15-744 Computer Networks (Fall 2002)
Compilation of questions for the final exam*

1. Scalable Reliable Multicast uses two techniques to limit the amount of traffic generated in response to errors. Describe these techniques and identify the types of configurations in which they are most appropriate.

2. Briefly explain why it is the receiver that decides whether to make reservations in RSVP or not? And what's the main reason for using soft state for PATH/RESV messages?

3. - Briefly describe the implementation difficulties of IntServ - specifically, why wasn't it widely deployed.
   - How does DiffServ solve at least one of these problems?

4. Explain why a teleconferencing application would benefit from application level framing while a bulk-transfer application (such as FTP) would not?

5. What are the most important reasons that multicast functionality in routers is not well deployed or heavily used?

6.
```
   Net1  Net2
Outside world--R1---------R2-----------
```

   Suppose filtering routers are arranged as shown in the above figure. How to configure R1 and R2 so that outside world can telnet to R2 but not hosts in Net1, and to avoid "leapfrogging" break-ins to Net1, also disallow Telnet connections from Net2 to Net1.

7. List at least 3 differences between the Integrated Services and Differentiated Services architectures. What aspects of IntServ make it infeasible for wide deployment, and how does DiffServ propose to account for these problems?

8. What are some arguments for and against sharing the same cable for different types of services (e.g. real time and best effort)?

9. Why does IP traceback use edge sampling rather than node sampling? What scheme does IP traceback use to reduce the number of extra bits required in the packet header?

10. Which of the following are true about IP Traceback mechanisms that use probabilistic packet marking:

    - Identifying the network path being taken by an attacker requires support from each ISP along the network path.
    - A user must identify the attack as it is happening. Once the attack has completed, it is not possible to detect the network path.
    - All routers along the path must employ packet marking for IP traceback to be successful.

*In no particular order