Name: Carlos Roque
Student Number: S01299757
Date: December 12th, 2023

1. (15 points) Referred to DNS
   a. (5 Points) Explain the difference between the iterative and recursive approach for Name Resolution in the DNS service.
   Recursive Resolution:

   - In a recursive query, the DNS client expects the DNS server to perform the full resolution process and return the final answer.
   - The client makes a single request to a DNS server. If this server doesn't have the answer, it will query other DNS servers on behalf of the client.
   - The recursive server will continue this process until it finds the authoritative answer or an error occurs.
   - This method can be more convenient for the client but puts more load on the server that handles the recursive queries.

   Iterative Resolution:

   - In an iterative query, the DNS client is willing to perform multiple requests to resolve the name.
   - The client asks a DNS server for the best answer it can provide. If the server doesn't have the final answer, it will return a referral to another DNS server closer to the authoritative source.
   - The client then queries the referred DNS server, and this process continues iteratively until the client reaches an authoritative server or an error occurs.
   - Here, the client handles the resolution process's complexity, reducing the load on individual DNS servers.

   b. (5 Points) Explain the purpose of DNS
   DNS serves a fundamental purpose in the internet infrastructure:

   - **Translates Domain Names into IP Addresses**: The primary purpose of DNS is to translate human-readable domain names (like `www.example.com`) into machine-readable IP addresses (like `192.0.2.1`). This translation is essential because while domain names are easy for humans to remember, computers and networks use IP addresses to locate and communicate with each other.

- **Facilitates Internet Browsing**: By providing this translation service, DNS allows users to easily access websites and services without needing to memorize complex IP addresses.
- **Supports Load Balancing and Redundancy**: DNS can direct traffic to multiple servers, which is useful for load balancing and ensuring high availability of services.

c. (5 Points) Why a secondary server is useful for DNS?
Having a secondary DNS server is crucial for several reasons:

- **Redundancy and Reliability**: If the primary DNS server fails or becomes unreachable, the secondary server can continue to resolve domain names, ensuring uninterrupted internet service.
- **Load Balancing**: A secondary server can share the DNS query load with the primary server, improving performance during high traffic periods.
- **Geographical Distribution**: Secondary servers can be located in different geographic locations, which can reduce latency for users who are far away from the primary server and ensure service continuity in case of regional outages.
- **Faster Updates**: In a setup with multiple DNS servers, updates to DNS records (like changing the IP address of a domain) can propagate more quickly, as each server updates its records.

2. (15 Points) Referred to DHCP
a. (5 Points) Sketch the finite state machine for a DHCP Client.

- INIT: Client starts here, ready to send DHCPDISCOVER.
- SELECTING: Waits for DHCPOFFER after sending DHCPDISCOVER.
- REQUESTING: Chooses an offer and sends DHCPREQUEST.
- BOUND: Enters after receiving DHCPACK, indicating successful configuration.
- RENEWING/REBINDING: Tries to renew or rebind when IP lease nears expiration.

b. (5 points) List at least 5 network configuration parameters that a DHCP message can carry.

- IP Address Lease Time: Duration for which the IP address is valid.
- Subnet Mask: Defines the subnet of the IP address.
- Default Gateway: Primary gateway for network communication.
- DNS Server Addresses: Addresses of DNS servers for resolution.
- Domain Name: Domain name associated with the network.

c. (5 Points) Why the DHCPDiscovery and DHCPOffer messages are broadcast?

- Unknown Server Address: Client doesn't know the DHCP server's address, so it broadcasts DHCPDISCOVER to reach any and all servers.

- Client IP Address Unassigned: Without a configured IP address, the client can't do unicast communication.
- Reaching Multiple Servers: Broadcasting allows the client to receive offers from multiple servers, providing options.

3. (30 Points) Referred to Routing protocols
   a. (10 Points) List three routing techniques and list a protocol for each one.

   - Distance-Vector Routing: Uses distance as a metric to determine the best path. Protocol Example: Routing Information Protocol (RIP).
   - Link-State Routing: Uses the state of each network link to construct a complete view of the network. Protocol Example: Open Shortest Path First (OSPF).
   - Path-Vector Routing: Similar to distance-vector but also includes the path information to reach a destination. Protocol Example: Border Gateway Protocol (BGP).

   b. (10 Points) Write the Dijkstra Algorithm.
   Dijkstra's Algorithm is used for finding the shortest path between nodes in a graph. The steps are:

   - Initialize distances from the source to all vertices as infinite and distance to the source itself as 0.
   - Create a set of all unvisited nodes called the unvisited set.
   - Select the node with the minimum distance from the source from the unvisited set. Call this node the "current node."
   - For the current node, consider all its unvisited neighbors and calculate their tentative distances. Compare the newly calculated distance to the current assigned value and assign the smaller one.
   - After considering all neighbors of the current node, mark the current node as visited. A visited node will not be checked again.
   - If the destination node has been marked visited or if the smallest tentative distance among the nodes in the unvisited set is infinity, then stop. The algorithm has finished.
   - Otherwise, select the unvisited node with the smallest tentative distance and repeat the process.

   c. (5 Points) Referred to RIP, what are the major differences between versions 1 and 2?
   Major differences between RIP version 1 and version 2 are:

   - Addressing: RIP v1 uses classful routing, which does not support subnet information. RIP v2 supports classless routing, allowing for subnet masks.
   - Route Summarization: RIP v2 supports automatic route summarization, whereas RIP v1 does not.

- Multicasting: RIP v2 uses multicasting to send updates, which is more efficient, while RIP v1 uses broadcasting.
- Authentication: RIP v2 can authenticate update messages, adding a layer of security, which is absent in RIP v1.

d. (5 Points) Explain the difference between inter-domains and intra-domains Routing protocols.

- Inter-Domain Routing Protocols: These protocols are used for routing between different domains or autonomous systems. They focus on scalability and policy-based routing. Example: Border Gateway Protocol (BGP).
- Intra-Domain Routing Protocols: These protocols operate within a single domain or autonomous system. They are designed for fast convergence and efficient routing within a smaller scale. Examples: Open Shortest Path First (OSPF), Routing Information Protocol (RIP).

4. (40 Points) Referred to network security

a. (10 Points) List and explain the three security goals (dimensions).

- Confidentiality: Ensures that information is not disclosed to unauthorized individuals, entities, or processes. It involves protecting private data from unauthorized access.
- Integrity: Ensures the accuracy and completeness of data. It protects data from being modified in an unauthorized or undetected manner.
- Availability: Ensures that information is accessible and usable upon demand by an authorized entity. It involves ensuring that network resources are available to legitimate users.

b. (10 Points) List and explain at least one attack type for each security dimensions.

- Confidentiality Attack: Eavesdropping/Sniffing - Attackers intercept and access sensitive information transmitted over the network without authorization.
- Integrity Attack: Data Tampering - This involves unauthorized alteration of data, such as modifying transactions or data files, to achieve malicious objectives.
- Availability Attack: Denial of Service (DoS) - Attackers overwhelm a system's resources, making it unable to respond to legitimate requests, thereby denying service to authorized users.

c. (10 Points) Explain the difference between symmetric and asymmetric cryptography

- Symmetric Cryptography: Uses the same key for both encryption and decryption. It's efficient for large data transfers but requires secure key distribution and management. Example: Advanced Encryption Standard (AES).

- Asymmetric Cryptography: Uses a pair of keys – a public key and a private key. The public key is used for encryption, while the private key is used for decryption. It's more secure for key distribution but less efficient for large data. Example: RSA (Rivest-Shamir-Adleman).

d. (5 Points) What is the objective of digital signature?

- The objective of a digital signature is to provide a secure and tamper-proof way to verify the authenticity and integrity of a message or document. It ensures that the content has not been altered since it was signed and confirms the identity of the signer.

e. (5 Points) Sketch the Message Authentication Method (MAC).
Message Authentication Code (MAC) involves the following steps:

- A sender who wants to send a message securely creates a MAC by encrypting the message with a secret key.
- The sender then sends both the message and the MAC to the receiver.
- Upon receiving, the receiver decrypts the MAC using the same secret key and generates a new MAC from the received message.
- The receiver compares the newly generated MAC with the received MAC. If they match, it confirms the message's integrity and authenticity.

Bonus:
5. (10 Bonus Points) What is the biggest issue in a symmetric cryptography scheme?
The biggest issue in a symmetric cryptography scheme is key distribution and management. In symmetric cryptography, the same key is used for both encryption and decryption. This means that the key must be shared between the sender and receiver in a secure manner. If the key is intercepted or acquired by an unauthorized party during distribution, the security of the encrypted data is compromised.

Key management also becomes complex, especially in large-scale systems with multiple users, as a unique shared key is required for each pair of users to maintain secure communication. This leads to a large number of keys that must be securely created, distributed, stored, and managed, increasing the complexity and potential for security vulnerabilities.