NET

Computer Science Department

Stanford University

Comprehensive Examination in Networks

SOLUTIONS

Fall 2000

READ THIS FIRST!!

1. You should write your answers for this part of the Comprehensive Examination in a BLUE BOOK. Be sure to write your MAGIC NUMBER on the cover of every blue book you use.
2. The number of POINTS for each problem indicates how elaborate an answer should be. For example, a question worth 6 points or less doesn't deserve an extremely detailed answer, even if you feel you could expound at length upon it. **Short, bulleted answers are encouraged.**
3. The total number of points is 60.
4. The exam is CLOSED BOOK. You may NOT use notes, books, computers, other people, etc.
5. Show your work, since PARTIAL CREDIT will be given for incomplete answers.
6. If you need to make an assumption to answer a question, state your assumption(s) as well as your answer.
7. Be sure to provide justification for your answers.

Problem 1 (15 points)

Wireless networks may suffer from interference and poor signal strength, causing packets to drop.

a. (3 points) Some wireless link layers will retransmit a dropped packet some finite number of times. What is the advantage to having the link layer perform such a service? The timeout for such retransmissions is typically quite small.

You don't have to incur the overhead of a TCP/transport-layer timeout.

b. (6 points) Given such a service at the link layer, what, if any, are the reasons to run TCP over such a network?

TCP handles additional kinds of functionality, for example:

1. *losses not in the network (e.g. losses in the host OS itself)*
2. *losses that exceed the link layer retransmit limit*
3. *losses as a result of congestion (i.e. packets dropped from queues)*

c. (6 points) Some wireless devices will attempt to retransmit a dropped packet indefinitely (retrying it periodically in the midst of sending other newer packets. Is there any disadvantage to a link layer performing this service rather than leaving all retransmissions up to TCP? If a link layer knew TCP was running on top of it, how might it adapt itself?

There are at least two disadvantages to this approach:

1. *it causes packets to be delivered out of order*
2. *it wastes bandwidth if TCP has already retransmitted the packet*

An ideal wireless link layer for TCP would avoid TCP coarse-grained timeouts and useless retransmissions and would keep packets in order by retransmitting a few times, but only within the time before TCP will retransmit.

Problem 2 (10 points)

Wireless access to the Internet is growing. These wireless access links, however, are often low-bandwidth. Some network architectures place proxies at the other end (from the user) of a wireless link, so that the proxy can perform "invisible" services on behalf of user to mitigate the effect of the low-bandwidth link. For instance, if a user asks for web pages from a server, the proxy may convert graphics on those pages to low-resolution, smaller, black&white pictures that consume little bandwidth. What issues arise if the data the user requests from the server is encrypted with the user's key, and what techniques can you come up with to address these issues?

The problem is that the proxy can't decrypt the server's data, so it cannot perform appropriate adaptations on it. One solution would be to give the proxy the user's keys, so the proxy can decrypt the data to perform various transformations on it, and then re-

encrypt the results. This presents some security concerns: the keys would need to be transferred to the proxy in a secure fashion, and they would need to be kept secure on the proxy.

Problem 3 (20 points)

The Border Gateway Protocol (BGP) is used to route packets between autonomous systems in the Internet.

a. (5 minutes) Why is a different routing protocol used between autonomous systems than is used within them? (The issues are not necessarily technical ones.)

Interior routing protocols need only maximize the efficiency of routing. External routing protocols must also deal with political issues, such as one company not being willing to allow its data to flow through its competitor's site.

b. (10 minutes) Instead of maintaining just a cost to each destination, as do most distance vector protocols, each BGP router keeps track of the exact path used. Each BGP router periodically tells its neighbors the exact path it is using to a destination. Why is this exact path information useful to BGP?

This allows a BGP router to avoid choosing paths that flow through itself, and it allows it to implement political decisions. To use the (rather naïve) example from above: by examining the path a packet would take if handed to a particular neighbor, the router can determine whether that neighbor might forward the packet to a competitor's site. If so, it could pick a different direction for the packet.

c. (5 minutes) Why do some autonomous networks decline to carry "transit traffic?" (Transit traffic is traffic that neither originates nor terminates in the autonomous system.)

Transit traffic performs no service for anyone inside the autonomous system, since it doesn't come from users there, and it isn't destined for users there. It nonetheless ties up bandwidth and other resources on the network.

Problem 4 (15 points)

Some wireless networks are unable to provide broadcast service. Does this affect any of the following services in the Internet, and if so, how? What could you do about it?

a. ARP

Yes, since ARP requires a broadcast to find out the hardware address for an IP address on the subnet. A possible solution is to make the address of an ARP server a well-known address, so ARP requests could be directed to a particular machine. This would mean some limited configuration information on hosts ahead of time, though, which is what ARP is attempting to avoid. A bit of an improvement might be to direct all ARP requests to the closest base station, and base stations would redirect the requests to an appropriate ARP server.

b. DHCP/BOOTP

Yes, since DHCP and BOOTP both require broadcasts to find out a host's own IP address upon initialization of the network on the host. A possible solution is to direct all requests to a well-known DHCP server. As above, the base station solution might be appropriate.

c. DNS lookups

No. The address of the DNS server is one of the pieces of information gained through whatever configuration process network initialization on a host uses. The actual lookups are directed to the DNS server and are not broadcast.