1. (12 pts) A policy was to allow inbound and outbound mail (SMTP, port 25), but only to our gateway machine. However, mail from site SPYGOT is to be blocked. Please complete the following table for this policy.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>SRC</th>
<th>PORT</th>
<th>DEST</th>
<th>PORT</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>block</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>block mail from SPYGOT</td>
</tr>
<tr>
<td>allow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>inbound mail to GW</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>outbound mail to GW</td>
</tr>
</tbody>
</table>

2. (10 pts) Why the IP fragmentation make the process of packet filtering gateway more difficult?

3. (14 pts) The following is the access right propagation graph. The number in the link indicates the timestamp while the propagation event occurred. If, at time 70, A decide to revoke the right from C, please draw the two resulting graphs for cascade and non-cascade modes.

![Access Right Propagation Graph]

4. (12 pts) Can a user cleared for < secret; \{dog, cat, pig\}> have access to documents classified in each of the following ways under the military security model (i.e., no read-up and no write-down)?
   
a. write to < secret; \{dog\}>
   b. write to < top secret; \{dog, cat, pig\}>
   c. read from < secret; \{dog, cow\}>
   d. read from < confidential; \{pig\}>
   e. read from < confidential; \{dog, pig, cat\}>
   f. write to < confidential; \{dog, moose\}>

5. (12 pts) Please describe what process sequence for an intermediate router needs to do after receiving a packet from the network. (Try to write your answer in a layered sequence, i.e., start from link layer up to some layer then down to link layer).