1. How does TCP handle network congestion?

- **Congestion Avoidance**: TCP uses algorithms like AIMD (Additive Increase, Multiplicative Decrease) to adjust the congestion window size based on network feedback.
- **Slow Start**: Initially, TCP starts with a small congestion window and increases it exponentially to detect network capacity.
- **Fast Retransmit and Recovery**: TCP retransmits lost packets quickly and reduces the congestion window to recover efficiently.
- **Explicit Congestion Notification (ECN)**: TCP can use ECN to detect congestion proactively without waiting for packet loss.

---

2. Assess the role of UDP in streaming services and online gaming.

- **Low Latency**: UDP's connectionless nature minimizes delay, crucial for real-time applications like streaming and gaming.
- **Data Loss Tolerance**: These applications can tolerate occasional data loss, prioritizing speed over reliability.
- **Multicasting**: UDP supports multicasting, making it efficient for distributing data to multiple clients simultaneously.

---

3. Explain the principles of the Leaky Bucket algorithm.

- **Fixed Rate**: The algorithm ensures a steady data flow by allowing data packets to be transmitted at a constant rate.
- **Queue Management**: Excess data is stored in a buffer (bucket) and discarded if the bucket overflows, controlling congestion.
- **Simplicity**: The algorithm smoothens traffic but does not allow for bursts, ensuring predictable output.

---

4. Describe the Token Bucket algorithm and how it allows for bursty traffic.

- **Token Accumulation**: Tokens are generated at a fixed rate and stored in a bucket; each token allows the transmission of one data packet.
- **Burst Handling**: Allows bursts of traffic if enough tokens are accumulated, balancing smooth and bursty flows.
- **Flexibility**: It adapts better to variable-rate traffic compared to the Leaky Bucket.

---

5. How do congestion control algorithms like Leaky Bucket and Token Bucket affect real-time applications?

- **Leaky Bucket**: Limits bursty traffic, ensuring predictable latency but potentially dropping packets under high load.
- **Token Bucket**: Accommodates bursts, making it more suitable for real-time applications like video streaming or VoIP.
- **Trade-offs**: Both algorithms balance traffic control and latency, influencing application performance based on traffic patterns.

---

6. Compare the functionality of DNS and FTP in network communication.

- **DNS**: Resolves domain names to IP addresses, enabling user-friendly internet navigation.
- **FTP**: Transfers files between systems, facilitating data sharing.
- **Contribution**: DNS simplifies access to resources, while FTP enables file exchange, complementing internet operations.

---

7. Explain the difference between HTTP and HTTPS.

- **Encryption**: HTTPS encrypts data using SSL/TLS, while HTTP does not, ensuring data confidentiality.
- **Security**: HTTPS provides authentication and prevents data tampering.
- **Preference**: HTTPS is essential for secure transactions like online banking and e-commerce.

---

8. Identify the key parameters of Quality of Service (QoS).

- **Bandwidth**: Ensures sufficient capacity for data transmission.
- **Latency**: Minimizes delay for time-sensitive applications.
- **Jitter**: Reduces variability in packet arrival times for smooth communication.
- **Packet Loss**: Ensures reliable delivery by minimizing dropped packets.

---

9. Evaluate the suitability of space division vs. time division switching.

- **Space Division**: Ideal for simultaneous communication channels like voice calls in circuit-switched networks.
- **Time Division**: Better for multiplexing multiple signals, making it suitable for data and video services.
- **Application**: Space division fits fixed-capacity systems, while time division supports dynamic traffic.

---

10. Discuss the role of the TDM bus in a network.

- **Multiplexing**: Shares a single communication channel among multiple users by allocating time slots.
- **Efficiency**: Optimizes bandwidth usage by sequentially transmitting data.
- **Traffic Management**: Reduces congestion by ensuring orderly access to network resources.

---

11. Analyze the impact of different application layer protocols on network performance.

- **HTTP**: High latency for real-time data due to its request-response model.
- **FTP**: High bandwidth usage for file transfers.
- **SMTP**: Efficient for asynchronous communication but unsuitable for real-time needs.
- **Impact**: Each protocol's design impacts efficiency, latency, and resource usage.

---

12. Examine different types of firewalls.

- **Packet-Filtering Firewalls**: Examine packets based on rules; efficient for basic filtering.
- **Stateful Inspection Firewalls**: Track active connections for more advanced filtering.
- **Application-Level Gateways**: Monitor traffic at the application layer for better security.
- **Scenario**: Packet-filtering is suitable for basic setups, while stateful and application firewalls are ideal for enterprise security.

---

13. Explain the process of converting an analog signal to digital data.

- **Sampling**: Measures the analog signal at regular intervals.
- **Quantization**: Maps sampled values to discrete levels.
- **Encoding**: Converts quantized values into binary code.
- **Techniques**: Proper sampling (Nyquist rate) and fine quantization ensure accuracy.

---

14. Explain the function of DNS in internet infrastructure.

- **Resolution**: Translates domain names into IP addresses for easier access.
- **Hierarchy**: Employs a distributed database with root, TLD, and authoritative servers.
- **Process**: Queries traverse this hierarchy to resolve names.

---

15. Explain how HTTP facilitates browser-server communication.

- **Request-Response Model**: HTTP uses this model to exchange data between clients and servers.
- **Statelessness**: Each request is independent, reducing server load.
- **Importance**: Statelessness simplifies communication but requires additional mechanisms like cookies for session tracking.

---

16. Describe the role of SMTP in email communication.

- **Message Transmission**: Transfers emails from the sender's to the recipient's mail server.
- **Process**: Uses commands like HELO, MAIL, RCPT, and DATA to communicate.
- **Reliability**: Ensures reliable delivery over TCP.

---

17. Explain the role of firewalls in network security.

- **Traffic Filtering**: Monitors and controls data entering or leaving the network.
- **Types**: Packet-filtering for basic needs, stateful inspection for advanced security, and application gateways for comprehensive filtering.
- **Recommendation**: Use a combination of firewalls for layered security in enterprise networks.