Problem 1 (25 points) Suppose host A is sending to a IP multicast group (router level multicast, not overlay multicast); the recipients are leaf nodes of a tree topology rooted at A with depth N and with each non-leaf node having k children; there are thus k^N recipients.

(a) How many individual link transmissions are involved if A sends a multicast message to all recipients? (10 points)

The answer is $k + k^2 + k^3 + \ldots + k^N = k(k^N-1)/(k-1)$

(b) How many individual link transmissions are involved if A sends a unicast message to each individual recipient? (10 points)

The answer is simply $N*k^N$

(c) Suppose A sends a message to all recipients, but some copies of the message are lost and retransmission is necessary. Unicast retransmissions to what fraction of the recipients is equivalent, in terms of individual link transmissions, to a multicast retransmission to all recipients? (5 points)

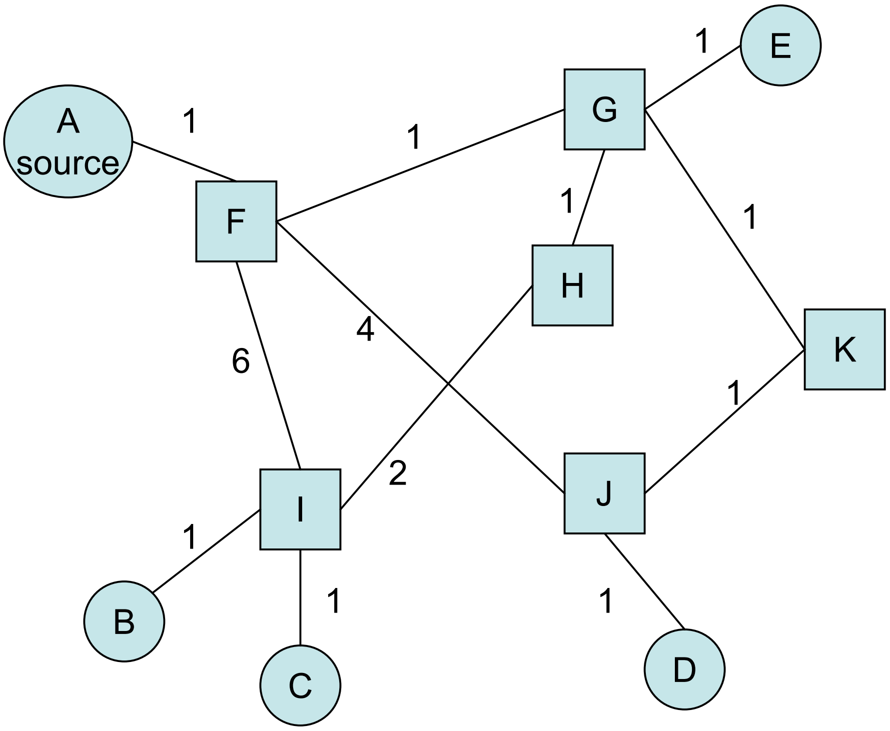
Let X be the fraction of recipients not getting the transmission.

Cost of unicast retransmission is $N*X*k^N$. Cost of multicast retransmission is $k(k^N-1)/(k-1)$.

$$N*X*k^N = k(k^N-1)/(k-1)$$

$$X = k(k^N-1)/((k-1)*N*k^N)$$

Problem 2 (25 points): Consider the following network. Circles are end hosts, squares are routers. The links are labeled with their lengths. Assume that shortest path routing is used in this network. A is a data source multicasting to receivers B, C, D, and E. Suppose the network implements Reverse Path Flooding to flood multicast packets throughout the network.

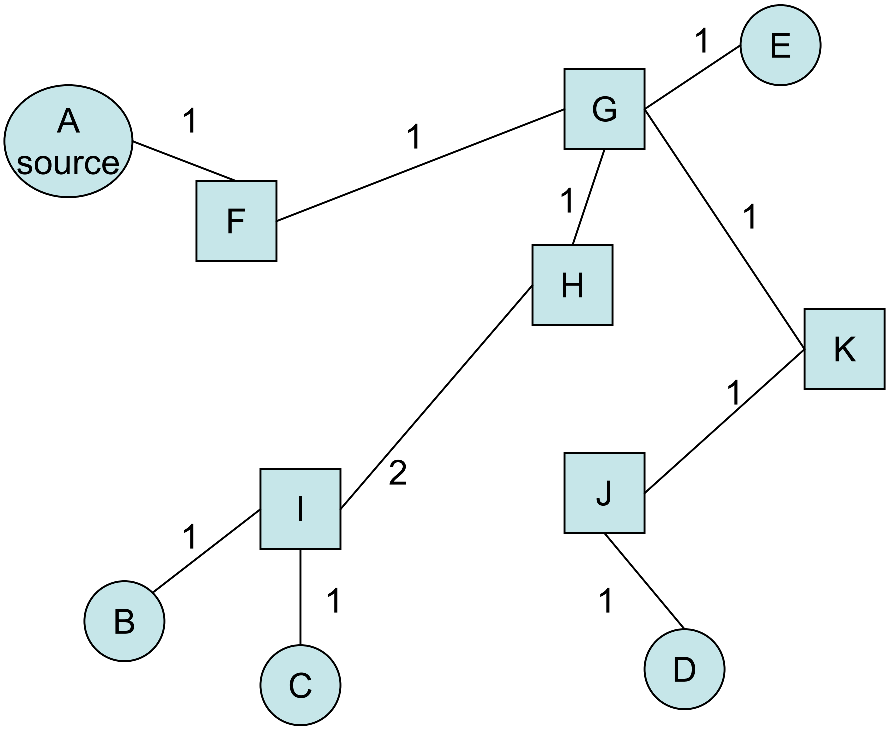


(a) Node A sends one multicast packet. Write down the sequence of packet transmissions in the network under Reverse Path Flooding using the notation A->F to indicate a copy of the packet is transmitted from A to F. Below is the beginning of the sequence:

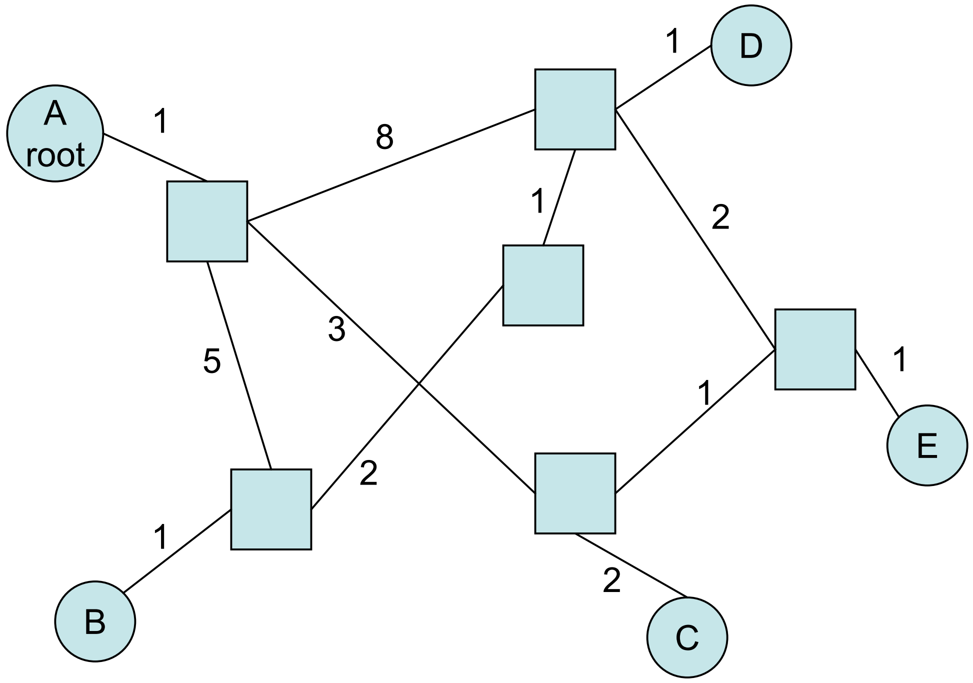
A->F; F->I, F->J, F->G; …. (complete the rest of the packet flooding sequence for this packet) (13 points)

G->H, G->E, G->K
H->I; K->J
I->F, I->B, I->C; J->F, J->D

(b) Now, suppose the core-based (rendezvous point-based) tree approach is used for multicast in this network, and node K is chosen as the core node. Draw the topology of the multicast tree formed showing all the nodes and links on the tree. Again, A is the sender, B, C, D, E are the receivers. (12 points)

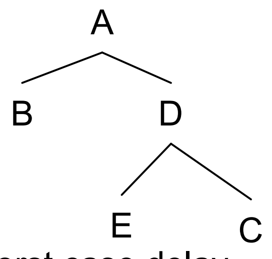


Problem 3 (25 points) In the following network, circles are end hosts, squares are routers. Note that the network is different from the one in previous problem. Each link is labeled with the link’s length. Assume the network uses the shortest path routing policy. Node A is a video broadcaster who wants to create an overlay network to distribute the video to the other end hosts B, C, D, E using overlay multicasting.

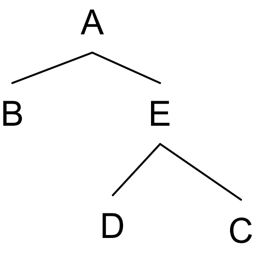


Suppose it is known that no node can forward more than 2 copies of the video, and that node C is joining and leaving the overlay very frequently while the other nodes join the overlay and remain in the overlay. What overlay tree would you construct to first avoid instability and then secondly minimize the worst case delay from the source to any receiver? Explain your reasoning clearly.

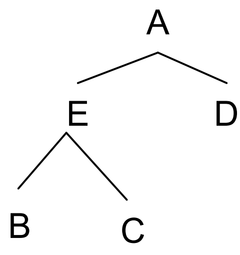
Since C is unstable, C must be a leaf node to maintain stability. To minimize delay, you definitely want to use up all the outbound capacity (2) of A. Thus, the possible combinations of nodes to be overlay children of A are (B,D), (B,E), (D,E). Once the children of A are decided, the best arrangement for the remaining two nodes is straightforward, yielding these 3 possibilities:



Worst case delay
A-D-C 14 units



Worst case delay
A-E-C/D 10 units



Worst case delay
A-E-B 13 units

Correct answer

Problem 4 (25 points) Consider the following simple UDP protocol for downloading files:

1. Client sends a file request
2. Server replies with first data packet
3. Client sends ACK, and the two proceed using the stop-and-go mechanism (i.e. a sliding window with window size of 1 packet)

Suppose client and server possess keys Kc and Ks, respectively, and that these keys are known to both client and server. Extend the file downloading protocol, using these keys and the MD5 hash technique, to provide sender authentication and message integrity. Your protocol should also be resistant to replay attacks. Explain clearly what information relevant to security does your packet need to carry and how you generate such information. Explain why your protocol satisfies the requirements.

In addition to sending the basic content of each data packet, the protocol will be extended to include two extra pieces of information in each packet.

1. Each packet carries a unique ID drawn from a large number space, say 64bit. This ID is different from the 1 bit sequence number used for the stop-and-go protocol.
2. Each packet also carries the MD5 hash value of the original packet's content, the unique ID number, as well as the server's (or client's, whichever is appropriate) secret key.

Using this mechansim, no one can forge any part of the content of the packet and still be able to compute the correct corresponding MD5 hash value since an attacker does not know the secret keys and it'd be hard to guess correctly. Thus, authentication and integrity are ensured.

Since each packet has a unique ID, if an attacker replays a packet, it will only be treated as a duplicate of a previous packet and be discarded. Thus, the protocol is resistant to replay attacks.