02 – BASIC SECURITY MECHANICS AND MECHANISMS

WIRELESS LAN SECURITY

Authentication and Identity Protocols

- In the wireless world, you need to ascertain the identity of the users (and devices) using authentication mechanisms.
- This is important because access control is established depending on the user's identity.

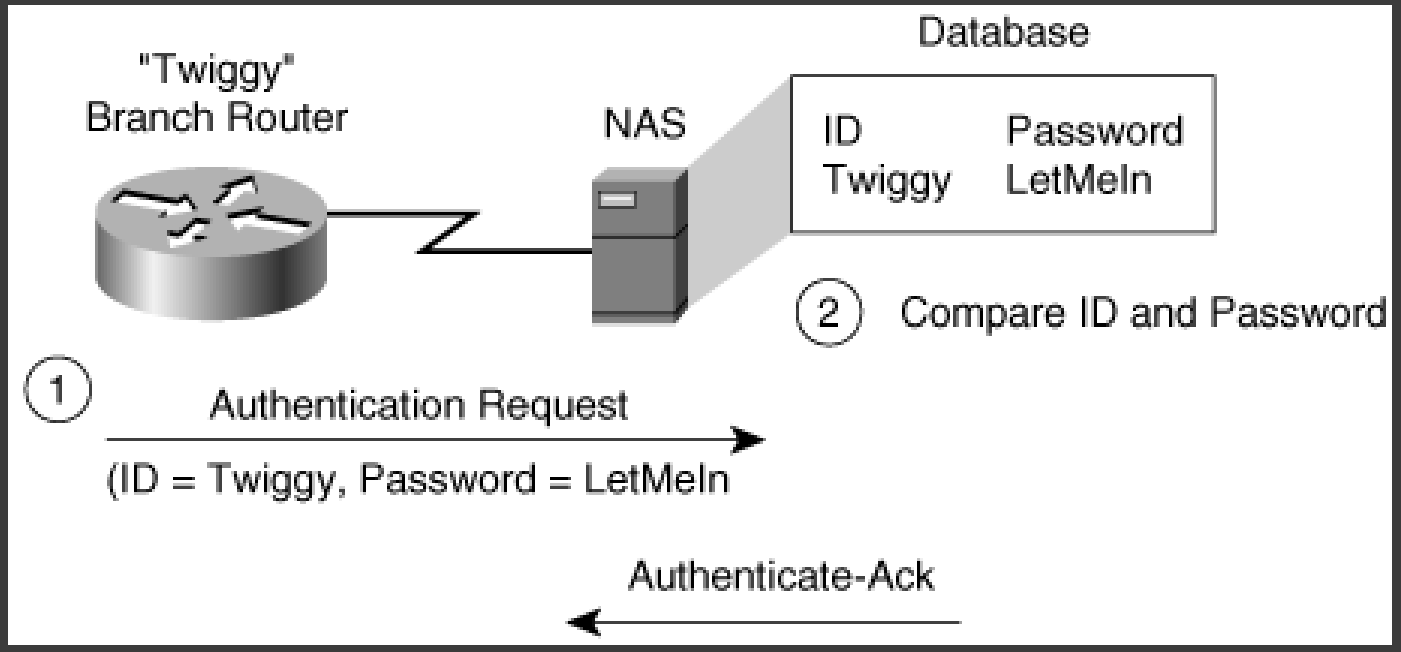
PPP Authentication Protocols

- Passwords are incorporated into many protocols that provide authentication services.
- For dial-in connections, the Point-to-Point Protocol (PPP) is most often used to establish a dial-in connection over serial lines or ISDN.
- PPP authentication mechanisms include PAP, CHAP, and EAP.

PPP Password Authentication Protocol (PAP)

- provides a simple way for a peer to establish its identity to the authenticator using a two-way handshake
- The authenticate-request packet, which contains the peer name and password, is used to initiate the PAP authentication
- If the authenticator receives a Peer-ID/Password pair that is both recognizable and acceptable, it should reply with an Authenticate-Ack. Otherwise, the authenticator should reply with an Authenticate-Nak.

PPP PAP Authentication



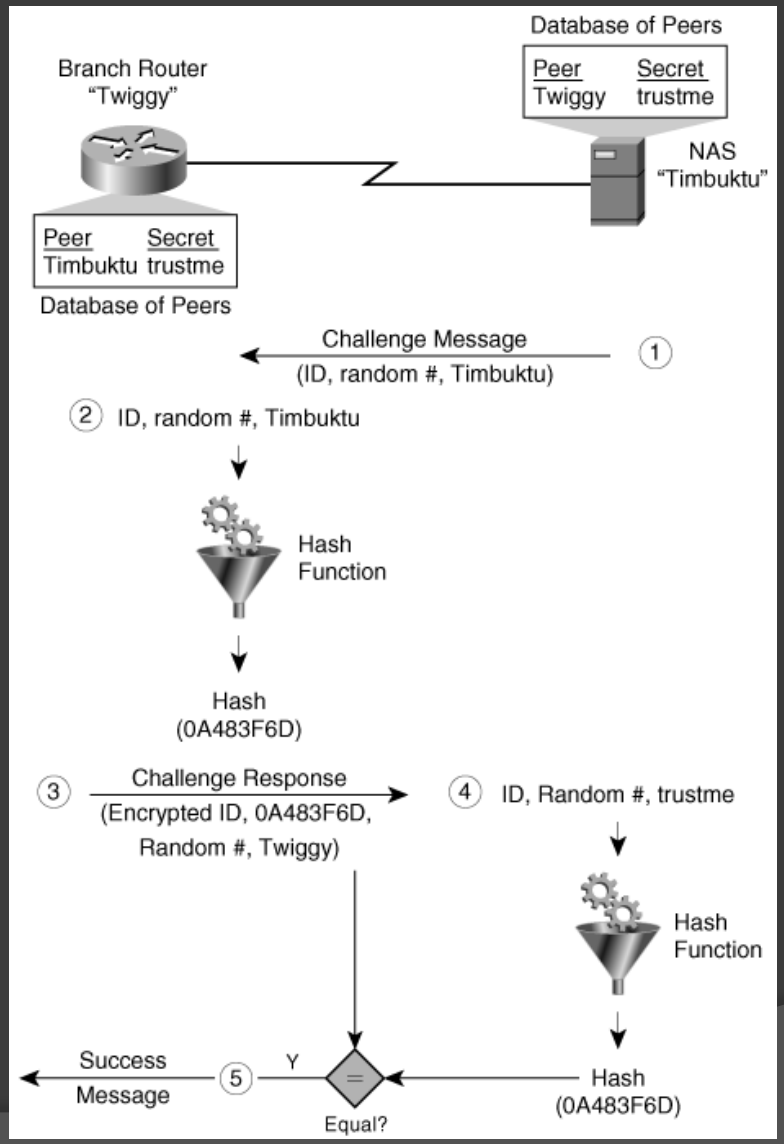
- PAP authenticates only the peer, and passwords are sent over the circuit "in the clear."

PPP Challenge Handshake Authentication Protocol (CHAP)

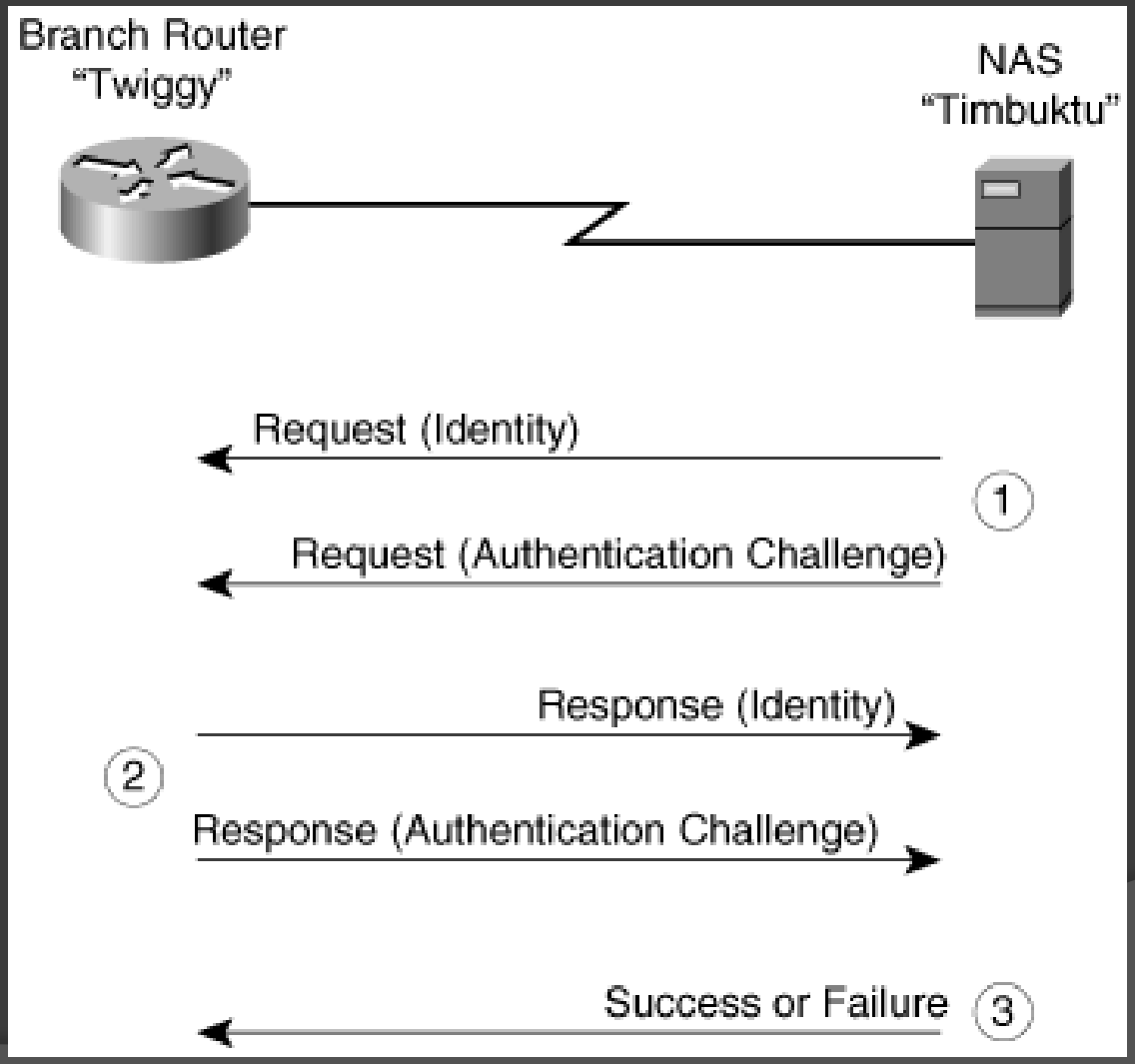
- used to periodically verify the identity of a host or end user using a three-way handshake.

- performed at initial link establishment and can be repeated any time after the link has been established.

PPP CHAP Authentication



PPP Extensible Authentication Protocol (EAP)



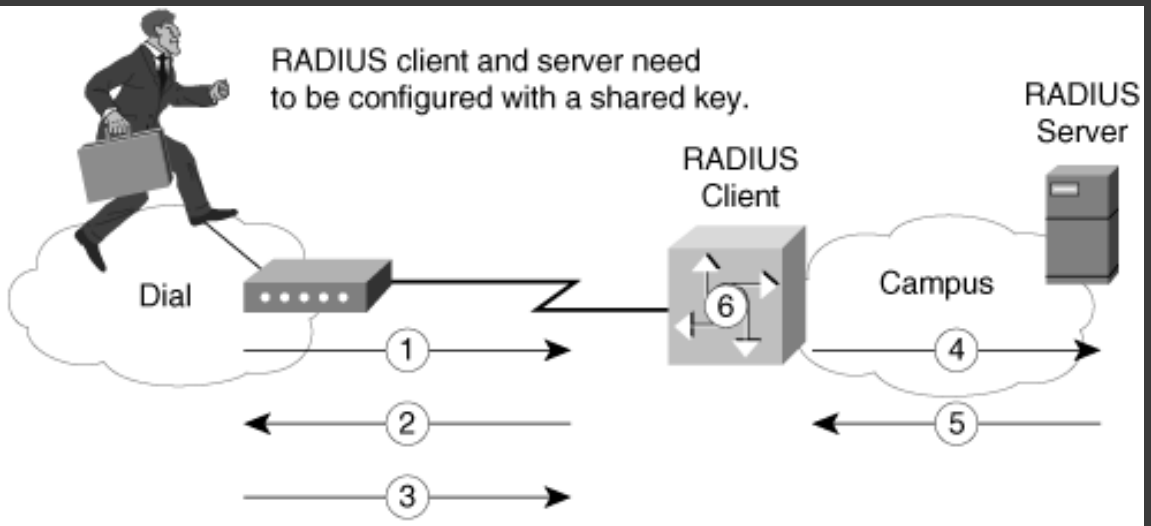
The Remote Address Dial-In User Service Protocol

- an access server authentication and accounting protocol
- RADIUS is a client/server protocol
- The client is responsible for passing user information to designated RADIUS servers and then acting on the response that is returned.
- RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver the service to the user

RADIUS Authentication

- A user login consists of a query (Access-Request) from the NAS to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server
- When the RADIUS server receives the Access-Request packet from the NAS, it searches a database for the username listed.

RADIUS Login and Authentication



1. User initiates PPP authentication to NAS.

2. NAS prompts user for username/password (PAP) or challenge (CHAP).

3. User replies.

4. RADIUS client sends username and encrypted password to RADIUS server.

5. RADIUS server responds with Accept, Reject, or Challenge.

6. RADIUS client acts upon services and service parameters bundled with Accept or Reject.

RADIUS Authorization

- In RADIUS, the authentication and authorization functionalities are coupled together.
- If the username is found and the password is correct, the RADIUS server returns an Access-Accept response, including a list of attribute-value pairs that describe the parameters to be used for this session.

RADIUS Accounting

- allow data to be sent at the start and end of sessions, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session.

- An Internet service provider (ISP) might use RADIUS access control and accounting software to meet special security and billing needs.

RADIUS Transactions

- Transactions between the client and the RADIUS server are authenticated through the use of a shared secret, which is never sent over the network.

- In addition, any user passwords are sent encrypted between the client and the RADIUS server to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.