

<b>Course Code :</b> MCS-022
<b>Course Title :</b> Operating System Concepts and Networking Management
<b>Assignment Number :</b> BCA(VI)/022/Assignment/2024-25
<b>Maximum Marks :</b> 100
<b>Weightage :</b> 25%
<b>Last Dates for Submission :</b> 31st October, 2024 (For July, Session) : 30th April, 2025 (For January, Session)

**Note:**

*Answer all the questions of the assignment having 80 marks in total. 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. Answer of each part of the question should be confined to about 300 words.*

**Q1. (a) Compare and contrast the Distributed operating system with the Network operating system. Give an example of each. (6 Marks)**

**Solution:**

**Introduction:**

In my study of "Operating System Concepts and Networking Management," I have encountered two distinct yet related concepts: Distributed Operating Systems (DOS) and Network Operating Systems (NOS). While both deal with managing resources across multiple computers, their approaches and functionalities differ significantly. This response will compare and contrast these two types of operating systems, highlighting their key characteristics and providing relevant examples.

### Comparison and Contrast:

Feature	Distributed Operating System (DOS)	Network Operating System (NOS)
<b>Definition</b>	A single OS that manages a collection of independent computers, making them appear as a single system to the user.	An OS that manages network resources and allows users to share these resources across a network.
<b>Resource Management</b>	Manages resources (CPU, memory, storage, etc.) transparently across the distributed system, providing a unified view to users.	Provides centralized control and management of network resources like files, printers, and security.
<b>Transparency</b>	Offers location transparency, allowing users to access resources without knowing their physical location.	Users are aware of the network and the different resources available across it.
<b>Communication</b>	Utilizes inter-process communication mechanisms between processes residing on different computers.	Relies on network protocols like TCP/IP for communication between computers and resources.
<b>Fault Tolerance</b>	Provides inherent fault tolerance by distributing tasks across multiple computers. If one computer fails, the system can continue operating.	Fault tolerance may be present but is not a core characteristic of the OS. Network failures can impact resource availability.
<b>Example</b>	<b>Google's File System (GFS):</b> GFS distributes data across multiple servers, allowing users to access files seamlessly without knowing their physical location.	<b>Windows Server:</b> Windows Server manages network resources like file sharing, printing, and user accounts within a network environment.

---

**Q1. (b) Define a Real Time Operating System. Give any two examples of a real time operating system. (4 Marks)**

### **Solution:**

In my study of "Operating System Concepts and Networking Management", I have learned about various types of operating systems, including Real-Time Operating Systems (RTOS).

### **Definition:**

A Real-Time Operating System is an operating system that guarantees a response within a specific time constraint. This is crucial in applications where timely responses are critical, such as in industrial control systems, medical equipment, and aerospace systems. RTOS prioritizes tasks based on their deadlines and ensures that critical operations are completed within their defined time windows.

### **Characteristics of an RTOS:**

- **Deterministic Behavior:** Predictable and consistent response times for tasks and events.
- **Fast Context Switching:** Enables rapid switching between tasks for timely execution.
- **Preemptive Scheduling:** Allows higher-priority tasks to interrupt lower-priority tasks.
- **Minimal Overheads:** Keeps system overhead to a minimum to ensure timely responses.

### **Examples of Real-Time Operating Systems:**

1. **VxWorks:** VxWorks is a widely used RTOS in aerospace, defense, and industrial automation. Its features like a small footprint, high performance, and real-time capabilities make it ideal for critical embedded systems.
2. **QNX:** QNX is another prominent RTOS known for its high reliability, scalability, and security features. It's often employed in automotive, medical, and industrial control applications due to its ability to meet stringent timing requirements.

---

**Q2. (a) What is EFS service? Describe the concept of encryption using EFS service. (5 Marks)**

## Solution:

In my study of "Operating System Concepts and Networking Management," I have encountered the Encrypting File System (EFS) service, a crucial security feature offered by Microsoft Windows operating systems.

### What is EFS Service?

EFS is a file system driver that provides encryption capabilities for files and folders stored on NTFS formatted volumes. It allows users to encrypt their sensitive data, protecting it from unauthorized access even if the computer is compromised or data is stolen.

### Concept of Encryption using EFS:

The core concept behind EFS encryption revolves around the following aspects:

1. **File Encryption:** When a user enables EFS for a file or folder, EFS encrypts the file content using a cryptographic algorithm, rendering the data unreadable without the appropriate decryption key.
2. **Encryption Key Management:** EFS manages encryption keys using a hierarchical approach.
  - **File Encryption Key:** Each encrypted file has its own unique encryption key.
  - **User Certificate:** Each user has a digital certificate associated with their user account, storing their public and private keys. The user's private key is used to decrypt the file encryption keys.
  - **Recovery Agent:** A designated user or service (like a domain administrator) can act as a recovery agent. This agent holds a certificate that can be used to decrypt files in case the original user loses access to their private keys.
3. **Data Decryption:** When a user attempts to access an encrypted file, EFS uses the user's private key to decrypt the file encryption key and subsequently decrypts the file content. This process is transparent to the user, ensuring seamless access to their encrypted data.
4. **Integration with NTFS:** EFS leverages the NTFS file system to store encryption information for each file, such as encryption status and key identifiers.

---

**Q2. (b) Compare TFTP and FTP. Which protocol is used by TFTP at the transport layer and why? (5 Marks)**

**Solution:**

**TFTP vs. FTP**

In my "Operating System Concepts and Networking Management" course, I have studied different network protocols, including TFTP and FTP. Both are used for transferring files over a network, but they differ in their features and complexity.

**Comparison:**

Feature	TFTP (Trivial File Transfer Protocol)	FTP (File Transfer Protocol)
<b>Complexity</b>	Simple and lightweight	Relatively complex and feature-rich
<b>Security</b>	No authentication or encryption	Supports user authentication and optional encryption (FTPS)
<b>Functionality</b>	Basic file transfer operations (upload/download)	Supports more complex operations like file listing, renaming, deleting, and directory creation
<b>Reliability</b>	Less reliable, no error recovery mechanisms	More reliable, includes error detection and recovery mechanisms
<b>Application</b>	Transferring configuration files, firmware updates, and small files	Transferring various file types, accessing remote file systems, and managing files on servers

**Transport Layer Protocol used by TFTP:**

TFTP utilizes the **User Datagram Protocol (UDP)** at the transport layer.

**Reason for using UDP:**

The primary reason for choosing UDP is its **simplicity and low overhead**. TFTP is designed to be a very basic file transfer protocol, focusing on speed and ease of implementation. UDP's connectionless nature aligns with this objective, as it does not require establishing a connection or managing complex handshakes, making the process faster and more efficient for simple file transfers.

---

**Q3. (a) List and explain the file systems supported by Linux operating system. Also, write the security features provided by Linux in each file system. (5 Marks)**

**Solution:**

#### **File Systems Supported by Linux:**

Linux supports a wide range of file systems, each with its own characteristics and strengths. Some of the most common include:

**1. Ext4 (Extended file system 4):**

- **Description:** Ext4 is the default file system for many Linux distributions. It's a journaling file system that provides improved performance, reliability, and scalability compared to its predecessors.
- **Security Features:**
  - **Access Control Lists (ACLs):** Allows granular control over file and directory permissions for individual users and groups.
  - **Journaling:** Ensures data integrity and consistency in case of system crashes or power failures.
  - **Data Integrity Checks:** Periodically verifies file system integrity and detects errors.

**2. XFS (X Filesystem):**

- **Description:** XFS is a high-performance journaling file system optimized for large file systems and high I/O workloads. It's commonly used in server environments.
- **Security Features:**
  - **ACLs:** Provides granular access control similar to Ext4.

- **Journaling:** Maintains data integrity during operations.
- **Large File Support:** Can handle very large files, making it suitable for storing massive datasets.

3. **Btrfs (B-tree file system):**

- **Description:** Btrfs is a relatively new file system that offers advanced features like snapshots, copy-on-write, and built-in data integrity checks.
- **Security Features:**
  - **Snapshots:** Enables creating point-in-time copies of the file system, useful for backups and recovery.
  - **Data Integrity Checks:** Ensures data consistency and detects corruption.
  - **RAID Support:** Supports RAID configurations for redundancy and fault tolerance.

4. **NTFS (New Technology File System):**

- **Description:** NTFS is a file system primarily associated with Windows operating systems, but Linux can read and write to it with the appropriate drivers.
- **Security Features:**
  - **ACLs:** Supports detailed access controls.
  - **Encryption:** Provides encryption capabilities for individual files and folders (using EFS in Windows).
  - **Compression:** Allows file compression to save storage space.

5. **FAT32 (File Allocation Table 32):**

- **Description:** FAT32 is an older file system primarily used for compatibility with older operating systems and devices.
  - **Security Features:**
    - **Basic Permissions:** Offers rudimentary permissions like read, write, and execute.
    - **Limited Security:** Security features are limited compared to more modern file systems.
-

**Q3. (b) Compare and Contrast the 'Mandatory Access Control' and 'Discretionary Access Control' mechanism in windows 2000. (5 Marks)**

**Solution:**

### **Mandatory Access Control vs. Discretionary Access Control in Windows 2000**

In my study of Operating System Concepts and Networking Management, I have learned about different access control mechanisms employed by operating systems to ensure security. Windows 2000 utilizes both Mandatory Access Control (MAC) and Discretionary Access Control (DAC) to manage access to resources. Let me compare and contrast these two mechanisms:

#### **Mandatory Access Control (MAC):**

- **Definition:** MAC enforces access control based on pre-defined security labels associated with both users and resources. These labels represent sensitivity levels (e.g., Confidential, Secret, Top Secret).
- **Enforcement:** The system automatically enforces access rules based on the security labels, regardless of the owner's wishes. A subject (user or process) can only access an object (file or resource) if its security clearance is equal to or higher than the object's security label.
- **Focus:** Maintaining data confidentiality and integrity in environments with strict security requirements, such as government agencies or military installations.
- **Example:** A user with a "Secret" clearance cannot access a file labeled "Top Secret," even if they have been granted explicit permission by the file owner.

#### **Discretionary Access Control (DAC):**

- **Definition:** DAC grants the owner of a resource the ability to control who can access it and what permissions they have.
- **Enforcement:** Access permissions are set by the owner of the resource, and the system enforces these permissions.
- **Focus:** Flexibility and convenience in managing access to resources within a specific group or organization.



- **Example:** A file owner can grant "Read" access to one user and "Read & Write" access to another user.

#### Comparison and Contrast:

Feature	Mandatory Access Control (MAC)	Discretionary Access Control (DAC)
<b>Control Mechanism</b>	Based on security labels and clearance levels	Based on owner's discretion and permissions
<b>Enforcement</b>	System enforced, regardless of owner	Enforced by the system based on owner's settings
<b>Flexibility</b>	Less flexible, strict rules	More flexible, allows for fine-grained control
<b>Complexity</b>	More complex to implement and manage	Relatively simpler to implement and manage
<b>Suitable for</b>	Environments with strict security requirements (e.g., military)	General-purpose environments with less stringent security requirements

**Q4. Write the step-by-step procedure to create a group named "MCS022". Now add a user "SOCIS" in Windows 2000 operating system. Assume user "SOCIS" is already a member of the guest account in your system. Also explain the basic purpose of enabling the offline features in Windows 2000 operating system. (10 Marks)**

#### **Solution:**

#### **Creating a Group and Adding a User in Windows 2000**

Following are the step-by-step procedures to create a group named "MCS022" and add the user "SOCIS" to it:

#### **Step 1: Creating the Group "MCS022"**

1. **Open the "Users and Computers" snap-in:** Go to Start > Programs > Administrative Tools > Users and Computers.
2. **Navigate to the desired domain or computer:** In the left pane, expand the domain or computer where my group is to be created.
3. **Right-click on the "Groups" folder:** This will open a context menu.
4. **Select "New Group":** This will launch the "New Object - Group" wizard.
5. **Enter the group name:** In the "Group name" field, type "MCS022".
6. **Choose the group scope:** Select "Global" or "Local" depending on the desired scope of the group.
7. **Click "OK":** This will create the new group named "MCS022".

#### **Step 2: Adding User "SOCIS" to Group "MCS022"**

1. **Locate the "MCS022" group:** In the left pane of "Users and Computers", expand the "Groups" folder and find the "MCS022" group.
2. **Right-click on "MCS022":** A context menu will appear.
3. **Select "Properties":** This will open the "MCS022 Properties" dialog box.
4. **Navigate to the "Members" tab:** This tab lists the current members of the group.
5. **Click "Add":** This will launch the "Select Users, Computers, or Groups" dialog box.
6. **Enter the user name "SOCIS":** Type "SOCIS" in the "Enter the object names to select" field.
7. **Click "Check Names":** This will verify the user name.
8. **Click "OK":** This will add "SOCIS" to the "MCS022" group.
9. **Click "OK" again:** This will close the "MCS022 Properties" dialog box.

**Note:** Since "SOCIS" is already a member of the "Guest" group, this step will add "SOCIS" to the "MCS022" group in addition to the "Guest" group.

#### **Enabling Offline Features in Windows 2000:**

Offline features in Windows 2000 enable users to work with files and resources even when they are not connected to the network. The basic purpose of enabling these features is to:

- **Improved Productivity:** Users can continue their work even when disconnected, which is particularly beneficial for mobile users or in environments with intermittent connectivity.
- **Enhanced Collaboration:** Users can work on shared documents and resources offline, and then synchronize their changes when they reconnect to the network.
- **Data Availability:** Offline files and folders remain accessible even when the server or network is unavailable.
- **Reduced Network Traffic:** Offline files reduce the need for constant network access, which can conserve bandwidth and improve network performance.

Enabling offline features requires the use of features like Offline Folders and Offline Files in Windows 2000. These features allow users to create copies of network files and folders on their local machines, providing access to those files when disconnected.

---

**Q5. Answer the following questions related to Linux commands: (10 Marks)**

- Show the users logged in on the network.**
- List the files having more than one digit in the name.**
- Tell the system to run the process continuously even if the user logs out.**
- To allow a user to communicate with another user, logged in by splitting the screen and providing two-way communication.**
- To kill a process after one hour.**

**Solution:**

Let me address the questions related to specific functionalities within Linux:

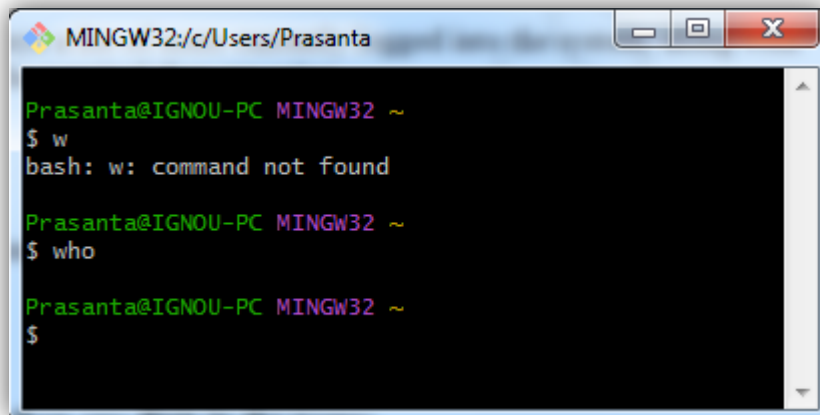
**(i) Show the users logged in on the network:**

The command `w` (or `who`) displays a list of users currently logged into the system, along with their login time, idle time, and the terminal they are using.

w

Alternatively, who provides a simpler output with the username, terminal, and login time.

who

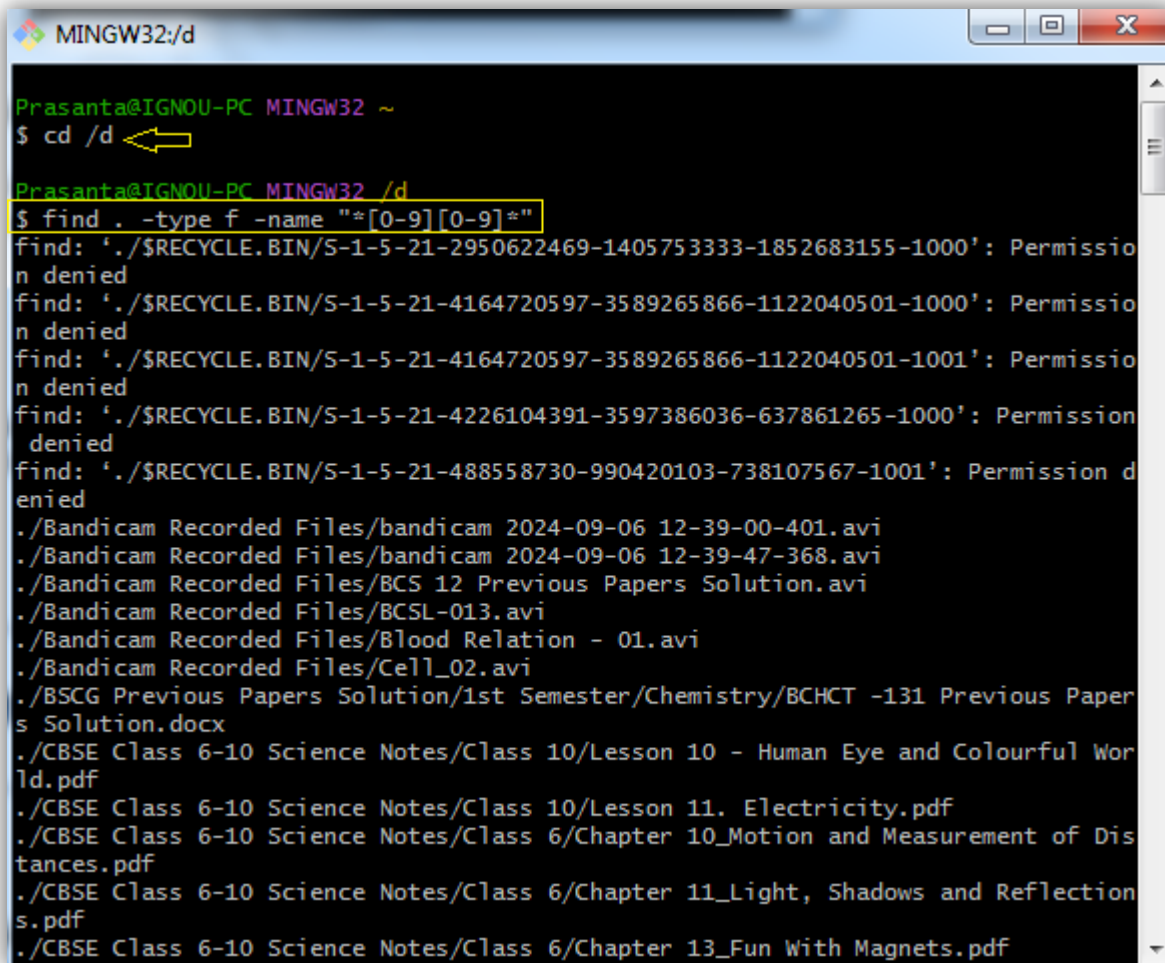
A screenshot of a MINGW32 terminal window. The title bar shows 'MINGW32:/c/Users/Prasanta'. The terminal content shows the user 'Prasanta@IGNOU-PC' in a 'MINGW32 ~' environment. The first command entered is '\$ w', which results in the error 'bash: w: command not found'. The second command entered is '\$ who', which results in no output, leaving the prompt '\$' on the next line.

```
Prasanta@IGNOU-PC MINGW32 ~  
$ w  
bash: w: command not found  
  
Prasanta@IGNOU-PC MINGW32 ~  
$ who  
  
Prasanta@IGNOU-PC MINGW32 ~  
$
```

**(ii) List the files having more than one digit in the name:**

This task can be accomplished using the find command with a regular expression to match filenames containing at least two digits.

```
find . -type f -name "[0-9][0-9]*"
```



```
MINGW32:/d

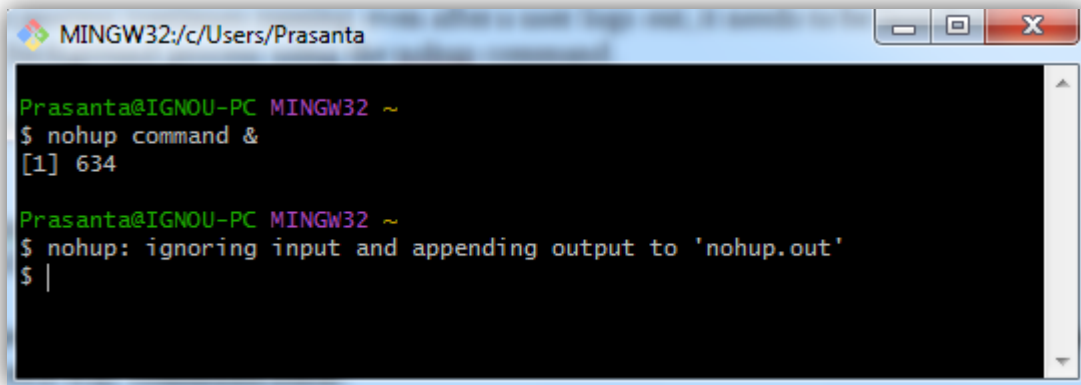
Prasanta@IGNOU-PC MINGW32 ~
$ cd /d
Prasanta@IGNOU-PC MINGW32 /d
$ find . -type f -name "[0-9][0-9]*"
find: './$RECYCLE.BIN/S-1-5-21-2950622469-1405753333-1852683155-1000': Permission denied
find: './$RECYCLE.BIN/S-1-5-21-4164720597-3589265866-1122040501-1000': Permission denied
find: './$RECYCLE.BIN/S-1-5-21-4164720597-3589265866-1122040501-1001': Permission denied
find: './$RECYCLE.BIN/S-1-5-21-4226104391-3597386036-637861265-1000': Permission denied
find: './$RECYCLE.BIN/S-1-5-21-488558730-990420103-738107567-1001': Permission denied
./Bandicam Recorded Files/bandicam 2024-09-06 12-39-00-401.avi
./Bandicam Recorded Files/bandicam 2024-09-06 12-39-47-368.avi
./Bandicam Recorded Files/BCS 12 Previous Papers Solution.avi
./Bandicam Recorded Files/BCSL-013.avi
./Bandicam Recorded Files/Blood Relation - 01.avi
./Bandicam Recorded Files/Cell_02.avi
./BSCG Previous Papers Solution/1st Semester/Chemistry/BCHCT -131 Previous Papers Solution.docx
./CBSE Class 6-10 Science Notes/Class 10/Lesson 10 - Human Eye and Colourful World.pdf
./CBSE Class 6-10 Science Notes/Class 10/Lesson 11. Electricity.pdf
./CBSE Class 6-10 Science Notes/Class 6/Chapter 10_Motion and Measurement of Distances.pdf
./CBSE Class 6-10 Science Notes/Class 6/Chapter 11_Light, Shadows and Reflections.pdf
./CBSE Class 6-10 Science Notes/Class 6/Chapter 13_Fun With Magnets.pdf
```

This command searches for files ( `-type f` ) within the current directory ( `.` ) whose names contain at least two digits ( `*[0-9][0-9]*` ).

**(iii) Tell the system to run the process continuously even if the user logs out:**

To ensure a process continues running even after a user logs out, it needs to be launched as a daemon or background process using the `nohup` command.

`nohup command &`

A screenshot of a MINGW32 terminal window. The title bar shows the path 'MINGW32:/c/Users/Prasanta'. The terminal content shows a user prompt 'Prasanta@IGNOU-PC MINGW32 ~' followed by the command '\$ nohup command &'. The output shows '[1] 634' on the next line. The user then enters '\$ nohup: ignoring input and appending output to 'nohup.out'' and the prompt '\$ |' appears on the next line.

```
MINGW32:/c/Users/Prasanta

Prasanta@IGNOU-PC MINGW32 ~
$ nohup command &
[1] 634

Prasanta@IGNOU-PC MINGW32 ~
$ nohup: ignoring input and appending output to 'nohup.out'
$ |
```

Where command is the process to be executed. The & symbol sends the process to the background, and nohup ensures that the process won't be terminated when the user logs out.

**(iv) To allow a user to communicate with another user, logged in by splitting the screen and providing two-way communication:**

The screen command can be used to create multiple sessions within a single terminal, allowing users to communicate and interact in separate windows. However, for direct two-way communication, a tool like xterm or gnome-terminal combined with screen can be employed.

Here's a basic example:

- User1: Launches a screen session and starts a chat program (e.g., xchat or irssi).
- User2: Attaches to User1's screen session.
- They can use the chat program within the shared screen environment for communication.

Alternatively, tools like tmux provide better flexibility in managing multiple sessions and panes for efficient communication.

**(v) To kill a process after one hour:**

To terminate a process after a specified time (one hour in this case), we can use a combination of sleep and kill commands.

```
sleep 3600; kill -9 <process_id>
```

This command waits for one hour (3600 seconds) and then sends a kill signal ( -9 ) to the process with the provided process\_id. This method is simple but may not be the most graceful way to terminate a process. Alternatively, using a process management tool like systemd or cron can provide more sophisticated scheduling and process management features.

---

**Q6. (a) List and describe the various security features in Windows 2000 operating system. (5 Marks)**

**Solution:**

### **Security Features in Windows 2000**

Windows 2000 incorporates a variety of mechanisms to protect system resources and data from unauthorized access. Here are some of the key security features:

#### **1. User Accounts and Groups:**

- **Description:** Windows 2000 utilizes user accounts and groups to manage access to resources. Each user has a unique account with specific permissions, and these users can be organized into groups to simplify access control management.
- **Purpose:** This feature helps restrict access to sensitive data and resources based on user roles and responsibilities.

#### **2. Access Control Lists (ACLs):**

- **Description:** ACLs are used to define specific permissions for users and groups on objects like files, folders, and registry keys. These permissions specify whether a user can read, write, execute, or modify the object.
- **Purpose:** This provides fine-grained control over access to resources, ensuring that only authorized users can perform specific actions.

### 3. Audit Policies:

- **Description:** Audit policies allow system administrators to track and log various security-related events, such as logon attempts, file access, and system changes.
- **Purpose:** These logs provide valuable insights into system activity and can be used to identify potential security breaches or suspicious behavior.

### 4. Security Policies:

- **Description:** Security policies define various system-wide security settings, such as password complexity requirements, account lockout policies, and network security settings.
- **Purpose:** These policies ensure consistent security practices across the network and help mitigate risks associated with unauthorized access and malicious activity.

### 5. Kerberos Authentication:

- **Description:** Kerberos is a network authentication protocol that provides strong authentication for users accessing network resources.
- **Purpose:** This eliminates the need for users to repeatedly provide their credentials for each resource access, enhancing security and simplifying the login process.

### 6. Internet Connection Firewall (ICF):

- **Description:** ICF is a built-in firewall that monitors and controls network traffic entering and leaving the computer. It can block unauthorized access to the system and restrict access to specific network resources.
- **Purpose:** This helps protect the system from external threats and malicious activities originating from the internet.

### 7. Certificate Services:

- **Description:** This feature allows the system to issue and manage digital certificates, which can be used for authentication and encryption.
- **Purpose:** Digital certificates enhance security by verifying the identity of users and computers, ensuring secure communication and data exchange.



---

**Q6. (b) What is Virtual Memory? Explain the abstract model of virtual to physical address mapping with reference to Linux operating system. (5 Marks)**

**Solution:**

### **Virtual Memory in Linux**

It is a crucial technique that allows an operating system to extend the address space available to a process beyond the physical memory capacity of the system.

### **What is Virtual Memory?**

Virtual memory is a memory management technique that uses a combination of RAM and disk storage to provide a larger address space to processes than the physical RAM available. It creates an illusion of a larger memory space than physically exists.

### **How it Works:**

1. **Logical Address Space:** Each process has its own logical address space, which is a range of addresses it can access. This address space is independent of the physical memory addresses.
2. **Physical Address Space:** The actual physical memory of the system forms the physical address space.
3. **Page Table:** A critical component is the page table, which maps logical addresses to physical addresses. Each entry in the page table corresponds to a page of the process's logical address space and holds the corresponding physical frame address in memory.
4. **Paging:** When a process accesses a logical address, the MMU (Memory Management Unit) uses the page table to translate it into a physical address. If the required page is not in physical memory, a page fault occurs.
5. **Swapping:** The OS handles the page fault by bringing the required page from the disk into a free frame in physical memory. This process of swapping pages between memory and disk is managed by the operating system.

## Abstract Model of Virtual to Physical Address Mapping in Linux:

Linux uses a multi-level page table structure for mapping virtual addresses to physical addresses. The process involves the following:

1. **Virtual Address:** A process generates a virtual address, which is split into various fields.
2. **Page Table Entry (PTE):** The virtual address is used to index the page table entries. These entries contain information about the corresponding physical frame and other attributes (e.g., valid/invalid, permissions).
3. **Physical Address:** The PTE provides the base physical address of the frame in memory.
4. **Offset:** The virtual address's offset field is combined with the base physical address to form the final physical address used by the MMU to access the data.

### Example:

Consider a 32-bit Linux system with a 4KB page size. A virtual address might be split into a 20-bit page number and a 12-bit offset.

- The page number is used to index the page table entries.
- The corresponding PTE contains the physical frame address.
- The 12-bit offset is combined with the physical frame address to produce the final physical address.

### Significance:

Virtual memory in Linux offers several advantages:

- **Larger address space:** Processes can access more memory than physically available.
  - **Memory sharing:** Multiple processes can share the same physical memory pages.
  - **Protection:** Memory protection is enforced through the page table and permissions.
  - **Efficient resource utilization:** Memory can be allocated and deallocated dynamically.
-

**Q7. Write a Linux shell script for automatic grouping of files given in a directory. All files will be grouped on the basis of their size and will be saved into the newly created folders based on file size groups given below: Files will be grouped into 0 to 5 kB, 5 kB to 5 MB, 5 MB to 1 GB and greater than 1 GB. (10 Marks)**

**Solution:**

```
#!/bin/bash

# Script to group files based on size into different directories

# Define size groups in bytes
size_o_5kb=5120
size_5kb_5mb=$((5 * 1024 * 1024))
size_5mb_1gb=$((1 * 1024 * 1024 * 1024))

# Check if the directories for each group exist, create them if not
mkdir -p "0-5KB" "5KB-5MB" "5MB-1GB" "1GB+"

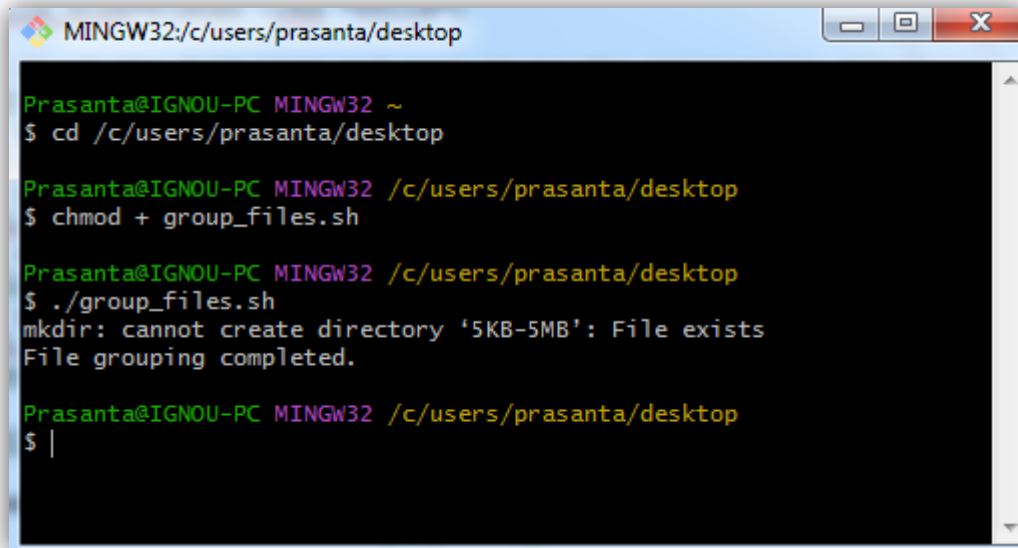
# Loop through all files in the current directory
for file in *; do
    # Get file size in bytes
    file_size=$(stat -c%s "$file")

    # Check the file size and move it to the appropriate directory
    if [ "$file_size" -le "$size_o_5kb" ]; then
        mv "$file" "0-5KB"
    elif [ "$file_size" -le "$size_5kb_5mb" ]; then
        mv "$file" "5KB-5MB"
    elif [ "$file_size" -le "$size_5mb_1gb" ]; then
        mv "$file" "5MB-1GB"
    else
        mv "$file" "1GB+"
    fi
done

echo "File grouping completed."
```

**Screenshot:**

---



```
MINGW32:/c/users/prasanta/desktop

Prasanta@IGNOU-PC MINGW32 ~
$ cd /c/users/prasanta/desktop

Prasanta@IGNOU-PC MINGW32 /c/users/prasanta/desktop
$ chmod + group_files.sh

Prasanta@IGNOU-PC MINGW32 /c/users/prasanta/desktop
$ ./group_files.sh
mkdir: cannot create directory '5KB-5MB': File exists
File grouping completed.

Prasanta@IGNOU-PC MINGW32 /c/users/prasanta/desktop
$ |
```

---

**Q8. Write short notes on the following: (10 Marks)**

- (a) LAN Topologies
- (b) Token Ring
- (c) Network Monitoring Tools
- (d) Firewall
- (e) Active Directory in Windows 2000

**Solution:**

#### **Short Notes on Networking Concepts**

##### **(a) LAN Topologies**

A LAN (Local Area Network) topology defines the physical and logical arrangement of devices and connections within a network. My understanding is that different topologies influence network performance, reliability, and cost. Common LAN topologies include:

- **Bus Topology:** All devices are connected to a single cable (the bus). Simple and inexpensive, but a single cable failure can bring down the whole network.
- **Star Topology:** All devices are connected to a central hub or switch. Easy to manage, fault-tolerant, and scalable, making it a popular choice.
- **Ring Topology:** Devices are connected in a circular fashion, with data flowing in one direction. Good for equal access to resources, but a single failure can impact the entire ring.
- **Mesh Topology:** Every device is connected to every other device. Highly reliable due to redundancy, but complex and expensive to implement.
- **Tree Topology:** Hierarchical structure resembling a tree, with a root node branching out to other nodes. Combines features of bus and star topologies, good for larger networks.

#### (b) Token Ring

Token Ring is a network topology where data is transmitted in a circular fashion, with a special frame called a "token" circulating through the network. My understanding is that only the device holding the token is allowed to transmit data.

- **Mechanism:** When a device needs to transmit, it waits for the token, attaches its data to it, sends it around the ring, and then releases the token.
- **Advantages:** Controlled access prevents collisions, provides deterministic performance, and is well-suited for real-time applications.
- **Disadvantages:** Performance degrades as the network grows, susceptible to single points of failure if a device fails, and less popular compared to Ethernet.

#### (c) Network Monitoring Tools

Network monitoring tools are essential for ensuring network performance, security, and troubleshooting. My understanding is that these tools help me collect data on network traffic, device availability, and potential issues. Examples include:

- **SNMP (Simple Network Management Protocol):** Enables monitoring of network devices through a centralized management system.

- **Wireshark:** A protocol analyzer that captures and analyzes network traffic, helping identify bottlenecks and security threats.
- **Nagios/Icinga:** Tools for monitoring network devices, services, and applications, alerting administrators to potential problems.
- **SolarWinds Network Performance Monitor:** Comprehensive tool for monitoring network performance, bandwidth utilization, and device health.
- **PRTG Network Monitor:** Another comprehensive tool that offers a user-friendly interface and a wide range of monitoring capabilities.

#### (d) Firewall

A firewall is a security system that controls network traffic entering and leaving a network or device. My understanding is that firewalls act as a barrier between a trusted internal network and an untrusted external network.

- **Function:** It examines network traffic based on pre-defined rules and blocks or allows traffic accordingly.
- **Types:** Hardware firewalls (dedicated devices) and software firewalls (programs running on a computer).
- **Benefits:** Protects against unauthorized access, malicious software, and network intrusions. Helps enforce security policies and manage network access.

#### (e) Active Directory in Windows 2000

Active Directory (AD) in Windows 2000 is a directory service that manages network resources and users within a Windows domain. My understanding is that it provides a centralized location for storing and managing user accounts, computers, and other network objects.

- **Key Features:**
  - **Centralized User Management:** Stores user accounts and their permissions, allowing administrators to manage access to resources efficiently.
  - **Group Policy Management:** Enables administrators to define and enforce security policies across the network.

- **Domain Controller:** AD relies on domain controllers that store and replicate directory data.
  - **Authentication:** Verifies user identities and controls access to resources.
- **Importance:** Provides a more structured and manageable way to administer network resources and security, especially within larger organizations.

learningscience.co.in