**1. RADIUS and TACACS**

* **RADIUS**:

Controls access for external devices such as VPN connections and WiFi users.

* **TACACS**:

Cisco proprietary protocol used for access to routers and switches.

**2. PAP and CHAP**

* **PAP**:

A simple two-way handshake for authentication. PAP only executes this process during the initial link to the authenticating server. A user machine repeatedly sends an Id/Password pair to the authenticating server until authentication is acknowledged or the connection is terminated.

* **CHAP**:

A more secure authentication scheme using a challenge-response mechanism. CHAP provides more security than PAP by frequently changing CHAP IDs and allowing the server to make authentication requests at any time.

**3. IEEE 802.1X Authentication**

* **Supplicant (Client):**

The device requesting access.

* **Authenticator (Network Device):**

Controls access to the network.

* **Authentication Server (e.g., RADIUS Server):**

Validates credentials.

* **EAP Methods**:

EAP-PSK, PEAP, EAP-TLS.

**4. Authorization**

* **Access Control Lists (ACLs):** Determine user access levels.

**MAC**: Mandatory Access Control assigns users to categories.

**DAC**: Discretionary Access Control allows resource owners to assign access levels.

**RBAC**: Role-Based Access Control assigns access based on user roles.

**5. AAA Servers and User Accounts**

* **Centralized Storage:**

User credentials stored on a central server, providing Authentication, Authorization, and Accounting.

**6. RADIUS**

* **Protocol**:

Open standard protocol initially designed for dial-up services.

* **Functionality**:

Combines authentication and authorization; separates accounting.

* **Transport Protocol:**

Uses UDP or TCP with TLS.

* **Confidentiality**:

Encrypts password exchanges.

* **Customization**:

Limited options for per-user or per-group authorization.

* **Accounting**:

Extensive.

**7. TACACS+**

* **Protocol**:

Cisco proprietary protocol.

* **Functionality**:

Separates authentication, authorization, and accounting.

* **Transport Protocol:**

Uses TCP.

* **Confidentiality**:

Encrypts entire packets.

* **Customization**:

Allows per-user or per-group command authorization.

* **Accounting**:

Limited.

**8. Microsoft Authentication and Authorization**

* **Kerberos:**

Authentication protocol used in Windows Active Directories.

* **Key Distribution Centre (KDC):**

Issues Ticket-Granting Tickets (TGTs) and service tickets.

**9. Controlling Access to Cisco Devices**

* **Access Methods:**

Console, Telnet/SSH, Auxiliary lines.

* **SSH:**

Provides encrypted remote access.

**10. Authentication Modes for Cisco Devices**

* **Local AAA Authentication:**

Uses local database for authentication.

* **Server-Based AAA Authentication:**

Uses a central AAA server (e.g., Cisco Secure Access Control System) and communicates using RADIUS or TACACS+ protocols.

**11. Configuring Local AAA Authentication**

1. **Add Usernames and Passwords:**

**Router(config)#**  **username John password Sexton**

1. **Enable AAA Globally:**

**Router(config)#** **aaa new-model**

1. **Configure AAA Authentication Parameters:**

**Router(config)#** **aaa authentication login default local**

**12. Server-Based AAA Implementations**

* **RADIUS**:

Combines authentication and authorization, uses UDP or TCP with TLS, and provides extensive accounting.

* **TACACS+**:

Separates authentication, authorization, and accounting, uses TCP, and allows per-user or per-group command authorization.

**13. Configuring Server-Based AAA Authentication**

1. **Enable AAA Globally**:

**Router(config)#**  **aaa new-model**

1. **Specify the Server:**
   * **TACACS+:**

**Router(config)#** **tacacs-server host 192.168.1.101**

**Router(config)#** **tacacs-server key TACACS-Pa55w0rd**

* + **RADIUS:**

**Router(config)#** **radius-server host 192.168.1.100**

**Router(config)#** **radius-server key RADIUS-Pa55w0rd**

1. **Configure Encryption Key:**
   * **TACACS+:**

**Router(config)#** **aaa authentication login default group tacacs+ local-case**

* + **RADIUS:**

**Router(config)#** **aaa authentication login default group radius local-case**

**14. Example Configurations**

* **TACACS+ Server:**

**Router(config)#** **tacacs-server host 192.168.1.101**

**Router(config)#** **tacacs-server key TACACS-Pa55w0rd**

* **RADIUS Server:**

**Router(config)#** **radius-server host 192.168.1.100**

**Router(config)#** **radius-server key RADIUS-Pa55w0rd**

**15. Fine-Tuning Authentication Configuration**

* **Limit Failed Attempts:**

**Router(config)#** **aaa local authentication attempts max-fail 3**

**Router#** **clear aaa local user lockout**

* **Show AAA User:**

**Router#** **show aaa user**

# Combined Packet Tracer Commands Examples:

1. **Enable AAA Globally and Configure Servers:**

**Router(config)#** **aaa new-model**

**Router(config)#** **tacacs-server host 192.168.1.101**

**Router(config)#** **tacacs-server key TACACS-Pa55w0rd**

**Router(config)#** **radius-server host 192.168.1.100**

**Router(config)#** **radius-server key RADIUS-Pa55w0rd**

1. **Configure Authentication:**

**Router(config)#** **aaa authentication login default group tacacs+ group radius local-case**

**Router(config)#** **aaa local authentication attempts max-fail 3**

1. **Add Usernames and Passwords:**

**Router(config)#** **username John password Sexton**

**Router(config)#** **username admin secret adminpass**

1. **Configure Console and VTY Lines:**

**Router(config)#** **line console 0**

**Router(config-line)#** **login authentication default**

**Router(config)#** **line vty 0 15**

**Router(config-line)#** **login authentication default**