



**Vendor: Cisco**

**Exam Code: 642-813**

**Exam Name: Implementing Cisco IP Switched Networks**

**Version: Demo**

**QUESTION 1**

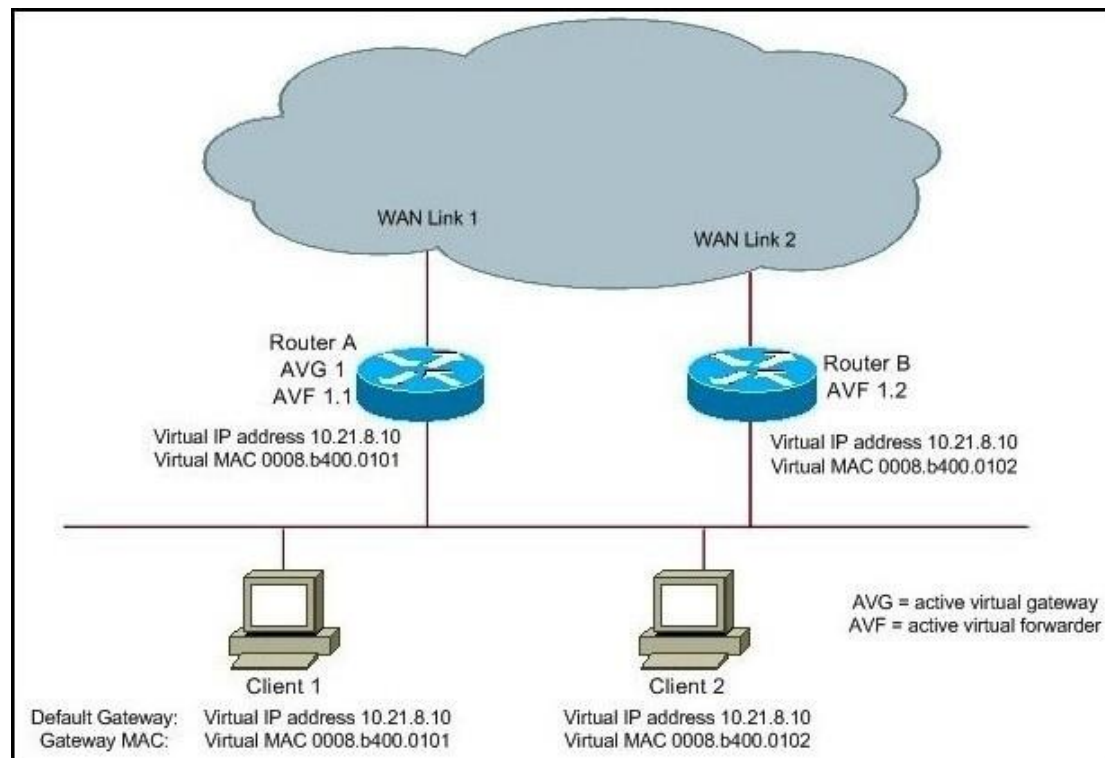
Which statement is true about RSTP topology changes?

- A. Any change in the state of the port generates a TC BPDU.
- B. Only nonedge ports moving to the forwarding state generate a TC BPDU.
- C. If either an edge port or a nonedge port moves to a block state, then a TC BPDU is generated.
- D. Only edge ports moving to the blocking state generate a TC BPDU.
- E. Any loss of connectivity generates a TC BPDU.

**Correct Answer: B**

**QUESTION 2**

Refer to the exhibit. Which four statements about this GLBP topology are true? (Choose four.)

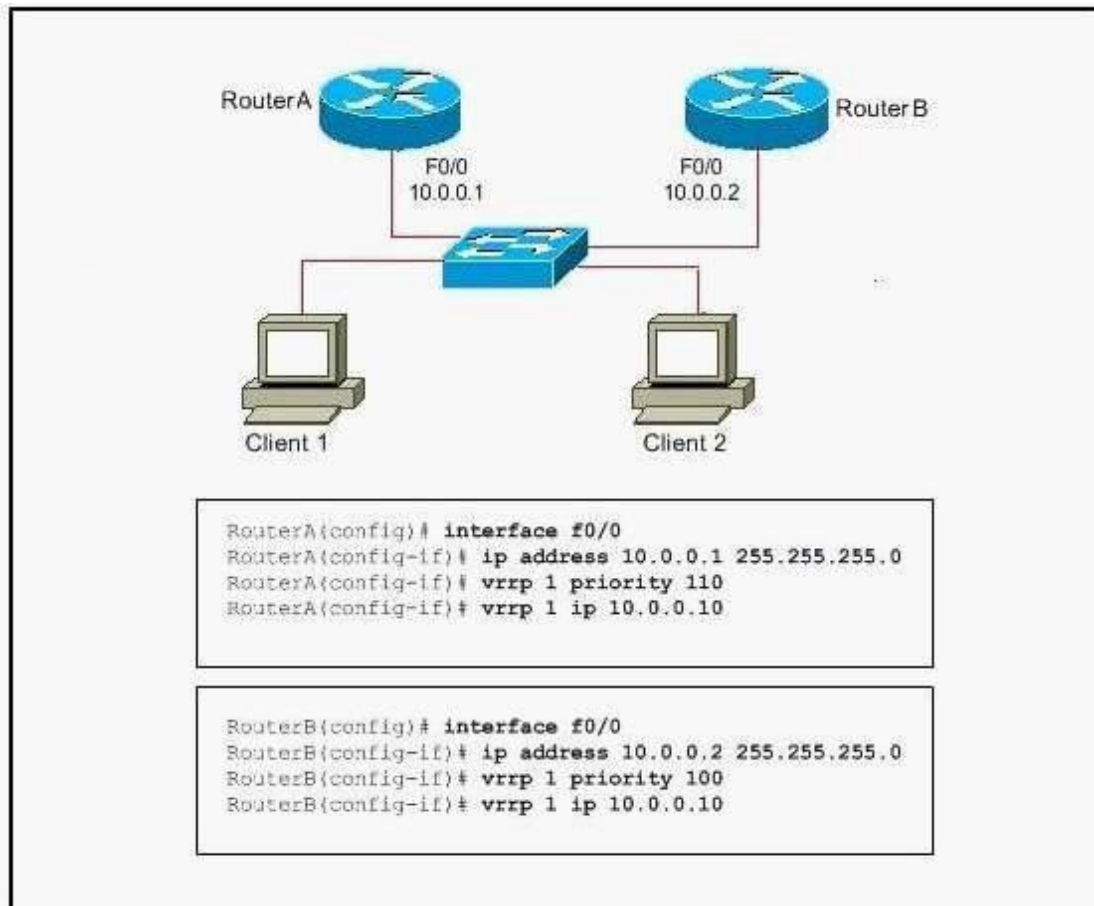


- A. Router A is responsible for answering ARP requests sent to the virtual IP address.
- B. If router A becomes unavailable, router B forwards packets sent to the virtual MAC address of router A.
- C. If another router is added to this GLBP group, there would be two backup AVGs.
- D. Router B is in GLBP listen state.
- E. Router A alternately responds to ARP requests with different virtual MAC addresses.
- F. Router B transitions from blocking state to forwarding state when it becomes the AVG.

Correct Answer: ABDE

**QUESTION 3**

Refer to the exhibit. Which VRRP statement about the roles of the master virtual router and the backup virtual router is true?



- A. Router A is the master virtual router, and router B is the backup virtual router. When router A fails, router B becomes the master virtual router. When router A recovers, router B maintains the role of master virtual router.
- B. Router A is the master virtual router, and router B is the backup virtual router. When router A fails, router B becomes the master virtual router. When router A recovers, it regain the master virtual router role.
- C. Router B is the master virtual router, and router A is the backup virtual router. When router B fails, router A becomes the master virtual router. When router B recovers, router A maintains the role of master virtual router.
- D. Router B is the master virtual router, and router A is the backup virtual router. When router B fails, router A becomes the master virtual router. When router B recovers, it regain the master virtual router role.

Correct Answer: B

**QUESTION 4**

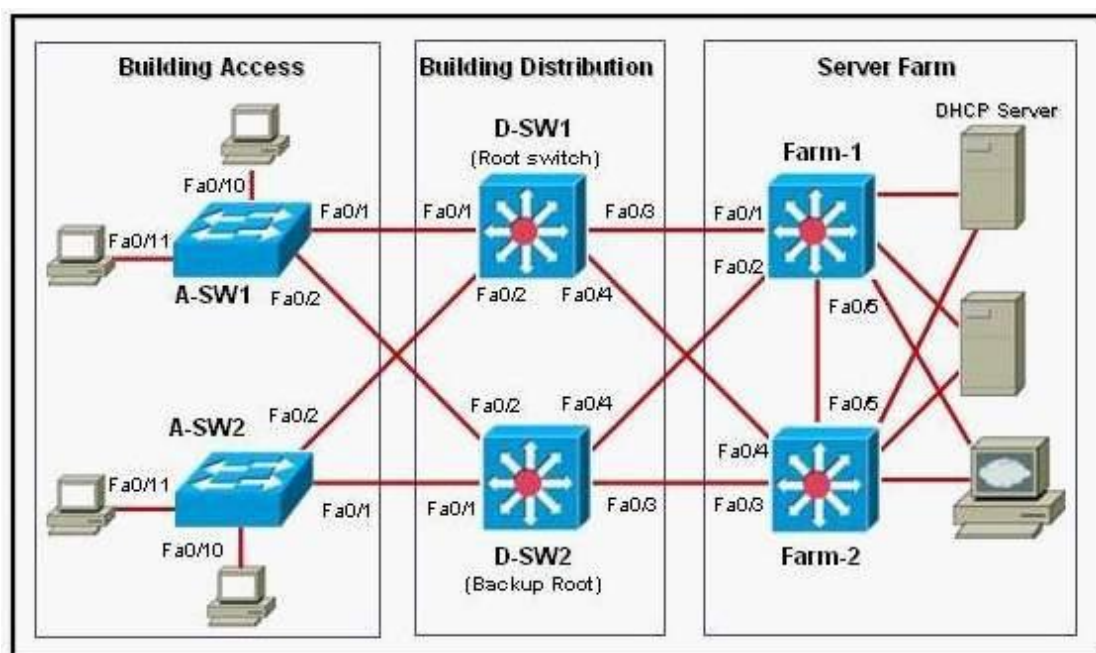
Which description correctly describes a MAC address flooding attack?

- A. The attacking device crafts ARP replies intended for valid hosts. The MAC address of the attacking device then becomes the destination address found in the Layer 2 frames sent by the valid network device.
- B. The attacking device crafts ARP replies intended for valid hosts. The MAC address of the attacking device then becomes the source address found in the Layer 2 frames sent by the valid network device.
- C. The attacking device spoofs a destination MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.
- D. The attacking device spoofs a source MAC address of a valid host currently in the CAM table. The switch then forwards frames destined for the valid host to the attacking device.
- E. Frames with unique, invalid destination MAC addresses flood the switch and exhaust CAM table space. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.
- F. Frames with unique, invalid source MAC addresses flood the switch and exhaust CAM table space. The result is that new entries cannot be inserted because of the exhausted CAM table space, and traffic is subsequently flooded out all ports.

**Correct Answer: F**

**QUESTION 5**

Refer to the exhibit. An attacker is connected to interface Fa0/11 on switch A-SW2 and attempts to establish a DHCP server for a man-in-middle attack. Which recommendation, if followed, would mitigate this type of attack?

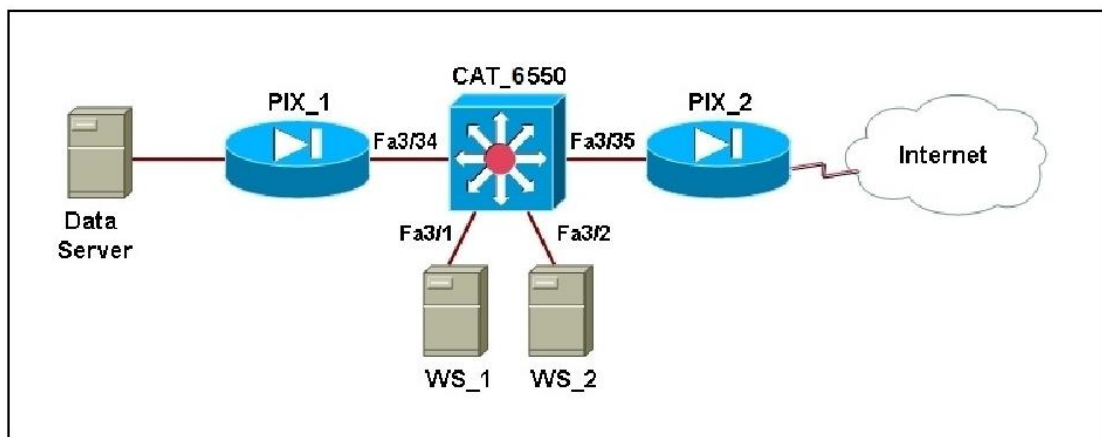


- A. All switch ports in the Building Access block should be configured as DHCP trusted ports.
- B. All switch ports in the Building Access block should be configured as DHCP untrusted ports.
- C. All switch ports connecting to hosts in the Building Access block should be configured as DHCP trusted ports.
- D. All switch ports connecting to hosts in the Building Access block should be configured as DHCP untrusted ports.
- E. All switch ports in the Server Farm block should be configured as DHCP untrusted ports.
- F. All switch ports connecting to servers in the Server Farm block should be configured as DHCP untrusted ports.

**Correct Answer: D**

### QUESTION 6

Refer to the exhibit. The web servers WS\_1 and WS\_2 need to be accessed by external and internal users. For security reasons, the servers should not communicate with each other, although they are located on the same subnet. However, the servers do need to communicate with a database server located in the inside network. Which configuration isolates the servers from each other?



- A. The switch ports 3/1 and 3/2 are defined as secondary VLAN isolated ports. The ports connecting to the two firewalls are defined as primary VLAN promiscuous ports.
- B. The switch ports 3/1 and 3/2 are defined as secondary VLAN community ports. The ports connecting to the two firewalls are defined as primary VLAN promiscuous ports.
- C. The switch ports 3/1 and 3/2 and the ports connecting to the two firewalls are defined as primary VLAN promiscuous ports.
- D. The switch ports 3/1 and 3/2 and the ports connecting to the two firewalls are defined as primary VLAN community ports

**Correct Answer: A**

**QUESTION 7**

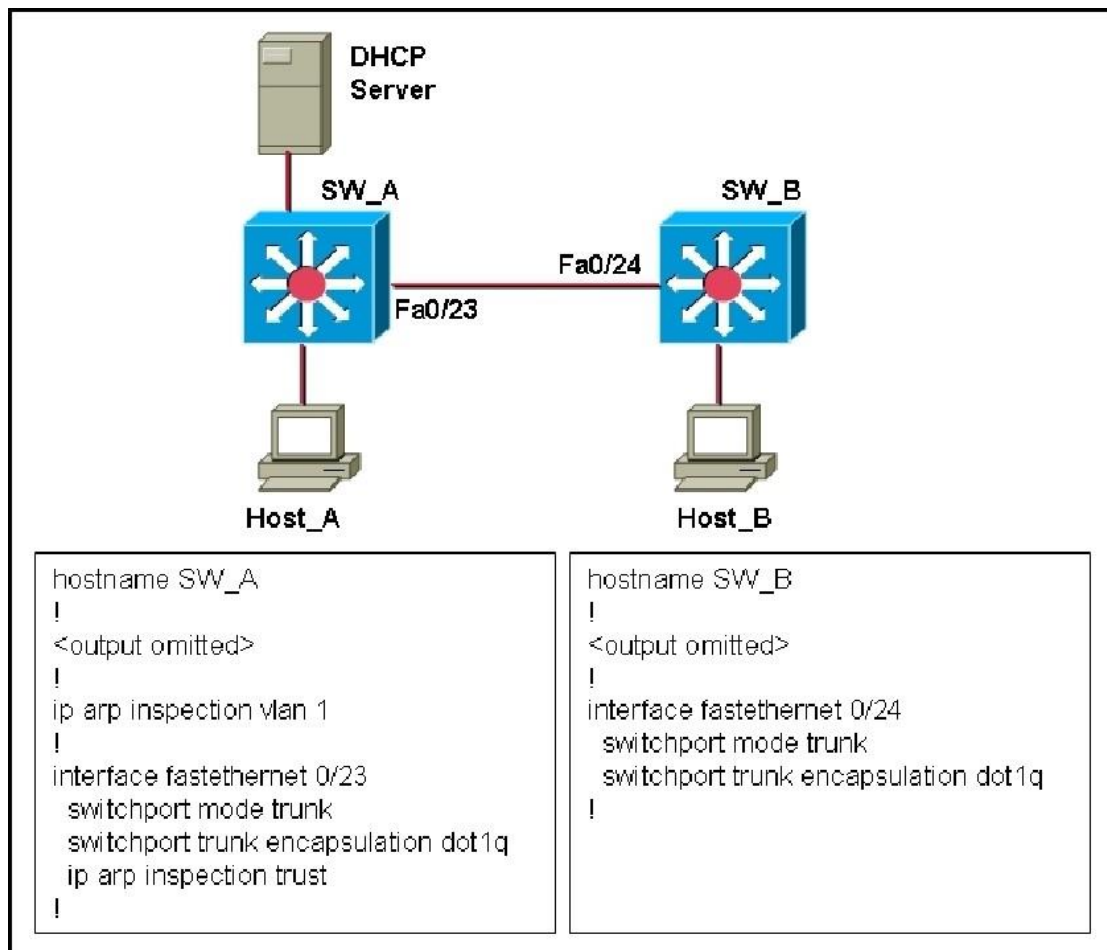
What does the command uddld reset accomplish?

- A. allows a UDLD port to automatically reset when it has been shut down
- B. resets all UDLD enabled ports that have been shut down
- C. removes all UDLD configurations from interfaces that were globally enabled
- D. removes all UDLD configurations from interfaces that were enabled per-port

**Correct Answer: B**

**QUESTION 8**

Refer to the exhibit. Dynamic ARP Inspection is enabled only on switch SW\_A. Host\_A and Host\_B acquire their IP addresses from the DHCP server connected to switch SW\_A. What would the outcome be if Host\_B initiated an ARP spoof attack toward Host\_A?



- A. The spoof packets are inspected at the ingress port of switch SW\_A and are permitted.
- B. The spoof packets are inspected at the ingress port of switch SW\_A and are dropped.
- C. The spoof packets are not inspected at the ingress port of switch SW\_A and are permitted.
- D. The spoof packets are not inspected at the ingress port of switch SW\_A and are dropped.

**Correct Answer: C**

**QUESTION 9**

Which statement is true about Layer 2 security threats?

- A. MAC spoofing, in conjunction with ARP snooping, is the most effective counter-measure against reconnaissance attacks that use Dynamic ARP Inspection to determine vulnerable attack points.
- B. DHCP snooping sends unauthorized replies to DHCP queries.
- C. ARP spoofing can be used to redirect traffic to counter Dynamic ARP Inspection.
- D. Dynamic ARP Inspection in conjunction with ARP spoofing can be used to counter DHCP snooping attacks.
- E. MAC spoofing attacks allow an attacking device to receive frames intended for a different network host.
- F. Port scanners are the most effective defense against Dynamic ARP Inspection.

**Correct Answer: E**

**QUESTION 10**

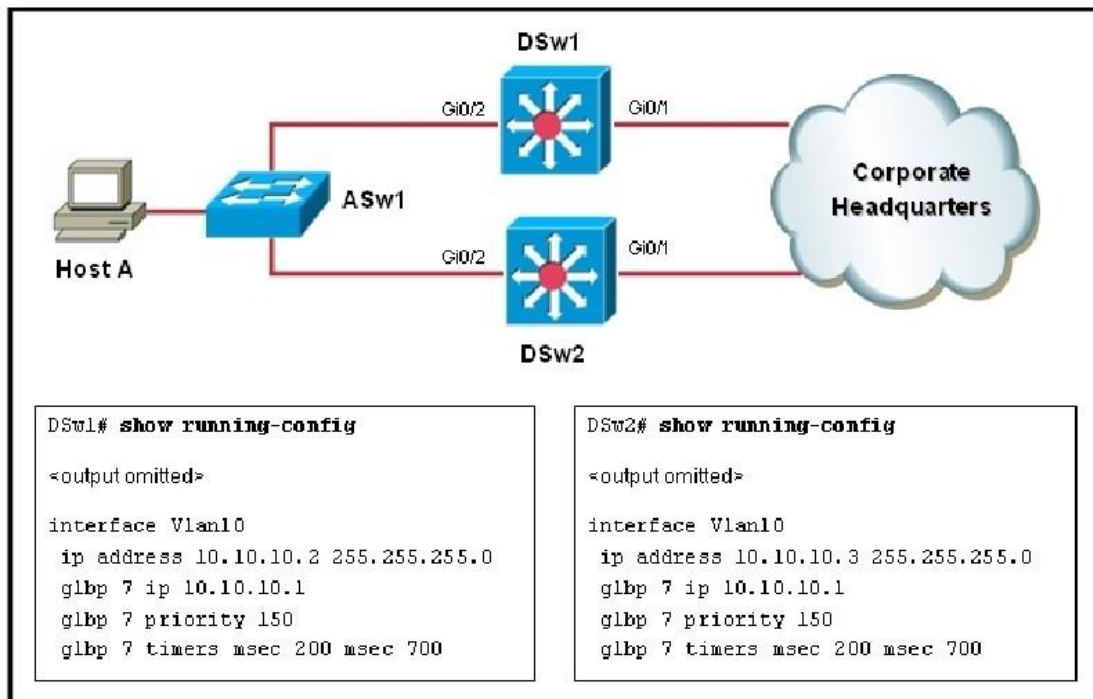
What does the global configuration command "ip arp inspection vlan 10-12,15" accomplish?

- A. validates outgoing ARP requests for interfaces configured on VLAN 10, 11, 12, or 15
- B. intercepts all ARP requests and responses on trusted ports
- C. intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings
- D. discards ARP packets with invalid IP-to-MAC address bindings on trusted ports

**Correct Answer: C**

**QUESTION 11**

Refer to the exhibit. Host A has sent an ARP message to the default gateway IP address 10.10.10.1. Which statement is true?



- A. Because of the invalid timers that are configured, DSw1 does not reply.
- B. DSw1 replies with the IP address of the next AVF.
- C. DSw1 replies with the MAC address of the next AVF.
- D. Because of the invalid timers that are configured, DSw2 does not reply.
- E. DSw2 replies with the IP address of the next AVF.
- F. DSw2 replies with the MAC address of the next AVF.

**Correct Answer: F**

**QUESTION 12**

What are two methods of mitigating MAC address flooding attacks? (Choose two.)

- A. Place unused ports in a common VLAN.
- B. Implement private VLANs.
- C. Implement DHCP snooping.
- D. Implement port security.
- E. Implement VLAN access maps.

**Correct Answer: DE**



**QUESTION 13**

Refer to the exhibit. What information can be derived from the output?

```
Switch#show spanning-tree inconsistentports
Name                Interface          Inconsistency
-----
VLAN0001            FastEthernet3/1   Port Type Inconsistent
VLAN0001            FastEthernet3/2   Port Type Inconsistent
VLAN1002            FastEthernet3/1   Port Type Inconsistent
VLAN1002            FastEthernet3/2   Port Type Inconsistent
VLAN1003            FastEthernet3/1   Port Type Inconsistent
VLAN1003            FastEthernet3/2   Port Type Inconsistent
VLAN1004            FastEthernet3/1   Port Type Inconsistent
VLAN1004            FastEthernet3/2   Port Type Inconsistent
VLAN1005            FastEthernet3/1   Port Type Inconsistent
VLAN1005            FastEthernet3/2   Port Type Inconsistent
Number of inconsistent ports (segments) in the system :10
```

- A. Interfaces FastEthernet3/1 and FastEthernet3/2 are connected to devices that are sending BPDUs with a superior root bridge parameter and no traffic is forwarded across the ports. After the sending of BPDUs has stopped, the interfaces must be shut down administratively, and brought back up, to resume normal operation.
- B. Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter, but traffic is still forwarded across the ports.
- C. Devices connected to interfaces FastEthernet3/1 and FastEthernet3/2 are sending BPDUs with a superior root bridge parameter and no traffic is forwarded across the ports. After the inaccurate BPDUs have been stopped, the interfaces automatically recover and resume normal operation.
- D. Interfaces FastEthernet3/1 and FastEthernet3/2 are candidates for becoming the STP root port, but neither can realize that role until BPDUs with a superior root bridge parameter are no longer received on at least one of the interfaces.

**Correct Answer: C**

**QUESTION 14**

What is one method that can be used to prevent VLAN hopping?

- A. Configure ACLs.
- B. Enforce username and password combinations.
- C. Configure all frames with two 802.1Q headers.
- D. Explicitly turn off DTP on all unused ports.
- E. Configure VACLs.

**Correct Answer: D**

**QUESTION 15**

Why is BPDU guard an effective way to prevent an unauthorized rogue switch from altering the spanning- tree topology of a network?

- A. BPDU guard can guarantee proper selection of the root bridge.
- B. BPDU guard can be utilized along with PortFast to shut down ports when a switch is connected to the port.
- C. BPDU guard can be utilized to prevent the switch from transmitting BPDUs and incorrectly altering the root bridge election.
- D. BPDU guard can be used to prevent invalid BPDUs from propagating throughout the network.

**Correct Answer: B**

**QUESTION 16**

What two steps can be taken to help prevent VLAN hopping? (Choose two.)

- A. Place unused ports in a common unrouted VLAN.
- B. Enable BPDU guard.
- C. Implement port security.
- D. Prevent automatic trunk configurations.
- E. Disable Cisco Discovery Protocol on ports where it is not necessary.

**Correct Answer: AD**

**QUESTION 17**

Refer to the exhibit. Assume that Switch\_A is active for the standby group and the standby device has only the default HSRP configuration. Which statement is true?

```
Switch_A(config-if)# ip address 10.10.10.1 255.255.255.0
Switch_A(config-if)# standby 1 priority 200
Switch_A(config-if)# standby 1 preempt
Switch_A(config-if)# standby 1 track interface fa 1/1
Switch_A(config-if)# standby 1 ip 10.10.10.10
```

- A. If port Fa1/1 on Switch\_A goes down, the standby device takes over as active.
- B. If the current standby device had the higher priority value, it would take over the role of active for the HSRP group.
- C. If port Fa1/1 on Switch\_A goes down, the new priority value for the switch would be 190.
- D. If Switch\_A had the highest priority number, it would not take over as active router.

**Correct Answer: C**

**QUESTION 18**

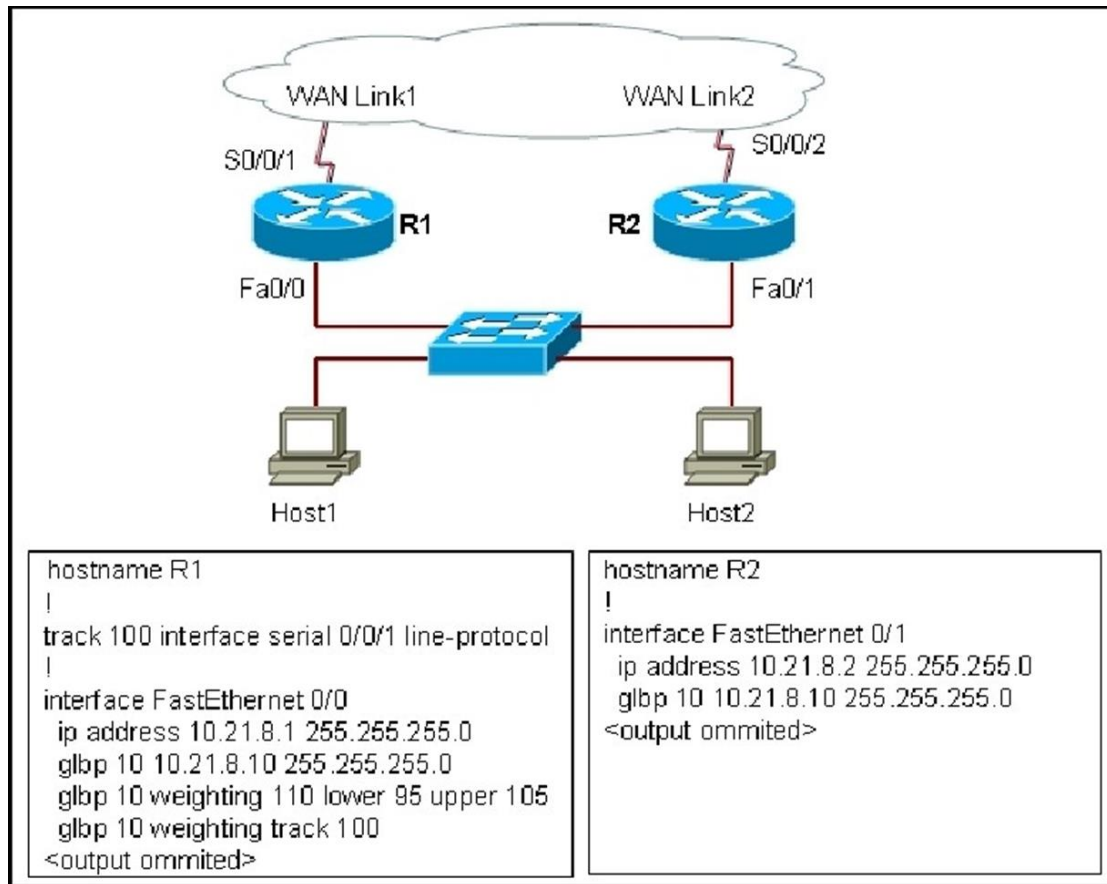
When an attacker is using switch spoofing to perform VLAN hopping, how is the attacker able to gather information?

- A. The attacking station uses DTP to negotiate trunking with a switch port and captures all traffic that is allowed on the trunk.
- B. The attacking station tags itself with all usable VLANs to capture data that is passed through the switch, regardless of the VLAN to which the data belongs.
- C. The attacking station generates frames with two 802.1Q headers to cause the switch to forward the frames to a VLAN that would be inaccessible to the attacker through legitimate means.
- D. The attacking station uses VTP to collect VLAN information that is sent out and then tags itself with the domain information to capture the data.

**Correct Answer: A**

**QUESTION 19**

Refer to the exhibit. GLBP has been configured on the network. When the interface serial0/0/1 on router R1 goes down, how is the traffic coming from Host1 handled?



- A. The traffic coming from Host1 and Host2 is forwarded through router R2 with no disruption.
- B. The traffic coming from Host2 is forwarded through router R2 with no disruption. Host1 sends an ARP request to resolve the MAC address for the new virtual gateway.
- C. The traffic coming from both hosts is temporarily interrupted while the switchover to make R2 active occurs.
- D. The traffic coming from Host2 is forwarded through router R2 with no disruption. The traffic from Host1 is dropped due to the disruption of the load balancing feature configured for the GLBP group.

**Correct Answer: A**

**QUESTION 20**

Refer to the exhibit. DHCP snooping is enabled for selected VLANs to provide security on the network. How do the switch ports handle the DHCP messages?

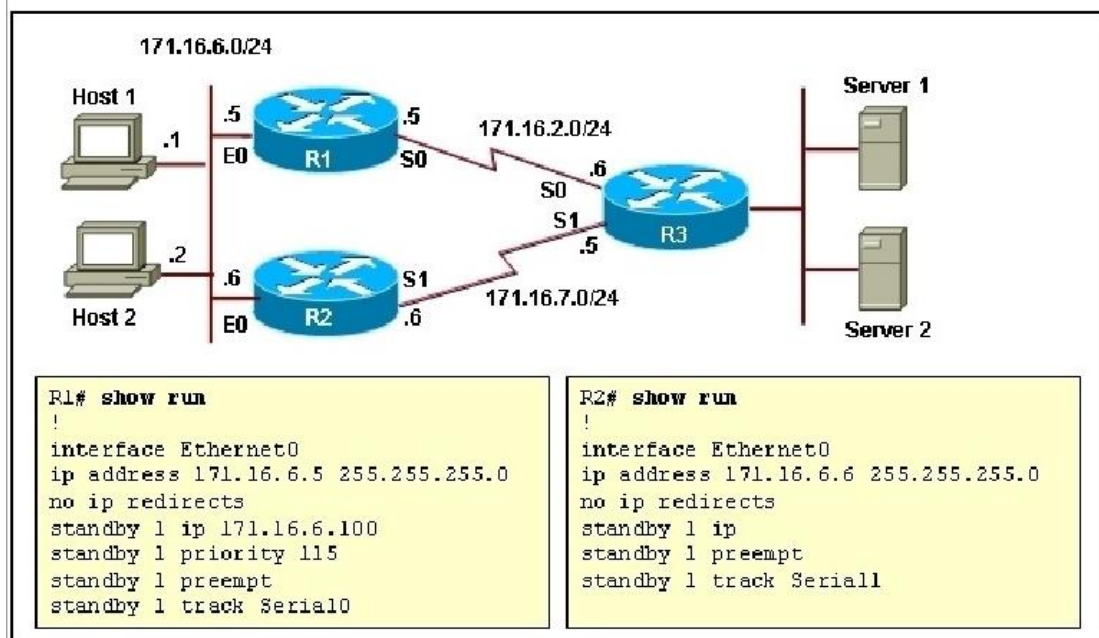
```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP Snooping is configured on the following VLANs:
 10 30-40 100 200-220
Insertion of option 82 information is enabled.
Interface           Trusted           Rate limit (pps)
-----
FastEthernet2/1     yes              none
FastEthernet2/2     yes              none
FastEthernet3/1     no               20
Switch#
```

- A. A DHCP OFFER packet from a DHCP server received on Ports Fa2/1 and Fa2/2 is dropped.
- B. A DHCP packet received on ports Fa2/1 and Fa2/2 is dropped if the source MAC address and the DHCP client hardware address does not match Snooping database.
- C. A DHCP packet received on ports Fa2/1 and Fa2/2 is forwarded without being tested.
- D. A DHCP RELEASE message received on ports Fa2/1 and Fa2/2 has a MAC address in the DHCP snooping binding database, but the interface information in the binding database does not match the interface on which the message was received and is dropped.

**Correct Answer: C**

**QUESTION 21**

Refer to the exhibit and the partial configuration on routers R1 and R2. HSRP is configured on the network to provide network redundancy for the IP traffic. The network administrator noticed that R2 does not become active when the R1 serial0 interface goes down. What should be changed in the configuration to fix the problem?



- A. R2 should be configured with an HSRP virtual address.
- B. R2 should be configured with a standby priority of 100.
- C. The Serial0 interface on router R2 should be configured with a decrement value of 20.
- D. The Serial0 interface on router R1 should be configured with a decrement value of 20.

**Correct Answer: D**

**QUESTION 22**

Which optional feature of an Ethernet switch disables a port on a point-to-point link if the port does not receive traffic while Layer 1 status is up?

- A. BackboneFast
- B. UplinkFast
- C. Loop Guard
- D. UDLD aggressive mode
- E. Fast Link Pulse bursts
- F. Link Control Word

**Correct Answer: D**

**QUESTION 23**

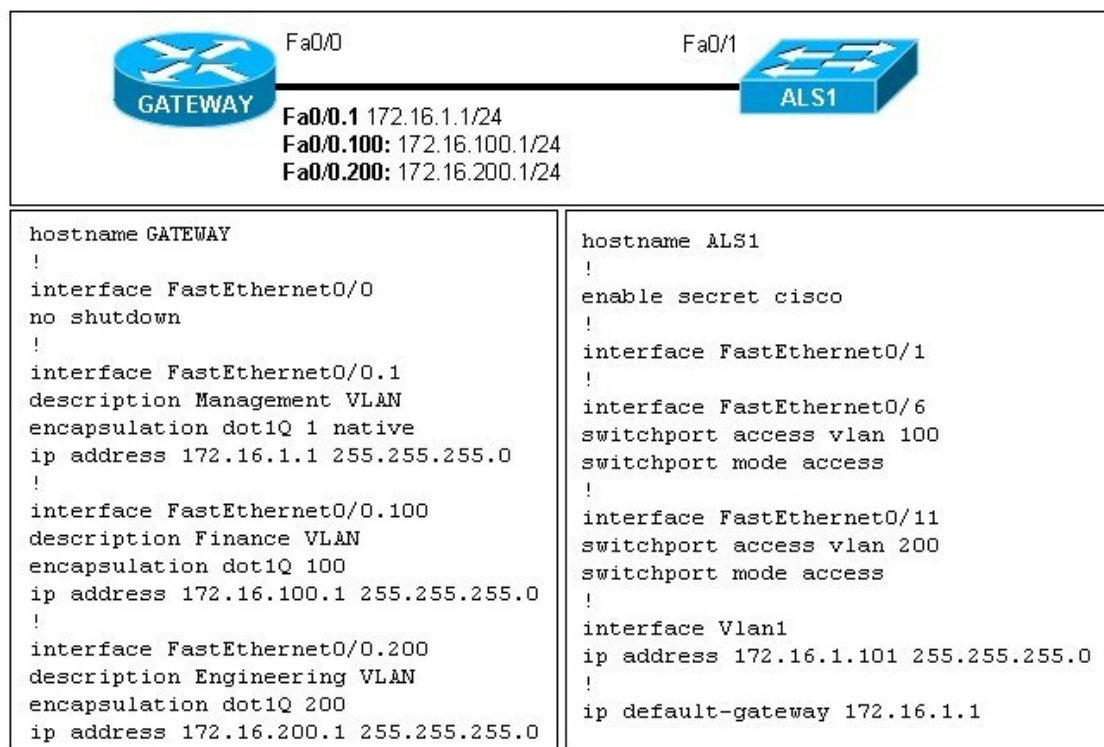
Which three statements about routed ports on a multilayer switch are true? (Choose three.)

- A. A routed port can support VLAN subinterfaces.
- B. A routed port takes an IP address assignment.
- C. A routed port can be configured with routing protocols.
- D. A routed port is a virtual interface on the multilayer switch.
- E. A routed port is associated only with one VLAN.
- F. A routed port is a physical interface on the multilayer switch.

**Correct Answer: BCF**

**QUESTION 24**

Refer to the exhibit. Why are users from VLAN 100 unable to ping users on VLAN 200?



- A. Encapsulation on the switch is wrong.
- B. Trunking must be enabled on Fa0/1.
- C. The native VLAN is wrong.
- D. VLAN 1 needs the no shutdown command.
- E. IP routing must be enabled on the switch.

**Correct Answer: B**

**QUESTION 25**

Which three statements about Dynamic ARP Inspection are true? (Choose three.)

- A. It determines the validity of an ARP packet based on the valid MAC address-to-IP address bindings stored in the DHCP snooping database.
- B. It forwards all ARP packets received on a trusted interface without any checks.
- C. It determines the validity of an ARP packet based on the valid MAC address-to-IP address bindings stored in the CAM table.
- D. It forwards all ARP packets received on a trusted interface after verifying and inspecting the packet against the Dynamic ARP Inspection table.
- E. It intercepts all ARP packets on untrusted ports.
- F. It is used to prevent against a DHCP snooping attack.

**Correct Answer: ABE**

**QUESTION 26**

A network administrator wants to configure 802.1x port-based authentication, however, the client workstation is not 802.1x compliant. What is the only supported authentication server that can be used?

- A. TACACS with LEAP extensions
- B. TACACS+
- C. RADIUS with EAP extensions
- D. LDAP

**Correct Answer: C**

**QUESTION 27**

The following command was issued on a router that is being configured as the active HSRP router.

```
standby ip 10.2.1.1
```

Which statement about this command is true?

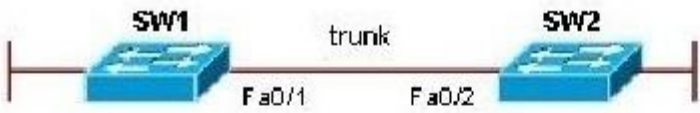
- A. This command will not work because the HSRP group information is missing.
- B. The HSRP MAC address will be 0000.0c07.ac00.
- C. The HSRP MAC address will be 0000.0c07.ac01.
- D. The HSRP MAC address will be 0000.070c.ac11.
- E. This command will not work because the active parameter is missing.

**Correct Answer: B**



**QUESTION 28**

Refer to the exhibit. The link between switch SW1 and switch SW2 is configured as a trunk, but the trunk failed to establish connectivity between the switches. Based on the configurations and the error messages received on the console of SW1, what is the cause of the problem?



```

SW1(config)#interface fa0/1
SW1(config-if)switchport trunk encapsulation dot1q 1 native
SW1(config-if)switchport mode trunk
SW1(config-if)#switchport trunk allowed vlan all
SW1(config-if)#exit

SW2(config)#interface fa0/2
SW2(config-if)switchport trunk encapsulation dot1q 2 native
SW2(config-if)switchport mode trunk
SW2(config-if)#switchport trunk allowed vlan all
SW2(config-if)#exit

```

**SW1 Console Messages**

```

2006 Dec 07 16:31:24 %SPANTRIEE-2-RX_IQPVIDERR: Rcvd
pvid_inc BPDU on IQ port 0/1 vlan 1.
2006 Dec 07 16:31:24 %SPANTRIEE-2-TX_BLKPORTPWID: Block 0/1
on xmting vlan 2 for inc peer vlan.
2006 Dec 07 16:31:24 %SPANTRIEE-2-RX_BLKPORTPWID: Block 0/1
on rcving vlan 1 for inc peer vlan 2.

```

- A. The two ends of the trunk have different duplex settings.
- B. The two ends of the trunk have different EtherChannel configurations.
- C. The two ends of the trunk have different native VLAN configurations.
- D. The two ends of the trunk allow different VLANs on the trunk.

**Correct Answer: C**

**QUESTION 29**

A campus infrastructure supports wireless clients via Cisco Aironet AG Series 1230, 1240, and 1250 access points. With DNS and DHCP configured, the 1230 and 1240 access points appear to boot and operate normally. However, the 1250 access points do not seem to operate correctly. What is the most likely cause of this problem?

- A. DHCP with option 150
- B. DHCP with option 43

- C. PoE
- D. DNS
- E. switch port does not support gigabit speeds

**Correct Answer: C**

**QUESTION 30**

A standalone wireless AP solution is being installed into the campus infrastructure. The access points appear to boot correctly, but wireless clients are not obtaining correct access. You verify that this is the local switch configuration connected to the access point:

```
interface ethernet 0/1
switchport access vlan 10
switchport mode access
spanning-tree portfast
mls qos trust dscp
```

What is the most likely cause of the problem?

- A. QoS trust should not be configured on a port attached to a standalone AP.
- B. QoS trust for switchport mode access should be defined as "cos".
- C. switchport mode should be defined as "trunk" with respective QoS.
- D. switchport access vlan should be defined as "1".

**Correct Answer: C**

## EnsurePass.com Members Features:

1. Verified Answers researched by industry experts.
2. Q&As are downloadable in PDF and VCE format.
3. 98% success Guarantee and **Money Back** Guarantee.
4. Free updates for **180** Days.
5. **Instant Access to download the Items**

View list of All Exam provided:

<http://www.ensurepass.com/certifications?index=A>

To purchase Lifetime Full Access Membership click here:

<http://www.ensurepass.com/user/register>

**Valid Discount Code for 2015: JREH-G1A8-XHC6**

To purchase the HOT Exams:

<u>Cisco</u>		<u>CompTIA</u>		<u>Oracle</u>	<u>VMWare</u>	<u>IBM</u>
<a href="#"><u>100-101</u></a>	<a href="#"><u>640-554</u></a>	<a href="#"><u>220-801</u></a>	<a href="#"><u>LX0-101</u></a>	<a href="#"><u>1Z0-051</u></a>	<a href="#"><u>VCAD510</u></a>	<a href="#"><u>C2170-011</u></a>
<a href="#"><u>200-120</u></a>	<a href="#"><u>200-101</u></a>	<a href="#"><u>220-802</u></a>	<a href="#"><u>N10-005</u></a>	<a href="#"><u>1Z0-052</u></a>	<a href="#"><u>VCP510</u></a>	<a href="#"><u>C2180-319</u></a>
<a href="#"><u>300-206</u></a>	<a href="#"><u>640-911</u></a>	<a href="#"><u>BR0-002</u></a>	<a href="#"><u>SG0-001</u></a>	<a href="#"><u>1Z0-053</u></a>	<a href="#"><u>VCP550</u></a>	<a href="#"><u>C4030-670</u></a>
<a href="#"><u>300-207</u></a>	<a href="#"><u>640-916</u></a>	<a href="#"><u>CAS-001</u></a>	<a href="#"><u>SG1-001</u></a>	<a href="#"><u>1Z0-060</u></a>	<a href="#"><u>VCAC510</u></a>	<a href="#"><u>C4040-221</u></a>
<a href="#"><u>300-208</u></a>	<a href="#"><u>640-864</u></a>	<a href="#"><u>CLO-001</u></a>	<a href="#"><u>SK0-003</u></a>	<a href="#"><u>1Z0-474</u></a>	<a href="#"><u>VCP5-DCV</u></a>	<a href="#"><u>RedHat</u></a>
<a href="#"><u>350-018</u></a>	<a href="#"><u>642-467</u></a>	<a href="#"><u>ISS-001</u></a>	<a href="#"><u>SY0-301</u></a>	<a href="#"><u>1Z0-482</u></a>	<a href="#"><u>VCP510PSE</u></a>	<a href="#"><u>EX200</u></a>
<a href="#"><u>352-001</u></a>	<a href="#"><u>642-813</u></a>	<a href="#"><u>JK0-010</u></a>	<a href="#"><u>SY0-401</u></a>	<a href="#"><u>1Z0-485</u></a>		<a href="#"><u>EX300</u></a>
<a href="#"><u>400-101</u></a>	<a href="#"><u>642-832</u></a>	<a href="#"><u>JK0-801</u></a>	<a href="#"><u>PK0-003</u></a>	<a href="#"><u>1Z0-580</u></a>		
<a href="#"><u>640-461</u></a>	<a href="#"><u>642-902</u></a>			<a href="#"><u>1Z0-820</u></a>		

