IT-DUMPS Q&A

Accurate study guides, High passing rate!
IT-dumps provides update free of charge in one year!

http://www.it-dumps.com

Exam : **HP0-Y11**

Title : ProCurve Security 7.31

Version : Demo

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
Answer: CE

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.
Answer: CD

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
Answer: 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.

Answer: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.

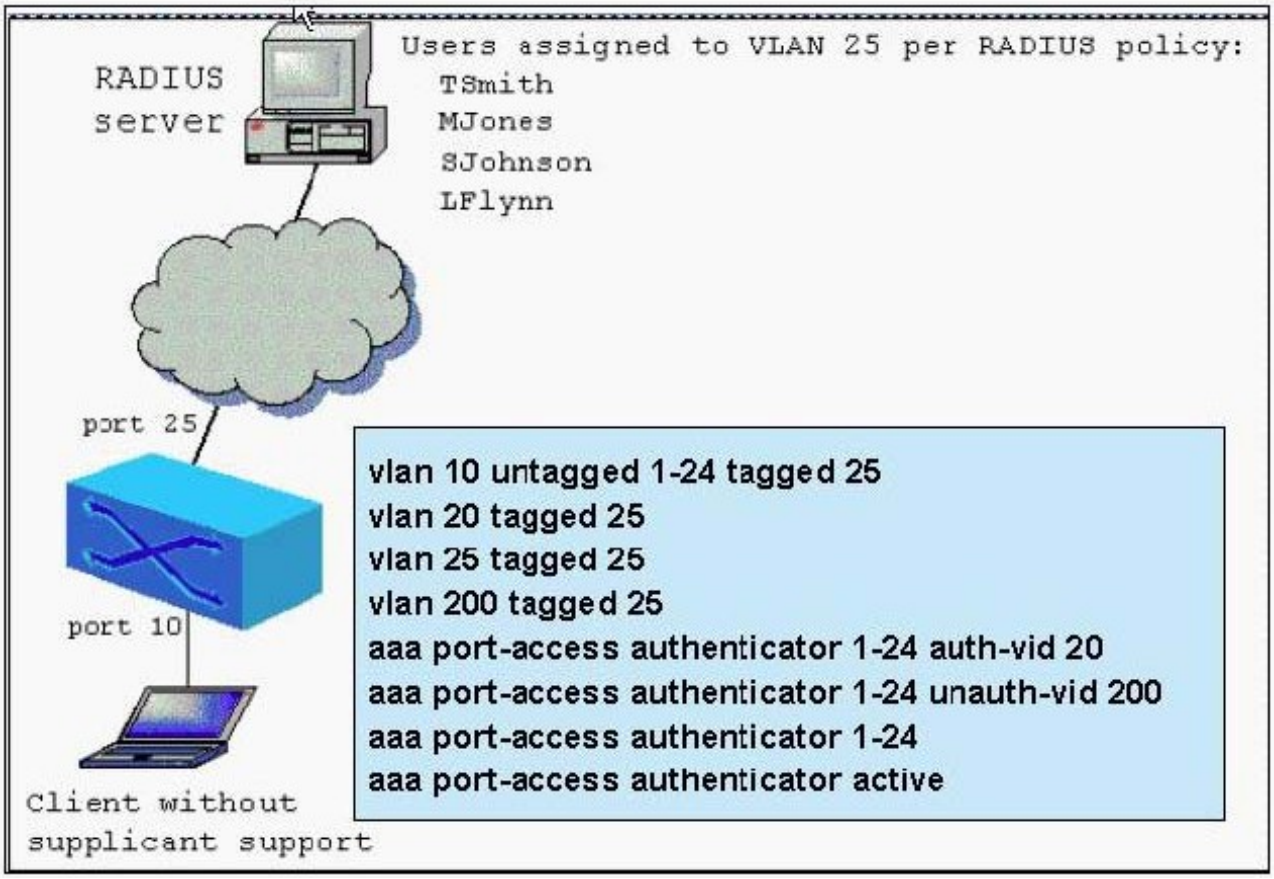
B. The VLAN ID must be defined in a GVRP configuration.

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.

Answer: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
Answer: 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.
Answer:AC

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.
Answer: 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.
Answer: 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.
Answer: BD

11. Which statement describing dynamic VLAN assignment for 802.1X authenticator ports on ProCurve switches is correct?

A. If a GVRP-learned VLAN is used, the RADIUS server must specify that attribute.

B. The VLAN used may be statically defined on the switch or learned through GVRP.

C. If a client fails authentication, the port is reassigned to the Secure Management VLAN.

D. If a client is authenticated, but no VLAN attribute is returned by a RADIUS server, the switch blocks the port.
Answer: B

12. Which two EAP methods support tunneling of a weaker authentication method such as MS-CHAPv2?

A. TLS and SIM

B. PAP and SPAP

C. LEAP and FAST

D. PEAP and TTLS
Answer: D

13. Which protocols are supported by a ProCurve switch for communication with a RADIUS server that is used to authenticate 802.1X supplicants? (Select two.)

A. EAP-RADIUS

B. MD5-RADIUS

C. CHAP-RADIUS

D. PAP-SPAP-RADIUS

E. MS-CHAPv2-RADIUS
Answer:AC

14. You have ProCurve Identity Driven Manager currently deployed in your network and have recently modified an Access Profile. Which task should you perform next?

A. Restart the IDM Agent.

B. Deploy the configuration.

C. Run the Secure Access Wizard.

D. Update the Access Policy Groups.

E. Start Active Directory synchronization.

F. Rediscover switches affected by the changes.
Answer: B

15. Which statements describing the ProCurve switch debug facility are correct? (Select two.)

A. The instrumentation monitor must be enabled first.

B. Specific debug message categories can be selectively enabled.

C. The debug destinations can be set to a session window and a Syslog server concurrently.

D. Debug messages have the same format as standard Event Log messages including the event type and timestamp.
Answer: BC

16. You have just installed two ProCurve 5406zl switches, one on the second floor and one on the third floor of your office. You are using 802.1X for port-access authentication. All users have an 802.1X supplicant installed on their computers and you have configured a RADIUS server with a remote access policy for each floor. Shortly after connecting the computers, users on the second floor report that they cannot access any network resources. You can ping the RADIUS server from both switches, but when you check the RADIUS log, you see authentication requests coming only from the third floor switch. Why are the second floor users unable to connect to the network?

A. The IP address of the RADIUS server has not been configured on the second floor switch.

B. The second floor computers are using the wrong EAP type for authentication with the RADIUS server.

C. The shared secret configured on the second floor switch does not match the shared secret configured on the RADIUS server.

D. No default gateway has been configured on the second floor switch, therefore no authentication requests can reach the RADIUS server.
Answer:A

17. A customer calls you and describes a switch management access problem involving SSH. The customer indicates that he is denied access after supplying the login credentials. The customer is using a RADIUS server for centralized authentication, and has used the ping command to verify that the SSH client, switch, and RADIUS server are all reachable. What is a potential cause of this problem?

A. A self-signed digital certificate has not been installed on the switch.

B. SSH has not been configured for the login access level on the switch.

C. A remote-access policy on the RADIUS server has not been configured to support the CHAP protocol.

D. The digital certificate of the public Certificate Authority used by the switch has not been installed in the SSH client.
Answer: C

18. Authentication of switch management or general network users can involve multiple network components. Which statement describing these network components is correct?

A. A user directory server operates as the policy enforcement point.

B. The authentication server is also known as the policy decision point.

C. A ProCurve switch functions as a policy repository for switch management access using a remote user account.

D. A RADIUS access-accept message is used by a client to acknowledge authentication settings assigned by the server.
Answer: B

19. A university shares a core routing switch between two departments. Each department has a separate ProCurve edge switch deployed and neither department wants the other to have management access to their respective switch. Which security measures can prevent management access by the respective departments? (Select three.)

A. Enable the Privilege Mode option.

B. Configure Authorized IP Managers.

C. Define Secure Management VLANs.

D. Implement Command Authorization.

E. Use RADIUS authentication with separate policies.
Answer: BCE

20. Network security can be described in terms of multiple layers of security. Which action describes a perimeter security measure?

A. limiting switch access to SSH

B. deploying 802.1X authentication

C. installing an Intrusion Prevention System

D. using a secure operating system for network applications
Answer: C