Introduction

> **System Administration** → The management and maintenance of computer systems.
> **Network Administration** → The management and upkeep of computer networks.

- Installing, configuring, and maintaining servers and networks.
- Ensuring system security and data integrity.
- Monitoring and optimizing performance.
- Troubleshooting issues and implementing solutions.

Roles and Responsibilities

- **System Administrator:**
  - User account management
  - System updates and patches
  - Backup and disaster recovery planning
- **Network Administrator:**
  - Network configuration → IP addressing, routing
  - Managing network services → DNS, DHCP
  - Monitoring and optimizing network performance and security
- **Shared Responsibilities:**
  - Security management → Firewalls, VPNs
  - Documentation and policy implementation
  - Ensuring system and network availability

Components of a Computer System:

- *Hardware* → Physical components (CPU, memory, storage)
- *Software* → Operating systems, applications, drivers
- *Firmware* → Embedded software controlling hardware
- *Networking* Components → Network Interface Cards (NICs), routers, switches

Networking

A collection of computers and devices connected to share resources and information.

Network Types:

- *LAN* (Local Area Network): Small geographical area
- *WAN* (Wide Area Network): Larger geographical area
- *MAN* (Metropolitan Area Network): Covers a city or campus

Network Topologies:

- *Bus*
- *Star*
- *Ring*
- *Mesh*

Networking Protocols

1. **TCP** (Transmission Control Protocol)
2. **UDP** (User Datagram Protocol)
3. **IP** (Internet Protocol)
4. **DNS** (Domain Name System) → Resolves human-readable domain names to IP addresses.
5. **DHCP** (Dynamic Host Configuration Protocol) → Automatically assigns IP addresses to devices on a network.

Policies

Policies are rules or guidelines to allow/deny access. Policies can be implemented on a Systems Level or on a Network Level (both kinds of policies having separate catalogues).

- *Inbound Policies* → Controls traffic coming into the network.
- *Outbound Policies* → Controls traffic leaving the network.

Documentation

It is the act of writing down information in a formal format. Documentation is essential for maintaining continuity, aiding in troubleshooting, and providing records for compliance and auditing. It should include information on network layouts and configurations, system settings, user accounts, security policies, and backup schedules.

Planning

Planning is the foundation for successful system and network administration. It involves several steps:

1. *Assessment*: It's important to understand the current state of your systems and networks before making any changes.
2. *Goal Setting*: Define clear objectives for what you want to achieve, such as improved security, enhanced performance, or increased scalability.
3. *Budgeting*: Allocate resources effectively to support the plan.
4. *Timeline*: Create a realistic schedule with milestones and deadlines.

But it has issues like how do we balance security with usability? or how do we provide high availability with disaster recovery? and how do we keep up with technology updates.

Operating System

> A program that controls the execution of application programs. It is an interface between applications and hardware and makes a computer more convenient, more efficient and able to evolve.

An OS provides many many services like

- Program development (Editors and debuggers) and Program execution.
- Access to I/O devices, System and Files.
- Error detection and response for internal and external hardware and software errors.

Accounting → Collect usage statistics, monitor performance, used to anticipate future enhancements and for billing purposes.

A computer system has

- **4** Layers → Applications, Utilities, Operating System, Hardware.
- **5** Resources → Processor, Memory, Storage Disk, Network, I/O Devices.

Kernel

It is the portion of the operating system that is in the main memory and contains the most frequently used functions. It is the first program that is loaded in the memory, in **kernel mode**. It has 4 main functions of "managing" *processes*, *memory*, *devices* and *files*.

> OS Kernel also enforces security policies and protects the system from unauthorized access.

Processes

It is an instance of a program running on a computer. It is the the entity that can be assigned to and executed on a "processor". Also called, a unit of activity characterized by a single sequential thread of execution, a current state, and an associated set of system resources.

Components of a Process → An executable program, Data needed by the program and Execution context of the program.

Design Considerations

- **Improper synchronization:** Ensure a process waiting for an I/O device receives the signal
- **Nondeterminate program operation:** Program should only depend on input to it, not on the activities of other programs
- **Deadlocks**

Memory Management

- **Features:**
  - Process isolation
  - Automatic allocation and management
  - Support of modular programming
  - Protection and access control
  - Long-term storage
- **Issues:**
  - Not enough Memory
  - Memory Fragmentation
  - Security Crash

Virtual Memory

Allows programmers to address memory from a logical point of view.

- **Benefits:** Eliminates the hiatus between the execution of successive processes while one process was written out to secondary store and the successor process was read in
- **Relationship to File System:**
  - Implements long-term store
  - Information stored in named objects called files

Paging → Paging is a memory management technique used by OS to store and retrieve data between main memory (RAM) and secondary storage (disk). Memory is divided into fixed-size blocks called pages and those pages are mapped to parts of the physical memory, creating an illusion of more memory than there is.

A **MMU** (Memory Management Unit) handles the translation of virtual addresses (used by applications) into physical addresses (used by the hardware to access actual memory).

More Complex Fragmentation ⇒ More Complex Mapping

Information Protection and Security

- **Availability:** Concerned with protecting the system against interruption
- **Confidentiality:** Assuring that users cannot read data for which access is unauthorized
- **Data integrity:** Protection of data from unauthorized modification
- **Authenticity:** Concerned with the proper verification of the identity of users and the validity of messages or data

Scheduling and Resource Management Goals

- **Fairness:** Give equal and fair access to resources
- **Differential responsiveness:** Discriminate among different classes of jobs
- **Efficiency:** Maximize throughput, minimize response time, and accommodate as many uses as possible

System Structure

- View the system as a series of levels
- Each level performs a related subset of functions
- Each level relies on the next lower level to perform more primitive functions
- This decomposes a problem into several more manageable

Process Hardware Levels

- **Level 1** → *Electronic Circuits*
- **Level 2** → *Processor's Instruction Set*
- **Level 3** → *Procedure*s
- **Level 4** → *Interrupts*

Concepts with Multiprogramming

- **Level 5** → *Processes*
- **Level 6** → *Secondary Storage Devices*
- **Level 7** → *Logical Address Space*

Deal with External Objects

- **Level 8** → *Interprocess Communication*
- **Level 9** → *File System*
- **Level 10** → *External Device Interfaces*

- **Level 11** → *External-Internal Identifier Mapping*
- **Level 12** → *Process Support Facilities*
- **Level 13** → *User Interface*: For the operating system.

UNIX is a powerful, multiuser, multitasking operating system. It uses a Layered Architecture where the layers are "Hardware", "Kernel", "System Call Interface", "Commands and Libraries". Each layer surrounds the one before it.

It comes with a number of user services and interfaces: Shell, Components of the C compiler etc.

Multithreading

Process is divided into threads that can run concurrently.

- **Thread:** Dispatchable unit of work - executes sequentially and is interruptable

Symmetric Multiprocessing (SMP): There are multiple processors which share the same main memory and I/O facilities, and can perform the same functions.

Kernel-Mode Components

1. **Executive** → Contains base operating system services: Memory management, Process and Thread management, Security, I/O and Interprocess communication.
2. **Kernel** → Consists of the most used
3. **HAL** (Hardware abstraction layer) → Isolates the operating system from platform-specific hardware differences.
4. **Device drivers** → Translate user I/O function calls into specific hardware device I/O requests
5. **Windowing and graphics systems** → Implements the graphical user

User-Mode Processes

- Special system support processes - Ex: logon process and the session manager
- Service processes
- Environment subsystems
- User applications

Client/Server Model → Provides a uniform means for applications to communicate via LPC (Local Procedure Calls).

File Systems

A file system is a method to manage and organize data in the form of files and directories (folders). These are the most common ones:

- Windows - **NTFS** (New Technology File System) → *Default file system on Windows*. It supports large files and partitions, file compression, encryption, disk quotas, and advanced permissions.
- Windows - **FAT32** (File Allocation Table 32) → It is widely compatible across many devices and operating systems, making it a common choice for external drives and USB sticks. However, it has significant limitations, such as a maximum file size of *4GB* and a partition limit of *8TB*, making it unsuitable for modern large storage needs.
- Linux - **ext4** (Fourth Extended File System) → *Default file system for many Linux*. It is an improvement over its predecessor, ext3, offering better performance, larger volume support, and enhanced journaling features.
- macOS - **APFS** (Apple File System) → *Default file system for macOS, iOS, and other Apple devices*. APFS is optimized for flash and SSD storage, offering fast file access, cloning, snapshots, and strong encryption.

Partitioning → Process of dividing a physical storage device, such as a hard drive or SSD, into separate sections called *partitions*.

- *Primary Partition* → A bootable partition where an operating system can be installed. Limit=4.
- *Extended Partition* → Since, only 4 primary are allowed on a drive, an extended partition acts as a container to hold additional partitions. Limit=1.
- *Logical Partition* → Resides inside the extended partition and can be used to store data, files, or additional operating systems. No Limit.

🛠️ Tools → Disk Management (Windows), GParted (Linux), Disk Utility (macOS)

? What is Distributed Computing?

It refers to a model where tasks are divided across multiple computers that work together to solve a problem or complete a process. These computers are connected over a network and they divide the workload and processing tasks in parallel, resulting in faster execution and scalability.

? Why is FAT32 still used?

Because of its wide compatibility and simplicity.

Why is UNIX so powerful?

Because of its simple, modular, flexible, and robust design.

System Maintenance

System maintenance involves a set of activities aimed at ensuring the smooth and efficient operation of computer systems, networks, and applications. These activities are carried out to prevent system failures, enhance performance, and prolong the lifespan of hardware and software.

It is important because of *Performance Optimization*, *Security*, *Cost-Effectiveness* and *Compliance*.

Key Tools and Techniques in System Maintenance:

- *Monitoring Tools*: Used to continuously monitor system performance and detect anomalies. Examples: Nagios, Zabbix, or SolarWinds.
- *Backup and Recovery*: Regular backups and disaster recovery plans ensure that data can be restored in case of system failure or data loss.
- *Documentation*: Keeping accurate records of maintenance schedules, system configurations, and any changes made to the system helps in troubleshooting and future upgrades.

Types of System Maintenance

1. **Preventive Maintenance** → Prevent problems before they occur.
2. **Corrective Maintenance** → Fix issues when they arise.
3. **Adaptive Maintenance** → Modify systems to cope with changing environments or requirements.
4. **Perfective Maintenance** → Improve performance or functionality.
5. **Emergency Maintenance** → Address unforeseen critical issues.

Routine System Maintenance Tasks

1. Updates and Patch Management

1. **Updates** → Larger software packages that introduce new features, enhancements, or significant changes to existing functionality.
2. **Patches** → Smaller software packages designed to address specific vulnerabilities, bugs, or security flaws in existing software.

🛠️ Tools → Windows Update (Windows), Synaptic/apt-get (Linux), Software Update (macOS)

2. Disk Cleanup and Defragmentation

1. **Disk Cleanup** → Removing unnecessary files to free up space.
2. **Defragmentation** → Re-organizing data to improve read/write speeds.

🛠️Tools → Disk Cleanup (Windows), fsck and defrag utilities (Linux), Disk Utility (macOS)

3. Backup and Restore Verification

Protects against data loss and Enables disaster recovery.

- *Types of backups:* Full, incremental, differential
- *Verification process:* Test restores to ensure backup integrity, Automated verification tools.

4. User Account Review and Management

Regularly review user accounts → Disable inactive accounts and Update permissions as needed.

Monitoring System Performance

Helps identify bottlenecks and performance issues
Key metrics: CPU usage, memory usage, disk I/O, network throughput

🛠️Tools → Task Manager (Windows), top/htop (Linux), Activity Monitor (macOS), Zabbix

System Logs

System logs record events that occur within a system. These include Application logs, Security logs and System logs.

🛠️Tools → Splunk, , Graylog and the ELK Stack (Elasticsearch, Logstash, Kibana).

User and Group Management

Users

Every person or entity that interacts with a system is identified as a "user." Users have unique IDs and roles, determining what resources they can access.

Types of Users

1. **Root/Administrator:** Has unrestricted access to the entire system.
2. **Standard Users:** Limited access based on assigned permissions.
3. **Service/System Users:** Accounts used by services, applications, and domains for background tasks.

User Account Types

1. **Local Accounts** → Stored on the local system and used for local access only.
2. **Domain Accounts** → Managed by a central server and used across multiple systems in a network.
3. **Service Accounts** → Non-human accounts, Used to run services or applications.

Groups

Groups are collections of users who share similar access permissions or roles. The purpose of groups is to simplify the administration of permissions and policies.

Types of Groups

1. **Local Groups**
2. **Domain Groups**

Permissions

Permissions determine what actions a user or group can perform. Assign permissions to groups to manage access efficiently.

Understanding Permissions and Access Control

Permissions in Linux → Files have three main permissions: Read (r), Write (w), Execute (x). Permissions apply to three categories: Owner, Group, Others.

Permissions in Windows → Files and folders have NTFS permissions which control access (Full Control, Modify, Read & Execute). Managed through Security Tab in

file/folder properties.

It is best to assign permissions to groups rather than individual users and Use the *principle of least privilege*: grant only necessary permissions.

A "Group Policy Misconfiguration" is a much bigger mistake when compared to a "User Account Compromise", as administrators are often suspended and in some cases terminated from the service for this mistake.

Best Practices

1. Regularly audit user and group access rights.
2. Use strong password policies and enforce multi-factor authentication.
3. Monitor and review group memberships, especially for privileged groups.
4. Regularly remove or disable inactive user accounts.

Security and Policy Administration

Authentication → The process of verifying a user's identity. There are 3 main methods of doing this: *Passwords*, *Biometrics*, *2FA* (Two-Factor Authentication)

1. Passwords

Enforce strong password policies to enhance security: Minimum length, complexity requirements; Regular password expiration; Avoid common passwords; Implement external key methods for higher management.

2. Two-Factor Authentication (2FA)

Adds an extra layer of security by requiring two forms of authentication. Methods include SMS codes, authentication apps, and hardware tokens. Example: Google Authenticator.

3. Biometrics

Unique physical characteristics to verify identity like Fingerprints, facial recognition, retina scans. Benefits include higher security and ease of use. Most notably used by higher management and administrators.

Managing User Sessions

Monitor and manage active user sessions for security. Methods include session timeouts, activity monitoring, and manual session termination.

🛠️Tools → Task Manager (Windows), top (Linux), Activity Monitor (macOS).

Security Best Practices

- Implement the principle of least privilege.
- Regularly update and patch systems.
- Educate users about phishing and social engineering.
- Backup data regularly and verify backups.

THE END