

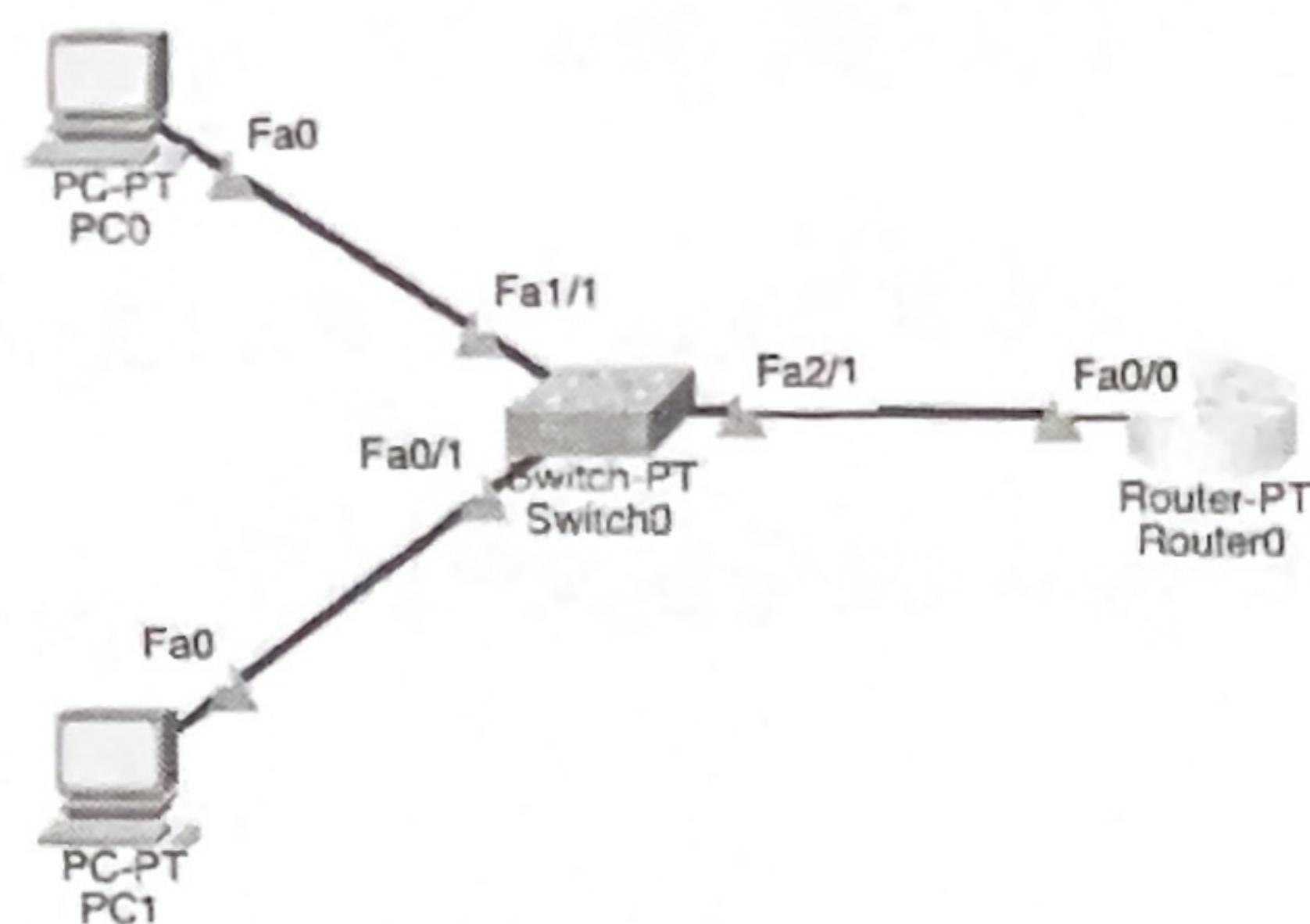
Aim → Implementation of user-authentication technique for remote access of the network device in computer network using Cisco Packet Tracer.

Objective I → 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 system. It ensures that only authorized 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 Scanning and Voice recognition.
- iv) Multi-Factor Authentication → Combines two or more authentication methods (e.g., Password + OTP, Fingerprint + PIN).
- v) Certificate-Based Authentication → Use 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. Use AI to detect anomalies and prevent unauthorized access.
- viii) Zero Trust Authentication → Continuous verification of users and devices based on context, location and risk levels. Often involves MFA, identity verification and end-point security checks.

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



IOS Command Line Interface

```

Cisco IOS Software, paragon1, Version 12.0
Bridging software,
4 FastEthernet/Ethernet S0/0.1 interface(s)
2 Low-speed serial (async/asynch) network interface(s)
32K bytes of non-volatile configuration memory.
634884 bytes of ATA CompactFlash (Read/Write)

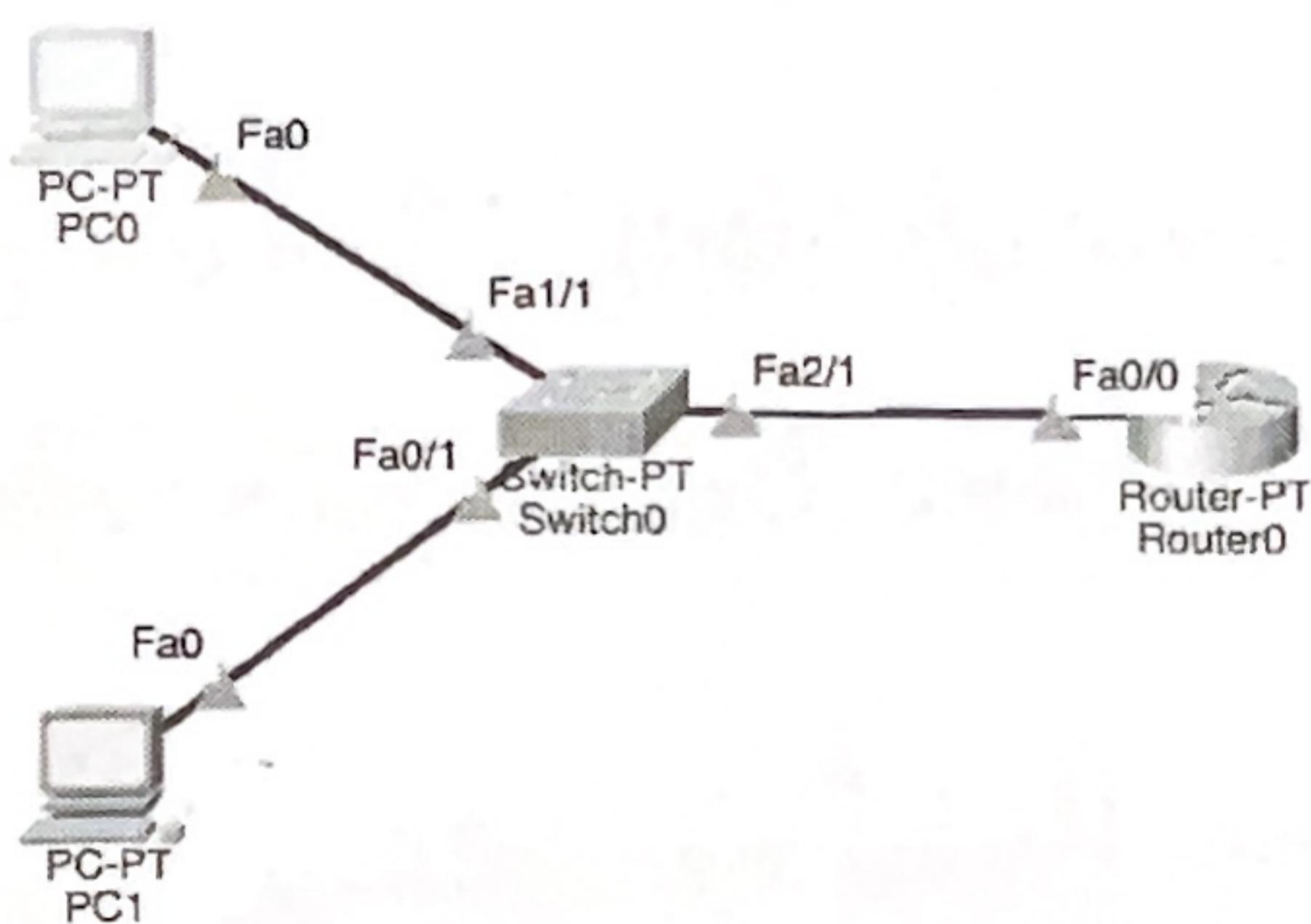
Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on interface FastEthernet0/0, changed state to up

Router>en
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#aaa new-model
Router(config)#aaa authentication login default local
Router(config)#username dinanath password cisco
Router(config)#line vty 0 3
Router(config-line)#login authentication default
Router(config-line)#exit
Router(config)#
  
```

Copy Paste

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

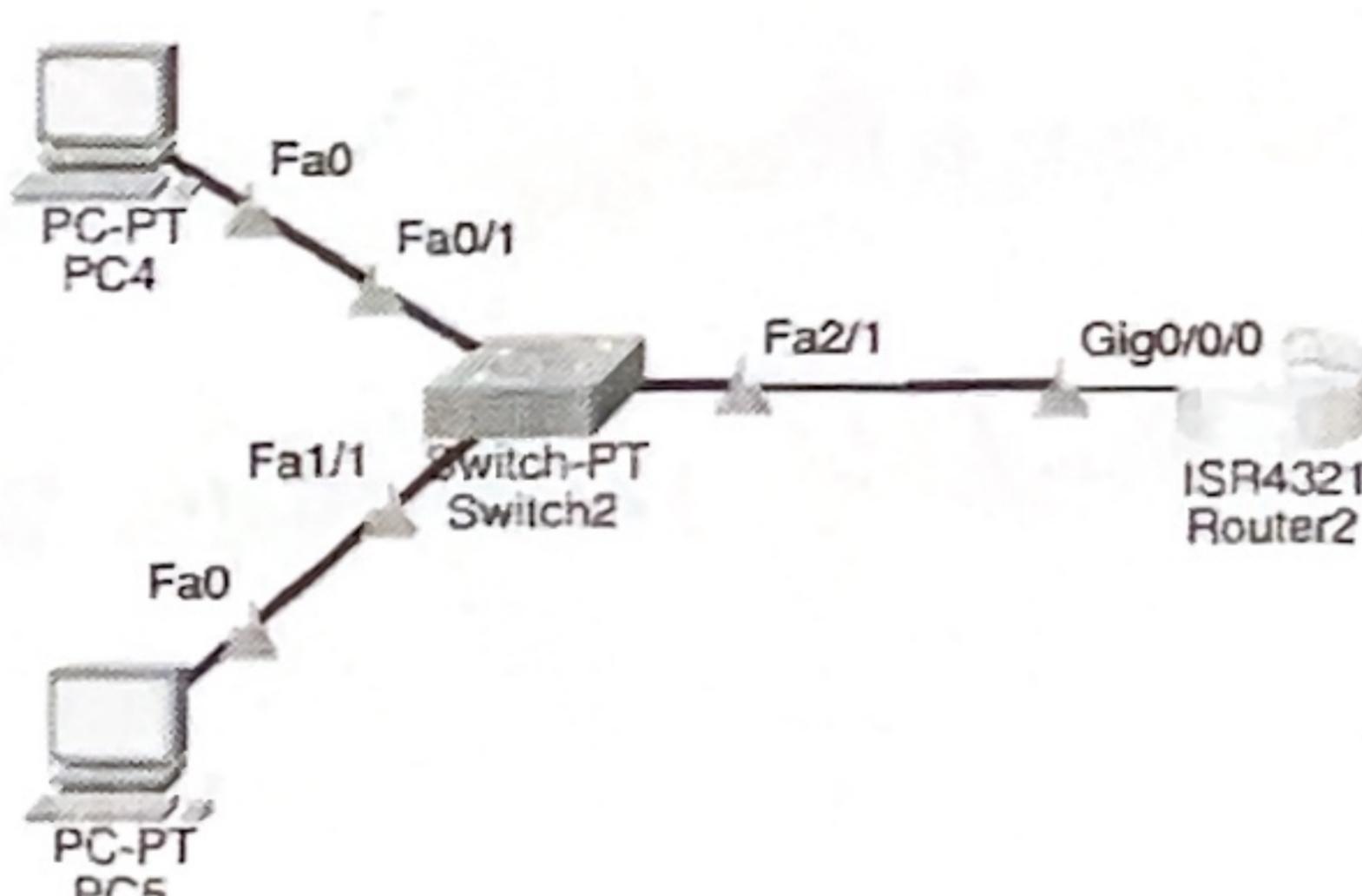


Command Prompt

```

Cisco Packet Tracer PC Command Line 1.0
C:\>telnet 192.168.10.5
Trying 192.168.10.5 ...Open
User Access Verification
Username: dinanath
Password: Routeren
  
```

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



IOS Command Line Interface

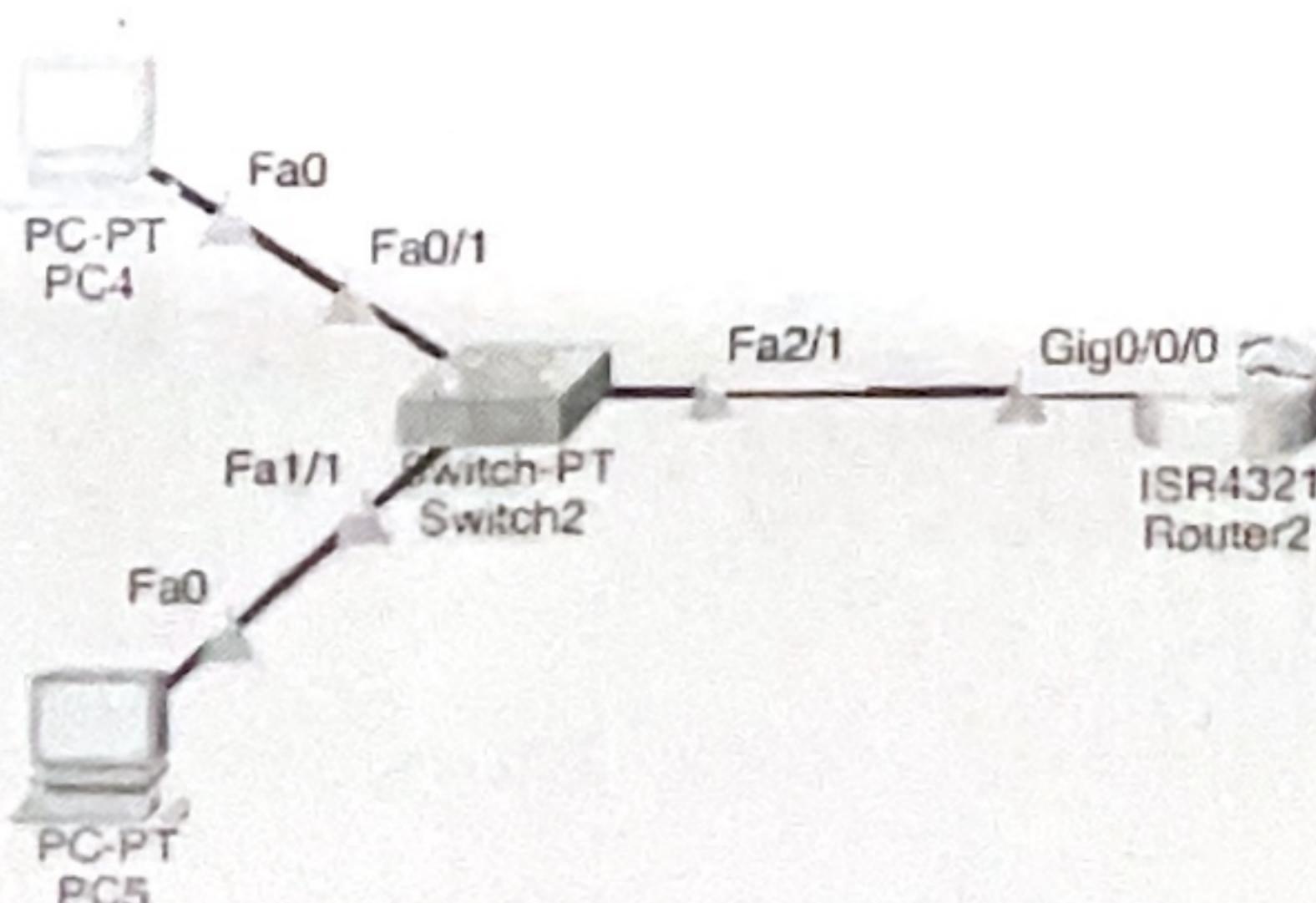
```

%LINEPROTO-5-UPDOWN: Line protocol on interface GigabitEthernet0/0/0, changed state to up
ip address 192.168.30.5 255.255.255.0
Router(config-if)#ip address 192.168.30.5 255.255.255.0
Router(config-if)#exit
Router(config)#hostname dinanath
dinanath(config)#ip domain name cisco.com
dinanath(config)#crypto key generate RSA
The name for the keys will be: dinanath.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: 1024
* Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

dinanath(config)#username dash password cisco
*Mar 1 0:1:23:30: SSH-5-ENABLED: SSH 1.39 has been enabled
dinanath(config)#aaa new-model
dinanath(config)#aaa authentication login default local
dinanath(config)#line vty 0 3
dinanath(config-line)#login authentication default
dinanath(config-line)#transport input SSH
dinanath(config-line)#exit
dinanath(config)#enable password 1234
dinanath(config)#
  
```

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



Cisco Packet Tracer PC Command Line 1.0

```

C:\>SSH -l dash 192.168.30.5
Password: dinanath
Password: 
dinanath(config)#
Enter configuration commands, one per line. End with CNTL/Z.
dinanath(config)#
  
```

(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 preferred 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 unauthorized access.
- ii) Authentication Mechanisms → Supports multiple authentication methods, including password-based authentication and public key authentication.
- iii) Secure Remote Access → Allows users to securely log in to remote systems, execute commands, and manage network devices without exposing credentials in plaintext.
- 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

	<u>SSH (Secure Shell)</u>	<u>Telnet</u>
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) ~~Explain~~ 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 legitimate users can execute critical operations, preventing malicious activities that could compromise system stability.
- v) Protection Against Cyber Threats → Reduces risks associated with cyber threats like phishing, 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 privilege level for the local user account to 15.

Ans → Router(Config)# username CNSLab privilege 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.