Course Code	:	**BCS-052**
Course Title	:	**Network Programming and Administration**
Assignment Number	:	**BCA(V)/052/Assignment/2024-25**
Maximum Marks	:	**100**
Weightage	:	**25%**
Last Dates for Submission	:	**31st October,2024(For July, Session)** **30th April, 2025(For January, Session)**

There are three questions in this assignment. In total, they carry 80 marks. Answer all the questions. 20 marks are for viva voce. You may use illustrations and diagrams to enhance the explanations. Please go through the guidelines regarding assignments given in the Programme Guide for the format of presentation.

Q1: Illustrate the complete procedure of mapping a domain name to an IP address **(30 marks)**

Q2: Explain different ways of sending a message to multiple recipients **(30 marks)**

Q3: Write a short note on Disk Security Management **(20 marks)**

Q1. Illustrate the complete procedure of mapping a domain name to an IP Address ? (30 Marks)

ANS. Mapping a domain name to an IP address involves a process known as Domain Name System (DNS) resolution. Below is a detailed illustration of this procedure, structured to suit a 30-mark answer:

1. Introduction to DNS (3 marks)

Definition : The Domain Name System (DNS) is a hierarchical and decentralized naming system used to resolve human-readable domain names (like www.example.com) into machine-readable IP addresses (like 192.168.1.1).

Importance : DNS makes it easier for users to access websites without needing to remember complex numerical IP addresses.

2. Components of DNS (5 marks)

DNS Resolver : The client-side component that initiates the DNS query.

Root Name Server : The top-level DNS server that directs the query to the appropriate top-level domain (TLD) server.

TLD Name Server : Handles queries for domains within the TLD (e.g., .com, .org) and directs them to the correct authoritative name server.

Authoritative Name Server : Contains the actual DNS records for the domain and provides the corresponding IP address.

3. Steps in DNS Resolution

a. User Request - The process begins when a user types a domain name into a browser or any application that requires a domain name resolution.

b. DNS Query to the DNS Resolver - The user's computer (client) sends a DNS query to a DNS resolver, usually provided by their Internet Service Provider (ISP).

c. Checking the Local DNS Cache - The DNS resolver checks its cache to see if it already knows the IP address for the requested domain. If the IP is found in the cache, the resolver returns it to the client.

d. Querying Root Name Servers - If the IP is not in the cache, the resolver sends a query to one of the root name servers. The root server does not have the exact IP but knows the authoritative TLD server for the domain.

e. Querying TLD Name Servers - The root server responds with the address of the appropriate TLD server (e.g., .com server for www.example.com). The resolver then queries this TLD server.

f. Querying Authoritative Name Servers - The TLD server provides the resolver with the address of the authoritative name server for the domain. The resolver queries this server for the IP address of the domain.

g. Receiving the IP Address - The authoritative name server responds with the IP address of the requested domain.

4. Returning the IP Address to the Client - The DNS resolver returns the IP address to the client's device, allowing it to establish a connection to the desired server.

5. Caching the Results - The resolved IP address is cached by both the DNS resolver and the client's device for future requests to improve speed and reduce the load on the DNS servers.

6. Conclusion Summary: DNS resolution is a critical process that ensures the seamless conversion of human-friendly domain names into machine-friendly IP addresses, facilitating internet navigation.

Efficiency: The process typically occurs in milliseconds, ensuring a quick and responsive user experience.

Q2.Explain different ways of sending a message to multiple recipient? (30 Marks)

ANS. When discussing different ways of sending messages to multiple recipients, we can explore various methods used in different contexts, such as email, SMS, instant messaging, and social media. Here's a structured explanation suitable for a 30-mark question:

1. Introduction to Message Broadcasting

Definition: Message broadcasting refers to the process of sending a single message to multiple recipients simultaneously.

Importance: This capability is crucial for communication in personal, professional, and marketing contexts, allowing for efficient dissemination of information.

2.Email-Based Methods

To, CC, and BCC Fields

To Field: All recipients in the "To" field are visible to each other. It's used when the sender wants all recipients to see who else received the message.

CC (Carbon Copy): Similar to the "To" field, but used to include additional recipients who need to be kept informed without being the primary audience. All CC'd recipients can see each other.

BCC (Blind Carbon Copy): Recipients in the "BCC" field receive the message, but their addresses are hidden from all other recipients. This is useful for protecting privacy when sending the same message to a large group.

Mailing Lists - Mailing lists allow senders to send messages to a predefined group of recipients via a single email address. They are commonly used for newsletters, announcements, and group communications.

Email Marketing Platforms - Tools like Mailchimp or Constant Contact allow for the mass sending of emails to large groups, often with advanced features like personalization, segmentation, and analytics to track engagement.

3. SMS and Mobile Messaging

Group SMS - SMS services allow for the sending of a message to multiple phone numbers at once. Group SMS is simple and effective, particularly in contexts like notifications or alerts.

Broadcast Lists in Messaging Apps - Apps like WhatsApp allow users to create broadcast lists, where a single message can be sent to multiple contacts. Each recipient receives the message individually, similar to BCC in email.

Bulk SMS Services - These services, often used in marketing or emergency alerts, allow businesses to send a single message to thousands of recipients at once. Features often include message scheduling and delivery reporting.

4. Social Media and Instant Messaging

Group Chats- Platforms like WhatsApp, Telegram, or Facebook Messenger allow users to create group chats, where all members can send and receive messages in a shared conversation.

Social Media Posts- Posting a message on a platform like Twitter, Facebook, or LinkedIn is a way to broadcast information to all followers or connections. While not a direct message, it reaches multiple people simultaneously.

5. Automated Messaging Systems

APIs for Programmatic Messaging - APIs (Application Programming Interfaces) allow developers to integrate messaging capabilities into applications. This enables automated sending of messages to multiple recipients based on triggers or schedules.

Chatbots and AI Systems - Chatbots can be programmed to send automated responses or broadcast messages to multiple users based on interactions or predefined conditions.

6. Conclusion

Summary: Different methods for sending messages to multiple recipients vary in complexity and use case, from simple email and SMS methods to more advanced tools like APIs and email marketing platforms.

Choosing the Right Method : The choice depends on the context, whether for personal use, professional communication, or mass marketing, ensuring effective and appropriate message delivery.

Q3.Write a short note on Disk Security Management?

ANS. Disk security management refers to the practices and technologies employed to protect data stored on computer disks, such as hard drives, SSDs, and external storage devices. Ensuring the security of data at rest is critical in safeguarding sensitive information from unauthorized access, theft, and loss.

1. Data Encryption

- Full Disk Encryption (FDE): This technique encrypts all the data on a disk, rendering it unreadable to unauthorized users without the correct decryption key. Popular tools include BitLocker for Windows and FileVault

File-Level Encryption**: In contrast to FDE, file-level encryption secures individual files or folders, allowing for more granular control over sensitive data.

2. Access Control

User Authentication: Ensuring that only authorized users can access the disk is a fundamental aspect of disk security. This is typically enforced through passwords, biometrics, or multi-factor authentication (MFA).

Permissions and ACLs: Access Control Lists (ACLs) define the permissions for each user or group, specifying who can read, write, or execute files on the disk.

3. Data Loss Prevention

Regular Backups: Regularly backing up disk data is essential to recover from accidental deletions, hardware failures, or malicious attacks like ransomware.

Redundant Storage: Implementing RAID (Redundant Array of Independent Disks) configurations can protect against data loss by duplicating data across multiple disks.

4. Disk Wiping and Secure Deletion

Disk Wiping: When data is no longer needed or before a disk is disposed of, disk wiping ensures that the data is irrecoverable. This is done by overwriting the disk with random data multiple times.

Secure Deletion: Tools like "shred" for Linux or "SDelete" for Windows securely delete files by overwriting the file's data before removal from the filesystem.

5. Physical Security

Secure Storage: Physical access to disks should be controlled, with measures such as locked cabinets, safes, or secure data centers to prevent theft or tampering.

Disk Destruction: When decommissioning disks, physically destroying the storage media (e.g., shredding or degaussing) ensures data cannot be recovered.

6. Monitoring and Auditing

Log Management: Monitoring access logs helps detect unauthorized access attempts or suspicious activity.

Auditing: Regular audits of disk security policies and practices help identify vulnerabilities and ensure compliance with security standards.

Conclusion

Effective disk security management is vital in protecting sensitive information from a variety of threats. By combining encryption, access control, data loss prevention, secure deletion, physical security, and ongoing monitoring, organizations can significantly reduce the risk of data breaches and ensure the integrity and confidentiality of their stored data.