CS 5480/6480: Computer Networks – Spring 2012
Homework 3
Due by 1:25 PM MT, Monday March 5th 2012

Important:

- **No cheating will be tolerated.**
- **No Late Submission will be allowed.**
- **Total points for 5480 = 37**
- **Total points for 6480 = 44**

Question 1 (IP/TCP Headers) 3 points: *Look at the 40byte dump of an IP packet containing a TCP segment below.*

```
45 20 03 c5 78 06 00 00 34 06 ca 1f d1 55 ad 71 c0 a8 01 7e
00 50 9a 03 3e 64 e5 58 df d0 08 b3 80 18 00 de 00 02 00 00
```

Identify all the fields of the IP and TCP header.

IP header: IP version 4, Header Length: 20 bytes, ToS = 20, Total Length = 0x03c5 = 965 bytes, Identification = 0x7806, Flags = 0, Fragment offset = 0, TTL = 0x34 = 52, Proto = TCP, Header Checksum = 0xca1f, Source IP address = 209.85.173.113, Destination IP address = 192.168.1.126.

TCP header: src port = 80, destination port = 39427, sequence number =0x3e64e558, ack number = 0xdfd008b3, header length = 8*4 = 32bytes, unused = 0, flags : URG = 0, ACK = 1, PSH =1, RST =0, SYN = 0, FIN = 0, receive window = 0x000de, Internet checksum = 0x0002, urgent data pointer = 0.

Question 2 (IP Fragmentation) 2 points: *Consider sending a 2400-byte datagram into a link that has an MTU of 700 bytes. Suppose the original datagram is stamped with the identification number 422. How many fragments are generated? What are the values in the various fields in the IP datagram(s) generated related to fragmentation?*

The maximum size of data field in each fragment = 680 (because there are 20 bytes IP header). Thus the number of required fragments $= \left\lceil \frac{2400-20}{680} \right\rceil = 4$

Each fragment will have Identification number 422. Each fragment except the last one will be of size 700 bytes (including IP header). The last datagram will be of size 360 bytes (including IP header). The offsets of the 4 fragments will be 0, 85, 170, 255. Each of the first 3 fragments will have flag=1; the last fragment will have flag=0.

Question 3 (IP addressing) 4 points:

(a) (2 points) Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet 1 is required to support up to 63

interfaces, Subnet 2 is to support up to 95 interfaces, and Subnet 3 is to support up to 16 interfaces. Provide three network addresses (of the form a.b.c.d/x) that satisfy these constraints.

223.1.17.0/26
223.1.17.128/25
223.1.17.192/28

(b) (2 points) Consider a subnet with prefix 128.119.40.128/26. 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 128.119.40.64/26. 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?

Any IP address in range 128.119.40.128 to 128.119.40.191

Four equal size subnets: 128.119.40.64/28, 128.119.40.80/28, 128.119.40.96/28, 128.119.40.112/28

Question 4 (NAT) 3 points: *Suppose you are interested in detecting the number of hosts behind a NAT. You observe that the 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.*
a. 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.
b. If the identification numbers are not sequentially assigned but randomly assigned, would your technique work? Justify your answer.

a. Since all IP packets are sent outside, so we can use a packet sniffer to record all IP packets generated by the hosts behind a NAT. As each host generates a sequence of IP packets with sequential numbers and a distinct (very likely, as they are randomly chosen from a large space) initial identification number (ID), we can group IP packets with consecutive IDs into a cluster. The number of clusters is the number of hosts behind the NAT.

   For more practical algorithms, see the following papers.

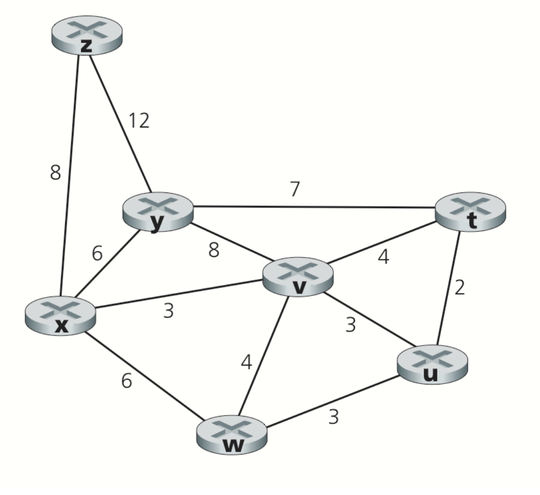
   “A Technique for Counting NATted Hosts”, by Steven M. Bellovin, appeared in IMW’02, Nov. 6-8, 2002, Marseille, France.
   “Exploiting the IPID field to infer network path and end-system characteristics.”

Weifeng Chen, Yong Huang, Bruno F. Ribeiro, Kyoungwon Suh, Honggang Zhang, Edmundo de Souza e Silva, Jim Kurose, and Don Towsley. PAM'05 Workshop, March 31 - April 01, 2005. Boston, MA, USA.

b. However, if those identification numbers are not sequentially assigned but randomly assigned, the technique suggested in part (a) won't work, as there won't be clusters in sniffed data.

Question 5 (Routing Protocols) 18 points:

(a) (3 points) Consider the following network. With the indicated link costs, use Dijkstra's shortest-path algorithm to compute the shortest path from x to all network nodes. Show how the algorithm works by computing a table similar to to the table on slide 4-80.



Step	*N'*	*D(t),p(t)*	*D(u),p(u)*	*D(v),p(v)*	*D(w),p(w)*	*D(y),p(y)*	*D(z),p(z)*
0	x	∞	∞	3,x	6,x	6,x	8,x
1	xv	7,v	6,v	3,x	6,x	6,x	8,x
2	xvu	7,v	6,v	3,x	6,x	6,x	8,x
3	xvuw	7,v	6,v	3,x	6,x	6,x	8,x
4	xvuwy	7,v	6,v	3,x	6,x	6,x	8,x
5	xvuwyt	7,v	6,v	3,x	6,x	6,x	8,x
6	xvuwytz	7,v	6,v	3,x	6,x	6,x	8,x

(b) (3 points) Consider the three-node topology shown on slide 4-89. Let the link costs be c(x,y) = 3, c(y,z) = 6, c(z,x) = 4. Compute the distance tables after the initialization step and after each iteration of the distance-vector algorithm as done for the example on slide 4-89.

Node x table

		Cost to		
		x	y	z
From	x	0	3	4
	y	∞	∞	∞
	z	∞	∞	∞

		Cost to		
		x	y	z
From	x	0	3	4
	y	3	0	6
	z	4	6	0

Node y table

		Cost to		
		x	y	z
From	x	∞	∞	∞
	y	3	0	6
	z	∞	∞	∞

		Cost to		
		x	y	z
From	x	0	3	4
	y	3	0	6
	z	4	6	0

Node z table

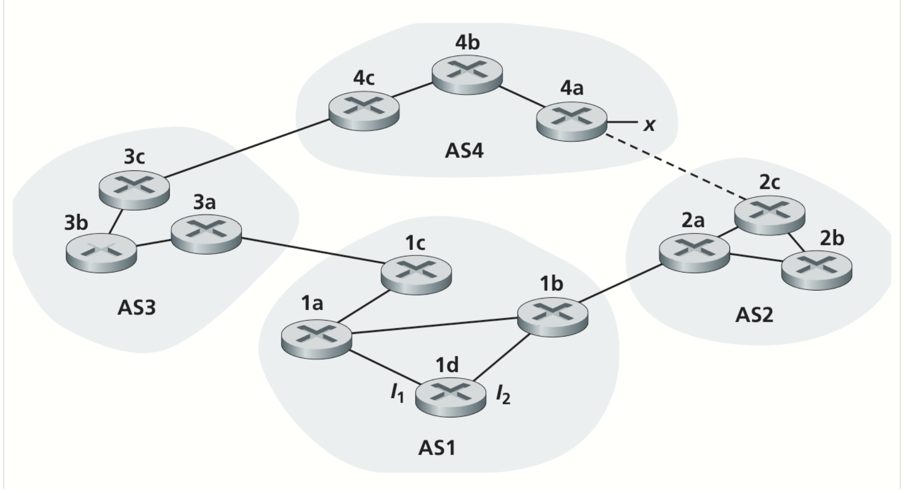
		Cost to		
		x	y	z
From	x	∞	∞	∞
	y	∞	∞	∞
	z	4	6	0

		Cost to		
		x	y	z
From	x	0	3	4
	y	3	0	6
	z	4	6	0

(c) (3 points) Consider the count-to-infinity problem in the distance vector routing. Will the count-to-infinity problem occur if we decrease the cost of a link? Why? How about if we connect two nodes which do not have a link?

NO, this is because that decreasing link cost won't cause a loop (caused by the next-hop relation of between two nodes of that link). Connecting two nodes with a link is equivalent to decreasing the link weight from infinite to the finite weight.

(d) (4 points) Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol. Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.



a. Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP, or iBGP?
b. Router 3a learns about x from which routing protocol?
c. Router 1c learns about x from which routing protocol?
d. Router 1d learns about x from which routing protocol?

a. eBGP
b. iBGP
c. eBGP
d. iBGP

(e) (3 points) Referring to the above problem, once router 1d learns about x it will put an entry (x, I) in its forwarding table.
a. Will I be equal to I1 or I2 for this entry? Explain why in one sentence.
b. Now suppose that there is a physical link between AS2 and AS4, shown by the dotted line. Suppose router 1d learns that x is accessible via AS2 as well as via AS3. Will I be set to I1 or I2? Explain why in one sentence.
c. Now suppose there is another AS, called AS5, which lies on the path between AS2 and AS4 (not shown in diagram). Suppose router 1d learns that x is accessible via AS2 AS5 AS4 as well as via AS3 AS4. Will I be set to I1 or I2? Explain why in one sentence.

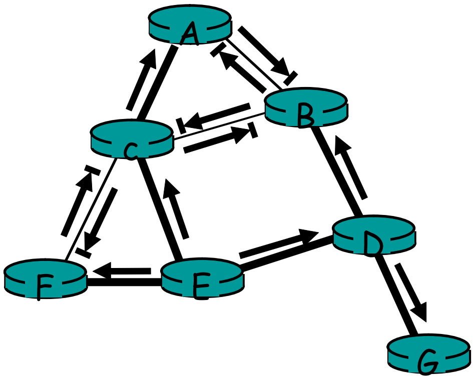
a. I_1 because this interface begins the least cost path from 1d towards the gateway router 1c.

b. I_2. Both routes have equal AS-PATH length but I_2 begins the path that has the closest NEXT-HOP router.
c. I_1. I_1 begins the path that has the shortest AS-PATH.

(f) (2 points) Consider the figure on slide 4-119. B would never forward traffic destined to Y via X based on BGP routing. But there are some very popular applications for which data packets go to X first and then flow to Y. Identify one such application, and describe how data packets follow a path not given by BGP routing.

BitTorrent file sharing and Skype P2P applications.
Consider a BitTorrent file sharing network in which peer 1, 2, and 3 are in stub networks W, X, and Y respectively. Due the mechanism of BitTorrent's file sharing, it is quire possible that peer 2 gets data chunks from peer 1 and then forwards those data chunks to 3. This is equivalent to B forwarding data that is finally destined to stub network Y.

Question 6 (Broadcast and Multicast Routing) 7 points:
(a) (2 points) Consider the topology shown in Figure 4.44. Suppose that all links have unit cost and that node E is the broadcast source. Using arrows like those shown in Figure 4.44 indicate links over which packets will be forwarded using RPF, and links over which packets will not be forwarded, given that node E is the source.



(b) (2 points) Describe the IP multicast service model.

The salient features of the IP multicast service model are as follows:
1. Any node can join a multicast group (subscribe to a multicast address) and receive data sent to that address.
2. Any node can send data to a multicast group (by setting the destination address field in the IP header to that of group's IP address). A sender node need not be a member of the multicast group.
3. The multicast sender to receiver latency should be the same (or close to) the unicast sender to receiver latency.

(c) (3 points) Describe the limitations of multicast routing based on flooding and pruning. How can Core-based-tree (CBT) multicast routing help overcome some of these limitations? What are two limitations of CBT multicast routing?

Two limitations of flooding and pruning multicast routing:

- When there are only a few members in the multicast group, flooding results in unnecessary transmissions on large part of the network without any group members.
- Pruned state can delay transmission of multicast data to receivers that join the group later.

CBT's does not use any flooding. Group members send join requests towards the well-known core. Those senders that are also members of the group send the multicast data along the CBT. Those senders that are not members of the group send their multicast data straight to the core that in turn forwards the data along the CBT.

Two limitations of CBT:

- Multicast data transmission in CBTs can take longer paths.

Cores will experience traffic concentration near themselves.

Question 7 (required for CS6480, extra credit for CS5480) 7 points:
Read the following paper: "On Fast and Accurate Detection of Unauthorized Access Points Using Clock Skews" by Suman Jana and Sneha Kumar Kasera, in the IEEE Transactions on Mobile Computing, March 2010. This paper is available from http://eng.utah.edu/~cs5480/readings/jana2010.pdf.
Answer the following questions that are based on this paper.

(a) *(1 point) Define clock skew.*

Clock skew is the rate of change of clock offset.

(b) (2 points) Let us plot the observed clock offset, in microseconds, on the y-axis and the time since the start of the fingerprinting measurements, in seconds, at the fingerprinter, on the x-axis. Let (5, 60) and (7.5, 75) be two points at times 5s and 7.5s, where the clock offset is observed by the fingerprinter to be 60 and 75, respectively. Estimate the clock skew of the fingerprintee from these two points. You can assume that the network delays are negligible.

The clock skew is the slope of the line connecting the two points = 15/2.5 = 6 ppm.

(c) (2 points) What clock skew behavior do the authors observe in the case of virtual access points?

They find that the clock skews of the virtual APs on the same physical AP hardware are the same.

(d) (2 points) Why is it not easy to fabricate clock skews of access points?

- unpredictable medium access control delay
- floating point operations on wireless cards could take a few microseconds