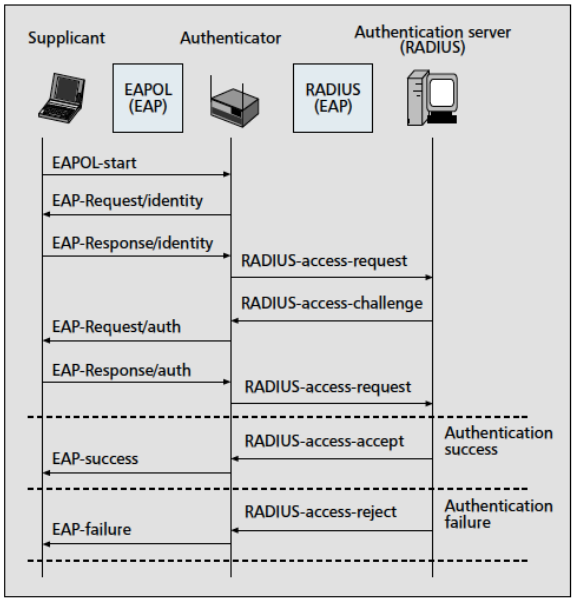
Reason about Protocols' Security (ROL)

To practice the knowledge gained during the master studies, the wireless network used in the students' accommodations is set up and managed by volunteer students. This year, the network admins graduate, so they need to pass the task to their younger colleagues. The new admins evaluate the security of the wireless network and deliver a report with the proposed recommendations.

They find out that the authentication framework used is EAP-MD5. This is an EAP method based on MD5 hash-function. More precise, the EAP/802.1x/RADIUS authentication flow is followed, as illustrated in the figure:



[Source: J.C. Chen and Y.P. Wang, *Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience, IEEE Communication Magazine, 43(12), 2005*]

The authenticator responds to the *EAPOL-start* message with an *EAP-Request/Identity* message. The supplicant replies with its identity in *EAP-Response/Identity*, which is forwarded to the RADIUS server (*RADIUS-access-request*). The RADIUS server sends a random challenge to the supplicant via the Authenticator (*RADIUS-access-challenge, EAP-Request/auth*). The supplicant computes the MD5 hash of the user password and the random challenge and sends back the response to the server (*EAP-Response/auth, RADIUS-access-request*). The server validates / invalidates the MD5 hash value using the password stored in the database for the received identity.

1. The new admins evaluate the security with respect to the following possible attacks: (1) brute-force / dictionary attacks, (2) replay attacks, (3) modification of messages, (4) Man-in-the-Middle attack. For each of the four mentioned attacks, explain why the authentication method is / is not secure and under which conditions / assumptions.

2. The admins suggest other vulnerabilities too. Name and explain one other vulnerability that can expose the privacy of users or their credentials. Explain your assumptions and reasoning.

3. What can the admins do to improve the security of their network?