Experiment-2

Aim→ Implementation of AAA server as user authentication and authorisation technique for remote access to the network device in computer network using Cisco Packet Tracer.

Objectives 1→ An overview on AAA(Authentication, Authorization and Accounting) used in secured system.

AAA is a secured framework used to control access to computer systems, networks and resources by enforcing user identity verification, access control and activity tracking. It ensures secure and accountable interactions within a system.

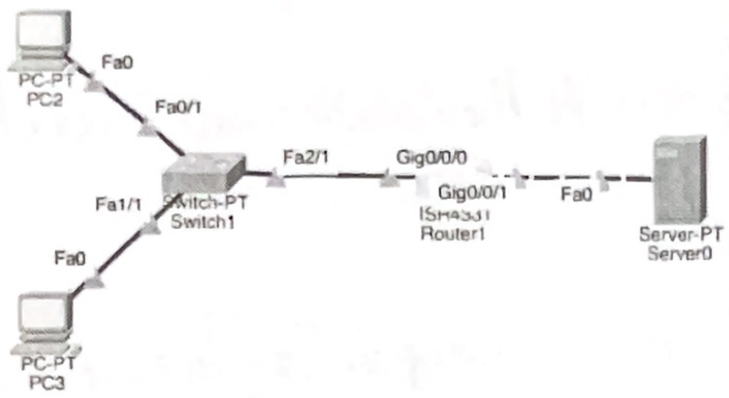
i) Authentication → a) Verifies the identity of users or devices trying to access a system.
b) Requires credentials like usernames, passwords, biometrics or certificates.
c) Methods include: Password-based, MultiFactor Authentication (MFA) & Certificate based Authentication
d) Example: A user entering a password to log in to a network.

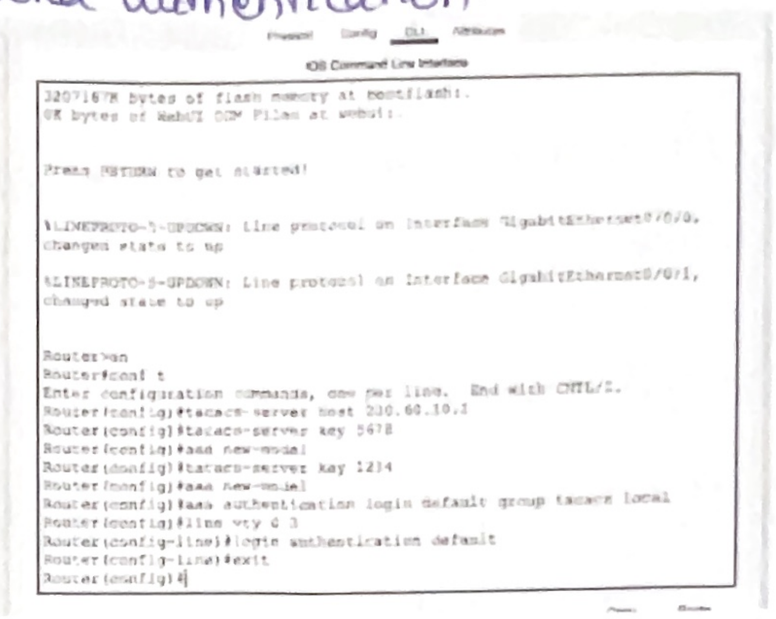
ii) Authorisation → a) Determines what authenticated users are allowed to do.
b) Enforces permissions based on roles, policies and attributes.
c) Methods include: Role-Based Access Control, Attribute-Based Access Control
d) Example: A user can view files but cannot edit them.

iii) Accounting → a) Tracks user activities and resource usage for auditing and reporting.
b) Logs session start/end times, accessed resources and data usage.
c) Supports billing, forensic analysis and compliance.
d) Example: Recording login attempts and file modifications.

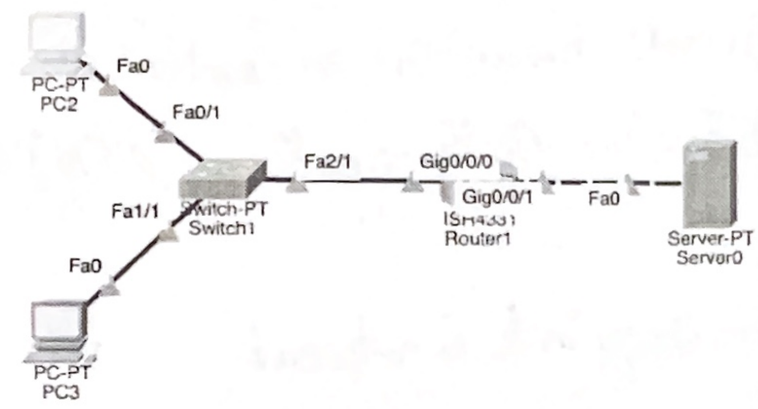
Name: _____ Regd No: _____

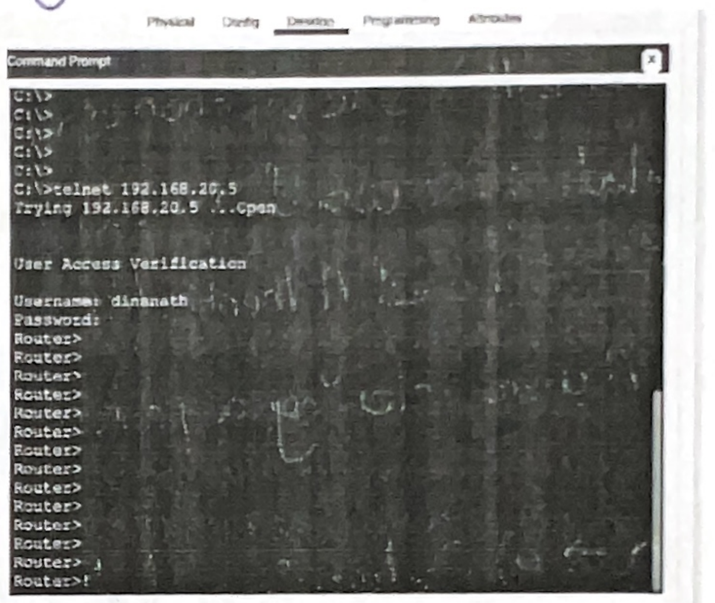
Objective 2 → Configuration and verification of remote user authentication on a Cisco router using AAA server based username-password authentication.



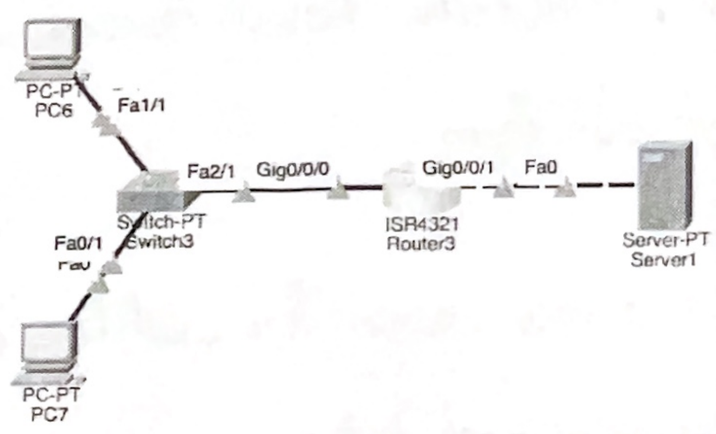


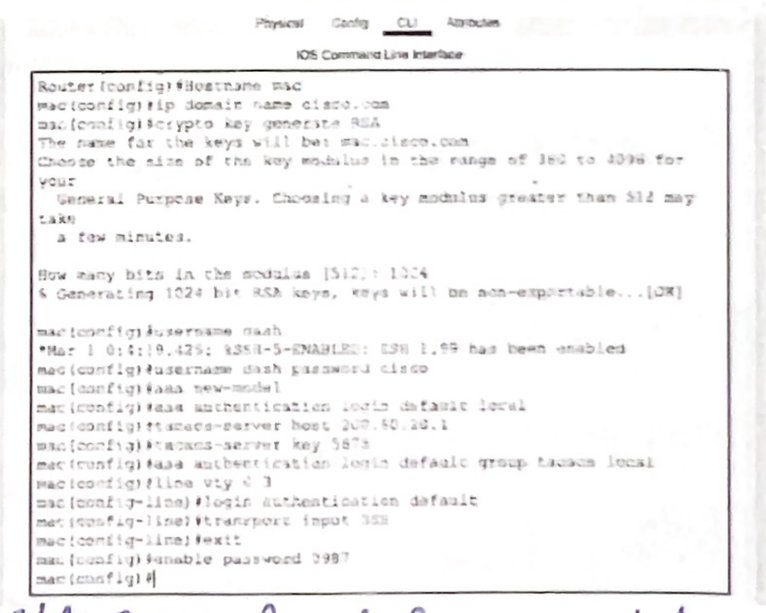
Configuring AAA server for being remotely accessed at PC2.



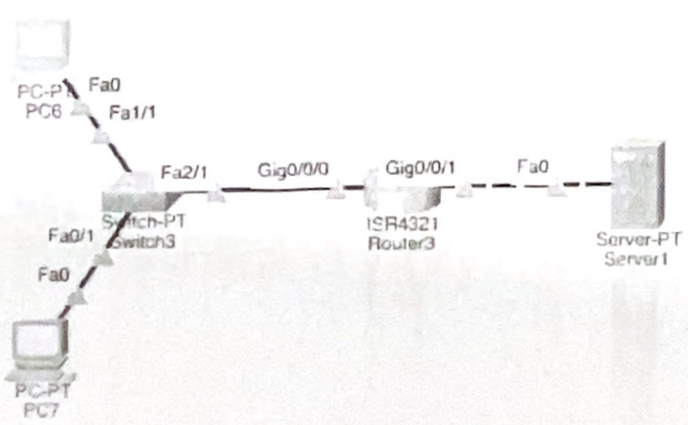


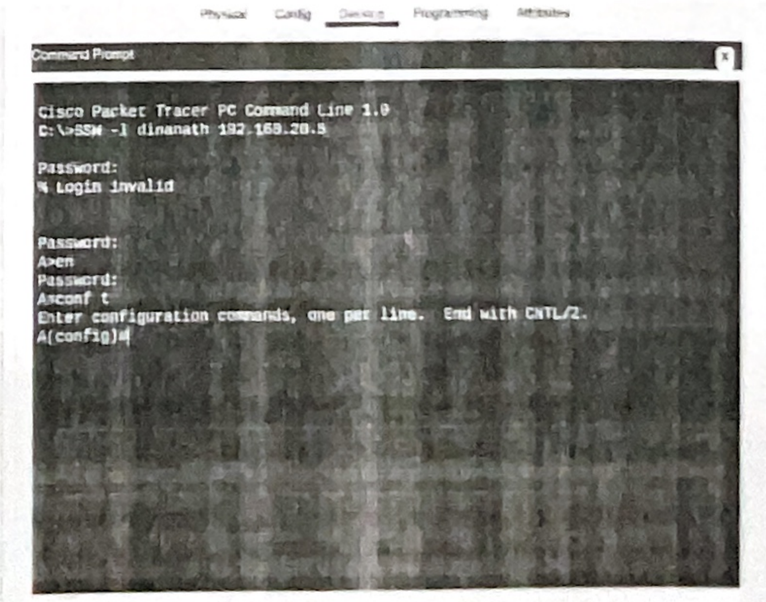
Objective 3 → Configuration and verification of remote user authentication on a Cisco router using AAA server based username-password authentication with SSH.





Configuring AAA server and router with SSH for being remotely accessed at PC6.





Name: _____ Regd No: _____

Conclusion → The implementation of the AAA (Authentication, Authorisation and Accounting) server for remote access to network devices ensures a robust and secure user authentication process. By configuring AAA on cisco routers, the experiment demonstrates how user identity verification, access control, and activity tracking can be effectively managed. This approach not only enhances network security but also provides detailed accountability for user actions.

Exercises →

1) An AAA configuration given as following. Which login credentials are required when connecting to the console port in this configuration?

```
aaa authentication login NO_AUTH none
line console 0
login authentication NO_AUTH
```

Ans → aaa authentication login NO_AUTH none → This command defines an authentication method named NO_AUTH that allows login without requiring any credentials.

line console 0: Specifies the console port configuration.

login authentication NO_AUTH → Applies the NO_AUTH method to the console port.

Required Login Credentials → No login credentials are required when connecting to the console port because the none option bypasses authentication entirely.

2) State the advantages and disadvantages of AAA server based user authentication process.

Ans → Advantages →

i) Enhanced Security → Ensures only authorised user access resources.

ii) Centralised Control → Manages credentials and policies from a single server.

iii) Granular Access → Restricts access based on user roles.

iv) Activity Tracking → Logs user actions for auditing.

v) Scalability → Supports large networks efficiently.

Disadvantages →

i) Single Point of Failure → Server failure can block access.

ii) Complex Setup → Requires technical expertise.

iii) Latency → Authentication may slow under load.

Name: _____ Regd No: _____

iv) Cost → Expensive for small setups.

v) Network Dependency → Requires constant connectivity.

3) Compare and contrast RADIUS (Remote Authentication Dial In User Service) and TACACS+ (Terminal Access Controller Access-Control System) protocol.

Ans →

Feature	RADIUS	TACACS+
i) Functionality	Combines authentication and authorization.	Separates authentication, authorisation and accounting.
ii) Encryption	Encrypts only passwords.	Encrypts the entire packet.
iii) Protocol	Uses UDP (Ports 1812, 1813)	Uses TCP (Port 49)
iv) Access Control	Design for network access (PPP, VPN).	Ideal for device administration (routers, switches).
v) Accounting	Basic session tracking.	More detailed command-level accounting.
vi) Vendor Support	Open standard, widely supported.	Cisco proprietary but widely used.
vii) Performance	Faster due to UDP but less reliable.	Reliable with TCP but slightly slower.

4) State the significance of the following command in AAA server configuration : "AAA authentication login default group TACACS+ local".

Ans → Significance →

i) Primary Authentication → It configures the router to use the TACACS+ servers as the primary method for user login authentication.

ii) Fallback Option → If the TACACS+ server is unreachable, it falls back to local authentication using the device's locally stored usernames and passwords.

iii) Default Method → The default keyword applies this authentication method to all login attempts unless a specific method is defined for a particular line or interference.

5) How does SSH works here to protect the message?

Ans → SSH protects message by encrypting communication between user and the network device. It ensures secure key exchange, verifies user identity and maintains data integrity using Message Authentication Codes (MACs). This prevents unauthorised access and tampering during AAA based authentication.

Name: _____ Regd No: _____