

Exam Code: HP0-Y11

Exam Name: ProCure Security 7.31

Vendor: HP

Version: DEMO

Part: A

1: Which EAP methods support authentication of an 802.1X supplicant based on a user's name and password? (Select two.)

- A.SIM
- B.TLS
- C.TTLS
- D.SPAP
- E.PEAP
- F.CHAP

Correct Answers: C E

2: Which statements describing Web authentication support on ProCurve switches are correct? (Select two.)

- A.An SSL-based login is required.
- B.It can be configured on ports that also have MAC authentication assigned.
- C.A successfully authenticated user can be redirected to a configurable URL.
- D.The switch's built-in DHCP, ARP, and DNS services assist with Web authentication while a port is in the authenticating state.
- E.When a client connects to a Web authenticator port and a Web browser is opened, the Web browser is automatically redirected to the switch's Web-Auth home page.

Correct Answers: C D

3: Which EAP method is considered the least secure solution for implementing 802.1X user authentication on a wireless LAN?

- A.SIM
- B.MD5
- C.TTLS
- D.FAST
- E.LEAP
- F.PEAP

Correct Answers: B

4: What is a capability of the Secure Access Wizard supported by ProCurve Identity Driven Manager?

- A.It configures 802.1X authenticator ports and RADIUS server settings on a switch.
- B.It verifies the integrity of the ProCurve Identity Driven Manager database using Active Directory.
- C.It conceals all security-related credentials stored in the switch configuration before backing up the file.
- D.It checks a switch configuration file's 802.1X, Web, or MAC authentication settings for consistency and reports any errors.

Correct Answers: A

5: You want to use 802.1X port-access authentication to assign Microsoft Active Directory users to a particular VLAN based on user credentials. Which condition must exist?

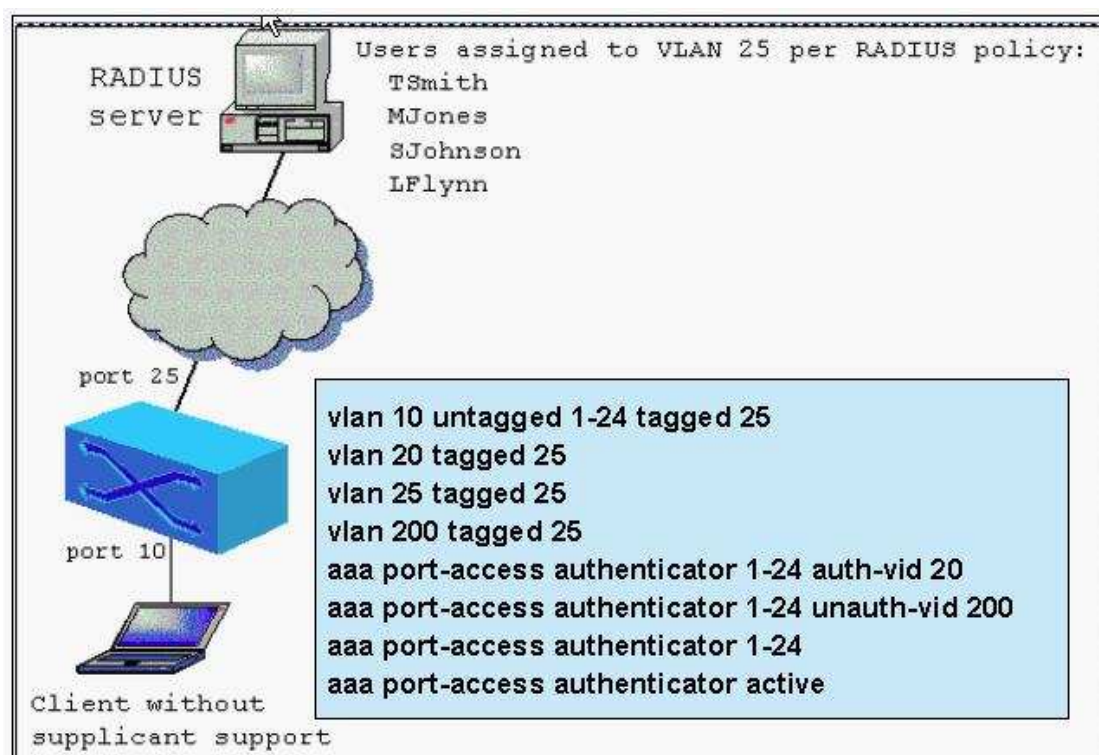
- A.The VLAN ID must exist on the switch.
- B.The VLAN ID must be defined in a GVRP configuration.
- C.The port through which the user is authenticating must be defined as a member of the VLAN.
- D.The user must be a member of an Active Directory Group that has an associated RADIUS remote- access policy.

Correct Answers: A

6: Click the Exhibit button.

The RADIUS server and switch are correctly configured. The switch has the VLAN assignments and port-access commands configured, as shown in the diagram.

What happens to port 10 after the user connects to the network?



- A.remains in an unauthorized state
- B.becomes a member of VLAN 20
- C.becomes a member of VLAN 25
- D.becomes a member of VLAN 200

Correct Answers: D

7: Which statements describing the 802.1X user authentication process are correct? (Select two.)

- A.The supplicant and authentication server must support the same EAP method for the authentication process to proceed.
- B.A switch passes EAP messages between the supplicant and authentication switch without modification or translation.
- C.After a RADIUS server confirms a user is authenticated, the switch sends an EAP-Success

message and sets the port state to authorized.

D. Different RADIUS servers must be configured on the switch if authentication of both switch management users and 802.1X supplicants will be performed.

E. If a supplicant receives an EAP-Request message specifying a particular EAP method to be supported, the authentication session is closed if the supplicant does not support that EAP method.

Correct Answers: A C

8: Which statement describing Web authentication support on the ProCurve Switch 5400zl series is correct?

A. User credentials or a digital certificate can authenticate the client.

B. It is mutually exclusive of other authentication methods on the same port.

C. After successful user authentication, a port is assigned to a VLAN based on an order of priority.

D. If a port is configured to support multiple users, different static untagged VLANs can be assigned concurrently.

Correct Answers: C

9: What is an operational difference between the TLS and MD5 EAP methods?

A. TLS uses a challenge/handshake mechanism for authentication; MD5 uses certificates for authentication.

B. TLS uses a challenge/handshake mechanism for authentication and encryption; MD5 uses certificates for authentication and encryption.

C. TLS uses digital certificates for mutual authentication; MD5 uses a challenge/handshake mechanism to authenticate the client to the server.

D. TLS uses a name and password along with digital certificates to produce a session key; MD5 uses a name and password to produce a session key.

Correct Answers: C

10: Which statements describing MAC authentication on ProCurve switches are correct? (Select two.)

A. It can be configured on the same port with Web authentication and 802.1X authentication.

B. The device's MAC address is sent to the RADIUS server as the user name and password.

C. The switch's built-in DHCP server initially assigns an IP address in the 192.168.0.0 private subnet.

D. The switch automatically initiates user authentication of a device when the device communicates on a MAC authenticator port.

E. Configuration involves defining ports as MAC authenticators, the RADIUS authentication protocol to use, and then activating the ports for MAC authentication operation.

Correct Answers: B D