**Routes**

1. **Register Route**
   * Endpoint: **POST /api/v1/users/register**
   * Description: Register a new user.
2. **Login Route**
   * Endpoint: **POST /api/v1/users/login**
   * Description: Authenticate a user and provide a session or token.
3. **Logout Route**
   * Endpoint: **POST /api/v1/users/logout**
   * Description: Clear user session or token.
4. **Create Profile**
   * Endpoint: **POST /api/v1/users/createProfile**
   * Description: A mandatory profile completion step post-registration to ensure users provide essential details before accessing core platform functionalities.

**For each of these routes, I'll need a corresponding controller function:**

1. **Register Controller**

* Input: User details (username, password, email, etc.)
* Action: Save the user to the database (hashed password, not plain text).
* Output: Confirmation message (and possibly a login token/session).

1. **Login Controller**

* Input: User credentials (username/email and password).
* Action: Authenticate the user, start a session or provide a token.
* Output: User details and a token or session ID.

1. **Logout Controller**

* Input: Session ID or token.
* Action: Invalidate the session or token.
* Output: Confirmation message.

1. **Create Profile Controller**

* Input: User profile details
* Action:
  + First, verify that the user is authenticated.
  + Check if the user already has a profile created. If one exists, return an error or prompt to update instead.
  + Save the profile details to the database.
* Output:
  + Successful creation message.
  + The created profile details.

**Let’s get started...!**

* **authorizationController.js** will deal primarily with authentication and related concerns (login, logout, JWTs, password resets, etc).
* **userController.js** will handle CRUD operations for users, profile updates, viewing user profiles, etc.

Here’s the structure:

**1. authorizationController.js**

* **Signup**
  + Check if user exists
  + Hash password
  + Create user
  + Return user
* **Login**
  + Check if user exists
  + Check if password matches
  + Generate a JWT
  + Return JWT and user
* **Logout**
  + For JWTs: Handled client-side by removing token. Optionally, maintain a server-side blacklist.
  + For sessions: Clear the user session.
* **Forgot Password**
  + Generate a unique token.
  + Send an email with a link containing that token.
* **Reset Password**
  + Check if token is valid.
  + Hash and update password.
* **Update Password**
  + Check current password.
  + Hash and update to new password.

**2. userController.js**

* **Get User Profile**
  + Return the user's data.
* **Update User Profile**
  + Update the user's details.
* **Delete User**
  + Delete the user from the database.
* **List of Online Users**
  + I can maintain online status in the user model.
* **Other User operations**
  + Any other operations specific to the user entity.

**Dependencies:**

1. **bcryptjs**: For hashing and verifying passwords.
2. **jsonwebtoken (JWT)**: For generating and verifying JSON web tokens.
3. **crypto**: Built-in Node.js package to generate random tokens, for use in features like "forgot password".
4. **nodemailer**: For sending emails (e.g., for password resets).
5. **validator**: For validating emails, passwords, and other input.