



[HP HP0-757](#)

Exam Name: HP ProCurve Security

Q & A : 70 Q&As

Pdf Demo

Quality and Value for the HP0-757 Exam

[Just4Exams Practice Exams](#) for HP Certification I HP0-757 are written to the highest standards of technical accuracy, using only certified subject matter experts and published authors for development.

100% Guarantee to Pass Your HP0-757 Exam

If you do not pass the Certification I HP0-757 exam on your first attempt using our Just4Exams **HP0-757 testing engine and pdf study guide**, we will give you a FULL REFUND of your purchasing fee.

Downloadable, Interactive HP0-757 Testing engines and PDF Version

Our Exam Preparation Material provides you everything you will need to take a [Certification I certification](#) examination. Details are researched and produced by [HP Certification](#) Experts who are constantly using industry experience to produce precise, and logical.

Free HP0-757 Exams:

This is demo only, this pdf do not include the questions and answers picture

Exam : HP HP0-757

Title : HP ProCurve Security

1. Click the Exhibit button.

A network administrator creates an ACL on the core 5300xl router that denies Telnet traffic from any IP source to any IP destination, but permits all other IP traffic. The ACL is applied as an "outbound" access group to VLAN 50. If no other ACLs have been configured on the router, what is a result of this configuration?

- A. Clients in VLAN 50 can Telnet to local devices but not to devices in other VLANs.
- B. Clients in VLAN 50 cannot Telnet to VLAN 100 but they can access the web servers in that VLAN.
- C. Clients in VLAN 1 can Telnet only to local devices and to devices on VLAN 100.
- D. Clients in VLAN 1 can Telnet to all devices on all three VLANs.

Answer: C

2. In an 802.1X authentication environment there are different methods by which a user can be placed on a VLAN. Which method has the highest priority on a given port?

- A. an authorized VLAN assignment configured on the switch at the time 802.1X was enabled for the port
- B. a dynamic VLAN assignment from the RADIUS server
- C. the statically assigned VLAN configured for the port
- D. the priority determined by the command used to configure the port for 802.1X authentication

Answer: B

3. Which statement is true with regard to the AAA security framework? It _____.

- A. defines standardized processes for access, authorization, and accountability
- B. defines standardized processes for authentication, authorization, and accounting
- C. is an application-neutral Internet standard that defines access control for layer 3 switches
- D. is an HP-proprietary specification that defines how HP ProCurve switches process login sessions

Answer: B

4. A customer wants to provide stricter access security for all network clients and implement a combination of 802.1X and MAC authentication. Which parameters must be configured on the RADIUS server to support the ports configured with MAC authentication? Select TWO.

- A. Configure PAP to support unencrypted authentication of network peripherals.
- B. Create a user on the RADIUS server using the MAC address of the device for the username and the password.
- C. Create a user on the RADIUS server using the MAC address of the device for the username and the RADIUS shared secret for the password.
- D. Configure CHAP RADIUS for the authentication method.
- E. Create a user on the RADIUS server using the MAC address of the device for the username and do not configure a password (leave it blank).
- F. Configure EAP RADIUS for the authentication method.

Answer: BD

5. Click the Exhibit button.

The RADIUS server and switch are correctly configured for proper interaction. The switch has the VLAN assignments and port-access commands shown in the diagram. When the user shown in the diagram connects to the network as shown, port 10 will _____.

- A. remain in an unauthorized state and prevent user traffic from being forwarded
- B. become a member of VLAN 20
- C. become a member of VLAN 25
- D. become a member of VLAN 200

Answer: D

6. The network administrator of a university realizes that students in the on campus housing are connecting wireless access points and switches to the network. The administrator wants to limit a particular port to one MAC address at a time, but is not concerned about the actual address. Which security feature on the 5300xl provides flexibility while effectively limiting a port to a single MAC address at a time?

- A. Port security learn mode limited-continuous
- B. MAC lockdown learn mode limited-continuous
- C. MAC lockout learn mode limited-continuous
- D. 802.1X MAC authentication

Answer: A

7. The HP ProCurve Access Control Security solution helps protect valuable network resources and intellectual property from internal and external security threats. As part of this solution, 802.1X and RADIUS technology on HP switches controls network access based on which criteria? Select THREE.

- A. locked out MAC addresses
- B. type of applications used on the network
- C. type of client OS
- D. login location on the network
- E. access control lists (ACLs)
- F. user's role within in an organization
- G. time of access

Answer: DFG

8. The network administrator of a private college wants to enable web authentication for all access ports in the student housing buildings. In addition, he wants to address the growing problem of students using unauthorized switches to network more than one device per access

port. What additional configuration is required to prevent more than one authenticated user from connecting to a port that has default web authentication enabled?

- A. Enable port security with the address-limit 1 option.
- B. The default client limit is 1 for Web authentication so no further configuration is required.
- C. Enable port security with the learn-mode port-access option.
- D. Add an option to the port-access command that limits the number of MAC addresses to 1.

Answer: B

9. What is true with regard to standard and extended access control lists (ACLs) on the HP ProCurve 5300xl?

- A. A standard ACL can only specify a filter based on a destination IP address, while an extended ACL can specify both source and destination IP addresses.
- B. Standard and extended ACLs can both specify Layer 4 TCP/UDP ports, but only an extended ACL can specify precedence and type of service traffic.
- C. An extended ACL can filter traffic from a source TCP/UDP port to a destination IP address, while a standard ACL only supports filters based on the source IP address.
- D. An extended ACL supports filtering on both source and destination TCP/UDP ports, while a standard ACL only supports source TCP/UDP ports.

Answer: C

10. You support a network that has ports in a conference room that is regularly used by guests. You have decided to define a guest VLAN that allows access to the internet and prevents access to corporate resources. Which solution provides the most flexibility and lowest management overhead while placing the guest users in the appropriate VLAN?

- A. Require that guests connect only to ports in the conference room that are members of the guest VLAN.
- B. Enable 802.1X on the conference room ports. Give guests a temporary logon ID and provide them with 802.1X supplicant software. Associate guest user IDs with a guest VLAN that prevents access to corporate resources.
- C. Enable IEEE 802.1X on the conference room ports and configure the guest VLAN as the authorized VLAN for these ports.
- D. Enable IEEE 802.1X on the conference room ports and configure the guest VLAN as the unauthorized VLAN for these ports.

Answer: D

11. You are designing a network security solution for the sales office of a manufacturing company that is upgrading their current network while attempting to use some of their existing network equipment and servers. Acting on your suggestion, they have decided to implement 802.1X for network authentication. What are the requirements to implement 802.1X throughout their network? Select THREE

- A. 802.1X Supplicant software on all clients
- B. A RADIUS server to provide centralized authentication
- C. An 802.1X compliant web browser on all clients
- D. A database of all MAC Addresses that will access the network
- E. Access Control Lists on all network switches that require port access authentication
- F. network switches that support 802.1X port-based network authentication
- G. a DHCP server to provide IP Addresses for clients so they can begin the authentication dialog

Answer: ABF

12. What is the main difference between EAP-TLS and EAP-MD5?

- A. EAP-TLS uses a challenge/handshake mechanism for authentication; EAP-MD5 uses certificates for authentication.
- B. EAP-TLS uses a challenge/handshake mechanism for authentication and encryption; EAP-MD5 uses certificates for authentication and encryption.
- C. EAP-TLS uses a name and password along with digital certificates to produce a session key; EAP-MD5 uses a name and password to produce a session key.
- D. EAP-TLS uses digital certificates for mutual authentication; EAP-MD5 uses a challenge/handshake mechanism to authenticate the client to the server.

Answer: D

13. Click the Exhibit button.

The RADIUS server and switch are correctly configured for proper interaction. The switch has the VLAN assignments and port-access commands shown in the diagram. When the user provides valid authentication information, port 10 will _____.

- A. remain in an unauthorized state and prevent user traffic from being forwarded
- B. become a member of VLAN 20
- C. become a member of VLAN 25
- D. become a member of VLAN 200

Answer: C

14. A network administrator wants to prevent users in the marketing department from accessing servers on the finance network. Both

departments are connected to the network with an 5300xl switch. Finance department users should have access to the finance servers as well as other common network resources. Which measures combined would accomplish this goal? Select TWO.

- A. Enforce resource operating system security on the finance servers in the form of user names and passwords.
- B. Place marketing department users in a different VLAN than the finance servers.
- C. Apply access control lists to router interfaces to prevent unauthorized traffic from reaching the finance servers.
- D. Isolate the "problem" users in the marketing department by placing them in a separate physical network.
- E. Provide multiple physical interfaces for the finance server.

Answer: BC

15. You have enabled port security using the "send-disable" action. Which administrative action, if any, is required after an intrusion to enable the device to return to normal operation?

- A. No action is required.
- B. The intrusion flag must be cleared.
- C. The port must be enabled.
- D. The intrusion flag must be cleared and the port must be enabled.

Answer: D

More [HP0-757 Braindumps](#) Information

Related HP0-757 Exams

| | | | | |
|---------|---------|---------|---------|---------|
| HP0-M15 | HP0-S18 | HP0-M16 | HP0-A01 | HP0-M18 |
| HP0-M19 | HP0-S19 | HP0-Y20 | HP0-Y19 | HP0-J24 |
| HP0-J15 | HP0-X02 | HP0-063 | HP0-J22 | HP0-S17 |
| HP0-Y21 | HP0-Y11 | HP0-M22 | HP0-P10 | HP0-P17 |

Other HP Exams

| | | | | |
|---------|---------|---------|---------|---------|
| HP0-685 | HP0-626 | HP0-733 | HP0-728 | HP0-438 |
| HP0-J10 | HP2-B11 | HP0-M30 | HP2-E27 | HP0-J31 |
| HP0-A21 | HP0-Y22 | HP0-022 | HP0-065 | HP0-802 |
| HP0-782 | HP0-S11 | HP0-D06 | HP0-058 | HP0-J20 |