CS 444
Computer Networks
Spring, 2017

Homework #4, Part 1

Due: Sunday March 12, at 10pm, via Blackboard

This assignment covers the first portion of Chapter 4 material.

Show all your work. Partial credit will be given.

Problem 1: What is the difference between routing and forwarding?

Problem 2: Discuss why each input port in a high-speed router stores a shadow copy of the forwarding table.

Problem 3: Describe how packet loss can occur at input ports. Describe how packet loss at input ports can be eliminated (without using infinite buffers).

Problem 4: Describe how packet loss can occur at output ports. Can this loss be prevented by increasing the switch fabric speed?

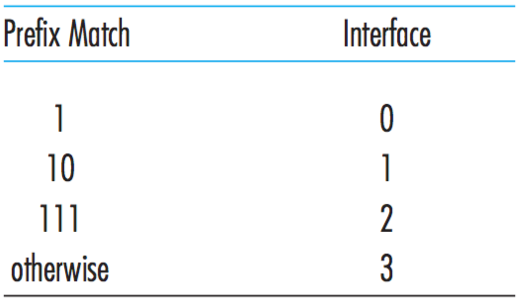
Problem 5: Visit a host that uses DHCP to obtain its IP address, network mask, default router, and IP address of its local DNS server. List these values.

Problem 6: Suppose an application generates chunks of 90 bytes of data every 20 msec, and each chunk gets encapsulated in a TCP segment and then an IP datagram. What percentage of each datagram will be overhead, and what percentage will be application data?

Problem 7: What happens when the same port numbers are used by a TCP and UDP socket?

Problem 8: A bare-bones forwarding table in a VC network has four columns. What is the meaning of the values in each of these columns? A bare-bones forwarding table in a datagram network has two columns. What is the meaning of the values in each of these columns?

Problem 9: Consider a datagram network using 8-bit host addresses. Suppose a router uses longest prefix matching and has the following forwarding table:



Prefix Match	Interface
1	0
10	1
111	2
otherwise	3

For each of the four interfaces, give the associated range of destination host addresses and the number of addresses in the range.

Problem 10: Consider a subnet with prefix 128.220.247.64/26. Give an example of one IP address (of form xxx.xxx.xxx.xxx) that can be assigned to this network. Suppose an ISP owns the block of addresses of the form 128.220.247.64/26. Suppose it wants to create four subnets from this block, with each block having the same number of IP addresses. What are the prefixes (of form a.b.c.d/x) for the four subnets?

Problem 11: Consider sending a 2,400-byte datagram into an Ethernet link that has an MTU of 1,500 bytes. Suppose the original datagram is stamped with the IP identification number 299. How many fragments are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation?

Problem 12: Suppose datagrams are limited to 1,500 bytes (including header) between source Host A and destination Host B. Assuming a 20-byte IP header, how many datagrams would be required to send a file consisting of 3 million bytes? Explain how you computed your answer.

Problem 13: Find a streetmap of your hometown (or some similar location you're familiar with). Express a fragment of this map as a graph consisting of (no less than) 12 vertices, where one is your starting point and the remainder represent intersections or similar decision points. Assign weights to the edges, in a manner that you think is meaningful. Now select a destination vertex and walk through Dijkstra's algorithm to find the shortest path between the starting point and destination point. Show all you work, including a picture of the graph.

Problem 14: Suppose you are interested in detecting the number of hosts behind a NAT. You observe that the sending host IP layer stamps an identification number sequentially on each IP packet. The identification number of the first IP packet generated by a host is a random number, and the identification numbers of the subsequent IP packets are sequentially assigned. Assume all IP packets generated by hosts behind the NAT are sent to the outside world.

- Based on this observation, and assuming you can sniff all packets sent by the NAT to the outside, can you outline a simple technique that detects the number of unique hosts behind a NAT? Justify your answer.
- If the identification numbers are not sequentially assigned but randomly assigned, would your technique work? Justify your answer.

Problem 15: Imagine that a bad guy is sending TCP SYN packets to a destination host in an effort to overwhelm it (i.e., conduct a DoS attack). The bad guy "spoofs" its source address by replacing it with apparently random IP addresses so that you cannot determine its true location. How would you propose to trace this host?

a. Imagine that you control most of the core network routers and can modify them as you see fit *provided that you don't break the IP protocol*, i.e., unmodified devices should still be able to work fine on your network. How might you implement this tracing service? You should feel free to use some sort of "out of band" channel for your routers to communicate with you on.

b. Now imagine that your routers can't use an "out of band" channel. That is, they need to include any tracing markup data *in the original IP packets being traced.* Where would you put that information, and what precisely would you put there? Think hard about the available fields in the IP and TCP headers.

c. Now imagine that you can't modify the core routers at all, but you can transmit large bursts of traffic towards different links on the network. Can you use this additional traffic to enable tracing? Describe exactly how this would work.