The final exam is on Monday evening, 14 December, from 7 to 10 p.m.

It will be comprehensive, covering the entire semester, although there might be several more questions on it about more recent material than about earlier material.

Please see the documents “Review for midterm 1,” “A few more review questions for midterm 1,” “Midterm 2 review questions” (links on course web site) for additional problems.

1. In the following graph, the horizontal axis represents “rounds” of packet transmissions between a sender and a receiver; the vertical axis represents the size of the congestion window.

For each of the sections of the graph, explain what is going on in terms of packet loss, duplicate acknowledgements, slow-start, congestion avoidance, etc. What do the two horizontal dotted lines indicate?

From transmissions 0 through 5 the process is in the “slow start” phase; the congestion window starts at a size of one MSS (maximum segment size) and keeps doubling until it reaches the “slow start threshold” (book calls this ssthresh), in this case, 32 (indicated by the left dotted line). From 5 through 13 the congestion window increases by one during the phase known as “congestion avoidance.” Between transmission rounds 13 and 14 a timeout occurs; as a result, the congestion window size drops back down to one and the slow-start threshold is reduced to half of the congestion window size when the timeout occurred: half of 40 is 20, and this threshold is the dotted line on the right. After a timeout the system is back into slow start mode. I am a bit surprised that at time 18 the congestion window jumps from 8 to 20 — I would have expected it to go up to 16 and then, at time 19, go from 16 to 20 — but it is still clear that there is exponential growth until the threshold of 20 is reached, after which the system is once again in congestion avoidance mode. There are no triple duplicate acknowledgements in this scenario.

2. What does the phrase “exponential backoff” mean and what protocol did we study that makes use of it?
This occurs in the Ethernet CSMA/CD protocol. When a host’s network card is transmitting and detects a collision, it chooses a random number $K$ that determines how many 512-bit intervals it should wait before retransmitting. Initially $K$ is limited to the range $\{0, 1\}$, after two collisions in a row its range is doubled, to $\{0, 1, 2, 3\}$, after three collisions it is chosen from the range $\{0, 1, \ldots, 7\}$, etc. Since the range of allowable values for $K$ doubles at each step, we see that the maximum possible delay time grows exponentially with each successive collision.

3. Two hosts, $A$ and $B$, are connected through an Ethernet cable of length 100 meters. Each one transmits at a rate of 10MBps. The propagation speed is $2 \times 10^8$ meters/sec. At time $t_0$ $A$ begins to transmit a 1500-byte frame.

(a) How long does it take for the first bit of $A$’s message to reach $B$?

The propagation delay is $100/(2 \times 10^8) = 50 \times 10^{-8} = .5\mu sec$, a half microsecond. The problem was somewhat ambiguously stated — if we are asking for the time from when the bit leaves $A$ until it arrives at $B$, the answer is $.5\mu sec$. However, if we also include the time needed for $A$ to transmit that one bit, we have to add on one more microsecond, since $1/(10 \times 10^6) = .1 \times 10^{-6} = .1\mu sec$.

(b) At almost exactly the same time that $A$’s first bit arrives at $B$, $B$ begins to transmit. It immediately detects a collision. Describe what happens next, from both $B$’s point of view and $A$’s point of view — for instance, when does $A$ realize that a collision has occurred?

The first bit from $B$ takes another $.5\mu sec$ to get back to $A$, so $A$ realizes that a collision takes place $1\mu sec$ after it begins transmitting. Both $A$ and $B$ stop transmitting their frames, then they transmit a 48-bit jam signal, then each enters the exponential backoff phase to determine when to re-transmit.

(c) Once $A$ is able to transmit again, how long does it take to transmit the entire 1500-byte frame, assuming no further collisions occur?

Transmission time is $1500 \times 8/(10 \times 10^6) = 1.2m sec$, 1.2 milliseconds.

4. What is the difference between a router, a switch, and a hub? Your answer should mention things like layers in the network protocol stack, collisions at the link layer level, and anything else you find relevant.

A hub is just a signal forwarding device — it receives a signal and retransmits it to all the other ports connected to it. A hub might be used to connect several hosts in a primitive Ethernet LAN. Hubs do not examine the contents of frames received, they just operate on a stream of bits, so they are part of the physical layer. Collisions can occur among hosts connected through a hub.

A switch is more sophisticated — it examines the frames received and examines the MAC address of the destination to determine what to do with the frame. If the MAC address appears in its switch table, it forwards the frame to the appropriate output interface (unless it is the same as the incoming interface, in which case it simply ignores it). If the address does not appear, it broadcasts the frame to all the other interfaces. It operates at the link-layer level of the protocol stack. Although collisions can occur within a subnet connected to the switch, messages passing through the switch will not collide with other such messages.

A router is a network layer device. It examines IP addresses (and other fields, for instance, the “time to live” field) and communicates with the network layers in other routers and hosts.
5. What is a VLAN? Tell me everything you know about VLANs.

Obviously I can’t tell you everything you know about VLANs! You should be aware that a VLAN, or Virtual LAN, is a way to partition a local area network into several smaller networks without actually changing the underlying physical network. Instead, switches can be used to isolate groups of hosts into smaller “virtual” networks. Several such switches can be connected via a VLAN trunk link, which maintains information about multiple VLANs using an extended Ethernet frame that contains additional information, such as a VLAN identifier tag. The switches are responsible for adding and removing the extra frame information.

6. At the link layer, when a message needs to be sent to a host that’s in a different subnet, e.g., a network in another country, how does the sender know what MAC address to put in the frame?

The router that connects a local network to the larger Internet has interfaces — network cards — at each end of the connection. The sender uses ARP to find the MAC address of the router interface connecting to its network. The router, which is a network layer device, looks at the destination IP address (remember, this frame contains information passed down from the network layer of the sender, and that has a destination IP addresss) and determines, from its routing table, what the corresponding output interface should be, then uses the MAC address of that interface in the frame. This process goes on, ending at the router connecting to the destination network, at which point another ARP command determines the MAC address of the receiver.

7. Do you believe in “datagram heaven”? (page 475)

I don’t want to get into theological discussions here.

8. What is the importance of “endianness” for networking?

When we are working at the byte level we need to know whether or not the message we are receiving uses a big-endian or little-endian representation (i.e., is the most significant byte in the smallest byte address of the word, or in the largest byte address of the word?). This is often transparent to the user, i.e., little-endian machines have software that automatically translates into big-endian format (also called network byte order) and vice-versa.

9. Which layers of the Internet protocol stack (not including the application layer) provide facilities for detecting bit errors? Describe the mechanisms used.

At the transport layer there is an Internet checksum field that uses the ones-complement of the sum of the 16-bit half-words, with carry wraparound, as described in chapter 3. At the network layer there is a header checksum that uses the same mechanism, but only on the datagram header, not on the entire datagram. At the link layer level there is a cyclic redundancy check (CRC) that uses a remainder based upon exclusive-or division by a fixed generator string. At the physical layer various signalling tricks are used to try to prevent signal drift, e.g., the use of preambles in Ethernet frames to synchronize the clocks of the sender and receiver. (Technically this latter is not so much for detecting errors as for preventing misalignments of data streams.)

10. Which layers of the Internet protocol stack provide facilities for reliable delivery (guaranteed delivery, in order)? Describe the mechanisms used.
Of the ones we have studied, only TCP provides a mechanism for reliable delivery. It uses a combination of sequence numbers, acknowledgements, timeouts, and re-transmissions to make sure that multi-segment messages arrive undamaged in their entirety.

11. What is a “distributed hash table” and in what kinds of situations would it be used?

A DHT is an indexing method for a database that is distributed among a number of different hosts. The example we saw in class is in peer-to-peer applications. The idea is that each peer has a unique identifying integer identifier. Each data item is assigned an integer (through a technique called hashing that you should have studied in CMPSC 112). That data item is then assigned to the peer machine whose id number is nearest to the number assigned to the data. To search for a data item, we calculate its associated id and then use a sequence of queries to route the request from peer to peer until it reaches the correct one.

12. A router has the property that its switching speed (time needed to move a packet from an input queue to an output queue) is \( n \) times faster than the fastest rate at which packets arrive at any of the router’s \( n \) input ports. The transmission rate at the output ports is also at least as fast as the fastest input rate. Can queueing delays still occur? If not, why? If so, how?

Queueing delays can occur because even if the router can keep up with packets as they arrive, they might, in the worst case, all be routed to the same output port, where they will be forced to form a queue.

13. You enter the Alden 101 classroom, log on to a machine, start up a Web browser, and visit an off-campus site where you watch a streaming video.

Describe as many of the various protocols used along the way as you can, including things like UDP, TCP, IP, DNS, ARP, BGP, etc. You can’t give a comprehensive answer to this in the available time, but you should try to squeeze in as much as possible. You can make up numbers (IP addresses, etc.) to illustrate what’s happening.

For further insight into this question, see pages 505–510. Briefly, our browser needs to consult the local DNS server to find the IP address of the site we want to visit. This might involve a sequence of requests if the address is not in the local table; these requests could go through a number of different DNS servers, from the local server to authoritative servers, top-level domain servers, or roos servers, in order to answer the request.

Once the IP address is determined, a TCP connected is established containing our port number (assigned by the system) as the source, port 80 as the destination. This is, in turn, encapsulated into an IP datagram with our own IP address as source and the result of our DNS search as destination. This is encapsulated into a link-layer frame with our machine’s MAC card number as source and the MAC number of the router connected to the local area network as destination.

We consult our local ARP table to find the MAC address of this router; if it’s not there, we can send an ARP packet out requesting the MAC address for the router’s IP address. The frame is transmitted, probably through a switch, to the router, and the internal BGP routing protocol is used to find a path through the local network to the correct gateway router. At this router, external BGP is used to cross the internet; along the way, of course, intermediate routers are updating time-to-live fields, recalculating header checksums, etc., possibly using internal BGP to router across autonomous networks from one gateway router to another, MAC addresses are being modified from entry router addresses to exit router addresses, segments are being dropped, etc.
When the TCP connection is finally established via a three-way exchange of TCP packets (the “handshake”), the “GET” command sets in motion several more rounds of TCP segment delivery from the Web server to our machine. Note that all the steps taken in the sender are in a sense “undone” by the receiver — its network card verified that the frame(s) received have the correct MAC address, checks the CRC, unpackages the datagram and sends it to the network layer, which verifies the header checksum, sends it up to the transport layer, which checks the checksum and then pass the payload up to the appropriate port associated with the application (in this case, port 80).

The HTML might be cached in our local machine or might be delivered; either way, when we click on the streaming video icon we begin what is most likely a stream of UDP packets containing the video frames to be displayed. Each of these travels through the same path, from the streaming video server through the transport layer, which packages it up into UDP segments, passes it along to the network layer, which sends it to the link layer, etc. At each router along the way the UDP packets are “unpackaged” up to the level of the network layer, then repackaged and sent back down the protocol stack, and so on.

None of the above made mention of things like ICMP packets that report, e.g., unreachable nodes in the network or that hold open connections when congestion has caused a momentary reduction of the congestion window to size zero, or of the RIP advertisements that are constantly being sent within local area networks to keep inter-AS routing tables up-to-date.