



Free Questions for HPE6-A75 by [braindumpscollection](#)

Shared by [Perez](#) on [24-05-2024](#)

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

```
Switch-1(config)# show running-config interface 1-20
Running configuration:

interface 1
  untagged vlan 20
  aaa port-access authenticator
  exit
#output the same for interfaces 2-20
```

Several interfaces on an AOS-Switch enforce 802.1X to a RADIUS server at 10.254.378.521. The interface 802.1X settings are shown in the exhibit, and 802.1X is also enabled globally. The security team have added a requirement for port security on the interfaces as well. Before administrators enable port security, which additional step must they complete to prevent issues?

Options:

- A- Set an 802.1X client limit on the interfaces.
- B- Manually add legitimate MAC addresses to the switch authorized MAC list.
- C- Enable eavesdropping protection on the interfaces.

D- Enable DHCP snooping on VLAN 20.

Answer:

D

Question 2

Question Type: MultipleChoice

OSPF is configured on an AOS-Switch, and the network administrator sets the router ID to 10.0.0.1. The administrator wants to be able to reach the switch at this ID from any location throughout the OSPF system. The administrator also needs the router ID to be stable and available, even if some links on the switch fail.

What should the administrator do?

Options:

- A-** Make sure that 10.0.0.1 is the IP address on the VLAN with the lowest ID.
- B-** Configure 10.0.0.1 on a loopback interface, and enable OSPF on that interface.
- C-** Configure 10.0.0.1 as a manual OSPF neighbor on each switch in the OSPF system.

D- Configure 10.0.0.1 as a secondary IP address on the switch 00BM poet.

Answer:

B

Question 3

Question Type: MultipleChoice

What is the purpose of the captive portal URL hash key on an AOS-Switch?

Options:

- A-** It authenticates guest users based on the password the users enter hi the portal.
- B-** It encrypts and secures the RADIUS messages that the AOS-Switch sends to ClearPass.
- C-** It does not let users alter the URL that redirects them to the portal.
- D-** It specifies the captive portal URL and conceals the setting in the config.

Answer:

C

Question 4

Question Type: MultipleChoice

Refer to the exhibit.

Exhibit 1

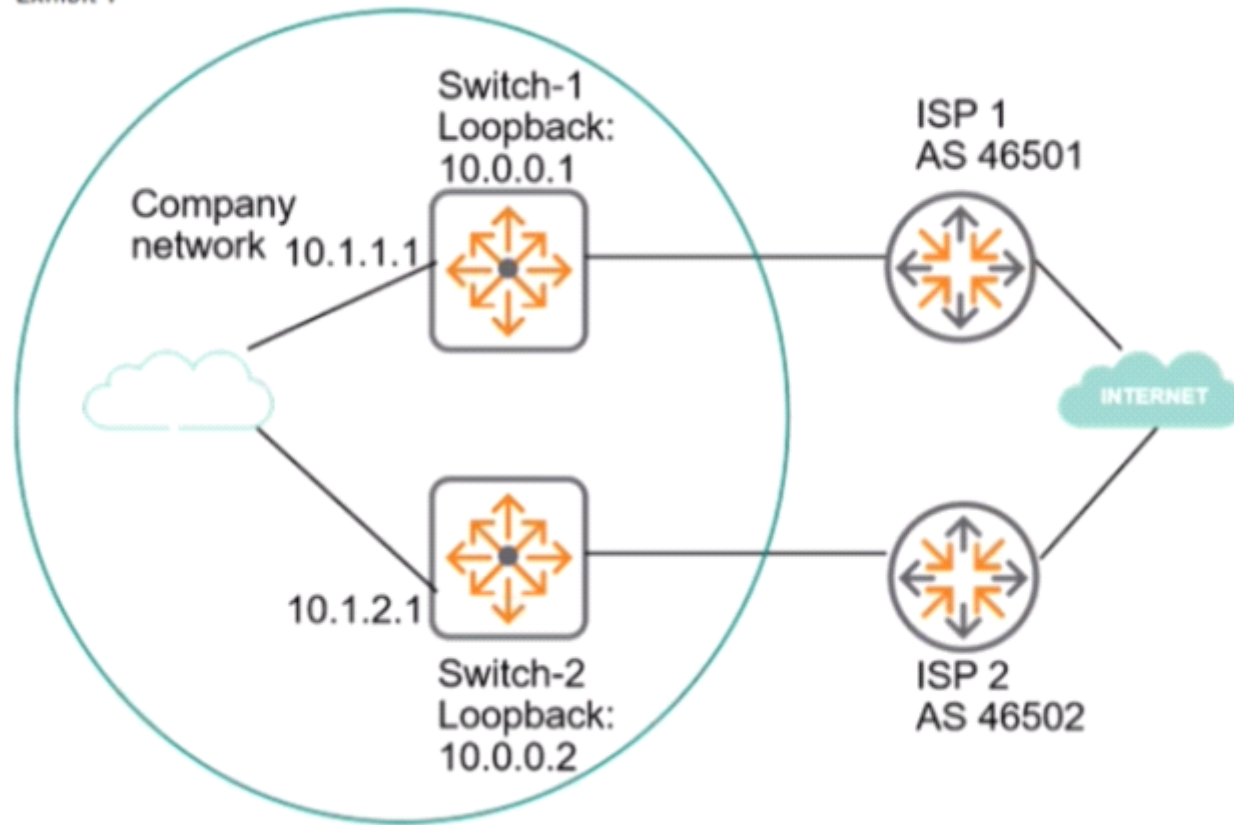


Exhibit 2

Switch-1# show ip bgp summary

Peer Information

Remote Address	Remote-AS	Local-AS	State	Admin Status
10.0.0.2	46500	46500	Connect	Start

Switch-1# show running-config router bgp

Running configuration:

```
router bgp 46500
  enable
  neighbor 10.0.0.2 remote-as 46500
  exit
```

Switch-2# show ip bgp summary

Peer Information

Remote Address	Remote-AS	Local-AS	State	Admin Status
10.0.0.1	46500	46500	Connect	Start

Switch-2# show running-config router bgp

Running configuration:

```
router bgp 46500
  enable
  neighbor 10.0.0.1 remote-as 46500
  exit
```

The network administrator needs to set up BGP between the two company switches. Switch-1 and Switch-2. The BGP connection does not establish. Based on the exhibits, what does the administrator need to do to fix the issue?

Options:

- A- Enable the multihop option for the neighbor on each of the switches.
- B- Enter the network command for 10.0.0.0/24 in the router BGP mode on each switch.
- C- Enable BGP on the interfaces that the switches use to reach each other.
- D- Set the update source for the neighbor to the local loopback interface on each switch.

Answer:

D

Question 5

Question Type: MultipleChoice

A network administrator configures V5F settings on two Aruba 2930F switches. The switches form two separate VSF fabrics. What should the administrator check?

Options:

- A- that the domain ID matches on both switches
- B- that each switch is assigned a unique VSF priority
- C- that the switch with the lower priority has the lower member ID
- D- that LLDP MAD is configured on both members

Answer:

C

Question 6

Question Type: MultipleChoice

A company has AOS-Switches deployed at sites with inexperienced IT staff. The main office network administrators want to track if configurations change on branch switches. What should be set up for this purpose?

Options:

- A- an SNMP trap

B- an RMON alarm

C- an auto-config server

D- an IP SLA profile

Answer:

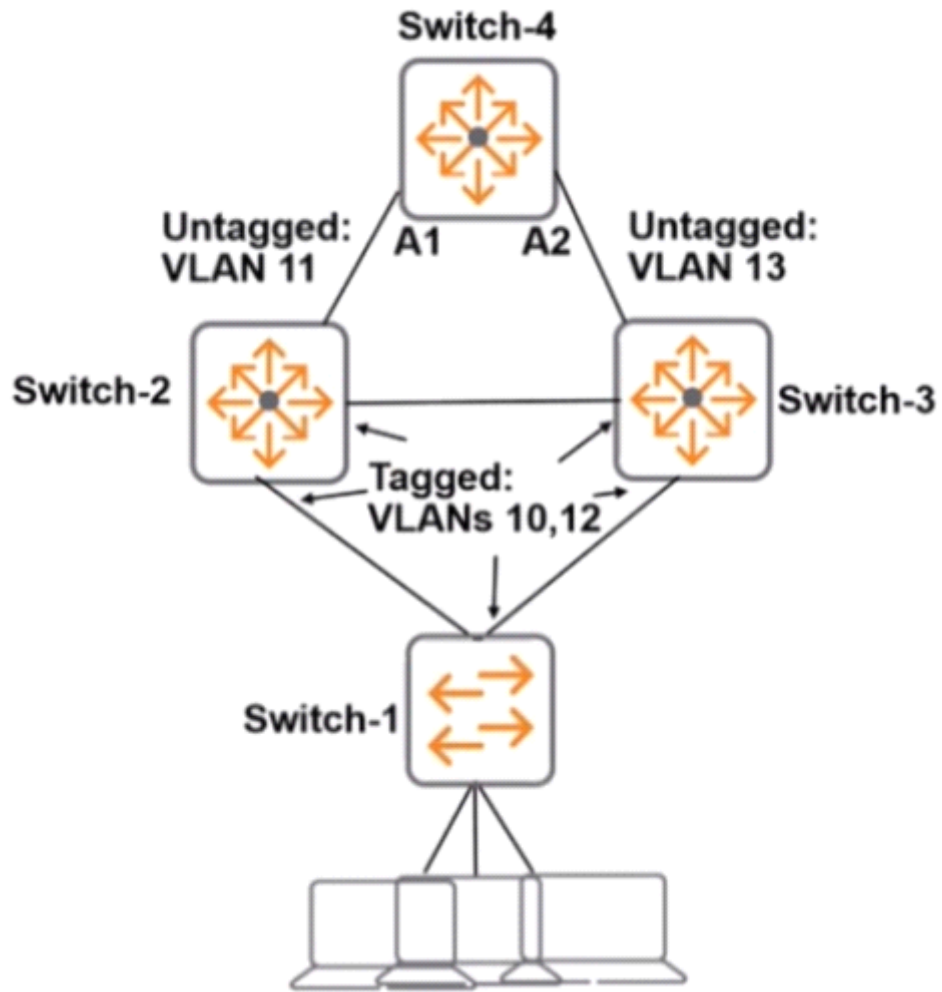
A

Question 7

Question Type: MultipleChoice

Refer to the exhibits.

Exhibit 1



```
Switch-1(config)# spanning-tree
Switch-1(config)# spanning-tree mode rapid-pvst
Switch-1(config)# spanning-tree vlan 10-13 enable

Switch-2(config)# spanning-tree
Switch-2(config)# spanning-tree mode rapid-pvst
Switch-2(config)# spanning-tree vlan 10-13 enable
Switch-2(config)# spanning-tree vlan 10-11 priority 0
Switch-2(config)# spanning-tree vlan 12-13 priority 1

Switch-3(config)# spanning-tree
Switch-3(config)# spanning-tree mode rapid-pvst
Switch-3(config)# spanning-tree vlan 10-13 enable
Switch-3(config)# spanning-tree vlan 10-11 priority 1
Switch-3(config)# spanning-tree vlan 12-13 priority 0

Switch-4(config)# spanning-tree
Switch-4(config)# spanning-tree mode rapid-pvst
Switch-4(config)# spanning-tree vlan 10-13 enable
```

The network administrator enters the commands shown in Exhibit 2. What is the spanning tree status on A1 and A2?

Options:

- A- A1 towards traffic, and A2 blocks traffic.
- B- Both A1 and A2 block traffic.
- C- A1 blocks traffic, and A2 forwards traffic.

D- Both A1 and A2 forward traffic

Answer:

D

Question 8

Question Type: MultipleChoice

Refer to the exhibit.

```
Switch# ping 10.1.10.5
10.1.10.5 is alive, time = 3 ms

Switch# show radius authentication

Status and Counters - RADIUS Authentication Information

NAS Identifier           : Access-1
Invalid Server Addresses : 0
                        UDP
Server IP Addr  Port  Timeouts  Requests  Challenges  Accepts  Rejects
-----
10.1.10.5      1812  6         3         0           0         0
```

A network administrator sets up 802.1X authentication to a RADIUS server on an AOS-Switch. The RADIUS server and user devices are both set up to use REAP MSCHAPv2. The administrator tests the authentication and sees the output shown in the exhibit. Which issue

could cause this output?

Options:

- A-** The RADIUS shared secret does not match on the switch and the server.
- B-** The administrator entered the wrong password for the test account.
- C-** The switch does not have a certificate for port-access installed on the switch.
- D-** The switch port is set for user mode 801. IX. but the RADIUS server is set for port mode.

Answer:

A

To Get Premium Files for HPE6-A75 Visit

<https://www.p2pexams.com/products/hpe6-a75>

For More Free Questions Visit

<https://www.p2pexams.com/hp/pdf/hpe6-a75>

