HW 3 - Surbhi

Monday, October 25, 2021 3:57 PM

Networks and Distributed Systems **Homework 3**
CS3700 Spring 2021

This homework is due at 11:59:59 PM on October 25, 2021 and is worth 3% of your grade.

Name: Surbhi Gulati

Khoury Username: surbhigulati

Problem	Possible	Score
1	30	
2	20	
3	10	
4	15	
5	10	
6	5	
7	30	
8	20	
9	10	
Total	150	

1a. What are the main functionalities in IP Addresses. `Hint: There are two.` (5 pts)

Main functionalities of IP addresses:

1. **Naming/ addressing:** recognizing different hosts
2. **Routing:** creating a scalable system with a location defined for the hosts, to build paths between them

1b. What is the Benefit of using IPv6? Give Three Examples of the Improvements. (5 pts)

Enhanced performance: IPv6 has much better performance than IPv4 due to many less fields being required . For example it was not useful to communicate checksums because this is already checked in upper and higher layers and doesn't add extra value in this layer.

Enhanced security: Because IPv6 does not fragment, there are also less security vulnerabilities. Hosts are expected to use path MTU discovery instead of working with IP fragments. In this way the buffers in the IP fragments from IPv4 can no longer be exploited by attackers.

Enhanced features: IPv6 has a number of enhanced features like source routing, mobile IP, privacy extensions and jumbograms. This basically means that hosts have more control over routes that packets take, bigger packets can be sent, and more. Overall, in our bigger internet, routers have more control and power to complete their communications.

1c. What happens when an IPv6 packet at the max MTU of one network traverses to a second network with a smaller MTU? (5 pts)

By DARPA principles the MTU of a network can be heterogenous so the packet can still be delivered to the destination. This is possible through fragmentation at the IP layer. This is when the datagram is split up in to pieces that will fit within the MTU of the second network, which can later reassemble the full datagram after it has received all the bytes.

1d. For the following IP addresses, give their class (A, B, or C) and their representation in binary: 129.10.115.10, 4.3.2.129, 220.33.9.21. (5 pts)

129.10.115.10 - Class B, Binary Representation: **10000001.00001010.01110011.00001010**
4.3.2.129 - Class A, Binary Representation: **00000100.00000011.00000010.10000001**
220.33.9.21 - Class C, Binary Representation: **11011100.00100001.00001001.00010101**

1e. The binary representation of 128.42.5.4 is shown below.

10000000 00101010 00000101 00000100

If the subnet mask is 255.255.248.0, label the bits that correspond to the (a) class prefix, (b) the network number, (c) the subnet number, and (d) the host number. You may assume that class-based IP addressing is being used for this question. (10 pts)

Subnet is /21

2a. Convert the following IP/subnet representations of networks to the equivalent CIDR representation. If the network cannot be represented in CIDR, briefly explain why.

(i) 128.42.0.0/255.255.0.0 **128.42.0.0 / 16**

(ii) 192.168.0.0/255.255.224.0 **192.168.0.0 / 19**

(iii) 172.10.12.0/255.255.253.0 **Cannot represent in CIDR: this does not correspond to a whole number prefix length.**

(iv) 64.0.0.0/192.0.0.0 **64.0.0.0 / 2** (10 pts)

2b. Suppose that you have been allocated the network 173.98.112.0/20, and you wish to divide your address space equally into four parts. What are the CIDR (Classless Interdomain Routing) representations of these four parts? (10 pts)

The prefix length would then be 22 rather than 20 because 2 extra bits can create 4 subnets. This gives us:

- 173.98.112.0 / 22
- 173.98.112.64 / 22
- 173.98.112.128 / 22
- 173.98.112.192 / 22

3a. Why does the Offset field in the IP header measure the offset in 8-byte units?
(Hint: Recall that the Offset field is 13 bits long.) (5 pts)

For every bit removed from the IP header the number of unique values is divided by 2 as we get rid of a 1 or 0 option in that location. This goes in to the offset.

The fragment offset field is 13 bits long out of 16 bits so we remove 3 bits. Moving each of these 3 bits out means we have 2^3 = 8 byte units of offset so that we can preserve the overall number of bits being sent.

3b. Some signaling errors can cause entire ranges of bits in a packet to be overwritten by all 0s or all 1s. Suppose all the bits in the packet including the Internet checksum are overwritten. Could a packet with all 0s or all 1s be a legal IPv4 packet? (5 pts)

No it is not a legal IPv4 packet.

This is because the header datagram fields (the first two denote version to indicate IPv4 packet in the first place, and header length) will be clearly misreported as they shouldn't be all 0's or 1's for v4, which will indicate that the packet has been corrupted.

4. Suppose you receive the following series of IP packets at a destination host (be sure to remember that the length field in the packet *includes the header*, and the offset is specified as the number of 8-byte blocks from the beginning of the data in the original IP datagram):

#	ID	Flags	Offset	Total Length
1	0xdb7a	-	370	300
2	0x7823	MF	370	1500
3	0x992a	MF	185	300
4	0x45a9	-	0	1500
5	0x7823	MF	0	1500
6	0x992a	MF	0	1500
7	0xdb7a	MF	185	1500
8	0x9ffb	-	200	1500
9	0xdb7a	MF	0	1500
10	0x33aa	-	0	1500

What packet IDs have you completely received (i.e., all fragments of the original packet have been received), and how many total data bytes are in each of the completely received packets? For this problem, you can assume that all IP packets have no options. (15 pts)

Not completely received:
0x9ffb: has offset, earlier fragment missing
0x992a: all fragments have MF flag (more fragments coming)
0x7283: all fragments have MF flag (more fragments coming)

Completely received and their bytes:
0x45a9: 1480 bytes (1500-20)
0x33aa: 1480 bytes (1500-20)
0xdb7a: 3240 bytes ((300 - 20) + (370*8))

5. You are a router, and one of your outgoing links has an MTU of 1000 bytes (ignore layer 2 headers). You receive the following packets that all need to be sent out over this link:

#	ID	Flags	Offset	Total Length	
0	0x1930	-	0	1000	
1	0x92ad	-	0	3000	
2	0x944f	DF	0	1000	
3	0xaa22	-	185	1001	incomplete
4	0x78a1	MF	370	1500	incomplete
5	0x3ac8	DF	0	1500	df, big len

Fill in the table below with the header fields of the packets that you send out (you may not need all of the rows). The first packet has been completed for you. (10 pts)

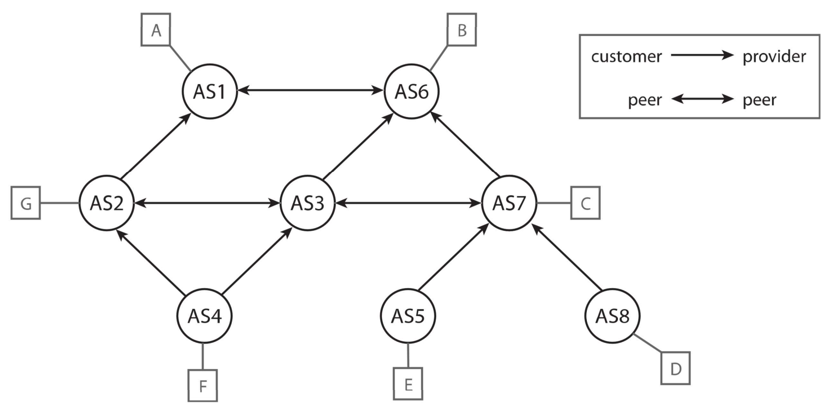
#	ID	Flags	Offset	Total Length
1	0x1930	-	0	1000
2	0x92ad	MF	0	500
3	0x92ad	MF	60	500
4	0x92ad	MF	120	500
5	0x92ad	MF	180	500
6	0x92ad	MF	240	500
7	0x92ad	-	300	500
8	0x944f	DF	0	1000
9				
10				

6. What are the three main steps that routers that use a distance vector routing protocol (e.g., RIP) perform to keep their routing tables up-to-date? (5 pts)

Each router maintains their own routing table for the destinations that the router can reach.

1. Periodically, each router will broadcast its up-to-date routing table to its neighbors.
2. Neighbors will utilize any route updates that are shorter to update their own tables' next hop toward a destination so that the information can be saved and propagated through the network.
3. If a router learns of a potential new path it will assess the path and see if the old or the new one is better and then choose the shortest to keep within its routing table so that in the next updates cycle this information can be made available to the network.

7. Consider the network shown in the following figure. In the event where an AS has multiple paths to a given destination, assume that it chooses the path with the shortest hop count metric (i.e., the ASes do not have local preferences or other traffic engineering meta-data about routes). In the case where two or more available paths have the same hop count metric, an AS will choose the path through the neighbor with the lowest AS number. `Hint: The key to answering the following questions is thinking about route import and export rules.`



7a. What path would host *F* take to reach host *B*? Explain briefly the routing choice made by each AS based upon the information it has available. (10 pts)

F -> AS4 -> AS3 -> AS7 -> AS6 -> G

AS4 is where host F initially is. They transmit to AS3 because AS3 has less hops to AS6. AS3, prioritizing its own cost saving, transmits to its peer AS7 which it knows will get to AS3 faster than its peer AS2, rather than sending directly to AS6 which is its provider. Then, AS7, having no new peers that are closer to forward to, transmits to AS6 which delivers to host B.

7b. What path would host E take to reach host G? Explain briefly the routing choice made by each AS based upon the information it has available. (10 pts)

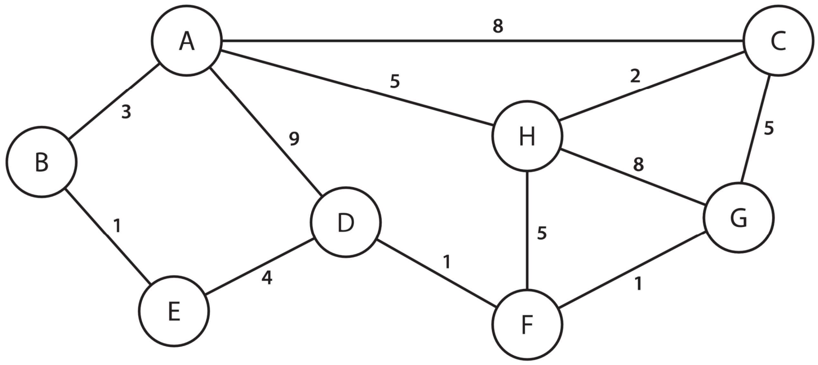
E -> AS5 -> AS7 -> AS6 -> AS1 -> AS2 -> G

Host E is a part of AS5 so the journey begins here. Then since AS5 is connected only to AS7 it transmits there. AS7 must transmit to AS6 even though it is a customer to peer relation as if it transmits to AS3 then AS3 will not have incentive to transmit to AS2, another peer, even though that would arrive at G. After this local decision we go from AS6 to its peer AS1 which is adjacent to AS2, and then AS1 takes us to AS2 which will finally forward the packet to host G.

7c. All traffic between $AS5$ and $AS8$ must transit through $AS7$. Suppose $AS5$ and $AS8$ want to avoid paying $AS7$ for this service. What could they do to reduce their cost? (10 pts)

With the condition that AS5 and AS8 both must transmit through AS7, they can attempt to peer with AS7. Alternatively they can peer among themselves to send messages directly, because peering eliminates the cost that providers charge customers. If the condition that the transmissions cannot happen through other AS, they would have been able to try to peer with other AS that can be intermediaries between the two.

8. Consider the networking of routers shown below, with the "link weight" for each link written next to the link:



8a. Use Dijkstra's shortest-path algorithm to compute the shortest path from A to all other routers. Show how the algorithm works by filling out the table on the final page, showing both the current cost to each destination ($D(X)$) and the corresponding shortest path ($p(X)$). (20 pts)

x	D(x)	p(x)
B	3	A-B
C	7	A-H-C
D	8	A-B-E-D
E	4	A-B-E
F	9	A-B-E-D-F
G	10	A-B-E-D-F-G
H	5	A-H

9a. Name one strength distance vector routing has over link state routing. (5 pts)

Distance vector routing enables nodes to communicate with each other easily periodically within a smaller network, whereas link state routing can cause traffic control issues because of how events cause flooding throughout the network and this causes a large amount of overhead.

9b. Name one strength link state routing has over distance vector routing. (5 pts)

Link state routing has the advantage of being loop free when every router in the link state database is consistent; the distance vector routing has the count to infinity and looping problem.

Step	S	D(B), p(B)	D(C), p(C)	D(D), p(D)	D(E), p(E)	D(F), p(F)	D(G), p(G)	D(H), p(H)
1	*A*	3, A	8, A	9, A	∞	∞	∞	5, A
2	AB				4, B			
3	ABE			8, E				
4	ABEH		7, H			10, H	13, H	
5	ABEHC						12, C	
6	ABEHCD					9, D		
7	ABEHCDF						10, C	
8	ABEHCDFG							