1. As a communication systems engineer, what are the metrics you would use in system design?

   Throughput, delay, packet loss at the network layer, Bit error rate at the physical layer, Security at the application layer.

2. Describe the layers and corresponding functions of the OSI reference model. What layers comprise the TCP/IP stack?

   See the notes for the OSI and TCP/IP stack definitions and descriptions.

3. What are the pros and cons of cross layer design?

   Communication system design is basically a tradeoff of performance versus complexity. Cross layer design leads to performance gains at the cost of complexity. This complexity can be at run-time or at the design stage. Since cross layer design violates the layered architecture, it could also lead to stifling of innovation and difficult maintenance.

4. I characterized Packet Switching and the End-to-End principle as the two key design choices for the Internet. Describe them.

   Packet switching exp[redacted]bits the idea of statistical multiplexing. The end-to-end principle is the design principle that communication network functions should be implemented at the end host[redacted]of the communication session. For example, TCP provides reliability by requiring the receiver to acknowledge packet receptions to the transmitter.

5. At what layer does ARQ exist? At what layer does TCP exist? Compare them in terms of how they provide reliability.

   ARQ provides link layer reliability at the hop-by-hop level. TCP is at the transport layer and provides end-to-end reliability.

6. Describe the hierarchical structure and addressing of the Internet.

   The internet a hierarchical network of networks with the Internet Protocol (IP) used for routing. IP addresses are assigned in a hierarchical fashion so that routers do not have to maintain entries for all possible addresses (for example, IPv4 has a 32 bit IP address allowing for over 4 billion addresses). If we assign addresses in a hierarchical fashion (so that addresses physically close together share a common address prefix), one entry in a routing table can match multiple addresses. IP addresses use a binary hierarchy (see CIDR in the notes) and routers use longest prefix matching to make forwarding decisions. In other words, hierarchical addressing facilitates routing by allowing blocks of addresses to be grouped together into single routing table entries.

7. Why do we have both MAC & IP Addresses?

   MAC addresses are used by the link layer within a LAN and IP addresses are used by the network layer within an Internet. We have both because LANs are designed to work with arbitrary network layer protocols. Additionally, we do not want the adapter ID of a node to change every time the node is moved. Finally, if the network layer were to read link-layer packets and do filtering, it would slow down processing. In summary, MAC & IP addressing allows for layers to be independent.

8. In setting up a network, should you use a switch or a router? Describe the pros and cons.

   A switch is appropriate for a LAN while a router is needed for connecting two networks. A switch is simpler than a router in that it can learn the forwarding table while the router must be configured. For example, in a home network, a router is needed to share the internet connection between multiple PCs. If you only use a switch, then one of the computers must have two network cards and be configured to do Internet Connection Sharing (which is essentially the router functions).

9. Think about security in a layer 2 switch. Lookup the broadcast storm and ARP/switch poisoning.

   Broadcast storm: http://bit.ly/PKXzzx
   ARP Poisoning: http://en.wikipedia.org/wiki/ARP_spoofing

10. Explain the tradeoff between Packet Switching and Circuit Switching?

    Packet switching exploits statistical multiplexing to increase overall system efficiency since resources are used opportunistically. The main problem is that individual users will not have performance guarantees such as bounded delay or minimum bandwidth. Circuit switching provides guarantees by allocating resources in a static fashion.

1. Retransmission of lost data can be done at the link, transport, and application layers. What are the pros and cons of doing it at each layer?

- Link Layer Retransmission
  - Pro: Avoids resending over end-to-end path, may be more efficient
  - Pro: Hide congestion losses from higher layers
  - Con: Still need end-to-end retransmission
- Transport Layer Retransmission
  - Pro: Do not need to implement retransmission in applications
- Application Layer Retransmission
  - Pro: Some applications can tolerate loss but not delay, so it may be better to let them make the decision.
  - Con: Application complexity is increased.

2. Implicit versus Explicit congestion signals?

- Implicit:
  - An Implicit congestion signal does not require router support.
  - Transport protocols always need to adapt to implicit congestion signals anyway. Explicit congestion signals can be lost, so a lack of an explicit signal does not imply a lack of congestion.
  - Some explicit signals require sending an extra packet to signal congestion. This can cause control traffic congestion collapse.
  - Some explicit signaling schemes set a congestion bit in packets. Selfish receivers can subvert this by not sending the bit back the sender.
- Explicit:
  - An explicit congestion signal can be used for congestion avoidance. Routers can signal congestion when their queues grow long, but before they have to drop packets.
  - An explicit congestion signal requires lower latency to interpret than implicit congestion signals. For example, TCP requires 3 duplicate acknowledgements to determine that a packet has been lost.
  - An explicit congestion signal distinguishes congestion loss from other loss. Wireless networks may drop packets because of signal fading or interference. Route fluttering can send packets into oblivion. This sources of packet loss can be misinterpreted by an implicit congestion signal scheme.

3. What are the main functions of the transport layer? Describe briefly.

   The main function of the Transport Layer is end-to-end reliability. This is achieved primarily through retransmissions, acknowledgments, flow control and congestion control. See the notes for more details.

4. How does the transport layer perform multiplexing and demultiplexing?

   Through the use of port numbers. Processes transmit and listen on certain port numbers and the computer operating system will send packets with that port number to that process. Recall that port numbers are also used by the NAT protocol (which sits at the network layer). What does NAT use port numbers for?

5. Why does TCP wait for three duplicate acknowledgments before retransmitting a packet? What do the triple duplicate acks represent?

   Duplicate acknowledgements are a sign of packet loss. TCP waits for three duplicate acks (which means four acks for a certain missing packet) to ensure the packet is not in flight and is likely lost. Remember there is nothing magical about the number “three”; it is more art than science.

6. How does TCP set its timeout value?

   TCP provides reliability by requiring the receiver to send an acknowledgement to the sender for every packet it receives. Since packets and acks can get lost, TCP sets a timer at the sender and if the data is not acknowledged before the timer expires, the sender resend the data. The timeout duration is a function of how long the sender expects the acknowledgement to arrive and this is a function of the Round Trip Time (RTT). It is the job of the TCP process at the sender to estimate the RTT, as well as its statistics (e.g., mean and variance).

7. TCP congestion avoidance is done via AIMD. Explain.

   TCP congestion avoidance is based on AIMD, which stands for Additive Increase Multiplicative Decrease. This means that TCP increases the congestion window for every window of packets acknowledged and cuts the congestion window in half for every packet that is lost (or inferred lost due to receiving triple duplicate acks). The idea of AIMD is to probe the network congestion limits by increasing the congestion window and then back off when loss occurs. This cycle of probe and backoff is the main principle behind TCP congestion avoidance.

   This cycle is shown in the TCP sawtooth behavior slide of the Transport Layer Protocol notes.

8. What is goal of network fairness? Is TCP fair? If so, explain what resources TCP allocates in a fair manner.

   Network fairness is a complicated issue and mostly depends on your perspective. One common notion of fairness is <u>equal</u> division of resources, for example, fair allocation of bandwidth amongst competing flows. However, flows may have differing bandwidth requirements, so "fair" could also mean allocation of resources <u>proportional</u> to demand. Another notion of fairness is <u>max-min</u> fairness, which aims to maximize the minimum resource that any flow gets.

9. What is the throughput of TCP? The throughput is the average rate that packets are successfully decoded at the receiver. Note that the rate that packets are sent by the sender is an upper bound on the actual throughput and since it is easily computable, we use it to estimate the throughput.

   TCP controls the amount of traffic by adjusting the transmit window size W at the sender. The TCP algorithm tries to give approximately the same window size W to all competing flows. In other words, the resources that TCP allocates fairly is the storage/buffer space in the downstream routers.

   The sending rate of a flow is computed as follows. A flow with a window size of W packets has a throughput of (W/RTT) packets/second. The RTT here is the total round trip time (in seconds), consisting of all possible delays, such as those due to processing, propagation, queuing and transmission delays.

1. What are the benefits of IPv6 over IPv4?

   See notes and the following link:
   http://en.wikipedia.org/wiki/IPv6#Comparison_to_IPv4
   http://www.networkcomputing.com/ipv6/six-benefits-of-ipv6/230500009

2. Describe both Link-State & Distance Vector approaches to routing.

   See notes and the following link:
   http://packetlife.net/blog/2008/oct/02/distance-vector-versus-link-state/
   http://www.javvin.com/routing-protocols.html
   http://en.wikipedia.org/wiki/Distance-vector_routing_protocol
   http://en.wikipedia.org/wiki/Link-state_protocol

3. Classify RIP/OSPF/BGP according to the following metrics: LS or DV, Intra-AS or Inter-AS, Centralized or Distributed.

   RIP – DV, Intra-AS, Distributed
   OSPF – LS, Intra-AS, Centralized
   BGP – DV, Inter-AS, Distributed

4. Many network engineering problems are about resource allocation – namely the allocation of a set of finite resources amongst users with certain needs. Suppose there are 3 users competing for a 90 mbps link. Users 1 and 2 want 50 mbps each and User 3 wants 10 mbps. My solution is to give each one 30 mbps. Is this fair?

   <u>Equal Distribution</u> could be considered fair. It depends on your definition of fairness.

   Another definition of fairness is <u>Proportional Fairness</u> – meaning you give each user bandwidth in proportion to what was requested:
   User 1 and User 2 each get 90*50/110 mbps and User 3 gets 90*10/110 mbps.

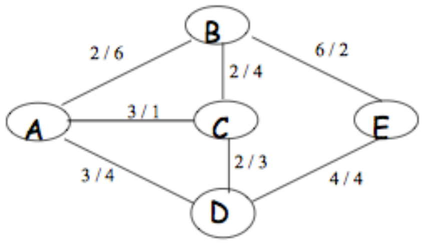
5. We discussed max-min fair in class. What is the max- min fair allocation? What is the TCP fair solution?

   <u>Max-Min Fairness</u>: The aim is to maximize the minimum resource any flow gets. This means that small flows receive what they demand and larger flows share the remaining capacity equally. Bandwidth is allocated equally to all flows until one is satisfied, then bandwidth is equally increased among the remainder and so on until all flows are satisfied or bandwidth is exhausted.

   For the previous problem, the max-min fair allocation is:
   User 3=10 mbps, User 1= User 2 = 40mbps

   <u>TCP Fairness</u> – the allocation algorithm must give the same average resources the same flow using TCP. See http://en.wikipedia.org/wiki/Fairness_measure

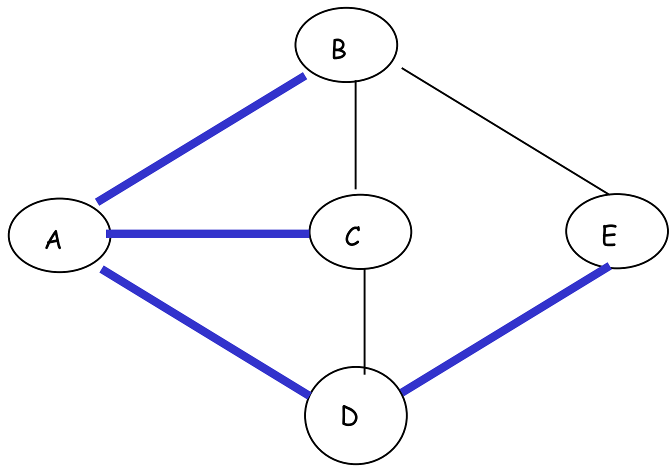
6. Consider the communication graph below. The edge labels are of the form a / b, where a is the cost in dollars of using that link and b is the delay in seconds of using that link. Run Dijkstra's algorithm on this graph and find the optimal route from A to E.



Let's compute least cost optimal routes.

	B	C	D	E
A	2A	3A	3A	∞
AB	--	3A	3A	8B
ABD	--	3A	--	7D
ABDC	--	--	--	7D
ABDCE	--	--	--	--

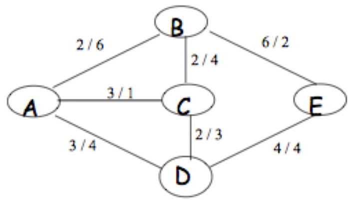
Shortest path: A-D-E
Shortest path Spanning tree shown in bold in graph



Question: What would happen if you had broken the tie differently?

7. For the communication graph above, state the distance vector table that would be computed by node D using the distance vector algorithm.

Let's compute least cost DVs.



		Via (Neighbors of D)		
		A	C	E
Destin-ation	A	3	5	11
	B	5	4	10
	C	6	2	10
	D	6	4	8
	E	10	8	4

$D_A(A)$

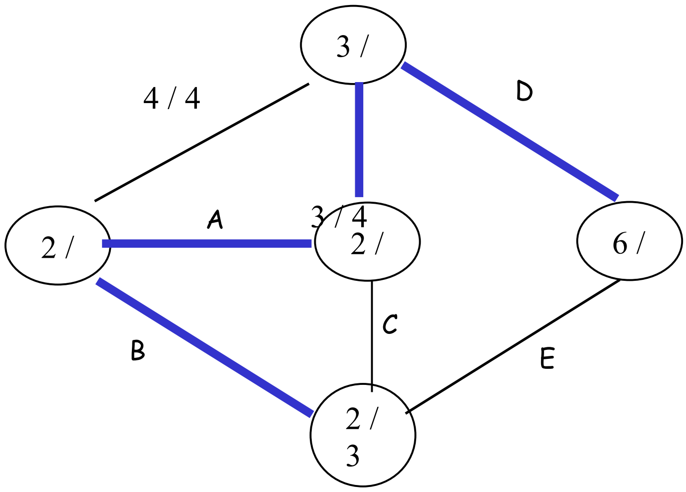
$D_A(C) = \min\{ C(A,C) + D_C(C), \; C(A,D) + D_D(C) = 3+2=5 \}$ $= 3+0=3$

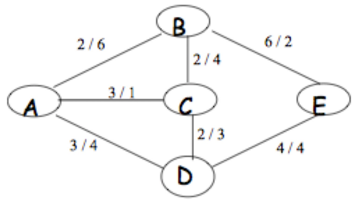
8. Did you notice that the previous two questions (6 &7) were not well defined? Remember that when you see the word "optimal", you should first ask what is the optimality metric? Is it cost? Or is it delay? Compute both the delay optimal route and the cost optimal routes.

   Let's compute <u>minimum delay</u> routes using Dijkstra's Algorithm.

	B	C	D	E
A	6A	1A	4A	∞
AC	5C	--	4A	∞
ACD	5C	--	--	8D
ACDB	--	--	--	7B
ACDBE	--	--	--	--

Shortest path: A-C-B-E
Minimum Delay Spanning tree shown in bold in graph



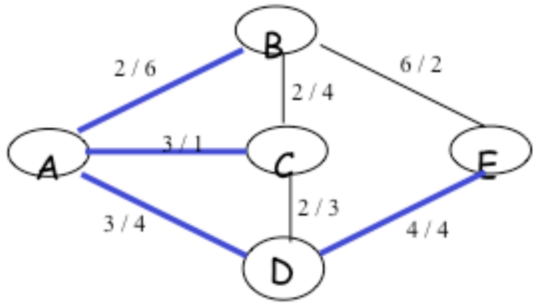


9. In the resource allocation problem, you were asked to compute a "fair" solution. Again, you need to ask first what is the fairness metric? What are some notions of fairness?

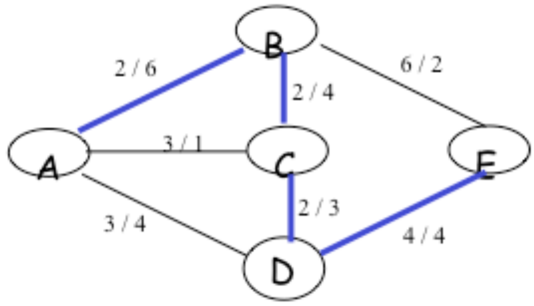
   Equal Distribution Fairness
   Proportional Fairness
   Max-min Fairness
   What other types of fairness can you think of?

10. Compare the Dijkstra Shortest Spanning Tree to the Minimum-cost Broadcast Spanning Tree for the graph in Question 6.

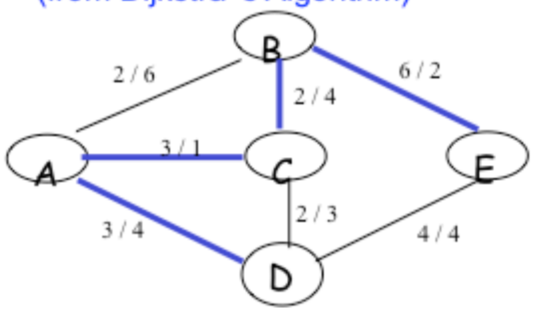
Minimum-cost spanning tree from A
(from Dijkstra's Algorithm)



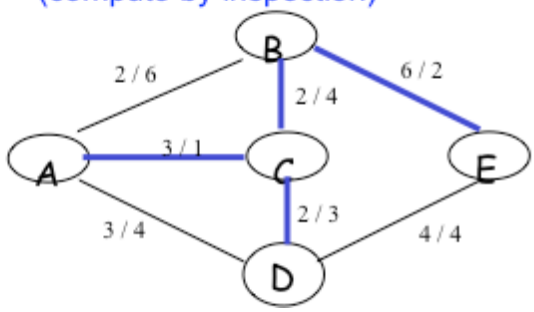
Minimum-cost broadcast spanning tree
(compute by inspection)



Minimum delay spanning tree from A
(from Dijkstra's Algorithm)



Minimum delay broadcast spanning tree
(compute by inspection)



11. Consider a wireless network. Does carrier sensing always work in wireless networks? What MAC does WiFi (802.11) use? Describe it and compare it to the MAC used in Ethernet.

For an overview, see: http://en.wikipedia.org/wiki/Carrier_sense_multiple_access

Ethernet uses CSMA/CD:
http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_detection

Wifi (802.11) uses CSMA/CA:
http://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance

802.11 also has an additional mechanism called the RTS/CTS mechanism:
http://en.wikipedia.org/wiki/IEEE_802.11_RTS/CTS