CPE 348 Final Study Guide

Blue: 10 pts

Green: 20 pts

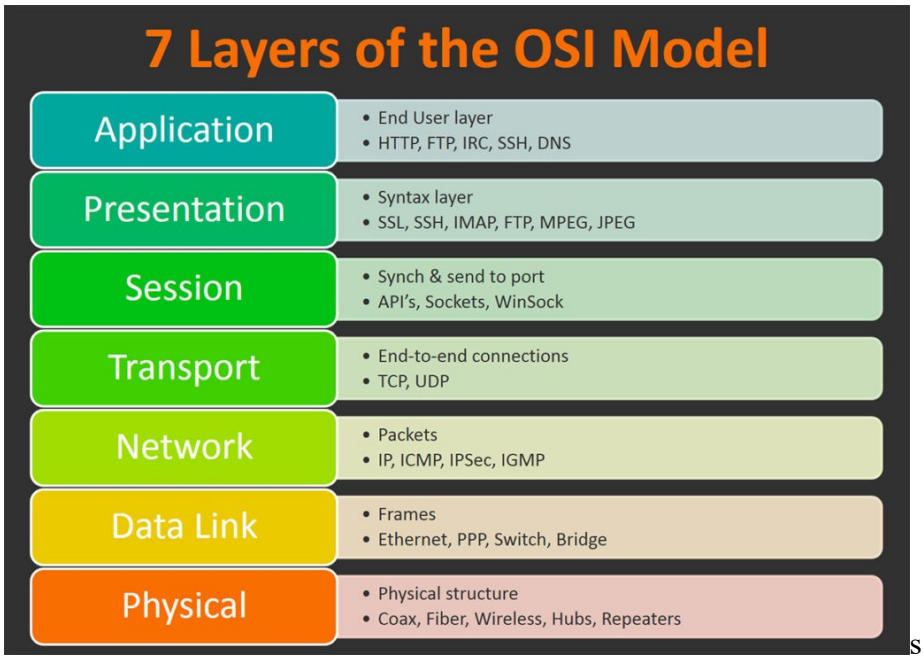
Orange: 30pts

Red: 40pts

? means I am unsure of the answer I put based on what I found in the notes, if someone finds something better feel free to let me know and I will add It!

Chapter 1:

- What is the OSI model?
  - It is the foundation of any computer network
  - It partitions a computer network into abstraction layers
  - A lower layer serves the layer above it
  - It encompasses a wide range of rules, algorithms, and protocols
  - How to remember the layers: All people seem to need Domino's pizza. Reads from top to bottom.
- What layers of OSI model are run on one device?
  - Seven layers? (not sure if this is what this is asking for)
- How to classify a service/function into one OSI layer?
  - ?
  - A data stream will have a series of headers, these headers will specify the layer that it is from and what needs to be done at this layer. (not sure if this is what it was asking for)



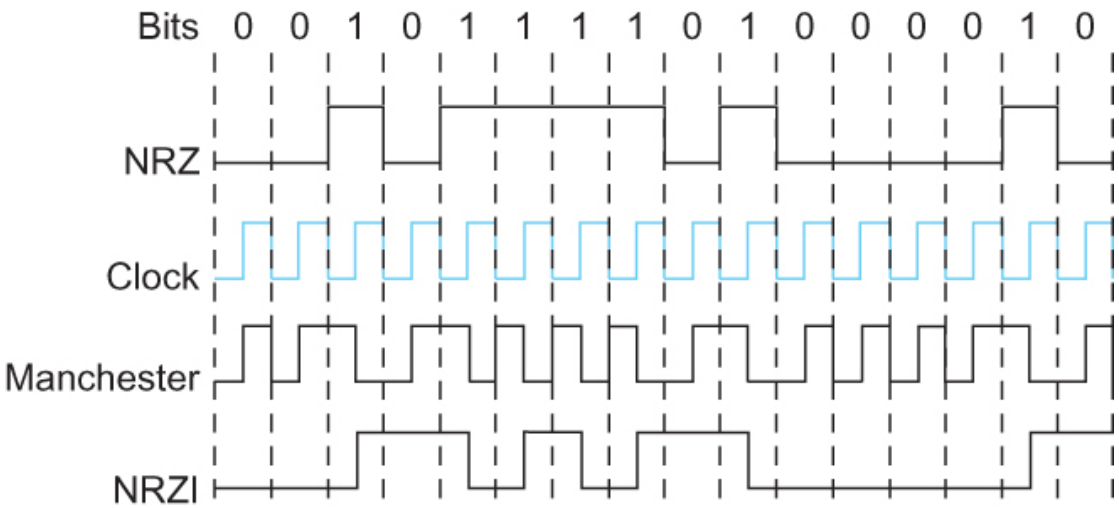
s

- Calculations
    - Delay times bandwidth: We saw this used on advertised window problems the delay was typically given as the RTT, and bandwidth was the speed at which it could send data.
    - Latency = Propagation + transmit + queue
    - Propagation time = distance/speed of light (Exam 1)
    - Transmit time = size/bandwidth
    - Queueing delays: the time at which packets are sent
    - RRT = 2x transmit time
    - **When in doubt look at the units of the values you have, and the unit of the value you are trying to find.**

Chapter 2:

- A communication link(fiber, wireless, etc.): bandwidth, speed of light, noise, capacity, etc.
    - Coaxial cable, Optical fiber, Bluetooth visible light
    - Unless the speed of transmission is otherwise specified, the speed of light is $3x10^8$ meter/second.
    - Can be characterized in Frequency, speed of light, wavelength etc
    - Capacity is $C = B * \log_2(1 + \frac{S}{N})$ where b is the bandwidth, S is the signal power at the receiver and N is the noise power at the receiver
- Encoding: NRZ, NRZI, Manchester, 4B/5B; how does it work? what are pros/cons?
    - NRZ- When the bit is a 1 the transmitted signal is a high, when the bit is a 0 the transmitted signal is a 0
    - The problem with NRZ is baseline wander
        - The receiver keeps an average of the signals it has seen so far to distinguish between low and high signal
        - When a signal is significantly lower than the average, it is 0, else it is 1
        - Too many consecutive 0's and 1's causes this average to change, making it difficult to detect
    - Another problem Clock recovery
        - Both the sending and decoding process is driven by a clock
        - Frequent transition from high to low or vice versa are necessary to enable clock recovery
        - The sender and receiver have to be precisely synchronized
    - NRZI
        - Sender makes a transition from the current signal to encode 1 and stay at the current signal to encode 0
        - Transition occurs on rising clock edge
        - Solves consecutive 1's, but does not solve problem with consecutive 0's

- Manchester
  - Merging the clock with signal by transmitting Ex-OR of the NRZ encoded data and the clock
  - In Manchester encoding
    - 0: low→ high transition
    - 1: high→ low transition
  - Solves consecutive 1's and 0's problem
  - But doubles the rate Which means the receiver has half of the time to detect each pulse of the signal. In other words, consuming more bandwidth
- 4B/5B
  - Insert extra bits into bit stream so as to break up the long sequence of 0's and 1's
  - Every 4-bits of actual data are encoded in a 5- bit code that is transmitted to the receiver
  - Then, transmitted using NRZI
  - 80% efficient
  - So two primary steps are 4 bits are mapped to 5bits and then encode using NZRI



- Framing: Why do we need it? How does HDLC work?
    - Blocks of data (i.e., frames), not bit streams, are exchanged between nodes.
    - any time five consecutive 1's transmitted from the body of the message the sender inserts 0 before transmitting the next bit (bit stuffing)
    - Error bit is a 6^{th} consecutive 1
- Error detection: CRC, 1-D/2-D parity code; how does it work?
    - Probably one of our normal parity code problems is for this
    - One and two D parity code, refer back to those square problems on exam 1 where you need to fill in bits to either get an even or odd amount of 1's
- Layer2 ARQ protocol: stop and wait, sliding window; how does it work; how to avoid their problems(window size, efficiency, etc.); draw transmission diagram given any ARQ protocol; its difference with Layer4 ARQ protocols.
- CSMA/CD or CSMA/CA: definition; its applications; why CSMA/CD not applicable in wireless environment; why 512bits minimal pkt is required in Ethernet for CSMA/CD? Hidden node and exposed node problem; how to address them
    - Carrier Sense Multiple Access with Collision Detection.
        - MA: A set of nodes send and receive frames over a shared link.
        - CS: all nodes can distinguish between an idle and a busy link.
        - CD: a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.
        - Can not use this in a wireless environment due to the hidden/exposed node problem
        - Need 512 bits due to 14 bytes of header + 46 bytes of data + 4 bytes of CRC
        - Because the nodes can only send and receive from one transmission at a time if the node does not see another on the network, it could try to transmit to a node when that node is already receiving data. The solution is to send a request to send frame to the receiver, then the receiver will return a clear to send frame.

Chapter 3:

- Switch and Bridge: virtual circuit switching, topology →switching table & switching table →topology; learning bridge, spanning tree; their differences and similarities (with routers).
- IP addressing: class A/B/C, subnetting, CIDR; why do we need them? IP address assignment efficiency calculation; IP address assignment design; read CIDR-based routing table; IP tunneling (steps, applications, pros and cons).
- Routing: distance vector routing algorithm, link state algorithm: how do they work; what are the problems; how to overcome them; how to derive routing table in network graphs of different settings.

Chapter 4:

- BGP: what is it and how does it work?
  - BGP is the Border Gateway Protocol, and it assumes that the internet is an arbitrarily interconnect set of autonomous systems
  - The goal is to find one path to the destination that is loop free. Priorities reachability more than Optimality
  - Why does the board gateway protocol only find a possible, but not optimal, path to the destination (or an autonomous system)?
    - Different autonomous systems have different cost metrics. There is no universal cost metrics set across them, so it is impossible to find the most optimal path
- IP multicast, particularly source specific multicast (SSM): what are its differences compared with layer 2 multicast? reverse path broadcast (how does it work, what is its disadvantage, simple calculation on its infected nodes); PIM-SM (how does it work, what is a RP).
  - ?
- Mobile routing: how does it work?
  - Has three primary parts – Home agent, home address, and foreign agent
  - *home agent*
    - Router located on the home network of the mobile hosts
  - *home address*
    - The permanent IP address of the mobile host.
    - Has a network number equal to that of the home network and thus of the home agent
  - *foreign agent*
    - Router located on a network to which the mobile node attaches itself when it is away from its home network

Chapter 5:

- TCP/UDP: what are their applications; their differences; what can TCP do; why do we need layer 4 over the IP network; how to establish/teardown a TCP connection.
    - In which application do you prefer UDP to TCP?
        - Very good for streaming services and online gaming that do not require high reliability.
    - In which application do you prefer TCP to UDP?
        - TCP is good for reliable transmission that has error control and remains reliable throughout the entire transmission of data.
    - Layer 4 deals with the process-to-process connection. It contains the ports that things are routed through. Contains a transport protocol
        - A transport protocol promises to
        - Guarantee message delivery
        - Deliver messages in the correct order
        - Support arbitrarily large messages; multiple application processes on each host
        - Allow flow control, congestion control and QoS provisioning
    - 3-way and 4-way handshake
- Flow control/congestion control: definitions and differences; how to achieve them.
    - Flow control is to prevent senders from overrunning the capacity of the receivers
    - Congestion control – prevents too much data from being inject into the network, thereby causing switches or links to become overloaded.
- TCP sequence number: why do we need it? wraparound calculation.
- TCP sliding window protocol:
    - How does tx select its sending window size; what is it based on;
    - delay times bandwidth; RTT estimation (two algorithms); what makes RTT estimation difficult;
    - protocols to adjust window size for congestion control: AIMD; slow start; fast retransmit and fast recovery; how do they work; how could they address each other's problems; draw transmission diagram.

Chapter 6:

- Where are the resources in a network?
  - Bandwidth of the links
  - Buffers at the routers and switches
  -
- What can the network benefit from resource allocation?
  - A network can benefit in having a more effective utilization of the network's resources.
- Queuing
  - FIFO- First in first out- also called first-come-first-served queuing
    - The first packet that arrives is the first packet to be transmitted
    - The amount of buffer space that a router contains is finite if a packet arrives and the queue (buffer space) is full, then the router will drop or discard that packet
    - Uses scheduling discipline- it determines the order in which packets are transmitted
    - Tail drop is its drop policy = it determines which packets get dropped
  - Priority queue – utilizes FIFO queuing
    - Each packet is marked with a priority; the mark is carried somewhere in the packet such as the IP header
    - Will implement FIFO queues, one for each of the priority classes.
    - Always transmit packet of the highest priority first
    - Will tend to dominate transmission time if users do not set the properties correctly
  - FQ – Fair queuing – each flow has its own queue
    - maintains a separate queue for each flow currently being handled by the router.
    - Routers service these queues using a round-robin methodology.
    - Tail drop is used on each queue – prevents any given source from increasing its share of network capacity

        - FQ is designed to be used with end-to-end congestion control methods
        -
    - WFQ – Weighted fair queuing – variation on FQ
        - A weight is assigned to each flow(queue)
        - The weight indicates how many bits are transmitted each time – FQ assigns a value of 1 to all queues
        - Flows could be considered as different classes of traffic
        - WFQ is moving toward a reservation-based resource allocation