300-115 cisco

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

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 Release3.3.0SE, 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

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.

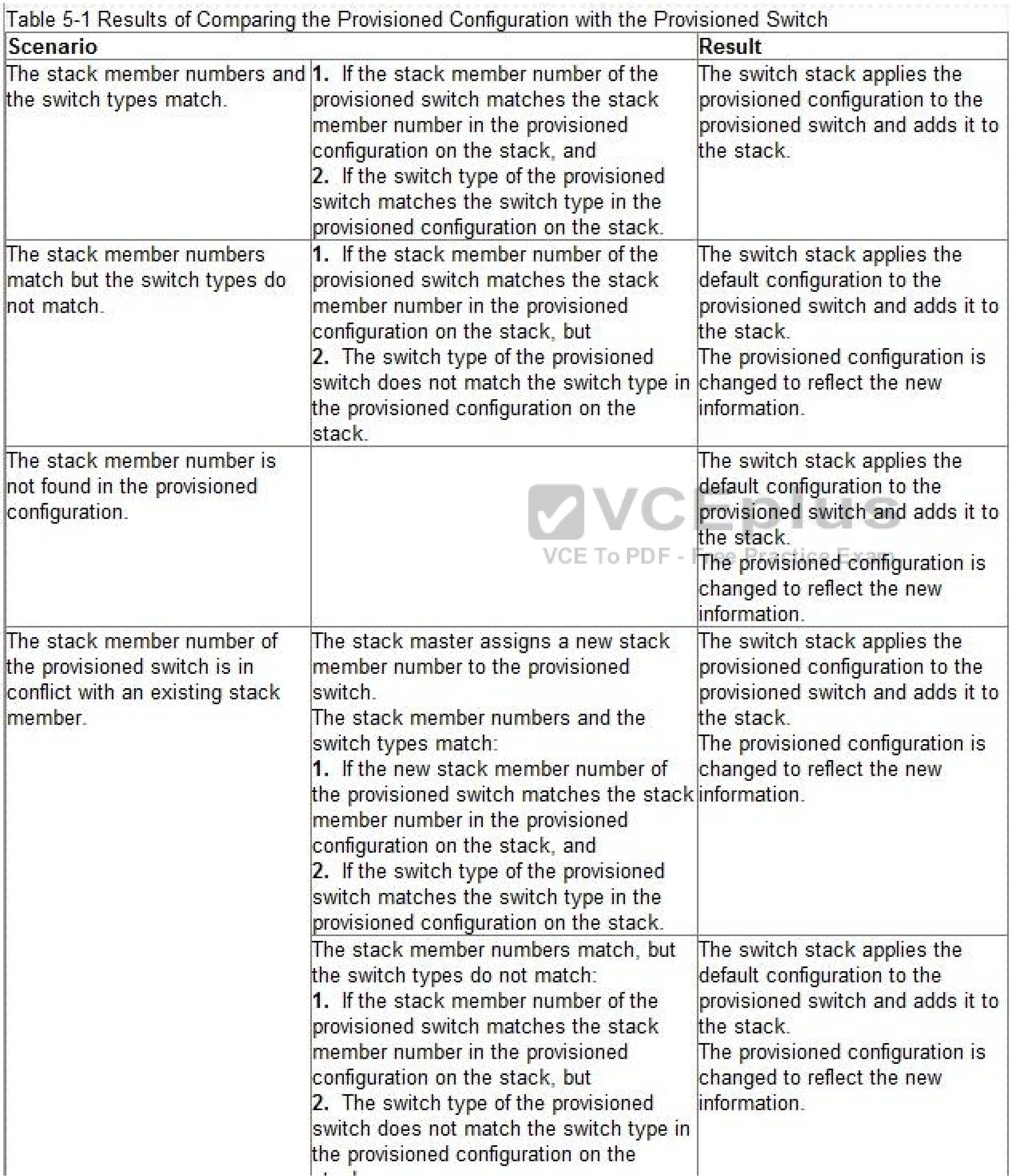


Table 5-1 Results of Comparing the Provisioned Configuration with the Provisioned Switch

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 **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 **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. 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. 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. The stack member numbers and the switch types match: **1.** If the new stack member number of the provisioned switch matches the stack member number in the provisioned configuration on the stack, and **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 provisioned configuration is changed to reflect the new information.
	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 **2.** The switch type of the provisioned switch does not match the switch type in the provisioned configuration on the	The switch stack applies the default configuration to the provisioned switch and adds it to the stack. The provisioned configuration is changed to reflect the new information.

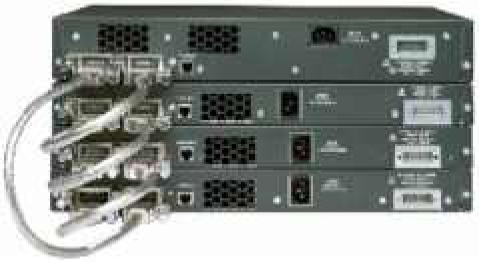
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swstack.html

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

QUESTION 4
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 5
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

QUESTION 6
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

QUESTION 7
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

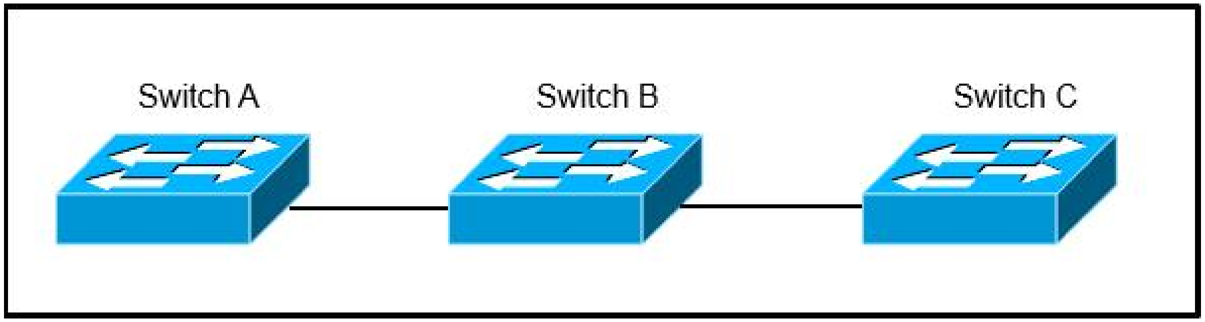
Explanation/Reference:
Explanation:

- 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

QUESTION 8
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?

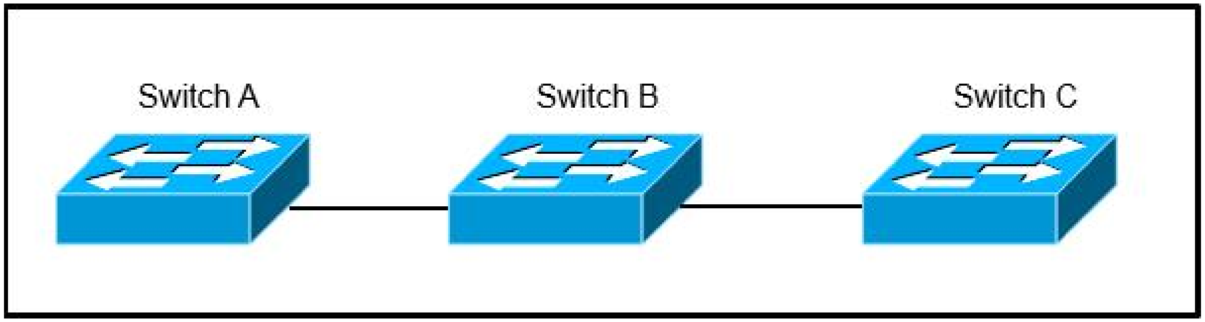
A. Switch B is configured in transparent mode.
B. Switch B is configured with an access port to Switch A, while Switch C is configured with a trunk port to Switch B.
C. The VTP revision number of the Switch B is higher than that of Switch A.
D. The trunk between Switch A and Switch B is misconfigured.

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

QUESTION 9
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 10
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 11
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 12

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.

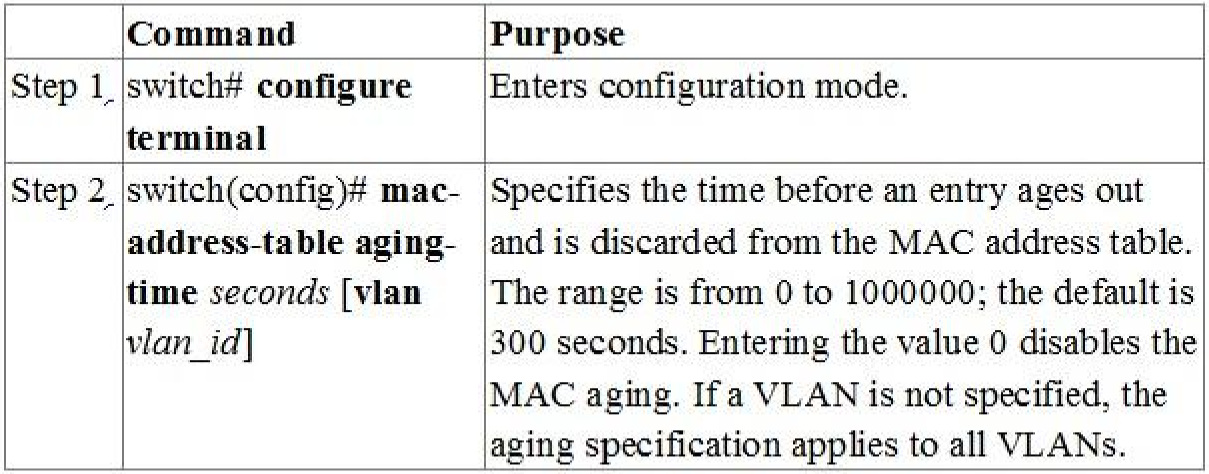
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/vtp.html#wp1020444

QUESTION 13
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	switch# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	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 14

While working in the core network building, a technician accidently 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 15
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 16
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.

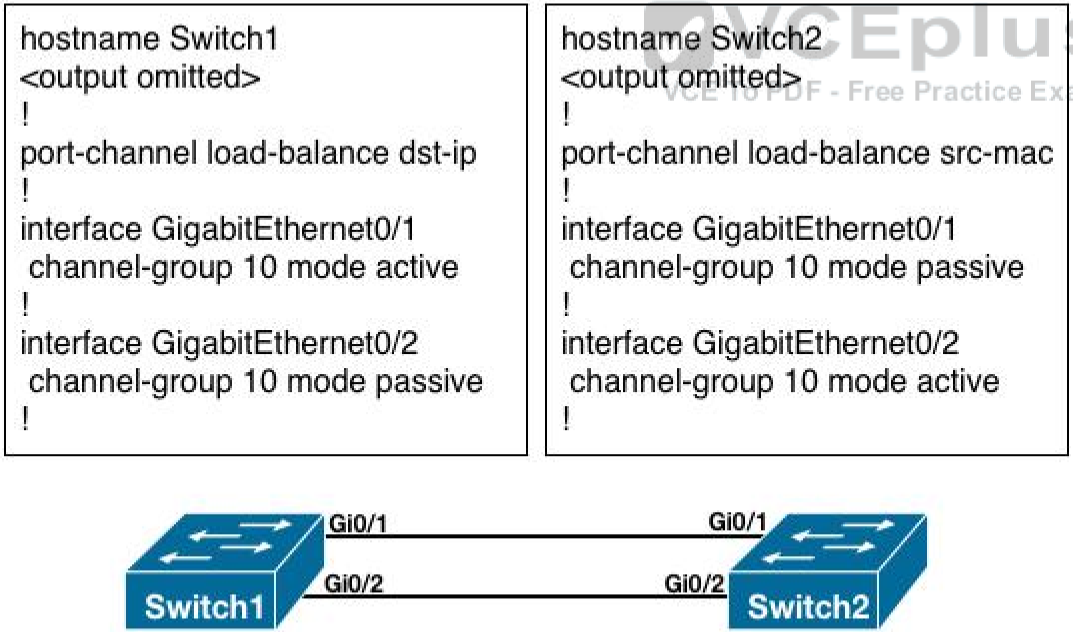
D. RSPAN must be used to capture EtherChannel bidirectional traffic.

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 17
Refer to the exhibit.



```
hostname Switch1
<output omitted>
!
port-channel load-balance dst-ip
!
interface GigabitEthernet0/1
 channel-group 10 mode active
!
interface GigabitEthernet0/2
 channel-group 10 mode passive
!
```

```
hostname Switch2
<output omitted>
!
port-channel load-balance src-mac
!
interface GigabitEthernet0/1
 channel-group 10 mode passive
!
interface GigabitEthernet0/2
 channel-group 10 mode active
!
```

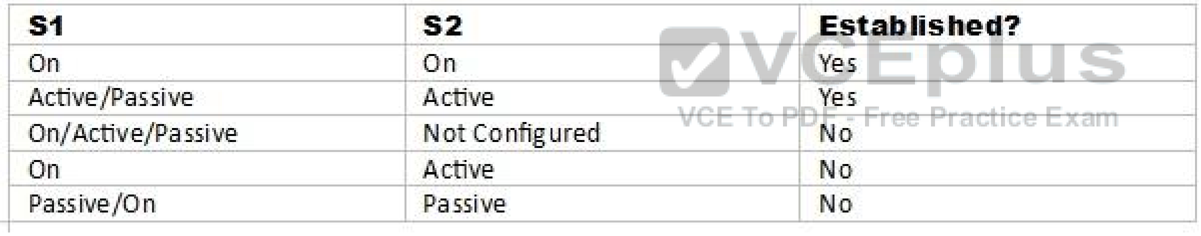
What is the result of the configuration?

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 18
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 19
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 20
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 21
After reviewing UDLD status on switch ports, an engineer notices that the.” 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.

Reference: http://packetlife.net/blog/2011/mar/7/udld/

QUESTION 22

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:
I f 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

QUESTION 23
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

QUESTION 24
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?

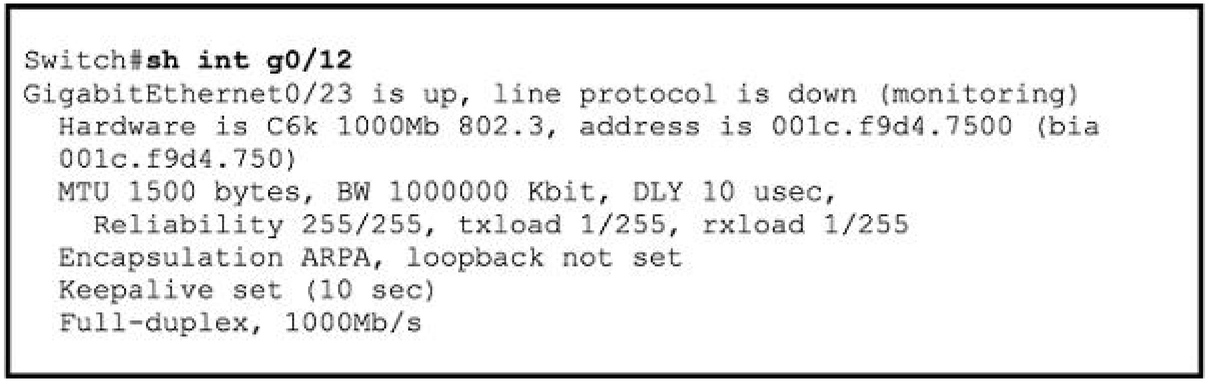
A. Configure the new load balancing method using port-channel load-balance.
B. Adjust the switch SDM back to “default”.
C. Ensure that IP CEF is enabled globally to support all load balancing methods.
D. Upgrade the PFC to support the latest load balancing methods.

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 25
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 SAPN 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

QUESTION 26
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

QUESTION 27
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.

Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_13_ea1/configuration/guide/swvlan.html

QUESTION 28
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 29
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 30

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 31
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

QUESTION 32
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

QUESTION 33
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 34
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 35
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 36
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

QUESTION 37
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 trInk 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 38
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)# sp–nning-tree portfast
```

Reference: http://www.informit.com/library/content.aspx?b=CCNP_Studies_Switching&seqNum=36

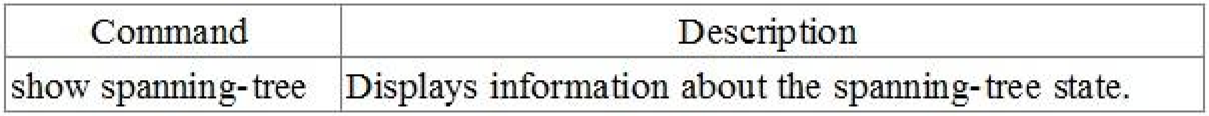
QUESTION 39
Which command does a network engineer use to verify the spanning-tree status for VLAN 10?

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

QUESTION 40
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 do”ain 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 revisio“ num”ers does 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://rowell.dionicio.net/configuring-cisco-vtp/

QUESTION 41
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. PVRST+ 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.

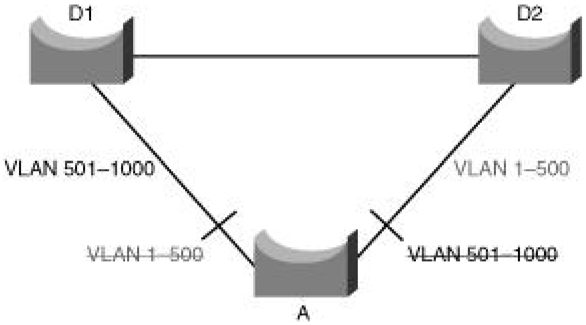


Figure 3-15: VLAN Load Balancing

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 42

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

QUESTION 43
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

QUESTION 44
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.**

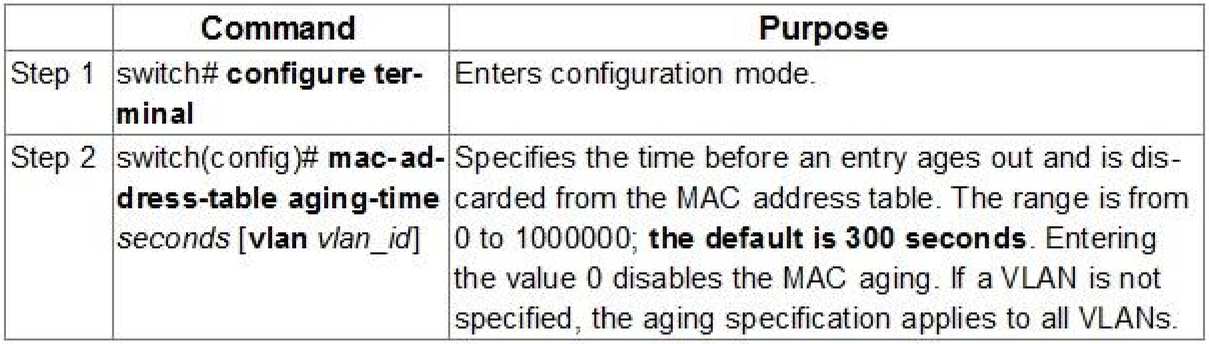
Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_55_se/configuration/guide/swsdm.pdf

QUESTION 45
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# **configure terminal**	Enters configuration mode.
Step 2	switch(config)# **mac-address-table aging-time** *seconds* [**vlan** *vlan_id*]	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.

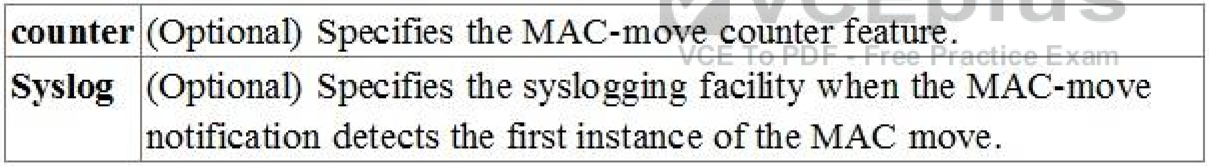
Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/MACAddress.html

QUESTION 46
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



counter	(Optional) Specifies the MAC-move counter feature.
Syslog	(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

QUESTION 47
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

QUESTION 48
What is the default value for the errdisable recovery interval in a Cisco switch?

A. 30 seconds
B. 100 seconds
C. 43sernads
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 reenable the ports manually. Issue the **shutdown** command and then the **no shutdown** interface mode command on the associated interface in order to manually reenable the ports.
The **errdisable recovery** command allows you to choose the type of errors that automatically reenable 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

QUESTION 49
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

QUESTION 50
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 51
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 0xFFF 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

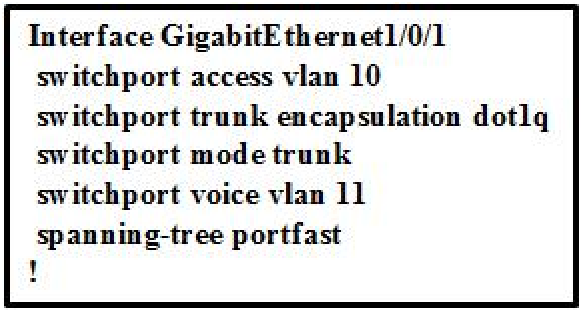
QUESTION 52
What is the maximum number of VLANs that can be assigned to an access switchport without a voice VLAN?

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.

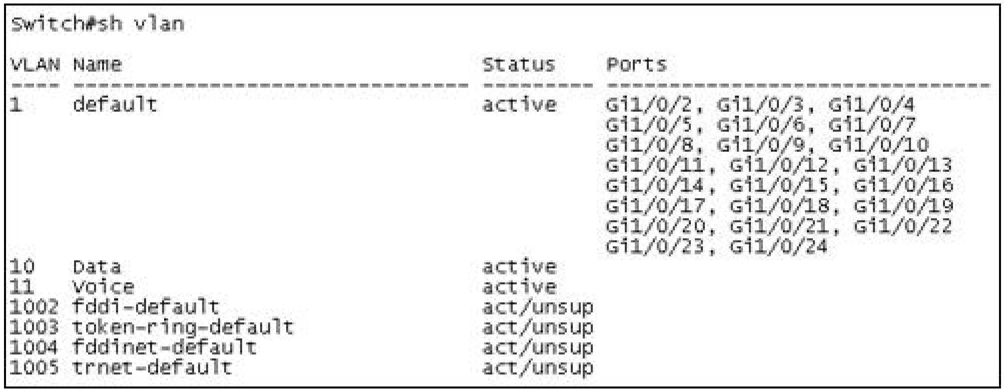
QUESTION 53
Refer to the exhibit.



```
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?

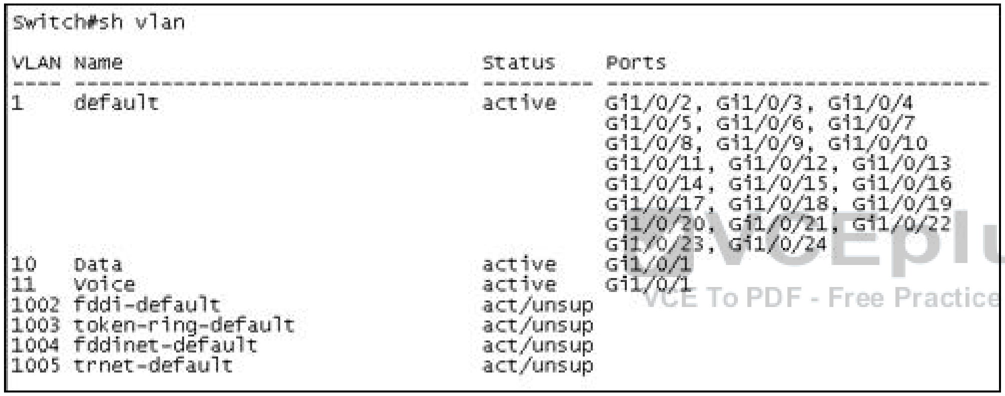
A.



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
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
```

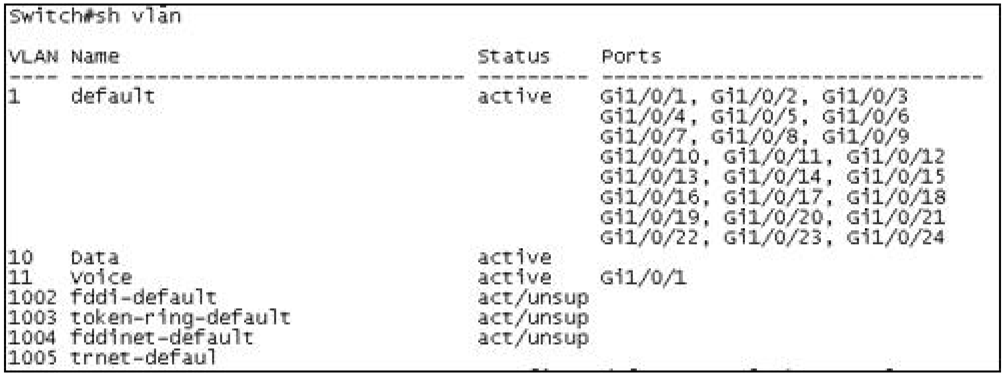
B.



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
10   Data                             active    Gi1/0/1
11   Voice                            active    Gi1/0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

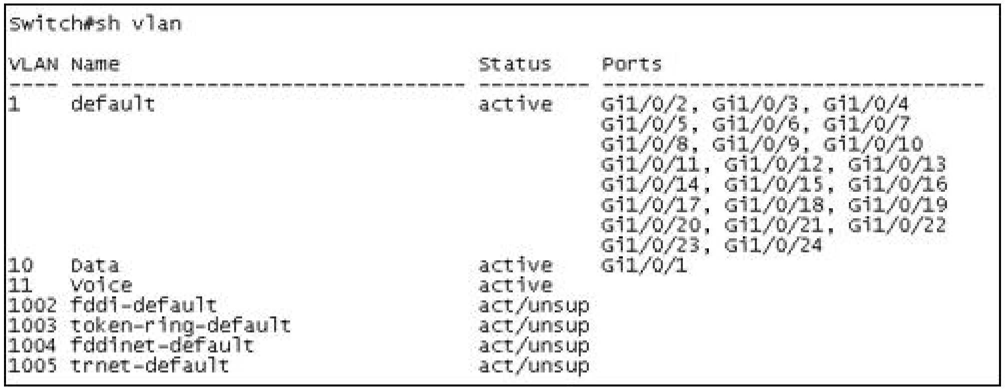
C.



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/1, Gi1/0/2, Gi1/0/3
                                                Gi1/0/4, Gi1/0/5, Gi1/0/6
                                                Gi1/0/7, Gi1/0/8, Gi1/0/9
                                                Gi1/0/10, Gi1/0/11, Gi1/0/12
                                                Gi1/0/13, Gi1/0/14, Gi1/0/15
                                                Gi1/0/16, Gi1/0/17, Gi1/0/18
                                                Gi1/0/19, Gi1/0/20, Gi1/0/21
                                                Gi1/0/22, Gi1/0/23, Gi1/0/24
10   Data                             active
11   Voice                            active    Gi1/0/1
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-defaul
```

D.



```
Switch#sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gi1/0/2, Gi1/0/3, Gi1/0/4
                                                Gi1/0/5, Gi1/0/6, Gi1/0/7
                                                Gi1/0/8, Gi1/0/9, Gi1/0/10
                                                Gi1/0/11, Gi1/0/12, Gi1/0/13
                                                Gi1/0/14, Gi1/0/15, Gi1/0/16
                                                Gi1/0/17, Gi1/0/18, Gi1/0/19
                                                Gi1/0/20, Gi1/0/21, Gi1/0/22
                                                Gi1/0/23, Gi1/0/24
10   Data                             active    Gi1/0/1
11   Voice                            active
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 54
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.

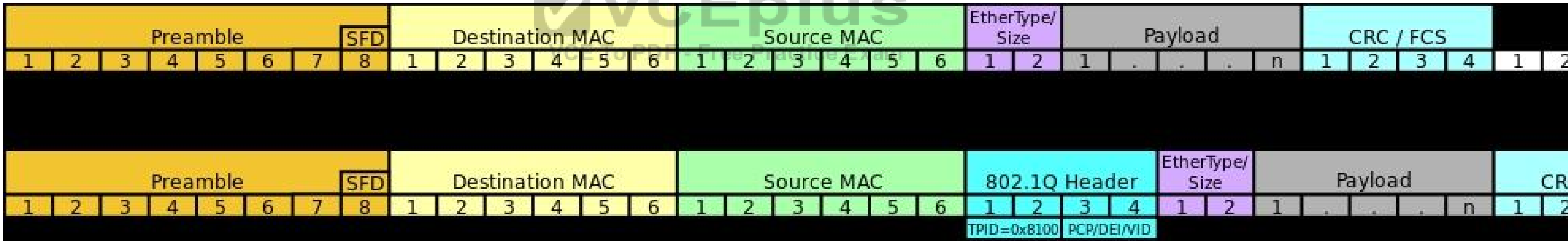
Reference: http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_22_ea11x/configuration/guide/swvoip.html

QUESTION 55
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

QUESTION 56
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.php

QUESTION 57
Which feature must be enabled to eliminate the broadcasting of all unknown traffic to switches that are not participating in the specific VLAN?

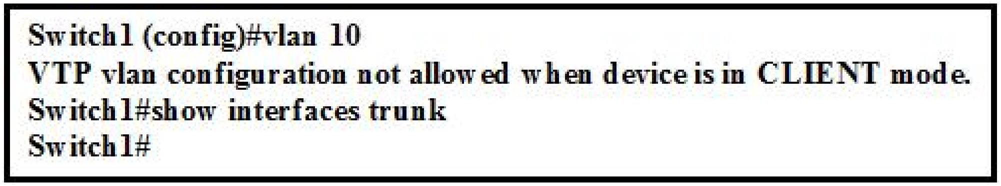
A. VTP pruning
B. port-security
C. storm control
D. bpdguard

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

QUESTION 58
Refer to the exhibit.



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

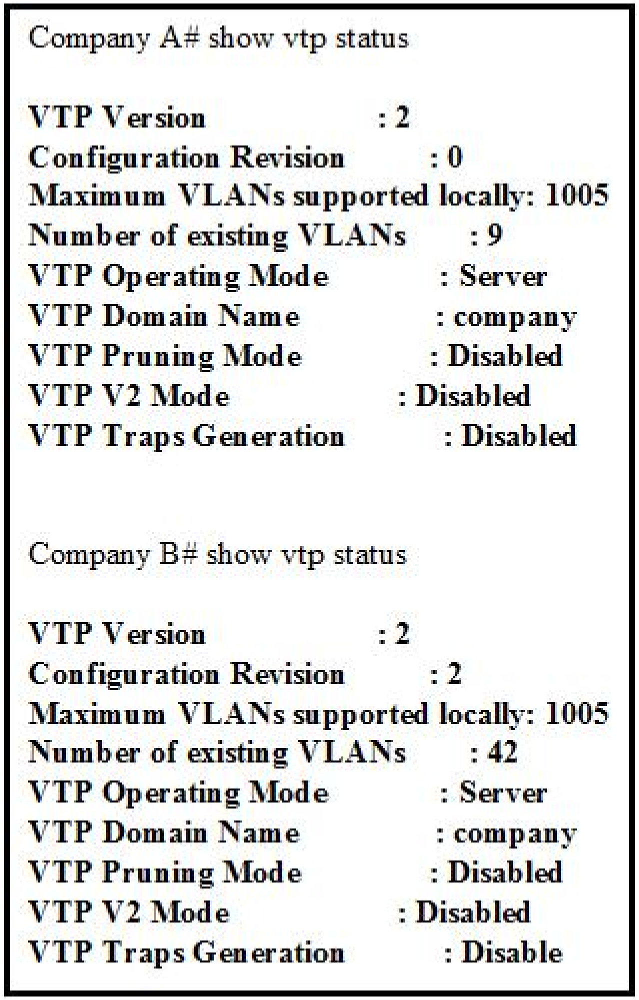
The users in an engineering department that connect to the same access switch cannot access the network. The network engineer found that the engineering VLAN is missing from the database. Which action resolves this problem?

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 59
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 60
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 61
Which statement about using native VLANs to carry untagged frames is true?

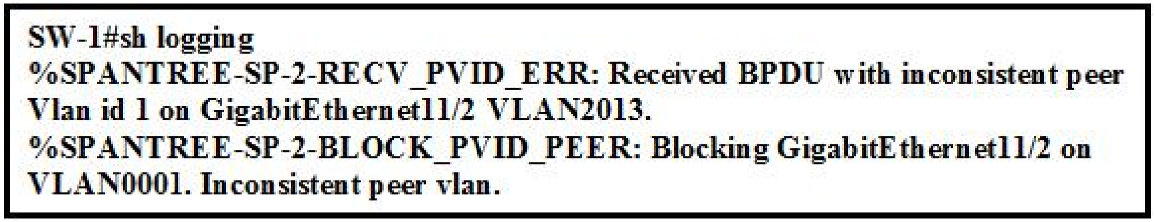
A. Cisco Discovery Protocol version 2 carries native VLAN information, but version 1 does not.
B. Cisco Discovery Protocol version 1 carries native VLAN information, but version 2 does not.
C. Cisco Discovery Protocol version 1 and version 2 carry native VLAN information.
D. Cisco Discovery Protocol 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 62
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 bpdu-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

QUESTION 63
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 64
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:
Manaully 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 65
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

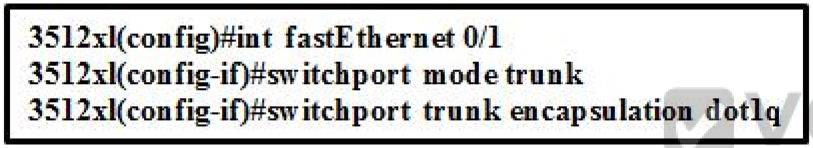
D. Support 1547 MTU only

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: http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_13_ea1/configuration/guide/swtunnel.html

QUESTION 66
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 67
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

QUESTION 68
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

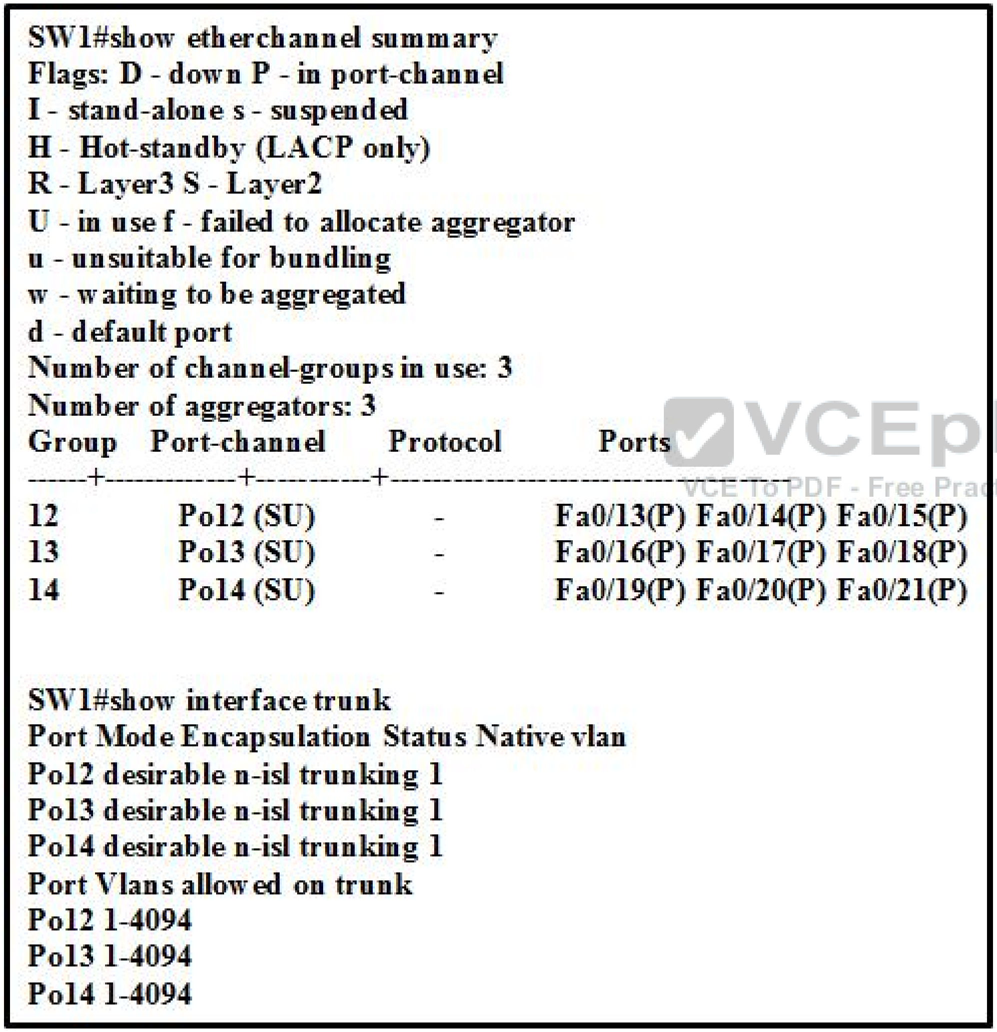
Explanation/Reference:
Explanation:
PagP modes are off, auto, desirable, and on. Only the combinations auto-desirable, desirable-desirable, and on-on will allow a channel to be formed. The PagP modes are explained below.

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 69
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. .

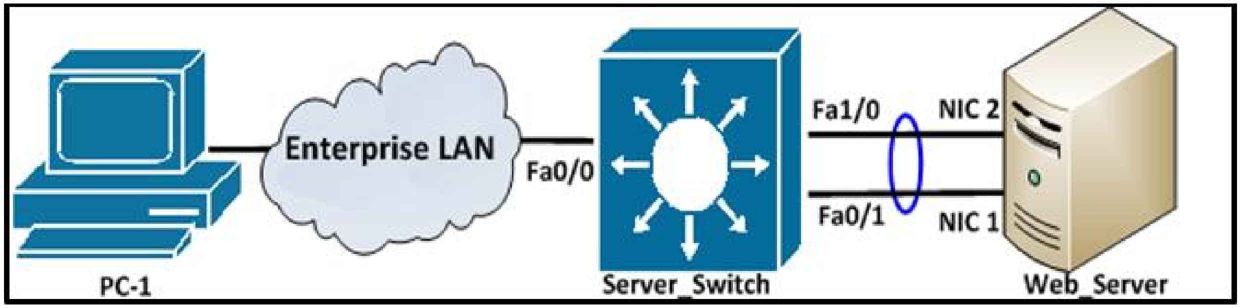
1. on: PAgP will not run. The channel is forced to come up.
2. off: PAgP will not run. The channel is forced to remain down.
3. auto: PAgP is running passively. The formation of a channel is desired; however, it is not initiated.
4. desirable: PAgP is running actively. The formation of a channel is desired 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 70
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#
```

HoweIer, 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 71
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 72
Which statement about using EtherChannel on Cisco IOS switches is true?

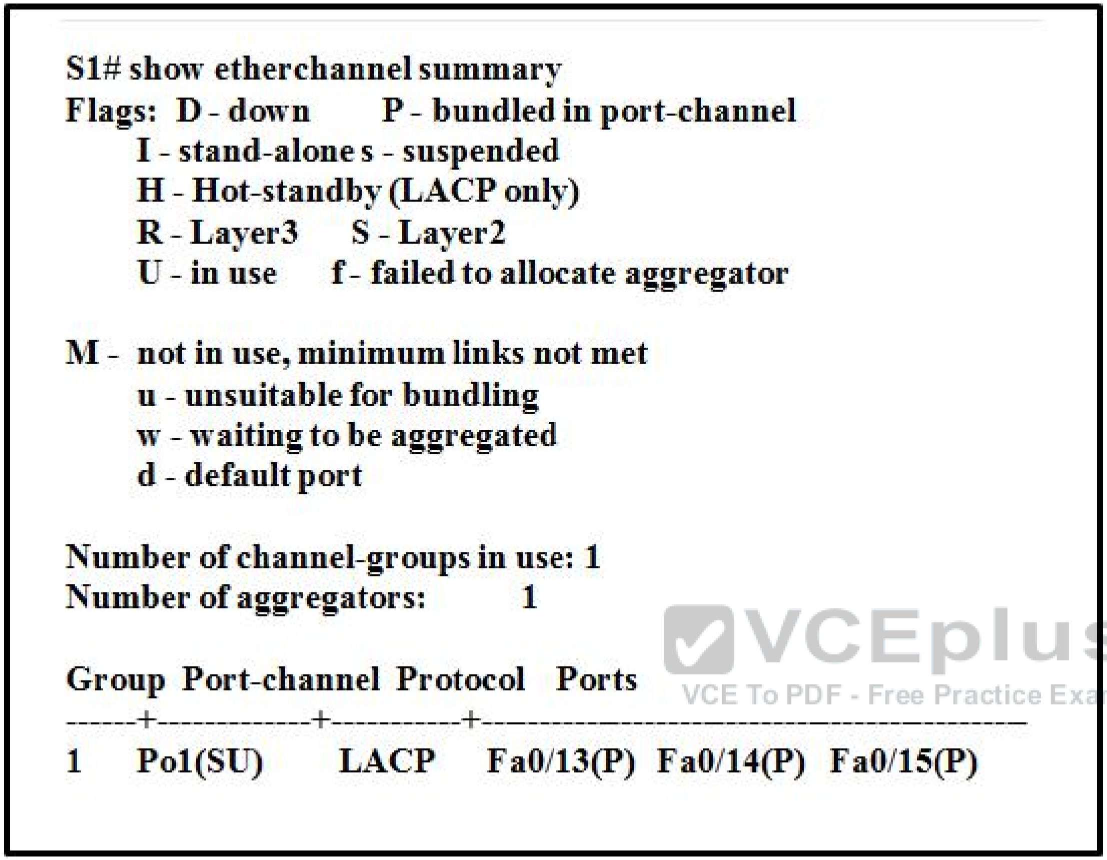
A. A switch can support up to eight compatibly configured Ethernet interfaces in an EtherChannel. The EtherChannel provides full-duplex bandwidth up to 800 Mbps only for Fast EtherChannel or 8 Gbps only for Gigabit EtherChannel.
B. A switch can support up to 10 compatibly configured Ethernet interfaces 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 73
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 74
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 75
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 68sername6868eed 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 68sernamcantly reduced.

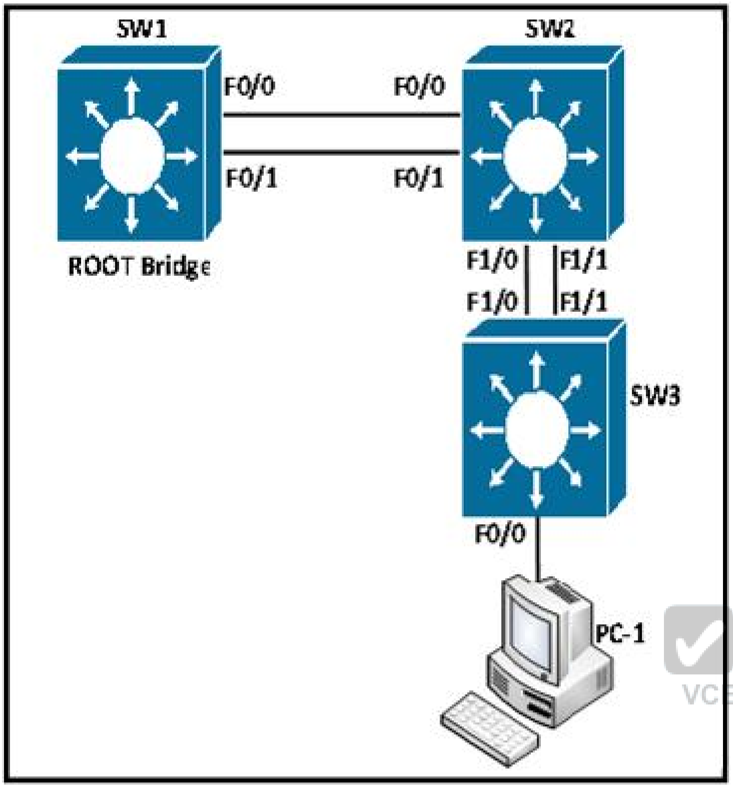
All MST instances within the same region share the same protocol timers, but each MST instance has its own topology parameters, such as root bridge ID, root path cost, and so forth. By default, all VLANs are assigned to the IST.

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 76
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.

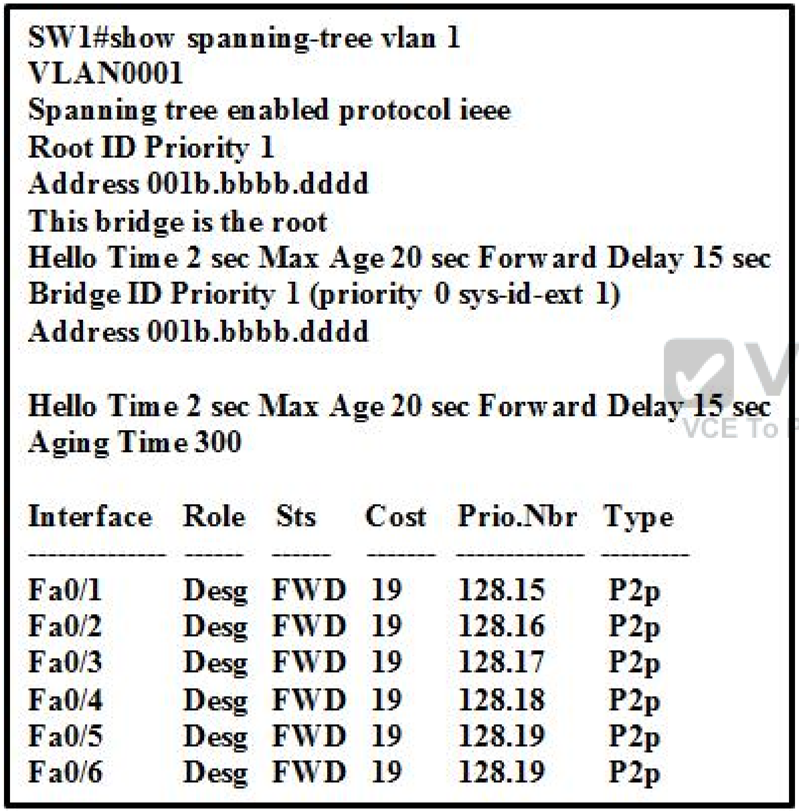
Correct Answer: C
Section: Layer 2 Technologies
Explanation

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: http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_9_ea1/configuration/guide/swstp.html#wp1105354

QUESTION 77
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.

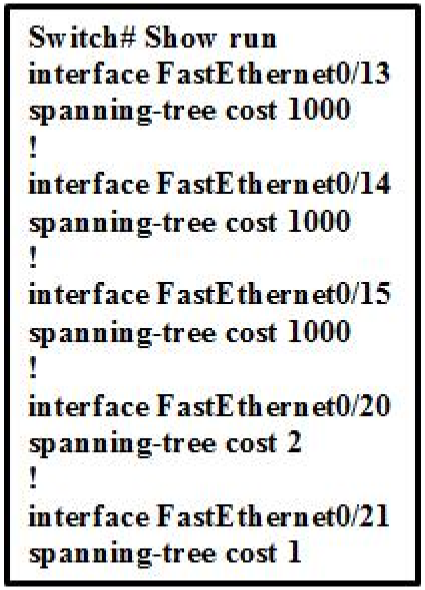
D. The switch priority value is zero, it has the lowest priority value for VLAN 1.

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

QUESTION 78
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. 71sername71e 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

QUESTION 79
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 80
A network engineer configured an Ethernet switch using these commands.

Switchone(config) # Spanning-tree portfast bpdufilter default

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

A. If an interface is enabled for portfast receives BDPU, the port goes through the spanning-tree listening, learning, and forwarding states.
B. If an interface is enabled for portfast receives BDPU, the port does not go through the spanning-tree listening, learning, and forwarding states.
C. If an interface is enabled for portfast receives BDPU, the port is shut down immediately.
D. If an interface is enabled for portfast receives BDPU, 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 bpdufilter 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 81
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 forIarded 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

QUESTION 82
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

QUESTION 83
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_qas0900aecd806ed74b.html

QUESTION 84
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_qas0900aecd806ed74b.html

QUESTION 85
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_qas0900aecd806ed74b.html

QUESTION 86
SIMULATION
Scenario:
You work for SWITCH.com. They have just added a new switch (SwitchB) to the existing network as shown in the topology diagram.
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. You have been tasked with competing the needed configuring of SwitchA and SwitchB. SwitchA and SwitchB use Cisco as the enable password.

Configuration Requirements for SwitchA
The VTP and STP configuration modes on SwitchA 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 are their default values.

Configuration Requirements for SwitchB
- Vlan 21

Name: Marketing
will support two servers attached to fa0/9 and fa0/10
- Vlan 22

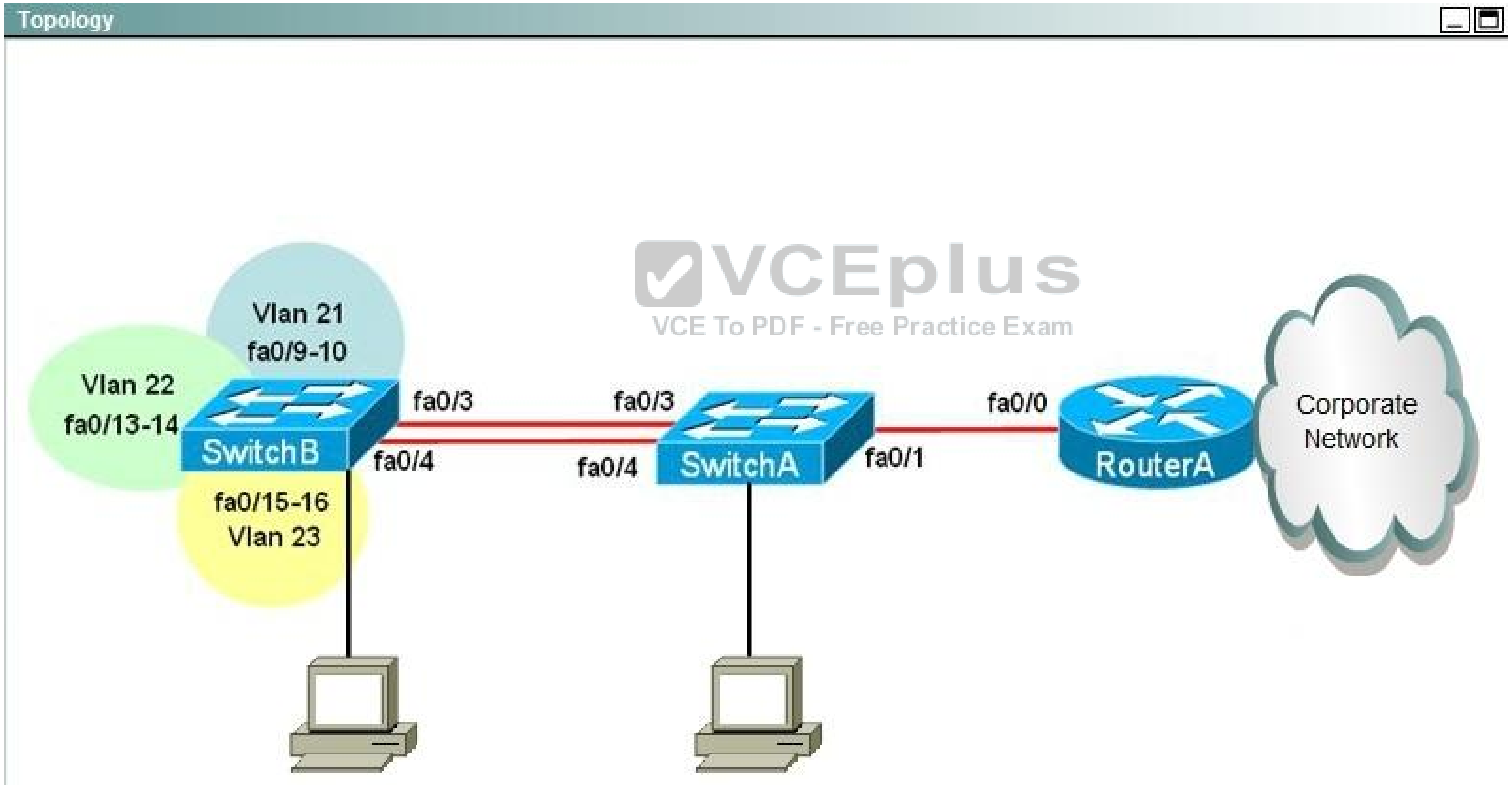
Name: Sales
will support two servers attached to fa0/13 and fa0/14
- Vlan 23

o 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 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.



Correct Answer: Here are steps
Section: Layer 2 Technologies
Explanation

Explanation/Reference:

```
hostname SWITCH_B
!
!
vlan 21
name Marketing
vlan 22
name Sales
vlan 23
name Engineering
!
!
interface FastEthernet0/3
switchport trunk allowed vlan 1,21-23
channel-protocol lacp
channel-group 1 mode passive
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk allowed vlan 1,21-23
channel-protocol lacp
channel-group 1 mode passive
switchport mode trunk
!
interface FastEthernet0/9
switchport access vlan 21
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/10
switchport access vlan 21
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/13
switchport access vlan 22
switchport mode access
spanning-tree portfast
!
!
interface FastEthernet0/14
switchport access vlan 22
switchport mode access
```

```
spanning-tree portfast
!
interface FastEthernet0/15
switchport access vlan 23
switchport mode access
spanning-tree portfast
!
interface FastEthernet0/16
switchport access vlan 23
switchport mode access
spanning-tree portfast
!
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Port-channel 1
switchport mode trunk
switchport trunk encapsulation dot1q
spanning-tree allowed vlans 1,21-23
!
interface Vlan1
ip address 192.168.1.11 255.255.255.0
!
end
SWITCH_B(config)#
hostname SWITCH_A
!
panning-tree vlan 11 root primary
spanning-tree vlan 12 root primary
spanning-tree vlan 13 root primary
spanning-tree vlan 21 root primary
spanning-tree vlan 22 root primary
spanning-tree vlan 23 root primary
!
interface FastEthernet0/3
switchport trunk allowed vlan 1,21-23
channel-protocol lacp
channel-group 1 mode active
switchport mode trunk
!
interface FastEthernet0/4
switchport trunk allowed vlan 1,21-23
```

```
channel-protocol lacp
channel-group 1 mode active
switchport mode trunk
!
interface FastEthernet0/21
switchport access vlan 21
switchport mode access
!
interface FastEthernet0/22
switchport access vlan 22
switchport mode access
!
interface FastEthernet0/23
switchport access vlan 23
switchport mode access
!
interface GigabitEthernet1/1
!
interface GigabitEthernet1/2
!
interface Port-channel 1
!
interface Vlan1
no ip address
shutdown
!
ip default-gateway 192.168.1.1
!
!
End
```

QUESTION 87

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 RouteC. RouterC is correctly configured. No trunking has been configured on RouterC.

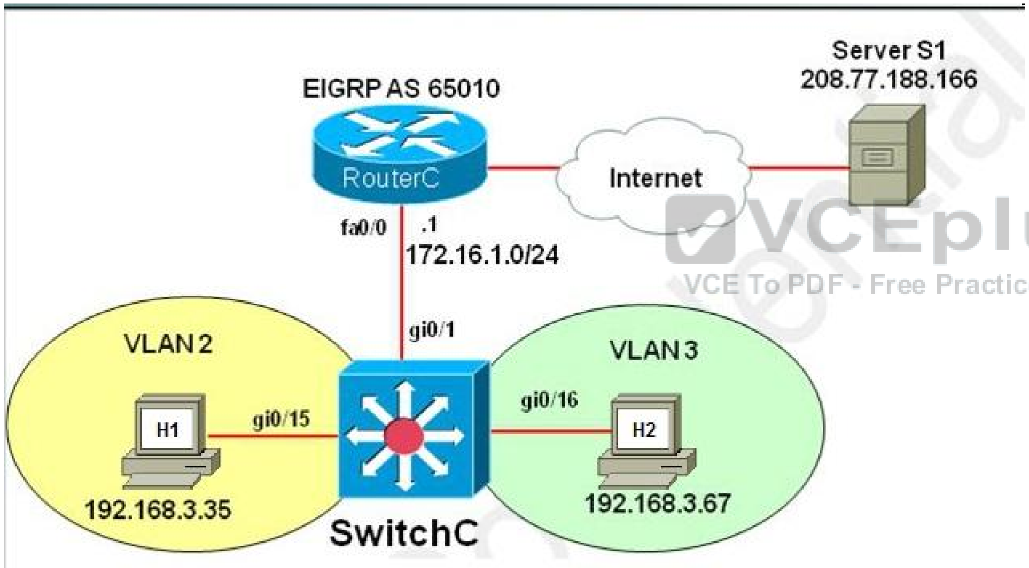
Routed interfaces should use the lowest host on a subnet when possible. The following subnets are available to implement this solution:

– 10.10.10.0/24
– 190.200.250.32/27
– 190.200.250.64/27

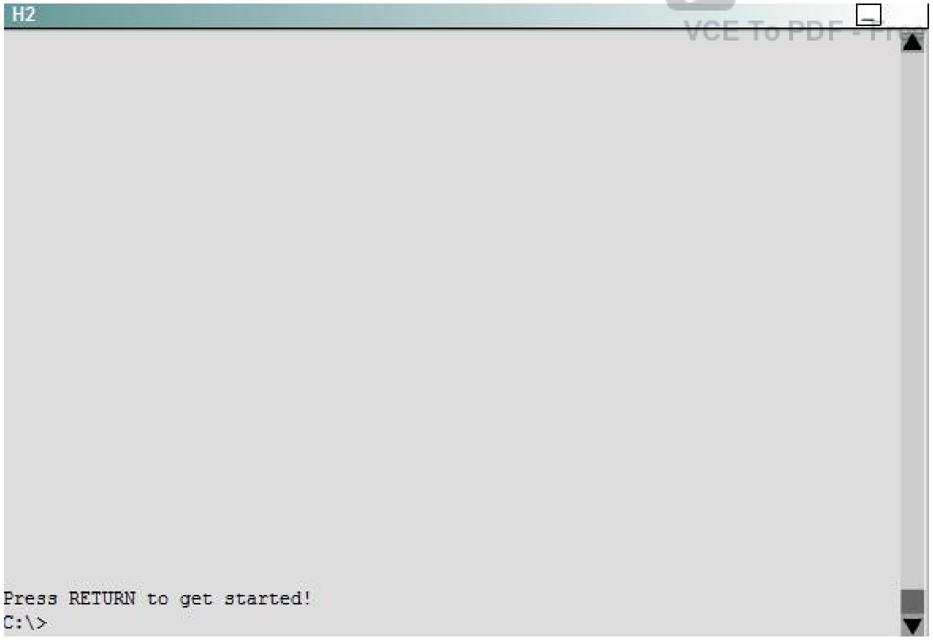
Hosts H1 and H2 are configured with the correct IP address and default gateway.
SwitchC uses Cisco as the enable password.

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

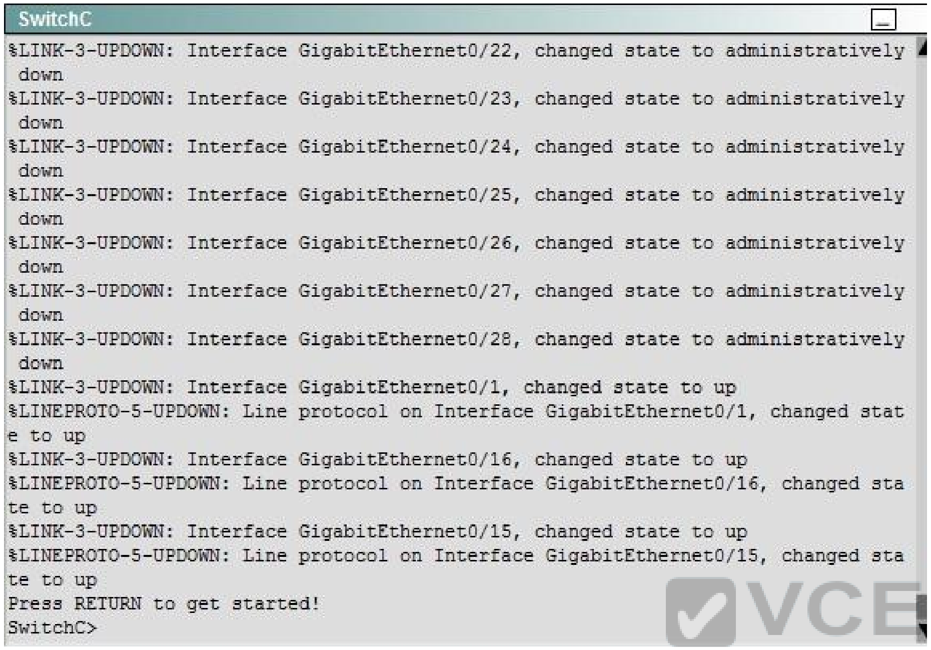
Note: Due to administrative restrictions and requirements you should not add or delete VLANs, changes VLAN port assignments or create trunks.
Company policies forbid the use of static or default routing. All routes must be learned via the EIGRP routing protocol.



```
Press RETURN to get started!
C:\>
```



```
Press RETURN to get started!
C:\>
```



SwitchC

```
%LINK-3-UPDOWN: Interface GigabitEthernet0/22, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/23, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/24, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/25, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/26, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/27, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/28, changed state to administratively
 down
%LINK-3-UPDOWN: Interface GigabitEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed stat
e to up
%LINK-3-UPDOWN: Interface GigabitEthernet0/16, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/16, changed sta
te to up
%LINK-3-UPDOWN: Interface GigabitEthernet0/15, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/15, changed sta
te to up
Press RETURN to get started!
SwitchC>
```

Correct Answer: There are two ways to configure interVLAN routing in this case
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
+ 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.

C:\>**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.

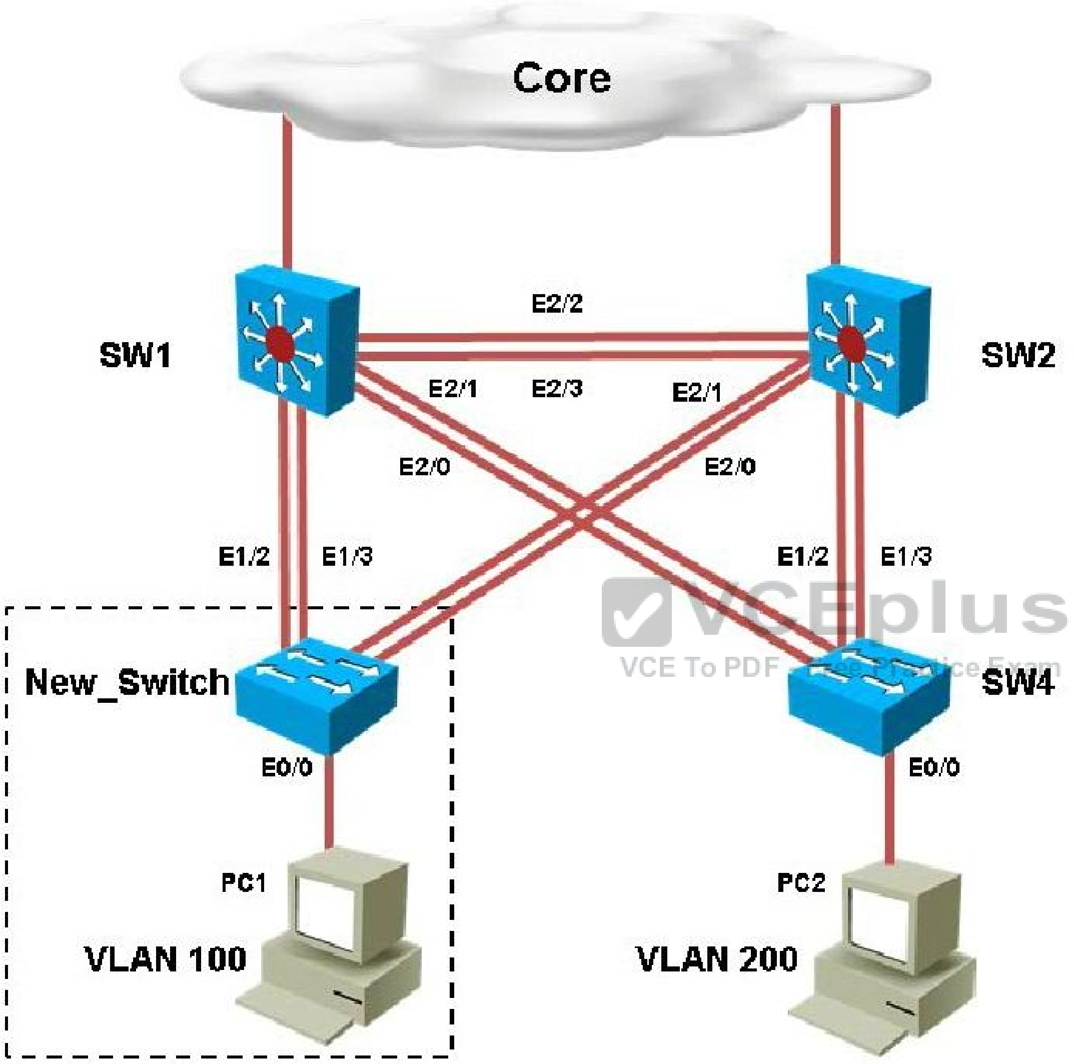
In order to complete the lab, you should expect the ping to SERVER to succeed from the MLS, and from the PCs as well.

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 88

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.


Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

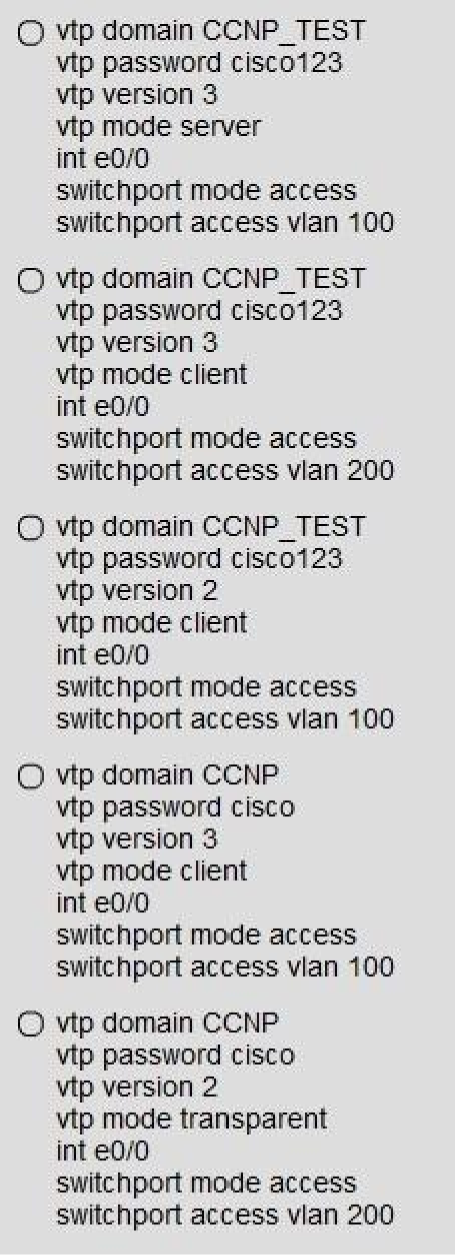
```
SW1#
```

```
SW2#
```

```
New_Switch#
```

```
SW4#
```

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?



```
○ vtp domain CCNP_TEST
  vtp password cisco123
  vtp version 3
  vtp mode server
  int e0/0
  switchport mode access
  switchport access vlan 100
```

```
○ vtp domain CCNP_TEST
  vtp password cisco123
  vtp version 3
  vtp mode client
  int e0/0
  switchport mode access
  switchport access vlan 200
```

```
○ vtp domain CCNP_TEST
  vtp password cisco123
  vtp version 2
  vtp mode client
  int e0/0
  switchport mode access
  switchport access vlan 100
```

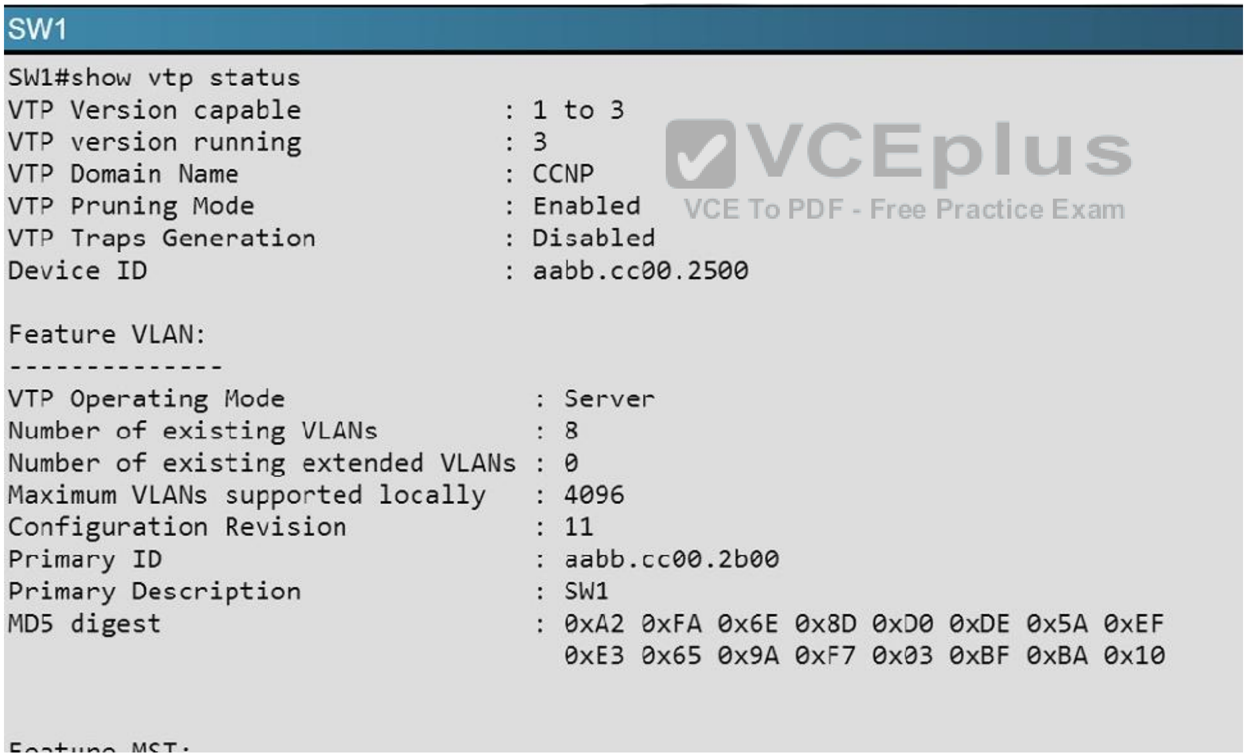
```
○ vtp domain CCNP
  vtp password cisco
  vtp version 3
  vtp mode client
  int e0/0
  switchport mode access
  switchport access vlan 100
```

```
○ vtp domain CCNP
  vtp password cisco
  vtp version 2
  vtp mode transparent
  int e0/0
  switchport mode access
  switchport access vlan 200
```

A. Option A
B. Option B
C. Option C
D. Option D
E. Option E

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

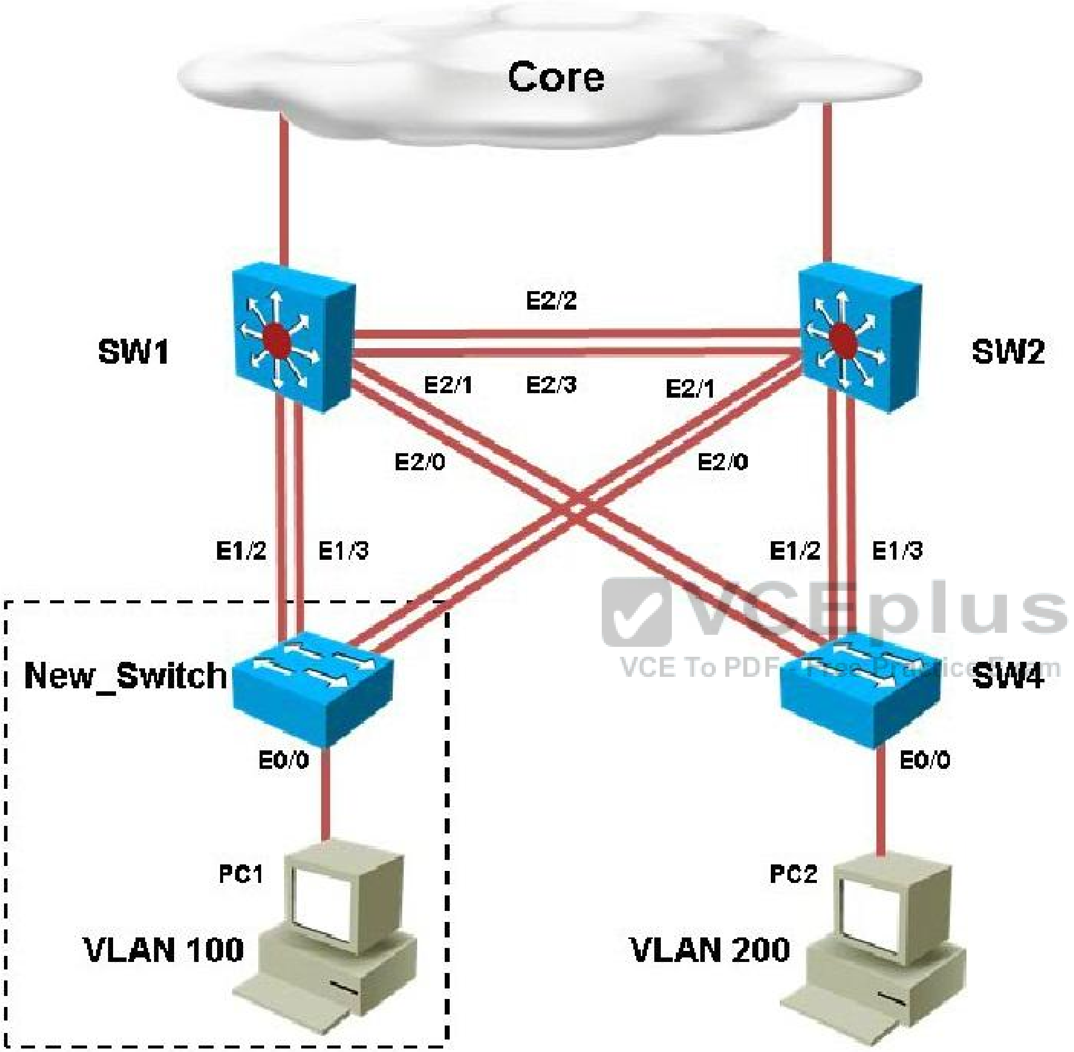
```
SW1#show vtp status
VTP Version capable               : 1 to 3
VTP version running               : 3
VTP Domain Name                   : CCNP
VTP Pruning Mode                  : Enabled
VTP Traps Generation              : Disabled
Device ID                         : aabb.cc00.2500

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 89
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.


Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

```
SW1#
```

```
SW2#
```

```
New_Switch#
```

```
SW4#
```

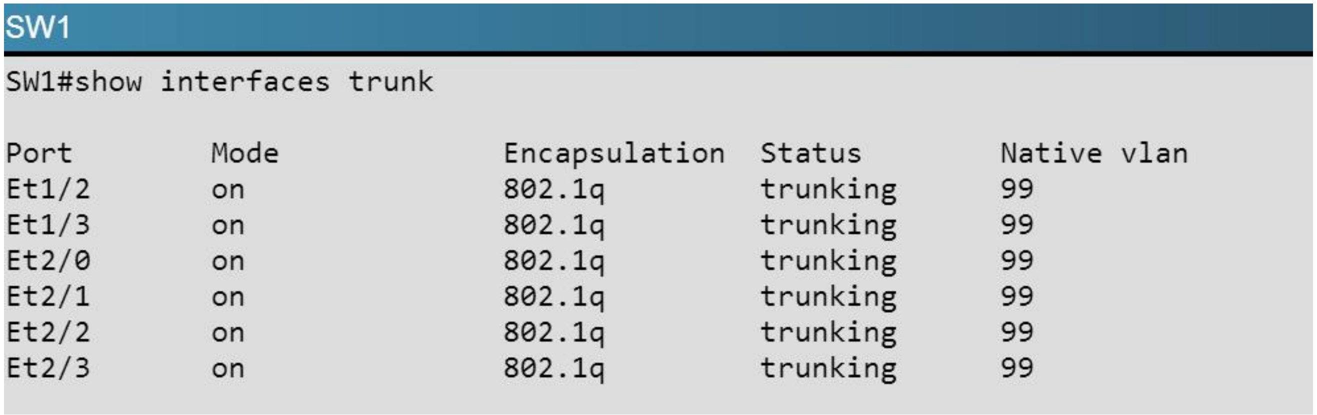
Refer to the configuration. For which configured VLAN are untagged frames sent over trunk between SW1 and SW2?

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:

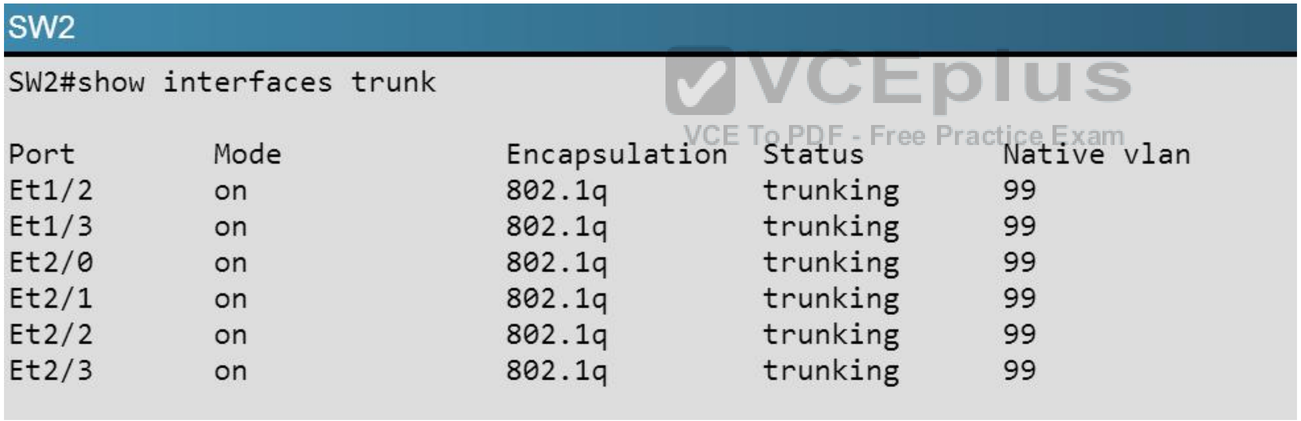
Explanation:
The native VLAN is used for untagged frames sent along a trunk. By issuing the “show interface trunk” command on SW1 and SW2 we see the native VLAN is 99.



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
```

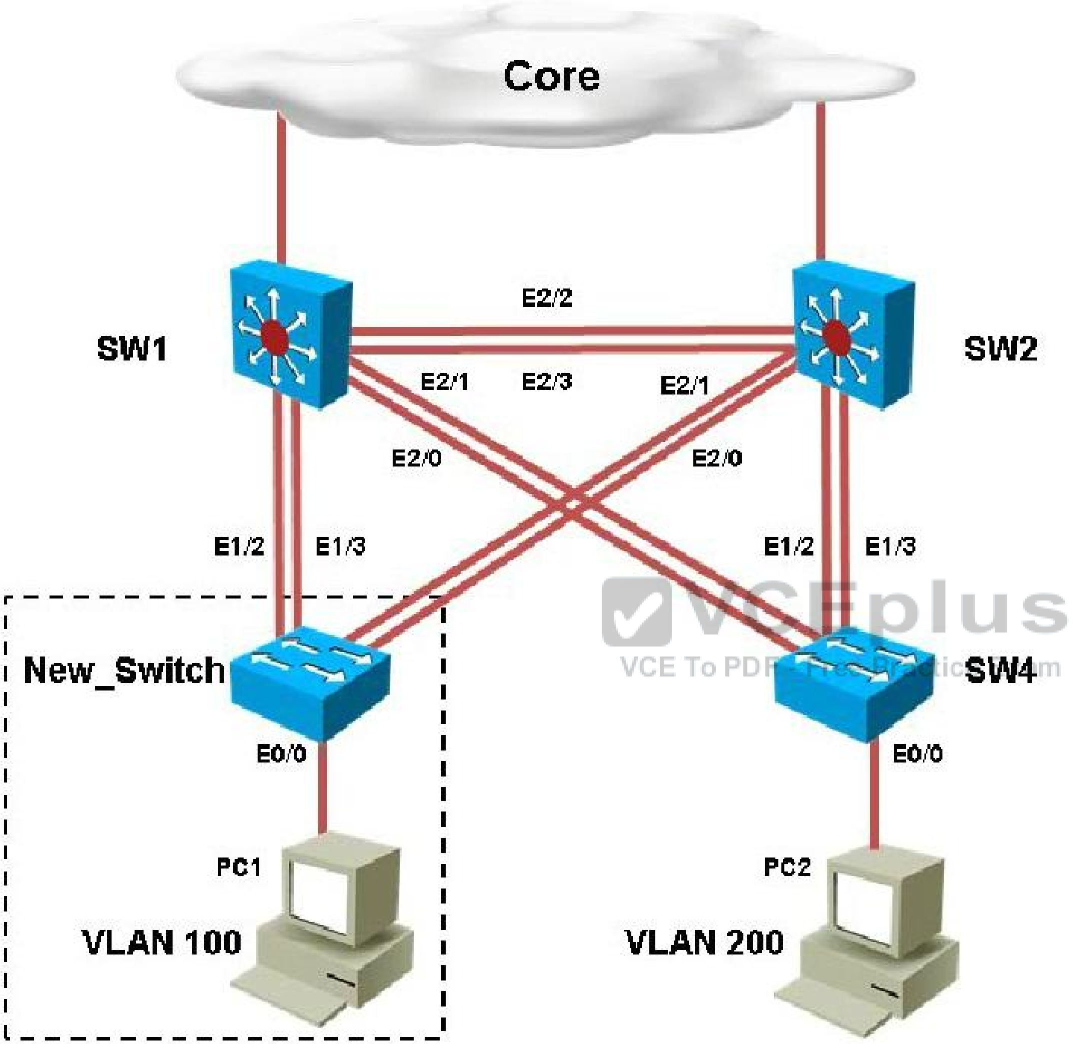


SW2

```
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 90
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.


Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

```
SW1#
```

```
SW2#
```

```
New_Switch#
```

```
SW4#
```

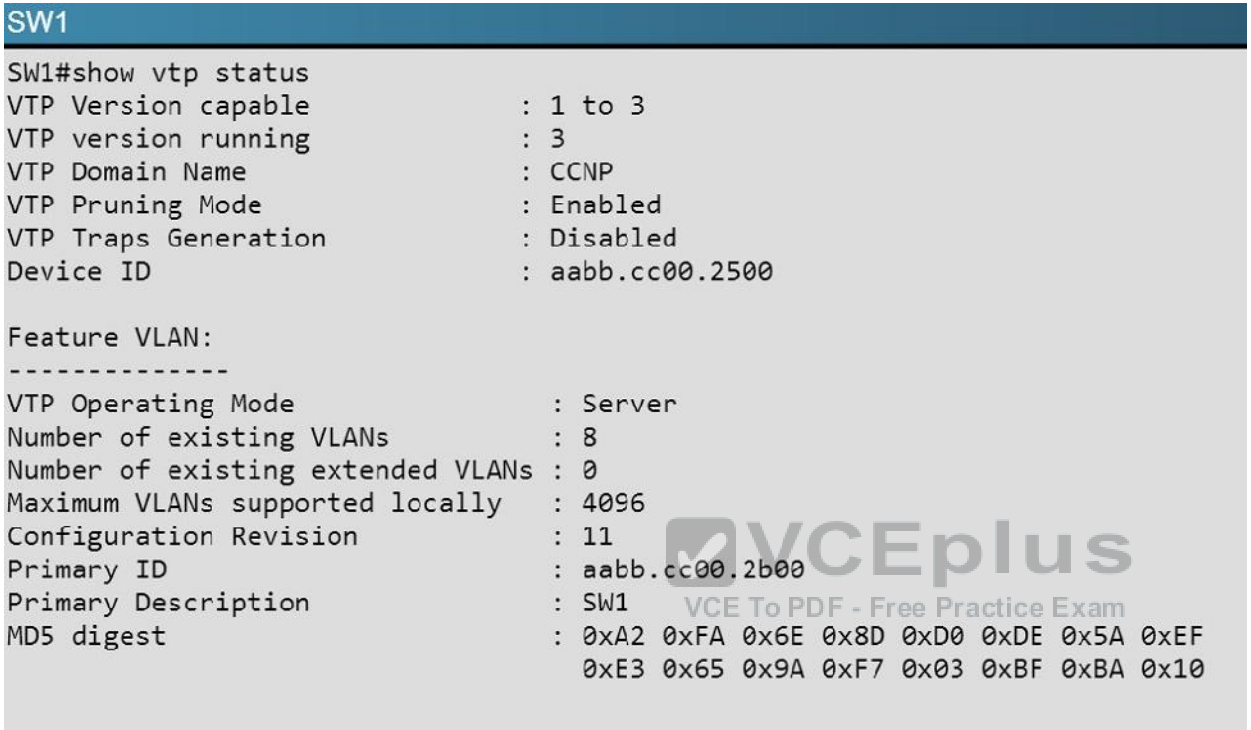
You are adding new VLANs. VLAN500 and VLAN600 to the topology in such way that you need to configure SW1 as primary root for VLAN 500 and secondary for VLAN 600 and SW2 as primary root for VLAN 600 and secondary for VLAN 500. Which configuration step is valid?

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

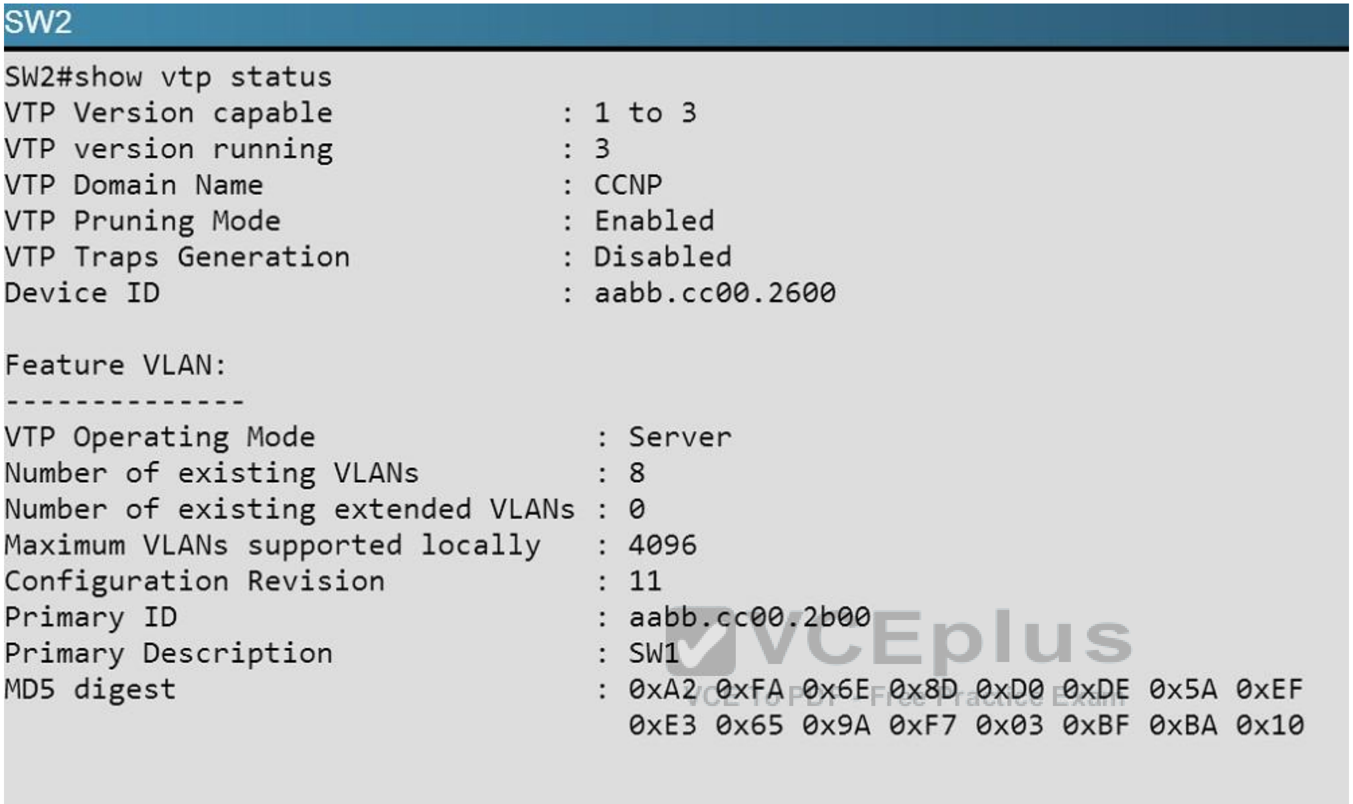
Explanation/Reference:
Explanation:

By issuing the “show vtp status command on SW2, 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.



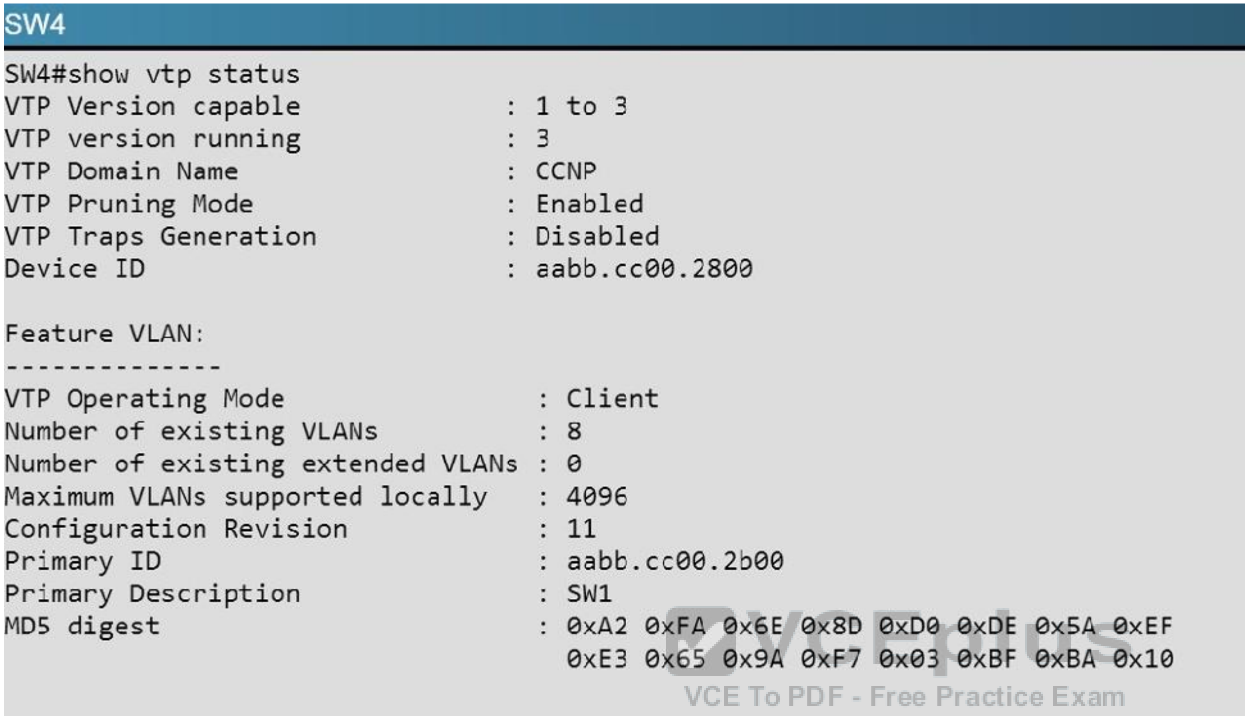
```
SW1#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 3
VTP Domain Name                 : CCNP
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc00.2500

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#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
```



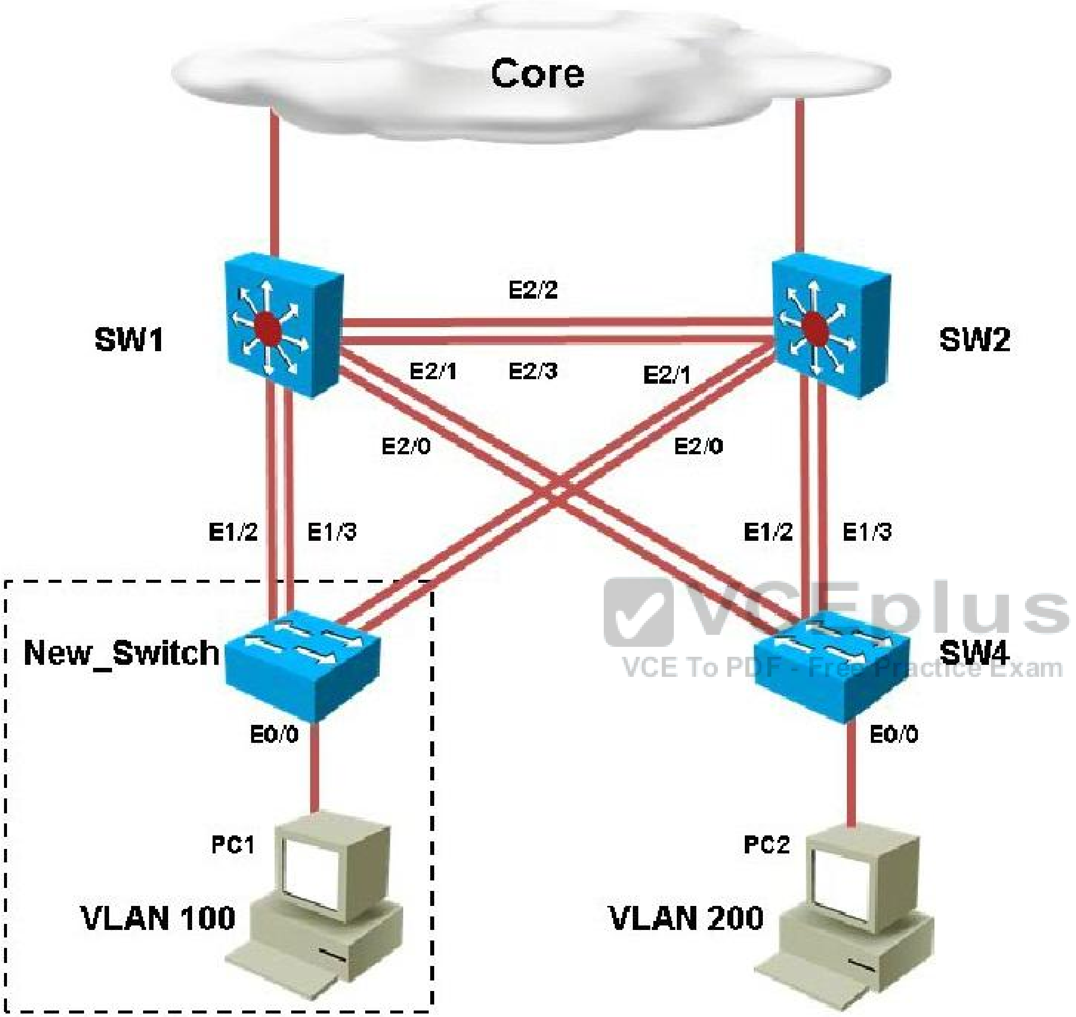
SW4

```
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 91

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.


Core
SW1
SW2
E2/2
E2/1
E2/3
E2/1
E2/0
E2/0
E1/2
E1/3
E1/2
E1/3
New_Switch
SW4
E0/0
E0/0
PC1
PC2
VLAN 100
VLAN 200

```
SW1#
```

```
SW2#
```

```
New_Switch#
```

```
SW4#
```

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 92
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 93
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 94
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 95
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

QUESTION 96
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 97
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 wIen 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-catl3fixed.html#ipsourceguard

QUESTION 98
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: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swdhcp82.html#wp1069615

QUESTION 99
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.

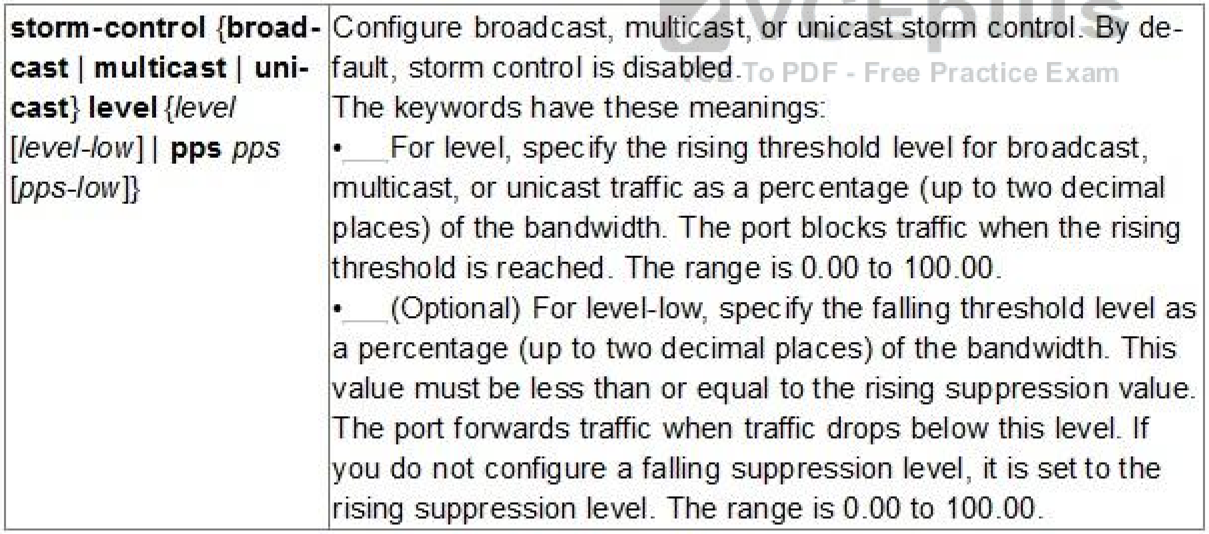
Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swdhcp82.html#wp1069615

QUESTION 100
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:



storm-control {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **pps** *pps* [*pps-low*]}	Configure broadcast, multicast, or unicast storm control. By default, storm control is disabled. The keywords have these meanings: • 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. • (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.

In this case, the broadcast keyword was used so only broadcast traffic is limited.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swtrafc.html

QUESTION 101
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

QUESTION 102
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 103

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: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_22ea/SCG/scg/swtrafc.html

QUESTION 104

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

QUESTION 105
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”
- Comma“ds — Applies to the EXEC mode com”ands 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

QUESTION 106
Which authentication service is needed to configure 802.1x?

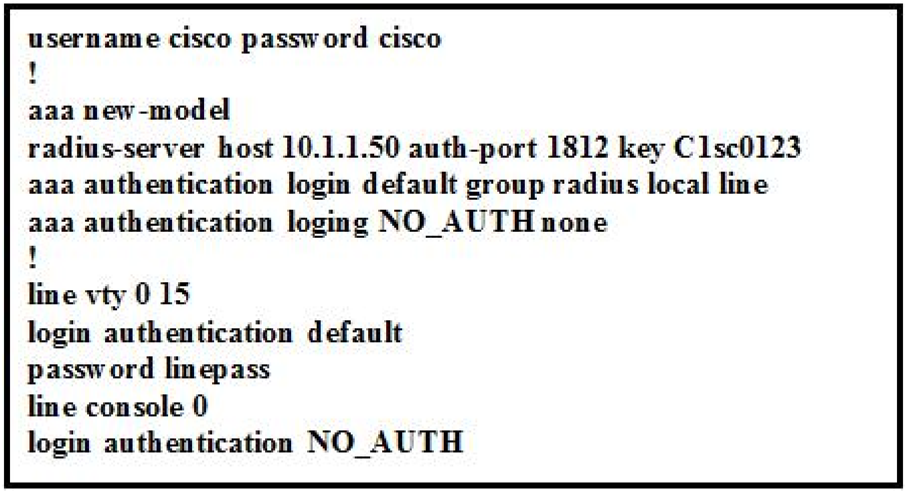
A. RADIUS with EAP Extension
B. TACACS+
C. RADIUS with CoA
D. RADIUS using VSA

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.**

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2940/software/release/12-1_19_ea1/configuration/guide/2940scg_1/sw8021x.pdf

QUESTION 107
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 loging NO_AUTH none
!
line vty 0 15
login authentication default
password linepass
line console 0
login authentication NO_AUTH
```

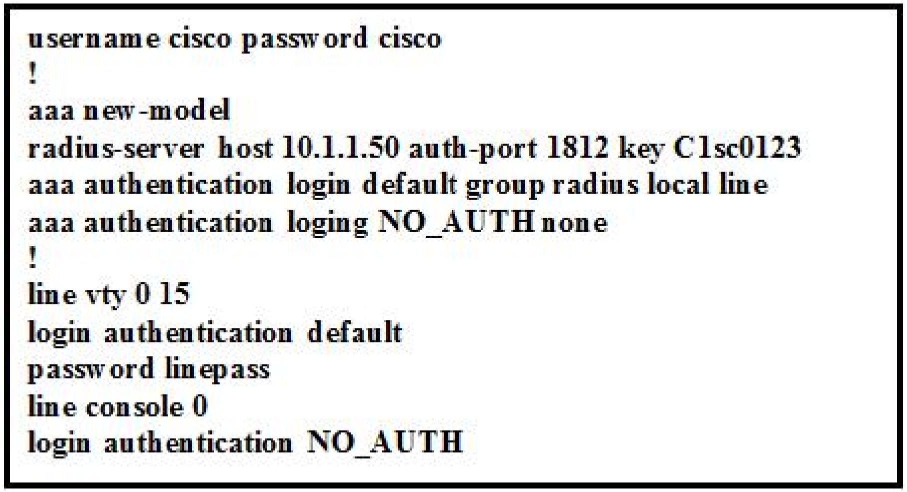
Which login credentials are required when connecting to the console port in this output?

A. none required
B. 115sernamee 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 108
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 loging 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 109
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 110
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-catl3fixed.html

QUESTION 111
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 112
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

QUESTION 113
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.

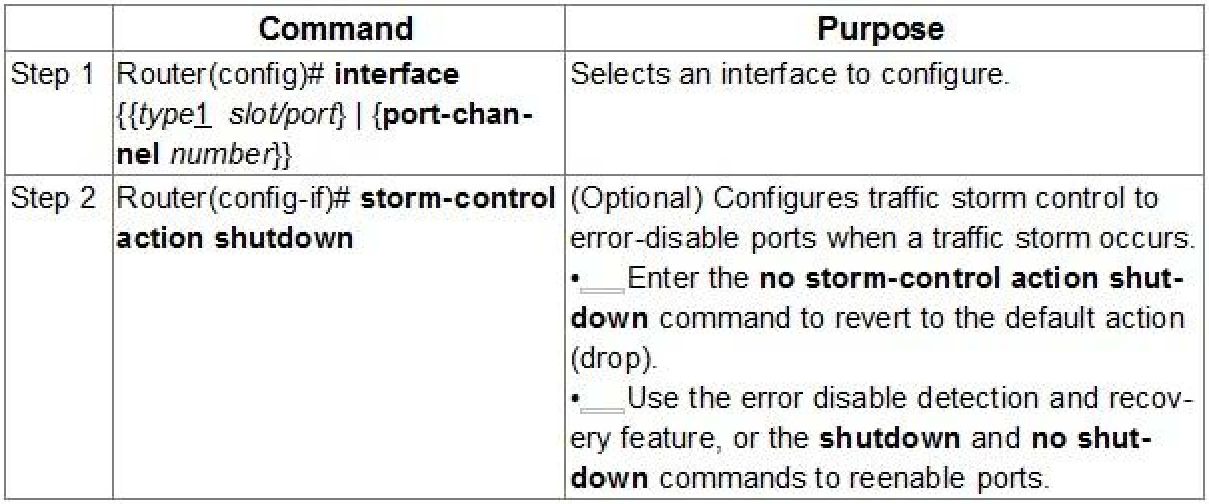
Reference: http://3c3cc.com/c/en/us/td/docs/routers/7600/ios/122SR/configuration/guide/swcg/dos.pdf

QUESTION 114
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)# **interface** {{*type1 slot/port*} | {**port-channel** *number*}}	Selects an interface to configure.
Step 2	Router(config-if)# **storm-control action shutdown**	(Optional) Configures traffic storm control to error-disable ports when a traffic storm occurs. • Enter the **no storm-control action shutdown** command to revert to the default action (drop). • Use the error disable detection and recovery feature, or the **shutdown** and **no shutdown** commands to reenable ports.

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

QUESTION 115
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

QUESTION 116
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

QUESTION 117
On which interface can port security be configured?

A. static trunk ports
B. destination port for SPAN
C. EtherChannel port group
D. dynamic access point

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

QUESTION 118
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

QUESTION 119
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

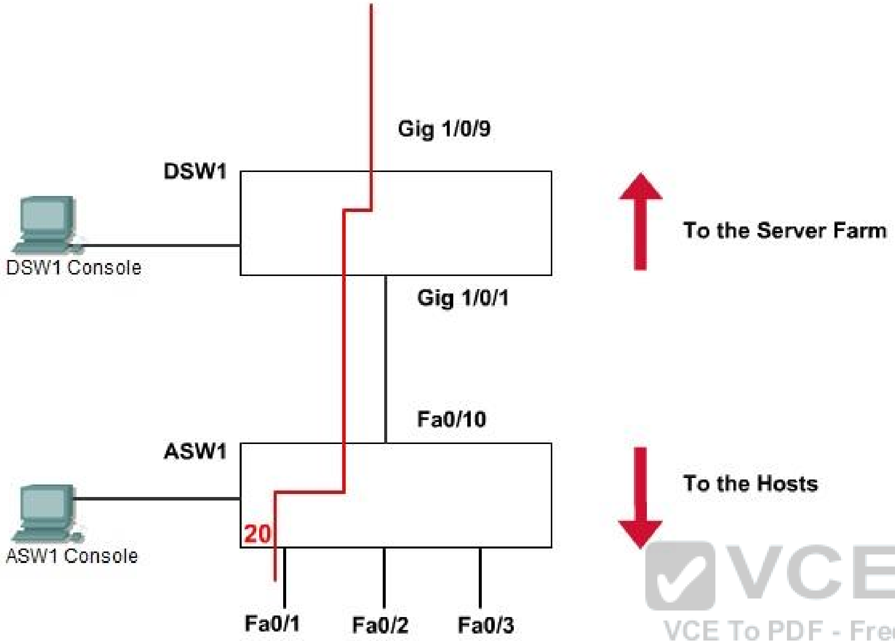
Explanation

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).

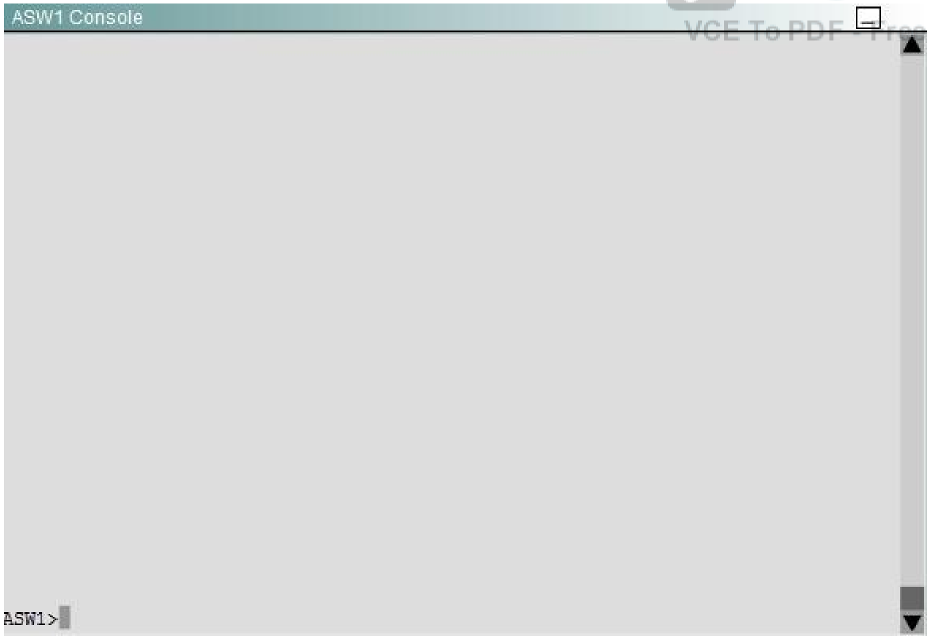
- Promiscuous port (P-Port): The switch port connects to a router, firewall or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port 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

Q32 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 polices 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 portfO/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.


Gig 1/0/9
DSW1
DSW1 Console
To the Server Farm
Gig 1/0/1
Fa0/10
ASW1
ASW1 Console
To the Hosts
20
Fa0/1
Fa0/2
Fa0/3

```
DSW1>
```



```
ASW1>
```

Answer: The configuration:

```
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
```

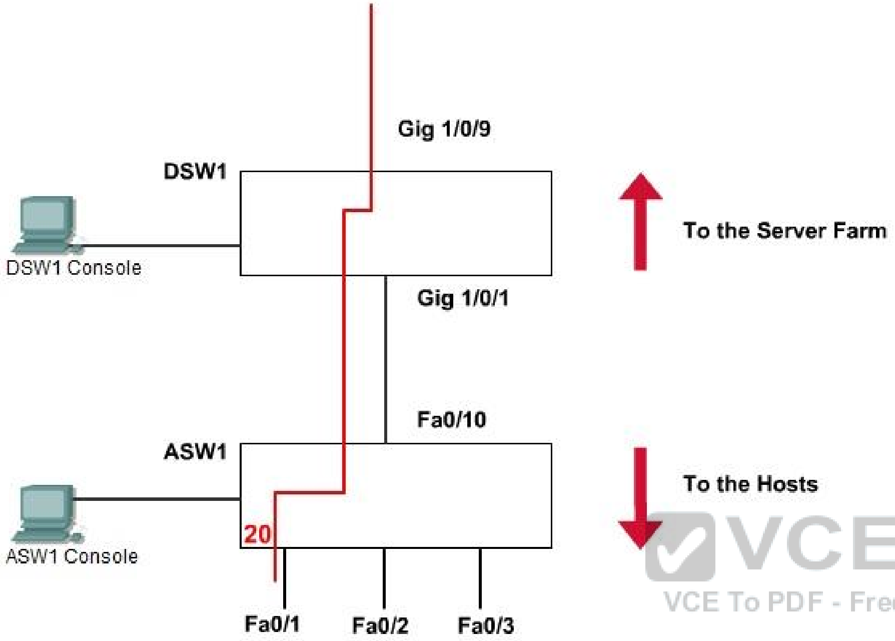
QUESTION 120

SIMULATION

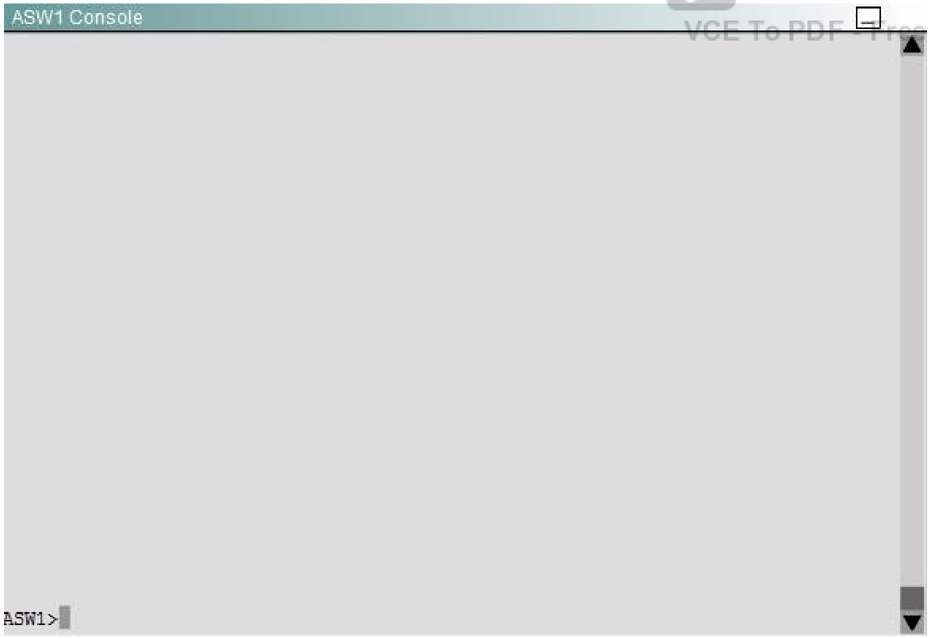
SWITCH.com is an IT company that has an existing enterprise network comprised of two layer 2 only switches; DSW1 and ASW1. The topology diagram indicates their layer 2 mapping. VLAN 20 is a new VLAN that will be used to provide the shipping personnel access to the server. Corporate polices do not allow 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 portfO/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.


Gig 1/0/9
DSW1
DSW1 Console
To the Server Farm
Gig 1/0/1
Fa0/10
ASW1
ASW1 Console
To the Hosts
20
Fa0/1
Fa0/2
Fa0/3

```
DSW1>
```



```
ASW1>
```

Correct Answer: Here is the solution below
Section: Infrastructure Security
Explanation

Explanation/Reference:
The configuration:
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
```

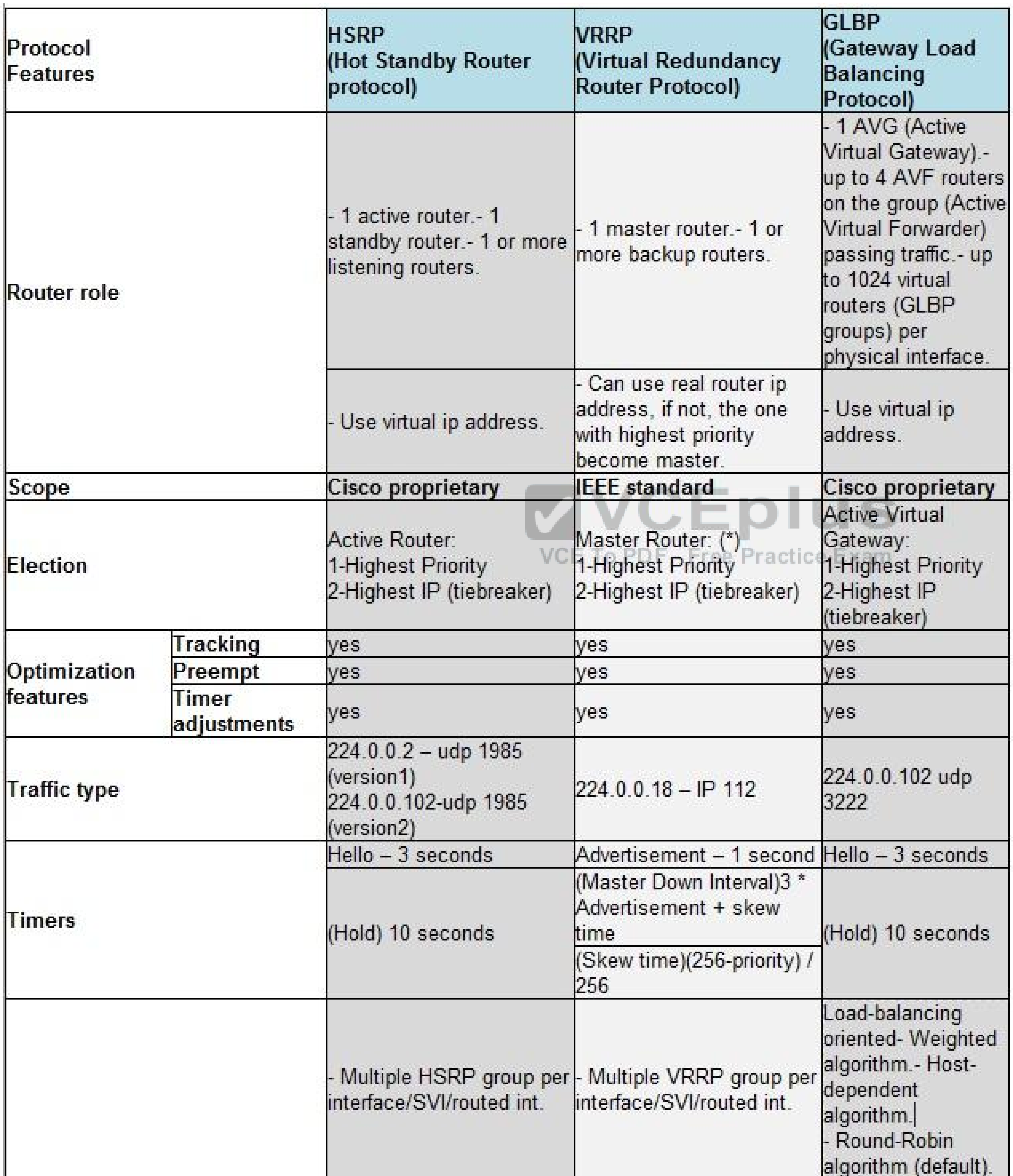
QUESTION 121
Which First Hop Redundancy Protocol is an IEEE Standard?

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 (Hot Standby Router protocol)	VRRP (Virtual Redundancy Router Protocol)	GLBP (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: 1-Highest Priority 2-Highest IP (tiebreaker)	Master Router: (*) 1-Highest Priority 2-Highest IP (tiebreaker)	Active Virtual Gateway: 1-Highest Priority 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) 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 * Advertisement + skew time	(Hold) 10 seconds
			(Skew time)(256-priority) / 256	
		- Multiple HSRP group per interface/SVI/routed int.	- Multiple VRRP group per interface/SVI/routed int.	Load-balancing oriented- Weighted algorithm.- Host-dependent algorithm. - Round-Robin algorithm (default).

Reference: http://cciethebeginning.wordpress.com/2008/08/23/router-high-availability-protocol-comparison-2/

QUESTION 122
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: http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/configuration/guide/swhsrp.html

QUESTION 123
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_glbp.html#wp1039651

QUESTION 124
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_glbp.html

QUESTION 125
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 — **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.** 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 126
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 127
Which command configures an HSRP group to become a slave of another HSRP group?

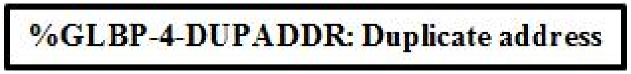
A. standby slave
B. standby group track
C. standby follow
D. standby group backup

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/fhp-hsrp-mgo.html

QUESTION 128
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

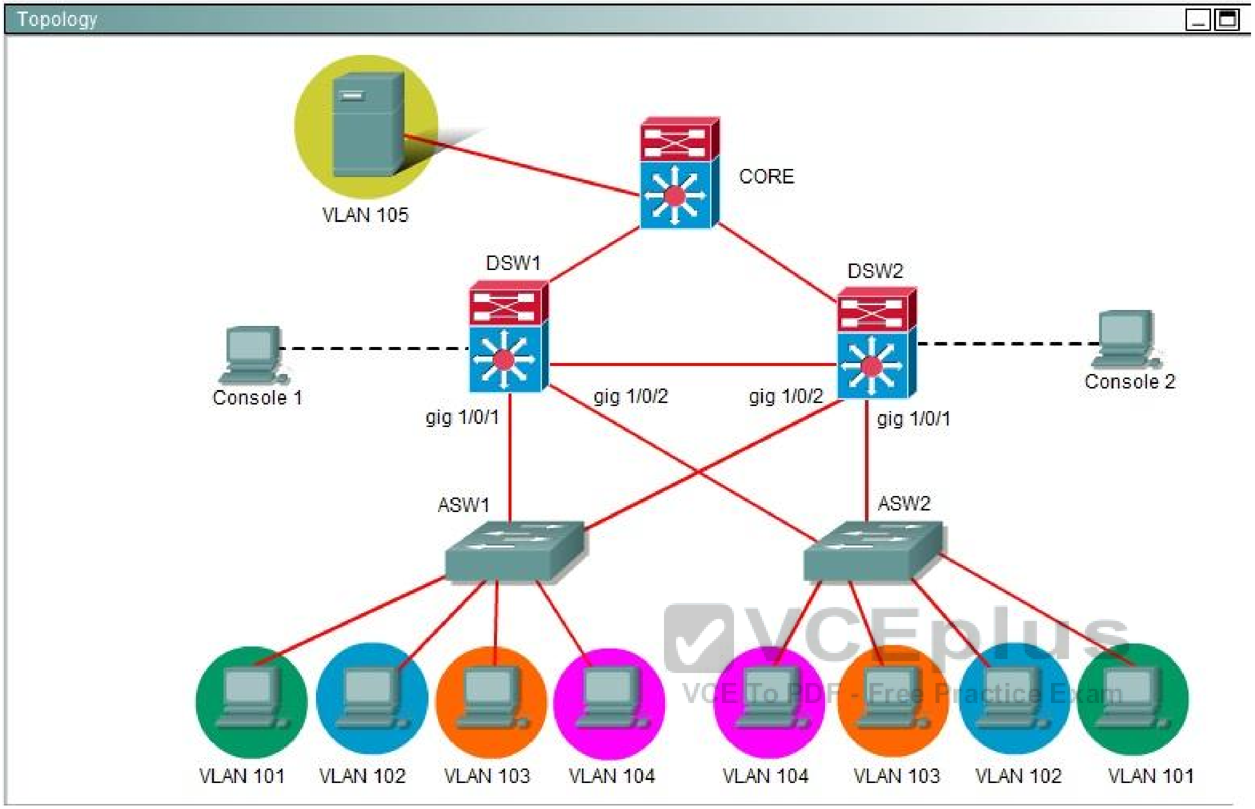
The error message indicates a possible layer2 loop and STP configuration issues.
In order to resolve this issue, issue the show interface command to verify the MAC address of the interface. If the MAC address of the interface is the same as the one reported in the error message, then it indicates that 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.

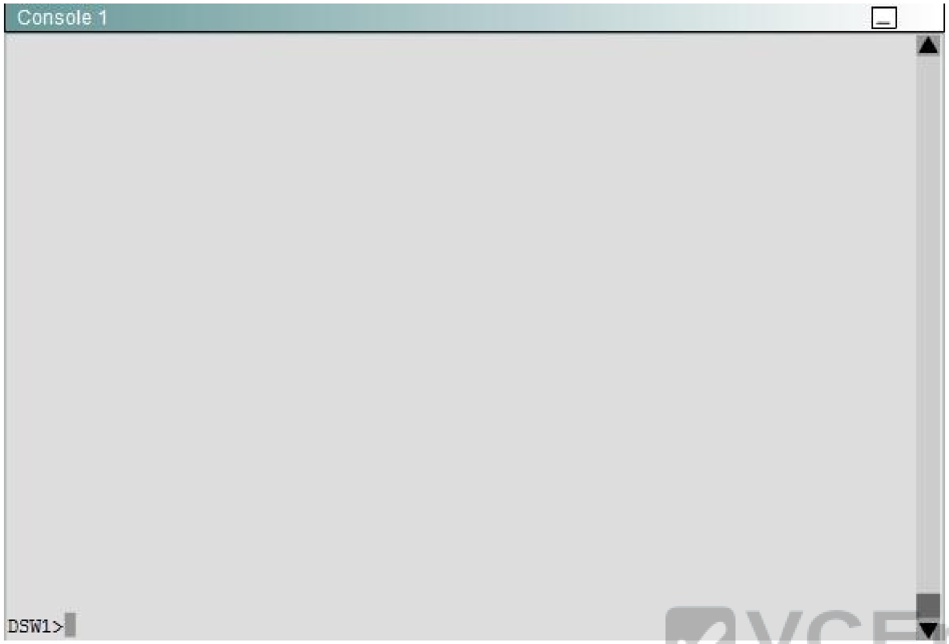
Reference: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807d2520.shtml#dr

QUESTION 129
Ferris Plastics, 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.

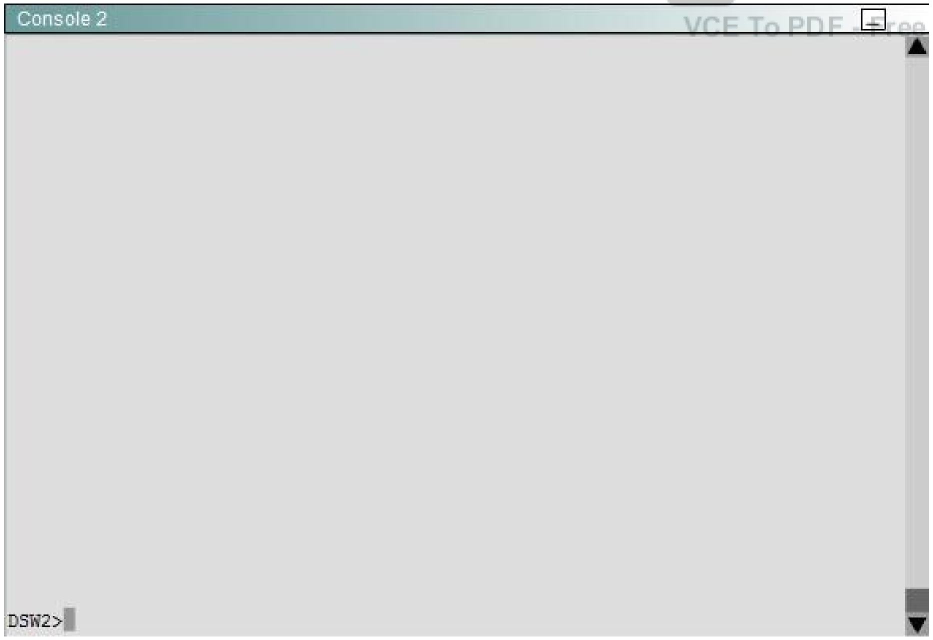
- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

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.


Topology
VLAN 105
CORE
DSW1
DSW2
Console 1
Console 2
gig 1/0/1
gig 1/0/2
gig 1/0/2
gig 1/0/1
ASW1
ASW2
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 104
VLAN 103
VLAN 102
VLAN 101



```
DSW1>
```



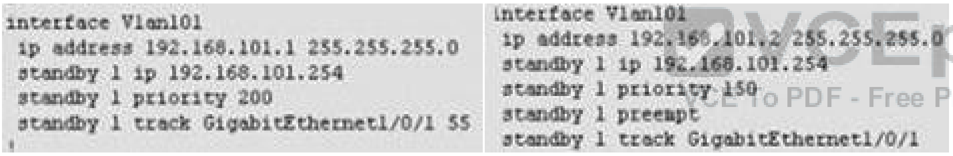
```
DSW2>
```

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 GigabitEthemet1/0/1 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 avaluethatis 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: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:



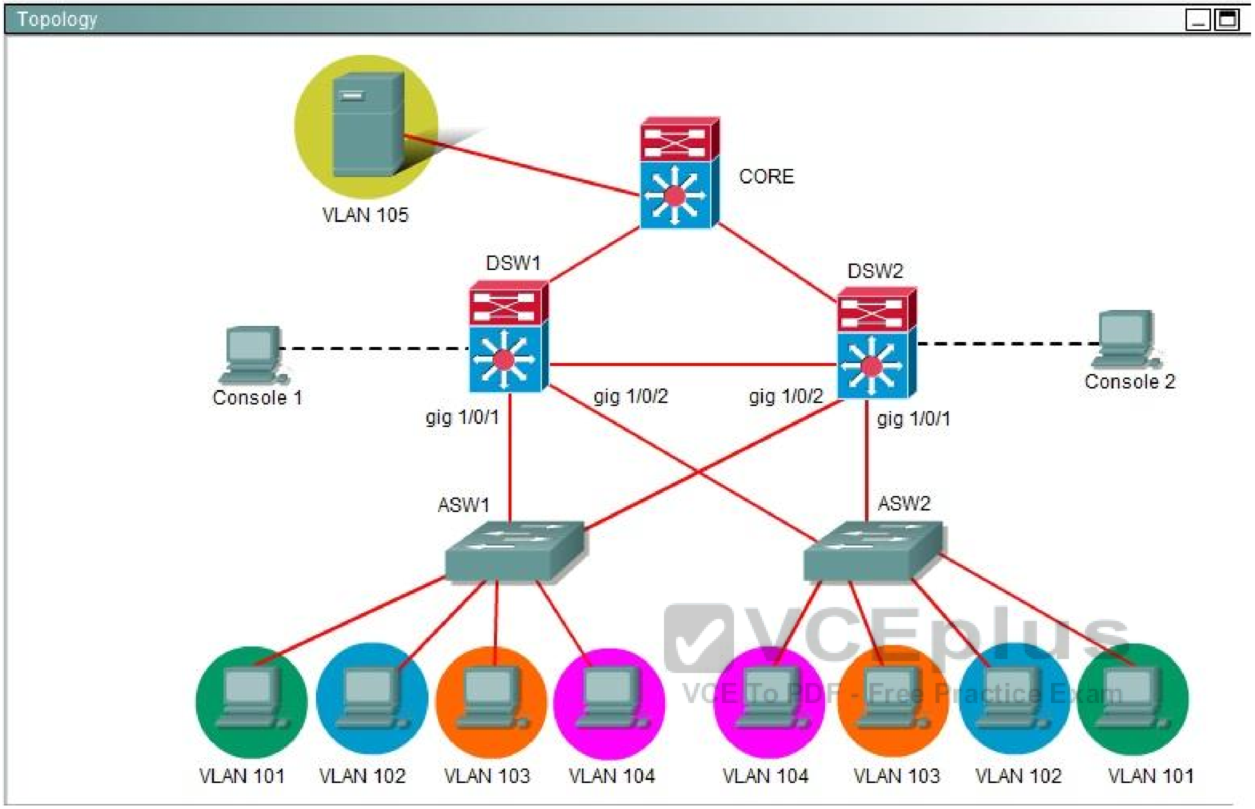
```
interface Vlan101
 ip address 192.168.101.1 255.255.255.0
 standby 1 ip 192.168.101.254
 standby 1 priority 200
 standby 1 track GigabitEthernet1/0/1 55
!
```

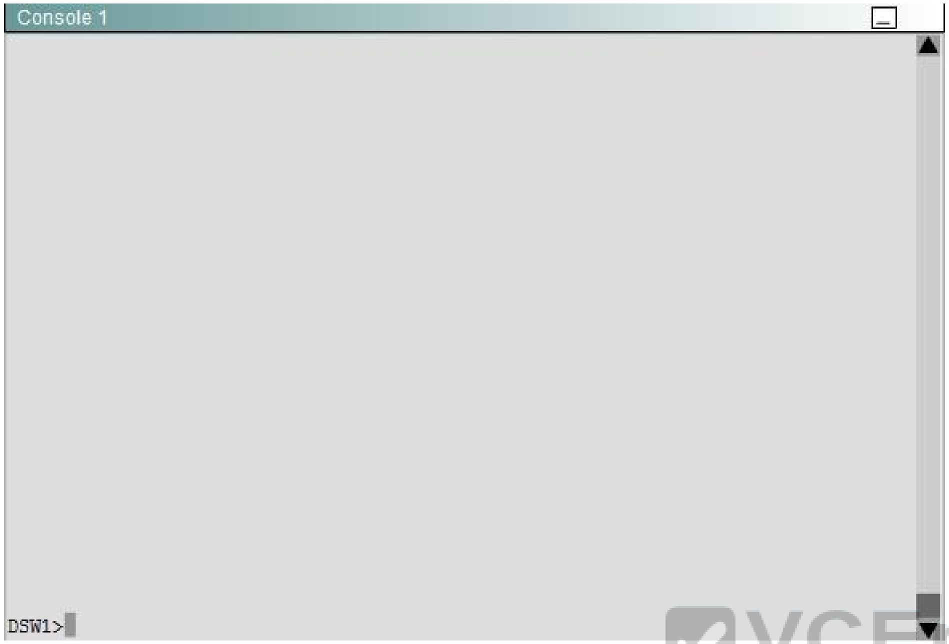
```
interface Vlan101
 ip address 192.168.101.2 255.255.255.0
 standby 1 ip 192.168.101.254
 standby 1 priority 150
 standby 1 preempt
 standby 1 track GigabitEthernet1/0/1
```

QUESTION 130
Ferris Plastics, 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.

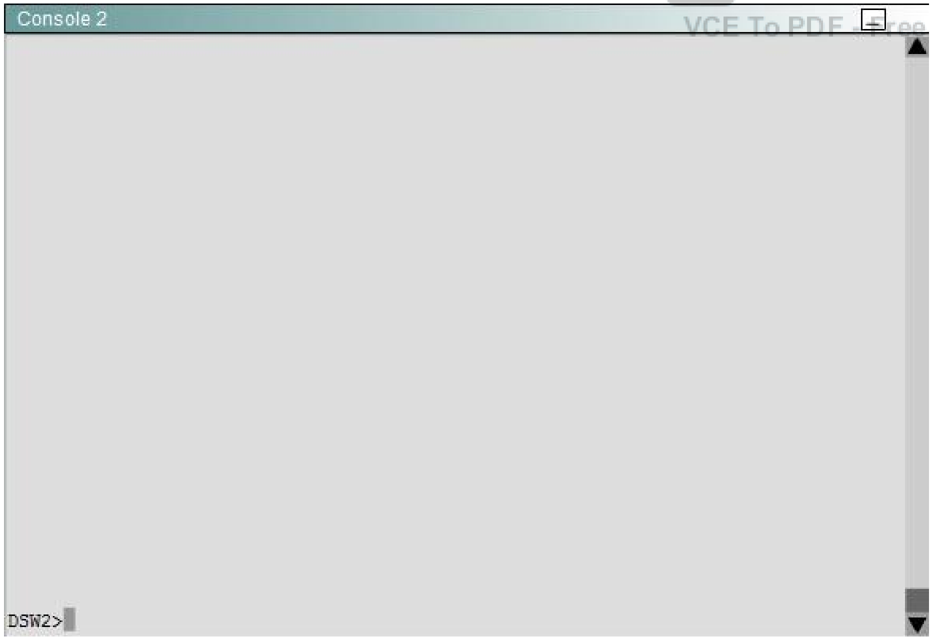
- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

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.


Topology
VLAN 105
CORE
DSW1
DSW2
Console 1
Console 2
gig 1/0/1
gig 1/0/2
gig 1/0/2
gig 1/0/1
ASW1
ASW2
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 104
VLAN 103
VLAN 102
VLAN 101



```
DSW1>
```



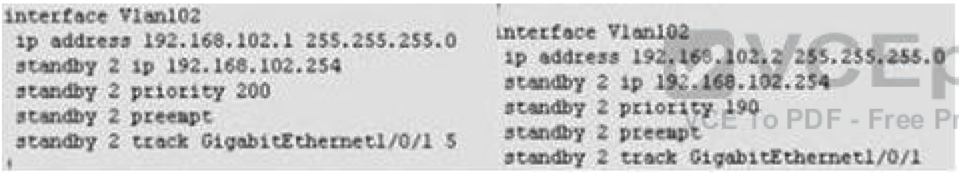
```
DSW2>
```

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 greaterthan 5 and less than 15. 0
B. The decrement value on DSW1 should be greaterthan 9 and less than 15.
C. The decrement value on DSW1 should be greaterthan 11 and less than 19.
D. The decrement value on DSWTs should be greaterthan 190 and less than 200.
E. The decrement value on DSWTs should be greaterthan 195 and less than 205.

Correct Answer: C
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:



```
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
```

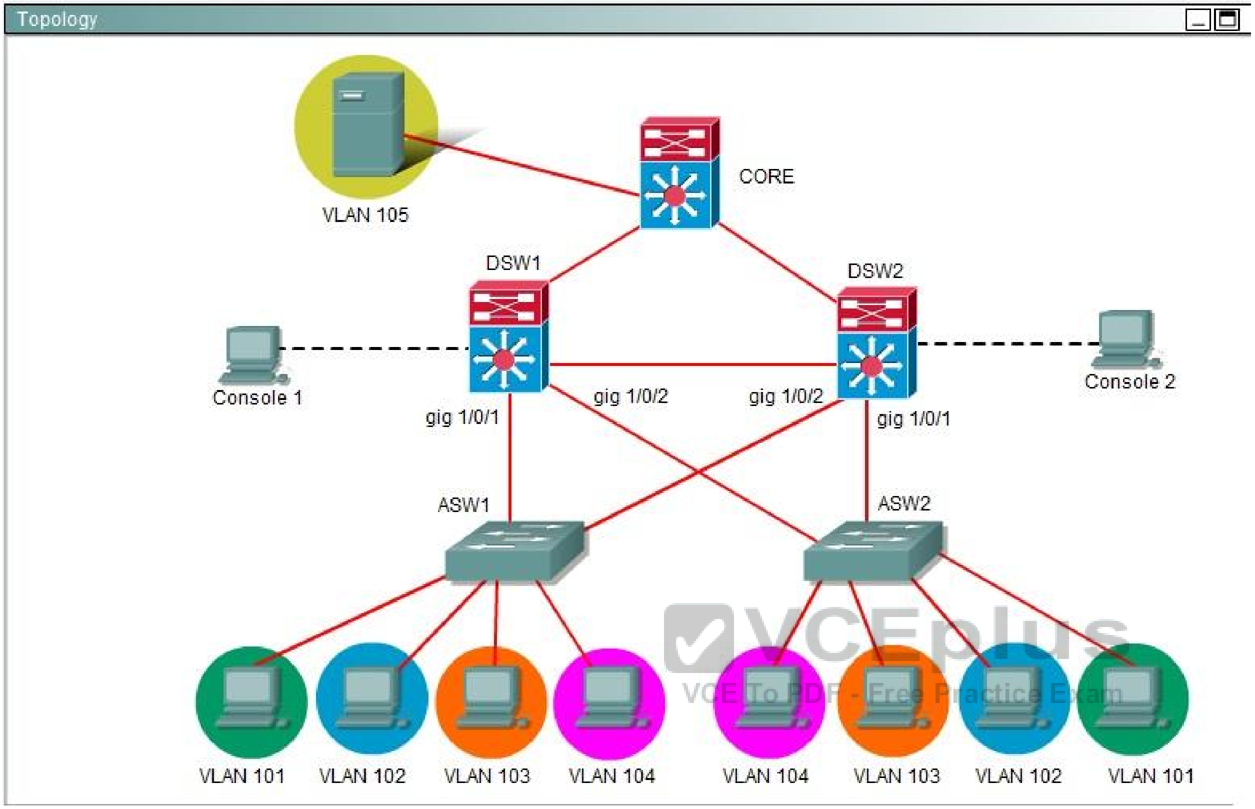
```
interface Vlan102
 ip address 192.168.102.2 255.255.255.0
 standby 2 ip 192.168.102.254
 standby 2 priority 190
 standby 2 preempt
 standby 2 track GigabitEthernet1/0/1
```

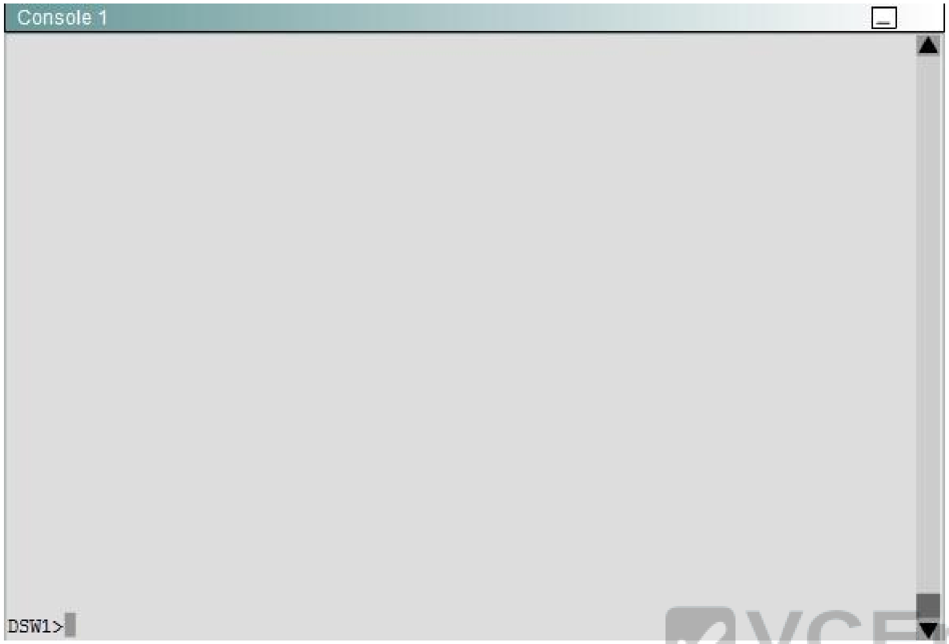
Use “show run” command to show. The left Vlan102 is console1 of DS1. Priority value is 200, we should decrement value in the track command from 11 to 18. Because 200 – 11 = 189 < 190 (priority of Vlan102 on DS2).

QUESTION 131
Ferris Plastics, 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.

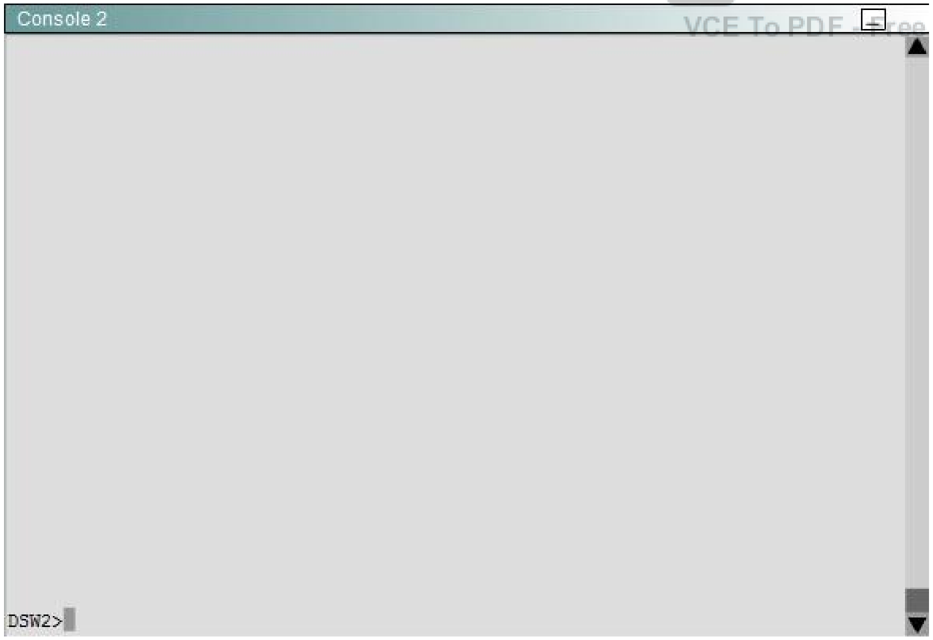
- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

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.


Topology
VLAN 105
CORE
DSW1
DSW2
Console 1
Console 2
gig 1/0/1
gig 1/0/2
gig 1/0/2
gig 1/0/1
ASW1
ASW2
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 104
VLAN 103
VLAN 102
VLAN 101



```
DSW1>
```



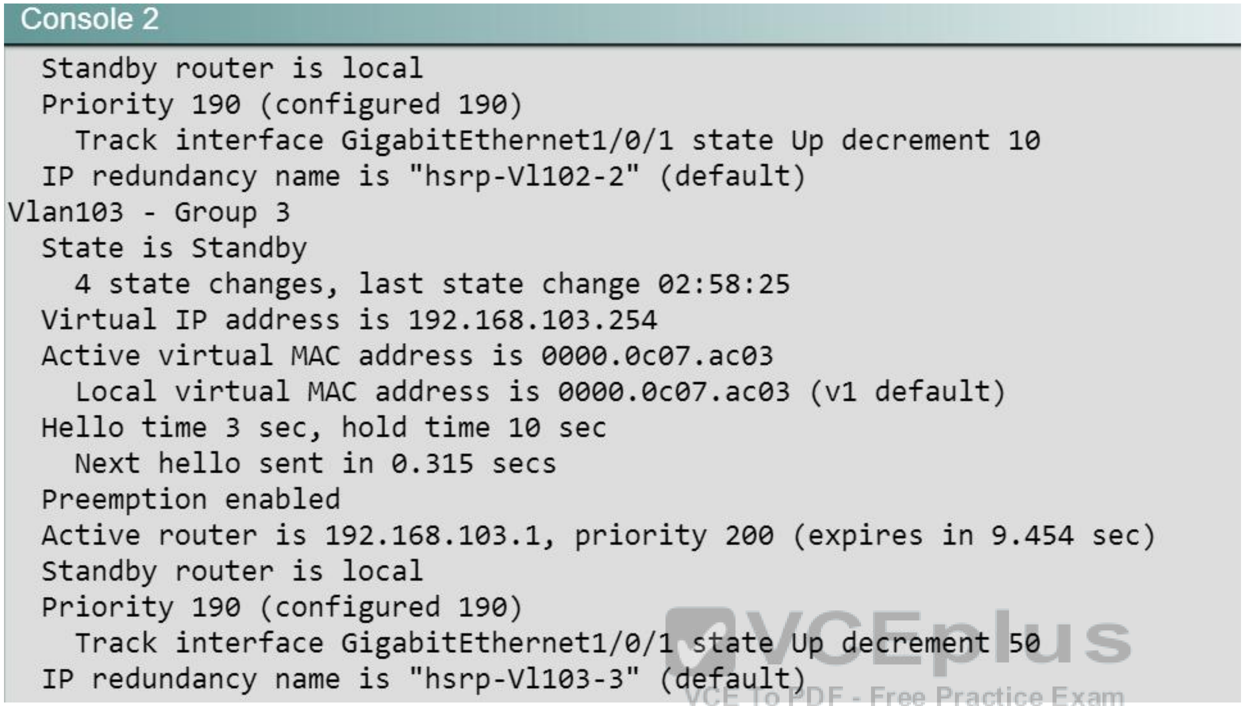
```
DSW2>
```

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

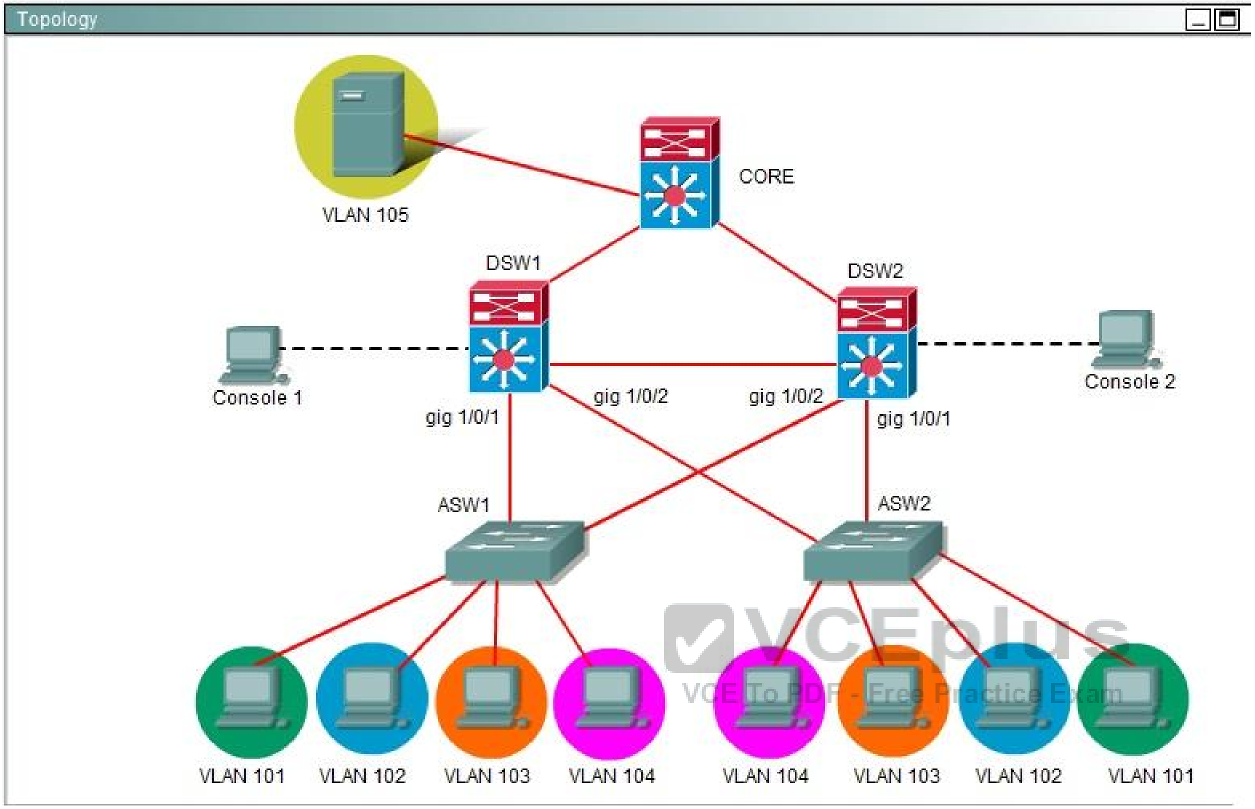
```
  Standby router is local
  Priority 190 (configured 190)
    Track interface GigabitEthernet1/0/1 state Up decrement 10
  IP redundancy name is "hsrp-Vl102-2" (default)
Vlan103 - Group 3
  State is Standby
    4 state changes, last state change 02:58:25
  Virtual IP address is 192.168.103.254
  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)
```

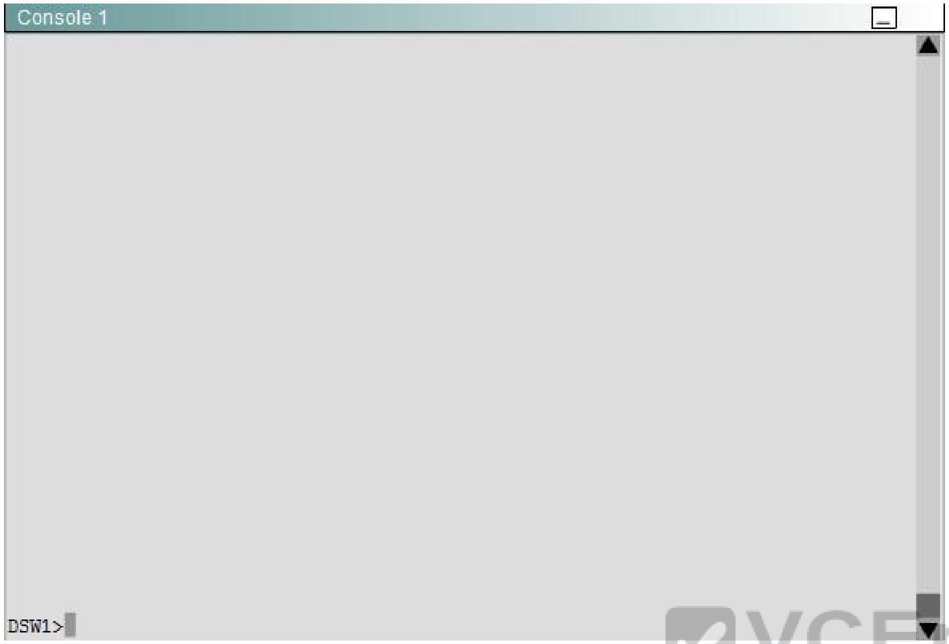
QUESTION 132

Ferris Plastics, 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.

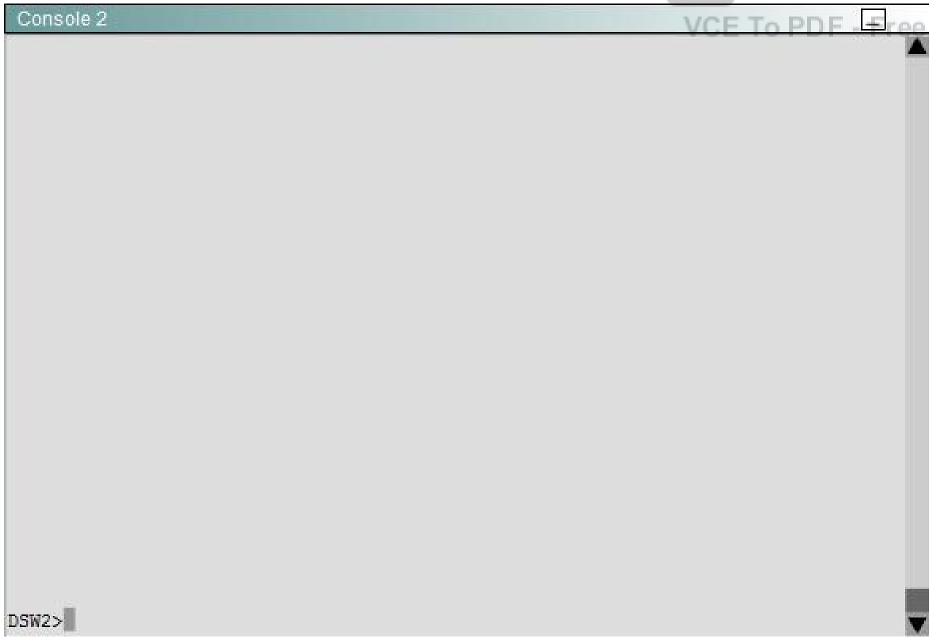
- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

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.


Topology
VLAN 105
CORE
DSW1
DSW2
Console 1
Console 2
gig 1/0/1
gig 1/0/2
gig 1/0/2
gig 1/0/1
ASW1
ASW2
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 104
VLAN 103
VLAN 102
VLAN 101



```
DSW1>
```



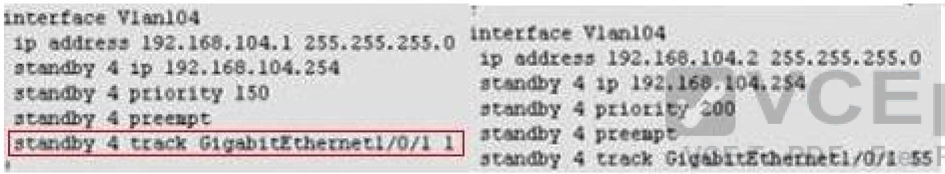
```
DSW2>
```

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 to 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:



```
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
```

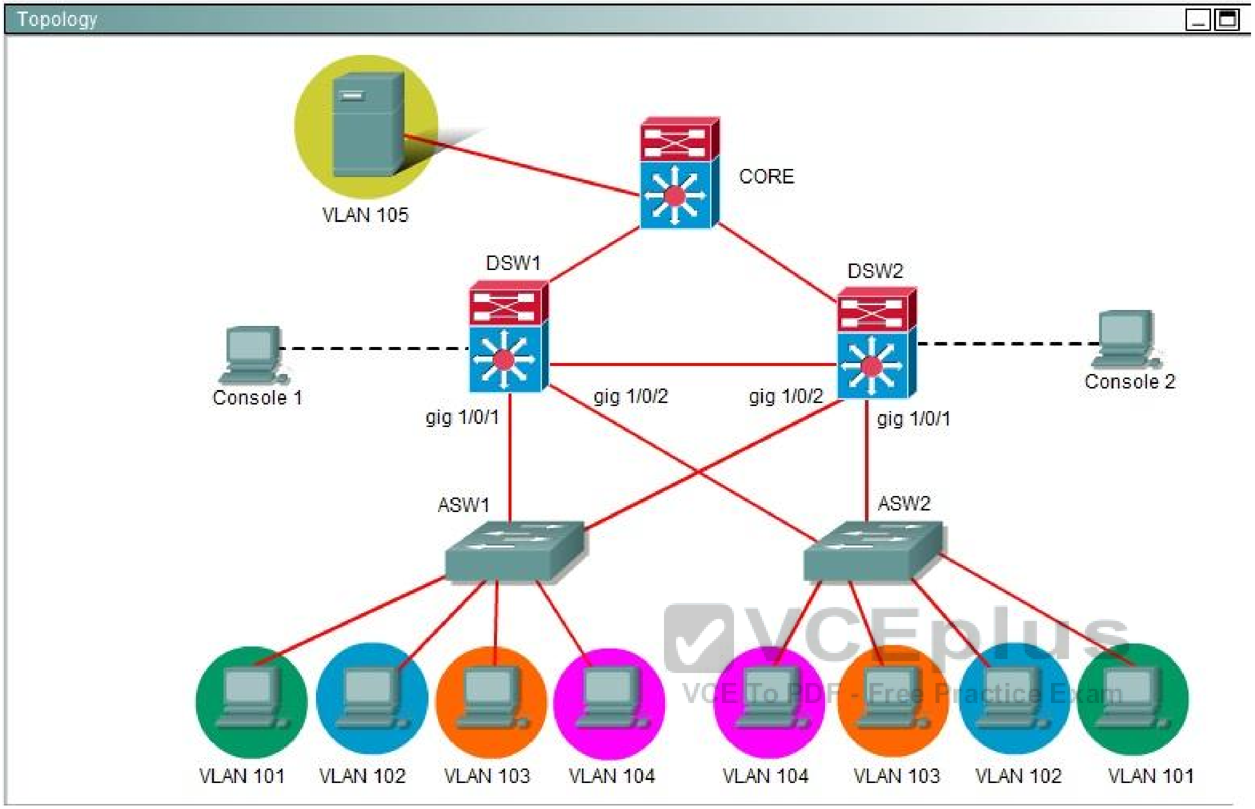
```
interface Vlan104
 ip address 192.168.104.2 255.255.255.0
 standby 4 ip 192.168.104.254
 standby 4 priority 200
 standby 4 preempt
 standby 4 track GigabitEthernet1/0/1 55
```

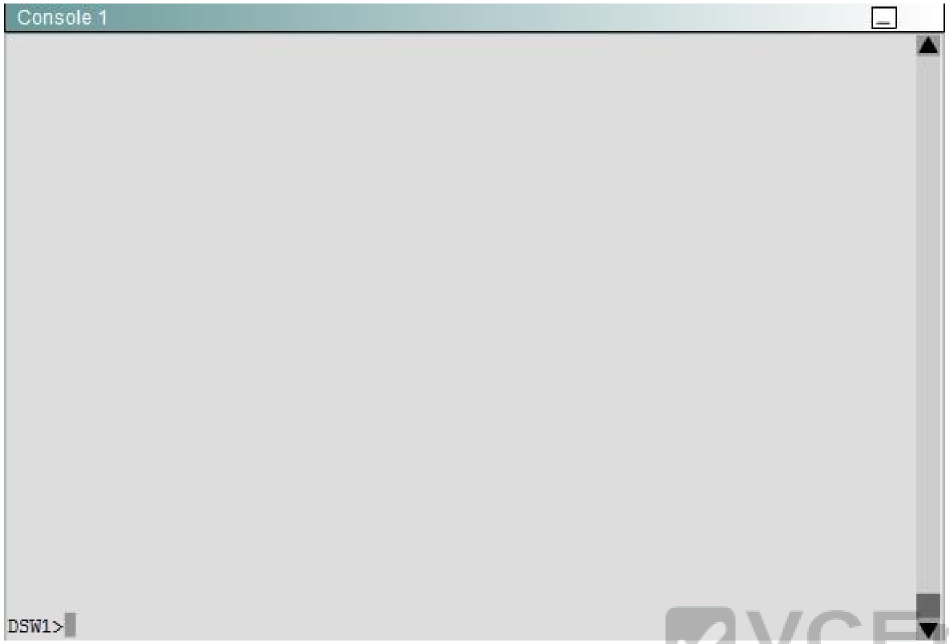
We should NOT disable preempt on DS1. By do that, you will make Vlan104's HSRP group fail function. Example: if we are disable preempt on DS1. It can not become active device when G1/0/1 on DS2 fail. In this question, G0/1/0 on DS1 & DS2 is shutdown. Vlan104 (left): 150 – 1 = 149. Vlan104 (right): 200 – 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 (> or = 6). Vlan104 (left): 150 – 6 = 144. Result is priority 144 < 145 (vlan104 on DS2 is active).

QUESTION 133
Ferris Plastics, 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.

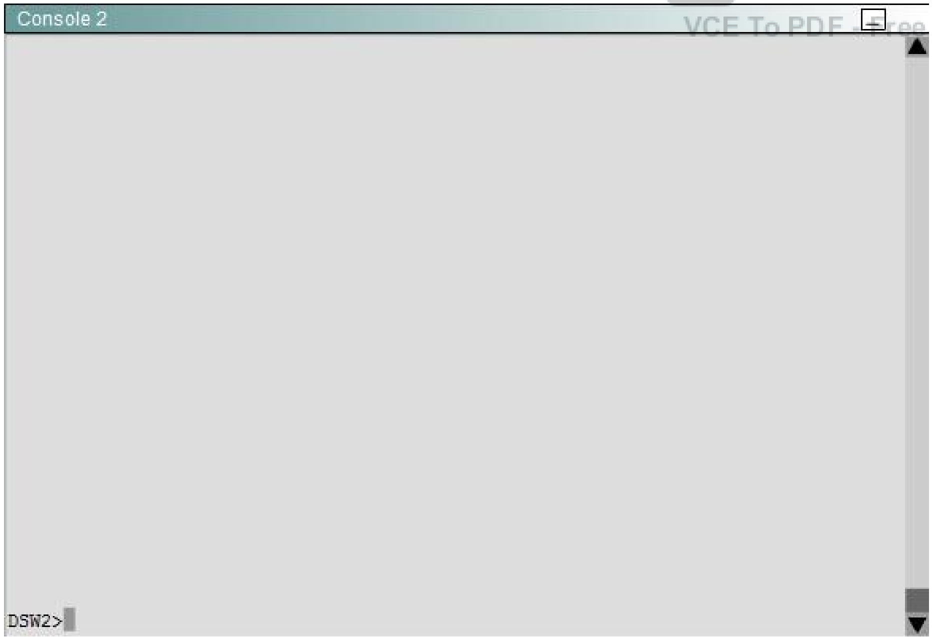
- DSW1 – primary device for VLAN 101 VLAN 102 and VLAN 105
- DSW2 – primary device for VLAN 103 and VLAN 104
- A failure of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

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.


Topology
VLAN 105
CORE
DSW1
DSW2
Console 1
Console 2
gig 1/0/1
gig 1/0/2
gig 1/0/2
gig 1/0/1
ASW1
ASW2
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 104
VLAN 103
VLAN 102
VLAN 101



```
DSW1>
```



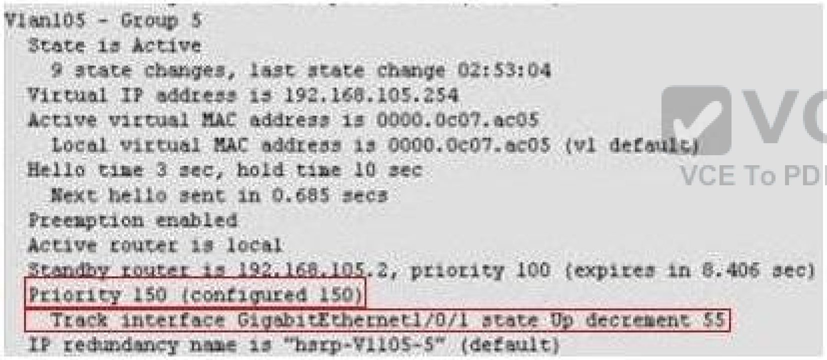
```
DSW2>
```

What is the priority value of the VLAN 105 HSRP group on DSW2?

A. 50
B. 100
C. 150
D. 200

Correct Answer: B
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Use "show standby brief" command on console2. Very easy to se“ priority of Vlan1”5 is 100.

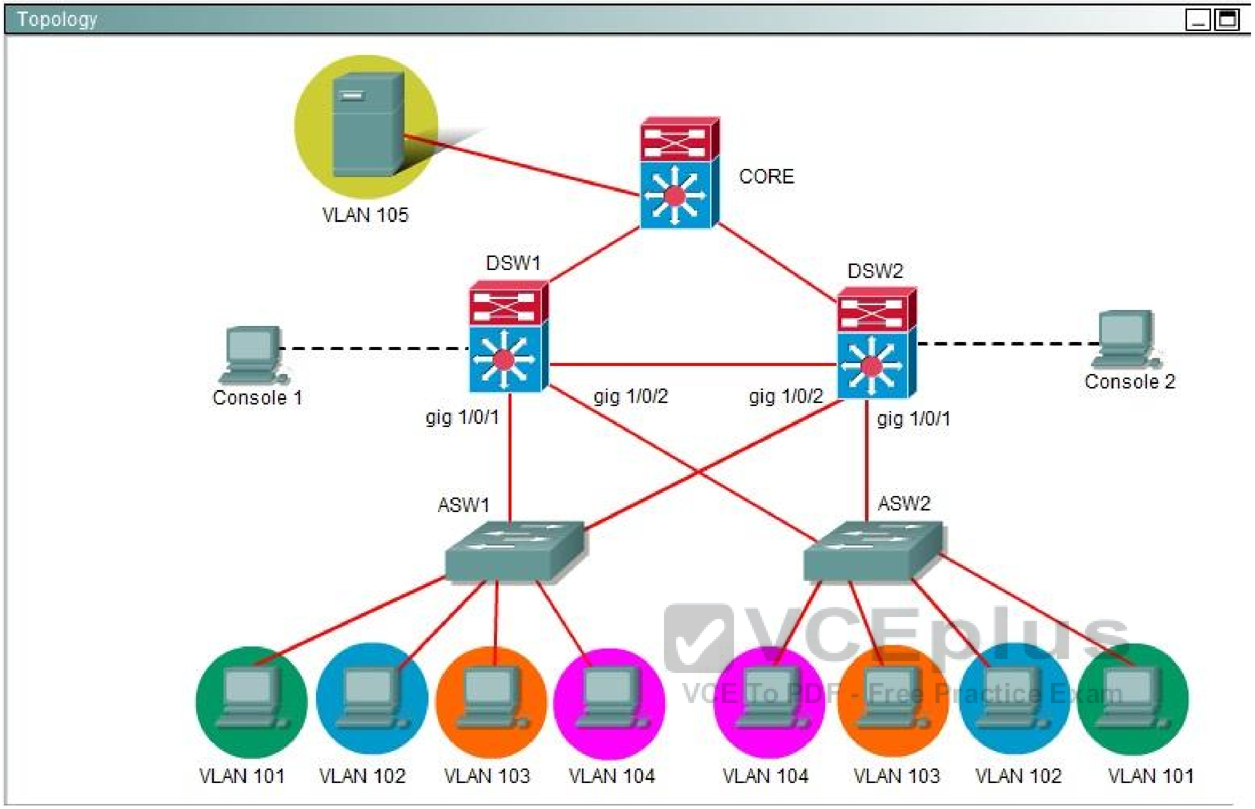


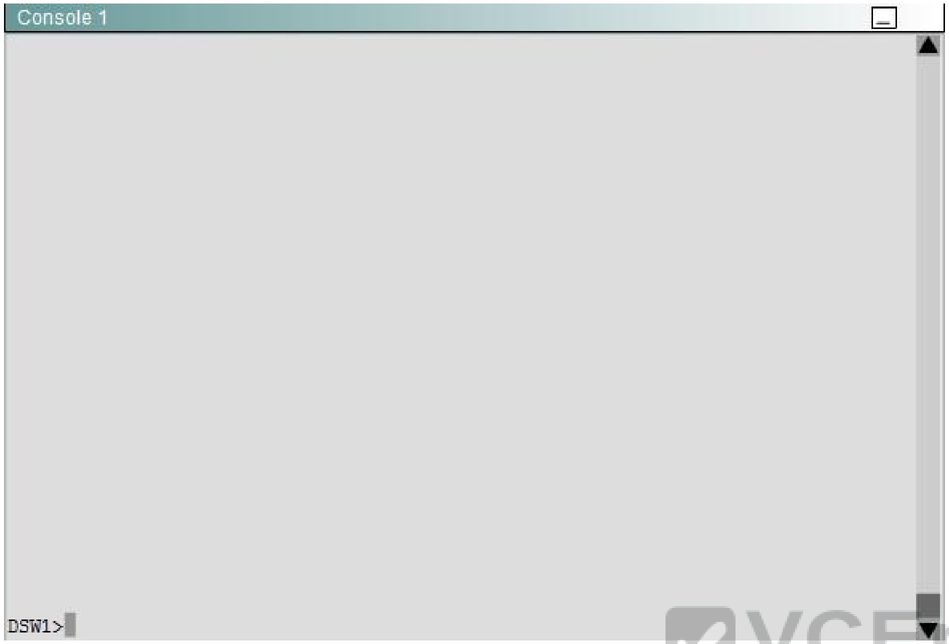
```
Vlan105 - Group 5
  State is Active
    9 state changes, last state change 02:53:04
  Virtual IP address is 192.168.105.254
  Active virtual MAC address is 0000.0c07.ac05
    Local virtual MAC address is 0000.0c07.ac05 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.685 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 "hsrp-Vl105-5" (default)
```

QUESTION 134
Ferris Plastics, 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.

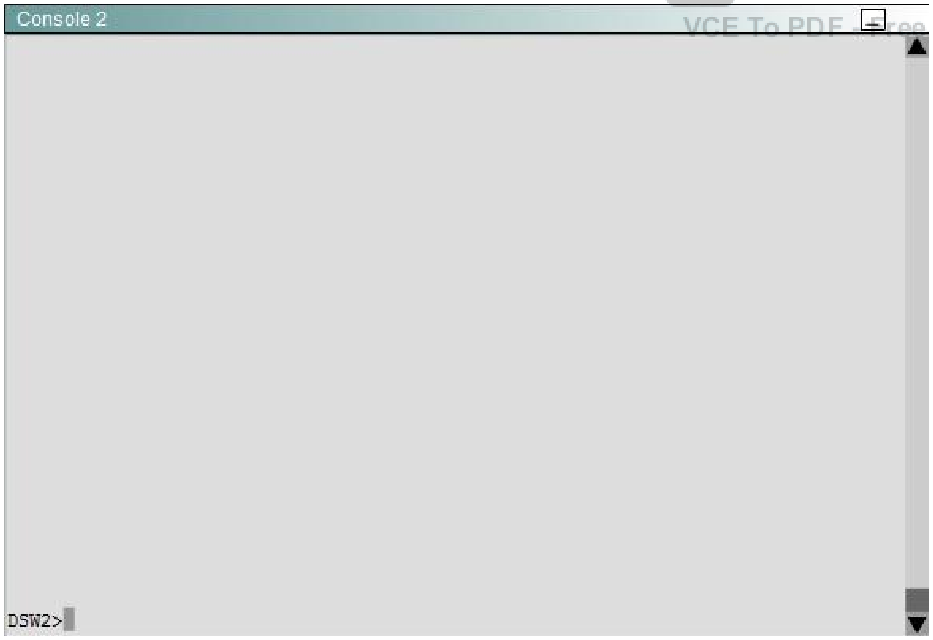
- DSW1 - primary device for VLAN 101 VLAN 102 and VLAN 105
- D–W2 - primary device for VLAN 103 and VLAN 104
- A failure–of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed.

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.


Topology
VLAN 105
CORE
DSW1
DSW2
Console 1
Console 2
gig 1/0/1
gig 1/0/2
gig 1/0/2
gig 1/0/1
ASW1
ASW2
VLAN 101
VLAN 102
VLAN 103
VLAN 104
VLAN 104
VLAN 103
VLAN 102
VLAN 101



```
DSW1>
```



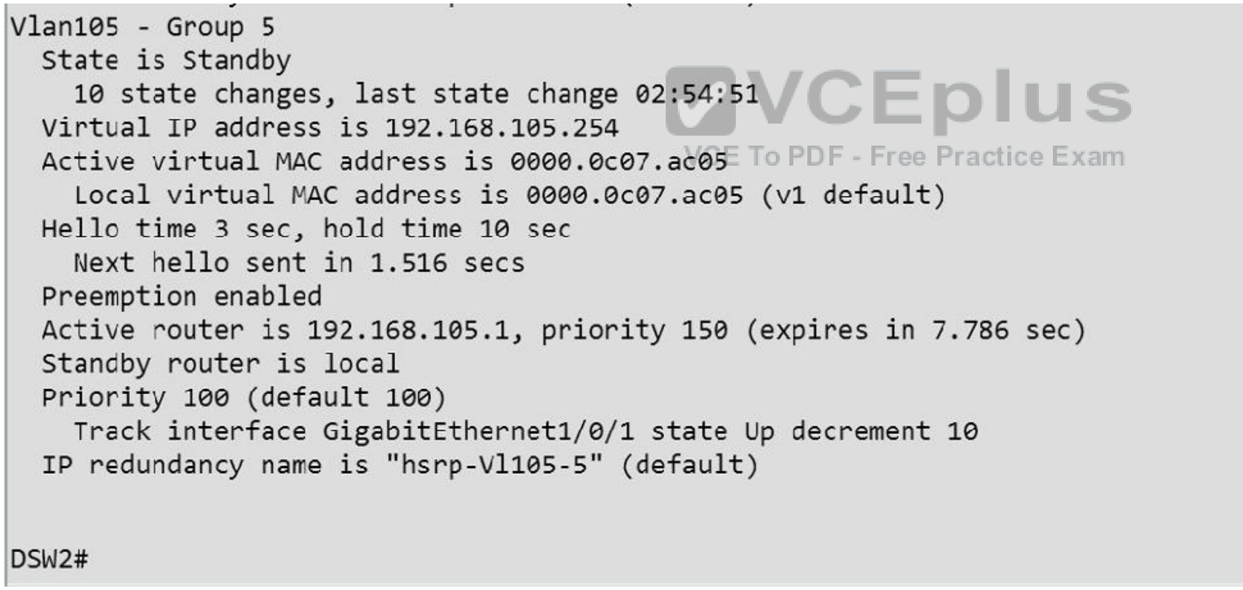
```
DSW2>
```

If GigabitEthemet1/0/1 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

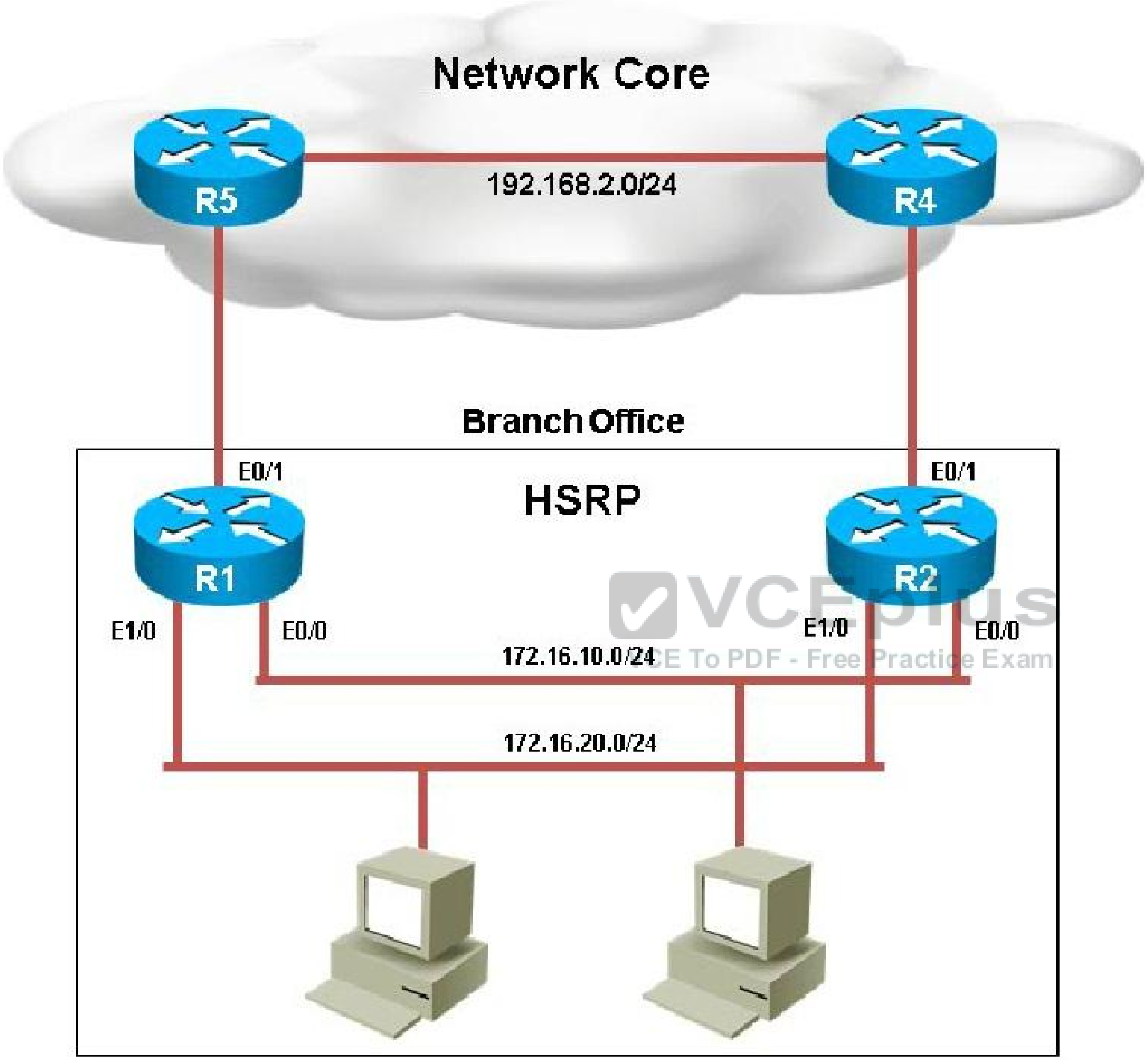
Explanation/Reference:
Explanation
As seen below, the current priority for VLAN 105 is 100, and the tracking feature for Gig 1/0/0 is enabled which will decrement the priority by 10 if this interface goes down for a priority value of 90.



```
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 135
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.


Network Core
R5
R4
192.168.2.0/24
Branch Office
HSRP
E0/1
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24

```
R1#
```

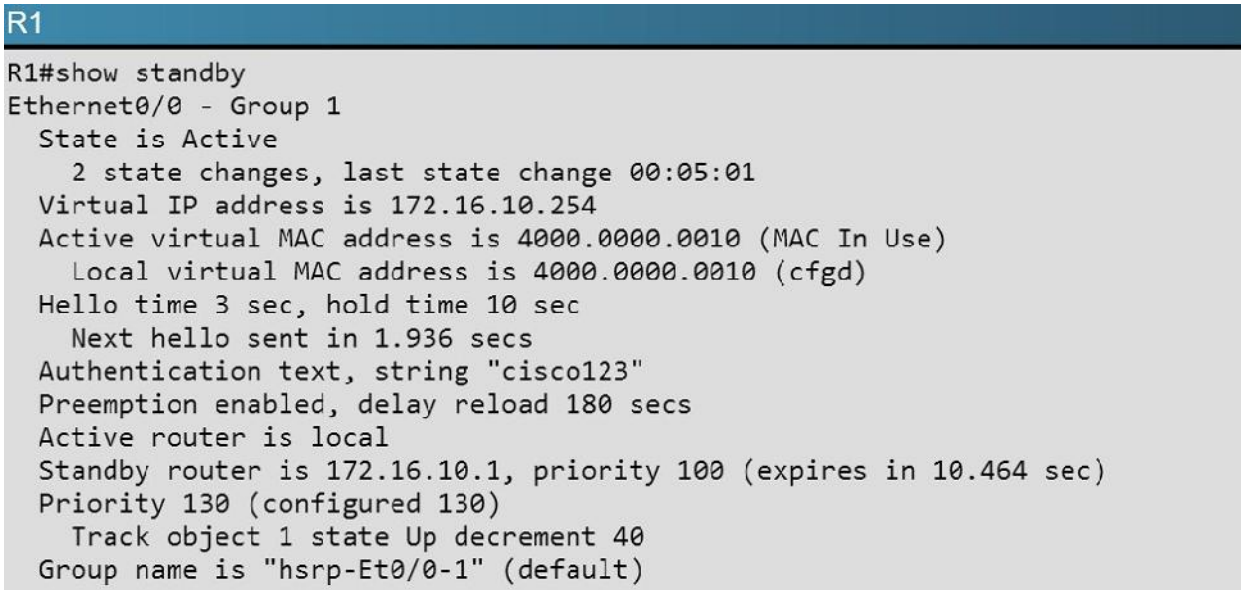
```
R2#
```

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.

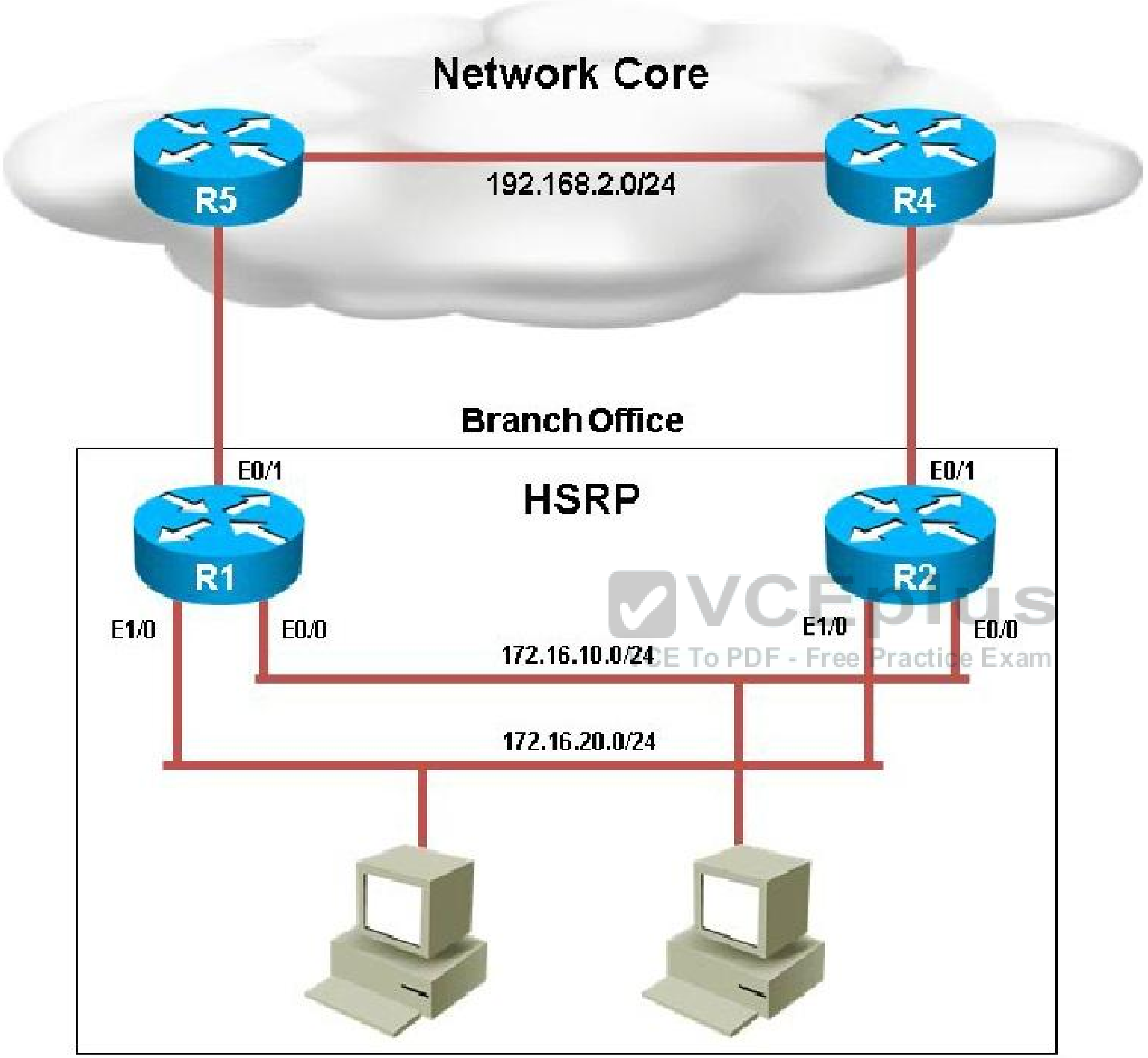


R1

```
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 136

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.


Network Core
R5
R4
192.168.2.0/24
Branch Office
HSRP
E0/1
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24

```
R1#
```

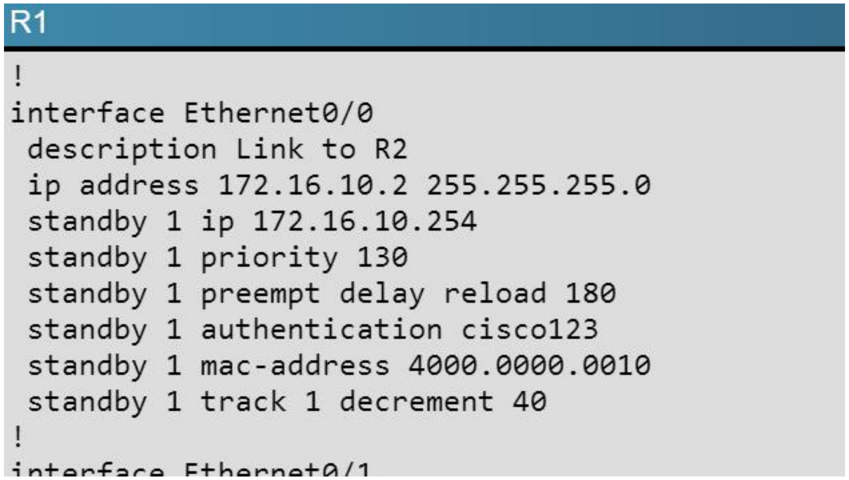
```
R2#
```

Refer to the exhibit. If router R1 interface Etherne0/0 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:



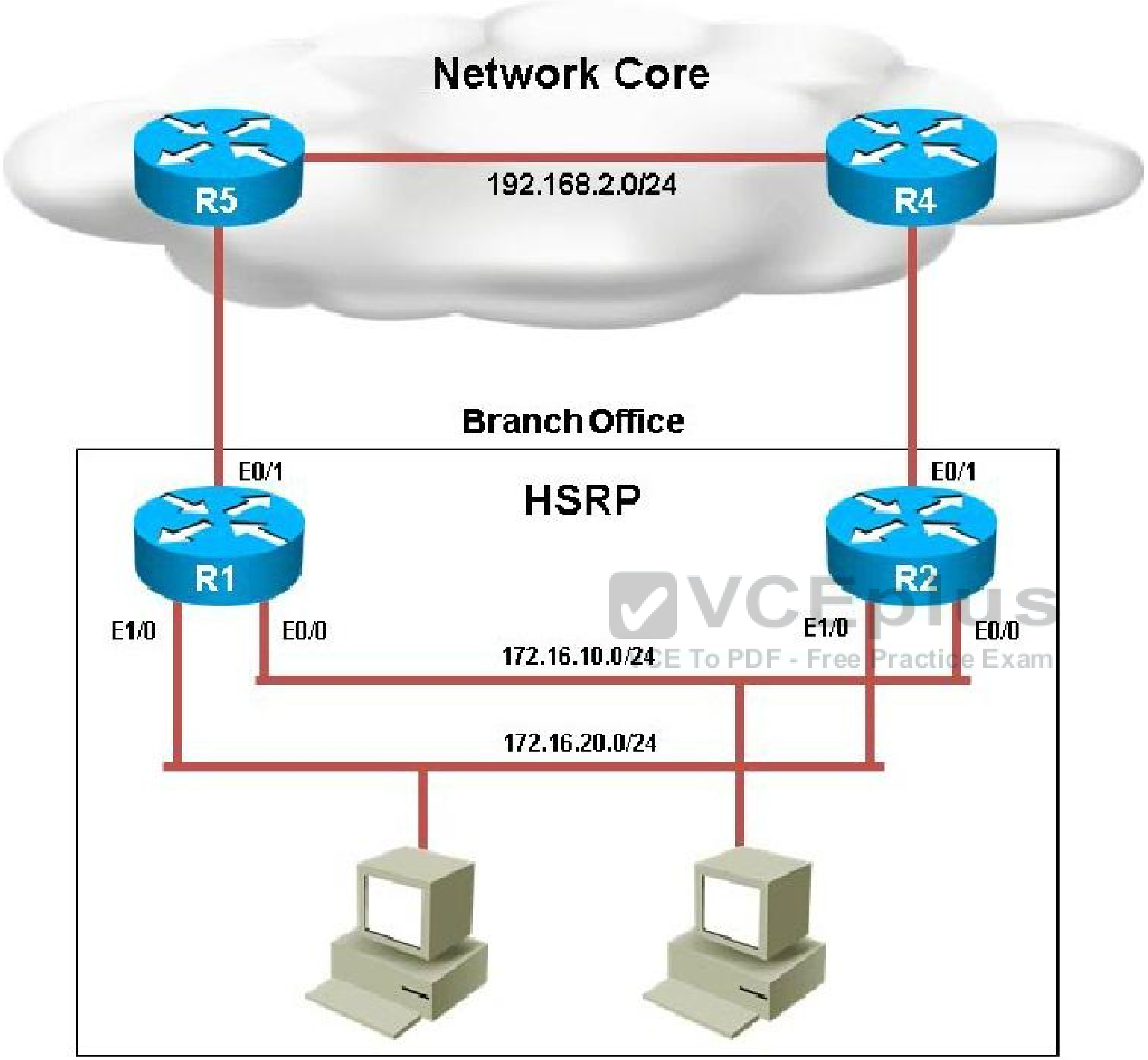
R1

```
!
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 137

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.


Network Core
R5
R4
192.168.2.0/24
Branch Office
HSRP
E0/1
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24

```
R1#
```

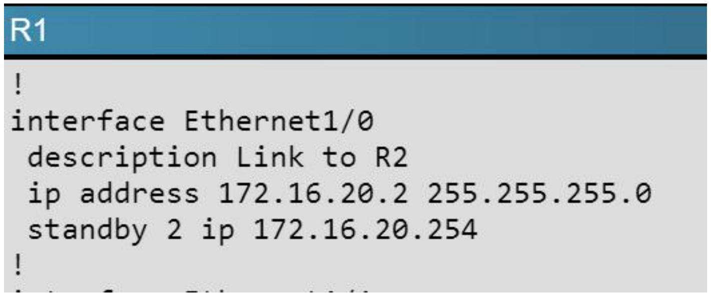
```
R2#
```

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

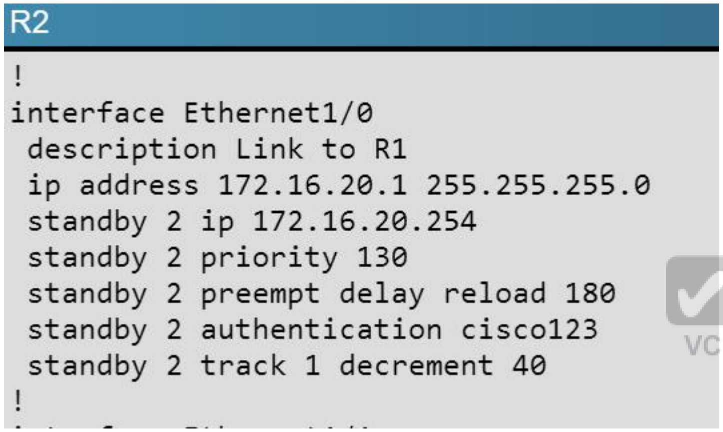
Correct Answer: B
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Based on the configuration output, we see that authentication is configured on R2, but not on R1:



R1

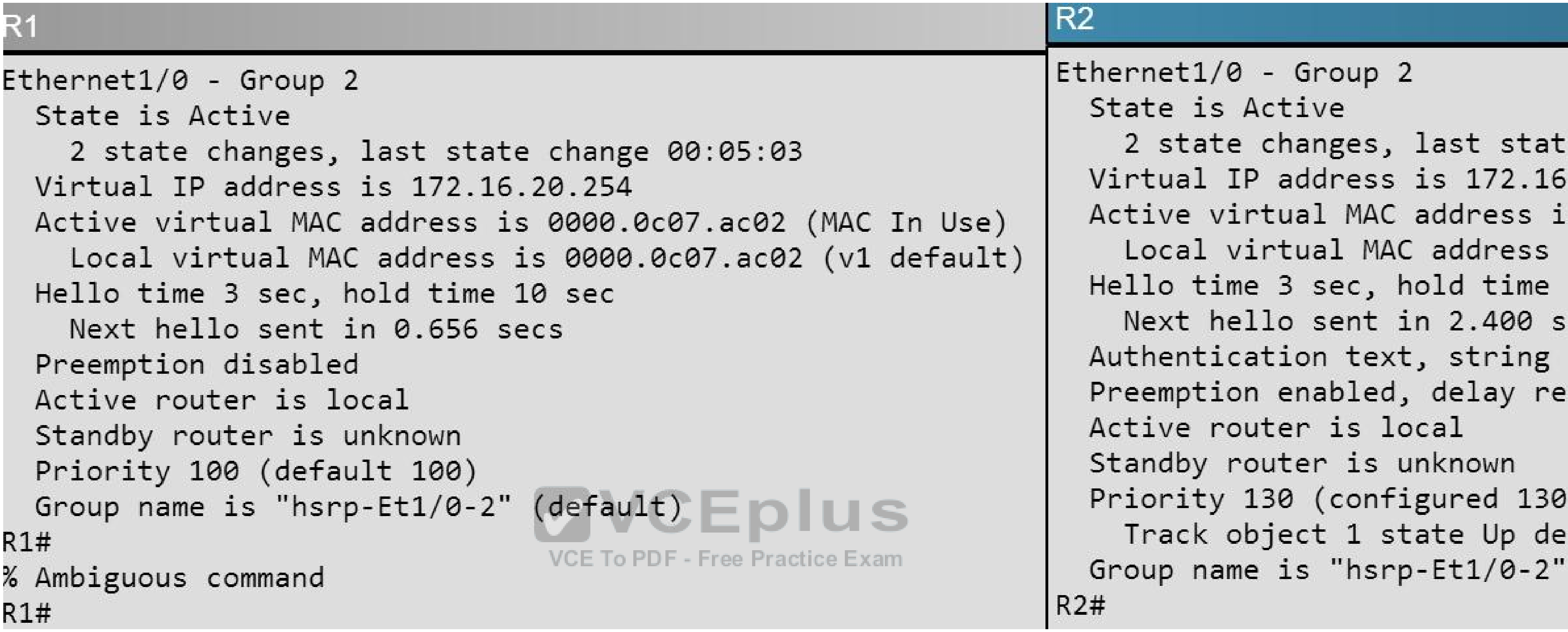
```
!
interface Ethernet1/0
 description Link to R2
 ip address 172.16.20.2 255.255.255.0
 standby 2 ip 172.16.20.254
!
```



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

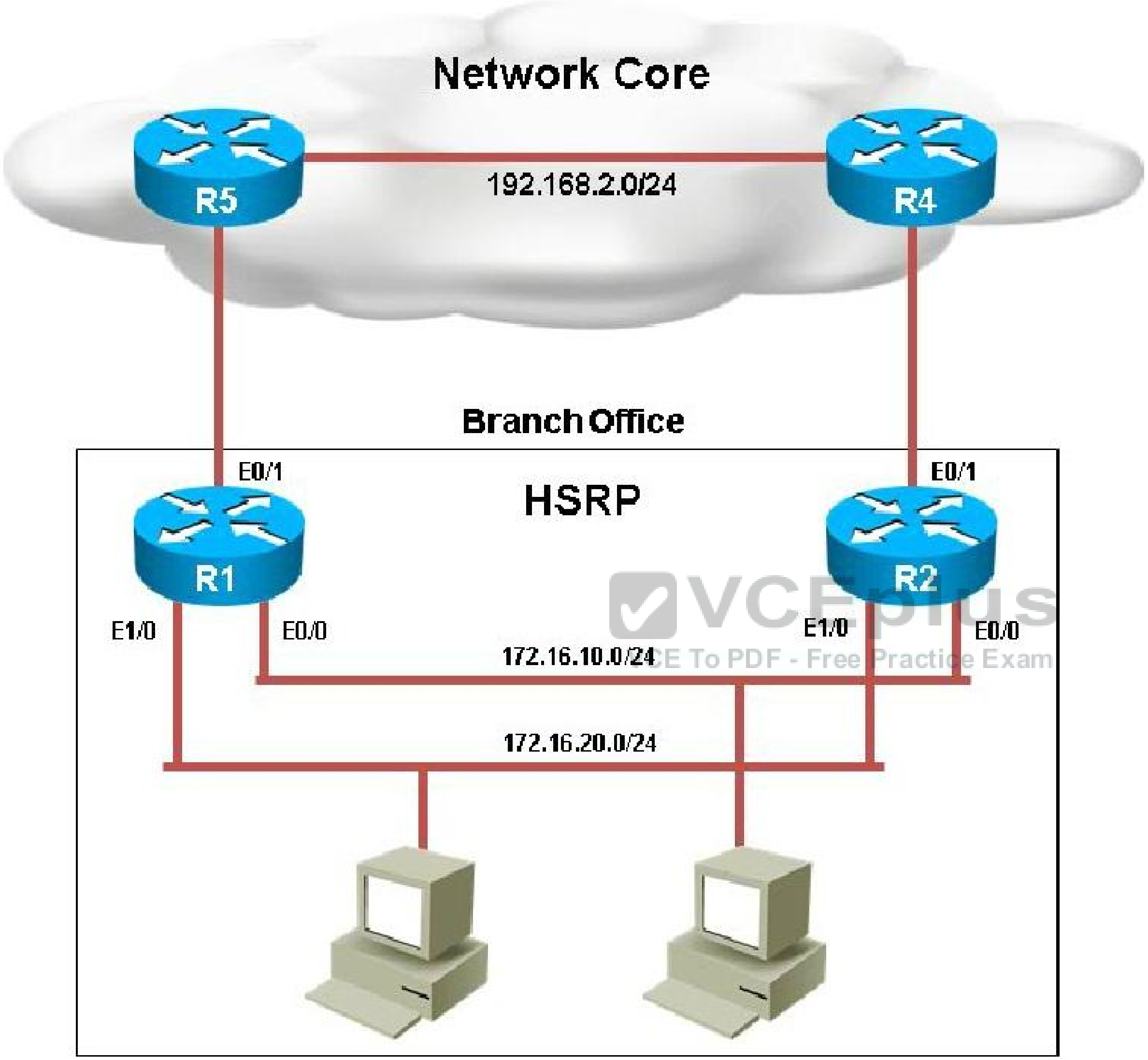
```
Ethernet1/0 - Group 2
  State is Active
    2 state changes, last state change 00:05:03
  Virtual IP address is 172.16.20.254
  Active virtual MAC address is 0000.0c07.ac02 (MAC In Use)
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello 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 stat
  Virtual IP address is 172.16
  Active virtual MAC address i
    Local virtual MAC address
  Hello time 3 sec, hold time
    Next hello sent in 2.400 s
  Authentication text, string
  Preemption enabled, delay re
  Active router is local
  Standby router is unknown
  Priority 130 (configured 130
    Track object 1 state Up de
  Group name is "hsrp-Et1/0-2"
R2#
```

QUESTION 138

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.


Network Core
R5
R4
192.168.2.0/24
Branch Office
HSRP
E0/1
E0/1
R1
R2
E1/0
E0/0
E1/0
E0/0
172.16.10.0/24
172.16.20.0/24

```
R1#
```

```
R2#
```

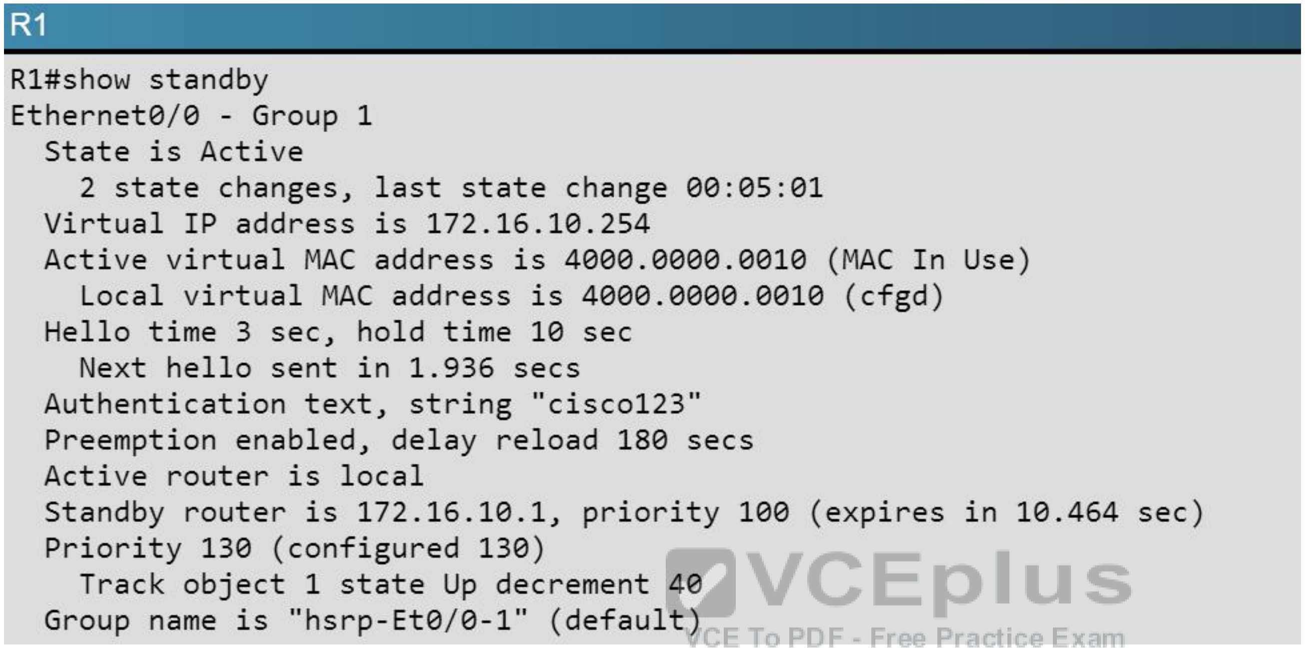
What is the virtual mac-address of HSRP group 1?

A. 0000.0c07.ac02
B. 4000.0000.0010
C. 0000.0c07.ac01
D. 4000.0000.ac01
E. 4000.0000.ac02
F. 0000.0c07.0010

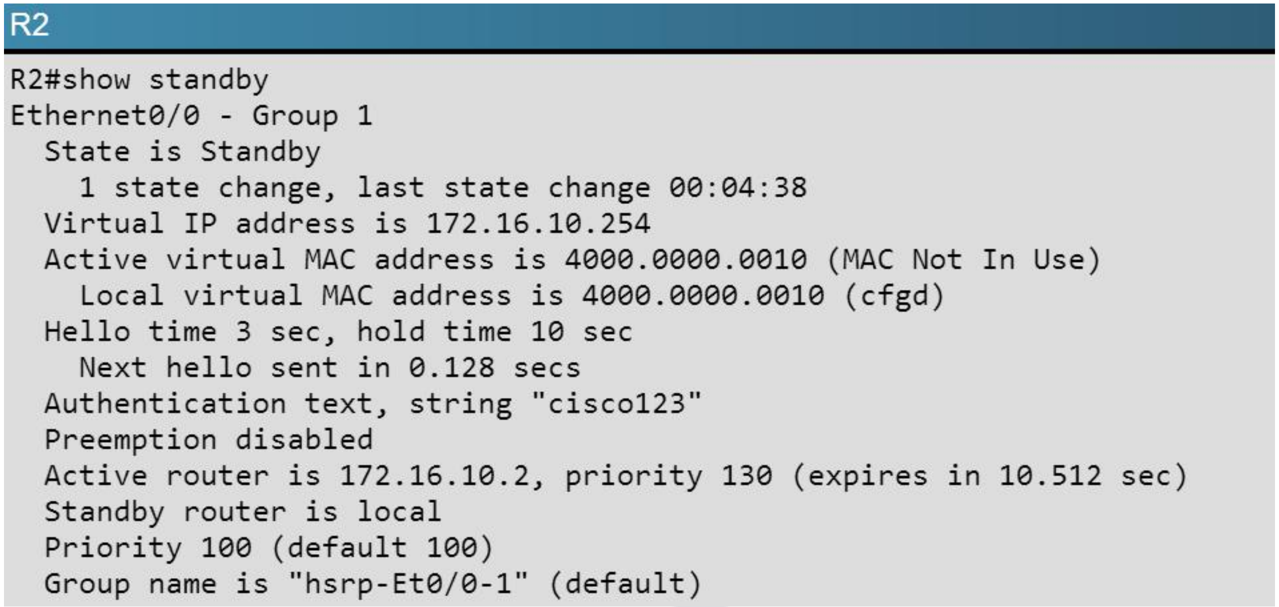
Correct Answer: B
Section: Infrastructure Services
Explanation

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:



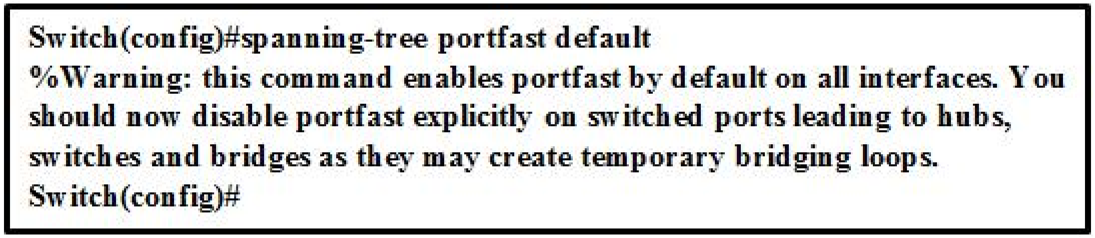
```
R1#show standby
Ethernet0/0 - Group 1
  State is Active
    2 state changes, last state change 00:05:01
  Virtual IP address is 172.16.10.254
  Active virtual MAC address is 4000.0000.0010 (MAC In Use)
    Local virtual MAC address is 4000.0000.0010 (cfgd)
  Hello time 3 sec, hold time 10 sec
    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 139
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 140
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 141
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 142
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: Mix QUESTIONS
Explanation

Explanation/Reference:

QUESTION 143
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 144
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?

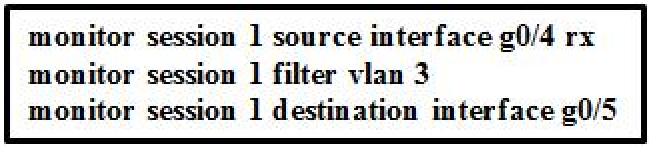
A. BPDUblock
B. BPDUfilter

C. BPDUignore
D. BPDUguard
E. BPDUdisable

Correct Answer: B
Section: Mix QUESTIONS
Explanation

Explanation/Reference:

QUESTION 145
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 146
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 147
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:

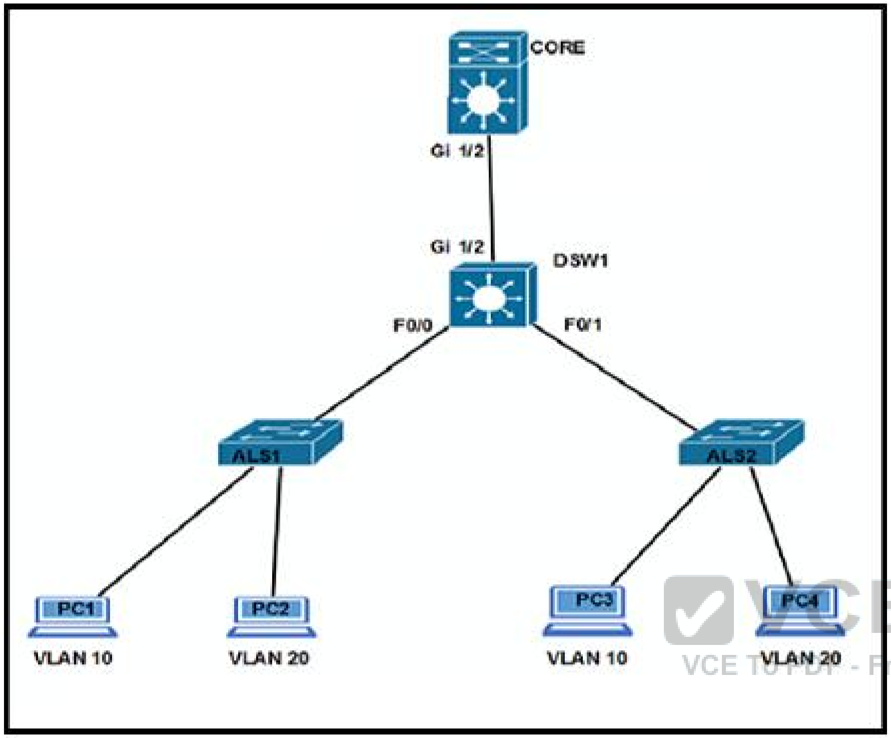
QUESTION 148
Enablement of which feature puts the port into err-disabled state when the port has PortFast enabled and it receives BPDUs?

A. BPDU filtering
B. BackboneFast
C. EtherChannel
D. BPDU guard

Correct Answer: D
Section: Mix QUESTIONS
Explanation

Explanation/Reference:

QUESTION 149
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 150
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 151
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 152
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 153
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 154
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 155

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:

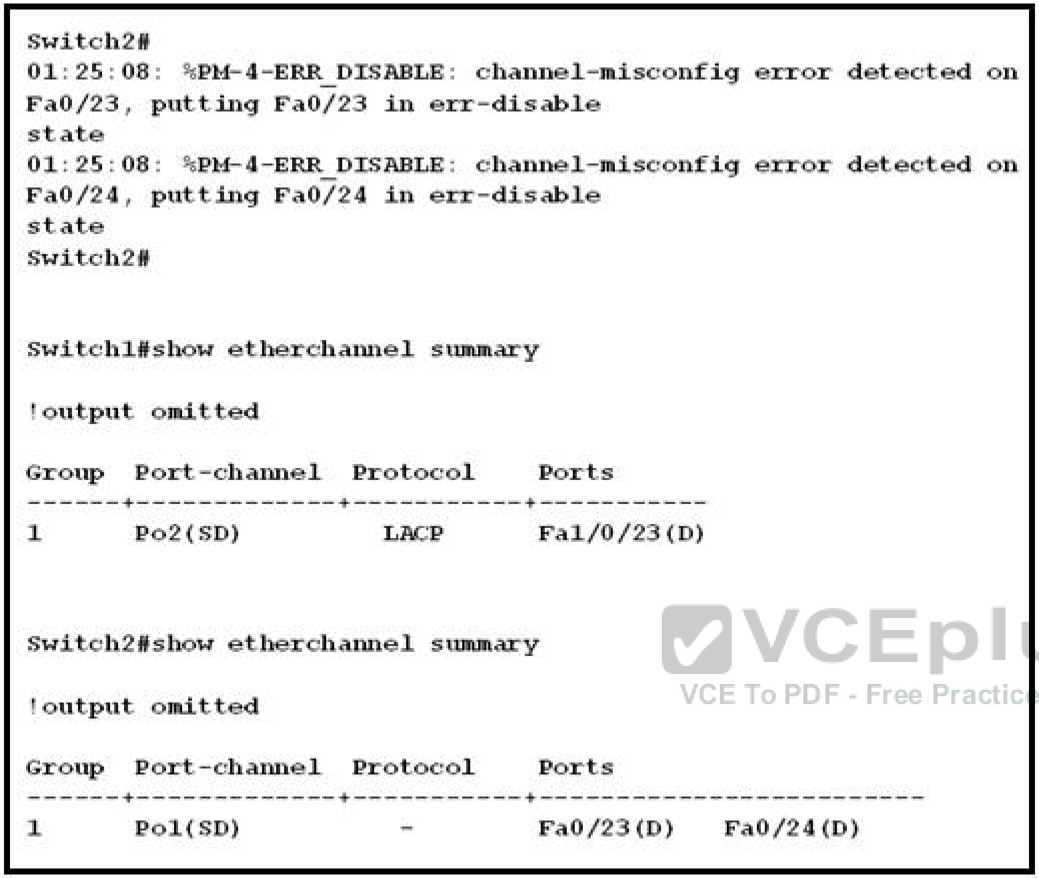
QUESTION 156
Which option is valid for EtherChannel load balancing?

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 157
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)
```

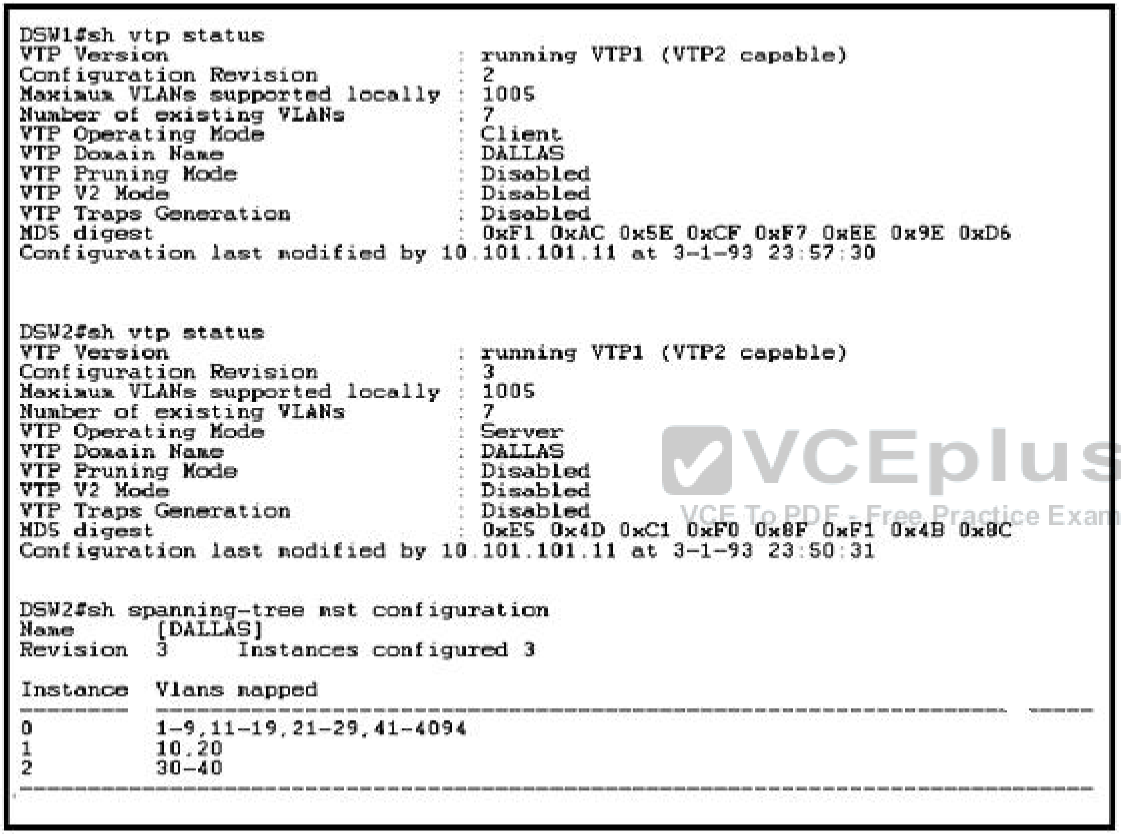
An engineer is configuring EtherChannel between two switches and notices the console message on switch 2. Based on the output, which option describes the reason for this error?

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 158
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                      : 0xE5 0x4D 0xC1 0xF0 0x8F 0xF1 0x4B 0x8C
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  Vlans 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 159
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:

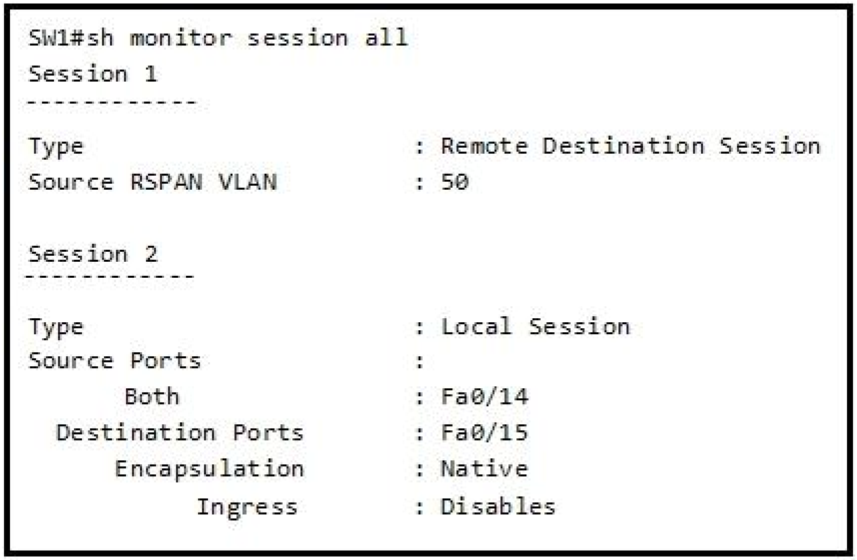
QUESTION 160
In a switch stack environment, what is the total bidirectional traffic flow between two logical counter-rotating paths?

A. 16 Gbps
B. 32 Gbps
C. 64 Gbps
D. 128 Gbps

Correct Answer: B
Section: Mix QUESTIONS
Explanation

Explanation/Reference:

QUESTION 161
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 162
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

D. routing information

Correct Answer: C
Section: Mix QUESTIONS
Explanation

Explanation/Reference:

QUESTION 163
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: