Network Exam 1 Review Sheet

1. What is a host? Are there more hosts on the internet or non-host network nodes? How do you know?
   1. A host is any computing device that connects to the Internet. This includes PCs, Linux Machines, servers, laptops, smartphones, tablets, TVs, gaming consoles, thermostats, home security systems, home appliances, watches, eyeglasses, cars, traffic control systems, and more. Another term for host is end system. This indicates that hosts are at the network edge.
   2. Definitely more hosts.
   3. I surmise this is true because one DNS server or IXPS node can handle the request of many hosts. According to [Gartner 2014] there were 5 billion devices and by 2020 there would be 25 billion. There certainly isn’t that many DNS, routers, and switches out there.
2. What is a protocol?
   1. A protocol defines the format and the order of messages exchanged between two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or event. The entities exchanging messages and taking actions are hardware or software components of some device (e.g., computer, smartphone, tablet, router, or other network-capable device). All activity on the Internet that involves two or more communicating remote entities is governed by a protocol. Examples: hardware-implemented protocols in two physically connected computers control the flow of bits on the “wire” between the two network interface cards; congestion-control protocols in end systems control the rate at which packets are transmitted between sender and receiver; protocols in routers determine a packet’s path from source to destination.
3. Bandwidth – what does it define, why is it something of a misnomer?
   1. **Bandwidth is the transmission rate of a link(wire).** There are two implementations of moving data through a network of links and switches. Circuit Switching and Packet Switching. In circuit switching the resources needed along a path (buffers, link transmission rate) to provide for communications between the end systems are reserved for the duration of the communication session between the end systems. In packet switch networks, these resources are NOT reserved; a session’s messages use the resources on demand and as a consequence may have to wait (queue) for access to a communication link. For circuit switched networks there is Frequency-Division Multiplexing and Time-Division Multiplexing. With FDM the frequency spectrum of a link is divided up among the connections established on the link. Each connection gets a dedicated frequency band for the duration of the connection. **The width of this band is called the bandwidth. This is inspired from telephone networks and radio towers b/c those technologies use FDM first. Hence the misnomer.** With TDM, time is divided into frames of fixed duration, and each frame is divided into a fixed number of time slots. The network dedicates one time slot in every frame for established connections across a link.
   2. Bandwidth can be a misnomer because people think it relates to speed when in fact it does not. It relates to how much information can travel through a pipe, not at what speed that information travels through the pipe.
4. Compare and contrast a statistical multiplexed (packet switched) vs. a statically multiplexed network. How are they different? What are the advantages and disadvantages of either? What are two classes of static multiplexing?
   1. *See above.* Packet switched networks do not reserve resources along a path to provide communication between the end systems. Instead, a session’s messages use the resources on demand and, as a consequence, may have to wait(queue) for access to a communication link. On the other hand, Circuit switching resources needed along a path to provided communication between two end systems are reserved for the duration of the communication session between the end systems.
   2. Pros vs. Cons: Circuit Switching
      1. PRO:
         1. A given communication session has a dedicated path so other network traffic won’t interfere with this connection. I.e., constant rate guaranteed.
      2. CON:
         1. Can be wasteful if a dedicated path doesn’t utilize the full potential of the resources it has dedicated to it. (Other connections can be using those resources!)
         2. Establishing end-to-end circuits and reserving end-to-end transmission capacity is complicated and requires complex signaling software to coordinate the operation of the switches along the end-to-end path.
   3. Pros vs Cons: Packet Switching
      1. PRO:
         1. The resources of the network are full utilized. Because there is no reservation of resources; everybody has access to all the resources which allows the network resources to be used at 100%. (See C.S. Con).
      2. CON:
         1. Because there are no reserved resources for a given connection, a packet sent into the network may have to be queued while it waits in a buffer for resources to become available. This creates a delay that Circuit Switching doesn’t have.
   4. *See 3a above.* For FDM vs TDM. TDM allows a connection to utilize a link’s full potential while FDM only allocates a percentage of a links frequency.
5. How long does it take a packet of length 1000 bytes to propagate over a link distance of 2500 km, propagation speed (*s*) of 2.5x10^8m/s, and transmission rate of 2mbps?
   1. Dnodal = Dprocessing + Dqueue + Dtrans + Dprop
   2. Dprocessing = processing delay: inspecting header info, determine where to direct packet, time needed to check for bit-level errors. Typically, microseconds.
   3. Dqueue = Waiting on line to be transmitted onto the link. Timing epends on how many packets before this packet. Can be zero if not queue and no packet being transmitted. Can be microseconds or milliseconds in practice.
   4. Dtransmission =This is the amount of time required to push(that is, transmit) all of the packet’s bits into the link. I.e., putting the packet on the wire. Typically, microseconds to milliseconds in practice. *L* = length of the packet in bits. *R* = transmission rate of the link from router A to router B by bits/sec. I.e., 10 Mbps ethernet link, *R* = 10 Mbps;
   5. Dprop = The time required to propagate from the beginning of the link to router B. The bit propagates at the propagation speed of the linkn. That depends on the physical medium of the link; fiber optics, twisted-pair copper, etc.)
   6. Equation Answer:
      1. Transmission = 1000 / 250,000 = 0.004 (remember B vs b)
         1. 1000 bytes / 2mbps
         2. 1000 bytes / (2 \* 10^6 bits/s)
         3. 1000 \* 8 bites / 2,000,000 bits/s
         4. 0.004s
      2. Propagation = 2500km (convert to meters) / 2.5x10^8 meters/sec = 0.01
      3. Total = T + P = 0.014 sec
         1. 2,500,000 m / (2.5 \* 10^8 m/s) + 1000 Bytes / (2 \* 10^6 bits/s)
         2. 0.01 s + 0.004 s
         3. 0.014 s
      4. Transmission Delay for pushing 1 bit onto the wire:
         1. 1 bit / bandwidth
         2. 1 bit / X bit/s
         3. = 1 / X s
      5. Transmission Delay for pushing 100 bits onto the wire:
         1. 100 bits / bandwidth\_of\_wire
         2. 100 bits / X bits/s
         3. 100 / X s
6. What is an ISP? What different types of ISPs exist?
   1. ISPs are Internet Service Providers. They act as entry points for end systems into the Internet(assuming low tier); high tier ISPs act as entry points for low tier ISPs into the Internet.. Each ISP is in itself a network of packet switches and communication links.
   2. There are tier 1 ISPs, Content Provider Networks, IXPs, Regional ISPs, and Access ISPs. Generally broken into two groups. High tier and low tier ISPs. High tier ISPs include Tier 1 and Content provider networks. Examples are Level 3 Communications, AT&T, and NTT, and Google. Low tier ISPs are IXPs, PoPs, Regional ISPs, and Access ISPs. Access ISPs typically include residential ISPs, corporate ISPs, university ISPs, ISPs that provide WiFi access at airports/coffee shops etc and cellular data ISPs. Regional ISPs typically have many access ISPs connect to them and then the regional ISP connects to high tier ISPs. in China, there are access ISPs in each city, which connect to provincial ISPs, which in turn connect to national ISPs, which finally connect to tier-1 ISPs. The lower-tier ISPs connect to the higher-tier ISPs, and the higher-tier ISPs interconnect with one another. Users and content providers are customers of lower-tier ISPs, and lower-tier ISPs are customers of higher-tier ISPs. In recent years, major content providers have also created their own networks and connect directly into lower-tier ISPs where possible.
7. What are Internet Exchange Points (IXPs) and Points of Presences (PoPs)?
   1. IXPs are a meeting place for multiple ISPs to peer together. Typically, it is its own stand-alone building with its own switches
   2. A PoP is simply a group of one or more routers (at the same location) in the provider’s network where customer ISPs can connect into the provider ISP. PoPs exist in all levels of the hierarchy, except for the bottom level (access ISPs). For a customer network to connect to a provider’s PoP, it can lease a high-speed link from a third-party telecommunications provider to directly connect one of its routers to a router at the PoP.
   3. Any ISP (except for tier-1 ISPs) may choose to multi-home, that is, to connect to two or more provider ISPs. So, for example, an access ISP may multi-home with two regional ISPs, or it may multi-home with two regional ISPs and also with a tier-1 ISP. Similarly, a regional ISP may multi-home with multiple tier-1 ISPs. When an ISP multi-homes, it can continue to send and receive packets into the Internet even if one of its providers has a failure.
   4. From someone else: IXPs: An Internet exchange point (IXP) is a physical location through which Internet infrastructure companies such as Internet Service Providers (ISPs) and CDNs connect with each other. These locations exist on the “edge” of different networks and allow network providers to share transit outside their own network. By having a presence inside of an IXP location, companies are able to shorten their path to the transit coming from other participating networks, thereby reducing latency, improving round-trip time, and potentially reducing costs.
8. How does the Traceroute command work?
   1. When the user specifies a destination hostname, the program in the source host sends multiple, special packets toward that destination. As these packets work their way toward the destination, they pass through a series of routers. When a router receives one of these special packets, it sends back to the source a short message that contains the name and address of the router. The source records the time that elapses between when it sends a packet and when it receives the corresponding return message; it also records the name and address of the router (or the destination host) that returns the message. In this manner, the source can reconstruct the route taken by packets flowing from source to destination, and the source can determine the round-trip delays to all the intervening routers. Traceroute actually repeats the experiment just described three times, so the source actually sends 3 • N packets to the destination.
9. What are two advantages of having a layered network? What about two disadvantages? What are the layers in the Internet model? In the OSI 7-layer model?
   1. Advantages:
      1. Organization
      2. Explicit structure allows identification, relationship of system’s pieces
      3. Modularization eases maintenance, updating of system
   2. Disadvantages
      1. One layer may duplicate lower-layer functionality. (Error recovery redundance)
      2. One layer may need information that is present only in another layer; this violates the goal of separation of layers.
   3. Application > Transport > Network > Link > Physical
   4. Application > Presentation > Session > Transport > Network > Link > Physical
10. Suppose users share a 2Mbps link. Also suppose each user transmits continuously at 1Mbps when transmitting, but each user transmits only 20% of the time.
    1. When circuit switching is used, how many users can be supported?
       1. 2 since circuit switching dives the bandwidth into equal parts for each user. Since each user transmits continuously at 1Mbps. That implies 2 users can use the 2Mbps link.
    2. When packet switching is used, how many users can be supported?
       1. A lot!
    3. What is the probability a given user is transmitting at any time?
       1. 20%... but it gets deeper than that.
11. What are the advantages of a P2P model over a client server model? Disadvantages?
    1. Advantages
       1. Self-scaling -new peers bring new service capacity (as well as demands)
       2. No reliance on dedicated servers so no 1 point of failure for a service.
       3. Cost effective due to low or no significant server infrastructure and server bandwidth.
    2. Disadvantages
       1. Peers are intermittently connected and change IP address which leads to complex management.
       2. Security , Performance, Reliability due to highly decentralized structure
12. What is a socket?
    1. A file descriptor, an end point of the pipe between a sender and receiver, a software interface. Utilizes a port number to identify the process using the socket. A way for two processes to talk on a machine locally.
13. What does TCP provide that UDP does not? Which is more impactful on the network?
    1. TCP provides reliability above all. Additionally, flow control, congestion control.
    2. I would say TCP is more impactful. It allows users to send and receive everything completely as it was meant to be. With UDP we could loss packets or have them become corrupt without knowing. Additionally, TCP provides flow and congestion control which adds stability to the Internet.
14. In general, what does an HTTP message between 200 and 299 mean?
    1. 2xx: Success - The action was successfully received, understood, and accepted. See RFC 2616.
    2. Others:
       1. 1xx informational response – the request was received, continuing process
       2. 3xx redirection – further action needs to be taken in order to complete the request
       3. 4xx client error – the request contains bad syntax or cannot be fulfilled
       4. 5xx server error – the server failed to fulfil an apparently valid request
15. What are the advantages and disadvantages of persistent vs. non-persistent HTTP? Which would I want to use for a large, one-time file transfer?
    1. Persistent HTTP
       1. PROs
          1. Light weight sites reduce internet traffic and minimize opened connections so the Web Server can serve more requests
       2. CONs
          1. Heavy websites will frequently open and close connections just for the request/response of 1 interaction/object. This can stress the server as well as make maintenance of connections more tedious since connections are opening and closing more frequently.
          2. So much more traffic going through the Internet because of the TCP handshake.
          3. Requires 2 RTTs per object
          4. OS overhead for each TCP connection
          5. Browsers often open multiple parallel TCP connections to fetch referenced objects in parallel
    2. Non-persistent HTTP
       1. PROs
          1. Connection-related resources are saved since 1 connection is maintained for a client. This allows multiple requests and responses to be used by only 1 socket thus saving resources on the server side.
          2. Less Internet traffic because only one TCP handshake per client connection.
          3. As little as one RTT for all the referenced objects (cutting response time in half)
       2. CONs
          1. Idle clients can waste a connection resource, but a timeout interval will eventually free up the connection resources
    3. A persistent HTTP connection would be better for a large, one-time file transfer. Presumably that file will be divided into chunks. If non-persistent http was used each chunk would require the set up and tear down of a TCP connection which is not ideal.
16. What is the difference between IMAP and POP?
    1. POP: Three phases Authorization, Transaction, Update
       1. Authorization: user agent sends a username and password (in the clear) to authenticate the user.
       2. Transaction: User agent retrieves messages, mark messages for deletion, remove deletion marks, and obtain mail statistics.
       3. Update: Occurs when client issues the ***quit*** command. It ends the POP3 session, and the mail server delete the messages marked for deletion.
       4. NO means for folders for the nomadic user. IMAP solves this issue.
    2. IMAP
       1. Like POP3, IMAP is a mail access protocol. It has many more features than POP3. But is significantly more complex.
       2. An IMAP server will associate each message with a folder; when a message first arrives at the server, it is associated with the recipient’s **INBOX** folder. The recipient can then move the message into a new, user-created folder, read the message, delete the message, and so on.
       3. IMAP also provides commands that allow users to search remote folders for messages matching specific criteria. **Note that, unlike POP3,** an IMAP server maintains user state information across IMAP sessions—for example, the names of the folders and which messages are associated with which folders.
       4. Another important feature is that it has commands that permit a user agent to obtain components of messages. For example, a user agent can obtain just the message header of a message or just one part of a multipart MIME message. This feature is useful in low-bandwidth connection scenarios b/c retrieving large messages would force the user to wait for completion of the download.
17. What roles may a Super Node play in a P2P network?
    1. By Super Node we mean a tracker node. When a peer joins a torrent, it registers itself with the tracker and periodically informs the tracker that it is still in the torrent. Thus, the tracker keeps track of the peers that are participating in the torrent. When a new peer joins the torrent, the tracker node randomly selects a subset of peers from the set of participating peers and sends the IP address of the selected peers to Alice. Now Alice can establish concurrent TCP connections with these peers on the subset given to her. These peers are called neighboring peers. Overtime a peer’s neighboring peers will fluctuate due to peers leaving or other peers (outside the original subset) establishing a connection with Alice. Each peer has a chunk from the file, Alice asks her neighbors what chunks they have, and they’ll return their list of chunks. Alice then asks her neighbors for the chunks she does not have. This goes deeper but is beyond the scope of the Tracker Node, admittedly what Alice does with her subset of peers is too (probably).
18. Give a high-level overview of the operation of SMTP from client and server perspectives.
    1. Client:
       1. Bob will connect to their SMTP server using the HELO command.
       2. Bob will then send emails using the MAIL FROM, RCPT TO, and DATA commands. As well as use commands to read messages.
       3. Eventually after Bob is done, they’ll disconnect using the QUIT command.
    2. Server:
       1. Will accept HELO messages to allow clients to connect to the SMTP server.
       2. When clients send a message it goes into the message queue. The server will see the queue is not empty. The server then opens a TCP connection to the corresponding SMTP server involved in the message (handshaking). The SMTP server sends the message to the other SMTP server.
       3. A SMTP server receives messages from other SMTP servers. It reads who the message is address to and puts it into that user’s mailbox.
       4. A server will handle a request to read messages from a user and send them the messages in their mailboxes.
19. Give a high-level overview of how DNS works. Make sure to include the concept of a Root and TLD domain server. Why do root servers exist?
    1. A typical Iterative DNS interaction proceeds in the following way:
       1. A request host asks for an IP address for a human readable name i.e., google.com. The request goes to the local DNS server. It may or may not have this cached. If so, it can directly response with the information needed.
       2. If not, the local DNS server needs to contact a Root DNS Server.
       3. The Root DNS server will respond to the local DNS request with information about the TLD (Top Level Domain) DNS Server that holds information the request is asking for.
       4. The local DNS server than requests this information from the TLD DNS server.
       5. The TLD DNS server responds with information about the Authoritative DNS server for the request.
       6. The local DNS then requests the information from the Authoritative DNS server.
       7. Finally, the Authoritative DNS server responds with the information requested.
       8. The local DNS server takes this information and sends it back to the requesting host.
    2. Hierarchy looks like: Root DNS > TLD DNS > Authoritative DNS
    3. Why does root servers exist?
       1. Root servers provide the IP address of TLD DNS servers. These include .com, .org, .edu, .uk, .fr, .ca etc. Thus they help every DNS request find the appropriate Authoritative DNS server by supplying the TLD DNS server that pertain information for Authoritative DNS servers.
20. Explain, at a high level, the code flow in C or Python of a socket connection and sending/receiving data. What types of sockets can be created and used?
    1. TCP Flow Server
       1. Socket()
       2. Bind()
       3. Listen()
       4. Accept()
       5. Recv()/Send() Loop
       6. Close()
    2. TCP Flow Client
       1. Socket()
       2. (Can use bind() but not necessary)
       3. Connect()
       4. Send()/Recv() Loop
       5. Close()
    3. UDP Flow Server
       1. Socket()
       2. Bind()
       3. Recv()/Send() Loop
       4. Close()
    4. UDP Flow Client
       1. Socket()
       2. (Can use bind() but not necessary)
       3. Send()/Recv() Loop
       4. Close()
    5. For TCP sockets we create a SOCK\_STREAM. For UDP sockets we create a SOCK\_DGRAM.
21. Explain the differences between stop-and-wait, go-back-N, and selective repeat reliable transfer mechanisms.
    1. Stop-And-Wait: Essentially Stop-and-Wait means a sender sends a TCP packet and does not send another one until some form of acknowledgement is received or a timeout event occurs. In the first case depending on the acknowledgement the sender might send a new packet or a previously sent packet. In the second case the sent packet is retransmitted because it is assumed it did not reach its destination.
    2. Go-Back-N: Now instead of waiting on the confirmation of 1 packet being delivered the sender will send a window size of N packets consecutively. Packets now include a sequence number so each packet can be correctly identified, ordered, and acknowledged. Now ACKs are cumulative in this paradigm. Meaning all packets up to, including seq # n on receiving ACK(n). So ACK(n-1) is ACK’d even if we didn’t receive an ACK for it but instead received and ACK for ACK(n). We also drop NAKs. Since this is ACK-only we always send ACK for correctly received packet so far, with highest in-order seq #. We may generate duplicate ACKs, TripDupAck could signify to sender of timeout. If receiver receives out of order packet, we can buffer or not buffer, but most importantly we re-ACK packet with highest in-order seq #; that is the last correctly received packet.
    3. Selective Repeat: S.R. fixes the pitfalls of Go-Back-N. Mainly the fact that GBN can retransmit a large number of packets unnecessarily based on one single packet error. SR avoids unnecessary retransmissions by having the sender retransmit only those packets that it suspects were received in error(i.e. lost or corrupted) at the receiver. This means the receiver must individually ACK correctly received packets. A window size of N is still used to limit the number of outstanding unACK’d packets. However, unlike GBN, the sender will have already received ACKs for some of the packets in the window. The receiver will ACK correctly received packets, out of order or not. Out of order packets are buffered until the missing packets before them arrive. At which point a batch of packets are sent to the upper layer. The sender and receiver will not always have an identical view of what has been received correctly and what has not. For SR protocols, this means that the sender and receiver windows will not always coincide. This has a big impact of the window size that needs to be chosen because a newly sent packet with a reused seq # can be mistaken for an old packet with the same seq #.
22. What is the difference between flow control and congestion control? Why do both exist?
    1. Flow control is when a receiver tells the sender to slow down how fast it is sending messages. This happens because the sender is sending messages faster than the receiver and process and get them out of the receiver’s buffer. This helps prevent buffer overflow issues.
    2. Congestion Control is when too many senders are sending too many messages too quickly. While flow control happens and is controlled by the receiver. Congestion control happens in routers/switches/links etc. Alternatively, congestion can be inferred from a sender by observed loss/delay. Meaning if ACK packets frequently time out.
    3. Both exist so the Internet or servers aren’t overloaded and fail. Without either of these in place various aspects of the Internet can fail due to too many requests or operations. Packets can get lost/dropped, delays increase, retransmission increases, unneeded duplicates are sent, wasted resources as packets can be lost downstream where congestion is happening.
23. Understand how a TCP 3-way handshake works and what initialization is performed.
    1. Step 1: Client chooses **init seq num x**, sends TCP SYN bit = 1 msg.
    2. Step 2: Server receives step 1 message. Server chooses **init seq num y**, send TCP SYN bit = 1 msg, ACK bit = 1, ACKnum = x + 1
    3. Step 3: Client receives step 2 message. Received SYN + ACK(x) indicates server is alive. Sends ACK for SYNACK. (This may contain client-to-server data). Ack bit = 1, ACKnum = y + 1. Server receives ACK(y) which indicates client is alive.
24. Suppose you have a 1Gbps link and two hosts separated on this link at 100ms RTT. How much data (in Bytes) will need to be “in-flight” to achieve full utilization using TCP as a transport?
    1. 1Gbps link = 1e^9 bytes
    2. Dtrans = L / R = L / 1e^9 Bps = 100 ms
    3. Dtrans = L = 100ms \* 1 e^9 Bps = 0.1
    4. 1Gb = 125MB = 125MB/sec link \* 0.1 = 12.5MB = 1.25e+8/sec data in flight
25. Explain TCP’s congestion control operation. What are AIMD, slow start, congestion avoidance? How does a sender respond by adjusting its congestion window and slow start threshold based on inferred loss events?
    1. AIMD = Additive Increase, Multiplicate Decrease. The approach is senders can increase the sending rate until packet loss (congestion) occurs, then decrease the sending rate on loss event. Increase sending rate by 1 (essentially doubling) maximum segment size every RTT until loss is detected. When loss is detected cut the sending rate in half. AIMD creates the sawtooth behavior. TripDupAck usually causes Multiplicative Decrease to kick in. AIMD (a distributed, asynchronous algorithm) has been shown to:
       1. Optimize congested flow rates network wide
       2. Have desirable stability properties.
    2. Other MD Approaches: TCP Cubic and TCP Ren(cut in half – first to implements fast recovery)/Tahoe(unconditionally cut to 1 MSS)
    3. TCP sending behavior: send cwnd bytes wait RTT for ACKS then send more bytes. TCP rate = cwnd/RTT bytes/sec. TCP sender limits transmission: LastByteSent – LastByteAck <= cwnd. Cwnd is dynamically adjusted in response to observed network congestion.
    4. Slow Start: When connection begins initially send cwnd = 1 MSS (Maximum segment size). Double cwnd every RTT. Done by incrementing cwnd for every ACK received. 1, 2, 4, 8, etc. Summary: INITIAL RATE IS SLOW BY RAMPS UP VERY QUICKLY!
    5. Congestion Avoidance: Slow start cannot be sustained for long so congestion avoidance kicks in. Essentially when to switch exponential MSS increase to linear MSS increase? A variable ssthresh SLOW START THREASH. On loss event, ssthresh is set to 1/2 of cwnd just before loss event. So when slow start begins again after a loss event it switches to linear increase once it passes the ssthresh. Thus, when the value of cwnd equals ssthresh, slow start ends and TCP transitions into congestion avoidance mode.
    6. When an inferred loss event occurs cwnd is set to 1 and ssthresh is cwnd/2 when the event occurred i.e., the value it was before it was set to 1.
26. Explain at a high level the operation of fast retransmit and fast recovery in TCP. Why are they useful compared to the alternative?
    1. TCP Fast retransmit: If sender receives TripDupAck for same data, resend unACK’d segment with smallest seq #. It is likely that unACK’d segment was lost, so don’t wait for the timeout.
    2. Fast Recovery, In F.R. the value of cwnd is increased by 1 MSS for every dup ACK received for the missing segment that caused TCP to enter the fast-recovery state. Eventually when an ACK arrives for the missing segment TCP enters the congestion avoidance state after deflating cwnd. If a timeout occurs, fast recovery transitions to Slow Start state after performing the same actions as in slow start and congestion avoidance. I.e., cwnd is set to 1 and ssthresh is set to cwnd/2 when the loss event occurred. (Recommended but not required component of TCP.)