Networking Qualifying Examination
Computer Sciences
Fall 2018

Please answer all parts of all six questions below.

1) End-to-end and design principles

a) Articulate the end-to-end principle. Outline the advantages and disadvantages to network implementation and management of applying the principle.

b) NATs are considered an abomination by Internet architectural purists. One argument is that they lead to ossification (i.e., artificially limiting the nature of communications that applications can employ). Explain how NATs lead to Internet ossification. There is argument against NATs that is distinct for ossification. What is it?

2) Transport

a) Since the development of the Tahoe version of TCP in the late 1980's many new versions of TCP have been developed and deployed. Name two of the versions of TCP that improve on Tahoe and describe how these versions improve on Tahoe.

b) Describe how long (*i.e.,* in distance), high bandwidth end-to-end paths such as those found in dedicated research networks present challenges to TCP. Name two ways in which TCP could be enhanced to address these challenges.

c) Describe how short (*i.e.,* in distance), high bandwidth end-to-end paths such as those found in data centers present challenges to TCP. Name two ways in which TCP could be enhanced to address these challenges.

3) Routing

a) Illustrate using an example when BGP can get stuck in persistent oscillations. What is the underlying reason for BGP to be stuck in such oscillations?

b) Suppose you were tasked with designing a multicast *routing protocol* that must scale to and work across the entire Internet. How would you design such a protocol? What special router support would that need? Argue why such support can be feasibly realized.

4) Mobility support

Supporting continuous mobility, where a client device continuously exchanges data with the infrastructure while on the move was not a key design requirementof the original Internet. However, today it is a common way of Internet data access.

a) What design choices of the early Internet led to failure of such continuous mobility support.

b) Sketch a possible design that lends itself better to continuous mobility support.

c) The Domain Name System (DNS) and the Dynamic Host Configuration Protocol (DHCP) are two mapping services in the Internet. How could you use the existing DNS and DHCP systems better to improve mobility support for mobile users.

5) Wireless systems

Scheduled access methods have traditionally been popular with many licensed systems, while random access methods have found adoption among unlicensed ones.

a) Explain a scenario each where a) scheduled access is expected to perform better than random access systems and b) random access systems are expected to perform better than scheduled access mechanisms.

b) Consider a single WiFi transmitter and receiver pair that is communicating with each other using a single UDP flow. The data rate chosen by the PHY layer is 54 Mbps. Assuming there is no data frame losses in the channel and no sources of interference in the vicinity. The realized application layer throughput is close to 30 Mbps. Explain the different reasons that lead to this reduced throughput.

c) Common wisdom suggests that two transceivers transmitting at the same time to each other will lead to near zero throughput in both directions. What wireless mechanisms can potentially address this issue and lead to the realization of "full-duplex" communication where both such flows can achieve significant data throughputs.

6) Network Security

a) The basic design of the Internet does not consider security threats. Give an example of *(i)* a network layer security threat, *(ii)* a transport layer security threat and *(iii)* an application layer security threat. In each case, give a basic description how these attacks are implemented.

b) Give two examples of how security capability is typically implemented at the network layer and name the treat(s) that these capabilities are trying to stop. In each instance describe how a smart attacker might be able to avoid these security capabilities (*i.e.,* so their attacks will still work).

c) Give two examples of how security capability is typically implemented at the application layer and name the treat(s) that these capabilities are trying to stop. In each instance describe how a smart attacker might be able to avoid these security capabilities (*i.e.,* so their attacks will still work).