Experiment - 1

Aim → Implementation of user-authentication technique for remote access of the network device in computer network using Cisco Packet Tracer.

Objective 1 → An overview on user authentication technique used in secured system.

User authentication is a crucial security mechanism used to verify the identity of users accessing a secured systems. It ensures that only authorised individuals can access sensitive information or services.

i) Knowledge-Based Authentication → Passwords & PINs: Users provide a unique password or Personal Identification Number. Security Questions: Users answer pre-set or dynamically generated security questions.

ii) Possession-Based Authentication → One Time Passwords (OTPs): Sent via SMS, email or authentication apps. Smart Cards & Tokens: Hardware-based authentication like USB security keys.

iii) Biometric Authentication → Fingerprint scanning, Facial recognition, Iris & Retina Scans and Voice recognition.

iv) Multi-Factor Authentication → Combines two or more authentication methods (e.g. password + OTP, fingerprint + PIN).

v) Certificate-Based Authentication → Uses digital certificates (x.509) to authenticate users, commonly used in enterprise environments. SSL/TLS certificates secure web-based communication.

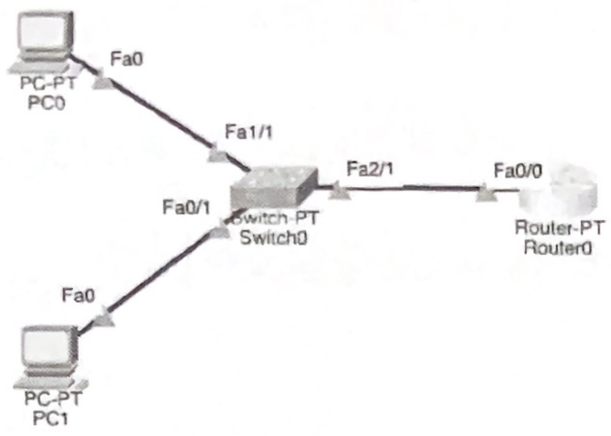
vi) Token-Based Authentication → JSON Web Tokens: Used in web applications for session authentication. SAML (Security Assertion Markup Language): Used for Single-Sign On (SSO) in enterprises.

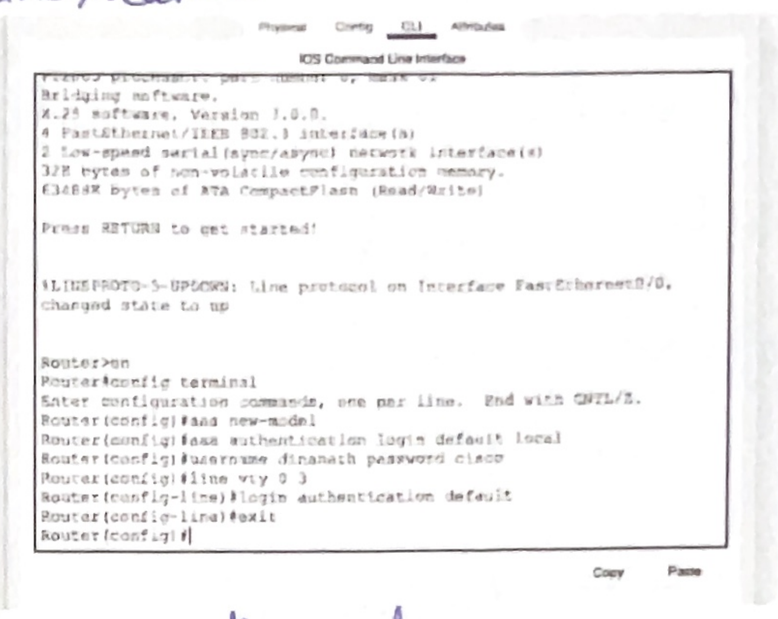
vii) Behavioral Authentication → Monitors user behaviour, such as typing patterns, mouse movements and browsing habits. Uses AI to detect anomalies and prevent unauthorized access.

viii) Zero Trust Authentication → Continous verification of users and devices based on context, location and risk levels. Often involves MFA, identity verification and end-point security checks.

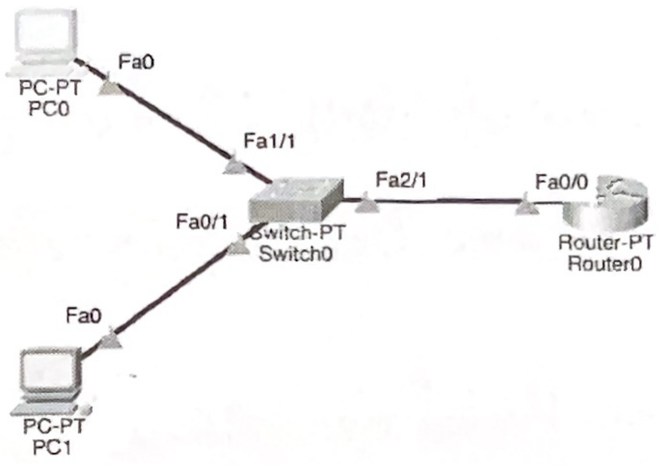
Name: _____ Regd No: _____

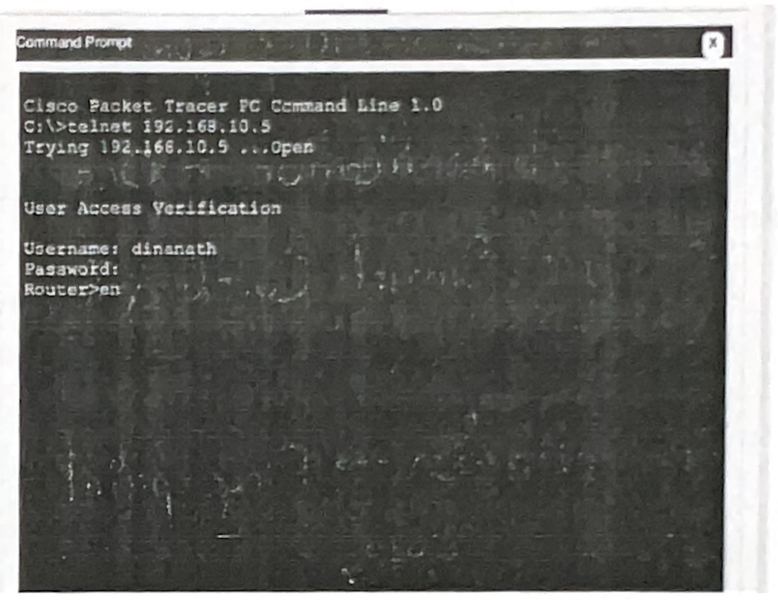
Objective 2 → Configuration and verification of remote user authentication on a Cisco router and switch using username-password authentication.



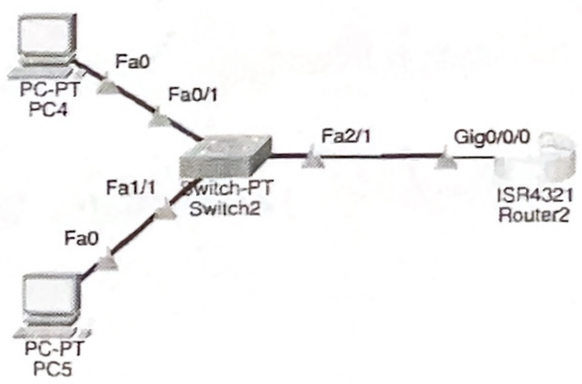


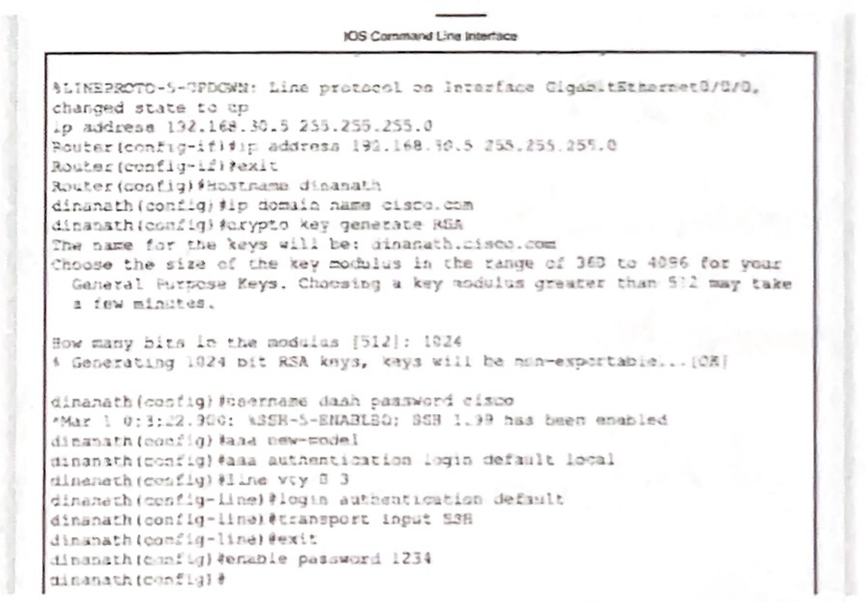
Configuring PCs and routers for remote user authentication and checking the authentication at PC0.



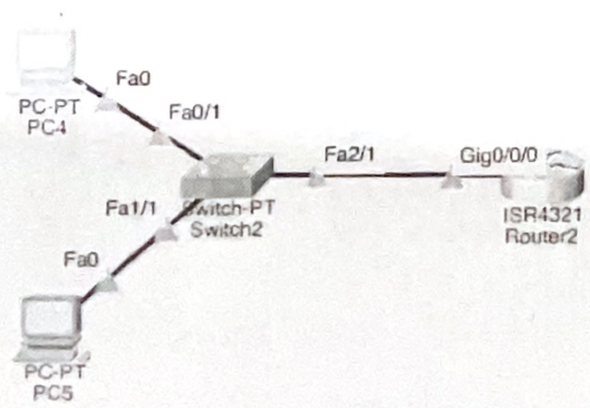


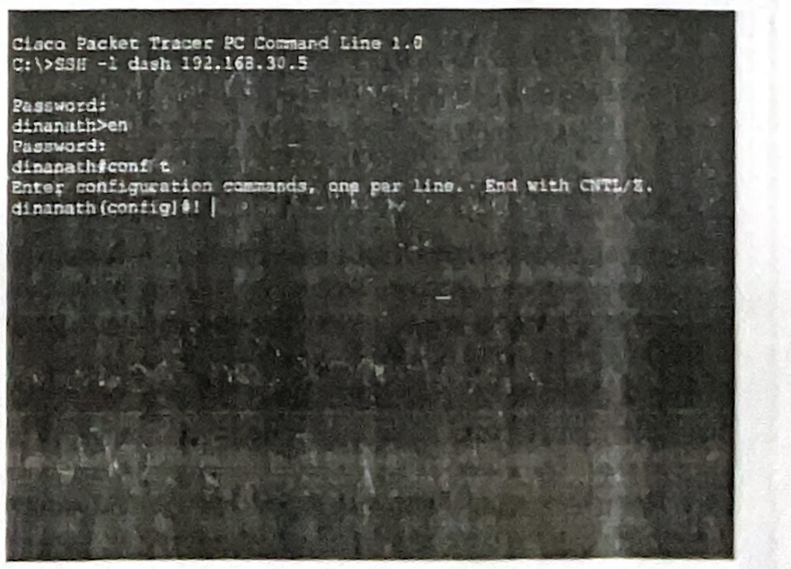
Objective 3 → Configuration and verification of remote user authentication on a Cisco router and switch local username-password authentication using SSH.





Configuring PCs and routers for remote access using SSH and accessing it at PC4.





Name: _____ Regd No: _____

Exercise

Q3) Explain the features of SSH protocol.

Ans → Secure Shell (SSH) is a cryptographic network protocol used to establish a secure connection between a client and a server. It provides encrypted communication over an insecure network, making it a preffered choice for remote system administration, secure file transfers and network device management.

i) Encryption & Security → SSH encrypts data transmission, preventing eavesdropping, man-in-the-middle attacks and unauthorised access.

ii) Authentication Mechanisms → Supports multiple authentication methods, including password based authentication and public key authentication.

iii) Secure Remote Access → Allows users to securely login to remote systems, execute commands, and manage network devices without exposing credentials in plain text.

iv) Port Forwarding → Enables secure tunneling of application data over SSH, often used for secure access to internal network services.

v) File Transfer Support → Provides secure file transfer via : Secure Copy Protocol (SCP) and SSH File Transfer Protocol (SFTP).

vi) Integrity & Data Protection → Uses cryptographic hashing (e.g., SHA-2) to ensure data integrity and prevent tampering.

Q4) Compare and contrast SSH and Telnet.

Ans →

Feature	SSH (Secure Shell)	Telnet
i) Security	Encrypted connection using cryptographic algorithms.	Plaintext communication (no encryption).
ii) Authentication	Supports public-key and password-based authentication.	Only supports password authentication.
iii) Data Integrity	Uses hashing algorithms (e.g. SHA-2) to ensure data integrity.	No integrity protection; data can be intercepted or modified.
iv) Encryption	Encrypts the entire session using protocols like AES, RSA & ECC.	Transmits data in plaintext, making it vulnerable to eavesdropping.
v) Port Used	Runs on port 22 by default	Runs on port 23 by default.
vi) Use cases	Secure remote access, encrypted file transfer	Used only in trusted environments with no security concerns.

1) ~~Exerc~~ State the importance of user authentication in a security system.

Ans → User authentication is essential for maintaining security in any system, ensuring that only authorised users can access sensitive resources.

i) Prevention of Unauthorised Access → Authentication verifies user identity, preventing attackers from gaining unauthorized entry into the system.

ii) Data Protection → Sensitive information, such as personal, financial or confidential business data, remains secure from unauthorised modifications or breaches.

iii) Access Control & User Management → Enables organisations to enforce role-based access restricting permissions based on user roles and responsibilities.

iv) System Integrity → Ensures that only legitmate users can execute criticale operations, preventing malicious activities that could compromise system stability.

v) Protection Against Cyber Threak → Reduces risks associated with cyber threats like phising, brute force attacks and identity theft.

2) What will be the command for the following tasks?

a) to create a local user account with the username "CNSLab" and the password "cisco".

Ans → Router(config)# username CNSLab password cisco

b) to set the priviledge level for the local user account to 15.

Ans → Router(config)# username CNSLab priviledge 15 password cisco

c) to create an encrypted password

Ans → Router(config)# service password-encryption.

Conclusion → User authentication is a critical component in securing network access and preventing unauthorised entry. Implementing authentication techniques ensures that only authorised users can access network devices, protecting sensitive data from potential threats. In this experiment authentication methods were applied using CPT, demonstrating local username-password authentication and secure remote access via SSH.