DIPLOMA WALLAH

(Your One Stop Hub For Diploma Resources)

OPERATING SYSTEM AND ADMINISTRATION

Complete Notes Based on Full Syllabus

- Diploma Engineering

4th Semester

www.diplomawallah.in

Notes prepared by **Sangam**

Diploma Walah

Sangam

Date
Page

unit - 10

User Authentication

1. User account –

It is a identity created in the OS for a person (or sometimes a process).

- Each user has :-
  - username - login name
  - password - used for authentication.
  - UID (User ID) - a unique number assigned by the OS.
- This allows the OS to know who is using the system and what permission they should have.

Ex. :- Windows :- Administrator, Guest
Linux : root, Student

2. Group Account –

- A group is a collection of users.
- Each group has a UID (Group ID).
- Groups used to assign common permission to multiple users at once.
- This make management easier (instead of giving permissions to each user individually).

Ex –
Linux : admin group, Students group.
Windows : Users, Administrators.

Roles in Authentication

- Authentication — verifying the user identity
- When a user logs in → they enter username + password.
- OS checks the user database (Linux: /etc/passwd, Windows: SAM database).

- If credential match: → authentication successful.

Ex
In a college computer lab.
- Every student has their own user account (e.g. roll no.)
- All students are part of the student group.
- When we log in → system checks our password (authentication)

- After login → we only get permission of the student group (can't access admin settings).

Interface

1. User Interface (UI)
- The way user interacts with the OS.
  two main types :-
  - CLI → user types command.
    GUI → user interacts using icons, windows, and menus.

working
- user gives input (command/mouse click).
- OS interprets it and send it to the right process.
- O/P → (text/graphical) is displayed back to user.

2. Application programming Interface.
- Interface b/w application and OS.
- APIs allow programs to request OS services (e.g. open file, allocate memory, connect to a network).

* Working
- An app calls an API function (e.g. fopen() in C).
- OS translates it into system calls.
- Kernel executes the request and returns result to the application.

3. Hardware Interface (Device driver) keyboard, mouse, NIC, printer.

working :- * Application request an action (e.g. print)
- OS passes request printer driver.
- Driver converts request into hardware-specific instruction
* Device execute the command.

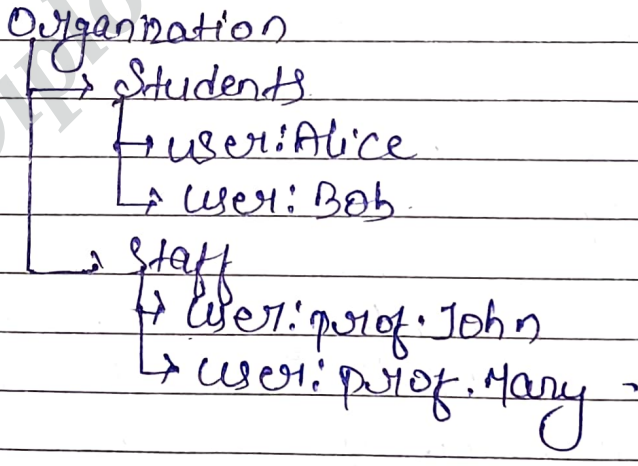
LDAP (Lightweight Directory Access protocol).

It is a protocol used to access and manage directory services, which are special databases optimized for reading and searching (not for frequent updates.)

A directory services stores information in a hierarchical structure (like a tree).
Ex- users, groups, computer, printers, and other resources in an organization.

* Features

1. Hierarchical (Tree like) structure:-
   - Data is organized in levels.



2. Centralized Authentication
   - All username & password are stored in one place.
   - Different apps/services (Email, wifi, ERP, Library system) check credential from this central LDAP server.

3. Lightweight
- It is simpler and faster compared to older directory protocols.

4. Cross-platform
- Works on windows, linux, MacOS etc.

What does LDAP do?
1. Authentication → Validating a username and password.
2. Directory lookup → Searching for users, groups, devices or resources.

* Active Directory in windows based on LDAP.

Ex- Login with LDAP
1. User enters login details → username = sagar, password = 12345.
2. Application sends the request to the LDAP server
3. LDAP Server searches its directory (three databases)
4. If details match → login success, else fail.