NE assesement

Layer	Question	Best Answer	Explanation
1 - Physical	What are the differences between single-mode and multi-mode fiber in terms of distance and bandwidth?	**Single-mode fiber (SMF)** supports longer distances (up to 40 km) using a small core and a laser light source, while **multi-mode fiber (MMF)** is limited to shorter distances (typically up to 550m) using an LED light source.	SMF is preferred for long-haul and metro networks, whereas MMF is used in short-range applications like data centers.
1 - Physical	How does signal attenuation affect network performance, and how can you mitigate it in fiber and copper cabling?	Signal attenuation weakens signals over distance. In **copper**, use repeaters or shorter cables. In **fiber**, use higher-quality optics and proper splicing.	Attenuation leads to packet loss and slower speeds; fiber is less prone to interference than copper.
2 - Data Link	What is the difference between VLANs and VXLANs, and how do they impact network segmentation?	VLANs segment Layer 2 traffic within a local network, while VXLANs extend Layer 2 segments over Layer 3 using encapsulation (UDP port 4789).	VXLANs allow scalability beyond traditional VLANs (4094 limit) and support multi-tenant cloud environments.
2 - Data Link	Explain how Spanning Tree Protocol (STP) prevents network loops and describe one alternative protocol that can replace STP.	STP detects and disables redundant links to prevent loops, using a root bridge election. **Alternative: RSTP (Rapid STP)** provides faster convergence, or **TRILL/SPB** eliminates the need for STP by using shortest-path forwarding.	Without STP, broadcast storms can cripple networks. Modern alternatives improve convergence and efficiency.
3 - Network	How does BGP determine the best route to a destination, and what factors can influence its decision?	BGP selects the best path using attributes like AS-Path (shortest route wins), Local Preference (higher is better), MED (lower is preferred), and Next-Hop reachability.	BGP is a path-vector protocol used for inter-domain routing and is critical for internet and ISP-level routing.

Layer	Question	Best Answer	Explanation
3 - Network	Explain the difference between NAT, PAT, and how they impact IPv4 addressing in a corporate environment.	**NAT (Network Address Translation)** maps private IPs to a public IP; **PAT (Port Address Translation)** allows multiple private IPs to share one public IP using port numbers.	PAT is widely used in enterprises to conserve public IPs, enabling many devices to access the internet using a single IP.
4 - Transport	Compare and contrast TCP and UDP. In what scenarios would you choose one over the other?	**TCP** is reliable (error checking, retransmissions) and used for HTTP, SSH, etc. **UDP** is faster but unreliable, used for VoIP, DNS, and video streaming.	TCP is preferred for critical applications, while UDP is used when low latency is required.
4 - Transport	Explain the significance of the TCP three-way handshake and how it impacts security vulnerabilities such as SYN floods.	The handshake (SYN → SYN-ACK → ACK) establishes a connection. **SYN flood attacks** exploit this by sending repeated SYNs without completing the handshake.	Firewalls and SYN cookies can help mitigate SYN flood attacks by preventing resource exhaustion.
5 - Session	How does SSL/TLS establish a secure session between a client and a server?	It uses asymmetric encryption for key exchange (handshake) and symmetric encryption for data transfer (AES, ChaCha20).	TLS ensures confidentiality, integrity, and authentication using certificates (X.509).
5 - Session	What is the role of session persistence (sticky sessions) in load balancing, and how does it affect performance?	It ensures requests from the same client go to the same backend server, improving user experience.	While helpful for stateful applications, it can cause uneven load distribution if not managed properly.
6 - Presentation	How do encryption and compression impact network performance at the presentation layer?	Encryption secures data but increases CPU usage. Compression reduces data size, improving transmission speeds.	Balancing security (encryption) and efficiency (compression) is key in optimizing network performance.
6 - Presentation	Explain the difference between Base64 encoding and actual encryption. In what scenarios would you use each?	**Base64** encodes data for safe transport but is reversible. **Encryption (AES, RSA, etc.)** secures data by making it unreadable without a key.	Use Base64 for data encoding (e.g., email attachments). Use encryption for security (e.g., passwords, confidential data).
7 - Application	What are the differences between HTTP/1.1, HTTP/2, and HTTP/3 in terms of performance and security?	HTTP/1.1 uses sequential requests; HTTP/2 introduces multiplexing and header compression; HTTP/3 uses QUIC for lower latency and better security.	HTTP/3 improves web performance by reducing round-trip delays and mitigating TCP head-of-line blocking.

Layer	Question	Best Answer	Explanation
7 - Application	How does DNS caching work, and what are the security risks associated with DNS cache poisoning?	DNS caching stores query results locally to speed up lookups. **Cache poisoning** injects malicious IP mappings into caches, redirecting users to fraudulent sites.	Mitigations include **DNSSEC** (signing records) and validating responses to prevent tampering.
7 - Application	What is the role of an API gateway in modern cloud networking, and how does it impact microservices architectures?	It manages API traffic, enforcing authentication, rate limiting, and load balancing for microservices.	API gateways help decouple services, improve security, and enable scalable architectures.

Revision #4
Created 2025-03-12 14:18:08 UTC by Mesut Bayrak
Updated 2025-03-17 05:59:16 UTC by Mesut Bayrak