Exam 1 Study Guide

Lesson 1: Introduction, History, and Internet Architecture

1. What are the advantages and disadvantages of a layered architecture?
   - Advantages:
     - Scalability
     - Modularity
     - Flexibility
   - Disadvantages:
     - Some layers functionality depends on the information from other layers, which can violate the goal of layer separation
     - One layer may duplicate lower layer functionalities. For example, the functionality of error recovery can occur in lower layers, but also on upper layers as well
     - Some additional overhead that is caused by the abstraction between layers
2. What are the differences and similarities between the OSI model and the five-layered Internet model?
   - Differences
     - In the five-layered model, the application, presentation, and session layers are combined into a single layer called the application layer
   - Similarities:
     - Physical, Data-link, Network, Transport layers
3. What are sockets?
   - Sockets are the interface between the transport and application layers
4. Describe each layer of the OSI model.
   - Physical: Responsible for transferring bits within a frame between two nodes that are connected with a physical link
   - Data-link: Responsible for moving frames from one node to the next (host or router)
   - Network: Responsible for moving datagrams from one Internet host to another
   - Transport: Responsible for end-to-end communication between hosts
   - Session: Manage different transport streams that belong to the same session between end-user application processes
   - Presentation: Formats information from session layer and delivers to application layer (translate big endian to little endian)
   - Application: End-user services run here
5. Provide examples of popular protocols at each layer of the five-layered Internet model.
   - Physical: Ethernet
   - Data-link: PPP, WiFi
   - Network: Internet Protocol
   - Transport: TCP, UDP
   - Application: HTTP, SMTP, FTP, DNS
6. What is encapsulation, and how is it used in a layered model?
   - Encapsulation: Process of taking data from one protocol and translating it into data that are used by another protocol
   - Each layer adds its own header to the message and forwards it to the next layer
7. What is the end-to-end (e2e) principle?
   - e2e principle is a design choice that suggests that specific application-level functions usually cannot, and preferably should not, be built into the lower levels of the system at the core of the network
   - Network should be simple and minimal, while end systems carry the intelligence
8. What are the examples of a violation of e2e principle?
   - Firewalls can drop communication between hosts
   - Hosts behind NAT boxes are not globally addressable or routable
9. What is the EvoArch model?
   - Model for understanding why some protocols persist and other are replaced often
10. Explain a round in the EvoArch model.

- Introduce new nodes and place them randomly at layers
- Examine all layers from top to bottom
  - Connect new nodes by choosing substrates based on the generality probabilities of the layer below and choosing products for them based on the generality probability of the current layer
  - Update the value of each node given the new nodes
  - Examine all nodes in order of decreasing value in that layer and remove nodes that should die
- Stop execution when the network reaches a given number of nodes

11. What are the ramifications of the hourglass shape of the internet?
    - Protocols that have many things depending on them are difficult to replace
12. Repeaters, hubs, bridges, and routers operate on which layers?
    - Repeaters: Layer 1
    - Hubs: Layer 1
    - Bridges: Layer 2
    - Routers: Layer 3
13. What is a bridge, and how does it "learn"?
    - Enable communication between hosts that are not directly connected
    - When a bridge receives a frame, it knows the source host is reachable through the port it received the frame on
14. What is a distributed algorithm?
    - An algorithm where no node has all of the data; each node must communicate to arrive at a solution
15. Explain the Spanning Tree Algorithm.
    - Algorithm runs in rounds. Each round, each nodes to each neighbor a message with three fields
      - Sending node's ID
      - ID of the root as perceived by the sending node
      - The number of hops between that (perceived) root and the sending node
    - At every round, each node keeps track of the best configuration message that it has received so far and compares that against the configuration messages it receives from the neighboring nodes at that round
    - The first round of the algorithm, every node thinks that it is the root
    - How does a node compare two configuration messages? Between two configurations, a node selects one configuration as better if:
      - The root of the configuration has a smaller ID
      - The roots have equal IDs, but one configuration indicates a smaller distance from the root
      - Both root IDs are the same and the distances are the same, then the node breaks the tie by selecting the configuration of the sending node that has the smallest ID
16. What is the purpose of the Spanning Tree Algorithm?
    - Prevent broadcast storms by eliminating loops in the topology
    - Calculates a minimum spanning tree

Lesson 2: Transport and Application Layers

1. What does the transport layer provide?
   - Provides an end-to-end connection between processes that are running on two hosts
2. What is a packet for the transport layer called?
   - Segment
3. What are the two main protocols within the transport layer?
   - TCP and UDP
4. What is multiplexing, and why is it necessary?
   - Allows a host to run multiple applications that use the network at the same time
   - Use ports to determine which application a port is destined for
5. Describe the two types of multiplexing/demultiplexing.
   - Connectionless: UDP, uses only destination IP and port number
   - Connection-oriented: TCP, uses source IP and port and destination IP and port

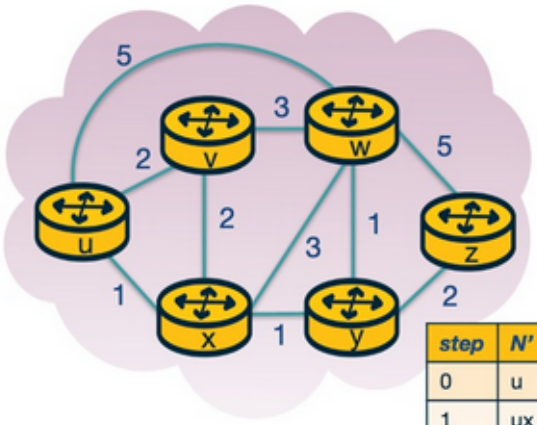
6. What are the differences between UDP and TCP?
    - UDP is connectionless and does not require the three-way handshake before sending packets
    - Fewer delays and better control over sending data
    - No congestion control
    - No connection management overhead
7. When would an application layer protocol choose UDP over TCP?
    - A real-time application that is sensitive to delays would prefer UDP
8. Explain the TCP Three-way Handshake.
    - TCP client sends a special segment (containing no data) with the SYN bit set to 1. The client also generates an initial sequence number (client isn) and includes it in this special TCP SYN segment
    - The server, upon receiving this packet, allocates the required resources for the connection and sends back the special "connection-granted" segment which we call SYNACK segment. This packet has the SYN bit set to 1, the acknowledgement field of the TCP segment header set to (client_isn+1), and a randomly chosen initial sequence number (server_isn) for the server
    - When the client receives the SYNACK segment it also allocates buffer and resources for the connection and sends an acknowledgement with SYN bit set to 0
9. Explain the TCP connection tear down.
    - When the client wants to end the connection, it sends a segment with FIN bit set to 1 to the server
    - The server acknowledges that it has received the connection closing request and is now working on closing the connection
    - The server then sends a segment with FIN bit set to 1, indicating that connection is closed
    - The client sends an ACK for it to the server. It also waits for sometime to resend this acknowledgement in case the first ACK segment is lost
10. What is Automatic Repeat Request or ARQ?
    - The recipient sends an ACK whenever a segment is received
    - If the sender doesn't receive the ACK in some duration, it can simply resend
11. What is Stop and Wait ARQ?
    - Sender waits for acknowledgement from the receiver
    - Requires a reasonable timeout value based on the estimated RTT
12. What is Go-back-N?
    - Receiver sends an ACK for the most recently received in-order packet
    - Sender sends all packets since then, receiver can discard if needed
    - Can cause many unnecessary retransmissions
13. What is selective ACKing?
    - Sender only retransmits packets that it suspects were received in error
14. What is fast retransmit?
    - If a sender receives duplicate acknowledgements for a packet, it considers the packet to be lost and will retransmit it instead of waiting for the timeout
15. What is transmission control, and why do we need to control it?
    - Transmission control is limiting the rate at which segments are sent
    - Needed because the sender doesn't know the link capacity or other traffic on the same link
16. What is flow control, and why do we need to control it?
    - Flow control is controlling the transmission rate to protect the receiver buffer
17. What is congestion control?
    - Limiting transmission rate to prevent protect the capacity of the link
18. What are the goals of congestion control?
    - Efficiency: High throughput
    - Fairness: User should have a fair share of bandwidth
    - Low delay: Real-time applications require responsiveness
    - Fast convergence: Flows should converge quickly to be fair to short flows
19. What is network-assisted congestion control?
    - Relying on network layer to provide explicit feedback to the sender about congestion in the network
20. What is end-to-end congestion control?
    - Hosts infer congestion from the network behavior and adapt transmission rate

- TCP uses this approach

21. How does a host infer congestion?
    - Packet delay (increase in RTT)
    - Packet loss
22. How does a TCP sender limit the sending rate?
    - TCP uses a congestion window similar to the receive window used for flow control
    - When congestion is detected, window is decreased
23. Explain Additive Increase/Multiplicative Decrease (AIMD) in the context of TCP.
    - Additive increase: Increase window by 1 packet every RTT
    - Multiplicated decrease: Halve the window when a loss event occurs
24. What is a slow start in TCP?
    - TCP Reno increases congestion window exponentially instead of linearly then switches to AIMD after meeting a threshold
25. Is TCP fair in the case where connections have the same RTT? Explain.
    - Yes, TCP will guarantee fairness due to AIMD and how it combats congestion
26. Is TCP fair in the case where two connections have different RTTs? Explain.
    - No. Connections with shorter RTT will increase their congestion window more quickly
27. Explain how TCP CUBIC works.
    - TCP CUBIC uses a cubic polynomial as a growth function
    - W(t) = C(t-K)ˆ3 + Wmax
28. Explain TCP throughput calculation.
    - BW < MSS/RTT * 1/sqrt(p)
        - BW: Bandwidth
        - MSS: Maximum Segment Size
        - RTT: Round Trip Time
        - p = Probability loss

Lesson 3: Intradomain Routing

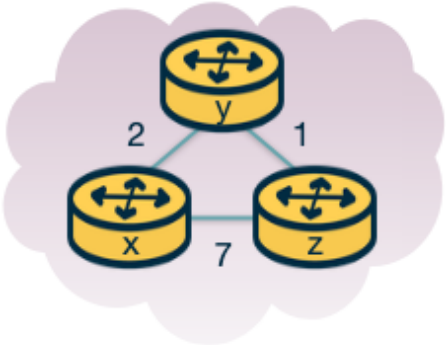
1. What is the difference between forwarding and routing?
    - Forwarding: Transferring a packet from an incoming link to an outgoing link within a single router
    - Routing: How routers work together using protocols to determine routes over which packets travel from the source to the destination node
2. What is the main idea behind a link-state routing algorithm?
    - The link costs and network topology are known to all nodes, so the shortest path can be calculated
3. What is an example of a link-state routing algorithm?
    - Dijkstra's algorithm
4. Walk through an example of the link-state routing algorithm.



step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2, u	5, u	1, u	∞	∞
1	ux	2, u	4, x		2, x	∞
2	uxy	2, u	3, y			4, y
3	uxyv		3, y			4, y
4	uxyvw					4, y
5	uxyvwz					

Link-state Routing Algorithm Example

5. What is the computational complexity of the link-state routing algorithm?
   - O(N^2)
6. What is the main idea behind the distance vector routing algorithm?
   - Similar to link-state routing, but works with negative path weights
7. Walk through an example of the distance vector algorithm.



Node x table

Cost to

From	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Node y table

Cost to

From	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

Node z table

Cost to

From	x	y	z
x	0	2	3
y	2	0	1
z	3	1	0

```
dz(x) =min{c(x,z) + dx(x),c(y,z)+dy(x) }
=min{0+7,1+2}=3
dz(y) =min{c(x,z) + dx(y),c(z,y)+dy(y) }
=min{2+7,1+0}=1
```

Distance-Vector Routing Algorithm Example

8. When does the count-to-infinity problem occur in the distance vector algorithm?
   - When there's a routing loop and one path significantly increases in weight, it can take many iterations for the change to propagate to all other nodes

9. How does poison reverse solve the count-to-infinity problem?
    - One node poisons the route by setting its weight to infinity
    - Only works with two nodes
10. What is the Routing Information Protocol (RIP)?
    - Based on distance vector protocol
    - Uses hop count instead of distance vectors (link cost of 1)
11. What is the Open Shortest Path First (OSPF) protocol?
    - Link-state protocol that uses flooding of link-state information and a Dijkstra's least-cost path algorithm
    - Advancement to RIP protocol
    - Link costs are preconfigured by a network administrator
12. How does a router process advertisements?
    - Router receives a link-state advertisement
    - Router calculates the shortest path use shortest path first algorithm
    - Information in the Forwarding Information Base (FIB) is used when a data packet arrives at an interface card of the router, where the next hop for the packet is decided and is forwarded to the outgoing card
13. What is hot potato routing?
    - When determining which egress point to use for interdomain routing, we pick the one with the lower Interior Gateway Protocol (IGP) cost

Lesson 4: AS Relationships and Interdomain Routing

1. Describe the relationships between ISPs, IXPs, and CDNs.
    - Internet Service Providers form the backbone over which smaller networks can connect
    - Internet Exchange Points (IXPs) provide physical infrastructure over which multiple networks (ISPs and CDNs) can connect and exchange traffic locally
    - Content Delivery Networks (CDNs) are networks that content providers create with the goal of having greater control over how content is delivered while reducing connectivity costs
2. What is an AS?
    - A group of routers (including the links among them) that operate under the same administrative authority
3. What kind of relationship does AS have with other parties?
    - Provider-customer relationship: Based on a financial settlement that determines how much the customer will pay the provider
    - Peering relationship: Two ASes agree to a subset of each other's routing tables
4. What is BGP?
    - Border Gateway Protocol (BGP) is the protocol that border routers of ASes use to exchange routing information
5. How does an AS determine what rules to import/export?
    - Exporting
        - Routes learned from customers: Always advertise, increases revenue
        - Routes learned from providers: Only advertise to customers because there is no financial incentive to advertise these routes
        - Routes learned from peers: Do not advertise because traffic will flow through the peer
    - Importing
        - Routes learned from customers
        - Routes learned from peers
        - Routes learned from providers
6. What were the original design goals of BGP? What was considered later?
    - Original design goals
        - Scalability
        - Express routing policies
        - Allow cooperation among ASes

- Considered later
  - Security

7. What are the basics of BGP?
   - BGP peers exchange routing information over a semi-permanent TCP port connection called a BGP session
   - After peers establish a session, they can exchange BGP messages to provide reachability information and enforce routing policies
     - UPDATE messages contain changes
     - KEEPALIVE messages keep session going
8. What is the difference between iBGP and eBGP?
   - iBGP: Internal, between routers in the same AS
   - eBGP: External, between routers in different ASes
9. What is the difference between iBGP and IGP-like protocols (RIP or OSPF)?
   - IGP-like protocols are used to establish paths between the internal routers of an AS based on specific costs within the AS
   - iBGP is only used to disseminate external routes within the AS
10. How does a router use the BGP decision process to choose which routes to import?
    - If there are multiple route advertisements to the same destination, the router compares a pair of routes by going through a list of attributes
    - LocalPref: Used to prefer routes learned through a specific AS over other ASes
      - Higher is better
    - Multi-exist Discriminator (MED) is used by ASes connected by multiple links to designate which of those links is preferred for inbound traffic
      - Lower is better
11. What are the 2 main challenges with BGP? Why?
    - Misconfiguration and faults: Can result in an excessively large number of updates, resulting in route instability, router processor and memory overloading, and router failures
      - Limit routing table size using filtering
      - Limit the number of routing changes using flap damping
12. What is an IXP?
    - Internet Exchange Points (IXPs) are physical infrastructures that provide the means for ASes to interconnect and directly exchange traffic with one another
13. What are four reasons for IXP's increased popularity?
    - Keeping local traffic local
    - Lower costs
    - Network performance is improved due to reduce delay
    - Critical players in today's Internet ecosystem incentivize other networks to connect at IXPs
14. Which services do IXPs provide?
    - Public peering
    - Private peering
    - Route servers and service level agreements
    - Remote peering through resellers
    - Mobile peering
    - DDoS blackholing
    - Free value-added services
15. How does a route server work?
    - Route servers are used to make peering more manageable
    - Collects and shares routing information from its peers or participants of the IXP that connect to the RS
    - Executes its own BGP decision process and re-advertises the resulting information to all RS's peer routers

Lesson 5: Router Design and Algorithms (Part 1)

1. What are the basic components of a router?
   - Input ports: Physically terminate the incoming links to the router, perform the lookup function (consult forwarding table)
   - Switching fabric: Moving packets from input to output ports
     - Memory
     - Bus
     - Crossbar
   - Output ports: Receive and queue packets from switching fabric and send them over the outgoing link
   - Processor: Perform control plane functions
     - Implement and maintain routing tables
     - Compute the forwarding table
2. Explain the forwarding (or switching) function of a router.
   - Lookup: Router determines output link by looking at the destination IP address
   - Switching: Transfers packet from input link to output link
   - Queueing: Packet may need to be queued if the link is congested
3. The switching fabric moves the packets from input to output ports. What are the functionalities performed by the input and output ports?
   - Input port: Perform the lookup function by consulting the forwarding table
   - Output port: Receive and queue packets from switching fabric and send them over outgoing link
4. What is the purpose of the router's control plane?
   - Determine how data packets are forwarded and decide which routes go into the main routing table
5. What tasks occur in a router?
   - Header validation and checksum
   - Route processing
   - Protocol processing (SNMP, TCP, UDP, ICMP)
6. List and briefly describe each type of switching. Which, if any, can send multiple packets across the fabric in parallel?
   - Memory: When an input receives a packet, it sends an interrupt to the routing processor and the packet is copied to the processor's memory
   - Bus: Routing processor does not intervene; input ports are connected to output ports via a bus
   - Interconnection Network: Use 2N buses to connect N input ports to N output ports, can carry multiple packets in parallel as long as they are using different input and output ports
7. What are two fundamental problems involving routers, and what causes these problems?
   - Bandwidth and Internet population scaling: Increasing number of devices and traffic
   - Services at high speeds: New applications require additional services such as protection against delays, congestion, and attacks
8. What are the bottlenecks that routers face, and why do they occur?
   - Routers can't have explicit entries for all possible destinations due to the increasing number of Internet hosts
   - Different quality-of-service guarantees
   - Crossbar parallelism can cause head of line blocking
9. Convert between different prefix notations (dot-decimal, slash, and masking).
   - Dot decimal
     - 132.234
     - 1000010011101010*
   - Slash notation
     - 132.234.0.0/16
     - 16 denotes only the first 16 bits are relevant for prefixing
   - Masking
     - 132.234.0.0 with mask 255.255.0.0
     - 255.255.0.0 denotes that only the first 16 bits are important

10. What is CIDR, and why was it introduced?
    - Classless Internet Domain Routing (CIDR) is an addressing model based on variable-length prefixes
    - Came into effect as IP addresses were exhausted and helps decrease the router table size
11. Name 4 takeaway observations around network traffic characteristics. Explain their consequences.
    - Large number of concurrent flows of short duration
        - Caching solutions are ineffective
    - Speed of lookup is important
        - Large part of computation cost is accessing memory
    - Unstable routing protocol may adversely impact the update time in the table to add, delete, or replace a prefix
        - Inefficient routing protocols increase this value up to additional milliseconds
    - Vital tradeoff is memory usage
        - Expensive, fast memory: Cache in software, SRAM in hardware
        - Cheaper, slow memory: DRAM, SDRAM
12. Why do we need multibit tries?
    - Unibit tries are very efficient and offer fast lookup and easier updates, but require many memory accesses per lookup
    - Instead, implement lookups using a stride
        - Stride: number of bits that we check at each step
13. What is prefix expansion, and why is it needed?
    - Expand a given prefix to more prefixes to reduce memory accesses
        - Ensure that the expanded prefix is a multiple of the chosen stride length
        - Remove all lengths that are not multiples of the chosen stride length
14. Perform a prefix lookup given a list of pointers for unibit tries, fixed-length multibit tries, and variable-length multibit tries.
15. Perform a prefix expansion. How many prefix lengths do old prefixes have? What about new prefixes?
16. What are the benefits of variable-stride versus fixed-stride multibit tries?
    - Variable-stride allows us to examine a different number of bits every time
    - This allows us to make our prefix database smaller and optimize for memory

Lesson 6: Router Design and Algorithms (Part 2)

1. Why is packet classification needed?
    - As the Internet grows in complexity, networks require quality of service and security guarantees for their traffic
        - Longest prefix matching packet forwarding based on destination IP address is insufficient
        - Need multiple criteria such as TCP flags, source address, etc.
2. What are three established variants of packet classification?
    - Firewalls: Filter out unwanted traffic or enforce security protocols
    - Resource reservation protocols: Reserve bandwidth between a source and destination
    - Routing based on traffic type: Avoid delays for time-sensitive applications
3. What are the simple solutions to the packet classification problem?
    - Linear search: Prohibitive if there are thousands of rules
    - Caching: Hit rate can be high, but still need to perform classification on misses
    - Passing labels: Edge routers do classification and add a header so intermediate routers don't have to reclassify
4. How does fast searching using set-pruning tries work?
    - If we want to search over both source and destination IP address, make a trie where we first search over destination IP address, then each leaf is another tree for source IP address
5. What's the main problem with the set pruning tries?
    - Can lead to memory explosion as we need to store a large amount of data, especially as the dimensionality of the rules grow
6. What is the difference between the pruning approach and the backtracking approach for packet classification with a trie?

- First traverse the destination trie and find the longest destination prefix matching the header
- Work back up the destination trie and search the source trie with every ancestor prefix of D that points to a nonempty source trie
- Trade computation time for memory usage

7. What's the benefit of a grid of tries approach?
   - Reduce time in the backtracking search using precomputation
   - Switch pointers allow us to take shortcuts by pointing to the next possible source trie
8. Describe the "Take the Ticket" algorithm.
   - Each output line maintains a distributed queue for all input lines that want to send packets to it
   - When an input line intends to send a packet to a specific output line, it requests a ticket
   - Input line waits for the ticket to be served
   - Then, the input line connects to the output line, the crosspoint is turned on, and the input line sends the packet
9. What is the head-of-line problem?
   - In the "Take a Ticket" algorithm, the entire queue is blocked by the progress of the head of the queue
10. How is the head-of-line problem avoided using the knockout scheme?
    - We expect that the expected number of outputs k at a link is less than the total N
    - Randomly pick an output using knockout trees to calculate the first k winners
11. How is the head-of-line problem avoided using parallel iterative matching?
    - Have multiple virtual queues for each queue that allow us to make progress even when the head is blocked
12. Describe FIFO with tail drop.
    - Router looks up a packet on an input link using the address lookup component
    - Switching system within the router places the packet in the corresponding output port
      - If the queue is full, drop the packet
13. What are the reasons for making scheduling decisions more complex than FIFO?
    - Need for quality of service, can't drop important data packets
14. Describe Bit-by-bit Round Robin scheduling.
    - One bit from each active flow is transmitted in a round-robin manner
      - Ensures fairness in bandwidth allocation
15. Bit-by-bit Round Robin provides fairness; what's the problem with this method?
    - Not possible to split packets in the real world
16. Describe Deficit Round Robin (DRR).
    - Assign a quantum size Qi and a deficit counter Dk for each flow
      - Qi determines the share of the bandwidth allocated to that flow
      - For each turn of the round robin, algorithm will serve as many packets in the flow i with size less than (Qi + Di)
      - If packets remain in the queue, it will store the remaining bandwidth Di for the next run
      - If all packets are servied, Di is set to 0
17. What is a token bucket shaping?
    - Token bucket shaping limits the burstiness of a flow by:
      - Limiting the average rate
      - Limiting the maximum bust size
18. In traffic scheduling, what is the difference between policing and shaping?
    - Policing: When the traffic reaches the maximum configured rate, excess traffic is dropped, or the packet's setting or "marking" is changed
      - Saw tooth shape
    - Shaping: Retains excess packets in a queue or buffer that is scheduled for later transmission
      - Smooth shape
19. How is a leaky bucket used for traffic policing and shaping?
    - Packets flow out of the bucket at a constant rate, irrespective of the input rate
    - If the bucket is full, additional packets are dropped (policing)
    - Otherwise, they're added to the queue (shaping)