the network.

b) How is Internet-wide multicast realized today? Is the current realization a violation of the end-to-end principle? Explain.