

**300-115.prepaway.premium.exam.921q**

Number: 300-115  
Passing Score: 800  
Time Limit: 120 min  
File Version: 24.0



**300-115**

**Implementing Cisco IP Switched Networks**

**Version 24.0**

**Sections**

1. Layer 2 Technologies
2. Infrastructure Security
3. Infrastructure Services
4. Mix Questions

## Exam A

### QUESTION 1

What is the maximum number of switches that can be stacked using Cisco StackWise?

- A. 4
- B. 5
- C. 8
- D. 9
- E. 10
- F. 13

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Up to 9 Cisco Catalyst switches can be stacked together to build single logical StackWise switch since Cisco IOS XE Release 3.3.0SE. Prior to Cisco IOS XE Release 3.3.0SE, up to 4 Cisco Catalyst switches could be stacked together.

Reference: [http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/qa\\_c67-722110.html](http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3850-series-switches/qa_c67-722110.html)

### QUESTION 2

A network engineer wants to add a new switch to an existing switch stack. Which configuration must be added to the new switch before it can be added to the switch stack?

- A. No configuration must be added.
- B. stack ID
- C. IP address
- D. VLAN information
- E. VTP information

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Switch Stack Offline Configuration

You can use the offline configuration feature to *provision* (to supply a configuration to) a new switch before it joins the switch stack. You can configure in advance the stack member number, the switch type, and the interfaces associated with a switch that is not currently part of the stack. The configuration that you create on the switch stack is called the *provisioned configuration*. The switch that is added to the switch stack and that receives this configuration is called the *provisioned switch*.

You manually create the provisioned configuration through the **switch stack-member-number provision type** global configuration command. The provisioned configuration is automatically created when a switch is added to a switch stack and when no provisioned configuration exists.

When you configure the interfaces associated with a provisioned switch (for example, as part of a VLAN), the switch stack accepts the configuration, and the information appears in the running configuration. The interface associated with the provisioned switch is not active, operates as if it is administratively shut down, and the **no shutdown** interface configuration command does not return it to active service. The interface associated with the provisioned switch does not appear in the display of the specific feature; for example, it does not appear in the **show vlan** user EXEC command output.

The switch stack retains the provisioned configuration in the running configuration whether or not the provisioned switch is part of the stack. You can save the provisioned configuration to the startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. The startup configuration file ensures that the switch stack can reload and can use the saved information whether or not the provisioned switch is part of the switch stack.

Effects of Adding a Provisioned Switch to a Switch Stack

When you add a provisioned switch to the switch stack, the stack applies either the provisioned configuration or the default configuration. [Table 5-1](#) lists the events that occur when the switch stack compares the provisioned configuration with the provisioned switch.

| Table 5-1 Results of Comparing the Provisioned Configuration with the Provisioned Switch         |                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                        |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scenario                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                   | Result                                                                                                                                                                                 |
| The stack member numbers and the switch types match.                                             | 1. If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and<br>2. If the switch type of the provisioned switch matches the switch type in the provisioned configuration on the stack.                                                                                                                                              | The switch stack applies the provisioned configuration to the provisioned switch and adds it to the stack.                                                                             |
| The stack member numbers match but the switch types do not match.                                | 1. If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but<br>2. The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack.                                                                                                                                          | The switch stack applies the default configuration to the provisioned switch and adds it to the stack.<br>The provisioned configuration is changed to reflect the new information.     |
| The stack member number is not found in the provisioned configuration.                           |                                                                                                                                                                                                                                                                                                                                                                                                                   | The switch stack applies the default configuration to the provisioned switch and adds it to the stack.<br>The provisioned configuration is changed to reflect the new information.     |
| The stack member number of the provisioned switch is in conflict with an existing stack member.  | The stack master assigns a new stack member number to the provisioned switch.<br>The stack member numbers and the switch types match:<br>1. If the new stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and<br>2. If the switch type of the provisioned switch matches the switch type in the provisioned configuration on the stack. | The switch stack applies the provisioned configuration to the provisioned switch and adds it to the stack.<br>The provisioned configuration is changed to reflect the new information. |
|                                                                                                  | The stack member numbers match, but the switch types do not match:<br>1. If the stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, but<br>2. The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the stack.                                                                    | The switch stack applies the default configuration to the provisioned switch and adds it to the stack.<br>The provisioned configuration is changed to reflect the new information.     |
| The stack member number of the provisioned switch is not found in the provisioned configuration. |                                                                                                                                                                                                                                                                                                                                                                                                                   | The switch stack applies the default configuration to the provisioned switch and adds it to the stack.                                                                                 |

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstack.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html)

### QUESTION 3

What percentage of bandwidth is reduced when a stack cable is broken?

- A. 0
- B. 25
- C. 50
- D. 75
- E. 100

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

#### Physical Sequential Linkage

The switches are physically connected sequentially, as shown in Figure 3. A break in any one of the cables will result in the stack bandwidth being reduced to half of its full capacity. Subsecond timing mechanisms detect traffic problems and immediately institute failover. This mechanism restores dual path flow when the timing mechanisms detect renewed activity on the cable.

**Figure 3.** Cisco StackWise Technology Resilient Cabling

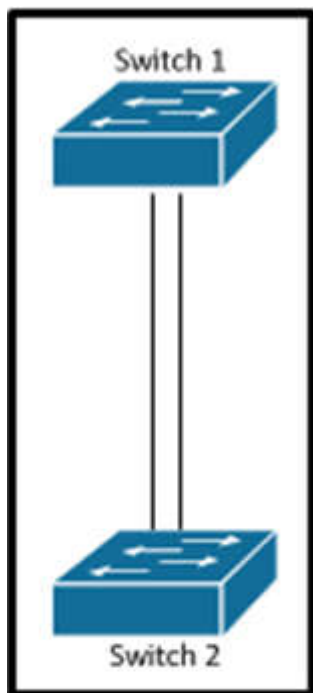


Reference: [http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod\\_white\\_paper09186a00801b096a.html](http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod_white_paper09186a00801b096a.html)

### QUESTION 4



Refer to the exhibit.



Which set of configurations will result in all ports on both switches successfully bundling into an EtherChannel?

- A. switch1  
channel-group 1 mode active  
switch2  
channel-group 1 mode auto
- B. switch1  
channel-group 1 mode desirable  
switch2  
channel-group 1 mode passive
- C. switch1  
channel-group 1 mode on  
switch2  
channel-group 1 mode auto
- D. switch1  
channel-group 1 mode desirable  
switch2  
channel-group 1 mode auto

**Correct Answer: D**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

The different etherchannel modes are described in the table below:

| Mode      | Description                                                                                                                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| active    | Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending LACP packets.                                                                                         |
| auto      | Places an interface into a passive negotiating state, in which the interface responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.                  |
| desirable | Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending PAgP packets.                                                                                         |
| on        | Forces the interface into an EtherChannel without PAgP or LACP. With the <b>on</b> mode, a usable EtherChannel exists only when an interface group in the <b>on</b> mode is connected to another interface group in the <b>on</b> mode. |
| passive   | Places an interface into a passive negotiating state, in which the interface responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.            |

Both the auto and desirable PAgP modes allow interfaces to negotiate with partner interfaces to determine if they can form an EtherChannel based on criteria such as interface speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.

Interfaces can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:

- An interface in the desirable mode can form an EtherChannel with another interface that is in the desirable or auto mode.
- An interface in the auto mode can form an EtherChannel with another interface in the desirable mode.

An interface in the auto mode cannot form an EtherChannel with another interface that is also in the auto mode because neither interface starts PAgP negotiation.

An interface in the on mode that is added to a port channel is forced to have the same characteristics as the already existing on mode interfaces in the channel.

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/20ew/configuration/guide/config/channel.html>

**QUESTION 5**

Refer to the exhibit.



```

interface GigabitEthernet0/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 1-100
!
interface GigabitEthernet0/48
  switchport
  switchport mode access
!
monitor session 1 source interface GigabitEthernet0/1
monitor session 1 destination interface GigabitEthernet0/48

```

How can the traffic that is mirrored out the GigabitEthernet0/48 port be limited to only traffic that is received or transmitted in VLAN 10 on the GigabitEthernet0/1 port?

- A. Change the configuration for GigabitEthernet0/48 so that it is a member of VLAN 10.
- B. Add an access list to GigabitEthernet0/48 to filter out traffic that is not in VLAN 10.
- C. Apply the monitor session filter globally to allow only traffic from VLAN 10.
- D. Change the monitor session source to VLAN 10 instead of the physical interface.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the monitor session filter global configuration command.

**Usage Guidelines**

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack.

You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [ , | -] options.

If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen ( - ).

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports.

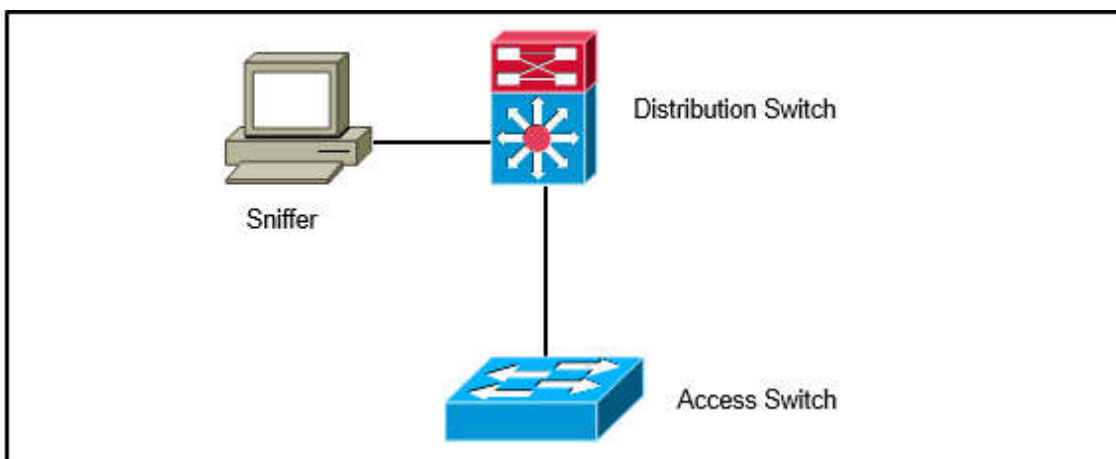
You can use the monitor session session\_number filter vlan vlan-id command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/network\\_management/command\\_reference/b\\_nm\\_3se\\_3850\\_cr/b\\_nm\\_3se\\_3850\\_cr\\_chapter\\_010.html#wp3875419997](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/network_management/command_reference/b_nm_3se_3850_cr/b_nm_3se_3850_cr_chapter_010.html#wp3875419997)

## QUESTION 6

Refer to the exhibit.



A network engineer wants to analyze all incoming and outgoing packets for an interface that is connected to an access switch. Which three items must be configured to mirror traffic to a packet sniffer that is connected to the distribution switch? (Choose three.)

- A. A monitor session on the distribution switch with a physical interface as the source and the remote SPAN VLAN as the destination
- B. A remote SPAN VLAN on the distribution and access layer switch
- C. A monitor session on the access switch with a physical interface source and the remote SPAN VLAN as the destination
- D. A monitor session on the distribution switch with a remote SPAN VLAN as the source and physical interface as the destination
- E. A monitor session on the access switch with a remote SPAN VLAN source and the physical interface as the destination
- F. A monitor session on the distribution switch with a physical interface as the source and a physical interface as the destination

**Correct Answer: BCD**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis.

RSPAN supports source ports, source VLANs, and destination ports on different switches (or different switch stacks), enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swspan.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html)

#### QUESTION 7

After an EtherChannel is configured between two Cisco switches, interface port channel 1 is in the down/down state. Switch A is configured with channel-group 1 mode active, while Switch B is configured with channel-group 1 mode desirable. Why is the EtherChannel bundle not working?

- A. The switches are using mismatched EtherChannel negotiation modes.
- B. The switch ports are not configured in trunking mode.
- C. LACP priority must be configured on both switches.
- D. The channel group identifier must be different for Switch A and Switch B.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Here we have a situation where one switch is using active mode, which is an LACP mode, and the other is using desirable, which is a PAGP mode. You can not mix the LACP and PAGP protocols to form an etherchannel. Here is a summary of the various etherchannel modes:

| EtherChannel PagP Modes |                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mode                    | Description                                                                                                                                                                                                                                                                                                                                         |
| auto                    | Places a port into a passive negotiating state, in which the port responds to PagP packets it receives but does not start PagP packet negotiation. This setting minimizes the transmission of PagP packets.<br>This mode is not supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel). |
| Desirable               | Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PagP packets.<br>This mode is not supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).                                                                             |

| EtherChannel LACP Modes |                                                                                                                                                                                                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mode                    | Description                                                                                                                                                                                                      |
| active                  | Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.                                                                                   |
| Passive                 | Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets. |

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_55\\_se/configuration/guide/scg\\_2960/swethchl.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swethchl.html)

#### QUESTION 8

An EtherChannel bundle has been established between a Cisco switch and a corporate web server. The network administrator noticed that only one of the EtherChannel links is being utilized to reach the web server.

What should be done on the Cisco switch to allow for better EtherChannel utilization to the corporate web server?

- A. Enable Cisco Express Forwarding to allow for more effective traffic sharing over the EtherChannel bundle.
- B. Adjust the EtherChannel load-balancing method based on destination IP addresses.
- C. Disable spanning tree on all interfaces that are participating in the EtherChannel bundle.
- D. Use link-state tracking to allow for improved load balancing of traffic upon link failure to the server.
- E. Adjust the EtherChannel load-balancing method based on source IP addresses.

**Correct Answer: E**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

EtherChannel load balancing can use MAC addresses, IP addresses, or Layer 4 port numbers, and either source mode, destination mode, or both. The mode you select applies to all EtherChannels that you configure on the switch. Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel only goes to a single MAC address (which is the case in this example, since all traffic is going to the same web server), use of the destination MAC address results in the choice of the same link in the channel each time. Use of source addresses or IP addresses can result in a better load balance.

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html>

#### QUESTION 9

Interface FastEthernet0/1 is configured as a trunk interface that allows all VLANs. This command is configured globally:

monitor session 2 filter vlan 1 – 8, 39, 52

What is the result of the implemented command?

- A. All VLAN traffic is sent to the SPAN destination interface.
- B. Traffic from VLAN 4 is not sent to the SPAN destination interface.
- C. Filtering a trunked SPAN port effectively disables SPAN operations for all VLANs.
- D. The trunk's native VLAN must be changed to something other than VLAN 1.
- E. Traffic from VLANs 1 to 8, 39, and 52 is replicated to the SPAN destination port.

**Correct Answer: E**

**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

The "monitor session filter" command is used to specify which VLANs are to be port mirrored using SPAN. This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the SPAN source is a trunk interface:  
Switch(config)# monitor session 2 filter vlan 1 – 5 , 9

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/span.html/index.html#wp1066836>

**QUESTION 10**

A network engineer notices inconsistent Cisco Discovery Protocol neighbors according to the diagram that is provided. The engineer notices only a single neighbor that uses Cisco Discovery Protocol, but it has several routing neighbor relationships.

What would cause the output to show only the single neighbor?

- A. The routers are connected via a Layer 2 switch.
- B. IP routing is disabled on neighboring devices.
- C. Cisco Express Forwarding is enabled locally.
- D. Cisco Discovery Protocol advertisements are inconsistent between the local and remote devices.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

If all of the routers are connected to each other using a layer 2 switch, then each router will only have the single switch port that it connects to as its neighbor. Even though multiple routing neighbors can be formed over a layer 2 network, only the physical port that it connects to will be seen as a CDP neighbor. CDP can be used to determine the physical topology, but not necessarily the logical topology.

**QUESTION 11**

After the implementation of several different types of switches from different vendors, a network engineer notices that directly connected devices that use Cisco Discovery Protocol are not visible.

Which vendor-neutral protocol could be used to resolve this issue?

- A. Local Area Mobility
- B. Link Layer Discovery Protocol
- C. NetFlow
- D. Directed Response Protocol

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol (CDP).

Reference: [http://en.wikipedia.org/wiki/Link\\_Layer\\_Discovery\\_Protocol](http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol)

**QUESTION 12**

Several new switches have been added to the existing network as VTP clients. All of the new switches have been configured with the same VTP domain, password, and version. However, VLANs are not passing from the VTP server (existing network) to the VTP clients.

What must be done to fix this?

- A. Remove the VTP domain name from all switches with "null" and then replace it with the new domain name.
- B. Configure a different native VLAN on all new switches that are configured as VTP clients.
- C. Provision one of the new switches to be the VTP server and duplicate information from the existing network.
- D. Ensure that all switch interconnects are configured as trunks to allow VTP information to be transferred.

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP allows switches to advertise VLAN information between other members of the same VTP domain. VTP allows a consistent view of the switched network across all switches. There are several reasons why the VLAN information can fail to be exchanged.

Verify these items if switches that run VTP fail to exchange VLAN information:

- **VTP information only passes through a trunk port. Make sure that all ports that interconnect switches are configured as trunks and are actually trunking.**

Make sure that if EtherChannels are created between two switches, only Layer 2 EtherChannels propagate VLAN information.

- Make sure that the VLANs are active in all the devices.
- One of the switches must be the VTP server in a VTP domain. All VLAN changes must be done on this switch in order to have them propagated to the VTP clients.
- The VTP domain name must match and it is case sensitive. CISCO and cisco are two different domain names.
- Make sure that no password is set between the server and client. If any password is set, make sure that the password is the same on both sides.

Reference: [http://www.cisco.com/en/US/tech/tk389/tk689/technologies\\_tech\\_note09186a0080890613.shtml](http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml)



**QUESTION 13**

After implementing VTP, the extended VLANs are not being propagated to other VTP switches. What should be configured for extended VLANs?

- A. VTP does not support extended VLANs and should be manually added to all switches.
- B. Enable VTP version 3, which supports extended VLAN propagation.
- C. VTP authentication is required when using extended VLANs because of their ability to cause network instability.
- D. Ensure that all switches run the same Cisco IOS version. Extended VLANs will not propagate to different IOS versions when extended VLANs are in use.

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

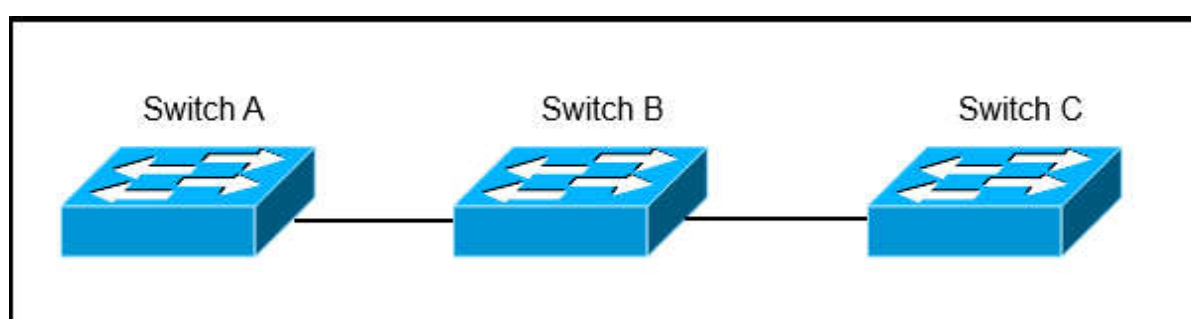
Explanation:

- VTP version 1 and VTP version 2 do not propagate configuration information for extended-range VLANs (VLAN numbers 1006 to 4094). You must configure extended-range VLANs manually on each network device.
- VTP version 3 supports extended-range VLANs (VLAN numbers 1006 to 4094). If you convert from VTP version 3 to VTP version 2, the VLANs in the range 1006 to 4094 are removed from VTP control.

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config\\_guide/sup2T/vtp.pdf](http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/15.1SY/config_guide/sup2T/vtp.pdf)

**QUESTION 14**

Refer to the exhibit.



Switch A, B, and C are trunked together and have been properly configured for VTP. Switch C receives VLAN information from the VTP server Switch A, but Switch B does not receive any VLAN information. What is the most probable cause of this behavior?

- A. Switch B is configured in transparent mode.
- B. Switch B is configured with an access port to Switch A, while Switch C is configured with a trunk port to Switch B.
- C. The VTP revision number of the Switch B is higher than that of Switch A.
- D. The trunk between Switch A and Switch B is misconfigured.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

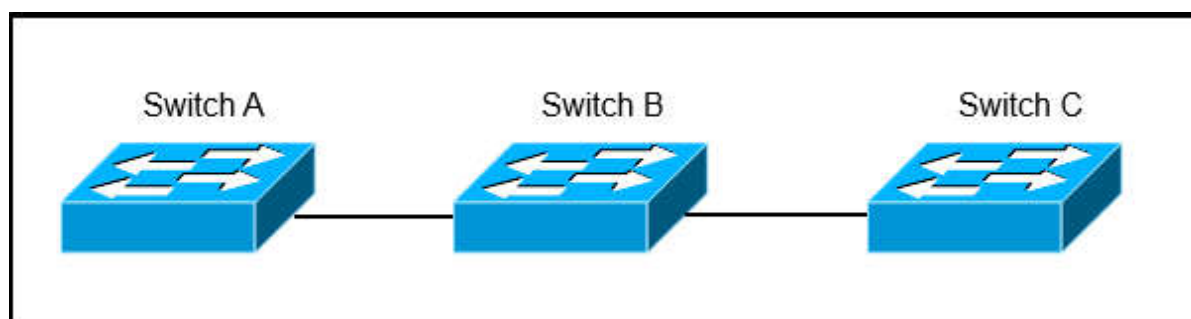
Explanation:

VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2.

Reference: [http://www.cisco.com/en/US/tech/tk389/tk689/technologies\\_tech\\_note09186a0080094c52.shtml](http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080094c52.shtml)

**QUESTION 15**

Refer to the exhibit.



Switch A, B, and C are trunked together and have been properly configured for VTP. Switch B has all VLANs, but Switch C is not receiving traffic from certain VLANs. What would cause this issue?

- A. A VTP authentication mismatch occurred between Switch A and Switch B.
- B. The VTP revision number of Switch B is higher than that of Switch A.
- C. VTP pruning is configured globally on all switches and it removed VLANs from the trunk interface that is connected to Switch C.
- D. The trunk between Switch A and Switch B is misconfigured.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving

switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. The best explanation for why switch C is not seeing traffic from only some of the VLANs, is that VTP pruning has been configured.

#### QUESTION 16

After the recent upgrade of the switching infrastructure, the network engineer notices that the port roles that were once “blocking” are now defined as “alternate” and “backup.” What is the reason for this change?

- A. The new switches are using RSTP instead of legacy IEEE 802.1D STP.
- B. IEEE 802.1D STP and PortFast have been configured by default on all newly implemented Cisco Catalyst switches.
- C. The administrator has defined the switch as the root in the STP domain.
- D. The port roles have been adjusted based on the interface bandwidth and timers of the new Cisco Catalyst switches.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.

RSTP bridge port roles:

\* Root port – A forwarding port that is the closest to the root bridge in terms of path cost

\* Designated port – A forwarding port for every LAN segment

\* Alternate port – A best alternate path to the root bridge. This path is different than using the root port. The alternative port moves to the forwarding state if there is a failure on the designated port for the segment.

\* Backup port – A backup/redundant path to a segment where another bridge port already connects. The backup port applies only when a single switch has two links to the same segment (collision domain). To have two links to the same collision domain, the switch must be attached to a hub.

\* Disabled port – Not strictly part of STP, a network administrator can manually disable a port

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>

#### QUESTION 17

An administrator recently configured all ports for rapid transition using PortFast. After testing, it has been determined that several ports are not transitioning as they should.

What is the reason for this?

- A. RSTP has been enabled per interface and not globally.
- B. The STP root bridge selection is forcing key ports to remain in non-rapid transitioning mode.
- C. STP is unable to achieve rapid transition for trunk links.
- D. The switch does not have the processing power to ensure rapid transition for all ports.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

RSTP can only achieve rapid transition to the forwarding state on edge ports and on point-to-point links, not on trunk links. The link type is automatically derived from the duplex mode of a port. A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port by default. This automatic link type setting can be overridden by explicit configuration. In switched networks today, most links operate in full-duplex mode and are treated as point-to-point links by RSTP. This makes them candidates for rapid transition to the forwarding state.

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/24062-146.html>

#### QUESTION 18

Which technique automatically limits VLAN traffic to only the switches that require it?

- A. access lists
- B. DTP in nonegotiate
- C. VTP pruning
- D. PBR

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets to only the switches that require it. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vtp.html#wp1020444>

#### QUESTION 19

What effect does the mac address-table aging-time 180 command have on the MAC address-table?

- A. This is how long a dynamic MAC address will remain in the CAM table.
- B. The MAC address-table will be flushed every 3 minutes.
- C. The default timeout period will be 360 seconds.
- D. ARP requests will be processed less frequently by the switch.
- E. The MAC address-table will hold addresses 180 seconds longer than the default of 10 minutes.

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

You can configure the amount of time that an entry (the packet source MAC address and port that packet ingresses) remain in the MAC table. To configure the aging time for all MAC addresses, perform this task:

|         | Command                                                                          | Purpose                                                                                                                                                                                                                                                                     |
|---------|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1, | <code>switch# configure terminal</code>                                          | Enters configuration mode.                                                                                                                                                                                                                                                  |
| Step 2, | <code>switch(config)# mac-address-table aging-time seconds [vlan vlan_id]</code> | Specifies the time before an entry ages out and is discarded from the MAC address table. The range is from 0 to 1000000; the default is 300 seconds. Entering the value 0 disables the MAC aging. If a VLAN is not specified, the aging specification applies to all VLANs. |

This example shows how to set the aging time for entries in the MAC address table to 600 seconds (10 minutes):

```
switch# configure terminal
switch(config)# mac-address-table aging-time 600
```

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/MACAddress.html#wp1126206>

**QUESTION 20**

While working in the core network building, a technician accidentally bumps the fiber connection between two core switches and damages one of the pairs of fiber. As designed, the link was placed into a non-forwarding state due to a fault with UDLD. After the damaged cable was replaced, the link did not recover.

What solution allows the network switch to automatically recover from such an issue?

- A. macros
- B. errdisable autorecovery
- C. IP Event Dampening
- D. command aliases
- E. Bidirectional Forwarding Detection

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

There are a number of events which can disable a link on a Catalyst switch, such as the detection of a loopback, UDLD failure, or a broadcast storm. By default, manual intervention by an administrator is necessary to restore the interface to working order; this can be done by issuing shutdown followed by no shutdown on the interface. The idea behind requiring administrative action is so that a human engineer can intercede, assess, and (ideally) correct the issue. However, some configurations may be prone to accidental violations, and a steady recurrence of these can amount to a huge time sink for the administrative staff.

This is where errdisable autorecovery can be of great assistance. We can configure the switch to automatically re-enable any error-disabled interfaces after a specified timeout period. This gives the offending issue a chance to be cleared by the user (for example, by removing an unapproved device) without the need for administrative intervention.

Reference: <http://packetlife.net/blog/2009/sep/14/errdisable-autorecovery/>

**QUESTION 21**

A network engineer deployed a switch that operates the LAN base feature set and decides to use the SDM VLAN template. The SDM template is causing the CPU of the switch to spike during peak working hours.

What is the root cause of this issue?

- A. The VLAN receives additional frames from neighboring switches.
- B. The SDM VLAN template causes the MAC address-table to overflow.
- C. The VLAN template disables routing in hardware.
- D. The switch needs to be rebooted before the SDM template takes effect.

**Correct Answer:** C  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

SDM Template Notes:

- All templates are predefined. There is no way to edit template category individual values.
- The switch reload is required to use a new SDM template.
- The ACL merge algorithm, as opposed to the original access control entries (ACEs) configured by the user, generate the number of TCAM entries listed for security and QoS ACEs.
- The first eight lines (up to Security ACEs) represent approximate hardware boundaries set when a template is used. If the boundary is exceeded, all processing overflow is sent to the CPU which can have a major impact on the performance of the switch.

Choosing the VLAN template will actually disable routing (number of entry for unicast or multicast route is zero) in hardware.



Reference: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/44921-swdatabase-3750ss-44921.html>

**QUESTION 22**

An access switch has been configured with an EtherChannel port. After configuring SPAN to monitor this port, the network administrator notices that not all traffic is being replicated to the management server.

What is a cause for this issue?

- A. VLAN filters are required to ensure traffic mirrors effectively.
- B. SPAN encapsulation replication must be enabled to capture EtherChannel destination traffic.
- C. The port channel can be used as a SPAN source, but not a destination.
- D. RSPAN must be used to capture EtherChannel bidirectional traffic.

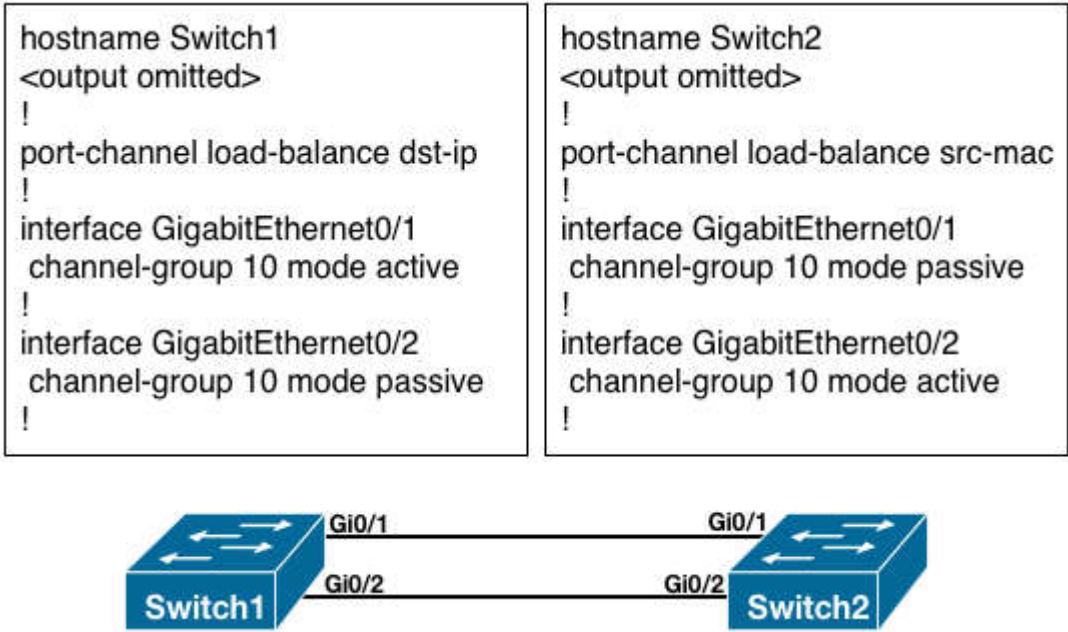
**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:  
A source port or EtherChannel is a port or EtherChannel monitored for traffic analysis. You can configure both Layer 2 and Layer 3 ports and EtherChannels as SPAN sources. SPAN can monitor one or more source ports or EtherChannels in a single SPAN session. You can configure ports or EtherChannels in any VLAN as SPAN sources. Trunk ports or EtherChannels can be configured as sources and mixed with nontrunk sources. A port-channel interface (an EtherChannel) can be a SPAN source, but not a destination.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/span.html#wp1040905>

**QUESTION 23**

Refer to the exhibit.



What is the result of the configuration?

- A. The EtherChannels would not form because the load-balancing method must match on the devices.
- B. The EtherChannels would form and function properly even though the load-balancing and EtherChannel modes do not match.
- C. The EtherChannels would form, but network loops would occur because the load-balancing methods do not match.
- D. The EtherChannels would form and both devices would use the dst-ip load-balancing method because Switch1 is configured with EtherChannel mode active.

**Correct Answer: B**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:  
An etherchannel will form if one end is active and the other is passive. The table below summarizes the results for LACP channel establishment based on the configuration of each side of a link:

LACP Channel Establishment

| S1                | S2             | Established? |
|-------------------|----------------|--------------|
| On                | On             | Yes          |
| Active/Passive    | Active         | Yes          |
| On/Active/Passive | Not Configured | No           |
| On                | Active         | No           |
| Passive/On        | Passive        | No           |

Load balancing can only be configured globally. As a result, all channels (manually configured, PagP, or LACP) use the same load-balancing. This is true for the switch globally, although each switch involved in the etherchannel can have non matching parameters for load balancing.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/54sg/configuration/guide/config/channel.html#wp1020804>

**QUESTION 24**

A network engineer tries to configure storm control on an EtherChannel bundle.

What is the result of the configuration?

- A. The storm control settings will appear on the EtherChannel, but not on the associated physical ports.
- B. The configuration will be rejected because storm control is not supported for EtherChannel.
- C. The storm control configuration will be accepted, but will only be present on the physical interfaces.
- D. The settings will be applied to the EtherChannel bundle and all associated physical interfaces.

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

After you configure an EtherChannel, any configuration that you apply to the port-channel interface affects the EtherChannel; any configuration that you apply to the physical interfaces affects only the interface where you apply the configuration.

Storm Control is an exception to this rule. For example, you cannot configure Storm Control on some of the members of an EtherChannel; Storm Control must be configured on all or none of the ports. If you configure Storm Control on only some of the ports, those ports will be dropped from the EtherChannel interface (put in suspended state). Therefore, you should configure Storm Control at the EtherChannel Interface level, and not at the physical interface level.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/31sg/configuration/guide/conf/channel.html>

#### QUESTION 25

What is the function of NSF?

- A. forward traffic simultaneously using both supervisors
- B. forward traffic based on Cisco Express Forwarding
- C. provide automatic failover to back up supervisor in VSS mode
- D. provide nonstop forwarding in the event of failure of one of the member supervisors

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VSS is network system virtualization technology that pools multiple Cisco Catalyst 6500 Series Switches into one virtual switch, increasing operational efficiency, boosting nonstop communications, and scaling system bandwidth capacity to 1.4 Tbps. Switches would operate as a single logical virtual switch called a virtual switching system 1440 (VSS1440). VSS formed by two Cisco Catalyst 6500 Series Switches with the Virtual Switching Supervisor 720-10GE. In a VSS, the data plane and switch fabric with capacity of 720 Gbps of supervisor engine in each chassis are active at the same time on both chassis, combining for an active 1400-Gbps switching capacity per VSS. Only one of the virtual switch members has the active control plane. Both chassis are kept in sync with the inter-chassis Stateful Switchover (SSO) mechanism along with Nonstop Forwarding (NSF) to provide nonstop communication even in the event of failure of one of the member supervisor engines or chassis.

Reference: <http://ciscorouterswitch.over-blog.com/article-cisco-catalyst-6500-series-vss-1440-124536783.html>

#### QUESTION 26

After UDLD is implemented, a Network Administrator noticed that one port stops receiving UDLD packets. This port continues to reestablish until after eight failed retries. The port then transitions into the errdisable state.

Which option describes what causes the port to go into the errdisable state?

- A. Normal UDLD operations that prevent traffic loops.
- B. UDLD port is configured in aggressive mode.
- C. UDLD is enabled globally.
- D. UDLD timers are inconsistent.

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/udld.html>

#### QUESTION 27

After reviewing UDLD status on switch ports, an engineer notices that the switch LEDs are green.

Which statement describes what this indicates about the status of the port?

- A. The port is fully operational and no known issues are detected.
- B. The bidirectional status of "unknown" indicates that the port will go into the disabled state because it stopped receiving UDLD packets from its neighbor.
- C. UDLD moved into aggressive mode after inconsistent acknowledgements were detected.
- D. The UDLD port is placed in the "unknown" state for 5 seconds until the next UDLD packet is received on the interface.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

By default, UDLD is disabled on all interfaces. We can enable UDLD globally on the device, or individually on specific interfaces with the command `udld port`. This enables UDLD in normal mode.

It would be prohibitively difficult to coordinate the configuration of UDLD on both ends of a link at the same time, so when UDLD is first enabled and does not detect a neighbor the link state is considered unknown, which is not necessarily an error condition. The port will remain operational during this time. When UDLD is finally enabled on the other end, the status will transition to bidirectional.

References: <http://packetlife.net/blog/2011/mar/7/udld/>

#### QUESTION 28

Pilot testing of the new switching infrastructure finds that when the root port is lost, STP immediately replaces the root port with an alternative root port. Which spanning-tree technology is used to accomplish backup root port selection?

- A. PVST+
- B. PortFast
- C. BackboneFast
- D. UplinkFast
- E. Loop Guard
- F. UDLD

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanning-tree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures.

UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 interfaces (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_55\\_se/configuration/guide/scg\\_2960/swstpopt.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swstpopt.html)

#### QUESTION 29

A network engineer must adjust the STP interface attributes to influence root port selection.

Which two elements are used to accomplish this? (Choose two.)

- A. port-priority
- B. cost
- C. forward-timers
- D. link type
- E. root guard

**Correct Answer: AB**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstp.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstp.html)

#### QUESTION 30

A network engineer must set the load balance method on an existing port channel. Which action must be done to apply a new load balancing method?

- A. Configure the new load balancing method using port-channel load-balance.
- B. Adjust the switch SDM back to "default".
- C. Ensure that IP CEF is enabled globally to support all load balancing methods.
- D. Upgrade the PFC to support the latest load balancing methods.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Example:

EtherChannel balances the traffic load across the links in a channel through the reduction of part of the binary pattern that the addresses in the frame form to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The mode applies to all EtherChannels that are configured on the switch. You configure the load balancing and forwarding method with use of the **port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}** global configuration command.

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html>

#### QUESTION 31

Refer to the exhibit.



```
Switch#sh int g0/12
GigabitEthernet0/23 is up, line protocol is down (monitoring)
  Hardware is C6k 1000Mb 802.3, address is 001c.f9d4.7500 (bia
  001c.f9d4.750)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    Reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 1000Mb/s
```

A network engineer investigates a recent network failure and notices that one of the interfaces on the switch is still down.

What is causing the line protocol on this interface to be shown as down?

- A. There is a layer 1 physical issue.
- B. There is a speed mismatch on the interface.
- C. The interface is configured as the target of the SPAN session.
- D. The interface is configured as the source of the SPAN session.
- E. There is a duplex mismatch on the interface.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

With the SPAN destination port, the state of the destination port is up/down by design. The interface shows the port in this state in order to make it evident that the port is currently not usable as a production port. This is the normal operational state for SPAN destinations.

Reference: [http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_tech\\_note09186a008015c612.shtml](http://www.cisco.com/en/US/products/hw/switches/ps708/products_tech_note09186a008015c612.shtml)

#### QUESTION 32

While doing network discovery using Cisco Discovery Protocol, it is found that rapid error tracking is not currently enabled.

Which option must be enabled to allow for enhanced reporting mechanisms using Cisco Discovery Protocol?

- A. Cisco Discovery Protocol version 2
- B. Cisco IOS Embedded Event Manager
- C. logging buffered
- D. Cisco Discovery Protocol source interface
- E. Cisco Discovery Protocol logging options

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

- CDP Version 1 — This is the first version of CDP which was used for the discovery of Cisco devices in the network. This version is mainly used for backward compatibility.
- CDP Version 2 — This is the most recent version of CDP which has enhanced features such as rapid reporting mechanism, which is used to track down errors and minimize costly downtime. It allows you to track instances even if the native VLAN ID or port duplex states do not match between connecting devices. This is the default version on all switches.

Reference: [http://sbkb.cisco.com/CiscoSB/GetArticle.aspx?docid=0ed03cbac49b446ab390a657917d817c\\_Cisco\\_Discovery\\_Protocol\\_CDP\\_Properties\\_Settings\\_on\\_Sx500\\_S.xml&pid=2&converted=0](http://sbkb.cisco.com/CiscoSB/GetArticle.aspx?docid=0ed03cbac49b446ab390a657917d817c_Cisco_Discovery_Protocol_CDP_Properties_Settings_on_Sx500_S.xml&pid=2&converted=0)

#### QUESTION 33

Which technique allows specific VLANs to be strictly permitted by the administrator?

- A. VTP pruning
- B. transparent bridging
- C. trunk-allowed VLANs
- D. VLAN access-list
- E. L2P tunneling

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the “switchport trunk allowed vlan remove vlan-list” interface configuration command to remove specific VLANs from the allowed list.

References: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_55\\_se/configuration/guide/3560\\_scg/swvlan.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/swvlan.html)

#### QUESTION 34

For security reasons, the IT manager has prohibited users from dynamically establishing trunks with their associated upstream switch.

Which two actions can prevent interface trunking? (Choose two.)

- A. Configure trunk and access interfaces manually.
- B. Disable DTP on a per interface basis.
- C. Apply BPDU guard and BPDU filter.
- D. Enable switchport block on access ports.

**Correct Answer:** AB

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The Dynamic Trunking Protocol (DTP) is used to negotiate forming a trunk between two Cisco devices. DTP causes increased traffic, and is enabled by default, but may be disabled. To disable DTP, configure “switchport nonegotiate.” This prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link, otherwise the link will be a non-trunking link.

Reference: <http://www.ciscopress.com/articles/article.asp?p=2181837&seqNum=8>

#### QUESTION 35

Which two protocols can be automatically negotiated between switches for trunking? (Choose two.)

- A. PPP
- B. DTP
- C. ISL
- D. HDLC
- E. DLCI
- F. DOT1Q

**Correct Answer:** CF

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Switches such as the Catalyst 3550 that are capable of either 802.1Q or ISL trunking encapsulation, the switchport trunk encapsulation [dot1q | isl | negotiate] interface command must be used prior to the switchport mode trunk command.

Reference: <https://learningnetwork.cisco.com/servlet/JiveServlet/previewBody/14792-102-1-57313/Dynamic%20Trunking%20Protocol.PDF>

#### QUESTION 36

A network is running VTPv2. After verifying all VTP settings, the network engineer notices that the new switch is not receiving the list of VLANs from the server.

Which action resolves this problem?

- A. Reload the new switch.
- B. Restart the VTP process on the new switch.
- C. Reload the VTP server.
- D. Verify connected trunk ports.

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

VTP should never need to have the switch reloaded or the VTP process to restart in order for it to work. The first thing that should be done is to verify that the trunk ports are connected and up.

#### QUESTION 37

After configuring new data VLANs 1020 through 1030 on the VTP server, a network engineer notices that none of the VTP clients are receiving the updates.

What is the problem?

- A. The VTP server must be reloaded.
- B. The VTP version number must be set to version 3.
- C. After each update to the VTP server, it takes up to 4 hours propagate.
- D. VTP must be stopped and restarted on the server.
- E. Another switch in the domain has a higher revision number than the server.

**Correct Answer:** B

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as hidden or secret. When hidden, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the secret keyword, you can directly configure the password secret key.
- **Support for extended range VLAN (VLANs 1006 to 4094) database propagation. VTP versions 1 and 2 propagate only VLANs 1 to 1005. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2.**

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2\\_52\\_se/configuration/guide/swvtp.html#wp1316856](http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_52_se/configuration/guide/swvtp.html#wp1316856)

#### QUESTION 38

A network engineer is extending a LAN segment between two geographically separated data centers. Which enhancement to a spanning-tree design prevents unnecessary traffic from crossing the extended LAN segment?

- A. Modify the spanning-tree priorities to dictate the traffic flow.
- B. Create a Layer 3 transit VLAN to segment the traffic between the sites.
- C. Use VTP pruning on the trunk interfaces.
- D. Configure manual trunk pruning between the two locations.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Pruning unnecessary VLANs from the trunk can be performed with one of two methods:

- Manual pruning of the unnecessary VLAN on the trunk—This is the best method, and it avoids the use of the spanning tree. Instead, the method runs the pruned VLAN on trunks.
- VTP pruning—Avoid this method if the goal is to reduce the number of STP instances. VTP-pruned VLANs on a trunk are still part of the spanning tree. Therefore, VTP-pruned VLANs do not reduce the number of spanning tree port instances.

Since the question asked for the choice that is an enhancement to the STP design, VTP pruning is the best choice.

Reference: [http://www.cisco.com/en/US/tech/tk389/tk689/technologies\\_tech\\_note09186a0080890613.shtml](http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml)

#### QUESTION 39

The network manager has requested that several new VLANs (VLAN 10, 20, and 30) are allowed to traverse the switch trunk interface. After the command `switchport trunk allowed vlan 10,20,30` is issued, all other existing VLANs no longer pass traffic over the trunk.

What is the root cause of the problem?

- A. The command effectively removed all other working VLANs and replaced them with the new VLANs.
- B. VTP pruning removed all unused VLANs.
- C. ISL was unable to encapsulate more than the already permitted VLANs across the trunk.
- D. Allowing additional VLANs across the trunk introduced a loop in the network.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The “switchport trunk allowed vlan” command will only allow the specified VLANs, and overwrite any others that were previously defined. You would also need to explicitly allow the other working VLANs to this configuration command, or use the “issue the switchport trunk allowed vlan add vlan-list” command instead to add these 3 VLANs to the other defined allowed VLANs.

Reference: <https://supportforums.cisco.com/document/11836/how-define-vlans-allowed-trunk-link>

#### QUESTION 40

When you design a switched network using VTPv2, how many VLANs can be used to carry user traffic?

- A. 1000
- B. 1001
- C. 1024
- D. 2048
- E. 4095
- F. 4096

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP versions 1 and 2 Supports normal VLAN numbers (1-1001). Only VTP version 3 supports extended VLANs (1-4095).

Reference: <http://cciememo.blogspot.com/2012/11/difference-between-vtp-versions.html>

#### QUESTION 41

What does the command `vlan dot1q tag native` accomplish when configured under global configuration?

- A. All frames within the native VLAN are tagged, except when the native VLAN is set to 1.
- B. It allows control traffic to pass using the non-default VLAN.
- C. It removes the 4-byte dot1q tag from every frame that traverses the trunk interface(s).
- D. Control traffic is tagged.

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The “vlan dot1q tag native” will tag all untagged frames, including control traffic, with the defined native VLAN.

**QUESTION 42**

A network engineer has just deployed a non-Cisco device in the network and wants to get information about it from a connected device. Cisco Discovery Protocol is not supported, so the open standard protocol must be configured.

Which protocol does the network engineer configure on both devices to accomplish this?

- A. IRDP
- B. LLDP
- C. NDP
- D. LLTD

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol (CDP).

Reference: [http://en.wikipedia.org/wiki/Link\\_Layer\\_Discovery\\_Protocol](http://en.wikipedia.org/wiki/Link_Layer_Discovery_Protocol)

**QUESTION 43**

A manager tells the network engineer to permit only certain VLANs across a specific trunk interface. Which option can be configured to accomplish this?

- A. allowed VLAN list
- B. VTP pruning
- C. VACL
- D. L2P tunneling

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

When a trunk link is established, all of the configured VLANs are allowed to send and receive traffic across the link. VLANs 1 through 1005 are allowed on each trunk by default. However, VLAN traffic can be removed from the allowed list. This keeps traffic from the VLANs from passing over the trunk link.

Note: The allowed VLAN list on both the ends of the trunk link should be the same.

For Integrated Cisco IOS Software based switches, perform these steps:

1. To restrict the traffic that a trunk carries, issue the switchport trunk vlan-list interface configuration command.

This removes specific VLANs from the allowed list.

Reference: <https://supportforums.cisco.com/document/11836/how-define-vlans-allowed-trunk-link>

**QUESTION 44**

For client server failover purposes, the application server team has indicated that they must not have the standard 30 second delay before their switchport enters a forwarding state. For their disaster recovery feature to operate successfully, they require the switchport to enter a forwarding state immediately.

Which spanning-tree feature satisfies this requirement?

- A. Rapid Spanning-Tree
- B. Spanning-Tree Timers
- C. Spanning-Tree FastPort
- D. Spanning-Tree PortFast
- E. Spanning-Tree Fast Forward

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

In order to allow immediate transition of the port into forwarding state, enable the STP PortFast feature. PortFast immediately transitions the port into STP forwarding mode upon linkup. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode.

Example configuration:

Switch-C# configure terminal

Switch-C(config)# interface range fa0/3 - 24

Switch-C(config-if-range)# spanning-tree portfast

Reference: [http://www.informit.com/library/content.aspx?b=CCNP\\_Studies\\_Switching&seqNum=36](http://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=36)

**QUESTION 45**

Which command does a network engineer use to verify the spanning-tree status for VLAN 10?

- A. switch# show spanning-tree vlan 10
- B. switch# show spanning-tree bridge
- C. switch# show spanning-tree brief
- D. switch# show spanning-tree summary
- E. switch# show spanning-tree vlan 10 brief

**Correct Answer: A**



Section: Layer 2 Technologies  
Explanation

Explanation/Reference:  
Explanation:

| Command            | Description                                         |
|--------------------|-----------------------------------------------------|
| show spanning-tree | Displays information about the spanning-tree state. |

Example output:  
SW2#show spanning-tree vlan 10

```
VLAN0010
Spanning tree enabled protocol rstp
Root ID    Priority    24586
           Address    0014.f2d2.4180
           Cost       9
           Port       216 (Port-channel21)
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID  Priority    32778 (priority 32768 sys-id-ext 10)
           Address    001c.57d8.9000
           Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
           Aging Time  300 sec

Interface          Role Sts Cost      Prio.Nbr Type
-----
Po21                Root FWD 9         128.216 P2p
Po23                Altn BLK 9         128.232 P2p
```

Reference: [http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw\\_s2.html](http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_s2.html)

**QUESTION 46**  
A new network that consists of several switches has been connected together via trunking interfaces. If all switches currently have the default VTP domain name "null", which statement describes what happens when a domain name is configured on one of the switches?

A. The switch with the non-default domain name restores back to "null" upon reboot.  
B. Switches with higher revision numbers do not accept the new domain name.  
C. VTP summary advertisements are sent out of all ports with the new domain name.  
D. All other switches with the default domain name become VTP clients.

Correct Answer: C  
Section: Layer 2 Technologies  
Explanation

Explanation/Reference:  
Explanation:  
By default, a switch will have a domain name of NULL and no password. If the switch hears a VTP advertisement it will automatically learn the VTP domain name, VLANs, and the configuration revision number.  
Summary advertisements – sent out every 300 seconds and every time a change occurs on the VLAN database. Contained in a summary advertisement:

- VTP version
- **Domain name**
- Configuration revision number
- Time stamp
- MD5 encryption hash code

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_52\\_se/configuration/guide/3560scg/swvtp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html)

**QUESTION 47**  
A network engineer is setting up a new switched network. The network is expected to grow and add many new VLANs in the future. Which Spanning Tree Protocol should be used to reduce switch resources and managerial burdens that are associated with multiple spanning-tree instances?

A. RSTP  
B. PVST  
C. MST  
D. PVST+  
E. RPVST+

Correct Answer: C  
Section: Layer 2 Technologies  
Explanation

Explanation/Reference:  
Explanation:  
Multiple Spanning Tree (MST) extends the IEEE 802.1w RST algorithm to multiple spanning trees. The main purpose of MST is to reduce the total number of spanning-tree instances to match the physical topology of the network and thus reduce the CPU cycles of a switch. PVST+ runs STP instances for each VLAN and does not take into consideration the physical topology that might not require many different STP topologies. MST, on the other hand, uses a minimum number of STP instances to match the number of physical topologies present.  
Figure 3-15 shows a common network design, featuring an access Switch A, connected to two Building Distribution submodule Switches D1 and D2. In this setup, there are 1000 VLANs, and the network administrator typically seeks to achieve load balancing on the access switch uplinks based on even or odd VLANs—or any other scheme deemed appropriate.

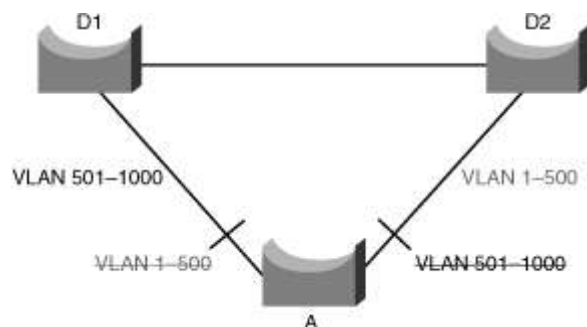


Figure 3-15: VLAN Load Balancing

Figure 3-15 illustrates two links and 1000 VLANs. The 1000 VLANs map to two MST instances. Rather than maintaining 1000 spanning trees, each switch needs to maintain only two spanning trees, reducing the need for switch resources.

Reference: <http://ciscodocuments.blogspot.com/2011/05/chapter-03-implementing-spanning-tree-19.html>

#### QUESTION 48

Which statement about the use of SDM templates in a Cisco switch is true?

- A. SDM templates are used to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network.
- B. SDM templates are used to create Layer 3 interfaces (switch virtual interfaces) to permit hosts in one VLAN to communicate with hosts in another VLAN.
- C. SDM templates are used to configure ACLs that protect networks and specific hosts from unnecessary or unwanted traffic.
- D. SDM templates are used to configure a set of ACLs that allows the users to manage the flow of traffic handled by the route processor.
- E. SDM templates are configured by accessing the switch using the web interface.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

You can use SDM templates to configure system resources in the switch to optimize support for specific features, depending on how the switch is used in the network. You can select a template to provide maximum system usage for some functions; for example, use the default template to balance resources, and use access template to obtain maximum ACL usage. To allocate hardware resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features.

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x\\_3560x/software/release/12.2\\_55\\_se/configuration/guide/swsdm.pdf](http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_55_se/configuration/guide/swsdm.pdf)

#### QUESTION 49

Which SDM template disables routing and supports the maximum number of unicast MAC addresses?

- A. VLAN
- B. access
- C. default
- D. routing

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:

- Access — The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default — The default template gives balance to all functions.
- Routing — The routing template maximizes system resources for IPv4 unicast routing, typically required for a router or aggregator in the center of a network.
- **VLANs — The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.**

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2\\_55\\_se/configuration/guide/swsdm.pdf](http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf)

#### QUESTION 50

Which SDM template is the most appropriate for a Layer 2 switch that provides connectivity to a large number of clients?

- A. VLAN
- B. default
- C. access
- D. routing

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

To allocate ternary content addressable memory (TCAM) resources for different usages, the switch SDM templates prioritize system resources to optimize support for certain features. You can select SDM templates to optimize these features:

- Access—The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default—The default template gives balance to all functions.
- Routing—The routing template maximizes system resources for IPv4 unicast routing, typically required for a router or aggregator in the center of a network.

- **VLANs**—The VLAN template disables routing and supports the maximum number of unicast MAC addresses (clients). It would typically be selected for a Layer 2 switch.

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2\\_55\\_se/configuration/guide/swsdm.pdf](http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf)

#### QUESTION 51

In a Cisco switch, what is the default period of time after which a MAC address ages out and is discarded?

- A. 100 seconds
- B. 180 seconds
- C. 300 seconds
- D. 600 seconds

**Correct Answer:** C

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

To configure the aging time for all MAC addresses, perform this task:

|        | Command                                                                    | Purpose                                                                                                                                                                                                                                                                             |
|--------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>configure terminal</b>                                          | Enters configuration mode.                                                                                                                                                                                                                                                          |
| Step 2 | switch(config)# <b>mac-address-table aging-time seconds [vlan vlan_id]</b> | Specifies the time before an entry ages out and is discarded from the MAC address table. The range is from 0 to 1000000; <b>the default is 300 seconds</b> . Entering the value 0 disables the MAC aging. If a VLAN is not specified, the aging specification applies to all VLANs. |

Reference: <http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/MACAddress.html>

#### QUESTION 52

If a network engineer applies the command mac-address-table notification mac-move on a Cisco switch port, when is a syslog message generated?

- A. A MAC address or host moves between different switch ports.
- B. A new MAC address is added to the content-addressable memory.
- C. A new MAC address is removed from the content-addressable memory.
- D. More than 64 MAC addresses are added to the content-addressable memory.

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

mac-address-table notification mac-move

To enable MAC-move notification, use the **mac-address-table notification mac-move** command in global configuration mode. To disable MAC-move notification, use the **no** form of this command.

**Mac-address-table notification mac-move [counter [syslog]]**

**no mac-address-table notification mac-move [counter [syslog]]**

Syntax Description

|                |                                                                                                                         |
|----------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>counter</b> | (Optional) Specifies the MAC-move counter feature.                                                                      |
| <b>Syslog</b>  | (Optional) Specifies the syslogging facility when the MAC-move notification detects the first instance of the MAC move. |

Usage Guidelines

MAC-move notification generates a syslog message whenever a MAC address or host moves between different switch ports.

Reference: [http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw\\_m1.html](http://www.cisco.com/en/US/docs/ios/lanswitch/command/reference/lsw_m1.html)

#### QUESTION 53

Which option is a possible cause for an errdisabled interface?

- A. routing loop
- B. cable unplugged
- C. STP loop guard
- D. security violation

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

There are various reasons for the interface to go into errdisable. The reason can be:

- Duplex mismatch
- Port channel misconfiguration
- BPDU guard violation
- UniDirectional Link Detection (UDLD) condition

- Late-collision detection
- Link-flap detection
- **Security violation**
- Port Aggregation Protocol (PAgP) flap
- Layer 2 Tunneling Protocol (L2TP) guard
- DHCP snooping rate-limit
- Incorrect GBIC / Small Form-Factor Pluggable (SFP) module or cable
- Address Resolution Protocol (ARP) inspection
- Inline power

Reference: [http://www.cisco.com/en/US/tech/tk389/tk621/technologies\\_tech\\_note09186a00806cd87b.shtml](http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00806cd87b.shtml)

#### QUESTION 54

What is the default value for the errdisable recovery interval in a Cisco switch?

- A. 30 seconds
- B. 100 seconds
- C. 300 seconds
- D. 600 seconds

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

After you fix the root problem, the ports are still disabled if you have not configured errdisable recovery on the switch. In this case, you must reen able the ports manually. Issue the **shutdown** command and then the **no shutdown** interface mode command on the associated interface in order to manually reen able the ports.

The **errdisable recovery** command allows you to choose the type of errors that automatically reen able the ports after a specified amount of time. The **show errdisable recovery** command shows the default error-disable recovery state for all the possible conditions.

cat6knative#**show errdisable recovery**

ErrDisable Reason Timer Status

```

-----
udld                Disabled
bpduguard           Disabled
security-violatio   Disabled
channel-misconfig   Disabled
pagp-flap           Disabled
dtp-flap            Disabled
link-flap           Disabled
l2ptguard           Disabled
psecure-violation   Disabled
gbic-invalid        Disabled
dhcp-rate-limit     Disabled
mac-limit           Disabled
unicast-flood       Disabled
arp-inspection      Disabled

```

Timer interval: 300 seconds

Interfaces that will be enabled at the next timeout:

**Note: The default timeout interval is 300 seconds** and, by default, the timeout feature is disabled.

Reference: [http://www.cisco.com/en/US/tech/tk389/tk621/technologies\\_tech\\_note09186a00806cd87b.shtml](http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00806cd87b.shtml)

#### QUESTION 55

Which statement about LLDP-MED is true?

- A. LLDP-MED is an extension to LLDP that operates between endpoint devices and network devices.
- B. LLDP-MED is an extension to LLDP that operates only between network devices.
- C. LLDP-MED is an extension to LLDP that operates only between endpoint devices.
- D. LLDP-MED is an extension to LLDP that operates between routers that run BGP.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, Power over Ethernet, and inventory management.

Reference: [http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2\\_58\\_se/configuration/guide/swlldp.pdf](http://www.cisco.com/en/US/docs/switches/metro/me3400/software/release/12.2_58_se/configuration/guide/swlldp.pdf)

#### QUESTION 56

Which statement about Cisco devices learning about each other through Cisco Discovery Protocol is true?

- A. Each device sends periodic advertisements to multicast address 01:00:0C:CC:CC:CC.
- B. Each device broadcasts periodic advertisements to all of its neighbors.
- C. Each device sends periodic advertisements to a central device that builds the network topology.
- D. Each device sends periodic advertisements to all IP addresses in its ARP table.

**Correct Answer: A**

**Section: Layer 2 Technologies**



## Explanation

### Explanation/Reference:

Explanation:

Cisco devices send periodic CDP announcements to the multicast destination address 01-00-0c-cc-cc-cc, out each connected network interface. These multicast packets may be received by Cisco switches and other networking devices that support CDP into their connected network interface.

Reference: <https://www.cisco.com/c/en/us/support/docs/network-management/discovery-protocol-cdp/118736-technote-cdp-00.html>

### QUESTION 57

Which option lists the information that is contained in a Cisco Discovery Protocol advertisement?

- A. native VLAN IDs, port-duplex, hardware platform
- B. native VLAN IDs, port-duplex, memory errors
- C. native VLAN IDs, memory errors, hardware platform
- D. port-duplex, hardware platform, memory errors

**Correct Answer: A**

**Section: Layer 2 Technologies**

### Explanation

### Explanation/Reference:

Explanation:

Type-Length-Value fields (TLVs) are blocks of information embedded in CDP advertisements. Table 21 summarizes the TLV definitions for CDP advertisements.

| Table 21 Type-Length-Value Definitions for CDPv2 |                                                                                                                                                                                                                       |
|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TLV                                              | Definition                                                                                                                                                                                                            |
| Device-ID TLV                                    | Identifies the device name in the form of a character string.                                                                                                                                                         |
| Address TLV                                      | Contains a list of network addresses of both receiving and sending devices.                                                                                                                                           |
| Port-ID TLV                                      | Identifies the port on which the CDP packet is sent.                                                                                                                                                                  |
| Capabilities TLV                                 | Describes the functional capability for the device in the form of a device type, for example, a switch.                                                                                                               |
| Version TLV                                      | Contains information about the software release version on which the device is running.                                                                                                                               |
| Platform TLV                                     | Describes the hardware platform name of the device, for example, Cisco 4500.                                                                                                                                          |
| IP Network Prefix TLV                            | Contains a list of network prefixes to which the sending device can forward IP packets. This information is in the form of the interface protocol and port number, for example, Eth 1/0.                              |
| VTP Management Domain TLV                        | Advertises the system's configured VTP management domain name-string. Used by network operators to verify VTP domain configuration in adjacent network nodes.                                                         |
| Native VLAN TLV                                  | Indicates, per interface, the assumed VLAN for untagged packets on the interface. CDP learns the native VLAN for an interface. This feature is implemented only for interfaces that support the IEEE 802.1Q protocol. |
| Full/Half Duplex TLV                             | Indicates status (duplex configuration) of CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements.                                                    |

Reference: [http://www.cisco.com/en/US/docs/ios/12\\_2/configfun/configuration/guide/fcf015.html](http://www.cisco.com/en/US/docs/ios/12_2/configfun/configuration/guide/fcf015.html)

### QUESTION 58

Which option describes a limitation of LLDP?

- A. LLDP cannot provide information about VTP.
- B. LLDP does not support TLVs.
- C. LLDP can discover only Windows servers.
- D. LLDP can discover up to two devices per port.

**Correct Answer: A**

**Section: Layer 2 Technologies**

### Explanation

### Explanation/Reference:

Explanation:

LLDP Versus Cisco Discovery Protocol TLV Comparison

| Function Description                                                                                                        | LLDP TLV                      | Cisco Discovery Protocol TLV            |
|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------|-----------------------------------------|
| IP network prefix support-Used to send the network prefix and used for ODR                                                  | No                            | <i>IP Network Prefix TLV</i>            |
| Hello piggybacking-Can be used to piggy back hello messages from other protocols                                            | No                            | <i>Protocol Hello TLV</i>               |
| Maximum-transmission-unit (MTU) support-Specifies the size of the MTU                                                       | No                            | <i>MTU TLV</i>                          |
| External port support-Used to identify the card terminating the fiber in the case of wavelength-division multiplexing (WDM) | No                            | <i>External Port-ID TLV</i>             |
| <b>VTP management support</b>                                                                                               | <b>No</b>                     | <b><i>VTP Management Domain TLV</i></b> |
| Port unidirectional mode-Used in fiber, where the connection may be unidirectional                                          | No                            | <i>Port UniDirectional Mode TLV</i>     |
| Management address                                                                                                          | <i>Management Address TLV</i> | <i>Management-Address TLV</i>           |
| Allows for organizational unique TLVs                                                                                       | Yes                           | <i>No</i>                               |

Reference: [http://www.cisco.com/en/US/technologies/tk652/tk701/technologies\\_white\\_paper0900aecd804cd46d.html](http://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html)

#### QUESTION 59

Which statement about the UDLD protocol is true?

- A. UDLD is a Cisco-proprietary Layer 2 protocol that enables devices to monitor the physical status of links and detect unidirectional failures.
- B. UDLD is a Cisco-proprietary Layer 2 protocol that enables devices to advertise their identity, capabilities, and neighbors on a local area network.
- C. UDLD is a standardized Layer 2 protocol that enables devices to monitor the physical status of links and detect unidirectional failures.
- D. UDLD is a standardized Layer 2 protocol that enables devices to advertise their identity, capabilities, and neighbors on a local area network.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The Cisco-proprietary UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links. When a unidirectional link is detected, UDLD puts the affected port into the errdisabled state and alerts the user.

Reference: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html>

#### QUESTION 60

Which option lists the modes that are available for configuring UDLD on a Cisco switch?

- A. normal and aggressive
- B. active and aggressive
- C. normal and active
- D. normal and passive
- E. normal and standby

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The Cisco-proprietary UDLD protocol monitors the physical configuration of the links between devices and ports that support UDLD. UDLD detects the existence of unidirectional links. When a unidirectional link is detected, UDLD puts the affected port into the errdisabled state and alerts the user. **UDLD can operate in either normal or aggressive mode.**

Reference: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/udld.html>

#### QUESTION 61

What is the default interval at which Cisco devices send Cisco Discovery Protocol advertisements?

- A. 30 seconds
- B. 60 seconds
- C. 120 seconds
- D. 300 seconds

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco Discovery Protocol is a Layer 2, media-independent, and network-independent protocol that networking applications use to learn about nearby, directly connected devices. Cisco Discovery Protocol is enabled by default. Each device configured for Cisco Discovery Protocol advertises at least one address at

which the device can receive messages and sends periodic advertisements (messages) to the well-known multicast address 01:00:0C:CC:CC:CC. Devices discover each other by listening at that address. They also listen to messages to learn when interfaces on other devices are up or go down. Advertisements contain time-to-live information, which indicates the length of time a receiving device should hold Cisco Discovery Protocol information before discarding it. **Advertisements supported and configured in Cisco software are sent, by default, every 60 seconds.**

Reference: <http://www.cisco.com/en/US/docs/ios-xml/ios/cdp/configuration/15-mt/nm-cdp-discover.html>

#### QUESTION 62

Which statement about Cisco Discovery Protocol configuration on a Cisco switch is true?

- A. CDP is enabled by default and can be disabled globally with the command no cdp run.
- B. CDP is disabled by default and can be enabled globally with the command cdp enable.
- C. CDP is enabled by default and can be disabled globally with the command no cdp enable.
- D. CDP is disabled by default and can be enabled globally with the command cdp run.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

CDP is enabled on your router by default, which means the Cisco IOS software will receive CDP information. CDP also is enabled on supported interfaces by default. To disable CDP on an interface, use the “no cdp enable interface” configuration command. To disable it globally, use the “no cdp run” command.

Reference: [http://www.cisco.com/en/US/docs/ios/12\\_2/configfun/command/reference/frf015.html#wp1017573](http://www.cisco.com/en/US/docs/ios/12_2/configfun/command/reference/frf015.html#wp1017573)

#### QUESTION 63

Which VTP mode is needed to configure an extended VLAN, when a switch is configured to use VTP versions 1 or 2?

- A. transparent
- B. client
- C. server
- D. Extended VLANs are only supported in version 3 and not in versions 1 or 2.

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP version 1 and version 2 support VLANs 1 to 1000 only. Extended-range VLANs are supported only in VTP version 3. If converting from VTP version 3 to VTP version 2, VLANs in the range 1006 to 4094 are removed from VTP control.

Reference: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/vtp.html>

#### QUESTION 64

What is the size of the VLAN field inside an 802.1q frame?

- A. 8-bit
- B. 12-bit
- C. 16-bit
- D. 32-bit

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The VLAN field is a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLANs

Reference: [http://en.wikipedia.org/wiki/IEEE\\_802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q)

#### QUESTION 65

What is the maximum number of VLANs that can be assigned to an access switchport without a voice VLAN?

- A. 0
- B. 1
- C. 2
- D. 1024

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

A standard (non-voice VLAN port) access switch port can belong to only a single VLAN. If more than one VLAN is needed, the port should be configured as a trunk port.

#### QUESTION 66

Refer to the exhibit.



```

Interface GigabitEthernet1/0/1
switchport access vlan 10
switchport trunk encapsulation dot1q
switchport mode trunk
switchport voice vlan 11
spanning-tree portfast
!

```

Which option shows the expected result if a show vlan command is issued?

- A. Switch#sh vlan
- | VLAN | Name               | Status    | Ports                                                                                                                                                                                                                                                             |
|------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Gig1/0/2, Gig1/0/3, Gig1/0/4<br>Gig1/0/5, Gig1/0/6, Gig1/0/7<br>Gig1/0/8, Gig1/0/9, Gig1/0/10<br>Gig1/0/11, Gig1/0/12, Gig1/0/13<br>Gig1/0/14, Gig1/0/15, Gig1/0/16<br>Gig1/0/17, Gig1/0/18, Gig1/0/19<br>Gig1/0/20, Gig1/0/21, Gig1/0/22<br>Gig1/0/23, Gig1/0/24 |
| 10   | Data               | active    |                                                                                                                                                                                                                                                                   |
| 11   | Voice              | active    |                                                                                                                                                                                                                                                                   |
| 1002 | fddi-default       | act/unsup |                                                                                                                                                                                                                                                                   |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                                                                                                   |
| 1004 | fddinet-default    | act/unsup |                                                                                                                                                                                                                                                                   |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                                                                                                   |
- B. Switch#sh vlan
- | VLAN | Name               | Status    | Ports                                                                                                                                                                                                                                                             |
|------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Gig1/0/2, Gig1/0/3, Gig1/0/4<br>Gig1/0/5, Gig1/0/6, Gig1/0/7<br>Gig1/0/8, Gig1/0/9, Gig1/0/10<br>Gig1/0/11, Gig1/0/12, Gig1/0/13<br>Gig1/0/14, Gig1/0/15, Gig1/0/16<br>Gig1/0/17, Gig1/0/18, Gig1/0/19<br>Gig1/0/20, Gig1/0/21, Gig1/0/22<br>Gig1/0/23, Gig1/0/24 |
| 10   | Data               | active    | Gig1/0/1                                                                                                                                                                                                                                                          |
| 11   | Voice              | active    | Gig1/0/1                                                                                                                                                                                                                                                          |
| 1002 | fddi-default       | act/unsup |                                                                                                                                                                                                                                                                   |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                                                                                                   |
| 1004 | fddinet-default    | act/unsup |                                                                                                                                                                                                                                                                   |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                                                                                                   |
- C. Switch#sh vlan
- | VLAN | Name               | Status    | Ports                                                                                                                                                                                                                                                                       |
|------|--------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Gig1/0/1, Gig1/0/2, Gig1/0/3<br>Gig1/0/4, Gig1/0/5, Gig1/0/6<br>Gig1/0/7, Gig1/0/8, Gig1/0/9<br>Gig1/0/10, Gig1/0/11, Gig1/0/12<br>Gig1/0/13, Gig1/0/14, Gig1/0/15<br>Gig1/0/16, Gig1/0/17, Gig1/0/18<br>Gig1/0/19, Gig1/0/20, Gig1/0/21<br>Gig1/0/22, Gig1/0/23, Gig1/0/24 |
| 10   | Data               | active    |                                                                                                                                                                                                                                                                             |
| 11   | Voice              | active    | Gig1/0/1                                                                                                                                                                                                                                                                    |
| 1002 | fddi-default       | act/unsup |                                                                                                                                                                                                                                                                             |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                                                                                                             |
| 1004 | fddinet-default    | act/unsup |                                                                                                                                                                                                                                                                             |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                                                                                                             |
- D. Switch#sh vlan
- | VLAN | Name               | Status    | Ports                                                                                                                                                                                                                                                             |
|------|--------------------|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | default            | active    | Gig1/0/2, Gig1/0/3, Gig1/0/4<br>Gig1/0/5, Gig1/0/6, Gig1/0/7<br>Gig1/0/8, Gig1/0/9, Gig1/0/10<br>Gig1/0/11, Gig1/0/12, Gig1/0/13<br>Gig1/0/14, Gig1/0/15, Gig1/0/16<br>Gig1/0/17, Gig1/0/18, Gig1/0/19<br>Gig1/0/20, Gig1/0/21, Gig1/0/22<br>Gig1/0/23, Gig1/0/24 |
| 10   | Data               | active    |                                                                                                                                                                                                                                                                   |
| 11   | Voice              | active    | Gig1/0/1                                                                                                                                                                                                                                                          |
| 1002 | fddi-default       | act/unsup |                                                                                                                                                                                                                                                                   |
| 1003 | token-ring-default | act/unsup |                                                                                                                                                                                                                                                                   |
| 1004 | fddinet-default    | act/unsup |                                                                                                                                                                                                                                                                   |
| 1005 | trnet-default      | act/unsup |                                                                                                                                                                                                                                                                   |

**Correct Answer: A**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

In this case, the port has been configured both as a trunk and as a switchport in data vlan 10. Obviously, a port can not be both, so even though Cisco IOS will accept both, the port will actually be used as a trunk, ignoring the switchport access VLAN 10 command.

#### QUESTION 67

Which feature is automatically enabled when a voice VLAN is configured, but not automatically disabled when a voice VLAN is removed?

- A. portfast
- B. port-security
- C. spanning tree
- D. storm control

**Correct Answer: A**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

Voice VLAN Configuration Guidelines



- You should configure voice VLAN on switch access ports.
- The voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the voice VLAN. Use the show vlan privileged EXEC command to see if the VLAN is present (listed in the display).
- The Port Fast feature is automatically enabled when voice VLAN is configured. When you disable voice VLAN, the Port Fast feature is not automatically disabled.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_52\\_se/configuration/guide/3560scg/swvoip.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvoip.html)

#### QUESTION 68

In which portion of the frame is the 802.1q header found?

- A. within the Ethernet header
- B. within the Ethernet payload
- C. within the Ethernet FCS
- D. within the Ethernet source MAC address

**Correct Answer: A**

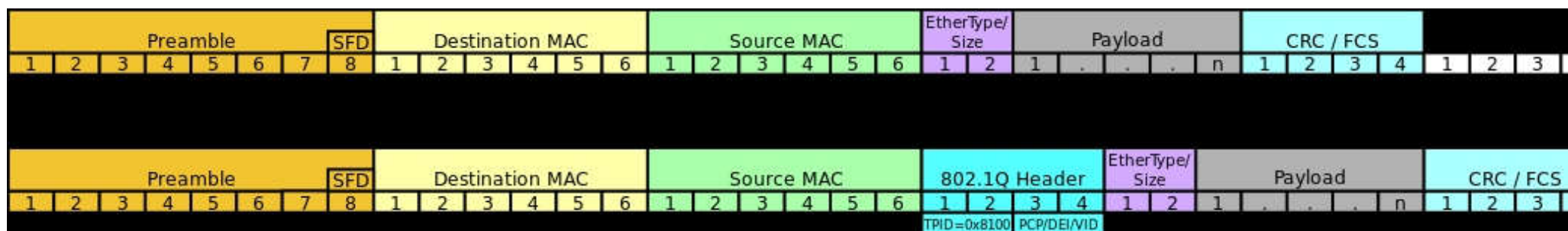
**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

**Frame format**



Insertion of 802.1Q tag in an Ethernet frame

802.1Q does not encapsulate the original frame. Instead, for Ethernet frames, it adds a 32-bit field between the source MAC address and the EtherType/length fields of the original frame

Reference: [http://en.wikipedia.org/wiki/IEEE\\_802.1Q](http://en.wikipedia.org/wiki/IEEE_802.1Q)

#### QUESTION 69

Which VLAN range is eligible to be pruned when a network engineer enables VTP pruning on a switch?

- A. VLANs 1-1001
- B. VLANs 1-4094
- C. VLANs 2-1001
- D. VLANs 2-4094

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP pruning should only be enabled on VTP servers, all the clients in the VTP domain will automatically enable VTP pruning. By default, VLANs 2 – 1001 are pruning eligible, but VLAN 1 can't be pruned because it's an administrative VLAN. Both VTP versions 1 and 2 supports pruning.

Reference: <http://www.orbit-computer-solutions.com/vtp-pruning/>

#### QUESTION 70

Which feature must be enabled to eliminate the broadcasting of all unknown traffic to switches that are not participating in the specific VLAN?

- A. VTP pruning
- B. port-security
- C. storm control
- D. bpdguard

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VTP ensures that all switches in the VTP domain are aware of all VLANs. However, there are occasions when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is a feature that you use in order to eliminate or prune this unnecessary traffic.

Reference: [http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html#vtp\\_pruning](http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html#vtp_pruning)

#### QUESTION 71

Refer to the exhibit.

```
Switch1 (config)#vlan 10
VTP vlan configuration not allowed when device is in CLIENT mode.
Switch1#show interfaces trunk
Switch1#
```

The users in an engineering department that connect to the same access switch cannot access the network. The network engineer found that the engineering VLAN is missing from the database. Which action resolves this problem?

- A. Disable VTP pruning and disable 802.1q.
- B. Update the VTP revision number.
- C. Change VTP mode to server and enable 802.1q.
- D. Enable VTP pruning and disable 802.1q.

**Correct Answer:** C

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Only VTP servers can add new VLANs to the switched network, so to enable vlan 10 on this switch you will first need to change the VTP mode from client to server. Then, you will need to enable 802.1Q trunking to pass this new VLAN along to the other switches.

#### QUESTION 72

Refer to the exhibit.

```
Company A# show vtp status

VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally: 1005
Number of existing VLANs    : 9
VTP Operating Mode          : Server
VTP Domain Name             : company
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled


Company B# show vtp status

VTP Version                : 2
Configuration Revision      : 2
Maximum VLANs supported locally: 1005
Number of existing VLANs    : 42
VTP Operating Mode          : Server
VTP Domain Name             : company
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disable
```

The network switches for two companies have been connected and manually configured for the required VLANs, but users in company A are not able to access network resources in company B when DTP is enabled. Which action resolves this problem?

- A. Delete vlan.dat and ensure that the switch with lowest MAC address is the VTP server.
- B. Disable DTP and document the VTP domain mismatch.
- C. Manually force trunking with switchport mode trunk on both switches.
- D. Enable the company B switch with the vtp mode server command.

**Correct Answer:** C

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Since the number of existing VLANs differ on the switches (9 on A and 42 on B) we know that there is a problem with VTP or the trunking interfaces. The VTP domain names do match and they are both VTP servers so there are no issues there. The only viable solution is that there is a DTP issues and so you must instead manually configure the trunk ports between these two switches so that the VLAN information can be sent to each switch.

#### QUESTION 73

A network engineer must implement Ethernet links that are capable of transporting frames and IP traffic for different broadcast domains that are mutually isolated. Consider that this is a multivendor environment.

Which Cisco IOS switching feature can be used to achieve the task?

- A. PPP encapsulation with a virtual template
- B. Link Aggregation Protocol at the access layer
- C. dot1q VLAN trunking
- D. Inter-Switch Link

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

Here the question asks for transporting “frames and IP traffic for different broadcast domains that are mutually isolated” which is basically a long way of saying VLANs so trunking is needed to carry VLAN information. There are 2 different methods for trunking, 802.1Q and ISL. Of these, only 802.1Q is supported by multiple vendors since ISL is a Cisco proprietary protocol.

**QUESTION 74**

Which statement about using native VLANs to carry untagged frames is true?

- A. Cisco Discovery Protocol version 2 carries native VLAN information, but version 1 does not.
- B. Cisco Discovery Protocol version 1 carries native VLAN information, but version 2 does not.
- C. Cisco Discovery Protocol version 1 and version 2 carry native VLAN information.
- D. Cisco Discovery Protocol version 3 carries native VLAN information, but versions 1 and 2 do not.

**Correct Answer: A**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

Cisco Discovery Protocol (CDP) version 2 passes native VLAN information between Cisco switches. If you have a native VLAN mismatch, you will see CDP error messages on the console output.

Reference: <http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3>

**QUESTION 75**

Refer to the exhibit.

```
SW-1#sh logging
%SPANTREE-SP-2-RECV_PVID_ERR: Received BPDU with inconsistent peer
Vlan id 1 on GigabitEthernet11/2 VLAN2013.
%SPANTREE-SP-2-BLOCK_PVID_PEER: Blocking GigabitEthernet11/2 on
VLAN0001. Inconsistent peer vlan.
```

A multilayer switch has been configured to send and receive encapsulated and tagged frames. VLAN 2013 on the multilayer switch is configured as the native VLAN. Which option is the cause of the spanning-tree error?

- A. VLAN spanning-tree in SW-2 is configured.
- B. spanning-tree bpd-filter is enabled.
- C. 802.1q trunks are on both sides, both with native VLAN mismatch.
- D. VLAN ID 1 should not be used for management traffic because its unsafe.

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Here we see that the native VLAN has been configured as 2013 on one switch, but 1 (the default native VLAN) on the other switch. If you use 802.1Q trunks, you must ensure that you choose a common native VLAN for each port in the trunk. Failure to do this causes Cisco switches to partially shut down the trunk port because having mismatched native VLANs can result in spanning-tree loops. Native VLAN mismatches are detected via spanning tree and Cisco Discovery Protocol (CDP), not via DTP messages. If spanning tree detects a native VLAN mismatch, spanning tree blocks local native VLAN traffic and the remote switch native VLAN traffic on the trunk; however, the trunk still remains up for other VLANs.

Reference: [http://www.informit.com/library/content.aspx?b=CCNP\\_Studies\\_Switching&seqNum=25](http://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=25)

**QUESTION 76**

A network engineer must improve bandwidth and resource utilization on the switches by stopping the inefficient flooding of frames on trunk ports where the frames are not needed.

Which Cisco IOS feature can be used to achieve this task?

- A. VTP pruning
- B. access list
- C. switchport trunk allowed VLAN
- D. VLAN access-map

**Correct Answer: A**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

Cisco advocates the benefits of pruning VLANs in order to reduce unnecessary frame flooding. The “vtp pruning” command prunes VLANs automatically, which stops the inefficient flooding of frames where they are not needed.

Reference: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/24330-185.html>

**QUESTION 77**

Which action allows a network engineer to limit a default VLAN from being propagated across all trunks?

- A. Upgrade to VTP version 3 for advanced feature set support.
- B. Enable VTP pruning on the VTP server.
- C. Manually prune default VLAN with switchport trunk allowed vlans remove.
- D. Use trunk pruning vlan 1.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Manually pruning the default VLAN (1) can only be done with the “switchport trunk allowed vlans remove” command. VLAN 1 is not VTP pruning eligible so it cannot be done via VTP pruning. The “trunk pruning vlan 1” option is not a valid command.

#### QUESTION 78

What is required for a LAN switch to support 802.1q Q-in-Q encapsulation?

- A. Support less than 1500 MTU
- B. Support 1504 MTU or higher
- C. Support 1522 layer 3 IP and IPX packet
- D. Support 1547 MTU only

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The default system MTU for traffic on Catalyst switches is 1500 bytes. Because the 802.1Q tunneling (Q-in-Q) feature increases the frame size by 4 bytes when the extra tag is added, you must configure all switches in the service-provider network to be able to process maximum frames by increasing the switch system MTU size to at least 1504 bytes.

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/tunnel.html>

#### QUESTION 79

Refer to the exhibit.

```
3512xl(config)#int fastEthernet 0/1
3512xl(config-if)#switchport mode trunk
3512xl(config-if)#switchport trunk encapsulation dot1q
```

How many bytes are added to each frame as a result of the configuration?

- A. 4-bytes except the native VLAN
- B. 8-bytes except the native VLAN
- C. 4-bytes including native VLAN
- D. 8-bytes including native VLAN

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN. A VLAN tag adds 4 bytes to the frame. Two bytes are used for the tag protocol identifier (TPID), the other two bytes for tag control information (TCI).

#### QUESTION 80

A network engineer configured a fault-tolerance link on Gigabit Ethernet links G0/1, G0/2, G0/3, and G0/4 between two switches using Ethernet port-channel.

Which action allows interface G0/1 to always actively forward traffic in the port-channel?

- A. Configure G0/1 as half duplex and G0/2 as full duplex.
- B. Configure LACP port-priority on G0/1 to 1.
- C. Configure LACP port-priority on G0/1 to 65535.
- D. LACP traffic goes through G0/4 because it is the highest interface ID.

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

A LACP port priority is configured on each port using LACP. The port priority can be configured automatically or through the CLI. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating. The higher the number, the lower the priority. The valid range is from 1 to 65535. The default is 32768.

Reference: [http://www.cisco.com/c/en/us/td/docs/ios/12\\_2sb/feature/guide/gigeth.html#wp1081491](http://www.cisco.com/c/en/us/td/docs/ios/12_2sb/feature/guide/gigeth.html#wp1081491)

#### QUESTION 81

Which statement about the use of PagP link aggregation on a Cisco switch that is running Cisco IOS Software is true?



- A. PagP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on allow the formation of a channel.
- B. PagP modes are active, desirable, and on. Only the combinations active-desirable, desirable-desirable, and on-on allow the formation of a channel.
- C. PagP modes are active, desirable, and on. Only the combinations active-active, desirable-desirable, and on-on allow the formation of a channel.
- D. PagP modes are off, active, desirable, and on. Only the combinations auto-auto, desirable-desirable, and on-on allow the formation of a channel.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

PagP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on will allow a channel to be formed. The PagP modes are explained below.

1. on: PagP will not run. The channel is forced to come up.
2. off: PagP will not run. The channel is forced to remain down.
3. auto: PagP is running passively. The formation of a channel is desired; however, it is not initiated.
4. desirable: PagP is running actively. The formation of a channel is desired and initiated.

Only the combinations of auto-desirable, desirable-desirable, and on-on will allow a channel to be formed. If a device on one side of the channel does not support PagP, such as a router, the device on the other side must have PagP set to on.

Reference: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2900-xl-series-switches/21041-131.html>

## QUESTION 82

Refer to the exhibit.

```
SW1#show etherchannel summary
Flags: D - down P - in port-channel
I - stand-alone s - suspended
H - Hot-standby (LACP only)
R - Layer3 S - Layer2
U - in use f - failed to allocate aggregator
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 3
Number of aggregators: 3
Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
12      Po12 (SU)        -           Fa0/13(P) Fa0/14(P) Fa0/15(P)
13      Po13 (SU)        -           Fa0/16(P) Fa0/17(P) Fa0/18(P)
14      Po14 (SU)        -           Fa0/19(P) Fa0/20(P) Fa0/21(P)

SW1#show interface trunk
Port Mode Encapsulation  Status Native vlan
Po12 desirable n-isl trunking 1
Po13 desirable n-isl trunking 1
Po14 desirable n-isl trunking 1
Port Vlans allowed on trunk
Po12 1-4094
Po13 1-4094
Po14 1-4094
```

Which EtherChannel negotiation protocol is configured on the interface f0/13 – f0/15?

- A. Link Combination Control Protocol
- B. Port Aggregation Protocol
- C. Port Combination Protocol
- D. Link Aggregation Control Protocol

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

PagP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on will allow a channel to be formed. .

1. on: PAGP will not run. The channel is forced to come up.
2. off: PAGP will not run. The channel is forced to remain down.
3. auto: PAGP is running passively. The formation of a channel is desired; however, it is not initiated.
4. desirable: PAGP is running actively. The formation of a channel is desired and initiated.

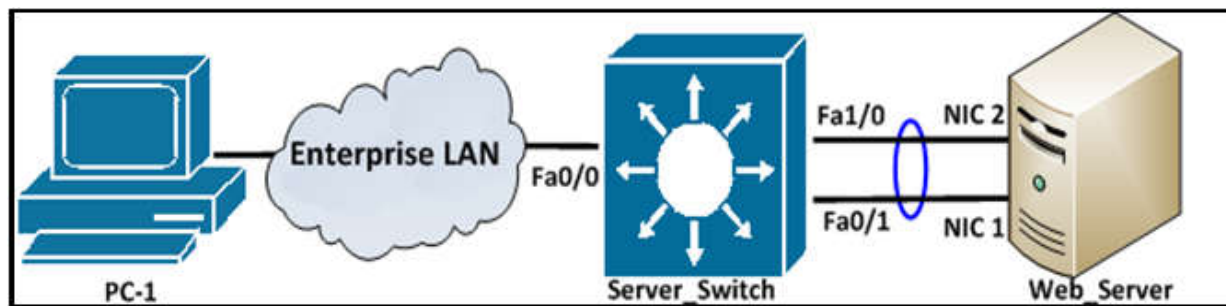
The Link Aggregate Control Protocol (LACP) trunking supports four modes of operation:

- On: The link aggregation is forced to be formed without any LACP negotiation .In other words, the switch neither sends the LACP packet nor processes any inbound LACP packet. This is similar to the on state for PAGP.
- Off: The link aggregation is not formed. We do not send or understand the LACP packet. This is similar to the off state for PAGP.
- Passive: The switch does not initiate the channel but does understand inbound LACP packets. The peer (in active state) initiates negotiation (when it sends out an LACP packet) which we receive and answer, eventually to form the aggregation channel with the peer. This is similar to the auto mode in PAGP.
- Active: We can form an aggregate link and initiate the negotiation. The link aggregate is formed if the other end runs in LACP active or passive mode. This is similar to the desirable mode of PAGP.

In this example, we see that fa 0/13, fa0/14, and fa0/15 are all in Port Channel 12, which is operating in desirable mode, which is only a PAgP mode.

#### QUESTION 83

Refer to the exhibit.



Users of PC-1 experience slow connection when a webpage is requested from the server. To increase bandwidth, the network engineer configured an EtherChannel on interfaces Fa1/0 and Fa0/1 of the server farm switch, as shown here:

```
Server_Switch#sh etherchannel load-balance
EtherChannel Load-Balancing Operational State (src-mac):
Non-IP: Source MAC address
IPv4: Source MAC address
IPv6: Source IP address
Server_Switch#
```

However, traffic is still slow. Which action can the engineer take to resolve this issue?

- A. Disable EtherChannel load balancing.
- B. Upgrade the switch IOS to IP services image.
- C. Change the load-balance method to dst-mac.
- D. Contact Cisco TAC to report a bug on the switch.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

#### Explanation/Reference:

Explanation:

Since this traffic is coming from PC-1, the source MAC address will always be that of PC-1, and since the load balancing method is source MAC, traffic will only be using one of the port channel links. The load balancing method should be changed to destination MAC, since the web server has two NICs traffic will be load balanced across both MAC addresses.

#### QUESTION 84

A network engineer changed the port speed and duplex setting of an existing EtherChannel bundle that uses the PAgP protocol. Which statement describes what happens to all ports in the bundle?

- A. PAgP changes the port speed and duplex for all ports in the bundle.
- B. PAgP drops the ports that do not match the configuration.
- C. PAgP does not change the port speed and duplex for all ports in the bundle until the switch is rebooted.
- D. PAgP changes the port speed but not the duplex for all ports in the bundle.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

#### Explanation/Reference:

Explanation:

PAgP aids in the automatic creation of EtherChannel links. PAgP packets are sent between EtherChannel-capable ports in order to negotiate the formation of a channel. Some restrictions are deliberately introduced into PAgP. The restrictions are:

- PAgP does not form a bundle on ports that are configured for dynamic VLANs. PAgP requires that all ports in the channel belong to the same VLAN or are configured as trunk ports. When a bundle already exists and a VLAN of a port is modified, all ports in the bundle are modified to match that VLAN.
- **PAgP does not group ports that operate at different speeds or port duplex. If speed and duplex change when a bundle exists, PAgP changes the port speed and duplex for all ports in the bundle.**
- PAgP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on allow the formation of a channel. The device on the other side must have PAgP set to on if a device on one side of the channel does not support PAgP, such as a router.

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html>

#### QUESTION 85

Which statement about using EtherChannel on Cisco IOS switches is true?

- A. A switch can support up to eight compatibly configured Ethernet interfaces in an EtherChannel. The EtherChannel provides full-duplex bandwidth up to 800 Mbps only for Fast EtherChannel or 8 Gbps only for Gigabit EtherChannel.
- B. A switch can support up to 10 compatibly configured Ethernet interfaces in an EtherChannel. The EtherChannel provides full-duplex bandwidth up to 1000 Mbps only for Fast EtherChannel or 8 Gbps only for Gigabit EtherChannel.
- C. A switch can support up to eight compatibly configured Ethernet interfaces in an EtherChannel. The EtherChannel provides full-duplex bandwidth up to 800 Mbps only for Fast EtherChannel or 16 Gbps only for Gigabit EtherChannel.
- D. A switch can support up to 10 compatibly configured Ethernet interfaces in an EtherChannel. The EtherChannel provides full-duplex bandwidth up to 1000 Mbps only for Fast EtherChannel or 10 Gbps only for Gigabit EtherChannel.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

#### Explanation/Reference:

Explanation:

An EtherChannel consists of individual Fast Ethernet or Gigabit Ethernet links bundled into a single logical link. The EtherChannel provides full-duplex

bandwidth up to 800 Mbps (Fast EtherChannel) or 8 Gbps (Gigabit EtherChannel) between your switch and another switch or host. Each EtherChannel can consist of up to eight compatibly configured Ethernet interfaces. All interfaces in each EtherChannel must be the same speed, and all must be configured as either Layer 2 or Layer 3 interfaces.

Reference: <http://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html>

#### QUESTION 86

Refer to the exhibit.

```
S1# show etherchannel summary
Flags: D - down      P - bundled in port-channel
      I - stand-alone s - suspended
      H - Hot-standby (LACP only)
      R - Layer3      S - Layer2
      U - in use      f - failed to allocate aggregator

      M - not in use, minimum links not met
      u - unsuitable for bundling
      w - waiting to be aggregated
      d - default port

Number of channel-groups in use: 1
Number of aggregators:          1

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
1      Po1(SU)        LACP        Fa0/13(P) Fa0/14(P) Fa0/15(P)
```

Which statement about switch S1 is true?

- A. Physical port Fa0/13, Fa0/14, and Fa0/15 successfully formed a Layer 2 port-channel interface using an open standard protocol.
- B. Logical port Fa0/13, Fa0/14, and Fa0/15 successfully formed a Layer 2 physical port-channel interface using a Cisco proprietary protocol.
- C. Physical port Fa0/13, Fa0/14, and Fa0/15 successfully formed a Layer 3 port-channel interface using a Cisco proprietary protocol.
- D. Logical port Fa0/13, Fa0/14, and Fa0/15 successfully formed a Layer 3 physical port-channel interface using an open standard protocol.

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

These three ports show that they are in Port Channel 1, and the (SU) means they are in use and operating at layer 2. The protocol used for this port channel shows as LACP, which is a standards based protocol, as opposed to PagP, which is Cisco proprietary.

#### QUESTION 87

What happens on a Cisco switch that runs Cisco IOS when an RSTP-configured switch receives 802.1d BPDU?

- A. 802.1d does not understand RSTP BPDUs because they are different versions, but when a RSTP switch receives an 802.1d BPDU, it responds with an 802.1d BPDU and eventually the two switches run 802.1d to communicate.
- B. 802.1d understands RSTP BPDUs because they are the same version, but when a RSTP switch receives a 802.1d BPDU, it responds with a 802.1d BPDU and eventually the two switches run 802.1d to communicate.
- C. 802.1d does not understand RSTP BPDUs because they are different versions, but when a RSTP switch receives a 802.1d BPDU, it does not respond with a 802.1d BPDU.
- D. 802.1d understands RSTP BPDUs because they are the same version, but when a RSTP switch receives a 802.1d BPDU, it does not respond with a 802.1d BPDU and eventually the two switches run 802.1d to communicate.

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

For backward compatibility with 802.1D switches, RSTP selectively sends 802.1D configuration BPDUs and TCN BPDUs on a per-port basis.

When a port is initialized, the migrate-delay timer is started (specifies the minimum time during which RSTP BPDUs are sent), and RSTP BPDUs are sent. While this timer is active, the switch processes all BPDUs received on that port and ignores the protocol type.

If the switch receives an 802.1D BPDU after the port migration-delay timer has expired, it assumes that it is connected to an 802.1D switch and starts using only 802.1D BPDUs. However, if the RSTP switch is using 802.1D BPDUs on a port and receives an RSTP BPDU after the timer has expired, it restarts the timer and starts using RSTP BPDUs on that port.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/spantree.html>

#### QUESTION 88

When two MST instances (MST 1 and MST 2) are created on a switch, what is the total number of spanning-tree instances running on the switch?

- A. 1
- B. 2
- C. 3



D. 4

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Unlike other spanning tree protocols, in which all the spanning tree instances are independent, MST establishes and maintains IST, CIST, and CST spanning trees:

- An IST is the spanning tree that runs in an MST region.

**Within each MST region, MST maintains multiple spanning tree instances. Instance 0 is a special instance for a region, known as the IST. All other MST instances are numbered from 1 to 4094. In the case for this question, there will be the 2 defined MST instances, and the special 0 instance, for a total of 3 instances.**

The IST is the only spanning tree instance that sends and receives BPDUs. All of the other spanning tree instance information is contained in MSTP records (M-records), which are encapsulated within MST BPDUs. Because the MST BPDU carries information for all instances, the number of BPDUs that need to be processed to support multiple spanning tree instances is usernamcantly reduced.

All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root bridge ID, root path cost, and so forth. By default, all VLANs are assigned to the IST.

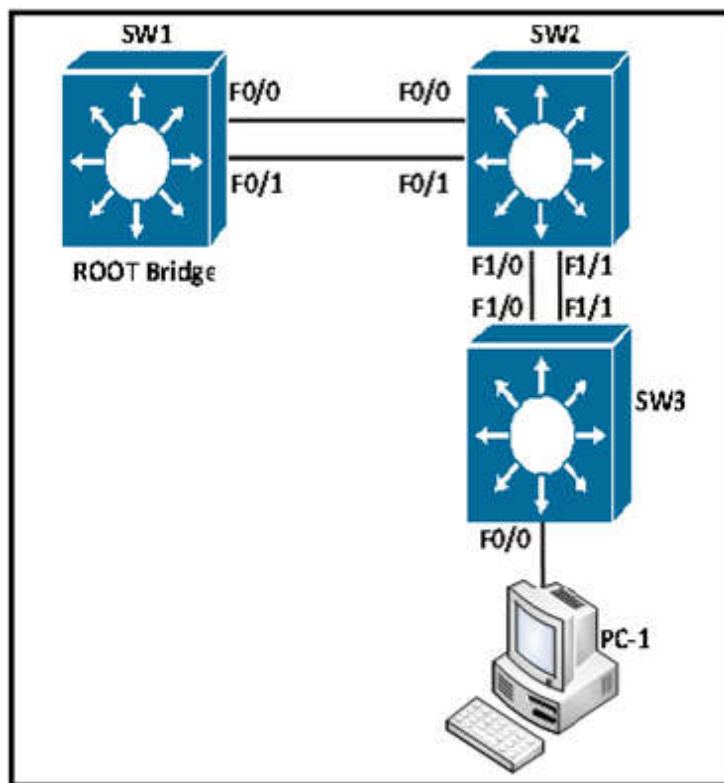
An MST instance is local to the region; for example, MST instance 1 in region A is independent of MST instance 1 in region B, even if regions A and B are interconnected.

- A CIST is a collection of the ISTs in each MST region.
- The CST interconnects the MST regions and single spanning trees.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/spantree.html>

#### QUESTION 89

Refer to the exhibit.



f1/0 and f1/1 have the same end-to-end path cost to the designated bridge. Which action is needed to modify the Layer 2 spanning-tree network so that traffic for PC1 VLAN from switch SW3 uses switchport f1/1 as a primary port?

- A. Modify the spanning-tree port-priority on SW1 f1/1 to 0 and f1/0 to 16.
- B. Modify the spanning-tree port-priority on SW1 f1/1 to 16 and f1/0 to 0.
- C. Modify the spanning-tree port-priority on SW2 f1/1 to 0 and f1/0 to 16.
- D. Modify the spanning-tree port-priority on SW2 f1/1 to 16 and f1/0 to 0.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

If a loop occurs, STP considers port priority when selecting a LAN port to put into the forwarding state. You can assign higher priority values to LAN ports that you want STP to select first and lower priority values to LAN ports that you want STP to select last. If all LAN ports have the same priority value, STP puts the LAN port with the lowest LAN port number in the forwarding state and blocks other LAN ports. The possible priority range is 0 through 240 (default 128), configurable in increments of 16. A lower path cost represents higher-speed transmission and is preferred.

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/lanswitch/configuration/xs-3s/lanswitch-xe-3s-book/lsw-span-tree-prot.pdf>

#### QUESTION 90

Refer to the exhibit.



```
SW1#show spanning-tree vlan 1
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 1
Address 001b.bbbb.dddd
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 1 (priority 0 sys-id-ext 1)
Address 001b.bbbb.dddd

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
```

| Interface | Role | Sts | Cost | Prio.Nbr | Type |
|-----------|------|-----|------|----------|------|
| Fa0/1     | Desg | FWD | 19   | 128.15   | P2p  |
| Fa0/2     | Desg | FWD | 19   | 128.16   | P2p  |
| Fa0/3     | Desg | FWD | 19   | 128.17   | P2p  |
| Fa0/4     | Desg | FWD | 19   | 128.18   | P2p  |
| Fa0/5     | Desg | FWD | 19   | 128.19   | P2p  |
| Fa0/6     | Desg | FWD | 19   | 128.19   | P2p  |

Why would the switch be considered as a root bridge?

- A. The bridge priority is 1 and all ports are forwarding.
- B. The switch priority for VLAN 1 and the macro specifies "This Bridge is the root".
- C. The bridge priority is 128.19 and all ports are forwarding.
- D. The switch priority value is zero, it has the lowest priority value for VLAN 1.

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

For priority, the range is 0 to 61440 in increments of 4096; the default is 32768. The lower the number, the more likely the switch will be chosen as the root switch.

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1\\_9\\_ea1/configuration/guide/swstp.html#wp1020666](http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swstp.html#wp1020666)

#### QUESTION 91

Refer to the exhibit.

```
Switch# Show run
interface FastEthernet0/13
spanning-tree cost 1000
!
interface FastEthernet0/14
spanning-tree cost 1000
!
interface FastEthernet0/15
spanning-tree cost 1000
!
interface FastEthernet0/20
spanning-tree cost 2
!
interface FastEthernet0/21
spanning-tree cost 1
```

All ports are members of VLAN 10. Considering the default cost of upstream bridges to the root bridge is equal, which option will be the new root port for VLAN 10?

- A. interface f0/13
- B. interface f0/14
- C. interface f0/15
- D. interface f0/21

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

**Root Port election on each bridge**

**Each (non-Root) bridge has exactly one Root Port, which represents the best path to the Root Bridge.**

- Total Path Cost to root - lowest prevails (local Root Port cost added upon receipt of Configuration – PDUs on that port, from the direction of Root Bridge)
- Connected Bridge ID - lowest prevails
- Connected Port ID (Port Priority + Port#) - lowest prevail–

- Local Port ID - lowest prevails

In this case, fa0/21 has the lowest cost, so it will be the root port.

Reference: [https://community.extremenetworks.com/extreme/topics/802\\_1d\\_spanning\\_tree\\_election\\_rules](https://community.extremenetworks.com/extreme/topics/802_1d_spanning_tree_election_rules)

#### QUESTION 92

A network engineer is trying to deploy a PC on a network. The engineer observes that when the PC is connected to the network, it takes 30 to 60 seconds for the PC to see any activity on the network interface card. Which Layer 2 enhancement can be used to eliminate this delay?

- A. Configure port duplex and speed to auto negotiation.
- B. Configure port to duplex full and speed 1000.
- C. Configure spanning-tree portfast.
- D. Configure no switchport.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

When first powered on, each port goes through 4 states to ensure that there are no physical loops in the layer 2 broadcast domain. These steps are outlined as follows. With the initial version of spanning tree, this process could take from 30-60 seconds.

1. Blocking – A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.
2. Listening – The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state.
3. Learning – While the port does not yet forward frames (packets) it does learn source addresses from frames received and adds them to the filtering database (switching database)
4. Forwarding – A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

STP PortFast causes a Layer 2 LAN interface configured as an access port to enter the forwarding state immediately, bypassing the listening and learning states.

Reference: <http://net.cmed.us/Home/ethernet-and-ip/spanning-tree-protocol>

#### QUESTION 93

A network engineer configured an Ethernet switch using these commands.

```
Switch#(config) # Spanning-tree portfast bpduguard default
```

Which statement about the spanning-tree portfast feature on the switch is true?

- A. If an interface is enabled for portfast receives BPDU, the port goes through the spanning-tree listening, learning, and forwarding states.
- B. If an interface is enabled for portfast receives BPDU, the port does not go through the spanning-tree listening, learning, and forwarding states.
- C. If an interface is enabled for portfast receives BPDU, the port is shut down immediately.
- D. If an interface is enabled for portfast receives BPDU, the port goes into the spanning-tree inconsistent state.

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

STP PortFast causes a Layer 2 LAN interface configured as an access port to enter the forwarding state immediately, bypassing the listening and learning states. However, the “Spanning-tree portfast bpduguard default” command specifies that if a BPDU is received on that port, then the default action of STP of listening, learning, and forwarding states should be used.

#### QUESTION 94

Which statement describes what happens when a port configured with root guard receives a superior BPDU?

- A. The port goes into errdisabled state and stops forwarding traffic.
- B. The port goes into BPDU-inconsistent state and stops forwarding traffic.
- C. The port goes into loop-inconsistent state and stops forwarding traffic.
- D. The port goes into root-inconsistent state and stops forwarding traffic.

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The root guard ensures that the port on which root guard is enabled is the designated port. Normally, root bridge ports are all designated ports, unless two or more ports of the root bridge are connected together. If the bridge receives superior STP Bridge Protocol Data Units (BPDUs) on a root guard-enabled port, root guard moves this port to a root-inconsistent STP state. This root-inconsistent state is effectively equal to a listening state. No traffic is forwarded across this port. In this way, the root guard enforces the position of the root bridge.

Reference: [http://www.cisco.com/en/US/tech/tk389/tk621/technologies\\_tech\\_note09186a00800ae96b.shtml](http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96b.shtml)

#### QUESTION 95

Which statement about restrictions for multichassis LACP is true?

- A. It is available only on a Cisco Catalyst 6500 Series chassis.
- B. It does not support 1Gb links.
- C. Converting a port channel to mLACP can cause a service disruption.
- D. It is not available in VSS.

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

When configuring mLACP for Server Access, follow these guidelines and restrictions:

- PFC3A mode does not support the mLACP for server access feature.
- VSS mode does not support the mLACP for server access feature.
- No more than 100 VLANs can be active on a switch configured as a PoA.
- mLACP does not support half-duplex links.
- mLACP does not support multiple neighbors.
- **Converting a port channel to mLACP can cause a service disruption.**
- The DHD system priority must be lower (higher numerically) than the PoA system priority.

Reference: [http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mlacp\\_server\\_support.html](http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/mlacp_server_support.html)

**QUESTION 96**

What is the maximum number of 10 Gigabit Ethernet connections that can be utilized in an EtherChannel for the virtual switch link?

- A. 4
- B. 6
- C. 8
- D. 12

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

The VSS is made up of the following:

- Virtual switch members: Cisco Catalyst 6500 Series Switches (up to two switches with initial release) deployed with the Virtual Switching Supervisor 720 10GE
- **Virtual switch link (VSL): 10 Gigabit Ethernet connections (up to eight using EtherChannel) between the virtual switch members.**

Reference: [http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod\\_gas0900aecd806ed74b.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_gas0900aecd806ed74b.html)

**QUESTION 97**

Which statement describes what happens if all VSL connections between the virtual switch members are lost?

- A. Both virtual switch members cease to forward traffic.
- B. The VSS transitions to the dual active recovery mode, and both virtual switch members continue to forward traffic independently.
- C. The virtual switch members reload.
- D. The VSS transitions to the dual active recovery mode, and only the new active virtual switch continues to forward traffic.

**Correct Answer: D**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

Q. What happens if all VSL connections between the virtual switch members are lost?

A. VSLs can be configured with up to eight links between the two switches across any combination of line cards or supervisor ports to provide a high level of redundancy. If for some rare reason all VSL connections are lost between the virtual switch members leaving both the virtual switch members up, the VSS will transition to the dual active recovery mode.

The dual active state is detected rapidly (subsecond) by any of the following three methods:

- Enhancement to PagP used in MEC with connecting Cisco switches
- L3 Bidirectional Forwarding Detection (BFD) configuration on a directly connected link (besides VSL) between virtual switch members or through an L2 link through an access layer switch
- L2 Fast-Hello Dual-Active Detection configuration on a directly connected link (besides VSL) between virtual switch members (supported with 12.2(33) SXI)

In the dual active recovery mode, all interfaces except the VSL interfaces are in an operationally shut down state in the formerly active virtual switch member. The new active virtual switch continues to forward traffic on all links.

Reference: [http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod\\_gas0900aecd806ed74b.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_gas0900aecd806ed74b.html)

**QUESTION 98**

Which statement describes what happens when a switch enters dual active recovery mode?

- A. The switch shuts down and waits for the VSL link to be restored before sending traffic.
- B. All interfaces are shut down in the formerly active virtual switch member, but the new active virtual switch forwards traffic on all links.
- C. The switch continues to forward traffic out all links and enables spanning tree on VSL link and all other links to prevent loops.
- D. The VSS detects which system was last in active state and shuts down the other switch.

**Correct Answer: B**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

In the dual active recovery mode, all interfaces except the VSL interfaces are in an operationally shut down state in the formerly active virtual switch member. The new active virtual switch continues to forward traffic on all links.

Reference: [http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod\\_gas0900aecd806ed74b.html](http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_gas0900aecd806ed74b.html)

## QUESTION 99

### SIMULATION

#### Instructions

To configure a switch click on the console host icon in the topology.

You can click on the buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation. The **help** command does not display all commands of the help system.

#### Scenario:

You work for SWITCH.com. They have just added a new switch (SwitchB) to the existing network as shown in the topology diagram. You have been tasked with completing the needed configuring of SwitchA and SwitchB. RouterA is currently configured correctly and is providing the routing function for devices on SwitchA and SwitchB. SwitchA is currently configured correctly, but will need to be modified to support the addition of SwitchB. SwitchB has a minimal configuration. SwitchA and SwitchB use Cisco as the enable password.

**All interface commands must be entered at the physical interface level.**

**When entering the range command, add a space between the interface numbers (e.g., fa0/1-2)**

#### Configuration Requirements for SwitchA

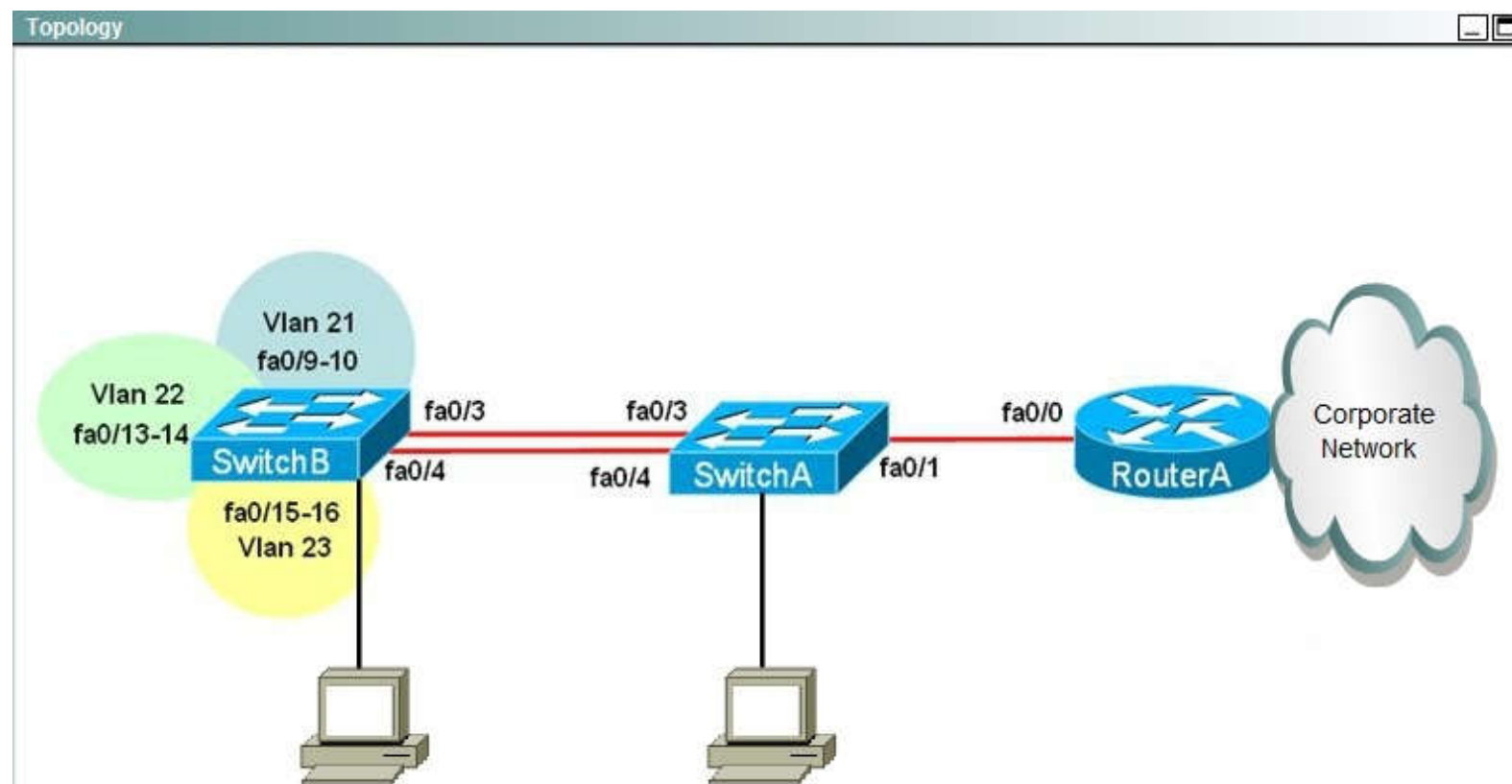
- The VTP and STP configuration models on Switch A should not be modified.
- SwitchA needs to be the root switch for vlans 11, 12, 13, 21, 22, and 23.
- All other vlans should be left at their default values.

#### Configuration Requirements for SwitchB

- Vlan21
- Name: Marketing
- will support two servers attached to fa0/9 and fa0/10
- Vlan22
- Name: Sales
- will support two servers attached to fa0/13 and fa0/14
- Vlan23
- Name: Engineering
- will support two servers attached to fa0/15 and fa0/16
- Access ports that connect to server should transition immediately to forwarding state upon detecting the connection of a device
- SwitchB VTP mode needs to be the same as SwitchA.
- SwitchB must operate in the same spanning tree mode as SwitchA.
- No routing is to be configured on SwitchB.
- Only the SVI Vlan 1 is to be configured and it is to use address 192.168.1.11/24.

#### Inter-switch Connectivity Configuration Requirements

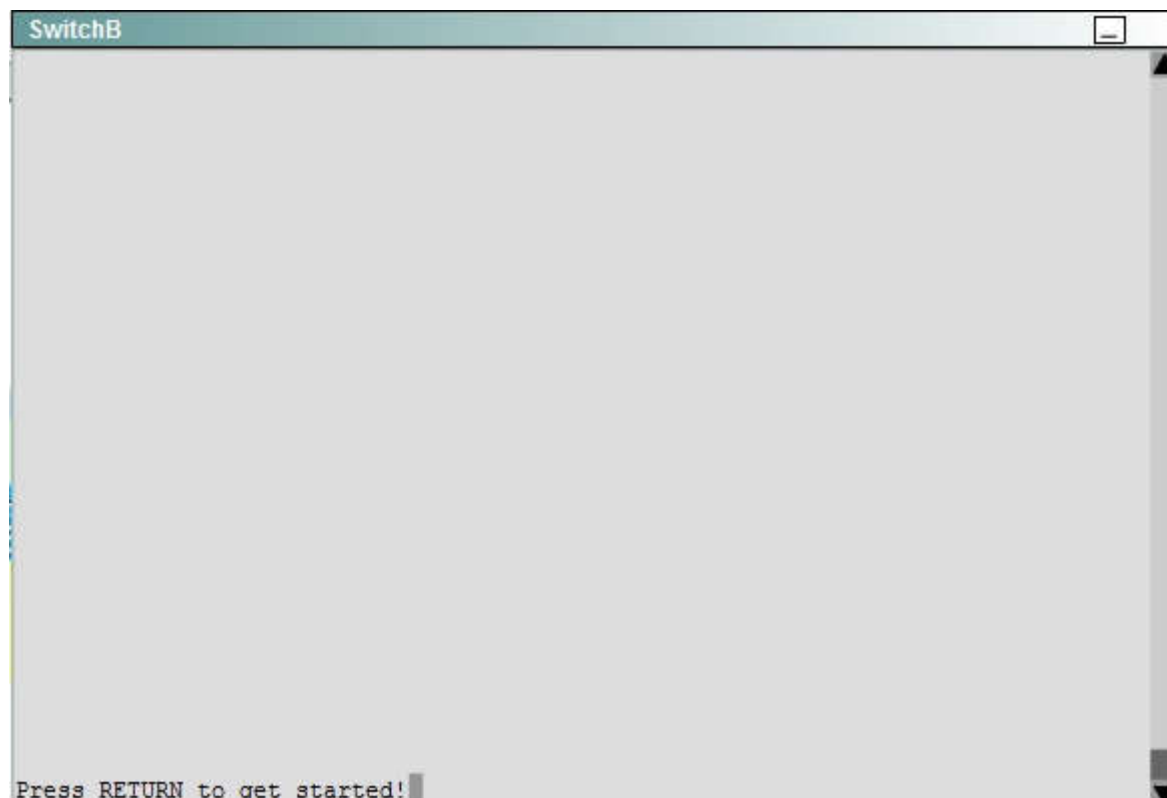
- For operational and security reasons trunking should be unconditional and Vlans 1, 21, 22 and 23 should be tagged when traversing the trunk link.
- The two trunks between SwitchA and SwitchB need to be configured in a mode that allows for the maximum use of their bandwidth for all vlans. This mode should be done with a non-proprietary protocol, with SwitchA controlling activation.
- Propagation of unnecessary broadcasts should be limited using manual pruning on this trunk link.





SwitchA

```
% Access VLAN does not exist. Creating vlan 98
%LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/3, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/4, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/7, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to administratively down
% Access VLAN does not exist. Creating vlan 11
% Access VLAN does not exist. Creating vlan 13
%LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/12, changed state to administratively down
% Access VLAN does not exist. Creating vlan 12
%LINK-3-UPDOWN: Interface FastEthernet0/17, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/18, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/19, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/20, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/21, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/22, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/23, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/24, changed state to administratively down
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to administratively down
%LINK-3-UPDOWN: Interface GigabitEthernet0/2, changed state to administratively down
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/16, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/16, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/15, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/15, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/14, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/14, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/13, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/13, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/10, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/10, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/9, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/9, changed state to up
Press RETURN to get started!
```



**Correct Answer:** Here are steps

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

**Initial Configuration** (some lines have been removed)

| SwA:                          | Sw-B:                          |
|-------------------------------|--------------------------------|
| hostname Sw-A                 | hostname Sw-B                  |
| !                             | !                              |
| vtp mode transparent          | vtp mode server                |
| !                             | !                              |
| spanning-tree mode rapid-pvst | spanning-tree mode pvst        |
| !                             | !                              |
| vlan 98                       | interface FastEthernet0/3      |
| !                             | !                              |
| vlan 99                       | interface FastEthernet0/4      |
| name TrunkNative              | !                              |
| !                             | interface FastEthernet0/9      |
| interface FastEthernet0/1     | !                              |
| switchport access vlan 98     | interface FastEthernet0/10     |
| switchport mode access        | !                              |
| !                             | interface FastEthernet0/13     |
| interface FastEthernet0/3     | !                              |
| switchport access vlan 98     | interface FastEthernet0/14     |
| switchport mode access        | !                              |
| !                             | interface FastEthernet0/15     |
| interface FastEthernet0/4     | !                              |
| switchport access vlan 98     | interface FastEthernet0/16     |
| switchport mode access        | !                              |
| !                             | interface Vlan1                |
| interface Vlan1               | no ip address                  |
| no ip address                 | shutdown                       |
| shutdown                      | !                              |
| !                             | ip default-gateway 192.168.1.1 |
| end                           | !                              |
|                               | end                            |

### Solution

SW-A (close to router)

Note: If Sw-A does not have Vlan 11, 12, 13 we have to create them first with command "SW-A(config)#vlan 11,12,13"

SW-A(config)#spanning-tree vlan 11-13,21-23 root primary

SW-A(config)#vlan 21

SW-A(config-vlan)#name Marketing

SW-A(config-vlan)#exit

SW-A(config)#vlan 22

SW-A(config-vlan)#name Sales

SW-A(config-vlan)#exit

SW-A(config)#vlan 23

SW-A(config-vlan)#name Engineering

SW-A(config-vlan)#exit

SW-A(config)#interface range fa0/3 – 4

SW-A(config-if-range)#no switchport mode access

SW-A(config-if-range)#no switchport access vlan 98 (These two commands must be deleted to form a trunking link)



```
SW-A(config-if-range)#channel-group 1 mode active
SW-A(config-if-range)#channel-protocol lacp
SW-A(config-if-range)#no shutdown
SW-A(config-if)#interface port-channel 1
SW-A(config-if)#switchport mode trunk
SW-A(config-if)#switchport trunk native vlan 99 //this command will prevent the "Native VLAN mismatched" error on both switches
SW-A(config-if)#switchport trunk allowed vlan 1,21-23
SW-A(config-if)#no shut
Note: When you apply commands under "interface port-channel 1", the same commands will be automatically applied to the physical member interfaces (of port-channel 1) so you don't need to type them under physical member interfaces again.
```

```
SW-B (far from router)
SW-B(config)#vlan 21
SW-B(config-vlan)#name Marketing
SW-B(config-vlan)#exit
SW-B(config)#vlan 22
SW-B(config-vlan)#name Sales
SW-B(config-vlan)#exit
SW-B(config)#vlan 23
SW-B(config-vlan)#name Engineering
SW-B(config-vlan)#exit
SW-B(config)#vlan 99
SW-B(config-vlan)#name TrunkNative // not necessary to name it but just name it same as SwitchA
SW-B(config-vlan)#exit
SW-B(config)#interface range fa0/9 – 10
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport access vlan 21
SW-B(config-if-range)#spanning-tree portfast
SW-B(config-if-range)#no shutdown
SW-B(config-if-range)#exit
SW-B(config)#interface range fa0/13 – 14
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport access vlan 22
SW-B(config-if-range)#spanning-tree portfast
SW-B(config-if-range)#no shutdown
SW-B(config-if-range)#exit
SW-B(config)#interface range fa0/15 – 16
SW-B(config-if-range)#switchport mode access
SW-B(config-if-range)#switchport access vlan 23
SW-B(config-if-range)#spanning-tree portfast
SW-B(config-if-range)#no shutdown
SW-B(config-if-range)#exit
SW-B(config)#vtp mode transparent
SW-B(config)#spanning-tree mode rapid-pvst //Same as Sw-A
SW-B(config)#ip default-gateway 192.168.1.1 (you can get this IP from SW-A with command show cdp neighbour detail)
SW-B(config)#interface vlan 1
SW-B(config-if)#ip address 192.168.1.11 255.255.255.0
SW-B(config-if)#no shutdown
SW-B(config-if)#exit
SW-B(config)#interface range fa0/3 – 4
SW-B(config-if-range)#channel-group 1 mode passive //mode passive because "SwitchA controlling activation"
SW-B(config-if-range)#channel-protocol lacp
SW-B(config-if-range)#no shutdown
SW-B(config-if)#interface port-channel 1
SW-B(config-if)#switchport trunk encapsulation dot1q
SW-B(config-if)#switchport mode trunk
SW-B(config-if)#switchport trunk native vlan 99 //this command will prevent the "Native VLAN mismatched" error on both switches
SW-B(config-if)#switchport trunk allowed vlan 1,21-23
SW-B(config-if)#no shut
Note: For Sw-B we have to set the 802.1q trunking protocol (switchport trunk encapsulation dot1q) before converting it into a trunk because it is a 3500 series (or higher) switch which supports both ISL and 802.1Q and we have to explicitly set which trunking protocol to be used. Sw-A is a 2900x series (or lower) switch and does not support ISL trunking protocol (802.1Q is the only supported trunking protocol) so we can apply "switchport mode trunk" directly.
```

**Some guidelines for configuring SwitchA & SwitchB:**  
**Configuration Requirements for SwitchA**

|                                                                                                                                                                                                                                                                     |                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>- The VTP and STP configuration modes on SwitchA should not be modified.</li><li>- SwitchA needs to be the root switch for vlans 11, 12, 13, 21, 22 and 23. All other vlans should be left are their default values</li></ul> | <pre>SW-A(config)#spanning-tree vlan 11-13,21-23 root primary</pre> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|

**Configuration Requirements for SwitchB**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                   |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Vlan 21, Name: Marketing, will support two servers attached to fa0/9 and fa0/10</li> <li>- Vlan 22, Name: Sales, will support two servers attached to fa0/13 and fa0/14</li> <li>- Vlan 23, Name: Engineering, will support two servers attached to fa0/15 and fa0/16</li> <li>- Access ports that connect to server should transition immediately to forwarding state upon detecting the connection of a device.</li> </ul> | <pre>vlan ... name ... (VLANs must be created on both switches if not exist) interface range fa0/x - y switchport mode access switchport access vlan spanning-tree portfast</pre> |
| <ul style="list-style-type: none"> <li>- SwitchB VTP mode needs to be the same as SwitchA.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                 | <pre>vtp mode transparent</pre>                                                                                                                                                   |
| <ul style="list-style-type: none"> <li>- SwitchB must operate in the same spanning tree mode as SwitchA.</li> </ul>                                                                                                                                                                                                                                                                                                                                                   | <pre>spanning-tree mode rapid-pvst</pre>                                                                                                                                          |
| <ul style="list-style-type: none"> <li>- No routing is to be configured on SwitchB.</li> <li>- Only the SVI vlan 1 is to be configured and it is to use address 192.168.1.11/24.</li> </ul>                                                                                                                                                                                                                                                                           | <pre>interface vlan 1 ip address 192.168.1.11 255.255.255.0</pre>                                                                                                                 |

#### Inter-switch Connectivity Configuration Requirements:

|                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- For operational and security reasons trunking should be unconditional and Vlans 1, 21, 22 and 23 should tagged when traversing the trunk link.</li> <li>- The two trunks between SwitchA and SwitchB need to be configured in a mode that allows for the maximum use of their bandwidth for all Vlans. This mode should be done with a non-proprietary protocol, with SwitchA controlling activation.</li> </ul> | <pre>SW-A(config)#interface range fa0/3 - 4 SW-A(config-if)#no switchport mode access SW-A(config-if)#no switchport access vlan 98 Note: Two above commands must be deleted first to form a trunking link.</pre> <p>Although the first requirement asks us to configure trunking but we can ignore this task because we only need to configure trunking under their Port-channel (in the next task)</p> <ul style="list-style-type: none"> <li>- The two trunks between SwitchA and SwitchB need to be configured in a mode that allows for the maximum use of their bandwidth for all Vlans:</li> </ul> <pre>SW-A(config)#interface range fa0/3 - 4 SW-A(config-if)#channel-group 1 mode active SW-A(config-if)#channel-protocol lacp SW-A(config-if)#no shutdown</pre> <ul style="list-style-type: none"> <li>- Trunking should be unconditional and Vlans 1, 21, 22 and 23 should tagged when traversing the trunk link:</li> </ul> <pre>SW-A(config-if)#interface port-channel 1 SW-A(config-if)#switchport mode trunk SW-A(config-if)#switchport trunk native vlan 99 //this command will prevent the "Native VLAN mismatched" error on both switches SW-A(config-if)#no shut</pre> <pre>----- SW-B(config)#interface range fa0/3 - 4 SW-B(config-if)#channel-group 1 mode passive SW-B(config-if)#channel-protocol lacp SW-B(config-if)#no shutdown SW-B(config-if)#interface port-channel 1 SW-B(config-if)#switchport trunk encapsulation dot1q SW-B(config-if)#switchport mode trunk SW-B(config-if)#switchport trunk native vlan 99 //this command will prevent the "Native VLAN mismatched" error on both switches SW-B(config-if)#no shut</pre> |
| <ul style="list-style-type: none"> <li>- Propagation of unnecessary broadcasts should be limited using manual pruning on this trunk link.</li> </ul>                                                                                                                                                                                                                                                                                                      | <pre>SW-A(config)#interface port-channel 1 SW-A(config-if)#switchport trunk allowed vlan 1,21-23 ----- SW-B(config)#interface port-channel 1 SW-B(config-if)#switchport trunk allowed vlan 1,21-23 Note: When configure this command under Port-channel 1, the same command will be applied to physical member interfaces (of port-channel 1) so you don't need to type them under physical member interfaces again.</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Some notes for this sim:

- + You should check the initial status of both switches with these commands: **show vtp status** (transparent mode on switchA and we have to set the same mode on switchB), **show spanning-tree [summary]** (rapid-pvst mode on switchA and we have to set the same mode on switchB), **show vlan** (check the native vlan and the existence of vlan99), **show etherchannel 1 port-channel** and **show ip int brief**(check if Port-channel 1 has been created and make sure it is up),**show run** (to check everything again).
- + When using "int range f0/x - y" command hit space bar before and after "-" otherwise the simulator does not accept it.
- + You must create vlan 99 for the switchB. SwitchA already have vlan 99 configured.
- + At the end, you can try to ping from SwitchB to RouterA (you can get the IP on RouterA via the show cdp neighbors detail on SwitchA), not sure if it can ping or not. If not, you can use the "ip default-gateway 192.168.1.1" on SwitchB.
- + The name of SwitchA and SwitchB can be swapped or changed so be careful to put your configuration into appropriate switch.



### QUESTION 100

#### SIMULATION

You have been tasked with configuring multilayer SwitchC, which has a partial configuration and has been attached to RouterC as shown in the topology diagram.

**You need to configure SwitchC so that Hosts H1 and H2 can successfully ping the server S1. Also SwitchC needs to be able to ping server S1.**

Due to administrative restrictions and requirements you should not add/delete vlans or create trunk links. Company policies forbid the use of static or default routing. All routes must be learned via EIGRP 65010 routing protocol.

You do not have access to RouterC. RouterC is correctly configured. No trunking has been configured on RouterC.

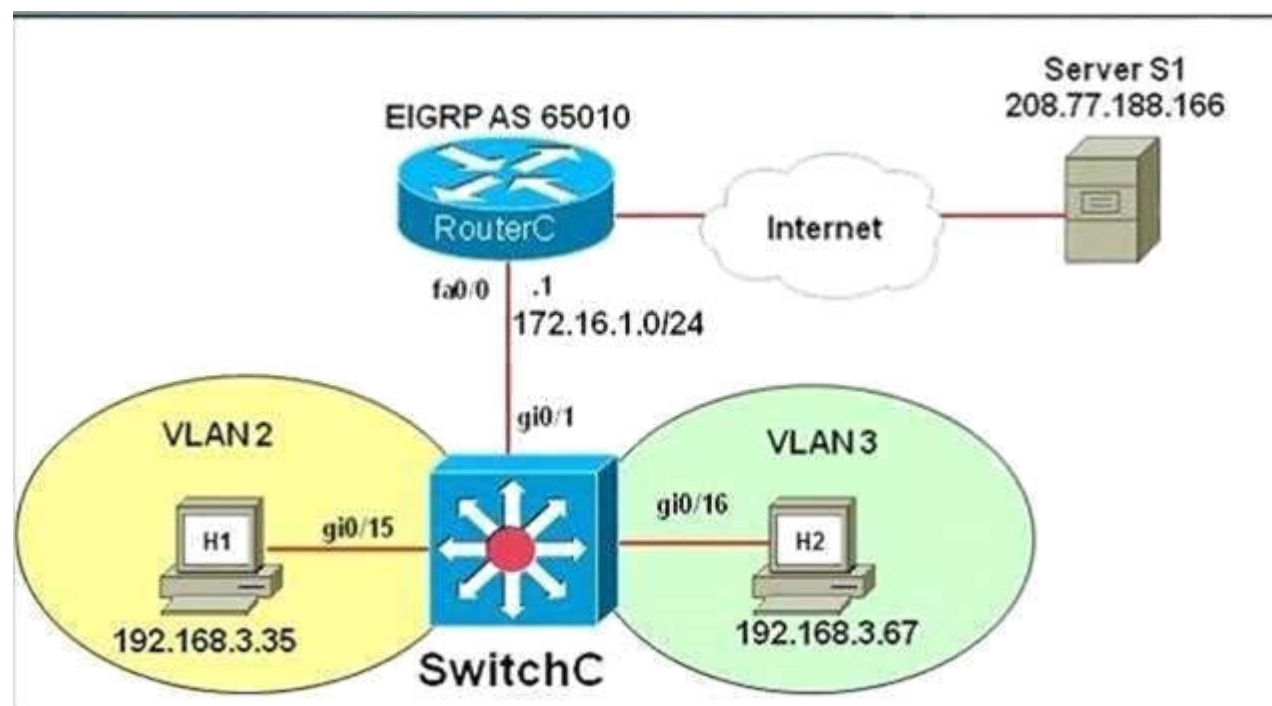
Routed interfaces should use the lowest host on a subnet when possible. The following subnets are available to implement this solution:

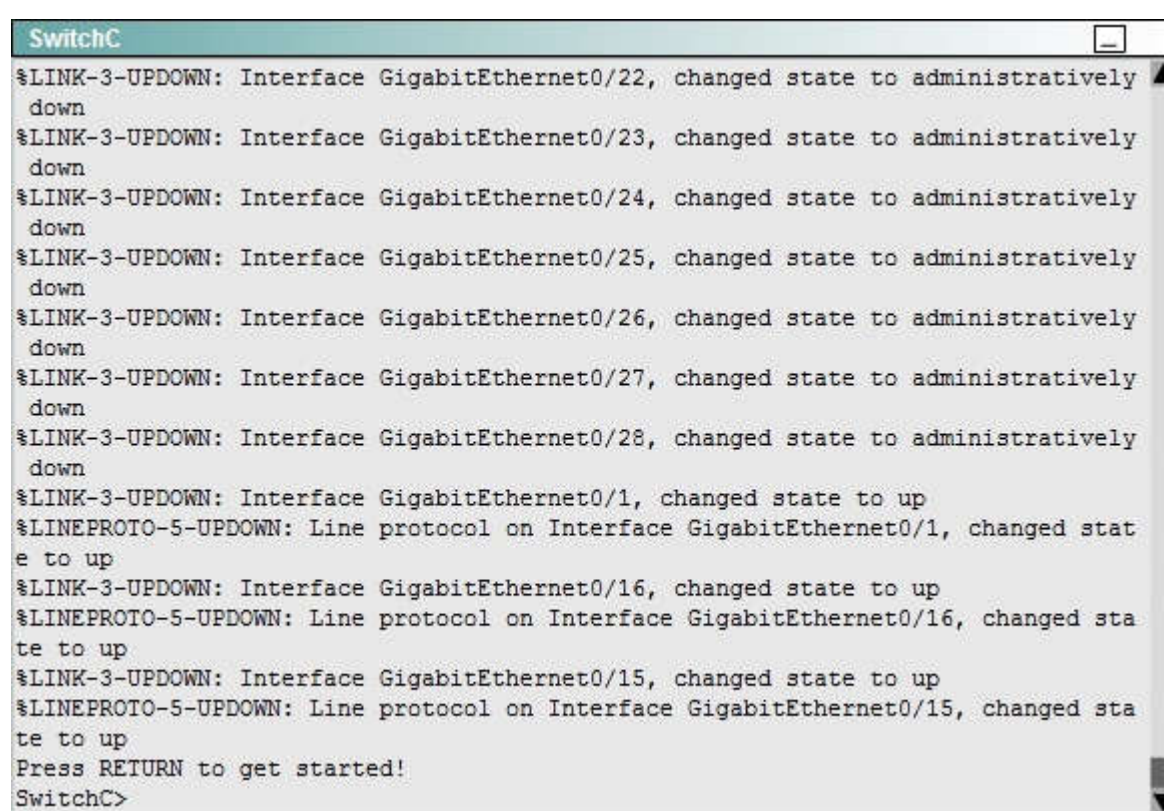
- 10.10.10.0/24
- 190.200.250.32/27
- 190.200.250.64/27

Hosts H1 and H2 are configured with the correct IP address and default gateway.  
SwitchC uses Cisco as the enable password.

Routing must only be enabled for the specific subnets shown in the diagram.

Note: Due to administrative restrictions and requirements you should not add or delete VLANs, changes VLAN port assignments or create trunks. Company policies forbid the use of static or default routing. All routes must be learned via the EIGRP routing protocol.





**Correct Answer:** See the solution below

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

There are two ways to configure interVLAN routing in this case:

- + Use RouterC as a "router on a stick" and SwitchC as a pure Layer2 switch. Trunking must be established between RouterC and SwitchC.
- + Only use SwitchC for interVLAN routing without using RouterC, SwitchC should be configured as a Layer 3 switch (which supports ip routing function as a router). No trunking requires.

The question clearly states "No trunking has been configured on RouterC" so RouterC does not contribute to interVLAN routing of hosts H1 & H2 -> SwitchC must be configured as a Layer 3 switch with SVIs for interVLAN routing.

We should check the default gateways on H1 & H2. Click on H1 and H2 and type the "ipconfig" command to get their default gateways.

Answer:

\>ipconfig

We will get the default gateways as follows:

**Host1:**

+ Default gateway: 190.200.250.33

**Host2:**

+ Default gateway: 190.200.250.65

Now we have enough information to configure SwitchC (notice the EIGRP AS in this case is 650)

Note: VLAN2 and VLAN3 were created and gi0/10, gi0/11 interfaces were configured as access ports so we don't need to configure them in this sim.

SwitchC# **configure terminal**

SwitchC(config)# **int gi0/1**

SwitchC(config-if)#**no switchport** -> without using this command, the simulator does not let you assign IP address on Gi0/1 interface.

SwitchC(config-if)# **ip address 10.10.10.2 255.255.255.0** ->RouterC has used IP 10.10.10.1 so this is the lowest usable IP address.

SwitchC(config-if)# **no shutdown**

SwitchC(config-if)# **exit**

SwitchC(config)# **int vlan 2**

SwitchC(config-if)# **ip address 190.200.250.33 255.255.255.224**

SwitchC(config-if)# **no shutdown**

SwitchC(config-if)# **int vlan 3**

SwitchC(config-if)# **ip address 190.200.250.65 255.255.255.224**

SwitchC(config-if)# **no shutdown**

SwitchC(config-if)#**exit**

SwitchC(config)# **ip routing** (Notice: MLS will not work without this command)

```
SwitchC(config)# router eigrp 65010
SwitchC(config-router)# network 10.10.10.0 0.0.0.255
SwitchC(config-router)# network 190.200.250.32 0.0.0.31
SwitchC(config-router)# network 190.200.250.64 0.0.0.31
```

NOTE: THE ROUTER IS CORRECTLY CONFIGURED, so you will not miss within it in the exam, also don't modify/delete any port just do the above configuration. Also some reports said the "no auto-summary" command can't be used in the simulator, in fact it is not necessary because the network 190.200.0.0/16 is not used anywhere else in this topology.

In order to complete the lab, you should expect the ping to SERVER to succeed from the MLS, and from the PCs as well.

Also make sure you use the correct EIGRP AS number (in the configuration above it is 650 but it will change when you take the exam) but we are not allowed to access RouterC so the only way to find out the EIGRP AS is to look at the exhibit above. If you use wrong AS number, no neighbor relationship is formed between RouterC and SwitchC.

In fact, we are pretty sure instead of using two commands "network 190.200.250.32 0.0.0.31" and "network 190.200.250.64 0.0.0.31" we can use one simple command "network 190.200.0.0" because it is the nature of distance vector routing protocol like EIGRP: only major networks need to be advertised; even without "no auto-summary" command the network still works correctly. But in the exam the sim is just a flash based simulator so we should use two above commands, just for sure. But after finishing the configuration, we can use "show run" command to verify, only the summarized network 190.200.0.0 is shown.

## QUESTION 101

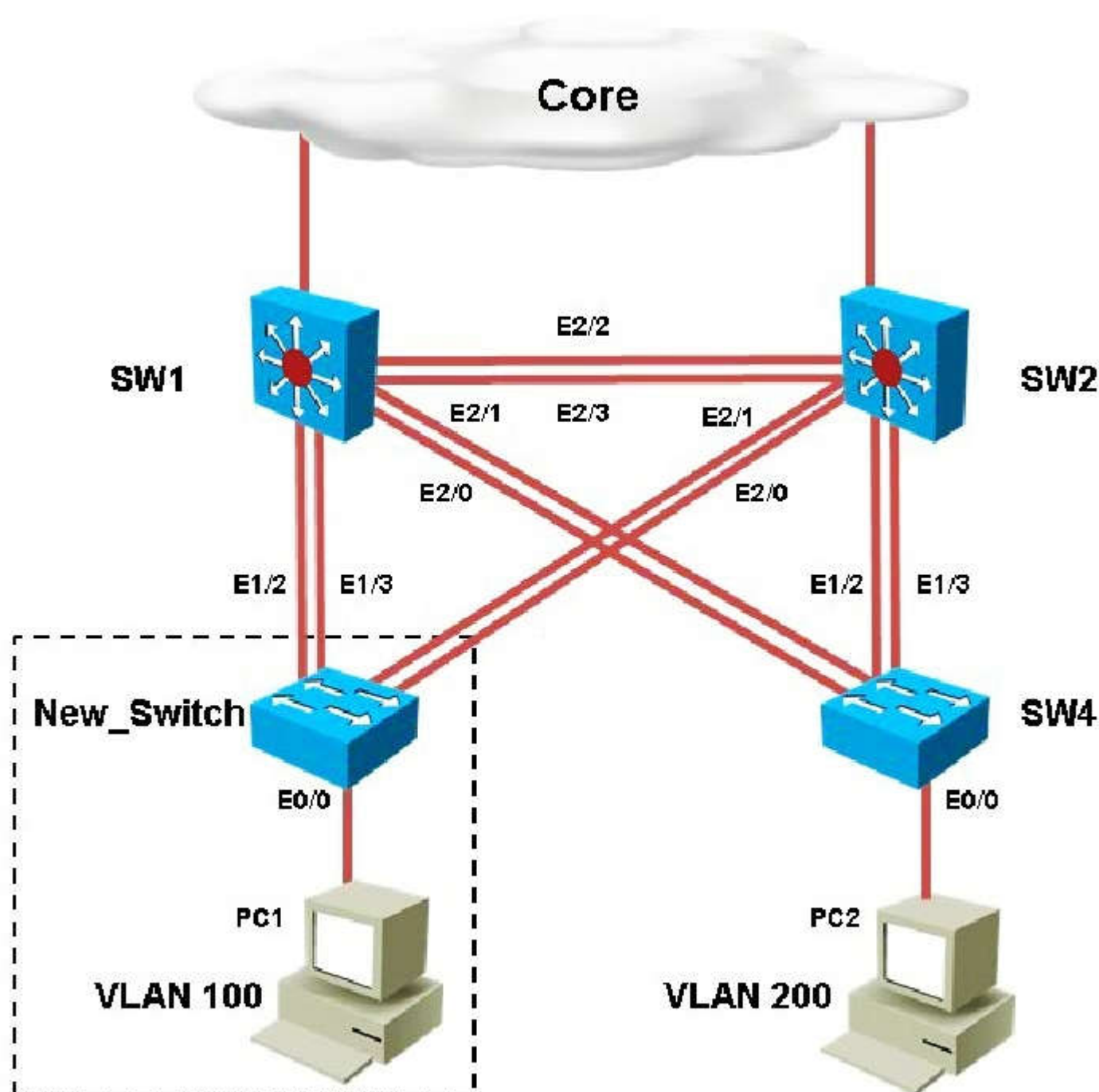
### Instructions

- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on SW1, SW2, New\_Switch or SW4 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

### Scenario

You have been asked to install and configure a new switch in a customer network. Use the console access to the existing and new switches to configure and verify correct device configuration.

### Topology





SW1



SW1#

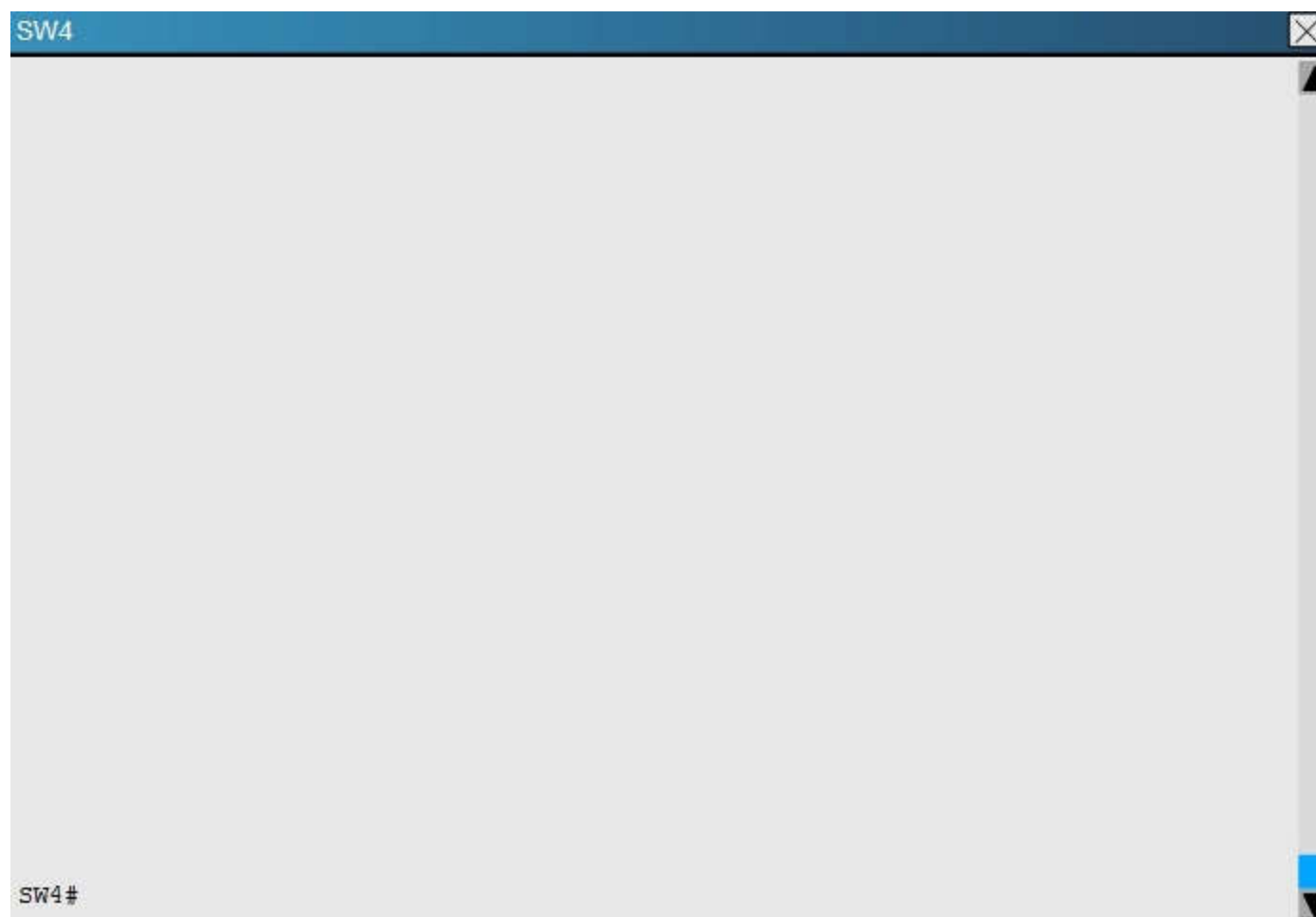
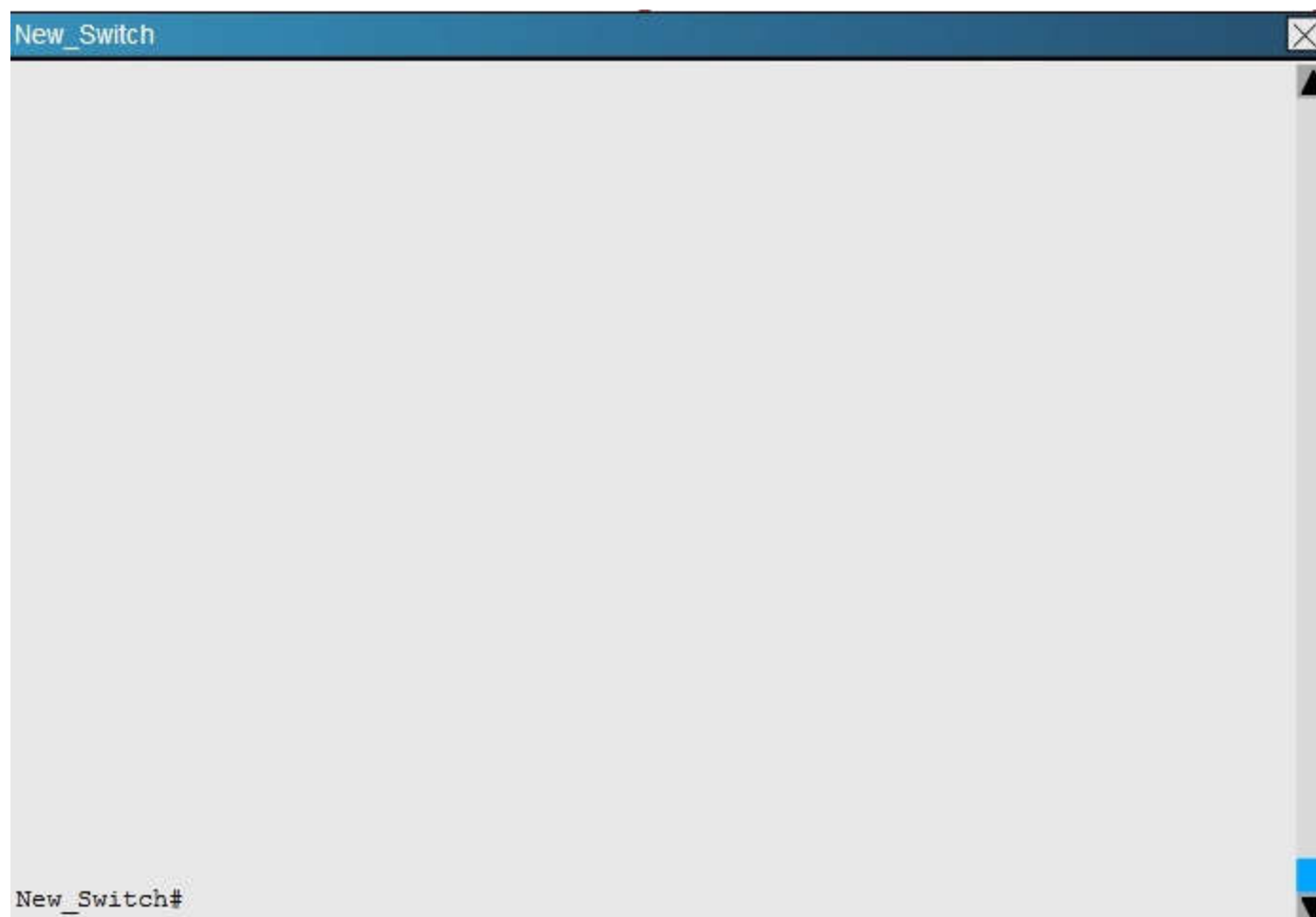


SW2



SW2#





You are connecting the New\_Switch to the LAN topology; the switch has been partially configured and you need to complete the rest of configuration to enable PC1 communication with PC2. Which of the configuration is correct?

- A. 

```
ntp domain CCNP_TEST
ntp password cisco 123
ntp version 3
ntp mode server
int e0/0
switchport mode access
switchport access vlan 100
```
- B. 

```
ntp domain CCNP_TEST
ntp password cisco 123
ntp version 3
ntp mode server
int e0/0
switchport mode access
switchport access vlan 200
```

- C. vtp domain CCNP\_TEST  
vtp password cisco 123  
vtp version 2  
vtp mode server  
int e0/0  
switchport mode access  
switchport access vlan 100
- D. vtp domain CCNP  
vtp password cisco 123  
vtp version 3  
vtp mode server  
int e0/0  
switchport mode access  
switchport access vlan 100
- E. vtp domain CCNP  
vtp password cisco 123  
vtp version 2  
vtp mode server  
int e0/0  
switchport mode access  
switchport access vlan 200

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

Within any VTP, the VTP domain name must match. So, step one is to find the correct VTP name on the other switches. Logging in to SW1 and using the “show vtp status” command we see this:

```

SW1
SW1#show vtp status
VTP Version capable           : 1 to 3
VTP version running           : 3
VTP Domain Name                : CCNP
VTP Pruning Mode               : Enabled
VTP Traps Generation           : Disabled
Device ID                      : aabb.cc00.2500

Feature VLAN:
-----
VTP Operating Mode             : Server
Number of existing VLANs       : 8
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision         : 11
Primary ID                     : aabb.cc00.2b00
Primary Description             : SW1
MD5 digest                     : 0xA2 0xFA 0x6E 0x8D 0xD0 0xDE 0x5A 0xEF
                               0xE3 0x65 0x9A 0xF7 0x03 0xBF 0xBA 0x10

Feature MST:

```

So we know that the VTP domain must be CCNP. This leaves only choice D and E. We also see from the topology diagram that eth 0/0 of the new switch connects to a PC in VLNA 100, so we know that this port must be an access port in VLAN 100, leaving only choice D as correct. Note that the VTP versions supported in this network are 1, 2, 3 so either VTP version 2 or 3 can be configured on the new switch.

**QUESTION 102**

Instructions

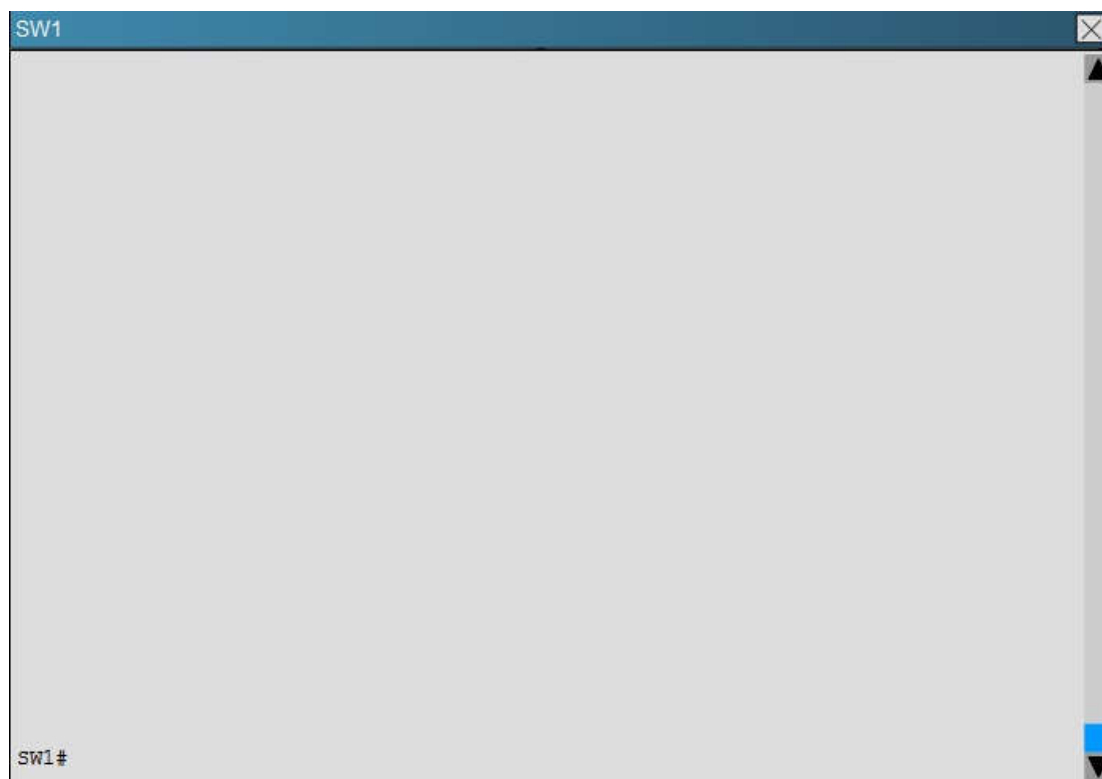
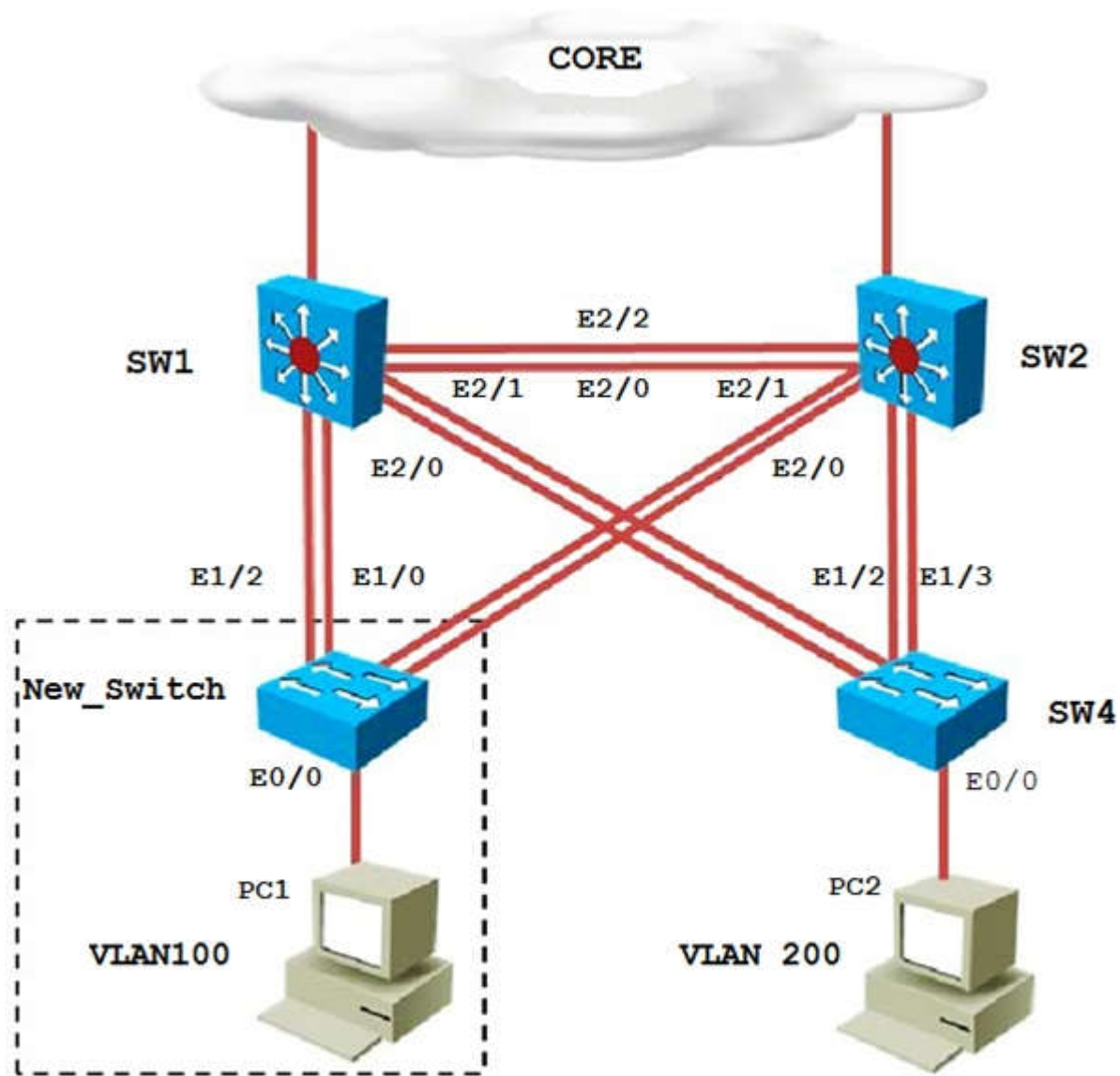
- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on SW1, SW2, New\_Switch or SW4 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

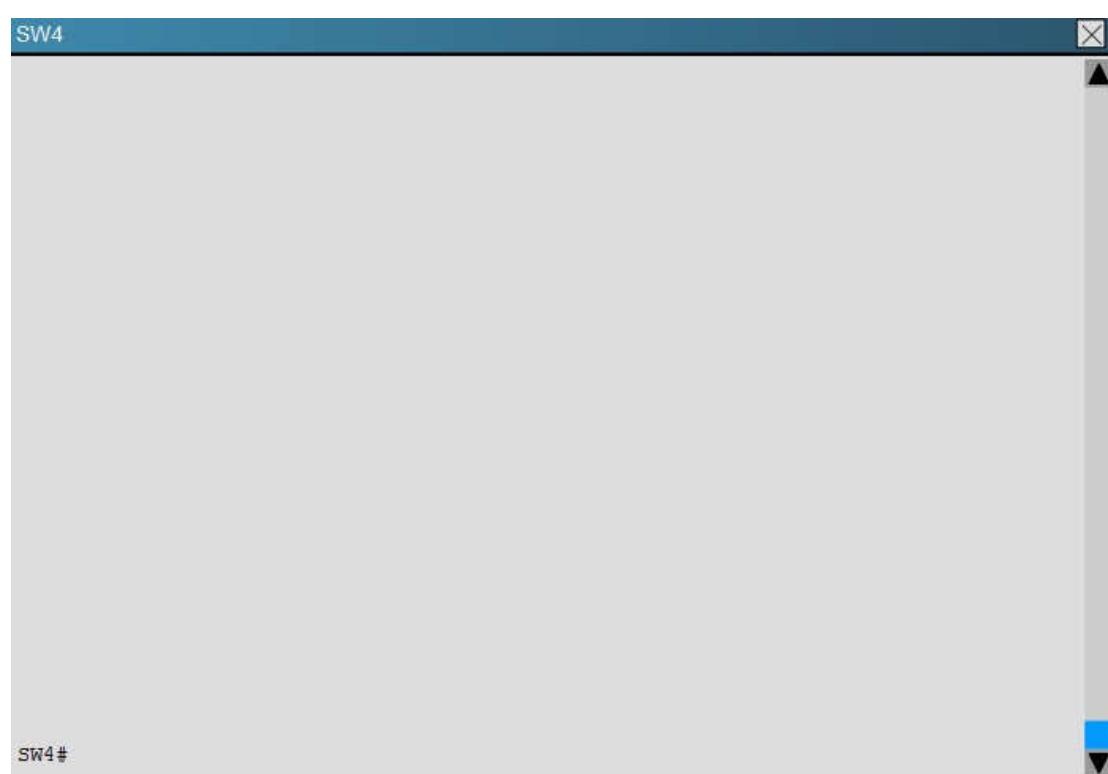
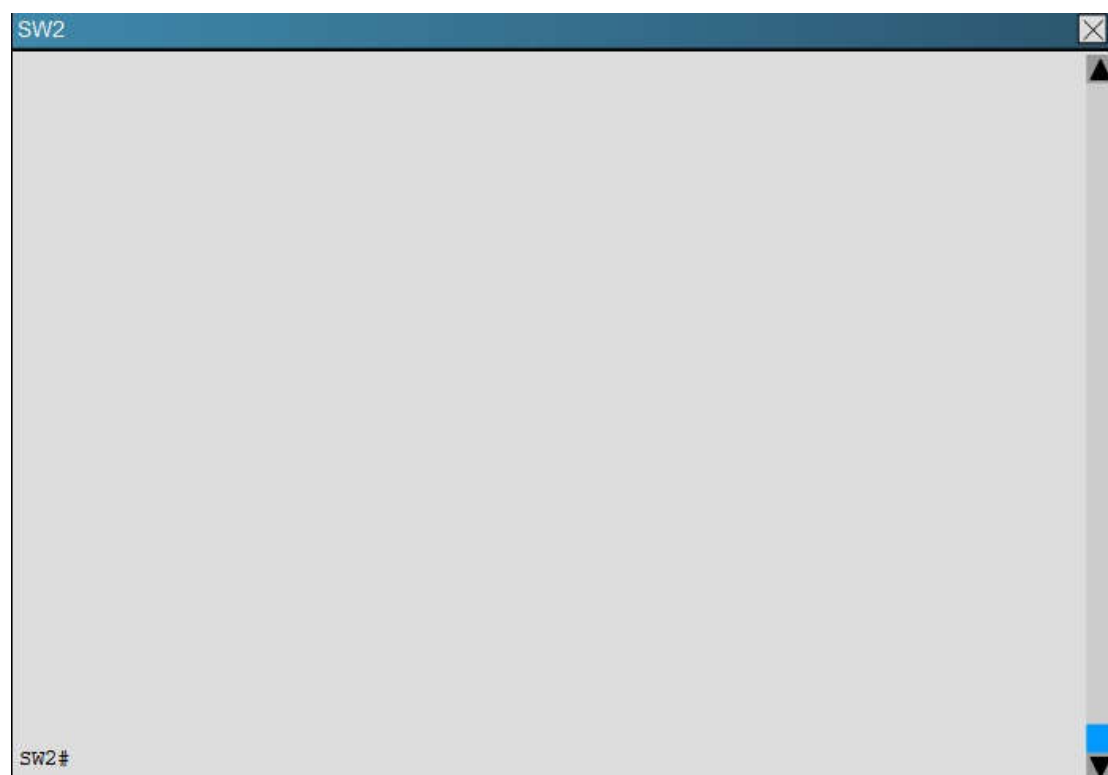
Scenario

You have been asked to install and configure a new switch in a customer network. Use the console access to the existing and new switches to configure and verify correct device configuration.



Topology





Refer to the configuration. For which configured VLAN are untagged frames sent over trunk between SW1 and SW2?

- A. VLAN1
- B. VLAN 99
- C. VLAN 999
- D. VLAN 40
- E. VLAN 50
- F. VLAN 200
- G. VLAN 300

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:  
The native VLAN is used for untagged frames sent along a trunk. By issuing the “show interface trunk” command on SW1 and SW2 we see the native VLAN is 99.

| SW1                       |      |               |          |             |
|---------------------------|------|---------------|----------|-------------|
| SW1#show interfaces trunk |      |               |          |             |
| Port                      | Mode | Encapsulation | Status   | Native vlan |
| Et1/2                     | on   | 802.1q        | trunking | 99          |
| Et1/3                     | on   | 802.1q        | trunking | 99          |
| Et2/0                     | on   | 802.1q        | trunking | 99          |
| Et2/1                     | on   | 802.1q        | trunking | 99          |
| Et2/2                     | on   | 802.1q        | trunking | 99          |
| Et2/3                     | on   | 802.1q        | trunking | 99          |

| SW2                       |      |               |          |             |
|---------------------------|------|---------------|----------|-------------|
| SW2#show interfaces trunk |      |               |          |             |
| Port                      | Mode | Encapsulation | Status   | Native vlan |
| Et1/2                     | on   | 802.1q        | trunking | 99          |
| Et1/3                     | on   | 802.1q        | trunking | 99          |
| Et2/0                     | on   | 802.1q        | trunking | 99          |
| Et2/1                     | on   | 802.1q        | trunking | 99          |
| Et2/2                     | on   | 802.1q        | trunking | 99          |
| Et2/3                     | on   | 802.1q        | trunking | 99          |

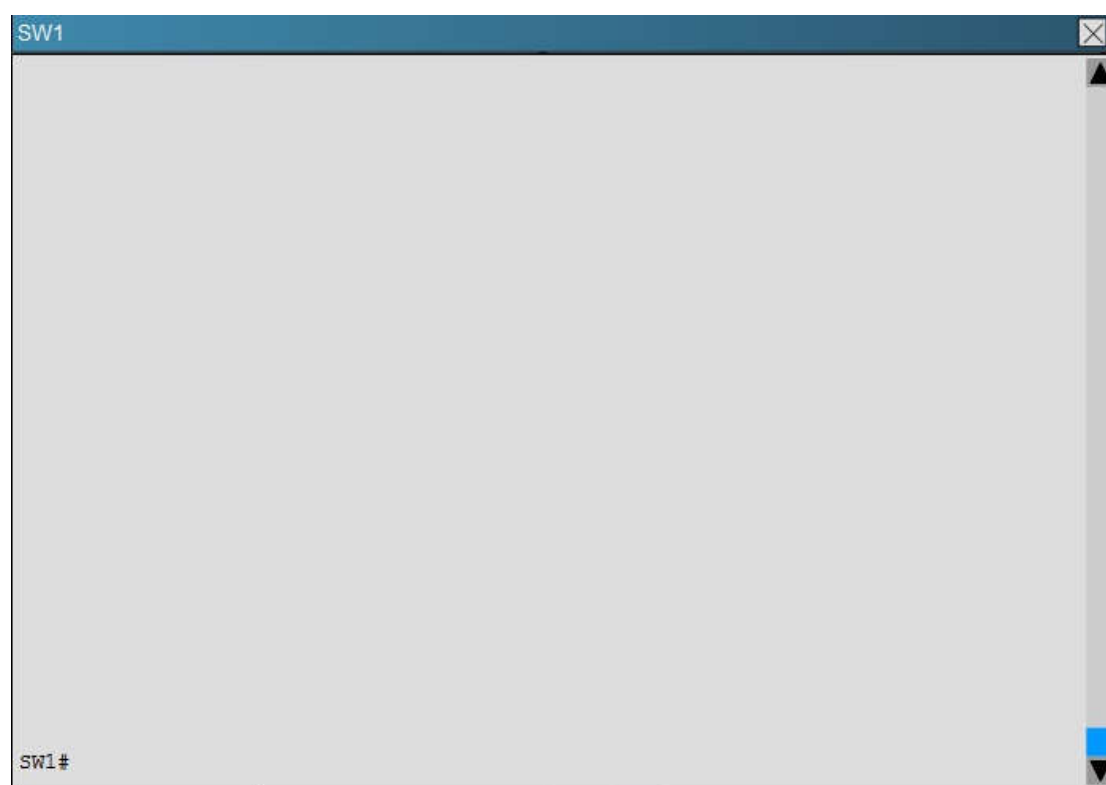
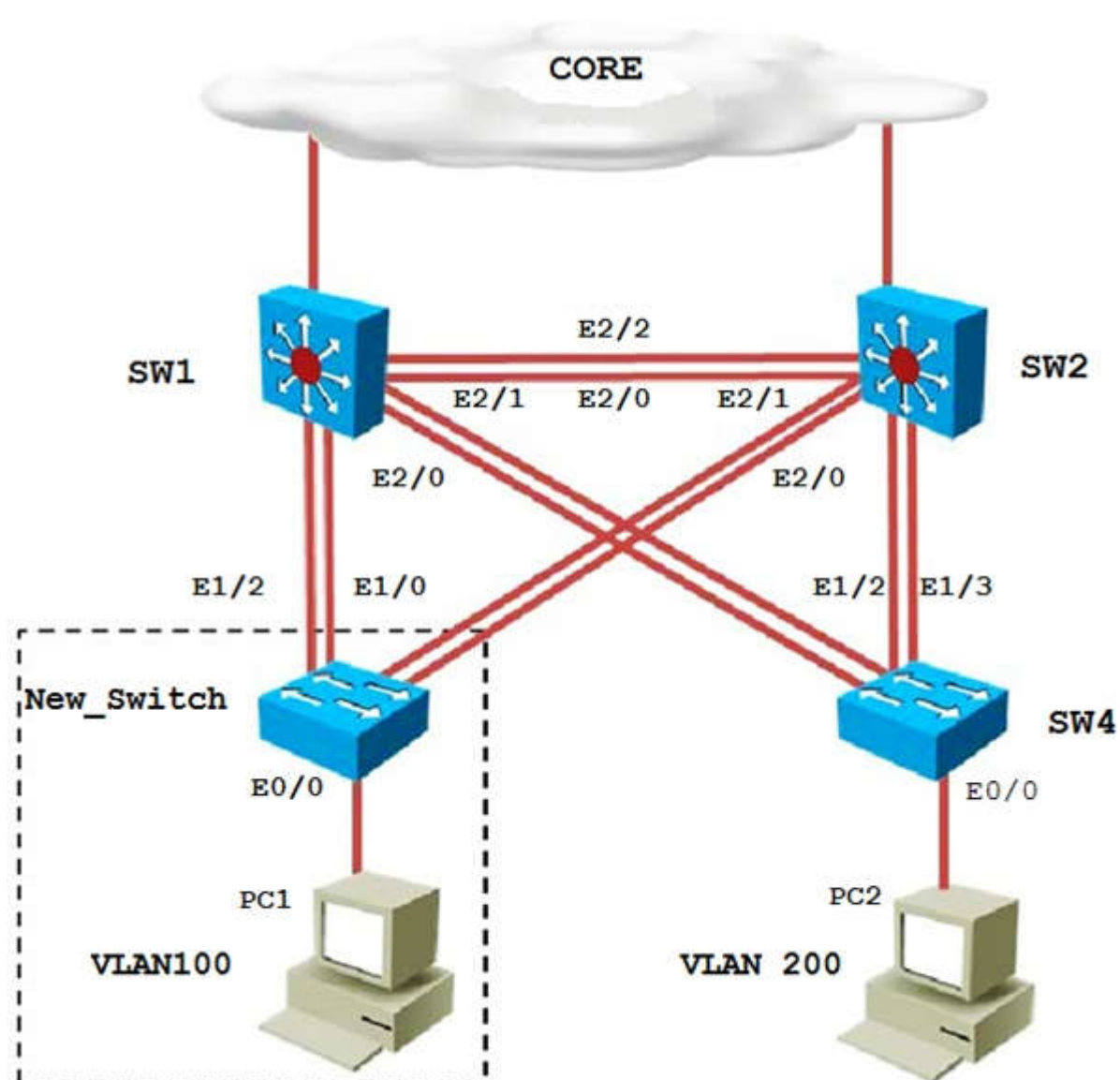
**QUESTION 103**  
Instructions

- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on SW1, SW2, New\_Switch or SW4 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

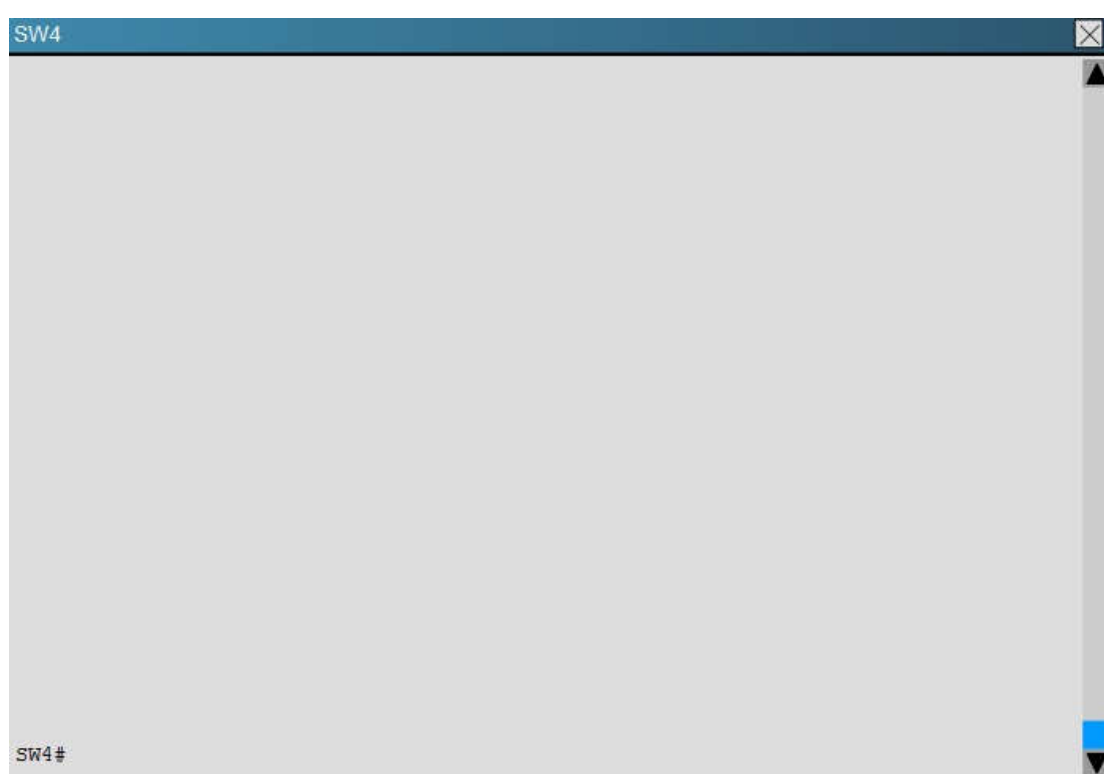
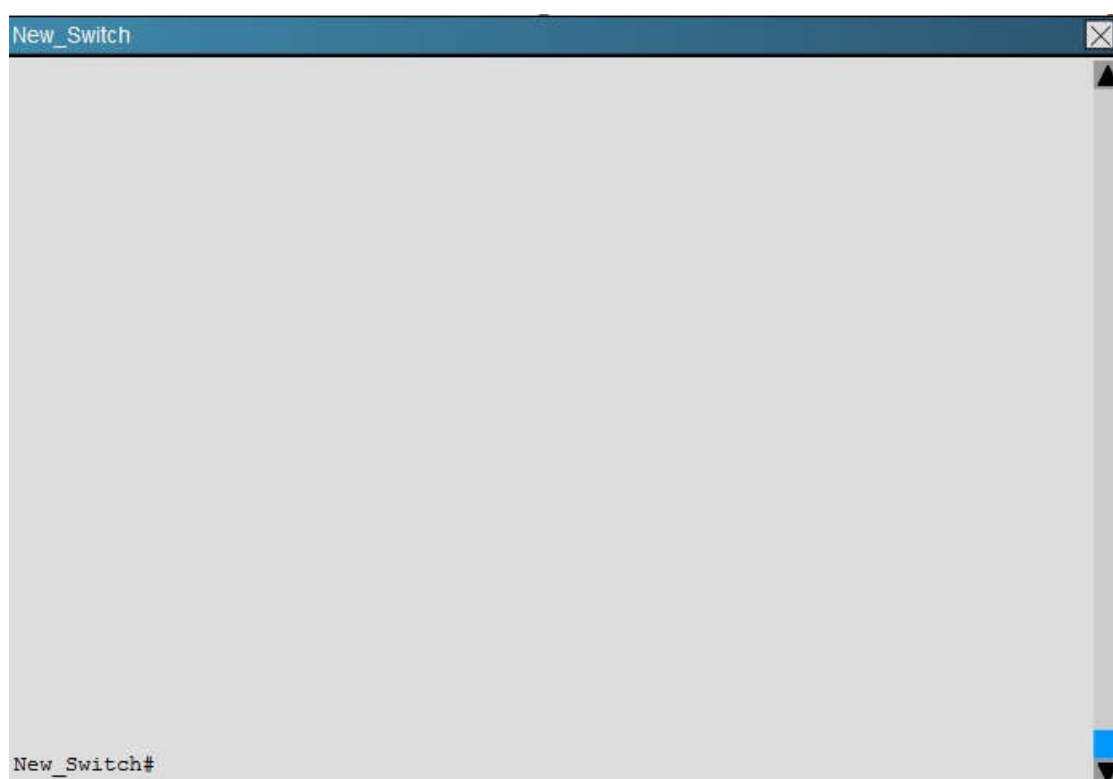
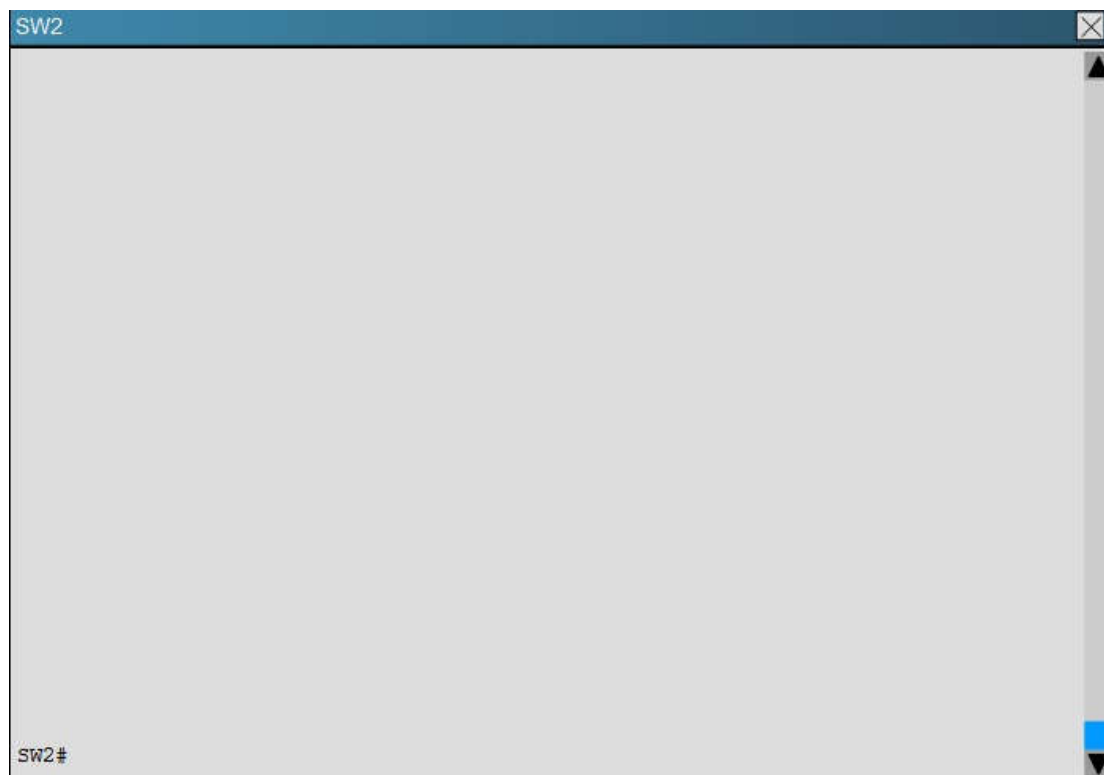
Scenario

You have been asked to install and configure a new switch in a customer network. Use the console access to the existing and new switches to configure and verify correct device configuration.

Topology







You are adding new VLANs. VLAN500 and VLAN600 to the topology in such way that you need to configure SW1 as primary root for VLAN 500 and secondary for VLAN 600 and SW2 as primary root for VLAN 600 and secondary for VLAN 500. Which configuration step is valid?

- A. Configure VLAN 500 & VLAN 600 on both SW1 & SW2
- B. Configure VLAN 500 and VLAN 600 on SW1 only
- C. Configure VLAN 500 and VLAN 600 on SW2 only
- D. Configure VLAN 500 and VLAN 600 on SW1, SW2 and SW4
- E. On SW2; configure vtp mode as off and configure VLAN 500 and VLAN 600; configure back to vtp server mode.

**Correct Answer: A**

**Section: Layer 2 Technologies**

## Explanation

### Explanation/Reference:

Explanation:

By issuing the "show vtp status command on SW1, SW2, and SW4 we see that both SW1 and SW2 are operating in VTP server mode, but SW4 is a client, so we will need to add both VLANs to SW1 and SW2.

#### SW1

```
SW1#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 3
VTP Domain Name          : CCNP
VTP Pruning Mode         : Enabled
VTP Traps Generation     : Disabled
Device ID                 : aabb.cc00.2500

Feature VLAN:
-----
VTP Operating Mode       : Server
Number of existing VLANs : 8
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision   : 11
Primary ID               : aabb.cc00.2b00
Primary Description      : SW1
MD5 digest               : 0xA2 0xFA 0x6E 0x8D 0xD0 0xDE 0x5A 0xEF
                        : 0xE3 0x65 0x9A 0xF7 0x03 0xBF 0xBA 0x10
```

#### SW2

```
SW2#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 3
VTP Domain Name          : CCNP
VTP Pruning Mode         : Enabled
VTP Traps Generation     : Disabled
Device ID                 : aabb.cc00.2600

Feature VLAN:
-----
VTP Operating Mode       : Server
Number of existing VLANs : 8
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision   : 11
Primary ID               : aabb.cc00.2b00
Primary Description      : SW1
MD5 digest               : 0xA2 0xFA 0x6E 0x8D 0xD0 0xDE 0x5A 0xEF
                        : 0xE3 0x65 0x9A 0xF7 0x03 0xBF 0xBA 0x10
```

## SW4

```
SW4#show vtp status
VTP Version capable      : 1 to 3
VTP version running      : 3
VTP Domain Name          : CCNP
VTP Pruning Mode         : Enabled
VTP Traps Generation     : Disabled
Device ID                : aabb.cc00.2800

Feature VLAN:
-----
VTP Operating Mode       : Client
Number of existing VLANs : 8
Number of existing extended VLANs : 0
Maximum VLANs supported locally : 4096
Configuration Revision   : 11
Primary ID               : aabb.cc00.2b00
Primary Description      : SW1
MD5 digest               : 0xA2 0xFA 0x6E 0x8D 0xD0 0xDE 0x5A 0xEF
                        : 0xE3 0x65 0x9A 0xF7 0x03 0xBF 0xBA 0x10
```

### QUESTION 104

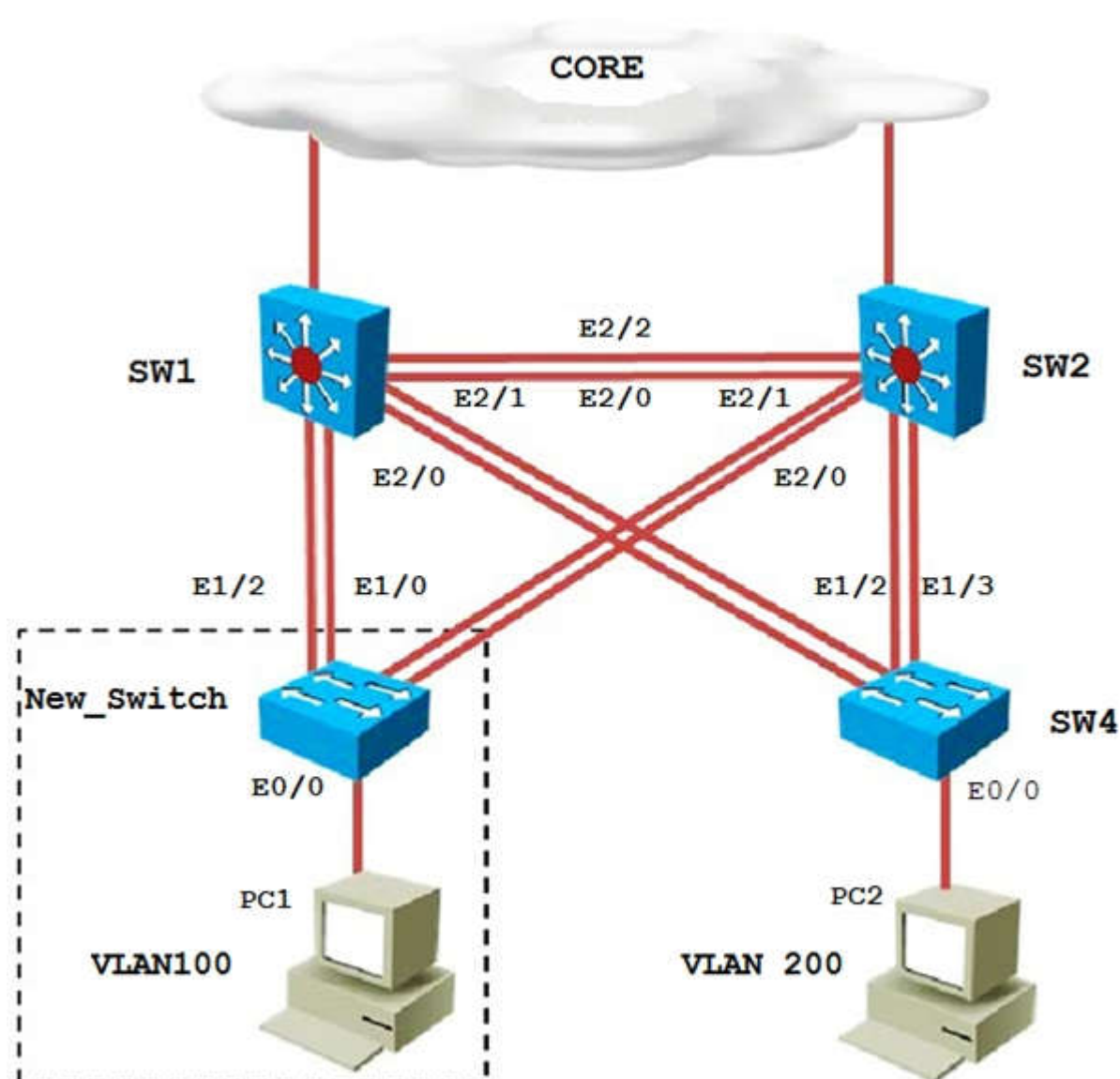
#### Instructions

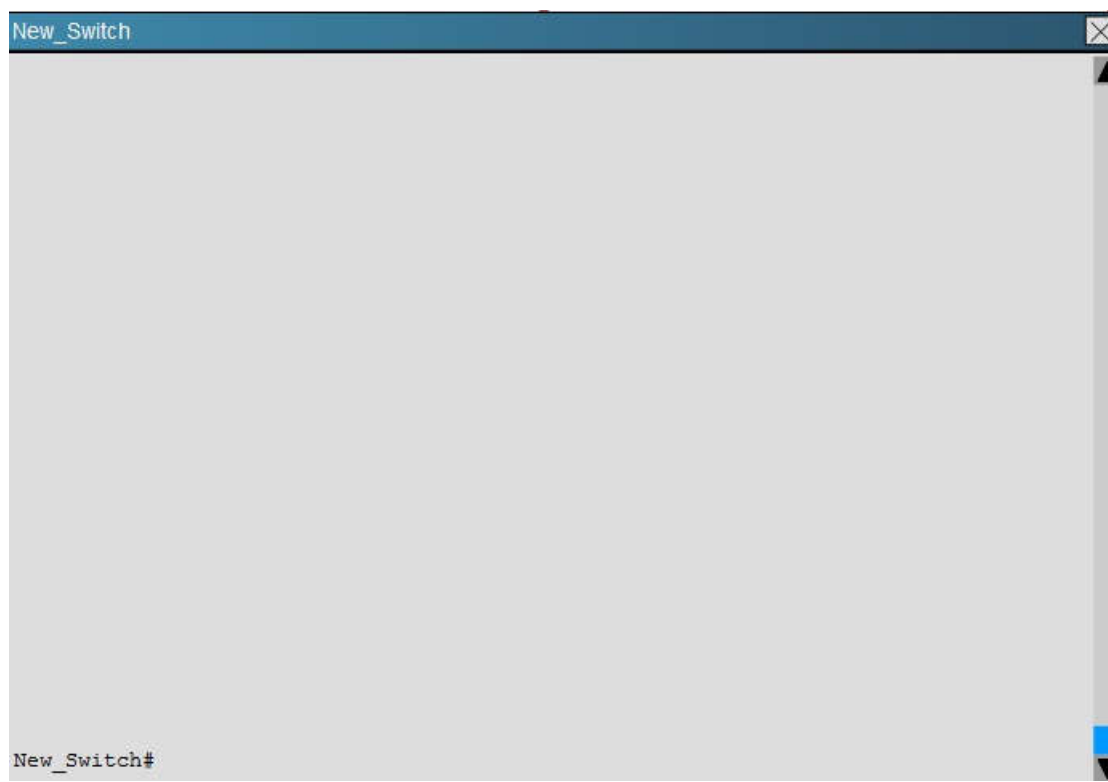
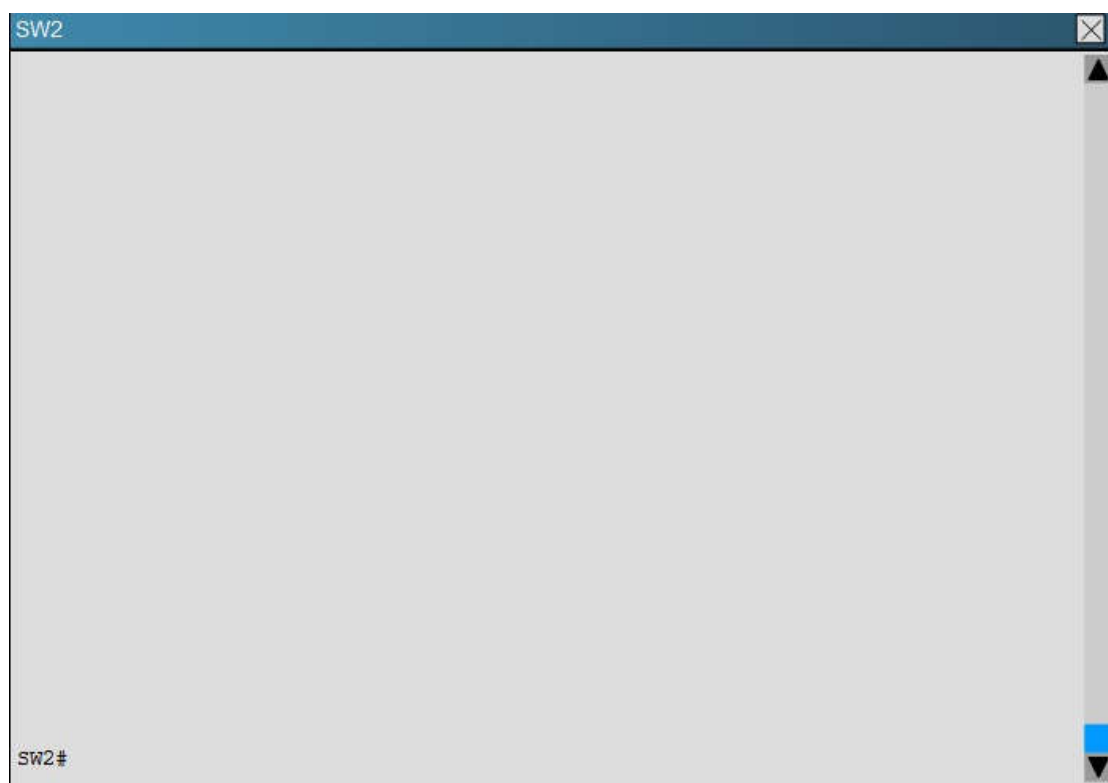
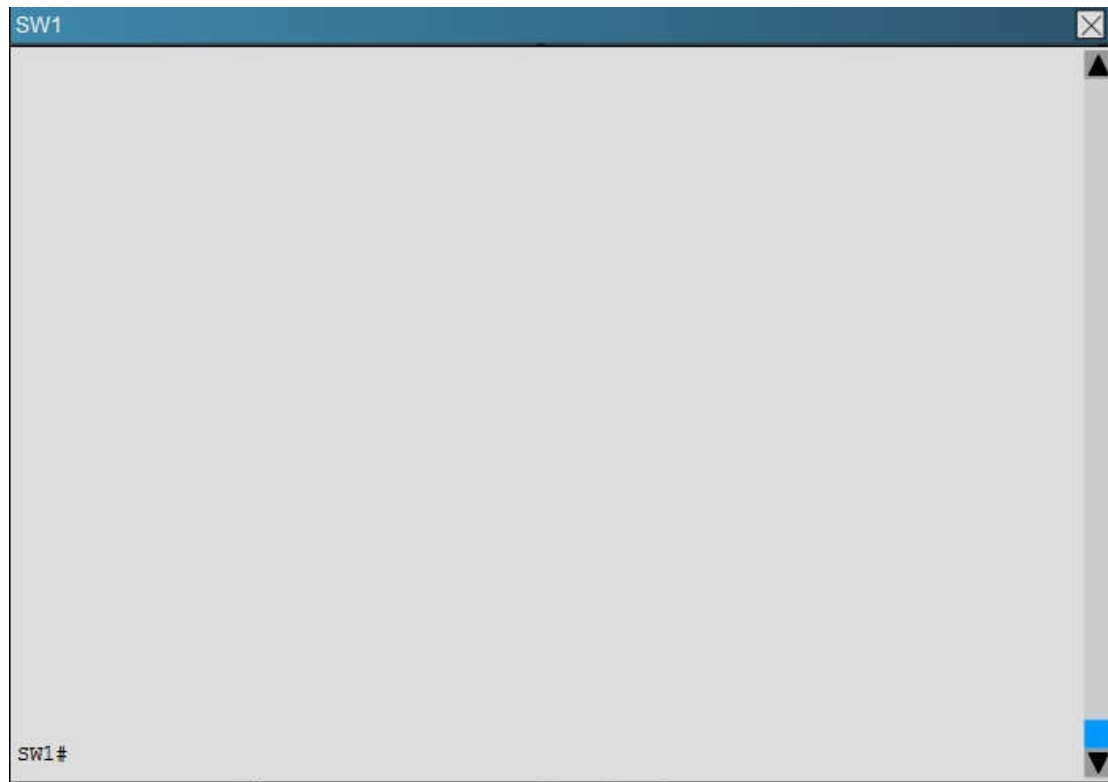
- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on SW1, SW2, New\_Switch or SW4 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

#### Scenario

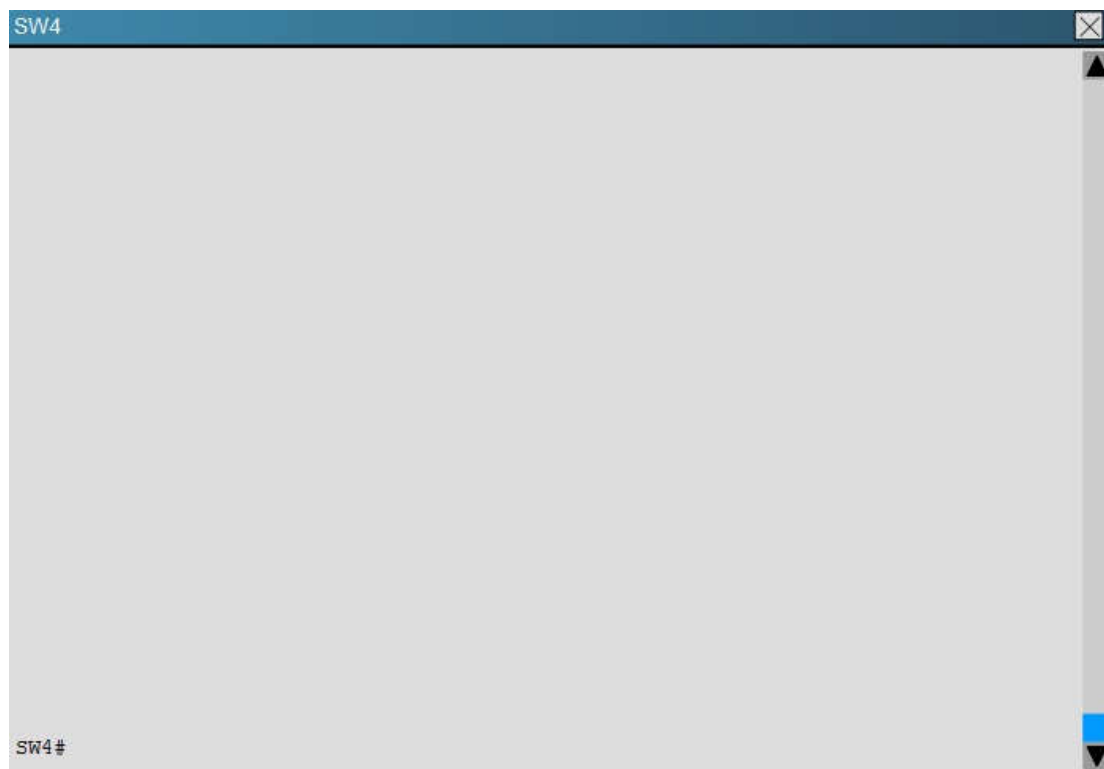
You have been asked to install and configure a new switch in a customer network. Use the console access to the existing and new switches to configure and verify correct device configuration.

#### Topology









Examine the VTP configuration. You are required to configure private VLANs for a new server deployment connecting to the SW4 switch. Which of the following configuration steps will allow creating private VLANs?

- A. Disable VTP pruning on SW1 only
- B. Disable VTP pruning on SW2 only
- C. Disable VTP pruning on SW4 only
- D. Disable VTP pruning on SW2, SW4 and New\_Switch
- E. Disable VTP pruning on New\_Switch and SW4 only.

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

To create private VLANs, you will need to only disable pruning on the switch that contains the private VLANs. In this case, only SW4 will connect to servers in a private VLAN.

#### QUESTION 105

Which command sets the interval at which a device sends LLDP updates to its neighbors?

- A. **lldp transmit**
- B. **lldp timer**
- C. **lldp holdtime**
- D. **lldp tlv-select**

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_53\\_se/configuration/guide/2960scg/swlldp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swlldp.html)

#### QUESTION 106

Which two statements about RPVST+ are true? (Choose two.)

- A. It is incompatible with spanning-tree PortFast.
- B. It supports two STP instances per VLAN.
- C. It requires approximately 50 seconds to complete reconvergence.
- D. Backwards compatibility with 802.1d is not supported.
- E. It elects one root switch per VLAN instance.
- F. It automatically enables UplinkFast and BackboneFast.

**Correct Answer: EF**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

#### QUESTION 107

Which statement is true when UDLD is configured on a link and the link is determined to be unidirectional?

- A. The port remains up for a configured time interval and then error disables if the link remains unidirectional.
- B. LLDP is enabled on the port.
- C. The port sends a log message to the console.
- D. The port is disabled immediately.

**Correct Answer: D**

**Section: Layer 2 Technologies**

## Explanation

### Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10591-77.html>

### QUESTION 108

Which command enables PortFast and disables port channel on a physical interface?

- A. **switchport host**
- B. **switchport mode access**
- C. **spanning-tree portfast**
- D. **switchport mode dynamic auto**

**Correct Answer: A**

**Section: Layer 2 Technologies**

## Explanation

### Explanation/Reference:

Reference: <https://learningnetwork.cisco.com/thread/21934>

### QUESTION 109

Under which two conditions does Cisco StackWise Virtual transmit data over a virtual link? (Choose two.)

- A. Packets are processed on the egress interface on the active switch.
- B. Packets are processed on the ingress interface on the active switch.
- C. Packets are processed on the egress interface on the standby switch.
- D. Packets are processed on the ingress interface on the standby switch.
- E. A VLAN is flooded over Layer 2.

**Correct Answer: DE**

**Section: Layer 2 Technologies**

## Explanation

### Explanation/Reference:

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration\\_guide/b\\_166\\_ha\\_9500/b\\_166\\_ha\\_9500\\_chapter\\_01.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration_guide/b_166_ha_9500/b_166_ha_9500_chapter_01.pdf)

### QUESTION 110

```
Switch# configure terminal
Switch(config)# vlan 3
Switch(config-vlan)# end
```

Refer to the exhibit. You have applied this configuration to Switches A, B, C and D, and the switches are connected to one another on access ports. Which two additional actions must you take to enable the hosts on VLAN 3 to communicate with one another considering future growth with hosts on additional VLANs? (Choose two.)

- A. Assign VLAN 3 to the ports connecting to the hosts.
- B. Reconfigure the access ports connecting the switches as trunk ports.
- C. Configure VLAN 3 as an SVI with a working IP address.
- D. Configure VTP transparent mode to allow hosts with additional VLANs.
- E. Configure VLAN 3 in VLAN database mode.

**Correct Answer: AB**

**Section: Layer 2 Technologies**

## Explanation

### Explanation/Reference:

### QUESTION 111

```
monitor session 1 source vlan 10 - 12 rx
monitor session 1 destination interface gigabitethernet0/1
```

Refer to the exhibit. Which effect of this configuration is true?

- A. Traffic received on VLANs 10 and 12 only is copied and sent to interface g0/1.
- B. Traffic sent on VLANs 10, 11, and 12 is copied and sent to interface g0/1.
- C. Traffic sent on VLANs 10 and 12 is copied and sent to interface g0/1.
- D. Traffic received on VLANs 10, 11 and 12 only is copied and sent to interface g0/1.

**Correct Answer: D**

**Section: Layer 2 Technologies**

## Explanation

### Explanation/Reference:

### QUESTION 112

Which two statements about Cisco StackWise are true? (Choose two.)

- A. It supports multiple switches in a stack.
- B. The LAN base feature set is supported on mixed stacks.
- C. Stacks running the LAN base feature set support Layer 3 features.
- D. Each stack identifies a stack master and a backup stack master.
- E. It supports both homogeneous and mixed stacks.

**Correct Answer:** AE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstack.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.pdf)

**QUESTION 113**

How does SPAN interact with STP?

- A. A designed SPAN source port maintains its STP learning status.
- B. STP is disabled on a destination port when a SPAN monitor session is active.
- C. STP is disabled on trunk ports carrying the SPAN VLAN.
- D. Designated SPAN source ports direct traffic to the root bridge of STP.

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

STP—A destination port does not participate in STP while its SPAN or RSPAN session is active. The destination port can participate in STP after the SPAN or RSPAN session is disabled. On a source port, SPAN does not affect the STP status. STP can be active on trunk ports carrying an RSPAN VLAN.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swspan.html#pgfId-1200733](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html#pgfId-1200733)

**QUESTION 114**

Which errdisable recovery command option enables a device to recover from an EtherChannel error?

- A. **sfp-config-mismatch**
- B. **security-violation**
- C. **port-mode-failure**
- D. **channel-misconfig**

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>

**QUESTION 115**

Which errdisable recovery command option enables a device to recover from an incorrect SFP state?

- A. **sfp-config-mismatch**
- B. **gbic-invalid**
- C. **port-mode-failure**
- D. **link-monitor-failure**

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>

**QUESTION 116**

Which two statements about VTP are true? (Choose two.)

- A. Switches running in transparent mode pass VTP messages.
- B. In VTPv2, a new switch can learn the VTP domain name from its peer over a trunk port.
- C. It supports only one server switch within a network.
- D. It supports clear-text passwords only.
- E. A switch running in transparent mode saves learned VLANs to its local database.

**Correct Answer:** AD  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

**QUESTION 117**

Which command must an administrator use to determine the native VLAN on a trunk?

- A. **show ip interface vlan**
- B. **show vlan**

- C. **show vlan mapping**
- D. **show interfaces trunk**

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

#### QUESTION 118

Which two commands prune VLAN 10 from a switch interface? (Choose two.)

- A. **switchport trunk native vlan 10**
- B. **switchport trunk allowed remove vlan 10**
- C. **switchport trunk allowed vlan add 10**
- D. **no vlan 10**
- E. **switchport trunk allowed except vlan 10**

**Correct Answer:** BE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/l2/switchport-trunk-allowed-vlan.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/l2/switchport-trunk-allowed-vlan.html)

#### QUESTION 119

Which command enables you to detect whether both sides of an aggregate link are configured properly?

- A. **spanning-tree etherchannel guard misconfig**
- B. **spanning-tree loopguard default**
- C. **spanning-tree backbonefast**
- D. **spanning-tree guard root**

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

#### QUESTION 120

Which two VLAN ranges can you add, modify, or delete on a switch? (Choose two.)

- A. 2 through 4094
- B. 2 through 1001
- C. 1 through 1001
- D. 1005 through 4094
- E. 1006 through 4094

**Correct Answer:** BE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/15-0\\_2\\_se/configuration/guide/3750x\\_cg/swvlan.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-0_2_se/configuration/guide/3750x_cg/swvlan.pdf)

#### QUESTION 121

Which Cisco component can be enabled on a switch port connected to a workstation to dramatically decrease the time a workstation must wait for spanning tree to converge?

- A. PortFast
- B. UplinkFast
- C. EtherChannel
- D. FastEthernet

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

When PortFast is enabled on a port, the attached end station can join the network almost immediately rather than waiting up to 50 seconds for spanning tree to converge. Instead of waiting for STP to cycle through the learning and blocking states, PortFast will place the port in the forwarding state immediately. PortFast does not disable Spanning Tree but instead causes it to skip some of the unnecessary steps. PortFast is also sometimes referred to as fast-start.

The following command enables PortFast:

```
switch(config-if)# spanning-tree portfast
```

You should only enable PortFast on a port that connects an end station. Enabling PortFast on a port that connects another switch could create a loop.

UplinkFast decreases convergence time to less than five seconds for inter-switch links. With UplinkFast enabled, the switch places the blocked port into the forwarding state once the switch detects a link failure. Without UplinkFast, all ports would stop forwarding during STP convergence.



EtherChannel and Gigabit EtherChannel provide the ability to combine up to eight physical links into one virtual link. When all links are up, traffic is load-balanced across all the links. However, if one link fails, the additional links can still provide connectivity. EtherChannel provides redundant links with bandwidths of from 200 to 800 Mbps. Recovery, in the event of link failure, typically takes place in a few microseconds or milliseconds and is transparent to users.

FastEthernet refers to a type of Ethernet (Fast Ethernet) and does not enhance STP convergence.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Cisco IOS Bridging Command Reference > rif through spanning-tree portfast (interface) > spanning-tree portfast (interface)

#### QUESTION 122

Which three methods can be used to manage Cisco APs that are running autonomously? (Choose three.)

- A. WLSE
- B. WLC
- C. WCS
- D. CLI
- E. Web interface

**Correct Answer:** ADE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

The three methods that can be used to manage autonomous APs are WLSE, CLI, and web interfaces. Autonomous access points (APs) maintain their management functionality and can be connected directly and configured. The wireless LAN solution engine (WLSE) allows for centralized coordination of autonomous APs. The WLSE can also work in coordination with another Cisco service, wireless domain services (WDS). The WDS enables the APs to provide fast, secure roaming between APs. The WDS registers all client devices in the subnet, establishes session keys for them, and caches their security credentials. When a client roams to another access point, the WDS device forwards the client's security credentials to the new access point

Wireless LAN controller (WLC) is a physical controller that provides centralized control of a WLAN environment. APs that are being managed by a WLC function in lightweight mode.

Wireless control system (WCS) is a software package that allows for management of a WLAN environment, managing one or multiple WLCs. APs managed by WCS function in lightweight mode.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify other LAN switching technologies

References:  
Cisco > Products and Services > Cloud and Systems Management>End-of-sale and End-of-life products>Ciscoworks Wireless Lan Solution E(WLSE>Data sheets and literature>Data sheets>Ciscoworks Wireless Lan Solution engine 2.13

#### QUESTION 123

When using auxiliary VLANs, how is a phone configured with the appropriate VLAN to join?

- A. the administrator configures the phone with CLI
- B. the switch connected to the phone provides the VLAN
- C. the PC attached to the phone provides the VLAN information
- D. a VMPS server provides the VLAN for the switch and phone

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

When using auxiliary VLANs, the switch connected to the phone provides the VLAN to the phone. IP telephones typically have a built in 3-port 10/100 hub. One port internally attaches to the phone, one port is attached to the switch access port, and the other is used to connect to the workstation. The PC attached to the switch port via the IP phone is unaware of the presence of the phone

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:  
Cisco > Home > Products and Services > Cisco Interfaces and Modules > Cisco Network Modules > Product Literature > Data Sheets > Cisco Catalyst 6500 Series Switches  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport voice vlan

#### QUESTION 124

Which two of the following procedures can be performed on a VTP server to reset the VTP configuration revision number to 0? (Choose two.)

- A. Disable VTP pruning, then enable VTP pruning.
- B. Change the VTP mode to client, and then back to server mode.
- C. Change the VTP mode to transparent, then back to server mode.
- D. Change the VTP domain name to a non-existent domain name, and then back to the correct domain name.

**Correct Answer:** CD  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

To reset the configuration revision number to 0, you should change the VLAN Trunking Protocol (VTP) domain to a non-existent domain name, and then back to the correct domain name. To change the domain name, issue the vtp domain command.

Alternatively, you can change the VTP mode to transparent mode, then back to client or server mode. To change the VTP mode, issue the vtp mode command from global configuration mode. To verify that the configuration revision number has been reset to 0, you should issue the show vtp status command.

Before adding a new switch to a VTP domain, you should reset the configuration revision number to 0. If the configuration revision number is higher than that of the other switches in the domain, then the switch can propagate incorrect configuration information to the other switches. This can cause virtual local area networks (VLANs) to be modified or deleted on every switch in the VTP domain.

The VTP configuration revision number will not be reset to 0 if you disable and then re-enable VTP pruning. VTP pruning can eliminate the flooding of broadcast traffic to switches that have no ports assigned to the virtual local area network (VLAN).

The VTP configuration revision number will not be reset to 0 if you change the VTP mode to client and then back to server. Both server-mode and client-mode switches propagate VTP information. Therefore, client-mode switches can cause incorrect information to be propagated if the configuration revision number is higher than other switches in the domain. Transparent-mode switches will not propagate its own VTP configuration, but will forward VTP information received from other switches.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)  
Cisco > Cisco IOS LAN Switching Command Reference > uddl through vtp v2-mode > vtp  
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > show vtp

#### QUESTION 125

Which VLAN trunking protocol adds four bytes to the Ethernet frames?

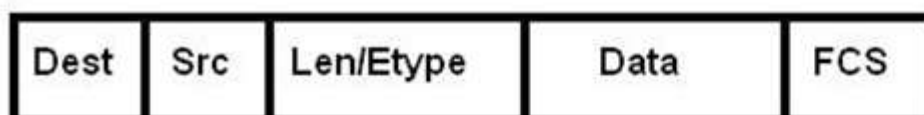
- A. ISL
- B. LANE
- C. 802.10
- D. 802.1Q

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

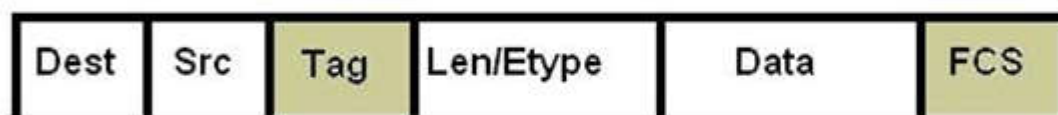
**Explanation/Reference:**  
Explanation:

802.1Q adds 4 bytes to the Ethernet frame. The process is known as 802.1Q tagging, and inserts a four-byte field into the Ethernet frame header between the source address and the Len/Etype fields. This tag identifies the frame as an 802.1Q frame and includes bits used to identify both the priority and the VLAN ID. The VLAN ID field indicates which VLAN the frame belongs to. An 802.1q trunk can support 4096 different VLANs. After the new tag field is inserted into the frame, the frame's previous FCS field is recalculated and replaced. The following graphic shows both the ISL and 802.1Q frame formats as well as the original Ethernet frame:

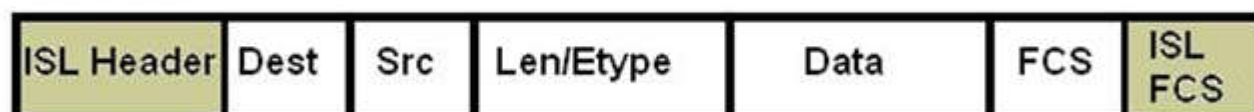
#### Untagged Ethernet Frame



#### 802.1Q Tagged Frame



#### ISL Encapsulated Frame



**Dest:** Destination MAC address  
**Src:** Source MAC address  
**Len/Etype:** Priority (CoS)  
**Data:** Data itself  
**FCS:** Frame check sequence

Inter switch link (ISL) is a Cisco proprietary trunking protocol that handles the frame in a different manner. It adds a 26- byte frame header and 4-byte trailer

to the frame.

LANE (LAN Emulation) is an IEEE standard for identifying VLANs on ATM networks.

802.10 is a Cisco proprietary method of identifying VLANs on FDDI media by writing VLAN information to the Security Association Identifier (SAID) of the 802.10 frame.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Support > Technology Support > LAN Switching > Virtual LAN/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Inter-Switch Link and IEEE 802.1Q Frame Format

#### QUESTION 126

What is the first step STP performs to establish a loop-free spanning tree in a switched network?

- A. Elects a root switch
- B. Disables redundant loops in the tree
- C. Sets a priority for each redundant link
- D. Selects a designated switch for each switched segment

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The first step taken by the Spanning-Tree Protocol (STP) is to elect a root bridge (switch). The root bridge keeps the STP database. The bridge ID is used to select the root bridge in the network. The bridge ID is a combination of the priority of the bridge (switch) and the MAC address. If two switches or bridges have the same priority value, the switch with the lowest MAC address will have the lowest priority and become the root bridge.

Once the STP process is complete (after switches go through the learning and listening stages), STP disables redundant loops in the network.

STP does not set a priority for each redundant link. The network administrator can manually set the priority of a switch. STP then uses the priority and the switch's MAC address to calculate the bridge ID, which is used to select the root bridge.

STP does not first select a designated switch for each switched segment. The first goal of STP is to select a root bridge for a switched segment (VLAN).

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring STP and IEEE 802.1s MST > Creating the Spanning Tree Topology  
Cisco > Support > Configuring Spanning Tree Protocol > How STP Works

#### QUESTION 127

Which IOS command configures the switch for the VTP mode that will propagate its VLAN database changes to others in the domain?

- A. vtp mode client
- B. vtp mode server
- C. vtp v1-mode
- D. vtp transparent mode

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

To configure a switch to operate as a VLAN Trunk Protocol (VTP) server, enter the vtp mode server command at the global configuration prompt.

```
switch(config)# vtp mode server
```

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create, modify, or delete VLANs. A Catalyst switch can create, modify, and delete VLANs in server or transparent mode, but not in client mode. However, VLANs created on a switch in transparent mode apply only to that switch, and information about these VLANs is not propagated throughout the VTP domain.

The VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM.

The VTP transparent mode forwards VTP advertisements and saves the VLAN configuration in NVRAM. It does not synchronize VLAN configuration information. A switch in transparent mode can create, delete, and modify VLANs, but changes are not transmitted to other switches in the domain. Changes only affect the local switch.

The VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers.

For added security, you can specify the VTP domain to which the client belongs and a password used to connect to the domain when configuring a switch for VTP client mode. The password is the same for all devices in the VTP domain. The commands to configure a VTP password are as follows:

```
switch(config)# vtp domain domain-name  
switch(config)# vtp password password
```

The vtp v1-mode command reverts the VTP version to version 1 (the default version). Use the vtp v2-mode command to set the VTP mode to version 2.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)  
Cisco > Cisco IOS LAN Switching Command Reference > udd through vtp v2-mode > vtp

#### QUESTION 128

Examine the following partial output of the show run command. The command was executed from Switch A, which is connected to Switch B through both the Fa0/1 interface and the Fa0/2 interface. Switch A is the root bridge.

```
Hostname Switch A
<output omitted>
interface fastethernet 0/1
spanningtree vlan 1-6
switchport mode trunk

interface fastethernet 0/2
spanningtree vlan 1-6
switchport mode trunk
```

Only one of the links is being used. Your intention was to load share the traffic using both links.

What commands do you need to execute to accomplish this? (Choose two.)

- A. switchA(config)# interface fa0/2switchA(config-if)#spanning-tree vlan 1-3 port-priority 16
- B. switchA(config)# interface fa0/1switchA(config-if)#spanning-tree vlan 4-6 port-priority 16
- C. switchA(config)# interface fa0/1switchA(config-if)#spanning-tree vlan 1-3 port-priority 128
- D. switchA(config)# interface fa0/2switchA(config-if)#spanning-tree vlan 4-6 port-priority 128
- E. switchA(config)# interface fa0/1switchA(config-if)#spanning-tree port-priority 20
- F. switchA(config)# interface fa0/2switchA(config-if)#spanning-tree port-priority 20

**Correct Answer:** AB

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The correct commands to load share the traffic using both links are:

```
switchA(config)# interface fa0/2
switchA(config-if)# spanning-tree vlan 1-3 port-priority 16
switchA(config)# interface fa0/1
switchA(config-if)# spanning-tree vlan 4-6 port-priority 16
```

The configuration that was reflected in the exhibit in the show run output indicated that VLANs 1 through 6 were configured under both interfaces. However, the normal operation of STP will block one of the interfaces to prevent a loop. By default, all VLANs are allowed on both trunk links. Load sharing allows you to send some of the VLANs over one of the links and the rest on the other. In this case, the correct option will send VLANs 1-3 over Fa0/1 and VLANs 4-6 over Fa0/2.

By altering the port priority of the VLAN 1-3 on one interface and VLANs 4-6 on the other on the root bridge (Switch A) with the port-priority keyword, the behavior of STP is altered on the other switch. The port priority value must be set in increments of 16. Now Switch A will send VLANs 1-3 over one interface without blocking and 4-6 over the other interface without blocking. The additional benefit to this configuration is that if either link goes down, all VLANs can be sent over the remaining link and until the redundant link comes back up.

The commands below will have no effect because the default port priority is already 128, so the situation will remain the same:

```
switchA(config)# interface fa0/1
switchA(config-if)# spanning-tree vlan 1-3 port-priority 128
switchA(config)# interface fa0/2
switchA(config-if)# spanning-tree vlan 4-6 port-priority 128
```

The commands below will have no effect because they omit the vlan 1-3 and vlan 4-6 parameters, and therefore change the port priority for all VLANs. Since the port priority is changed equally on both interfaces, there will be no load sharing as a result. More over the priority value is not entered in an increment of 16, which will generate an error message indicating that it must be set in increments of 16.

```
switchA(config)# interface fa0/1
switchA(config-if)# spanning-tree port-priority 20
switchA(config)# interface fa0/2
switchA(config-if)# spanning-tree port-priority 20
```

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Design > Design Technotes > VLAN Load Balancing Between Trunks Using the Spanning-Tree Protocol Port Priority  
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > spanning-tree port-priority

#### QUESTION 129



Which two tables are used by Cisco Express Forwarding? (Choose two.)

- A. FIB
- B. ACL table
- C. Routing table
- D. MAC address table
- E. Adjacency table

**Correct Answer:** AE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Cisco Express Forwarding (CEF) is a Layer 3 switching technology based on information contained in the forwarding information base (FIB) and the adjacency table.

The FIB is conceptually equivalent to a routing table in that it contains information used in the packet-forwarding decision. It is derived from the routing table and is optimized for maximum lookup throughput. The adjacency table contains information about the adjacent route processors. The adjacency table contains the MAC information for the next-hop addresses for all FIB entries. A device is considered adjacent if it is reachable over a single Layer 2 connection. It is stored in DRAM. The adjacency table is derived from the ARP table.

CEF is a topology-based Layer 3 switching technology that is enabled by default on the latest Cisco products. The FIB table stores IP destination prefixes from the most specific to the least specific entry in the Ternary Content Addressable Memory (TCAM). The content of the FIB table is similar to the routing table and contains the forwarding information similar to what is found in the IP routing table. A single FIB entry can point to up to six adjacencies. When changes are made to the IP routing table, the FIB table is also updated.

The Layer 3 processor engine builds the FIB and adjacency tables in software. That information is distributed from the control-plane hardware to the data-plane hardware Application Specific Integrated Circuits (ASICs) at the port or line card. This enhances the Layer 3 forwarding operation by moving it from the software-based engine to the ASICs. Of course, there are exception packets that are still software-processed, such as:  
Non-conforming protocols  
Data link encapsulations

Packets sent to a destination address that the CEF-based switch does not yet have a valid MAC address for will be sent instead to the Layer 3 engine. The Layer 3 engine will then perform the ARP request. Packets that arrive requiring fragmentation are also first sent to the Layer 3 engine.

When the adjacency table is full, a CEF TCAM table entry points to the Layer 3 engine to redirect the adjacency. Therefore, it will be forwarded by routing.

With respect to CEF switching, there is no ACL table. Access Control Lists (ACL) are used to filter traffic, but are not contained in a table and are not involved directly in Cisco Express Forwarding.

The routing table is not directly involved by CEF, although the FIB is derived from the routing table.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Cisco > IP Switching Cisco Express Forwarding Configuration Guide, Cisco IOS Release 15 > CEF Overview > CEF Adjacency Tables Overview

#### QUESTION 130

Which of the following statements best describes the result of issuing the instance 3 vllans 7 command?

- A. VLAN 7 is mapped to MST instance 3.
- B. VLAN 7 is mapped to switchport 3.
- C. VLAN 7 is mapped to three MST instances.
- D. Seven VLANs are mapped to MST instance 3.

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

When the instance 3 vllans 7 command is issued, the virtual local area network (VLAN) 7 is mapped to Multiple Spanning Tree (MST) Protocol instance 3. MST, which is defined by the 802.1s standard, maps a distinct group of VLANs to one STP instance. Multiple STP instances can be used with MST. The Cisco implementation of MST supports 256 instances. However, each instance must support a different group of VLANs because each VLAN can only be mapped to one instance.

To map one or more VLANs to an MST instance, issue the instance instance-ID vllans vllan-range command, where ID is the number of the MST instance and vllan-range is the VLAN or VLANs that should be mapped to the instance. For example, the command instance 1 vllans 14-16,99 maps VLANs 14 through 16 and VLAN 99 to MST instance 1.

The instance 3 vllans 7 command will not map VLAN 7 to switchport 3. The instance vllans command cannot be used to map multiple instances to a single VLAN. Each VLAN can only be mapped to one instance. When the instance 3 vllans 7 command is issued, only a single VLAN will be mapped to MST instance 3.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco IOS LAN Switching Command Reference > bridge-domain through instance (VLAN) > instance (VLAN)  
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Multiple Spanning Tree Protocol (802.1s) > Document ID: 24248

#### QUESTION 131

Which IOS commands are entered in interface configuration mode to configure a switch port to actively negotiate to be an 802.1Q trunk port? (Choose two.)

- A. switchport trunk dot1q
- B. switchport mode dynamic auto
- C. switchport trunk allowed vlan
- D. switchport mode trunk
- E. switchport trunk encapsulation dot1q

**Correct Answer:** DE

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Entering the IOS commands switchport mode trunk and switchport trunk encapsulation dot1q in interface configuration mode will allow a switch port to actively negotiate to be an 802.1Q trunk port. This allows Dynamic Trunking Protocol (DTP) to actively negotiate to be a trunk if the other side is set to trunk, desirable, or auto.

Use the following steps to configure a port as an 802.1Q trunk:

1. Enter the interface configuration.  
switch(config)# interface interface-id
2. Configure the port to use 802.1Q encapsulation.  
switch(config-if)# switchport trunk encapsulation dot1q
3. Configure the port as a trunk port.  
switch(config-if)# switchport mode trunk

Note: Trunking modes can be configured as dynamic desirable, dynamic auto, trunk, access, and nonegotiate. If both sides are set to auto, no negotiations will occur.

Verification of the configuration can be done by executing the show run command on both switches. An example partial output for two switches is shown below:

```
<output omitted>
hostname switcha
interface fastethernet 0/1
switchport mode dynamic auto
switchport trunk encapsulation dot1q
switchport trunk native vlan 5
<output omitted>
hostname switchb
interface fastethernet 0/2
switchport mode dynamic desirable
switchport trunk encapsulation dot1q
```

In the above partial output, the following can be determined:

Since it is configured as dynamic desirable, SwitchB will send DTP packets to SwitchA

Since the two switches are set to dynamic desirable and dynamic auto, they will form a trunk. When one end is set to desirable, the other must be set to trunk, desirable, or auto for a trunk link to form.

The native VLAN for SwitchA is VLAN 5 as indicated in the last line of its output. SwitchB is set to the default, which is VLAN 1. This configuration would result in a failure of the switches to form a trunk since the native VLANs do not match.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco IOS Master Command List, Release 12.4T>switchport mode

#### QUESTION 132

Which of the following standards describes the details of RSTP?

- A. 802.1d
- B. 802.1w
- C. 802.1s
- D. 802.1x

**Correct Answer:** B

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Rapid Spanning Tree Protocol (RSTP) is described in the IEEE 802.1w standard. It has several enhancements over Spanning Tree Protocol (STP), which uses 802.1d. The result of these enhancements is a more rapid convergence when topology changes occur. The two protocols can coexist in the network.

If a switch running RSTP receives an 802.1d Bridge Protocol Data Unit (BPDU), on a port it will begin to use 802.1d rules on that port. However, the IEEE 802.1d standard describes STP and not RSTP.

The IEEE 802.1s standard describes Multiple Spanning Tree Protocol (MST). This enhancement allows for multiple instances of STP. Unlike Common Spanning Tree Protocol (802.1q) and Per-VLAN Spanning Tree Protocol Plus (PVST+), which allow for a single instance of STP or an instance for every VLAN, respectively, MST allows the administrator to map several VLANs to the same instance, without committing them all to the same instance.

IEEE 802.1x describes a standard for port-based access control. It is not related to VLANs or their management.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify spanning tree

References:

Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

### QUESTION 133

The following commands have been issued on a Catalyst switch:

```
switchport trunk allowed vlan all
switchport trunk allowed vlan remove 1,101-4094
switchport trunk allowed vlan except 3001-4094
switchport trunk allowed vlan 1
switchport trunk allowed vlan add 101-200
```

Which of the following VLANs is allowed on the trunk?

- A. VLAN 1 and VLANs 101 through 200
- B. VLANs 101 through 200
- C. VLANs 1 through 3000
- D. VLANs 1 through 4094

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Virtual local area network (VLAN) 1 and VLANs 101 through 200 are allowed on the trunk. The switchport trunk allowed vlan command configures a trunk to carry one or more VLANs. The syntax for the switchport trunk allowed vlan command is switchport trunk allowed vlan {vlan-list | all | {add | except | remove} vlan-list}. VLANs specified in the vlan-list parameter should be separated by commas. However, if a contiguous group of VLANs is specified, the starting and ending VLAN numbers can be separated by a hyphen.

If no keywords are specified with the switchport trunk allowed vlan command, then only the VLANs contained within the vlan-list parameter will be allowed on the trunk. The all keyword specifies that all VLANs from 1 through 4094 should be allowed on the trunk. The add keyword specifies the VLANs that should be added to the list of VLANs that are already allowed by the trunk. The except keyword specifies that all VLANs from 1 through 4094 are allowed except the listed VLANs. The remove keyword specifies the VLANs that should be removed from the list of VLANs that are already allowed by the trunk.

In this scenario, the first command issued is switchport trunk allowed vlan all, which allows VLANs 1 through 4094. The second command issued is switchport trunk allowed vlan remove 1,101-4094, which removes VLAN 1 and VLANs 101-4094. Therefore, VLANs 2 through 100 are allowed. The third command issued is switchport trunk allowed vlan except 3001-4094, which specifies that all VLANs should be allowed except VLANs 3001 through 4094. Therefore, VLANs 1 through 3000 are allowed. The fourth command issued is switchport trunk allowed vlan 1, which specifies that only VLAN 1 should be allowed. The fifth command issued is switchport trunk allowed vlan add 101-200, which adds VLANs 101 through 200 to the list of allowed VLANs. Therefore, VLAN 1 and VLANs 101 through 200 are allowed on the trunk.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport trunk

### QUESTION 134

How long does it take for a port to transition from the STP blocking state to the forwarding state by default?

- A. 2 seconds
- B. 10 seconds
- C. 25 seconds
- D. 50 seconds
- E. 70 seconds

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

It usually takes 50 seconds for a port to transition from the blocking state to the forwarding state in STP. This delay is a function of the default settings for the forward-delay and max-age settings. The max-age delay is 20 seconds by default, and is used to transition from the blocking to the listening state. The forward-delay setting is 15 seconds by default. This timer is used in the transition from the listening to learning states, and again for the transition from the learning to the forwarding state. These timers give STP time to gather the correct information about the network topology. While they can be modified to make convergence more efficient, the default settings work for most networks. To change the timers on all switches in the VTP domain, change the timer settings on the root bridge and the changes will be forwarded to the other switches.

To prevent switching loops, spanning tree transitions each port through several states whenever there is a change in the network topology. Each state is briefly defined as follows:

**Blocking:** In the blocking state, a port does not forward frames, learn information, or send information. A forwarding port is placed in the blocked state when the port senses an absence of BPDUs, which are sent in the interval defined by the hello timer (two seconds by default). If the blocked port does not detect a BPDU for the length of time defined in the max-age setting (20 seconds by default), the port will transition into the listening state.

**Listening:** In the listening state, a port receives traffic but does not send information. This is the first transitional state after the blocking state. No user data is forwarded at this time, but the switch is very busy. It is during this stage that the switch participates in the election of the root bridge, the designation of root ports on the non-root bridges, and the selection of designated ports on each segment. Ports that are designated or root ports will transition to the learning state after the time defined in the forward delay (15 seconds by default) has elapsed.

**Learning:** In the learning state, a switch port can add the MAC addresses that it has learned into its address table, but cannot forward user data. The switch port will remain in this state until the amount of time defined in the forward-delay setting has elapsed (15 seconds by default), at which time it will transition into the forwarding state.

**Forwarding:** In the forwarding state, a port is actively forwarding packets. It will remain in the forwarding state until it does not detect a BPDU within the defined hello time, at which time the port is placed in the blocking state and the process starts again.

**NOTE:** One of the issues that can adversely affect the operation of STP is a duplex mismatch between the NICs on either end of a link between two switches. While this causes more of a performance problem than a loss of the link, the intermittent nature of the outage can cause one of the other links on the switch to transition into a forwarding state, as it may interpret this as a loss of connectivity. If one of the other links switches to forwarding and the link with the duplex mismatch comes back online (which could happen quickly), it can create a switching loop.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify spanning tree

References:

Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Design > Design Technotes > Understanding and Tuning Spanning Tree Protocol Timers > Document ID: 19120

Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Design > Design Technotes > Spanning Tree Protocol Problems and Related Design Considerations > Document ID: 10566

### QUESTION 135

Which of the following is true about CDP?

- A. It can be used to discover the network topology
- B. It is used to generate a denial of service attack
- C. It can be used as part of a MAC address flooding attack
- D. It is used to generate a MAC spoofing attack

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Cisco Discovery Protocol (CDP) is a Cisco proprietary protocol used by Cisco devices to obtain information about directly connected devices that are also made by Cisco. Since this information includes name, device type and capabilities, IP address, and other identifying information, if these packets are captured they can be used to map the network topology. Since the first step in the hacking process (Discovery, Penetration, and Control) is discovery, this can be a security threat.

CDP is not used to generate a DoS (denial-of-service) attack, which is an attack designed to overwhelm a device with work requests that make it unavailable for its normal jobs.

CDP is not used as part of a MAC address flooding attack. This is performed by a hacker creating packets with unique MAC addresses and flooding the switch's CAM table with these packets. When the CAM buffer is full, the switch will start sending packets out all interfaces enabling the hacker to capture packets from all switch ports, which is normally not possible on a switch, where each port is its own collision domain. CDP plays no role in this process.

CDP is not used to generate a MAC spoofing attack. This type of attack involves the creation of a packet using the MAC address of a known host in the network for the purpose of redirecting traffic to the hacker's machine instead. CDP plays no role in this process.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify Layer 2 protocols

References:

Cisco > Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring CDP

### QUESTION 136

Which of the following commands configures a port with a VLAN?

- A. vlan
- B. vlan database
- C. switchport access vlan
- D. switchport mode access

**Correct Answer: C**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The switchport access vlan command configures a port with a virtual local area network (VLAN). The syntax for the switchport access vlan command is as follows:

```
switchport access vlan {vlan-id | dynamic}
```

If the vlan-id parameter is specified, then a static VLAN will be configured. If the dynamic keyword is specified, then dynamic VLAN assignment by a VLAN Membership Policy Server (VMPS) will occur. Static VLAN configuration is easy to configure, secure and works well in networks where moves, additions, and changes are rare. In environments where this not the case, dynamic VLANs may be preferable.



The vlan command is used to add VLANs to the VLAN database and to configure VLAN settings.

The vlan database command is issued to enter VLAN configuration mode. The following commands can be issued from VLAN configuration mode:

abort - exits without applying changes  
apply - applies changes and bumps the revision number  
exit - applies changes, bumps the revision number and exits VLAN configuration mode  
no - negates a command  
reset - discards changes and rereads the VLAN database  
show - displays information  
vlan - configures the VLAN database  
vtp - configures VLAN Trunking Protocol (VTP) settings

The switchport mode access command disables trunking for a port. The syntax for the switchport mode command is as follows:

switchport mode {access | trunk | dynamicdesirable | dynamicauto}

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport access

#### QUESTION 137

A new switch that contains a configuration consisting of only VLAN 5 was just added to the network. Now users assigned to VLANs 9 and 10 are complaining of communication problems.

Using the show vlan command, you discover that only VLAN 5 and the default VLANs exist on all your switches.

What could have caused this problem?

- A. The new switch had the default password set.
- B. The domain name on the new switch did not match the rest of the network.
- C. The new switch was configured in server mode and the revision number was lower than the current number in the network.
- D. The new switch was configured in server mode and the revision number was higher than the current number in the network.
- E. The new switch was configured in transparent mode and the revision number was higher than the current number in the network.

**Correct Answer: D**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Adding a switch that is configured in VTP server mode and has a revision number higher than the current number in the network could cause the communication problem in the scenario. If the new switch was configured in server mode and the revision number was higher than the revision number on existing switches, it could cause the rest of the switches to update with the information contained in that new advertisement.

VTP advertisements are flooded throughout the management domain every five minutes or whenever a change occurs in the network. These advertisements are originated from a switch that is in server mode, and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the domain name and password (if defined) against its own configuration. Next, the revision number is checked to see if it is higher than the last value stored in the receiving switch. If the revision number is higher, the receiving switch will overwrite its VLAN database with the information in the advertisement.

A VTP switch in transparent mode will receive and forward VTP advertisements. It will not use the contents of the advertisement to synchronize with its own VLAN database.

The password, domain name, and VTP mode will not cause the switch to overwrite the other switches. This is a revision number issue.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

#### QUESTION 138

Which IOS commands should you enter in interface configuration mode to configure a switch port as an access port and assign it to VLAN 25? (Choose two.)

- A. trunk on
- B. switchport mode access
- C. vlan-membership static 25
- D. switchport access vlan 25

**Correct Answer: BD**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

Use the following steps to assign ports to a VLAN:

1. Enter the interface to be added to the VLAN.  
switch(config)# interface interface-id

2. Configure the port as a Layer 2 access port.  
switch(config-if)# switchport mode access

3. Assign the port to a VLAN.  
<fon

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport access vlan

#### QUESTION 139

What Cisco switch feature allows IP phones to be automatically placed into a separate VLAN from data traffic?

- A. marking
- B. AutoQoS
- C. private VLANs
- D. auxiliary VLANs

**Correct Answer: D**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

Auxiliary VLANs allows IP phones to be automatically placed into a separate VLAN from data traffic. The information the phones need regarding this voice VLAN is provided by the switch. This allows the data and voice traffic to use the same physical topology but remain logically separate. The following is an example of the commands that should be executed on the switch to instruct it to provide this information to the IP phone by CDP:

```
Switch> (enable) set port auxiliaryvlan 2/1-3 222
```

This command creates the auxiliary VLAN 222 and adds ports 2/1 to 2/3 to the VLAN.

Private VLANs are not used for voice traffic. Private VLANs are secondary VLANs created by an administrator that are not accessible by other secondary VLANs.

Marking is the process of setting the Class of Service (CoS), IP precedence, or DSCP of a packet to a specific value that will provide appropriate QoS throughout the network. It is not involved in separating voice and data traffic.

Auto QoS is a method of configuring commonly used QoS features on a Cisco switch with a single command. It is not involved in separating voice and data traffic.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:  
Cisco > Catalyst 4500 Series Software Configuration Guide, 8.1 > Configuring VLANs > Configuring Auxiliary VLANs

#### QUESTION 140

What attack technique attempts to fill a switching table so the attackers can capture traffic passing through a switch?

- A. VLAN hopping
- B. MAC spoofing
- C. Rogue device
- D. MAC flooding

**Correct Answer: D**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

MAC flooding is an attack technique in which frames with unique, but invalid, source MAC addresses flood the switch and exhaust the CAM table space. Eventually no more MAC addresses can be added because the table is full. When this occurs, any packets destined for a MAC address not in the table will be flooded to all other ports. This would allow the attacker to see the flooded traffic and capture information. The switch would be essentially functioning as a hub in this case.

Two methods of mitigating these attacks are:  
Implementing port security  
Implementing VLAN access maps

VLAN hopping is an attack that allows an attacker to access network resources on a different VLAN without passing through a router. The attacker can create a packet with two 802.1Q VLAN headers on it (called double tagging) and send it to a switch. The switch port will strip off the first header and leave the second. The second header will be seen as the originating VLAN, allowing the attacker access to a VLAN they are not connected to. Executing the switchport mode access command on all non-trunk ports can help prevent this attack. Pruning the native VLAN from a trunk link can also help.

VLAN hopping is a security concern because it can be accomplished without the packet passing through a router and its security access lists. For this reason, private VLANs and VACLs should be used to secure access between VLANs. Techniques to prevent these attacks are:  
Prevent automatic trunk configurations by explicitly turning off Dynamic Trunking Protocol on all unused ports  
Place unused ports in a common unrouted VLAN

MAC spoofing is an attack that allows an attacking device to receive frames intended for a different host by changing an assigned Media Access Control (MAC) address of a networked device to a different one. Changing the assigned MAC address may allow the device to bypass access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer.

A rogue device is a device attached to the network that is not under the control of the organization. This term is normally used to mean a wireless device, perhaps an access point that is not operating as a part of the company's infrastructure. Employees may bring their own access points and connect them to

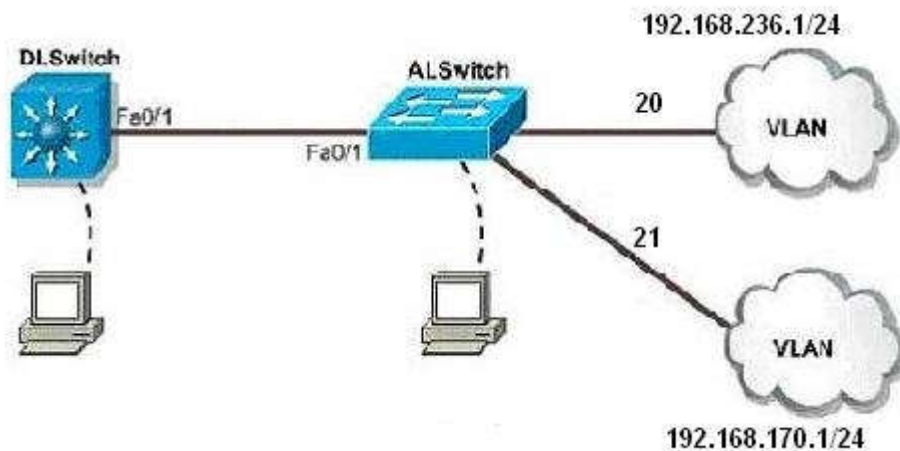
the network so they can use their computer wirelessly. This creates a security gap since the device is probably not secured to protect the traffic. An attacker could connect a rogue access point to a company's network and capture traffic from outside the company's premises.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Cisco > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > Cisco Catalyst 6500 Series Switches > VLAN Security White Paper > MAC Flooding Attack

#### QUESTION 141

A company has a following network infrastructure. Refer to the exhibit:



To enable inter-VLAN routing on the distribution layer switch, which of the following commands should be used?

- A. dls switch# switchport mode access
- B. dls switch (config) # switchport mode trunk
- C. dls switch(config-if) # switchport mode trunk
- D. dls switch(config-if) # switchport mode access

**Correct Answer:** C

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

You should use switchport mode trunk command at the interface configuration prompt to enable inter-VLAN routing. This command sets the port as a trunk port. Trunks carry traffic from all VLANs to and from the switch by default, and can be configured to carry specific VLAN traffic as well.

A port on a Cisco switch is either an access port or a trunk port. An access port only carries traffic for the VLAN of which it is a member and does not tag or mark the frame with a VLAN ID. A trunk port carries traffic from multiple VLANs and tags or marks each frame with a VLAN ID so it can be determined where it goes when it gets to the other switch.

You can enable inter-VLAN routing by enabling trunking using the following command:

switchport mode trunk

You would not use the dls switch# switchport mode access command to enable inter-VLAN routing. This command sets the port as an access port, which is capable of carrying only the traffic a single VLAN. Moreover, even if that were the intent, the command must be executed in interface mode and not global configuration mode.

You would not use the dls switch (config) # switchport mode trunk command to enable inter-VLAN routing. This is the correct command, but is shown being executed in global configuration mode instead of interface mode.

You would not use the dls switch(config-if)# switchport mode access command to enable inter-VLAN routing. This is both the wrong command and is being executed at an incorrect prompt.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco Press > Articles > Network Technology > General Networking > VLANs and Trunking  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport mode trunk

#### QUESTION 142

What IOS VLAN commands would create a new VLAN and assign it to a port? (Choose two.)

- A. switch(config)# vlan 10
- B. switch(config-if)# switchport access vlan 10
- C. switch(config)# vlan database 10
- D. switch(config-if)# switchport vlan 10 enable

**Correct Answer:** AB

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The commands necessary to create a VLAN and assign it to a port are `switch(config)# vlan 10` and `switch(config-if)# switchport access vlan 10`. The global configuration mode is used to create VLANs with the command `vlan {vlan_id}`. VLANs can be removed with the `no` form of the command.

Ports are assigned as members of VLANs in the interface configuration mode with the command `switchport access vlan {vlan_id}`. At this point, if the port is in access mode, it will participate as a member of the VLAN. The mode of the port can be forced to be access in the interface configuration mode with the command `switchport mode access`.

The command `vlan database 10` is not a valid command, but it is similar to a valid command. An optional, but not recommended, way to create a VLAN is in VLAN database mode. This is accessed from global configuration mode with the command `vlan database`. The prompt would be `switch(vlan)#`. At this prompt, a VLAN can be created with the command `vlan 10`. The problem with VLAN database mode is that the configurations issued here have to be applied with either the `apply` or `exit` commands. Using `CTRL-Z` to exit would cancel the changes made in this mode.

The command `switchport vlan 10 enable` is not correct due to invalid syntax.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANs/VTP) > Configure > Configuration Examples and Technotes > Creating Ethernet VLANs on Catalyst Switches

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport access

Cisco > Cisco IOS LAN Switching Command Reference > uddid through vtp v2-mode > vlan

### QUESTION 143

Which devices are required to provide connectivity between VLANs? (Choose two.)

- A. hub
- B. router
- C. bridge
- D. multilayer switch
- E. DSU/CSU

**Correct Answer:** BD

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Routing between different VLANs can be accomplished using VLAN-capable multilayer switches or routers.

Devices within a single VLAN can communicate without the aid of a Layer 3 device, but as a rule, devices in different VLANs require a Layer 3 device for communication. The only situation where two computers in different VLANs located on different switches can ping one another is if they have addresses in the same subnet, and if the link between the two switches is an access port rather than trunk port.

Since traffic is sent untagged in an access link, if the link between the switches is an access link and the computers are in the same subnet, they will be able to ping one another. The following steps can be used to configure inter-VLAN routing on a multilayer switch:

1. Enable IP routing.  
`switch(config)# ip routing`

Note: Routing must be enabled on a Layer 3 switch for interVLAN routing to occur. This can be verified by examining the output of the `show run` command executed on the switch. The example below is output from the `show run` command executed on a switch that has IP routing enabled, as can be seen in the third line (`ip routing`):

```
hostname SwitchA
!
ip subnet-zero
ip routing
!
vtp domain Cisco
vtp mode transparent
<output omitted>
```

2. Specify an IP routing protocol, such as RIP.  
`switch(config)# router rip`

3. Specify a VLAN interface.  
`switch(config)# interface vlan vlanid`

4. Assign an IP address to the VLAN.  
`switch(config-if)# ip address address subnet-mask`

Hubs operate at the Physical layer (Layer 1) and do not have the ability to route.

Bridges operate at the Data Link layer (Layer 2) and do not have the ability to route.

CSU/DSUs convert signals from a LAN to a type necessary for the telco. They do not have the ability to route.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:



#### QUESTION 144

Which redundancy mode for supervisor engine modules exhibits all of the following characteristics?

- Static routes are maintained during a switchover
- The Forwarding Information Base (FIB) is cleared during a switchover
- Dynamic route information is cleared during a switchover
- Route engine is initialized and switch modules are loaded

- A. RPR
- B. RPR+
- C. SSO
- D. NSF

**Correct Answer:** B

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Redundant supervisor engine modules can be configured in several modes. In route processor redundancy plus (RPR+) mode, the backup module is booted up and the supervisor and route engines initialize. However, no Layer 2 or Layer 3 functions are started, which means it will be necessary to start them after a failover. This also means the routing protocols must re-converge and the FIB table must be rebuilt, since it is derived from the routing table. The static routes are maintained in the running configuration, so they are not lost in the failover.

In route processor redundancy (RPR) mode, the module is booted, but the supervisor and route engines are not initialized.

In stateful switchover (SSO) mode, all functionality provided by RPR+ is available at failover, and the FIB table is not

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify other LAN switching technologies

References:

Cisco > Catalyst 6500 Release 12.2SX Software Configuration Guide > RPR Supervisor Engine Redundancy

Cisco > Catalyst 6000/6500 Series Switches with Redundant Supervisor Engines Software Image Upgrade Configuration Guide (4.5) > Background Information> Supervisor Engine Redundancy

#### QUESTION 145

Which Cisco switch feature enables IP phones to be assigned IP addresses from a different subnet than the workstation attached to the same port?

- A. Auxiliary VLAN
- B. 802.1P
- C. 802.1Q
- D. in-line power

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Auxiliary VLANs can assist in the deployment of Cisco IP telephones by allowing a Catalyst switch access port to support the data device on one VLAN and have the IP telephone assigned to a different VLAN. The auxiliary VLAN ID is not required to match the native VLAN associated with the access port of the switch. Therefore, the two port attached devices (the phone and the workstation) can be on two different broadcast domains or IP subnets. Some Cisco Catalyst switches provide the auxiliary VLAN feature that provides the automatic assignment of an IP telephone to a VLAN. This auxiliary VLAN feature is also known as the voice VLAN feature.

IP telephones typically have a built in 3-port 10/100 hub. One port internally attaches to the phone, one port is attached to the switch access port, and the last port is used to connect to the workstation. The switch uses CDP on a port on which an auxiliary VLAN has been configured to advertise 802.1Q and 802.1P information. The attached IP telephone can use the advertised information to learn which VLAN ID and priority tag to use. The default Class of Service (CoS) value for incoming traffic is 0.

Having the telephone and the data device use different frame types and belong to different VLANs allows the administrator to place the telephones on their own subnet. Voice traffic on a separate VLAN is less likely to contend with the data devices.

To configure the interface on the switch to support auxiliary VLANs, use the following commands:

switchport voice vlan VVID: This command is used to enable the access port to forward 802.1Q packets received tagged with the ID of the voice VLAN (VVID) to the VLAN defined as the voice VLAN. By default, 802.1Q packets are sent by IP phones with a QoS priority of 5.

switchport voice vlan dot1p: This command is used to instruct the attached IP telephone to send packets using the VLAN ID of the port's native VLAN with a dot1p priority of 5.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Cisco > Cisco Catalyst 6500 Series Switches > Data Sheets > Cisco Catalyst 6500 Series 10/100- 10/100/1000-MBPS Ethernet Interface Modules Data Sheet

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport voice vlan

#### QUESTION 146

Which command do you use on a switch to put an interface that is in Layer 3 mode into Layer 2 mode?

- A. vlan

- B. no vlan
- C. switchport
- D. no switchport

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

Use the switchport command to put an interface that is in Layer 3 mode into Layer 2 mode.

```
switch(config-if)# switchport
```

Use the no switchport command to remove Layer 2 configurations and return an interface to Layer 3 mode.

```
switch(config-if)# no switchport
```

The enhanced multilayer switch image must be installed on the switch to use this command.

The vlan vlan-id configuration command is used to configure VLAN characteristics for a specific VLAN. Use the no keyword without additional parameters to delete a VLAN.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Catalyst 3560 Switch Command Reference, Rel. 12.2(25)SEE > Catalyst 3560 Switch Cisco IOS Commands - shutdown through vtp > switchport  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport

#### QUESTION 147

What information is displayed by the command switch# show ip interface brief?

- A. a summary of the IP addresses and subnet mask on the interface
- B. a summary of the IP addresses on the interface and the interface's status
- C. the IP packet statistics for the interfaces
- D. the IP addresses for the interface and the routing protocol advertising the network

**Correct Answer: B**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command show ip interface brief displays a summary of the IP address on the interface and the interface's status. The status means whether the interface is up. This command is useful when you are connected a router or switch with which you are not familiar, because it allows you to obtain the state of all interfaces or switch ports. Sample output is shown below:

```
Switch88# show ip interface brief
Interface IP-Address OK? Method Status Protocol
FastEthernet0/1 unassigned YES manual down down
FastEthernet0/2 unassigned YES manual down down
FastEthernet0/3 unassigned YES manual down down
FastEthernet0/4 unassigned YES manual down down
FastEthernet0/5 unassigned YES manual down down
FastEthernet0/6 unassigned YES manual down down
FastEthernet0/7 unassigned YES manual down down
FastEthernet0/8 unassigned YES manual up up
FastEthernet0/9 unassigned YES manual down down
FastEthernet0/10 unassigned YES manual d own down
```

This command does not display subnet mask information. Use other commands, such as show ip interface or show run interface, to verify the subnet mask.

IP statistics about the interface are displayed with the command show ip interface. Adding the brief keyword tells the switch to leave out everything but the state of the interface and its IP address.

To view the routing protocol advertising an interfaces network, you would use the command show ip protocol.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Cisco IOS IP Addressing Services Command Reference > show ip interface

#### QUESTION 148

Which characteristics apply to multilayer switching? (Choose three.)

- A. Uses CPU-based packet forwarding
- B. Performs collision detection
- C. Provides isolation of the collision domain
- D. Provides Network-layer and Transport-layer access controls
- E. Determines the forwarding path based on the Network layer address

**Correct Answer:** CDE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Multilayer switching characteristics include determining the forwarding path based on the Network layer address (Layer 3), providing isolation of the collision domain (Layer 2); and providing Network-layer and Transport-layer access controls (Layers 3 and 4).

Multilayer switching combines the functionalities of Layer 2 switching and Layer 3 switching. Layer 3 switching is routing performed by hardware, specifically by utilizing application-specific integrated circuits (ASICs). The Layer 3 switch can perform all of the basic operations of traditional routers, including the following:

Path selection based on the packet's Layer 3 protocol information  
Layer 3 packet validation  
Flow accounting (Layers 3 and 4)  
Layer 3-based access controls and security

In contrast to Layer 2 switches, which provide the benefits of bridging, Layer 3 switches offer another high-performance packet switching solution.

CPU- based packet forwarding and collision detection are not unique characteristics of multilayer switching. CPU-based packet forwarding is not a concept used by routers or switches. Collision detection is a characteristic of Ethernet, which is not unique to multilayer switching.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Cisco > Home > Support > Configuring IP MLS > Understanding How IP MLS Works

#### QUESTION 149

Which IOS command do you use to remove Layer 2 configurations and return an interface to Layer 3 mode?

- A. vlan
- B. no vlan
- C. switchport
- D. no switchport

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Use the no switchport command to remove Layer 2 configurations and return an interface to Layer 3 mode. The syntax of the command is:

```
switch(config-if)# no switchport
```

The enhanced multilayer switch image must be installed on the switch to use this command.

The switchport command without the no keyword converts the port back to a Layer 2-switched interface.

```
switch(config-if)# switchport
```

The vlan vlan-id configuration command is used to configure VLAN characteristics for a specific VLAN. Use the no keyword without additional parameters to delete a VLAN.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport  
Catalyst 3560 Switch Command Reference, Rel. 12.2(25)SEE > Catalyst 3560 Switch Cisco IOS Commands - shutdown through vtp > switchport

#### QUESTION 150

You made changes to a VLAN, but the changes were not propagated to the other switches in the VTP domain. You enter a show vtp command at the switch where the changes were made, which displays the following output:

```
Switch1# show vtp
VTP version: 1
Configuration revision: 4
Maximum VLANs supported locally: 1005
Number of existing VLANs: 3
VTP domain name : Mobile
VTP password :
VTP operating mode : Transparent
VTP pruning mode : Enabled
VTP traps generation : Enabled
Configuration last modified by: 10.1.1.34 at 00-00-0000 00:00:00
```

What should you do to solve this problem?

- A. Disable VTP pruning.
- B. Change the VTP operating mode to server.
- C. Upgrade the VTP version to version 2.
- D. Upgrade the VTP version to version 3.

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

The output of the show vtp command shows that the VTP operating mode is transparent mode. This means that you can make VLAN changes on the switch, but they will only affect that switch. Changes will not be propagated to other switches in the Layer 2 network. You will need to change the operating mode to server if you want to VLAN changes to be propagated to other switches.

To change the VTP operating mode to server, you would enter the vtp server global command as shown:

```
switch1#(config) vtp server
```

You should not disable VTP pruning. This will have no effect on the propagation. You must change the mode of the switch.

You should not upgrade the VTP version to version 2 or version 3. This will have no effect on the propagation. You must change the mode of the switch.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp server

**QUESTION 151**  
What are the three RSTP port states? (Choose three.)

- A. Initializing
- B. Blocking
- C. Learning
- D. Listening
- E. Forwarding
- F. Discarding

**Correct Answer:** CEF  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Rapid Spanning Tree Protocol (RSTP) uses only three port states: discarding, learning, and forwarding. The learning and forwarding states are the same as the original STP standard, but the discarding state performs the functions originally performed in the disabled, blocking, and listening STP states.

With STP, you can safely assume that a listening port is either designated or root, and is on its way to the forwarding state. Unfortunately, once a port is in the forwarding state, there is no way to tell whether the port is root or designated. There is no difference in the operation of a port in blocking state and a port in listening state, since they both discard frames and do not learn MAC addresses. The real difference is in the role the spanning tree assigns to the port. RSTP decouples the role and the state of a port.

With RSTP, a role is assigned to a port. The root port and designated port roles are the same as with STP, while the blocking port role is split into the backup and alternative port roles. The Spanning Tree Algorithm (STA) determines the role of a port based on Bridge Protocol Data Units (BPDUs). The RSTP roles can be defined as follows:

Root port: The port receiving the best BPDU on a bridge (lowest-cost path to the root bridge) is the root port.

Designated port: The port that has the best path to the root bridge on a given segment is the designated port. The bridges connected to a given segment listen to each other's BPDUs and agree on the bridge sending the best BPDU as the designated bridge for the segment. The corresponding port on that bridge is the designated port.

Alternative port: An alternative port is a port blocked by receiving more useful BPDUs from another bridge. It becomes the root port if the active port fails.

Backup port: A backup port is a port blocked by receiving more useful BPDUs originating from the same bridge. It becomes the designated port if the existing designated port fails.

Ports on the switch can also be classified as edge ports and non-edge ports. Access ports or edge ports are those that attach to devices such as workstations or printers. Non-edge ports are those that connect to other switches. If a non-edge port transitions to a forwarding state, a TC BPDU will be generated. On the other hand, when an edge ports transitions to the forwarding state, such as after a computer boots up or a device is connected to the port, no TC BPDU is generated.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

**QUESTION 152**  
Which of the following statements best describes the purpose of ARP with respect to CEF?

- A. ARP is used to build the FIB.
- B. ARP is used to reindex the routing table.
- C. ARP is used to build the adjacency table.
- D. ARP is used to decrease the amount of time spent searching for an entry within a routing table.

**Correct Answer:** C  
**Section:** Layer 2 Technologies  
**Explanation**



**Explanation/Reference:**

Explanation:

Address Resolution Protocol (ARP) is used by Cisco Express Forwarding (CEF) to build the adjacency table. CEF is the switching method used by Catalyst switches. Unlike traditional multilayer switching (MLS), which merely caches Layer 3 information received when traffic passes through a switch, CEF attempts to optimize the routing process by reindexing the routing table and then building an adjacency table based on the routing table information. The type of MLS performed by CEF is called topology-based switching; traditional MLS is known as route caching, demand-based switching, and flow-based switching.

The routing table is reindexed by using a binary search method. The reindexed routing table is called the forwarding information base (FIB). Reindexing the routing table reduces the amount of time spent searching for an entry within a routing table.

After the FIB is created, an adjacency table is created to map the appropriate Layer 2 next-hop address or addresses to each FIB entry. ARP is used to retrieve the Layer 2 address information. If multiple Layer 2 next-hop addresses are available for an entry in the FIB, then CEF can employ load balancing for packets headed to that destination.

The final result is a single database of routing information (FIB) is built for the switching hardware.

Two extremely useful commands for verifying CEF are:

show ip cef network address - displays entries in the forwarding information base (FIB)

show adjacency detail | begin adjacency address - shows information about a specific adjacency in the adjacency table

Both commands are shown below with explanations.

```
SwitchA# show ip cef 192.168.6.0
192.168.6.0/24, version 302, cached adjacency 192.168.166.5, 0 packets, 0 bytes
Via 192.168.166.5, VLAN 185, 0 dependencies
Next-hop 192.168.166.5, VLAN 185
Valid cached adjacency
```

Above it can be determined that there is a valid CEF entry for the destination network 192.168.6.0 and that there is a valid cached adjacency to the 192.168.166.5 next hop IP address.

In the command output below, it can be determined that 005565946856 is the MAC address of the 192.168.166.5 next-hop address:

```
SwitchA# show adjacency detail | begin 192.168.166.5
```

```
IP VLAN 185 192.168.166.5(6) 0 packets, 0 bytes
005565946856
```

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify switch administration

References:

Cisco > Cisco IOS IP Switching Configuration Guide, Release 12.4 > Part 1: Cisco Express Forwarding > Cisco Express Forwarding Overview > Cisco Express Forwarding Adjacency Tables Overview

Cisco > Cisco IOS IP Switching Command Reference > show adjacency through show ipv6 cef with source > show adjacency

Cisco > Cisco IOS IP Switching Command Reference > show adjacency through show ipv6 cef with source > show ip cef

**QUESTION 153**

You want to create a VTP domain named myvtpdomain and define this switch as one that can be configured with VLANs and advertises VLAN changes to other switches.

What commands should you use? (Choose two.)

- A. switch(config)# vtp mode server
- B. switch(config)# vtp domain myvtpdomain
- C. switch(config)# vtp domain server
- D. switch(config)# vtp server myvtpdomain

**Correct Answer:** AB

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

To create a VTP domain and configure the switch so it can configure and advertise VLANs (server mode), use the global configuration commands vtp mode server and vtp domain myvtpdomain. The VTP domain is created with the command switch(config)# vtp domain {domainname}. The mode of the switch is defined with the command switch(config)# vtp mode {mode}. The possible modes are server, client, and transparent. Server means that the switch can be used to create, delete, and modify VLANs; and send and receive advertisements about VLAN changes. Client means that the switch cannot be used to create or change VLANs, but only send and receive advertisements, adjusting its own database to match advertisements that it hears. Transparent means that the switch can be used to create, delete, and modify VLANs; but does not advertise those changes to other switches. Any advertisements that a transparent switch receives are forwarded on to other switches, but not applied by the switch.

The commands vtp domain server and vtp server myvtpdomain are not valid due to incorrect syntax.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

Cisco > Cisco IOS LAN Switching Command Reference > udd through vtp v2-mode > vtp

Cisco > Cisco IOS LAN Switching Command Reference > udd through vtp v2-mode > vtp domain

**QUESTION 154**

Which parameters are found in VTP advertisements? (Choose three.)

- A. Password
- B. VTP mode
- C. IP address
- D. Switch name
- E. Revision number
- F. Management domain name

**Correct Answer:** AEF

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The management domain name, password, and revision number are all checked before the VTP frame is processed. To propagate VTP information between switches, both switches must have a trunk port configured and must have a matching native VLAN, which is VLAN 1 by default.

VTP advertisements are flooded throughout the management domain every five minutes or whenever there is a change. These advertisements are originated from a switch that is in server mode and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the management domain name and password (if defined) against its own configuration. The revision number is checked. If the revision number is higher than the last value store in the receiving switch, the receiving switch will overwrite its VLAN database with the information in the advertisement.

A VTP switch in transparent mode will receive and forward VTP advertisements. It will not use the contents of the advertisement to synchronize with its own VLAN database.

The VTP mode, IP address, and switch name are not found in VTP advertisements.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

#### QUESTION 155

In what mode does an LWAPP-enabled access point operate?

- A. lightweight mode
- B. autonomous mode
- C. WGB
- D. ad hoc mode

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Lightweight access point protocol (LWAPP)-enabled access points operate in lightweight mode. LWAPP is a protocol used to allow centralized management of APs. The management components are removed from the APs, and a WLAN controller provides a single point of management. This controller coordinates WLAN access, managing the load on the APs and user movement between APs. Upon starting, an LWAPP-enabled access point must obtain an IP address. It can then discover the controller using DHCP, DNS, or a subnet broadcast. When multiple wireless controllers are detected by an AP, it chooses to associate with the controller that has the fewest existing associated APs.

Individually configured APs that operate without central management are operating in autonomous mode. This would be the opposite of lightweight mode, which is made possible by LWAPP. Autonomous access points can be upgraded to lightweight. If they are upgraded, they will only function in conjunction with a WLAN controller. Moreover, when an autonomous access point is upgraded to lightweight, the console port only provides read access to the unit.

Characteristics that autonomous and lightweight access points have in common:

Both support Power over Ethernet (PoE)

Both can use a Cisco Secure Access Control server (ACS) for security

A wireless gateway bridge (WGB) is used to connect a computer without a wireless network card to a wireless network, but not separate WLANs. The WGB can connect up to eight computers to a WLAN. The WGB connects to the root AP through a wireless interface.

Ad hoc is a WLAN mode used for peer-to-peer connectivity. Ad hoc mode allows wireless-enabled computers to communicate with each other without having an AP involved.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify other LAN switching technologies

References:

Cisco > Support > Product Support > Wireless > Cisco Aironet 1200 Series > Reference Guides > Technical References > Upgrading Autonomous Cisco Aironet Access Points to Lightweight Mode

Cisco > Support > Technology Support > Wireless/Mobility > Wireless, LAN (WLAN) > Design > Design Technotes > Cisco Wireless Devices Association Matrix

#### QUESTION 156

Which command produced the following output?

```

VLAN0100
Spanning tree enabled protocol ieee
Root ID      Priority      32768
              Address      00d0.00b8.41a3
              This bridge is the root
              Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec

Bridge ID     Priority      32768
              Address      00d0.00b8.41a3
              Hello Time   2 sec    Max Age 20 sec    Forward Delay 15 sec
              Aging Time   300

Interface      Role  Sts  Cost      Prio.Nbr  Status
-----
Fa2/4          Desg  FWD  200000     128.196   P2p
Fa2/5          Back  BLK  200000     128.197   P2p

```

- A. switch# show spanning-tree vlan 100
- B. switch# show vlan 100
- C. switch# show spanning-tree summary
- D. switch# show interface vlan 100
- E. switch# show spanning-tree inconsistent ports

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command show spanning-tree vlan 100 was used to provide the output in the exhibit. This output helps to identify the state of each port on the switch that is a member of VLAN 100. It is also used to identify the root bridge in the spanning tree.

The command show vlan 100 will provide basic information about VLAN 100, such as what ports are assigned to it, but will not display the STP information about the VLAN as the exhibit shows.

The command show spanning-tree summary can be used to verify the enabling of the extended system ID. This command is not used to provide the output in the exhibit.

The command show interface vlan 100 displays the same kind of information as would be displayed for any other interface, including the IP address configuration and whether the interface is up. It does not provide STP information about the switch as displayed in the exhibit.

The command show spanning-tree inconsistent port is used to identify inconsistent ports on a switch. This can occur as a result of implementing the Root Guard feature on a switch. Root Guard can be implemented on a port to prevent the reception of superior BPDUs from causing a new root bridge from being elected. This can sometimes occur when a new switch is introduced with an unknown bridge ID. When a port is configured with Root Guard and it receives a superior BPDU, it will block the port, discard the BPDU, and assign a state of inconsistent to the port.

Below is an example of the partial output of the show spanning-tree inconsistent ports command:

```
Switcha# show spanning-tree inconsistentports

Name Interface Inconsistency
-----
VLAN0010 fastethernet0/1 Root Inconsistent
VLAN0010 fastethernet0/2 Root Inconsistent
VLAN0030 fastethernet0/1 Root Inconsistent
VLAN0030 fastethernet0/2 Root Inconsistent
Number of inconsistent ports (segments) in the system :4
```

The output shows that devices connected to ports Fa0/1 and Fa0/2 are sending superior BPDUs (perhaps from a new switch). Because of this, no traffic will be forwarded across the ports. Once these superior BPDUs are stopped by changing the priority of the new switch, the interfaces will recover and resume normal operation.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Cisco IOS LAN Switching Command Reference > set port flowcontrol through show uddl > show spanning-tree

**QUESTION 157**  
In which VTP modes can you create and delete local VLANs? (Choose two.)

- A. User
- B. Host
- C. Client
- D. Server
- E. Transparent

**Correct Answer:** DE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create or delete VLANs. You can create local VLANs in server and transparent VTP modes. However, VLANs created on a switch in transparent mode apply only to that switch, and information about these VLANs is not propagated throughout the VTP domain.

VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM. To propagate VLAN information, the switch must be configured with a VTP domain name.

VTP transparent mode forwards VTP advertisements and saves the VLAN configuration in NVRAM. It does not synchronize VLAN configuration information. A switch in transparent mode can create, delete, and modify VLANs, but changes are not transmitted to other switches in the domain. Changes only affect the local switch.

VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers. A Catalyst switch can create, modify, and delete VLANs in server or transparent modes, but not in client mode.

VTP user and host modes do not exist.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

#### QUESTION 158

How is a VLAN best described?

- A. subnet
- B. segment
- C. collision domain
- D. broadcast domain

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

A VLAN can best be described as a broadcast domain. A broadcast domain is a group of devices such that when one device in the group sends a broadcast, all the other devices in the group will receive that broadcast. Switching can segment a flat network into many smaller collision domains, but all stations must process all broadcasts. VLANs solve this problem by creating separate broadcast domains.

A subnet is an IP-addressing division where one subnet's broadcasts are isolated to only that subnet, and no broadcast traffic crosses the subnet divisions without being routed. While in most cases each VLAN may be its own subnet, this is not always the case.

A LAN segment is a general term for a subnet or broadcast domain.

A collision domain is a domain where two or more devices in the domain could cause a collision by sending frames at the same time. Each port on a switch will host a collision domain.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > Creating Ethernet VLANs on Catalyst Switches

#### QUESTION 159

Which VTP mode and version should be configured on a switch so that its VLAN database can be separately maintained while it forwards all VTP advertisements it receives?

- A. Server mode and version 1
- B. Client mode and version 1
- C. Server mode and version 2
- D. Client mode and version 2
- E. Transparent mode and version 2
- F. Transparent mode and version 1

**Correct Answer:** E  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

A switch configured in VTP transparent mode allows the administrator to maintain the switch VLAN configuration information and not advertise its database to other switches in the network. A switch configured in VTP transparent mode using version 1 will only forward VTP advertisements it receives if the version used to send the update is also version 1. Using version 2 it will forward advertisements it receives without checking the version number.

There are two versions of VTP: version 1 and version 2. VTP version 1 is the default. The two versions are not interoperable. To support version 2, all of the switches in a network need to be configured to run in VTP version 2.

To enable, or revert back to, VTP version 1 at the configuration prompt, use the following command:

```
switch(config)# no vtp v2-mode
```

VTP version 2 offers some features that are not available in version 1.

Token Ring support: Version 2 provides the ability to support Token Ring LAN parameters, such as ring numbers and hop counts, used in Token Ring LAN switching and VLANs.

Unrecognized type, length, value (TLV) support: A version 2-enabled switch in server or client modes will propagate configuration changes to its other trunks,



even for TLVs it is not able to parse.

Version-independent transparent mode: In version 1, a transparent mode switch checks the domain name and the version of a received VTP advertisement before forwarding it. Using version 2, it ignores the version when forwarding the advertisement.

Consistency checks: With version 2, the switch performs consistency checks of VLAN information, such as names and values, when new information is entered through the CLI or using SNMP. It does not do this when updating with information from a new advertisement.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

Cisco > Cisco IOS LAN Switching Command Reference > udld through vtp v2-mode > vtp

#### QUESTION 160

Which IOS interface configuration commands are required to configure a switch port to actively negotiate to be an 802.1Q trunk port that, when active, will send packets destined for VLAN 3 untagged? (Choose three.)

- A. switchport mode trunk
- B. switchport trunk dot1q 3
- C. switchport native vlan 3
- D. switchport trunk mode dot1q
- E. switchport mode dynamic auto
- F. switchport trunk native vlan 3
- G. switchport trunk encapsulation dot1q

**Correct Answer:** AFG

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Entering the IOS commands switchport mode trunk and switchport trunk encapsulation dot1q in interface configuration mode will allow a switch port to actively negotiate to be an 802.1Q trunk port. Setting the trunk native VLAN to 3 with the command switchport trunk native vlan 3 will allow VLAN 3 traffic to be sent and received untagged over the trunk port.

The command switchport mode trunk instructs DTP to actively negotiate to be a trunk if the other side is set to trunk, desirable, or auto.

Use the following steps to configure a port as an 802.1Q trunk:

1. Enter the interface configuration.  
switch(config)# interface interface-id
2. Configure the port to using 802.1Q encapsulation.  
switch(config-if)# switchport trunk encapsulation dot1q
3. Configure the port as a trunk port.  
switch(config-if)# switchport mode trunk
4. (Optional) Set the native VLAN number.  
switchport trunk native vlan number

If the native VLAN is changed as above, it must be changed on both ends of the link. Failure to do so will cause the link to not be successfully built because the native VLAN numbers must match. When left to the default (VLAN 1) the issue takes care of itself. If a native VLAN mismatch occurs, it will be reflected in the debug command output of one of the switches, as shown below.

```
2009 Aug 11 16:36:11 %SPNTREE-2-RX_IQPVIDERR:Rcvd pvid_inc BPDU on 1Q port 0/2 vlan3
2009 Aug 11 16:36:11 %SPNTREE-2-TX_BLKPORTPVID:Block 0/2 on xmitting vlan 1 for inc peer vlan
2009 Aug 11 16:36:11 %SPNTREE-2-RX_BLKPORTPVID:Block 0/2 on rcving vlan 3 for inc peer vlan 1
```

Note: Trunking modes can be configured as access, dynamic desirable, dynamic auto, trunk, and nonegotiate. If both sides are set to auto, no negotiations will occur.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Product Support > Switches > Cisco Catalyst VST 2950 Series Switches > Configure > Configuration Examples and Technotes > Configuring EtherChannel and 802.1Q Trunking Between Catalyst L2 Fixed Configuration Switches and a Router (InterVLAN Routing)

Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport trunk

Cisco > Cisco IOS Interface and Hardware Component Command Reference > I through K > interface

#### QUESTION 161

You must add a new switch to the existing network using VTP to maintain the VLAN databases.

Which mode should be configured on this switch so that VLANs can be separately maintained on this switch?

- A. None
- B. Client
- C. Server
- D. Transparent

**Correct Answer:** D

**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

Adding a switch configured in VTP transparent mode allows the administrator to maintain the switch VLAN configuration information and not advertise its database to other switches in the network.

A VTP transparent mode switch will receive and forward VTP advertisements. The VTP transparent mode switch will not use the contents of the advertisement to synchronize with its own VLAN database.

VTP advertisements are flooded throughout the management domain every five minutes or whenever there is a change. These advertisements originate from a switch that is in server mode and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the domain name and password (if defined) against its own configuration. Next, the revision number is checked to see if it is higher than the last value stored in the receiving switch. If the revision number is higher, the receiving switch will overwrite its VLAN database with the information in the advertisement.

The VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM.

The VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANs/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

**QUESTION 162**

Which are valid configurable VLAN ID numbers for 802.1Q networks?

- A. 0-1005
- B. 1-4094
- C. 0-4095
- D. 1-1001

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

IEEE 802.1Q supports configuring VLAN IDs 1 through 4094.

The 802.1Q standard specifies support for a maximum of 4,094 VLANs. (IDs 0 and 4095 are reserved.) Therefore, ID values of 1-4094 are assignable. In contrast, the valid range of configurable ISL VLANs is 1-1001. The following is a summary of VLAN IDs:

0 and 4095: Reserved

1: Cisco default management

2-1001: Available for Ethernet VLANs

1002-1005: Defaults for FDDI and Token Ring VLANs

1006-4094: Extended range available for Ethernet VLANs (802.1Q only)

Recognizing the differences between supported VLAN ID ranges highlights several issues in constructing a network of both ISL and 802.1Q VLAN networks. Ethernet VLAN IDs above the supported ISL range must be mapped to IDs within the range supported by ISL. Among other limitations, you are limited to eight mappings. This process of mapping 802.1Q to ISL VLAN IDs will further restrict and define which IDs are available to be used.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Cisco Nexus 5000 Series Switch CLI Software Configuration Guide > Configuring Access and Trunk Interfaces

**QUESTION 163**

What command configures a port with a voice VLAN using 802.1Q?

- A. switch(config-if)# switchport voice vlan 10
- B. switch(config-if)# switchport voice vlan 10 q
- C. switch(config-if)# switchport voice vlan 10 802.1q
- D. switch(config-if)# switchport voice vlan 10 dot1p

**Correct Answer: A**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

The command that configures a port with a voice VLAN using 802.1Q is switchport voice vlan 10. This configuration uses 802.1Q as a default. 802.1P is configured with the command switchport voice vlan 10 dot1p . These are the only two valid commands to configure voice VLANs on a switch port.

The following is an example of voice VLAN configuration and QoS:

```
switch(config)# mls qos
```

```
switch(config)# interface fastethernet 0/10
switch(config-if)# switchport voice vlan 100
switch(config-if)# switchport access vlan 1
switch(config-if)# switchport priority extend trust
switch(config-if)# mls qos trust cos
switch(config-if)# mls qos trust device cisco-phone
```

In this example, the mls qos command enables QoS on the switch. The interface command moves the administrator into interface configuration mode. The switchport voice vlan 100 command configures the voice VLAN to be 100 using 802.1Q. If you wanted 802.1P, the command would have been switchport voice vlan 100 dot1p .

The VLAN for data traffic is defined with the fourth command, switchport access vlan 1 . The switchport priority extend trust command instructs the port to trust the CoS of the data traffic being passed from a PC connected to the IP phone. The mls qos trust cos command tells the port to use the CoS value of traffic passed to it from the phone or PC to classify traffic. (It is included here for illustration purposes only, as this command is not necessary when using the switchport priority extend trust command since the CoS value of the PC will be trusted anyway.) The mls qos trust device cisco-phone command tells the port to trust the QoS information provided from the IP phone if it is a Cisco phone.

The other options are incorrect due to invalid syntax.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Cisco > Catalyst 3750-E and 3560-E Switch Software Configuration Guide, 12.2(46)SE > Configuring Voice VLANs

Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport voice vlan

Cisco > Cisco IOS Quality of Service Solutions Command Reference > mls qos (global configuration mode) through mpls experimental > mls qos (interface configuration mode)

#### QUESTION 164

What commands can be used to verify the trunking configuration of a router performing inter-VLAN routing? (Choose all that apply. Each correct answer is a complete solution.)

- A. router# show trunk
- B. router# show vlans
- C. router# show vtp status
- D. router# show ip interface brief
- E. router# show ip route

**Correct Answer:** BE

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The command show vlans verifies the trunking configuration of a router performing inter-VLAN routing. This command will indicate what subinterfaces are associated with what VLANs, the trunking protocol being used, and the IP addresses that the router is using on each of the VLANs. Below is sample output of the show vlans command:

```
RouterA# show vlans
Virtual LAN ID: 2 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: Fa0/1.1
Protocols Configured: Address: Received: Transmitted:
IP 10.1.1.1 14 16
Virtual LAN ID: 3 (Inter Switch Link Encapsulation)
VLAN Trunk Interface: Fa0/1.2
Protocols Configured: Address: Received: Transmitted:
IP 10.2.2.1 13 19
```

The show ip route command can also be used to determine the correct configuration of inter-VLAN routing. If routing is configured correctly, there should be a route to each VLAN displayed in the output. If a route to a VLAN is missing, most likely the router is missing the command to assign an IP address to the VLAN in VLAN configuration mode. Below is output of the command on the same router as in the previous sample output, showing a route to both VLANs. If an IP address is not configured for a VLAN, a route to the VLAN will not be present.

```
RouterA# show ip route

Gateway of last resort is not set

10.0.0.0/8 is subnetted, 2 subnets

C 10.1.1.0 is directly connected, Fasthethernet0/1.1
C 10.2.2.0 is directly connected, Fasthethernet0/1.2
```

The command show trunk is not a valid command to issue on a router. Routers do not understand trunking in the same way switches do. Routers must be configured with a unique subinterface representing each VLAN, mimicking how the router normally connects different network with physical interfaces.

The command show ip interface brief is not used to verify trunking on a router. This command is useful in identifying IP addresses assigned to interfaces, and the state of the interfaces. No VLAN or trunking information is included in the output.

The command show vtp status is not a valid command on a router. The router does not use or understand VTP.

Objective:

Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > show vlans

#### QUESTION 165

With RSTP hello timers set to the default interval, how quickly can a non-edge port discover that its neighbor is down?

- A. 20 seconds
- B. 10 seconds
- C. 6 seconds
- D. 5 seconds

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

With Rapid Spanning Tree Protocol (RSTP) hello timers set at the default interval, a non-edge port can discover that its neighbor is down in 6 seconds. One of the advantages of RSTP over STP is quicker convergence when changes occur in the topology. After a non-edge port fails to receive three Bridge Protocol Data Units (BPDUs) from its neighbor, it will assume the neighbor to be down and will age out all information regarding the neighbor. Since hellos are sent at 2-second intervals in RSTP, it will take only 6 seconds for this to occur, as compared to 20 seconds for STP.

All other options are incorrect values for the default convergence time for RSTP.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Technology Information > Technology White Paper > Understanding Rapid Spanning Tree Protocol (802.1w)

#### QUESTION 166

Which IOS commands are entered in interface configuration mode to configure a switch port to unconditionally be an 802.1Q trunk port and not generate DTP packets? (Choose two.)

- A. trunk dot1q
- B. switchport trunk dot1q
- C. switchport nonegotiate
- D. switchport trunk allowed vlan
- E. switchport trunk encapsulation dot1q

**Correct Answer: CE**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

Entering the IOS commands switchport nonegotiate and switchport trunk encapsulation dot1q in interface configuration mode will only allow a switch port to be an 802.1Q trunk port. This disables the generation of dynamic trunking protocol (DTP) negotiation packets. Since DTP also negotiates encapsulation type, the encapsulation type must be identified (for example, dot1q).

Use the following steps to configure a port as an 802.1Q trunk:

1. Enter the interface configuration:  
switch(config)# interface interface-id
2. Configure the port to using 802.1Q encapsulation:  
switch(config-if)# switchport trunk encapsulation dot1q
3. Configure the port as a trunk port:  
switch(config-if)# switchport nonegotiate

Note: Trunking modes can be configured as trunk, dynamic auto, dynamic desirable, nonegotiate, and access.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport trunk  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > I through K > interface

#### QUESTION 167

In which VTP modes can you propagate VTP advertisements and create or delete local VLANs? (Choose two.)

- A. User
- B. Server
- C. Client
- D. Private



E. Transparent

**Correct Answer:** BE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

You can propagate VTP advertisements and create or delete local VLANs on a switch when it is in server mode or transparent mode.

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create or delete VLANs. You can create local VLANs in server and transparent VTP modes. However, VLANs created on a switch in transparent mode apply only to that switch, and information about these VLANs is not promulgated throughout the VTP domain.

VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM.

VTP transparent mode forwards VTP advertisements and saves the VLAN configuration in NVRAM. It does not synchronize VLAN configuration information. A switch in transparent mode can create, delete, and modify VLANs, but changes are not transmitted to other switches in the domain. Changes only affect the local switch.

VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers. A Catalyst switch can create, modify, and delete VLANs in server or transparent modes, but not in client mode.

VTP user mode and private mode do not exist.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)

**QUESTION 168**

Refer to the following partial output of the show spanning-tree command.

```
SW1# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0A61.0015.4D02
             Cost        19
             Port        1(FastEthernet0/2)
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0F2C.08A1.330E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/2        Root FWD 3         128.2    P2p
Fa0/3        Desg FWD 19        128.3    P2p
Fa0/5        Altn BLK 19        128.5    P2p

VLAN0121
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0F2C.08A1.330E
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0F2C.08A1.330E
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time  20

Interface    Role Sts Cost      Prio.Nbr Type
-----
Fa0/4        Desg FWD 19        128.4    P2p
Fa0/6        Desg FWD 19        128.6    P2p
```

Which of the following statements are TRUE for the given output? (Choose all that apply.)

- A. SW1 is the root bridge for VLAN0001
- B. Fa0/2 is the root port for VLAN0001
- C. The switch having the 0A61.0015.4D02 bridge ID is the root bridge for VLAN0001
- D. The switch having the 0F2C.08A1.330E bridge ID is the root bridge for VLAN0001
- E. The switch connected to the Fa0/6 port of SW1 is using its root port
- F. The port Fa0/4 is in a blocking state for VLAN 0121
- G. The STP protocol in use is RSTP

**Correct Answer:** BCE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

The following statements are correct about the given output:  
Fa0/2 is the root port for VLAN001  
The switch having the 0A61.0015.4D02 bridge ID is the root bridge for VLAN0001  
The switch connected to the Fa0/6 port of SW1 is using its root port

The value in the Role column in the output for VLAN0001 is Root for the Fa0/2 port of SW1. This implies that the Fa0/2 port is a root port. A root port is the port on a non-root bridge that has the least cost to reach the root bridge. Every non-root bridge must elect a root port. A root bridge does not have any root ports.

The output for VLAN0121 specifies Desg in the Role column for the Fa0/6 port of SW1. This implies that the Fa0/6 port is a designated port. This means that the switch on the other end is using its root port.

The switch having the 0A61.0015.4D02 bridge ID is the root bridge for VLAN0001. For VLAN0001, the bridge ID of the root and the local switch are different. The bridge ID of the local switch (SW1) is 0F2C.08A1.330E, while the bridge ID of the root bridge is 0A61.0015.4D02. The text Port 1 (FastEthernet0/2) in the Root ID section for VLAN0001 in the output indicates that the root bridge is connected to the Fa0/2 port of the local switch.

The options stating that SW1 is the root bridge for VLAN0001 and that the switch having the 0F2C.08A1.330E bridge ID is the root bridge for VLAN0001 are incorrect. The Bridge ID section in the output for VLAN0001 and VLAN0121 specifies the bridge ID of the local switch. In this case, the bridge ID of the local switch (SW1) is 0F2C.08A1.330E. SW1 is not the root bridge for VLAN0001; however, SW1 is the root bridge for VLAN0121.

You can determine if a local switch is the root bridge by any of the following:  
The text This bridge is the root appears in the Root ID section of the output for VLAN0121.  
The bridge IDs in the Root ID and Bridge ID sections of the output are the same.  
All the ports of the local switch are Desg (designated) ports and in forwarding state.

The port Fa0/4 is NOT in a blocking state for VLAN 0121. As indicated in the STS column for Fa0/4 under the section on VLAN 0121, it states that is in an FWD (forwarding) state.

The STP protocol in use is NOT Rapid Spanning Tree protocol (RSTP). If that were the case, the output would display Spanning tree enabled protocol rstp, rather than Spanning tree enabled protocol ieee. This indicates that IEEE 802.1d is in use.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco Press > Articles > Network Technology > General Networking > CCNP Exam Prep: Traditional Spanning Tree Protocol  
Cisco > Cisco IOS Bridging Command Reference > show spanning-tree

#### QUESTION 169

What is the approximate amount of time it takes for a PortFast-enabled port to transition from blocking to forwarding?

- A. Immediately
- B. 15 seconds
- C. 20 seconds
- D. 30 seconds
- E. 50 seconds

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Instead of waiting for STP to cycle through the blocking, learning, and listening states, PortFast will place the port in the forwarding state immediately.

When PortFast is enabled on a port, the attached end station can join the network almost immediately rather than waiting up to 50 seconds for spanning tree to converge. This feature is designed to enable the connections to workstations and servers to be put into the forwarding state as soon as possible after a spanning-tree reconvergence.

Bypassing the listening and learning states creates an exposure for spanning-tree loops. The default behavior of a PortFast-enabled port is to put the port immediately into a blocking state if a BPDU is received.

The following command enables PortFast:

```
switch(config-if)# spanning-tree portfast
```

You should only enable PortFast on a port that connects an end station. Enabling PortFast on a port that connects another switch could create a loop.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE > Configuring Optional Spanning-Tree Features > Understanding Port Fast

#### QUESTION 170

By default, which VLAN is the Cisco management VLAN?

- A. 1
- B. 0
- C. 1001
- D. 1005

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**

Explanation:

Cisco uses VLAN1 as the default management VLAN.

All ports are automatically assigned to VLAN1. Cisco Discovery Protocol (CDP) and VLAN Trunking Protocol (VTP) advertisements are transmitted on VLAN1. VLAN1 is the management VLAN and is used for administration. It cannot be deleted or pruned from a trunk line.

VLAN IDs that are implemented can vary based on whether the trunk implementation is Cisco's Inter-Switch Link (ISL) or the IEEE 802.1Q standard.

The following is a summary of the VLAN IDs:

0 and 4095 - Reserved

1 - Cisco default management

2-1001 - Available for Ethernet VLANs

1002-1005 - Defaults for FDDI and Token Ring VLANs

1006-4094 - Extended range available for Ethernet VLANs (802.1Q only)

Objective:

Layer 2 Technologies

Sub-Objective:

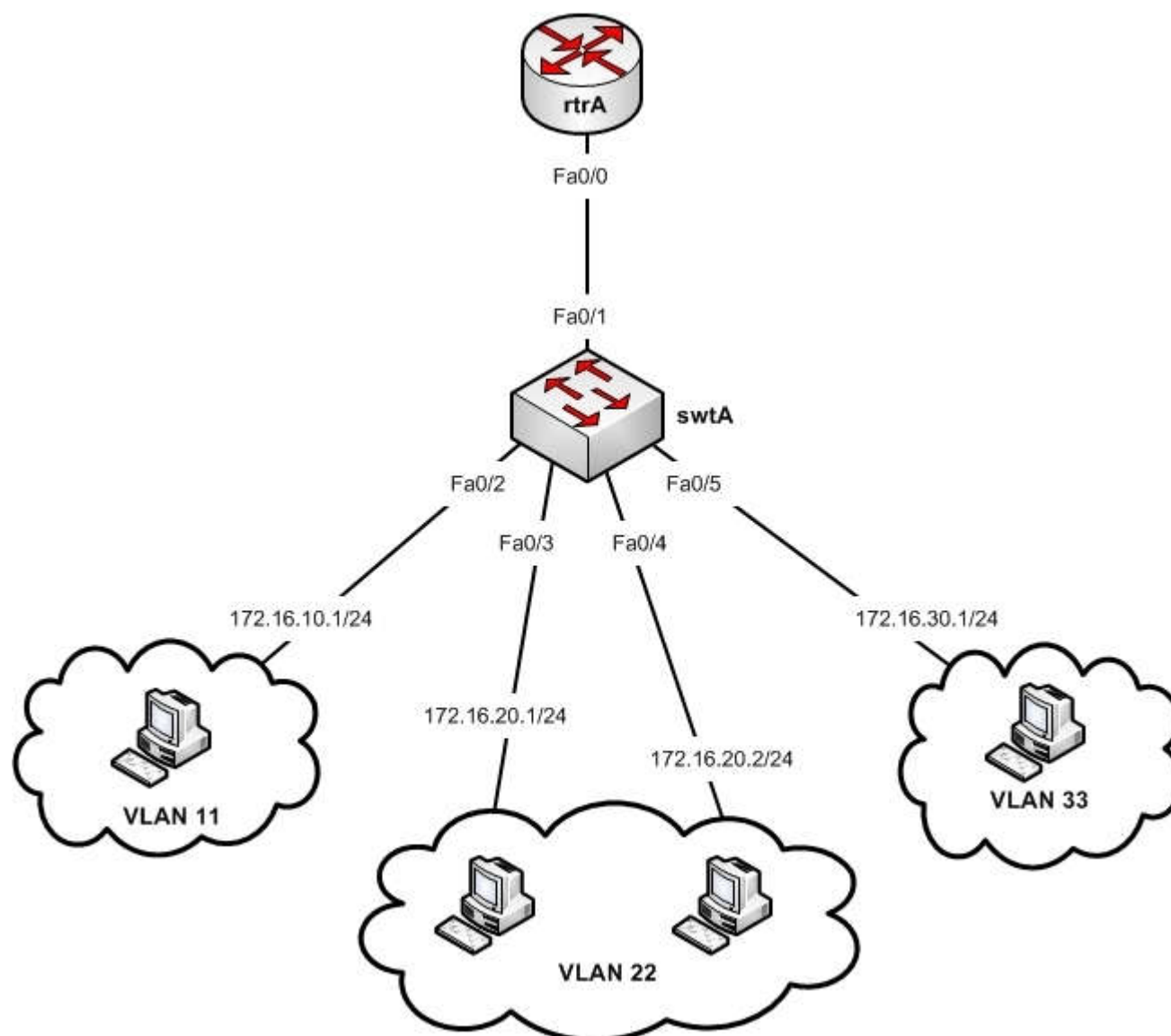
Configure and verify VLANs

References:

Cisco > Support > Technology Support > LAN Switching > Layer-Three Switching and Forwarding > Configure > Configuration Examples and Technotes > How To Configure InterVLAN Routing on Layer 3 Switches

**QUESTION 171**

Refer to the following network diagram:



You executed the following commands on the swtA switch:

```

swtA(config)#vlan 11
swtA(config-vlan)#name Sales
swtA(config-vlan)#exit
swtA(config)#vlan 22
swtA(config-vlan)#name Administration
swtA(config-vlan)#exit
swtA(config)#vlan 33
swtA(config-vlan)#name Accounts
swtA(config-vlan)#exit
swtA(config)#interface fa0/1
swtA(config-if)#switchport trunk encapsulation dot1q
swtA(config-if)#switchport mode trunk
swtA(config-if)#switchport trunk allowed vlan 11,22,33
swtA(config)#interface fa0/2
swtA(config-if)#switchport mode access
swtA(config-if)#switchport access vlan 11
swtA(config)# interface fa0/3
swtA(config-if)# switchport mode access
swtA(config-if)# switchport access vlan 22
swtA(config)# interface fa0/4
swtA(config-if)# switchport mode access
swtA(config-if)# switchport access vlan 22
swtA(config)# interface fa0/5
swtA(config-if)# switchport mode access
swtA(config-if)# switchport access vlan 33

```

You executed the following commands on the rtrA switch:

```

rtrA(config)# interface fa0/0
rtrA(config-if)# no shutdown
rtrA(config)# interface fa0/0.1
rtrA(config-subif)# encapsulation dot1q 11
rtrA(config-subif)# ip address 172.16.10.2 255.255.255.0
rtrA(config-subif)# no shutdown
rtrA(config)# interface fa0/0.2
rtrA(config-subif)# ip address 172.16.20.3 255.255.255.0
rtrA(config-subif)# no shutdown
rtrA(config)# interface fa0/0.3
rtrA(config-subif)# encapsulation dot1q 33
rtrA(config-subif)# ip address 172.16.30.2 255.255.255.0
rtrA(config-subif)# no shutdown

```

Which of the following VLANs do(es) NOT participate in inter-VLAN routing through the rtrA router?

- A. VLAN 11 only
- B. VLAN 22 only
- C. VLAN 33 only
- D. VLAN 11 and VLAN 22
- E. VLAN 22 and VLAN 33
- F. VLAN 33 and VLAN 11

**Correct Answer: B**

**Section: Layer 2 Technologies**

**Explanation**

**Explanation/Reference:**

Explanation:

VLAN 22 is the only VLAN that does not participate in inter-VLAN routing through the rtrA router. The given network diagram and the commands reflect a router-on-a-stick (RoaS) configuration. In a RoaS configuration, inter-VLAN routing is achieved in two steps.

The first step sets up the switch:

- Configure the switch
- Configure the required VLANs
- Configure the switch port connecting to the router interface as a trunk port
- Enable dot1q or ISL encapsulation on the trunk port
- Configure the switch ports connecting to the VLANs as access ports
- Assign the access switch ports to respective VLANs

The second step sets up the router:

- Configure the router
- Enable the router interface connected to the trunk switch port
- Create separate subinterfaces on the trunk router interface for each VLAN
- Enable dot1q or ISL encapsulation on the subinterfaces
- Assign IP addresses to each subinterface in the same subnet as the VLAN of which the interface will be a member. Consequently, this address will become the default gateway for each host in that VLAN.

In the scenario, the subinterface created for VLAN 22 is not configured for inter-VLAN routing because the encapsulation command is missing. Without this command, the encapsulation type and the VLAN ID remain

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Home > Support > Configuring InterVLAN Routing > Configuring InterVLAN Routing on an External Cisco Router > Configuring IP InterVLAN Routing on an External Router

Home > Support > Configuring InterVLAN Routing > InterVLAN Routing Configuration Examples > InterVLAN Routing with an External Cisco 7505 Router Example



**QUESTION 172**

Which of the following capabilities does a multilayer switch possess that an Access layer switch does not? (Choose all that apply.)

- A. the ability to make forwarding decisions based on MAC addresses
- B. the ability to make forwarding decisions based on host names
- C. the ability to make forwarding decisions based on IP addresses
- D. the ability to make forwarding decisions based on UDP/TCP port numbers
- E. the ability to make forwarding decisions based on NetBIOS names

**Correct Answer:** CD

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Multilayer switches are capable of making forwarding decisions based on IP addresses and UDP/TCP port numbers, while Access layer switches are not. The term multilayer describes the ability of the multilayer switch to utilize information that exists on more than one layer of the TCP model for forwarding decisions. This device combines the functionality of a switch and a router. Additionally, it possesses the ability to do something that neither a switch or router alone: perform Fast Switching, a process whereby the device can route the first packet in a traffic flow and then use hardware switching for the remaining packets in the flow. This process of routing once, switching many, results in less routing (a slower process) and more switching (a faster process), with a net result of speeding traffic flow.

Multilayer switches usually operate in the Distribution and Core layers of the Cisco Enterprise Composite model. There are important considerations for each layer:

Access layer - This is the layer where end-user stations should connect. It consists of Access layer or Layer 2 switches. VLANs, QoS, and protocol filtering operate at this layer.

Distribution layer - This is the layer where routing is performed and where access lists are enforced. Devices in this layer operate in Layer 3 of the OSI model.

Core layer - High-speed backbone switches exist on this layer. It should be designed with a low number of Layer 3 peers, switches that can efficiently forward traffic even when every uplink is at 100% capacity and the switches should have many high-speed ports.

When migrating to the Cisco Enterprise Composite model from earlier models, keep the following practices in mind:

Add redundancy between the hierarchical layers

Identify groups of end users as switch blocks

Group common resources into switch blocks

Multilayer switches are also capable of making forwarding decisions based on MAC addresses, but access layer switches can do this as well.

Neither multilayer switches nor Access layer switches can make forwarding decisions based on host names or NetBIOS names. This function is performed by Domain Name Servers (DNS) and Windows Internet Naming (WINS), servers respectively.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify switch administration

References:

Cisco > Home > Support > Configuring IP MLS

**QUESTION 173**

When provisioning bandwidth for an IP telephony network, which elements are unique to an IP telephony call? (Choose two.)

- A. voice stream
- B. IGMP packets
- C. call-control signaling
- D. routing protocol packets
- E. speed of the segment to the telephone

**Correct Answer:** AC

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Bandwidth provisioning for an IP telephony call consists of the voice stream traffic and the call control traffic. These elements are unique to an IP telephony call.

The network infrastructure should be examined to see if the required bandwidth exists to support the voice and call-control applications. The sum of the bandwidth necessary for each major application, including voice, video, and data, should not exceed 75% of the total available bandwidth for each link. Voice traffic can be characterized as:

Smooth

Benign

Drop sensitive

Delay sensitive

Voice packets are typically around 60 to 120 bytes in size. For good voice quality, packet loss should be less than 1 percent and delay should be no more than 150 ms.

The IP telephony voice call-control procedures also generate traffic. The call control procedures are in the areas of call setup, maintenance, redirect, and tear down. There are special protocols such as H.323 and Media Gateway Control Protocol (MGCP) that handle these procedures.

Voice applications are delay-sensitive. Speech is sampled by voice processors referred to as a codec (coder/decoder). Then the digitized voice-sample outputs of the codecs are sent into the network towards the receiver at regular intervals in real-time transport protocol (RTP) packets. If these packets containing the voice samples are delayed for any reason behind other data traffic, the quality of the voice conversation suffers.

The transportation of these voice applications in RTP packets through the IP network handled by H.323 protocols and devices is referred to as Voice over IP (or VoIP for short).

The following are other network and design considerations besides bandwidth relating to IP telephony infrastructure support:

Determine if the cabling plant can support the IP telephony equipment.  
Determine if the switch hardware can supply power to attached IP telephony equipment or if additional hardware is required.  
Ensure that infrastructure supports priority end-to-end VLANs and QoS networking.

Internet Group Management Protocol (IGMP) is used for managing the membership of IP multicast groups and is not an element unique to an IP telephony call.

Routing protocol packets (RIP, OSPF, and EIGRP) are used by routers to share routing information, and are not elements unique to an IP telephony call.

The speed of the segment to the telephone is important to VoIP, but that is not an element unique to an IP telephony call.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:  
Cisco > Support > Technology Support > Voice > Telephony Signaling

#### QUESTION 174

What occurs when an untagged frame is received by an 802.1Q trunk port?

- A. It discards the frame.
- B. It tags the frame with the identified native VLAN value.
- C. It forwards the frame out each port of the switch not assigned to a VLAN.
- D. It forwards the frame to a port belonging to the same VLAN as the native VLAN.

**Correct Answer: D**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

IEEE 802.1Q supports configuring native VLANs. A native VLAN is the VLAN a port is in when not in trunking mode. Native VLAN packets are sent untagged. If an 802.1Q trunk receives an untagged frame, it will forward that frame to a port that belongs to the same VLAN as the identified native VLAN. The frame is treated as if it were tagged with the same VLAN ID as the native VLAN. Frames received through ports having the same membership as the identified native VLAN of the trunk will be forwarded untagged out of the trunk.

It is important that the native VLAN settings on each end of an 802.1Q trunk match.

The 802.1Q standard specifies support for a maximum 4094 VLANs (IDs 0 and 4095 are reserved). Therefore, ID values of 1-4094 are assignable. In contrast, the valid range of configurable ISL VLANs is 1-1001. The following is a summary of VLAN IDs:

0 and 4095: Reserved  
1: Cisco default management  
2-1001: Available for Ethernet VLANs  
1002-1005: Defaults for FDDI and Token Ring VLANs  
1006-4094: Extended range available for Ethernet VLANs (802.1Q only)

Recognizing the difference in supported VLAN ID ranges highlights several issues in constructing a network of both ISL and 802.1Q VLAN networks. Ethernet VLAN IDs above the supported ISL range must be mapped to IDs within the range supported by ISL. Among other limitations, you are limited to eight total mappings. This process of mapping 802.1Q to ISL VLAN IDs will further restrict and define what IDs are actually available to be used.

Untagged frames are not discarded, but are sent to the native VLAN.

Untagged frames are not tagged with the tag of the native VLAN. They are simply forwarded to that VLAN. No packets in the native VLAN have tags.

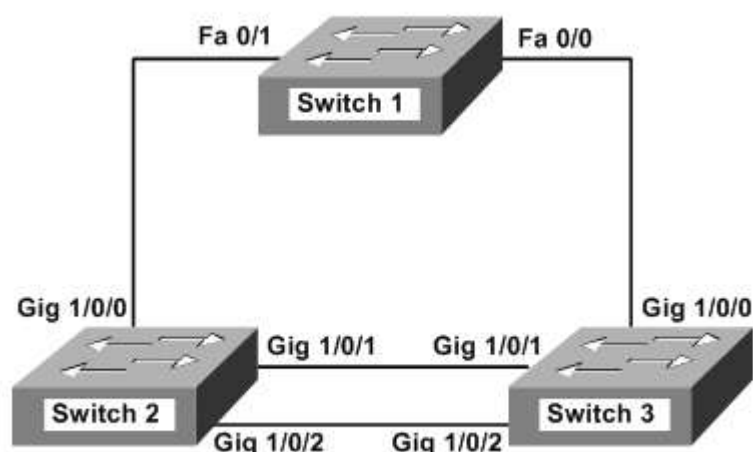
Untagged frames are not forwarded out all ports not assigned to a VLAN. It will only be forwarded to the switchport where the destination MAC address resides.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco Nexus 5000 Series Switch CLI Software Configuration Guide > Configuring Access and Trunk Interfaces  
Cisco Press > Articles > Determining IP Routes

#### QUESTION 175

You have three switches connected as shown in the diagram below: S1, S2, and S3.



You instructed your assistant to configure the switches so that the following requirements would be met:

Switch 1 should be the root bridge for VLAN A

VLAN C should forward over the Gig 1/0/1 link between Switch 2 and Switch 3

VLAN B should forward over the Gig 1/0/2 link between Switch 2 and Switch 3

However, after your assistant performs the configuration, you discover that:

Switch 2 is the root bridge for VLAN A

VLAN C is forwarding over the Gig 1/0/2 link between Switch 2 and Switch 3

VLAN B is forwarding over the Gig 1/0/1 link between Switch 2 and Switch 3

When you execute the show spanning tree command on Switch 2, you determine that all link costs and priorities are set at the defaults.

Which of the following actions performed on Switch 2 would enable the desired configuration? (Choose three.)

- A. switch2(config)# spanning-tree vlan a priority 61440
- B. switch2(config)# spanning-tree vlan a priority 1
- C. switch2(config)# int G1/0/2switch2(config-if)# spanning-tree vlan b cost 1
- D. switch2(config)# int G1/0/2switch2(config-if)# spanning-tree vlan b cost 19
- E. switch2(config)# int G1/0/1switch2(config-if)# spanning-tree vlan c port-priority 64
- F. switch2(config)# int G1/0/1switch2(config-if)# spanning-tree vlan c port-priority 128

**Correct Answer:** ACE

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The commands that will achieve the desired results are:

```
switch2(config)# spanning-tree vlan a priority 61440
switch2(config)# interface G1/0/2
switch2(config-if)# spanning-tree vlan b cost 1
switch2(config)# interface G1/0/1
switch2(config-if)# spanning-tree vlan c port-priority 64
```

The first command raises the bridge priority for Switch 2 with respect to VLAN A, which will cause Switch 1 to be the root bridge for VLAN A. By default, the bridge priorities for Switch 2 and Switch 3 will set to 32769.

The second command will lower the cost of G1/0/2 with respect to VLAN B. Since the cost for G1/0/1 is the default cost of 4, this will cause interface G1/0/2 to become the root port for VLAN B, which will in turn cause it to forward instead of block for VLAN B.

The third command will lower the port priority for G1/0/1 with respect to VLAN C. Since the port priority of G1/0/2 will remain set at the default of 128, this will result in switching the ports that are blocking and forwarding. The end result will be that VLAN C will start forwarding over the Gig 1/0/1 link between Switch 2 and Switch 3.

The other commands will have no effect because they change the cost and port priority to the defaults, which are how the links are currently set.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify spanning tree

References:

Cisco IOS LAN Switching Configuration Guide, Release 12.4 > EtherSwitch Network Module > Configuring Spanning Tree on a VLAN > VLAN Root Bridge and VLAN Bridge Priority

#### QUESTION 176

You have executed the following set of commands on a Layer 3 switch:

```
switchA(config)# ip routing
switchA(config)# vlan 5
switchA(config-vlan)# name Finance
switchA(config-vlan)# exit
switchA(config)# interface Fa0/1
switchA(config-if)# no switchport
switchA(config-if)# ip address 10.55.5.1 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 5
switchA(config-if)# no shutdown
switchA(config-if)# interface Fa0/2
switchA(config-if)# ip address 10.55.5.1 255.255.255.0
switchA(config-if)# switchport mode trunk
switchA(config-if)# switchport trunk encapsulation dot1q
switchA(config-if)# no shutdown
switchA(config-if)# exit
switchA(config)# interface vlan 5
switchA(config-if)# ip address 10.33.3.1 255.255.255.0
switchA(config-if)# no shutdown
```

You have verified that the configuration on all the physical and logical interfaces is correct. All the Layer 2 interfaces configured on the switch are in the up/up state.

What is the state of the VLAN and the line protocol when you execute the show interfaces vlan 5 command?

- A. administratively down/down
- B. down/down
- C. up/up
- D. up/down

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

The VLAN and the line protocol are in the up/up state when you execute the show interfaces vlan 5 command. You can view the state of the VLAN and the line protocol using the show interfaces vlan command, which is as follows:

```
switchA# show interfaces vlan 5
Vlan5 is up, line protocol is up
Hardware is Ethernet SVI, address is 031B.70A2.166F (bia 031B.70A2.166F)
Internet address is 10.33.3.1/24
<output omitted>
```

As you can see in the given output, the text Vlan5 is up, line protocol is up indicates that VLAN 5 and the Layer 2 line protocol both are in the up state. Both the VLAN and line protocol are in the up/up state if the following conditions are true:

The VLAN is configured on the switch and is enabled in the VLAN database

The VLAN is not in the administratively down state

The VLAN has at least one Layer 2 (access or trunk) port in the up state

The VLAN and the line protocol will not be in the administratively down/down state. An interface is in the administratively down state only when the shutdown command is used on that interface. In this case, the no shutdown command is used on the VLAN 5 interface, not the shutdown command. The no shutdown command enables the VLAN 5 interface.

The VLAN and the line protocol will not be in the down/down state. An interface is in the down state when there is some Layer 1, Layer 2, or Layer 3 problem such as incorrect cabling used or an incorrect IP address assigned. Interfaces can also be in the down state if the either of the interfaces at the end of a link is in down state due to erroneous configuration. However, in this case, the configuration is correct and the VLAN 5 is in the up state because of the no shutdown command.

The VLAN and the line protocol will not be in the up/down state. An interface is in the down state when there are some Layer 1, Layer 2, or Layer 3 problems such as incorrect cabling used or an incorrect IP address assigned. In Layer 3 switches, line protocol will be in the down state if all of the Layer 2 ports in the VLAN are in the down state. In this case, the configuration is correct and all the ports in VLAN 5 are in the up state. This implies that the line protocol cannot be in the down state.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring Layer 3 Interface > Configuring VLANs as Layer 3 Interfaces  
Home > Articles > Network Technology > Routing & Switching > Cisco LAN Switching Fundamentals: Configuring Switches > Configuring the Access Layer  
Home > Support > Technology Support > LAN Switching > Layer-Three Switching and Forwarding > Configure > Configuration Examples and Technotes > How to Configure InterVLAN Routing on Layer 3 Switches > Configure InterVLAN Routing

**QUESTION 177**

Which feature can you enable on a switch to prevent potential bridging loops caused by invalid configurations on PortFast-configured interfaces?

- A. UDLD
- B. Root Guard
- C. BPDU Guard
- D. Loop Guard

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**

Explanation:

BPDU Guard prevents bridging loops caused by an invalid configuration on a PortFast-configured interface by shutting down the interface when it receives BPDUs.

PortFast-configured interfaces should not receive BPDUs in a valid configuration because only end devices should be connected to the PortFast interfaces (only switches and bridges send BPDUs). However, if a switch were improperly connected to the PortFast-configured interface, it would begin to receive BPDUs from the switch at the other end of the link. The port would immediately go into the spanning-tree blocking state and the port would begin to send BPDUs, which could cause a bridging loop. BPDU Guard can prevent this situation by providing a secure response to BPDUs received on PortFast-configured interfaces. When enabled, BPDU Guard shuts down a PortFast-configured interface when it receives BPDUs. When BPDU Guard brings down an interface, the interface stays down until an administrator manually puts it back into service.

The following command enables BPDU Guard on an interface:

```
switch(config-if)# spanning-tree portfast bpduguard
```

To further enhance the ability of Root Guard to prevent the introduction of rogue switches in the network, PortFast can be used as well to shut down the port when a switch is connected to it. When you globally enable BPDU guard, STP shuts down ports that receive BPDUs. This is called STP PortFast BPDU Guard.

The following command enables STP PortFast BPDU Guard globally.

```
switch(config)# spanning-tree portfast bpduguard default
```

Unidirectional Link Detection (UDLD) improves the stability of Layer 2 networks by detecting and shutting down unidirectional links.

Root Guard provides a mechanism for enforcing root-bridge placement in the network. When enabled on a Layer 2 access port, it forces the port to become a designated port. Root Guard prevents the port from becoming an STP root port.

Loop Guard provides protection against Layer 2 forwarding loops in a physically redundant topology by moving a non-designated port that has not received



BPDUs as expected into the STP loop-inconsistent blocking state, preventing the port from cycling through the normal STP listening, learning, and forwarding states. It cannot be used to force a Layer 2 access port to become a designated port. Loop guard can be implemented on a switch either globally or per interface with the following commands.

Globally, the command would be:

```
switch(config)# spanning-tree loopguard default
```

Per interface, the commands would be:

```
switch(config)# interface fastethernet0/1
switch(config-if)# spanning-tree guard loop
```

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify spanning tree

References:

Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > spanning-tree portfast bpduguard default

#### QUESTION 178

Which parameters in VTP advertisements are checked before being accepted and processed? (Choose three.)

- A. VLAN ID
- B. Password
- C. VTP mode
- D. Switch name
- E. Revision number
- F. Management domain name

**Correct Answer:** BEF

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The management domain name, password, and revision number are all checked before the VTP frame is processed.

VTP advertisements are flooded throughout the management domain every five minutes or whenever there is a change. These advertisements are originated from a switch that is in server mode and are propagated by switches that are in either client or transparent mode. Before a client or another server accepts or incorporates the information sent in the advertisement, it checks the management domain name and password (if defined) against its own configuration. The revision number is then checked. If the revision number is higher than the last value stored in the receiving switch, the receiving switch will overwrite its VLAN database with the information in the advertisement.

A VTP switch in transparent mode will receive and forward VTP advertisements. It will not use the contents of the advertisement to synchronize with its own VLAN database.

To set the VTP mode of a switch execute the following command at the global prompt. All switches are set to server mode by default; therefore, the command is only necessary to set a switch to client or transparent mode. The command syntax is:

```
switch(config)# vtp mode {transparent | client}
```

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Configure > Configuration Examples and Technotes > All Transparent VTP Domain to Server-Client VTP Domain Migration Configuration Example  
Cisco > Cisco IOS LAN Switching Command Reference > udd through vtp v2-mode > vtp

#### QUESTION 179

At which OSI layer does STP operate?

- A. Physical
- B. Network
- C. Transport
- D. Data Link

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

Spanning Tree Protocol (STP) operates at the Data Link layer (Layer 2) of the OSI model.

Switches and bridges running the spanning-tree algorithm communicate by exchanging multicast messages called bridge protocol data units (BPDUs) at regular intervals. BPDUs are used to build and maintain the spanning tree, ensuring a stable loop-free topology.

BPDUs exchange facilitates the following:

Election of a root switch (only one per spanning tree)

Election of a designated switch for each switched segment

Removal of loops by placing redundant switch ports in a backup (non-forwarding) state

STP is implemented on bridges and switches in order to prevent loops in the network. STP should be used in situations where redundant links are used.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Spanning Tree Protocol > Configure > Configuration Examples and Technotes > Spanning Tree Protocol > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches  
Cisco > Support > Configuring Spanning Tree Protocol > How STP Works

#### QUESTION 180

Which IOS command configures a switch for VTP client mode?

- A. vtp mode client
- B. no vtp v2-mode
- C. no vtp mode
- D. vtp terminal

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

To configure a switch to operate as a VLAN Trunk Protocol (VTP) client, simply enter the vtp mode client command at the global configuration prompt:

```
switch(config)# vtp mode client
```

When a switch is in VTP client mode, you cannot change its VLAN configuration. The switch will receive VTP updates from a VTP server in the VTP domain and then modify its configuration accordingly.

For added security, you can specify the VTP domain to which the client belongs and a password used to connect to the domain when configuring a switch for VTP client mode. The password is the same for all devices in the VTP domain. The commands to configure a VTP password are as follows:

```
switch(config)# vtp domain domain-name  
switch(config)# vtp password password
```

The no vtp v2-mode command reverts the VTP version to version 1 (the default version). Use the vtp v2-mode command to set the VTP mode to version 2.

The no vtp mode command reverts the VTP mode back to its default state, which is server mode. To set the VTP mode of a VTP client back to server mode, you can use either the no vtp mode command or the vtp server command.

vtp terminal is not a valid command.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)  
Cisco > Cisco IOS LAN Switching Command Reference > udd through vtp v2-mode > vtp

#### QUESTION 181

Which IOS commands do you enter in interface configuration mode to configure a switch port to actively negotiate to be an ISL trunk port if possible? (Choose two.)

- A. switchport trunk isl
- B. switchport mode dynamic auto
- C. switchport trunk allowed vlan
- D. switchport mode dynamic desirable
- E. switchport trunk encapsulation isl

**Correct Answer:** DE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Entering the IOS commands switchport mode dynamic desirable and switchport trunk encapsulation isl in interface configuration mode will allow a switch port to actively negotiate to be an ISL trunk port if possible.

Use the following steps to configure a port as an ISL trunk:

1. Enter the interface configuration.  
switch(config)# interface interface-id
2. Configure the port to use ISL encapsulation.  
switch(config-if)# switchport trunk encapsulation isl
3. Configure the port as a trunk port.  
switch(config-if)# switchport mode dynamic desirable

Note: Trunking modes can be configured as trunk, dynamic auto, dynamic desirable, nonegotiate, and access.

This allows DTP to actively negotiate to be a trunk if the other side is set to trunk, desirable , or auto. If one side is set to auto and the other side is also set to auto, no negotiations will occur.

The switchport allowed vlan command is also valid for configuring dot1q trunks, but is not required. By default, all VLANs are allowed on the trunk.

The other commands use incorrect syntax.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > squelch through system jumbomtu > switchport trunk  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > I through K > interface

#### QUESTION 182

Which IOS command sets the native VLAN to VLAN3?

- A. switchport mode trunk 3
- B. switchport native vlan 3
- C. switchport trunk native vlan 3
- D. switchport trunk allowed vlan 3
- E. switchport default native vlan 3

**Correct Answer: C**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The IOS command switchport trunk native vlan 3 sets the native VLAN to VLAN3.

Use the following command to configure the native VLAN on an 802.1Q trunk:

```
switch(config-if)# switchport trunk native vlan vlan_id
```

The 802.1Q native VLAN is the VLAN from which or to which Layer 2 frames are transmitted untagged on the 802.1Q trunk port. The default native VLAN on an 802.1Q is VLAN 1. The native VLAN IDs should be set to the same value for both sides of an 802.1Q trunk.

The command switchport trunk allowed vlan 3 is used to assign VLANs whose frames are allowed to be passed over the trunk.

The other options are incorrect due to invalid syntax.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport trunk

#### QUESTION 183

What command is used to enable CEF on a Cisco switch?

- A. ip cef
- B. ip cef distributed
- C. ip route-cache cef
- D. ip cef enable

**Correct Answer: A**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command to enable Cisco Express Forwarding (CEF) on a Cisco switch is ip cef. This enables CEF support on the entire switch. All interfaces that are configured to use CEF will be able to. The no form of this command will disable CEF support, including support on interfaces that have CEF configured on them.

Cisco Express Forwarding allows a Layer 3 switch to determine the next-hop destination MAC address of the first frame in a transmission made of many frames, and then utilizes the much faster switching process for all the remaining frames. This requires that routing be enabled on the switch, since the route to the initial frame must be determined.

The output of the show ip interface vlan id command can be used to determine whether IP routing is enabled. Partial output of the show ip interface vlan id command for two switches is shown below. The first (Switch A) has IP routing enabled and the second (Switch B) does NOT have IP routing enabled. The second switch is missing the section about CEF, since CEF cannot be enabled unless IP routing is enabled.

```
Switcha# show ip interface vlan 2<output omitted>IP flow switching is disabledIP CEF switching is enabled
IP CEF Fast Switching turbo vector
IP multicast fast switching is enabled

Switchb# show ip interface vlan 2
<output omitted>
IP flow switching is disabled
IP multicast fast switching is enabled
```

The command ip cef distributed is used to enable distributed CEF (dCEF), not the CEF mentioned in the scenario.

The command ip route-cache cef is a valid command to enable CEF on an individual interface, but the command is only valid in interface configuration mode.

The command `ip cef enable` is an invalid command due to incorrect syntax.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Cisco > Cisco IOS IP Switching Command Reference > `ip cef`

#### QUESTION 184

What feature allows the administrator to put phones into a separate logical network from the data network while keeping both in the same physical network?

- A. auxiliary VLANs
- B. queuing
- C. 802.1Q
- D. marking

**Correct Answer:** A  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Auxiliary VLANs allows the data and voice traffic to use the same physical topology but remain logically separate. The information the phones need regarding this voice VLAN is provided by the switch. Auxiliary VLANs allows IP phones to be automatically placed into a separate VLAN from data traffic.

Queuing is the process of placing traffic in appropriate queues depending on the class of traffic.

Marking is the process of setting the CoS, IP precedence, or DSCP of a packet to a specific value that will provide appropriate QoS throughout the network.

802.1Q is a trunking protocol used to allow traffic from multiple VLANs to pass through a single link and still be logically separate.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify VLANs

References:  
Cisco > Catalyst 4500 Series Software Configuration Guide, 8.1 > Configuring VLANs > Configuring Auxiliary VLANs

#### QUESTION 185

Which port will the spanning-tree algorithm select as a bridge's root port?

- A. The first port on the root bridge to receive an STP packet
- B. The port through which the root bridge can be reached with the lowest-cost path
- C. The port through which the root bridge can be reached with the lowest-value interface identifier
- D. The port through which the root bridge can be reached with the highest-value interface identifier

**Correct Answer:** B  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Root ports are ports that are in the forwarding state and provide connectivity to the root bridge. The port through which the root bridge can be reached with the lowest-cost path is the root port. All the ports on the root bridge (the bridge with the lowest bridge ID) are in the forwarding state and are referred to as designated ports.

Bridges and switches use the Spanning-Tree Protocol (STP) to prevent network loops. Without a loop-avoidance service on the network, Layer 2 devices, in certain situations, will endlessly flood broadcasts. An STP-enabled device recognizes a loop in the topology and blocks one or more redundant paths, preventing the loop. STP allows the switches to continually explore the network so that the loss or addition of a switch or bridge is also quickly discovered. STP is enabled by default on Catalyst switches.

For example, if two switches have an active connection between them that is forwarding traffic and a second link is connected between the same two switches, one of the two switch ports will go into a blocking state when BPDUs are received on the link. This helps to ensure that a loop does not form using the redundant connections. In some situations, heavy traffic may prevent the reception of BPDUs when the second link is put in place, and in that case, a loop may still form.

The root port is not selected based on the first port to receive an STP packet on the root bridge. Neither is it based on the lowest or highest interface identifier values.

Note: In some situations, there may be two ports with equal cost to the root bridge. When this occurs, the port with the lowest port number becomes the root port.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring STP and IEEE 802.1s MST > Creating the Spanning Tree Topology  
Cisco > Support > Configuring Spanning Tree Protocol > How STP Works

#### QUESTION 186

Consider the following output from the `show interfaces trunk` command:



```
Port Mode Encapsulation Status Native VLAN
gi0/1 desirable isl trunking 1
```

```
Port Vlans allowed on trunk
gi0/1 1-43,45-4094
```

```
Port Vlans allowed and active in management domain
gi0/1 1-17,40,43,101-172
```

```
Port Vlans in spanning tree forwarding state and not pruned
gi0/1 1-12,16,40,101-172
```

Which two of the following statements can be confirmed regarding the trunking configuration on the switch? (Choose two.)

- A. VLAN 44 is allowed on the trunk.
- B. VLAN 46 is not allowed on the trunk.
- C. VLAN 45 is configured for the VTP domain.
- D. VLAN 41 is not configured for the VTP domain.
- E. VLAN 43 is pruned or is not in the spanning-tree forwarding state.
- F. VLAN 41 is not pruned.

**Correct Answer:** DE  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Virtual local area network (VLAN) 41 is not configured for the VLAN Trunking Protocol (VTP) domain, and VLAN 43 is pruned or is not in the spanning-tree forwarding state. The show interfaces trunk command can be used to determine which VLANs are allowed, which VLANs are configured for the VTP domain, and which VLANs are in the spanning-tree forwarding state and are not pruned.

The VLANs listed under the Vlans allowed on trunk section are allowed on the trunk. Therefore, VLANs 1 through 43 and 45 through 4094 are allowed on the trunk. VLAN 44 is not allowed on the trunk; VLAN 46 is allowed on the trunk.

The VLANs listed under the Vlans allowed and active in management domain section are allowed on the trunk and configured for the VTP domain. In this scenario, this section includes VLANs 1 through 17, VLAN 40, VLAN 43, and VLANs 101 through 172. Because VLANs 41 and 45 are allowed on the trunk, but are not listed under the Vlans allowed and active in management domain section, VLANs 41 and 45 must not be configured for the VTP domain. VLANs 18 through 43, VLANs 45 through 100, and VLANs 173 through 4094 are not configured for the VTP domain.

VLANs 1 through 12, VLAN 16, VLAN 40, and VLANs 101 through 172 are listed under the Vlans in spanning tree forwarding state and not pruned section. Because VLAN 43 is allowed and is in the spanning-tree forwarding state, but is not listed under the Vlans in spanning tree forwarding state and not pruned section, VLAN 43 must be pruned or must not be in the spanning-tree forwarding state. This is also true of VLANs 13 through 15 and VLAN 17. As stated previously, VLAN 41 is allowed on the trunk but is not configured for the VTP domain. Therefore, it cannot be confirmed whether VLAN 41 has or has not been pruned manually. If VLAN 41 were in the spanning-tree forwarding state, but were not listed under the Vlans in spanning tree forwarding state and not pruned section, then it could be confirmed that VLAN 41 were being pruned.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify trunking

References:  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > show hw-module slot tech-support through show interfaces vgl-anylan > show interfaces trunk

#### QUESTION 187

What protocol allows for centralized management of multiple wireless access points?

- A. WPA
- B. WEP
- C. ad hoc
- D. LWAPP

**Correct Answer:** D  
**Section:** Layer 2 Technologies  
**Explanation**

**Explanation/Reference:**  
Explanation:

Lightweight access point protocol (LWAPP) is a protocol used to allow centralized management of access points (APs). The management components are removed from the APs and centralized into a wireless LAN controller. This controller can coordinate WLAN access, managing the load on the APs and user movement between APs. A lightweight AP receives control and configuration from the WLAN controller.

LWAPP defines the following activities:  
Packet encapsulation, fragmentation, and formatting  
Access point certification and software control  
Access point discovery, information exchange, and configuration

The processing of 802.11 data and the handling of management protocols and access point capabilities is distributed between the lightweight access point and the WLAN controller. For example, the AP handles the transmission of beacon frames and responses to probe request frames and the controller handles authentication. The WLC enhances:  
Mobility  
Authentication  
Security management

When lightweight APs are used, the data path from one wireless station to another includes the AP and its controller.

Wi-Fi protected access (WPA) is an encryption and authentication protocol for wireless access. It supports 802.1x authentication and EAP on a wireless

client. The AP would function as the authenticator.

WEP is a wireless encryption protocol that uses static keys and no authentication.

Ad hoc is a WLAN mode used for peer-to-peer connectivity. Ad hoc allows wireless-enabled computers to communicate with each other without having an AP involved.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify other LAN switching technologies

References:

Cisco > Support > Product Support > Wireless > Cisco Aironet 1200 Series > Product Literature > Solution Overviews > Cisco Unified Wireless Network Overview

#### QUESTION 188

Consider the following commands executed on a Layer 3 switch named switchA:

```
switchA(config)# ip routing
switchA(config)# vlan 10
switchA(config-vlan)# name Finance
switchA(config-vlan)# exit
switchA(config)# interface Fa0/1
switchA(config-if)# ip address 10.1.1.1 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# no shutdown
switchA(config)# interface Fa0/2
switchA(config-if)# ip address 10.2.2.2 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# switchport autostate exclude
switchA(config-if)# no shutdown
switchA(config)# interface Fa0/3
switchA(config-if)# ip address 10.3.3.3 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# switchport autostate exclude
switchA(config-if)# no shutdown
switchA(config-if)# interface Fa0/4
switchA(config-if)# ip address 10.4.4.4 255.255.255.0
switchA(config-if)# switchport mode access
switchA(config-if)# switchport access vlan 10
switchA(config-if)# no switchport autostate exclude
switchA(config-if)# no shutdown
switchA(config-if)# interface vlan 10
switchA(config-if)# ip address 10.66.66.1 255.255.255.0
switchA(config-if)# no shutdown
```

Which of the following physical interfaces do NOT affect the uplink state of VLAN 10? (Choose two.)

- A. Fa0/1
- B. Fa0/2
- C. Fa0/3
- D. Fa0/4

**Correct Answer:** BC

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The Fa0/2 and Fa0/3 physical interfaces of switchA do not affect the uplink state of VLAN 10. This is because the switchport autostate exclude command is used on the Fa0/2 and Fa0/3 interfaces. This command causes the exclusion of an interface from the determination of the uplink state of the VLAN (SVI interface) to which the interface belongs.

An SVI or switch virtual interface is a logical interface that allows you to enable inter-VLAN routing on Layer 3 switches. SVIs are configured as VLAN interfaces and have at least one physical interface assigned to the VLANs. An SVI is up and running when all of the following conditions are met:

It is configured on the switch and is enabled in the VLAN database

It is not in the administratively down state

It has at least one Layer 2 (access or trunk) interface in the up state

When an SVI services multiple interfaces (the switch ports in the VLAN to which the SVI connects) and all of them go down, the SVI also goes down by default. When any of the interfaces comes up, the SVI also comes up. By default, all interfaces assigned to the SVI are involved in determining its uplink state. However, if you do not want a particular interface to participate in this determination, use the switchport autostate exclude command on that interface.

You can use the switchport autostate exclude command on any Layer 2 access or trunk interface. This command applies to all VLANs to which the interface belongs. If the excluded interface of an SVI is in the up state and all the other interfaces of the SVI are in the down state, the SVI remains in the down state. The state of the SVI does not change to up.

The Fa0/1 and Fa0/4 interfaces of switchA affect the uplink state of VLAN 10 because all the interfaces assigned to an SVI contribute towards the uplink state determination of the SVI by default.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify VLANs

References:

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring Layer 3 Interfaces > Configuring VLANs as Layer 3 Interfaces > Understanding SVI Autostate Exclude  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport autostate exclude

#### QUESTION 189

Inter-VLAN routing has been operating successfully for several months. Users who connect to a newly installed switch report that they are unable to communicate with the rest of the company's networks. You decide to ensure that the switch is properly connected to the VTP domain before taking any other troubleshooting steps.

What command would be best used to verify this?

- A. switch# show vlan
- B. switch# show ip route
- C. switch# show interfaces trunk
- D. switch# show vtp status
- E. switch #show interface

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The command show vtp status would be the best command to verify the switch's connection to the company's VTP domain. This command displays the version of VTP, the VTP domain the switch is a member of, the VTP mode of the switch, and other configuration settings relating to VTP.

The command show vlan will display the VLANs that exist and the ports that are members of the VLANs, but will not identify whether switch is a member of the VTP domain. If the VLANs that are displayed with this command are the same as those in the VTP domain, it does not necessarily mean the switch is a member of the domain. This data needs to be verified with the show vtp status command.

The command show ip route is used to verify the routing table, but it does not provide any VTP information. This command is used to verify routes to other networks discovered or configured on the switch. It will display the routing protocol used to discover each route, and the next hop used to forward traffic to the destination network.

The command show interfaces trunk is used to verify which VLANs are being forwarded to another device, but does not indicate whether the switch is a member of the VTP domain.

The command show interfaces would not allow you to verify the switch's connection to the company's VTP domain. This command would allow you to determine the following features of the switch:

Port state  
Port speed  
Input errors  
Collisions

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.1(13)EW > Understanding and Configuring VTP  
Cisco > Cisco IOS LAN Switching Command Reference > show vlan through ssl-proxy module allowed-vlan > show vtp

#### QUESTION 190

During which STP state can ports add information to their address tables, but not send any data?

- A. Learning
- B. Listening
- C. Blocked
- D. Forwarding

**Correct Answer:** A

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

In the learning state, a switch port can add learned information into its address table, but cannot forward data.

Spanning tree transitions each port through several states whenever there is a change in the network topology to prevent switching loops. Each state is briefly defined as follows:

Blocking: In the blocking state, a port does not forward frames, learn information, or send out information. A forwarding port is placed in the blocked state when the port senses an absence of BPDUs, which are sent out in the interval defined by the hello time (two seconds by default). If the blocked port does not detect a BPDU for the length of time defined in the max-age setting (20 seconds by default), the port will transition into the listening state.

Listening: In the listening state, a port receives traffic, but does not send information. This is the first transitional state after the blocking state. No user data is forwarded at this time, but the switch is very busy. It is during this stage that the switch participates in the election of the root bridge, the root ports on the non-root bridges, and the designated ports on each segment. Ports that remain as designated or root ports will transition to the learning state after the time defined in the forward delay (15 seconds by default) has elapsed.

Learning: In the learning state, a switch port can add the MAC addresses that it has learned into its address table but cannot forward user data. The switch port will remain in this state until the amount of time defined in the forward-delay setting has elapsed (15 seconds by default), at which time it will transition into the forwarding state.

Forwarding: In the forwarding state, a port is actively forwarding packets. It will remain in the forwarding state until it does not detect a BPDU within the defined hello time, at which time the port is placed in the blocking state and the process starts again.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify spanning tree

References:

Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring STP and IEEE 802.1s MST > Creating the Spanning Tree Topology  
Cisco > Support > Configuring Spanning Tree Protocol > How STP Works

#### QUESTION 191

Which IOS command enables the VTP feature that eliminates unnecessary trunk traffic being flooded to switches that do not have memberships in particular VLANs?

- A. vtp mode client
- B. no vtp mode
- C. vtp v1-mode
- D. vtp pruning

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

To enable pruning on a switch operating in VLAN Trunk Protocol (VTP) server mode, enter the vtp pruning command at the global configuration prompt.

```
switch(config)# vtp pruning
```

VTP pruning enhances network bandwidth usage by restricting unnecessary flooded traffic on trunk links. If a trunk link does not have devices in the VLAN attached, flooded traffic on that VLAN is blocked. VTP pruning can reduce broadcasts, multicasts, unknown traffic, and flooded unicast packets.

Enabling VTP pruning on a switch in VTP server mode enables pruning for the entire domain.

Multicast and unicast traffic are not blocked for the VLANs that are not being pruned.

There are three modes in VTP: server, client, and transparent. The main differentiator among the three modes is whether a switch can create, modify, or delete VLANs. A Catalyst switch can create, modify, and delete VLANs in server or transparent mode, but not in client mode. However, VLANs created on a switch in transparent mode apply only to that switch, and information about these VLANs is not propagated throughout the VTP domain.

The VTP server mode sends or forwards VTP advertisements, synchronizes VLAN configuration information with other switches, and saves the VLAN in NVRAM.

The VTP transparent mode forwards VTP advertisements and saves the VLAN configuration in NVRAM. It does not synchronize VLAN configuration information. A switch in transparent mode can create, delete, and modify VLANs, but changes are not transmitted to other switches in the domain. They only affect the local switch.

The VTP client mode sends or forwards VTP advertisements and synchronizes VLAN configuration information with other switches. It does not save VLAN information in NVRAM. In client mode, VTP clients only can receive VLAN information from VTP servers.

The command vtp mode client sets the switch to client mode. It does not eliminate unnecessary trunk traffic.

The no vtp mode command reverts the VTP mode back to its default state, which is server mode. To set the VTP mode of a VTP client back to server mode, you can use either the no vtp mode command or the vtp server command.

The vtp v1-mode command reverts the VTP version to version 1 (the default version). Use the vtp v2-mode command to set the VTP mode to version 2.

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify trunking

References:

Cisco > Home > Support > Technology Support > LAN Switching > Virtual LANS/VLAN Trunking Protocol (VLANS/VTP) > Design > Design Technotes > Understanding VLAN Trunk Protocol (VTP)  
Cisco > Cisco IOS LAN Switching Command Reference > udd through vtp v2-mode > vtp

#### QUESTION 192

During a CEF packet rewrite, which of the following changes are NOT made to the packet?

- A. The source MAC address is changed to the MAC address of the outbound Layer 3 switch interface.
- B. The destination MAC address is changed to the MAC address of the next-hop router's MAC address.
- C. Layer 3 TTL is decremented by one.
- D. Layer 2 TTL is decremented by one.

**Correct Answer:** D

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

There is no Layer 2 TTL in the packet, so the Layer 2 time to live (TTL) cannot be decremented by one. All other options are correct. The following changes will be made when the Cisco Express Forwarding (CEF) packet rewrite process occurs:

The source MAC address is changed to the MAC address of the outbound Layer 3 switch interface.

The destination MAC address is changed to the MAC address of the next hop routers MAC address

The Layer 3 IP TTL is decremented by one

The Layer 3 IP checksum is recalculated

The Layer 2 frame checksum is recalculated

Objective:

Layer 2 Technologies

Sub-Objective:

Configure and verify switch administration



References:

Cisco > Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.1E > Configuring IP Unicast Layer 3 Switching on Supervisor Engine 2 > Understanding How IP Multicast Layer 3 Switching Works

**QUESTION 193**

Consider the following output of the show spanning-tree command for the SW1 switch:

```
SW1# show spanning-tree
VLAN0001
Spanning tree enabled protocol ieee
Root ID Priority 23195
Address 002A.10C8.F04B
Cost 19
Port 1 (Fa0/1)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 30769 (priority 30768 sys-id-ext 1)
Address 003E.7A3B.9B01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/1      Root FWD 19 128.1 P2p
Fa0/2 Altn BLK 19 128.2 P2p
Fa0/3 Desg FWD 19 128.3 P2p

VLAN0101
Spanning tree enabled protocol ieee
Root ID Priority 15123
Address 003E.7A3B.9B01
This bridge is the root
Bridge ID Priority 15123 (priority 15022 sys-id-ext 101)
Address 003E.7A3B.9B01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/1 Desg FWD 19 128.1 P2p
Fa0/2 Desg BLK 19 128.2 P2p
Fa0/3 Desg BLK 19 128.3 P2p

VLAN0202
Spanning tree enabled protocol ieee
Root ID Priority 9305
Address 0010.0B1A.3C3D
Cost 19
Port 3 (Fa0/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 30508 (priority 30306 sys-id-ext 202)
Address 003E.7A3B.9B01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300
Interface Role Sts Cost Prio.Nbr Type
-----
Fa0/1 Desg FWD 19 128.1 P2p
Fa0/2 Altn BLK 19 128.5 P2p
Fa0/3 Root FWD 19 128.6 P2p
```

You need to change the spanning-tree configuration such that the following is true:

SW1 is the root bridge for VLAN0001

SW1 is not the root bridge for VLAN0101

Fa0/2 port of SW1 should be in the forwarding state for VLAN0202 traffic

Which of the following commands should be executed on SW1 to achieve the desired results? (Choose all that apply.)

- A. spanning-tree vlan 1 priority 23189 in global configuration mode
- B. spanning-tree vlan 1 priority 32768 in global configuration mode
- C. spanning-tree vlan 101 priority 32768 in global configuration mode
- D. spanning-tree vlan 202 cost 2 in interface configuration mode of Fa0/2
- E. spanning-tree vlan 202 cost 252 in interface configuration mode of Fa0/2

**Correct Answer:** ACD

**Section:** Layer 2 Technologies

**Explanation**

**Explanation/Reference:**

Explanation:

The following commands should be executed to achieve the desired results:

```
spanning-tree vlan 1 priority 23189 in global configuration mode
spanning-tree vlan 101 priority 32768 in global configuration mode
spanning-tree vlan 202 cost 2 in interface configuration mode on Fa0/2
```

The spanning-tree vlan 1 priority 23189 command changes the bridge priority of SW1 to 23189 for the native VLAN (VLAN0001). According to the show spanning-tree output in the scenario, the root bridge for VLAN0001 has a priority of 23195. Therefore, if SW1 has to become the root bridge for VLAN0001, then SW1 should have the least bridge priority for that VLAN. Setting the bridge priority of SW1 to 23189, which is less than 23195, serves the purpose.

The spanning-tree vlan 101 priority 32768 command changes the bridge priority of SW1 to 32768 for VLAN0101. The maximum priority that can be assigned to a switch is 32768, which implies that the switch cannot be a root bridge for the VLAN provided its MAC address is higher than the other switches. This will



ensure that SW1 will NOT be the root bridge for VLAN 101

The spanning-tree vlan 202 cost 2 command sets the port cost to 2 for VLAN0202. The port cost is used by STP to determine a loop-free path. The port with the least cost is selected and placed in Forwarding state. Therefore, as a result of this command, the Fa0/2 port will be in the Forwarding state to pass the VLAN0202 traffic, rather than Fa0/1.

Executing the spanning-tree vlan 1 priority 32768 command in the global configuration mode does not achieve the desired results. This command sets the bridge priority of SW1 to the highest possible value for VLAN0001. As 32768 is greater than 23190, the new bridge priority of SW1 does not affect the root bridge for VLAN0001 and SW1 remains a non-root bridge.

The spanning-tree vlan 202 cost 252 command in the interface configuration mode of Fa0/2 does not achieve the desired results. This command changes the port cost of Fa0/2 for VLAN0202 to 252, which is the maximum cost value. STP selects the port with the least cost as the best loop-free path. Therefore, setting the cost to 252 for Fa0/2 will not put Fa0/2 in the Forwarding state.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco > Cisco IOS Bridging Command Reference > rif through spanning-tree portfast (interface mode)  
Cisco > Technology Support > Lan Switching > Understanding and Configuring Spanning Tree Protocol (STP) on Catalyst Switches

#### QUESTION 194

What is the easiest way to force a specific switch to become the spanning-tree root bridge for a VLAN?

- A. Raise the spanning-tree priority value on the switch.
- B. Lower the spanning-tree priority value on the switch.
- C. Raise the port-cost value of an interface on the switch.
- D. Lower the port-cost value of an interface on the switch.

**Correct Answer: B**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The spanning-tree root bridge is the bridge with the lowest bridge ID. The bridge ID is a value calculated from the bridge priority and the bridge MAC address. Therefore, lowering the bridge-priority value lowers the bridge ID, which can force the switch to become the root bridge.

The easiest way to force a specific switch to become the spanning-tree root bridge for a VLAN is to lower its priority using the spanning-tree vlan vlan\_id priority priority command. For example, the following command will configure the switch as the root bridge for VLAN 10:

```
switch(config)# spanning-tree vlan 10 priority 4096
```

The priority value of 4096 is used by convention. It could be set to any value as long as it is lower than any other switch in the VLAN. The priority value 4096 is typically used when forcing the placement of the root bridge, and 8192 is used to force placement of the secondary root bridge. These values work because the default priority value for switches is 32768.

Lowering the port cost of an interface is an effective way to force spanning tree to put the interface into a forwarding state. However, it does not affect the placement of the root bridge.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify spanning tree

References:  
Cisco IOS LAN Switching Configuration Guide, Release 12.4 > EtherSwitch Network Module > Configuring Spanning Tree on a VLAN > VLAN Root Bridge and VLAN Bridge Priority

#### QUESTION 195

Which protocol is used to maintain the contents of the Cisco Express Forwarding (CEF) adjacency table?

- A. ARP
- B. RARP
- C. PING
- D. INARP

**Correct Answer: A**  
**Section: Layer 2 Technologies**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The CEF adjacency table is maintained as each adjacent node is discovered. Link header entries are created and stored in the adjacency table as the information is learned through the ARP protocol.

Cisco Express Forwarding (CEF) is a Layer 3 switching technology based on information contained in the Forwarding Information Base (FIB) and the adjacency table.

The FIB is conceptually equivalent to a routing table in that it contains information used in the packet forwarding decision. The adjacency table contains information about the adjacent route processors. The adjacency table contains the MAC information for the next-hop addresses for all FIB entries. A device is considered adjacent if it is reachable over a single Layer 2 connection. It is stored in DRAM.

The Layer 3 processor engine builds the FIB and adjacency tables in software. That information is distributed from the control-plane hardware to the data-plane hardware Application Specific Integrated Circuits (ASICs) at the port or line card. This enhances the Layer 3 forwarding operation by moving it from the software-based engine to the ASICs. Of course, there are exception packets that are still software-processed, such as non-conforming protocols and datalink encapsulations.

Reverse ARP (RARP) is used an obsolete networking protocol used by a host computer to obtain its Internet Protocol (IPv4) address when it has available its link-layer address, such as an Ethernet address. It has been replaced with DHCP. It is not used maintain the contents of the Cisco Express Forwarding (CEF) adjacency table

INverse ARP (INARP) is used by Frame relay connection to dynamically learn the DLCI associated with a connection. It is not used maintain the contents of the Cisco Express Forwarding (CEF) adjacency table

PING is a diagnostic tool used to test connectivity. It is not used maintain the contents of the Cisco Express Forwarding (CEF) adjacency table.

Objective:  
Layer 2 Technologies  
Sub-Objective:  
Configure and verify switch administration

References:  
Cisco >IP Switching Cisco Express Forwarding Configuration Guide, Cisco IOS Release 15 > CEF Overview > CEF Adjacency Tables Overview

**QUESTION 196**

A Cisco Catalyst switch that is prone to reboots continues to rebuild the DHCP snooping database. What is the solution to avoid the snooping database from being rebuilt after every device reboot?

- A. A DHCP snooping database agent should be configured.
- B. Enable DHCP snooping for all VLANs that are associated with the switch.
- C. Disable Option 82 for DHCP data insertion.
- D. Use IP Source Guard to protect the DHCP binding table entries from being lost upon rebooting.
- E. Apply ip dhcp snooping trust on all interfaces with dynamic addresses.

**Correct Answer: A**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**  
Explanation:  
Minimum DHCP Snooping Configuration  
The minimum configuration steps for the DHCP snooping feature are as follows:

|                                                                                     |
|-------------------------------------------------------------------------------------|
| 1. Define and configure the DHCP server.                                            |
| 2. Enable DHCP snooping on at least one VLAN.                                       |
| By default, DHCP snooping is inactive on all VLANs.                                 |
| 3. Ensure that DHCP server is connected through a trusted interface.                |
| By default, the trust state of all interfaces is untrusted.                         |
| 4. Configure the DHCP snooping database agent.                                      |
| This step ensures that database entries are restored after a restart or switchover. |
| 5. Enable DHCP snooping globally.                                                   |

The feature is not active until you complete this step.

Reference: <http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snoodhcp.html#wp1090479>

**QUESTION 197**

Which portion of AAA looks at what a user has access to?

- A. authorization
- B. authentication
- C. accounting
- D. auditing

**Correct Answer: A**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**  
Explanation:  
AAA consists of the following three elements:

- Authentication: Identifies users by login and password using challenge and response methodology before the user even gains access to the network. Depending on your security options, it can also support encryption.
- Authorization: **After initial authentication, authorization looks at what that authenticated user has access to do.** RADIUS or TACACS+ security servers perform authorization for specific privileges by defining attribute-value (AV) pairs, which would be specific to the individual user rights. In the Cisco IOS, you can define AAA authorization with a named list or authorization method.
- Accounting: The last "A" is for accounting. It provides a way"o" collecting security information that you can use for billing, auditing, and reporting. You can use accounting to see what users do once they are authenticated and authorized. For example, with accounting, you could get a log of when users logged in and when they logged out.

Reference: <http://www.techrepublic.com/blog/data-center/what-is-aaa-and-how-do-you-configure-it-in-the-cisco-ios/>

**QUESTION 198**

Which command creates a login authentication method named "login" that will primarily use RADIUS and fail over to the local user database?

- A. (config)# aaa authentication login default radius local
- B. (config)# aaa authentication login login radius local
- C. (config)# aaa authentication login default local radius
- D. (config)# aaa authentication login radius local

**Correct Answer: B**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

Explanation:

In the command “aaa authentication login login radius local” the second login is the name of the AAA method. It also lists radius first then local, so it will primarily use RADIUS for authentication and fail over to the local user database only if the RADIUS server is unreachable.

#### QUESTION 199

A server with a statically assigned IP address is attached to a switch that is provisioned for DHCP snooping. For more protection against malicious attacks, the network team is considering enabling dynamic ARP inspection alongside DHCP snooping.

Which solution ensures that the server maintains network reachability in the future?

- A. Disable DHCP snooping information option.
- B. Configure a static DHCP snooping binding entry on the switch.
- C. Trust the interface that is connected to the server with the ip dhcp snooping trust command.
- D. Verify the source MAC address of all untrusted interfaces with ip dhcp snooping verify mac-address command.

**Correct Answer: B**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP requests and responses on untrusted ports
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drops invalid ARP packets

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid. To ensure network reachability to the server, configure a static DHCP snooping binding entry on the switch.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2\\_55\\_se/configuration/guide/scg3750/swdynarp.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swdynarp.html)

#### QUESTION 200

A network engineer wants to ensure Layer 2 isolation of customer traffic using a private VLAN. Which configuration must be made before the private VLAN is configured?

- A. Disable VTP and manually assign VLANs.
- B. Ensure all switches are configured as VTP server mode.
- C. Configure VTP Transparent Mode.
- D. Enable VTP version 3.

**Correct Answer: C**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

You must configure VTP to transparent mode before you can create a private VLAN. Private VLANs are configured in the context of a single switch and cannot have members on other switches. Private VLANs also carry TLVs that are not known to all types of Cisco switches.

Reference: <http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=6>

#### QUESTION 201

DHCP snooping and IP Source Guard have been configured on a switch that connects to several client workstations. The IP address of one of the workstations does not match any entries found in the DHCP binding database.

Which statement describes the outcome of this scenario?

- A. Packets from the workstation will be rate limited according to the default values set on the switch.
- B. The interface that is connected to the workstation in question will be put into the errdisabled state.
- C. Traffic will pass accordingly after the new IP address is populated into the binding database.
- D. The packets originating from the workstation are assumed to be spoofed and will be discarded.

**Correct Answer: D**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

You can configure IP source guard with source IP address filtering, or with source IP and MAC address filtering. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table. If there is no match, the packets are assumed to be spoofed and will be discarded.

Reference: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-cat13fixed.html#ipsourceguard>

#### QUESTION 202

A DHCP configured router is connected directly to a switch that has been provisioned with DHCP snooping. IP Source Guard with the ip verify source port-security command is configured under the interfaces that connect to all DHCP clients on the switch. However, clients are not receiving an IP address via the DHCP server.

Which option is the cause of this issue?

- A. The DHCP server does not support information option 82.
- B. The DHCP client interfaces have storm control configured.
- C. Static DHCP bindings are not configured on the switch.
- D. DHCP snooping must be enabled on all VLANs, even if they are not utilized for dynamic address allocation.

**Correct Answer:** A

**Section:** Infrastructure Security

**Explanation**

**Explanation/Reference:**

Explanation:

When you enable both IP Source Guard and Port Security, using the ip verify source port-security interface configuration command, there are two caveats:

- The DHCP server must support option 82, or the client is not assigned an IP address.
- The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swdhcp82.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swdhcp82.html)

#### QUESTION 203

A switch is added into the production network to increase port capacity. A network engineer is configuring the switch for DHCP snooping and IP Source Guard, but is unable to configure ip verify source under several of the interfaces.

Which option is the cause of the problem?

- A. The local DHCP server is disabled prior to enabling IP Source Guard.
- B. The interfaces are configured as Layer 3 using the no switchport command.
- C. No VLANs exist on the switch and/or the switch is configured in VTP transparent mode.
- D. The switch is configured for sdm prefer routing as the switched database management template.
- E. The configured SVIs on the switch have been removed for the associated interfaces.

**Correct Answer:** B

**Section:** Infrastructure Security

**Explanation**

**Explanation/Reference:**

Explanation:

**IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces** by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.

You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.

The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled.

**IP source guard is supported only on Layer 2 ports, including access and trunk ports.** You can configure IP source guard with source IP address filtering or with source IP and MAC address filtering.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swdhcp82.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swdhcp82.html)

#### QUESTION 204

The command storm-control broadcast level 75 65 is configured under the switch port connected to the corporate mail server. In which three ways does this command impact the traffic? (Choose three.)

- A. SNMP traps are sent by default when broadcast traffic reaches 65% of the lower-level threshold.
- B. The switchport is disabled when unicast traffic reaches 75% of the total interface bandwidth.
- C. The switch resumes forwarding broadcasts when they are below 65% of bandwidth.
- D. Only broadcast traffic is limited by this particular storm control configuration.
- E. Multicast traffic is dropped at 65% and broadcast traffic is dropped at 75% of the total interface bandwidth.
- F. The switch drops broadcasts when they reach 75% of bandwidth.

**Correct Answer:** CDF

**Section:** Infrastructure Security

**Explanation**

**Explanation/Reference:**

Explanation:



|                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>storm-control {broadcast   multicast   unicast} level {level [level-low]   pps pps [pps-low]}</b> | Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled.<br>The keywords have these meanings: <ul style="list-style-type: none"><li>• ___ For level, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00.</li><li>• ___ (Optional) For level-low, specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00.</li></ul> |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

In this case, the broadcast keyword was used so only broadcast traffic is limited.

Reference: [https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2\\_0\\_se/multibook/configuration\\_guide/b\\_consolidated\\_config\\_guide\\_3850\\_chapter\\_011100.html](https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011100.html)

**QUESTION 205**

After port security is deployed throughout an enterprise campus, the network team has been overwhelmed with port reset requests. They decide to configure the network to automate the process of re-enabling user ports. Which command accomplishes this task?

- A. switch(config)# errdisable recovery interval 180
- B. switch(config)# errdisable recovery cause psecure-violation
- C. switch(config)# switchport port-security protect
- D. switch(config)# switchport port-security aging type inactivity
- E. switch(config)# errdisable recovery cause security-violation

**Correct Answer: B**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**  
Explanation:  
When a secure port is in the error-disabled state, you can bring it out of this state automatically by configuring the errdisable recovery cause psecure-violation global configuration command or you can manually reenable it by entering the shutdown and no shut down interface configuration commands. This is the default mode. If a port is in per-VLAN errdisable mode, you can also use clear errdisable interface name vlan range command to re-enable the VLAN on the port.  
You can also customize the time to recover from the specified error disable cause (default is 300 seconds) by entering the errdisable recovery interval interval command.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/53SG/configuration/config/port\\_sec.pdf](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/53SG/configuration/config/port_sec.pdf)

**QUESTION 206**

The network monitoring application alerts a network engineer of a client PC that is acting as a rogue DHCP server. Which two commands help trace this PC when the MAC address is known? (Choose two.)

- A. switch# show mac address-table
- B. switch# show port-security
- C. switch# show ip verify source
- D. switch# show ip arp inspection
- E. switch# show mac address-table address <mac address>

**Correct Answer: AE**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**  
Explanation:  
These two commands will show the MAC address table, including the switch port that the particular host is using. Here is an example output:  
Switch> **show mac-address-table**

```
Dynamic Addresses Count:          9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:      41
Total MAC addresses:              50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-----
0010.0de0.e289      Dynamic      1     FastEthernet0/1
0010.7b00.1540      Dynamic      2     FastEthernet0/5
0010.7b00.1545      Dynamic      2     FastEthernet0/5
```

**QUESTION 207**

While troubleshooting a network outage, a network engineer discovered an unusually high level of broadcast traffic coming from one of the switch interfaces. Which option decreases consumption of bandwidth used by broadcast traffic?

- A. storm control
- B. SDM routing
- C. Cisco IOS parser



- D. integrated routing and bridging
- E. Dynamic ARP Inspection

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on a port. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm.

Storm control is configured for the switch as a whole but operates on a per-port basis. By default, storm control is disabled.

Storm control uses rising and falling thresholds to block and then restore the forwarding of broadcast, unicast, or multicast packets. You can also set the switch to shut down the port when the rising threshold is reached.

Reference: [https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2\\_0\\_se/multibook/configuration\\_guide/b\\_consolidated\\_config\\_guide\\_3850\\_chapter\\_011100.html](https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3.2_0_se/multibook/configuration_guide/b_consolidated_config_guide_3850_chapter_011100.html)

#### QUESTION 208

Which command globally enables AAA on a device?

- A. aaa new-model
- B. aaa authentication
- C. aaa authorization
- D. aaa accounting

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

To configure AAA authentication, enable AAA by using the aaa new-model global configuration command. AAA features are not available for use until you enable AAA globally by issuing the aaa new-model command.

Reference: [http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfathen.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html)

#### QUESTION 209

Which AAA Authorization type includes PPP, SLIP, and ARAP connections?

- A. network
- B. IP mobile
- C. EXEC
- D. auth-proxy

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods defined are exhausted.

Method lists are specific to the authorization type requested:

- Auth-proxy — Applies specific security policies on a per-user basis. For detailed information on the authentication proxy feature, refer to the chapter "Configuring Authentication Proxy" in the "Traffic Filtering and Firewalls" part of this book
- Command Authorization — Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.
- EXEC — Applies to the attributes associated with a user EXEC terminal session.
- **Network — Applies to network connections. This can include a PPP, SLIP, or ARAP connection.**
- Reverse Access — Applies to reverse Telnet sessions.

When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.

Reference: [http://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecur\\_c/scfathor.html](http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathor.html)

#### QUESTION 210

Which authentication service is needed to configure 802.1x?

- A. RADIUS with EAP Extension
- B. TACACS+
- C. RADIUS with CoA
- D. RADIUS using VSA

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

With 802.1x, the authentication server — performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. **The Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication**

Protocol (EAP) extensions is the only supported authentication server.

References: [https://www.cisco.com/c/en/us/td/docs/switches/metro/me3400/software/release/12-2\\_25\\_ex/configuration/guide/3400scg/sw8021x.pdf](https://www.cisco.com/c/en/us/td/docs/switches/metro/me3400/software/release/12-2_25_ex/configuration/guide/3400scg/sw8021x.pdf) page 8-2

#### QUESTION 211

Refer to the exhibit.

```
username cisco password cisco
!
aaa new-model
radius-server host 10.1.1.50 auth-port 1812 key C1sc0123
aaa authentication login default group radius local line
aaa authentication logging NO_AUTH none
!
line vty 0 15
login authentication default
password linepass
line console 0
login authentication NO_AUTH
```

Which login credentials are required when connecting to the console port in this output?

- A. none required
- B. username cisco with password cisco
- C. no username with password linepass
- D. login authentication default

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Here the console has been configured with the NO\_AUTH name, which lists none as the authentication method. None means no authentication, meaning that credentials are not required and all sessions are allowed access immediately.

#### QUESTION 212

Refer to the exhibit.

```
username cisco password cisco
!
aaa new-model
radius-server host 10.1.1.50 auth-port 1812 key C1sc0123
aaa authentication login default group radius local line
aaa authentication logging NO_AUTH none
!
line vty 0 15
login authentication default
password linepass
line console 0
login authentication NO_AUTH
```

When a network administrator is attempting an SSH connection to the device, in which order does the device check the login credentials?

- A. RADIUS server, local username, line password
- B. RADIUS server, line password, local username
- C. Line password, local username, RADIUS server
- D. Line password, RADIUS server, local username

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

sessions use the vty lines, where the configured authentication method is named “default.” The AAA default login preference is stated in order from first to last, so here the “aaa authentication login default group radius local line” means to use RADIUS first, then if that fails use the local user database. Finally, if that fails use the line password.

#### QUESTION 213

Which type of information does the DHCP snooping binding database contain?

- A. untrusted hosts with leased IP addresses
- B. trusted hosts with leased IP addresses
- C. untrusted hosts with available IP addresses
- D. trusted hosts with available IP addresses

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
- Rate-limits DHCP traffic from trusted and untrusted sources.
- **Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.**
- Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.pdf>

**QUESTION 214**

Which switch feature determines validity based on IP-to-MAC address bindings that are stored in a trusted database?

- A. Dynamic ARP Inspection
- B. storm control
- C. VTP pruning
- D. DHCP snooping

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

Reference: <http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-cat13fixed.html>

**QUESTION 215**

Which command is needed to enable DHCP snooping if a switchport is connected to a DHCP server?

- A. ip dhcp snooping trust
- B. ip dhcp snooping
- C. ip dhcp trust
- D. ip dhcp snooping information

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

When configuring DHCP snooping, follow these guidelines:

- DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP globally on the switch.
- Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.
- **If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the “ip dhcp snooping trust” interface configuration command.**
- If a Layer 2 LAN port is connected to a DHCP client, configure the port as untrusted by entering the no ip dhcp snooping trust interface configuration command.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html>

**QUESTION 216**

Which private VLAN access port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports?

- A. promiscuous port
- B. isolated port
- C. community port
- D. trunk port

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

The types of private VLAN ports are as follows:

- Promiscuous — A promiscuous port belongs to the primary VLAN. **The promiscuous port can communicate with all interfaces, including the community and isolated host ports**, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN. You can have several promiscuous ports in a primary VLAN. Each promiscuous port can have several secondary VLANs, or no secondary VLANs, associated to that port. You can associate a secondary VLAN to more than one promiscuous port, as long as the promiscuous port and secondary VLANs are within the same primary VLAN. You may want to do this for load-balancing or redundancy purposes. You can also have secondary VLANs that are not associated to any promiscuous port.
- Isolated — An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.
- Community — A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports. These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html>

#### QUESTION 217

Which private VLAN can have only one VLAN and be a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway?

- A. isolated VLAN
- B. primary VLAN
- C. community VLAN
- D. promiscuous VLAN

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Understanding Primary, Isolated, and Community Private VLANs

Primary VLANs and the two types of secondary VLANs (isolated and community) have these characteristics:

- Primary VLAN — The primary VLAN carries traffic from the promiscuous ports to the host ports, both isolated and community, and to other promiscuous ports.
- Isolated VLAN — **An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports.** You can configure multiple isolated VLANs in a private VLAN domain; all the traffic remains isolated within each one. Each isolated VLAN can have several isolated ports, and the traffic from each isolated port also remains completely separate.
- Community VLAN — A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN.

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html>

#### QUESTION 218

Which database is used to determine the validity of an ARP packet based on a valid IP-to-MAC address binding?

- A. DHCP snooping database
- B. dynamic ARP database
- C. dynamic routing database
- D. static ARP database

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

Information About Dynamic ARP Inspection

DAI is used to validate ARP requests and responses as follows:

- Intercepts all ARP requests and responses on untrusted ports.
- Verifies that a packet has a valid IP-to-MAC address binding before updating the ARP cache or forwarding the packet.
- Drops invalid ARP packets.

**DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a DHCP snooping binding database.** This database is built by DHCP snooping when it is enabled on the VLANs and on the device. It may also contain static entries that you have created.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/hyperv/sw/5\\_2\\_1\\_s\\_m\\_1\\_5\\_2/troubleshooting/configuration/guide/n1000v\\_troubleshooting/n1000v\\_trouble\\_19dhcp.html](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/hyperv/sw/5_2_1_s_m_1_5_2/troubleshooting/configuration/guide/n1000v_troubleshooting/n1000v_trouble_19dhcp.html)

#### QUESTION 219

When IP Source Guard with source IP filtering is enabled on an interface, which feature must be enabled on the access VLAN for that interface?

- A. DHCP snooping
- B. storm control
- C. spanning-tree portfast
- D. private VLAN

**Correct Answer: A**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

IP Source Guard Configuration Guidelines

- You can configure static IP bindings only on nonrouted ports. If you enter the ip source binding mac-address vlan vlan-id ip-address interface interface-id global configuration command on a routed interface, this error message appears:

Static IP source binding can only be configured on switch port.

- **When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.**
- If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.
- You can enable this feature when 802.1x port-based authentication is enabled.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0\\_2\\_EX/security/configuration\\_guide/b\\_sec\\_152ex\\_2960-x\\_cg/b\\_sec\\_152ex\\_2960-x\\_cg\\_chapter\\_01110.html](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01110.html)

#### QUESTION 220

Which switch feature prevents traffic on a LAN from being overwhelmed by continuous multicast or broadcast traffic?



- A. storm control
- B. port security
- C. VTP pruning
- D. VLAN trunking

**Correct Answer:** A  
**Section:** Infrastructure Security  
**Explanation**

**Explanation/Reference:**

Explanation:

A traffic storm occurs when packets flood the LAN, which creates excessive traffic and degrades network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces from either mistakes in network configurations or from users issuing a DoS attack.

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.pdf>

**QUESTION 221**

Which command would a network engineer apply to error-disable a switchport when a packet-storm is detected?

- A. router(config-if)#storm-control action shutdown
- B. router(config-if)#storm-control action trap
- C. router(config-if)#storm-control action error
- D. router(config-if)#storm-control action enable

**Correct Answer:** A  
**Section:** Infrastructure Security  
**Explanation**

**Explanation/Reference:**

Explanation:

Configuring the Traffic Storm Control Shutdown Mode

To configure the traffic storm control shutdown mode on an interface, perform this task:

|        | Command                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>interface</b><br><i>{{type1 slot/port}}   {port-channel number}}</i> | Selects an interface to configure.                                                                                                                                                                                                                                                                                                                                                                                    |
| Step 2 | Router(config-if)# <b>storm-control</b><br><b>action shutdown</b>                       | (Optional) Configures traffic storm control to error-disable ports when a traffic storm occurs. <ul style="list-style-type: none"> <li>• <u>  </u> Enter the <b>no storm-control action shutdown</b> command to revert to the default action (drop).</li> <li>• <u>  </u> Use the error disable detection and recovery feature, or the <b>shutdown</b> and <b>no shutdown</b> commands to reenab le ports.</li> </ul> |

Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.html>

**QUESTION 222**

A network engineer configures port security and 802.1x on the same interface. Which option describes what this configuration allows?

- A. It allows port security to secure the MAC address that 802.1x authenticates.
- B. It allows port security to secure the IP address that 802.1x authenticates.
- C. It allows 802.1x to secure the MAC address that port security authenticates.
- D. It allows 802.1x to secure the IP address that port security authenticates.

**Correct Answer:** A  
**Section:** Infrastructure Security  
**Explanation**

**Explanation/Reference:**

Explanation:

802.1X and Port Security

You can configure port security and 802.1X on the same interfaces. Port security secures the MAC addresses that 802.1X authenticates. 802.1X processes packets before port security processes them, so when you enable both on an interface, 802.1X is already preventing inbound traffic on the interface from unknown MAC addresses.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4\\_1/nx-os/security/configuration/guide/sec\\_nx-os-cfg/sec\\_portsec.html](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_portsec.html)

**QUESTION 223**

Which feature describes MAC addresses that are dynamically learned or manually configured, stored in the address table, and added to the running configuration?

- A. sticky
- B. dynamic
- C. static
- D. secure

**Correct Answer:** A



**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

Explanation:

With port security, you can configure MAC addresses to be sticky. These can be dynamically learned or manually configured, stored in the address table, and added to the running configuration. If these addresses are saved in the configuration file, the interface does not need to dynamically relearn them when the switch restarts. Although sticky secure addresses can be manually configured, it is not recommended.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port\\_sec.pdf](http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.pdf)

**QUESTION 224**

On which interface can port security be configured?

- A. static trunk ports
- B. destination port for SPAN
- C. EtherChannel port group
- D. dynamic access ports

**Correct Answer: A**

**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

Explanation:

Port Security and Port Types

You can configure port security only on Layer 2 interfaces. Details about port security and different types of interfaces or ports are as follows:

- Access ports — You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN.
- Trunk ports — You can configure port security on interfaces that you have configured as Layer 2 trunk ports. VLAN maximums are not useful for access ports. The device allows VLAN maximums only for VLANs associated with the trunk port.
- SPAN ports — You can configure port security on SPAN source ports but not on SPAN destination ports.
- Ethernet Port Channels — Port security is not supported on Ethernet port channels.

Reference: [http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4\\_1/nx-os/security/configuration/guide/sec\\_nx-os-cfg/sec\\_portsec.html](http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_portsec.html)

These are some other guidelines for configuring port security:

Port security can only be configured on static access ports. A secure port cannot be a dynamic access port or a trunk port. A secure port cannot be a destination port for Switch Port Analyzer (SPAN). A secure port cannot belong to an EtherChannel port group. A secure port cannot be an 802.1X port. You cannot configure static secure MAC addresses in the voice VLAN.

Reference: <https://supportforums.cisco.com/t5/network-infrastructure-documents/unable-to-configure-port-security-on-a-catalyst-2940-2950-2955/ta-p/3133064>

**QUESTION 225**

When you configure private VLANs on a switch, which port type connects the switch to the gateway router?

- A. promiscuous
- B. community
- C. isolated
- D. trunked

**Correct Answer: A**

**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

Explanation:

There are mainly two types of ports in a Private VLAN: Promiscuous port (P-Port) and Host port. Host port further divides in two types – Isolated port (I-Port) and Community port (C-port).

- Promiscuous port (P-Port): The switch port connects to a router, firewall or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port on the VLAN.

- Host Ports:

- Isolated Port (I-Port): Connects to the regular host that resides on isolated VLAN. This port communicates only with P-Ports.

- Community Port (C-Port): Connects to the regular host that resides on community VLAN. This port communicates with P-Ports and ports on the same community VLAN.

Reference: [http://en.wikipedia.org/wiki/Private\\_VLAN](http://en.wikipedia.org/wiki/Private_VLAN)

**QUESTION 226**

When you configure a private VLAN, which type of port must you configure the gateway router port as?

- A. promiscuous port
- B. isolated port
- C. community port
- D. access port

**Correct Answer: A**

**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

Explanation:

There are mainly two types of ports in a Private VLAN: Promiscuous port (P-Port) and Host port. Host port further divides in two types – Isolated port (I-Port) and Community port (C-port).

- Promiscuous port (P-Port): The switch port connects to a router, firewall or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port on the VLAN.
- Host Ports:
  - Isolated Port (I-Port): Connects to the regular host that resides on isolated VLAN. This port communicates only with P-Ports.
  - Community Port (C-Port): Connects to the regular host that resides on community VLAN. This port communicates with P-Ports and ports on the same community VLAN.

Reference: [http://en.wikipedia.org/wiki/Private\\_VLAN](http://en.wikipedia.org/wiki/Private_VLAN)

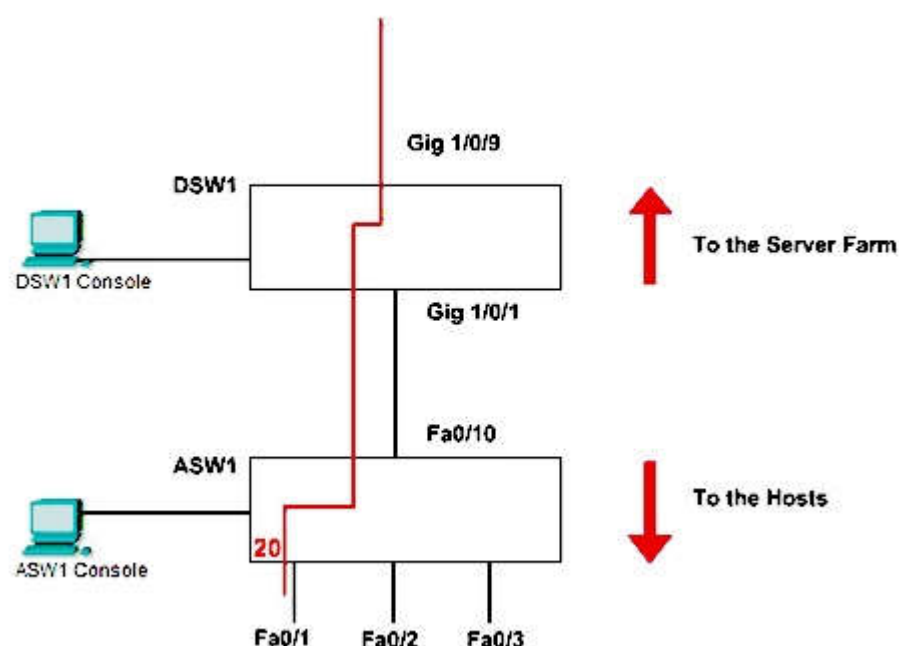
## QUESTION 227 SIMULATION

SWITCH.com is an IT company that has an existing enterprise network comprised of two layer 2 only switches; DSW1 and ASW1. The topology diagram indicates their layer 2 mapping. VLAN 20 is a new VLAN that will be used to provide the shipping personnel access to the server. Corporate policies do not allow layer 3 functionality to be enabled on the switches. For security reasons, it is necessary to restrict access to VLAN 20 in the following manner:

- Users connecting to VLAN 20 via port f0/1 on ASW1 must be authenticated before they are given access to the network. Authentication is to be done via a Radius server:
  - Radius server host: 172.120.40.46
  - Radius key: rad123
  - Authentication should be implemented as close to the host as possible.
- Devices on VLAN 20 are restricted to the subnet of 172.120.40.0/24.
  - Packets from devices in the subnet of 172.120.40.0/24 should be allowed on VLAN 20.
  - Packets from devices in any other address range should be dropped on VLAN 20.
  - Filtering should be implemented as close to the server farm as possible.

The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers. You must use the available IOS switch features.

Note: Named access list is not supported.





**Correct Answer:** See the explanation below

**Section:** Infrastructure Security

**Explanation**

**Explanation/Reference:**

Step1: Console to ASW1 from PC console 1

```
ASW1(config)#aaa new-model
```

```
ASW1(config)#radius-server host 172.120.39.46 key rad123
```

```
ASW1(config)#aaa authentication dot1x default group radius
```

```
ASW1(config)#dot1x system-auth-control
```

```
ASW1(config)#inter fastEthernet 0/1
```

```
ASW1(config-if)#switchport mode access
```

```
ASW1(config-if)#dot1x port-control auto
```

```
ASW1(config-if)#exit
```

```
ASW1#copy run start
```

Step2: Console to DSW1 from PC console 2

```
DSW1(config)#ip access-list standard 10
```

```
DSW1(config-ext-nacl)#permit 172.120.40.0 0.0.0.255
```

```
DSW1(config-ext-nacl)#exit
```

```
DSW1(config)#vlan access-map PASS 10
```

```
DSW1(config-access-map)#match ip address 10
```

```
DSW1(config-access-map)#action forward
```

```
DSW1(config-access-map)#exit
```

```
DSW1(config)#vlan access-map PASS 20
```

```
DSW1(config-access-map)#action drop
```

```
DSW1(config-access-map)#exit
```

```
DSW1(config)#vlan filter PASS vlan-list 20
```

```
DSW1#copy run start
```

#### QUESTION 228

Which keyword must you use with the **storm-control** command to set both upper and lower thresholds for unicast, multicast, and broadcast traffic?

- A. **limit**
- B. **pps**
- C. **set**
- D. **level**

**Correct Answer:** D

**Section:** Infrastructure Security

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.html>

#### QUESTION 229

You want a device to use the local user database if the TACACS+ server is unreachable. Which AAA login authentication command must you configure?

- A. **aaa authentication login default group local tacacs+**
- B. **aaa authentication login default group tacacs+ local**
- C. **aaa authentication login default group local**
- D. **aaa authentication login TACACS group tacacs+ local**

**Correct Answer:** B

**Section:** Infrastructure Security

**Explanation**

**Explanation/Reference:**

#### QUESTION 230

DRAG DROP

Drag and drop the statements about remote security databases from the left onto the correct security database types on the right:

**Select and Place:**

- Encryption is performed only on the password component of the packet.
- Encryption is performed on the entire packet.
- Processes authentication and authorization functions together.
- Processes each AAA function separately.

**TACACS+**

**RADIUS**

Correct Answer:

**TACACS+**

Encryption is performed on the entire packet.

Processes each AAA function separately.

**RADIUS**

Encryption is performed only on the password component of the packet.

Processes authentication and authorization functions together.

**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

- QUESTION 231**  
 Which information in a RADIUS access-request packet is encrypted?
- A. entire header
  - B. username and password
  - C. entire payload
  - D. password

**Correct Answer: D**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**  
 Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

- QUESTION 232**  
 Which three characteristics of AAA with TACACS+ are true? (Choose three.)
- A. It runs on TCP port 49.
  - B. It uses a client-private cloud architecture.
  - C. It is a Cisco-proprietary implementation.
  - D. It is a standards-based implementation.
  - E. It runs on UDP port 49.
  - F. It uses a client-server architecture.

**Correct Answer: ACF**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**

**QUESTION 233**

Which AAA authorization type applies security policies on a per-user basis?

- A. EXEC
- B. command
- C. auth-proxy
- D. network

**Correct Answer: D**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/ios/12\\_2/security/configuration/guide/fsecu\\_c/scfathor.html](https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecu_c/scfathor.html)

#### QUESTION 234

Which command maximizes system resources for ACLs?

- A. **sdm prefer default**
- B. **sdm prefer routing**
- C. **sdm prefer vlan**
- D. **sdm prefer access**

**Correct Answer: D**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Reference: [http://www3.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/15-2\\_1\\_e/configuration/guide/scg3750x/swsdm.pdf](http://www3.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_1_e/configuration/guide/scg3750x/swsdm.pdf)  
page 6

#### QUESTION 235

Which two accounting types does AAA support? (Choose two.)

- A. connection
- B. privilege
- C. authorization
- D. authentication
- E. system

**Correct Answer: AE**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_usr\\_aaa/configuration/xr-3s/sec-usr-aaa-xr-3s-book/sec-cfg-accountg.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/xr-3s/sec-usr-aaa-xr-3s-book/sec-cfg-accountg.html)

#### QUESTION 236

What command disables 802.1x authentication on a port and permits traffic without authentication?

- A. dot1x port-control disable
- B. dot1x port-control force-unauthorized
- C. dot1x port-control auto
- D. dot1x port-control force-authorized

**Correct Answer: D**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

The command dot1x port-control force-authorized is used to disable 802.1x on a port and permit traffic without authentication. Dot1x ports are in one of two states, authorized or unauthorized. Authorized ports permit user traffic to flow through the port. This state usually follows successful authentication. Unauthorized ports only permit authorization traffic to flow through the port. Usually a port begins in the unauthorized state. A user is then allowed to exchange AAA authentication traffic with the port. Once the user has been authenticated successfully, the port is changed to the authorized state and the user is permitted to use the port normally.

Normal use of 802.1x has the port configured with the dot1x port-control auto statement. This places the port in the unauthorized state until successful authentication. After successful authentication, the port is changed to the authorized state.

When 802.1x is initially configured, the default port control of the ports is force-authorized. This forces the port to be in the authorized state without successful authentication. This setting disables the need for authentication and permits all traffic.

The force-unauthorized keyword configures the port as an unauthorized port regardless of authentication traffic. A port configured with this key word would not permit user traffic, not even authentication traffic.

The command dot1x port-control disable is not a valid command due to incorrect syntax.

Objective:

Infrastructure Security

Sub-Objective:

Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

References:

Cisco > Catalyst 6500 Series Release 15.0SY Software Configuration Guide > Security > IEEE 802.1X Port-Based Authentication

Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > dot1x port-control



Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > dot1x port-control

#### QUESTION 237

What attack technique can be used to force user traffic through an attacking device, causing a man-in-the-middle attack?

- A. VLAN hopping
- B. DHCP spoofing
- C. Rogue device
- D. MAC flooding

**Correct Answer: B**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

DHCP spoofing is an attack that can be used to force user traffic through an attacking device. This is accomplished by an attacker responding to DHCP queries from users. Eliminating the response from the correct DHCP server would make this more effective, but if the attacker's response gets to the client first, the client will accept it. The DHCP response from the attacker will include a different gateway or DNS server address. If they define a different gateway, the user traffic will be forced to travel through a device controlled by the attacker. This will allow the attacker to capture traffic and gain company information. If the attacker changes the DNS server in the response, they can use their own DNS server to force traffic to selected hosts to go to a device they control. Again, this would allow the attacker to capture traffic and gain information.

VLAN hopping is an attack that allows an attacker to access network resources on a different VLAN without passing through a router. The attacker can create a packet with two VLAN headers on it and send it to a switch. The switch port will strip off the first header and leave the second. The second header will be seen as the originating VLAN allowing the attacker access to a VLAN they are not connected to. This becomes a security concern because this hopping can be accomplished without passing through a router and its security access lists. For this reason, private VLANs and VACLs should be used to secure access between VLANs.

MAC flooding is an attack technique which attempts to fill a switch table so the attacker can capture flooded traffic sent from the switch. The concept of this attack is to use the CAM table limit to the attacker's advantage. The attacker would send packets addressed from a large number of MAC addresses to the switch. The switch adds the source MAC address to the MAC address table. Eventually no more MAC addresses can be added because the table is full. When this occurs, any packets destined for a MAC address not in the table will be flooded to all other ports. This would allow the attacker to see the flooded traffic and capture information. The switch would be essentially functioning as a hub in this case.

A rogue device is a device attached to the network that is not under the control of the organization. This term is normally used to mean a wireless device, perhaps an access point that is not operating as a part of the company's infrastructure. Employees may bring their own access points and connect them to the network so they can use their computer wirelessly. This creates a security gap since the device is probably not secured to protect the traffic. An attacker could connect a rogue access point to a company's network and capture traffic from outside the company's premises.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > Cisco Catalyst 6500 Series Switches > VLAN Security White Paper

#### QUESTION 238

Which Catalyst 6500 feature provides network-security enforcement based on Layer 2, Layer 3, and Layer 4 information on a VLAN?

- A. NAM
- B. SPAN
- C. VACL
- D. 802.1X

**Correct Answer: C**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

VLAN access control lists (VACLs) provide network-security enforcement based on Layer 2, Layer 3, and Layer 4 information on a VLAN.

VACLs can be used to provide security based on MAC address, source and destination IP address, Layer 4 protocols, or port numbers. The VACL will act on all traffic of a select VLAN whether bridged or switched. The actions performed on a packet can include permit, redirect, or deny. The VACL entries are checked in sequence, which is similar in concept to route-map structures. The following procedure is used to create VACLs:

Define a VLAN access map:

```
switch(config)# vlan access-map name [seq#]
```

Configure a match clause:

```
switch(config-access-map)# match {ip address {1-99 | 1300-2699 | acl_name} | mac address acl_name}
```

Configure an action clause:

```
switch(config-access-map)# action {drop | forward | redirect}
```

Apply the map to a VLAN:

```
switch(config)# vlan filter map_name vlan-list list
```

Once created, you should verify the VACLs using the following commands:

```
switch# show vlan access-map map_name
```

```
switch# show vlan filter
```

In the sample configuration shown below, all VLAN traffic in VLANs 1 through 3 that match access list SAFE will be forwarded. All other traffic will be dropped.

```
switch(config)# vlan access-map cisco 10
switch(config-access-map)# match ip-address SAFE
switch(config-access-map)# action forward
switch(config)# vlan filter cisco vlan-list 1-3
```

If access list cisco were configured as shown below, for example, traffic with a source address of 172.16.10.8 would be dropped.

```
Switch# show ip access-list cisco 10
Extended ip access list cisco 10
10 permit 10.0.0.0 255.255.255.0 any
```

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists  
Cisco > Cisco IOS LAN Switching Command Reference > vlan access-map  
Cisco > Cisco IOS LAN Switching Command Reference > match (vlan access-map)

### QUESTION 239

In the following partial output of the show run command, which MAC address or addresses will be removed from the list of secure addresses after 240 seconds?

```
<output omitted>

interface FastEthernet0/1
    switchport mode access
    switchport port-security
    switchport port-security maximum 10
    switchport port-security aging time 4
    switchport port-security aging static
    switchport port-security mac-address sticky
    switchport port-security mac-address 0000.0000.aaaa
    switchport port security mac-address sticky 0000.0000.bbbb
```

- A. 0000.0000.aaaa
- B. 0000.0000.bbbb
- C. 0000.0000.aaaa and 0000.0000.bbbb
- D. none of the MAC addresses will be removed after 240 seconds

**Correct Answer: A**  
**Section: Infrastructure Security**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The only address that will be removed or aged out of the secure MAC address list will be 0000.0000.aaaa. When port security is used on an interface, not only can you set a maximum number of MAC addresses that can use the interface, but you can also set the amount of time that an address can reside in the secure list.

When the switchport port-security command is used, you can specify whether the command applies to statically assigned MAC addresses or dynamically learned MAC addresses, called sticky addresses. In this scenario, line 6 of the output specifies that the command applies to static addresses. Since 0000.0000.aaaa is the only statically assigned MAC address (assigned in line 8 of the output), it is the only address that will age out. The amount of time is configured in terms of minutes and is done on line 5 with the switchport port-security aging time 4 command.

The MAC address 0000.0000.bbbb will not age out because it is a sticky secure address. The aging command only applies to static MAC addresses.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA > Configuring Port Security  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport port-security

### QUESTION 240

You are the network administrator in your company. You have executed the following commands on the Fa0/1 interface of a switch named swtA:

```
swtA(config)# interface Fa0/1
swtA(config-if)# switchport mode access
swtA(config-if)# switchport port-security
swtA(config-if)# switchport port-security maximum 4
swtA(config-if)# switchport port-security mac-address sticky
swtA(config-if)# switchport port-security mac-address 1111.1111.1111
swtA(config-if)# switchport port-security mac-address 3333.3333.3333
swtA(config-if)# exit
```

Over a period of time, different hosts are connected to the Fa0/1 switch port of swtA. The MAC addresses of the hosts that were connected to the Fa0/1 port and the order in which they connected are as follows:

```
1111.1111.1111
2222.2222.2222
4444.4444.4444
5555.5555.5555
3333.3333.3333
```

After a few days, you notice that the Fa0/1 port is in the shutdown state.

Which of the following MAC addresses causes the Fa0/1 port to shut down?

- A. 2222.2222.2222
- B. 3333.3333.3333
- C. 4444.4444.4444
- D. 5555.5555.5555

**Correct Answer: D**

**Section: Infrastructure Security**

**Explanation**

**Explanation/Reference:**

Explanation:

The MAC address 5555.5555.5555 caused the Fa0/1 port to shut down because it violates the port security enabled on the port. The switchport port-security maximum 4 command allows at most four MAC addresses or hosts to be connected to the Fa0/1 switch port. Two secure MAC addresses, 1111.1111.1111 and 3333.3333.3333, are statically configured on the Fa0/1 port by using the switchport port-security mac-address command. This implies that these two MAC addresses are allowed to be connected to the Fa0/1 port.

The switchport port-security mac-address sticky command enables sticky learning of MAC addresses on the Fa0/1 port. With sticky learning, the dynamically learned MAC addresses are stuck to the port. The first MAC address that is connected to the port becomes the sticky secure address. In this case, 1111.1111.1111 and 3333.3333.3333 MAC addresses are statically configured as secure addresses. This implies that there can be at most two sticky secure MAC addresses for Fa0/1. The hosts w

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Catalyst 6500 Series Release 15.0SY Software Configuration Guide > Security > Port Security

Cisco IOS Security Command Reference > show vlan group Through switchport port-security violation > switchport port-security mac-address

Cisco IOS Security Command Reference > show parameter-map type consent Through show users > show port-security

#### QUESTION 241

Which configuration command ties the router hot standby priority to the availability of its interfaces?

- A. standby group
- B. standby priority
- C. backup interface
- D. standby track

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The standby track interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/blades/3040/software/release/12-2\\_44\\_se/configuration/guide/swhsrp.html](https://www.cisco.com/c/en/us/td/docs/switches/blades/3040/software/release/12-2_44_se/configuration/guide/swhsrp.html)

#### QUESTION 242

What is the default HSRP priority?

- A. 50
- B. 100
- C. 120
- D. 1024

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

|                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>standby</b> [ <i>group-number</i> ] <b>priority</b> priority<br>[ <b>preempt</b> [ <i>delay</i> <i>delay</i> ]] | <p>Set a <b>priority</b> value used in choosing the active router. The range is 1 to 255; <b>the default priority is 100</b>. The highest number represents the highest priority.</p> <ul style="list-style-type: none"> <li>• (Optional) <i>group-number</i>—The group number to which the command applies.</li> <li>• (Optional) <b>preempt</b>—Select so that when the local router has a higher priority than the active router, it assumes control as the active router.</li> <li>• (Optional) <b>delay</b>—Set to cause the local router to postpone taking over the active role for the shown number of seconds. The range is 0 to 36000 (1 hour); the default is 0 (no delay before taking over).</li> </ul> <p>Use the <b>no</b> form of the command to restore the default values.</p> |
|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/ blades/3040/software/release/12-2\\_44\\_se/configuration/guide/swhsrp.html](https://www.cisco.com/c/en/us/td/docs/switches/ blades/3040/software/release/12-2_44_se/configuration/guide/swhsrp.html)

#### QUESTION 243

Which option is a benefit of using VSS?

- A. reduces cost
- B. simplifies configuration
- C. provides two independent supervisors with two different control planes
- D. removes the need for a First Hop Redundancy Protocol

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation: First Hop Redundancy Protocols (FHRPs) such as VRRP and HSRP were designed to allow for a highly available first IP route hop for host systems. FHRPs allow two (or more) distinct routers to share a common IP address providing a redundant Layer-3 default gateway for end nodes. The VSS system creates a single logical router at Layer 3. This VSS routing instance fulfills this first-hop role without the need for a dedicated protocol. The VSS IP route is highly available due to MEC and the resiliency of the VSS system. VSS eliminates the need for FHRP at the aggregation layer of the data center.

Reference: [http://www.cisco.com/en/US/docs/solutions/Enterprise/Data\\_Center/vssdc\\_integrate.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/vssdc_integrate.html)

#### QUESTION 244

Which First Hop Redundancy Protocol is an IEEE Standard?

- A. GLBP
- B. HSRP
- C. VRRP
- D. OSPF

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

A comparison of the three First Hop Redundancy Protocols are listed below:



| Protocol Features            |                   | HSRP<br>(Hot Standby Router protocol)                                                                              | VRRP<br>(Virtual Redundancy Router Protocol)                                                                       | GLBP<br>(Gateway Load Balancing Protocol)                                                                                                                                         |
|------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router role                  |                   | - 1 active router.- 1 standby router.- 1 or more listening routers.                                                | - 1 master router.- 1 or more backup routers.                                                                      | - 1 AVG (Active Virtual Gateway).- up to 4 AVF routers on the group (Active Virtual Forwarder) passing traffic.- up to 1024 virtual routers (GLBP groups) per physical interface. |
|                              |                   | - Use virtual ip address.                                                                                          | - Can use real router ip address, if not, the one with highest priority become master.                             | - Use virtual ip address.                                                                                                                                                         |
| Scope                        |                   | Cisco proprietary                                                                                                  | IEEE standard                                                                                                      | Cisco proprietary                                                                                                                                                                 |
| Election                     |                   | Active Router:<br>1-Highest Priority<br>2-Highest IP (tiebreaker)                                                  | Master Router: (*)<br>1-Highest Priority<br>2-Highest IP (tiebreaker)                                              | Active Virtual Gateway:<br>1-Highest Priority<br>2-Highest IP (tiebreaker)                                                                                                        |
| Optimization features        | Tracking          | yes                                                                                                                | yes                                                                                                                | yes                                                                                                                                                                               |
|                              | Preempt           | yes                                                                                                                | yes                                                                                                                | yes                                                                                                                                                                               |
|                              | Timer adjustments | yes                                                                                                                | yes                                                                                                                | yes                                                                                                                                                                               |
| Traffic type                 |                   | 224.0.0.2 – udp 1985 (version1)<br>224.0.0.102-udp 1985 (version2)                                                 | 224.0.0.18 – IP 112                                                                                                | 224.0.0.102 udp 3222                                                                                                                                                              |
| Timers                       |                   | Hello – 3 seconds                                                                                                  | Advertisement – 1 second                                                                                           | Hello – 3 seconds                                                                                                                                                                 |
|                              |                   | (Hold) 10 seconds                                                                                                  | (Master Down Interval)3 *<br>Advertisement + skew time<br>(Skew time)(256-priority) / 256                          | (Hold) 10 seconds                                                                                                                                                                 |
| Load-balancing functionality |                   | - Multiple HSRP group per interface/SVI/routed int.                                                                | - Multiple VRRP group per interface/SVI/routed int.                                                                | Load-balancing oriented- Weighted algorithm.- Host-dependent algorithm.<br>- Round-Robin algorithm (default).                                                                     |
|                              |                   | Requires appropriate distribution of Virtual GW IP per Clients for optimal load-balancing.(generally through DHCP) | Requires appropriate distribution of Virtual GW IP per Clients for optimal load-balancing.(generally through DHCP) | Clients are transparently updated with virtual MAC according to load-balancing algorithm through ARP requesting a unique virtual gateway.                                         |

Reference: <http://ccithebeginning.wordpress.com/2008/08/23/router-high-availability-protocol-comparison-2/>

#### QUESTION 245

What is the default amount by which the hot standby priority for the router is decremented or incremented when the interface goes down or comes back up?

- A. 1
- B. 5
- C. 10
- D. 15

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The standby track interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. **When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10.** If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/blades/3040/software/release/12-2\\_44\\_se/configuration/guide/swhsrp.html](https://www.cisco.com/c/en/us/td/docs/switches/blades/3040/software/release/12-2_44_se/configuration/guide/swhsrp.html)

#### QUESTION 246

What is the maximum number of virtual MAC addresses that GLBP allows per group?

- A. 2
- B. 4



- C. 6
- D. 8

**Correct Answer:** B  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**

Explanation:

**GLBP Virtual MAC Address Assignment**

A GLBP group allows up to four virtual MAC addresses per group. The AVG is responsible for assigning the virtual MAC addresses to each member of the group. Other group members request a virtual MAC address after they discover the AVG through hello messages. Gateways are assigned the next MAC address in sequence. A virtual forwarder that is assigned a virtual MAC address by the AVG is known as a primary virtual forwarder. Other members of the GLBP group learn the virtual MAC addresses from hello messages. A virtual forwarder that has learned the virtual MAC address is referred to as a secondary virtual forwarder.

Reference: [http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ft\\_glb.html#wp1039651](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glb.html#wp1039651)

**QUESTION 247**

Which gateway role is responsible for answering ARP requests for the virtual IP address in GLBP?

- A. active virtual forwarder
- B. active virtual router
- C. active virtual gateway
- D. designated router

**Correct Answer:** C  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**

Explanation:

**GLBP Active Virtual Gateway**

Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address.

**The AVG is responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address.** Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.

Reference: [http://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ft\\_glb.html](http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glb.html)

**QUESTION 248**

Which VRRP router is responsible for forwarding packets that are sent to the IP addresses of the virtual router?

- A. virtual router master
- B. virtual router backup
- C. virtual router active
- D. virtual router standby

**Correct Answer:** A  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**

Explanation:

VRRP Definitions

|                       |                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VRRP Router           | A router running the Virtual Router Redundancy Protocol. It may participate in one or more virtual routers.                                                                                                                                                                   |
| Virtual Router        | An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN. A VRRP Router may backup one or more virtual routers.                      |
| IP Address Owner      | The VRRP router that has the virtual router's IP address(es) as real interface address(es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, etc.                                            |
| Primary IP Address    | An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.                                     |
| Virtual Router Master | <b>The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses.</b> Note that if the IP address owner is available, then it will always become |

the Master.

Reference: <http://www.ietf.org/rfc/rfc3768.txt>

#### QUESTION 249

Which command correctly configures standby tracking for group 1 using the default decrement priority value?

- A. standby 1 track 100
- B. standby 1 track 100 decrement 1
- C. standby 1 track 100 decrement 5
- D. standby 1 track 100 decrement 20

**Correct Answer: A**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The default decrement value for HSRP standby tracking is 10. There is no need to explicitly state the value if the desired value is the default value.

#### QUESTION 250

Which command configures an HSRP group to become a slave of another HSRP group?

- A. standby slave
- B. standby group track
- C. standby follow
- D. standby group backup

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Perform this task to configure multiple HSRP client groups.

The “standby follow” command configures an HSRP group to become a slave of another HSRP group.

HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.

Reference: [http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp\\_fhrp/configuration/15-mt/fhrp-hsrp-mgo.html](http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhrp-hsrp-mgo.html)

#### QUESTION 251

Refer to the exhibit.

**%GLBP-4-DUPADDR: Duplicate address**

Which option describes the reason for this message in a GLBP configuration?

- A. Unavailable GLBP active forwarder
- B. Incorrect GLBP IP address
- C. HSRP configured on same interface as GLBP
- D. Layer 2 loop

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

This section provides information you can use to troubleshoot your configuration.

%GLBP-4-DUPADDR: Duplicate address

**The error message indicates a possible layer2 loop and STP configuration issues.**

In order to resolve this issue, issue the show interface command to verify the MAC address of the interface. If the MAC address of the interface is the same as the one reported in the error message, then it indicates that this router is receiving its own hello packets sent. Verify the spanning-tree topology and check if there is any layer2 loop. If the interface MAC address is different from the one reported in the error message, then some other device with a MAC address reports this error message.

Note: GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102 and User Datagram Protocol (UDP) port 3222 (source and destination). When configuring the multicast boundary command, permit the Multicast address by permit 224.0.0.0 15.255.255.255.

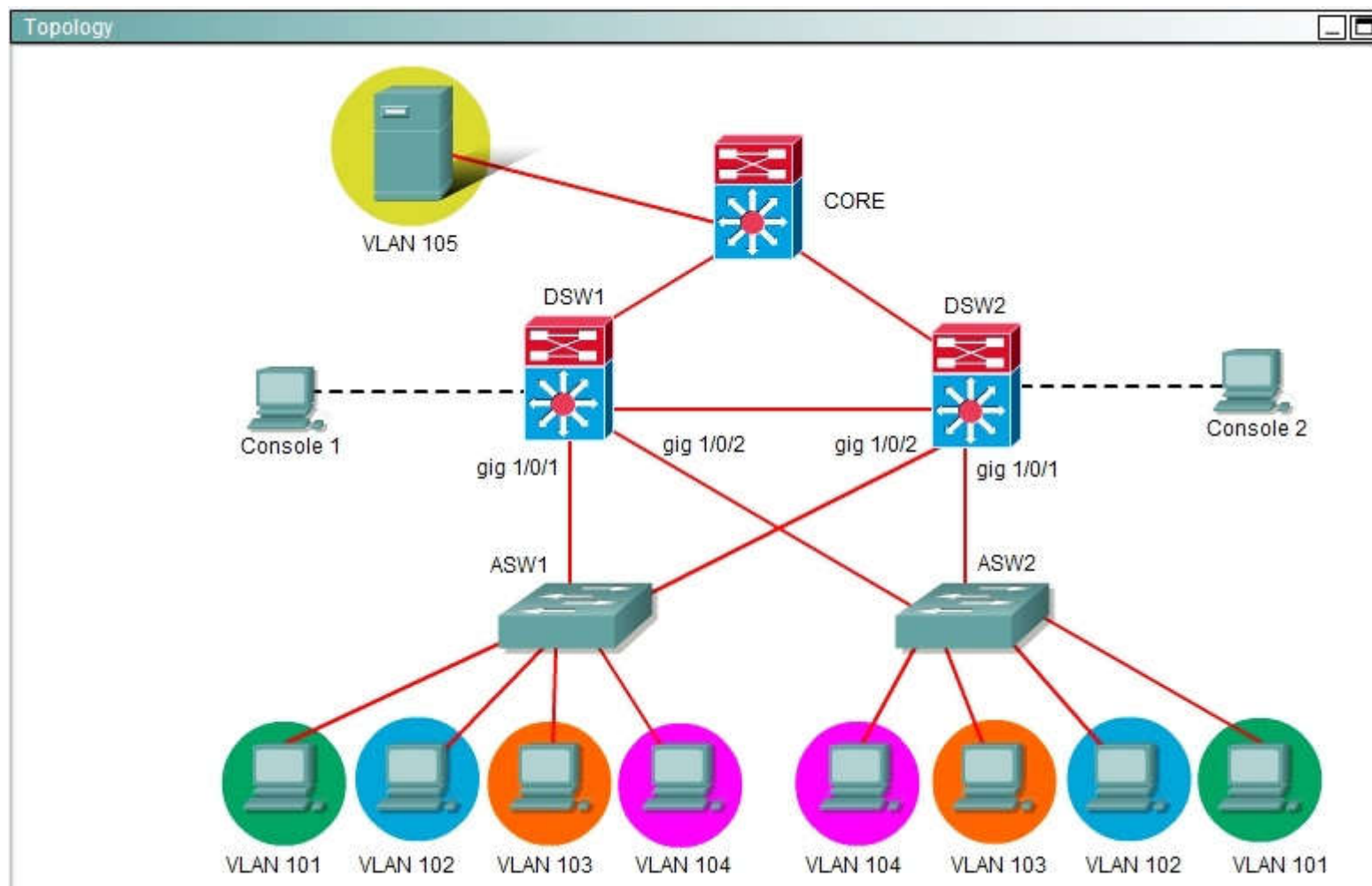
Reference: [http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_example09186a00807d2520.shtml#dr](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807d2520.shtml#dr)

#### QUESTION 252

ABC, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question.



Console 1

DSW1>

Console 2

DSW2>

During routine maintenance, GigabitEthernet1/0/1 on DSW1 was shut down. All other interfaces were up. DSW2 became the active HSRP device for VLAN 101 as desired. However, after GigabitEthernet1/0/1 on DSW1 was reactivated, DSW1 did not become the active router for VLAN 101 as desired. What

needs to be done to make the group for VLAN 101 function properly?

- A. Enable preempt in the VLAN 101 HSRP group on DSW1.
- B. Disable preempt in the VLAN 101 HSRP group on DSW2's.
- C. In the VLAN 101 HSRP group on DSW1, decrease the priority value to a value that is less than the priority value configured in the VLAN 101 HSRP group on DSW2.
- D. Decrease the decrement value in the track command for the VLAN 101 HSRP group on DSW1 to a value less than the value in the track command for the VLAN 101 HSRP group on DSW2.

**Correct Answer: A**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

```
interface Vlan101
ip address 192.168.101.1 255.255.255.0
standby 1 ip 192.168.101.254
standby 1 priority 200

standby 1 track GigabitEthernet1/0/1 55
```

```
interface Vlan101
ip address 192.168.101.2 255.255.255.0
standby 1 ip 192.168.101.254
standby 1 priority 150
standby 1 preempt
standby 1 track GigabitEthernet1/0/1
```

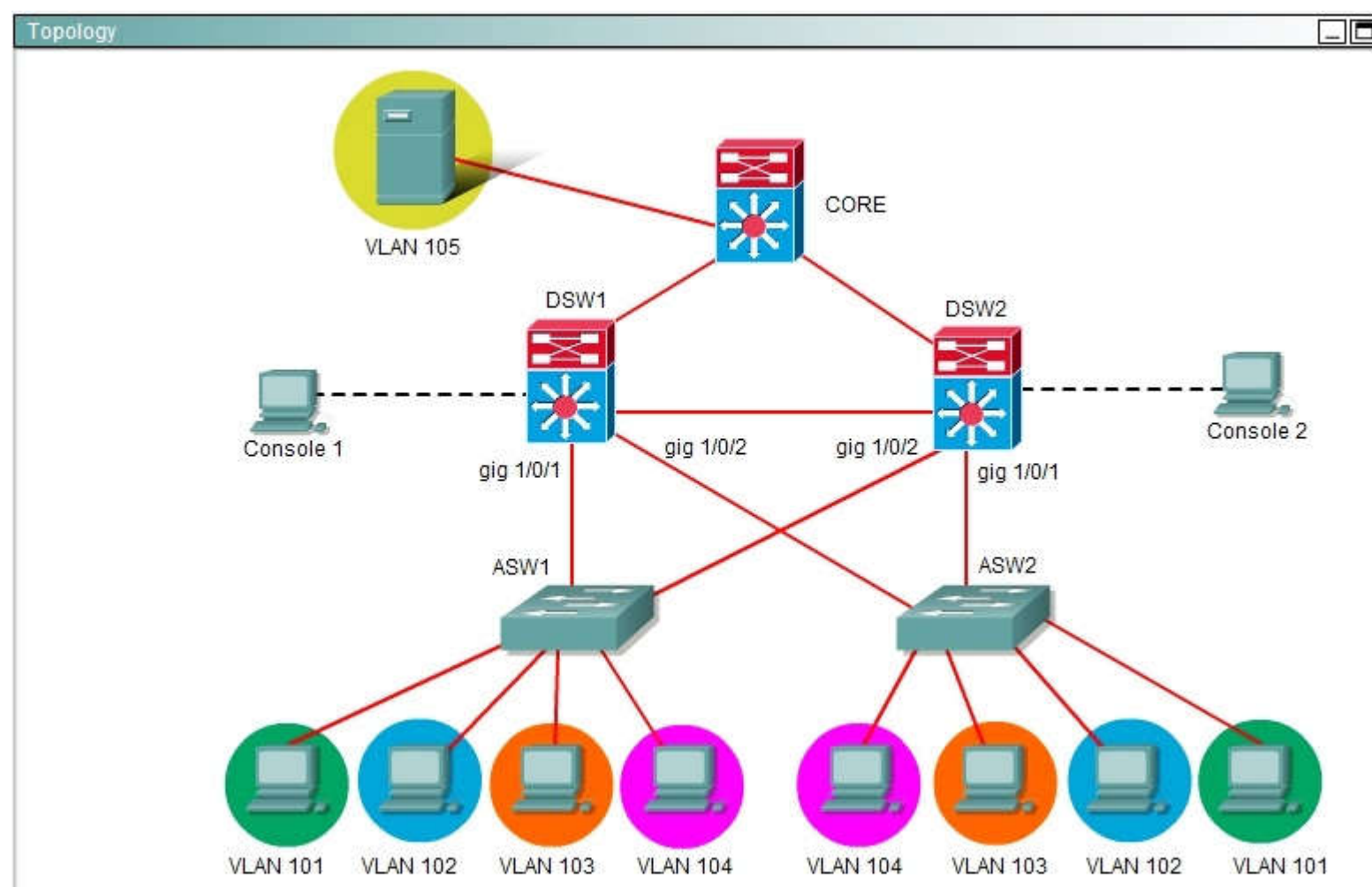
A is correct. All other answers are incorrect. Because Vlan101 on DSW1 ( left ) disable preempt. We need enable preempt to after it reactive, it will be active device. If not this command, it never become active device.

#### QUESTION 253

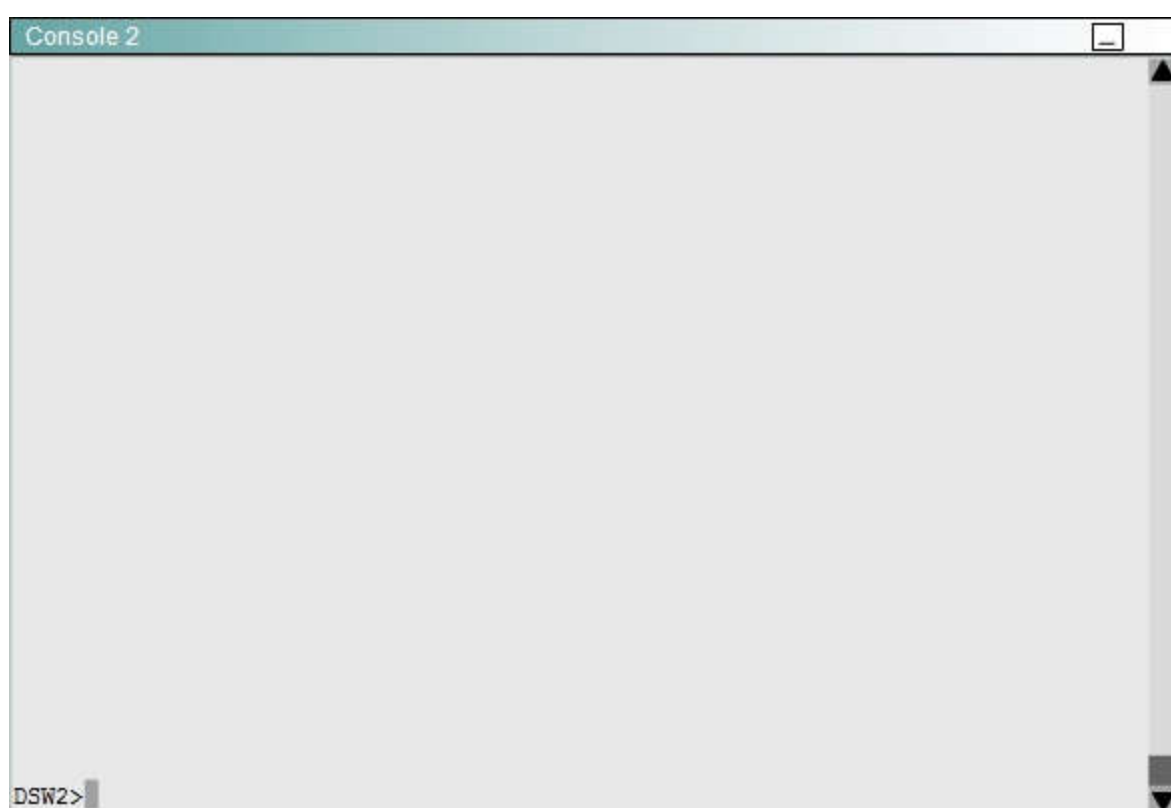
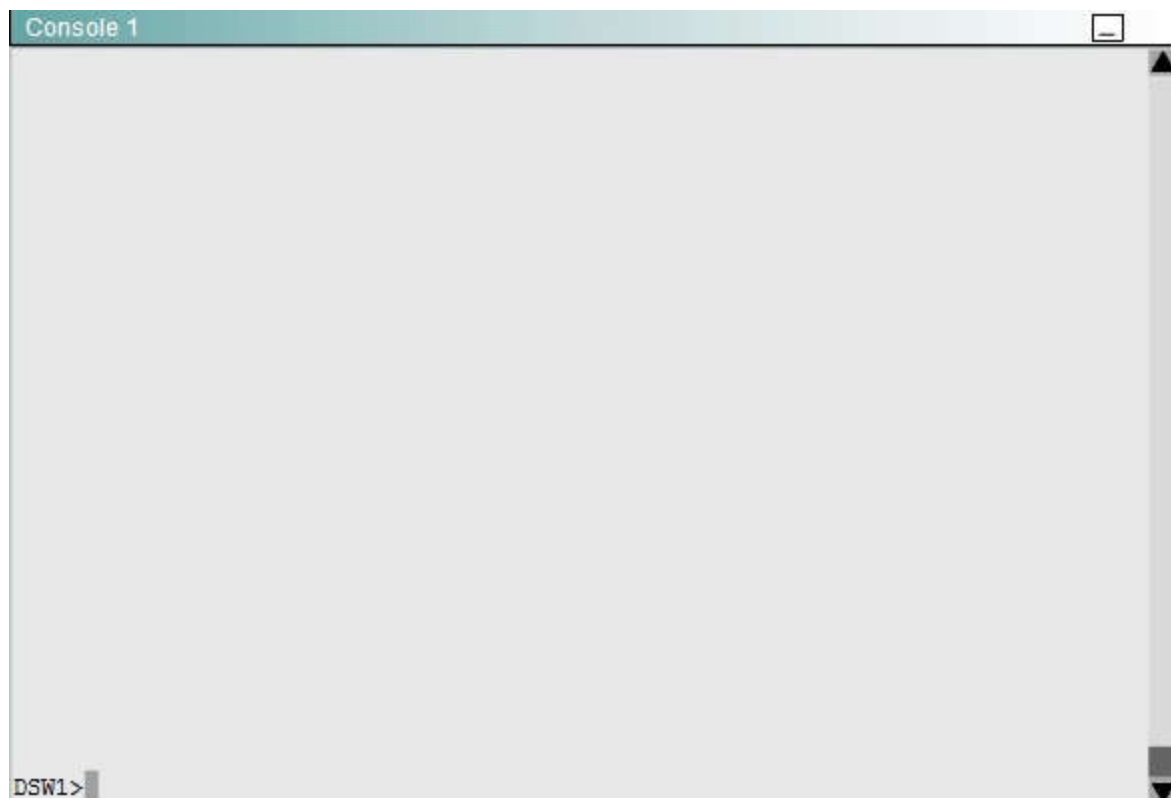
ABC, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question.







During routine maintenance, it became necessary to shut down the GigabitEthernet1/0/1 interface on DSW1. All other interfaces were up. During this time, DSW1 remained the active device for the VLAN 102 HSRP group. You have determined that there is an issue with the decrement value in the track command for the VLAN 102 HSRP group. What needs to be done to make the group function properly?

- A. The decrement value on DSW1 should be greater than 5 and less than 15.
- B. The decrement value on DSW1 should be greater than 9 and less than 15.
- C. The decrement value on DSW1 should be greater than 11 and less than 19.
- D. The decrement value on DSWTs should be greater than 190 and less than 200.
- E. The decrement value on DSWTs should be greater than 195 and less than 205.

**Correct Answer: C**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

|                                                                                                                                                                                  |                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface Vlan102 ip address 192.168.102.1 255.255.255.0 standby 2 ip 192.168.102.254 standby 2 priority 200 standby 2 preempt standby 2 track GigabitEthernet1/0/1 5</pre> | <pre>interface Vlan102 ip address 192.168.102.2 255.255.255.0 standby 2 ip 192.168.102.254 standby 2 priority 190 standby 2 preempt standby 2 track GigabitEthernet1/0/1</pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

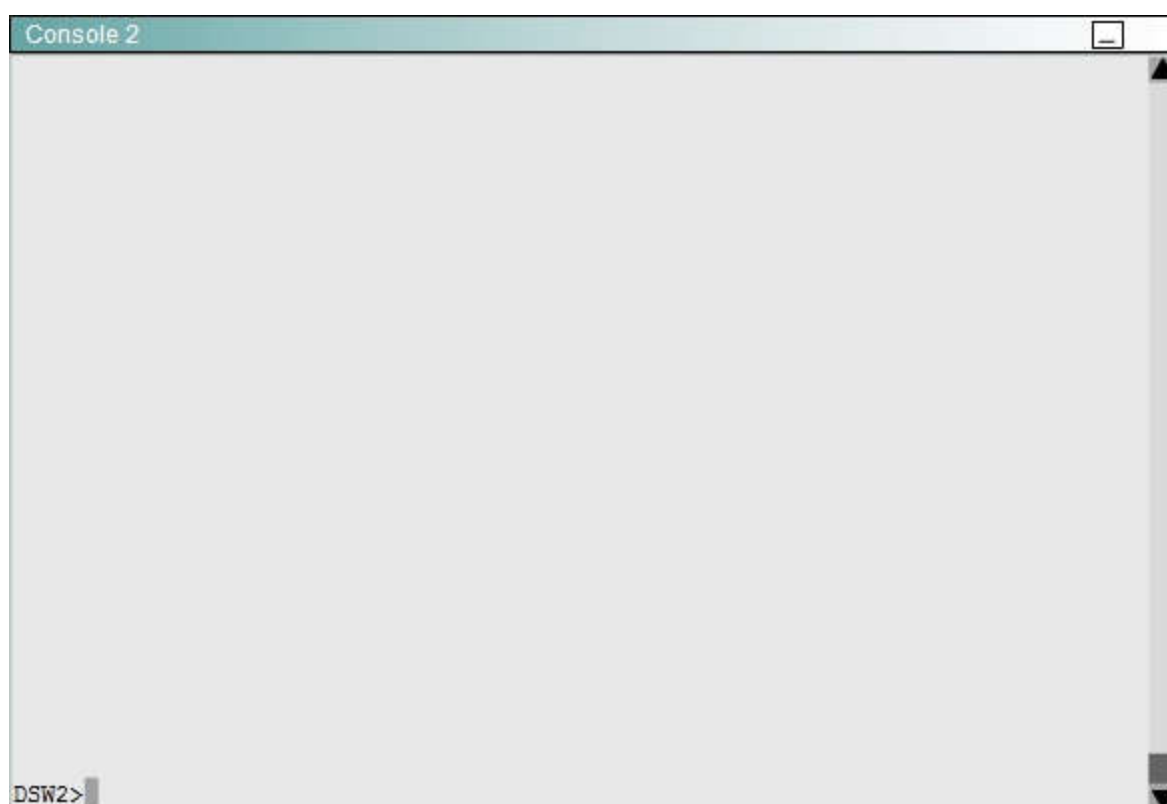
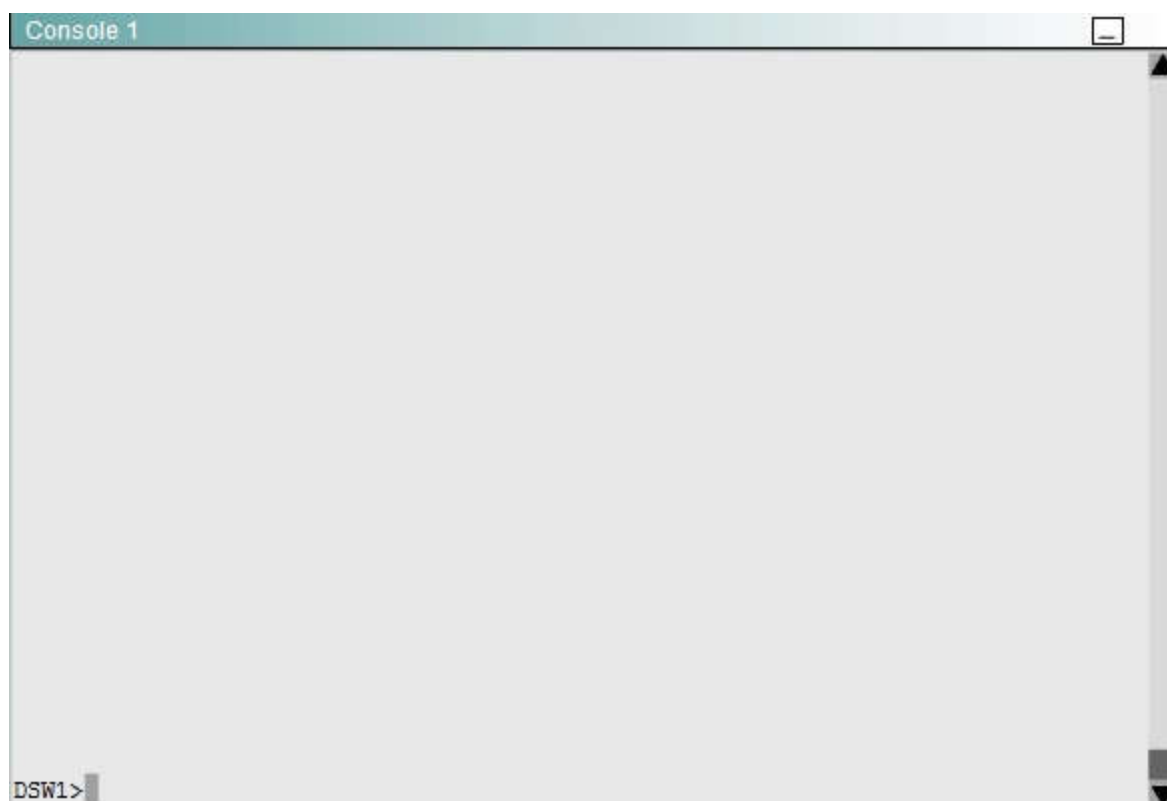
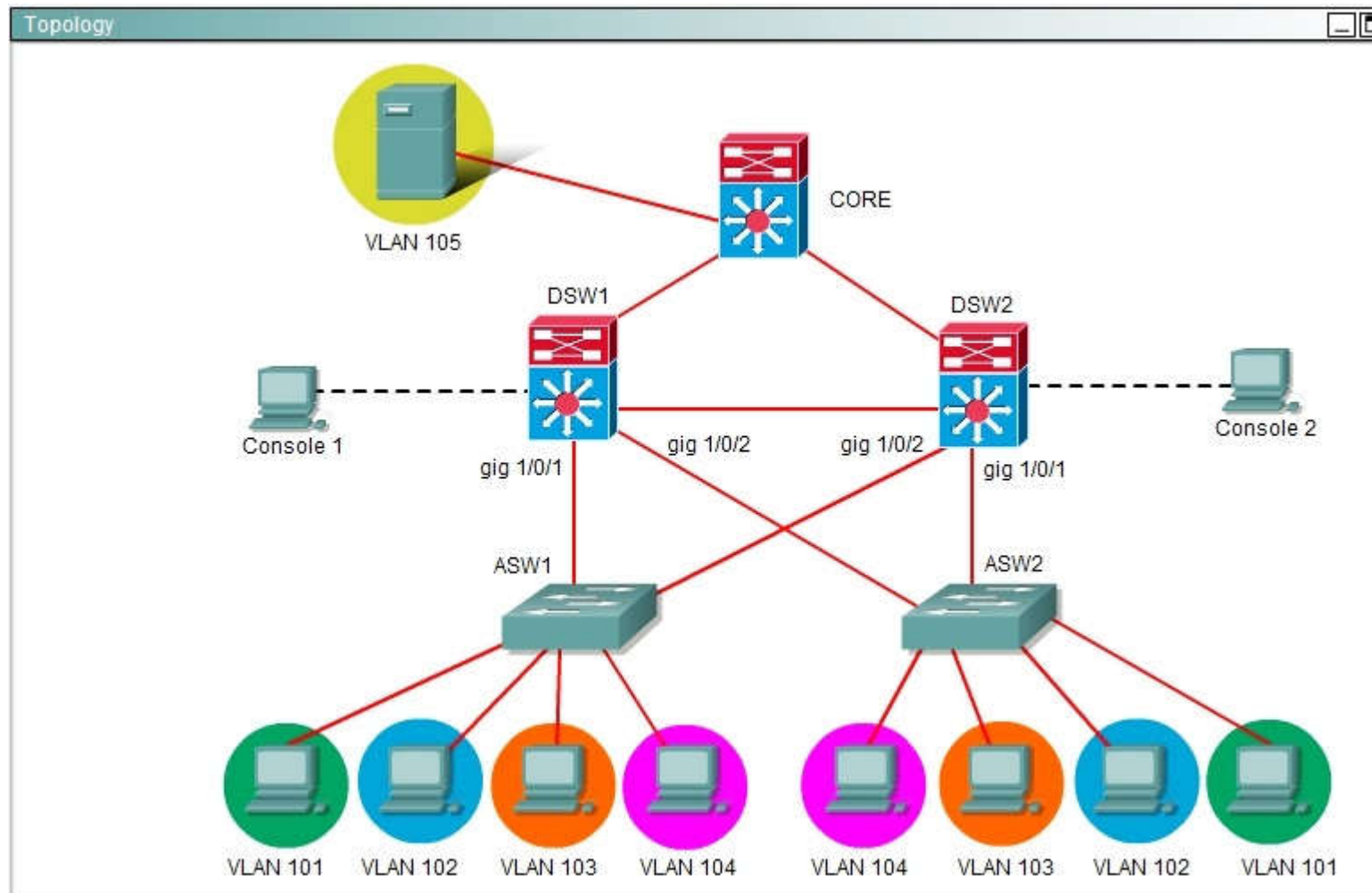
Use "show run" command to show. The left Vlan102 is console1 of DS1. Priority value is 200, we should decrement value in the track command from 11 to 18. Because  $200 - 11 = 189 < 190$  (priority of Vlan102 on DS2).

#### QUESTION 254

ABC, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question.



All interfaces are active. DSW2 has not become the active device for the VLAN 103 HSRP group. As related to the VLAN 103 HSRP group, what can be done to make the group function properly?

- A. On DSW1, disable preempt.
- B. On DSW1, decrease the priority value to a value less than 190 and greater than 150.
- C. On DSW2, increase the priority value to a value greater 200 and less than 250.
- D. On DSW2, increase the decrement value in the track command to a value greater than 10 and less than 50.

**Correct Answer:** C

**Section:** Infrastructure Services

**Explanation**

**Explanation/Reference:**

Explanation:

From the output shown below of the HSRP status of DSW2, we see that the active router has a priority of 200, while the local priority is 190. We need to increase the priority of DSW2 to greater than 200, but it should be less than 250 so that if the gig 1/0/1 interface goes down, DSW1 will become active. DSW2 is configured to decrement the priority by 50 if this interface goes down, so the correct answer is to increase the priority to more than 200, but less than 250.

#### Console 2

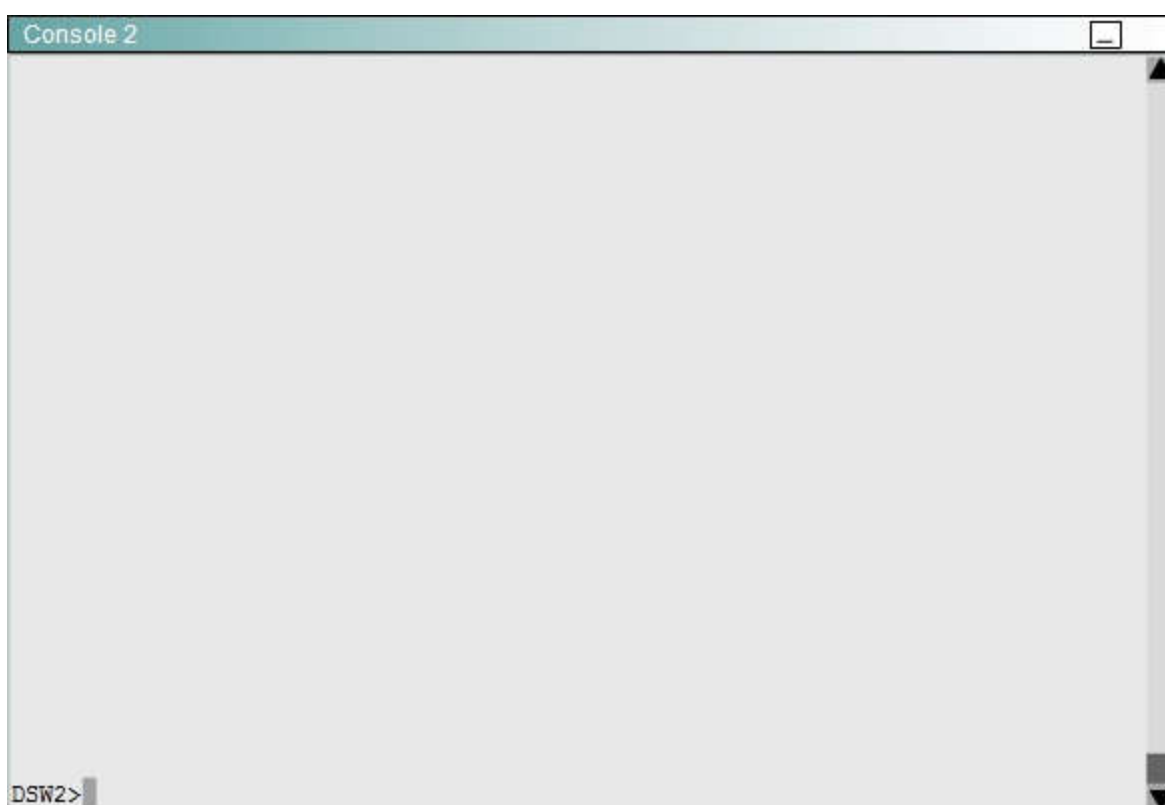
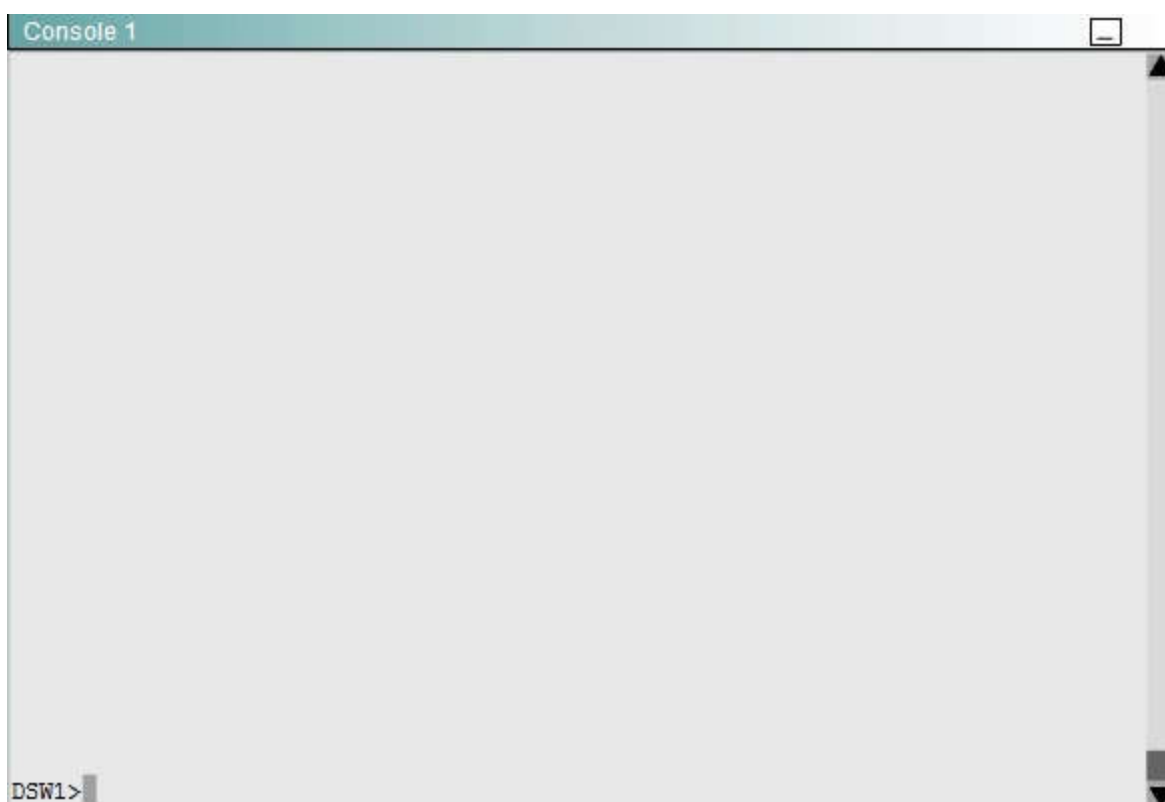
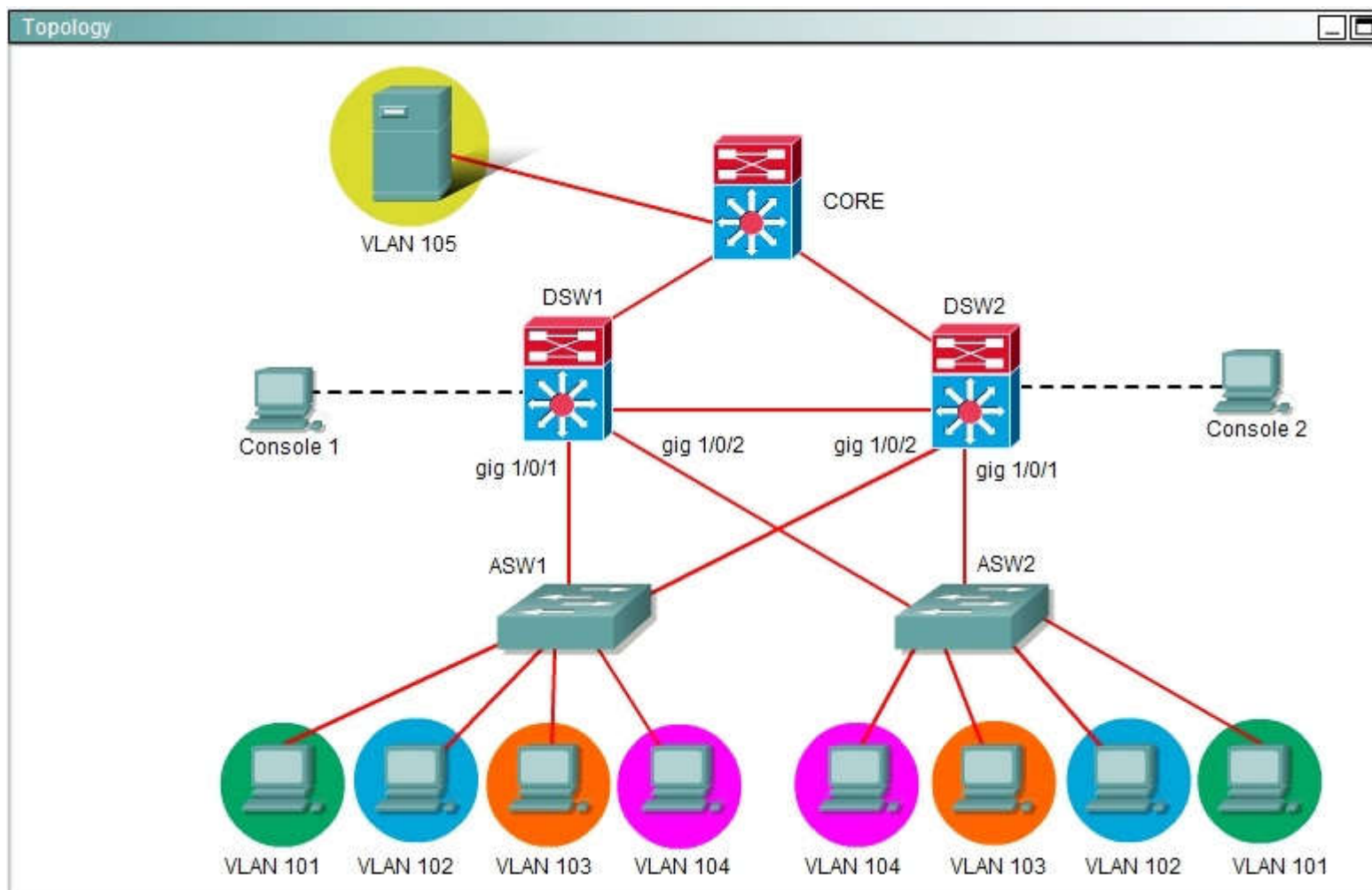
```
Standby router is local
Priority 190 (configured 190)
  Track interface GigabitEthernet1/0/1 state Up decrement 10
IP redundancy name is "hsrp-Vl102-2" (default)
Vlan103 - Group 3
State is Standby
  4 state changes, last state change 02:58:25
Virtual IP address is 192.168.103.254
Active virtual MAC address is 0000.0c07.ac03
  Local virtual MAC address is 0000.0c07.ac03 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 0.315 secs
Preemption enabled
Active router is 192.168.103.1, priority 200 (expires in 9.454 sec)
Standby router is local
Priority 190 (configured 190)
  Track interface GigabitEthernet1/0/1 state Up decrement 50
IP redundancy name is "hsrp-Vl103-3" (default)
```

#### QUESTION 255

ABC, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question.



During routine maintenance, it became necessary to shut down the GigabitEthernet1/0/1 interface on DSW1 and DSW2. All other interfaces were up. During this time, DSW1 became the active router for the VLAN 104HSRP group. As related to the VLAN 104HSRP group, what can be done to make the group



function properly?

- A. On DSW1, disable preempt.
- B. On DSW2 decrease the priority value to a value less than 150.
- C. On DSW1, increase the decrement value in the track command to a value greater than 6.
- D. On DSW1, decrease the decrement value in the track command to a value less than 1.

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

|                                                                                                                                                                                  |                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>interface Vlan104 ip address 192.168.104.1 255.255.255.0 standby 4 ip 192.168.104.254 standby 4 priority 150 standby 4 preempt standby 4 track GigabitEthernet1/0/1 1</pre> | <pre>interface Vlan104 ip address 192.168.104.2 255.255.255.0 standby 4 ip 192.168.104.254 standby 4 priority 200 standby 4 preempt standby 4 track GigabitEthernet1/0/1 55</pre> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

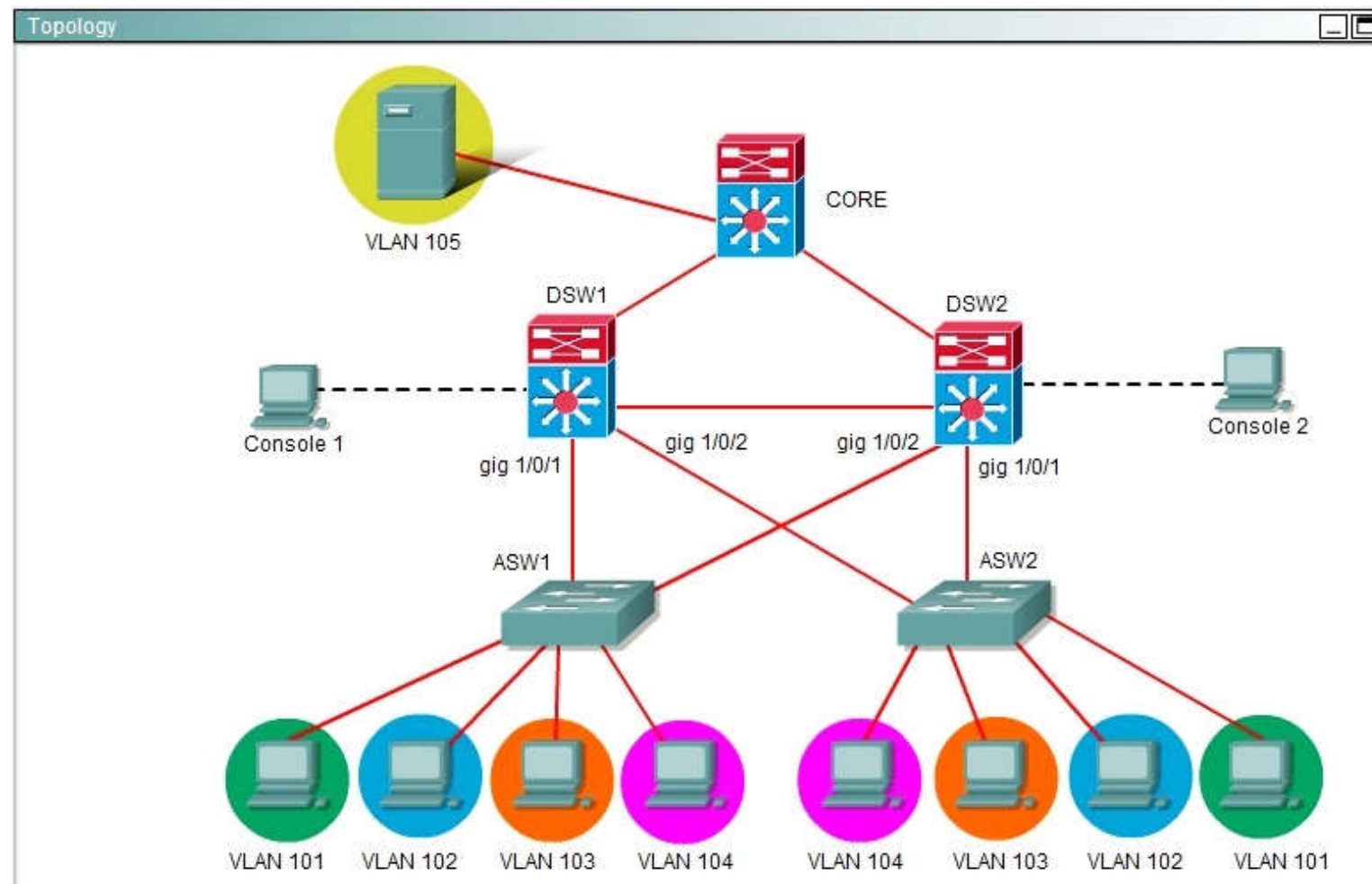
We should NOT disable preempt on DS1. By do that, you will make Vlan104's HSRP group fail function. Example: if we are disable preempt on DS1. It can not become active device when G1/0/1 on DS2 fail. In this question, G0/1/0 on DS1 & DS2 is shutdown. Vlan104 (left):  $150 - 1 = 149$ . Vlan104 (right):  $200 - 155 = 145$ . Result is priority  $149 > 145$  (Vlan104 on DS1 is active). If increase the decrement in the track value to a value greater than 6 ( $> \text{ or } = 6$ ). Vlan104 (left):  $150 - 6 = 144$ . Result is priority  $144 < 145$  (vlan104 on DS2 is active).

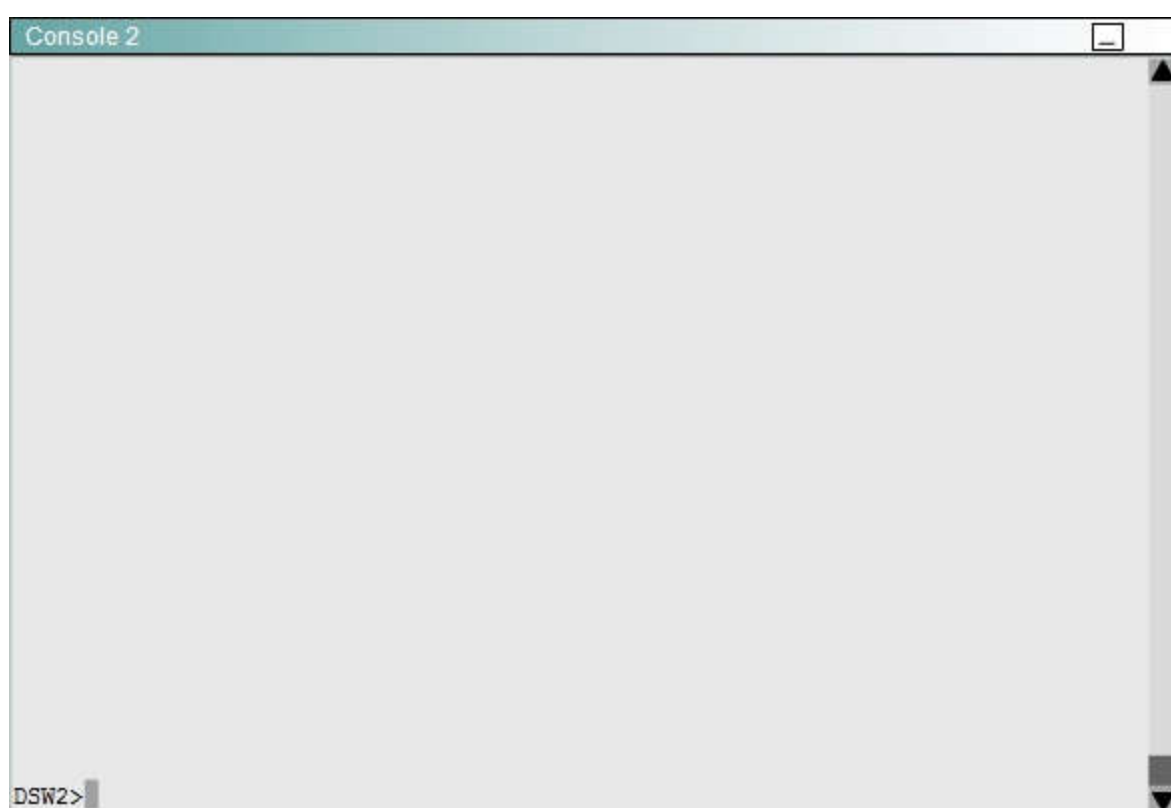
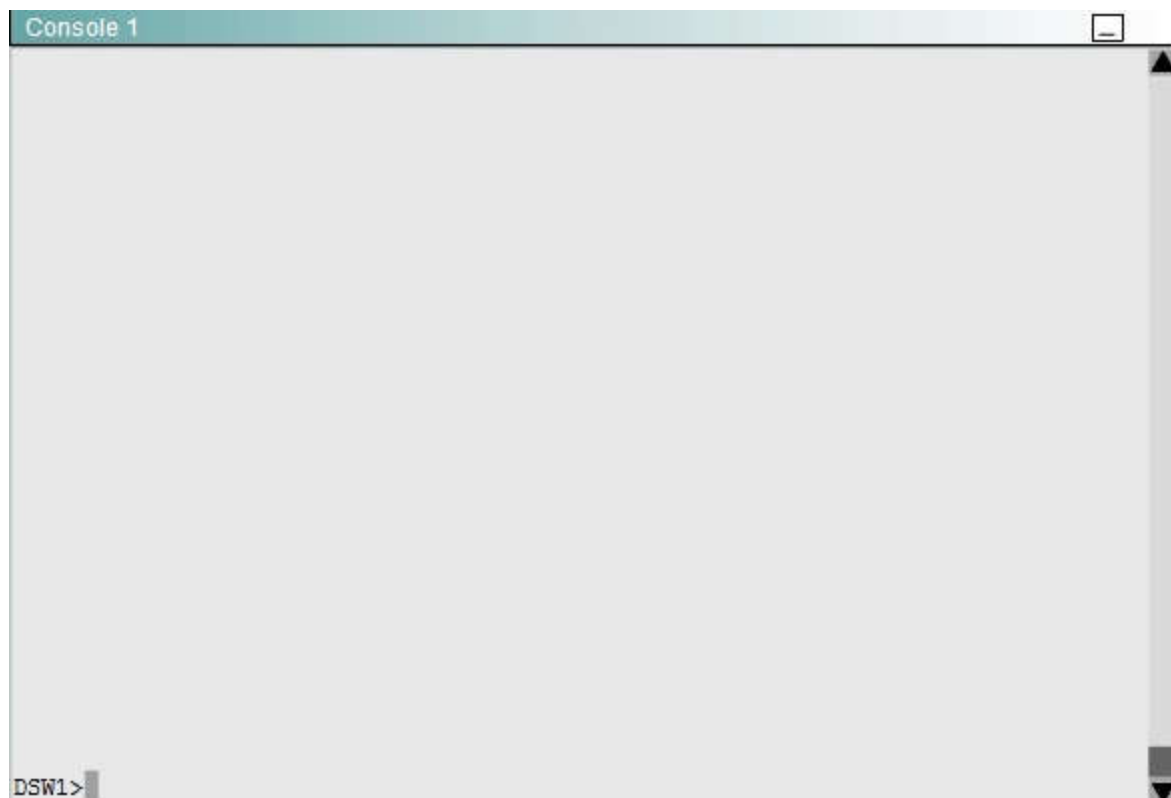
#### QUESTION 256

ABC, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question.





What is the priority value of the VLAN 105 HSRP group on DSW2?

- A. 50
- B. 100
- C. 150
- D. 200

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Use "show standby brief" command on console2. Very easy to see that the priority of Vlan105 is 150.

```
Vlan105 - Group 5
  State is Active
    9 state changes, last state change 02:53:04
  Virtual IP address is 192.168.105.254
  Active virtual MAC address is 0000.0c07.ac05
    Local virtual MAC address is 0000.0c07.ac05 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.685 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.105.2, priority 100 (expires in 8.406 sec)
Priority 150 (configured 150)
Track interface GigabitEthernet1/0/1 state Up decrement 55
  IP redundancy name is "harp-Vl105-5" (default)
```

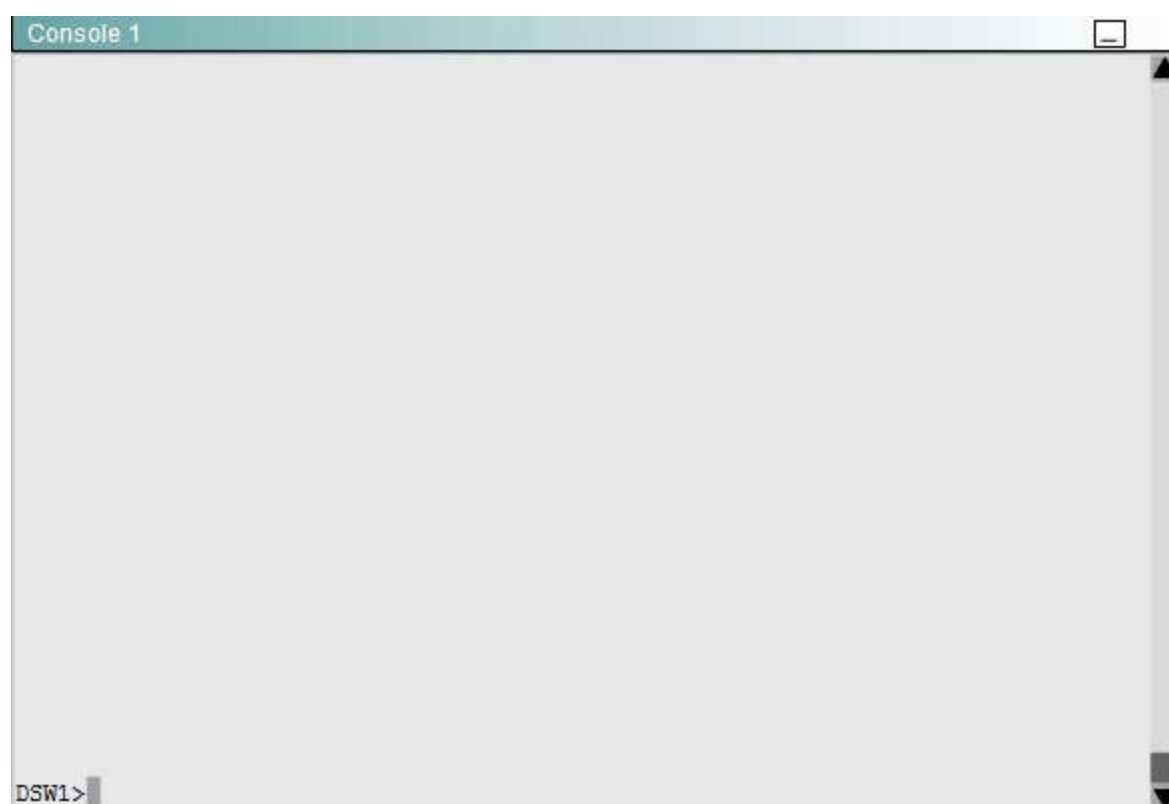
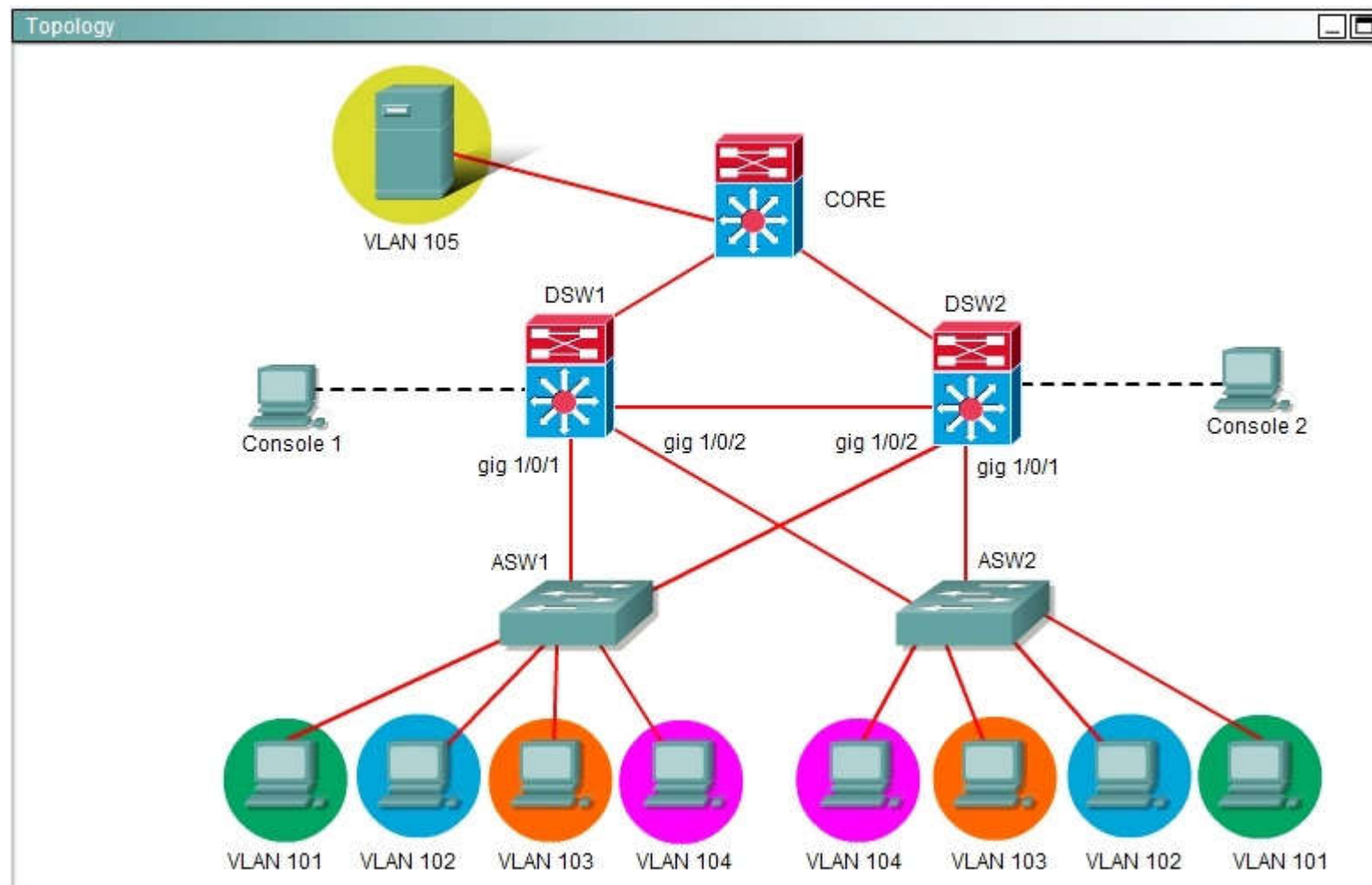
#### QUESTION 257

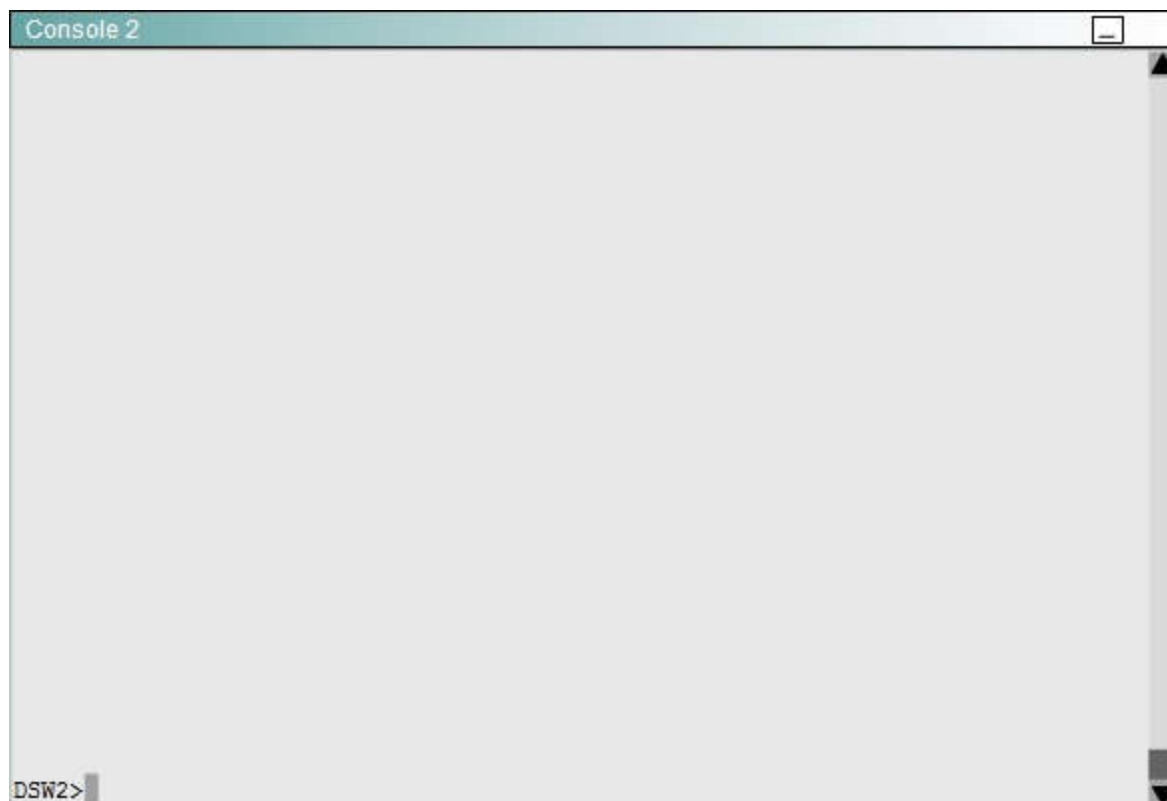
ABC, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRP to provide a high availability solution.

- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105

- D-W2 - primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthernet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question.





If GigabitEthernet1/0/1 on DSW2 is shutdown, what will be the resulting priority value of the VLAN 105 HSRP group on router DSW2?

- A. 90
- B. 100
- C. 150
- D. 200

**Correct Answer:** A

**Section:** Infrastructure Services

**Explanation**

**Explanation/Reference:**

Explanation

As seen below, the current priority for VLAN 105 is 100, and the tracking feature for Gig 1/0/0 is enabled which will decrement the priority by 10 if this interface goes down for a priority value of 90.

```
Vlan105 - Group 5
State is Standby
  10 state changes, last state change 02:54:51
Virtual IP address is 192.168.105.254
Active virtual MAC address is 0000.0c07.ac05
  Local virtual MAC address is 0000.0c07.ac05 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.516 secs
Preemption enabled
Active router is 192.168.105.1, priority 150 (expires in 7.786 sec)
Standby router is local
Priority 100 (default 100)
  Track interface GigabitEthernet1/0/1 state Up decrement 10
IP redundancy name is "hsrp-Vl105-5" (default)
```

DSW2#

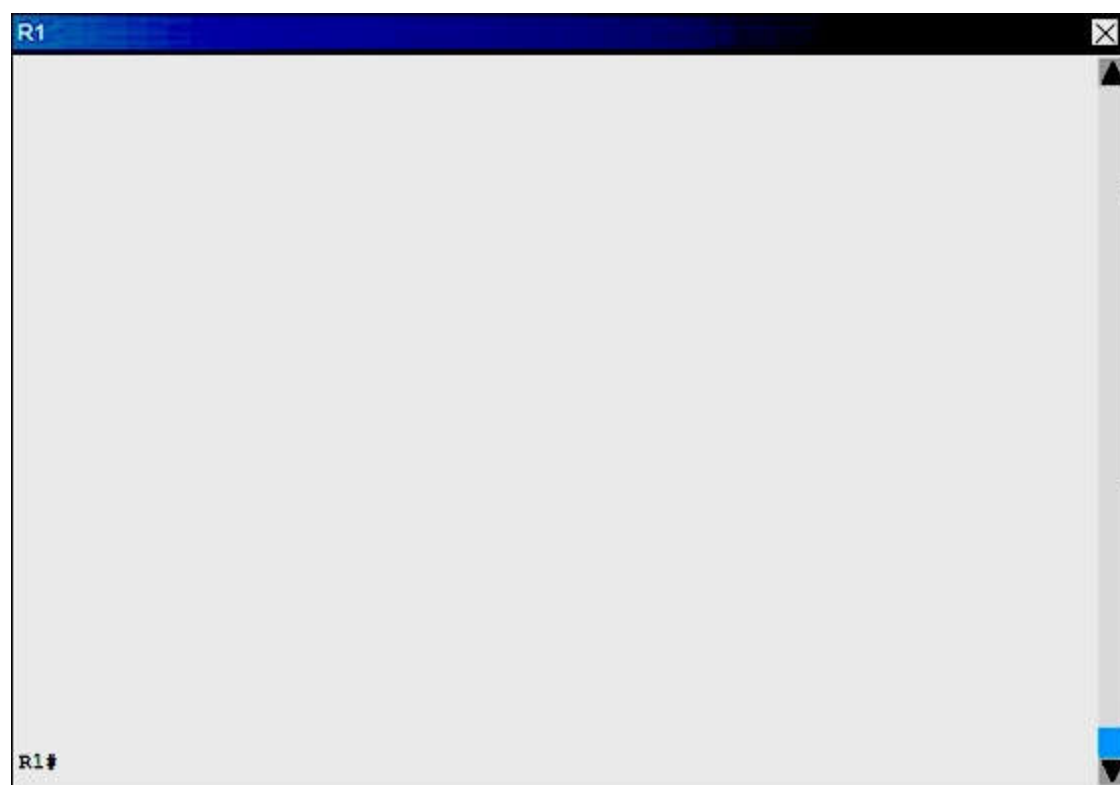
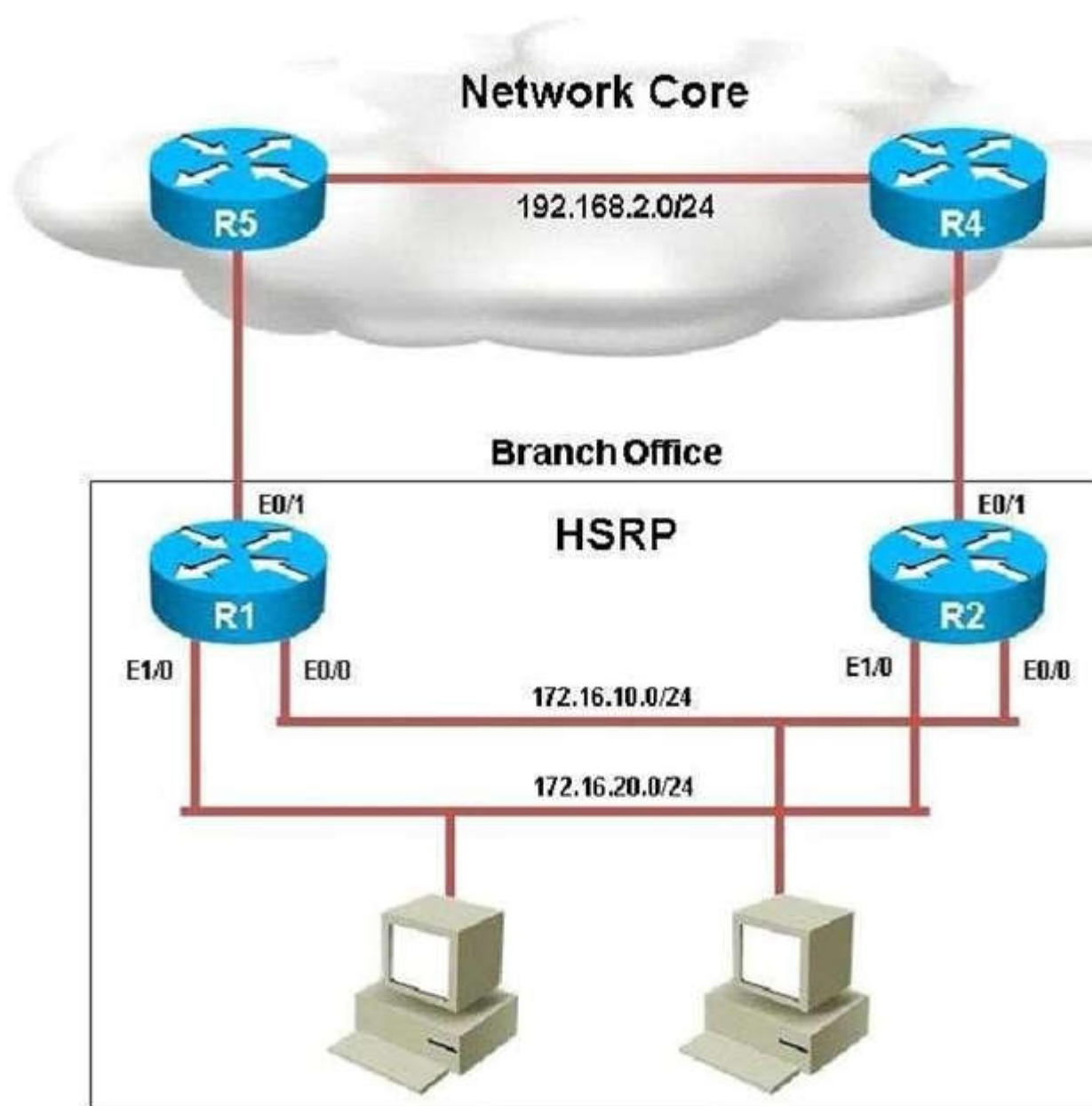
#### QUESTION 258

Instructions:

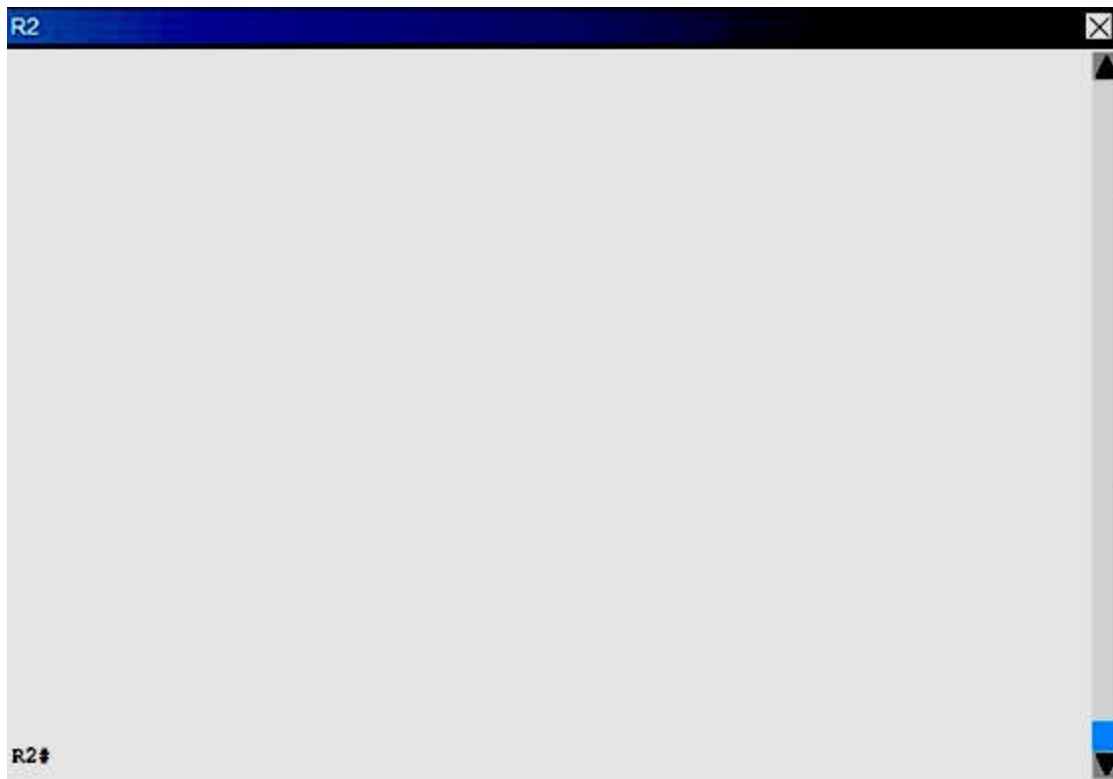
- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on R1 and R2 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

Scenario:

Your customer has asked you to come in and verify the operation of routers R1 and R2 which are configured to use HSRP. They have questions about how these two devices will perform in the event of a device failure. Click on the devices or the tabs at the bottom of the screens to access the CLI to answer their questions.







What percentage of the outgoing traffic from the 172.16.10.0/24 subnet is being forwarded through R1?

- A. R1-0%
- B. R1-50 %, R2-50%
- C. R2-100%
- D. R1-100%

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Based on the following output, we see that R1 is the active standby router for the Ethernet 0/0 link, so all outgoing traffic will be forwarded to R1.

```
R1
R1#show standby
Ethernet0/0 - Group 1
  State is Active
    2 state changes, last state change 00:05:01
  Virtual IP address is 172.16.10.254
  Active virtual MAC address is 4000.0000.0010 (MAC In Use)
    Local virtual MAC address is 4000.0000.0010 (cfgd)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.936 secs
  Authentication text, string "cisco123"
  Preemption enabled, delay reload 180 secs
  Active router is local
  Standby router is 172.16.10.1, priority 100 (expires in 10.464 sec)
  Priority 130 (configured 130)
    Track object 1 state Up decrement 40
  Group name is "hsrp-Et0/0-1" (default)
```

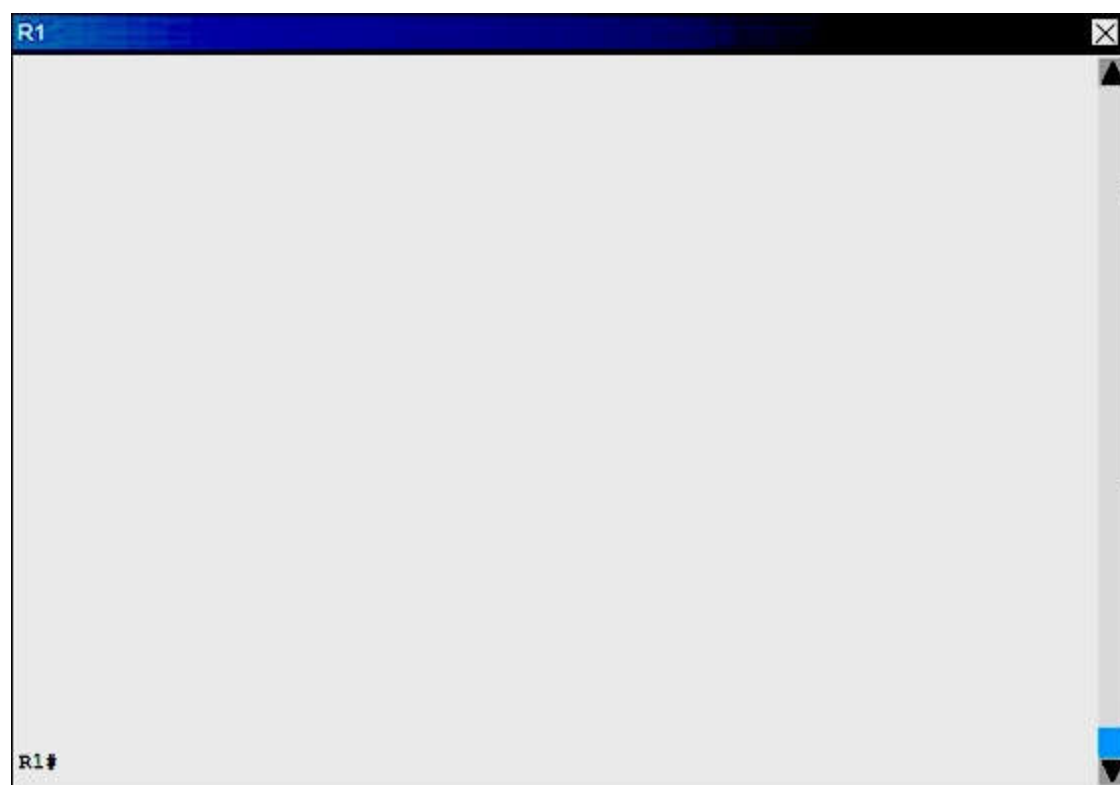
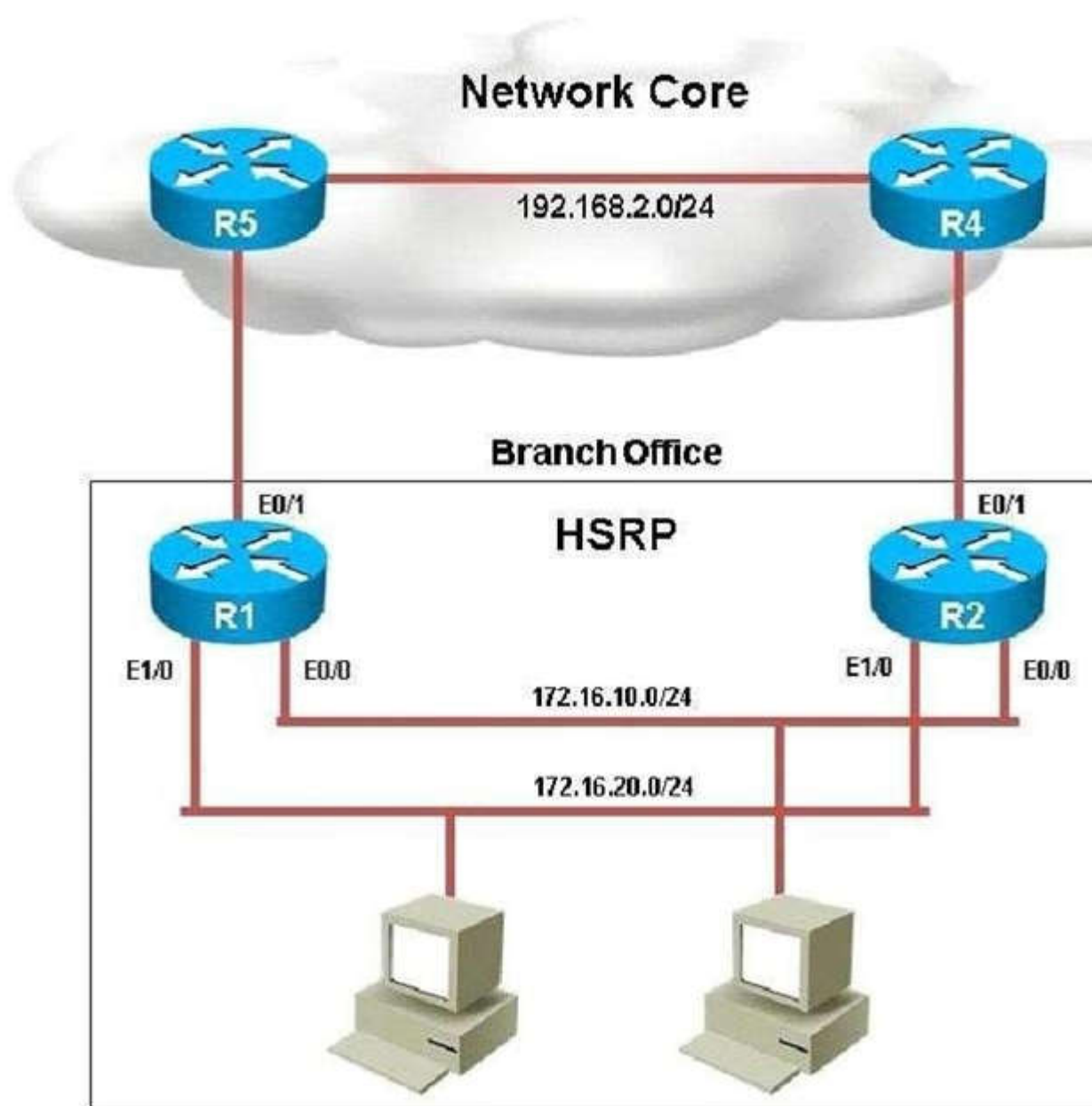
#### QUESTION 259

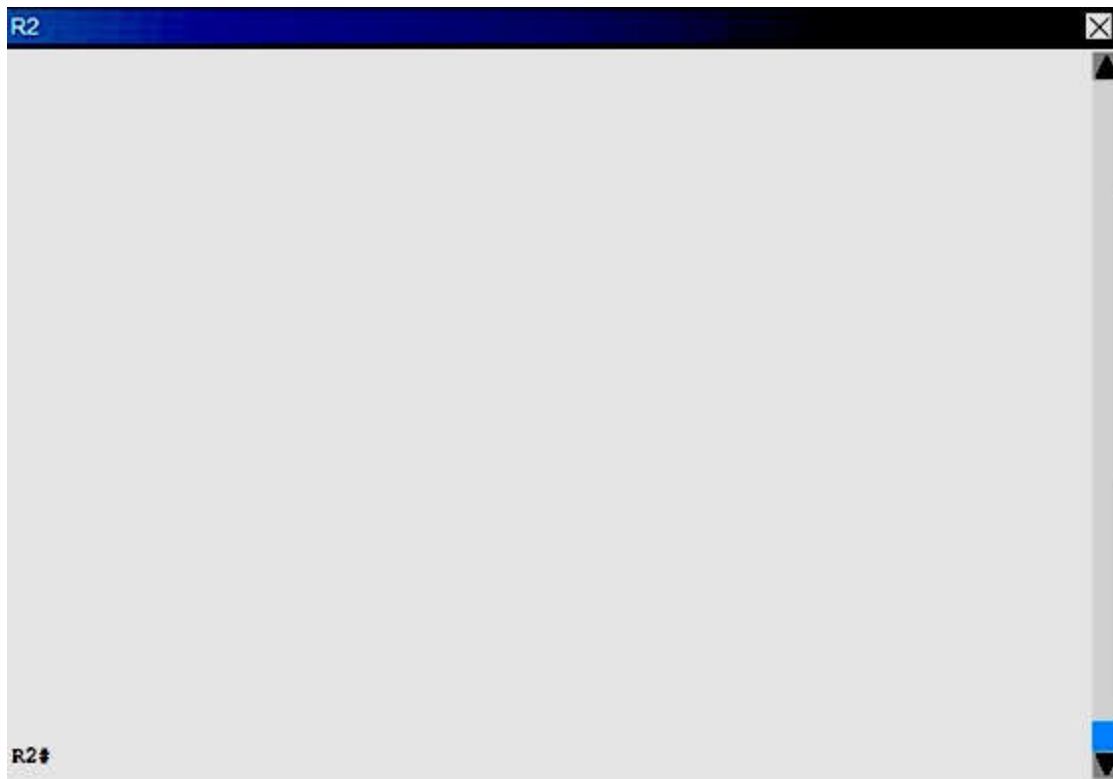
Instructions:

- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on R1 and R2 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

Scenario:

Your customer has asked you to come in and verify the operation of routers R1 and R2 which are configured to use HSRP. They have questions about how these two devices will perform in the event of a device failure. Click on the devices or the tabs at the bottom of the screens to access the CLI to answer their questions.





Refer to the exhibit. If router R1 interface Ethernet0/0 goes down and recovers, which of the statement regarding HSRP priority is true?

- A. The interface will have the priority decremented by 40 for HSRP group 1.
- B. The interface will have the priority decremented by 60 for HSRP group 1
- C. The interface will have its current priority incremented by 40 for HSRP group 1
- D. The interface will have its current priority incremented by 60 for HSRP group 1
- E. The interface will default to the a priority of 100 for HSRP group 1

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Here is the HSRP configuration seen on R1:

```
R1
!
interface Ethernet0/0
  description Link to R2
  ip address 172.16.10.2 255.255.255.0
  standby 1 ip 172.16.10.254
  standby 1 priority 130
  standby 1 preempt delay reload 180
  standby 1 authentication cisco123
  standby 1 mac-address 4000.0000.0010
  standby 1 track 1 decrement 40
!
interface Ethernet0/1
```

Here, when the Ethernet 0/0 interface goes down, the standby 1 track decrement command will lower the priority from 130 to 90. However, when it comes back up, it will then increment it by 40 back to 130 for HSRP group 1.

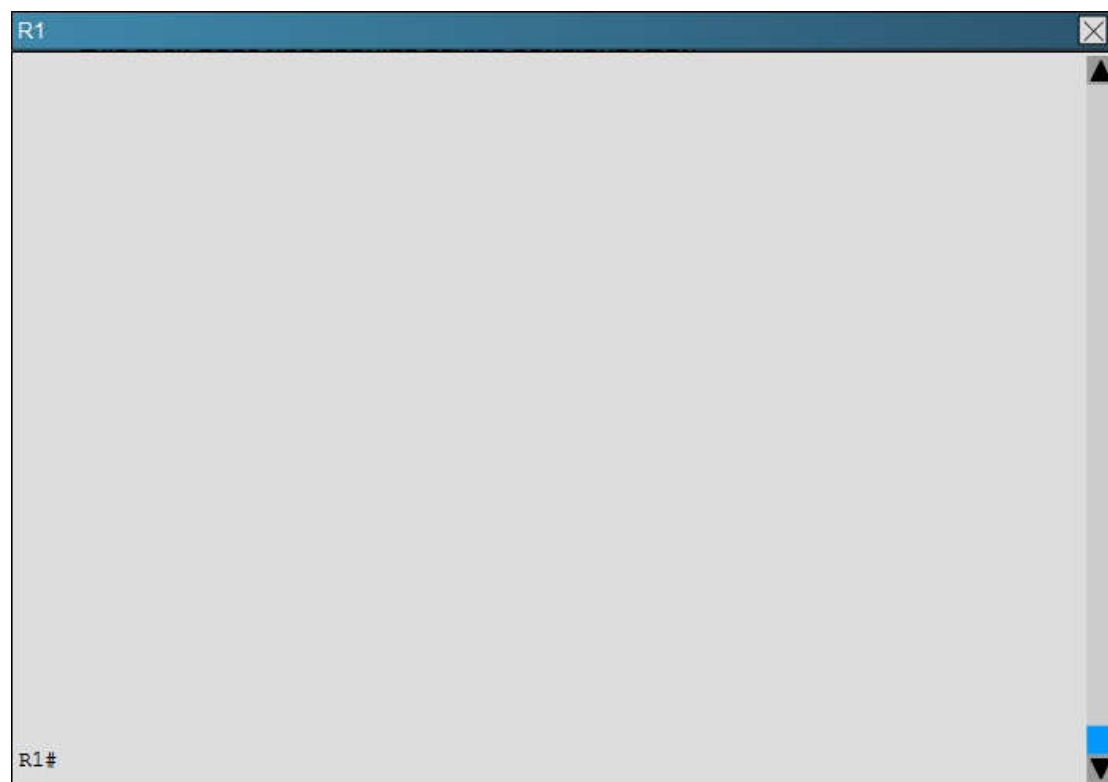
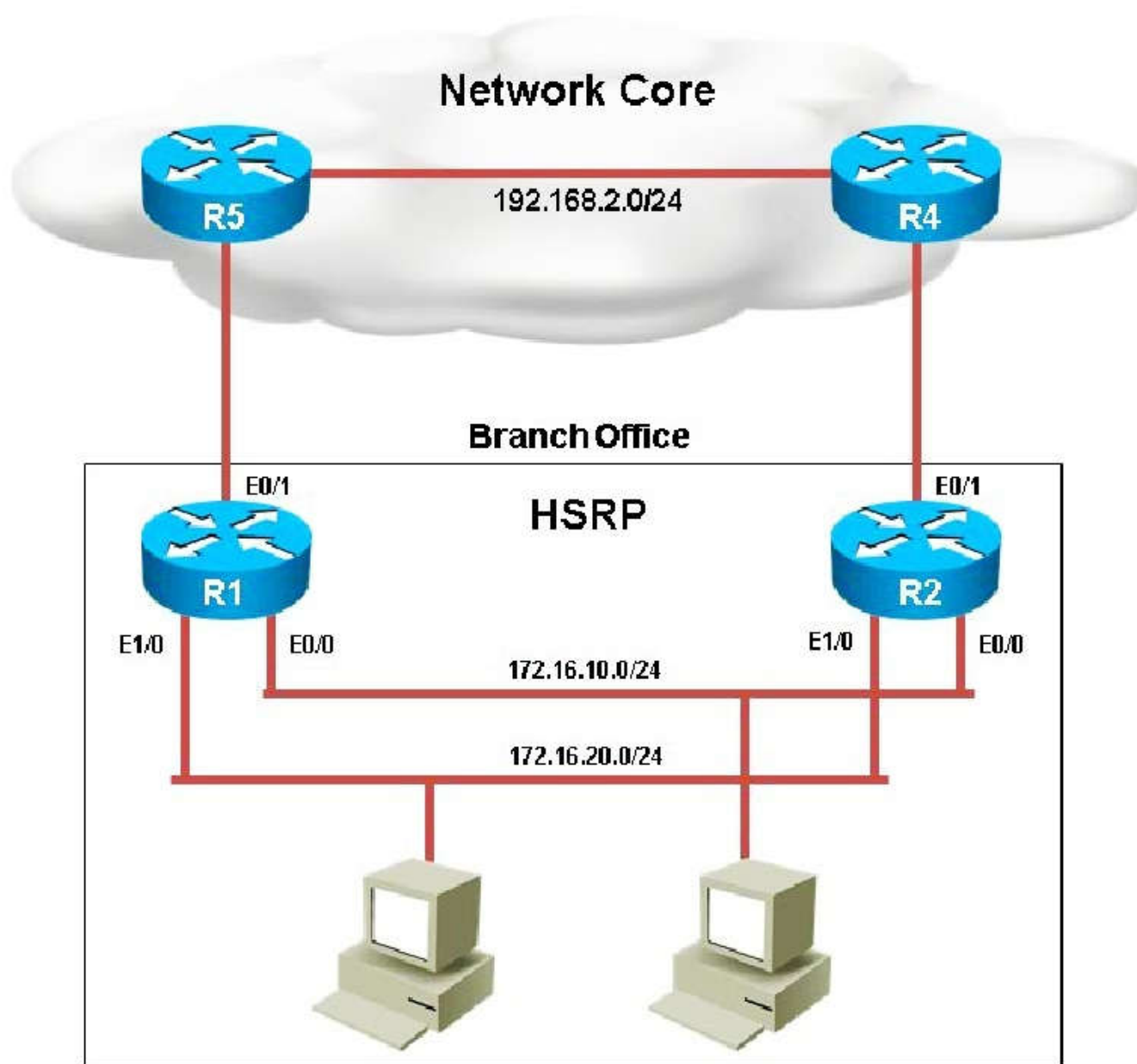
#### QUESTION 260

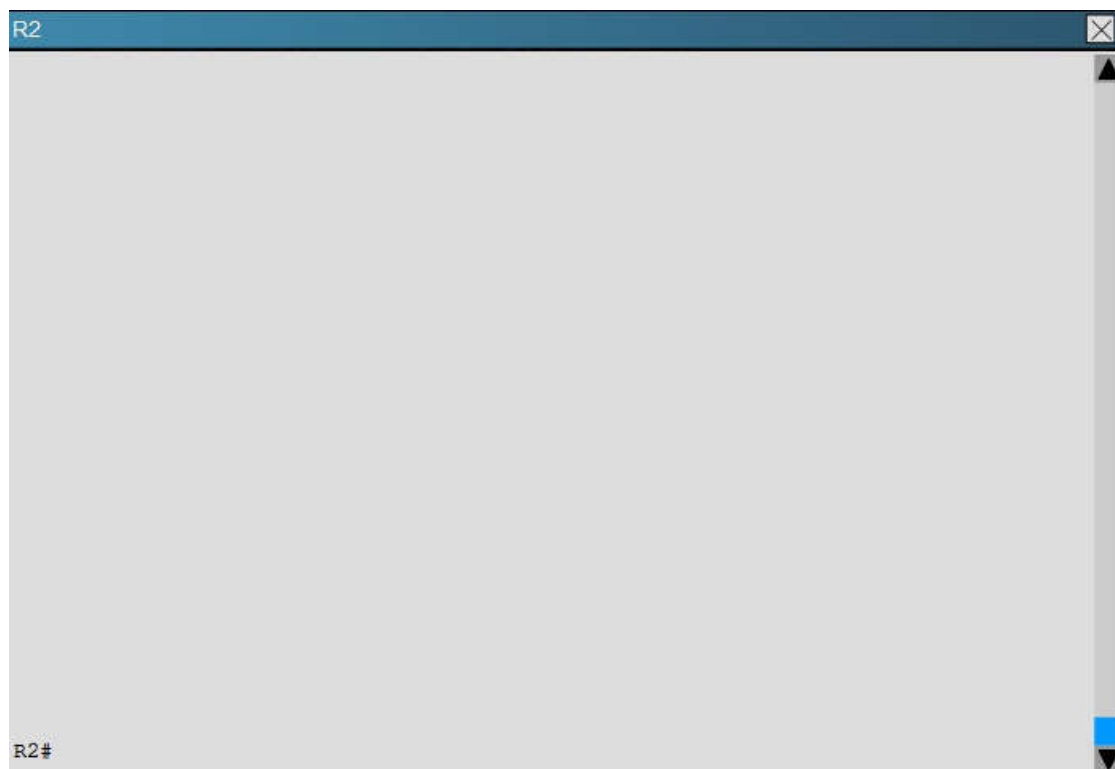
Instructions:

- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on R1 and R2 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

Scenario:

Your customer has asked you to come in and verify the operation of routers R1 and R2 which are configured to use HSRP. They have questions about how these two devices will perform in the event of a device failure. Click on the devices or the tabs at the bottom of the screens to access the CLI to answer their questions.





What issue is causing Router R1 and R2 to both be displayed as the HSRP active router for group 2?

- A. The HSRP group number mismatch
- B. The HSRP group authentication is misconfigured
- C. The HSRP Hello packets are blocked
- D. The HSRP timers mismatch
- E. The HSRP group priorities are different

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Based on the configuration output, we see that authentication is configured on R2, but not on R1:

```
R1
!
interface Ethernet1/0
  description Link to R2
  ip address 172.16.20.2 255.255.255.0
  standby 2 ip 172.16.20.254
!
```

```
R2
!
interface Ethernet1/0
  description Link to R1
  ip address 172.16.20.1 255.255.255.0
  standby 2 ip 172.16.20.254
  standby 2 priority 130
  standby 2 preempt delay reload 180
  standby 2 authentication cisco123
  standby 2 track 1 decrement 40
!
```

This can be further verified by issuing the “show standby” command on each router.



R1

```

Ethernet1/0 - Group 2
  State is Active
    2 state changes, last state change 00:05:03
  Virtual IP address is 172.16.20.254
  Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.656 secs
  Preemption disabled
  Active router is local
  Standby router is unknown
  Priority 100 (default 100)
  Group name is "hsrp-Et1/0-2" (default)

```

R1#

% Ambiguous command

R1#

R2

```

Ethernet1/0 - Group 2
  State is Active
    2 state changes, last state change 00:05:03
  Virtual IP address is 172.16.20.254
  Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.400 secs
  Authentication text, string "cisco123"
  Preemption enabled, delay reload 180 secs
  Active router is local
  Standby router is unknown
  Priority 130 (configured 130)
    Track object 1 state Up decrement 40
  Group name is "hsrp-Et1/0-2" (default)

```

R2#

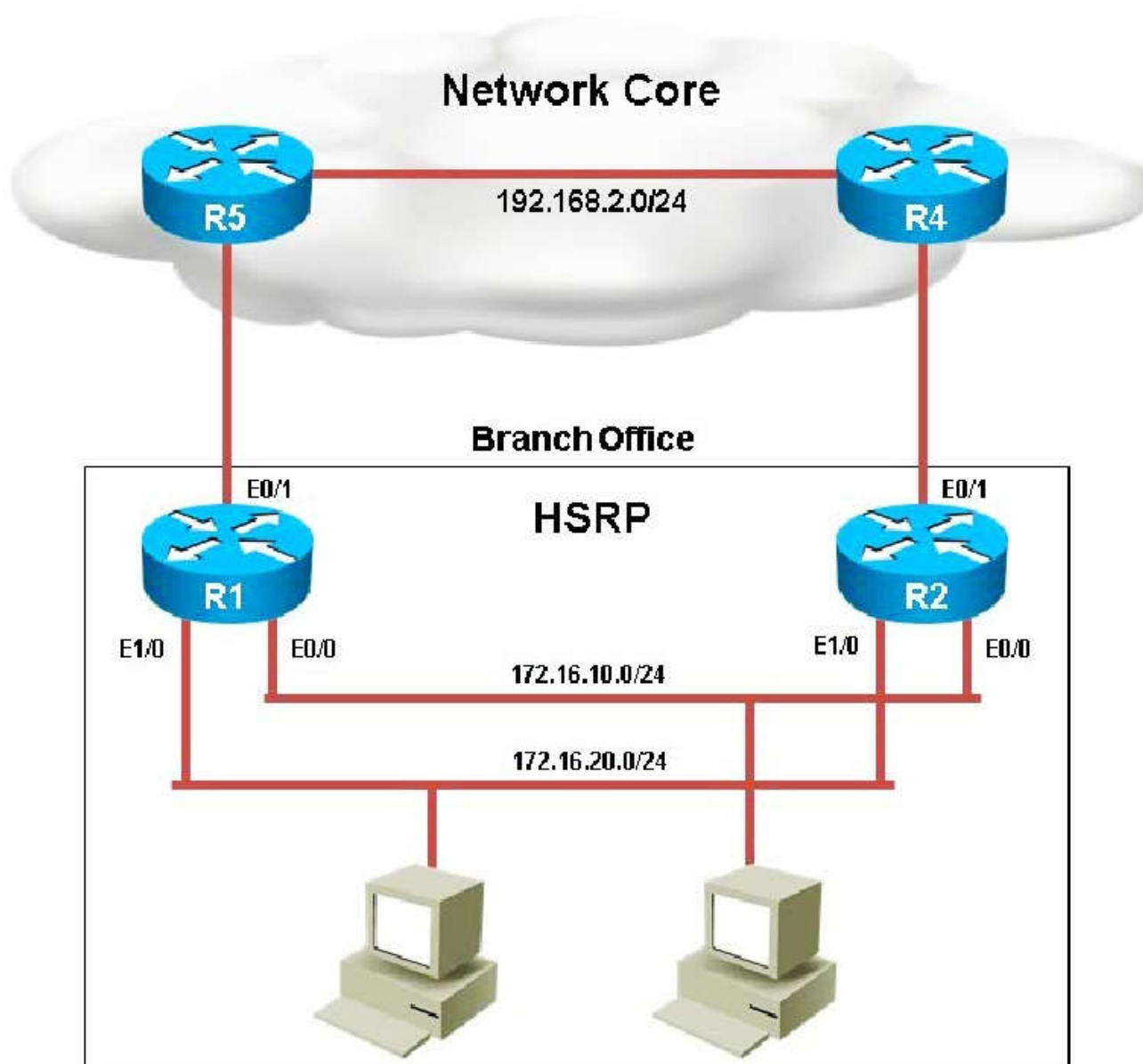
**QUESTION 261**

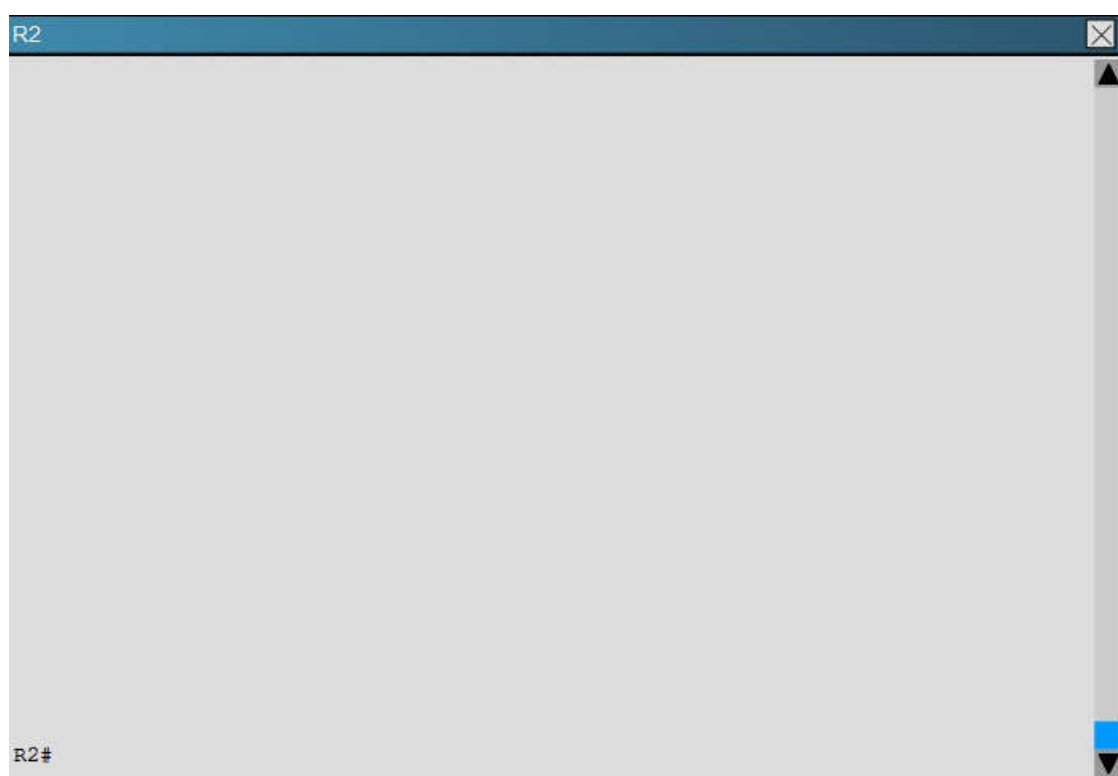
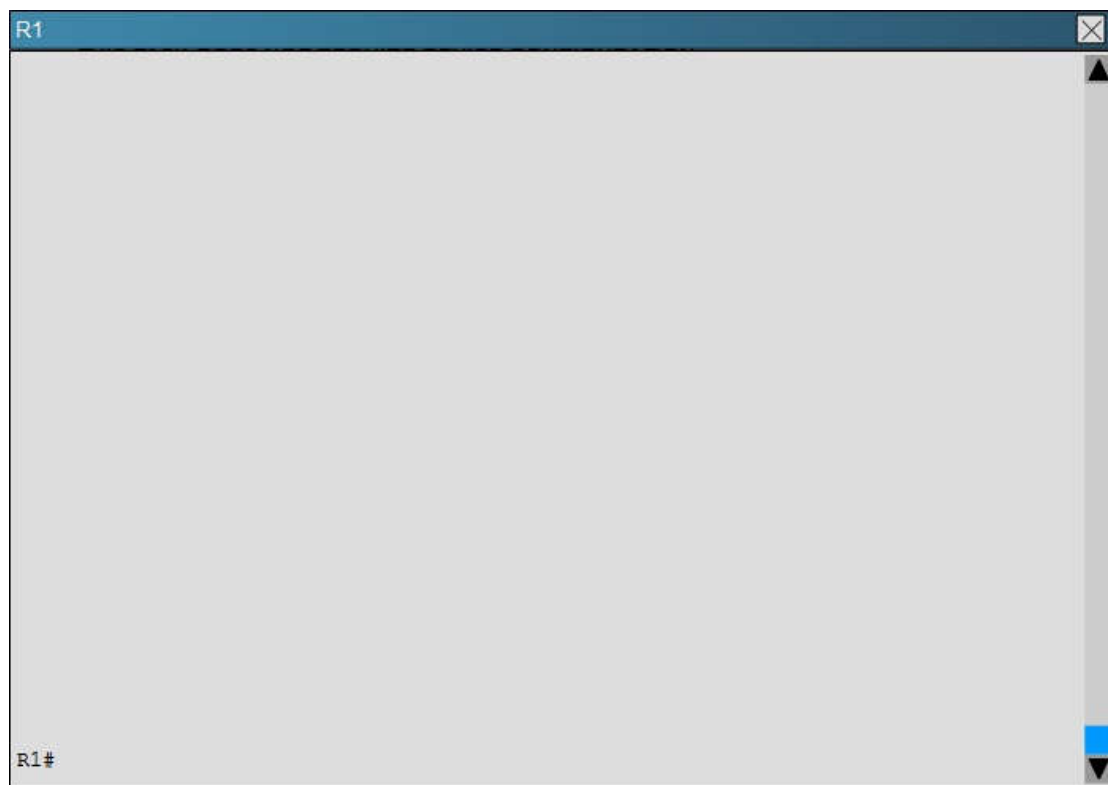
Instructions:

- Enter IOS commands on the device to verify network operation and answer the multiple-choice questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on R1 and R2 to gain access to the consoles of these devices. No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button

Scenario:

Your customer has asked you to come in and verify the operation of routers R1 and R2 which are configured to use HSRP. They have questions about how these two devices will perform in the event of a device failure. Click on the devices or the tabs at the bottom of the screens to access the CLI to answer their questions.





What is the virtual mac-address of HSRP group 1?

- A. 0000.0c07.ac02
- B. 4000.0000.0010
- C. 0000.0c07.ac01
- D. 4000.0000.ac01
- E. 4000.0000.ac02
- F. 0000.0c07.0010

**Correct Answer:** B  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**

Explanation:

Issuing the “show standby” command on either router shows us that the virtual MAC used by HSRP group 1 is 4000.0000.0010 as shown below:

## R1

```
R1#show standby
Ethernet0/0 - Group 1
  State is Active
    2 state changes, last state change 00:05:01
  Virtual IP address is 172.16.10.254
  Active virtual MAC address is 4000.0000.0010 (MAC In Use)
    Local virtual MAC address is 4000.0000.0010 (cfgd)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.936 secs
  Authentication text, string "cisco123"
  Preemption enabled, delay reload 180 secs
  Active router is local
  Standby router is 172.16.10.1, priority 100 (expires in 10.464 sec)
  Priority 130 (configured 130)
    Track object 1 state Up decrement 40
  Group name is "hsrp-Et0/0-1" (default)
```

## R2

```
R2#show standby
Ethernet0/0 - Group 1
  State is Standby
    1 state change, last state change 00:04:38
  Virtual IP address is 172.16.10.254
  Active virtual MAC address is 4000.0000.0010 (MAC Not In Use)
    Local virtual MAC address is 4000.0000.0010 (cfgd)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.128 secs
  Authentication text, string "cisco123"
  Preemption disabled
  Active router is 172.16.10.2, priority 130 (expires in 10.512 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Et0/0-1" (default)
```

### QUESTION 262

Which feature is enabled automatically when you configure HSRP on an interface?

- A. HSRP preemption
- B. ICMP redirect messages
- C. HSRP tracking
- D. IGMP snooping

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

### QUESTION 263

DRAG DROP

Drag and drop the GLBP components from the left onto the correct functions on the right.

**Select and Place:**



|                  |                                                                    |
|------------------|--------------------------------------------------------------------|
| ARP              | value that determines the role of the router in a GLBP environment |
| AVF              | method of learning the MAC address of a network device             |
| AVG              | assigns virtual MAC addresses                                      |
| gateway priority | forwards packets sent to an assigned virtual MAC address           |

Correct Answer:

|  |                  |
|--|------------------|
|  | gateway priority |
|  | ARP              |
|  | AVG              |
|  | AVF              |

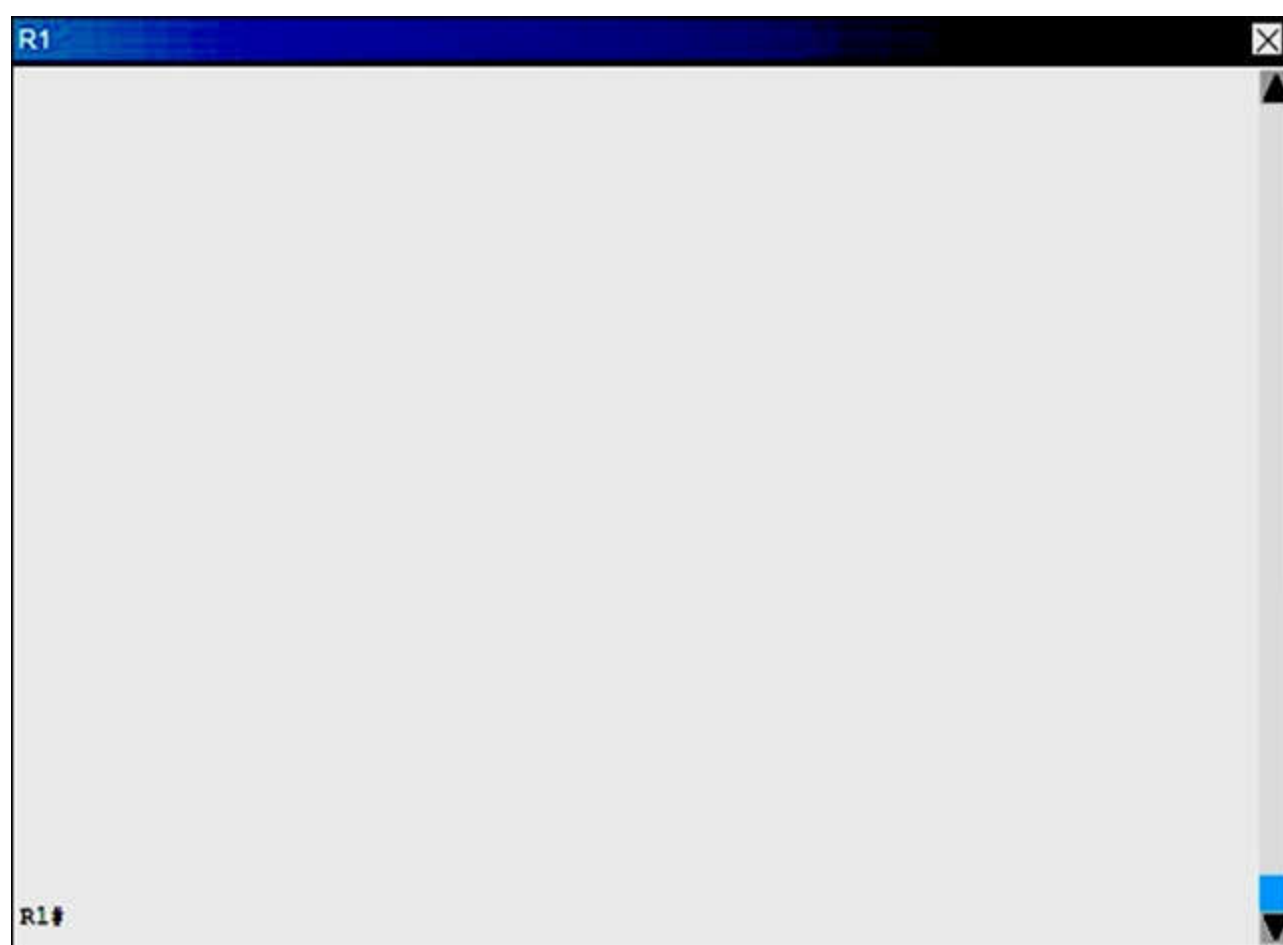
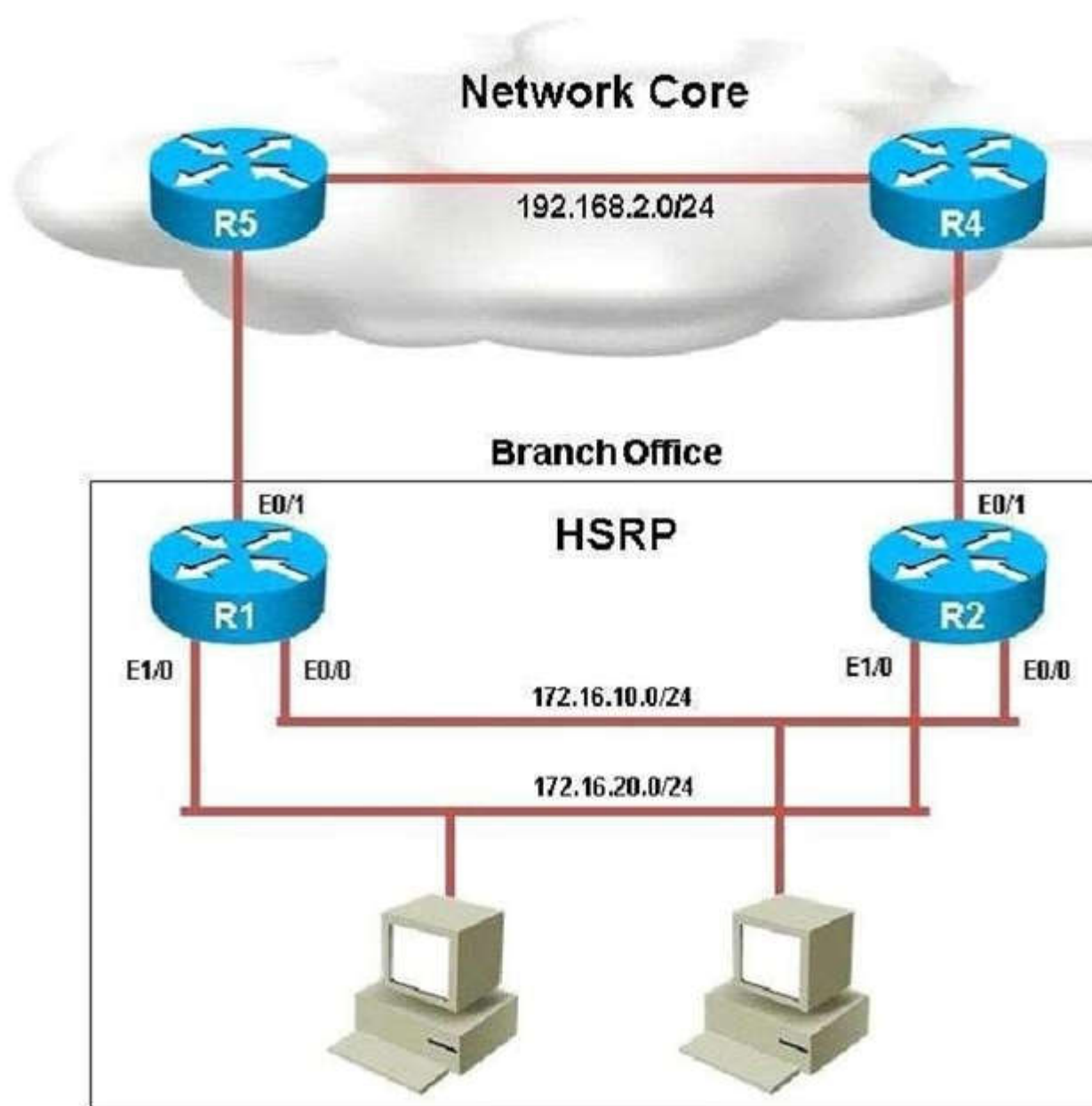
Section: Infrastructure Services

Explanation

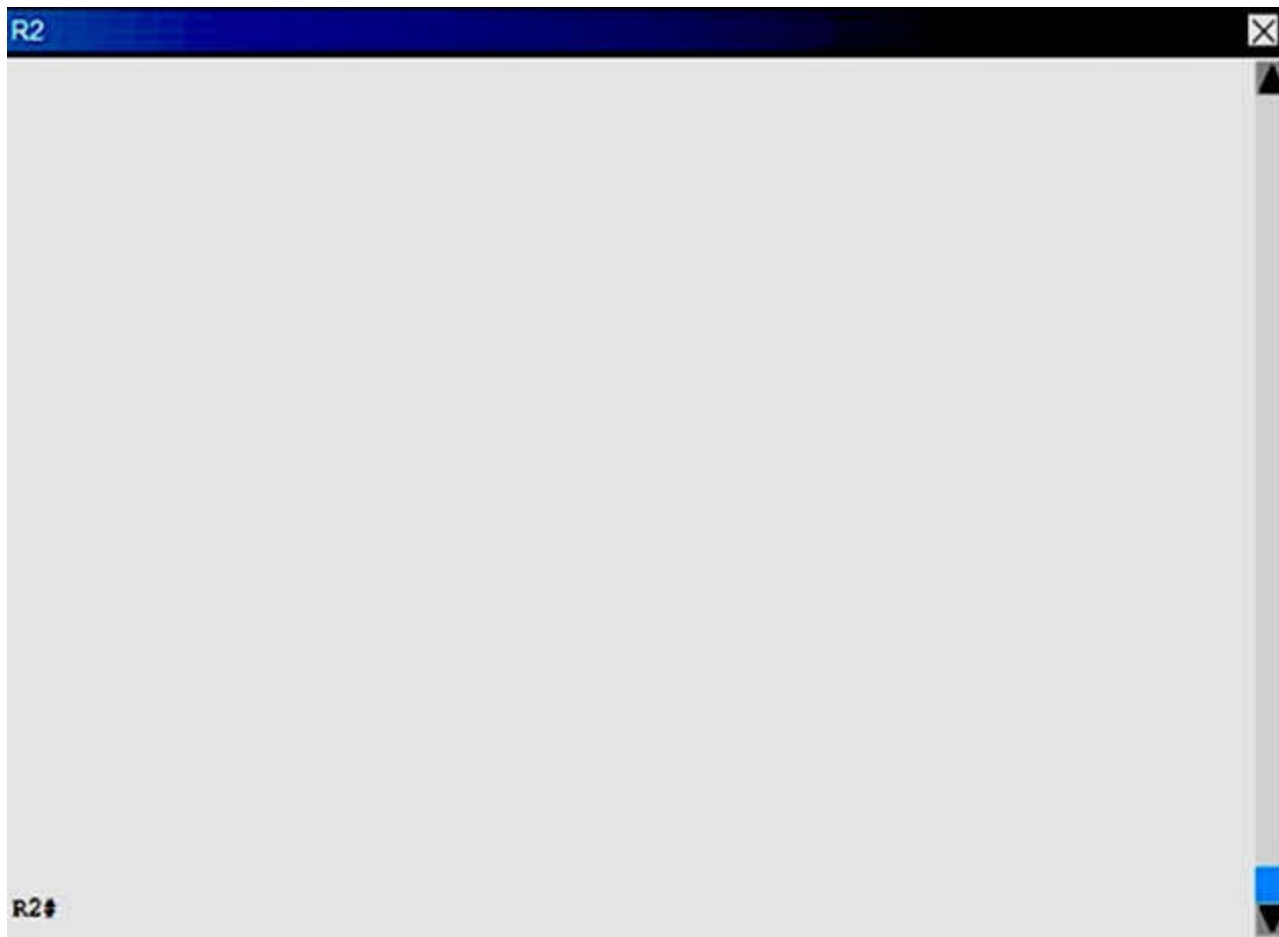
Explanation/Reference:

Reference: [https://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ft\\_glbp.html](https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html)

QUESTION 264







Which causes routers R1 and R2 to be displayed as HSRP active routers for group 2?

- A. The HSRP group numbers do not match.
- B. The HSRP group authentication misconfigured.
- C. The HSRP group Hello packets are blocked.
- D. The HSRP group timers do not match.
- E. The HSRP group priorities do not match.

**Correct Answer:** B

**Section:** Infrastructure Services

**Explanation**

**Explanation/Reference:**

Based on the configuration output, we see that authentication is configured on R2, but not on R1:

## R1

```
!  
interface Ethernet1/0  
  description Link to R2  
  ip address 172.16.20.2 255.255.255.0  
  standby 2 ip 172.16.20.254  
!
```

## R2

```
!  
interface Ethernet1/0  
  description Link to R1  
  ip address 172.16.20.1 255.255.255.0  
  standby 2 ip 172.16.20.254  
  standby 2 priority 130  
  standby 2 preempt delay reload 180  
  standby 2 authentication cisco123  
  standby 2 track 1 decrement 40  
!
```

This can be further verified by issuing the "show standby" command on each router.

| R1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | R2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ethernet1/0 - Group 2<br>State is Active<br>2 state changes, last state change 00:05:03<br>Virtual IP address is 172.16.20.254<br>Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)<br>Local virtual MAC address is 0000.0c07.ac02 (v1 default)<br>Hello time 3 sec, hold time 10 sec<br>Next hello sent in 0.656 secs<br>Preemption disabled<br>Active router is local<br>Standby router is unknown<br>Priority 100 (default 100)<br>Group name is "hsrp-Et1/0-2" (default)<br>R1#<br>% Ambiguous command<br>R1# | Ethernet1/0 - Group 2<br>State is Active<br>2 state changes, last state change 00:04:48<br>Virtual IP address is 172.16.20.254<br>Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)<br>Local virtual MAC address is 0000.0c07.ac02 (v1 default)<br>Hello time 3 sec, hold time 10 sec<br>Next hello sent in 2.400 secs<br>Authentication text, string "cisco123"<br>Preemption enabled, delay reload 180 secs<br>Active router is local<br>Standby router is unknown<br>Priority 130 (configured 130)<br>Track object 1 state Up decrement 40<br>Group name is "hsrp-Et1/0-2" (default)<br>R2# |

### QUESTION 265

What command provides the output shown in the exhibit? (Click on the Exhibit button.)

```
FastEthernet0/0 - Group 100  
State is Active  
2 state changes, last state change 40:20:05  
Virtual IP address is 192.168.8.10  
Hello time 5 sec, hold time 18 sec  
Next hello sent in 4.300 secs  
Redirect time 600 sec, forwarder time-out 7200 sec  
Authentication text "authenticate"  
Preemption enabled, min delay 60 sec  
Active is local  
Standby is unknown  
Priority 254 (configured)  
Weighting 105 (configured 110), thresholds: lower 95, upper 105  
Track object 2 state Down decrement 5  
Load balancing: host-dependent  
There is 1 forwarder (1 active)  
Forwarder 1  
State is Active  
1 state change, last state change 40:20:05  
MAC address is 0007.b400.0101 (default)  
Owner ID is 0005.0050.6c08  
Redirection enabled  
Preemption enabled, min delay 60 sec  
Active is local, weighting 105
```

- A. switch# show glbp
- B. switch# show standby
- C. switch# show glbp status
- D. switch# show standby brief

**Correct Answer:** A

**Section:** Infrastructure Services

## Explanation

### Explanation/Reference:

Explanation:

The command show glbp displays the output in the exhibit. This command displays detailed information about GLBP groups on the switch. In this scenario, the switch is a member of GLBP group 100, and it is the active switch. The output indicates that the virtual IP address is 192.168.8.10 and that preemption is enabled.

The command show glbp status does not exist on Cisco routers.

The command show standby brief is used to display a summary of the HSRP groups to which the switch belongs. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. This command is for HSRP only.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Cisco IOS IP Application Services Command Reference > sctp through show ip slb vservers > show glbp

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

### QUESTION 266

What command would display a single line of information for each virtual gateway or virtual forwarder on a switch?

- A. switch# show glbp
- B. switch# show glbp brief
- C. switch# show standby
- D. switch# show standby brief

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

### Explanation/Reference:

Explanation:

A brief single line view of virtual forwarder and virtual gateway information is provided with the command show glbp brief. Virtual forwarders and virtual gateways are terms used for GLBP groups. A brief output of GLBP information is provided with the brief key word. This output includes the interface, priority, state, and address of GLBP interfaces on the switch.

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled.

The command show standby brief is used to display a summary of the HSRP groups to which the switch belongs. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. This command is for HSRP only.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

Cisco > Cisco IOS IP Application Services Command Reference > show glbp

### QUESTION 267

Which command enables GLBP on an interface?

- A. glbp
- B. glbp 10 ip 192.168.1.1
- C. standby mode glbp
- D. switchport mode glbp

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

### Explanation/Reference:

Explanation:

The glbp ip interface configuration command enables Group Load Balancing Protocol (GLBP). The syntax for this command is as follows:

```
switch(config-if)# glbp group-number ip ip-address
```

The following example activates GLBP for group 5 on Fast Ethernet interface 1/0. The virtual IP address to be used by the GLBP group is set to 10.5.5.5. The default gateway of each host should be set to the virtual IP address.

```
switch(config)# interface FastEthernet 1/0
switch(config-if)# ip address 10.5.5.1 255.255.255.0
switch(config-if)# glbp 5 ip 10.5.5.5
```

GLBP is a Cisco-designed protocol that provides for the dynamic use of redundant routers in a broadcast network. It differs from HSRP and VRRP in that it is not necessary to configure multiple groups to fully use redundant paths or routers. GLBP has a configurable load-balancing mechanism that will distribute the use of redundant gateways servicing a broadcast network such as an Ethernet LAN. When a host issues an ARP to resolve its gateway's MAC address, the active virtual gateway (AVG) will respond with the virtual MAC address of a selected active virtual forwarder (AVF). The AVG will perform load balancing by

varying which virtual MAC it selects to use in the response. The AVF will own that assigned virtual MAC as long as the gateway is active. If an AVF becomes unable to provide service as gateway, then another AVF can assume ownership of the virtual MAC.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

#### QUESTION 268

What command would be used to display detailed information regarding VRRP groups on the switch?

- A. switch# show vrrp
- B. switch# show standby
- C. switch# show vrrp detail
- D. switch# show standby detail

**Correct Answer: A**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command that would display detailed information regarding VRRP groups on the switch is show vrrp. The information provided for each VRRP group by this command includes the status, virtual IP and MAC addresses, whether preemption is enabled, priority of the switch, and the address of the group master.

The command show vrrp detail does not exist on a Cisco device. The detail view is provided by the command show vrrp.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

The command show standby detail provides the same output as show standby. It can be used to display detailed information about HSRP groups a switch is a member of. This command is for HSRP only.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Command Reference > show vrrp

#### QUESTION 269

You have configured switches A and B in a network. The gigabitethernet0/1 interface of switch A has HSRP enabled on it for VLAN 30. Switch A has a priority of 240 and switch B has a priority of 200 for the HSRP group. You want to ensure that if the gigabitethernet0/1 interface of switch A goes down, then switch B becomes the active HSRP switch for the VLANs. You have executed the standby preempt command on switch B.

Which of the following commands should be used on switch A to achieve the desired results?

- A. standby 30 track gigabitethernet0/1
- B. standby 30 track gigabitethernet0/1 10
- C. standby 30 track gigabitethernet0/1 30
- D. standby 30 track gigabitethernet0/1 45

**Correct Answer: D**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The standby 30 track gigabitethernet0/1 45 command should be used on switch A so that switch B becomes the active switch in case the gigabitethernet0/1 interface of switch A fails. The standby track command allows you to track an HSRP-enabled interface on a switch. When the tracked interface fails or goes down, the priority of the active switch in the given HSRP group is decremented. The default decrement value for the tracked interface is 10, which means that the priority value of the HSRP switch is decremented by 10. Additionally, if the standby preempt command is used on another switch, then that switch becomes the active switch for the group if it has a higher priority.

In this case, the standby 30 track gigabitethernet0/1 45 command decrements the HSRP priority of switch A for group 30 (VLAN 30) by 45 when gigabitethernet0/1 goes down. As a result, the priority of switch A is reduced to 195, which is less than the priority of switch B. Therefore, switch B now has the highest priority and hence becomes the active switch for the group.

The other options are incorrect, as they do not reduce the priority of switch A to an extent that the priority of switch B is higher.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands  
Cisco Press > Articles > Cisco Certification > CCNP > High Availability Commands for CCNP BCMSN  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 270

Assuming that preempt is not configured, when does a router in an HSRP group assume the role of the active router for the group?

- A. A router in standby status will become the active router if it has a higher priority than the active router.

- B. A router in standby status will become the active router when it does not detect three consecutive hello messages from the active router.
- C. A router in standby status will become the active router when it does not detect any hello messages from the active router within the configured holdtime.
- D. A router in listening status will become the active router when it does not detect any hello messages from the active router within the configured holdtime.

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

A router in standby status will become the active router when it does not detect any hello messages from the active router within the configured holdtime.

There are two ways for a router to become the HSRP active router. On startup, the router with the highest priority or IP address will become the active router. If the active router fails, the HSRP standby router is a candidate to become the next active HSRP router. Failure of the active router is detected by the loss of hello messages for a configurable amount of time referred to as holdtime. By default, hellos are sent every three seconds (hello time) and the holdtime is 10 seconds.

A router with the highest priority will be selected as the active router during the startup election process. If the active router fails and the standby router is promoted to be the active router, the first router will not immediately resume being the active router even if it has higher priority. This characteristic can be overridden with the configuration option of preempt. The router with the highest priority can initiate a coup to become the active router in the group if it has preempt enabled in the configuration. By default, all routers have an HSRP priority of 100. The range of values that can be assigned is 1 - 255. Other default values are:

Standby holdtime is 10 seconds

Standby track interface priority is 10

To illustrate these concepts, consider the following example. Router A is configured with a priority of 150 and Router B is configured with a priority of 100. Neither router is configured to preempt. If both routers were shut down and Router 5 was rebooted first, then Router B would become the active router. If Router A was then rebooted, it would not become the active router even though it has a higher priority than Router B, because it was NOT configured with the preempt command to allow it to assume the active role with a higher priority.

The six HSRP states are defined as follows:

Initial state: All routers start in this state.

Learn state: The router is in the learn state when it has not communicated with the active router. It does not know which router is the active router and does not know the IP address of the virtual router (if no HSRP IP address configured in the router).

Listen state: Once the router hears from the active router and knows the virtual IP address, it enters the listen state. It is not the active or standby router.

Speak state: After a router learns the IP address of the virtual router, it enters the speak state. It participates in the active and standby router election. It sends hello messages to the active router.

Standby state: When the active router has been elected, the second router enters the standby state. This is the standby router and it will become the active router if the active router fails.

Active state: The router is in active state when it is forwarding packets. It receives packets via the virtual IP address.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 271

You have configured three routers in HSRP group 10 to provide gateway redundancy for VLAN 56. Your intention was for Router 1 to be the active router in the group and for Router 3 to be the standby router. Furthermore, in the event that Router 1 became unavailable, resulting in Router 3 becoming active, you intended for Router 1 to resume its role as active when it came back online. However, you discover that in practice, Router 1 does NOT resume the active role when it comes back online.

What command should be executed on Router 1?

- A. router1(config)# interface VLAN 56  
router1(config-if)# standby 10 preempt
- B. router1(config)# interface VLAN 10  
router1(config-if)# standby 56 preempt
- C. router1(config)# standby 10 preempt
- D. router1(config)# standby 56 preempt

**Correct Answer: A**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

For Router 1 to resume its role as active when it comes back online, it must be configured to preempt the router with a lower priority. In this scenario, Router 3 must have been configured with a lower priority than Router 1, or else it would have been the active router to begin with. To allow Router 1 to take back over as active, it must be configured with the following commands that will allow it to preempt the router with the lower priority:

```
router1(config)# interface VLAN 56
router1(config-if)# standby 10 preempt
```

This condition can be illustrated by executing the debug standby command on Router 1 as shown in the partial output below. The IP address of Router 1 is 192.168.11.112. The IP address of Router 3 is 192.168.11.150. The virtual IP address of the HSRP group is 192.168.11.156.



```

router1# debug standby

SB:56:V156 Hello out 192.168.11.112 Speak pri 100 ip 192.168.11.156
SB:56:V156 Hello in 192.168.11.150 Active pri 50 ip 192.168.11.156
SB:56:V156 Speak h/hello rcvd from lower pri Active router (50/192.168.11.150)
SB:56:V156 Hello in 192.168.11.150 Active pri 50 ip 192.168.11.156
SB:56:V156 Speak h/hello rcvd from lower pri Active router (50/192.168.11.150)
SB:56:V156 Hello out 192.168.11.112 Speak pri 100 ip 192.168.11.156
SB:56:V156 Hello in 192.168.11.150 Active pri 50 ip 192.168.11.156

```

Router 1 sends a hello in line 1 of the output and receives its hello in line 2. Line 1 shows that Router 1 has a priority of 100. Line 2 shows that Router 3 (192.168.11.150) has a priority of 50. Although Router 1 has a higher priority, it is not configured to preempt, so it will not be able to take the active role back from Router 3. If Router 1 were configured to preempt, there would be a series of output as shown below:

```

SB:56:V156 Hello in 192.168.11.112 Active pri 100 ip 192.168.11.156
SB:56:V156 Active router is 192.168.11.112, was local

```

If the HSRP router is the only HSRP router on the segment, then the output will show the router sending out hello packets with no hellos coming back.

The commands below are incorrect because the VLAN is 56, not 10, and the group number is 10, not 56:

```

router1(config)# interface VLAN 10
router1(config-if)# standby 56 preempt

```

The command below is incorrect because it is not executed under the VLAN 56 interface:

```

router1(config)# standby 10 preempt

```

The command below is incorrect because it is not executed under the VLAN 56 interface and the HSRP number is incorrect:

```

router1(config)# standby 56 preempt

```

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing

Cisco > Cisco IOS IP Application Services Command Reference > standby preempt through weight > standby preempt

#### QUESTION 272

The partial output displayed in the exhibit is a result of what IOS command? (Click on the Exhibit(s) button.)

```

Vlan 1 - Group 1
State is Active
  2 state changes, last state change 00:30:59
Virtual IP address is 172.16.1.20
Active virtual MAC address is 0004.4d82.7981
  Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
  Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is local
Standby router is 172.16.1.6, priority 75 (expires in 9.184 sec)
Priority 95 (configured 120)
IP redundancy name is "Group1", advertisement interval is 34 sec

```

- A. switch# show running-config
- B. switch# show standby vlan1 active brief
- C. switch# show hsrp 1
- D. switch# show standby

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The command show standby produces the output displayed in the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. Important information in the exhibit includes that this router is the active router, the virtual IP address for the HSRP group is 172.16.1.20, the address of the standby router is 172.16.1.6, and the router is configured to preempt.

The command show running-config will display the complete configuration of the device, including the configuration of HSRP, but will not display the current status of HSRP on the switch.

The command show standby vlan 1 active brief provides a summary display of all HSRP groups on the switch that are in the active state. This output would provide basic information, not nearly the detail indicated in the exhibit. The following is an example of output for show standby vlan 1 active brief:

```

Interface Grp Prio P State Active addr Standby addr Group addr
Vlan1 0 120 Active 172.16.1.5 Unknown 172.16.1.20

```

The command show hsrp 1 is not valid due to incorrect syntax.

Objective:

Infrastructure Services

Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Command Reference > show ip sockets through standby name > show standby  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 273

You have been assigned to create a plan to implement HSRP on the router connecting your company's network to the Internet. The router should be the active router in the HSRP group. On the active router, the following conditions should be met:

Enable preemption with no delay  
Set Hello timer to 10 seconds and hold time to 25 seconds  
Set the priority to 150

Which of the following commands should be included in the plan to meet the given requirements? (Choose all that apply.)

- A. standby 1 preempt delay minimum 10
- B. standby 1 preempt
- C. standby 1 priority 150
- D. standby 1 timers 10 25
- E. standby 1 timers 25 10
- F. standby track interface S0/1

**Correct Answer:** BCD  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

The following commands should be included in the implementation plan to meet the given requirements:

```
standby 1 preempt
standby 1 priority 150
standby 1 timers 10 25
```

The standby 1 preempt command configures the preempt settings on the router. This command allows preemption without any delay. The standby 1 priority 150 command sets the priority of the router to 150. The default priority of HSRP routers is 100. This implies that this router becomes the active router if there are no other routers in the group with a higher priority. The standby 1 timers 10 25 command sets the Hello timer and the hold time on the local router. The first value, 10, specifies the Hello timer, and the second value, 25, indicates the hold time.

The most essential steps to configure HSRP on routers are as follows:  
Assign IP addresses to the interfaces using the ip address command  
Enable HSRP on the interfaces and assign the virtual IP address using the standby ip command  
Set the HSRP priority of the interfaces using the standby priority command  
Configure HSRP preempt settings on the interfaces using the standby preempt command  
Set the Hello timers using the standby timers command  
Enable interface tracking for other HSRP-enabled interfaces using the standby track command

The standby 1 preempt delay minimum 10 command should not be included in the implementation plan. This command causes the router to preempt the active router after a minimum of 10 seconds. However, the requirement states that there should be no delay in preemption (a delay of 0 seconds), which is the default behavior.

The standby 1 timers 25 10 command should not be included in the implementation plan. This command sets the Hello timer to 25 seconds and the hold time to 10 seconds. However, the requirement is to set the Hello timer to 10 seconds and the hold time to 25 seconds.

The standby track interface S0/1 command should not be included in the implementation plan. This command enables tracking of the S0/1 interface on the local router. However, there is no requirement in the scenario to track an interface. Tracking can be used to decrement the priority of an HSRP router when the interface goes down. Using the default decrement value, if S0/1 were to go down, the priority of the router would be reduced by 10.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Home > Support > Configuring HSRP > How to Configure HSRP  
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring HSRP

#### QUESTION 274

Which protocol allows the network to fully use standby routers in a redundancy group without additional administrative burden?

- A. HSRP
- B. VRRP
- C. GLBP
- D. IRDP

**Correct Answer:** C  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

Gateway Load Balancing Protocol (GLBP) allows the network to fully utilize standby routers in a redundancy group. Unlike HSRP and VRRP, GLBP allows automatic selection and simultaneous use of multiple gateways. It also allows for router load balancing from a segment without using different host configuration as in HSRP.

Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) provide gateway redundancy, but only one router in a group can forward traffic for a redundancy group. The bandwidth and resources associated with the non-actively forwarding routers are wasted. GLBP allows this wasted bandwidth and resources to be utilized by providing automatic selection and use of multiple available gateways to destinations.

ICMP Router Discovery Protocol (IRDP) is an extension of the Internet Control Message Protocol (ICMP) that allows routers to advertise useful routes. IRDP does not require hosts to recognize routing protocols, nor does it require manual configuration.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

#### QUESTION 275

Which command enables HSRP on an interface?

- A. hsrp
- B. standby ip
- C. standby mode hsrp
- D. switchport mode hsrp

**Correct Answer: B**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The standby ip interface configuration command enables Hot Standby Router Protocol (HSRP). The syntax for this command is as follows:

```
switch(config-if)# standby group-number ip ip-address
```

The group-number argument specifies the HSRP group number on the interface. You do not need to enter a group number if there is only one HSRP group.

At least one interface on one of the routers in the group must be configured with the virtual IP address of the group. It is optional on all other interfaces on the other routers, which can learn the address through the hellos sent among the group.

A complete HSRP configuration is shown below with an explanation of each command.

```
RouterA (config) #interface Fa0/1
RouterA (config-if) # ip address 192.168.5.6 255.255.255.0
RouterA (config-if) # standby 2 ip 192.168.5.10
RouterA (config-if) # standby 2 priority 150
RouterA (config-if) #standby 2 Preempt
RouterA (config-if) #standby 2 track interface fa0/2
```

Line 1 specifies the interface  
Line 2 addresses the interface  
Line 3 specifies the HSRP group number and the virtual IP address  
Line 4 sets the HSRP priority  
Line 5 allows the router to take the active role if its priority becomes higher than that of the active router

In the above, the router is tracking its own Fa0/1 interface. If that interface goes down it will reduce its priority by 10 (this is the default decrement when not specified). The new value would be 140 if that happened. To specify a decrement value, add it to the track command, as in this example: track interface Fa0/2 20.

When you configure routers to be part of an HSRP group, they listen for the HSRP MAC address for that group as well as their own burned-in MAC addresses.

HSRP uses the following MAC address:  
0000.0c07.ac\*\* (where \*\* is the HSRP group number)

The switchport mode interface configuration command will configure the VLAN membership mode of a port. It is not used to enable HSRP.

The options standby mode hsrp and hsrp are not valid commands.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Home > Technology Support > IP > IP Application Services > Design > Design Technotes > Hot Standby Router Protocol Features and Functionality  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 276

The output displayed below is a result of what command?

```
Interface Grp Fwd Pri State Address Active router Standby router
Vl10 10 - 254 Active 192.168.8.10 local unknown
Vl10 10 1 7 Active 0007.b400.0101 local -
```

- A. switch# show standby
- B. switch# show glbp
- C. switch# show standby brief
- D. switch# show glbp brief

**Correct Answer: D**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**

Explanation:

The output of the exhibit is provided with the command show glbp brief. This output includes the interface, priority, state, and address of GLBP interfaces on the switch. In this case, VLAN 10 is the active virtual gateway using IP address 192.168.8.10.

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled.

The command show standby brief is used to display a summary of the HSRP groups the switch is a member of. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. This command is for HSRP only.

The command show standby can be used to display detailed information about HSRP groups a switch is a member of. This command is for HSRP only.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Cisco IOS IP Application Services Command Reference > sctp through show ip slb vservers > show glbp

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

#### QUESTION 277

Which statement best describes the function of Hot Standby Router Protocol (HSRP)?

- A. HSRP specifies a single IP address that all routers in the group must use.
- B. HSRP defines a set of routers that represent one virtual, fault-tolerant router.
- C. HSRP provides a round-robin gateway selection process to increase fault tolerance.
- D. HSRP defines a frame-tagging scheme that allows end stations to use any router as a gateway.

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Hot Standby Router Protocol (HSRP) is specified by RFC 2281. The primary function of HSRP is to define a set of routers that work together to represent one virtual, fault-tolerant router. Thus, redundancy is provided in the event that any one of the routers fails. HSRP can be configured on the following interface types:

Routed ports

Switched virtual interfaces (SVI)

Etherchannel port channels

HSRP does use a single IP address to represent a group of routers, but this does not fully describe the function of HSRP.

HSRP does not provide round-robin gateway selection. HSRP uses router priority to select a primary and standby router.

HSRP does not define a frame-tagging scheme that allows end stations to use any router as a gateway. End stations use the virtual IP address of a group of HSRP routers as the default gateway.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 278

Which of the following statements best describes the result of issuing the command standby 44 timers 3 1 on an HSRP router?

- A. The holdtime will be set to a value of 3, and the hellotime will be set to a value of 1.
- B. The status of the standby router will be displayed as unknown expired.
- C. The role of active router will be passed repeatedly from one router to another.
- D. The router will be configured to reassume the role of active router in the event that the router fails and is subsequently restarted.

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

When the command standby 44 timers 3 1 is issued on a Hot Standby Routing Protocol (HSRP) router, the role of active router will be passed repeatedly from one router to another. This behavior occurs when the timers are set incorrectly. The syntax for the standby timers command is standby [group-number] timers [hellotime holdtime].

The hellotime variable is the number of seconds between hello messages and is set to a value of 3 by default.

The holdtime variable is the number of seconds that the HSRP standby router will wait before assuming that the active router is down; if the standby router believes the active router to be down, it will assume the role of active router.

The holdtime is set to a value of 10 by default. The holdtime should be set to a value at least three times the value of the hellotime. Otherwise, the active router might not be able to respond before the standby router assumes that the active router is down and becomes the new active router.

Because the command standby 44 timers 3 1 sets the hellotime to a value of 3 and the holdtime to a value of 1, the role of active router will be passed from one standby router to the next. To set the holdtime to a value of 3 and the hellotime to a value of 1, the command standby 44 timers 1 3 should be issued. To reset the timer values to their default values, the command no standby group-number timers should be issued.

The status of the standby router will be displayed as unknown expired if a Physical layer problem exists. The unknown expired status can also be displayed if only one HSRP router is configured for the subnet.

To configure an HSRP router to reassume the role of active router in the event that the router fails and is subsequently restarted, the command standby group-number preempt should be issued. When the HSRP active router fails or is shut down, the standby router assumes the role of active router. By default, when the original HSRP active router is restarted, it does not take the role of active router away from the original standby router, even if the original active router has a higher priority value. The command standby group-number preempt changes this default behavior.

The holdtime will not be set to a value of 3, and the hellotime will not be set to a value of 1. On the contrary, the hellotime will be set to a value of 3 and the holdtime will be set to a value of 1.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco IOS IP Application Services Command Reference > show vrrp through synguard (virtual server) > standby timers

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 279

Which load-balancing algorithm does GLBP use by default?

- A. Random load-balancing
- B. Weighted load-balancing
- C. Round-robin load-balancing
- D. Host-dependent load-balancing

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

Round-robin load-balancing is the default load-balancing method used by Gateway Load Balancing Protocol (GLBP).

The active virtual gateway (AVG) can be configured to use one of three load-balancing algorithms when selecting which active virtual forwarder (AVF) MAC address to use in its ARP response.

Round-Robin Load-Balancing: Using round-robin load-balancing, the AVG in turn points to each AVF virtual MAC address in its ARP reply (default method).

Weighted Load-Balancing: Using weighted load-balancing, the AVG selects an AVF virtual MAC address to use in the ARP reply, proportionally based on the advertised weight value configured in a GLBP gateway.

Host Dependant Load-Balancing: Using host-dependant load-balancing, the AVG selects an AVF virtual MAC address to use in the ARP reply based on which one the host used previously. A host will use the same AVF as long as the GLBP group is unchanged.

GLBP is a Cisco-designed protocol that provides for the dynamic use of redundant routers in a broadcast network. It differs from HSRP and VRRP in that it is not necessary to configure multiple groups to fully use redundant paths or routers. GLBP has a configurable load-balancing mechanism that will distribute the use of redundant gateways servicing a broadcast network such as an Ethernet LAN. When a host issues an ARP to resolve its gateway's virtual IP address, the active virtual gateway (AVG) reply includes the virtual MAC address of a selected active virtual forwarder (AVF). The AVG is therefore responsible for performing load balancing, varying which virtual MAC it selects to use in the response. The AVF will own that virtual MAC as long as the gateway is active. If an AVF becomes unable to provide service as gateway, another AVF can assume ownership of the virtual MAC.

There is no random load balancing method.

GLBP and HSRP are Cisco-developed solutions. VRRP is defined in RFC 2338.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

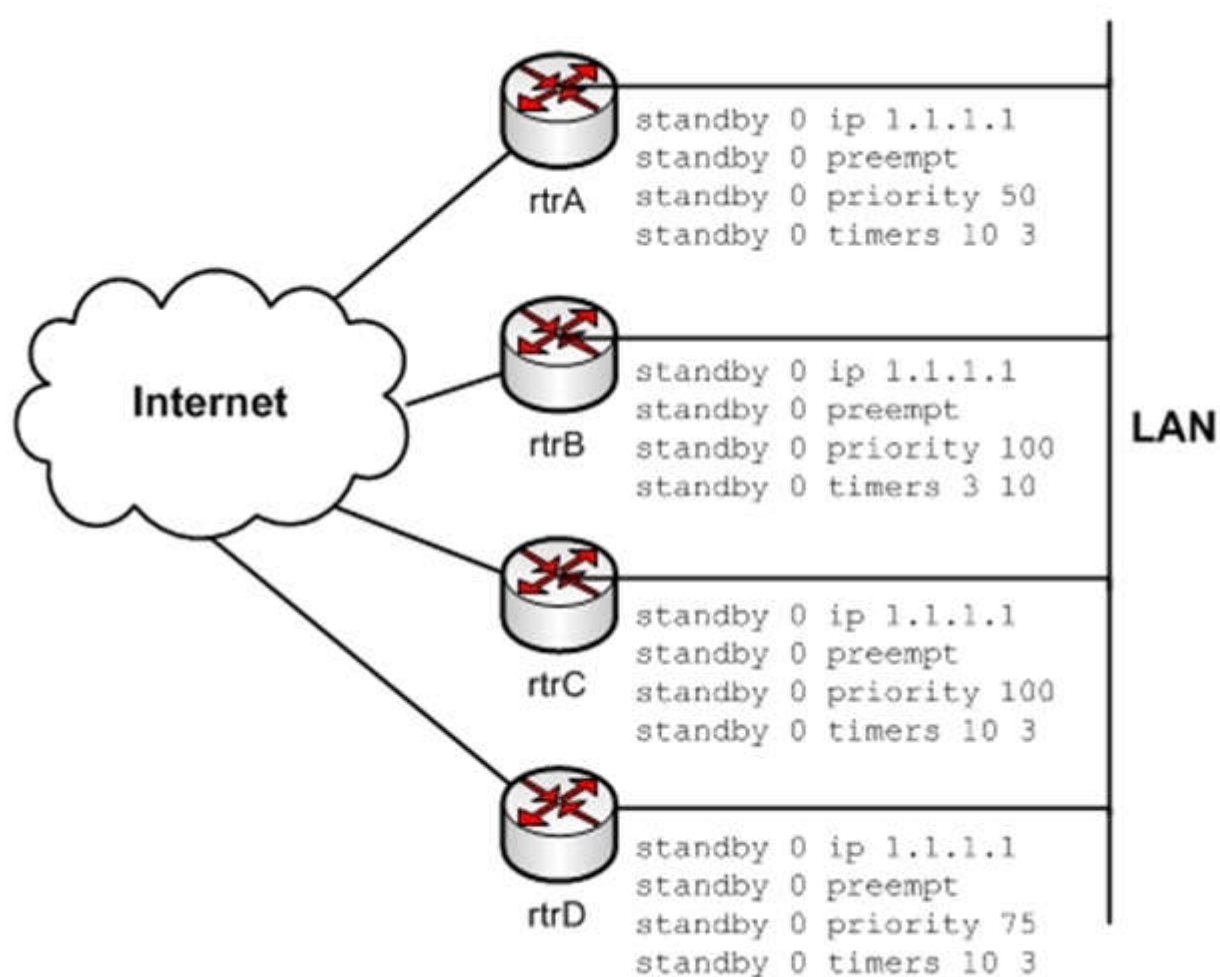
References:

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

#### QUESTION 280

Refer to the following exhibit:





You have configured the routers in the diagram for HSRP, resulting in the displayed configurations.

Which of the following routers were configured with the default HSRP values for each command?

- A. rtrA
- B. rtrB
- C. rtrC
- D. rtrD

**Correct Answer:** B  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
 Explanation:

Only rtrB has the default HSRP settings. The default values for some of the important parameters for an HSRP-enabled router are listed in the following table:

| HSRP Attribute                         | Default Value |
|----------------------------------------|---------------|
| Priority                               | 100           |
| Hold time                              | 10 seconds    |
| Hello timer                            | 3 seconds     |
| Decrement value for tracked interfaces | 10            |
| HSRP group number                      | 0             |
| Preempt delay                          | 0 seconds     |

In this case, the routers have the default group number 0. The two routers rtrB and rtrC have the default priority value of 100, rtrB also has the default timer values, which are 3 seconds for the Hello timer and 10 seconds for the hold time.

The rtrA router is not configured with the default settings because the priority is set to 50, which is not the default value. In addition, the Hello timer is set to 10 seconds (default is 3 seconds) and the hold time is set to 3 seconds (default is 10 seconds).

The rtrC router is not configured with the default settings. Although the priority is 100, which is the default, the Hello timer is set to 10 seconds (default is 3 seconds) and the hold time is set to 3 seconds (default is 10 seconds).

The rtrD router is not configured with the default settings. It has a priority of 75 and the default is 100.

**Objective:**  
 Infrastructure Services

Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Home > Support > Configuring HSRP > How to Configure HSRP  
Cisco IOS Master Command List, Release 12.4>show lnm station through system (ERM policy) > standby track  
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring HSRP

**QUESTION 281**  
What command would provide the output displayed in the exhibit? (Click on the Exhibit(s) button.)

| Interface | Grp | Prio | P | State   | Active        | Standby       | Virtual IP   |
|-----------|-----|------|---|---------|---------------|---------------|--------------|
| Vl64      | 2   | 100  | P | Standby | 192.168.64.10 | local         | 192.168.64.1 |
| Vl65      | 1   | 110  | P | Active  | local         | 192.168.65.20 | 192.168.65.1 |
| Vl66      | 2   | 100  | P | Standby | 192.168.66.10 | local         | 192.168.66.1 |
| Vl67      | 1   | 110  | P | Active  | local         | 192.168.67.20 | 192.168.67.1 |
| Vl68      | 2   | 100  | P | Standby | 192.168.68.10 | local         | 192.168.68.1 |
| Vl69      | 1   | 110  | P | Active  | local         | 192.168.69.20 | 192.168.69.1 |
| Vl70      | 2   | 100  | P | Active  | local         | 192.168.70.20 | 192.168.70.1 |

- A. switch# show hsrp
- B. switch# show standby
- C. switch# show interface vlan
- D. switch# show standby brief

**Correct Answer:** D  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command show standby brief displays the output in the exhibit. It is used to display a summary of the HSRP groups of which the switch is a member. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address. In the exhibit, the interface VLAN 64 is a member of HSRP group 2. Its priority in the group is 100 and it is currently the standby switch. Since preemption is configured (as indicated by the P following the priority), we know that the priority of this switch must be lower than the priority of the active device. The active device has an IP address of 192.168.64.10 and the group IP address is 192.168.64.1.

The command show standby can be used to display detailed information about HSRP groups of which a switch is a member. It does not provide the quick summary display of the exhibit. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The command syntax is show standby [type number [group]].

Below is an example of this command's output:

```
RouterA#show standby vlan 5

VLAN 5 - group 1
Local state is Active, priority 105, may preempt
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.10 configured
Active router is local
Standby router is 192.12.23.3 expires in 9.600
Virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:01:38
<output omitted>

VLAN 5- group 2
Local state is Standby, priority 100
Hellotime 3 sec, holdtime 10 sec
Next hello sent in 1.424
Virtual IP address is 192.12.23.11 configured
Active router is 192.168.23.3 expires in 9.600
Standby router is local
2 state changes, last state change 00:01:38
<output omitted>
```

In the above output, Router A is load-sharing traffic for VLAN 5. It is active for group 1 and standby for group 2. The router at address 192.168.23.3 is active for group 2 and standby for group 1. This allows traffic to be sent to both routers while still allowing for redundancy. Router A was also configured with the standby 1 preempt command (results seen in line 1), which allows it to resume its role as active for group 1 if it comes back up from an outage.

The command show interface vlan is not a complete command. A VLAN number must follow the command. When provided with a VLAN number, the output would display the status of the SVI, but no HSRP information.

The command show hsrp is not a valid command due to incorrect syntax.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Command Reference > show standby through show udp > show standby

**QUESTION 282**

Which of the following features does GLBP provide, but not HSRP and VRRP? (Choose all that apply.)

- A. Support for single active router
- B. Support for automatic load balancing
- C. Support for multiple gateways
- D. Support for interface tracking

**Correct Answer:** BC

**Section:** Infrastructure Services

**Explanation**

**Explanation/Reference:**

Explanation:

Support for automatic load balancing and support for multiple gateways are two features that are provided by Gateway Load Balancing Protocol (GLBP) but not by Hot Standby Routing Protocol (HSRP) or Virtual Router Redundancy Protocol (VRRP).

GLBP, HSRP, and VRRP provide a redundant and fault-tolerant solution in case of first-hop router failure in a network. The basic operation of these three protocols is the same. In all three protocols, a group of routers on the same LAN is formed. One of the routers is selected as the active router and another as the standby router. The router with the highest priority is automatically selected as the active router. If the active router fails, the standby router assumes the responsibilities of the active router. The role of the active router is to forward the packets from the hosts to the virtual router (default gateway).

GLBP provides automatic load balancing between multiple routers by configuring multiple MAC addresses but a single virtual IP address. Every active virtual forwarder (AVF) in the group is configured with the virtual IP address but with different MAC addresses. All such AVFs can then participate in the packet-forwarding process. Multiple gateways then can share the load. On the contrary, HSRP and VRRP do not support automatic load balancing. Both these protocols require additional configuration on all the routers that need to load balance. The additional configuration involves using multiple groups on the routers or assignment of different default gateways for the hosts.

Note that GLBP and VRRP are supported by both Cisco and non-Cisco routers, whereas, HSRP is supported only by Cisco routers.

Single active router and interface tracking both are supported by GLBP, HSRP, and VRRP.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Home > End-of-Sale and End-of-Life Products > Cisco IOS Software Releases 12.2.T > Product Literature > White Papers > GLBP Gateway Load Balancing Protocol > Information About Gateway Load Balancing Protocol

Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Hot Standby Router Protocol Features and Functionality > HSRP Background and Operations > HSRP Operation

**QUESTION 283**

Your network consists of one HSRP group of six routers. All of the routers are functioning properly. The network has been stable for several days.

In which HSRP state are most of the routers?

- A. Learn
- B. Listen
- C. Standby
- D. Active

**Correct Answer:** B

**Section:** Infrastructure Services

**Explanation**

**Explanation/Reference:**

Explanation:

If all of the routers in the Hot Standby Routing Protocol (HSRP) group are functioning properly, then most of the routers in the group are in the listen state. Four routers will be in the listen state, one router will be in the standby state, and one router will be in the active state.

HSRP is used by a group of routers to create the appearance of a virtual router with which end stations can communicate in the event that the default gateway becomes unavailable. The active router is responsible for forwarding packets that are sent to the virtual router. The standby router is responsible for assuming the role of active router should the active router fail or become unavailable. All other HSRP routers monitor the hello messages sent by the active and standby routers. Should the active and standby routers both become unavailable, the HSRP router with the highest priority is elected to become the active router by default. For routers with equal priority values, the router with the highest IP address becomes the active router.

HSRP routers can exist in one of the following six states:

Initial  
Learn  
Listen  
Speak  
Standby  
Active

All HSRP routers start in the initial state. A router in the learn state is waiting for its first hello message from the active router so that it can learn the virtual router's IP address. When the hello message is received and the virtual router's IP address is discovered, the HSRP router is in the listen state. A router in the listen state listens for hello messages from the active and standby routers. If an election for a new active router and a new standby router is required, then an HSRP router will enter the speak state and begin transmitting hello messages. The standby state is reserved for the standby router, and the active state is reserved for the active router. Only routers in speak, standby, and active states will transmit hello packets.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:



#### QUESTION 284

What command can be used on a Cisco switch to display the virtual MAC address for the HSRP groups of which the switch is a member?

- A. switch# show standby mac
- B. switch# show hsrp mac
- C. switch# show standby
- D. switch# show standby brief

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The command show standby can be used to display the virtual MAC address for HSRP groups of which a switch is a member. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch. The standby switch will take over as the active switch if the timer expires before it hears a heartbeat from the active switch. Below is an example of the show standby command for the HSRP group 1:

```
Tacoma# show standby

FastEthernet0/1 - group 1
  State is active
    3 state changes, last state change 00:22:49
  Virtual IP address is 192.168.5.3
    Secondary virtual ip address 192.168.5.3
  Active virtual MAC address is 0006.6b45.5801
    Local virtual MAC address is 0006.6b45.5812(bia)
  Hello time is 4 sec, hold time 12 sec
    Next hello sent in 1.664 sec
  Preemption enabled, min delay 50 sec, sync delay 40 sec
  Active router is local
  Standby router is unknown expired
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface FastEthernet0/2, pri 15
      Down Interface FastEthernet0/3
  IP redundancy name is "HSRP1", advertisement interval is 34 sec
```

In the above output, the following can be determined:

The router is currently active for the group, as can be seen in line 2. The Active Virtual MAC address is 0006.6b45.5801, which includes the group number (1) in the last two positions, which is why the address is different from the routers actual MAC address shown on the next line. Special Note: Some router models (Cisco 2500, 4000 and 4500) WILL NOT use this altered MAC address format, but will instead use the real MAC address for the virtual MAC address and will display that MAC address as the virtual MAC address in the output of the show standby command. An example of the output of the show standby command on an older router such as the 2500 would be as follows:

```
Router# show standby

Ethernet0/1 - Group 1

  State is Active

    2 state changes, last state change 00:30:59

  Virtual IP address is 10.1.0.20

    Secondary virtual IP address 10.1.0.21

  Active virtual MAC address is 0004.4d82.7981

    Local virtual MAC address is 0004.4d82.7981 (bia)
```

These routers have Ethernet hardware that only recognize a single MAC address. In either case, if for some reason this router becomes the standby router, such as due to loss of interfaces, then when the interfaces come back up it will be able to recover the active role because it is set for preemption, as shown on line 10.

The router is tracking two of its own interfaces. Because both interfaces are down, the router's priority has been reduced by 25 (15 for FastEthernet0/2 and 10 for FastEthernet0/3), from the configured value of 120 to 95. This data is shown on lines 13-16. The default is 10 if not otherwise specified, as is the case for FastEthernet0/3.

If either of the two interfaces comes back up, the priority will be increased by the amount assigned to the interface. For example, if FastEthernet0/3 comes back up, the priority will become 105 (95 + 10).

The standby router is unreachable, which can be determined because it is marked unknown expired in line 12. This could be due to either a physical layer issue or an HSRP misconfiguration.

The command show standby brief can be used to view summary information about HSRP groups of which the switch is a member. This information includes the group number, priority, state, active device address, standby address, and group address. It does not include the virtual MAC address.

The commands show standby mac and show hsrp mac are invalid due to incorrect syntax.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Command Reference > show standby  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 285

What command displays detailed information about the GLBP groups to which the switch belongs?

- A. switch# show standby
- B. switch# show glbp state
- C. switch# show glbp
- D. switch# show standby detail

**Correct Answer: C**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled. Below is an example of the command output.

```
RouterA# show glbp
FastEthernet0/0 - Group 20
State is listen
2 state changes, last state change 23:50:33
Virtual IP address is 192.168.5.3
Hello time 5 sec, hold time 18 sec
Next hello sent in 4.300 secs
Redirect time 1800 sec, forwarder time-out 28800 sec
Authentication text "cisco"
Preemption enabled, min delay 60 sec
Active is 192.168.5.9, priority 110 (expires in 0.164 sec)
Standby is 192.168.5.10, priority is 105 (expires in 0.142 sec)
Priority 95 (configured)
Weighting 105 (configured 105), thresholds: lower 90, upper 100
Track object 1 state up decrement 10
Track object 2 state up decrement 10
Load balancing: round robin
<output omitted>
```

The following can be learned from this output:

This router is the active virtual forwarder (AVF). In line 3, the output indicates the state is listen. This is the state of the active AVF.

As indicated in line 14, this router is configured with a weighting for tracking of 105. It also is configured with an upper limit of 100 and a lower limit of 90.

When a tracked object goes down, the value of 105 will be reduced by the decrement value associated with that object. If this results in the weighting dropping below the lower limit (90), this router will give up its role as AVF.

The router is tracking two objects, and both have decrement values of 10. This means that ONLY if both objects go down will this router relinquish its role as AVF. As there is another router to take the role of AVF, there will be no disruption of traffic, even if hosts were using the tracked interface that went down.

The show glbp state will only display the glbp state of the router (standby, listen etc). Detailed output is accomplished with the command show glbp.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

The command show standby detail provides the same output as show standby. It can be used to display detailed information about HSRP groups to which a switch belongs. This command is for HSRP only.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring GLBP

#### QUESTION 286

Which next-hop router redundancy protocol provides backup for an assigned real IP address?

- A. HSRP
- B. GLBP
- C. VRRP
- D. CGMP

**Correct Answer: C**  
**Section: Infrastructure Services**



## Explanation

### Explanation/Reference:

Explanation:

Using VRRP, the shared address of the next-hop router redundancy group can be the real address of a router interface.

Virtual Router Redundancy Protocol (VRRP) is defined in RFC 2338. VRRP enables a group of routers to form a single virtual router, known as a VRRP group. Routers are configured in VRRP groups to provide redundancy for an IP address shared among members of the VRRP group. This address can be the real address of a router interface or a virtual address (or addresses) shared by the group. Each group is comprised of a master and one or more backup routers. If the shared address is the real IP address of a router, that router will always be the master when the address is available. The master router is responsible for forwarding packets sent to the virtual router. The backup routers provide redundancy and stand ready to assume the role of the master router in the event that it is unable to forward packets.

The master virtual router owns the VRRP IP address and is responsible for handling all packets sent to the VRRP IP address. Backup VRRP routers monitor for hello activity from the master virtual router. The master router will advertise using IP 224.0.0.18 and MAC 0000.0c00.01xx (xx is the VRRP Group ID). The advertisements by default will be sent every second, and the master down interval is three seconds.

If the VRRP IP address is NOT the physical address of one of the VRRP routers, then the router with the highest priority will assume the role of the master. The configurable priority range is from 0 to 255, and the default value is 100. The higher the value is, the higher the priority is. If activity stops for the duration of the master router's down interval, the backup router with the highest priority will become the master router. When the old master router comes back online, it will assume the master role again if it still has the highest priority among all routers.

In the configuration shown below, Router A will be the master router unless it goes down, in which case B will take over. If A comes back up it will assume the master role again.

```
routerA(config-if)# vrrp 3 priority 130
routerB(config-if)# vrrp 3 priority 110
```

Hot Standby Router Protocol (HSRP) defines a set of routers that work together to represent one virtual, fault-tolerant router. Thus, redundancy is provided in the event that any one of the routers fails. The shared address of the next-hop router redundancy group is not the real address of a router interface.

Gateway Load Balancing Protocol (GLBP) is a Cisco-designed protocol that provides for the dynamic utilization of redundant routers in a broadcast network. The shared address of the next-hop router redundancy group is not the real address of a router interface. A virtual group address is used.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring VRRP

### QUESTION 287

When executed on a HSRP group member named Router 10, what effect does the following command have?

```
Router10(config-if)# standby 1 track serial0 25
```

- A. It will cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down
- B. It will cause the router to shut down the Serial0 interface if 25 packets have been dropped
- C. It will cause the router to notify Router 25 if serial 0 goes down
- D. It will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

### Explanation/Reference:

Explanation:

This command will cause the router to decrement its HSRP priority by 25 if Serial 0 goes down. Interface tracking can be configured in Hot Standby Routing Protocol (HSRP) groups to switch traffic to the standby router if an interface goes down on the active router. This is accomplished by having the active router track its interface. If that interface goes down, the router will decrement its HSRP priority by the value configured in the command. When properly configured, this will cause the standby router to have a higher HSRP priority, allowing it to become the active router and to begin serving traffic.

When the standby router in an HSRP group is not taking over the active role when the active router loses its tracked interface, it is usually a misconfigured decrement value, such that the value does not lower the HSRP priority of the active router far enough for the standby to have a superior priority value.

The command will not cause the router to increase its HSRP priority by 25 if the Serial0 interface on the standby router goes down. HSRP routers track their own interfaces, not those of another router. The command will not cause the router to shut down the Serial0 interface if 25 packets have been dropped. It will only do this if the link becomes unavailable.

The command will not cause the router to notify Router 25 if serial 0 goes down. The number 25 in the command is the decrement value, not the ID of another router.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands

### QUESTION 288

Which statement best describes the interaction between a workstation and an HSRP virtual router?

- A. The workstation must have the real IP address of one of the HSRP routers defined as its default gateway.
- B. The workstation must support IRDP in order to switch to the alternate router in an HSRP group.
- C. The active HSRP router replies to the workstation's ARP request with the virtual router's MAC address.
- D. The workstation sends packets to the active router's real MAC address.

**Correct Answer: C**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The active HSRP router replies to the workstation's ARP request with the HSRP virtual MAC address. The HSRP virtual router presents a consistently available router to the end user, reachable by a single unique, virtual MAC address. Only the active router responds to frames destined to this virtual MAC address, which identifies the HSRP group.

The primary function of HSRP is to define a set of routers that work together to represent one virtual, fault-tolerant router. Thus, redundancy is provided in the event that one of the routers fails. An HSRP group consists of an active router and a standby router, which together present the appearance of a virtual router. The active router is elected from the routers configured to belong to the HSRP group. The virtual router's MAC address identifies the virtual router, and the end user will send packets to that destination MAC address. The end-user device will send an ARP request using the known IP address of its default gateway to discover the virtual router's MAC address. Only the active router will respond to the ARP request. The active router will then forward packets sent to the virtual router. The standby router monitors the status of the HSRP group and assumes packet-forwarding responsibilities of the virtual router if the active router fails.

The six HSRP states are defined as follows:

Initial state: All routers start in this state.

Learn state: The router is in the learn state when it has not communicated with the active router. It does not know which router is the active router and does not know the IP address of the virtual router (if no HSRP IP address configured in the router).

Listen state: Once the router hears from the active router and knows the virtual IP address, it enters the listen state. It is not the active or standby router.

Speak state: After a router learns the IP address of the virtual router, it enters the speak state. It participates in the active and standby router election. It sends hello messages to the active router.

Standby state: When the active router has been elected, the second router enters the standby state. This is the standby router and it will become the active router if the active router fails.

Active state: The router is in active state when it is forwarding packets. It receives packets via the virtual IP address.

Neither the workstation nor any other device is required to support ICMP Router Discovery Protocol (IRDP) in order to implement an HSRP virtual router. An IRDP-compliant device (RFC 1256) listens for IRDP hello messages, which advertise default routes.

It is not required for the workstation to know the actual IP address of any of the routers in the group. The end-user device will send an ARP request using the known IP address of its default gateway to discover the virtual router's MAC address.

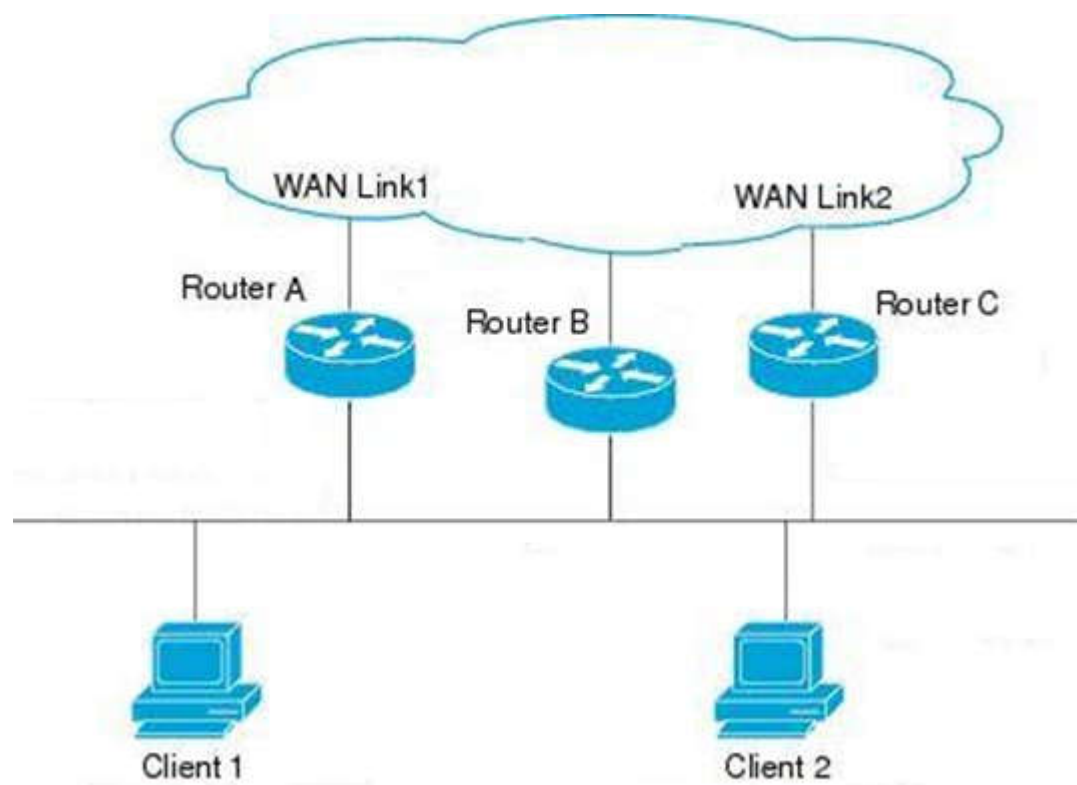
The workstation does not send packets to the active router's real MAC address. It will send packets to virtual router's MAC address.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 289

A company has the following network infrastructure. (Refer to the exhibit.)



Router A is a GLBP active virtual gateway with priority level set to 250. Routers B and C are configured with the default GLPB configurations. The configuration of the active virtual gateway needs to be changed such that if the AVG fails, Router C should be elected to be used as an active virtual gateway. As the network administrator, you have been asked to make corresponding changes to the configuration.

Which command would you use for this purpose on Router C, and where would the command be configured?

- A. glbp 10 preempt (on Router B)
- B. glbp 10 preempt (on Router C)
- C. glbp 10 priority 200 (on Router B)
- D. glbp 10 priority 200 (on Router C)

**Correct Answer: D**

**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**

Explanation:

You would configure the `glbp 10 priority 200` command on Router C to change the configuration as required. Gateway Load Balancing Protocol (GLBP) gateway priority determines the role that each GLBP gateway plays and what happens if the AVG fails. In the given scenario, Router A is used as an active virtual gateway. If the AVG in a LAN topology fails, an election process takes place to determine which backup virtual gateway should take over. When you configure this command on Router C, Router C will be elected when Router A fails as an AVG.

Once the configuration change is made, it can be verified by examining the output of the `show run` command as shown below:

```
RouterC# show run
<output omitted>
interface gigabitEthernet0/0
    ip address 192.168.5.1 255.255.255.0
    duplex auto
    speed auto
    media-type RJ45
    negotiation auto
    glbp ip 192.168.5.3
    glbp timers msec 250 msec 750
    glbp priority 200
<output omitted>
```

In the above output, it can be determined that the `glbp priority 200` command has been applied to the `gigabitEthernet0/0` interface on Router C. If the default priority of 100 had been applied, there would be no line in the output for priority. Because Router B is configured with the default configuration, it will have its priority set to the default level as 100.

You would not use the `glbp 10 preempt` command on Router B or the `glbp 10 preempt` command on Router C to change the configuration. You would use this command on a router to enable preemption. Preemption allows a virtual router that was once the AVG to assume its role as active virtual router when it comes back online if it has a higher priority than the current AVG. Alternatively, it can enable a new router with a higher priority to take the role of AVG from the current AVG if the new router has a higher AVG.

You would use not the `glbp 10 priority 200` command on Router B to change the configuration. You would run this command if you needed Router B to be elected as the AVR instead of Router C, as running this command on Router B would configure it with higher priority than Router C.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Home > End-of-Sale and End-of-Life Products > Cisco IOS Software Releases > 12.2T > Product Literature > White Papers > GLBP - Gateway Load Balancing Protocol

Cisco > Cisco IOS IP Application Services Command Reference > `glbp priority`

**QUESTION 290**

Which of the following statements are TRUE about the selection of the active router in an HSRP group? (Choose two.)

- A. The router with the highest priority becomes the active router.
- B. The router with the lowest priority becomes the active router.
- C. The router with the highest IP address becomes the active router if the priorities of all routers are the same.
- D. The router with the lowest IP address becomes the active router if the priorities of all routers are the same.

**Correct Answer:** AC

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The following two statements are TRUE about the selection of the active router in an HSRP group:

The router with the highest priority becomes the active router.

The router with the highest IP address becomes the active router if the priorities of all routers are the same.

All routers in an HSRP group have a priority. The default priority of HSRP routers is 100. However, HSRP routers can be assigned any value from 0 through 255 by using the `standby priority` command. The router with the highest priority becomes the active router of that HSRP group. The active router is responsible for forwarding packets to and from the virtual router (default gateway).

If the priorities of all the routers in the HSRP group are all the same, then the IP addresses of the routers are considered. The router with the highest IP address of an HSRP interface becomes the active router.

A standby router is also selected for the HSRP group. When the active router of the HSRP group fails, the standby router becomes the active router. You can decrement the priority of the active router if one of its interfaces goes down if you have enabled tracking for the respective HSRP interface. Interface tracking can be enabled by using the `standby track` command. By default, the priority of the active router is decreased by 10 when it goes down.

When the original active router recovers the failed interface, it may become the active router again if the `standby preempt` command was used on the router. This command specifies that if the router has the highest priority in the HSRP group, then it is immediately selected as the active router for the group. Therefore, if you want the original active router to resume the role when it comes online again, the `standby preempt` command should be used during its configuration.

Consider a network segment that has three routers `rtrA`, `rtrB`, and `rtrC` with HSRP enabled all of them. The `rtrA` router is selected as the active route, while `rtrB` is the standby router. The partial output of the `show running-config` command for `rtrA` is as follows:

```

rtrA(config)# show running-config
!
interface FastEthernet0/1
ip address 172.16.88.1 255.255.255.0
standby 1 ip 172.16.88.50
standby 1 priority 150
standby 1 preempt
standby 1 track S0/1 decrement 30
<output omitted>

```

The partial output of the show running-config command for rtrB is as follows:

```

rtrB(config)# show running-config
!
interface FastEthernet0/0
ip address 172.16.88.2 255.255.255.0
standby 1 ip
standby 1 priority
standby 1 preempt
standby 1 track S0/0
<output omitted>

```

Note that either router will be capable of assuming the role of active router if its priority becomes higher for the following reasons:

Decrements in the priority of the active router due to the loss of an interface

A manual change in the priorities by the administrator

The recovery of a down route that comes back online with a higher priority

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Home > Support > Configuring HSRP > How to Configure HSRP

Home > Support > Configuring HSRP > Information About HSRP > HSRP Operation

Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring HSRP

Home > Support > Configuring HSRP > Information About HSRP > HSRP Priority and Preemption

#### QUESTION 291

Which of the following sets of commands CANNOT be included in the plan to implement HSRP on a Layer 3 switch port?

- A. interface port-channel  
no switchport
- B. interface fastethernet  
no switchport  
ip address
- C. interface fastethernet  
switchport mode access
- D. interface vlan  
ip address

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The following set of commands cannot be included in the implementation plan to configure HSRP on a Layer 3 switch port:

```

interface fastethernet
switchport mode access

```

This set of commands creates an access port on the switch. The access port can then be assigned to a VLAN. HSRP cannot be enabled on access ports. To enable HSRP on a switch port, the port has to be any of the following:

EtherChannel port Refers to a Layer 3 switch port used for EtherChannel

Routed port Refers to a Layer 3 port on a switch used for routing

Switch virtual interface (SVI) Refers to a Layer 2 switch port used for inter-VLAN routing

The interface port-channel and no switchport commands allow you to create a Layer 3 port-channel interface, which can be logically bound with other port-channel interfaces to form an EtherChannel. Port-channel interfaces can be configured as either Layer 2 or Layer 3 interfaces. The interface port-channel command is used to create a Layer 3 port-channel interface.

The following set of commands creates a routed port:

```

interface fastethernet
no switchport
ip address

```

Routed ports are physical Layer 3 interfaces that allow you to configure a switch as a router. The no switchport command allows the port to be used purely as a Layer 3 port. This command restarts the port thereby deleting any Layer 2 configuration settings on the switch.

The following set of commands is used to create an SVI, which is a logical interface that allows you to enable inter-VLAN routing on Layer 3 switches:

```

interface vlan
ip address

```



SVIs are configured as VLAN interfaces and have at least one physical interface assigned to the VLANs.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(37)SG > Configuring Layer 3 Interface > Configuring VLANs as Layer 3 Interfaces

#### QUESTION 292

What command provides the output shown below?

```
Vlan10 - Group 1
State is Master
Virtual IP address is 192.168.10.1
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
min delay is 0.000 sec
Priority 100
Mater Router is 192.168.10.100 (local), priority is 100
Master Advertisement interval is 3.000 sec
Mater Down interval is 9.609 sec
```

- A. switch# show vrrp brief
- B. switch# show standby
- C. switch# show glbp
- D. switch# show vrrp

**Correct Answer: D**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command that displays the output in the exhibit is show vrrp. This command displays detailed information regarding VRRP groups on the switch. The information provided for each VRRP group by this command includes the status, virtual IP and MAC addresses, whether preemption is enabled, priority of the switch, and the address of the group master.

The command show vrrp brief is used to display a summary of the VRRP groups to which the switch belongs. The summary information it provides includes the group number, priority, state, whether preemption is enabled, the Master IP address, and the group IP address.

The command show glbp displays detailed information about GLBP groups on the switch. This information includes the GLBP groups the switch is a member of, whether this is the active switch, the virtual IP address, and whether preemption is enabled.

The command show standby can be used to display detailed information about HSRP groups to which a switch belongs. This command displays information about HSRP on all configured interfaces and for all HSRP groups. This command is for HSRP only.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Command Reference > show vrrp

#### QUESTION 293

What command should you use to quickly view the HSRP state of the switch for all HSRP groups of which the switch is a member?

- A. switch# show standby brief
- B. switch# show ip interface brief
- C. switch# show hsrp
- D. switch# show standby

**Correct Answer: A**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command show standby brief should be used to quickly view the HSRP state of a switch for all HSRP groups of which it is a member. The summary information it provides includes the group number, priority, state, active device address, standby address, and group address.

The command show standby can be used to display detailed information about HSRP groups of which a switch is a member. This command would not provide a quick view. This command displays information about HSRP on all configured interfaces and for all HSRP groups. It also displays hello timer information and the expiration timer for the standby switch.

The command show ip interface brief is useful in that lists the interfaces and displays the basic IP configuration of each. This output would include the IP address of the interface and the state of the interface, but not HSRP information.

The command show hsrp is not a valid command due to incorrect syntax.



Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Command Reference > show standby  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 294

Examine the configuration shown below in a partial output of the show run command executed from Router 5.

```
<output omitted>
track 1 interface POS 1/0 ip routing
track 2 interface POS 2/0 ip routing
interface fastethernet 0/0
glbp 156 weighting 120 lower 95 upper 110
glbp 156 weighting track 1 decrement 20
glbp 156 weighting track 2 decrement 10
<output omitted>
```

With this configuration, which of the following is true?

- A. if POS 1/0 goes down, Router 5 will become the AVG.
- B. if POS 1/0 goes down, Router 5 will relinquish its role as AVG.
- C. if POS 1/0 and POS 2/0 go down, Router 5 will relinquish its role as AVG.
- D. if POS 1/0 and POS 2/0 go down, Router 5 will become the AVG.

**Correct Answer: C**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

If POS 1/0 and POS 2/0 go down, Router 5 will relinquish its role as active virtual gateway (AVG). The example indicates that Router 5 is configured a member of Gateway Load Balancing Protocol (GLBP) group 156 and that it is tracking the state of two of interfaces, POS 1/0 and 2/0. An initial weighting value of 120 has been assigned to the router in line 4, and upper and lower thresholds of 95 and 110 have been configured, respectively.

In lines 5 and 6, decrement values of 20 and 10 have assigned to the tracking of interface POS 1/0 and POS2/0, respectively. If either of the tracked interfaces goes down, the weight value of the router will be decreased by the amount of the decrement value. If the weight falls below the lower threshold (95), the router will relinquish its role as the AVG. If either single interface that is being tracked goes down, the weight value will not fall below the lower threshold, and the router will maintain its role of AVG. This occurs because  $120 - 20 = 100$ , which is higher than 95 (the lowest threshold), and  $120 - 10 = 110$ , which is also higher than 95. If both interfaces go down, the value will fall below the lower threshold ( $120 - 10 - 20 = 90$ , which is lower than 95), and the router will give up its role as the AVG.

The loss of interfaces will never cause a router to become the AVG. That can only occur if the router functioning as the current AVG in the group loses its interfaces.

The loss of either of the interfaces alone will not decrement the initial weighting value enough for it to fall below the lower threshold, and therefore will not cause the router to relinquish its role as AVG.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Home > End-of-Sale and End-of-Life Products > Cisco IOS Software Releases > 12.2T > Product Literature > White Papers > GLBP - Gateway Load Balancing Protocol  
Cisco > Cisco IOS IP Application Services Command Reference > threshold metric through weight (real server) > track

#### QUESTION 295

You need to create an implementation plan for providing Layer 3 redundancy in your switched network. You included Hot Standby Routing Protocol (HSRP) as the protocol to avoid first-hop router failure. However, your supervisor suggests including Virtual Router Redundancy Protocol (VRRP) instead of HSRP in the implementation plan.

Which of the following statements is TRUE about the reasons for the suggested change in the implementation plan? (Choose two.)

- A. HSRP works only on Cisco routers and VRRP works on both Cisco and non- Cisco routers.
- B. HSRP works on both Cisco and non-Cisco routers and VRRP works only Cisco routers.
- C. HSRP-enabled routers need to be configured manually to preempt the active router and VRRP-enabled routers preempt it automatically.
- D. HSRP-enabled routers automatically preempt the active router and VRRP-enabled routers need to be configured manually to preempt the active router.

**Correct Answer: AC**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The following two statements are TRUE:  
HSRP works only on Cisco routers and VRRP works on both Cisco and non- Cisco routers.  
HSRP-enabled routers need to be configured manually to preempt the active router and VRRP-enabled routers preempt it automatically.

HSRP was developed by Cisco intended for only Cisco routers and VRRP was developed by IETF intended as a standard for routers. HSRP was defined in RFC 2281 and VRRP was defined in RFC 2338. Both these protocols provide a fault tolerance solution by grouping several routers together but presenting

them as a single router. One of the routers in the group acts as the active or master router. A second router is selected as the standby router. In case the active or master router fails, the standby router takes over the responsibilities of the active router.

The router with the highest priority is automatically selected as the active or master router. In HSRP, preempt settings have to be manually configured on every router in the group, even if the routers have a priority higher than that of the active router. However, in VRRP, the routers with higher priority automatically preempt the master router. Another advantage that VRRP has over HSRP is a faster Hello timer (1 second). HSRP has a Hello timer of 3 seconds

Two other protocols ICMP Router Discovery Protocol (IRDP) and Gateway Load Balancing Protocol (GLBP) provide redundancy for first-hop router failure. IRDP also allows the selection of a new router if the active router fails, while GLBP provides load balancing in addition to redundancy.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Home > Articles > Cisco Certification > CCDP > CCDP Self Study: Designing High-Availability Services  
Cisco First Hop Redundancy Protocols Configuration Guide, Cisco Release 15MT

#### QUESTION 296

In which HSRP state is the router a candidate to become the next active router for the group?

- A. Learn
- B. Backup
- C. Listen
- D. Initial
- E. Standby

**Correct Answer: E**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The HSRP router in standby state (the standby router) is a candidate to become the next active HSRP router should the current active router fail.

The six HSRP states are defined as follows:

Initial state: All routers start in this state.

Learn state: The router is in the learn state when it has not communicated with the active router. It does not know which router is the active router and does not know the IP address of the virtual router (if no HSRP IP address configured in the router).

Listen state: Once the router hears from the active router and knows the virtual IP address, it enters the listen state. It is not the active or standby router.

Speak state: After a router learns the IP address of the virtual router, it enters the speak state. It participates in the active and standby router election. It sends hello messages to the active router.

Standby state: When the active router has been elected, the second router enters the standby state. This is the standby router and it will become the active router if the active router fails.

Active state: The router is in active state when it is forwarding packets. It receives packets via the virtual IP address.

Backup is not a valid HSRP router state.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring HSRP

#### QUESTION 297

How is load balancing achieved when implementing HSRP?

- A. By configuring multiple gateways on the routers
- B. By using multiple HSRP groups
- C. By configuring the same priority on all HSRP group members
- D. By configuring multiple virtual router addresses

**Correct Answer: B**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

When implementing Hot Standby Router Protocol (HSRP), load balancing is achieved by using multiple HSRP groups. Routers configured for HSRP can belong to multiple groups and multiple VLANs. By configuring one group to be active for Router A and standby for Router B, and the second group to be active for Router B and standby for Router A, both routers A and B can be used to pass traffic, as opposed to one sitting idle.

Load balancing cannot be achieved by configuring multiple gateways on the routers. The routers have one IP address. Each group will have a virtual IP address. In the configuration below, line 4 configures the virtual IP address, and is therefore the address that clients will use as their gateway:

```
interface fastethernet 0/1
no switchport
ip address 192.168.5.5 255.255.255.0
standby 1 ip 192.168.5.10
```

Load balancing cannot be achieved by configuring the same priority on all HSRP group members. If that were done, one of the routers would become active and the others would remain inactive standbys. The active router will be the one with the highest IP address.

Load balancing cannot be achieved by configuring multiple virtual router addresses. Each HSRP group can only have one virtual address.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing

#### QUESTION 298

Which routers comprise a VRRP group?

- A. Host and client
- B. Master and backup
- C. Active and standby
- D. Primary and secondary

**Correct Answer: B**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

Virtual Router Redundancy Protocol (VRRP) enables a group of routers to form a single virtual router, known as a VRRP group. Routers are configured in VRRP groups to provide redundancy for a virtual IP address shared among members of the VRRP group. Each group is comprised of a master router and one or more backup routers. The physical IP address of the master router will be the virtual IP address of the group.

The master router is responsible for forwarding packets sent to the virtual router. The backup routers provide redundancy and stand ready to assume the role of the master router in the event that the master is unable to forward packets.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco > Cisco IOS IP Application Services Configuration Guide, Release 12.4 > Part 1: First Hop Redundancy Protocols > Configuring VRRP

#### QUESTION 299

Which of the following is required to allow load balancing between three HSRP routers connected to the same LAN?

- A. A single HSRP group with all three routers as active routers for the group
- B. A single HSRP group with one active router for the group
- C. Two HSRP groups, each with an active router
- D. Two HSRP groups with one active router for both the groups
- E. Three HSRP groups, each with an active router
- F. Three HSRP groups with one active router for all groups

**Correct Answer: E**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

You should configure three HSRP groups on all three routers and select an active router for each of the groups. You can create up to 256 (0 to 255) groups. Each router should be the active router for one of the three groups and the standby router for the remaining two groups.

If you want to use HSRP on a Layer 3 switch, the switch ports must be one of the following:  
EtherChannel port Refers to a Layer 3 switch port used for EtherChannel  
Routed port Refers to a Layer 3 port on a switch used for routing and for inter-VLAN routing  
Switch virtual interface (SVI) Refers to a Layer 2 switch port used for inter-VLAN routing

Routed ports are the physical Layer 3 interfaces that allow you to configure a switch as a router. The no switchport command allows the port to be used purely as a Layer 3 port. SVIs are Layer 3 logical interfaces of a switch that allow you to enable inter-VLAN routing on Layer 3 switches. An SVI is configured as a VLAN interface and has at least one physical interface assigned to the VLANs.

Creating a single HSRP group with all three routers as active routers for the group is incorrect. An HSRP group cannot have multiple active routers; it can have only one active router at a time.

Creating a single HSRP group with one active router for the group is incorrect because it does not allow load balancing between the three routers. All traffic will be passed through the active router.

Creating two HSRP groups with an active router each is incorrect because it only allows load balancing between two of the routers and not three of them.

Creating two HSRP groups with one active router for both groups, or three HSRP groups with one active router for all groups, is incorrect. Doing so does not enable load balancing on all three routers. Only the active router will be used for traffic forwarding.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Internetworking Case Studies > Using HSRP for Fault-Tolerant IP Routing > Configuring Multiple Hot Standby Groups > Load Sharing  
Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE > Configuring HSRP > Configuring HSRP > HSRP Configuration Guidelines  
Catalyst 3750 Switch Software Configuration Guide, 12.2(40)SE > Configuring HSRP > Configuring HSRP > Multiple HSRP

#### QUESTION 300

Which virtual router states are defined in the GLBP protocol? (Choose two.)

- A. Backup gateway
- B. Primary gateway
- C. Active virtual gateway
- D. Active secondary gateway
- E. Active virtual forwarder

**Correct Answer:** CE

**Section:** Infrastructure Services

**Explanation**

**Explanation/Reference:**

Explanation:

Active virtual gateway and active virtual forwarder are the two states defined in the Gateway Load Balancing Protocol (GLBP). The active virtual gateway (AVG) is elected by the members of the GLBP group. The AVG creates the virtual MAC addresses that are assigned to each of the routers in the group. Each router is responsible for handling packets sent to its virtual MAC address. A GLBP router that forwards packets sent to its virtual MAC address is known as the active virtual forwarder (AVF). GLBP members communicate through hello messages sent every 3 seconds to the multicast address 224.0.0.102.

The election of the AVG can be influenced by use of the priority command. By default, all routers configured for GLBP have a priority of 100. A higher value indicates a higher priority. The configured priority of a router can be seen in the show run command as shown below:

```
<output omitted>
interface FastEthernet0/0
ip address 192.168.5.6 255.255.255.00
duplex auto
speed auto
<output omitted>
glbp ip 192.168.5.10
glbp priority 150
```

In the above scenario, all other members of the group were left to the default, which can be determined on those routers by the absence of any priority entry in the show run command. In that case, this router would become the AVG. To remove a priority configuration, execute the nostandby priority command. When this command is executed, the router will revert to the default of 100. When all routers are left to the default, the router with the highest configured IP address will become the active router.

GLBP is a Cisco-designed protocol that provides for the dynamic utilization of redundant routers in a broadcast network. It differs from HSRP and VRRP in that it is not necessary to configure multiple groups to fully use redundant paths or routers. GLBP has a configurable load-balancing mechanism that will distribute the use of redundant gateways servicing a broadcast network, such as an Ethernet LAN. Each host will have its gateway set to the address of the AVG. When a host issues an ARP to resolve its gateway's MAC Address, the AVG will respond with the virtual MAC address of a selected AVF. The AVG will perform load balancing by varying which virtual MAC it selects to use in the response. The AVF will own that assigned virtual MAC as long as the gateway is active. If an AVF becomes unable to provide service as gateway, another AVF can assume ownership of the virtual MAC.

Consider the partial output of the show run command for two routers participating in the GLBP group shown below:

```
RouterA# show run
<output omitted>
interface vlan 12
ip address 192.168.5.3 255.255.255.0
glbp 15 ip 192.168.5.5
glbp priority 100

RouterB#show run
<output omitted>
interface vlan 12
ip address 192.168.5.6 255.255.255.0
glbp 15 ip 192.168.5.5
glbp priority 100
```

In the above scenario, both routers have the same priority, so Router B will become AVG. Hosts will use a gateway address of 192.168.5.5 (the GLBP virtual address in line 4 of both outputs). When hosts send an ARP message for the MAC address of the gateway, Router B will reply with the MAC address of the next AVF.

The AVG can be configured to use one of three load-balancing algorithms:

Round-Robin Load-Balancing: Using round-robin load- balancing the AVG in turn points to each AVF virtual MAC address in its ARP reply (default method).

Weighted Load-Balancing: Using weighted load- balancing, the AVG selects an AVF virtual MAC address to use in the ARP reply proportionally based on the advertised weight value configured in a GLBP gateway.

Host Dependant Load-Balancing: Using host-dependant load- balancing, the AVG selects an AVF virtual MAC address to use in the ARP reply based on which one the host used previously. A host will use the same AVF as long as the GLBP group is unchanged.

GLBP allows better use of network resources by using the standby router through the load-balancing mechanism. The standby router is an available gateway for the network.

GLBP and HSRP are Cisco-developed solutions. VRRP is defined in RFC 2338.

Backup gateway, primary gateway, and active secondary gateway are not terms used when discussing GLBP.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

**QUESTION 301**

You are in the process of verifying the operation of your core switches, which are using HSRP. One core switch was left with the default priority; the other was given a lower priority to make it the standby switch. The command show standby brief was executed on one of the switches. Output of the command is shown below:

| Interface | Grp | Prio | P | State  | Active | Standby       | Virtual IP   |
|-----------|-----|------|---|--------|--------|---------------|--------------|
| Vl10      | 1   | 90   | P | Active | local  | 192.168.10.20 | 192.168.10.1 |
| Vl20      | 1   | 90   | P | Active | local  | 192.168.20.20 | 192.168.20.1 |

What does this output mean? (Choose all that apply.)

- A. this switch is using the default priority
- B. this switch is the active HSRP switch
- C. the HSRP devices are up and functioning correctly
- D. the switch intended to be the active switch has failed and this switch has taken over
- E. preemption is enabled for the group

**Correct Answer:** BDE  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

The output in the exhibit indicates that this switch is the active HSRP switch, the switch intended to be the active switch has failed, and that preemption is enabled for the group.

This is the active switch because Active is the State listed for each interface that is a member of HSRP.

The question states that the switch that was intended to be the standby switch was given a priority lower than the default. The default priority is 100, so this is not the switch intended to be the active switch. This information indicates that the switch intended to be the active switch has failed.

Preemption is enabled, as indicated by the P following the priority value in line 2. Since preemption is enabled, the switch with the priority of 100 is still down. When that switch is corrected and joins the group again, it will take over as active.

The HSRP group is still providing access for users, but not all devices are functioning properly.

Objective:  
Infrastructure Services  
Sub-Objective:  
Configure and verify first-hop redundancy protocols

References:  
Cisco IOS Master Command List, Release 12.4T>show ip route profile through sshow mpls atm-ldp summary>Cisco IOS IP Application Services Command Reference>show standby through show udp>show standby

**QUESTION 302**

You are troubleshooting a problem with two routers configured in a HSRP group. You intended to configure the routers so that Router A and Router B would each track their respective Fa0/1 interfaces and decrement their priorities for several VLAN groups if the tracked interface went down. However, you find that Router A is not taking over as the active device for the HSRP group on VLAN 101 when the Fa0/1 interface on Router B fails.

Which command would NOT be useful for discovering the problem?

- A. show running-configuration
- B. show vlans
- C. show standby brief
- D. show standby

**Correct Answer:** B  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

The show vlans command would NOT be useful for discovering the problem. When troubleshooting a problem with Hot Standby Router Protocol (HSRP), the show vlans command will yield no useful information. The output of the command is shown below, demonstrating that there is no HSRP information provided.

| router# show vlan trunk |          |        |         |                  |
|-------------------------|----------|--------|---------|------------------|
| VLAN                    | Name     | Status | IfIndex | Mod/Ports, Vlans |
| 1                       | default  | active | 5       | 2/1-2 6/4-8      |
| 15                      | VLAN0015 | active | 18      | 6/1, 6/3         |
| 16                      | VLAN0016 | active | 19      | 6/2              |
| 23                      | VLAN0023 | active | 20      |                  |
| 26                      | VLAN0026 | active | 21      |                  |
| 31                      | VLAN0031 | active | 22      |                  |
| 39                      | VLAN0039 | active | 23      |                  |

All three of the remaining commands will be useful in discovering information. Each is shown below with an example of its application to troubleshooting.

Example A:show running-configuration



Router B is not taking over as the active device for VLAN 101's HSRP group when the Fa0/1 interface on Router A fails. Below is a partial output of show run for both routers with the output focused on the section concerning VLAN 101's configuration on each.

```
routerA                               routerB
interface Vlan101                     interface vlan101
<output omitted>
Standby 5 ip 172.63.51.250            Standby 5 ip 172.63.51.250
Standby 5 priority 180                 Standby 5 priority 170
standby preempt                        standby preempt
standby track Fastethernet 0/1 5      Standby track Fastethernet 0/1
```

The above output displays the source of the problem. Router A has a decrement value of 5 configured for Fa0/1, as shown on the last line of the output after the specification of Fastethernet 0/1. This means that when its Fa0/1 interface goes down, Router A will subtract 5 from its priority for the VLAN 101 group, lowering it to 175. This is still higher than the priority of Router B, which is 170. Therefore, the solution is to change the decrement value for Router A to at least 11. When the interface goes down, Router A's priority will be decremented to 169, allowing Router B to take the role as active for the HSRP group in VLAN 101.

Example B: show standby brief

Router C is not taking over as the active device for VLAN 102's HSRP group when the Fa0/1 interface on Router D fails. Below is a partial output of show standby brief for both routers C and D, with the output focused on the section concerning VLAN 102's configuration on each.

Router C

```
Interface Grp Prio P State Active addr Standby addr Group addr
Fa0/1 102 200 Active local 10.10.10.253 10.10.10.251
```

Router D

```
Interface Grp Prio P State Active addr Standby addr Group addr
Fa0/1 102 200 P Active local 10.10.10.253 10.10.10.251
```

The absence of a P in the P (preempt) column in the output for Router C shows that it is not set to preempt. If not configured to preempt, it will never take over for Router D, regardless of its priority with respect to Router D.

Example C: show standby

Router F is supposed to be the active router for VLAN 103's HSRP group. Occasionally both routers are shut down for maintenance over the weekend. After the routers are rebooted, Router F is not taking over as the active device for VLAN 103's HSRP group. Below is a partial output of the show standby command for both routers, with the output focused on the section concerning VLAN 103's configuration on each

Router E

```
Fastethernet 0/1 - Group 1
State is Active
2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is 10.1.6.0.6, priority 200(expires in 9.184 sec)
Standby router is local
Priority 200 (configured 200)
Tracking interface Fastethernet 0/1 state up decrement 10
```

Router F

```
Fastethernet 0/1 - Group 1
State is Active
2 state changes, last state change 00:30:59
Virtual IP address is 10.1.0.20
Secondary virtual IP address 10.1.0.21
Active virtual MAC address is 0004.4d82.7981
Local virtual MAC address is 0004.4d82.7981 (bia)
Hello time 4 sec, hold time 12 sec
Next hello sent in 1.412 secs
Preemption enabled, min delay 50 sec, sync delay 40 sec
Active router is local
Standby router is 10.1.0.6, priority 200 (expires in 9.184 sec)
Priority 190 (configured 190)
Tracking interface Fastethernet 0/1 state up decrement 50
```

The output shows that Router F is not assuming the active role because of the priority and decrement values configured on the routers. When both routers

go down, Router E will decrement its priority (200) by 10, as shown in last two lines of its output, leaving the priority at 190. Router F will decrement its priority (190) by 50 as shown in last two lines of its output, leaving the priority at 140. Therefore, to ensure that Router F maintains its role as active even after the dual shutdowns, the priority of Router F should be increased to at least 241. When both routers decrement their priorities after shutdown, Router F will then have a priority of 191, which will be higher than the priority value of Router E.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks

Cisco > Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > How to Use the standby preempt and standby track Commands

### QUESTION 303

Refer to the following partial output of the debug standby command on an HSRP-enabled router rtrA:

```
rtrA#debug standby
!
!
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 Active router is 10.5.5.1
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 state Listen - > Speak
SB:FastEthernet0/0 Hello out 10.5.5.2 Speak pri 120 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 Hello in 10.5.5.1 Active pri 100 hel 3 hol 10 ip 10.5.5.5
SB:FastEthernet0/0 state Standby - > Active
SB:FastEthernet0/0 Active router is local, was 10.5.5.1
SB:FastEthernet0/0 Hello out 10.5.5.2 Active pri 120 hel 3 hol 10 ip 10.5.5.5
<output omitted>
```

Which of the following information CANNOT be gathered from the given partial output?

- A. IP address of the virtual router
- B. IP address of the current active router
- C. Priority of the active router
- D. The tracked interfaces

**Correct Answer: D**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The debug standby command does not provide any information about the tracked HSRP interfaces. This command displays information regarding the changes in the state of the HSRP routers and packet transmissions between the routers. Some of the information that you can view using the debug standby command is as follows:

IP address of the virtual router

IP address of the current active router

Priority of the active router

Hello timer values

Hold time values

State of the router

Interface used to exchange HSRP packets

HSRP packets contain the IP address of the virtual router. The IP address preceded by the text ip in the debug standby output is the address of the virtual router. In this case, the packets contain 10.5.5.5 after the text ip. This implies that 10.5.5.5 is the IP address of the virtual router.

After HSRP selects the active and standby routers for a group, only the active and standby routers send HSRP packets to the virtual router. If the active router fails, the standby router becomes the active router. The text Hello in and the text Hello out indicate the hello packets received from and sent to the given IP address. Initially the router with IP address 10.5.5.1 is the active router, as indicated by the text Active router is 10.5.5.1.

The priority of the active router is 100, which is indicated by the text pri 100. However, when a hello packet from 10.5.5.2 is received, which has a higher priority (120) than the active router, the 10.5.5.2 router automatically and instantly becomes the active router. This implies that the router with the IP address 10.5.5.2 was the standby router and the standby preempt command was executed.

Objective:

Infrastructure Services

Sub-Objective:

Configure and verify first-hop redundancy protocols

References:

Cisco IOS Debug Command Reference > debug snmp adjust Through debug tag-switching xtagatm vc > debug standby

Home > Support > Technology Support > IP > IP Application Services > Configure > Configuration Examples and Technotes > Avoiding HSRP Instability in a Switching Environment with Various Router Platforms > Troubleshoot > Troubleshooting Commands > Sample Debug Output

Home > Support > Technology Support > IP > IP Application Services > Design > Design Technotes > Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks > Understand HSRP

### QUESTION 304

You have executed the following commands on switchA:



```

switchA(config)# dot1x system-auth-control
switchA(config)# aaa new-model
switchA(config)# radius-server host 192.168.105.67 key firstKey111
switchA(config)# aaa authentication dot1x default group radius
switchA(config)# interface range Fa 0/1 - 11
switchA(config-if)# switchport mode access
switchA(config-if)# dot1x port-control auto

```

What is the result of executing the given commands? (Choose two.)

- A. Only the listed RADIUS server is used for authentication
- B. 802.1X authentication is enabled on the Fa0/1 interface only
- C. The key for the RADIUS server is firstKey111
- D. AAA is not enabled on the switch

**Correct Answer:** AC  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

A default list is used for the RADIUS server for authentication and the key for the RADIUS server is firstKey111. A RADIUS server combines the authentication and authorization processes. Before you configure the RADIUS server, you should enable AAA by using the aaa new-model command in the global configuration mode. Then, you can specify the location of the RADIUS server and the key using the radius-server host command. In this case, the RADIUS server is located at the IP address 192.168.105.67 and requires the key firstKey111 as the encryption key. This key must be mutually agreed upon by the server and the clients.

The aaa authentication dot1x default group radius command creates a method list for 802.1X authentication. The default group radius keywords specify that the default method will be to use all listed RADIUS servers to authenticate clients. Since only one is listed, it will be the only one used.

It is incorrect to state that 802.1X authentication is enabled on the Fa0/1 interface only. The interface range Fa 0/1 - 11 and the dot1x port-control auto commands specify that 802.1X authentication is enabled on the interfaces Fa0/1 to Fa0/11.

It is incorrect to stat that AAA is not enabled on the switch. The aaa new-model command enables AAA globally on the switch.

Objective:  
Infrastructure Security  
Sub-Objective:  
Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

References:  
Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(31)SG > Configuring 802.1X Port-Based Authentication  
Cisco IOS LAN Switching Command Reference (PDF)

### QUESTION 305

DRAG DROP

Match the name of the Layer 2 network attack on the left with the description on the right.

**Select and Place:**

| Network Attack: | Descriptions:                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAC Flooding    | This attack involves unauthorized clients or servers on the network that may be running applications that allow unauthorized access to the network.              |
| VLAN Hopping    | This attack causes an overflow in a switch CAM table thus causing the switch to act like a hub.                                                                  |
| Rogue Devices   | This attack involves an unauthorized server that provides incorrect configuration information to clients thus allowing the attacker to view all network traffic. |
| DHCP Spoofing   | This attack sends packets with double tagged frames thus allowing access to normally inaccessible broadcast domains.                                             |

**Correct Answer:**

| Network Attack: | Descriptions:                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 | Rogue Devices<br>This attack involves unauthorized clients or servers on the network that may be running applications that allow unauthorized access to the network.              |
|                 | MAC Flooding<br>This attack causes an overflow in a switch CAM table thus causing the switch to act like a hub.                                                                   |
|                 | DHCP Spoofing<br>This attack involves an unauthorized server that provides incorrect configuration information to clients thus allowing the attacker to view all network traffic. |
|                 | VLAN Hopping<br>This attack sends packets with double tagged frames thus allowing access to normally inaccessible broadcast domains.                                              |

**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**

Explanation:

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > Cisco Catalyst 6500 Series Switches > VLAN Security White Paper

#### QUESTION 306

You want to configure your Catalyst 6500 switch to redirect certain IP traffic from VLANs 22 through 33 to the Gigabit Ethernet interface that resides at slot 4, port 1. The IP traffic to be redirected must match an ACL named tn1.

Which of the following sets of commands should you issue?

- A. `vlan access-map 22-33``match ip address tn1``action redirect gigabitethernet 4/1``vlan filter tn1`
- B. `vlan access-map ge1``match ip address tn1``action redirect gigabitethernet 4/1``vlan filter ge1` `vlan-list 22-33`
- C. `vlan access-map tn1``match ip address ge1``action redirect gigabitethernet 4/1``vlan filter tn1` `vlan-list 22 33`
- D. `vlan access-map ge1``match ip address tn1``action redirect gigabitethernet 4/1``vlan filter ge1` `vlan-list 22 33`

**Correct Answer: B**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

To appropriately configure your Catalyst 6500 switch in this scenario, you should issue the following commands:

```
Switch(config) vlan access-map ge1
Switch(config-access-map) match ip address tn1
Switch(config-access-map) action redirect gigabitethernet 4/1
Switch(config-access-map) exit
Switch(config) vlan filter ge1 vlan-list 22-33
```

VLAN access control lists (VACLs) are used to control how packets are switched within a virtual local area network (VLAN). To configure a VACL, you should perform the following actions:

Define the VLAN access map by issuing the `vlan access-map` command.

Define the configured ACL that traffic must match for an action to be triggered by issuing the `match` command; any traffic that does not match the conditions specified by the configured ACL or ACLs is dropped.

Define the action that will be triggered when traffic matches the configured ACL by issuing the `action` command.

Apply the VACL to one or more VLANs by issuing the `vlan filter` command.

The syntax for the `vlan access-map` command is `vlan access-map map-name [sequence-number]`, where `map-name` is the name assigned to the VLAN access map. The optional `sequence-number` parameter defines the order in which the access map statements are checked. Therefore, the command `vlan access-map ge1` creates a VLAN access map named `ge1` with no sequence number.

The `match` command can filter traffic based on IP address, IPX address or Media Access Control (MAC) address. The syntax for the `match` command is `match {ip address {acl-number | acl-name} | ipx address {acl-number | acl-name} | mac address acl-name}`, where `acl-number` and `acl-name` are the number and name of the access list, respectively. Therefore, the command `match ip address tn1` specifies that only traffic that matches ACL `tn1` will trigger the action specified in the action command.

The action command will configure the VACL to drop, forward, or redirect traffic that matches the access list specified in the match command. The syntax for the action command is `action {drop | forward | redirect interface slot/port}`. Therefore, the command `action redirect gigabitethernet 4/1` will redirect traffic that matches the access list to Gigabit Ethernet interface 4-1.

The syntax for the `vlan filter` command is `vlan filter map-name {vlan-list vlan-list}`, where `map-name` is the name of the VLAN access map and `vlan-list` is the VLAN or VLANs that should be filtered by the VACL. Therefore, the command `vlan filter ge1 vlan-list 22-33` applies the VLAN access map named `ge1` to VLANs 22 through 33.

The following command set incorrectly specifies the VLAN access map and filter:

```
Switch(config) vlan access-map 22-33
Switch(config-access-map) match ip address tn1
Switch(config-access-map) action redirect gigabitethernet 4/1
Switch(config-access-map) exit
Switch(config) vlan filter tn1
```

The following command set incorrectly specifies the VLAN access map and the match statement. This command is also missing the required hyphen in the list of VLANs specified after the `vlan-list` keyword:

```
Switch(config) vlan access-map tn1
Switch(config-access-map) match ip address ge1
Switch(config-access-map) action redirect gigabitethernet 4/1
Switch(config-access-map) exit
Switch(config) vlan filter tn1 vlan-list 22 33
```

This following command is missing the required hyphen in the list of VLANs specified after the `vlan-list` keyword:

```
Switch(config) vlan access-map ge1
Switch(config-access-map) match ip address tn1
Switch(config-access-map) action redirect gigabitethernet 4/1
Switch(config-access-map) exit
Switch(config) vlan filter ge1 vlan-list 22 33
```

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists  
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > snmp ifindex clear through vtp v2-mode > vlan access-map

Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > interface port-channel through shape > match  
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > snmp ifindex clear through vtp v2-mode > vlan filter  
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > action

**QUESTION 307**

Which PVLAN port type can only send frames to promiscuous ports?

- A. private
- B. promiscuous
- C. isolated
- D. community
- E. public

**Correct Answer: C**

**Section: Infrastructure Services**

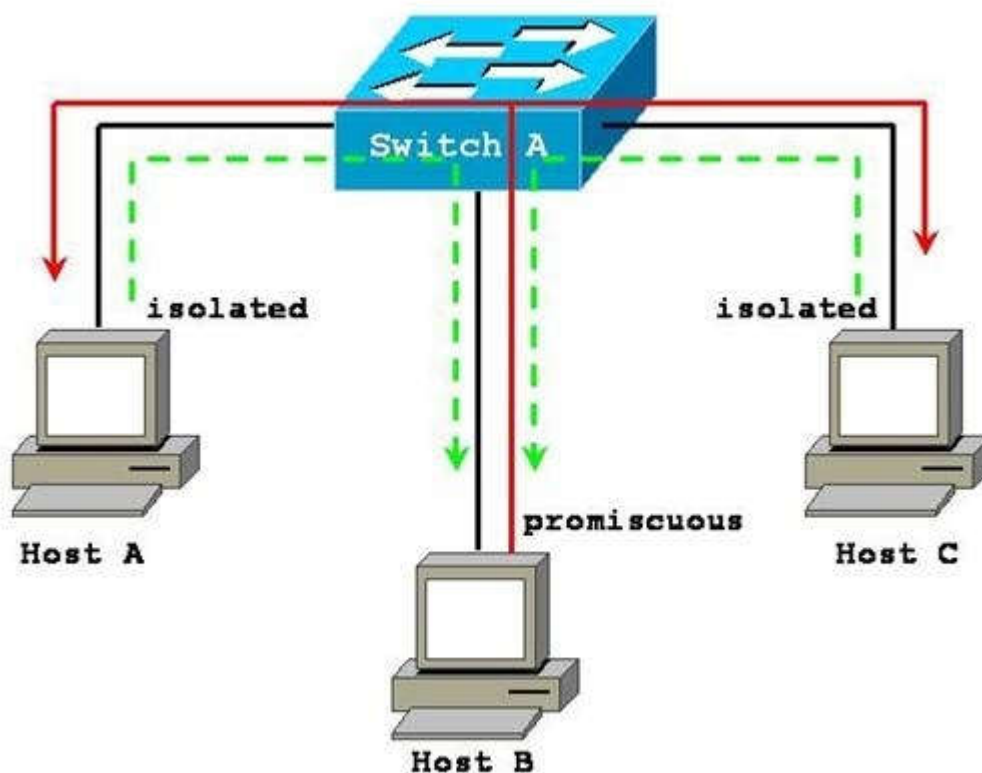
**Explanation**

**Explanation/Reference:**

Explanation:

There are three types of ports in a private VLAN (PVLAN): promiscuous, isolated, and community. A PVLAN isolated port type can only send frames to promiscuous ports.

Consider the following graphic:



Host B is attached to a promiscuous mode port. In this mode, Host B can send and receive frames with other promiscuous, isolated, or community ports assigned to the same private VLAN. Therefore, frames can be exchanged with Hosts A or C. Hosts A and C are attached to isolated ports. Isolated ports are able to send frames to promiscuous ports but not to each other.

Isolated and promiscuous ports can be combined to achieve a desired level of separation between particular machines while still allowing required access to services. As another example, suppose that security policy dictated that Host A and Host C cannot communicate with one another, but both computers needed to access a database on Host B. The isolated ports keep them from communicating with one another, while the use of a promiscuous port to Host B allows them to access the database. Any other resources in the network that either machine needs access to should be therefore connected with a promiscuous port.

The third type of port is a community port. A community port can communicate with other community ports of the same private VLAN or promiscuous ports.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists

**QUESTION 308**

Which IOS interface configuration command is required to configure a switch port to be a promiscuous PVLAN access port?

- A. switchport mode promiscuous
- B. switchport mode promiscuous-vlan
- C. switchport mode private-vlan host
- D. switchport mode private-vlan promiscuous

**Correct Answer: D**

**Section: Infrastructure Services**



## Explanation

### Explanation/Reference:

Explanation:

A promiscuous port type can send frames to all other ports in the same private VLAN (PVLAN). The switchport mode private-vlan promiscuous command configures a port to be a promiscuous port. The syntax is as follows:

```
switch(config-if)# switchport mode private-vlan promiscuous
```

There are three types of ports in a private VLAN (PVLAN): promiscuous, isolated, and community. A promiscuous port can send and receive frames with other promiscuous, isolated, or community ports assigned to the same private VLAN. Isolated ports are able to send frames to promiscuous ports, but not to each other. A community port can communicate with other community ports of the same private VLAN or with promiscuous ports.

Private VLANs are supported on switches that allow the configuration of primary and secondary VLANs. A primary VLAN carries the traffic between the promiscuous port and the isolated and community ports assigned to the same primary VLAN. There are two types of secondary VLANs, isolated and community. Isolated VLANs carry traffic from isolated ports to promiscuous ports. Community VLANs carry traffic between community ports and to the promiscuous port. Therefore, on a promiscuous port, you would use the following command syntax to configure its primary and secondary VLANs:

```
switch(config-if)# private-vlan mapping primary_vlan_id secondary_vlan_id
```

PVLANS are created using the following special VLAN configuration commands:

```
switch(config)# vlan vlan_id
switch(config-vlan)# private-vlan [primary | isolated | community]
switch(config-vlan)# private-vlan association secondary_vlan_list
```

Host ports are defined using the following special PVLAN configuration command:

```
switch(config-if)# switchport mode private-vlan host
```

The command used for isolated and community ports is as follows:

```
switch(config-if)# switchport mode private-vlan host-association primary_vlan_id secondary_vlan_id
```

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists  
Cisco > Cisco IOS Interface and Hardware Component Command Reference > switchport mode

### QUESTION 309

As the network administrator, you have enabled port security on the Fa0/1 port of a switch. Fa0/1 is not a trunk port. You have configured the port security so that the MAC addresses 1111.1111.1111 and 2222.2222.2222 are allowed to connect to the switch port.

Which of the following commands were required to configure the port security so that only the MAC addresses 1111.1111.1111 and 2222.2222.2222 are allowed to connect to the switch port.? (Choose all that apply.)

- A. switchport mode trunk
- B. switchport port-security
- C. switchport mode access
- D. switchport port-security maximum 2
- E. switchport port-security maximum 3

**Correct Answer:** BCD

**Section:** Infrastructure Services

**Explanation**

### Explanation/Reference:

Explanation:

The following commands were executed on the switch port:

```
switchport mode access
switchport port-security
switchport port-security maximum 2
```

The switchport mode access command configures the switch port as an access port. The switchport port-security command enables port security on the switch port. The switchport port-security maximum 2 command specifies that at most two MAC addresses can be connected to the switch port.

The complete set of commands that were executed on the Fa0/1 of the switch port is as follows:

```
swtA(config)# interface Fa0/1
swtA(config-if)# switchport mode access
swtA(config-if)# switchport port-security
swtA(config-if)# switchport port-security maximum 2
swtA(config-if)# switchport port-security mac-address 1111.1111.1111
swtA(config-if)# switchport port-security mac-address 2222.2222.2222
```

It is not required that the switchport port-security aging be executed. This can be used to specify the duration for which all addresses are secured.

The switchport port-security maximum 3 command was not execute on the switch port. This command specifies that three MAC addresses can be allowed on that switch port, instead of only two secure MAC addresses.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Home > Articles > Network Technology > General Networking > Basic Cisco IOS Software and Catalyst 3550 Series Security > Catalyst 3550 Security  
Cisco > Cisco IOS Security Command Reference > switchport port-security

#### QUESTION 310

Which type of network attack takes advantage of the Dynamic Trunking Protocol (DTP)?

- A. VLAN hopping
- B. MAC flooding
- C. DHCP spoofing
- D. Rogue access points

**Correct Answer: A**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

VLAN hopping is an attack designed to gain unauthorized access to a VLAN by using DTP to negotiate a trunk link with another switch. If a switch port configured as DTP auto was to receive a fake DTP packet, it might become a trunk port and begin accepting traffic destined for any VLAN. Therefore, a malicious user could start communicating with other VLANs through that compromised port.

A MAC flooding attack does not use DTP as a part of its operation. This attack floods the switch with fake MAC addresses until the MAC table is full. When this happens, the switch starts sending all frames out all ports, allowing the hacker to capture data from all ports.

DHCP snooping does not use DTP as a part of its operation. It is not an attack but a security measure. DHCP snooping filters un-trusted DHCP messages using a DHCP snooping binding database. A DHCP snooping binding database is also referred to as a DHCP snooping binding table. This can be used to prevent a rogue DHCP server from assigning configuration information to clients.

Rogue access points do not use DTP as a part of their operation. These are unauthorized access points connected to an open switch port or wall outlet for the purpose of gaining access to the wired network wirelessly.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Home > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > VLAN Security White Paper

#### QUESTION 311

What command should be used to view the private VLANs configured on ports and the private VLAN mappings?

- A. show vlan brief
- B. show pvlan
- C. show interfaces switchport
- D. show mac-address-table

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The command show interfaces switchport is used to verify private VLANs configured on ports and the private VLAN mappings. The following is a sample of the output:

```

Switch# show interfaces fastethernet 3/1 switchport
Name:Fa3/1
Switchport:Enabled
Administrative Mode:private-vlan promiscuous
Operational Mode:private-vlan promiscuous
Administrative Trunking Encapsulation:negotiate
Operational Trunking Encapsulation:native
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Voice VLAN:none
Administrative Private VLAN Host Association:none
Administrative Private VLAN Promiscuous Mapping:200 (VLAN0200) 20 (VLAN0020)
Private VLAN Trunk Native VLAN:none
Administrative Private VLAN Trunk Encapsulation:dot1q
Administrative Private VLAN Trunk Normal VLANs:none
Administrative Private VLAN Trunk Private VLANs:none
Operational Private VLANs:
200 (VLAN0200) 20 (VLAN0020)
Trunking VLANs Enabled:ALL
Pruning VLANs Enabled:2-1001
Capture Mode Disabled
Capture VLANs Allowed:ALL

```

This output reveals that Fa3/1 is a promiscuous port in private VLAN (PVLAN) 20. PVLAN 20 is a member of the primary VLAN 200. Since this is a promiscuous port, it is able to exchange information with all other PVLANS associated with VLAN 200.

The show vlan brief command is only used to view the VLANs that exist and the ports that are members of them. No information about PVLANS and member association is included.

The show mac-address-table command is used to view the MAC addresses stored in the switches memory and the port and VLAN they are members of. No information about PVLANS is included in this output.

The command show pvlan is incorrect due to invalid syntax.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Cisco IOS Interface and Hardware Component Command Reference > show hw-module slot tech-support through show interfaces vg-anylan > show interfaces fastethernet

### QUESTION 312

What is accomplished by the command switchport port-security violation protect?

- A. The switch will generate a log message but will not block any packets
- B. The switch will drop packets that are in violation and generate a log message
- C. The switch will drop packets that are in violation, but not generate a log message
- D. The switch will shut down the interface when packets in violation are detected

**Correct Answer: C**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

The command switchport port-security port violation protect will cause the switch to drop packets that are in violation, but does not generate a log message. The complete syntax of the command is:

```
switch(config-if)# switchport port-security violation protect
```

The port-security command is used to lock a port to a specific MAC addresses. Port security can be used to limit access to a port by MACaddress. It can be applied to:

access ports

VoIP ports

ports where multiple MAC addresses are expected, such as a port connecting to a hub

It cannot be applied to trunk ports or to ports that are part of an Etherchannel.

Three keywords can be used with this command: protect, restrict and shutdown. The restrict keyword tells the port to drop packets and generate a log message for packets that are in violation. The protect keyword tells the port to drop packets without generating a log message for packets that are in violation. The shutdown keyword causes the port to be place into the errdisable state if a violation is detected.

The following configuration, generated from a partial output of the show run command, would apply port security to the Fa0/1 interface. It would allow five addresses to access the interface at time. This count includes addresses that have been seen by the port but are currently inactive. Therefore, if five addresses have been seen and three are inactive, then a sixth address would not be allowed. If the port security maximum command has not been issued, the default behavior will only allow one address on the port.

The aging command can be used to force inactive addresses to be dropped from the list of addresses seen, thereby allowing active addresses access to the port.

```

interface fa0/1
switchport mode access
switchport port-security
switchport port-security violation protect
switchport port-security mac-address 0006.0006.0006
switchport port-security maximum 5
switchport port-security aging time 30

```

The above configuration also includes a static entry for the MAC address 0006.0006.0006. This means that this address is always in the list, and so in effect, this configuration leaves only four other dynamic MAC addresses that can connect at a time.

There is no option to generate a log message but not block any packets.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Catalyst 6500 Release 15.0SY Software Configuration Guide > Security > Port Security > How to Configure Port Security

### QUESTION 313

What Cisco Catalyst switch feature can be used to define ports as trusted for DHCP server connections?

- A. DHCP snooping
- B. port security
- C. 802.1x
- D. private VLANs

**Correct Answer: A**

**Section: Infrastructure Services**

**Explanation**

**Explanation/Reference:**

Explanation:

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP spoofing is an attack that can be used to force user traffic through an attacking device. This is accomplished by an attacker responding to DHCP queries from users. Eliminating the response from the correct DHCP server would make this more effective, but if the attacker's response gets to the client first, the client will accept it.

The DHCP response from the attacker will include a different gateway or DNS server address. If they define a different gateway, the user traffic will be forced to travel through a device controlled by the attacker. This will allow the attacker to capture traffic and gain company information. If the attacker changes the DNS server in the response, they can use their own DNS server to force traffic to selected hosts to go to a device they control. Again, this would allow the attacker to capture traffic and gain information.

DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCP OFFER, DHCP ACK, and DHCP NAK, from the company DHCP server. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

The three required steps to implement DHCP snooping are:

1. Enable DHCP snooping globally with the ip dhcp snooping command.  
switch(config)# ip dhcp snooping
2. Enable DHCP snooping for a VLAN with the vlan parameter:  
switch(config)# ip dhcp snooping vlan vlan #  
(for example, ip dhcp snooping 10 12 specifies snooping on VLANs 10 and 12)
3. Define an interface as a trusted DHCP port with the trust parameter:  
switch(config-if)# ip dhcp snooping trust

When specifying trusted ports, access ports on edge switches should be configured as untrusted, with the exception of any ports that may have company DHCP servers connected. Only ports where DHCP traffic is expected should be trusted. Most certainly, ports in any area of the network where attacks have been detected should be configured as untrusted.

Some additional parameters that can be used with the ip dhcp snooping command are:

switch(config)# ip dhcp snooping verify mac-address - this command enables DHCP MAC address verification.

switch(config)# ip dhcp snooping information option allow-untrusted - this command enables untrusted ports to accept incoming DHCP packets with option 82 information. DHCP option 82 is used to identify the location of a DHCP relay agent operating on a subnet remote to the DHCP server.

When DHCP snooping is enabled, no other relay agent-related commands are available. The disabled commands include:

```

ip dhcp relay information check global configuration command
ip dhcp relay information policy global configuration command
ip dhcp relay information trust-all global configuration command
ip dhcp relay information option global configuration command
ip dhcp relay information trusted interface configuration command

```

DHCP Authorized ARP can also be used to mitigate DHCP spoofing. When implemented, the server assigns an IP address to a client and then creates a static mapping. The DHCP server then sends periodic ARPs to clients to make sure that the clients are still active. Clients respond with an ARP reply. Unauthorized clients cannot respond to these periodic ARPs. The unauthorized ARP responses are blocked at the DHCP server.

Private VLANs are a method of protecting or isolating different devices on the same port and VLAN. A VLAN can be divided into private VLANs, where some devices are able to access other devices and some are completely isolated from others. This was designed so service providers could keep customers on the same port isolated from each other, even if the customers had the same Layer 3 networks.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not to limit which ports can have DHCP servers connected to them.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch, but it cannot control which ports are permitted to have a DHCP server attached to it.



Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Cisco IOS IP Addressing Services Command Reference > ip dhcp snooping  
Cisco > Cisco IOS IP Addressing Services Command Reference > ip dhcp relay information option

**QUESTION 314**  
Which PVLAN port types can send frames through a switch to community and promiscuous ports? (Choose two.)

- A. public
- B. private
- C. isolated
- D. community
- E. promiscuous

**Correct Answer:** DE  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

Community ports and promiscuous ports can send frames to other community ports and promiscuous ports in the same private VLAN.

There are three types of ports in a private VLAN (PVLAN): promiscuous, isolated, and community. A PVLAN community port (a port in the same VLAN) and promiscuous ports (a port that can forward to all interfaces, including the isolated and community ports within a PVLAN) can send traffic to other community or promiscuous ports.

Isolated ports are able to send frames to promiscuous ports, but not to other isolated ports.

A community port can communicate with other community ports in the same privateVLAN or with promiscuous ports.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists

**QUESTION 315**  
What command produced the output in the exhibit?

| Secure Port<br>Action | MaxSecureAddr<br>(Count) | CurrentAddr<br>(Count) | Securityviolation<br>(Count) | Security |
|-----------------------|--------------------------|------------------------|------------------------------|----------|
| Fa5/1                 | 10                       | 10                     | 0                            | Shutdown |
| Fa5/5                 | 5                        | 2                      | 0                            | Restrict |
| Fa5/11                | 5                        | 4                      | 0                            | Protect  |

Total Addresses in System: 16  
Max Addresses limit in System: 128

- A. show port-security interface
- B. show vlan private-vlan type
- C. show port-security
- D. show ip dhcp snooping

**Correct Answer:** C  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

The exhibit displays the output of the show port-security command. This command is useful in verifying the reaction set for packets in violation. In the exhibit, Fa5/1 is configured to shut down if a violating packet is received. Port Fa5/5 is configured to drop violating packets, and port Fa5/11 is configured to drop packets and generate a log message.

The output also indicates the number of secure MAC addresses permitted on each interface, the number of secure MAC addresses currently in use on the port, and how many security violations have already occurred.

The show port-security interface command shows the port security configuration on the specified interface. Below is an example of that command output:

```

Router# show port-security interface fastethernet 0/2
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 7
Total MAC Addresses: 7
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0

```

In the above example, seven MAC addresses are allowed on this interface. It can be seen that seven are now connected. Therefore, if one more user connects to the hub or switch that is connected to this port, the port will be placed into the err-disabled state and an SMTP trap message will be sent.

The show vlan private-vlan type command displays the private VLANs on the switch and whether they are primary, isolated, or community VLANs. An example of the command output is below:

```

Router# show vlan private-vlan type
Vlan Type
----
202 primary
303 isolated
304 community

```

In the output, VLAN 202 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 303 carries traffic from isolated ports to a promiscuous port.

The show ip dhcp snooping command displays whether DHCP snooping is enabled, what VLANs it is configured for, and what ports are trusted DHCP ports. An example output is below.

```

Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
10 30-40
Insertion of option 82 information is enabled.
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled

Interface Trusted Rate limit (pps)
-----
FastEthernet2/1 yes 10
FastEthernet3/1 yes none
GigabitEthernet1/1 no 20
Switch#

```

The show ip dhcp snooping command output indicates that:  
The switch is defending against a DHCP spoofing attack (indicated by lines 2 and 3)  
Two ports are trusted and one is not (shown in bottom table)  
Option 82 (relay agent information) is only allowed on trusted ports (indicated by lines 4 and 5)  
ARP spoofing is being monitored (indicated by line 6)

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Support > show multicast protocols status through show rif > show port-security

### QUESTION 316

What attack technique uses double VLAN tagging to access network devices that might not otherwise be accessible?

- A. VLAN hopping
- B. DHCP spoofing
- C. Rogue devices
- D. MAC flooding

**Correct Answer: A**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

Double VLAN tagging is used by a VLAN hopping attack. An attacker can create a packet with two VLAN headers on it and send it to a switch. The switch port will strip off the first header and leave the second. The second header will be seen as the originating VLAN, allowing the attacker access to a VLAN they are not connected to. This becomes a security concern because this hopping can be accomplished without passing through a router and its security access lists. For this reason, private VLANs and VACLs should be used to secure access between VLANs.

DHCP spoofing is an attack that can be used to force user traffic through an attacking device. This is accomplished by an attacker responding to DHCP queries from users. Eliminating the response from the correct DHCP server would make this more effective, but if the attacker's response gets to the client first, the client will accept it. The DHCP response from the attacker will include a different gateway or DNS server address. If they define a different gateway, the user traffic will be forced to travel through a device controlled by the attacker. This will allow the attacker to capture traffic and gain company information. If the attacker changes the DNS server in the response, they can use their own DNS server to force traffic to selected hosts to go to a device they control. Again, this would allow the attacker to capture traffic and gain information.

MAC flooding is an attack technique that attempts to fill a switch's MAC address table so the attacker can capture flooded traffic sent from the switch. The concept of this attack is to use the CAM table limit to the attacker's advantage. The attacker would send packets addressed from a large number of MAC addresses to the switch. The switch adds the source MAC address to the MAC address table. Eventually no more MAC addresses can be added because the table is full. When this occurs, any packets destined for a MAC address not in the table will be flooded to all other ports. This would allow the attacker to see the flooded traffic and capture information. The switch would be essentially functioning as a hub in this case.

A rogue device is a device attached to the network that is not under the control of the organization. This term is normally used to mean a wireless device, perhaps an access point that is not operating as a part of the company's infrastructure. Employees may bring their own access points and connect them to the network so they can use their computer wirelessly. This creates a security gap since the device is probably not secured to protect the traffic. An attacker could connect a rogue access point to a company's network and capture traffic from outside the company's premises.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Products and Services > Switches > Cisco Catalyst 6500 Series Switches > Product Literature > White Papers > Cisco Catalyst 6500 Series Switches > VLAN Security White Paper > Double-Encapsulated 802.1Q/Nested VLAN Attack

#### QUESTION 317

What Cisco switch features are designed to work together to mitigate ARP spoofing attacks? (Choose two.)

- A. DHCP snooping
- B. port security
- C. 802.1x
- D. DAI

**Correct Answer:** AD  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

Dynamic ARP inspection (DAI) and DHCP snooping are Cisco features designed to work together to mitigate ARP spoofing attacks. DAI validates ARP packets in a network. DAI determines the validity of an ARP packet based on the valid MAC address-to-IP-address bindings stored in the DHCP snooping database. This capability protects the network from some man-in-the-middle attacks. The following global configuration command instructs the switch to intercept, log, and discard packets with invalid IP-to-MAC address bindings for the specified VLANs.

```
switch(config)# ip arp inspection vlan 10-12,15
```

When configuring DAI, ports are configured as either trusted or untrusted. DAI forwards all packets received on a trusted interface without checks but intercepts all packets on an untrusted port.

DHCP snooping creates an IP address to MAC address database that DAI uses to validate ARP packets. It compares the MAC address and IP address in ARP packets and only permits the traffic if the addresses match. This eliminates attackers spoofing MAC addresses. The following command enables DHCP MAC address verification:

```
router(config)# ip dhcp snooping verify mac-address
```

DHCP Authorized ARP can also be used to mitigate ARP spoofing. When implemented, the server assigns an IP address to a client and then creates a static mapping. The DHCP server then sends periodic ARPs to clients to make sure that the clients are still active. Clients respond with an ARP reply. Unauthorized clients cannot respond to these periodic ARPs. The unauthorized ARP responses are blocked at the DHCP server.

DHCP snooping also is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets such as DHCP OFFER, DHCPACK, and DHCPNAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not eliminate ARP spoofing.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch; it does not inspect ARP packets.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Catalyst 6500 Release 12.2SXF and Rebuilds Software Configuration Guide > Configuring Dynamic ARP Inspection (DAI)  
Cisco > Cisco IOS IP Addressing Services Command Reference > ARP Commands > ip arp inspection vlan

#### QUESTION 318

What command would be used to verify trusted DHCP ports?

- A. show mls qos
- B. show ip dhcp snooping
- C. show ip trust
- D. show ip arp trust

**Correct Answer:** B

**Section: Infrastructure Services****Explanation****Explanation/Reference:**

Explanation:

The command show ip dhcp snooping is used to verify trusted DHCP ports. This command is used to verify which ports are intended to have DHCP servers connected to them. DHCP snooping creates an IP address to MAC address database that Dynamic ARP Inspection (DAI) uses to validate ARP packets. It compares the MAC address and IP address in ARP packets and only permits the traffic if the addresses match. This eliminates attackers that are spoofing MAC addresses.

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCPOFFER, DHCPACK, and DHCPNAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

MLS QOS has no bearing on DHCP services, so show mls qos is not correct.

The other commands are incorrect because of invalid syntax.

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Cisco IOS IP Addressing Services Command Reference > DHCP Commands > show ip dhcp snooping

**QUESTION 319**

What switch security configuration requires AAA to be configured on the switch?

- A. VACL
- B. 802.1x
- C. Private VLAN
- D. port security

**Correct Answer: B**

**Section: Infrastructure Services****Explanation****Explanation/Reference:**

Explanation:

802.1x requires AAA to be configured on the switch. 802.1x uses AAA authentication to control access to the port.

The overall steps required to configure a switch for 802.1x are:

Enable AAA on the switch.

Define the external RADIUS server(s) and the key to be used for encryption.

Define the authentication method.

Enable 802.1x on the switch.

Configure each switch port that will use 802.1x.

Optionally allow multiple hosts on the switch port.

<font size="2" face=

Objective:

Infrastructure Security

Sub-Objective:

Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

References:

Cisco > Catalyst 6500 Series Cisco IOS Software Configuration Guide, 12.1E > Configuring 802.1X Port-Based Authentication

**QUESTION 320**

Which protocol provides port-based access control and authentication?

- A. 802.1X
- B. 802.1W
- C. 802.1P
- D. 802.1Q

**Correct Answer: A**

**Section: Infrastructure Services****Explanation****Explanation/Reference:**

Explanation:

IEEE 802.1X provides port-based access control and authentication.

IEEE 802.1X is a client-server based access control model. If IEEE 802.1X is enabled on a switch interface, the interface is in an unauthorized state until it is authenticated. Until the station is authenticated, the only protocols allowed through switch ports are:

CDP

STP

EAP-over-LAN (EAPOL is the only type of traffic accepted from a station)

The supplicant PAE sends EAPOL packets that indicate its request for access through the switch to the LAN. The switch performs the authenticator role by processing the EAPOL packets from the port-attached supplicant PAE and forwarding an authentication request to the authentication server. The only supported authentication server is a Remote Access Dial-In User Server (RADIUS) server with EAP extensions. The authentication server checks the identity of the client (the supplicant PAE) and will either accept or reject the request. If the server accepts the request, the port is authorized and the switch will send and receive all frames. If it fails, only EAPOL packets will continue to be processed. Once the client is finished with the connection, an EAPOL logoff is issued, and the switch port once again becomes unauthorized.



Below is a sample configuration to enable 802.1X authentication and enable it on an interface:

```
switch(config)# aaa new-model
switch(config)# aaa authentication dot1x default group radius
switch(config)# dot1x system-auth-control
switch(config-if)# dot1x port-control auto
```

802.1w is the standard for Rapid Spanning Tree Protocol (RSTP). It is not related to port-based access control and authentication.

802.1P is a method for assigning priority to packets traversing a network. It is not related to port-based access control and authentication.

802.1Q describes VLAN tagging. It is not related to port-based access control and authentication.

Objective:  
Infrastructure Security  
Sub-Objective:  
Describe device security using Cisco IOS AAA with TACACS+ and RADIUS

References:  
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > aaa accounting dot1x default start-stop group radius  
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > dot1x port-control  
Cisco > Catalyst 4500 Series Switch Cisco IOS Command Reference, 12.2(52)SG > aaa accounting dot1x default start-stop group radius through instance > dot1x system-auth-control  
Cisco > Cisco IOS Security Command Reference > aaa new-model

**QUESTION 321**  
What command produces the output in the exhibit?

| Secure Port<br>Action | MaxSecureAddr<br>(Count) | CurrentAddr<br>(Count) | Securityviolation<br>(Count) | Security |
|-----------------------|--------------------------|------------------------|------------------------------|----------|
| Fa5/1                 | 10                       | 10                     | 0                            | Shutdown |
| Fa5/5                 | 5                        | 2                      | 0                            | Restrict |
| Fa5/11                | 5                        | 4                      | 0                            | Protect  |

Total Addresses in System: 16  
Max Addresses limit in System: 128

- A. show port-security interface
- B. show vlan private-vlan type
- C. show port-security
- D. show ip dhcp snooping

**Correct Answer: C**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

The exhibit displays the output of the show port-security command. This command is useful in verifying the reaction set for packets in violation. In the exhibit, Fa5/1 is configured to shut down if a violating packet is received. Port Fa5/5 is configured to drop violating packets and port Fa5/11 is configured to drop packets and generate a log message.

The output also indicates the number of secure MAC addresses permitted on each interface, the number of secure MAC addresses currently in use on the port, and how many security violations there have been.

The show port-security interface command shows the port security configuration on the specified interface. Below is an example of the command and its output:

```
Router# show port-security interface fastethernet 0/2
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 7
Total MAC Addresses: 7
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
```

In the example, seven MAC addresses are allowed on this interface. It can be seen that seven are now connected. Therefore, if one more user connects to the hub or switch connected to this port, the port will be placed into the err-disabled state and an SMTP trap message will be sent.

The show vlan private-vlan type command displays the private VLANs on the switch and indicates whether they are primary, isolated, or community VLANs. An example of the output is below:

```
Router# show vlan private-vlan type
Vlan Type
-----
202 primary
303 isolated
304 community
```

In the output, VLAN 202 carries traffic from promiscuous ports to isolated, community, and other promiscuous ports in the same VLAN. VLAN 303 carries traffic from isolated ports to a promiscuous port.

The show ip dhcp snooping command displays whether DHCP snooping is enabled, what VLANs it is configured for, and what ports are trusted DHCP ports. An example of the output is below:

```
Switch# show ip dhcp snooping
Switch DHCP snooping is enabled.
DHCP Snooping is configured on the following VLANs:
10 30-40
Insertion of option 82 information is enabled.
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled

Interface Trusted Rate limit (pps)
-----
FastEthernet2/1 yes 10
FastEthernet3/1 yes none
GigabitEthernet1/1 no 20
```

The output indicates that:  
The switch is defending against a DHCP spoofing attack (indicated by lines 2 and 3)  
Two ports are trusted and one is not (shown in bottom table)  
Option 82 (relay agent information) is only allowed on trusted ports (indicated by lines 4 and 5)  
ARP spoofing is being monitored (indicated by line 6)

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Support > show multicast protocols status through show rif > show port-security

#### QUESTION 322

What Cisco Catalyst switch feature is designed to inspect ARP packets and mitigate ARP spoofing attacks?

- A. DHCP snooping
- B. port security
- C. 802.1x
- D. DAI

**Correct Answer: D**  
**Section: Infrastructure Services**  
**Explanation**

**Explanation/Reference:**  
Explanation:

ARP spoofing attacks are attempts to redirect traffic to an attacking host by sending an ARP message with a forged identity to a transmitting host. Dynamic ARP inspection (DAI) is a Cisco feature designed to inspect ARP packets and mitigate spoofing attacks. It works in combination with DHCP snooping. DHCP snooping creates an IP address to MAC address database that DAI uses to validate ARP packets. It compares the MAC address and IP address in ARP packets and only permits the traffic if the addresses match. This eliminates attackers from spoofing MAC addresses. Characteristics of DAI include:  
DAI can only be performed on ingress ports  
DAI is supported on access ports, trunk ports, Etherchannel ports, and private VLAN ports  
DAI should be configured on all access switch ports as untrusted, and on all switch ports connected to other switches as trusted

An interface can be configured as trusted by using the ip arp inspection trust command. Consider the configuration shown below. If an ARP spoof attack arrives on interface Fa0/2, it will not be inspected because the port is set as trusted, and the spoof packets will be allowed.

```
<output omitted>
ip arp inspection vlan 5
interface fastethernet 0/2
switchport mode trunk
switchport trunk encapsulation dot1q
ip arp inspection trust
```

DHCP snooping is used to define ports as trusted for DHCP server connections. The purpose of DHCP snooping is to mitigate DHCP spoofing attacks. DHCP snooping can be used to determine what ports are able to send DHCP server packets, such as DHCP OFFER, DHCP ACK, and DHCP NAK. DHCP snooping can also cache the MAC address to IP address mapping for clients receiving DHCP addresses from a valid DHCP server.

Port security is a method of only permitting specified MAC addresses access to a switch port. This can be used to define what computer or device can be connected to a port, but not eliminate ARP spoofing.

802.1x is a method of determining authentication before permitting access to a switch port. This is useful in restricting who can connect to the switch; it does not inspect ARP packets.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Catalyst 6500 Release 12.2SX and Rebuilds Software Configuration Guide > Configuring Dynamic ARP Inspection (DAI)

#### QUESTION 323

What is accomplished by the command switchport port-security violation restrict?

- A. The switch will generate a log message but will not block any packets.
- B. The switch will drop packets that are in violation and generate a log message.
- C. The switch will drop packets that are in violation, but not generate a log message.
- D. The switch will shut down the interface when packets in violation are detected.

**Correct Answer:** B  
**Section:** Infrastructure Services  
**Explanation**

**Explanation/Reference:**  
Explanation:

The command switchport port-security violation restrict drops packets that are in violation and generates a log message. The complete syntax of the command is:

```
switch(config-if)# switchport port-security violation restrict
```

The port security command is used to lock a port down to specific MAC addresses. The three keywords that can be used with this command are protect, restrict, and shutdown. The protect keyword tells the port to drop packets without generating a log message for packets that are in violation. The restrict keyword tells the port to drop packets and generates a log message for packets that are in violation. The shutdown keyword causes the port to be disabled if a violation is detected.

There is no option to generate a log message but not block any packets.

Objective:  
Infrastructure Security  
Sub-Objective:  
Configure and verify switch security features

References:  
Cisco > Catalyst 6500 Release 15.0SY Software Configuration Guide > Security > Port Security > How to Configure Port Security

**QUESTION 324**  
Refer to the exhibit.

```
Switch(config)#spanning-tree portfast default
%Warning: this command enables portfast by default on all interfaces. You
should now disable portfast explicitly on switched ports leading to hubs,
switches and bridges as they may create temporary bridging loops.
Switch(config)#
```

When troubleshooting a network problem, a network analyzer is connected to Port f0/1 of a LAN switch. Which command can prevent BPDU transmission on this port?

- A. spanning-tree portfast bpduguard enable
- B. spanning-tree bpduguard default
- C. spanning-tree portfast bpdufilter default
- D. no spanning-tree link-type shared

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 325**  
Which four LACP components are used to determine which hot-standby links become active after an interface failure within an EtherChannel bundle? (Choose four.)

- A. LACP system priority
- B. LACP port priority
- C. interface MAC address
- D. system ID
- E. port number
- F. hot-standby link identification number
- G. interface bandwidth

**Correct Answer:** ABDE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 326**  
RSPAN has been configured on a Cisco Catalyst switch; however, traffic is not being replicated to the remote switch. Which type of misconfiguration is a cause?

- A. The RSPAN designated VLAN is missing the remote span command.
- B. The local and remote RSPAN switches are configured using different session IDs.
- C. The local RSPAN switch is replicating only Rx traffic to the remote switch.
- D. The local switch is overloaded with the amount of sourced traffic that must be replicated to the remote switch.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 327**

How can you set VLAN 99 on a trunk to become a native VLAN?

- A. switchport trunk native vlan 99
- B. switchport trunk vlan 99 native
- C. switchport native vlan 99 trunk
- D. switchport native trunk vlan 99
- E. switchport vlan 99 native
- F. switchport vlan native trunk 99

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 328**

To follow the Layer 2 switching guidelines, a network engineer decides to create a separate spanning tree for every group of 10 VLANs.

Which version of spanning tree is appropriate to meet the company policy?

- A. MST
- B. PVST+
- C. RSTP
- D. RPVST+
- E. STP

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 329**

A network engineer is installing a switch for temporary workers to connect to. The engineer does not want this switch participating in Spanning Tree with the rest of the network; however, end user connectivity is still required.

Which spanning-tree feature accomplishes this?

- A. BPDUblock
- B. BPDUfilter
- C. BPDUignore
- D. BPDUguard
- E. BPDUDisable

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 330**

Refer to the exhibit.

```
monitor session 1 source interface g0/4 rx
monitor session 1 filter vlan 3
monitor session 1 destination interface g0/5
```

What is the result of the SPAN configuration on a Cisco switch?

- A. Configure a SPAN session to monitor the received traffic on interface g0/4 only for VLAN 3.
- B. Configure a SPAN session to monitor the received traffic on interface g0/4 for all VLANs except VLAN 3.
- C. Configure a SPAN session to monitor the received traffic on interface g0/5 only for VLAN 3.
- D. Configure a SPAN session to monitor the received traffic on interface g0/5 for all VLANs except VLAN 3.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 331**

When SDM templates are configured, which action must be performed for the configuration to take effect?

- A. reload
- B. shutdown
- C. write memory
- D. backup config

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 332**

Which statement about the MAC address sticky entries in the switch when the copy run start command is entered is true?

- A. A sticky MAC address is retained when the switch reboots.
- B. A sticky MAC address can be a unicast or multicast address.
- C. A sticky MAC address is lost when the switch reboots.
- D. A sticky MAC address ages out of the MAC address table after 600 seconds.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 333**

Enablement of which feature puts the port into err-disabled state when the port has PortFast enabled and it receives BPDUs?

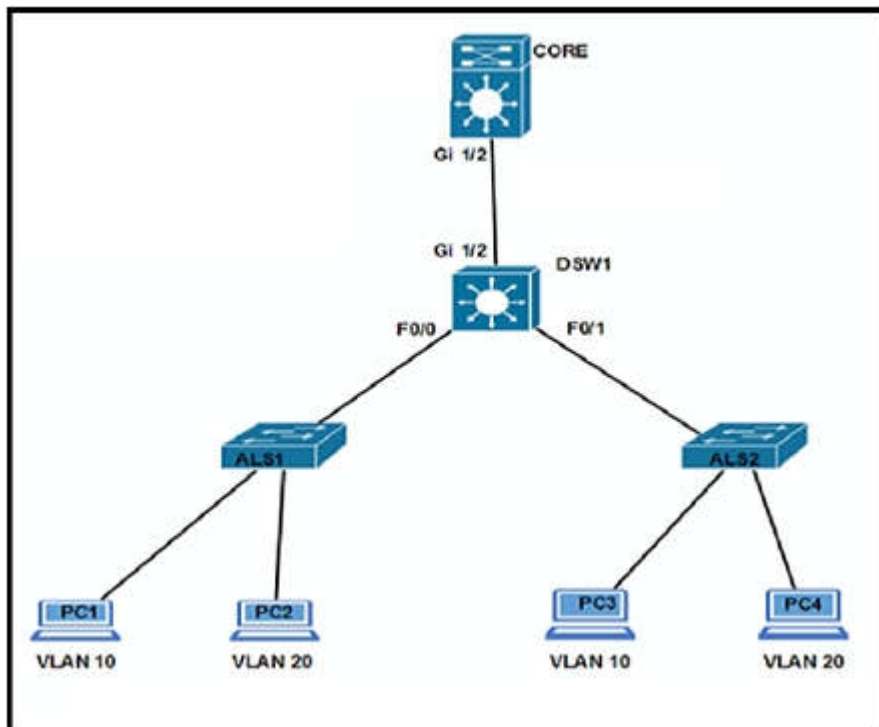
- A. BPDU filtering
- B. BackboneFast
- C. EtherChannel
- D. BPDU guard

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 334**

Refer to the exhibit.



Which configuration ensures that the Cisco Discovery Protocol packet update frequency sent from DSW1 to ALS1 is half of the default value?

- A. DSW1(config)#cdp timer 90
- B. DSW1(config-if)#cdp holdtime 60
- C. DSW1(config)#cdp timer 30
- D. DSW1(config)#cdp holdtime 90
- E. DSW1(config-if)#cdp holdtime 30
- F. DSW1(config-if)#cdp timer 60

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 335**

Interfaces are assigned to a VLAN, and then the VLAN is deleted. Which state are these interfaces in after the VLAN is deleted?

- A. They remain up, but they are reassigned to the default VLAN.
- B. They go down until they are reassigned to a VLAN.
- C. They go down, but they are reassigned to the default VLAN.



D. They remain up, but they are reassigned to the native VLAN.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 336**

Which feature is automatically configured when an administrator enables a voice VLAN?

- A. 802.1Q trunking
- B. PortFast
- C. QoS
- D. private VLANs

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 337**

Which statement describes one major issue that VTP can cause in an enterprise network when a new switch is introduced in the network in VTP mode server?

- A. It can cause network access ports to go into err-disabled state.
- B. It can cause a network-wide VLAN configuration change if the revision number on the new switch is higher.
- C. It can cause a network-wide VLAN configuration change if the revision number on the new switch is lower.
- D. It can cause routing loops.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 338**

A network administrator configures 10 extended VLANs ranging from VLANs 3051 to 3060 in an enterprise network. Which version of VTP supports these extended VLANs?

- A. version 1
- B. version 2
- C. version 3
- D. VTP does not recognize extended VLANs.

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 339**

An engineer is configuring an EtherChannel between two switches using LACP. If the EtherChannel mode on switch 1 is configured to active, which two modes on switch 2 establish an operational EtherChannel? (Choose two.)

- A. active
- B. auto
- C. desirable
- D. on
- E. passive

**Correct Answer:** AE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 340**

When a Layer 2 EtherChannel is configured, which statement about placement of the IP address is true?

- A. The IP address is placed on the highest numbered member port.
- B. The IP address is placed on the port-channel logical interface.
- C. The IP address is placed on the lowest numbered member port.
- D. The IP address is assigned via DHCP only.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 341**

Which option is valid for EtherChannel load balancing?

- A. source MAC address and source IP address
- B. destination MAC address and destination IP address
- C. source MAC address and destination IP address
- D. source MAC address and destination MAC address

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 342**

Refer to the exhibit.

```
Switch2#
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/23, putting Fa0/23 in err-disable
state
01:25:08: %PM-4-ERR_DISABLE: channel-misconfig error detected on
Fa0/24, putting Fa0/24 in err-disable
state
Switch2#

Switch1#show etherchannel summary

!output omitted

Group Port-channel Protocol Ports
-----+-----+-----+-----
1      Po2(SD)          LACP  Fa1/0/23(D)

Switch2#show etherchannel summary

!output omitted

Group Port-channel Protocol Ports
-----+-----+-----+-----
1      Po1(SD)          -     Fa0/23(D) Fa0/24(D)
```

An engineer is configuring EtherChannel between two switches and notices the console message on switch 2. Based on the output, which option describes the reason for this error?

- A. Switch 1 does not have enough member ports configured.
- B. Switch 2 has too many member ports configured.
- C. The port channel interface numbers do not match.
- D. The EtherChannel protocols do not match.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 343**

Refer to the exhibit.

```
DSW1#sh vtp status
VTP Version                : running VTP1 (VTP2 capable)
Configuration Revision      : 2
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 7
VTP Operating Mode          : Client
VTP Domain Name             : DALLAS
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xF1 0xAC 0x5E 0xCF 0xF7 0xEE 0x9E 0xD6
Configuration last modified by 10.101.101.11 at 3-1-93 23:57:30

DSW2#sh vtp status
VTP Version                : running VTP1 (VTP2 capable)
Configuration Revision      : 3
Maximum VLANs supported locally : 1005
Number of existing VLANs    : 7
VTP Operating Mode          : Server
VTP Domain Name             : DALLAS
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xES 0x4D 0xC1 0xF0 0x0F 0xF1 0x4B 0x0C
Configuration last modified by 10.101.101.11 at 3-1-93 23:50:31

DSW2#sh spanning-tree mst configuration
Name [DALLAS]
Revision 3      Instances configured 3

Instance  Vlan mapped
-----
0         1-9,11-19,21-29,41-4094
1         10,20
2         30-40
```

- DSW1 should share the same MST region with switch DSW2. Which statement is true?
- A. Configure DSW1 with the same version number, and VLAN-to-instance mapping as shown on DSW2.
  - B. DSW2 uses the VTP server mode to automatically propagate the MST configuration to DSW1.
  - C. DSW1 automatically inherits MST configuration from DSW2 because they have the same domain name.
  - D. Configure DSW1 with the same region name, revision number, and VLAN-to-instance mapping as shown on DSW2.
  - E. DSW1 is in VTP client mode with a lower configuration revision number, therefore, it automatically inherits MST configuration from DW2.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 344**  
Which two statements about SPAN source and destination ports during an active session are true? (Choose two.)

- A. The source port can be only an Ethernet physical port.
- B. The source port can be monitored in multiple SPAN sessions.
- C. The destination port can be destination in multiple SPAN sessions.
- D. The destination port does not participate in STP.
- E. You can mix individual source ports and source VLANs within a single session.

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 345**  
In a switch stack environment, what is the total bidirectional traffic flow between two logical counter-rotating paths?

- A. 16 Gbps
- B. 32 Gbps
- C. 64 Gbps
- D. 128 Gbps

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 346**  
Refer to the exhibit.

```

SW1#sh monitor session all
Session 1
-----
Type                : Remote Destination Session
Source RSPAN VLAN   : 50

Session 2
-----
Type                : Local Session
Source Ports        :
  Both              : Fa0/14
Destination Ports    : Fa0/15
Encapsulation        : Native
Ingress              : Disables

```

Which statement about the SPAN and RSPAN configuration on SW1 is true?

- A. SPAN session 2 only monitors egress traffic exiting port FastEthernet 0/14.
- B. RSPAN session 1 monitors activity on VLAN 50 of a remote switch.
- C. RSPAN session 1 is incompletely configured for monitoring.
- D. SPAN session 2 monitors all traffic entering and exiting port FastEthernet 0/15.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 347

Which option is the minimum number of bindings that the DHCP snooping database can store?

- A. 1000 bindings
- B. 2000 bindings
- C. 5000 bindings
- D. 8000 bindings

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 348

On which layer does IP source guard provide filtering to prevent a malicious host from impersonating the IP address of a legitimate host?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 7

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 349

By default, what is the state of port security on a switch?

- A. disabled
- B. on
- C. off
- D. learning

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 350

Which two statements about HSRP, GLBP, and VRRP are true? (Choose two.)

- A. HSRP is the preferred protocol to be used on multivendor environments.
- B. VRRP has one master router, one standby router, and many listening routers.
- C. GLBP allows for a maximum of four MAC addresses per group.
- D. HSRP supports up to 255 groups on the same switch or router.
- E. VRRP is a Cisco proprietary protocol.

Correct Answer: CD  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 351

Refer to the exhibit.

```
R2#show standby
FastEthernet1/0 - Group 50
  State is Active
    2 state changes, last state change 00:04:02
  Virtual IP address is 10.10.1.1
  Active virtual MAC address is 0000.0c07.ac32 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac32 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.504 secs
  Preemption enabled, delay reload 90 secs
  Active router is local
  Standby router is unknown
  Priority 200 (configured 200)
    Track interface FastEthernet0/0 state Up decrement 20
  Group name is "hsrp-Fa1/0-50" (default)
R2#
%IP-4-DUPADDR: Duplicate address 10.10.1.1 on FastEthernet1/0, sourced by 0000.0c07.ac28
R2#
```

Which option is the most likely explanation of the duplicate address message logged?

- A. spanning-tree loop
- B. HSRP misconfiguration
- C. a PC with IP of 10.10.1.1
- D. a hardware problem

Correct Answer: B  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 352

DRAG DROP

Drag and drop the characteristic from the left to the matching Layer 2 protocol on the right.

Select and Place:

sends topology change notification

Default time between protocol frames is 60 seconds.

uses multicast address 01-80-C2-00-00-0E

Default time between protocol frames is 30 seconds.

uses multicast address 0100.0ccc.cccc

supports IEEE 802.2 and 802.3 encapsulation

CDP

LLDP

Correct Answer:



|                                                     |
|-----------------------------------------------------|
| CDP                                                 |
| uses multicast address 0100.0ccc.cccc               |
| supports IEEE 802.2 and 802.3 encapsulation         |
| Default time between protocol frames is 60 seconds. |
| LLDP                                                |
| sends topology change notification                  |
| uses multicast address 01-80-C2-00-00-0E            |
| Default time between protocol frames is 30 seconds. |

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 353

Refer to the exhibit.

```
switch#sh run
Building configuration...

Interface FastEthernet0/1
description Uplink to Core
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1-90,100-199,200-900,1000-4000
switchport mode trunk
```

A network engineer changes the default native VLAN to VLAN 999. After applying the settings on the uplinks to the core switches, the switch control traffic, such as CDP and VTP, is no longer working. The standard configuration is used for each uplink. What is wrong with the configuration?

- A. The interface is administratively down.
- B. The encapsulation type is incorrect.
- C. The switchport mode trunk command should be first in the output.
- D. The native VLAN is not present on the trunk.
- E. The control traffic must be manually enabled on the new native VLAN.

**Correct Answer: D**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 354

Which two options are two results of using the command **spanning-tree vlan 50 root primary** within a spanning-tree network under global configuration? (Choose two.)

- A. Spanning tree determines the priority of the current root for VLAN 50 and reduces the priority of the local switch to a lower value.
- B. The priority value for VLAN 50 is set to 4094 on the root while the local switch priority is set to 32768.
- C. The spanning-tree timers are reduced to improve the convergence time for VLAN 50.
- D. All ports that are configured on the current switch with VLAN 50 transition to designated ports.
- E. The switchport that is configured for VLAN 50 is the primary connection to the spanning-tree root switch.

**Correct Answer: AD**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 355

An access switch at a remote location is connected to the spanning-tree root with redundant uplinks. A network engineer notices that there are issues with the physical cabling of the current root port. The engineer decides to force the secondary link to be the desired forwarding root port.

Which action accomplishes this task?

- A. Change the link-type to point-to-point.

- B. Enable Rapid Spanning Tree to converge using the secondary link.
- C. Adjust the secondary link to have a lower priority than the primary link.
- D. Apply a BPDU filter on the primary interface of the remote switches.

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 356

A network engineer wants to make sure that an access switch will never become a Spanning Tree root for VLAN 5. What action will accomplish this task?

- A. adjust STP priority to the maximum value
- B. disable STP globally
- C. apply root guard to all outgoing neighbor interfaces
- D. enable MSTP and use a different revision number than all other switches

**Correct Answer:** A

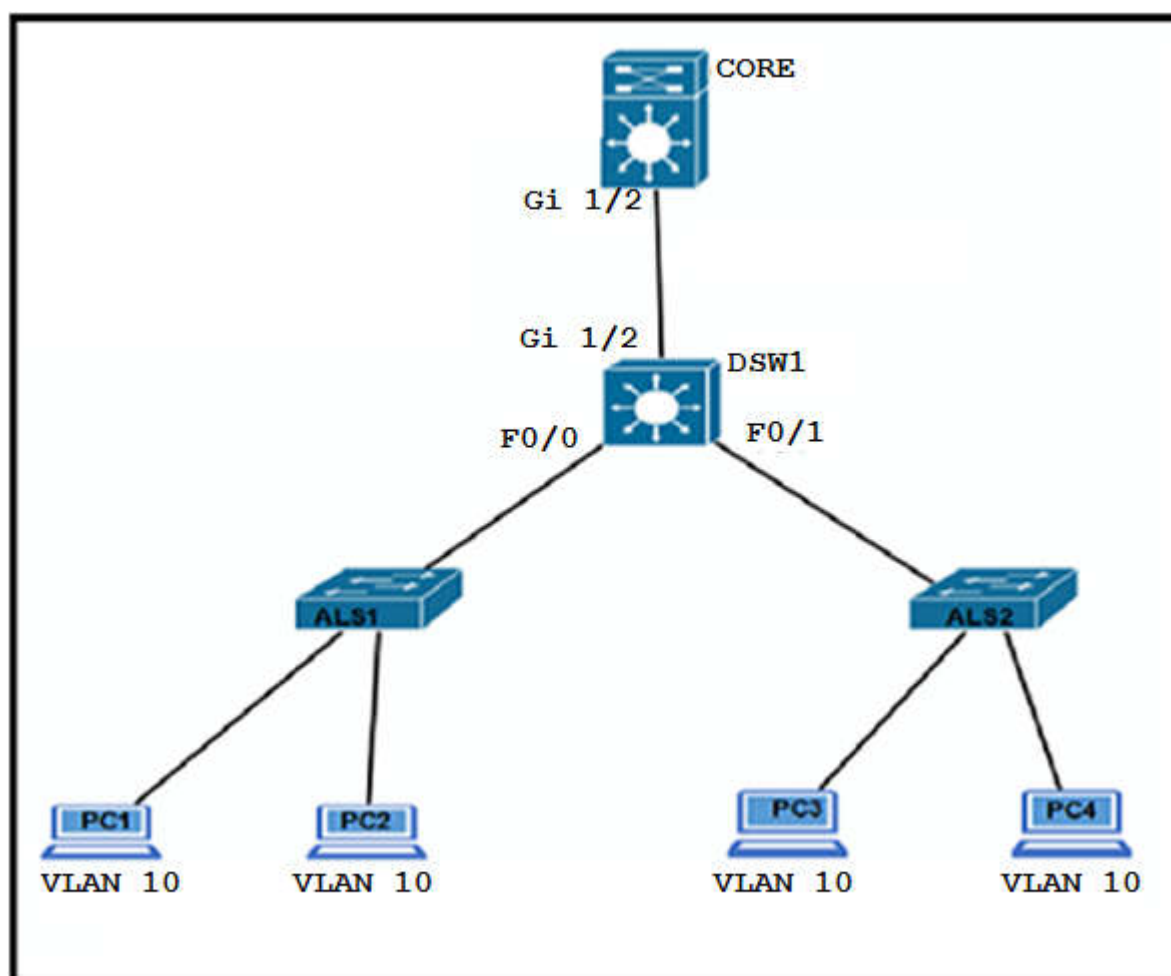
**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 357

Refer to the exhibit.



Which configuration ensures that the Cisco Discovery Protocol packet update frequency sent from DSW1 to ALS1 is half of the default value?

- A. DSW1(config)#cdp timer 90
- B. DSW1(config-if)#cdp holdtime 60
- C. DSW1(config)#cdp timer 30
- D. DSW1(config)#cdp holdtime 90
- E. DSW1(config-if)#cdp holdtime 30
- F. DSW1(config-if)#cdp timer 60

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 358

SIMULATION

##### Instructions

To configure the switch click on the console host icon.

You can click on the buttons below to view the different windows.

Each of the windows can be minimized by clicking on the [-]. You can also reposition a window by dragging it by the title bar.

Most commands that use the "Control" or "Escape" keys are not supported and are not necessary to complete this simulation. The help command does not display all commands of the help system.

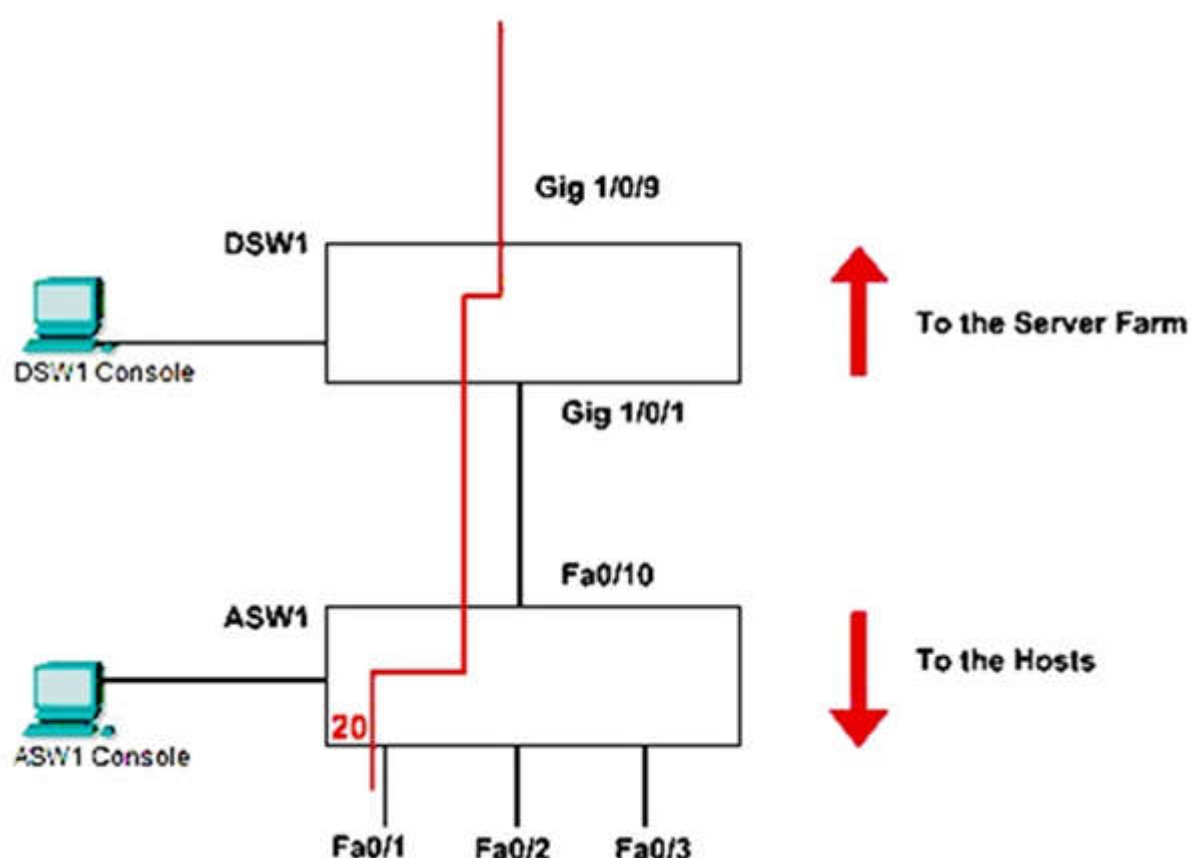
### Scenario

ABC.com is an IT company that has an existing enterprise network comprised of two layer 2 only switches; DSW1 and ASW1. The topology diagram indicates their layer 2 mapping. VLAN 20 is a new VLAN that will be used to provide the shipping personnel access to the server. Corporate policies do not allow layer 3 functionality to be enabled on the switches. For security reasons, it is necessary to restrict access to VLAN 20 in the following manner:

- Users connecting to VLAN 20 via port f0/1 on ASW1 must be authenticated before they are given access to the network. Authentication is to be done via a Radius server:
  - Radius server host 172.120.40.46
  - Radius key: rad123
  - Authentication should be implemented as close to the host as possible.
- Devices on VLAN 20 are restricted to the subnet of 172.120.40.0/24.
  - Packets from devices in the subnet of 172.120.40.0/24 should be allowed on VLAN 20.
  - Packets from devices in any other address range should be dropped on VLAN20.
  - Filtering should be implemented as close to the server farm as possible.

The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers. You must use the available IOS switch features.

**Note:** Named access list is not supported.



**Correct Answer:** See explanation below

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

```
ASW>en
ASW#conf t
ASW (config) #aaa new-model
ASW (config) #radius-s
ASW (config) #radius-server host 172.120.40.46 key rad123
ASW (config) #aaa auth
ASW (config) #aaa authent
ASW (config) #aaa authentication dot
ASW (config) #aaa authentication dot1x def
ASW (config) #aaa authentication dot1x default group rad
ASW (config) #aaa authentication dot1x default group radius
ASW (config) #dot
ASW (config) #dot1x system-a
ASW (config) #dot1x system-auth-control
ASW (config) #int fa0/1
ASW (config-if) #dot1
ASW (config-if) #dot1x port-con
ASW (config-if) #dot1x port-control au
ASW (config-if) #dot1x port-control auto
ASW (config-if) #switch
ASW (config-if) #switchport mode acce
ASW (config-if) #switchport mode access
ASW (config-if) #end
ASW #copy run start
```



```

DSW1 Console
DSW1>en
DSW1#conf t
DSW1(config)#ip acce
DSW1(config)#ip access-list standard 10
DSW1(config-std-nacl)#permit 172.120.40.0 0.0.0.255
DSW1(config-std-nacl)#exit
DSW1(config)#vlan acce
DSW1(config)#vlan access-map MAP 10
DSW1(config-access-map)#match ip addre
DSW1(config-access-map)#match ip address 10
DSW1(config-access-map)#action for
DSW1(config-access-map)#action forward
DSW1(config-access-map)#exit
DSW1(config)#vlan acce
DSW1(config)#vlan access-map MAP 20
DSW1(config-access-map)#action drop
DSW1(config-access-map)#exit
DSW1(config)#vlan fil
DSW1(config)#vlan filter MAP vlan-l
DSW1(config)#vlan filter MAP vlan-list 20
DSW1(config)#end
DSW1#copy run start
Building configuration...
[OK]
DSW1#

```

#### QUESTION 359

Refer to the exhibit. Which two statements about the network environment are true? (Choose two.)

| switch#show mac address-table |                |         |       |
|-------------------------------|----------------|---------|-------|
| Mac Address Table             |                |         |       |
| Vlan                          | Mac Address    | Type    | Ports |
| 10                            | aaaa.aaaa.aaaa | DYNAMIC | Fa0/1 |
| 10                            | cccc.cccc.cccc | DYNAMIC | Fa0/3 |
| 20                            | aaaa.aaaa.aaaa | DYNAMIC | Fa0/2 |

- A. The two aaaa.aaaa.aaaa MAC address entries must be from the same VLAN
- B. Interfaces Fa0/1 and Fa0/3 cannot communicate via Layer 2 switching
- C. Interfaces Fa0/1 and Fa0/2 cannot communicate via Layer 2 switching
- D. The two aaaa.aaaa.aaaa MAC address entries must be from different VLANs
- E. Interfaces Fa0/2 and Fa0/3 can communicate via Layer 2 switching

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 360

When port security is configured on a switch, which violation mode is the default?

- A. no change
- B. error disable
- C. logging
- D. shutdown

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 361

Which command configures VLAN 99 as an untagged VLAN on a trunk?

- A. switchport trunk allowed vlan 99
- B. switchport trunk pruning vlan except 99
- C. switchport trunk native vlan 99
- D. switchport access vlan 99

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 362**  
Which two DTP negotiated interface mode combinations negotiate to form an access port? (Choose two.)

- A. dynamic auto and dynamic auto
- B. nonegotiate and trunk
- C. dynamic auto and trunk
- D. dynamic desirable and access
- E. dynamic desirable and dynamic auto

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 363**  
A network engineer is trying to prevent users from connecting unauthorized equipment to a production network. Which option can be implemented campus-wide to satisfy this requirement?

- A. UplinkFast
- B. BPDU Guard
- C. private VLANs
- D. switchport block
- E. IP Source Guard

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 364**  
Refer to the exhibit. Which statement about the interface is true?

|                                           |          |                                                                                                                             |
|-------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------|
| Interface GigabitEthernet0/10             |          |                                                                                                                             |
| switchport trunk allowed vlan 34, 36, 519 |          |                                                                                                                             |
| switchport mode trunk                     |          |                                                                                                                             |
| end                                       |          |                                                                                                                             |
| Switch-2#show vlan                        |          |                                                                                                                             |
| VLAN                                      | Name     | Status Ports                                                                                                                |
| -----                                     |          |                                                                                                                             |
| --                                        |          |                                                                                                                             |
| 1                                         | default  | active G10/1, G10/2, G10/3, G10/4, G10/5, G10/6, G10/7, G10/8 G10/9, G10/10, G10/11, G10/12, G10/13, G10/14, G10/15, G10/16 |
| 34                                        | VLAN0034 | active                                                                                                                      |
| 36                                        | VLAN0036 | active                                                                                                                      |
| 519                                       | VLAN0519 | active                                                                                                                      |
| Switch-2#show interfaces trunk            |          |                                                                                                                             |
| Switch-2#                                 |          |                                                                                                                             |

- A. The interface needs to shutdown configured
- B. The other side of the interface is set as access
- C. The interface is down
- D. The switchport command is missing from the configuration

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 365**  
Refer to the exhibit. An engineer has run the show EtherChannel summary command and the output is displayed. Which statement about the status of the EtherChannel is true?



Number of channel-groups in use: 1  
Number of aggregators: 1

| Group | Port-channel | Protocol | Ports                   |
|-------|--------------|----------|-------------------------|
| 1     | Po1(SU)      |          | Fa1/0/23(P) Fa1/0/24(P) |

- A. The EtherChannel is down because of a mismatched EtherChannel protocol
- B. The EtherChannel is operational and is using no EtherChannel protocol
- C. The EtherChannel is down and configured for LACP
- D. The EtherChannel is operational and configured for PAgP
- E. IP Source Guard

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 366

Which two statements about HSRP timers are true? (Choose two.)

- A. The default Hold timer is 30 seconds
- B. The default Hold timer is 10 seconds
- C. The default Hello timer is 3 seconds
- D. The default Hold timer is 15 seconds
- E. The default Hello timer is 30 seconds
- F. The default Hello timer is 5 seconds

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 367

After you connected a host to switch port G0/1, the port error disabled. Which command can you enter to determine the reason?

- A. show log
- B. show run interface g0/1
- C. show interfaces g0/1 status
- D. show ip interface brief

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 368

A switch has been configured with the vlan dot1q tag native command. Which statement describes what the switch does with untagged frames that it receives on a trunked interface?

- A. Untagged frames are forwarded via the default VLAN
- B. The trunked port is put in err-disable state
- C. It drops the untagged frames
- D. Untagged frames are forwarded via the native VLAN

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference:

[http://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/l2/vlan-dot1q-tag-native.html](http://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/l2/vlan-dot1q-tag-native.html)

#### QUESTION 369

Refer to the exhibit.

Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20? (Choose two.)

DSW1#nh spanning-tree

MST1

Spanning tree enabled protocol mstp

|           |            |                                           |
|-----------|------------|-------------------------------------------|
| Root ID   | Priority   | 32769                                     |
|           | Address    | 0018.7363.4300                            |
|           | Cost       | 2                                         |
|           | Port       | 13 (FastEthernet 1/0/11)                  |
|           | Hello Time | 2 sec Max Age 20 sec Forward Delay 15 sec |
| Bridge ID | Priority   | 32769 (priority 32768 sys-id-ext 1)       |
|           | Address    | 001b.0d8e.e080                            |
|           | Hello Time | 2 sec Max Age 20 sec Forward Delay 15 sec |

| Interface | Role | Sts | Cost | Prio.Nbr | Type             |
|-----------|------|-----|------|----------|------------------|
| Fa1/0/7   | Desg | FWD | 2    | 128.9    | P2p Bound (PVST) |
| Fa1/0/10  | Desg | FWD | 2    | 128.12   | P2p Bound (PVST) |
| Fa1/0/11  | Root | FWD | 2    | 128.13   | P2p              |
| Fa1/0/12  | Altn | BLK | 2    | 128.14   | P2p              |

DSW1#sh spanning-tree mst

```
#### MST1    vlans mapped:    10.20
Bridge       address 001b.0d8e.e080    priority    32769 (32768 sysid 1)
Root         address 001b.7363.4300    priority    32769 (32760 sysid 1)
              Port Fa1/0/11          cost        2      rem hops 19
!
... output omitted
!
```

- A. spanning-tree mst 1 root primary
- B. spanning-tree mstp vlan 10, 20 root primary
- C. spanning-tree mst 1 priority 4096
- D. spanning-tree mst vlan 10, 20 priority root
- E. spanning-tree mst 1 priority 1

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 370

Refer to the exhibit. Currently, R1 is the VRRP master virtual router. Which statement about the VRRP configuration on R1 and R2 is true?

```
R1#show running-config interface fa0/0
Building configuration...
```

```
Current configuration: 192 bytes
!
interface FastEthernet0/0
 ip address 192.168.3.5 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 priority 110
 vrrp 1 authentication text cisco
 vrrp 1 track 20 decrement 20
end
```

```
R1#show running-config | include track 20
track 20 ip route 10.10.1.1 255.255.255.255 reachability
```

```
R2#show running-config interface fa0/0
Building configuration...

Current configuration: 141 bytes
!
interface FastEthernet0/0
 ip address 192.168.3.2 255.255.255.0
 duplex full
 vrrp 1 ip 192.168.3.1
 vrrp 1 authentication text cisco
end
```

- A. R2 does not have a route to 10.10.1.1/32 in its routing table
- B. R2 becomes master if R1 reboots or track in R1 does not fail
- C. Communication between VRRP members is encrypted using md5
- D. R1 has a route to 10.10.1/32 in its routing table

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 371

Which two options are advantages of deploying VTPv3? (Choose two.)

- A. It supports the use of AES to encrypt VTP messaging
- B. It stores the VTP domain password securely as a SHA-1 hash
- C. It adds an FCS field at the end of each VTP frame for consistency checking
- D. It supports the propagation of private VLANs
- E. It can be configured to allow only one VTP server to make changes to the VTP domain

**Correct Answer:** DE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 372

Which two statements about StackWise are true? (Choose two.)

- A. It groups multiple switch ports as a single EtherChannel
- B. It uses a single IP address to communicate with the network
- C. It monitors multiple switches from a central console
- D. It enables multiple switch ports to share a single master configuration
- E. It allows multiple switches to operate as a single switch

**Correct Answer:** DE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 373

A physical switch port is part of an EtherChannel group. What happens while the same port is configured as a SPAN destination?

- A. The port forwards traffic in the EtherChannel group and acts as a SPAN source simultaneously
- B. The port is removed from the EtherChannel group
- C. The port is put in the errdisabled state and can only be reenabled manually
- D. The operation is not allowed as an EtherChannel member cannot be a SPAN source port

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 374

Which two conditions must be met to establish a Layer 2 EtherChannel? (Choose two.)

- A. The trunking protocol must be the same for all links in the EtherChannel
- B. SPAN must be disabled on the ports
- C. All ports in the EtherChannel must operate in half-duplex
- D. LAN ports in the EtherChannel must be contiguous
- E. All ports in the EtherChannel must be on the same module

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 375**

Which two authentication types does VRRP support? (Choose two.)

- A. CHAP
- B. plain-text
- C. PAP
- D. MD5
- E. 802.1x

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 376**

When using EtherChannel misconfiguration guard, which technology is used to prevent this type of misconfiguration from affecting the network?

- A. LACP
- B. STP
- C. PAgP
- D. port security

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 377**

Which two new features are included in VTPv3? (Choose two.)

- A. VTP now supports MD5 passwords
- B. VLANs in the extended range are now eligible to participate in VTP
- C. VTPs can now be configured in off mode
- D. It can be configured to prevent the override of the VLAN database
- E. VLANs configured for token ring are now eligible to participate in VTP

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 378**

Which switch is chosen as the stack master during a stack master election or re-election?

- A. the switch with the highest stack member ID
- B. the switch with the lowest stack member ID
- C. the switch with the lowest stack member priority value
- D. the switch with the highest stack member priority value

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 379**

Which feature actively validates DHCP messages and drops invalid messages?

- A. DHCP host tracking
- B. CGMP binding
- C. Dynamic ARP Inspection
- D. DHCP inspection
- E. DHCP snooping
- F. IGMP snooping

**Correct Answer:** E

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 380**

Which two limitations of local SPAN are true? (Choose two.)

- A. Each SPAN session supports only one source VLAN or interface
- B. A switch can support only one local SPAN session at a time
- C. It can monitor only traffic that ingresses or egresses on the source interface or VLAN
- D. A SPAN session can support multiple destination ports only if they are on the same VLAN
- E. The source and destination ports must reside in the same switch or switch stack

**Correct Answer:** CE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 381**  
Which command enables root guard on a Cisco switch at location id: XXXXXXXX?

- A. Switch(config)#spanning-tree guard root
- B. Switch(config-if)#spanning-tree root guard
- C. Switch(config)#spanning-tree root guard
- D. Switch(config-if)#spanning-tree guard root

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 382**  
When EtherChannel guard is enabled and a misconfiguration is detected on a port, how does the port respond?

- A. It enters the shutdown state
- B. It enters the channel-error state
- C. The port remains up, but it is unable to pass traffic
- D. The port state remains unchanged, but the EtherChannel stays down
- E. It enters the errdisable state

**Correct Answer:** E  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 383**  
DRAG DROP  
Drag and drop the characteristics from the left to the matching STP category on the right:

**Select and Place:**

|                                           |                      |
|-------------------------------------------|----------------------|
| increment of 4096                         | STP: Switch Priority |
| default value is based on interface speed |                      |
| increments of 16                          | STP: Port Priority   |
| The lowest value is preferred             |                      |
| value range of 1-200000000                | STP: Path Cost       |
| default value of 128                      |                      |

**Correct Answer:**



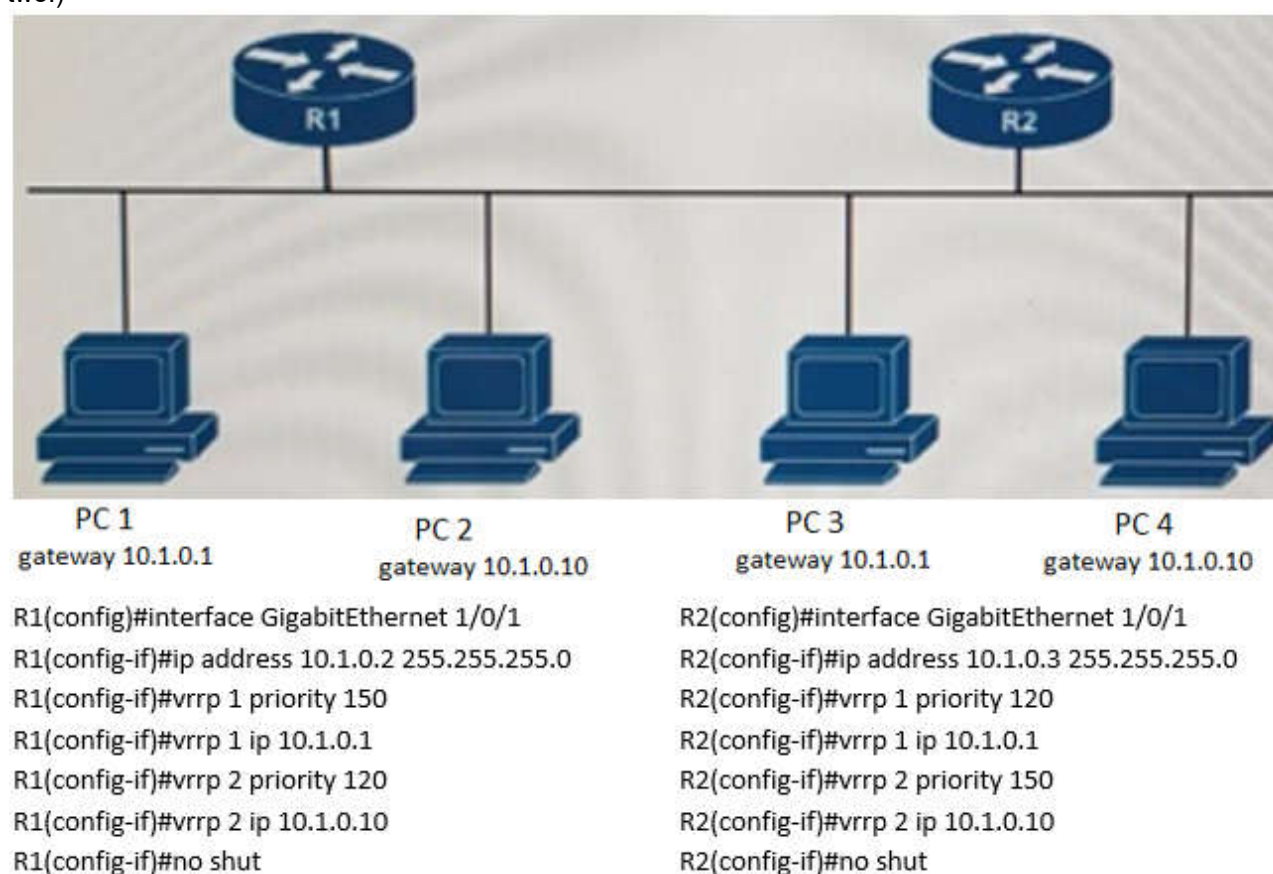
|  |                                           |
|--|-------------------------------------------|
|  | <b>STP: Switch Priority</b>               |
|  | The lowest value is preferred             |
|  | increment of 4096                         |
|  | <b>STP: Port Priority</b>                 |
|  | default value of 128                      |
|  | increments of 16                          |
|  | <b>STP: Path Cost</b>                     |
|  | default value is based on interface speed |
|  | value range of 1-200000000                |

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 384

Refer to the exhibit. You have configured routers R1 and R2 with VRRP for load sharing as shown. Which two effects of this configuration are true? (Choose two.)



- A. Router R1 is the primary gateway for 10.1.0.1 and router R2 is the primary gateway for 10.1.0.10
- B. The four PCs send all requests to router R1, which forward traffic to router R2 as necessary
- C. Router R2 is the primary gateway for 10.1.0.1 and router R1 is the primary gateway for 10.1.0.10
- D. The four PCs send packets round-robin between routers R1 and R2
- E. PC2 and PC4 use router R1 as the primary gateway
- F. PC1 and PC3 use router R1 as the primary gateway

**Correct Answer: AF**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 385

Which two prerequisites for HSRP to become active on an interface are true? (Choose two.)

- A. A virtual MAC address must be configured on the interface
- B. Cisco Express Forwarding must be disabled globally
- C. PIM routing must be disabled on the interface
- D. An IP address must be configured on the interface
- E. The VIP must be in the same subnet as the primary IP address

**Correct Answer:** DE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 386**

Refer to the exhibit. Which two statements about the network environment of the device that generated this output are true? (Choose two.)

```
FastEthernet1/0/47 - Group 1 (version 2)
  State is Standby
    7 state changes, last state change 00:00:02
  Virtual IP address is 10.1.1.1
  Active virtual MAC address is 0000.0c9f.f001 (v2 default)
    Local virtual MAC address is 0000.0c9f.f001 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.375 secs
  Authentication MD5, key-string "cisco"
  Preemption enabled, delay min 5 secs
  Active router is 10.1.1.2, priority 255 (expires in 9.396 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa1/0/47-1" (default)
```

- A. The virtual IP address of the HSRP group is 10.1.1.1
- B. If a router with a higher IP address and same HSRP priority as the active router becomes available, that router becomes the new active router 5 seconds later
- C. The local device has a higher priority setting than the active router
- D. The hello and hold timers are set to custom values
- E. If the local device fails to receive a hello from the active router for more than 5 seconds, it can become the active router

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 387**

If StormControl is enabled on a port and the traffic reaches the configured level, which two actions can be configured to occur? (Choose two.)

- A. trap
- B. log
- C. notify admin
- D. redirect traffic
- E. shut down

**Correct Answer:** AE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 388**

In which two ways can a port respond to a port-security violation? (Choose two.)

- A. The port enters the err-disabled state
- B. The port enters the shutdown state
- C. The port triggers an EEM script to notify support staff and continues to forward traffic normally
- D. The SecurityViolation counter is incremented and the port sends an SNMP trap
- E. The SecurityViolation counter is incremented and the port sends a critical syslog message to the console
- F. The port immediately begins to drop all traffic

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:

protect - The PFC drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.

restrict - The PFC drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value and causes the security violation counter to increment.

shutdown - Puts the interface into the error-disabled state immediately and sends an SNMP trap notification.

Restrict increments the counter and sends an SNMP trap. And shutdown puts the interface in err-disabled state.

**QUESTION 389**

Which two statements about Cisco Discovery Protocol are true? (Choose two.)

- A. It is not supported with SNMP

- B. It runs on OSI Layer 2
- C. It is supported on Frame Relay subinterfaces
- D. It uses a TLV to advertise the native VLAN
- E. It runs on OSI Layer 1

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 390**  
DRAG DROP

Drag and drop the characteristic from the left to the matching STP feature on the right.

**Select and Place:**

disables Spanning Tree on a configured interface

configured trunk interface goes immediately to a forwarding state from blocking state

shuts down port and places it in err-disabled mode

protects configured interface from sending and receiving unauthorized BPDU frames

configured on access port with a single host device

protects configured interface from receiving unauthorized BPDU frames

PortFast

BPDUGuard

BPDUFILTER

**Correct Answer:**

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |

**PortFast**

configured on access port with a single host device

configured trunk interface goes immediately to a forwarding state from blocking state

**BPDU Guard**

protects configured interface from receiving unauthorized BPDU frames

shuts down port and places it in err-disabled mode

**BPDU Filter**

protects configured interface from sending and receiving unauthorized BPDU frames

disables Spanning Tree on a configured interface

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 391  
Which two statements about GLBP are true? (Choose two.)

- A. The AVF assigns virtual MAC addresses to GLBP group members
- B. The AVG assigns virtual MAC addresses to GLBP group members
- C. The AVF responds to ARP requests for the virtual IP address
- D. The AVG responds to ARP requests for the virtual IP address
- E. LAN client traffic is handled by the active AVF only

Correct Answer: BD  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 392  
When a Cisco Catalyst switch that is configured in VTP server mode is first booted, which two VLAN ranges are loaded on the switch?

- A. all VLAN are in the VLAN database.
- B. VLANs greater than 1005 in the startup-config file
- C. the first 1005 VLANs in the VLAN database file
- D. the first 1005 VLANs in the startup-config file
- E. VLANs greater than 1005 in the VLAN database file

Correct Answer: BC  
Section: Mix Questions  
Explanation

Explanation/Reference:  
Explanation:

If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are selected by VLAN database information, such as the vlan.dat file. VLANs greater than 1005 are configured from the switch configuration file.

QUESTION 393  
An enterprise network has port security sticky enabled on all access ports.  
A network administrator moves a PC from one office desk to another.  
After the PC is moved, the network administrator clears the port security on the new network switch port connecting to the PC, but the port keeps going back into err-disabled mode.

Which two factors are possible causes of this issue? (Choose two)

- A. Port security sticky exists on the new network switch port.

- B. Port security sticky is disabled on the new network switch port.
- C. Port security must be disabled on all access ports.
- D. Port security is still enabled on the older network switch port.
- E. Port security sticky is still enabled on the older network switch port.

**Correct Answer:** AE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 394 SIMULATION

Lab Simulation - AAA dot1x

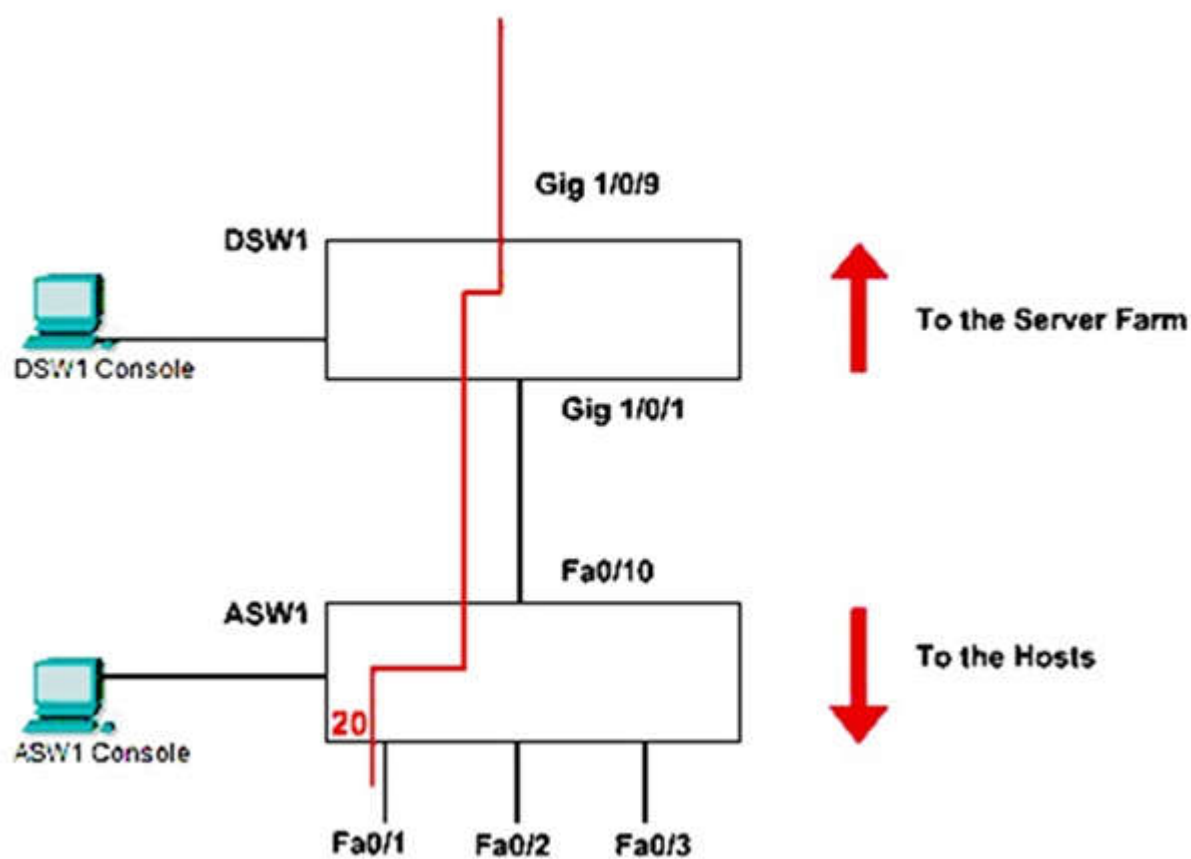
ABC.com is an IT company that has an existing enterprise network comprised of two layer 2 only switches; DSW1 and ASW1. The topology diagram indicates their layer 2 mapping. VLAN 20 is a new VLAN that will be used to provide the shipping personnel access to the server. Corporate policies do not allow layer 3 functionality to be enabled on the switches.

For security reasons, it is necessary to restrict access to VLAN 20 in the following manner:

Users connecting to VLAN 20 via portF0/1 on ASW1 must be authenticated before they are given access to the network. Authentication is to be done via a Radius server:

- Radius server host: 172.120.40.46
- Radius key: rad123
- Authentication should be implemented as close to the host as possible.
- Devices on VLAN 20 are restricted to the subnet of 172.120.40.0/24.
- Packets from devices in the subnet of 172.120.40.0/24 should be allowed on VLAN 20.
- Packets from devices in any other address range should be dropped on VLAN 20.
- Filtering should be implemented as close to the serverfarm as possible.

The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers. You must use the available IOS switch features.



**Correct Answer:** See the explanation  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:

1. Verification of Pre-configuration:

- a. Check that the denoted vlan [vlan20] is created in both switches and ports [fa0/1 of ASW1] are assigned.
- b. Take down the radius-server ip [172.120.39.46] and the key [rad123].
- c. Take down the IP range [172.120.40.0/24] to be allowed the given vlan [vlan20]

Configure the Port based authentication on ASW1: Enable AAA on the switch:

```
ASW1> enable
ASW1# conf t
ASW1(config)# aaa new-model
```

The new-model keyword refers to the use of method lists, by which authentication methods and sources can be grouped or organized. Define the server along with its secret shared password:



```
ASW1(config)# aaa authentication dot1x default group radius ASW1(config)# radius-server host 172.120.39.46 key rad123
```

This command causes the RADIUS server defined on the switch to be used for 802.1x authentication.  
Enable 802.1x on the switch:

```
ASW1(config)# dot1x system-auth-control
```

Configure Fa0/1 to use 802.1x:

```
ASW1(config)# interface fastEthernet 0/1
ASW1(config-if)# switchport mode access
ASW1(config-if)# dot1x port-control auto
```

Notice that the word “auto” will force connected PC to authenticate through the 802.1x exchange.

```
ASW1(config-if)# exit
ASW1# copy running-config startup-config
```

Filter the traffic and create vlan access-map to restrict the traffic only for a range on DSW1 Define an access-list:

```
DSW1> enable
DSW1# conf t
DSW1(config)# ip access-list standard 10 (syntax: ip access-list {standard | extended} acl-name)
```

```
DSW1(config-ext-nacl)# permit 172.120.40.0 0.0.0.255 DSW1(config-ext-nacl)# exit
```

Define an access-map which uses the access-list above:

```
DSW1(config)# vlan access-map MYACCMAP 10 (syntax: vlan access-map map_name [0-65535]
)
```

```
DSW1(config-access-map)# match ip address 10 (syntax: match ip address {acl_number | acl_name})
DSW1(config-access-map)# action forward
DSW1(config-access-map)# exit
DSW1(config)# vlan access-map MYACCMAP 20
DSW1(config-access-map)# action drop (drop other networks)
DSW1(config-access-map)# exit
```

Apply a vlan-map into a vlan:

```
DSW1(config)# vlan filter MYACCMAP vlan-list 20 (syntax: vlan filter mapname vlan-list list)
DSW1# copy running-config startup-config
```

4. Note:

It is not possible to verify the configuration in this lab. All we have do the correct configurations. Most of the exam takers report that “copy running-config startup-config” is not working. It does not a matter. Do not try unwanted/wrong commands in the consoles. They are not real switches.

#### QUESTION 395

Based on the show spanning-tree vlan 200 output shown in the exhibit, which two statements about the STP process for VLAN 200 are true? (Choose two.)

```
Switch#show spanning-tree vlan 200
```

```
VLAN200
  Spanning tree enabled protocol IEEE
    Root ID    Priority    32968
              Address     000c.ce29.ef00
              Cost        19
              Port        2 (FastEthernet0/2)
              Hello Time  10 sec Max Age 20 sec Forward Delay 30 sec
    Bridge ID  Priority    32968 (priority 32768 sys-id-ext 200)
              Address     000c.ce2a.4180
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time 300
Interface    Role  Sts  Cost      Prio.Nbr  Type
-----
Fa0/2        Root  FWD  19         128.2     P2p
Fa0/3        Altn  BLK  19         128.3     P2p
```

- A. BPDUs will be sent out every two seconds.
- B. The time spent in the listening state will be 30 seconds.
- C. The time spent in the learning state will be 15 seconds.
- D. The maximum length of time that the BPDU information will be saved is 30 seconds
- E. This switch is the root bridge for VLAN 200.
- F. BPDUs will be sent out every 10 seconds.

**Correct Answer:** BF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 396

Which three statements are correct with regard to the IEEE 802.1Q standard? (Choose three.)

- A. The IEEE 802.1Q frame format adds a 4 byte field to a Ethernet frame
- B. The packet is encapsulated with a 26 byte header and a 4 byte FCS

- C. The protocol uses point-to-multipoint connectivity
- D. The protocol uses point-to-point connectivity
- E. The IEEE 802.1Q frame uses multicast destination of 0x01-00-0c-00-00
- F. The IEEE 802.1Q frame retains the original MAC destination address

**Correct Answer:** ADF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 397**  
Refer to the exhibit. Based upon the output of show vlan on switch CAT2, what can we conclude about interfaces Fa0/13 and Fa0/14?

| CAT2#show vlan |                 |           |                                                                                                                                                                                               |
|----------------|-----------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN           | Name            | Status    | Ports                                                                                                                                                                                         |
| 1              | default         | active    | Fa0/1, Fa0/2, Fa0/3, Fa0/4<br>Fa0/5, Fa0/6, Fa0/7, Fa0/8<br>Fa0/9, Fa0/10, Fa0/11, Fa0/12<br>Fa0/15, Fa0/16, Fa0/17, Fa0/18<br>Fa0/19, Fa0/20, Fa0/21, Fa0/22<br>Fa0/23, Fa0/24, Gi0/1, Gi0/2 |
| 2              | VLAN0002        | active    |                                                                                                                                                                                               |
| 3              | VLAN0003        | active    |                                                                                                                                                                                               |
| 4              | VLAN0004        | active    |                                                                                                                                                                                               |
| 5              | VLAN0005        | active    |                                                                                                                                                                                               |
| 1002           | fddi-default    | act/unsup |                                                                                                                                                                                               |
| 1003           | trcrf-default   | act/unsup |                                                                                                                                                                                               |
| 1004           | fddinet-default | act/unsup |                                                                                                                                                                                               |
| 1005           | trbrf-default   | act/unsup |                                                                                                                                                                                               |

- A. That interfaces Fa0/13 and Fa0/14 are in VLAN 1
- B. That interfaces Fa0/13 and Fa0/14 are down
- C. That interfaces Fa0/13 and Fa0/14 are trunk interfaces
- D. That interfaces Fa0/13 and Fa0/14 have a domain mismatch with another switch
- E. That interfaces Fa0/13 and Fa0/14 have a duplex mismatch with another switch

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 398**  
VLAN maps have been configured on switch R1. Which of the following actions are taken in a VLAN map that does not contain a match clause?

- A. Implicit deny feature at end of list.
- B. Implicit deny feature at start of list.
- C. Implicit forward feature at end of list
- D. Implicit forward feature at start of list.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 399**  
Given the configuration on a switch interface, what happens when a host with the MAC address of 0003.0003.0003 is directly connected to the switch port?

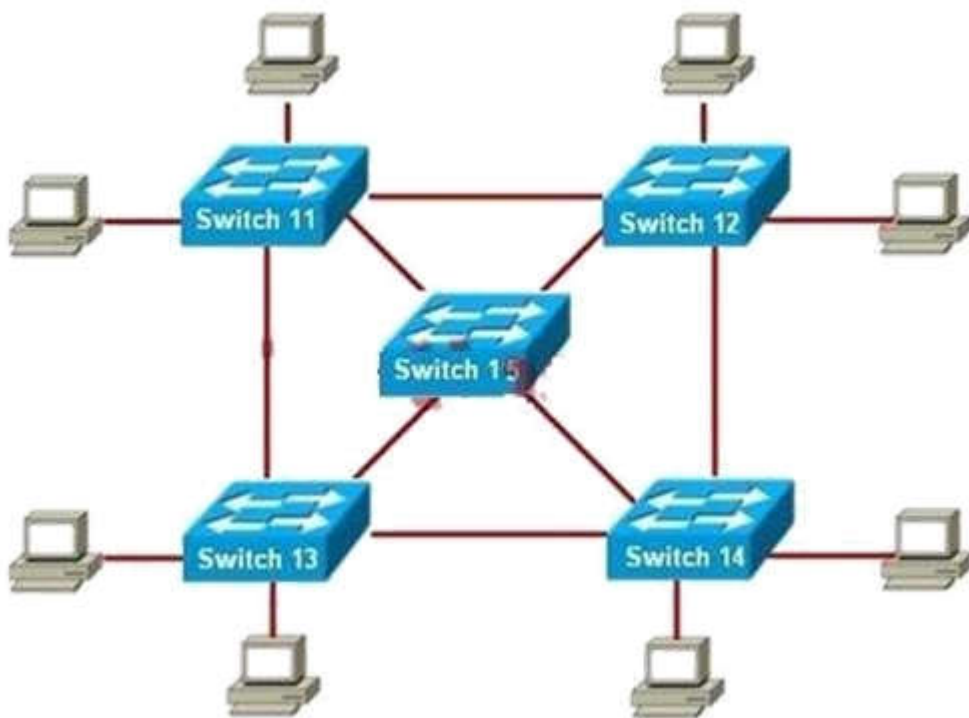
```
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security mac-address 0002.0002.0002
switchport port-security violation shutdown
```

- A. The host will be allowed to connect.
- B. The port will shut down.
- C. The host can only connect through a hub/switch where 0002.0002.0002 is already connected.
- D. The host will be refused access.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 400**  
Refer to the exhibit. Switch 15 is configured as the root switch for VLAN 10 but not for VLAN 20. If the STP configuration is correct, what will be true about Switch 15?



- A. All ports will be in forwarding mode.
- B. All ports in VLAN 10 will be in forwarding mode.
- C. All ports in VLAN 10 will be in forwarding mode and all ports in VLAN 20 will be in blocking mode.
- D. All ports in VLAN 10 will be in forwarding mode and all ports in VLAN 20 will be in standby mode.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 401**  
 Which of the following HSRP router states does an active router enter when it is preempted by a higher priority router?

- A. active
- B. speak
- C. learn
- D. listen
- E. init
- F. standby

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 402**  
 Refer to the exhibit. On the basis of the output of the show spanning- tree inconsistentports command, which statement about interfaces FastEthernet 0/1 and FastEthernet 0/2 is true?

| SW1# show spanning-tree inconsistentports                 |                  |                   |
|-----------------------------------------------------------|------------------|-------------------|
| Name                                                      | Interface        | Inconsistency     |
| VLAN0001                                                  | FastEthernet0/ 1 | Root Inconsistent |
| VLAN0001                                                  | FastEthernet0/2  | Root Inconsistent |
| Number of inconsistent ports (segments) in the system : 2 |                  |                   |

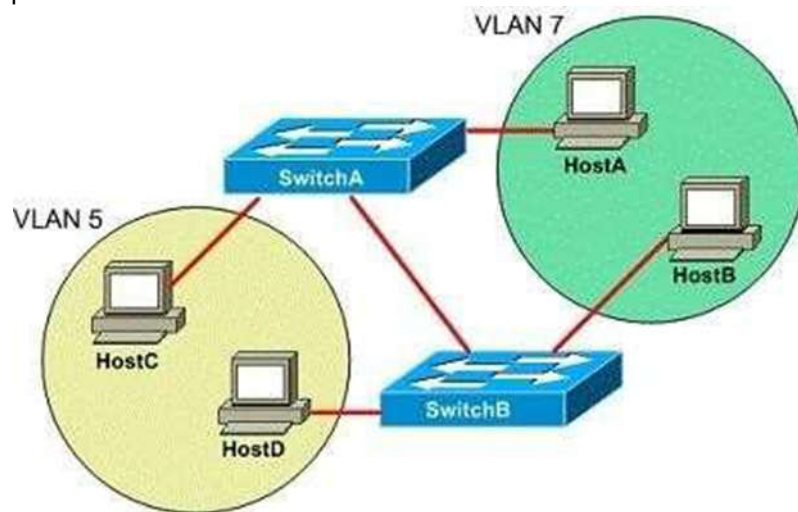
- A. They have been configured with the spanning-tree bpduguard disable command.
- B. They have been configured with the spanning-tree bpduguard enable command.
- C. They have been configured with the spanning-tree bpduguard disable command.
- D. They have been configured with the spanning-tree bpduguard enable command.
- E. They have been configured with the spanning-tree guard loop command.
- F. They have been configured with the spanning-tree guard root command.

**Correct Answer:** F  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 403**  
 You want to configure a switched internetwork with multiple VLANs as shown above. Which of the following commands should you issue on SwitchA for the

port connected to SwitchB?



- A. switchport mode trunk
- B. switchport access vlan 5
- C. switchport mode access vlan 5
- D. switchport trunk native vlan 5

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 404

You administer a network that uses two routers, R1 and R2, configured as an HSRP group to provide redundancy for the gateway. Router R1 is the active router and has been configured as follows:

```
R1#configure terminal
R1(config)#interface fa0/0
R1(config-if)#ip address 10.10.0.5 255.255.255.0
R1(config-if)#standby 1 priority 150
R1(config-if)#standby preempt delay minimum 50
R1(config-if)#standby 1 track interface fa0/2 15
R1(config-if)#standby 1 ip 10.10.0.20
```

Which of the following describes the effect the "standby preempt delay minimum 50" command will have on router R1?

- A. The HSRP priority for router R1 will increase to 200.
- B. Router R1 will become the standby router if the priority drops below 50.
- C. The HSRP priority for router R1 will decrease to 50 points when Fa0/2 goes down.
- D. Router R1 will wait 50 seconds before attempting to preempt the active router.

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 405

Which statement is correct about 802.1Q trunking?

- A. Both switches must be in the same VTP domain.
- B. The encapsulation type of both ends of the trunk does not have to match.
- C. The native VLAN on both ends of the trunk must be VLAN 1.
- D. 802.1Q trunking can only be configured on a Layer 2 port.
- E. In 802.1Q trunking, all VLAN packets are tagged on the trunk link, except the native VLAN.

**Correct Answer: E**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 406

Which of the following commands can be issued without interfering with the operation of loop guard?

- A. Switch(config-if)#spanning-tree guard root
- B. Switch(config-if)#spanning-tree portfast
- C. Switch(config-if)#switchport mode trunk
- D. Switch(config-if)#switchport mode access

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 407**

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 is true about this command?

- 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 ad01.
- E. This command will not work because the active parameter is missing

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 408**

Routers R1 and R2 are configured for HSRP as shown below:

Router R1:  
interface ethernet 0  
ip address 20.6.2.1 255.255.255.0  
standby 35 ip 20.6.2.21  
standby 35 priority 100  
interface ethernet 1  
ip address 20.6.1.1.2 255.255.255.0  
standby 34 ip 20.6.1.21

Router R2:  
interface ethernet 0  
ip address 20.6.2.2 255.255.255.0  
standby 35 ip 20.6.2.21  
interface ethernet 1  
ip address 20.6.1.1.1 255.255.255.0  
standby 34 ip 20.6.1.21  
standby 34 priority 100

You have configured the routers R1 & R2 with HSRP. While debugging router R2 you notice very frequent HSRP group state transitions. What is the most likely cause of this?

- A. physical layer issues
- B. no spanning tree loops
- C. use of non-default HSRP timers
- D. failure to set the command standby 35 preempt

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 409**

Which two statements about the HSRP priority are true? (Choose two.)

- A. To assign the HSRP router priority in a standby group, the standby group-number priority priority-value global configuration command must be used.
- B. The default priority of a router is zero (0).
- C. The no standby priority command assigns a priority of 100 to the router.
- D. Assuming that preempting has also been configured, the router with the lowest priority in an HSRP group would become the active router.
- E. When two routers in an HSRP standby group are configured with identical priorities, the router with the highest configured IP address will become the active router.

**Correct Answer: CE**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 410**

Which three statements are true of a default HSRP configuration? (Choose three.)

- A. The Standby hello time is 2 seconds.
- B. Two HSRP groups are configured.
- C. The Standby track interface priority decrement is 10.
- D. The Standby hold time is 10 seconds
- E. The Standby priority is 100.
- F. The Standby delay is 3 seconds.

**Correct Answer: CDE**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**



**QUESTION 411**

Refer to the exhibit. What is the result of setting GLBP weighting at 105 with lower threshold 90 and upper threshold 100 on this router?

```
Router# show glbp FastEthernet0/1 1
FastEthernet0/1 - Group 1
State is Listen
 64 state changes, last state change 00:00:54
Virtual IP address is 10.1.0.7
Hello time 50 msec, hold time 200 msec
Next hello sent in 0.030 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Authentication text "authword"
Preemption enabled, min delay 0 sec
Active is 10.1.0.2, priority 105 (expires in 0.184 sec)
Standby is 10.1.0.3, priority 100 (expires in 0.176 sec)
Priority 96 (configured)
Weighting 105 (configured 105), thresholds: lower 90, upper 100
Track object 1 state Up decrement 10
Track object 2 state Up decrement 10
Load balancing: round-robin
IP redundancy name is "glbp1"
Group members:
 0004.4d83.4801 (10.0.0.0)
 0010.7b5a.fa41 (10.0.0.1)
 00d0.bbd3.bc21 (10.0.0.2) local
```

- A. Only if both tracked objects are up will this router will be available as an AVF for group 1.
- B. Only if the state of both tracked objects goes down will this router release its status as an AVF for group 1.
- C. If both tracked objects go down and then one comes up, but the other remains down, this router will be available as an AVF for group 1.
- D. This configuration is incorrect and will not have any effect on GLBP operation.
- E. If the state of one tracked object goes down, then this router will release its status as an AVF for group 1.

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 412**

Which describes the default load balancing scheme used by the Gateway Load Balancing Protocol (GLBP)?

- A. Per host using a strict priority scheme
- B. Per session using a round-robin scheme
- C. Per session using a strict priority scheme
- D. Per GLBP group using a strict priority scheme
- E. Per host basis using a round robin-scheme
- F. Per GLBP group using a round-robin scheme

**Correct Answer: E**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 413**

DRAG DROP

Select and Place:

Syslog information can generate messages up to and including the configured severity level. Organize the levels by dragging each the highest level all the top and the lowest level at the bottom.

**Select and Place:**

debugging

notification

error

alert

emergency

critical

warning

informational

Correct Answer:

emergency

alert

critical

error

warning

notification

informational

debugging

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 414  
DRAG DROP

Select and Place:

Drag the choices on the left to the boxes on the right that should be included when creating an implementation plan. Not all choices will be used.

Select and Place:

reference to design documents

roll back guidelines

VTP assignments

detailed implementation plans

time required to perform the implementation

Correct Answer:

VTP assignments

reference to design documents

roll back guidelines

detailed implementation plans

time required to perform the implementation

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 415  
DRAG DROP

Select and Place:

You have been tasked with planning a VLAN solution that will connect a server in one building to several hosts in another building of the local VLAN model and Layer 3 switching at the distribution layer. Drag the questions that you would ask the network administrator from the left to the right. Not all questions will be used.

Select and Place:

Is there interswitch connectivity?

What version of VTP is being used?

What routing protocol will be used?

What VLANs are availbale on each switch?

What operating system is used on the server?

What switch ports are available in each building?

What IP addresses are available on each subnet?

What operating system is used on each host?

Questions related to the VLAN Solution

Correct Answer:

What version of VTP is being used?

What operating system is used on the server?

What operating system is used on each host?

Questions related to the VLAN Solution

Is there interswitch connectivity?

What routing protocol will be used?

What VLANs are availbale on each switch?

What switch ports are available in each building?

What IP addresses are available on each subnet?

Section: Mix Questions

Explanation

Explanation/Reference:

**QUESTION 416**

DRAG DROP

Select and Place:

Drag the attributes on the left to the types of VLAN designs that they describe on the right.

Select and Place:

|                                                                                                                                                      |                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|
| Created with physical boundaries in mind rather than the departments or organizations of the users on the end devices                                | <b>End-to-end VLANs</b><br><div></div> <div></div> |
| VLANs on one switch are not advertised to all other switches in the network, nor do they need to be created in the VLAN database of any other switch |                                                    |
| As a user moves through a campus, the VLAN membership of the user remains the same regardless of the physical switch this user attaches to           | <b>Local VLANs</b><br><div></div> <div></div>      |
| Users are grouped into each VLAN regardless of physical location                                                                                     |                                                    |

Correct Answer:

|  |                                                                                                                                                                                                                                                                                                                        |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <b>End-to-end VLANs</b><br><div>As a user moves through a campus, the VLAN membership of the user remains the same regardless of the physical switch this user attaches to</div> <div>Users are grouped into each VLAN regardless of physical location</div>                                                           |
|  |                                                                                                                                                                                                                                                                                                                        |
|  | <b>Local VLANs</b><br><div>Created with physical boundaries in mind rather than the departments or organizations of the users on the end devices</div> <div>VLANs on one switch are not advertised to all other switches in the network, nor do they need to be created in the VLAN database of any other switch</div> |
|  |                                                                                                                                                                                                                                                                                                                        |

Section: Mix Questions

Explanation

Explanation/Reference:

**QUESTION 417**

DRAG DROP

Select and Place:

Select and Place:



Place the DTP mode with its correct description.

|                   |                                                                          |
|-------------------|--------------------------------------------------------------------------|
| Trunk             | specifies that DTP packets are not sent out this interface               |
| Nonegotiate       | sets the switch port to trunk mode and negotiates to become a trunk      |
| Access            | sets a switch port to permanent nontrunking mode                         |
| Dynamic Auto      | sets the switch port to respond, but not actively send DTP frames        |
| Dynamic Desirable | makes the interface actively attempt to convert the link to a trunk link |

Correct Answer:

Place the DTP mode with its correct description.

|  |                   |
|--|-------------------|
|  | Nonegotiate       |
|  | Trunk             |
|  | Access            |
|  | Dynamic Auto      |
|  | Dynamic Desirable |

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 418  
DRAG DROP

Select and Place:  
Drag the port states to their correct description

Select and Place:

|            |                                                                                                   |
|------------|---------------------------------------------------------------------------------------------------|
| blocking   | Sends and receives BPDUs to determine root, but does not update the MAC address table - listening |
| listening  | Does not participate in frame forwarding or in STP                                                |
| learning   | Does not participate in frame forwarding                                                          |
| forwarding | Sends and receives data frames                                                                    |
| disabled   | Populates the MAC address table, but will not forward user data                                   |

Correct Answer:



listening

disabled

blocking

forwarding

learning

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 419  
DRAG DROP

Select and Place:

Capabilities of SNMP are dependent on the version implemented. Drag the feature descriptions on the left to the respective SNMP.

Select and Place:

Increased 64-bit counters for new data types

Security levels

Get next request

Informed request

Unsolicited agent alarm message

Username

SNMPv1

SNMPv2

SNMPv3

Correct Answer:

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |

SNMPv1

Get next request

Unsolicited agent alarm message

SNMPv2

Increased 64-bit counters for new data types

Informed request

SNMPv3

Security levels

Username

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 420
DRAG DROP

Select and Place:

You have a VLAN implementation that requires inter-VLAN routing using Layer 3 switches. Drag the steps from the left to the right. Not all choices will be used.

Select and Place:

Verify that VTP is pruning the proper access ports

Verify that there is inter-switch connectivity

Verify that the data and voice VLANs are NOT assigned a trunk's native VLAN

Verify that the needed switch virtual interfaces have been created

Verify that the VLAN ports are in promiscuous mode

Verify that the proper ports are assigned to the VLAN

Correct Answer:

|                                                    |
|----------------------------------------------------|
| Verify that VTP is pruning the proper access ports |
|                                                    |
|                                                    |
|                                                    |
| Verify that the VLAN ports are in promiscuous mode |
|                                                    |

|                                                                             |
|-----------------------------------------------------------------------------|
| Verify that there is inter-switch connectivity                              |
| Verify that the data and voice VLANs are NOT assigned a trunk's native VLAN |
| Verify that the needed switch virtual interfaces have been created          |
| Verify that the proper ports are assigned to the VLAN                       |

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 421  
DRAG DROP

Select and Place:

Prioritize the traffic types by dragging them from the left to the appropriate Cisco priority level on the right. Put the highest priority at the bottom.

Select and Place:

|                    |
|--------------------|
| network management |
| video-interactive  |
| IP routing         |
| voice              |
| video-streaming    |
| call signaling     |

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |

Correct Answer:

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |

|                    |
|--------------------|
| voice              |
| video-interactive  |
| video-streaming    |
| call signaling     |
| IP routing         |
| network management |

Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 422  
DRAG DROP

Match the HSRP states on the left with the correct definition on the right.  
Select and Place:

Select and Place:

| Select from these | Place here                                                                |
|-------------------|---------------------------------------------------------------------------|
| Learn             | <div></div> State from which the routers begin the HSRP process           |
| Listen            | <div></div> A candidate to become the next active router                  |
| Speak             | <div></div> The router is still waiting to hear from the active router    |
| Standby           | <div></div> The router is currently forwarding packets                    |
| Active            | <div></div> Listens for hello messages from the active and standby router |
| Initial           | <div></div> Participates in the election for the active or standby router |

Correct Answer:

| Select from these | Place here                                                                      |
|-------------------|---------------------------------------------------------------------------------|
| <div></div>       | Initial <div>State from which the routers begin the HSRP process</div>          |
| <div></div>       | Standby <div>A candidate to become the next active router</div>                 |
| <div></div>       | Learn <div>The router is still waiting to hear from the active router</div>     |
| <div></div>       | Active <div>The router is currently forwarding packets</div>                    |
| <div></div>       | Listen <div>Listens for hello messages from the active and standby router</div> |
| <div></div>       | Speak <div>Participates in the election for the active or standby router</div>  |

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 423  
DRAG DROP

Select and Place:

Categorize the high availability network resources or feature items on the left by dragging them to the appropriate resiliency or management level on the right.

Select and Place:

dual power supplies

RSTP

IP SLA responder

NSF

NTP

SSO

Management Level

Network Level

System Level

Correct Answer:

Management Level

IP SLA responder

NTP

Network Level

RSTP

NSF

System Level

dual power supplies

SSO

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 424  
Which two statements about default FHRP behavior are true? (Choose two.)

- A. A backup GLBP active virtual gateway can become active only if the current active virtual gateway fails.
- B. Preemption is enabled by default.
- C. Unless specifically Configured, the priority of an HSRP router is 200.
- D. A standby HSRP router becomes active if it has a higher priority than the priority of the current active router.
- E. A VRRP backup virtual router becomes the master router if its priority is higher than the priority of the current master router.

Correct Answer: AE  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 425  
To provide security, a service provider configures various private VLANs in its backbone network infrastructure to prevent certain VLANs from communicating to each other. Which version of VTP supports the use of private VLANs?

- A. Version 1



- B. Version 3
- C. VTP does not support private VLANs
- D. Version 2

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 426

Which statement about HSRP, GLBP, and VRRP is true?

- A. VRRP group members communicate using multicast address 224.0.0.102.
- B. MAC address 0000.0c07.ac0c indicates that default gateway redundancy is provided through GLBP.
- C. HSRP group members communicate using multicast address 224.0.0.18.
- D. GLBP uses UDP port 3222 (source and destination) for hello messages.
- E. MAC address 0c07.A698.8904 indicates that default gateway redundancy is provided through HSRP.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 427

What action should a network administrator take to enable VTP pruning on an entire management domain?

- A. Enable VTP pruning on any client switch in the domain.
- B. Enable VTP pruning on every switch in the domain.
- C. Enable VTP pruning on any switch in the management domain.
- D. Enable VTP pruning on a VTP server in the management domain.

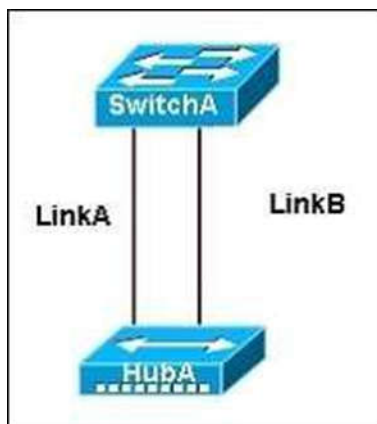
**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 428

Refer to the exhibit. BPDUGuard is enabled on both ports of SwitchA. Initially, LinkA is connected and forwarding traffic. A new LinkB is then attached between SwitchA and HubA.

Which two statements about the possible result of attaching the second link are true? (Choose two.)



- A. The switch port attached to LinkB does not transition to up.
- B. One or both of the two switch ports attached to the hub goes into the err-disabled state when a BPDU is received.
- C. Both switch ports attached to the hub transition to the blocking state.
- D. A heavy traffic load could cause BPDU transmissions to be blocked and leave a switching loop.
- E. The switch port attached to LinkA immediately transitions to the blocking state.

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 429

What is the effect of configuring the following command on a switch?

Switch(config) # spanning-tree portfast bpduguard default

- A. If BPDUs are received by a port configured for PortFast, then PortFast is disabled and the BPDUs are processed normally.
- B. If BPDUs are received by a port configured for PortFast, they are ignored and none are sent.
- C. If BPDUs are received by a port configured for PortFast, the port transitions to the forwarding state.
- D. The command enables BPDU filtering on all ports regardless of whether they are configured for BPDU filtering at the interface level.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 430**

Which protocol will enable a group of routers to form a single virtual router and will use the real IP address of a router as the gateway address?

- A. Proxy ARP
- B. HSRP
- C. IRDP
- D. VRRP
- E. GLBP

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 431**

Which two statements are true about recommended practices that are to be used in a local VLAN solution design where layer 2 traffic is to be kept to a minimum? (Choose two.)

- A. Routing should occur at the access layer if voice VLANs are utilized. Otherwise, routing should occur at the distribution layer.
- B. Routing may be performed at all layers but is most commonly done at the core and distribution layers.
- C. Routing should not be performed between VLANs located on separate switches.
- D. VLANs should be local to a switch.
- E. VLANs should be localized to a single switch unless voice VLANs are being utilized.

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 432**

What two things occur when an RSTP edge port receives a BPDU? (Choose two.)

- A. The port immediately transitions to the forwarding state.
- B. The switch generates a Topology Change Notification BPDU.
- C. The port immediately transitions to the err-disable state.
- D. The port becomes a normal STP switch port.

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 433**

How does VTP pruning enhance network bandwidth?

- A. by restricting unicast traffic across VTP domains
- B. by reducing unnecessary flooding of traffic to inactive VLANs
- C. by limiting the spreading of VLAN information
- D. by disabling periodic VTP updates

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 434**

In the hardware address 0000.0c07.ac0a, what does 07.ac represent?

- A. vendor code
- B. HSRP group number
- C. HSRP router number
- D. HSRP well-known physical MAC address
- E. HSRP well-known virtual MAC address

**Correct Answer:** E  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 435**

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

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 436**

Refer to the exhibit. Based on the debug output, which three statements about HSRP are true? (Choose three.)

```
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: V111 Interface up
*Mar 1 00:16:43.099: SB11: V111 Init: a/HSRP enabled
*Mar 1 00:16:43.099: SB11: V111 Init => Listen
*Mar 1 00:16:43.295: SB11: V111 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.295: SB11: V111 Active router is 172.16.11.112
*Mar 1 00:16:43.295: SB11: V111 Listen: b/Hello revd from lower pri Active router
(50/172.16.11.112)
*Mar 1 00:16:43.295: SB11: V111 Active router is local, was 172.16.11.112
*Mar 1 00:16:43.299: % STANDBY-6-STATECHANGE: Vlan11 Group 11 state Listen => Active
*Mar 1 00:16:43.299: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:43.303: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:46.207: SB11: V111 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:49.095: SB11: V111 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
```

- A. The final active router is the router with IP address 172.16.11.111.
- B. The router with IP address 172.16.11.111 has preempt configured.
- C. The priority of the router with IP address 172.16.11.112 is preferred over the router with IP address 172.16.11.111.
- D. The IP address 172.16.11.115 is the virtual HSRP IP address.
- E. The router with IP address 172.16.11.112 has nonpreempt configured.
- F. The router with IP address 172.16.11.112 is using default HSRP priority.

**Correct Answer:** ABD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 437**

In a switch stack where is the SDM template stored?

- A. All switches in stack
- B. Master switch
- C. Flash memory

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 438**

Refer to exhibit, which two statements correctly indicate when an SNMP trap is set to the switch? (Choose two.)

```
Switch(config)# snmp-server enable traps mac-notification
Switch(config)# mac address-table notification threshold
Switch(config)# mac address-table notification threshold limit 60
Switch(config)# mac address-table notification mac-move
```

- A. When a new workstation connects to port Fa0/1

- B. When 61 MAC address are in the switch table
- C. When 61 percent of the MAC address table capacity is used
- D. When the switch loses power and reboots
- E. When the phone previously on Fa0/2 is now connect to Fa0/5

**Correct Answer:** CE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 439

What is the default port security violation?

- A. log
- B. shutdown
- C. no change
- D. error-disable

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 440

What is the command for configuring root guard?

- A. (config)#spanning-tree guard root
- B. (config-if)#spanning-tree guard root
- C. (config-if)#spanning-tree root guard
- D. (config-if)#spanning tree guard root
- E. (config)#spanning-tree root guard

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 441

Network engineer wants to use UDLD, what he need to consider?

- A. udld is a non-propriety
- B. udld is working with non cisco devices
- C. udld is layer 1
- D. udld can aggressively disabled the port after eight failed retries

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 442

What is cisco recommendation for RSPAN best practice?

- A. you should configure remote vlan first
- B. use different vlan for multiple/different switches
- C. use different portchannel

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 443

What is needed for Virtual Switching System "VSS"?

- A. portchannel
- B. trunk
- C. Virtual Switching Link "or VSL"

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 444**

Which will identify the master switch in stack wise?

- A. lower priority
- B. higher priority
- C. lower id
- D. higher id

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 445**

What happens if you apply this command "vlan dot1q tag native"?

- A. packet will be dropped
- B. packet go to default vlan
- C. packet go to native vlan

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 446**

An engineer is configuring an EtherChannel between two switches using PAgP If the EtherChannel mode on switch 1 is configured to auto, which modes on switch 2 establish an operational EtherChannel?

- A. active
- B. auto
- C. desirable
- D. on
- E. passive

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 447**

Refer to the exhibit. Which two statements can be derived from the output of the show standby command? (Choose two.)

```
switch#show standby
FastEthernet0/0 - Group 40
State is Standby
2 state changes,last state change 00:20:53
Virtual IP address is 192.168.1.1
Active virtual MAC address is 0000.0c07.ac28
local virtual MAC address is 0000.0c07.ac28 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is 192.168.1.3 priority 85
Standby router is local
Priority 90 (configured 90)
Track interface Fa0/0 state decrement 10
```

- A. The active router will change as soon as the fa0/0 link is restored
- B. 192.168.1.3 is active because it has higher IP address
- C. when Fa0/0 is down priority will be 80
- D. it is using default hello and hold values

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 448**

What happens spoofed packet or something like untrusted packet is detected? (Choose three)

- A. log
- B. deletes
- C. intercepts
- D. accepts
- E. discad

**Correct Answer:** ACE

**Section:** Mix Questions

**Explanation**



**Explanation/Reference:**

**QUESTION 449**

Refer to the exhibit. An engineer is configuring an etherchannel between two switches, he notices the error message on Switch 2 (error message channel-misconfiguring error), based on the output what is the problem?

- A. the etherchannel on the switch 1 using incorrect member port
- B. the etherchannel interface of switch 1 is not configured
- C. the etherchannel protocol on switch 1 is not correct
- D. the etherchannel interface of switch 2 is not configured

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 450**

What is the Ethernet frame size for 802.1Q?

- A. 64
- B. 128
- C. 1518
- D. 1522

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 451**

Which two statements are true about StackWise? (Choose two.)

- A. It looks like one device.
- B. It can use one IP address.
- C. It can use multiple IP address.
- D. It looks like a multiple device.
- E. StackWise manages like a hybrid device.

**Correct Answer: AB**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 452**

If HSRP group number is 45 what would be the MAC address?  
(Basically conversion of digit to hexadecimal with group of 16.)

- A. 00-00-0c-07-ac-2D
- B. 00-00-0c-07-ac-2E
- C. 00-00-0c-07-ac-25
- D. 00-00-0c-07-ac-45

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Explanation:

00-00-0c- 07-ac-2D

CISCO\_ID:HSRP\_ID:GROUP\_ID

2d=45

**QUESTION 453**

Select a valid VRRP configuration from a list of possible configurations.

- A. vrrp [group-number] ip [ip-address]
- B. vrrp [group-number] priority [priority]
- C. vrrp [group-number] preempt

**Correct Answer: ABC**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Explanation:

You can eliminate configurations with the word `standby', as that would be HSRP, not VRRP. Also, I think the options that put things like vrrp group 1 ip x.x.x.x are wrong.

You don't need the word `group' in the configuration line. The number 1 is the group number. Anyway, just take a good look at a few valid VRRP configuration examples so that you will be able to recognize invalid ones.

**QUESTION 454**

Which two secondary VLAN types of Private VLANs (PVLANS)? (Choose two)

- A. community
- B. isolated
- C. promiscuous
- D. host

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

Secondary VLANs provide Layer 2 isolation between ports within the same private VLAN domain.

There are two types of secondary VLANs:

- Isolated VLANs - Ports within an isolated VLAN cannot communicate with each other at the Layer 2 level.
- Community VLANs - Ports within a community VLAN can communicate with each other but cannot communicate with ports in other communities at the Layer 2 level

**QUESTION 455**

What types of SDM templates you can use in switch? (Choose all that apply.)

- A. Access
- B. Default
- C. Routing
- D. VLANs

**Correct Answer:** ABCD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

- Access - The access template maximizes system resources for access control lists (ACLs) to accommodate a large number of ACLs.
- Default - The default template gives balance to all functions.
- Routing - The routing template maximizes system resources for IPv4 unicast routing, typically required for a router or aggregator in the center of a network.
- VLANs - The VLAN template disables routing and supports the maximum number of unicast MAC addresses. It would typically be selected for a Layer 2 switch.

**QUESTION 456**

What is the process to configure EtherChannel?

- A. shutdown both interface ports
- B. shutdown the interface on one side only

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 457**

What is the default spanning tree port priority?

- A. 128
- B. 129
- C. 1
- D. 64

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 458**

How do you configure Spanning-tree EtherChannel guard?

- A. (config)#spanning-tree etherchannel guard misconfig
- B. (config-if)#spanning-tree etherchannel guard misconfig
- C. (config)#spanning-tree etherchannel misconfig guard
- D. (config-if)#spanning-tree etherchannel misconfig guard

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 459**

DRAG DROP

Select and Place:

Select and Place:

|                      |                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------|
| bridge transit delay | Measure of the time between the receipt and transmission of a frame                                       |
| root bridge          | Measure of the time required for a frame to begin leaving the bridge after the CPU has decided to send it |
| transmit halt delay  | Measure of the time required for a port to be blocked after a blocking trigger                            |
| medium access delay  | Directs all traffic                                                                                       |

Correct Answer:

|  |                                                                                    |
|--|------------------------------------------------------------------------------------|
|  | Measure of the time between the receipt and transmission of a frame                |
|  | bridge transit delay                                                               |
|  | Measure of the time required for a frame to begin leaving the bridge after the CPU |
|  | medium access delay                                                                |
|  | Measure of the time required for a port to be blocked after a blocking trigger     |
|  | transmit halt delay                                                                |
|  | Directs all traffic                                                                |
|  | root bridge                                                                        |

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 460  
If EtherChannel guard is configured, how the interface status is (or looks like) if misconfigured?

A. errdisabled  
B. shutdown

Correct Answer: A  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 461  
Which option is the value of the Tag Protocol Identifier 802.1Q tagged frame?

- A. 0x0806
- B. 0x888E
- C. 0x0800
- D. 0x8100

Correct Answer: D  
Section: Mix Questions  
Explanation

Explanation/Reference:  
Explanation:  
16-bit field set to 0x8100 in order to identify the frame as 802.1q tagged frame.

QUESTION 462  
DRAG DROP  
Select and Place:

Select and Place:

|                       |                                                              |
|-----------------------|--------------------------------------------------------------|
| inventory management  | Advertises the Layer 2 and Layer 3 configuration of the port |
| LLDP-MED capabilities | Indicates whether the device supports specific features      |
| location              | Shares caller ELIN                                           |
| network policy        | Shares the endpoint hardware profile                         |

Correct Answer:

|  |                                                              |
|--|--------------------------------------------------------------|
|  | Advertises the Layer 2 and Layer 3 configuration of the port |
|  | network policy                                               |
|  | Indicates whether the device supports specific features      |
|  | LLDP-MED capabilities                                        |
|  | Shares caller ELIN                                           |
|  | location                                                     |
|  | Shares the endpoint hardware profile                         |
|  | inventory management                                         |

Section: Mix Questions  
Explanation

Explanation/Reference:

**QUESTION 463**

How do you configure loop guard?

- A. (config)#spanning-tree loop guard default
- B. (config-if)#spanning-tree loop
- C. (config)#spanning-tree loop-guard default
- D. (config-if)#spanning-tree guard loop

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 464**

A dynamic access port is member of which VLAN by default?

- A. VLAN 1 is the default VLAN
- B. Same as the native VLAN
- C. none until the port VLAN is determined
- D. VLAN 4096

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 465**

What will be behavior of an access port when a tagged packet is received with a VLAN ID of an access port?

- A. Not Available
- B. tag is removed and packet is forwarded to the VLAN mentioned in the tag
- C. packet is dropped
- D. tag is removed and packet is forwarded on the VLAN of the access port

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 466**

What is an extension of HSRP that allows load sharing between two or more HSRP groups?

- A. MHSRP
- B. GLBP
- C. GHSRP
- D. Not Available

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 467**

Which of the following will cause a switch port to go into the errdisable state?

- A. configuration ports into EtherChannel
- B. storm control
- C. security violation
- D. Dynamic ARP inspection
- E. IGMP Snooping
- F. BPDUguard

**Correct Answer:** BCF

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 468**

Which switchport feature will block the packet with unknown MAC address from sending it via port?

- A. Switchport block unicast
- B. Packet with unknown MAC will be dropped
- C. Switchport portfast



D. Switchport protect

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 469**

What happens if a switch with dhcp snooping and ip source guard enabled globally, what does the switch do when it receives a packet with option 82?

- A. Drop
- B. Remove 82 and forward
- C. Proxy
- D. NA

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 470**

Which type of packet does DHCP snooping continuously check in a production network?

- A. DHCP Snooping
- B. DHCP Relay
- C. DHCP Request
- D. DHCP Acknowledge
- E. DHCP Reply
- F. DHCP Allow

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 471**

Which three functions does Dynamic ARP Inspection perform with invalid IP-to MAC address bindings? (Choose three.)

- A. deletes
- B. logs
- C. accepts
- D. intercepts
- E. discards
- F. bypasses

**Correct Answer:** BDE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 472**

Which three features can be optimized by using SDM templates? (Choose three.)

- A. port security
- B. trunk
- C. VLAN
- D. access
- E. DHCP snooping
- F. routing

**Correct Answer:** CDF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 473**

If all devices on an EtherChannel are sending traffic to a single MAC address, which two methods of load balancing on the EtherChannel are preferred? (Choose two.)

- A. destination-MAC
- B. src-dst-MAC
- C. destination-IP
- D. source-MAC
- E. source-IP

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 474**

Which command is used to verify trunk native VLANs?

- A. show access ports
- B. show interfaces trunk
- C. show trunk
- D. show vlan native trunk

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 475**

Which information does CDP supply from connected devices? (Choose three.)

- A. Hardware Platform
- B. Interface ID
- C. Hostname
- D. Config Register

**Correct Answer:** ABC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 476**

How to configure dynamic ARP inspection on a VLAN?

- A. (config)# ip arp inspection vlan
- B. (config-if)# ip arp inspection vlan
- C. (config)# arp inspection default
- D. (config-if)# inspection arp vlan

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 477**

What keyword in macro command is used to configure a root bridge and automatically adjust STP timers?

- A. root primary
- B. diameter
- C. reflector
- D. STP bridge root

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 478**

Your manager asked you to make every port on your switch bypass the normal spanning-tree timers which includes your uplink to other switches.

What two commands can you apply on the interfaces? (Choose two.)

- A. spanning-tree portfast
- B. spanning-tree portfast default
- C. spanning-tree portfast access
- D. spanning-tree portfast trunk

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 479**

Which IOS configuration command is required to configure a VLAN as a private VLAN?

- A. switch(config-vlan)# private-vlan common
- B. switch(config-vlan)# private-vlan private
- C. switch(config-vlan)# private-vlan primary
- D. switch(config-vlan)# private-vlan transparent

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

Private VLANs (PVLANS) are created using the following special VLAN configuration commands:

```
switch(config)# vlan vlan_id
switch(config-vlan)# private-vlan [primary | isolated | community]
switch(config-vlan)# private-vlan association secondary_vlan_list
```

There are three types of ports in a PVLAN: promiscuous, isolated, and community. A promiscuous port can send and receive frames with other promiscuous, isolated, or community ports assigned to the same private VLAN. The interface on the switch that is the default gateway for the segment should be a promiscuous port. Isolated ports are able to send frames to promiscuous ports, but not to each other. A community port can communicate with other community ports of the same private VLAN or with promiscuous ports.

Private VLANs are supported on switches that allow the configuration of primary and secondary VLANs. A primary VLAN carries the traffic between the promiscuous port and the isolated and community ports assigned to the same primary VLAN. There are two types of secondary VLANs: isolated and community. Isolated VLANs carry traffic from isolated ports to promiscuous ports. Community VLANs carry traffic between community ports and to the promiscuous port.

Ports are defined using the following special PVLAN configuration command:

```
switch(config-if)# switchport mode private-vlan [promiscuous | host]
```

The command used for isolated and community ports is as follows:

```
switch(config-if)# switchport mode private-vlan host-association primary_vlan_id secondary_vlan_id
```

The following command syntax is used to configure a promiscuous port's primary and secondary VLANs:

```
switch(config-if)# private-vlan mapping primary_vlan_id secondary_vlan_id
```

Objective:

Infrastructure Security

Sub-Objective:

Configure and verify switch security features

References:

Cisco > Home > Support > Product Support > End-of-Sale and End-of-Life Products > Cisco Catalyst 6000 Series Switches > Configure > Configuration Examples and Technotes > Securing Networks with Private VLANs and VLAN Access Control Lists

#### QUESTION 480

Regarding high availability, with the MAC address 0000.0c07.ac03, what does the "03" represent?

- A. The GLBP group number
- B. The type of encapsulation
- C. The HSRP router number
- D. The VRRP group number
- E. The HSRP group number
- F. The active router number

**Correct Answer:** E

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 481

HSRP has been configured between two Company devices. Which of the following describe reasons for deploying HSRP? (Choose three)

- A. HSRP provides redundancy and fault tolerance
- B. HSRP allows one router to automatically assume the function of the second router if the second router fails
- C. HSRP allows one router to automatically assume the function of the second router if the second router starts
- D. HSRP provides redundancy and load balancing

**Correct Answer:** ABD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 482

Refer to the exhibit. Which configuration on the HSRP neighboring device ensures that it becomes the active HSRP device in the event that port fa1/1 on Switch\_A goes down?

- A. Switch\_B(config-if)#ip address 10.10.10.2  
255.255.255.0 Switch\_B(config-if)#standby 1 priority  
200 Switch\_B(config-if)#standby 1 preempt  
Switch\_B(config-if)#standby 1 ip 10.10.10.10  
Switch\_B(config-if)#standby 1 track interface fa 1/1
- B. Switch\_B(config-if)#ip address 10.10.10.2  
255.255.255.0 Switch\_B(config-if)#standby 1 priority  
200 Switch\_B(config-if)#standby 1 ip 10.10.10.10
- C. Switch\_B(config-if)#ip address 10.10.10.2  
255.255.255.0 Switch\_B(config-if)#standby 1 priority  
195 Switch\_B(config-if)#standby 1 preempt  
Switch\_B(config-if)#standby 1 ip 10.10.10.10
- D. Switch\_B(config-if)#ip address 10.10.10.2  
255.255.255.0 Switch\_B(config-if)#standby 1 priority  
190 Switch\_B(config-if)#standby 1 ip 10.10.10.10  
Switch\_B(config-if)#standby 1 track interface fa 1/1

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 483

What are three possible router states of HSRP routers on a LAN? (Choose three)

- A. Standby
- B. Established
- C. Active
- D. Idle
- E. Backup
- F. Init

**Correct Answer:** ACF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 484

HSRP was implemented and configured on two switches while scheduled network maintenance was performed.

After the two switches have finished rebooting, you notice via show commands that Switch2 is the HSRP active router. Which two items are most likely the cause of Switch1 not becoming the active router? (Choose two)

- A. booting delays
- B. standby group number does not match VLAN number
- C. IP addressing is incorrect
- D. preemption is disabled
- E. incorrect standby timers
- F. IP redirect is disabled

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 485

Which protocol specified by RFC 2281 provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first-hop failures in network edge devices or access circuits?

- A. ICMP
- B. IRDP
- C. HSRP
- D. STP

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 486

What statement about MAC address table is true?

- A. Every entry in MAC address table has VLAN assigned
- B. Extended VLANs doesn't have VLAN assigned in MAC address table.
- C. Private VLANs doesn't have to be assigned in MAC address table.
- D. Static bindings can't be removed from MAC address table.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 487**

What is the default mode for LACP EtherChannel when configured?

- A. On
- B. Active
- C. Passive
- D. Desirable
- E. Off

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 488**

Which layer private VLAN partition the broadcast domain?

- A. Layer 1
- B. Layer 2
- C. Layer 3
- D. Layer 4

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 489**

What statements about STP path cost are true? (Choose two.)

- A. Long path cost is 64 bits
- B. Short path cost is 32 bits
- C. MST uses long path cost
- D. Default path cost is short
- E. They have equal path cost by default

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 490**

In a Virtual Switching System, DSW1 and DSW2 need to communicate with each other to determine the role. Which technology is it using?

- A. STP
- B. NA
- C. VSL Protocol (Virtual Switch Link)
- D. LACP

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 491**

Which two statements about frame LLDP is true? (Choose two.)

- A. Frame has destination multicast address
- B. NA
- C. Frame has CRC

**Correct Answer:** AC  
**Section:** Mix Questions  
**Explanation**



**Explanation/Reference:**

**QUESTION 492**

Which statement about frame SPAN is true?

- A. Destination and source port SPAN works on L2 (Layer 2).
- B. Source ports SPAN work on L2 (Layer 2).
- C. Destination ports SPAN work on L2 (Layer 2).
- D. Destination and source port SPAN don't work on L2.

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 493**

Which two commands is used to remove VLAN 55 from the trunk port? (Choose two.)

- A. switchport trunk allowed vlan add 3, remove 55
- B. switchport trunk allowed vlan remove 55
- C. switchport trunk allowed vlan except 55

**Correct Answer: BC**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 494**

Which two operational attributes can be checked for EtherChannel ports that are in err-disabled state? (Choose two.)

- A. Port mode
- B. Port cost
- C. Duplex
- D. DTP
- E. VLAN

**Correct Answer: CE**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Explanation:

See "compatibility requirements"

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>

**QUESTION 495**

What statement is true about PVST?

- A. PVST+ is the default STP mode on Cisco switches
- B. Rapid PVST+ is the default STP mode on Cisco switches
- C. Is the default mode on Cisco switches
- D. STP is the default mode on Cisco switches

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 496**

What is the value of the TPID/tag protocol identifier in dot1q?

- A. 0x8100
- B. 0x8a88
- C. 0x8b45
- D. 0x8200

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 497**

What is the value of the TPID/tag protocol identifier of QinQ?

- A. 0x8a88

- B. 0x8100
- C. 0x8b45
- D. 0x8200

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 498**  
Which two configurations cause the frames to be tagged? (Choose two.)

- A. interface gi 0/1.116 encapsulation dot1q
- B. trunk allowed vlan 116
- C. interface with access and voice VLAN configured to 116
- D. interface encapsulation native vlan
- E. switchport mode on

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

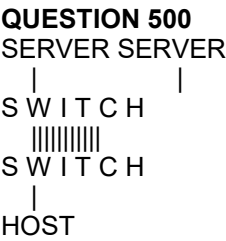
**Explanation/Reference:**

**QUESTION 499**  
What VSS technology allows you to share downstream resources?

- A. LACP
- B. PAgP
- C. MEC
- D. EOA

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**



Which EtherChannel load balancing algorithm should be used to optimize the EtherChannel links between switches?

- A. Source MAC
- B. Source-dest MAC
- C. Destination IP
- D. Destination MAC

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 501**  
Where should the Root Guard be implemented in the network topology that Cisco recommends? (Choose two.)

- A. All non-root ports of the Access Switches.
- B. Downstream links from Distribution to Access Switches
- C. Access Switches to uplink ports to Distribution Switches
- D. On Layer 3 Switches.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 502**  
A Cisco switch was configured using the “switchport trunk allowed vlan 1,80,99-250” command.

Which two commands will remove VLAN 100 from the allowed VLAN list? (Choose two.)

- A. switchport trunk allowed vlan remove vlan 100

- B. switchport trunk allowed vlan 1-80,99,101-250
- C. switchport trunk allowed vlan except vlan 100

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:  
A & B are right  
1- after applying the question command:switchport trunk allowed vlan 1,80,99-250  
Switch(config)#do show int trunk  
Port Mode Encapsulation Status Native vlan  
Fa0/1 on 802.1q trunking 1  
Port Vlans allowed on trunk  
Fa0/1 1,80,99-250  
Port Vlans allowed and active in management domain Fa0/1 1  
Port Vlans in spanning tree forwarding state and not pruned Fa0/1 1  
now after applying "except 100": Switch(config-if)#switchport trunk allowed vlan except 100 Switch(config-if)#do show int trunk  
Port Mode Encapsulation Status Native vlan  
Fa0/1 on 802.1q trunking 1  
Port Vlans allowed on trunk  
Fa0/1 1-99,101-1005  
Port Vlans allowed and active in management domain Fa0/1 1  
Port Vlans in spanning tree forwarding state and not pruned Fa0/1 none  
You can see that except 100, allowed all vlans except 100, which is against what is required in the question.

**QUESTION 503**  
What is the benefit of UDLD?

- A. provides backup for fiber
- B. help in preventing loops
- C. removes loops
- D. determines switch path

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 504**  
Behavior of an access port when a tagged packet is received other than the access VLAN value.

- A. Tag is removed and packet is forwarded of the VLAN mentioned in the tag.
- B. tag is removed and packet is forwarded on the VLAN of the access port
- C. Not Available
- D. packet is dropped

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 505**  
Which option is the maximum frame size for an 802.1Q frame?

- A. 64 bytes
- B. 68 bytes
- C. 1518 bytes
- D. 1522 bytes

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 506**  
Which option is the minimum frame size of an 802.1Q frame?

- A. 64 bytes
- B. 68 bytes
- C. 1518 bytes
- D. 1522 bytes

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 507**

What SPAN configuration is required to enable on a switch?

- A. A monitor VLAN is created for the SPAN traffic.
- B. Configure a source and destination port
- C. Disable VTP pruning on trunk links
- D. LLDP must be enabled in an interface.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 508**

Which two actions can be configured for storm control violation? (Choose two.)

- A. Shutdown
- B. Trap
- C. Notify admin
- D. Discard Port

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 509**

Which statements about RSPAN are true? (Choose two.)

- A. It supports MAC address learning.
- B. RSPAN VLANS can carry RSPAN traffic only.
- C. only one RSPAN VLAN can be configured per device.
- D. RSPAN VLANs are exempt from VTP pruning.
- E. MAC address learning is not supported
- F. RSPAN uses GRE tunnel to transmit captured traffic.

**Correct Answer:** BE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. It has these special characteristics:

All traffic in the RSPAN VLAN is always flooded.

No MAC address learning occurs on the RSPAN VLAN.

RSPAN VLAN traffic only flows on trunk ports.

RSPAN VLANs must be configured in VLAN configuration mode by using the remote-span VLAN configuration mode command.

STP can run on RSPAN VLAN trunks but not on SPAN destination ports.

An RSPAN VLAN cannot be a private-VLAN primary or secondary VLAN.

For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristic are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate switches. It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

Reference:

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_40\\_se/configuration/guide/scg/swspan.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swspan.pdf)

**QUESTION 510**

When a private VLAN is configured, which mode must be configured as a router facing port?

- A. isolated
- B. promiscuous
- C. community
- D. host

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 511**

When a switch is added to a stack, which switch automatically configures the new switch with the correct IOS?

- A. master
- B. peer
- C. adjacent
- D. slave

**Correct Answer:** A

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 512**

Which HSRP extension allows groups to share traffic loads?

- A. GLBP
- B. CHSRP
- C. MHSRP
- D. CGMP
- E. FHRP

**Correct Answer: C**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 513**

A network engineer is considering implementing UDLD throughout the network. Which option must the network engineer consider?

- A. UDLD aggressively disables the port after eight failed retries to connect to neighbor.
- B. UDLD works at layer 1 of the OSI model.
- C. UDLD is an IEEE standard that can be configured on non-cisco devices.
- D. UDLD is already enabled by default on all ports on cisco switches.

**Correct Answer: A**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 514**

Which mechanism is specific for RSPAN and not for SPAN?

- A. source port
- B. monitor port
- C. reflector port
- D. redundant port
- E. destination port

**Correct Answer: C**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 515**

Which three pieces of information about the remote device are reported by Cisco Discovery Protocol? (Choose three.)

- A. the routing protocols in use on the device
- B. its spanning-tree state
- C. its hostname
- D. its port number
- E. its configuration register value
- F. its hardware platform

**Correct Answer: CDF**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 516**

Where can netflow export data for long term storage and analysis?

- A. another network device
- B. flat file
- C. syslog
- D. collector

**Correct Answer: D**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 517**



Which two types of threshold can you configure for tracking objects? (Choose two.)

- A. weight
- B. bandwidth
- C. MTU
- D. percentage
- E. administrative distance15
- F. delay

**Correct Answer:** AD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 518

What do subordinate switches in a switch stack keep?

- A. Subordinate switches keep their own spanning trees for each VLAN that they support.
- B. Subordinate switches keep entire VLAN database
- C. Store running config all the switches
- D. Subordinate switches does not keep their own spanning trees

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 519

802.1Q trunking, what does it do? (Choose two.)

- A. Encapsulate frame with VLAN tag
- B. Makes the frame size 1596
- C. Adds 32-bit header
- D. Allows 8-bits in VLAN tag header

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 520

What are the possible results of port-security?

- A. error disable (shut down)
- B. send a trap
- C. port disabled
- D. loop inconsistent

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 521

Which two statements about SDM templates are true? (Choose two.)

- A. They are used to allocate system resources
- B. Changing the SDM template will not disturb switch operation.
- C. You can verify the SDM template that is in use with the show sdm prefer command
- D. SDM templates are defined by the switch model and can't be changed
- E. SDM templates changes don't require switch to be rebooted

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 522

Which two statements apply to LLDP? (Choose two.)

- A. It runs on the data link layer
- B. It runs on the network layer
- C. It is not enabled by default on Cisco devices
- D. Enabled on Cisco devices by default
- E. Hold-time is 100 seconds on Cisco devices

**Correct Answer:** AC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 523**

Which two statements apply to topology-based switching? (Choose two.)

- A. It is functionally equivalent to Cisco Express Forwarding
- B. It is the preferred switching mode in Cisco multilayer switches
- C. It uses Loop free protocol for switching
- D. disabled by default
- E. Multi-vendor Protocol

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 524**

In which two ways are IEEE STP BPDUs forwarded if VLAN 99 is configured as native? (Choose two)

- A. VLAN 1 STP BPDUs are sent tagged on VLAN 1
- B. VLAN 1 STP BPDUs are sent tagged on VLAN 99
- C. VLAN 1 and VLAN 99 BPDUs are sent tagged on VLAN 1
- D. VLAN 1 STP BPDUs are sent untagged on VLAN 1
- E. VLAN 1 STP BPDUs are sent untagged on VLAN 99

**Correct Answer:** AE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 525**

A workstation technician moves a PC from one office desk to another. Before the move the PC has network connectivity After the move as the PC plugged into the now network port, it loses network connectivity and the network switch port becomes err disabled.

Which option can cause the issue?

- A. wrong VLAN
- B. wrong switch port mode
- C. port security
- D. speed issue

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 526**

Which feature do you implement so that an interface enters the root inconsistent state if it receives a superior BPDU?

- A. BPDU filter
- B. root guard
- C. BPDU guard
- D. loop guard

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 527**

Which two statements about 802.1q are true? (Choose two.)

- A. It encapsulates the original Ethernet frame and adds a VLAN identifier.
- B. It increases the maximum size an Ethernet frame to 1594 bytes.
- C. It is a Cisco proprietary protocol.
- D. When It is enabled, it forces a recalculation of the frame check sequence field.
- E. It supports 8-byte VLAN identifiers.
- F. It adds a 32-bit field to the Ethernet frame between the source MAC address and length fields.

**Correct Answer:** DF  
**Section:** Mix Questions  
**Explanation**

Explanation/Reference:

QUESTION 528

Which two statements about CDP are true? (Choose two.)

- A. CDP uses a TLV to advertise the native VLAN
- B. CDP is not supported with SNMP
- C. CDP is supported on Frame Relay sub interfaces.
- D. CDP runs on OSI layer 2
- E. CDP runs on OSI layer 1

Correct Answer: AD  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 529

Which two combinations of Ether Channel modes support the formation of an EtherChannel? (Choose two.)

- A. desirable, passive
- B. desirable, desirable
- C. active, passive
- D. passive, passive
- E. active, desirable

Correct Answer: BC  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 530

DRAG DROP

Select and Place:

Select and Place:

Maps VLANs to instances

Based on IEEE 802.1w

Default STP mode

Based on IEEE 802.1D

Based on IEEE 802.1s

Discarding port state

PVST

RapidPVST

MST

Correct Answer:

PVST

Based on IEEE 802.1D

Default STP mode

RapidPVST

Based on IEEE 802.1w

Discarding port state

MST

Based on IEEE 802.1s

Maps VLANs to instances

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 531  
DRAG DROP

Select and Place:

Select and Place:

Time when BPDU expires

10 seconds

New BPDU

20 seconds

Listening or learning

15 seconds

Hello

Forward

Hold

Correct Answer:

Hello

10 seconds

New BPDU

Forward

15 seconds

Listening or learning

Hold

20 seconds

Time when BPDU expires

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 532  
DRAG DROP

Select and Place:

Select and Place:

Multiple of 4096

8 default is being the interface value

Lower the better

Multiple of 16

Range 1-200k (200,000)

Default value is 128

Port Cost

Switch Port Priority

Switch Priority

Correct Answer:



Port Cost

8 default is being the interface value

Range 1-200k (200,000)

Switch Port Priority

Default value is 128

Multiple of 16

Switch Priority

Lower the better

Multiple of 4096

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 533  
DRAG DROP

Select and Place:

Select and Place:

Port self recovery

Protect designated port from receiving superior BPDU

A better BPDU disables the port as err-disabled

Detecting unidirectional switching links

Guard Root

Guard Loop

Correct Answer:

Guard Root

A better BPDU disables the port as err-disabled

Protect designated port from receiving superior BPDU

Guard Loop

Detecting unidirectional switching links

Port self recovery

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 534  
DRAG DROP

Select and Place:

Select and Place:

Directs all traffic. (Keyword – Directs all traffic)

This value is the time that is necessary in order to effectively block a port. (Keyword – halt delay, block port)

This value is the time that elapsed between the reception and the transmission of the same frame by the bridge. (Keyword – receipt and transmission)

Time between the CPU decision to send a frame and the moment when the frame effectively begins to leave the bridge. (Keyword – CPU decision)

Medium Access Delay

Bridge Transit Delay

Maximum Transmission Halt Delay

Root Bridge

Correct Answer:

Medium Access Delay

Time between the CPU decision to send a frame and the moment when the frame effectively begins to leave the bridge. (Keyword – CPU decision)

Bridge Transit Delay

This value is the time that elapsed between the reception and the transmission of the same frame by the bridge. (Keyword – receipt and transmission)

Maximum Transmission Halt Delay

This value is the time that is necessary in order to effectively block a port. (Keyword – halt delay, block port)

Root Bridge

Directs all traffic. (Keyword – Directs all traffic)

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 535  
DRAG DROP

Select and Place:

Select and Place:

Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision. (Keyword – hardware information)

Provides location information from the switch to the endpoint device. (ELIN location) (Keyword – ELIN Location)

Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and what capabilities the device has enabled. (Keywords – capabilities/supported feature)

Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. (Keyword – L2 and L3)

LLDP-MED

Network Policy TLV

Inventory Management TLV

Location

Correct Answer:

#### LLDP-MED

Allows LLDP-MED endpoints to determine the capabilities that the connected device supports and what capabilities the device has enabled. (Keywords – capabilities/supported feature)

#### Network Policy TLV

Allows both network connectivity devices and endpoints to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. (Keyword – L2 and L3)

#### Inventory Management TLV

Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision. (Keyword – hardware information)

#### Location

Provides location information from the switch to the endpoint device. (ELIN location) (Keyword – ELIN Location)

#### Section: Mix Questions

##### Explanation

##### Explanation/Reference:

#### QUESTION 536

Which two commands sequences must you enter on a pair switches so that they negotiate? (Choose two.)

- A. channel-protocol lacp  
channel-group 1 mode auto
- B. channel-protocol lacp  
channel-group 1 mode passive
- C. channel-protocol pagp  
channel-group 1 mode on
- D. channel-protocol pagp  
channel-group 1 mode auto
- E. channel-protocol lacp  
channel-group 1 mode active

**Correct Answer:** BE

#### Section: Mix Questions

##### Explanation

##### Explanation/Reference:

#### QUESTION 537

Which Statement about the default SWITCH Database Management Template is true?

- A. The default template maximizes system resources for unicast routing
- B. The default template disables and supports the maximum number of unicast MAC addresses
- C. The default template gives balance to all functions
- D. The default template maximizes system resources for access control lists

**Correct Answer:** C

#### Section: Mix Questions

##### Explanation

##### Explanation/Reference:

#### QUESTION 538

Which results happens when a non-trunking port that is configured with BPDU guard is connected to a device that is transmitting?

- A. The port is moved into the spanning-tree blocking state.
- B. The port is error-disabled.
- C. A routing loop can occur on the network.
- D. The port transitions to the connected state.

**Correct Answer:** B

#### Section: Mix Questions

##### Explanation

##### Explanation/Reference:



**QUESTION 539**

Refer to the exhibit. Which two statements can be derived from the output of the show standby command? (Choose two.)

```
R2#show standby
FastEthernet1/0 – Group 40
State is Standby
  4 state changes, last state change 00:01:51
Virtual IP address is 10.10.1.1
Active virtual MAC address is 0000.0c07.ac28 (MAC Not In Use)
  Local virtual MAC address is 0000.0c07.ac28 (v1 default)
Hello time 3 sec, hold time 10 sec
  Next hello sent in 1.856 secs
Preemption disabled
Active router is 10.10.1.3, priority 85 (expires in 8.672 sec)
Standby router is local
Priority 90 (configured 90)
  Track interface FastEthernet0/0 state Up decrement 10
Group name is "hsrp-Fa1/-40" (default)
```

- A. R2 Fa1/0 regains mastership when the link comes back up
- B. Router with IP 10.10.1.3 is active because it has a higher IP address
- C. If Fa0/0 is shut down, the HSRP priority on R2 becomes 80
- D. R2 is using the default HSRP hello and hold timers
- E. R2 becomes the active router after the hold time expires

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 540**

Which two settings are the parts of a Default LLDP configuration? (Choose two.)

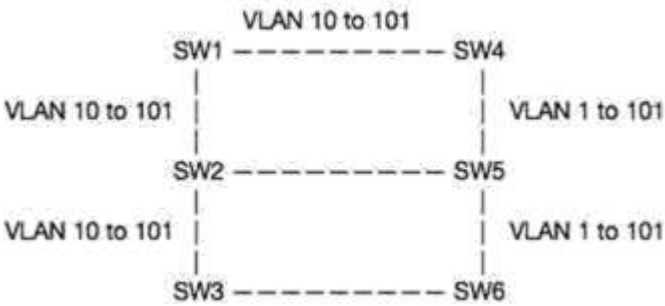
- A. The LLDP hold time is 60 seconds.
- B. The LLDP global state is Disabled.
- C. The LLDP reinitialization delay is 5 seconds.
- D. The LLDP interface state is Enabled.
- E. The LLDP timer is 60 seconds.

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 541**

Refer to the exhibit. If switch SW6 is operating VTP Server and the other devices have the same configuration as SW4, which statement about the VLANs network is true?



```
SW4# show run | include vtp
vtp mode client
vtp domain cisco
vtp domain ciscotest
vtp pruning
vtp version 3
```

- A. Traffic on VLANs 1 through 9 is flooded to all switches in the network.
- B. VLANs 1 through 101 are operational on all switch trunks.
- C. VLANs 1 through 9 are pruned on the link between SW1 and SW4.
- D. VLANs 1 through 101 are pruned on the link between SW1 and SW2.



**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 542**

Which option is a CISCO recommended RSPAN configuration practice?

- A. Define an RSPAN VLAN before configuring an RSPAN source and destination session.
- B. Assign access ports to an RSPAN VLAN like any other campus VLAN.
- C. Use a different RSPAN VLAN for each session if configuring RSPAN on multiple switches.
- D. Use only one destination port for each RSPAN session.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**  
Explanation:

Reference:

[http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod\\_white\\_paper0900aecd805457cc.html](http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-series-switches/prod_white_paper0900aecd805457cc.html)

**QUESTION 543**

Which two pieces of information are carried in a Cisco Discovery Protocol advertisement? (Choose two.)

- A. Processor Type
- B. VTP domain name
- C. Routing protocol
- D. Memory usage
- E. Spanning-Tree mode
- F. Native VLAN-ID

**Correct Answer:** BF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 544**

Which Cisco StackWise feature is supported?

- A. using different SDM templates on each switch
- B. using different versions of the Cisco IOS on each switch
- C. using mixed software feature set on all members
- D. using same software feature set on all members

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 545**

Which statement about the VTP v2 is true?

- A. IT supports the use of multiple instances.
- B. IT propagates VLANs 1 - 1005 only.
- C. IT can be enabled on a per-port basis.
- D. IT performs consistency checks only when a new VLAN is added
- E. IT can be enabled on a per-interface basis

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 546**

Which options of VLANs IDs are in extended range? (Choose three.)

- A. 1006
- B. 1001
- C. 999
- D. 4021
- E. 3003
- F. 99

**Correct Answer:** ADE  
**Section:** Mix Questions

**Explanation****Explanation/Reference:****QUESTION 547**

Which two differences between RADIUS and TACACS+ are true? (Choose two.)

- A. Only TACACS+ uses user privilege levels to determine which commands the user can execute.
- B. Only RADIUS provides granular control over the CLI commands that a user can execute.
- C. Only RADIUS uses UDP.
- D. Only TACACS+ uses UDP.
- E. Only TACACS+ can combine authentication and authorization functions.

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation****Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

**QUESTION 548**

What are possible Etherchannel load balancing mechanism based on layer 3? (Choose two.)

- A. Mac source
- B. Mac source-destination
- C. IP Source
- D. IP Source-destination
- E. Mac destination

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation****Explanation/Reference:****QUESTION 549**

Which of the following are true regarding TACACS+ ? (Choose three.)

- A. Supports backwards compatible with TACACS
- B. Encrypts the header
- C. Encrypts the whole payload
- D. Utilizes TCP port 49
- E. Utilizes UDP port 49
- F. Separates Authentication & Authorization

**Correct Answer:** CDE

**Section:** Mix Questions

**Explanation****Explanation/Reference:****QUESTION 550**

Which two statements about MST are true? (Choose two.)

- A. it can operate without a root bridge
- B. it supports one STP instance per VLAN
- C. it is vendor neutral
- D. all vlans must reside in a single MST region
- E. it can map multiple vlans to a single STP instance

**Correct Answer:** CE

**Section:** Mix Questions

**Explanation****Explanation/Reference:****QUESTION 551**

Which two statements about HSRP are true? (Choose two.)

- A. You must manually configure ICMP redirect messages on HSRP interfaces
- B. It is supported on switch virtual interfaces and routed ports
- C. Primary and secondary HSRP switches forward traffic in a round-robin style
- D. The interfaces in a HSRP group share a virtual MAC address
- E. An HSRP group can support a maximum of eight switches.

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation****Explanation/Reference:**

**QUESTION 552**

Which vtp2 mode does the switch operate without participating in vtp?

- A. Client
- B. Server
- C. Transparent
- D. Off

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 553**

Which two features can you configure on an access port? (Choose two)

- A. QinQ
- B. portfast
- C. voice VLAN
- D. STP mode
- E. 802.1q

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 554**

What is true about CDP? (Choose two.)

- A. disabled when native vlan mismatched
- B. can be disable on interface only
- C. send periodic broadcast
- D. send periodic multicast

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 555**

DRAG DROP

Match the steps needed to configure RSPAN in the proper order.

**Select and Place:**

|                                                                         |        |
|-------------------------------------------------------------------------|--------|
| Associate an RSPAN source session number with the RSPAN VLAN            | Step 1 |
| Associate an RSPAN destination session number with the RSPAN VLAN       | Step 2 |
| Associate an RSPAN source session number with source ports or VLANs     | Step 3 |
| Configure a VLAN as an RSPAN VLAN                                       | Step 4 |
| Associate an RSPAN destination session number with the destination port | Step 5 |

**Correct Answer:**

|  |                                                                         |
|--|-------------------------------------------------------------------------|
|  | Configure a VLAN as an RSPAN VLAN                                       |
|  | Associate an RSPAN source session number with source ports or VLANs     |
|  | Associate an RSPAN source session number with the RSPAN VLAN            |
|  | Associate an RSPAN destination session number with the destination port |
|  | Associate an RSPAN destination session number with the RSPAN VLAN       |

Section: Mix Questions  
Explanation

Explanation/Reference:

**QUESTION 556**  
DRAG DROP

Match the features on the left to the correct VRRP version on the right.

Select and Place:

|                                                    |                                                                                          |
|----------------------------------------------------|------------------------------------------------------------------------------------------|
| Same priority but high IP cause preemption         | <b>VRRPv2</b><br><div></div> <div></div> <div></div> <div></div> <div></div> <div></div> |
| Only high priority cause preemption                |                                                                                          |
| Timers in seconds                                  |                                                                                          |
| Support IPv4 and IPv6                              |                                                                                          |
| VRRP need to be enabled globally                   |                                                                                          |
| Multicast: 224.0.0.18                              |                                                                                          |
| Support IPv4 only                                  | <b>VRRPv3</b><br><div></div> <div></div> <div></div> <div></div> <div></div>             |
| Multicast: 224.0.0.18 for IPv4 (FF02::12 for IPv6) |                                                                                          |
| RID MAC: 0000.5E00.01xx                            |                                                                                          |
| Timers in milliseconds                             |                                                                                          |
| VRRP enable per interface                          |                                                                                          |

Correct Answer:

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

VRRPv2

Multicast: 224.0.0.18

RID MAC: 0000.5E00.01xx

Same priotity but high IP cause preemption

Support IPv4 only

Timers in seconds

VRRP enable per interface

VRRPv3

Multicast: 224.0.0.18 for IPv4 (FF02::12 for IPv6)

Only high priority cause preemption

Support IPv4 and IPv6

Timers in milliseconds

VRRP need to be enabled globally

Section: Mix Questions  
 Explanation

Explanation/Reference:

QUESTION 557  
 DRAG DROP

Select and Place:

Select and Place:

Initializing

Progressing

Provisioned

Ready

Waiting

Ports have been assigned in the running configuration of the stacks

The stack master has successfully installed a configuration on device

The stack master is actively performed discovery

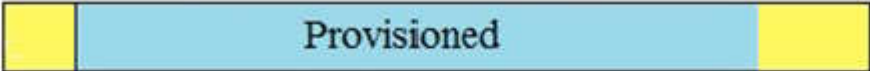
The stack master is communicating with a new switch

The switch is operational

Correct Answer:



Ports have been assigned in the running configuration of the stacks



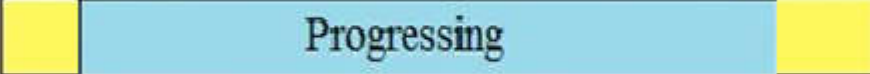
The stack master has successfully installed a configuration on device



The stack master is actively performed discovery



The stack master is communicating with a new switch



The switch is operational



Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 558  
DRAG DROP

Select and Place:

Select and Place:

- monitor session 1 destination remote vlan
- Create VLAN for RSPAN session (destination)
- Create VLAN for RSPAN session (source)
- monitor session 1 destination (interface or vlan)
- monitor session 1 source remote vlan
- monitor session 1 source (interface or vlan)  
direction rx or tx or both

Source Switch

Destination Switch

Correct Answer:

Source Switch

Create VLAN for RSPAN session (destination)

monitor session 1 source (interface or vlan)  
direction rx or tx or both

monitor session 1 source remote vlan

Destination Switch

Create VLAN for RSPAN session (source)

monitor session 1 destination (interface or vlan)

monitor session 1 destination remote vlan

Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 559

Which of these options supports to maintain the network architecture and stability of the root bridge in a spanning-tree service?

- A. BPDU Filter
- B. BPDU Guard
- C. Root Guard
- D. Loop Guard

Correct Answer: C

Section: Mix Questions  
Explanation

Explanation/Reference:

Explanation:

BPDU Guard puts a portfast port in err-disabled in case of receiving a BPDU. But root guard is a feature specially designed in order to enforce the root bridge placement in the network forcing an interface to become a designated port to prevent surrounding switches from becoming a root switch.

#### QUESTION 560

Which STP feature used to monitor BPDU traffic and enable STP to transition between states?

- A. Root Guard
- B. Loop Guard
- C. BPDU Filter
- D. BPDU Guard

Correct Answer: C

Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 561

Which of the following are valid methods of VRRP authentication? (Choose three.)

- A. SHA-124
- B. SHA-254
- C. No authentication
- D. WAP
- E. Plain text authentication
- F. MD5

Correct Answer: CEF

Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 562

Storm control options apart from the default one. (Choose two.)

- A. log
- B. shutdown
- C. trap
- D. err-disable
- E. let admin know

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 563

Which two statements about GLBP are true? (Choose two.)

- A. Can have 128 AVFs on an interface
- B. Maximum 4 AVFs allowed in a group
- C. Can work with dual active AVGs
- D. Can have 6 AVFs in a group
- E. GLBP supports up to 1024 virtual routers per group.

**Correct Answer:** BE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 564

Which of these two options are true about RADIUS? (Choose two.)

- A. Uses TCP port 49
- B. Uses client server model
- C. Uses UDP to exchange traffic
- D. Support for multiple protocols
- E. Is compatible with TACACS+

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 565

Which of the following are true regarding TACACS+. ? (Choose two.)

- A. Backward compatible with TACACS.
- B. More secure then RADIUS as it uses UDP.
- C. Has support for multiple protocols other than IP.
- D. Separates authentication and authorization.
- E. Encrypts just the header.

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 566

Refer to the exhibit. You can change the SDM template to maximize the number of supported MAC addresses. You noticed that the switch routing performance has been significantly degraded. Which action do you take to correct the problem?

```
*****START EXHIBIT*****
#show sdm prefer
The current template is the selected template optimizes the resources on the
switch to support this level of features for a routed interface and 1024.

number of unicast MAC addresses
number of igmp groups
number of multicast routes 0
number of unicast routes 0
number of policy based routing access
number of qos access 512
number of security access
*****END EXHIBIT*****
```

- A. Configure sdm prefer vlan
- B. Configure sdm prefer routing
- C. Execute clear ip route command to reset the routing table.
- D. Configure sdm prefer default

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 567**

Which three characteristics of AAA with RADIUS are true? (Choose three.)

- A. It uses a client-server architecture.
- B. It uses standards-based implemented.
- C. It runs on UDP port 1812.
- D. It is a Cisco proprietary implementation.
- E. It runs on TCP port 49.
- F. It uses a client-private cloud architecture.

**Correct Answer:** ABC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 568**

Which two statements about an access port with voice VLAN are true? (Choose two.)

- A. They support a single VLAN for data traffic.
- B. They require VTP.
- C. Frame on the voice VLAN are tagged with a Layer 2 CoS value.
- D. They can be configured on VLANs 1 through 1001 only.
- E. They can be configured on trunk ports and access ports.

**Correct Answer:** AC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 569**

Why the network administration can want to disable MAC address learning on the router?

- A. To free up space in MAC address table.
- B. To use space in MAC address table
- C. To wipe space in MAC address table.
- D. There was a security violation.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 570**

Where can you disable MAC address learning on the switch?

- A. On the VLAN or interface.
- B. Per switch port.
- C. A VLAN filter template is necessary.
- D. With the global command mac-address disable

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 571**

Which three advantages of TACACS+ are true? (Choose three.)

- A. It integrates authentication and authorization
- B. It controls access to network devices
- C. It controls access to endpoint devices
- D. It encrypted the passwords
- E. It encrypted the whole transition
- F. It separates authentication and authorization

**Correct Answer:** BEF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 572**

Which two restrictions of the port security feature are true? (Choose two.)

- A. trunk ports
- B. SPAN ports
- C. tunnel ports
- D. EtherChannel
- E. private VLANs

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 573**

Which of the following commands are valid to configure DHCP snooping with Dynamic ARP Inspection for a VLAN? (Choose four.)

- A. (config)# ip dhcp snooping vlan arp trust
- B. (config)# ip dhcp snooping
- C. (config)# ip dhcp snooping vlan 10
- D. (config)# ip arp inspection vlan 10
- E. (config)# interface ethernet 0/0 (config-if)# ip dhcp snooping trust (config-if)# ip arp inspection trust
- F. (config)# interface ethernet 0/0 (config-if)# ip dhcp arp inspect-snoop trust

**Correct Answer:** BCDE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 574**

Which two statements about extended-range VLANs are true? (Choose two.)

- A. Created in VTP server mode in VTP version 3.
- B. Created when switch is in VTP server mode.
- C. They support pruning.
- D. VTP version 3 stores extended-range VLAN in VLAN database.
- E. VTP version 1 and 2 stores extended-range VLAN in VLAN database.

**Correct Answer:** AD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 575**

How many VLANs can be assigned to a user access port configured for VoIP?

- A. 1
- B. 2
- C. 3
- D. unlimited

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 576**

Which three authentication methods does VRRP use? (Choose three.)

- A. 802.1x authentication
- B. Cipher authentication
- C. SHA-256 authentication
- D. No authentication
- E. Plain text authentication
- F. MD5 authentication

**Correct Answer:** DEF



**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 577**

Which three authentication methods does GLBP use? (Choose three.)

- A. Single Sign On authentication
- B. MD5 authentication
- C. No authentication
- D. Plain text authentication
- E. DCSP authentication
- F. 6-to-4 authentication

**Correct Answer:** BCD  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 578**

Which two authentication methods does HSRP use? (Choose two.)

- A. WPA2 authentication
- B. SHA-128 authentication
- C. MD5 authentication
- D. Plain text authentication
- E. Teredo
- F. No authentication methods do exist

**Correct Answer:** CD  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 579**

Which three HSRP exchange states are used in multicast messages? (Choose three.)

- A. err-disabled
- B. coup
- C. inherit
- D. hold
- E. hello
- F. resign

**Correct Answer:** BEF  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 580**

Which two tasks can be accomplished to configure multiple HSRP client groups? (Choose two.)

- A. Use the standby priority command to configure an HSRP group to become a backup of another HSRP group.
- B. Use the standby follow command to configure an HSRP group to become a slave of another HSRP group.
- C. Use the standby track command to configure an HSRP group to become a primary HSRP group.
- D. Use the standby mac-refresh <seconds> command to change the refresh interval of the HSRP client group.
- E. Use the standby mac-resurrect <seconds> command to change the refresh interval of the HSRP client group.

**Correct Answer:** BD  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

Explanation:

Perform this task to configure multiple HSRP client groups.

The standby follow command configures an HSRP group to become a slave of another HSRP group.

HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.

Use the standby mac-refresh seconds command to directly change the HSRP client group refresh interval. The default interval is 10 seconds and can be configured to as much as 255 seconds.

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b> | <ul style="list-style-type: none"> <li>• Client or slave groups must be on the same physical interface as the master group.</li> <li>• A client group takes its state from the group it is following. Therefore, the client group does not use its timer, priority, or preemption settings. A warning is displayed if these settings are configured on a client group:</li> </ul> <pre> Router(config-if)# standby 1 priority 110 %Warning: This setting has no effect while following another group. Router(config-if)# standby 1 timers 5 15   % Warning: This setting has no effect while following another group. Router(config-if)# standby 1 preempt delay minimum 300   % Warning: This setting has no effect while following another group. </pre> |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/12-4/fhp-12-4-book/fhp-hsrp.html#GUID-EBDA2930-B8E5-4E54-9ECC-F9F232EC2955](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/12-4/fhp-12-4-book/fhp-hsrp.html#GUID-EBDA2930-B8E5-4E54-9ECC-F9F232EC2955)

#### QUESTION 581

Which three statements about RSPAN VLAN are true? (Choose three.)

- A. RSPAN VLAN traffic only flows on trunk ports.
- B. RSPAN VLAN prevents from carrying traffic
- C. RSPAN VLAN cannot be a private primary VLAN or secondary VLAN.
- D. All RSPAN VLAN traffic is flooded.
- E. RSPAN VLAN traffic only flows on access ports.
- F. RSPAN VLAN does not support Spanning-Tree Protocol.

**Correct Answer:** ACD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 582

Which two statements about RSPAN VLAN are true? (Choose two.)

- A. RSPAN VLAN must be configured in VLAN configuration mode using the remote-span command.
- B. RSPAN VLAN trunks can handle Spanning-Tree protocol, except for SPAN destination ports.
- C. RSPAN VLAN access ports can handle Spanning-Tree protocol in conjunction with SPAN destination ports.
- D. RSPAN VLAN does not support any protocols
- E. RSPAN VLAN traffic does not get flooded.

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 583

Which two restrictions of the port security feature are true? (Choose two.)

- A. Static port MAC address assignments are not supported.
- B. It is not supported on PVLAN ports.
- C. It is not supported on EtherChannel port-channel interfaces.
- D. A single device can learn a maximum of three sticky MAC addresses.
- E. It is supported on destination SPAN ports.

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 584

Which configuration do you apply to an interface so that it uses port security to learn and commit the first MAC address?

- A. Configure the switchport switch-port security violation restrict 1 command.
- B. Enable the sticky MAC addresses feature.
- C. Enable the static secure MAC addresses feature.
- D. Configure the switch for port-security aging type inactivity command.
- E. Configure the switchport port-security maximum 1 command.
- F. Disable the sticky MAC addresses feature.

**Correct Answer:** E  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:

Here is a concept example on how to learn and commit MAC addresses.

This example shows how to configure a maximum of 64 secure MAC addresses on the Fast Ethernet port 5/12:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface fastethernet 3/12
Router(config-if)# switchport port-security maximum 64
Router(config-if)# do show port-security interface fastethernet 5/12 | include Maximum
Maximum MAC Addresses      : 64
```

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port\\_sec.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.pdf) (see page 62-9)

**QUESTION 585**

Which two commands can you enter to configure load-balancing at Layer 2? (Choose two.)

- A. port-channel load-balance dst-ip
- B. port-channel load-balance src-dst-ip
- C. port-channel load-balance src-mac
- D. port-channel load-balance src-dest-mac
- E. port-channel load-balance src-ip

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 586**

Which two statements about CDP are true? (Choose two.)

- A. It can be disabled only at the interface level.
- B. Devices with Cisco Discovery Protocol configured send advertisement messages to a multicast address on a periodic basis
- C. It is disabled when switches have mismatched native VLANs
- D. Devices with Cisco Discovery Protocol configured send advertisement messages to a broadcast address on a periodic basis.
- E. VTP relies on Cisco Discovery Protocol to carry VTP domain information

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 587**

Which two command sequences must you enter on a pair of switches so that they negotiate an EtherChannel using the Cisco proprietary port-aggregation protocol? (Choose two.)

- A. channel-protocol lacp  
channel-group 1 mode on
- B. channel-protocol pagp  
channel-group 1 mode auto
- C. channel-protocol lacp chan-  
nel-group 1 mode active
- D. channel-protocol pagp channel-  
group 1 mode desirable
- E. channel-protocol pagp  
channel-group 1 mode on

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 588**

Which two ways can you use to disable Cisco Discovery Protocol? (Choose two.)

- A. Enter the no cdp enable command to disable it on a device.
- B. Enter the no cdp run command to disable it in the global configuration
- C. Enter the no cdp run command to disable it on an individual interface.
- D. Enter the cdp disable command to disable it on an individual interface
- E. Enter the no cdp enable command to disable it on an individual interface.

**Correct Answer:** BE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 589

Which two statements about errdisable recovery are true? (Choose two.)

- A. You can use the show errdisable recovery command to view the reason a port was error-disabled.
- B. Errdisable detection is enabled by default on ports with port security enabled
- C. You can use the show errdisable detect command to view the reason a port was error-disabled.
- D. Errdisabled autorecovery is enabled by default.
- E. Errdisabled detection is disabled by default on ports with port security enabled

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 590

What are the prerequisite for HSRP interface to come up? (Choose two.)

- A. VIP on same subnet.
- B. Physical IP address must be set.
- C. Virtual MAC address need to be configured.
- D. VIP on a separate subnet.
- E. There are no prerequisites required to configure HSRP.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 591

Which two prerequisites are required for an HSRP interface to come up? (Choose two.)

- A. The virtual IP address must be in the same subnet as the interface IP address.
- B. Configure a physical IP address for the interface and enable that interface before HSRP becomes active
- C. It requires to configure more than one first-hop redundancy protocol on the same interface.
- D. Configure HSRP version 2 to interoperate with HSRP version 1.
- E. The virtual IP address is prohibited to be in the same subnet as the interface IP address under IPv4.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 592

DRAG DROP

Select and Place:

**Select and Place:**

RSPAN was Layer 3 (L3) traffic to carry the traffic

Supports only VTP

The source can only be an access port

Range 1 – 2045 is allowed

Only supports STP

Source can only be trunk

Range 1 – 1005 is allowed

True

False

Correct Answer:

True

Only supports STP

Range 1 – 2045 is allowed

Source can only be trunk

Supports only VTP

False

Range 1 – 1005 is allowed

RSPAN was Layer 3 (L3) traffic to carry the traffic

The source can only be an access port

Section: Mix Questions  
Explanation  
Explanation/Reference:

QUESTION 593  
DRAG DROP

Drag and drop the statements about SPAN source and destination ports from the left onto the correct port types on the right.

Select and Place:



- Its original configuration is overwritten by the SPAN configuration
- It can be monitored as a bundled logical port or as individual physical ports
- It can be trunk or an access port
- It acts as the monitoring port
- It is not supported as part of a VLAN
- Multiple VLANs can be included in a single session

Source Port

Destination Port

Correct Answer:

Source Port

- It can be trunk or an access port
- It can be monitored as a bundled logical port or as individual physical ports
- Multiple VLANs can be included in a single session

Destination Port

- It acts as the monitoring port
- It is not supported as part of a VLAN
- Its original configuration is overwritten by the SPAN configuration

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 594  
DRAG DROP

Select and Place:

Select and Place:

- Advertises and learns millisecond timer values
- Provides improved management and troubleshooting
- Group numbers are restricted to the range from 0 to 255
- Expands the group number range from 0 to 4095
- The multicast address 224.0.0.2
- Millisecond timer values are not advertised or learned
- Uses the new IP multicast address 224.0.0.102
- Version 1 is the default version of HSRP

#### HSRP Version 1


#### HSRP Version 2


Correct Answer:


#### HSRP Version 1

- Group numbers are restricted to the range from 0 to 255
- Millisecond timer values are not advertised or learned
- The multicast address 224.0.0.2
- Version 1 is the default version of HSRP

#### HSRP Version 2

- Advertises and learns millisecond timer values
- Expands the group number range from 0 to 4095
- Provides improved management and troubleshooting
- Uses the new IP multicast address 224.0.0.102

Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 595

Which two statements about VRRP are true? (Choose two.)

- A. It requires each device in the group to participate in the same dynamic routing protocol.
- B. Preemption is not supported.

- C. It can use a single virtual address to provide default gateway redundancy.
- D. It uses a shared VIP to support default gateway redundancy.
- E. It support clear-text authentication only.

**Correct Answer:** CE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 596

Which two device types does DHCP snooping treat as untrusted in an ISP environment? (Choose two.)

- A. provider devices
- B. customer edge devices
- C. user-facing provider edge devices
- D. end host devices
- E. provider edge devices

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 597

Which feature can prevent ARP poisoning attacks on a device?

- A. Dynamic MAC Inspection
- B. CGMP snooping
- C. Dynamic ARP Inspection
- D. MAC snooping
- E. DHCP snooping
- F. Static ARP Inspection

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 598

Which two statements about LLDP frames are true? (Choose two.)

- A. They contain a CRC for error checking.
- B. The destination MAC address in a LLDP frame is a multicast address.
- C. Each LLDP frame contains a sequence of TLVs.
- D. Each LLDP frame includes a field containing the CoS value.
- E. They have an EtherType of 0x8080.
- F. All switches forward the destination MAC address in a LLDP frame.

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 599

Which virtual MAC address does HSRP group 37 use with default configuration?

- A. 00:00:0c:07:ac:25
- B. C0:00:00:25:00:00
- C. 00:00:0c:07:ac:37
- D. C0:00:00:37:00:00

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 600

Which two commands or command sequences configure a switch so that it tags native VLAN 3939? (Choose two.)

- A. `interface GigabitEthernet0/0`  
`description to HR Building M 3680-668`  
`encapsulation dot1q vlan native 3939`

- B. switch(config)#set switch native vlan 3939
- C. interface GigabitEthernet0/0  
description to HR Building M 3680-668  
switch(config)#vlan dot1q tag native
- D. switch(config)#vlan dot1q tag native
- E. switch(config)#vlan dot1q native vlan 3939

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 601

Which two tasks must you perform to enable DHCP option 82 on an untrusted port? (Choose two.)

- A. Enter the **ip dhcp snooping trust** command to enable data insertion for DHCP option 82.
- B. Enter the **ip dhcp snooping information option** command to enable option 82.
- C. Enter the **ip dhcp snooping trust** command to enable DHCP option 82.
- D. Enter the **ip dhcp snooping information option allow-untrusted** command to enable the untrusted port.
- E. Enter the **ip dhcp snooping information option replace** command to enable DHCP option 82.

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 602

```
DSW1#sh spanning-tree vlan 20

VLAN0020
  Spanning tree enabled protocol ieee
  Root ID    Priority    24596
             Addresses   0018.7363.4300
             Cost        2
             Port        13 (FastEthernet1/0/11)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    28692  (priority 28672 sys-id-ext 20)
             Address     001b.0d8e.e080
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time   300

Interface                Role STS Cost        Prio.Nbr Type
-----
Fa1/0/7                  Desq FWD 2          128.9    P2p
Fa1/0/10                 Desq FWD 2          128.12   P2p
Fa1/0/11                 Root FWD 2          128.13   P2p
Fa1/0/12                 Altn BLK 2          128.14   P2p
```

Refer the exhibit. Which two statements about the spanning-tree operation of this switch are true? (Choose two.)

- A. The **spanning-tree mode stp ieee** command was entered on this switch
- B. The spanning-tree operation mode for this switch is PVST.
- C. The switch is operating in the default cisco spanning-tree mode.
- D. The spanning-tree operation mode for this switch is IEEE/
- E. the spanning-tree operation mode for this switch is PVST+.

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 603

Which feature prevents a newly-added switch from being the primary?

- A. root guard
- B. BPDU guard
- C. BPDU filtering
- D. loop guard

Correct Answer: A  
Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 604  
DRAG DROP

Drag and drop the correct statements about HSRP from the left onto the True column on the right. Not all options are used.

Select and Place:

|                                                                       |      |
|-----------------------------------------------------------------------|------|
| HSRPv1 and HSRPv2 use different multicast for hello packets.          | true |
| HSRPv1 and HSRPv2 use the same packet format.                         | true |
| It can share a virtual MAC or IP address among a group of routers.    | true |
| It is a Cisco-proprietary implementation of FHRP.                     | true |
| It is supported on Layer 3 interfaces, including tunneled interfaces. |      |
| It supports authentication.                                           |      |
| The HSRPv2 group number ranges from 0 to 255.                         |      |

Correct Answer:

|                                                                       |                                                                    |
|-----------------------------------------------------------------------|--------------------------------------------------------------------|
|                                                                       | HSRPv1 and HSRPv2 use different multicast for hello packets.       |
| HSRPv1 and HSRPv2 use the same packet format.                         | It can share a virtual MAC or IP address among a group of routers. |
|                                                                       | It is a Cisco-proprietary implementation of FHRP.                  |
|                                                                       | It supports authentication.                                        |
| It is supported on Layer 3 interfaces, including tunneled interfaces. |                                                                    |
|                                                                       |                                                                    |
| The HSRPv2 group number ranges from 0 to 255.                         |                                                                    |

Section: Mix Questions  
Explanation

Explanation/Reference:



QUESTION 605

```
FastEthernet2/0/47 - Group 1
  State is Active
    7 state changes, last state change 00:00:19
  Virtual IP address is 10.1.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.616 secs
  Authentication MD5, key-string "cisco"
  Preemption enabled
  Active router is local
  Standby router is 10.1.1.3, priority 100 (expires in 9.455 sec)
  Priority 255 (configured 255)
  IP redundancy name is "hsrp-Fa2/0/47-1" (default)
```

Refer to the exhibit. Which two statements about the network environment of the device that generated this output are true? (Choose two.)

- A. The default hello and hold timer values are in use
- B. HSRP version 2 is in use.
- C. The standby router can take the active HSRP role if it fails to receive a hello packet from the active within 10 seconds.
- D. The standby router can take the active HSRP role if it fails to receive a hello packet from the active within 1.616 seconds.
- E. The priority value of the HSRP group is 1.

**Correct Answer:** AC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

QUESTION 606  
DRAG DROP

Drag and drop the description of VRRP from the left onto the correct versions of VRRP on the right.

**Select and Place:**

| Answer Area                                          | VRRP Version 2 and 3  |
|------------------------------------------------------|-----------------------|
| supports IPv6                                        |                       |
| compatible with CGMP                                 |                       |
| incompatible with HSRP                               |                       |
| supports millisecond timers                          |                       |
| supports EtherChannel port channels in layer 3 mode  |                       |
| sends hello messages to multicast address 224.0.0.18 |                       |
|                                                      | <b>VRRP Version 3</b> |
|                                                      |                       |
|                                                      |                       |

**Correct Answer:**

### Answer Area

### VRRP Version 2 and 3

compatible with CGMP

incompatible with HSRP

supports EtherChannel port channels  
in layer 3 mode

sends hello messages to multicast  
address 224.0.0.18

### VRRP Version 3

supports IPv6

supports millisecond timers

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 607  
DRAG DROP

Drag and drop the characteristic from the left to the matching STP timer variables on the right.

Select and Place:

default value of 20

time spent in the listening and learning states

controls how long the switch stores BPDU information

maximum value of 10

default value of 15

how often BPDUs are sent between switches

### STP: Hello Timer

### STP: Forward-Delay Timer

### STP: Maximum-Age Timer

Correct Answer:

STP: Hello Timer

maximum value of 10

how often BPDUs are sent between switches

STP: Forward-Delay Timer

default value of 15

time spent in the listening and learning states

STP: Maximum-Age Timer

default value of 20

controls how long the switch stores BPDU information

Section: Mix Questions  
Explanation

Explanation/Reference:

**QUESTION 608**  
Which two statements about GLBP are true? (Choose two.)

A. Member devices can elect one or more AVGs.  
B. Member devices send hello messages to multicast address 224.0.0.39.  
C. It supports up to 32 groups on a single interface.  
D. Member devices must elect exactly one AVG.  
E. The AVG assigns virtual MAC addresses to all group members.

Correct Answer: DE  
Section: Mix Questions  
Explanation

Explanation/Reference:

**QUESTION 609**  
When a Layer 2 trunking EtherChannel is configured, which two attributes must match across the member ports? (Choose two.)

A. spanning-tree cost  
B. spanning-tree priority  
C. allowed VLANs on the trunk  
D. trunking mode  
E. interface description

Correct Answer: CD  
Section: Mix Questions  
Explanation

Explanation/Reference:

**QUESTION 610**  
DRAG DROP

Drag and drop the descriptions of switching technologies from the left onto the correct technologies on the right.

Select and Place:

- combines exactly two devices
- supported on Cisco 3750 and 3850 devices
- supported on the Cisco 4500 and 6500 series
- supports devices that are geographically separated
- supports up to nine devices
- uses proprietary cabling

StackWise

VSS

Correct Answer:

StackWise

supports up to nine devices

supported on Cisco 3750 and 3850 devices

uses proprietary cabling

VSS

combines exactly two devices

supported on the Cisco 4500 and 6500 series

supports devices that are geographically separated

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 611

```

SW1#show int trunk
Port      Mode      Encapsulation  Status      Native vlan
Gi5/1     on        802.1q         trunking    1
Gi6/2     on        802.1q         trunking    600
Port      Vlans allowed on trunk
Gi5/1     113
Gi6/2     1,3,10,36,600
Port      Vlans allowed and active in management domain
Gi5/1     113
Gi6/2     1,3,10,36,600
Port      Vlans in spanning tree forwarding state and not pruned
Gi5/1     113
Gi6/2     1,3,10,36,600

```

Refer to the exhibit. Which two statements about SW1 are true? (Choose two.)

- A. Interface Gi6/2 is the root for VLAN 36.
- B. Interface Gi5/1 is using an industry-standard trunking protocol.
- C. Interface Gi5/1 is using a Cisco proprietary trunking protocol.
- D. On interface Gi6/2, all untagged traffic is tagged with VLAN 600.
- E. On interface Gi6/1, all untagged traffic is tagged with VLAN 113.
- F. The device is configured with the default MST region.

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 612

Which two statements about the LACP port priority of a device are true? (Choose two.)

- A. To manually configure a link within an EtherChannel to come up first, set its lacp port-priority value lower than the default.
- B. To manually configure a link within an EtherChannel to come up first, set its lacp port-priority value higher than the default.
- C. The system uses the port priority of the local and remote devices to determine which links in an EtherChannel group are active.
- D. The system uses the port priority of the local and remote devices to determine which links in an EtherChannel group are hot-standby.
- E. It determines which links in an EtherChannel group are active.
- F. LACP port-priority is used in the hashing algorithm to load-balance links within an EtherChannel.

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 613

In which two circumstances does a port security violation occur? (Choose two.)

- A. when sticky MAC address learning is enabled and the port has a link-down condition
- B. when a port with a secure MAC address attempts to use a different port in the same VLAN
- C. when the same MAC addresses enters a port more than once
- D. when the CAM table overflows with dynamically learned MAC addresses
- E. when the port has received more MAC addresses than allowed

**Correct Answer:** BE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port\\_sec.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/port_sec.pdf)

#### QUESTION 614

Which three VLANs are part of the extended range of available VLANs? (Choose three.)

- A. 1006
- B. 4095
- C. 4195
- D. 3000
- E. 4094
- F. 1001

**Correct Answer:** ADE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 615

Which three options are reasons for an interface to go into err-disable state? (Choose three.)



- A. security violation
- B. BPDU guard violation
- C. hard-coded speed duplex match on both sides
- D. ARP inspection
- E. storm-control broadcast
- F. grouping ports into a port channel

**Correct Answer:** ABD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>

#### QUESTION 616

In a switch stack is configured to use SDM template, where are the templates stored?

- A. all stack members
- B. stack master
- C. flash memory
- D. TFTP server

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_53\\_se/configuration/guide/3750xscg/swsdm.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_53_se/configuration/guide/3750xscg/swsdm.html)

#### QUESTION 617

Network engineer want to use UDLD, what he need to consider?

- A. udld is a non-propriety
- B. udld is working with non cisco devices
- C. udld is layer 1
- D. udld can aggressively disabled the port after eight failed retries

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 618

Which command enables root guard on a cisco switch?

- A. switch(config-if)# spanning-tree guard root
- B. switch(config)# spanning-tree guard root
- C. switch(config-if)# spanning-tree guard-root
- D. switch(config)# spanning-tree root guard
- E. switch(config-if)# spanning-tree root guard

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>

#### QUESTION 619

Refer to the exhibit. Which statement describes the result if a switch that is running PVST+ is added to this network?

```
DSW#sh spanning-tree vlan 10
VLAN0010
Spanning-tree enabled protocol
Root ID    Priority    4106
          Address    0018.7363.4300
          This bridge is the root
          Hello Time  2 sec Max Age 20 sec Forward delay 15 sec

Bridge ID Priority    4106 (priority 4096 sys-id-ext 20)
          Address    0018.7363.4300
          Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
          Aging Time  300

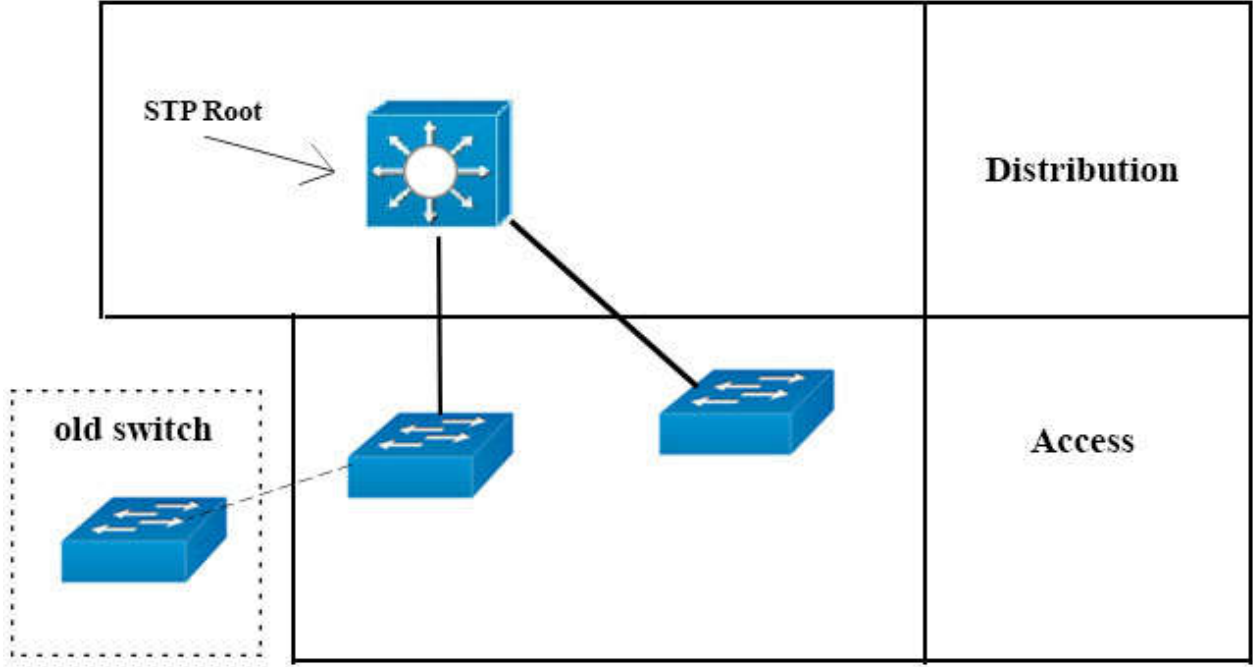
Interface      Role Sts Cost          Prio.Nbr Type
-----
Fa1/0/7        Desq FWD 2          128.9   P2p Peer (STP)
Fa1/0/10       Desq FWD 4          128.12  P2p Peer (STP)
Fa1/0/11       Desq FWD 2          128.13  P2p Peer (STP)
Fa1/0/12       Desq FWD 2          128.14  P2p Peer (STP)
```

- A. Spanning tree is disabled automatically on the network
- B. Spanning tree continues to operate in Rapid PVST+ on DSW2 and the new switch operates in PVST+
- C. Both switches operate in the PVST+ mode
- D. Both switches operate in the Rapid PVST+ mode

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 620**



A network engineer deployed an older switch with the same spanning-tree priority as the existing root, which caused a network outage. In which two locations should the Spanning Tree protocol root guard feature be implemented? (Choose two.)

- A. On the designated root switch downlinks to the access layer.
- B. On all of non-root switch facing ports of the access layer
- C. On the access layers root facing ports
- D. On Layer 3 boundaries in the distribution layer
- E. Globally on all network switches.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 621**

How will a switch become a stack master during election?

- A. highest member ID value
- B. highest member priority value

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 622**

Technician moves PC from one switch port to another switch port. After the move, the new switch port goes errdisabled. Why?

- A. Security violation
- B. Duplex mismatch
- C. different vlan

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 623**

What happens when a port configured with root-inconsistent receives a superior BPDU?

- A. Loop Guard
- B. Root Guard
- C. BPDU Guard
- D. BPDU Filter

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 624**

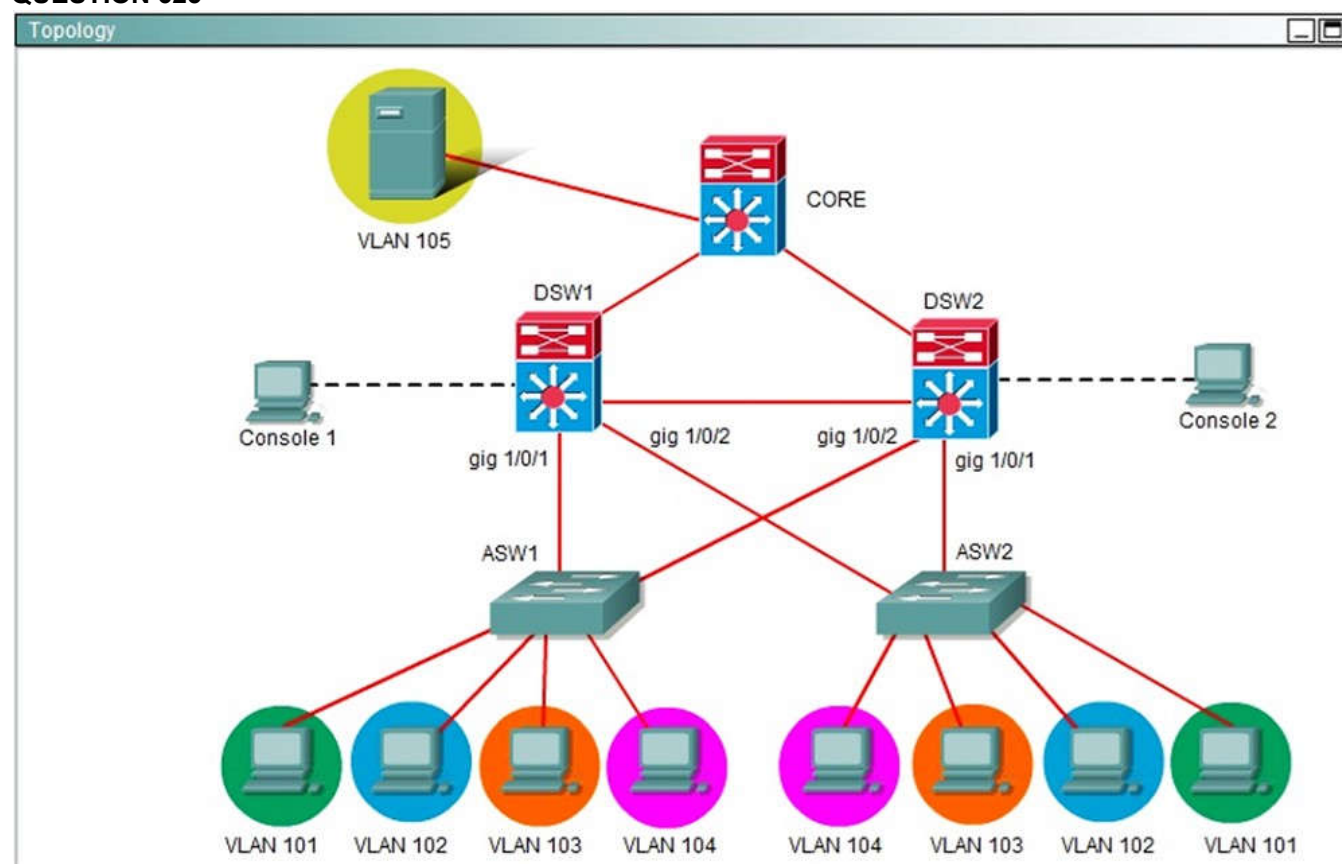
Which configuration do you apply to an interface so that it uses port security to learn and commit the first MAC address?

- A. Sticky
- B. Restrict
- C. Shutdown
- D. Protect

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 625**



- DSW1 (Distribution Switch 1) is the primary device for VLAN 101, 102, 105
- DSW2 (Distribution Switch 2) is the primary device for VLAN 103 and 104
- A failure on gig1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet 1/0/1 on backup device has also failed.

During routine maintenance, G1/0/1 on DSW1 was shutdown. All other interfaces were up. DSW2 became the active HSRP device for Vlan101 as desired. However, after G1/0/1 on DSW1 was reactivated. DSW1 did not become the active HSRP device as desired.

What need to be done to make the group for Vlan101 function properly?

- A. Enable preempt in the VLAN 101 HSRP group on DSW1.
- B. Disable preempt in the VLAN 101 HSRP group on DSW2's.
- C. In the VLAN 101 HSRP group on DSW1, decrease the priority value to value that is less ' than the priority value configured in the VLAN 101 HSRP group on DSW2.
- D. Decrease the decrement value in the track command for the VLAN 101 HSRP group on U DSWTs to a values less than the value in the track command for the VLAN 101 HSRP group on DSW2.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

Continue to check VLAN 101 on both switches

```
DSW1#show running-config
<output omitted>

interface Vlan101
  ip address 192.168.101.1 255.255.255.0
  standby 1 ip 192.168.101.254
  standby 1 priority 200
  standby 1 track GigabitEthernet1/0/1 55
!
```

```
DSW2#show running-config
<output omitted>

interface Vlan101
  ip address 192.168.101.2 255.255.255.0
  standby 1 ip 192.168.101.254
  standby 1 priority 150
  standby 1 preempt
  standby 1 track GigabitEthernet1/0/1
!
```

We learned that DSW1 doesn't have the "standby 1 preempt" command so it can't take over the active role again even if its priority is the highest. So we need to enable this command on VLAN 101 of DSW1.

**QUESTION 626**

If G1/0/1 on DSW1 is shutdown, what will be the current priority value of the Vlan105's group on DSW1?

- A. 95
- B. 100
- C. 150
- D. 200

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

Below is the output of VLAN 105:

```
DSW1#show running-config
<output omitted>

interface Vlan105
  ip address 192.168.105.1 255.255.255.0
  standby 5 ip 192.168.105.254
  standby 5 priority 150
  standby 5 preempt
  standby 5 track GigabitEthernet1/0/1 55
```

Priority is configured 150, Track is 55. So, if shutdown interface G1/0/1 it would be  $150 - 55 = 95$ .

#### QUESTION 627

Which statement about the current configuration on port GigabitEthernet 2/0/1 is true?

```
!
interface GigabitEthernet2/0/1
  swithport access vlan 700
  switchport trunk allowed vlan 200,300,700
  switchport mode trunk
end
!
```

- A. It is an access port configured for a phone and a PC
- B. It is a trunk port and native VLAN is VLAN 1
- C. It is a trunk port and native VLAN is VLAN 700
- D. It is an access port in VLAN 700

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 628

Refer to the exhibit. Three switches are configured for HSRP. Switch1 remains in the HSRP listen state. What is the most likely cause of this status?

|                                                                                                                                                                                                          |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>hostname Switch1 interface Vlan10 ip address 172.16.10.32 255.255.255.0 no ip redirects standby 1 ip 172.16.10.110 standby 1 timers msec 200 msec 700 standby 1 preemt</pre>                        |
| <pre>hostname Switch2 interface Vlan10 ip address 172.16.10.33 255.255.255.0 no ip redirects standby 1 ip 172.16.10.110 standby 1 timers msec 200 msec 750 standby 1 priority 110 standby 1 preemt</pre> |
| <pre>hostname Switch3 interface Vlan10 ip address 172.16.10.34 255.255.255.0 no ip redirects standby 1 ip 172.16.10.110 standby 1 timers msec 200 msec 750 standby 1 priority 150 standby 1 preemt</pre> |

- A. this is normal operation
- B. standby group number does not match VLAN number
- C. IP addressing is incorrect
- D. incorrect priority commands
- E. incorrect standby timers



**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 629**

An engineer is configuring EtherChannel between two switches using PAgP. If the EtherChannel mode on switch 1 is configured using auto, which mode on switch 2 establishes an operational EtherChannel?

- A. desirable
- B. passive
- C. active
- D. auto

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 630**

Which two requirements for dot1q trunking in IOS are true? (Choose two.)

- A. Spanning-tree PortFast must be enabled.
- B. MST must be running if extended VLANs are in use.
- C. The encapsulation protocol must be the same on each end of the trunk.
- D. The native VLAN must have the same number on each side of the link.
- E. ISL must be enabled on the same link.

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/8758-43.html>

**QUESTION 631**

In regards to Cisco Virtual Switching System which technology is needed between two switches for them to act as one network element and share control information and data traffic?

- A. trunk
- B. virtual port channel
- C. EtherChannel
- D. virtual switch link

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 632**

Refer to the exhibit. What is the effect of the given configuration?

```
spanning-tree extend system-id
spanning-tree mode pvst
spanning-tree backbonefast
```

- A. It enables the switch to become the spanning-tree root bridge.
- B. It enables the reduced MAC address feature.
- C. It enables spanning-tree to create dynamic system IDs.
- D. It enables extended VLANs.

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 633**

Which command do you enter so that the default authentication group on a device falls back to the case-sensitive local user database when the initial authentication fails?

- A. aaa authentication login default group tacacs+ radius local
- B. aaa authentication exec default group tacacs+ local if-authenticated
- C. aaa authentication login default group tacacs+ local-case if-authenticated
- D. aaa authentication exec default group tacacs+ if-authenticated local

**Correct Answer:** C

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 634**

Which three statements about VRRP are true? (Choose three.)

- A. Authentication commands must be entered under the interface.
- B. It sends advertisements to multicast address 224.0.0.9.
- C. It supports MD5 and IP sec authentication.
- D. It can use an interface IP address as the virtual IP address.
- E. It sends advertisements to multicast address 224.0.0.18.
- F. It is a Cisco proprietary protocol.

**Correct Answer: ADE**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 635**

Which statement about Layer 2 protocol participation of ports involved in a SPAN session is true?

- A. Neither a SPAN source nor SPAN destination participates in any Layer 2 protocols.
- B. A SPAN source does not participate in any Layer 2 protocols.
- C. A SPAN destination does not participate in any Layer 2 protocols.
- D. Both SPAN source and SPAN destination participate in any Layer 2 protocols.

**Correct Answer: C**

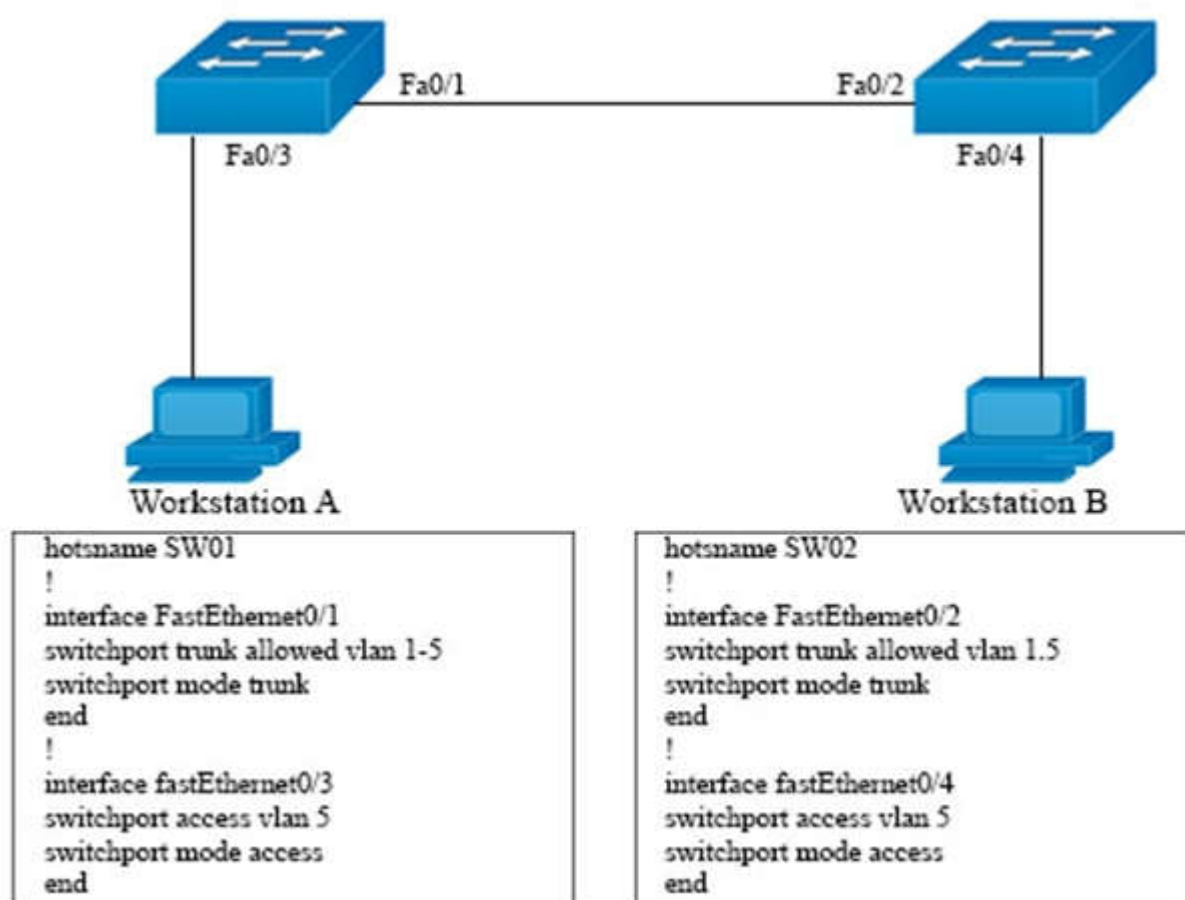
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_53\\_se/configuration/guide/2960scg/swspan.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swspan.pdf)

**QUESTION 636**

Refer to the exhibit. Which description of the effect of entering the switch port trunk allowed vlan 2,3,4 command on FastEthernet0/2 is true?



- A. The two workstations continue to communicate without a default gateway configured.
- B. The command is unsupported on a trunk where VLANs have already been pruned manually.
- C. The running configuration displays switch port trunk allowed vlan 1-5 for Fa0/2.
- D. The two workstations stop communicating because they are on VLAN 5, which is not allowed on the trunk.

**Correct Answer: D**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 637**

Which three responses from a RADIUS server are valid? (Choose three.)

- A. REJECT
- B. CHALLENGE
- C. ACCEPT
- D. UPDATE PASSWORD
- E. CONFIRM
- F. ACKNOWLEDGE

**Correct Answer:** ABC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 638**

Which two configurations can you apply to a port so that it tags traffic with VLAN 915? (Choose two.)

- A. 

```
interface GigabitEthernet0/0
switchport mode access
switchport access vlan 915
```
- B. 

```
interface GigabitEthernet0/0
switchport mode trunk
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 915
```
- C. 

```
interface GigabitEthernet0/0
switchport mode access
switchport voice vlan 915
switchport access vlan 915
```
- D. 

```
interface GigabitEthernet0/0.915
encapsulation dot1q 915
```
- E. 

```
interface GigabitEthernet0/0.915
switchport mode access
switchport access vlan 915
```

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 639**

During the implementation of a voice solution, which two required items are configured at an access layer switch that will be connected to an IP phone to provide VoIP communication? (Choose two.)

- A. allowed codecs
- B. untagged VLAN
- C. auxiliary VLAN
- D. Cisco Unified Communications Manager IP address
- E. RSTP

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 640**



Requirements:  
You will configure FastEthernet ports 0/12 through 0/24 for users who belong to VLAN 20. Also all VLAN and VTP configurations are to be completed in global configuration mode as VLAN database mode is being deprecated by Cisco. You are required to accomplish the following tasks:  
1. Ensure the switch does not participate in VTP but forwards VTP advertisements received on trunk ports.  
2. Ensure all non-trunking interfaces (Fa0/1 to Fa0/24) transition immediately to the forwarding state of Spanning-Tree.  
3. Ensure all FastEthernet interfaces are in a permanent non-trunking mode.  
4. Place FastEthernet interfaces 0/12 through 0/24 in VLAN 20.

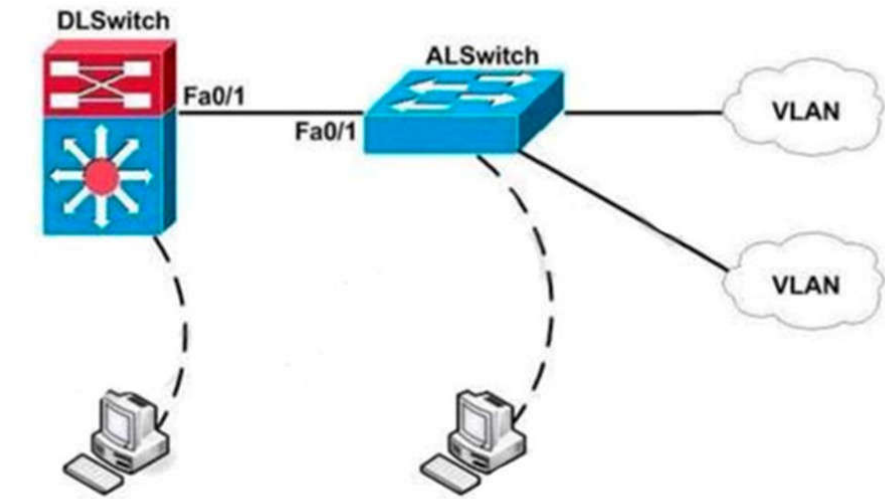
**Correct Answer:** See the explanation below  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**  
Explanation:

```
switch#conf t
switch(config)#vtp mode transparent
switch(config)#interface range fa0/12 – 24
switch(config-if-range)#switchport mode access
switch(config-if-range)#spanning-tree portfast
switch(config)#interface range fa0/12 – 24
switch(config-if-range)#switchport access vlan 20
switch(config-if-range)#end
switch# copy run start
```

**QUESTION 642**  
**SIMULATION**

The headquarter offices for a book retailer are enhancing their wiring closets with Layer3 switches. The new distribution-layer switch has been installed and a new access-layer switch cabled to it. Your task is to configure VTP to share VLAN information from the distribution-layer switch to the access-layer devices. Then, it is necessary to configure interVLAN routing on the distribution layer switch to route traffic between the different VLANs that are configured on the access-layer switches; however, it is not necessary for you to make the specific VLAN port assignments on the access-layer switches. Also, because VLAN database mode is being deprecated by Cisco, all VLAN and VTP configurations are to be completed in the global configuration mode. Please reference the following table for the VTP and VLAN information to be configured:



**Requirements:**

|                 |                |                 |
|-----------------|----------------|-----------------|
| VTP Domain name | cisco          |                 |
| VLAN Ids        | 20             | 21              |
| IP Addresses    | 172.16.71.1/24 | 172.16.132.1/24 |

These are your specific tasks:  
1. Configure the VTP information with the distribution layer switch as the VTP server.  
2. Configure the VTP information with the access layer switch as a VTP client.  
3. Configure VLANs on the distribution layer switch.  
4. Configure inter-VLAN routing on the distribution layer switch.  
5. Specific VLAN port assignments will be made as users are added to the access layer switches in the future.  
6. All VLANs and VTP configurations are to be completed in the global configuration. To configure the switch, click on the host icon that is connected to the switch be way of a serial console cable.

**Correct Answer:** See the explanation below  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**  
Explanation:

- 1) Configure the VTP information with the distribution layer switch as the VTP server:
- ```
DLSwitch#configure terminal
DLSwitch(config)#vtp mode server
DLSwitch(config)#vtp domain cisco (use cisco, not CISCO because it is case sensitive)
```
- 2) Configure the VTP information with the access layer switch as a VTP client
- ```
ALSwitch#configure terminal
ALSwitch(config)#vtp mode client
ALSwitch(config)#vtp domain cisco
ALSwitch(config)#exit
```
- 3) Configure VLANs on the distribution layer switch



To create VLANs on a switch, use the `vlan vlanID` command:

```
DLSwitch(config)#vlan 20
DLSwitch(config)#vlan 21
Configure Ip addresses for Vlans:
DLSwitch(config)#interface vlan 20
DLSwitch(if-config)#ip address 172.16.71.1 255.255.255.0
DLSwitch(if-config)#no shutdown
DLSwitch(if-config)#interface vlan 21
DLSwitch(if-config)#ip address 172.16.132.1 255.255.255.0
DLSwitch(if-config)#no shutdown
DLSwitch(if-config)#exit
```

4) Configure inter-VLAN routing on the distribution layer switch

```
DLSwitch(config)#ip routing
DLSwitch(config)#exit
DLSwitch#copy running-config startup-config
```

```
ALSwitch#copy running-config startup-config
```

#### QUESTION 643

##### SIMULATION

Acme is a small export company that has an existing enterprise network comprised of 5 switches;

- CORE, DSW1, DSW2, ASW1 and ASW2.

The topology diagram indicates their desired pre-VLAN spanning tree mapping.

Previous configuration attempts have resulted in the following issues:

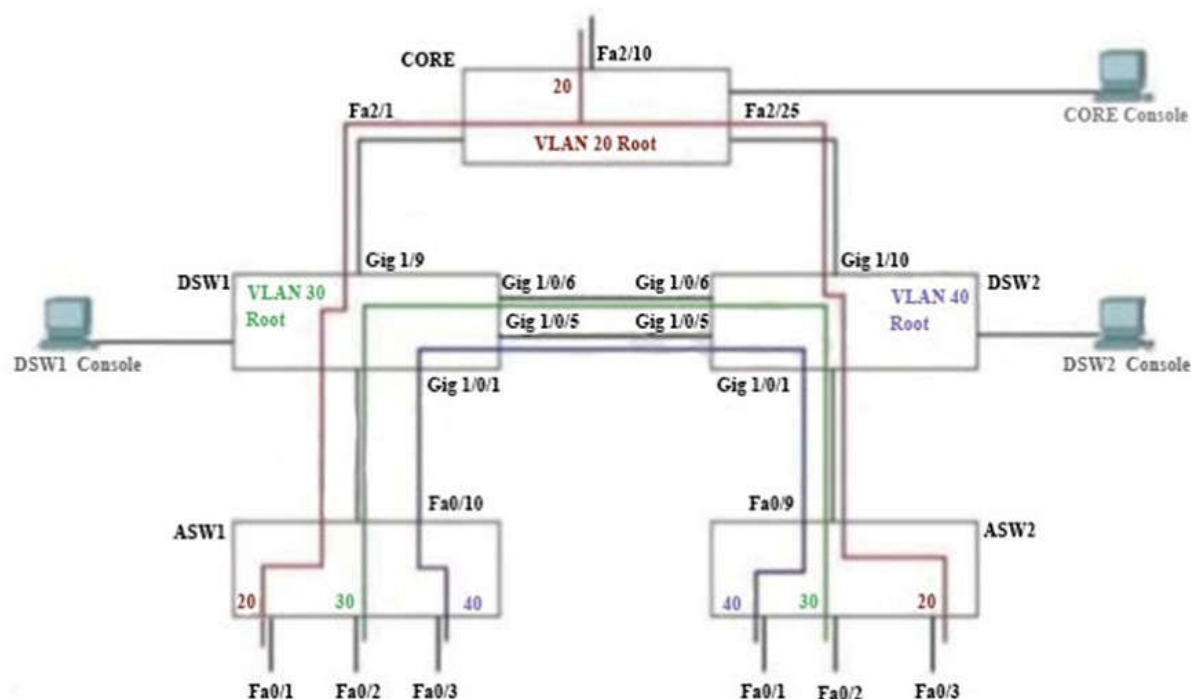
- CORE should be the root bridge for VLAN 20; however, DSW1 is currently the root bridge for VLAN 20.
- Traffic for VLAN 30 should be forwarding over the gig 1/0/6 trunk port between DSW1 and DSW2. However, VLAN 30 is currently using gig 1/0/5.
- Traffic for VLAN 40 should be forwarding over the gig 1/0/5 trunk port between DSW1 and DSW2. However, VLAN 40 is currently using gig 1/0/6.

You have been tasked with isolating the cause of these issues and implementing the appropriate solutions.

Your task is complicated by the fact that you only have full access to DSW1, with isolating the cause of these issues and implementing the appropriate solutions. Your task is complicated by the fact that you only have full access to DSW1, with the enable secret password cisco. Only limited show command access is provided on CORE, and DSW2 using the enable 2 level with a password of acme.

No configuration changes will be possible on these routers.

No access is provided to ASW1 or ASW2.



**Correct Answer:** See Explanation below.

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

```
DSW1#conf t
DSW1(config)#spanning-tree vlan 20 priority 61440
DSW1(config)#int g1/0/5
DSW1(config-if)#spanning-tree vlan 40 cost 1
DSW1(config-if)#no shut
DSW1(config-if)#exit
DSW1(config)#int g1/0/6
DSW1(config-if)#spanning-tree vlan 30 port-priority 64
DSW1(config-if)#no shut DSW1(config-if)#end
DSW1#copy run start
Verification:
DSW1# show spanning-tree vlan 20
DSW1# show spanning-tree vlan 40
DSW2# show spanning-tree vlan 30
```

#### QUESTION 644

##### DRAG DROP

Drag and drop the characteristic from the left to the matching STP mode on the right.  
Select and Place.

**Select and Place:**

maps VLANs to instances

based on IEEE 802.1w

default STP mode

based in IEEE 802.1D

based on IEEE 802.1s

discarding port state

PVST

RapidPVST

MST

Correct Answer:

PVST

default STP mode

based in IEEE 802.1D

RapidPVST

based on IEEE 802.1w

discarding port state

MST

maps VLANs to instances

based on IEEE 802.1s

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 645  
DRAG DROP

Drop the STP components from the left onto the correct descriptions on the right.

Select and Place:

bridge transit delay

root bridge

transmit halt delay

medium access delay

Measure of the time between the receipt and transmission of a frame

Measure of the time required for a frame to begin leaving the bridge after the CPU has decided to send it

Measure of the time for a port to be blocked after a blocking trigger

Directs all traffic

Correct Answer:

Measure of the time between the receipt and transmission of a frame

bridge transit delay

Measure of the time required for a frame to begin leaving the bridge after the CPU has decided to send it

medium access delay

Measure of the time for a port to be blocked after a blocking trigger

transmit halt delay

Directs all traffic

root bridge

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 646  
DRAG DROP

Drag and drop the LLDP-MED TLVs from the left onto the correct statements on the right.

Select and Place:

inventory management

LLDP-MED capabilities

location

network policy

Advertises the Layer 2 and Layer 3 configuration of the port

Indicates whether the device supports specific features

Shares caller ELIN

Shares the endpoint hardware profile

Correct Answer:

Advertises the Layer 2 and Layer 3 configuration of the port

network policy

Indicates whether the device supports specific features

LLDP-MED capabilities

Shares caller ELIN

location

Shares the endpoint hardware profile

inventory management

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 647  
DRAG DROP

Drag and drop the characteristic from the left to the matching STP category on the right.  
Select and place.

Select and Place:

- increments of 16
- The lowest value os preferred.
- default value of 128
- increment of 4096
- Default value is based on interface speed.
- value range from 1 - 20000000

#### STP: Switch Priority

#### STP: Port Priority

#### STP: Path Cost

Correct Answer:

#### STP: Switch Priority

increment of 4096

The lowest value os preferred.

#### STP: Port Priority

increments of 16

default value of 128

#### STP: Path Cost

Default value is based on interface speed.

value range from 1 - 20000000

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 648  
DRAG DROP

LACP vs PAGP  
Select and Place:

Select and Place:



- mode desirable
- mode active
- mode auto
- mode passive

LACP

PAGP

Correct Answer:

LACP

mode active

mode passive

PAGP

mode desirable

mode auto

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 649  
DRAG DROP

Drag and Drop - RSPAN True and False  
Select and Place:

Select and Place:

- Uses VLAN ID 2-1024
- Uses VLAN ID 2-1001
- Supports only STP
- MAC address learning is disabled
- Supports only VTP

**True**

**False**

Correct Answer:

**True**

MAC address learning is disabled

Uses VLAN ID 2-1001

Supports only VTP

**False**

Uses VLAN ID 2-1024

Supports only STP

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 650  
DRAG DROP

Drag and Drop - VRRPv2 & VRRPv3 vs VRRPv3 Comparison  
Select and Place:

Select and Place:

Supports IPv6

Send hello messages to multicast address  
224.0.0.18

Timers in millisecond

Sometimes about IGMP

Supports VTP

Assign IP address in the Layer 3 Ethernet

VRRPv2 and VRRPv3

VRRPv3

Correct Answer:

Sometimes about IGMP

VRRPv2 and VRRPv3

Send hello messages to multicast address  
224.0.0.18

Assign IP address in the Layer 3 Ethernet

Supports VTP

VRRPv3

Supports IPv6

Timers in millisecond

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 651  
DRAG DROP

Drag and Drop - LLDP-TLV (Concepts Only)

- LLDP-MED Capabilities TLV
- Network Policy TLV

Select and Place:

Select and Place:

The phone can connect to any switch, obtain its VLAN number, and then start communicating with the call control.

Allows LDDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.

The switch can notify a phone of the VLAN number that it should use

Allow both network connectivity devices and endpoints to advertise VLAN configuration and associated Layer 2 and Layer 3 attributes for the specific application on that port.

By defining a network-policy profile TLV, you can create profile for voice and voice-signalling by specifying the values for VLAN, class of service (Cos), differentiated services code point (DSCP), and tagging mode.

Profile attributes are then maintained centrally on the switch and propagated to the phone.

LLDP-MED Capabilities TLV

Network Policy TLV

Correct Answer:

**LLDP-MED Capabilities TLV**

Allows LDDP-MED endpoints to determine the capabilities that the connected device supports and has enabled.

**Network Policy TLV**

The phone can connect to any switch, obtain its VLAN number, and then start communicating with the call control.

The switch can notify a phone of the VLAN number that it should use

Allow both network connectivity devices and endpoints to advertise VLAN configuration and associated Layer 2 and Layer 3 attributes for the specific application on that port.

By defining a network-policy profile TLV, you can create profile for voice and voice-signalling by specifying the values for VLAN, class of service (Cos), differentiated services code point (DSCP), and tagging mode.

Profile attributes are then maintained centrally on the switch and propagated to the phone.

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 652**  
**DRAG DROP**

Drag and Drop - LLDP-TLV (Concepts Only)

- Power Management TLV
- Inventory Management TLV
- Location TLV

Select and Place:

**Select and Place:**



ELIN location information - Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.

**Civic location information**  
Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.

LLDP-MED also supports an extended power TLV to advertise fine-grained power requirements, endpoint power priority, and endpoint and network connectivity-device power status.

Allows switches and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs.

It does not provide for power negotiation between the endpoint and the network connectivity devices.

Enables advanced power management between LLDP-MED endpoint and network connectivity devices.

#### Power Management TLV

#### Inventory Management TLV

#### Location TLV

Correct Answer:

#### Power Management TLV

LLDP-MED also supports an extended power TLV to advertise fine-grained power requirements, endpoint power priority, and endpoint and network connectivity-device power status.

Allows switches and phones to convey power information, such as how the device is powered, power priority, and how much power the device needs.

It does not provide for power negotiation between the endpoint and the network connectivity devices.

Enables advanced power management between LLDP-MED endpoint and network connectivity devices.

#### Inventory Management TLV

Allows an endpoint to send detailed inventory information about itself to the switch, including information hardware revision, firmware version, software version, serial number, manufacturer name, model name, and asset ID TLV.

#### Location TLV

ELIN location information - Provides the location information of a caller. The location is determined by the Emergency location identifier number (ELIN), which is a phone number that routes an emergency call to the local public safety answering point (PSAP) and which the PSAP can use to call back the emergency caller.

Civic location information  
Provides the civic address information and postal information. Examples of civic location information are street address, road name, and postal community name information.

#### Section: Mix Questions Explanation

##### Explanation/Reference:

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/int\\_hw\\_components/configuration\\_guide/b\\_int\\_3se\\_3850\\_cg/b\\_int\\_3se\\_3850\\_cg\\_chapter\\_0101.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/int_hw_components/configuration_guide/b_int_3se_3850_cg/b_int_3se_3850_cg_chapter_0101.html)

#### QUESTION 653

##### DRAG DROP

Drag and Drop - STP Timer Delay (Concepts Only)

- Diameter of the STP Domain (dia)
- Bridge Transit Delay (transit delay)
- BPDU Transmission Delay (bpdudelay)

Select and Place:

Select and Place:



This value is the time that elapsed between the reception and the transmission of the same frame by the bridge.

This is logically the latency through the bridge.

The IEEE recommendation is to consider a maximum diameter of seven bridges for the default STP timers.

The IEEE recommendation is to consider 1 sec as the maximum bridge transit delay.

This value is the maximum number of bridges between any two points of attachment of end stations.

The IEEE recommends 1 sec as the maximum BPDU transmission delay

The value is the delay between the time a BPDU is received on a port and the time that the configuration BPDU is

#### Diameter of the STP Domain (dia)

#### Bridge Transit delay (transit delay)

#### BPDU Transmission Delay (bpdu\_delay)

Correct Answer:

#### Diameter of the STP Domain (dia)

The IEEE recommendation is to consider a maximum diameter of seven bridges for the default STP timers.

This value is the maximum number of bridges between any two points of attachment of end stations.

#### Bridge Transit delay (transit delay)

This value is the time that elapsed between the reception and the transmission of the same frame by the bridge.

This is logically the latency through the bridge.

The IEEE recommendation is to consider 1 sec as the maximum bridge transit delay.

#### BPDU Transmission Delay (bpdu\_delay)

The IEEE recommends 1 sec as the maximum BPDU transmission delay

The value is the delay between the time a BPDU is received on a port and the time that the configuration BPDU is

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/19120-122.html>

**QUESTION 654**

DRAG DROP

Drag and Drop - STP Timer Delay (Concepts Only)

Message Age Increment Overestimate (msg\_overestimate)

Lost Message (lost\_msg)

Transmit Halt Delay (Tx\_halt\_delay)

Select and Place:

Select and Place:

This value is the number of BPDUs that can be lost as a BPDU moves from one end of the bridged network to the other end.

The IEEE recommendation is to use 1 sec for this parameter.

The IEEE recommendation is to use three as the number of BPDUs that can be lost.

The IEEE recommendation is to consider 1 sec as the maximum bridge transit delay.

This value is the increment that each bridge adds to the message age before forwarding a BPDU.

This value is the maximum amount of time that necessary for a bridge to effectively move a port into the blocking state after the determination that the port needs to be

As the Spanning Tree Protocol Timers section states, Cisco switches (and probably all switches) add 1 sec to the message age before the switches forward a BPDU.

**Message Age Increment Overestimate (msg\_overestimate)**

**Lost Message (lost\_msg)**

**Transmit Halt Delay (Tx\_halt\_delay)**

Correct Answer:

The IEEE recommendation is to consider 1 sec as the maximum bridge transit delay.

#### Message Age Increment Overestimate (msg\_overestimate)

This value is the increment that each bridge adds to the message age before forwarding a BPDU.

As the Spanning Tree Protocol Timers section states, Cisco switches (and probably all switches) add 1 sec to the message age before the switches forward a BPDU.

#### Lost Message (lost\_msg)

This value is the number of BPDUs that can be lost as a BPDU moves from one end of the bridged network to the other end.

The IEEE recommendation is to use three as the number of BPDUs that can be lost.

#### Transmit Halt Delay (Tx\_halt\_delay)

The IEEE recommendation is to use 1 sec for this parameter.

This value is the maximum amount of time that necessary for a bridge to effectively move a port into the blocking state after the determination that the port needs to be

#### Section: Mix Questions Explanation

##### Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/19120-122.html>

#### QUESTION 655

##### DRAG DROP

Drag and Drop - STP Timer Delay (Concepts Only)

Medium Access Delay (med\_access\_delay)

End-to-end BPDU Propagation Delay

Maximum Transmission Halt Delay

Select and Place:

Select and Place:



The IEEE recommendation is to use 0.5 sec as the maximum time.

Assume a diameter of seven hops, three BPDUs that can be lost, and a hello time of 2 sec.

The IEEE counts 1 sec as the maximum for this event.

This value is the time that is necessary for a device to gain access to the media for initial transmission.

This value is the time that is necessary in order to effectively block a port, after the decision to block is made.

It is the time between the CPU decision to send a frame and the moment when the frame effectively begins to leave the bridge.

This value is the amount of time that is necessary for a BPDU to travel from one end of the network to the other end.

#### Medium Access delay (med\_access-delay)

#### End-to-end BPDU Propagation Delay

#### Maximum Transmission Halt Delay

Correct Answer:

#### Medium Access delay (med\_access-delay)

The IEEE recommendation is to use 0.5 sec as the maximum time.

This value is the time that is necessary for a device to gain access to the media for initial transmission.

It is the time between of the CPU decision to send a frame and the moment when the frame effectively begins to leave the bridge.

#### End-to-end BPDU Propagation Delay

Assume a diameter of seven hops, three BPDUs that can be lost, and a hello time of 2 sec.

This value is the amount of time that is necessary for a BPDU to travel from one end of the network to the other end.

#### Maximum Transmission Halt Delay

The IEEE counts 1 sec as the maximum for this event.

This value is the time that is necessary in order to effectively block a port, after the decision to block is made.

#### Section: Mix Questions Explanation

##### Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/19120-122.html>

#### QUESTION 656

##### DRAG DROP

Drag and Drop - RSPAN Steps (Concept 1) - CONCEPT ONLY (UNOFFICIAL)  
Select and Place:

Select and Place:

monitor session 1 destination remote vlan

create VLAN for RSPAN session (destination)

create VLAN for RSPAN session (source)

monitor session 1 destination (interface or VLAN)

monitor session 1 source remote VLAN

monitor session 1 source (interface or VLAN)  
direction rx or tx or both

Source Switch

Destination Switch

Correct Answer:

monitor session 1 destination remote vlan

create VLAN for RSPAN session (destination)

create VLAN for RSPAN session (source)

monitor session 1 destination (interface or VLAN)

monitor session 1 source remote VLAN

monitor session 1 source (interface or VLAN)  
direction rx or tx or both

Source Switch

create VLAN for RSPAN session (source)

monitor session 1 destination remote vlan

monitor session 1 source (interface or VLAN)  
direction rx or tx or both

Destination Switch

create VLAN for RSPAN session (source)

monitor session 1 destination (interface or VLAN)

monitor session 1 source remote VLAN

Explanation/Reference:

QUESTION 657  
DRAG DROP

Drag and Drop - RSPAN Steps (Concept 2) - CONCEPT ONLY (UNOFFICIAL)  
Select and Place:

Select and Place:

Associate an RSPAN source session number with the RSPAN VLAN.

Associate an RSPAN destination session number with the destination port.

Associate an RSPAN source session number with source ports or VLANs.

Configure a VLAN as an RSPAN VLAN.

Associate an RSPAN destination session number with the RSPAN VLAN.

Step 1

Step 2

Step 3

Step 4

Step 5

Correct Answer:



|  |
|--|
|  |
|  |
|  |
|  |
|  |

**Step 1**

Configure a VLAN as an RSPAN VLAN.

**Step 2**

Associate an RSPAN source session number with source ports or VLANs.

**Step 3**

Associate an RSPAN destination session number with the RSPAN VLAN.

**Step 4**

Associate an RSPAN source session number with the RSPAN VLAN.

**Step 5**

Associate an RSPAN destination session number with the destination port.

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 658**  
DRAG DROP

Drag and Drop - VRRPv2 vs VRRPv3 (Concept 1) - CONCEPT ONLY (UNOFFICIAL)  
Select and Place:

**Select and Place:**



- Timers in seconds
- Multicast 224.0.0.18 for IPv4 (FF02::12 for IPv6)
- Multicast: 224.0.0.18
- VRRP needs to be enabled globally
- Timers in milliseconds
- VRRP enable per interface
- Support IPv4 and IPv6
- RID MAC: 0000.5E00.01xx
- Support IPv4 only
- Only high priority cause preemption
- Same priority but high IP cause preemption

VRRP2 v2

VRRP v3

Correct Answer:

VRRP2 v2

Timers in seconds

Multicast: 224.0.0.18

VRRP enable per interface

Support IPv4 only

Only high priority cause preemption

RID MAC: 0000.5E00.01xx

VRRP v3

Multicast 224.0.0.18 for IPv4 (FF02::12 for IPv6)

VRRP need to be enabled globally

Timers in milliseconds

Same priority but high IP cause preemption

Support IPv4 and IPv6

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 659  
DRAG DROP

Drag and Drop - HSRPv1 vs HSRPv2 (Concept 1) - CONCEPT ONLY (UNOFFICIAL)  
Select and Place:

Select and Place:

- Advertises and learns millisecond timer values
- Provides improved management and troubleshooting
- Group numbers are restricted to the range from 0 to 255
- Expands the group number range from 0 to 4095
- The multicast address 224.0.0.2
- Millisecond timer values are not advertised or learned
- Uses the new IP multicast address 224.0.0.102
- Version 1 is the default version of HSRP

#### HSRP Version 1


#### HSRP Version 2


Correct Answer:


#### HSRP Version 1

- Group numbers are restricted to the range from 0 to 255
- The multicast address 224.0.0.2
- Millisecond timer values are not advertised or learned
- Version 1 is the default version of HSRP

#### HSRP Version 2

- Advertises and learns millisecond timer values
- Provides improved management and troubleshooting
- Expands the group number range from 0 to 4095
- Uses the new IP multicast address 224.0.0.102

Section: Mix Questions  
Explanation

Explanation/Reference:

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhnp/configuration/15-mt/fhnp-15-mt-book/fhnp-hsrp-v2.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhnp/configuration/15-mt/fhnp-15-mt-book/fhnp-hsrp-v2.pdf)

**QUESTION 660**  
**DRAG DROP**

Drag and Drop - Stack Master Election Process (CONCEPT ONLY)  
Select and Place:

**Select and Place:**

Uses the non-default interface-level configuration

Uses the higher Hardware/Software priority

Uses the lowest MAC address

Uses the longest system up-time

Currently the stack master

Uses the highest stack member priority value

Step 1

Step 2

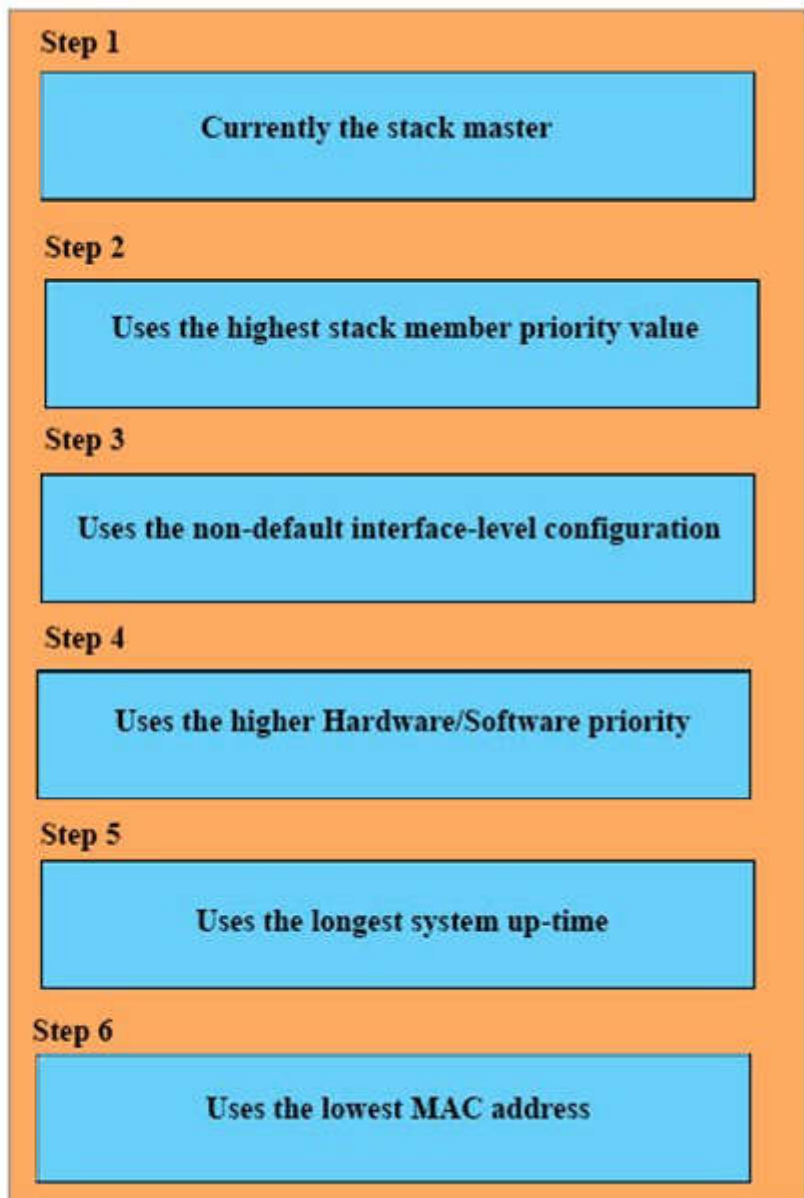
Step 3

Step 4

Step 5

Step 6

**Correct Answer:**



Section: Mix Questions  
Explanation

Explanation/Reference:

Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html>

QUESTION 661  
DRAG DROP

Drag and Drop - DHCP Snooping Process (Concept 1) - CONCEPT ONLY (UNOFFICIAL)  
Select and Place:

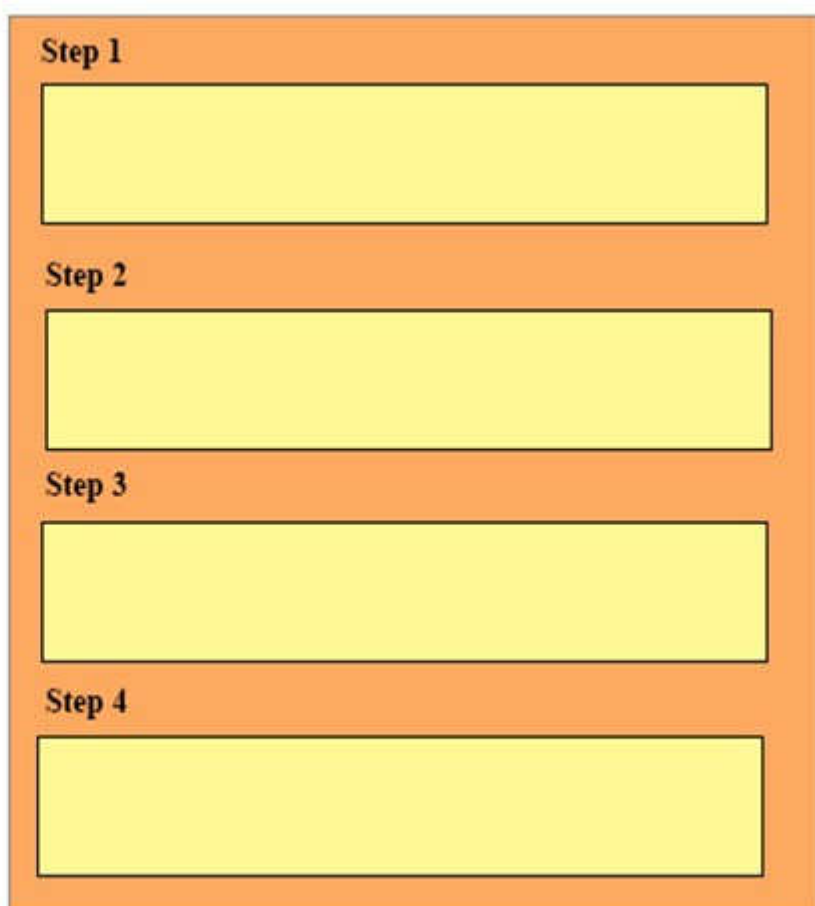
Select and Place:

Enable ARP inspection on selected VLANs

Enable Dynamic ARP Inspection (DAI)

Enable DHCP snooping globally

Enable DHCP snooping on selected VLAN



Correct Answer:



|  |
|--|
|  |
|  |
|  |
|  |

Step 1

Enable DHCP snooping globally

Step 2

Enable Dynamic ARP Inspection (DAI)

Step 3

Enable ARP inspection on selected VLANs

Step 4

Enable DHCP snooping on selected VLAN

Section: Mix Questions  
Explanation

Explanation/Reference:

QUESTION 662  
DRAG DROP

Drag and Drop - RADIUS vs TACACS+ (Concept 1) - CONCEPT ONLY (UNOFFICIAL)  
Select and Place:

Select and Place:

- Cisco proprietary
- Uses UDP port 1812
- Separates AAA and performs three-way challenge
- Does offer Multiprotocol
- Is a client-server model
- Uses TCP port 49
- Encrypts only the password in access-request packet from client to server
- Encrypts the entire body of the packet
- Does not offer Multiprotocol support
- Combines authentication and authorization

**RADIUS**

**TACACS+**

Correct Answer:

Section: Mix Questions  
Explanation

Explanation/Reference:  
Reference: [https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp\\_multi\\_prot](https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp_multi_prot)

QUESTION 663  
DRAG DROP

Drag and Drop -RADIUS vs TACACS+ (Concept 2) - CONCEPT ONLY (UNOFFICIAL)

Select and Place:

Select and Place:

- Is not as useful for router management or as flexible for terminal services
- Allow router verify whether if the user is authorized at specified privilege level
- Assign privelege levels to commands
- Does not allow users to control which commands can be executed on a router
- Provides two methods to control authorization of router commands on a per-user or per-group
- Supports PPP, PAP, CHAP, UNIX, login and other authonthenication are allowed
- Authenticated specify on a per-user or per-group basis of which commands are allowed
- Authenticated through the use of shared secret

## RADIUS

## TACACS+

Correct Answer:

|  |
|--|
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**RADIUS**

Is not as useful for router management or as flexible for terminal services

Does not allow users to control which commands can be executed on a router

Supports PPP, PAP, CHAP, UNIX, login and other authentication are allowed

Authenticated through the use of shared secret

**TACACS+**

Allow router verify whether if the user is authorized at specified privilege level

Assign privelege levels to commands

Provides two methods to control authorization of router commands on a per-user or per-group

Authenticated specify on a per-user or per-group basis of which commands are allowed

Section: Mix Questions  
Explanation

Explanation/Reference:  
Reference: [https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp\\_multi\\_prot](https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp_multi_prot)

**QUESTION 664**  
What happens if an interface within channel group is configured as SPAN destination?

- A. Portchannel will forward traffic to source span
- B. will not be operational
- C. the link will be in error-disable
- D. The interface will be removed from the channel group

Correct Answer: D  
Section: Mix Questions  
Explanation

Explanation/Reference:

**QUESTION 665**  
EtherChannel guard misconfig is configured on a switch, which technology supports that?

- A. LACP
- B. PagP
- C. STP
- D. Port Security

Correct Answer: C  
Section: Mix Questions  
Explanation

Explanation/Reference:



**QUESTION 666**

Which will identify the master switch in stackwise?

- A. The switch that is currently the stack master
- B. The switch with the highest stack member priority value
- C. The switch that uses the non-default interface-level configuration
- D. The switch with the lower priority stack member priority value

**Correct Answer:** A

**Section:** Mix Questions

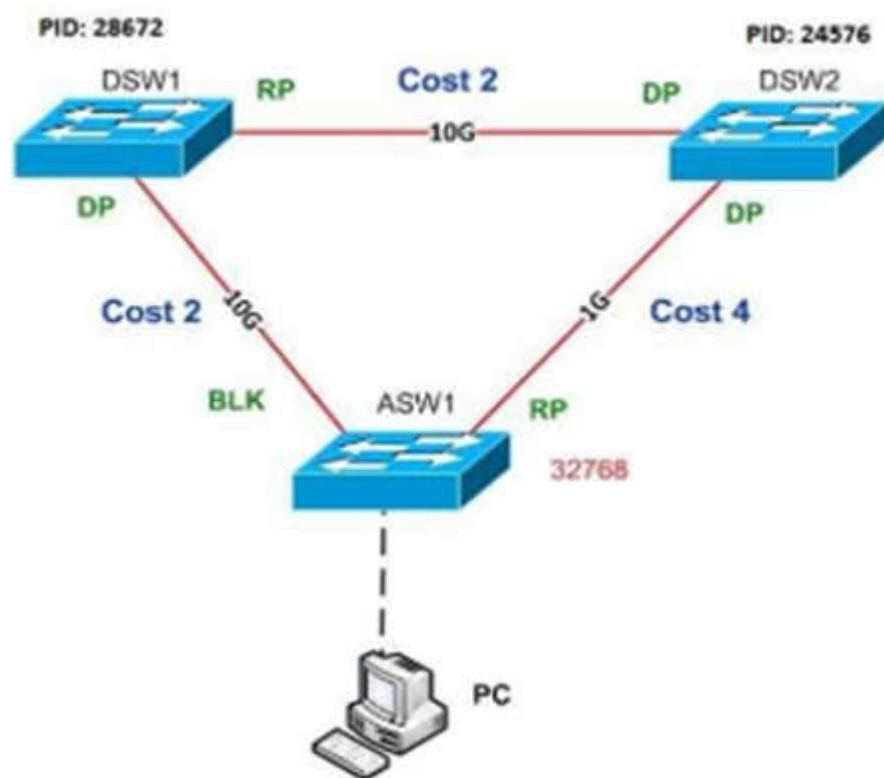
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/71925-cat3750-create-switch-stks.html>

**QUESTION 667**

How will the traffic reach the core switch from AS switch to DS core switch?



(Based on a topology shown with one core, two distribution and two access switches on each distribution switch, with redundant links and bandwidth mentioned.)

- A. ASW1 to DWS1 to core
- B. ASW1 to DWS2 to core
- C. ASW1 to DSW1 to DSW2 to core
- D. ASW1 to DSW2 to DSW1 to core

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 668**

If HSRP group number is 37, what would be the vMAC (virtual MAC) address?

- A. 00-00-0C07-AC25
- B. 0000-0C07-AC37
- C. 0000-C007-AC25
- D. 0000-C007-AC37

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 669**

What is the default value for spanning-tree port-priority?

- A. 128
- B. 64
- C. 32
- D. 1024

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/n5k/commands/spanning-tree-port-priority.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/spanning-tree-port-priority.html)

**QUESTION 670**

What statement is true if a new switch with a lower bridge ID is introduced in a network with root guard enhancement?

- A. Prevent unknown switch be a root port
- B. Root Guard puts the port into root-inconsistent
- C. Allow two root bridges in a network
- D. All ports of the new switch are changed to listening state

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10588-74.html>

**QUESTION 671**

How to configure loop guard in a Cisco switch IOS?

- A. (config)#spanning-tree loop guard default
- B. (config-if)#spanning-tree loop
- C. (config)#spanning-tree loop-guard default
- D. (config-if)#spanning-tree guard loop
- E. (config-if)#spanning-tree guard

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10596-84.html#loop\\_guard](https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10596-84.html#loop_guard)

**QUESTION 672**

Which statement is true about dynamic access port?

- A. VLAN 1 is the default VLAN.
- B. None until the port VLAN is determined.
- C. All VLANs are permitted in a dynamic access port link.
- D. By default the port has to participate in a VLAN election to determine which VLAN a port is assigned.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:****QUESTION 673**

What can happen after a RSPAN configuration in a Cisco switch?

- A. Destination port is unusable for normal use
- B. Traffic in network is doubled
- C. CDP or LLDP must be enable on switch
- D. The traffic is cached in NVRAM

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:****QUESTION 674**

Which two statements are true about Option 82? (Choose two.)

- A. Layer 2 ingress
- B. Layer 3 egress
- C. Layer 3 ingress
- D. Layer 2 egress
- E. Layer 4 egress
- F. Layer 4 ingress

**Correct Answer: AB**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:****QUESTION 675**

Where is SDM template stored in a Stackwise configuration?

- A. master
- B. slave
- C. NVRAM
- D. flash

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_53\\_se/configuration/guide/3750xscg/swsdm.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_53_se/configuration/guide/3750xscg/swsdm.html)

#### QUESTION 676

Which information is true about RSPAN?

- A. RSPAN VLAN carries only RSPAN traffic
- B. On a switch there can be only one RSPAN VLAN
- C. RSPAN VLAN carries RSPAN traffic along multiple switches
- D. RSPAN can be enable only in a Layer 3 switch

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 677

What is the link called between a VSS?

- A. VSL (Virtual Switch Link)
- B. SVI
- C. DCSP
- D. VLAN

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 678

Which statement is true about GLBP?

- A. GLBP uses multicast address 224.0.0.102 with UDP port 3222.
- B. GLBP uses multicast address 224.0.0.2 with TCP port 3222.
- C. GLBP uses multicast address 224.0.0.102 with TCP port 3222.
- D. GLBP uses multicast address 224.0.0.18 with UDP port 3222

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 679

How many Active Virtual Gateways (AVG) can be used in a GLBP protocol?

- A. Only one AVG can be elected on a switch
- B. Two AVG could be elected on a switch
- C. Two AVG just could be elected in GLBP v2
- D. GLBP supports 8 AVGs per group

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 680

Which statement is true about VRRP?

- A. VRRP uses multicast address 224.0.0.18 and uses IP Protocol 112
- B. VRRP uses multicast address 224.0.0.28 and uses UDP port 112
- C. VRRP uses multicast address 224.0.0.2 and uses IP Protocol port 3222
- D. VRRP uses multicast address 224.0.0.18 and uses TCP port 112
- E. VRRP uses multicast address 224.0.0.9 and uses UCP port 112

**Correct Answer:** A

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 681**

Which statement is true about HSRP?

- A. HSRP uses multicast address 224.0.0.2 and uses UDP port 1985.
- B. HSRP uses multicast address 224.0.0.22 with TCP port 1122
- C. HSRP uses broadcast address 224.0.0.2 with UDP port 1985
- D. HSRP uses broadcast address 224.0.0.22 with UDP port 32229

**Correct Answer: A**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 682**

What is the multicast address for HSRPv2?

- A. 224.0.0.102
- B. 127.0.0.1
- C. 224.1.1.2
- D. 224.1.1.102

**Correct Answer: A**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 683**

What will be the behavior of an access port when a tagged packet is received, with a VLAN ID of an access port?

- A. The tag is removed and packet is forwarded to a VLAN of access port.
- B. The tag is removed and packet is forwarded of the VLAN mentioned in the tag.
- C. The tag is not removed and packet is forwarded of the VLAN mentioned in the tag.
- D. Packet is dropped.

**Correct Answer: D**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 684**

An engineer needs to add a customer private VLAN to the network. What configuration is required to isolate the customer's traffic on the network?

- A. Configure transparent mode
- B. Enable VTP v3
- C. Configure VTP in server mode
- D. Disable VTP and manually configure the customer VLAN

**Correct Answer: A**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 685**

What is the behavior of an access port when a tagged packet is received other than the access VLAN value?

- A. Tag is removed and packet is forwarded of the VLAN mentioned in the tag.
- B. Tag is removed and packet is forwarded on the VLAN of the access port.
- C. Not available
- D. Packet is dropped

**Correct Answer: D**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 686**

If you have a new switch (that runs spanning-tree mode pvst+) connect to the exist switch, which statement is true?

- A. It will not work between two switches.
- B. It will work, the new switch will communicate to the existing switch with PVST+

- C. It will work, the new switch will communicate to the existing switch with Rapid-PVST
- D. It will work, the new switch will communicate to the existing switch with MSTP

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 687

What is the default violation status of port security?

- A. none
- B. shutdown
- C. trap
- D. enabled

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 688

What is the storm control violation defined by default on a Cisco switch?

- A. Disabled
- B. Enabled
- C. Enabled by broadcast only
- D. Enabled by multicast only

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 689

What happens when a destination SPAN port that is configured as EtherChannel receives traffic?

- A. Shutdown
- B. Err-disable
- C. Nothing
- D. Broadcast threshold is doubled in an interface

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 690

Refer to the exhibit. Which three statements about the network environment of the interface that generated? (Choose three.)

```
Router# show vrrp
FastEthernet2/0/47 - Group 1
  State is Master
  Virtual IP address is 10.1.1.1
  Virtual MAC address is 0000.0c07.ac01
  Advertisement interval is 1.000 sec
  Preemption is enabled
    min delay is 0.000 sec
  Priority is 105
    Track object 1 state Down decrement 15
  Master Router is 10.1.1.2 (local), priority is 105
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.531 sec
```

- A. The configured VRRP priority of the interface is 120
- B. The device on which the interface resides is acting as a standby router
- C. The Skew time .531 seconds
- D. The Configured VRRP Priority of the interface is 105
- E. If the priority of another router is higher than the priority of the master router, it becomes the master router

**Correct Answer:** ACE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**



**QUESTION 691**

Which statement about the VTPv2 is true?

- A. It supports the use of multiple instances.
- B. It propagates VLANs 1 – 1005 only.
- C. It can be enabled on a per-port basis.
- D. It performs consistency checks only when a new VLAN is manually added.
- E. It can be enabled on a per-interface basis.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 692**

Which two possible EtherChannel load balancing mechanisms are based on Layer 3? (Choose two.)

- A. MAC Source
- B. MAC Source-destination
- C. IP Source
- D. IP Source-destination
- E. MAC Destination

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 693**

Which VTPv2 mode does the switch operate without participating in VTP?

- A. client
- B. server
- C. transparent
- D. off

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 694**

How to disable CDP? (Choose two.)

- A. no cdp run on interface
- B. no cdp run in global configuration
- C. cdp disable on interface
- D. no cdp enable on interface
- E. no cdp enable in global configuration

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 695**

What happens if we add "line" on AAA command?

- A. Disable TACACS+ authentication
- B. Disable RADIUS authentication
- C. It's a last resource (or resort) login
- D. Is the prefer logging method in Cisco switches

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 696**

Which one is related to Stackwise technology?

- A. Switches can be stack with port-channel.
- B. Multiple switches can be stacked.

- C. Master switch and backup switch is listed in line.
- D. ProStack with mix switch.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 697**

A switch which was connected with 2 fiber cables attached to another switch. After initial boot (I think another switch), one of the link get error-disable or shutdown. What was the reason for that?

- A. Due to STP.
- B. Due to UDLD aggressive mode, the other switch didn't get the BPDU message.
- C. Due to UDLD normal mode, the other switch didn't get the BPDU message.
- D. Due to port security configuration.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 698**

Which technique will control broadcast, multicast and unicast problems?

- A. port security
- B. STP
- C. storm control
- D. SPAN

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 699**

How to recover err-disable after an UDLD failure?

- A. UDLD reset
- B. Err-disable auto recovery
- C. Shut and no shutdown (restart)
- D. Reboot the switch
- E. UDLD recovery

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 700**

How to configure DHCP snooping and DAI (Dynamic ARP Inspection) in VLAN? (Choose all that apply.)

- A. Define and configure a DHCP server
- B. Enable DHCP snooping on at least one VLAN
- C. Ensure that DHCP server is connected in a trusted interface
- D. Configure DHCP snooping DB agent
- E. Enable DHCP snooping globally
- F. Redirect DHCP snooping locally
- G. Disable DHCP snooping on at least one VLAN
- H. Prevent DHCP server from connecting to a trusted interface

**Correct Answer:** BCF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 701**

Which three feature sets are used in Stackwise technology? (Choose three.)

- A. LAN Base
- B. IP Base
- C. WAN Services
- D. IP Services
- E. ARP Base
- F. LAN Agent

**Correct Answer:** ABD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 702

Which statement is true about Stackwise?

- A. When building a switch stack, you cannot mix software feature sets.
- B. When building a switch stack, you can mix software feature sets.
- C. When building a Switch stack, a broadcast storm would occur.
- D. When building a Switch stack, performance will be degraded.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 703

Which three statements about SPAN and RSPAN are true? (Choose three.)

- A. The switch port monitor provides data on network switches by port in use, CPU load and memory used.
- B. It provides specific port data to obtain active and historical port utilization information.
- C. Accurate information on unused switch ports helps the administrator keep these ports closed for security risk best practices.
- D. Does not provide specific port data to obtain active and historical port utilization information.
- E. Accurate information on unused switch ports is not necessary.

**Correct Answer:** ABC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.solarwinds.com/topics/switch-port-monitor>

#### QUESTION 704

Refer to the exhibit. Which two statements about the flag of the EtherChannel is true? (Choose two.)

```
=====START EXHIBIT=====
Switch# show etherchannel summary
Flags: D - down                P - bundled in port-channel
I - standard-alone            s - suspended
H - Hot-standby (LACP only)
R - Layer 3                   S - Layer 2
U - in use                    f - failed to allocate aggregator
M - not in use, minimum links not met
u - unsuitable for bundling
w - waiting to be aggregated
d - default port
Number of channel-groups in use: 1
Number of aggregators: 1
Group Port-channel Protocol Ports
-----
1 Po1(SU) LACPFa0/13(P) Fa0/14(P)
=====END OF EXHIBIT=====
```

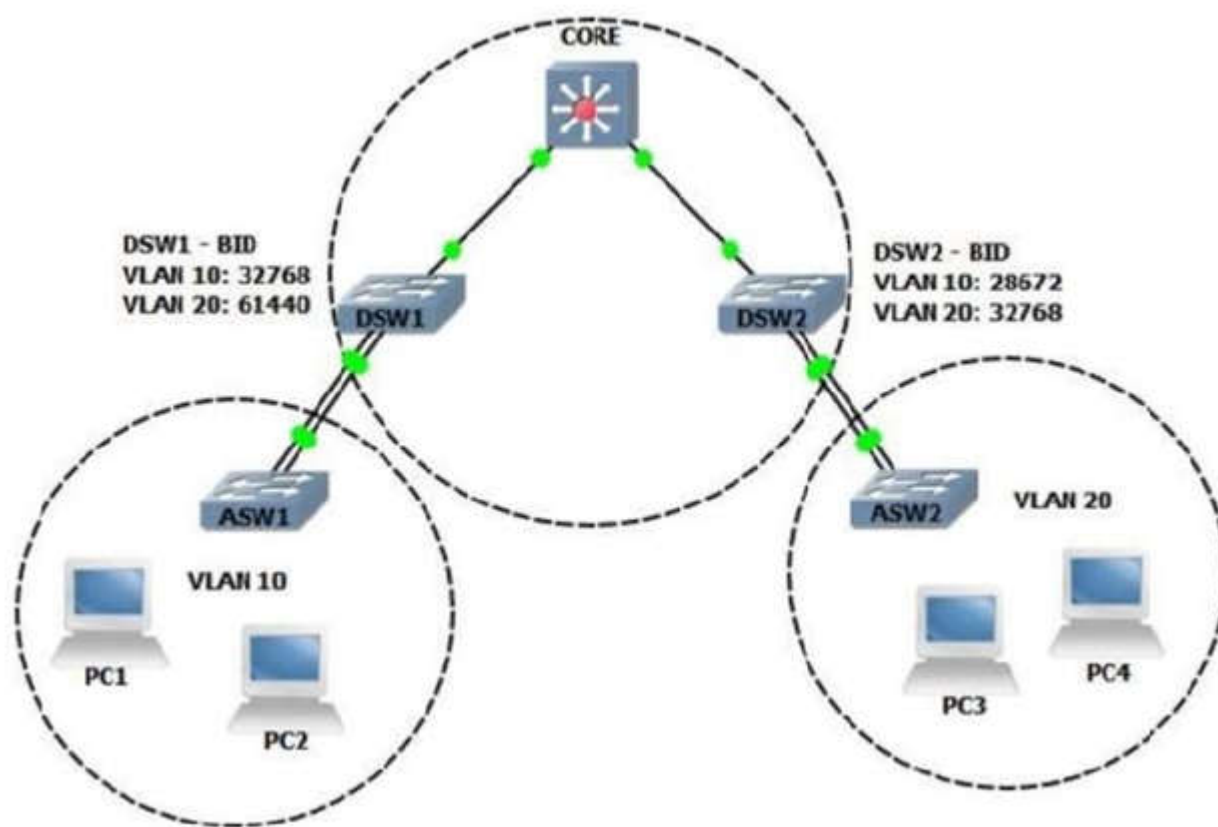
- A. Flag S indicates Layer 2 is operational.
- B. Flag U indicates EtherChannel is operational.
- C. Flag R indicates Layer 2 is operational.
- D. Flag U indicates Layer 2 is operational.
- E. Flag H indicates EtherChannel is operational.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 705

Refer to exhibit: How to make DSW1 the primary root for VLAN 10. (Choose two.)



- A. Change DSW2 bridge priority to VLAN 20 to 61440
- B. Change DSW1 bridge priority to VLAN 10 to 4096
- C. Change DSW1 bridge priority to VLAN 20 for 4096
- D. Change DSW1 bridge priority to VLAN 10 for 1
- E. Change DSW1 bridge priority to VLAN 10 with the command priority root

**Correct Answer:** BE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 706

Which information does the subordinate switch in a switch stack keep for all the VLANs that are configured on it?

- A. VLAN database
- B. DHCP snooping database
- C. Spanning trees information
- D. Routing information

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 707

Which two TLVs are included in Cisco Discovery Protocol advertisements? (Choose two.)

- A. Network Policy TLV
- B. VTP Management Domain TLV
- C. System Name TLV
- D. Inventory Management TLV
- E. Native VLAN TLV

**Correct Answer:** BE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/cdp/configuration/15-mt/cdp-15-mt-book/nm-cdp-discover.html>

#### QUESTION 708

Which fallback method can you configure to allow all AAA authorization requests to be granted if the other methods do not respond or return an error?

- A. enable
- B. RADIUS
- C. none
- D. TACACS+

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 709**

Which two statements about VRRP advertisements are true? (Choose two.)

- A. They are sent from the master router and standby routers.
- B. They include VRRP timer information.
- C. They are sent only from the master router.
- D. They include priority information.
- E. They are sent every three seconds by default.

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4\\_2/nx-os/unicast/configuration/guide/l3\\_cli\\_nxos/l3\\_vrrp.pdf](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_vrrp.pdf)

**QUESTION 710**

Which two StackWise configuration setting types are applied at the system level? (Choose two.)

- A. 802.1x settings
- B. speed/duplex settings
- C. port-security settings
- D. VLAN settings
- E. SNMP settings

**Correct Answer:** DE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstack.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.pdf)

**QUESTION 711**

Which three values can Cisco IOS device use as the basis for EtherChannel load-balancing? (Choose three.)

- A. MAC address
- B. port number
- C. IP address
- D. VLAN ID
- E. IP precedence
- F. DSCP

**Correct Answer:** ABC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/etherchannel/12023-4.html>

**QUESTION 712**

Which command can you enter to set the time between BPDUs in an MST environment by route bridge?

- A. spanning-tree mst 1 cost 5
- B. spanning-tree mst mst forward-time 5
- C. spanning-tree mst hello-time 2
- D. spanning-tree mst max-age 20

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 713**

Which two configuration requirements for port security are true? (Choose two.)

- A. Port must be in access mode
- B. Port security must be enabled on the port level
- C. Port must be in interface VLAN mode
- D. Port security must be disabled on the port level
- E. Port must be in encapsulation mode

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 714**



Which two ISP devices should have trust Port-Statement with DHCP Snooping feature? (Choose two.)

- A. User responsible to control ISP edge devices
- B. Only ISP edge devices
- C. Edge devices
- D. Network devices
- E. Local only devices
- F. Nobody is responsible to control ISP edge devices

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 715

Which two requirements are required to form a Layer 2 EtherChannel? (Choose two.)

- A. Ports should be contiguous.
- B. Ports should be in same module of switch stack.
- C. Same trunking protocol should be used on all ports.
- D. No port should be a part of SPAN destination session.
- E. All ports should be a part of SPAN source and destination session.

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 716

Which two port err-disabled recovery options are used to detect the reason? (Choose two.)

- A. show errdisable detect
- B. show errdisable recovery
- C. error-disable notifications/traps are active by default.
- D. error-disable notifications/traps are disabled by default.
- E. error-disable notifications/traps is never possible.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>

#### QUESTION 717

Which two functions of DHCP snooping are true? (Choose two.)

- A. It rate-limits DHCP traffic from trusted and untrusted sources.
- B. It listens to multicast messages between senders and receiver.
- C. It helps build the route table.
- D. It filters invalid messages from untrusted sources.
- E. It correlates IP address to hostnames.

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html>

#### QUESTION 718

Refer to the exhibit. Which two statements about the network environment are true? (Choose two.)

| VLAN | MAC             | Interface |
|------|-----------------|-----------|
| 10   | aaa.aaa.aaa.aaa | Fa0/1     |
| 20   | bbb.bbb.bbb.bbb | Fa0/3     |
| 30   | aaa.aaa.aaa.aaa | Fa0/2     |

- A. Interface fa0/1 and fa0/2 cannot communicate via Layer 2 switching.
- B. Interface fa0/1 and fa0/3 cannot communicate via Layer 2 switching.
- C. Interface fa0/2 and fa0/3 can communicate via Layer 2 switching.
- D. The two aaaa.aaaa.aaaa MAC address entries must be from the same VLANs.
- E. The two aaaa.aaaa.aaaa MAC address entries must be from different VLANs.

**Correct Answer:** AB  
**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 719**

If VLAN 99 is set to trunk, how can you set it to untagged from trunk VLAN 99?

- A. switchport access vlan 99
- B. switchport vlan 99 access
- C. switchport vlan 99 allow access
- D. switchport allow access vlan 99

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 720**

Which feature rate-limits DHCP traffic?

- A. DHCP Snooping
- B. DHCP Acknowledge
- C. DHCP Request
- D. DHCP Spoofing

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 721**

Which two statements are true about StackWise? (Choose two.)

- A. It groups multiple switch ports as a single EtherChannel.
- B. It can use one IP address to communicate with n/w (network).
- C. It monitors multiple switches from a central console.
- D. It enables multiple switch ports to share a single master configuration.
- E. It allows multiple switches to operate as a single switch.

**Correct Answer: BE**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 722**

Which statement about GLBP is true?

- A. Unused bandwidth is never utilized.
- B. They communicate under TCP port 3222 for both source and destination.
- C. They become active if any of the existing forwarding switches fail.
- D. They become restricted if any of the existing forwarding switches fail.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 723**

With GLBP, in which state is the standby virtual gateway in?

- A. learn
- B. listen
- C. init
- D. reply

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 724**

Which statement is true when one of its virtual gateway redundancy with an AVF has failed?

- A. If an AVF has failed, one of the primary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.
- B. If an AVF has failed, one of the secondary virtual forwarders in the listen state assumes responsibility for the virtual MAC address.

- C. If an AVF has failed, one of the secondary virtual forwarders in the listen state will also fail.
- D. If an AVF has failed, one of the primary virtual forwarders in the listen state will also fail.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 725

Which three design types of capable Ethernet LANs does HSRP support? (Choose three.)

- A. Multicaccess
- B. Multicast
- C. Broadcast
- D. Unicast
- E. Token Ring
- F. FDDI

**Correct Answer:** ABC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:  
HSRP is designed for use over multiaccess, multicast, or broadcast capable Ethernet LANs. HSRP is not intended as a replacement for existing dynamic protocols.

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/12-2sr/fhp-12-2sr-book/fhp-hsrp.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sr/fhp-12-2sr-book/fhp-hsrp.pdf)

#### QUESTION 726

Which hot standby groups numbers are used in a HSRP token ring?

- A. 0, 1 and 2
- B. 3, 5, and 7
- C. 0 and 1
- D. 2 and 4

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/12-2sx/fhp-12-2sx-book/fhp-hsrp.pdf](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/12-2sx/fhp-12-2sx-book/fhp-hsrp.pdf)

#### QUESTION 727

Which component does the GLBP client cache stores for each host of a particular GLBP group?

- A. IP address
- B. MAC address
- C. VLAN
- D. Token ring
- E. DCSP

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 728

What will extend a trust boundary (There is a switch interface configuration with separate voice VLAN and data VLAN to, also showing endpoint (host), IPPhone, Access Switch, Distribution Switch, Core Switch and Data Centre Aggregation switch)?

- A. Multiple Layers PC
- B. IP Phone
- C. Access Switch
- D. Distribution Switch
- E. Core Switch

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 729

Which of the following LLDP mandatory TLVs are valid for basic management? (Choose five.)

- A. Port description TLV
- B. System name TLV

- C. System description
- D. System capabilities TLV
- E. Management address TLV
- F. Isolated address TLV
- G. Source and destination capabilities TLV

**Correct Answer:** ABCDE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors. This protocol can advertise details such as configuration information, device capabilities, and device identity.

The switch supports these basic management TLVs. These are mandatory LLDP TLVs.

- + Port description TLV
- + System name TLV
- + System description TLV
- + System capabilities TLV
- + Management address TLV

These organizationally specific LLDP TLVs are also advertised to support LLDP-MED.

- + Port VLAN ID TLV ((IEEE 802.1 organizationally specific TLVs)
- + MAC/PHY configuration/status TLV(IEEE 802.3 organizationally specific TLVs)

#### QUESTION 730

Which two of the following organizationally specific LLDP TLVs are also advertised to support LLDP-MED? (Choose two.)

- A. Port VLAN ID TLV (IEEE 802.1 organizationally specific TLVs)
- B. MAC/PHY configuration/status TLV (IEEE 802.3 organizationally specific TLVs)
- C. IP Address TLV (IEEE 802.9 organizationally specific TLVs)
- D. DSCP TLV (IEEE 802.3 organizationally specific TLVs)
- E. Descriptive TLV (IEEE 802.5 organizationally specific TLVs)

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 731

Which two mandatory TLV types does LLDP advertise? (Choose two.)

- A. Native VLAN TLV
- B. Platform TLV
- C. Network TLV
- D. Hostname TLV
- E. Port ID TLV
- F. Chassis ID TLV

**Correct Answer:** EF

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: <https://learningnetwork.cisco.com/docs/DOC-26851>

#### QUESTION 732

Which four mandatory TLVs are valid in CDP? (Choose four.)

- A. End of LLDPDU
- B. Chassis ID
- C. Port ID
- D. Time To Live
- E. VLAN ID
- F. System name ID
- G. Description ID

**Correct Answer:** ABCD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: <https://learningnetwork.cisco.com/docs/DOC-26851>

#### QUESTION 733

Which six optional TLVs are valid? (Choose six.)

- A. Port description TLV
- B. System name TLV
- C. System description TLV
- D. System capabilities TLV

- E. Management address TLV
- F. Specific TLVs
- G. Source ID TLV
- H. Native hostname TLV

**Correct Answer:** ABCDEF

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: <https://learningnetwork.cisco.com/docs/DOC-26851>

#### QUESTION 734

When you enable MST on the switch, what happens?

- A. Enables RSTP and use BPDU type 2, maximum 16 instances to be used.
- B. Enables RSTP and use BPDU type 4, maximum 16 instances to be used.
- C. Disables RSTP and use BPDU type 2, maximum 16 instances to be used.
- D. Disables RSTP and use BPDU type 4, maximum 16 instances to be used.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 735

Which two methods are used to configure a trusted option 82? (Choose two.)

- A. 

```
(config)# ip dhcp snooping information option
```

```
(config)# do show ip dhcp snooping | include 82
```

```
(config)# ip dhcp snooping information option allow-untrusted
```
- B. 

```
(config-if)# ip dhcp snooping information option allow-untrusted
```
- C. 

```
(config)# ip dhcp untrusted-allow information
```
- D. 

```
(config-if)# ip dhcp snooping trust-allow information
```
- E. 

```
(config)# dhcp allow-untrusted option information
```

**Correct Answer:** AB

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 736

Which of the following commands to configure a DHCP trust is valid?

- A. 

```
(config)# interface FastEthernet 0/1
```

```
(config-if)# ip dhcp snooping trust
```

```
(config-if)# do show ip dhcp snooping | begin pps
```
- B. 

```
(config)# interface FastEthernet 0/1
```

```
(config-if) ip dhcp snooping granted
```

```
(config-if)# do show ip dhcp snooping | enable pps
```
- C. 

```
(config)# interface FastEthernet 0/1
```

```
(config-if) ip dhcp snooping allowed-enable
```

```
(config-if)# do show ip dhcp snooping | start pps
```
- D. 

```
(config)# interface FastEthernet 0/1
```

```
(config-if)# ip dhcp snooping enable
```

```
(config-if)# ip dhcp show snoop | begin pps
```

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 737

If switch SW1 is connected in a mesh with four other switches and all switches retain the default configuration, which command do you enter on SW1 interface to make it the root bridge for all VLANs?

- A. SW1(config)#spanning-tree port-priority 129
- B. SW1(config)#spanning-tree port-priority 127
- C. SW1(config-if)#spanning-tree port-priority 129
- D. SW1(config-if)#spanning-tree port-priority 127



**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 738**

Which two attributes must match across the member ports, when a Layer 2 EtherChannel is configured? (Choose two.)

- A. switchport mode
- B. spanning-tree cost
- C. spanning-tree priority
- D. VLAN membership

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 739**

Which tool can error-disable an interface if the storm control threshold is exceeded?

- A. storm control action shutdown
- B. storm control action default
- C. storm control enable
- D. storm control action trap

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.html>

**QUESTION 740**

A switch has a pair of fiber and it has been damaged. Which two statements is true about the configuration below? (Choose two.)

```
errdisable recovery cause udld
errdisable recovery internal 15
interface gig0/0
udld mode aggressive
```

- A. It would prevent loops.
- B. It would be in shutdown mode until fiber is replaced.
- C. It would be up for 15 minutes after fiber is fixed.
- D. The port would try to activate the repaired damaged fiber after 15 seconds.

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 741**

Which two statements about PortFast is true? (Choose two.)

- A. It will skip all spanning-tree states.
- B. Only when the port is active when it moves to the forwarding state.
- C. It is mostly used when connecting to workstations and servers.
- D. It skips the learning state.

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10553-12.html>

**QUESTION 742**

Which two statements about HSRP is true? (Choose two.)

- A. It required all the groups to have the same routing protocols.
- B. It must have an IP address that is active.
- C. It must have the same virtual MAC address for all groups.
- D. It must have the same VIP address in all groups.

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 743**

Which two statements about dynamic MAC address learning are true? (Choose two.)

- A. Dynamically-learned MAC addresses can be cleared on a per-interface basis only.
- B. It must be enabled on ports with port security enabled.
- C. It can be disabled on a per-VLAN basis only.
- D. Switch interfaces learn MAC addresses dynamically by default.
- E. Dynamically-learned MAC addresses supersede static MAC addresses

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 744**

Which command is used to configure DHCP snooping for Option 82?

- A. dhcp snooping trust
- B. dhcp snooping information option untrust
- C. ip dhcp snooping option replace
- D. ip dhcp snooping information option allow-untrusted

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 745**

Which three commands are valid to configure DHCP snooping for Option 82? (Choose three.)

- A. On the interface configuration mode;  
(config-if)# ip dhcp snooping trust
- B. On the global configuration mode;  
(config)# ip dhcp snooping information option allow-untrusted
- C. On the interface configuration mode;  
(config-if)# ip dhcp snooping information option allow-untrusted
- D. On the interface configuration mode;  
(config-if)# ip dhcp snooping granted
- E. On the global configuration mode;  
(config)# ip dhcp snooping information option enable-untrusted
- F. On the interface configuration mode;  
(config-if)# ip dhcp snooping information option enable-untrusted

**Correct Answer:** ABC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 746**

Which two advantages of LLDP are used over CDP? (Choose two.)

- A. It supports topology change notification.
- B. It supports ATM.
- C. It supports checksum.
- D. It supports vendor-agnostic.
- E. It supports FrameRelay

**Correct Answer:** AD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 747**

Which statement about RSPAN session is true?

- A. Only the source switch in a session must support RSPAN.
- B. The same RSPAN VLAN is used for a RSPAN session on all switches.
- C. At least one access port must be configured in the RSPAN VLAN.
- D. RSPAN support by default monitors at Layer 2 switch protocols.

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Explanation:

You can configure any VLAN as an RSPAN VLAN as long as these conditions are met:

- The same RSPAN VLAN is used for an RSPAN session in all the switches.
- All participating switches support RSPAN.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2\\_40\\_se/configuration/guide/scg/swspan.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg/swspan.pdf)

**QUESTION 748**

Which two VLAN ranges can you add, modify or delete on a switch? (Choose two.)

- A. VLANs 1-1001
- B. VLANs 1005-4094
- C. VLANs 1006-4094
- D. VLANs 2-1001
- E. VLANs 2-4094

**Correct Answer: CD**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3se/vlan/configuration\\_guide/b\\_vlan\\_3se\\_3650\\_cg/b\\_vlan\\_3se\\_3650\\_cg\\_chapter\\_011.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/3se/vlan/configuration_guide/b_vlan_3se_3650_cg/b_vlan_3se_3650_cg_chapter_011.html)

**QUESTION 749**

Where does the VLAN information get saved to?

- A. The information is saved to the vlan.dat file.
- B. The information is saved to the running configuration file.
- C. The information is saved to the vlan.txt file.
- D. The information is saved to the vlan.conf file.

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 750**

Which two statements are true in regards to normal and extended range VLANs? (Choose two)

- A. Normal range VLANs from 1-1005 are stored in vlan.dat.
- B. Extended range VLANs from 1006-4096 are stored in the startup configuration.
- C. Normal range VLANs from 1-1005 are stored in the startup configuration.
- D. Extended range VLANs from 1006-4096 are stored in vlan.dat.
- E. Both normal and extended VLANs are stored in vlan.dat file.

**Correct Answer: AB**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 751**

Which normal VLAN range are valid and is stored in the vlan.dat configuration file?

- A. VLANs 1-1005
- B. VLANs 1005-2030
- C. VLANs 2094-4094
- D. VLANs 4094-8030

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 752**

Which extended VLAN range are valid and is stored in the startup configuration?

- A. VLANs 1006-4096
- B. VLANs 2006-6096
- C. VLANs 1-1005
- D. VLANs 1005-2060

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 753**

Which type of MAC address can be dropped by a switch that is configured for MAC address filtering?

- A. unicast
- B. router
- C. multicast
- D. CPU-destined

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://supportforums.cisco.com/t5/lan-switching-and-routing/mac-address-based-traffic-blocking/td-p/2688819>

**QUESTION 754**

Which feature prevents an interface from sending BPDUs on a portfast enabled port?

- A. BPDU guard
- B. PortFast
- C. root guard
- D. BPDU filtering

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 755**

Which feature do you implement so that a physical port will enter the loop-inconsistent state if it fails to receive BPDUs?

- A. loop guard
- B. loop disable
- C. root guard
- D. flex links
- E. BPDU ignore
- F. loop block

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp\\_enha.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html)

**QUESTION 756**

Which feature places a port in an err-disabled state when it receives an unanticipated BPDU?

- A. loop guard
- B. root guard
- C. BPDU guard
- D. BPDU filtering

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 757**

On which PVLAN type can host ports communicate with promiscuous ports?

- A. primary
- B. community
- C. promiscuous
- D. isolated

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 758

Which statement about the configuration of a trunk port as the source of a SPAN session is true?

- A. Only VLANs that are configured individually as SPAN sources are monitored.
- B. All VLANs in the trunk are monitored.
- C. The trunk is errdisabled automatically.
- D. All VLANs in the trunk are monitored, provided the SPAN destination port is a trunk.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 759

Which configuration do you apply to a device to place interface GigabitEthernet0/0 into VRRP group 10?

- A. 

```
interface GigabitEthernet0/0
ip address 172.16.13.2 255.255.0
standby 10 ip 172.16.13.254 255.255.255.0
standby 10 priority 120
standby 10 preempt
```
- B. 

```
interface GigabitEthernet0/0
description to Executive Offices A 08-38338
ip address 172.16.13.2 255.255.255.0
vrrp 10 ip 172.16.13.254 255.255.255.0
vrrp 10 active
```
- C. 

```
interface GigabitEthernet0/0
description to Executive Offices A 08-38338
ip address 172.16.13.2 255.255.250.0
vrrp group 10 ip 172.16.13.254 255.256.255.0
vrrp group 10 priority 120
```
- D. 

```
interface GigabitEthernet0/0
ip address 172.16.13.2 255.255.255.0
vrrp 10 ip 172.16.13.254
vrrp 10 priority 120
vrrp 10 preempt
```
- E. 

```
interface GigabitEthernet0/0
ip address 172.16.13.2 255.255.255.0
standby 10 ip 172.16.13.254
```

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 760

Which two statements about the monitored traffic in a SPAN session are true? (Choose two.)

- A. You cannot configure two separate SPAN or RSPAN source sessions with separate or overlapping sets of SPAN source ports and VLANs
- B. By default, all monitored packets are captured without the IEEE 802.1Q tag
- C. Egress SPAN monitors packets sent by the source interface before any QoS modifications
- D. Sources can be ports or VLANs or any combination in the same session
- E. By default, all monitored packets include the IEEE 802.1Q tag that they had on the source port
- F. Ingress SPAN monitors packets received by the source interface before any QoS modifications

**Correct Answer:** EF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 761

Which statement about the default behavior of a Cisco switch MAC address table is true?

- A. MAC addresses are not learned on extended VLANs.
- B. MAC addresses are aged out of the MAC table after 600 seconds.
- C. MAC addresses are associated with a VLAN.
- D. MAC address filtering is enabled on trunk ports.

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**



**Explanation/Reference:**

**QUESTION 762**

When a Layer 2 EtherChannel is configured, which statement about interaction with the Spanning Tree Protocol is true?

- A. Spanning Tree uses only the member ports for forwarding.
- B. Spanning Tree uses the port channel for forwarding.
- C. Spanning Tree uses the port channel and member ports for forwarding.
- D. Spanning Tree does not use port channels in loop prevention.

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 763**

Which command can be used to block a frame with an unknown destination MAC address from being forwarded out of an interface?

- A. switchport protected
- B. It is not forwarded if the destination MAC address is unknown.
- C. switchport port-fast
- D. switchport block unicast

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 764**

For which reason does an administrator disable MAC address learning within a VLAN?

- A. to configure a VLAN as an SVI
- B. to free up space in the MAC address table
- C. to implement port security
- D. to reduce flooding in the network

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/wireless/mwr\\_2941\\_dc/software\\_config/guide/3\\_3/2941\\_33\\_Config\\_Guide/mac\\_lrn.pdf](https://www.cisco.com/c/en/us/td/docs/wireless/mwr_2941_dc/software_config/guide/3_3/2941_33_Config_Guide/mac_lrn.pdf)

**QUESTION 765**

Which two statements about manually-configured LACP EtherChannels are true? (Choose two.)

- A. LACP negotiation must be disabled on both devices in the EtherChannel.
- B. They require Cisco Discovery Protocol.
- C. Each physical port in the EtherChannel must have the same speed and duplex settings.
- D. LACP negotiation must be disabled on one device in the EtherChannel.
- E. They use an MD5 hash for equal load balancing.
- F. If the physical port configurations on the two devices are different, the ports are placed into the errdisabled state.

**Correct Answer: AC**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 766**

Which two statements correctly describe the benefits of GLBP? (Choose two.)

- A. It can load-share LAN traffic across up to four AVFs in a GLBP group.
- B. It uses dual active AVGs for redundancy.
- C. LAN traffic can be distributed to up to six routers in a GLBP group.
- D. It supports up to 128 virtual routers per physical interface.
- E. It can automatically adjust group weighting when an interface goes down.

**Correct Answer: AE**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/en/US/docs/ios/12\\_2t/12\\_2t15/feature/guide/ft\\_glbp.html](https://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html)

**QUESTION 767**

Which two statements about native VLANs are true? (Choose two.)

- A. VLAN 1 and VLAN 1001 are native VLANs by default.
- B. The native VLAN is untagged over trunks.
- C. The native VLAN can be changed on a per port basis.
- D. Only one VLAN can be the native VLAN on a device.
- E. Cisco Discovery Protocol versions 1 and 2 can carry native VLAN information.

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 768

Refer to the exhibit.

```
Spanning-tree mode pvst
Spanning-tree etherchannel guard misconfig
```

Which effect of this configuration is true?

- A. The switch port continues to negotiate an EtherChannel even when there are configuration discrepancies between the two ports.
- B. Spanning tree blocks EtherChannel formation on the device.
- C. The switch port error disables when a port attempts to form an EtherChannel with a port that has a different configuration.
- D. Spanning tree is disabled if the switch port establishes an EtherChannel.

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstpopt.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstpopt.html)

#### QUESTION 769

Which keyword can be applied to the spanning-tree priority command that allows the IT department to adjust the timers based on the number of switches between any two end stations?

- A. root primary
- B. priority
- C. cost
- D. diameter
- E. hello-time

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_52\\_se/configuration/guide/3560scg/swstp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swstp.html)

#### QUESTION 770

Which command do you enter to enable Dynamic ARP Inspection for VLAN 15?

- A. SW1(config-vlan)# ip arp inspection vlan 15
- B. SW1(config-vlan)# ip arp inspection trust
- C. SW1(config-if)# ip arp-inspection trust
- D. SW1(config)# ip arp inspection vlan 15

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 771

Which three restrictions of port security features are true? (Choose three.)

- A. It is not supported on EtherChannel port-channel interfaces.
- B. Static MAC address assignments are not supported.
- C. It is not supported on destination SPAN ports.
- D. It is not supported on PVLAN ports.
- E. A single device supports up to two sticky MAC addresses.

**Correct Answer:** ABC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:

Follow these guidelines when configuring port security:

- A secure port cannot be a trunk port.

- A secure port cannot be a destination port for Switch Port Analyzer (SPAN).
- A secure port cannot belong to an EtherChannel port-channel interface.
- A secure port and static MAC address configuration are mutually exclusive

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port\\_sec.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/port_sec.pdf)

#### QUESTION 772

For which reason would you configure RSPAN instead of SPAN on your network?

- A. RSPAN provides more complete monitoring of the traffic on a single switch.
- B. Only RSPAN devices can monitor traffic on other device.
- C. Only RSPAN can log traffic on a VLAN that spans multiple switches.
- D. Only RSPAN supports STP on multiple switches across a campus.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 773

Which benefit of Stackwise is true?

- A. It allows multiple switches to operate independently while sharing a single management address.
- B. It enables a Layer 2 switch to be converted to a Layer 3 switch when additional switches are added to the stack.
- C. It allows multiple switches to be managed by a single management address.
- D. It supports single-chassis EtherChannel mode option.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 774

Refer to the exhibit.

```
errdisable recovery cause udd
errdisable recovery interval 15
interface Gi0/1
udld port aggressive
```

A fiber pair that is connected to Gi0/1 has been damaged. What is the result?

- A. The interface is shut down until the fiber pair is replaced.
- B. The interface is prevented from causing spanning-tree loops.
- C. After the fiber pair is replaced, the interface recovers within 15 minutes.
- D. The interfaces actively tries to fix the damaged fiber link.

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 775

Which two statements about error-disabled ports are true? (Choose two.)

- A. When a port is error-disabled, it may continue to pass management traffic.
- B. When a port is error-disabled, all traffic on the port stops.
- C. By default, error-disabled ports automatically recover once the issue is resolved.
- D. When a port is error-disabled, the port LED changes to solid orange.
- E. They can be recovered only by resetting the interface.

**Correct Answer: BD**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 776

Which statement describes the result of configuring SPAN on a Cisco device?

- A. SPAN doubles traffic internally.
- B. SPAN halves the capacity of the source port.
- C. SPAN blocks for normal use on one additional port for each configured source port.
- D. If not carefully planned, SPAN can lead to loops between source and destination ports.

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 777**

Which two statements about PortFast are true? (Choose two.)

- A. It forces the port to skip all spanning-tree states.
- B. The port is error-disabled if it attempts to move into the listening or learning states.
- C. It allows the port to skip the learning state only.
- D. The port moves immediately to the forwarding state when a device is connected.
- E. It is most appropriate for ports that provide connectivity to individual workstations or servers.

**Correct Answer:** DE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 778**

Which configuration do you apply to an interface so that a host can be placed into VLAN 593?

- A. 

```
interface GigabitEthernet0/0.593
encapsulation dot1q 593
switchport access vlan 593
```
- B. 

```
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport trunk native vlan 593
switchport access vlan 593
```
- C. 

```
interface GigabitEthernet0/0
switchport mode trunk
switchport trunk allowed vlan 593
```
- D. 

```
interface GigabitEthernet0/0
switchport mode access
switchport access vlan 593
switchport host
```

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 779**

Which security feature inspects ARP packets based on valid IP –to-MAC address bindings?

- A. IP Source Guard
- B. BPDU guard
- C. DAI
- D. port security

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 780**

```
Switch# show udld f0/1
Interface Fa0/1
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state: Disabled port
Message interval: 7
Time out interval: 5
No neighbor cache information stored

Switch# show interfaces f0/1
FastEthernet0/13 is down, line protocol is down (err-disabled)
  Hardware is Fast Ethernet, address is aaaa.bbbb.cccc (bia aaaa.bbbb.cccc)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
```

Refer to the exhibit. Which two statements about the network environment are true? (Choose two.)

- A. UDLD aggressive mode put the interface into an error-disabled state.
- B. After the error is corrected, the udld reset command recovers the disabled ports.
- C. The UDLD mode changed from normal to aggressive when the error was detected.
- D. The interface was error-disabled as the result of STP.
- E. UDLD negotiation failed when the neighbor switch went offline.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**  
Reference: <http://packetlife.net/blog/2011/mar/7/udld/>

#### QUESTION 781

Which two options are benefits of using VSS for chassis virtualization? (Choose two.)

- A. It supports GLBP to balance VSS traffic.
- B. It provides multiple points of management for redundancy and improved support.
- C. It uses a single database to manage configuration for multiple switches.
- D. It provides a single point of management for improved efficiency.
- E. It requires only one gateway per VLAN.

**Correct Answer:** DE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 782

If EtherChannel guard is configured on a device, which result happens when the device detects a misconfiguration on a connected device?

- A. Spanning tree is disabled for the VLANs associated with the EtherChannel.
- B. The port generates a syslog message.
- C. The EtherChannel configuration is removed from the running configuration of the device.
- D. The port is error disabled.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**  
Explanation:  
Understanding EtherChannel Guard  
You can use EtherChannel guard to detect an EtherChannel misconfiguration between the switch and a connected device. A misconfiguration can occur if the switch interfaces are configured in an EtherChannel, but the interfaces on the other device are not. A misconfiguration can also occur if the channel parameters are not the same at both ends of the EtherChannel. For EtherChannel configuration guidelines, see the “EtherChannel Configuration Guidelines” section.  
If the switch detects a misconfiguration on the other device, EtherChannel guard places the switch interfaces in the error-disabled state, and displays an error message.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstpopt.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstpopt.html)

#### QUESTION 783

How does the Spanning Tree Protocol determine path cost?

- A. interface hop count
- B. interface reliability
- C. interface bandwidth
- D. interface load
- E. interface delay

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 784

Which feature can protect a Layer 2 port from spoofed IP addresses?

- A. port security
- B. IP source guard
- C. uRPF
- D. DHCP snooping

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**



Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html>

#### QUESTION 785

You have recently deployed an access switch with two fiber cables that connect it to a distribution switch in EtherChannel mode. Soon after it booted up, one of the uplink ports to the distribution switch was error-disabled. Which option is the most likely reason for the problem?

- A. The switch is operating in UDLD aggressive mode and it failed to receive a UDLD message from the peer.
- B. The port-channel detected an inconsistent configuration.
- C. The switch is operating in UDLD normal mode and it failed to receive a UDLD message from the peer.
- D. Spanning tree is detected a loop.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 786

Which statement about SPAN functionality for an EtherChannel group is true?

- A. It can be configured as a SPAN source or a SPAN destination port.
- B. It can be configured as a SPAN source but not as a SPAN destination port.
- C. It can be configured as a SPAN destination but not as a SPAN source port.
- D. It cannot be configured as a SPAN source or a SPAN destination port.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Explanation:

#### Can You Configure SPAN on an EtherChannel Port?

An EtherChannel does not form if one of the ports in the bundle is a SPAN destination port. If you try to configure SPAN in this situation, the switch tells you: Channel port cannot be a Monitor Destination Port

Failed to configure span feature

You can use a port in an EtherChannel bundle as a SPAN source port.

Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html#anc63>

#### QUESTION 787

Which two statements about configuring a voice VLAN on a switch port are true? (Choose two.)

- A. The port must be operating in untrusted mode.
- B. Tagged traffic is not supported.
- C. It must be configured separately from the VLAN that carries data traffic.
- D. If the port is trusted, data traffic that passes through the Cisco IP Phone maintains its QoS values.
- E. The port must be operating in trusted mode.
- F. Cisco Discovery Protocol must be disabled on the switch port.

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 788

Which statement about the connection of two switches with several links using LACP link aggregation on IOS is true?

- A. By default, when an LACP channel is configured, the LACP channel mode is off.
- B. By default, when an LACP channel is configured, the LACP channel mode is on.
- C. By default, when an LACP channel is configured, the LACP channel mode is active.
- D. By default, when an LACP channel is configured, the LACP channel mode is passive.

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/interfaces/configuration/guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_Interfaces\\_Configuration\\_Guide/b\\_Cisco\\_Nexus\\_9000\\_Series\\_NX-OS\\_Interfaces\\_Configuration\\_Guide\\_chapter\\_0110.html#concept\\_98946DAEC5AA41B085E5D04709CDCB4B](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/interfaces/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_Interfaces_Configuration_Guide/b_Cisco_Nexus_9000_Series_NX-OS_Interfaces_Configuration_Guide_chapter_0110.html#concept_98946DAEC5AA41B085E5D04709CDCB4B)

#### QUESTION 789

Refer to the output below. Which effect of this configuration is true?

```
interface GigabitEthernet1/0
description to IT Room B 9745-173
switchport mode trunk
switchport trunk encapsulation dot1q
```

- A. It enables tagging support for 1000 VLANs, including the native VLAN.
- B. It enables tagging for up to 4096 VLANs, but tagging on the native VLAN is not supported.
- C. It prevents the port from operating with VTP.
- D. It enables a Cisco-proprietary trunking protocol.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 790

Which command do you enter to troubleshoot a misconfigured EtherChannel?

- A. CORE-SW (config-if)#**spanning-tree etherchannel guard misconfig**
- B. CORE-SW (config)#**spanning-tree etherchannel guard misconfig**
- C. CORE-SW (config-if)#**spanning-tree loopguard default**
- D. CORE-SW (config-if)#**spanning-tree guard root**

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swstpopt.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstpopt.html)

#### QUESTION 791

Which two TLVs are mandatory in LLDP advertisements? (Choose two.)

- A. Platform TLV
- B. System Capability TLV
- C. Network Policy TLV
- D. System Name TLV
- E. Native VLAN TLV

**Correct Answer:** BD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:

Following are the LLDP TLV's. Only System Capability TLV and System Name TLV are valid LLDP TLV's but they are optional, not mandatory. These are the two best answer choices based on the alternatives, perhaps the question was meant to read "Which two TLVs are optional in LLDP advertisements"

| TLV type values |                     |                 |
|-----------------|---------------------|-----------------|
| TLV type        | TLV name            | Usage in LLDPDU |
| 0               | End of LLDPDU       | Mandatory       |
| 1               | Chassis ID          | Mandatory       |
| 2               | Port ID             | Mandatory       |
| 3               | Time To Live        | Mandatory       |
| 4               | Port description    | Optional        |
| 5               | System name         | Optional        |
| 6               | System description  | Optional        |
| 7               | System capabilities | Optional        |
| 8               | Management address  | Optional        |
| 9–126           | Reserved            | -               |
| 127             | Custom TLVs         | Optional        |

#### QUESTION 792

```
DSW2#sh spanning-tree vlan 10
VLAN0010
  Spanning tree enabled protocol ieee
  Root ID    Priority      10
            Address      0013.80f9.8880
            Cost         2
            Port         9 (FastEthernet 1/0/7)
            Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec

  Bridge ID  Priority      4106 (priority 4096 sys-id-ext 10)
            Address      0018.7363.4300
            Hello Time   2 sec Max Age 20 sec Forward Delay 15 sec
            Aging Time   300

Interface Role Sts Cost Prio.Nbr Type
-----
Fa1/0/7   Root FWD 2    128.9  p2p
Fa1/0/10  Desg FWD 4    128.12 p2p
Fa1/0/11  Desg FWD 2    128.13 p2p
Fa1/0/12  Desg FWD 2    128.14 p2p

DSW2#
*Mar 3 07:29:24.854: #SPANTREE-2-BLOCK_BPUGUARD: Received BPDU on port Fa1/0/7
with BPDU Guard enabled. Disabling port.
*Mar 3 07:29:24.854: %PM-4-ERR_DISABLE: bpuguard error detected on Fa1/0/7, put
ting Fa1/0/7 in err-disable state
*Mar 3 07:29:24.879: #SPANTREE-2-BLOCK_BPUGUARD: Received BPDU on port Fa1/0/7
with BPDU Guard enabled. Disabling port.
*Mar 3 07:29:25.869: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0/7,
changed state to down
*Mar 3 07:29:26.884: %LINK-3-UPDOWN: Interface FastEthernet1/0/7, changed state to down
```

Refer to the exhibit. An engineer entered the **no spanning-tree bpduguard enable on interface Fa1/0/7** command. Which statement describes the effect of this command?

- A. Interface Fa1/0/7 remains in err-disabled state until the **shutdown/no shutdown** command is entered in the interface configuration mode.
- B. Interface Fa1/0/7 returns to an up and operational state.

- C. Interface Fa1/0/7 remains in err-disabled state until the **spanning-tree portfast bpduguard disable** command is entered in the interface configuration mode.
- D. Interface Fa1/0/7 remains in err-disabled state until the **errdisable recovery bpduguard** command is entered in the interface configuration mode.
- E. Interface Fa1/0/7 remains in err-disabled state until the **errdisable recovery cause bpduguard** command is entered in the interface configuration mode.

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 793**  
DRAG DROP

Drag and drop the statements about RSPAN VLANs from the left onto the correct section on the right.

**Select and Place:**

MAC address learning is not supported.

They are not supported with VTP.

They can be configured only on access ports.

They can be configured only on trunk ports.

They can be configured with STP only on the source port.

They can use VLAN IDs from 2 through 1005.

They can use VLAN IDs from 2 through 1024.

True of RSPAN VLANs

False of RSPAN VLAN

**Correct Answer:**

True of RSPAN VLANs

MAC address learning is not supported.

They can be configured only on trunk ports.

They can be configured with STP only on the source port.

They can use VLAN IDs from 2 through 1024.

False of RSPAN VLAN

They are not supported with VTP.

They can be configured only on access ports.

They can use VLAN IDs from 2 through 1005.

Section: Mix Questions
Explanation

Explanation/Reference:
Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_52\\_se/configuration/guide/3560scg/swspan.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swspan.html)

QUESTION 794
Which two statements about native VLANs are true? (Choose two.)

- A. All outgoing traffic without a VLAN tag is tagged with the native VLAN.
- B. All untagged traffic that arrives on the device is placed into the native VLAN.
- C. The VLAN tag is stripped from all incoming traffic that matches the native VLAN.
- D. They are propagated through VTP.
- E. The default native VLAN is VLAN 11.
- F. All incoming traffic that matches the native VLAN is dropped at the switch.

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 795
Which statement describes the result of issuing the spanning-tree portfast trunk command under interface configuration mode?

- A. The port is allowed to go into the forwarding state immediately regardless of whether the interface is configured as an access or trunk port.
- B. The port enters the errdisable state if BPDUs are received.
- C. Trunk interfaces can be configured for portfast.
- D. The portfast trunk port immediately replaces the lost root port with an alternate root port.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp\\_enha.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/stp_enha.html)

QUESTION 796
DRAG DROP
Drag and drop the statements about SPAN ports from the left onto the correct port types on the right.

Select and Place:



- It can be an EtherChannel port.
- It can be any physical Ethernet port.
- It is excluded from STP.
- It is removed from the EtherChannel group when a SPAN configuration is applied.
- It is the monitored port.
- Multiple ports can be included in a single session.

Source Port




Destination Port




Correct Answer:







Source Port

- It can be an EtherChannel port.
- Multiple ports can be included in a single session.
- It is the monitored port.

Destination Port

- It can be any physical Ethernet port.
- It is excluded from STP.
- It is removed from the EtherChannel group when a SPAN configuration is applied.

Section: Mix Questions  
Explanation

Explanation/Reference:

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_55\\_se/configuration/guide/3750xscg/swspan.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html)

#### QUESTION 797

Which feature can you enable on your network to most effectively limit unknown traffic?

- A. DHCP packet rate limiting
- B. unicast storm control
- C. multicast storm control
- D. broadcast storm control
- E. ARP packet rate limiting

Correct Answer: B

Section: Mix Questions  
Explanation

Explanation/Reference:

Explanation:

Storm control configuration:

- broadcast—Configures broadcast storm control.
- multicast—Configures multicast storm control.
- unicast—Configures unknown unicast storm control

Reference: [https://www.cisco.com/c/en/us/td/docs/wireless/asr\\_901/Configuration/Guide/b\\_asr901-scg/b\\_asr901-scg\\_chapter\\_0101001.pdf](https://www.cisco.com/c/en/us/td/docs/wireless/asr_901/Configuration/Guide/b_asr901-scg/b_asr901-scg_chapter_0101001.pdf)

#### QUESTION 798

Which command must be configured on the physical ports of a Layer 3 EtherChannel?

- A. ip address <subnet mask>
- B. switchport trunk encapsulation dot1q
- C. no switchport
- D. switchport mode access

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/3-1-1SG/configuration/guide/config/channel.pdf> page 19-7

#### QUESTION 799

Which three statements about extended VLANs are true? (Choose three.)

- A. The lowest extended VLAN number is 1006.
- B. The lowest extended VLAN number is 1002.
- C. Any VLAN ID can be used as an extended VLAN.
- D. They are recognized only by VTP version 3.
- E. They are propagated by VTP by default.
- F. They require the extended system ID to be enabled on the device.

**Correct Answer: ADF**

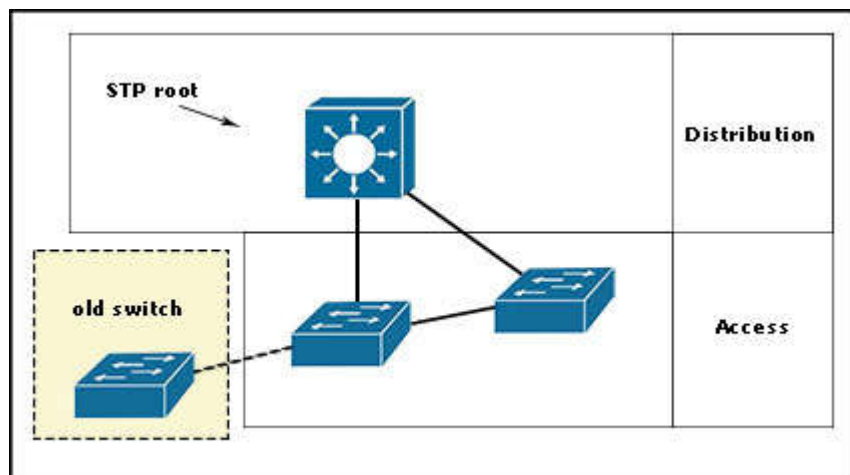
**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 800

Refer to the exhibit.



A network engineer deployed an older switch with the same spanning-tree priority as the existing root, which caused a network outage. In which two locations should the Spanning Tree Protocol root guard feature be implemented? (Choose two.)

- A. on all of the non-root switch facing ports of the access layer
- B. on Layer 3 boundaries in the distribution layer
- C. on the designated root switch downlinks to the access layer
- D. on the access layers root facing ports
- E. globally on all network switches

**Correct Answer: AC**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 801

You move a switch from a network where it performed Layer 2 switching only to a network where it performs Layer 2 switching and Layer 3 routing. You notice that the switch is showing high CPU usage and significantly degraded routing performance.

Which command sequence do you use to troubleshoot and fix the problem?

- A. #show running-config  
(config)#ip routing
- B. #show sdm prefer  
(config)#sdm prefer vlan
- C. #show sdm prefer  
(config)#sdm prefer routing
- D. #show sdm prefer  
(config)#sdm prefer default

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/68461-high-cpu-utilization-cat3750.html>

#### QUESTION 802

Which two statements about normal-range VLANs are true? (Choose two.)

- A. You can delete VLANs 1002 through 1005 in transparent mode only.
- B. The vlan.dat file is stored in RAM and copied to the NVRAM when you save the configuration.
- C. Configurations are saved in the vlan.dat file.
- D. You can add, modify, and remove configurations in VTP server mode and VTP client mode.
- E. You can add VLANs in VTP server mode.

**Correct Answer:** CE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 803

Which two statements are true of loop guard? (Choose two.)

- A. Configure loop guard on root port to help detect and isolate unidirectional link failure.
- B. Configure loop guard when root guard is enabled for optimal loop prevention mechanism.
- C. Configure loop guard on a PortFast-enabled port to ensure optimal loop prevention mechanism.
- D. Configure loop guard on a point-to-point link for an effective loop prevention mechanism.
- E. Configure loop guard to prevent root port from becoming a designated port.

**Correct Answer:** DE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 804

Which two statements about STP path cost are true? (Choose two.)

- A. The default path cost method is short.
- B. MST supports the short and long path cost methods.
- C. The default path cost method is long.
- D. MST supports only the long path cost method.
- E. The long method uses a 64-bit value for path costs.
- F. The short method uses a 32-bit value for path costs.

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/l2/spanning-tree-pathcost-method.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/l2/spanning-tree-pathcost-method.html)

#### QUESTION 805

Which command can you enter to most effectively rate-limit multicast traffic based on available bandwidth?

- A. storm-control multicast level pps 10k
- B. storm-control multicast level bps 10k
- C. storm-control multicast level 20 10
- D. storm-control multicast level 10

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 806

Which two limitations of IP Source Guard are true? (Choose two.)

- A. It is supported only on packets switched in hardware.
- B. It is supported only on ingress Layer 2 ports.
- C. It is supported only on egress Layer 3 ports.
- D. It is supported only on PAgP EtherChannels.
- E. It is supported only on ingress Layer 3 ports.

**Correct Answer:** AB  
**Section:** Mix Questions

## Explanation

### Explanation/Reference:

Explanation:

#### Restrictions for IP Source Guard

Because the IP source guard feature is supported only in hardware, IP source guard is not applied if there are insufficient hardware resources available.

These hardware resources are shared by various other ACL features that are configured on the system. The following restrictions apply to IP source guard:

- Supported only on ingress Layer 2 ports.
- Supported only in hardware; not applied to any traffic that is processed in software.
- Does not support filtering of traffic based on MAC address.
- Is not supported on private VLANs.

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy\\_swcg/ip\\_source\\_guard.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/ip_source_guard.html)

### QUESTION 807

Which statement about SPAN is true?

- A. It is an industry-standard protocol for mirroring traffic.
- B. It uses a specific VLAN to transfer mirrored traffic.
- C. SPAN destinations also can be SPAN sources.
- D. It mirrors traffic from a source port to a destination port on the same switch only.
- E. SPAN destinations participate in spanning-tree instances.

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

### Explanation/Reference:

### QUESTION 808

Refer to the output below.

```
interface FastEthernet0/1
description to server room A 76-79430
switchport trunk allowed vlan 81-97,99-121
switchport mode trunk
end
!
```

Which two commands remove VLAN 100 from the VLANs allowed on the trunk port? (Choose two.)

- A. switchport trunk allowed vlan 81-97,99,101-121
- B. no switchport trunk allowed vlan 100
- C. switchport trunk allowed vlan remove 100
- D. switchport trunk allowed vlan 81-121 remove 98,100
- E. switchport trunk vlan remove 100

**Correct Answer: AC**

**Section: Mix Questions**

**Explanation**

### Explanation/Reference:

### QUESTION 809

Which statement about the configuration of MST on an IOS switch is true?

- A. When MST is enabled, RSTP is automatically enabled and MST will use BPDU version 4, maximum of 16 instances of MST can exist.
- B. When MST is enabled, RSTP is automatically disabled and MST will use BPDU version 4, maximum of 16 instances of MST can exist.
- C. When MST is enabled, RSTP is automatically disabled and MST will use BPDU version 2, maximum of 16 instances of MST can exist.
- D. When MST is enabled, RSTP is automatically enabled and MST will use BPDU version 2, maximum of 16 instances of MST can exist.

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

### Explanation/Reference:

### QUESTION 810

Which two circumstances can cause a port to errdisable? (Choose two.)

- A. It learned a new MAC address.
- B. It is connected to a host with an NIC that is unable to recognize.
- C. It detected a peer with a matching duplex.
- D. It detected a collision.
- E. The switch incurred a port security violation.

**Correct Answer: DE**

**Section: Mix Questions**

**Explanation**

### Explanation/Reference:

There are various reasons for the interface to go into errdisable. The reason can be:

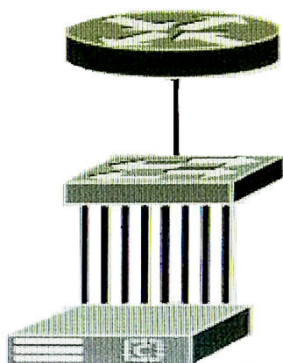
- Duplex mismatch
- Port channel misconfiguration

- BPDU guard violation
- UniDirectional Link Detection (UDLD) condition
- Late-collision detection
- Link-flap detection
- **Security violation**
- Port Aggregation Protocol (PAgP) flap
- Layer 2 Tunneling Protocol (L2TP) guard
- DHCP snooping rate-limit
- Incorrect GBIC / Small Form-Factor Pluggable (SFP) module or cable
- Address Resolution Protocol (ARP) inspection
- Inline power

References: [http://www.cisco.com/en/US/tech/tk389/tk621/technologies\\_tech\\_note09186a00806cd87b.shtml](http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00806cd87b.shtml)

#### QUESTION 811

Refer to the exhibit.



A single server in Company ABC is connected via EtherChannel to a single upstream Layer 2 switch. Which EtherChannel load balancing methods on the switch make optimal use of the redundant links as traffic flows from the router that is the default gateway to the server?

- A. source MAC address
- B. source IP address
- C. destination MAC address
- D. destination IP address

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 812

Which type of attack can be mitigated by dynamic ARP inspection?

- A. DDoS attacks
- B. viruses
- C. Trojan infiltration
- D. smurf attacks
- E. man-in-the-middle attacks
- F. worm infiltration

**Correct Answer: E**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### QUESTION 813

Which protocol is used to propagate voice VLANs to a Cisco phone?

- A. Cisco Discovery Protocol
- B. LLDP
- C. SIP
- D. SKINNY
- E. DTMF

**Correct Answer: A**

**Section: Mix Questions**

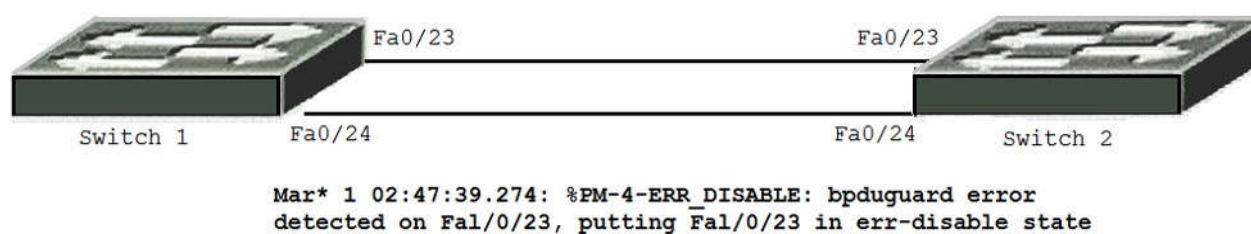
**Explanation**

**Explanation/Reference:**

#### QUESTION 814

Refer to the exhibit.





An engineer is configuring a trunking port-channel between switch 1 and switch 2 and receives an error message on switch 1. Which option corrects this error?

- A. disabling BPDU guard on interfae Fa0/23 on switch 2
- B. enabling BPDU guard on interfae Fa0/23 on switch 2
- C. disabling BPDU guard on interfae Fa0/23 on switch 1
- D. enabling BPDU guard on interfae Fa0/23 on switch 1

**Correct Answer: C**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 815

Which two statements about IP Source Guard are true? (Choose two.)

- A. When it is first enabled, it allows all IP packets except DHCP packets.
- B. When it is configured on a Layer 2 port channel, it is applied only to the port channel interface.
- C. When it is first enabled it blocks all IP packets except DHCP packets.
- D. It must be enabled globally for all ports.
- E. It works together with DHCP snooping to verify source IP packets.
- F. It is enabled automatically when DHCP snooping is enabled.

**Correct Answer: CE**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 816

Refer to the exhibit.

| DSW1#sh spanning-tree int fa1/0/7 |      |     |      |          |      |      |
|-----------------------------------|------|-----|------|----------|------|------|
| Vlan                              | Role | Sts | Cost | Prio.Nbr | Type |      |
| VLAN0001                          | Desg | FWD | 2    | 128.9    | P2p  | Edge |
| VLAN0010                          | Desg | FWD | 2    | 128.9    | P2p  | Edge |
| VLAN0020                          | Desg | FWD | 2    | 128.9    | P2p  | Edge |
| VLAN0030                          | Desg | FWD | 2    | 128.9    | P2p  | Edge |
| VLAN0040                          | Desg | FWD | 2    | 128.9    | P2p  | Edge |

Which spanning-tree feature is configured on this interface?

- A. The command **spanning-tree portfast** in the interface configuration mode was entered.
- B. The command **spanning-tree portfast trunk** in the interface configuration mode was entered.
- C. The command **shut** then a **no shutdown** in the interface configuration mode was entered.
- D. The command **spanning-tree vlan 10,20,30,40 root primary** in the interface configuration mode for faster convergence.
- E. The command **spanning-tree mst1 vlan 10,20,30,40** in the global configuration mode was entered.

**Correct Answer: D**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 817

When you connect an internal switch to an upstream provider switch, which feature is most appropriate to implement to avoid potential broadcast storms?

- A. loop guard
- B. BPDU guard
- C. flex links
- D. BPDU filter
- E. BPDU ignore

**Correct Answer: D**  
**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

**QUESTION 818**

Which two statements about 802.1q are true? (Choose two.)

- A. Each frame contains a 12-byte VLAN Identifier field
- B. Trunking devices add an 8-byte VLAN tag to all VLAN packets
- C. The header is found within the Ethernet trailer.
- D. It insert a 4-byte tag filed to the Ethernet frame.
- E. When it is enabled, the minimum Ethernet frame size is 68 bytes.

**Correct Answer:** DE

**Section:** Mix Questions

**Explanation**

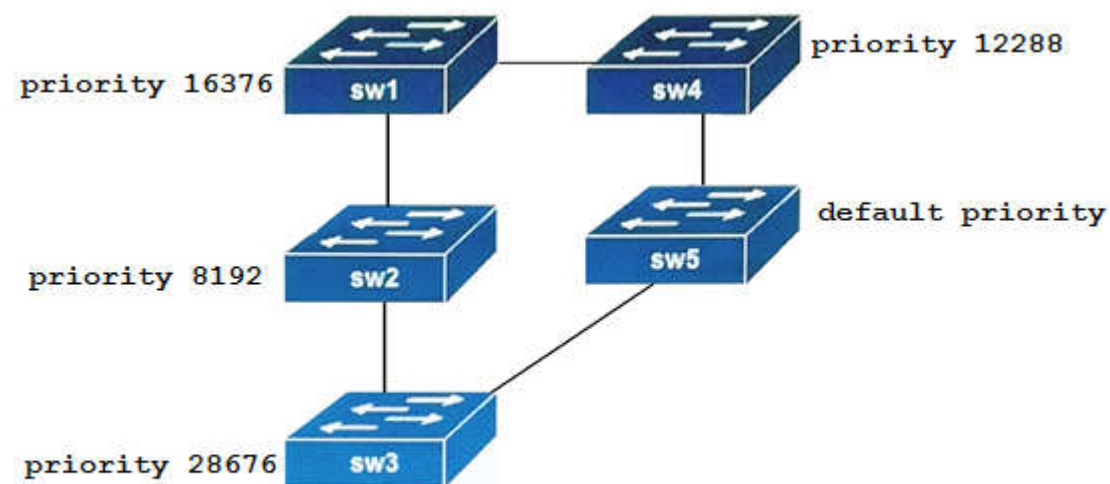
**Explanation/Reference:**

The 802.1Q tag is 4 bytes. Therefore, the resulting Ethernet frame can be as large as 1522 bytes. The minimum size of the Ethernet frame with 802.1Q tagging is 68 bytes.

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/8021q/17056-741-4.html>

**QUESTION 819**

Refer to the exhibit.



If all switches in this environment are running PVSTP+, which switch is elected as the STP root switch when a new VLAN is added to the network?

- A. switch 1
- B. switch 2
- C. switch 3
- D. switch 4
- E. switch 5

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 820**

DRAG DROP

Drag and drop the steps in the process of configuring RSPAN on an extended-range VLAN from the left onto the correct sequence on the right. Not all options are used.

**Select and Place:**

|                                                              |        |
|--------------------------------------------------------------|--------|
| Create the RSPAN VLAN on the source and destination switches | step 1 |
| Create the RSPAN VLAN on one switch only.                    | step 2 |
| Specify the destination interface                            | step 3 |
| Specify the destination RSPAN VLAN                           |        |
| Specify the source interface or VLAN                         |        |
| Specify the source RSPAN VLAN                                |        |

Correct Answer:

|                                           |                                                              |
|-------------------------------------------|--------------------------------------------------------------|
|                                           | Create the RSPAN VLAN on the source and destination switches |
| Create the RSPAN VLAN on one switch only. | Specify the source interface or VLAN                         |
| Specify the destination interface         | Specify the destination RSPAN VLAN                           |
|                                           |                                                              |
|                                           |                                                              |
| Specify the source RSPAN VLAN             |                                                              |

Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 821

Which two control protocols use the native VLAN 1 by default? (Choose two.)

- A. STP
- B. CDP
- C. LACP
- D. NTP
- E. VTP

Correct Answer: BE  
Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 822

Which technology provides a multichassis IP connection between VSS-enabled switches and downstream devices?

- A. LACP
- B. MEC
- C. ICCP
- D. LAG
- E. BFD

F. PAgP

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 823

Which two tasks must you perform on a device to ensure that an Etherchannel operates at Layer 3? (Choose two.)

- A. configure the **no switchport** command on physical interface(-s)
- B. configure EtherChannel directly on the interface
- C. configure the switchport mode trunk command on the device
- D. configure the channel-group 10 mode on command on the port channel
- E. configure the switchport mode access command on the device

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 824

Which two reasons to deploy UDLD on a switch are true? (Choose two.)

- A. It can interact with Layer 2 mechanisms to monitor the status of physical links
- B. It can prevent forwarding loops that result from unidirectional links.
- C. It can interact with Layer 1 mechanisms to monitor the status of physical links
- D. It can replace the Cisco Discovery Protocol
- E. It can replace spanning tree

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10591-77.html>

#### QUESTION 825

Which option is a benefit of configuring UDLD on a link between two switches?

- A. UDLD determines the best switching path
- B. UDLD helps prevent switching loops
- C. UDLD provides a backup mechanism for fiber
- D. UDLD removes switching loops

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 826

Refer to the output below. Which effect of this configuration is true?

```
Interface GigabitEthernet1/0
  Description to IT Room B 1406-703
  switchport mode trunk
  switchport trunk encapsulation dot1q
```

- A. It enables tagging support for 1000 VLANs, including the native VLAN.
- B. It enables a Cisco-proprietary trunking protocol.
- C. It prevents the port from operating with VTP.
- D. It enables tagging for up to 4096 VLANs, but tagging on the native VLAN is not supported.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 827

After reviewing UDLD status on switch ports, an engineer notices that the current bidirectional state for an access port is “Unknown”. Which statement describes what this indicates about the status of the port?

- A. UDLD moved into aggressive mode after inconsistent acknowledgements were detected.
- B. The UDLD port is placed in the “unknown” state for 5 seconds until the next UDLD packet is received on the interface.

C. The port is fully operational and no known issues are detected.

D. The bidirectional status of “unknown” indicates that the port will go into the disabled state because it stopped receiving UDLD packets from its neighbor.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 828**

Which three features of AAA with RADIUS are true? (Choose three.)

A. It encrypts the password for transmission

B. It encrypts the entire transmission

C. It integrates authorization and authentication functions

D. It separates authorization and authentication functions

E. It secures access to endpoint devices

F. It secures access to network devices

**Correct Answer: ACE**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 829**

If a switch that is configured globally with DHCP snooping receives a packet that has DHCP option-82 set to 192.168.1.254, how does the switch handle the packet?

A. It forwards the packet normally

B. It sends a proxy ARP request for the MAC address of 192.168.1.254

C. It replaces the source IP address of the packet with its own management IP address and forwards the packet

D. It drops the packet

E. It removes the Option-82 information from the packet and forwards the packet

F. It replaces the source MAC address of the packet with its own MAC address and forwards the packet

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

#### **QUESTION 830**

Which two statements about recovering error-disabled interfaces are true? (Choose two.)

A. Errdisable recovery is enabled by default and operates normally without additional configuration

B. Removing and reinserting network media recovers an interface from the error-disabled state

C. Reloading the switch recovers it from the error disabled state

D. If errdisable recovery is configured, the interface is recovered automatically when the root problem is corrected

E. The **show errdisable recovery** command displays the conditions for which autorecovery is enabled

**Correct Answer: DE**

**Section: Mix Questions**

**Explanation**

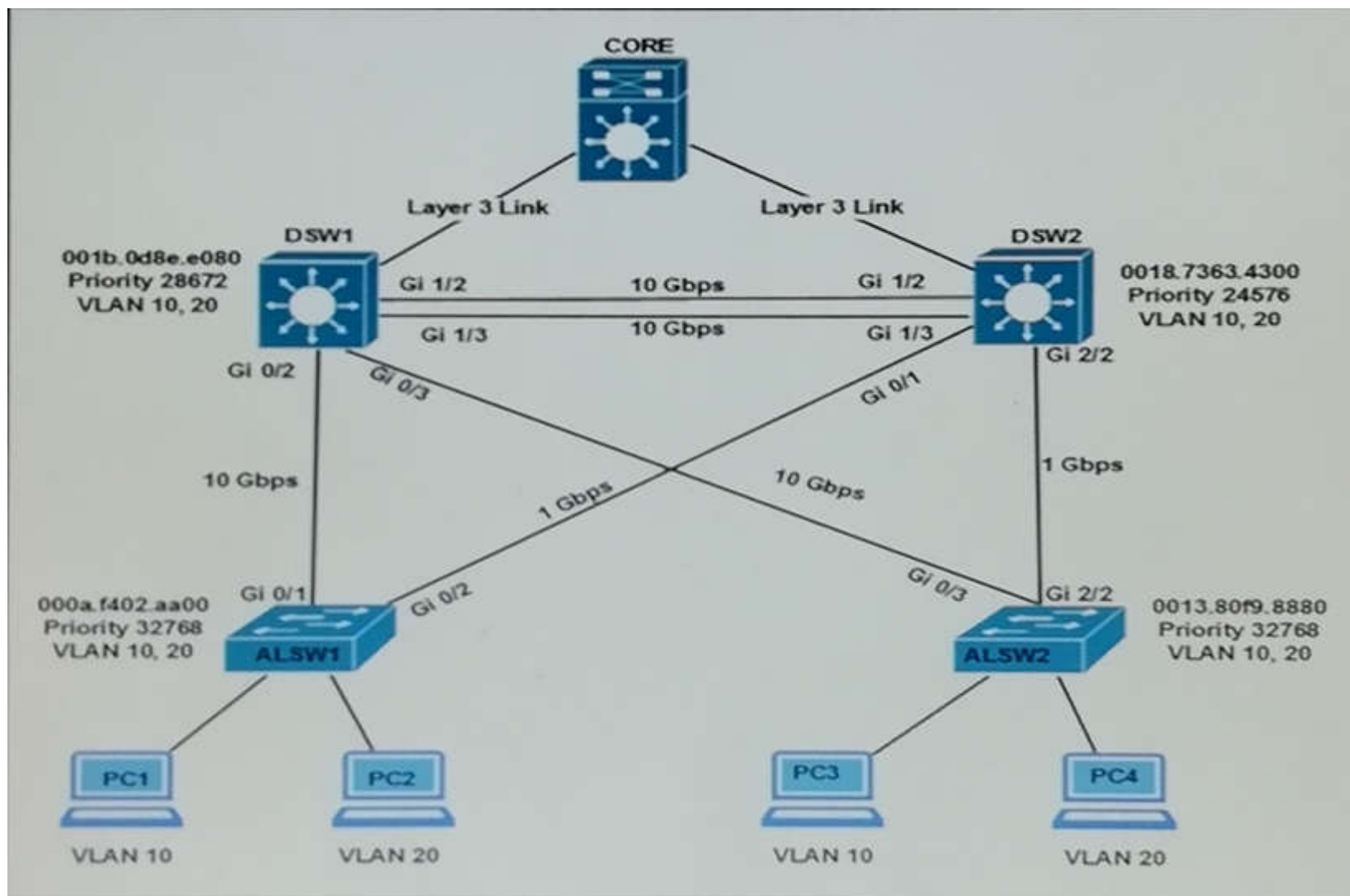
**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/69980-errdisable-recovery.html>

#### **QUESTION 831**

Refer to the exhibit. Which path does PC1 take to reach DSW1?





- A. PC1 goes from ALSW1 to reach DSW1
- B. PC1 goes from ALSW1 to DSW2 to CORE to reach DSW1
- C. PC1 goes from ALSW1 to DSW2 to reach DSW1
- D. PC1 goes from ALSW1 to DSW2 to ALSW2 to reach DSW1
- E. PC1 goes from ALSW1 to ALSW2 to reach DSW1

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 832

Which command do you enter on a device so that users are automatically placed in enable mode after they authenticate with TACACS+?

- A. `aaa authorization exec default group tacacs+ if-authenticated`
- B. `aaa authorization exec default group tacacs+ enable`
- C. `aaa authentication exec default group tacacs+ local-case`
- D. `aaa authentication exec default group tacacs+ if-authenticated`

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 833

Which effect of the line keyword entered at the end of an AAA method list is true?

- A. It overrides the **tacacs+** authentication method
- B. It overrides the **enable** authentication method
- C. It overrides the **radius** authentication method
- D. It sets a last-resort fallback authentication method

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 834

Refer to the output below. Which two effect of this configuration are true? (Choose two.)

```

!
interface GigabitEthernet1/1
description to Accounting Floor A 0506-363
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 2, 4, 6, 8
switchport trunk native vlan 2
switchport mode trunk
end
!

```

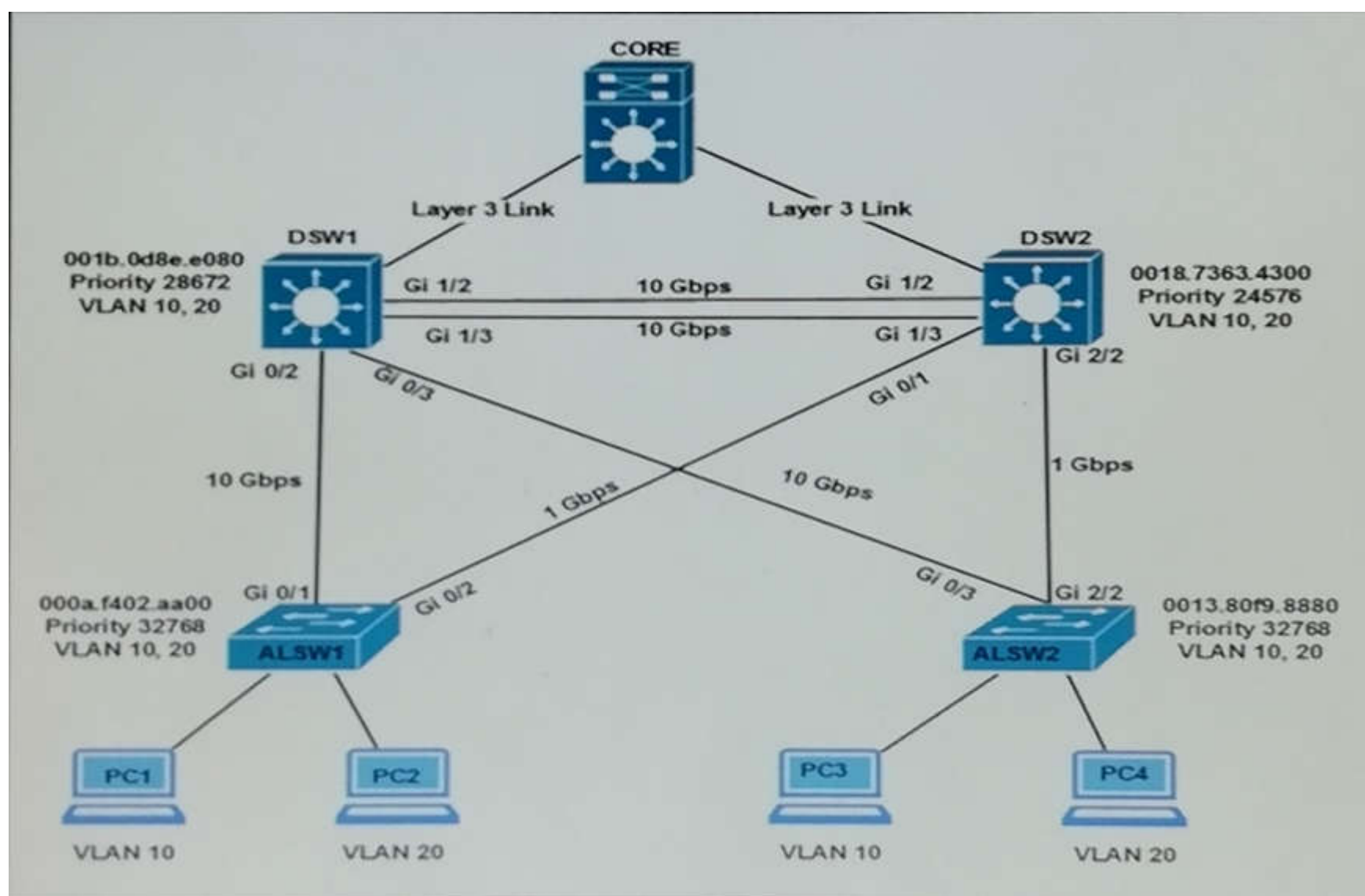
- A. Data on VLANs 4, 6, and 8 remains untagged
- B. The device adds a 4-byte VLAN tag to data on VLAN 2 only
- C. The device adds an 8-byte VLAN tag to data on VLAN 2
- D. Data on VLAN 2 remains untagged
- E. The switch adds a 4-byte VLAN tag to data on VLANs 4, 6 and 8

**Correct Answer:** DE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 835

Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10? (Choose two.)



- A. DSW1(config)#spanning-tree vlan 10 priority root
- B. DSW1(config)#spanning-tree vlan 10 port-priority 0
- C. DSW1(config)#spanning-tree vlan 10 priority 4096
- D. DSW1(config)#spanning-tree vlan 20 priority 0
- E. DSW2(config)#spanning-tree vlan 10 priority 61440

**Correct Answer:** AC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 836

Which two configuration requirements for port security are true? (Choose two.)

- A. Port security must be enabled at the global level
- B. Port security must be enabled at the port level
- C. The port must be part of a trunk
- D. The port must be a SPAN port

- E. The port must be part of an EtherChannel bundle
- F. The port must be in access mode

**Correct Answer:** BF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 837

To which VLAN is a dynamic access port assigned by default?

- A. the native VLAN
- B. none, until the VLAN membership of the port is discovered
- C. the same VLAN as the VLAN membership policy server
- D. VLAN 1, the default VLAN

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 838

Which two statements about sticky MAC address learning are true? (Choose two.)

- A. A single device can learn up to three sticky MAC addresses
- B. Learned addresses are saved to the running configuration by default
- C. Learned addresses are saved to the startup configuration file by default
- D. It can be used only on devices that operate in a single layer
- E. Devices can learn sticky MAC addresses dynamically
- F. Learned addresses are automatically preserved when the device reboots

**Correct Answer:** BE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 839

Which security violation mode drops packets with unknown source addresses and increments the violation counter?

- A. restrict
- B. shutdown
- C. drop
- D. protect
- E. inhibit

**Correct Answer:** A  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 840

Which two statements about isolated private VLAN ports are true? (Choose two.)

- A. They can communicate only with other ports in the private VLAN
- B. They can communicate only with promiscuous ports
- C. They can be configured on only port on a device
- D. They can be configured on the EtherChannel ports
- E. They can be configured on more than one port in the same VLAN

**Correct Answer:** BE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Explanation:

An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html>

#### QUESTION 841

Which two statements about TACACS+ are true? (Choose two.)

- A. It is a Cisco-proprietary technology
- B. It supports several less-common protocols in addition to IP
- C. It is backwards-compatible with TACACS

- D. It is more reliable than RADIUS because it communicates with UDP packets
- E. It encrypts only the packet header
- F. It combines accounting and authorization functions

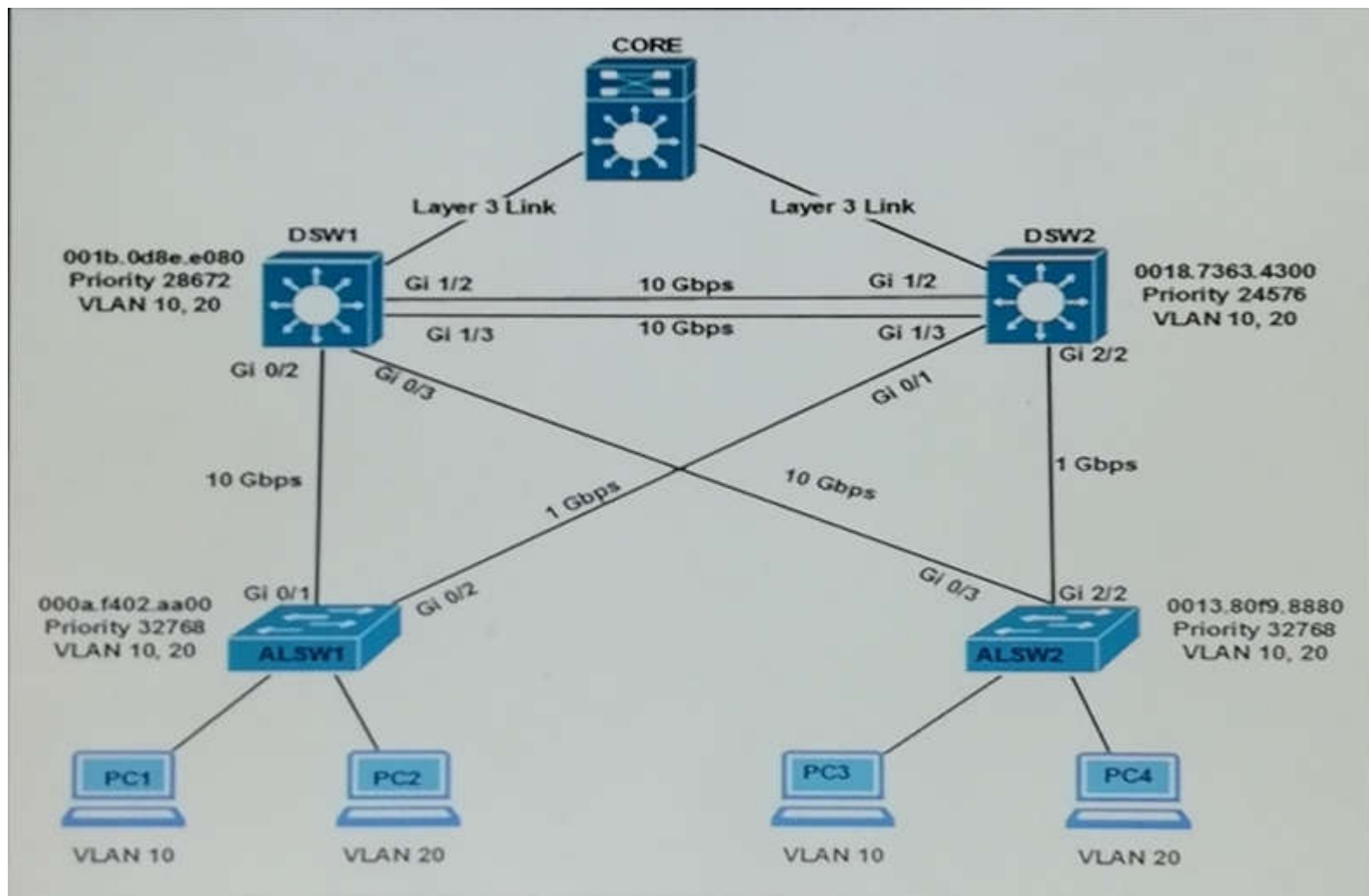
**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html>

#### QUESTION 842

Refer to the exhibit. All switches are configured with the default port priority value. Which two commands ensure that traffic from PC1 is forwarded over the Gi1/3 trunk port between DSW1 and DSW2? (Choose two.)



- A. DSW1(config-if)#spanning-tree port-priority 16
- B. DSW1(config-if)#spanning-tree port-priority 0
- C. DSW1(config)#interface gi1/3
- D. DSW2(config-if)#spanning-tree port-priority 16
- E. DSW2(config)#interface gi1/3
- F. DSW2(config-if)#spanning-tree port-priority 128

**Correct Answer:** DE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 843

Which two tasks must you perform to configure DHCP snooping on a device? (Choose two.)

- A. Enable DHCP packet validation on the device
- B. Enable DHCP option 82
- C. Enable DHCP snooping on the VLAN
- D. Enable DHCP snooping globally
- E. Enable VRF support for the DHCP relay agent

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4\\_1/nx-os/security/configuration/guide/sec\\_nx-os-cfg/sec\\_dhcp Snoop.html](https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_dhcp Snoop.html)

#### QUESTION 844

Which two commands configure RSPAN to capture incoming and outgoing traffic on a single interface? (Choose two.)

- A. monitor session 1 source interface gigabitethernet1/0/2 both
- B. monitor session 1 destination remote vlan 910

- C. monitor session 1 source interface gigabitethernet1/0/2 tx
- D. monitor session 1 source interface gigabitethernet1/0/1 rx
- E. monitor session 1 destination interface gigabitethernet1/0/2 rx

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 845

When the switches in a Cisco StackWise stack elect a new master switch, which value is used as the primary selector?

- A. lowest MAC address
- B. highest MAC address
- C. highest administrator-assigned priority
- D. lowest uptime

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 846

Which command overrides the default priority of frames on an IP phone?

- A. mls qos trust cos
- B. mls qos trust dscp
- C. priority-queue out
- D. switchport priority extend trust

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/l2/switchport-priority-extend.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/l2/switchport-priority-extend.html)

#### QUESTION 847

If all switches in a network have the same spanning-tree priority, which switch is elected as the root bridge?

- A. the switch with the highest physical interface IP address
- B. the switch with the lowest MAC address
- C. the switch with the highest MAC address
- D. the switch with the lowest loopback interface IP address

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 848

Which command displays the current SDM template?

- A. show sdm prefer layer-2
- B. show sdm prefer default
- C. show sdm prefer
- D. show sdm prefer routing

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x\\_3560x/software/release/12-2\\_53\\_se/configuration/guide/3750xscg/swsdm.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_53_se/configuration/guide/3750xscg/swsdm.html)

#### QUESTION 849

Which type of port can serve as a Cisco StackWise Virtual link?

- A. a switched port only
- B. a downlink port only
- C. any physical port
- D. an uplink port only

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**



Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration\\_guide/b\\_166\\_ha\\_9500/b\\_166\\_ha\\_9500\\_chapter\\_01.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration_guide/b_166_ha_9500/b_166_ha_9500_chapter_01.pdf)

#### QUESTION 850

Which two commands display trunking information on one or more Ethernet interfaces? (Choose two.)

- A. show interface switchport
- B. show interfaces
- C. show interface brief
- D. show interface trunk
- E. show interfaces summary

**Correct Answer:** AD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 851

Which two statements about configuring VLANs on switches in VTP server mode are true? (Choose two.)

- A. Newly configured VLANs remain in the down state until they are manually enabled
- B. The first VLAN configured on a switch becomes the native VLAN
- C. Devices in a topology without a router can communicate only with other devices on the same VLAN
- D. Switches in the same domain propagate their VLAN configurations over VTP
- E. VLANs must be configured individually

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 852

Which form of centralized device authentication allows each AAA feature to function separately?

- A. local database
- B. TACACS+
- C. Kerberos
- D. RADIUS

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 853

Which command enables you to determine whether any interface on a device was shut down as a result of a port security violation?

- A. show interface err-disabled status
- B. show port-security address
- C. show errdisable detect
- D. show port-security

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 854

Which two commands must you use to configure an interface to send traffic from a non-default native VLAN across a link that supports all VLANs? (Choose two.)

- A. switchport mode trunk
- B. encapsulation dot1Q 90 native
- C. switchport trunk native vlan 90
- D. switchport access vlan 90
- E. switchport access vlan 1

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 855

Which three features of AAA with TACACS+ are true? (Choose three.)

- A. It separates authorization and authentication functions
- B. It secures access to endpoint devices
- C. It integrates authorization and authentication functions
- D. It encrypts the password for transmission
- E. It secures access to network devices
- F. It encrypts the entire transmission

**Correct Answer:** AEF

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 856

Which two statements about VRRP object tracking are true? (Choose two.)

- A. The VRRP interface priority must be manually configured by the administrator
- B. VRRP supports only interface tracking
- C. VRRP can track the status of interfaces and routes
- D. The priority of a VRRP device can change in accordance with the up or down status of a VRRP object
- E. A VRRP group can track only one object at a time

**Correct Answer:** CD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 857

Which command configures all access ports on a switch to immediately enter the forwarding state when the switch is reset?

- A. spanning-tree portfast bpdufilter default
- B. spanning-tree portfast default
- C. spanning-tree portfast bpduguard default
- D. spanning-tree portfast

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 858

Which Cisco technology provides network redundancy by combining two physically separate switches to a single logical switch?

- A. VSS
- B. PAGP
- C. LACP
- D. IPPC

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 859

Which statement about local database device authentication is true?

- A. It can be used as a fallback authentication method when the connection to the remote network access server fails.
- B. It supports the full functionality of the AAA accounting feature.
- C. It is primarily used for authentication without usernames.
- D. It is most appropriate for authentication on a large network with many end users.

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 860

Which type of load balancing is most appropriate for an EtherChannel that passes traffic from multiple sources to a single end device?

- A. destination MAC address forwarding
- B. source MAC address forwarding
- C. source and destination IP address forwarding
- D. destination IP address forwarding

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 861**

Which command configures an interface to accept LLDP packets without enabling the interface to send the packets?

- A. **lldp receive**
- B. **lldp tlv-select**
- C. **lldp run**
- D. **lldp transmit**

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/46sg/configuration/guide/Wrapper-46SG/swlldp.pdf>

**QUESTION 862**

In which UDLD mode does a link remain up, even when a unidirectional link failure is detected?

- A. enable
- B. normal
- C. aggressive
- D. reset

**Correct Answer: B**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/lan-switching/spanning-tree-protocol/10591-77.html>

**QUESTION 863**

Which two tasks must you perform to correctly configure IP Source Guard on a switch? (Choose two.)

- A. Configure the **ip verify source vlan dhcp-snooping** command
- B. Enable DHCP option 82.
- C. Enable DHCP snooping on the switch.
- D. Configure the DHCP snooping relay.
- E. Enable DHCP packet validation on the device.

**Correct Answer: AB**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/dhcp.html#wp1098774>

**QUESTION 864**

Which VTP mode must you configure on a VTP domain so that the switch with the highest VTP configuration revision number in the domain propagates VLAN information to the other switches?

- A. client mode
- B. off mode
- C. transparent mode
- D. server mode

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_52\\_se/configuration/guide/3560scg/swvtp.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swvtp.html)

**QUESTION 865**

Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)

```
R1
interface GigabitEthernet0/0
ip address 192.168.250.2 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 120
```

```
R2
interface GigabitEthernet0/0
ip address 192.168.250.3 255.255.255.0
standby 20 ip 192.168.250.1
standby 20 priority 110
```

- A. R1 becomes the standby router.
- B. If R1 goes down, R2 becomes active and remains the active device when R1 comes back online.
- C. R1 becomes the active router.
- D. If R2 goes down, R1 becomes active but reverts to standby when R2 comes back online.
- E. Hello messages are sent to multicast address 224.0.0.5.
- F. If R1 goes down, R2 becomes active but reverts to standby when R1 comes back online.

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/10583-62.html>

#### QUESTION 866

Which AAA authorization method uses a vendor-neutral directory information protocol?

- A. TACACS+
- B. Kerberos
- C. RADIUS
- D. LDAP

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 867

Which two statements about RADIUS are true? (Choose two.)

- A. It is less secure than TACACS+ because it encrypts only the user name and password.
- B. It combines authentication and accounting functions.
- C. It uses UDP packets to communicate.
- D. It supports several less-common protocols in addition to IP.
- E. It combines authentication and authorization functions.

**Correct Answer:** CE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/security/vpn/remote-authentication-dial-user-service-radius/13838-10.html>

#### QUESTION 868

Which two statements about source port monitoring in SPAN are true? (Choose two.)

- A. It can monitor individual interfaces within a port channel.
- B. It can monitor only FastEthernet and GigabitEthernet port types.
- C. The entire EtherChannel must be monitored.
- D. Traffic through a destination port can be copied and included in the SPAN session.
- E. It can monitor ingress and egress traffic.

**Correct Answer:** AE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_55\\_se/configuration/guide/3560\\_scg/swspan.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_55_se/configuration/guide/3560_scg/swspan.pdf)

**QUESTION 869**

Which command identifies the learned addresses in the MAC address table for a device?

- A. show mac address-table multicast
- B. show mac address-table dynamic
- C. show mac address-table move update
- D. show mac address-table static

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/m/en\\_us/techdoc/dc/reference/cli/nxos/commands/l2/show-mac-address-table.html](https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/l2/show-mac-address-table.html)

**QUESTION 870**

How many active virtual gateways can each GLBP group support?

- A. 1
- B. 2
- C. 4
- D. 16

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\\_fhrp/configuration/xr-3s/fhrp-xr-3s-book/fhrp-glb.html#GUID-6536F55B-44C4-4772-B846-1D81A3AAAFCD](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xr-3s/fhrp-xr-3s-book/fhrp-glb.html#GUID-6536F55B-44C4-4772-B846-1D81A3AAAFCD)

**QUESTION 871**

Which two statements about the local user database are true? (Choose two.)

- A. It can be used as the only method of authentication or as a backup for other methods.
- B. It can store passwords in clear text only.
- C. It can be configured to grant a user-specific privilege level.
- D. For console connections, it can be used only as a backup authentication method.
- E. For VTY connections, it can be used only as a backup authentication method.

**Correct Answer:** AC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 872**

Which two commands display the VLANs that are present in the VLAN database? (Choose two.)

- A. show vlan database
- B. show vlan id
- C. show vlan brief
- D. show running-config
- E. show vlan

**Correct Answer:** AE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 873**

Refer to the exhibit. You have applied these configurations to Switches A, B, C, and D respectively, and the switches are connected to one another on a trunk port that is passing all VLAN traffic.

Which statement about traffic on the network is true?



```
Switch A
SwitchA#configure terminal
SwitchA#(config)#interface FastEthernet 0/1
SwitchA(config-if) #switchport mode access
SwitchA(config-if)#switchport access vlan 10

Switch B
SwitchB#configure terminal
SwitchB#(config)#interface FastEthernet 0/1
SwitchB(config-if) #switchport mode access
SwitchB(config-if)#switchport access vlan 10

Switch C
SwitchC#configure terminal
SwitchC#(config)#interface FastEthernet 0/1
SwitchC(config-if) #switchport mode access
SwitchC(config-if)#switchport access vlan 10

Switch D
SwitchD#configure terminal
SwitchD#(config)#interface FastEthernet 0/1
SwitchD(config-if) #switchport mode access
SwitchD(config-if)#switchport access vlan 20
```

- A. Hosts on all four switches can communicate normally with one another on VLAN 10 only.
- B. Unless a Layer 3 device is installed, hosts on any of the switches will be able to communicate only with other hosts on the same switch.
- C. Hosts on all four switches can communicate normally with one another over the trunk port.
- D. Unless a Layer 3 device is installed, hosts on the FastEthernet 0/1 interface of switch D will be unable to communicate with hosts on the other switches.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 874

Which two tasks must you perform to enable AAA operations with a remote security database? (Choose two.)

- A. Configure SSH to provide remote access to network equipment.
- B. Configure Cisco Discovery Protocol on all interfaces used for authentication.
- C. Configure user profiles on the remote security database.
- D. Configure network equipment to query the remote security database.
- E. Configure a user profile in the local database of each device to which the user will have access.

**Correct Answer:** CD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 875

DRAG DROP

Drag and drop the statements from the left onto the correct first-hop redundancy protocols on the right.

**Select and Place:**

requires a unique IP address to use as the virtual IP address

uses multicast address of 224.0.0.102

tracks the reachability of an IP address

uses IP protocol 112

uses the physical IP address of the interface as the virtual IP address

uses a virtual MAC address that begins with 0000.0C9F.F000

### HSRP

### VRRP

Correct Answer:

### HSRP

uses multicast address of 224.0.0.102

tracks the reachability of an IP address

uses a virtual MAC address that begins with 0000.0C9F.F000

### VRRP

requires a unique IP address to use as the virtual IP address

uses IP protocol 112

uses the physical IP address of the interface as the virtual IP address

Section: Mix Questions  
Explanation

Explanation/Reference:

#### QUESTION 876

Which two commands displays IP Source Guard bindings? (Choose two.)

- A. show ip verify source
- B. show ip source binding
- C. show ip dhcp snooping database

- D. show ip guard source
- E. show ip dhcp binding

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15\\_0\\_sy\\_swcg/ip\\_source\\_guard.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-0SY/configuration/guide/15_0_sy_swcg/ip_source_guard.pdf)

#### QUESTION 877

Which two features are new in VTPv3? (Choose two.)

- A. support for token ring VLANs.
- B. private VLAN propagation
- C. using multiple switches in the server role
- D. transparent mode
- E. extended VLAN support

**Correct Answer:** BE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: <http://brbccie.blogspot.com/2014/07/vtp-v3.html>

#### QUESTION 878

Which device type can act as a client in a system that uses TACACS+?

- A. end user wireless device
- B. router
- C. end user workstation
- D. AD server

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 879

Which command disables spanning tree on multiple ports?

- A. no spanning-tree mode mst
- B. no spanning-tree mode pvst
- C. no spanning-tree vlan <vlan\_range>
- D. no spanning-tree mode rapid-pvst

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 880

Which command sequence do you enter to configure an RSPAN VLAN?

- A. vlan 51  
name RSPAN
- B. vlan 4097 name RSPAN
- C. vlan 4097 remote-span
- D. vlan 51  
remote-span

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2\\_52\\_se/configuration/guide/3560scg/swspan.html](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3560/software/release/12-2_52_se/configuration/guide/3560scg/swspan.html)

#### QUESTION 881

In which EtherChannel mode does a port receive and respond to PAgP messages without initiating EtherChannel communication?

- A. on
- B. auto
- C. active
- D. desirable

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 882**

Which option is a primary difference between HSRP and GLBP?

- A. Only GLBP supports gateway load balancing over multiple routers.
- B. Only HSRP can use multiple MAC addresses to provide gateway load balancing over multiple routers.
- C. Only HSRP uses multiple virtual IP addresses to provide gateway redundancy in a single standby group.
- D. Only GLBP uses a router BIA to provide gateway redundancy.

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 883**

Which statement describes what a port that is configured as an access port does if it receives an 802.1Q tagged frame?

- A. It drops the frame
- B. It removes the tag and forwards the frame in the VLAN assigned to the port.
- C. It err-disables the port.
- D. It passes the frame on to the VLAN that the frame is tagged for.

**Correct Answer: A**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 884**

Which two commands enable you to determine the native VLAN that is configured on an interface? (Choose two.)

- A. show interface status
- B. show interface trunk
- C. show interface brief
- D. show interfaces
- E. show running-config

**Correct Answer: BC**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

**QUESTION 885**

Which feature is new in RPVST+?

- A. Only the root bridge sends configuration BPDUs.
- B. BackboneFast is implemented.
- C. All ports can generate and send BPDUs.
- D. UplinkFast is implemented.

**Correct Answer: C**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/72836-rapidpvst-mig-config.html>

**QUESTION 886**

Which command enables a RADIUS server configuration to use vendor-proprietary attributes?

- A. radius-server configure-nas
- B. radius-server attribute nas-port extended
- C. radius-server vsa send authentication
- D. radius-server host non-standard

**Correct Answer: D**

**Section: Mix Questions**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cisco.com/c/dam/en/us/td/docs/routers/asr920/configuration/guide/sec-usr-rad/16-6-1/b-sec-usr-rad-xe-16-6-asr920.html>

**QUESTION 887**

Which two statements about configuring EtherChannels are true? (Choose two.)

- A. They can be configured with the **no switchport** command to place them in Layer 3 mode.
- B. They can be configured to send Layer 2 packets.
- C. They can be configured to operate with up to links in a single channel.

- D. They can be configured to passively negotiate a channel with a connected peer.
- E. They can be configured to load-balance traffic based on Layer 7 information.

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 888

Which two features does TACACS+ support? (Choose two.)

- A. PAP and CHAP authentication
- B. decentralizing network access management, reducing the potential impact of a security breach to a central device
- C. encrypting the entire TCP packet containing TACACS+ information
- D. UDP communication between the network access server and the security server
- E. combining authorization and authentication to streamline AAA services

**Correct Answer:** AC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 889

Which statement about VLAN pruning on trunk ports is true?

- A. Manually pruning extended VLANs increases switch security.
- B. Manually pruning VLANs reduces unnecessary forwarding of broadcast traffic.
- C. Broadcast traffic for a manually pruned VLAN is allowed to cross the trunk port.
- D. VLANs can be pruned only via VTP pruning.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 890

Which statement about VSPAN is true?

- A. It can monitor token ring VLANs.
- B. It can monitor ingress traffic on the source VLAN.
- C. It sends all VLAN traffic to the destination port regardless of the VLAN's status.
- D. It can monitor destination port traffic that belongs to a source VLAN.

**Correct Answer:** B  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 891

Which two commands verify the DHCP snooping configuration on a device? (Choose two.)

- A. show ip dhcp pool
- B. show ip dhcp snooping
- C. show running-config | include shooping
- D. show ip dhcp relay
- E. clear ip dhcp snooping binding

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

#### QUESTION 892

Which statement about Cisco StackWise is true?

- A. If a single interconnect cable in the stack fails, the stack can continue to operate at full bandwidth.
- B. When a new switch is added, the master switch suspends traffic forwarding until the new switch is updated with the latest running configuration.
- C. The stack elects a master switch and standby switch to support rapid failover.
- D. The entire stack communicates using a single management IP address.

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**



**QUESTION 893**

Which switch management feature can you configure to drop traffic from specific source or destination addresses?

- A. MAC threshold notification traps
- B. unicast MAC address filtering
- C. static address entries
- D. switchport port security

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 894**

In a Cisco StackWise Virtual environment, which planes on the component devices are virtually combined in the common logical switch?

- A. control and data only
- B. management and data only
- C. control, data, and management
- D. control and management only

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 895**

You are configuring dynamic ARP inspection. Which command must you configure on the device to detect unexpected IP addresses in the ARP packet?

- A. ip verify source
- B. ip arp inspection validate ip
- C. ip arp inspection trust
- D. ip arp inspection vlan

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration\\_guide/sec/b\\_166\\_sec\\_9500\\_cg/configuring\\_dynamic\\_arp\\_inspection.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-6/configuration_guide/sec/b_166_sec_9500_cg/configuring_dynamic_arp_inspection.pdf)

**QUESTION 896**

Which two commands add VLAN 20 to the VLAN configuration file? (Choose two.)

- A. switch(config-if)#switchport access vlan 20
- B. switch(config)#vlan configuration 20
- C. switch(config)#interface vlan 20
- D. switch(config-if)#switchport trunk allowed vlan 20
- E. switch(config)#vlan 20

**Correct Answer:** CE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 897**

Refer to the output below. Which two effects of this configuration are true? (Choose two.)

```
!
interface GigabitEthernet1/1
  description to Accounting Floor A 8155-198
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2, 4, 6, 8
  switchport trunk native vlan 2
  switchport mode trunk
end
!
```

- A. data on VLAN 2 remains untagged
- B. The switch adds a 4-byte VLAN tag to data on VLANs 4, 6 and 8.
- C. The device adds an 8-byte VLAN tag to data on VLAN 2.
- D. Data on VLANs 4, 6, and 8 remains untagged.
- E. The device adds a 4-byte VLAN tag to data on VLAN 2 only.

**Correct Answer:** AB  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 898**  
Refer to the exhibit.

|                                                                                                                            |                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Router A</b><br><b>interface GigabitEthernet 1/0</b><br><b>ip address 192.168.0.1 255.255.255.0 vrrp 1 priority 120</b> | <b>Router C</b><br><b>interface GigabitEthernet 1/0</b><br><b>ip address 192.168.0.3 255.255.255.0 vrrp 1 priority 130</b> |
| <b>Router B</b><br><b>interface GigabitEthernet 1/0</b><br><b>ip address 192.168.0.2 255.255.255.0 vrrp 1 priority 100</b> | <b>Router B</b><br><b>interface GigabitEthernet 1/0</b><br><b>ip address 192.168.0.2 255.255.255.0 vrrp 1 priority 90</b>  |

Which router is elected as the VRRP virtual router master?

- A. router D
- B. router B
- C. router A
- D. router C

**Correct Answer:** D  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**  
Explanation:  
Router C has the Highest pritority.

**QUESTION 899**  
Which command prevents all access ports on a switch from sending or receiving BPDUs?

- A. spanning-tree bpdufilter default
- B. spanning-tree bpdufilter enable
- C. spanning-tree portfast bpdufilter default
- D. spanning-tree portfast bpduguard default

**Correct Answer:** C  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 900**  
Which two statements about UDLD aggressive mode are true? (Choose two.)

- A. UDLD automatically chooses the messaging interval based on the configured timers.
- B. If a unidirectional link is detected, the port stake is determined by spanning tree.
- C. If a unidirectional link is detected, the port state is changed to errdisable.
- D. UDLD attempts to re-establish a downed link one time before declaring the link down.
- E. The UDLS detection timer is four times the messaging interval by default.
- F. UDLD messages are sent every 15 seconds.

**Correct Answer:** CF  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 901**  
Which two statements about LLDP are true? (Choose two.)

- A. When it is enabled on a switch, Cisco Discovery Protocol must be disabled.
- B. Switches can run LLDP and Cisco Discovery Protocol simultaneously.
- C. Devices with LLDP configured send advertisement messages to a multicast address on a periodic basis.
- D. When LLDP is enabled globally, it is enabled on all ports including tunnel ports.
- E. Devices with LLDP configured send advertisement messages to a unicast address on a periodic basis.

**Correct Answer:** BC  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 902**

Which errdisable recovery command option enables a device to recover from a potential loop condition?

- A. udd
- B. security-violation
- C. link-flap
- D. dtp-flap

**Correct Answer:** A

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 903**

Which two statements about VTP are true? (Choose two.)

- A. VTP pruning can be configured on all VLANs.
- B. A configuration revision number is included in VTP packets.
- C. When you update from VTP version 1 to VTP version 2, the switch must be reloaded.
- D. Advertisements are sent periodically from trunk ports to a multicast address.

**Correct Answer:** BD

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 904**

Which two statements about MAC address learning are true? (Choose two.)

- A. It can be disabled only on nonmanagement interfaces.
- B. The administrator must disable MAC address learning only on VLANs with exactly two ports.
- C. It can be disabled globally and then reactivated on selected VLANs.
- D. It can be disabled only on secure ports.
- E. It must be disabled on SVIs.

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 905**

You have added a new switch to a Cisco StackWise stack. If the previous master switch remains the master switch after the master election, which action does the master take?

- A. It clears the MAC table of the stack and relearns the attached devices.
- B. It removes any Layer 3 configuration on the new switch to maintain normal Layer 2 functionality on the stack.
- C. It checks the IOS and running configuration of the new switch and updates them if necessary to match the other switches in the stack.
- D. It suspends traffic forwarding until the new switch is updated with the current running configuration of the stack.

**Correct Answer:** C

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 906**

Which HSRP feature allows a router to take over as the active router when it is configured with a higher priority?

- A. use-BIA
- B. HSRP groups
- C. tracking
- D. preemption

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 907**

You are configuring an interface, and you want to enable Layer 3 mode on an EtherChannel. Which task must you perform?

- A. issue the **no switchport** command
- B. Set the channel group to **desirable**
- C. Set the channel group to **active**

D. Issue the **ip address** command

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 908

Which statement about EtherChannels are true?

- A. Ports in on mode accept PAgP requests.
- B. A port in auto mode can form an Ether Channel with another port in auto mode.
- C. Ports in on mode accept LACP requests.
- D. PAgP is a Cisco-proprietary technology.

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 909

You are configuring Layer 2 EtherChannel, and you want a PAgP port channel to come up only if the device on the other end is sending negotiations. Which keyword must you see?

- A. desirable
- B. auto
- C. active
- D. on

**Correct Answer:** B

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 910

Which command enables you to determine the spanning-tree guard features that are enabled globally?

- A. **show spanning-tree**
- B. **show spanning-tree summary**
- C. **show spanning-tree active**
- D. **show spanning-tree detail**

**Correct Answer:** D

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 911

Which two statements about the VLAN database are true? (Choose two.)

- A. It supports VLANs 1 to 1001.
- B. It supports extended VLANs.
- C. VLAN information is stored in the running configuration.
- D. VLAN IDs can be duplicated, but their names must be unique.
- E. If the switch is in VTP transparent mode, the VLAN can be configured if it is in VLAN database mode.

**Correct Answer:** AE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

#### QUESTION 912

What are two advantages of LLDP over Cisco Discovery Protocol? (Choose two.)

- A. LLDP supports Frame Relay.
- B. LLDP supports ATM.
- C. LLDP is vendor-agnostic.
- D. LLDP supports checksums.
- E. LLDP supports topology-change notification.

**Correct Answer:** CE

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

Reference: [https://www.cisco.com/en/US/technologies/tk652/tk701/technologies\\_white\\_paper0900aecd804cd46d.html](https://www.cisco.com/en/US/technologies/tk652/tk701/technologies_white_paper0900aecd804cd46d.html)

**QUESTION 913**

Which two commands configure SPAN to monitor outgoing traffic across multiple interfaces? (Choose two.)

- A. `monitor session 1 destination interface gigabitethernet1/0/2 rx`
- B. `monitor session 1 source vlan 10 - 20 tx`
- C. `monitor session 1 destination interface gigabitethernet1/0/2`
- D. `monitor session 1 source interface gigabitethernet1/0/1 tx`
- E. `monitor session 1 source interface gigabitethernet1/0/1 rx`

**Correct Answer:** BC

**Section:** Mix Questions

**Explanation**

**Explanation/Reference:**

**QUESTION 914**

DRAG DROP

Drag and drop the DNS lookup commands from the left onto the correct effects on the right.

**Select and Place:**

|                                                |                                                                               |
|------------------------------------------------|-------------------------------------------------------------------------------|
| <code>ip dns server</code>                     | <code>enables DNS lookup on an individual interface</code>                    |
| <code>ip domain list</code>                    | <code>enables the DNS server on the device</code>                             |
| <code>ip domain lookup source-interface</code> | <code>identifies a DNS server to provide lookup services</code>               |
| <code>ip domain name</code>                    | <code>specifies a sequence of domain names</code>                             |
| <code>ip host</code>                           | <code>specifies the default domain to append to unqualified host names</code> |
| <code>ip name-server</code>                    | <code>statically maps an IP address to a hostname</code>                      |

**Correct Answer:**



|  |                                   |
|--|-----------------------------------|
|  | ip domain lookup source-interface |
|  | ip dns server                     |
|  | ip name-server                    |
|  | ip domain list                    |
|  | ip domain name                    |
|  | ip host                           |

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 915

Which command should you enter to configure a device as an NTP server?

- A. ntp server
- B. ntp peer
- C. ntp master
- D. ntp authenticate

**Correct Answer: C**

**Section: Mix Questions**  
**Explanation**

**Explanation/Reference:**

#### QUESTION 916

```

Vlan503 - Group 1
  State is Active
    1 state change, last state change 32w6d
  Virtual IP address is 10.0.3.241
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.064 secs
  Preemption enabled
  Active router is local
  Standby router is 10.0.3.242, priority 100 (expires in 10.624 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-v1503-1" (default)

```

Refer to the exhibit. Based on the output, which two statements are true? (Choose two.)

- A. The device is using the default HSRP hello timer.
- B. The device is configured with the default HSRP priority.
- C. The device's HSRP group uses the virtual IP address 10.0.3.242

D. The device sends unicast messages to its peers.

**Correct Answer:** AD  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 917**  
Which two commands configure SPAN to monitor incoming traffic across multiple interfaces? (Choose two.)

- A. monitor session 1 destination interface gigabitethernet1/0/2
- B. monitor session 3 source vlan 10- 20 tx
- C. monitor session 3 destination interface gigabitethernet 1/0/2
- D. monitor session 1 source interface gigabitethernet1/0/1
- E. monitor session 3 source vlan 10 – 20 rx

**Correct Answer:** CE  
**Section:** Mix Questions  
**Explanation**

**Explanation/Reference:**

**QUESTION 918**  
DRAG DROP

Drag and drop the HSRP terms from the left onto the correct definitions on the right.

**Select and Place:**

|                |                                                                                                         |
|----------------|---------------------------------------------------------------------------------------------------------|
| active router  | feature that changes the priority of a router when an interface goes down                               |
| preemption     | feature that immediately changes the active router when a router with higher priority becomes available |
| standby group  | forwards packets send to the shared virtual IP address                                                  |
| standby router | provides a redundant default gateway to hosts on a LAN                                                  |
| tracking       | provides forwarding services for hosts on a LAN when a previous device fails                            |

**Correct Answer:**

|  |                |
|--|----------------|
|  | tracking       |
|  | preemption     |
|  | active router  |
|  | standby group  |
|  | standby router |

**Section:** Mix Questions

## Explanation

### Explanation/Reference:

#### QUESTION 919

Which three commands configure RSPAN to capture outgoing traffic from one VLAN on an interface while ignoring other VLAN traffic on the same interface? (Choose three.)

- A. monitor session 2 destination remote vlan 912
- B. monitor session 2 source interface gigabitethernet0/3 tx
- C. monitor session 2 filter vlan 2 – 7, 12
- D. monitor session 2 source interface gigabitethernet0/3 rx
- E. monitor session 2 source interface gigabitethernet0/3 both
- F. monitor session 2 destination interface gigabitethernet1/0/2

**Correct Answer:** ABC

**Section:** Mix Questions

## Explanation

### Explanation/Reference:

#### QUESTION 920

Refer to the exhibit. Which two actions recover the UDLD error-disabled port? (Choose two.)

```
Switch# show udld f0/1
Interface Fa0/1
Port enable administrative configuration setting: Enabled / in aggressive mode
Port enable operational state: Enabled / in aggressive mode
Current bidirectional state: Unknown
Current operational state: Disabled port
Message interval: 7
Time out interval: 5
No neighbor cache information stored

Switch# show interfaces f0/1
FastEthernet0/13 is down, line protocol is down (err-disabled)
    Hardware is Fast Ethernet, address is aaaa.bbbb.cccc (bia aaaa.bbbb.cccc)
    MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
        reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
```

- A. Shut down and restart the error-disabled interface
- B. Disable aggressive mode
- C. Remove and reinsert the network media
- D. Enable errdisable recovery
- E. Enter the **udld reset** command in privileged exec mode

**Correct Answer:** AD

**Section:** Mix Questions

## Explanation

### Explanation/Reference:

#### QUESTION 921

DRAG DROP

Drag and drop the StackWise states from the left onto the correct descriptions on the right.

### Select and Place:

|              |
|--------------|
| initializing |
| progressing  |
| provisioned  |
| ready        |
| waiting      |

|                                                                         |
|-------------------------------------------------------------------------|
| Ports have been assigned in the running configuration of the stack      |
| The stack master has successfully installed a configuration on a device |
| The stack master is actively performing discovery                       |
| The stack master is communicating with a new switch                     |
| The switch is operational                                               |

Correct Answer:

|  |
|--|
|  |
|  |
|  |
|  |
|  |

|              |
|--------------|
| provisioned  |
| waiting      |
| initializing |
| progressing  |
| ready        |

Section: Mix Questions  
Explanation

Explanation/Reference: