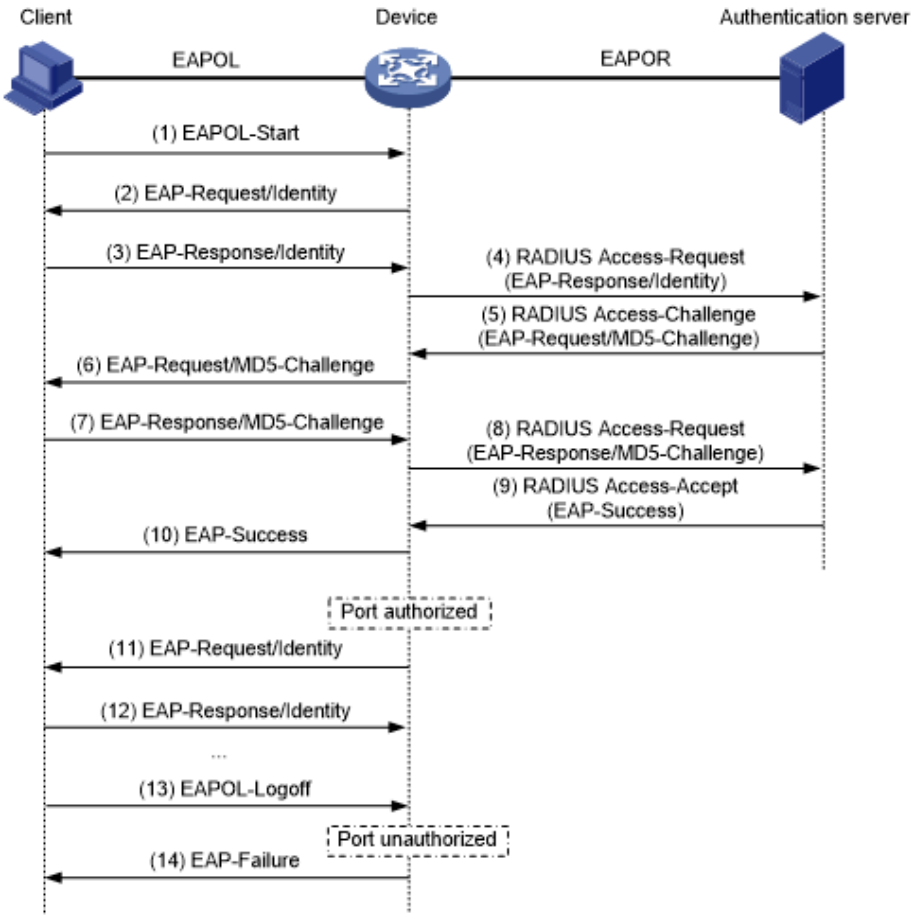
802.1X authentication procedures

802.1X authentication has two methods: EAP relay and EAP termination. You choose either mode depending on support of the RADIUS server for EAP packets and EAP authentication methods.

EAP relay

Figure 39 shows the basic 802.1X authentication procedure in EAP relay mode, assuming that MD5-Challenge EAP authentication is used.

Figure 39: 802.1X authentication procedure in EAP relay mode



The following steps describe the 802.1X authentication procedure:

1. When a user launches the 802.1X client and enters a registered username and password, the 802.1X client sends an EAPOL-Start packet to the access device.

2. The access device responds with an EAP-Request/Identity packet to ask for the client username.

INFOEXPRESS, INC. - EX2546
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]
Page 1 of 3

3. In response to the EAP-Request/Identity packet, the client sends the username in an EAP-Response/Identity packet to the access device.

4. The access device relays the EAP-Response/Identity packet in a RADIUS Access-Request packet to the authentication server.

5. The authentication server uses the identity information in the RADIUS Access-Request to search its user database. If a matching entry is found, the server uses a randomly generated challenge (EAP-Request/MD5-Challenge) to encrypt the password in the entry. Then, the server sends the challenge in a RADIUS Access-Challenge packet to the access device.

6. The access device transmits the EAP-Request/MD5-Challenge packet to the client.

7. The client uses the received challenge to encrypt the password, and sends the encrypted password in an EAP-Response/MD5-Challenge packet to the access device.

8. The access device relays the EAP-Response/MD5-Challenge packet in a RADIUS Access-Request packet to the authentication server.

9. The authentication server compares the received encrypted password with the encrypted password it generated at step 5. If the two passwords are identical, the server considers the client valid and sends a RADIUS Access-Accept packet to the access device.

10. Upon receiving the RADIUS Access-Accept packet, the access device performs the following operations:

    1. Sends an EAP-Success packet to the client.

    2. Sets the controlled port in authorized state.

    The client can access the network.

11. After the client comes online, the access device periodically sends handshake requests to check whether the client is still online. By default, if two consecutive handshake attempts fail, the device logs off the client.

12. Upon receiving a handshake request, the client returns a response. If the client fails to return a response after a number of consecutive handshake attempts (two by default), the access device logs off the client. This handshake mechanism enables timely release of the network resources used by 802.1X users that have abnormally gone offline.

13. The client can also send an EAPOL-Logoff packet to ask the access device for a logoff.

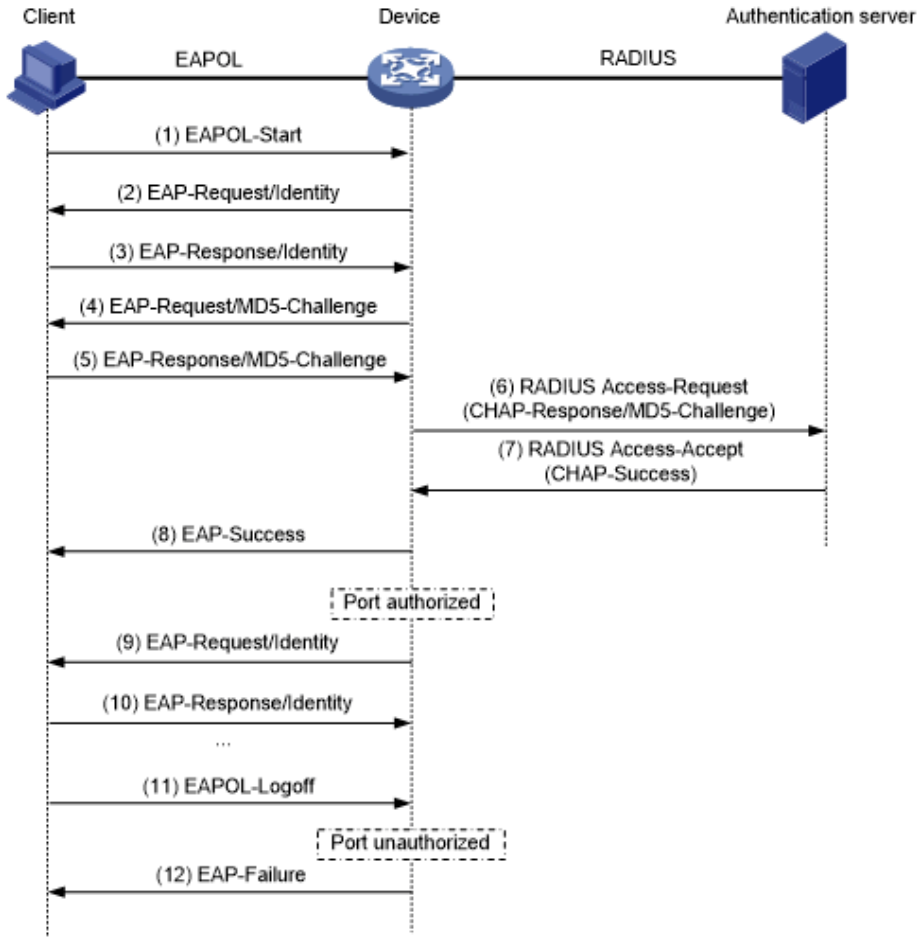
14. In response to the EAPOL-Logoff packet, the access device changes the status of the controlled port from authorized to unauthorized. Then, the access device sends an EAP-Failure packet to the client.

EAP termination

Figure 40 shows the basic 802.1X authentication procedure in EAP termination mode, assuming that CHAP authentication is used.

Figure 40: 802.1X authentication procedure in EAP termination mode

INFOEXPRESS, INC. - EX2546
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]



In EAP termination mode, the access device rather than the authentication server generates an MD5 challenge for password encryption. The access device then sends the MD5 challenge together with the username and encrypted password in a standard RADIUS packet to the RADIUS server.

prev up next

Packet formats home 802.1X authentication initiation

© Copyright 2015, 2017 Hewlett Packard Enterprise Development LP

INFOEXPRESS, INC. - EX2546
CISCO SYSTEMS, INC., et al. v. INFOEXPRESS, INC. [IPR2024-00675]