EXPERIMENT: 22

IoT based AAA Local and Server based authentication configuration

Aim: Designing an IoT based AAA Local and Server based authentication configuration.

Software/Apparatus required: Packet Tracer/End devices, Hubs, connectors.

Procedure:

Algorithm:

1. Define the Components:

IoT Devices: These are the devices that need to be authenticated and authorized to access the network resources.

Local AAA Server: This server will handle authentication and authorization requests locally.

Central AAA Server: This server will provide an additional layer of authentication and authorization for higher-level access control.

2. Setup Local AAA Server:

Configure the local AAA server with the necessary software and databases to handle authentication and authorization requests.

Define user profiles or roles and their associated permissions on the local AAA server.

Set up a secure communication channel between the IoT devices and the local AAA server.

3. Implement Local Authentication:

When an IoT device wants to connect to the network, it sends an authentication request to the local AAA server.

The local AAA server verifies the credentials provided by the IoT device against its user database.

If the credentials are valid, the local AAA server generates an authentication token or session key and sends it back to the IoT device.

4. Implement Local Authorization:

Once authenticated, the IoT device sends an authorization request to the local AAA server.

The local AAA server checks the user profile or role associated with the IoT device and verifies if it has the necessary permissions to access the requested resources.

If authorized, the local AAA server sends an authorization response to the IoT device.

5. Configure Central AAA Server:

Set up a central AAA server that will provide an additional layer of authentication and authorization for critical resources or higher-level access control.

Configure the central AAA server with user profiles or roles and associated permissions.

6. Implement Server Authentication:

After local authentication, the IoT device establishes a secure connection with the central AAA server.

The IoT device sends its authentication token or session key to the central AAA server for verification.

The central AAA server validates the authentication token or session key received from the IoT device.

7. Implement Server Authorization:

Once the central AAA server verifies the authentication token or session key, it performs additional authorization checks.

The central AAA server ensures that the IoT device has the necessary permissions to access critical resources or perform higher-level operations.

If authorized, the central AAA server sends an authorization response to the IoT device.

8. Logging and Accounting:

Both the local and central AAA servers maintain logs of authentication and authorization events for auditing and accounting purposes.

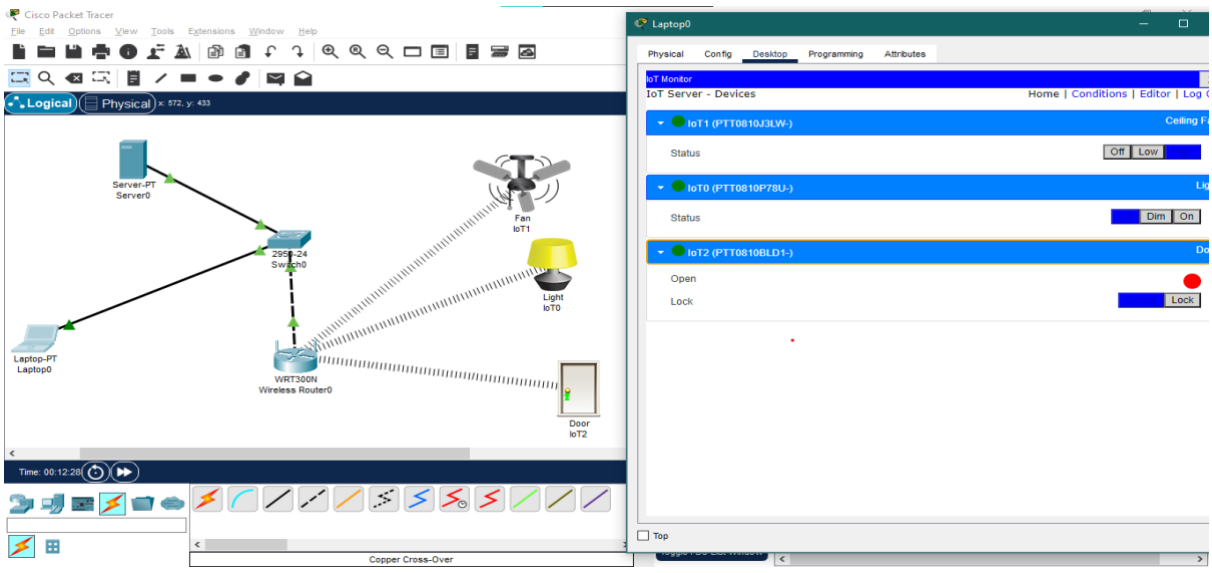
They record information such as user/device identification, timestamps, and actions taken.

9. Revocation and Updates:

Implement mechanisms to handle credential revocation, such as disabling user accounts or tokens when necessary.

Regularly update user profiles, roles, and permissions in both the local and central AAA servers to reflect changes in the network environment.

Remember to implement appropriate security measures such as encryption, secure communication protocols, and strong password policies to ensure the integrity and confidentiality of the authentication process.



Result: IoT based AAA Local and Server based authentication is designed successfully.