Exam 2 Study Guide

Lesson 7: SDN (Part 1)

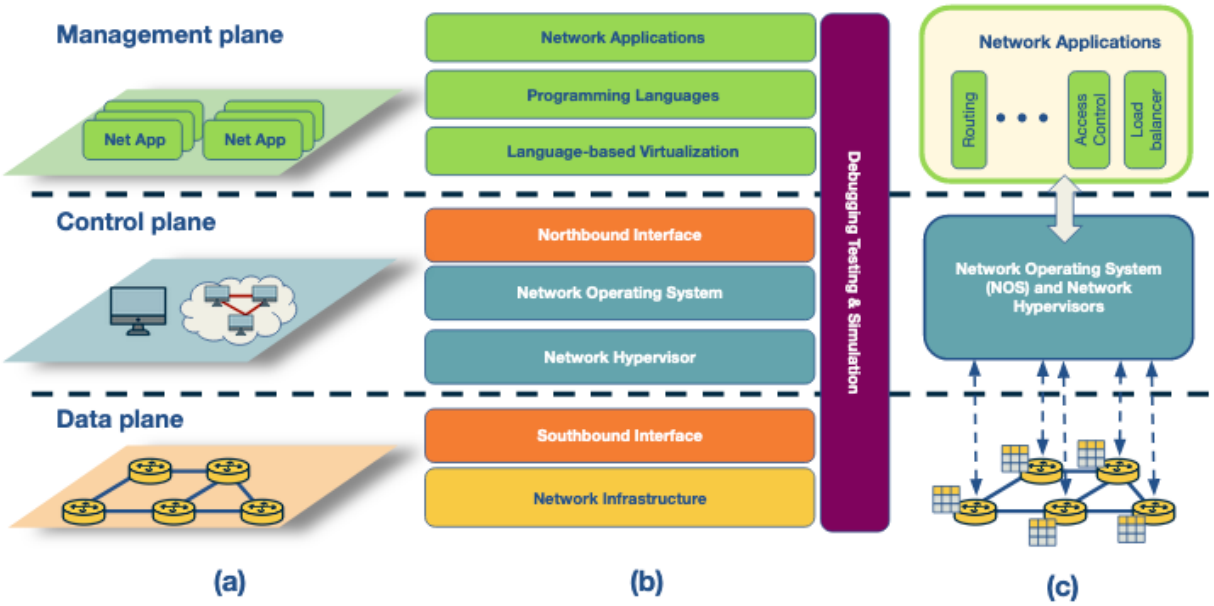
1. What spurred the development of Software Defined Networking (SDN)?
   - Desire to make networks easier to manage
   - Equipment is diverse (middleboxes, routers, switches)
   - Different equipment runs proprietary software, making it difficult to manage
2. What are the three phases in the history of SDN?
   - Active networks
   - Control and data plane separation
   - OpenFlow API and network operating systems
3. Summarize each phase in the history of SDN.
   - Active networks: Open up network control though an API and supported customization of functionalities for aubsets of packets passing through nodes
   - Control and Data Plane Separation: Increase in traffic made network reliability, predictability, and performance more important
     - Focus on programming control plane instead of data plane
   - OpenFlow API: Balance fully programmable networks and practicality of ensuring real world deployment
     - Adopted in industry, unlike its predecessors
4. What is the function of the control and data planes?
   - Control plane: Contains logic that controls the forwarding behavior of routers such as routing protocols and network middlebox configurations
   - Data plane: Performs actual forwarding as dictated by the control plane
5. Why separate the control from the data plane?
   - Independent evolution and deployment
   - Control from high-level software program for easier debugging
   - Software can develop independently from hardware
6. Why did the SDN lead to opportunities in various areas, such as data centers, routing, enterprise networks, and research networks?
   - Data centers: Easier management of thousands of servers and VMs
   - Routing: BGP contrains routes; SDN allows for easier updating of the router's state and more control over path selection
   - Enterprise networks: Easier to protect a network from DDoS attacks by dropping traffic at strategic locations
   - Research networks: Can coexist with production networks
7. What is the relationship between forwarding and routing?
   - Forwarding: Router looks at header of incoming packet and consults the forwarding table to determine the outgoing link to send the packet to
     - Implemented in hardware, function of data plane
   - Routing: Determines the path from the sender to the receiver across the network
     - Implemented in software, function of control plane
8. What is the difference between a traditional and SDN approach in terms of coupling of control and data plane?
   - In traditional approach, routing and forwarding are tightly coupled
   - In SDN approach, a remote controller computes and distributes the forwarding tables to be used by every router
     - Routers are solely responsible for forwarding
9. What are the main components of an SDN network and their responsibilities?
   - SDN-controlled network elements: Responsible for forwarding of traffic in a network based on the rules computed by the SDN control plane
   - SDN controller: Logically centralized entity that acts as an interface between the network elements and the network-control applications

- Network-control applications: Programs that manage the underlying network by collecting information about network elements with the help of the SDN controller

10. What are the four defining features of an SDN architecture?
    - Flow-based forwarding: Compute rules based on transport, network, or link layers
    - Separation of data and control plane
    - Network control functions: Controller maintains information about network devices and the network-control applications monitor and control the devices
    - Programmable network: Network-control applications act as the brain of the SDN control plane by managing the network
11. What are the three layers of SDN controllers?
    - Communication layer: Communication between controller and network elements
    - Network-wide state-management: Information about network state
    - Interface to the network-control application layer: Communicating between controller and applications

Lesson 8: SDN (Part 2)

1. Describe the three perspectives of the SDN landscape.
    - Plane-oriented view
    - SDN layers
    - System design perspective
2. Describe the responsibility of each layer in the SDN layer perspective.
    - Infrastructure: Physical networking equipment are merely forwarding elements and any logic to operate them is directed from the centralized control system
        - OpenFlow
    - Southbound interfaces: Act as connected bridges between control and forwarding elements
        - Play a crucial role in separating control and data plane functionality
        - OpenFlow, ForCES, OVSDB, OpFlex, OpenState
    - Network virtualization: Need to provide support for arbitrary network topologies and addressing schemes, similar to the computing layer
        - VLAN, NAT, MLPS can provide full network abstractions, but are connected on a box-by-box basis and there is no unifying abstraction to configure them in a global manner
        - VxLAN, NVGRE, FlowVisor, FlowN, NVP
    - Network operating systems: Ease network management and solve networking problems by using a logically centralized controller by way of a network operating system
        - OpenDayLight, OpenContrail, Onix, Beacon, HP VAN SDN
    - Northbound interfaces: Abstraction that guarantees programming language and controller independence
        - Floodlight, Trema, NOX, Onix, and SFNet
    - Language-based virtualization: Express modularity and allow different levels of abstractions to view a single physical device in different ways
        - Pyretic, libNetVirt, AutoSlice, RadioVisor, OpenVirteX
    - Network programming languages: Network programmability can be achieved using high- or low-level programming languages
        - Low-level makes it difficult to write and reuse modular code
        - High-level provides abstractions, improves modularity, and does away with specific and low-level configurations
        - Pyretic, Frenetic, Merlin, Nettle, Procera, FML
    - Network applications: Functionalities that implement the control plane logic and translate to commands in the data plane
        - Hedera, Asterx, OSP, OpenQoS, Pronto, Plug-N-Serve, SIMPLE, FAMS, FlowSense, OpenTCP, NetGraph, FortNOX, FlowNAC, VAVE



SDN Landscape

3. Describe a pipeline of flow tables in OpenFlow.
   - Matching rule
   - Actions to be executed on matching packets
   - Counters that keep statistics of matching packets
4. What's the main purpose of southbound interfaces?
   - API for separating data and control planes
   - OpenFlow
5. What are three information sources provided by the OpenFlow protocol?
   - Event-based messages when there is a link or port change
   - Flow statistics generated by forwarding devices
   - Packet messages sent by forwarding devices to controller when they don't know what to do with a packet
6. What are the core functions of an SDN controller?
   - Topology, statistics, notifications, device management, shortest path forwarding, security mechanisms
7. What are the differences between centralized and distributed architectures of SDN controllers?
   - Centralized: Single entity that manages all forwarding devices
     - Single point of failure, scaling issues
   - Distributed: Can scale to meet the requirements of large or small networks
8. When would a distributed controller be preferred to a centralized controller?
   - Very large scale network where a centralized controller can't meet the scale requirements
9. Describe the purpose of each component of ONOS (Open Networking Operating System) a distributed SDN control platform.
   - Global network view: Built from network topology and state information
   - Titan: Graph database used to implement the view
   - Cassandra: Distributed key-value store used to implement the view
   - Applications consume information from the view and update these decisions back to the view
10. How does ONOS achieve fault tolerance?
    - ONOS redistributes work of a failed instance to other remaining instances
11. What is P4?
    - Programming Protocol-Independent Packet Processors
    - High-level programming language to configure switches which works in conjunction with SDN

control protocols

12. What are the primary goals of P4?
    - Reconfigurability: Modify how parsing and processing of packets takes place
    - Protocol independence: Switches shouldn't be tied to a single protocol
    - Target independence: Packet processing programs should be programmed independent of underlying target devices
13. What are the two main operations of P4 forwarding model?
    - Configure: Used to program the parser
    - Populate: Entries in the match/action tables specified during configuration may be altered using the populate operations
14. What are the applications of SDN? Provide examples of each application.
    - Traffic engineering: ElasticTree
    - Mobility and Wireless: OpenRadio
    - Measurement and Monitoring
    - Security and Dependability: DDoS detection
    - Data Center Networking: Live migration of networks, real-time monitoring
15. Which BGP limitations can be addressed by using SDN?
    - BGP routes only on destination IP prefix and networks have little control over end-to-end paths
    - SDN addresses this by matching over various header fields
16. What's the purpose of SDX?
    - SDN-based architecture for IXPs
    - Application specific peering, traffic engineering, traffic load balancing, traffic redirection through middleboxes
17. Describe the SDX architecture.
    - Each AS has the illusion of its own virtual SDN switch that connects its border router to every other participant AS
    - Each AS can define forwarding policies as if it is the only participant at the SDX, without influencing how other participants forward packets on their own virtual switches
    - Each AS can have its own SDN applications for dropping, modifying, or forwarding their traffic
18. What are the applications of SDX in the domain of wide-area traffic delivery?
    - Application-specific peering
    - Inbound traffic engineering
    - Wide-area server load balancing
    - Redirection through middleboxes

Lesson 9: Internet Security

1. What are the properties of secure communication?
    - Confidentiality: Only available to sender and receiver
    - Integrity: Hasn't been modified in transit
    - Authentication: Two parties are who they say they are
    - Availability: Communication channel functions correctly
2. How does Round Robin DNS (RRDNS) work?
    - Cycles through DNS records in a round robin manner
    - Distributes the load of incoming requests to several servers at a single physical location
3. How does DNS-based content delivery work?
    - CDNs distribute servers across the world to deliver content
    - Servers are selected using DNS
4. How do Fast-Flux Service Networks work?
    - After the TTL expires, the FFSN returns a different set of A records from a larger set of compromised machines
    - These machines act as proxies between the incoming request and control node, forming a resilient, one-hop overlay network
5. What are the main data sources used by FIRE (FInding Rogue nEtworks) to identify hosts that likely

belong to rogue networks?
   - Botnet command and control providers
   - Drive-by-download hosting providers
   - Phish housing providers
   - Each data source produces a list of malicious IP addresses. FIRE combines information from these lists to identify rogue ASes
6. The design of ASwatch is based on monitoring global BGP routing activity to learn the control plane behavior of a network. Describe 2 phases of this system.
   - Training phase: Learn control-plane behavior typical of both types of ASes by computing statistical features of each AS
   - Operational phase: Given an unknown AS, calculate the features for this AS
7. What are three classes of features used to determine the likelihood of a security breach within an organization?
   - Mismanagement symptoms: Policies aren't in place to prevent attacks
   - Malicious activities: How much malicious activity is originating from the organization's network and infrastructure
   - Security incident reports: Data based on actual security incidents used to train models
8. (BGP hijacking) What is the classification by affected prefix?
   - Exact prefix hijacking: Two different ASes announce a path for the same prefix
   - Sub-prefix hijacking: Works with a sub-prefix of the genuine prefix of the real AS
   - Squatting: Hijacking AS annoucnes a prefix that has not yet been announced by the owner AS
9. (BGP hijacking) What is the classification by AS-Path announcement?
   - Illegitimate AS announces the AS-path for a prefix for which it doesn't have ownership rights
10. (BGP hijacking) What is the classification by data plane traffic manipulation?
   - Attacker hijacks and manipulates network traffic on its way to the receiving AS
   - Dropped: Never reaches the intended destination (blackholing)
   - Eavesdropped: Man-in-the-middle attack
   - Impersonated: Victim is impersonated and response is sent back
11. What are the causes or motivations behind BGP attacks?
   - Human error
   - Targeted attack: MITM attack
   - High impact attack: Widespread disruption of services
12. Explain the scenario of prefix hijacking.
   - Attacker uses a router to send false announcements and hijack the prefix belonging to another AS
13. Explain the scenario of hijacking a path.
   - Attacker manipulates received updates before propagating them to neighbors
14. What are the key ideas behind ARTEMIS?
   - Configuration file: All prefixes owned by the network are listed for reference
   - Mechanism for receiving BGP updates: Allows receiving updates from local routers and monitoring services
15. What are the two automated techniques used by ARTEMIS to protect against BGP hijacking?
   - Prefix deaggregation: Deaggregate prefix or advertise more specific prefix
   - Mitigation with Multiple Origin AS: Third party announces hijacked prefix, network traffic is attracted to the third party organization, which scrubs it and tunnels it to the legitimate AS
16. What are two findings from ARTEMIS?
   - Outsource the task of BGP announcement to third parties
   - Comparison of outsourcing BGP announcements vs prefix filtering: Prefix filtering was found to be less optimal
17. Explain the structure of a DDoS attack.
   - Attacker compromises and deploys flooding servers
   - Attacker instructs flooding servers to send a high volume of traffic to the victim
18. What is spoofing, and how is it related to a DDoS attack?
   - Act of setting a false IP address in the source field of a packet with the purpose of impersonating a legitimate server

19. Describe a Reflection and Amplification attack.
    - Reflection attack: Master commands slaves to send spoofed requests to the reflectors, which send traffic to the victim
    - Reflection and amplification: Requests are chosen in a way that the reflectors send large responses to the victim
20. What are the defenses against DDoS attacks?
    - Traffic scrubbing service: Divert traffic to a specialized server to determine if it's clean or unwanted
    - ACL Filters: ISPs or IXPs deploy at their AS border routers to filter out unwanted traffic
    - BGP Flowspec: Flow specification feature of BGP allows for fine-grained filters across AS domain borders
21. Explain provider-based blackholing.
    - All traffic to a targeted DDoS destination is dropped to a null location
22. Explain IXP blackholing.
    - Victim AS uses BGP to communicate the attacked destination prefix to its upstream AS, which then drops the attack traffic towards this prefix
23. What is one of the major drawbacks of BGP blackholing?
    - Destination under attack becomes unreachable because all the traffic is being dropped

Lesson 10: Internet Surveillance and Censorship

1. What is DNS censorship?
    - Large scale network traffic filtering strategy opted by a network to enforce control and censorship over Internet infrastructure to suppress material which they deem as objectionable
2. What are the properties of GFW (Great Firewall of China)?
    - Locality of GFW Nodes: GFW nodes present at the edge ISPs
    - Centralized management: GFW manager orchestrates blocklists at nodes
    - Load balancing: GFW load balances between processes based on source and destination IP address
3. How does DNS injection work?
    - GFW uses a ruleset to determine when to inject DNS replies to censor network traffic
4. What are the three steps involved in DNS injection?
    - DNS probe is sent to the DNS resolvers
    - Probe is checked against the blocklist of domains and keywords
    - For domain-level blocking, a fake DNS A record response is sent back
        - Block domain directly, or based on keywords in domain
5. List five DNS censorship techniques and briefly describe their working principles.
    - Packet dropping: Traffic going to a specific IP address is blocked
    - DNS poisoning: DNS receives a query for a hostname, but the server returns no answer or an incorrect answer
    - Content inspection: Network traffic passes through to a proxy where the traffic is examined for content and rejects requests that serve objectionable content
    - Blocking with resets: Send a TCP reset to block individual connections that contain requests with objectionable content
    - Immediate reset of connections: Blocking rules that suspend traffic coming from a source immediately for a short period of time
6. Which DNS censorship technique is susceptible to overblocking?
    - Packet dropping: Two websites that share an IP address might both be blocked
7. What are the strengths and weaknesses of the "packet dropping" DNS censorship technique?
    - Strengths: Easy to implement, low cost
    - Weaknesses: Maintaining blocklist, overblocking
8. What are the strengths and weaknesses of the "DNS poisoning" DNS censorship technique?
    - Strengths: No overblocking
    - Weaknesses: Blocks the entire domain
9. What are the strengths and weaknesses of the "content inspection" DNS censorship technique?
    - Strengths: Precise censorship, flexible

- Weaknesses: Not scalable: Expensive to implement on a large scale network as the processing overhead is large

10. What are the strengths and weaknesses of the "blocking with resets" DNS censorship technique?
    - Strengths: Precise
    - Weaknesses: Unforgiving, one questionable requests will cut the connection
11. What are the strengths and weaknesses of the "immediate reset of connections" DNS censorship technique?
    - Strengths: Precise
    - Weaknesses: Unforgiving, one questionable requests will cut the connection
12. Our understanding of censorship around the world is relatively limited. Why is it the case? What are the challenges?
    - Diverse measurements: Span different geographic regions, ISPs, countries, and regions within a country
    - Scale: Need methods and tools that are independent of human intervention and participation
    - Intent to restrict access: Not just DNS misconfiguration
    - Ethics and minimizing risks: Not safe to involve citizens in studies
13. What are the limitations of main censorship detection systems?
    - Volunteers performed measurements on home networks, making continuous and diverse measurements very difficult
14. What kind of disruptions does Augur focus on identifying?
    - Focuses on IP-based disruptions as opposed to DNS-based manipulations
15. How does Iris counter the lack of diversity while studying DNS manipulation? What are the steps associated with the proposed process?
    - Uses open DNS resolvers located all over the globe to avoid using home routers
    - Main steps:
      - Scanning the Internet's IPv4 space for open DNS resolvers
      - Identifying infrastructure DNS resolvers
16. What are the steps involved in the global measurement process using DNS resolvers?
    - Perform global DNS queries
    - Annotate DNS responses with auxiliary information
    - Additional PTR and TLS scanning: One IP address could host several websites via virtual hosting
17. What metrics does Iris use to identify DNS manipulation once data annotation is complete? Describe the metrics. Under what condition do we declare the response as being manipulated?
    - Consistency metrics: IP address, AS, HTTP content, HTTPS certificate, PTRs for CDN
    - Independent verifiability metrics: HTTPS certificate and HTTPS certificate with SNI
    - If any consistency metric or independent verifiability metric is satisfied, the response is correct; otherwise, it's manipulated
18. How to identify DNS manipulation with Iris?
    - Measurement artifacts
    - Global DNS resolutions
    - Annotate results
    - Secondary scanning (PTR/SNI certificates)
    - Filter
    - Identify correct
    - Results
19. How is it possible to achieve connectivity disruption using the routing disruption approach?
    - Disrupt BGP on critical routers to make parts of the network unreachable
20. How is it possible to achieve connectivity disruption using the packet filtering approach?
    - Block packets meeting a certain criteria
21. Explain a scenario of connectivity disruption detection in the case when no filtering occurs.
    - The measurement machine probes the IP ID of the reflector by sending a TCP SYN-ACK packet. It receives a RST response packet with IP ID set to 6 (IPID (t1)).
    - Now, the measurement machine performs perturbation by sending a spoofed TCP SYN to the site.
    - The site sends a TCP SYN-ACK packet to the reflector and receives a RST packet as a response.

The IP ID of the reflector is now incremented to 7.
    - The measurement machine again probes the IP ID of the reflector and receives a response with the IP ID value set to 8 (IPID (t4)).
22. Explain a scenario of connectivity disruption detection in the case of inbound blocking.
    - Blocking on path to reflector, so the SYN-ACK packet sent from the site in step 3 does not reach the reflector.
    - No response generated, IP ID of the reflector does not increase
23. Explain a scenario of connectivity disruption detection in the case of outbound blocking.
    - Reflector receives SYN-ACK packet and generates a RST packet.
    - IP ID increments to 7.
    - RST packet does not reach the site
    - Can be detected when IP ID increases by 2

Lesson 11: Applications (Video)

1. Compare the bit rate for video, photos, and audio.
    - Video: 2 Mbps
    - Audio: 128 kbps
    - Photos: 320 kbps
2. What are the characteristics of streaming stored video?
    - Interactive
    - Can pause, fast forward, skip ahead, move back
    - Continuous playout, shouldn't freeze up in the middle
3. What are the characteristics of streaming live audio and video?
    - Similar to stored, but with many simultaneous users
    - Delay sensitive
4. What are the characteristics of conversational voice and video over IP?
    - Highly delay sensitive
        - 150 ms acceptable, 400 ms is noticeable
    - Loss tolerant
5. How does the encoding of analog audio work (in simple terms)?
    - Continuous signal is sampled thousands of times per second (44100)
    - Quantized into a discrete number in a particular range
6. What are the three major categories of VoIP encoding schemes?
    - Narrowband
    - Broadband
    - Multimode
7. What are the functions that signaling protocols are responsible for?
    - User location
    - Session establishment
    - Session negotiation
    - Call participation management
8. What are three QoS VoIP metrics?
    - End-to-end delay
    - Jitter
    - Packet loss
9. What kind of delays are included in "end-to-end delay"?
    - Encoding
    - Putting into packets
    - Network delays (queueing)
    - Playback delay from receiver's playback buffer
    - Decoding
10. How does "delay jitter" occur?
    - Different buffer sizes, queueing delays, and network congestion can cause packets to arrive at

different times

11. What are the mitigation techniques for delay jitter?
    - Maintaining a "jitter buffer" - Hides variation in lost packets by buffering them and playing them out for decoding at a steady rate
12. Compare the three major methods for dealing with packet loss in VoIP protocols.
    - Forward error correction: Transmit redundant data
      - Increases bandwidth
    - Interleaving: Mixing chunks of audio together so if one set of chunks is lost, the lost packets aren't consecutive
      - Increases latency, but no extra bandwidth
    - Error concealment: Guessing what the lost audio packet might be
      - Similarity between really small audio snippets
13. How does FEC (Forward Error Correction) deal with packet loss in VoIP? What are the tradeoffs of FEC?
    - FEC transmits redundant data, usually with lower quality
    - Pros: Get the exact data that is missing
    - Cons: Increased bandwidth
14. How does interleaving deal with the packet loss in VoIP/streaming stored audio? What are the tradeoffs of interleaving?
    - Interleaving mixes different chunks of audio together so if packets are lost, they aren't consecutive
    - Pros: No increased bandwidth
    - Cons: Increased latency because the receiver has to wait longer for consecutive chunks
15. How does the error concealment technique deal with packet loss in VoIP?
    - Error concealment guesses what the lost packet might be
      - Probably similar to surrounding packets
      - Can also interpolate
    - Pros: No increased bandwidth or latency
    - Cons: More computationally intensive, might be wrong
16. What developments lead to the popularity of consuming media content over the Internet?
    - Bandwidth has increased tremendously
    - Video compression technologies have become more efficient
    - Digital Rights Management culture has encouraged content providers to put their content on the Internet
17. Provide a high-level overview of adaptive video streaming.
    - Video is created, typically in high quality
    - Compressed using an encoding algorithm
    - Secured using DRM and hosted on a server
    - End-users download the video content over the Internet
    - Content is decoded and rendered on a user's screen
18. (Optional) What are two ways to achieve efficient video compression?
    - Exploit temporal and spatial redundancy
19. (Optional) What are the four steps of JPEG compression?
    - Tranform from RGB to chrominance and brightness
    - Divide the image into 8x8 blocks and apply the Discrete Cosine Transform to each sub-image
    - Compress the matrix of coefficients using a pre-defined quantization table
    - Perform a lossless encoding to store the coefficients
20. (Optional) Explain video compression and temporal redundancy using I-, B-, and P-frames.
    - Instead of encoding each JPEG separately, encode one and then the differences between images
      - I-frame: Initial frame
      - P-frame: Predicted frame (diff)
      - B-frame: Bi-directional, encode a frame as a function of past and future frames
21. (Optional) Why is video compression unable to use P-frames all the time?
    - If a frame is lost, the current frame has to be recomputed from the initial I-frame
22. (Optional) What is the difference between constant bitrate encoding and variable bitrate encoding

(CBR vs. VBR)?
   - CBR: Output size of video is fixed over time
   - VBR: Output size of video remains same on average, but varies
23. Which protocol is preferred for video content delivery - UDP or TCP? Why?
   - TCP: Decoding might fail if data is lost, and TCP offers congestion control
24. What was the original vision of the application-level protocol for video content delivery, and why was HTTP chosen eventually?
   - Original vision: Specialized servers that stored the state of the client
   - HTTP was chosen because it didn't require any specialized hardware
     - Could use existing CDN infrastructure
25. Summarize how progressive download works.
   - Send byte-range requests for content
     - Filling state: Video buffer isn't full so the client tries to fill it
     - Steady state: Video buffer is full, so client waits for it to become lower than a threshold and sends a request for more content
26. How to handle network and user device diversity?
   - Content providers encode their video at multiple bitrates
   - Bitrate adaptation: Picking the best bitrate based on current circumstances
27. How does the bitrate adaptation work in DASH?
   - Client dynamically adjusts the video bitrate based on network conditions and device type
   - Video bitrate is based on its estimation of network conditions
28. What are the goals of bitrate adaptation?
   - Low or zero re-buffering
   - High video quality
   - Low video quality variations
   - Low startup latency
29. What are the different signals that can serve as an input to a bitrate adaptation algorithm?
   - Network throughput: Pick bitrate less than or equal to available throughput
   - Video buffer: Full buffer means we can afford to download high quality chunks
30. Explain buffer-filling rate and buffer-depletion rate calculation.
   - Buffer-filling rate: Network bandwidth divided by chunk bitrate
   - Buffer-depletion rate: 1
   - Need filling to be greater than depleting to have stall-free streaming
31. What steps does a simple rate-based adaptation algorithm perform?
   - Estimate future bandwidth by considering throughput of last few downloaded chunks
   - Quantization: Continuous throughput is mapped to discrete bitrate
   - Client only requests next chunk when there is space in its buffer
32. Explain the problem of bandwidth over-estimation with rate-based adaptation.
   - When the bandwidth changes rapidly, the client has no way of knowing and takes time to converge to the right estimate of bandwidth
33. Explain the problem of bandwidth under-estimation with rate-based adaptation.
   - As bitrate decreases, chunk size also reduces
   - In the presence of a competing flow, a smaller chunk size would lower the probability for the video flow to get its fair share

Lesson 12: Applications (CDNs and Overlay Networks)

1. What is the drawback to using the traditional approach of having a single, publicly accessible web server?
   - Global distribution: Vast distance between users and data center
   - Viral clips: Sending same content over the same link
   - Single point of failure: Server could crash, natural disaster
2. What is a CDN?
   - Content Distribution Network: Networks of multiple, geographically distributed servers and/or

data centers with copies of content that direct users to a server or server cluster that can best serve the user's request

3. What are the six major challenges that Internet applications face?
   - Peering point congestion: No motivation to ugprade the "middle mile"
   - Inefficient routing protocols: BGP not designed for modern demands
   - Unreliable networks: Outages occur often
   - Inefficient communication protocols: TCP not designed for modern demands
   - Scalabilty: Applications need to be able to respond to current demand by changing resource usage
   - Application limitations and slow rate of change of adoption: Even if better protocols are developed, adoption can be slow
4. What are the major shifts that have impacted the evolution of the Internet ecosystem?
   - Demand for large scale content delivery
   - Topological flattening: IXPs offer interconnection between networks
5. Compare the "enter deep" and "bring home" approach to CDN server placement.
   - Enter deep: Many small clusters to decrease geographic distance
   - Bring home: Fewer large clusters at key points
6. What is the role of DNS in the way CDN operates?
   - By intercepting requetss with DNS, CDNs have the opportunity to choose where to direct users, based on location and/or current conditions
7. What are the two main steps in CDN server selection?
   - Map client to a cluster
   - Select a server from the cluster
8. What is the simplest approach to selecting a cluster? What are the limitations of this approach?
   - Pick the geographically closest cluster
   - Limitations: Not necessarily the best end-to-end performance due to routing inefficiencies and congestion
9. What metrics could be considered when using measurements to select a cluster?
   - Network-layer: Delay, available bandwidth, both
   - Application-layer: Re-buffering ratio, average bitrate, page load time
10. How are the metrics for cluster selection obtained?
    - Active: LDNS could probe clusters and monitor RTT, creates lots of traffic
    - Passive: Name server in the CDN keeps track of performance metrics based on current traffic conditions
11. Explain the distributed system that uses a 2-layered system. What are the challenges of this system?
    - Coarse-grained global view of client quality measurements
    - Fine-grained per-client decision layer that operates at the millisecond time scale
    - Challenges:
      - Need to have data for different subnet-cluster pairs
      - Some clients deliberately need to be routed to sub-optimal clusters
12. What are the strategies for server selection? What are the limitations of these strategies?
    - Random: Better to do some load balancing
    - Requests should be routed to the server with the data in cache
      - Keep a hash of the content and always map requests for the same content to the same server
13. What is consistent hashing? How does it work?
    - Consistent hashing: Balance load by assigning roughly the same number of keys to each server, but with minimal movement of these IDs when nodes join and leave the system
      - Map the servers and content to the same space; when a server leaves, we don't have to recalculate anything
14. Why would a centralized design with a single DNS server not work?
    - Single point of failure
    - Can't handle that volume of traffic
    - Central database can't be close to all querying clients
    - Maintaining the database would be a huge undertaking
15. What are the main steps that a host takes to use DNS?

- User host runs client side of DNS application
- Browser extracts the hostname and passes it to the client side of the DNS application
- DNS client sends a query containing the hostname of DNS
- DNS client eventually receives a reply which included IP address for the hostname
- When the host receives the IP address, it can initiate a TCP connection

16. What are the services offered by DNS, apart from hostname resolution?
    - Mail server/host aliasing
    - Load distribution
17. What is the structure of the DNS hierarchy? Why does DNS use a hierarchical scheme?
    - Root DNS server
    - Top level domain (TLD) servers
    - Authoritative servers
    - Local DNS servers
    - DNS hierarchy solves the problems of the single DNS server
18. What is the difference between iterative and recursive DNS queries?
    - Iterative: Querying host is referred to a different DNS server in the chain until it can fully resolve the request
    - Recursive: Querying host, and each DNS server in the chain, query the next server and delegates the query to it
19. What is DNS caching?
    - After a server receives the DNS reply of mapping from any host to IP address, it stores this information in the cache memory before sending it to the client
20. What is a DNS resource record?
    - DNS servers store mapping between hostnames and IP address as RRs
      - Name, value, type, TTL
21. What are the most common types of resource records?
    - A: Name is domain name, value is IP address
    - NS: Name is domain name, value is appropriate authoritative DNS server
    - CNAME: Name is alias hostname, value is canonical name
    - MX: Name is alias hostname of a mail server, value is the canonical name of the email server
22. Describe the DNS message format.
    - ID: Identifier for the query
    - Flags: Query or response, recursive or not
    - Question: Information about the query
    - Answer: Resource records for the hostname that was originally queried
    - Authority: Resource records for more authoritative servers
    - Additional: Other helpful records
23. What is IP Anycast?
    - Routes a client to the closest server as determined by BGP
    - Achieved by assigning the same IP address to multiple servers belonging to different clusters
24. What is HTTP Redirection?
    - When a client sends a GET request to a server, it can redirect the client to another server by sending an HTTP response with a code 3xx and the name of the new server
    - Client fetches content from the new server
      - Incurs additional HTTP request, which can correspond to one or more RRTs, for the client to fetch the content