Chapter 18

RADIUS

RADIUS

- Remote Authentication Dial-In User Service
- Protocol used for communication between NAS and AAA server
- Supports authentication, authorization, and accounting
- Defined in RFC 2865

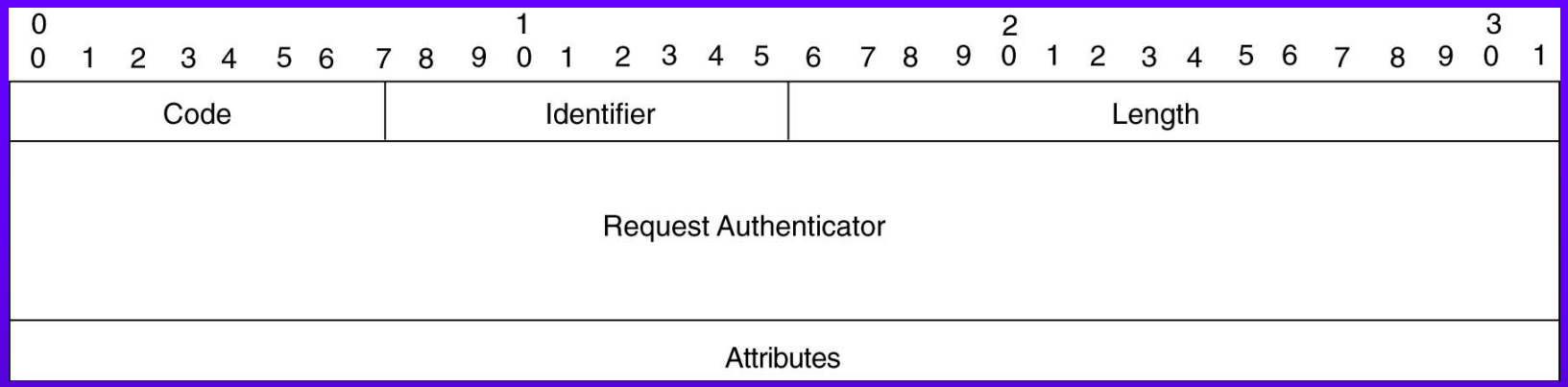
Features of RADIUS

- Client/Server model
  - NAS operates as a RADIUS client by passing user info to RADIUS server and acting on response from server
  - RADIUS server receives connection requests, authenticates user, and provides configuration settings to client
  - RADIUS server can act as a proxy client to other authentication servers
- Flexible authentication mechanisms
  - Can support PPP PAP or CHAP, Unix login, and other authentication mechanisms
- Extensible
  - All transactions con attribute/value tuples
  - New attributes can be added to existing protocol

RADIUS Architecture

- Defined in RFC 2865
- Uses UDP port 1645 or 1812
- Communication between RADIUS server and client is in clear-text except for passwords

RADIUS Packet Format



- Code field used to identify type of packet: access-request, access-accept, access-reject, accounting-request, accounting-response, access-challenge
- Identifier field used to match requests with replies
- Authenticator field contains a 16-byte random number used to authenticate the reply from the RADIUS server and to hide the password

Password Encryption

- Encrypted password transmitted is equal to

  (Hash_A) XOR (padded user password)

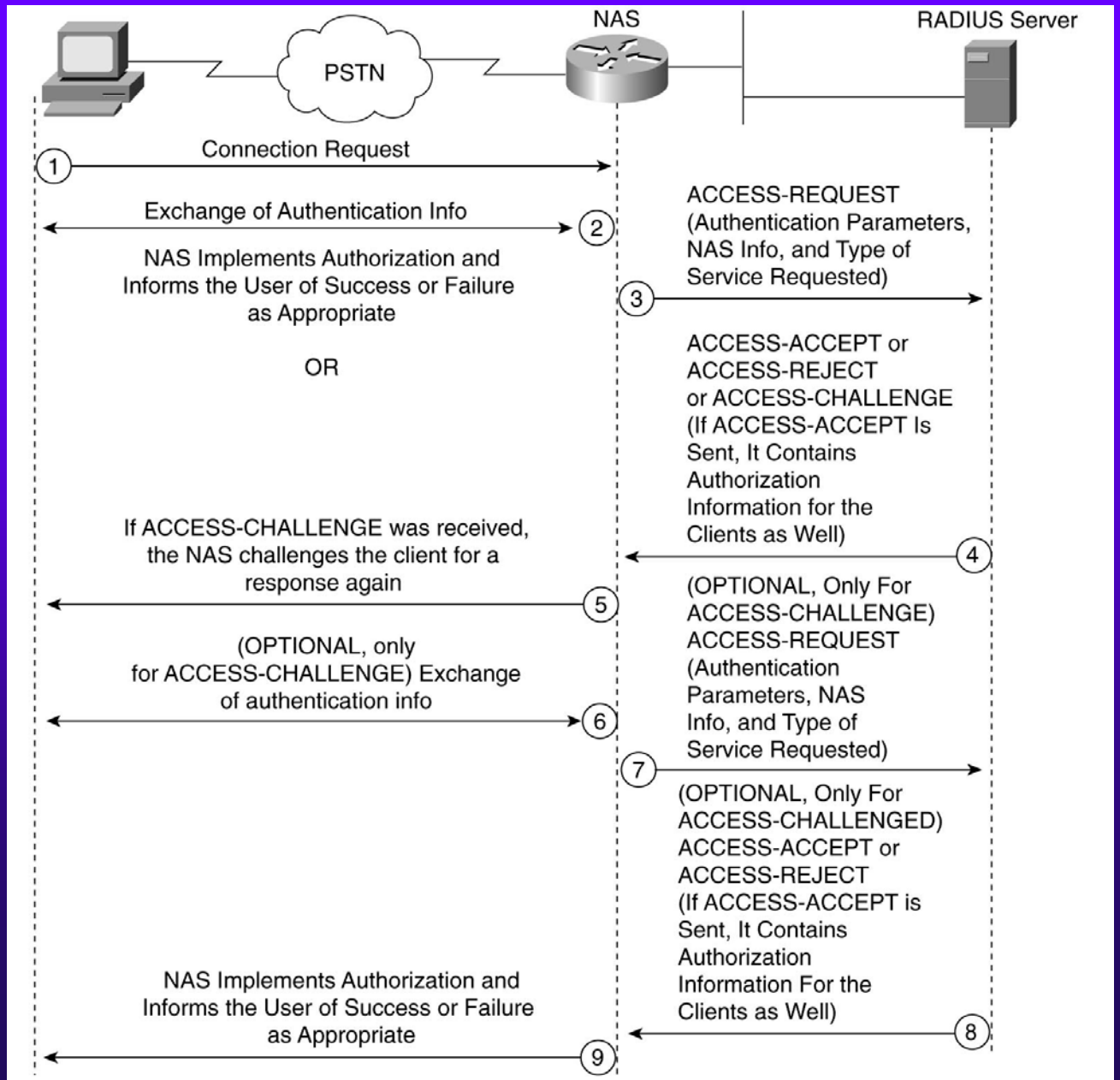
  Where Hash_A = MD5 { request authenticator, preshared secret}

- Receiver calculates Hash_A on its own and XORs it with the encrypted password to get the padded password back in clear-text

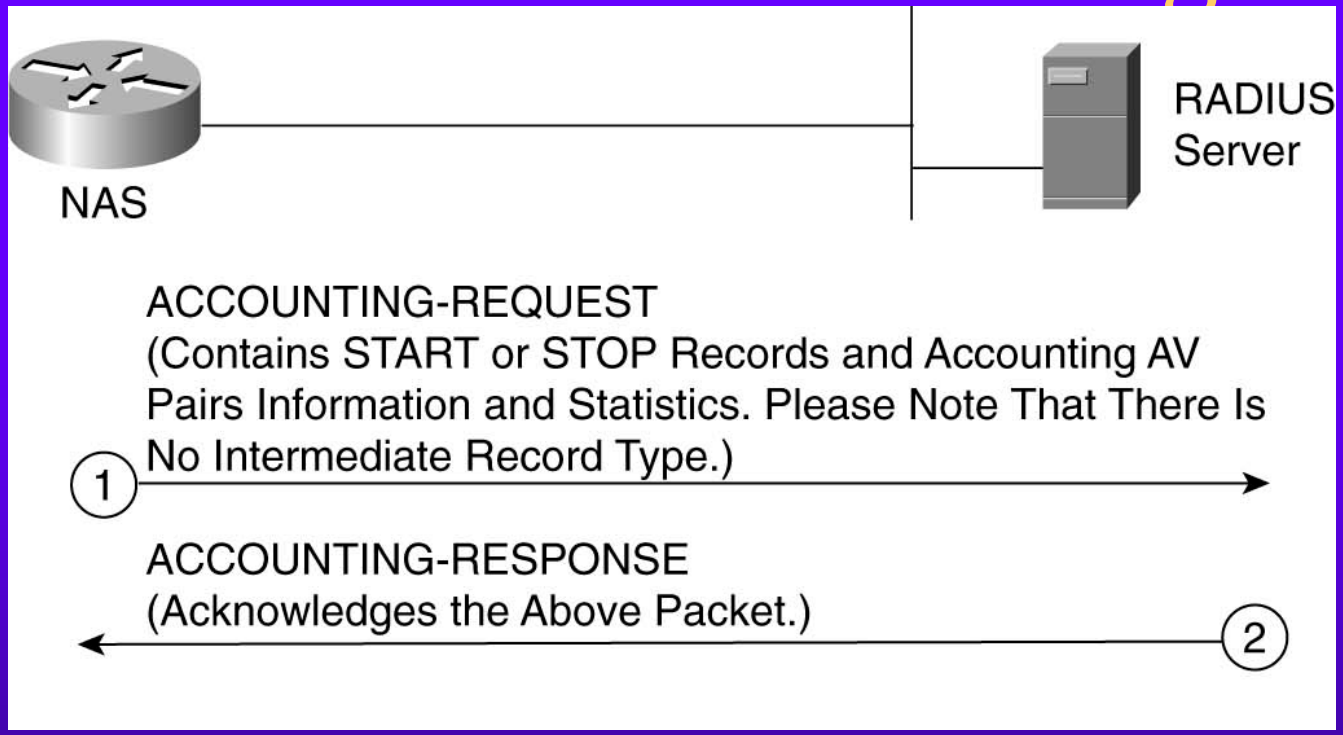
RADIUS Authentication

- NAS sends Access-Request message to RADIUS server containing username, encrypted password, IP address of NAS, and type of service
- RADIUS server replies with Access-Accept, Access-Reject, or Access-Challenge message

RADIUS Authentication

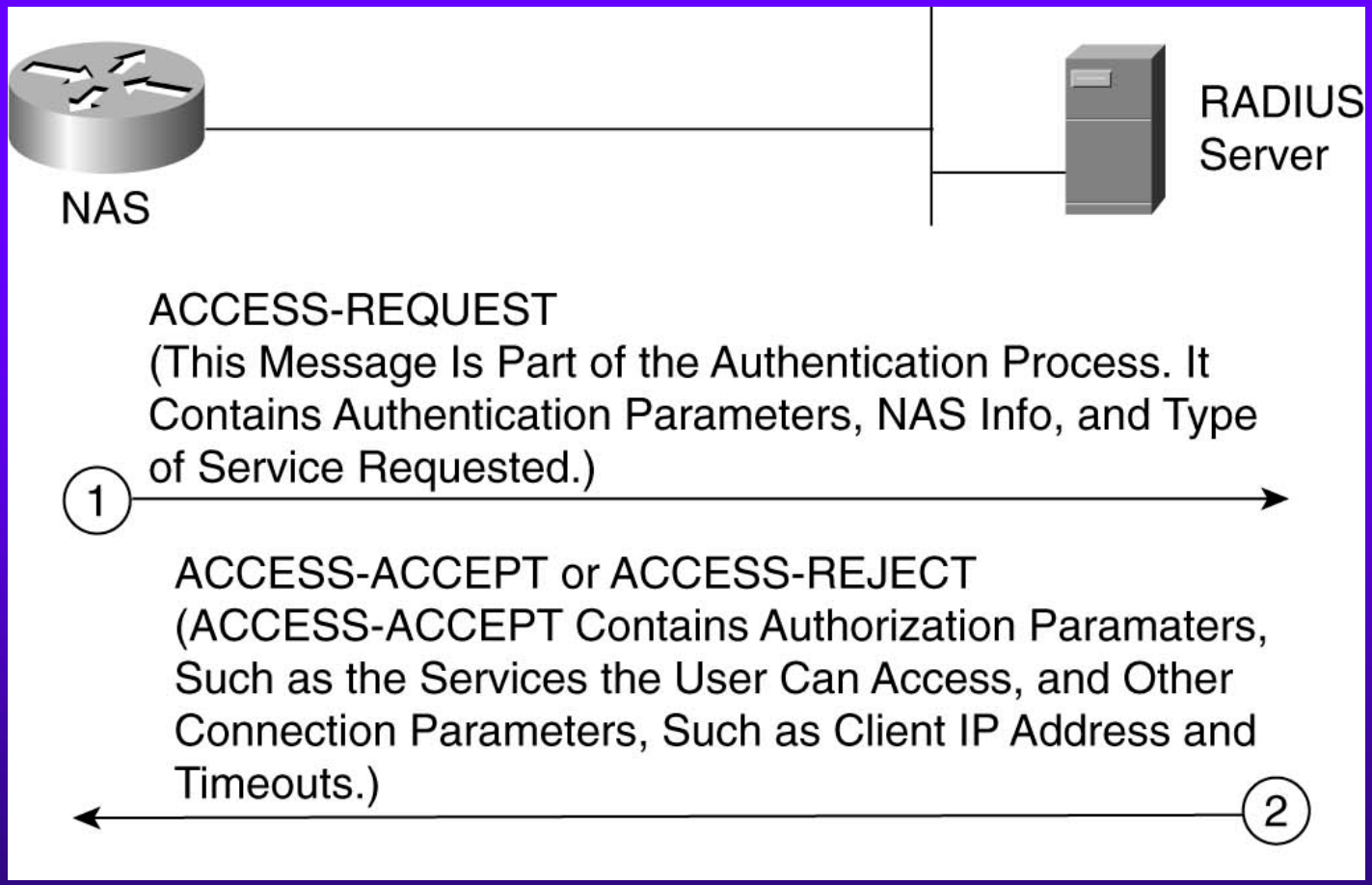


RADIUS Accounting



- Start/Stop records sent at start/end of sessions using UDP port 1646 or 1813
- RFC 2866

RADIUS Authorization



- Authorization data in Accept message lists user authorized services (eg. telnet, rlogin, PPP) and client IP address