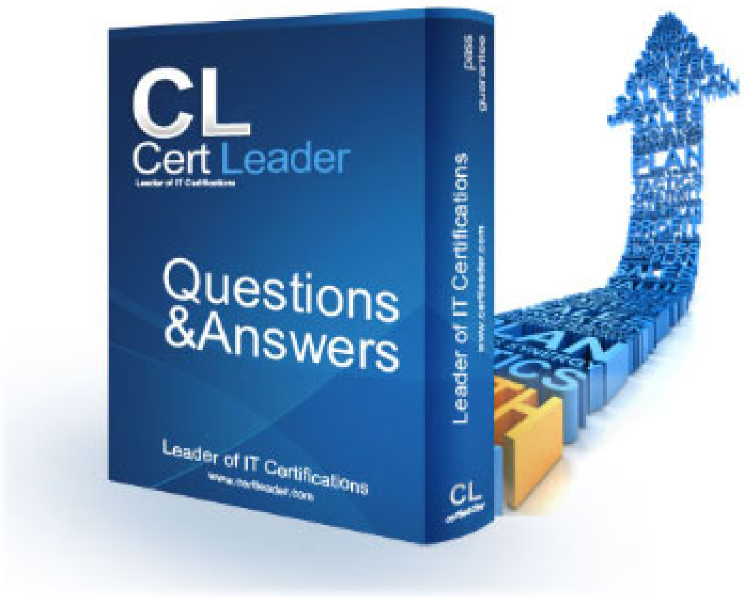
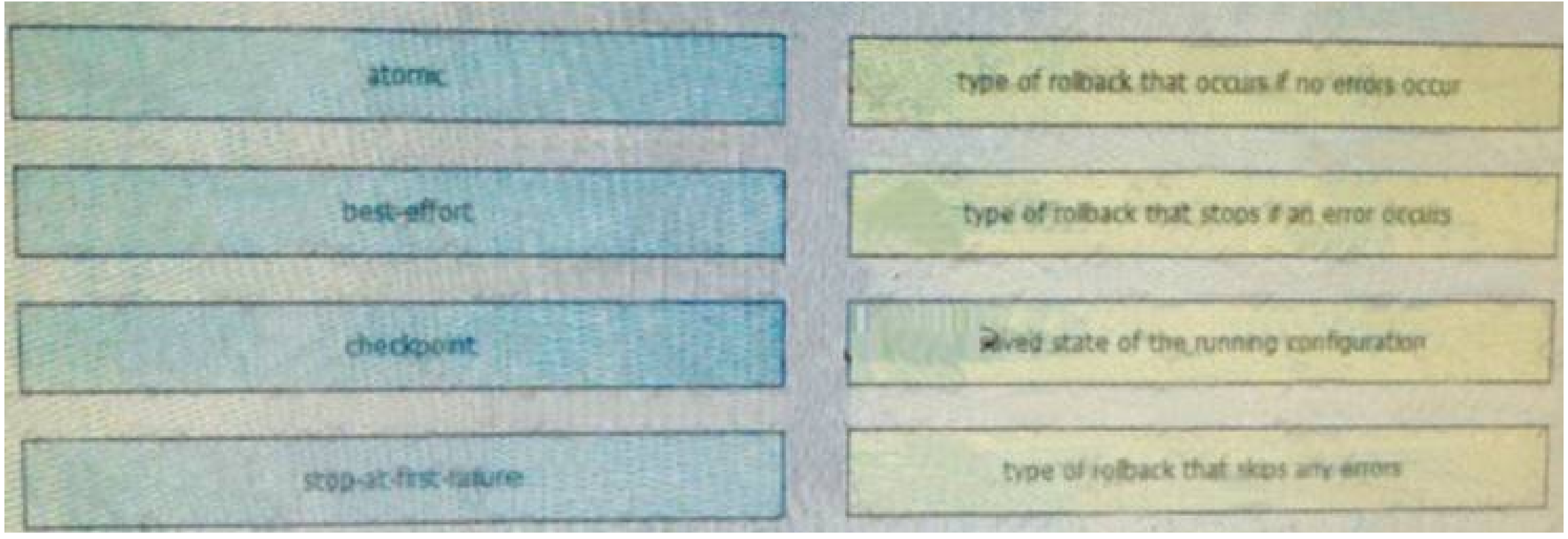
300-165 Dumps

DCII Implementing Cisco Data Center Infrastructure (DCII)

https://www.certleader.com/300-165-dumps.html



NEW QUESTION 1
DRAG DROP
Drag and drop the configuration management commands on the left to their correct definitions on the right.



atomic

best-effort

checkpoint

stop-at-first-failure

type of rollback that occurs if no errors occur

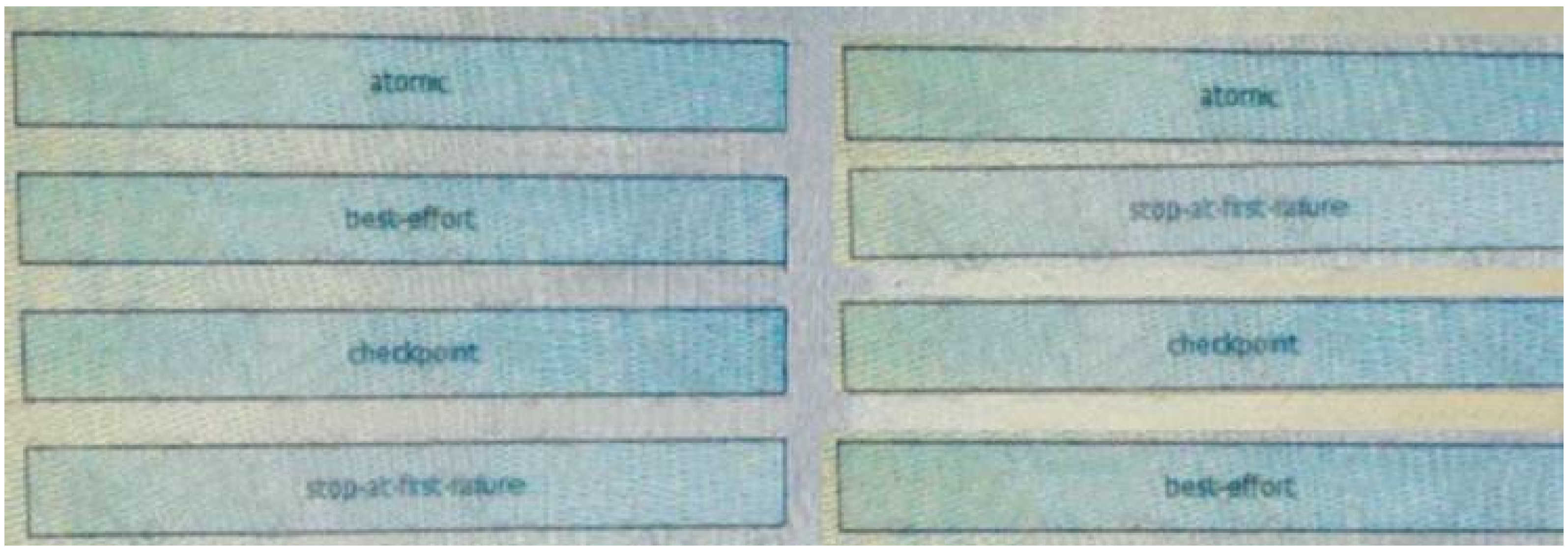
type of rollback that stops if an error occurs

saved state of the running configuration

type of rollback that skips any errors

Answer:

Explanation:



atomic

best-effort

checkpoint

stop-at-first-failure

atomic

stop-at-first-failure

checkpoint

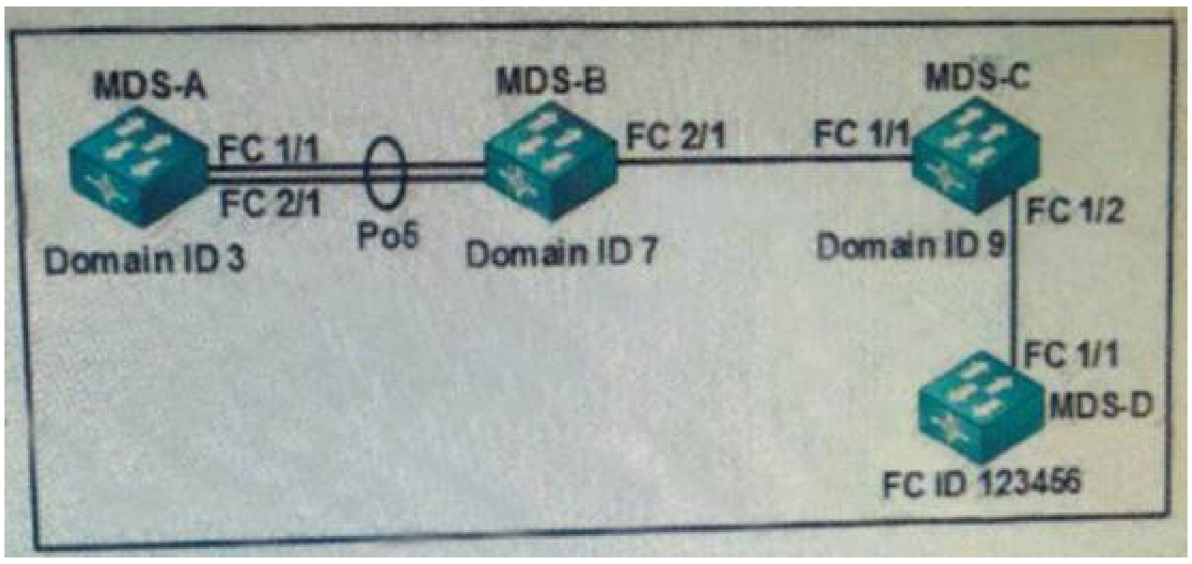
best-effort

NEW QUESTION 2
Which option describes the atomic rollback feature in Cisco NX-OS?

A. Rollback is implemented only if no errors occur.
B. Rollback is implemented and any errors are skipped.
C. Rollback is implemented and stops if an error occurs.
D. Rollback is implemented instantly and there is no option to cancel the operation if errors are encountered.

Answer: A

NEW QUESTION 3
Refer to the exhibit.



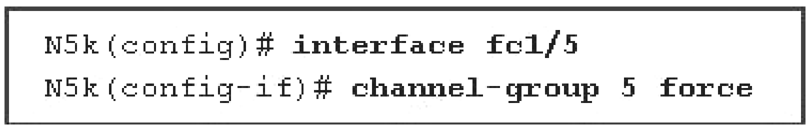
Which command configures a static FSPF route from MDS-A to FC ID 123456?

A. switch(config)# fcroute 0x123456 interface san-port-channel 5 domain 7 vsan 10
B. switch(config)# fcroute 0x123456 interface san-port-channel 5 domain 3 vsan 10
C. switch(config)# fcroute 123456 interface fc 1 2 domain 7
D. switch(config)# fcroute 123456 interface fc 1 1 domain 9

Answer: A

Explanation: Reference:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/fcroute.html

NEW QUESTION 4
Refer to the exhibit.



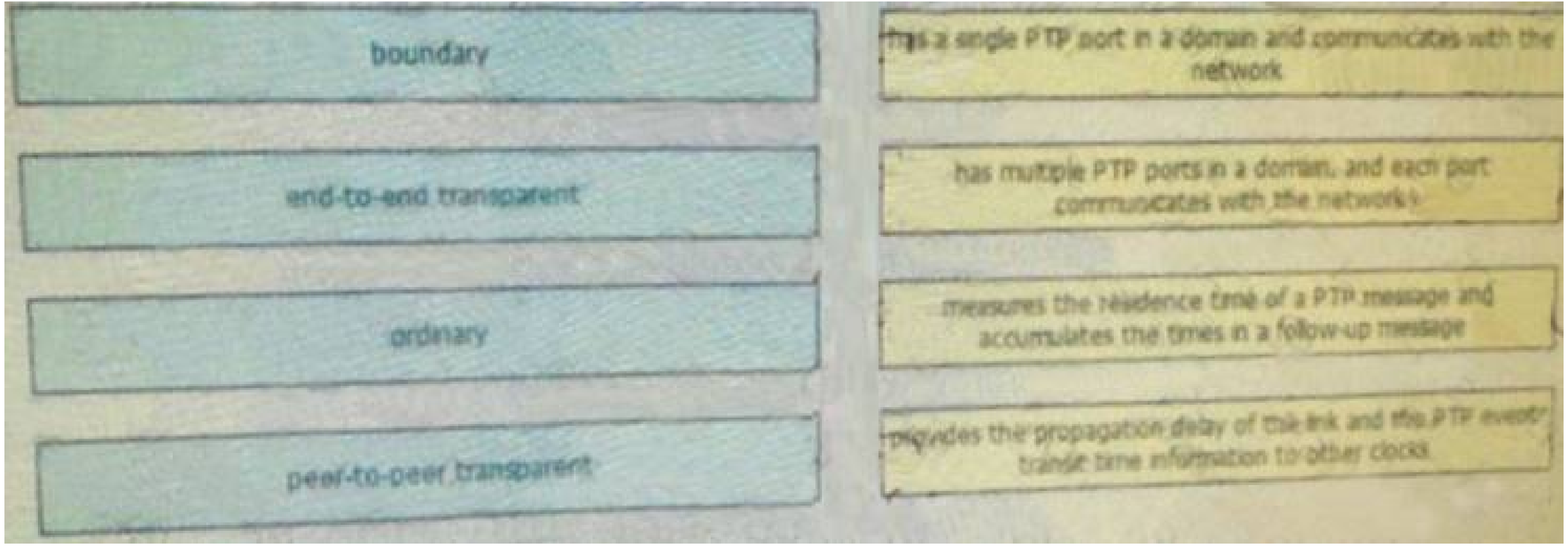
```
N5k(config)# interface fc1/5
N5k(config-if)# channel-group 5 force
```

What is the result when you run the force command?

A. Port channel mode uses force mode
B. The command forces the addition of a port to a SAN port channel.
C. The port is enabled and active.
D. The command forces the deletion of a port to a SAN port channe

Answer: B

NEW QUESTION 5
DRAG DROP
Drag and drop the types of PTP clocks on the left to their correct descriptions on the right.



boundary

end-to-end transparent

ordinary

peer-to-peer transparent

has a single PTP port in a domain and communicates with the network

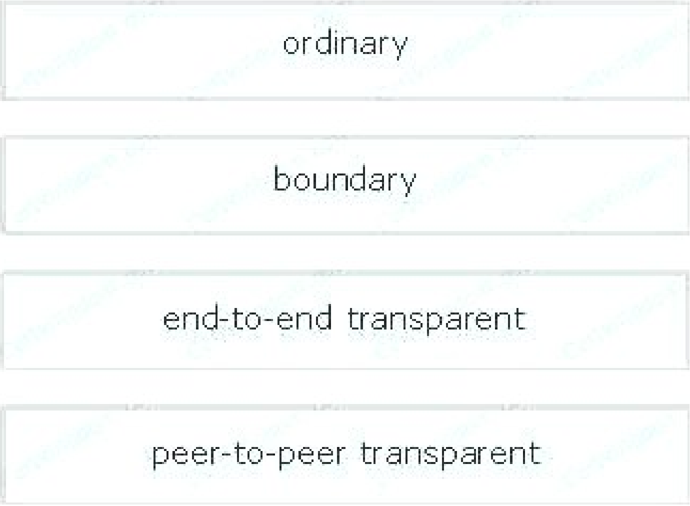
has multiple PTP ports in a domain, and each port communicates with the network

measures the residence time of a PTP message and accumulates the times in a follow-up message

provides the propagation delay of the link and the PTP event transit time information to other clocks

Answer:

Explanation:



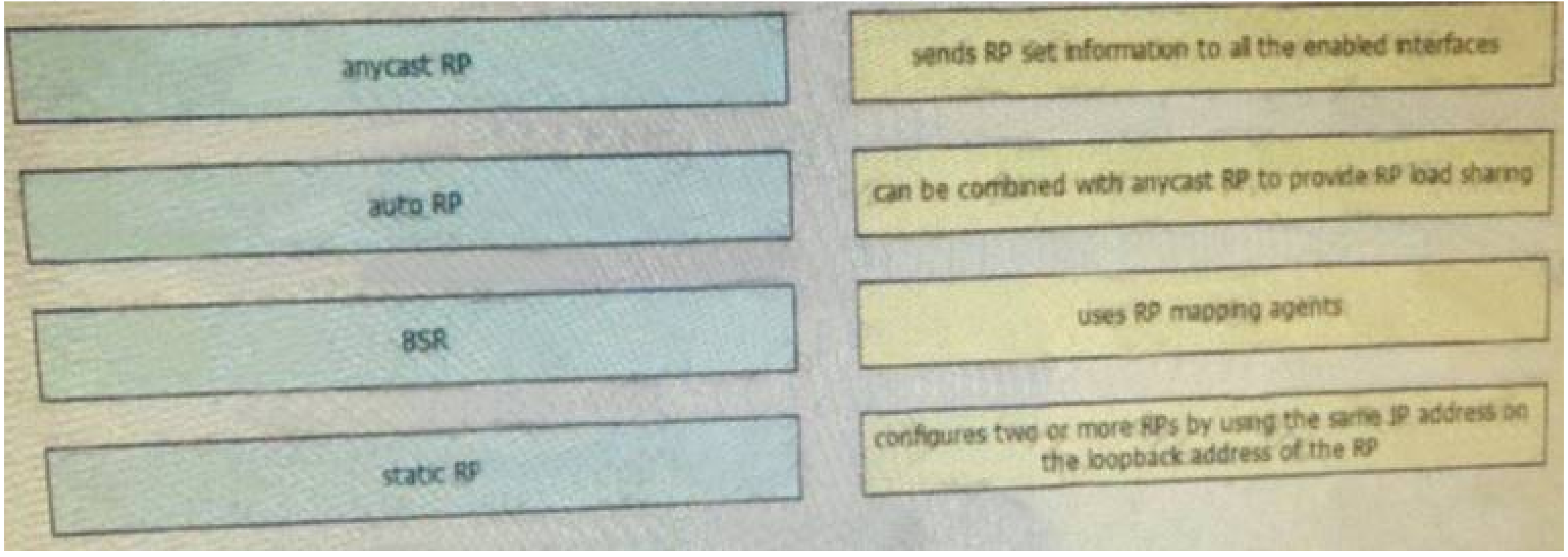
ordinary

boundary

end-to-end transparent

peer-to-peer transparent

NEW QUESTION 6
DRAG DROP
Drag and drop the RP mechanisms on the left to their correct redundancy implementations on the right.



anycast RP

auto RP

BSR

static RP

sends RP set information to all the enabled interfaces

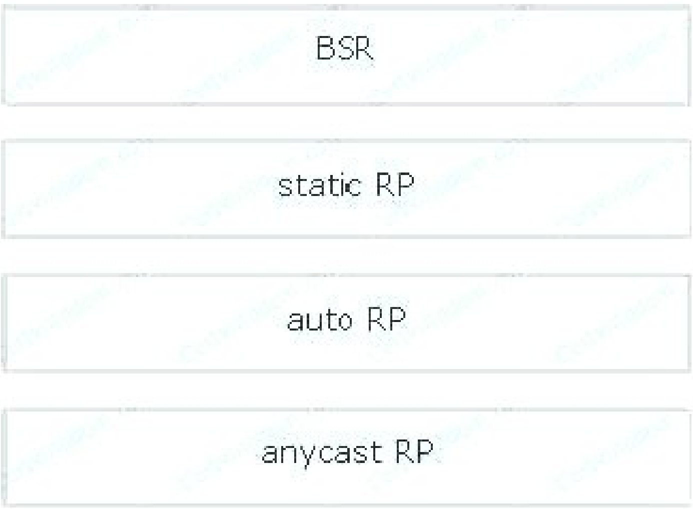
can be combined with anycast RP to provide RP load sharing

uses RP mapping agents

configures two or more RPs by using the same IP address on the loopback address of the RP

Answer:

Explanation:



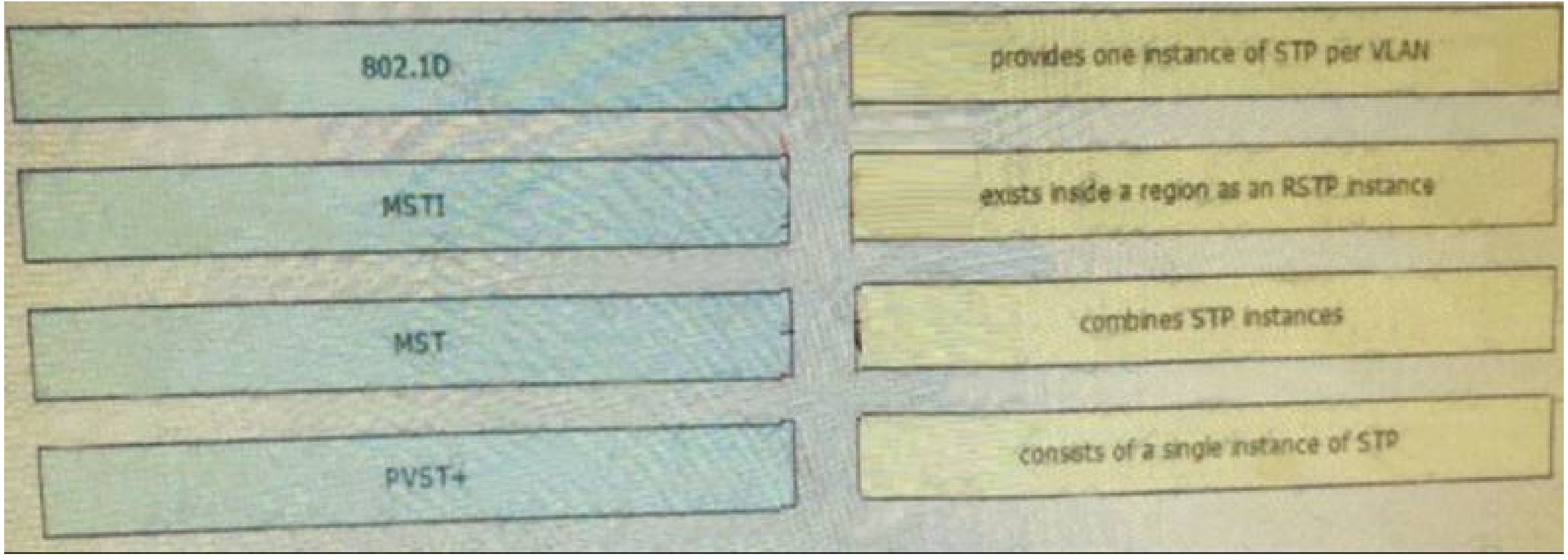
BSR

static RP

auto RP

anycast RP

NEW QUESTION 7
DRAG DROP
Drag and drop the spanning tree types on the left to their correct descriptions on the right



802.1D

MSTI

MST

PVST+

provides one instance of STP per VLAN

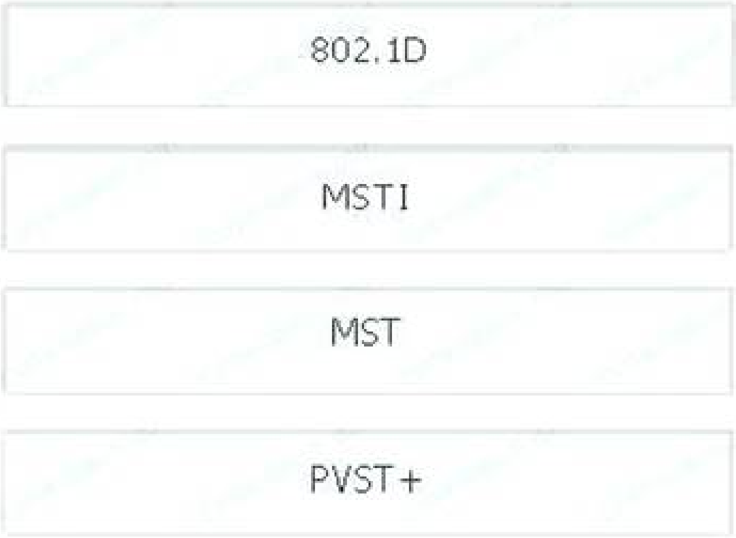
exists inside a region as an RSTP instance

combines STP instances

consists of a single instance of STP

Answer:

Explanation:



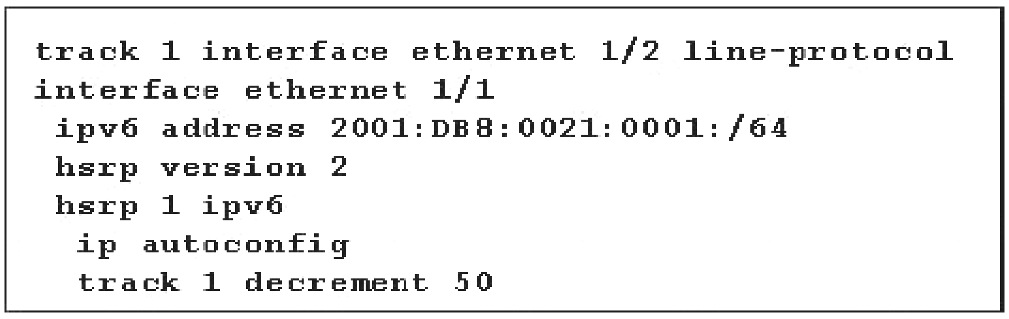
802.1D

MSTI

MST

PVST+

NEW QUESTION 8
Refer to the exhibit.



```
track 1 interface ethernet 1/2 line-protocol
interface ethernet 1/1
 ipv6 address 2001:DB8:0021:0001:/64
 hsrp version 2
 hsrp 1 ipv6
  ip autoconfig
  track 1 decrement 50
```

Which statement about the result of the configuration is true?

A. The virtual IPv6 address is derived from the physical IPv6 address of the interface
B. Hello packets are sent by using an address of 224.0.0.102.
C. Hello packets are sent by using an address of FF02 : 66
D. The virtual MAC address is derived from the physical IPv6 address of the interfac

Answer: D

NEW QUESTION 9
In policy-based routing, which action is taken for packets that do not match any of the route-map statements?

A. forwarded after the egress queue empties on the outbound interface
B. forwarded using the last statement in the route map
C. forwarded using the closest matching route-map statement
D. forwarded using destination-based routing

Answer: D

Explanation: Each entry in a route map contains a combination of match and set statements. The match statements define the criteria for whether appropriate packets meet the particular policy (that is, the conditions to be met). The set clauses explain how the packets should be routed once they have met the match criteria.
You can mark the route-map statements as permit or deny. You can interpret the statements as follows:
• If the statement is marked as permit and the packets meet the match criteria, the set clause is applied. One of these actions involves choosing the next hop.
• If a statement is marked as deny, the packets that meet the match criteria are sent back through the normal forwarding channels, and destination-based routing is performed.
• If the statement is marked as permit and the packets do not match any route-map statements, the packets are sent back through the normal forwarding channels, and destination-based routing is performed.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/unicast/configuration/guide/l3_cli_nxos/l3pbr.pdf

NEW QUESTION 10
switch# configure terminal
switch (config) # interface ethernet 1/4 switch (config-if) # switchport mode trunk
switch (config-if) # channel-group 1 mode active
Refer to the exhibit. Which type of port channel was created?

A. LACP
B. static
C. PAgP
D. desirable

Answer: A

NEW QUESTION 10
Which statement about electronic programmable logic device image upgrades is true?

A. EPLD and ISSU image upgrades are nondisruptive.
B. An EPLD upgrade must be performed during an ISSU system or kickstart upgrade.
C. Whether the module being upgraded is online or offline, only the EPLD images that have different current and new versions are upgraded.
D. You can execute an upgrade or downgrade only from the active supervisor modul

Answer: D

Explanation: You can upgrade (or downgrade) EPLDs using CLI commands on the Nexus 7000 Series device. Follow these guidelines when you upgrade or downgrade EPLDs:
• You can execute an upgrade from the active supervisor module only. All the modules, including the active supervisor module, can be updated individually.
• You can individually update each module whether it is online or offline as follows:
– If you upgrade EPLD images on an online module, only the EPLD images with version numbers that differ from the new EPLD images are upgraded.
– If you upgrade EPLD images on an offline module, all of the EPLD images are upgraded.
• On a system that has two supervisor modules, upgrade the EPLDs for the standby supervisor and then switch the active supervisor to standby mode to upgrade its EPLDs. On a system that has only one supervisor module, you can upgrade the active supervisor, but this will disrupt its operations during the upgrade.
• If you interrupt an upgrade, you must upgrade the module that is being upgraded again.
• The upgrade process disrupts traffic on the targeted module.
• Do not insert or remove any modules while an EPLD upgrade is in progress. Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_0/epld/release/notes/epld_rn.ht ml

NEW QUESTION 12
Which GLBL load-balancing method ensures that a client is always mapped to the same virtual MAC address?

A. host-dependent
B. vmac-weighted
C. dedicated-vmac-mode
D. shortest-path and weighting

Answer: A

NEW QUESTION 13
Which command configures the aging for VLAN 100 to 500 minutes?

A. mac address-table aging-time 50
B. mac address-table aging-time 50 vlan 100
C. mac address-table aging-time 3000 vlan 100
D. mac address-table aging-time 300

Answer: C

NEW QUESTION 17
You experience an issue on a Cisco Nexus 7700 Series switch. You must gather detailed information about the system state and the configuration of the switch. Which command should you run?

A. switch# show logging > bootflash:Log.txt
B. switch# show tech-support > bootflash:Log.txt
C. switch# show running-config > bootflash:Log.txt
D. switch# show system > bootflash:Log.txt

Answer: B

NEW QUESTION 18
Which two options should you consider when you configure a SAN zone set? (Choose two.)

A. VSANs can be activated by using enhanced zoning.
B. A SAN zone set consists of one or more SAN zones.
C. A SAN zone set must be activated manually on all of the fabric nodes.
D. Only the SAN zone set can be activated simultaneously.
E. One SAN zone can be the member of only one zone se

Answer: BC

NEW QUESTION 22
Which statement about SNMP support on Cisco Nexus switches is true?

A. Cisco NX-OS only supports SNMP over IPv4.
B. Cisco NX-OS supports one instance of the SNMP per VDC.
C. SNMP is not VRF-aware.
D. SNMP requires the LAN_ENTERPRISE_SERVICES_PKG license.
E. Only users belonging to the network operator RBAC role can assign SNMP group

Answer: B

Explanation: Cisco NX-OS supports one instance of the SNMP per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. SNMP supports multiple MIB module instances and maps them to logical network entities. SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/system_management/configuration/guide/sm_nx_os_cg/sm_9snmp.html

NEW QUESTION 25
Which command should you ran to distribute NTP configuration changes by using Cisco Fabric Services?

A. ntp distribute
B. ntp server 1.2.3.4
C. ntp commit
D. ntp authenticate

Answer: A

NEW QUESTION 26
You are connecting a Cisco Nexus 2300 Series FEX to a Cisco Nexus 5600 Series parent switch. Which command should you use to configure the interfaces on the Nexus switch that connects to the FEX?

A. switch(config-if)# switchport mode f
B. switch(config-if)# switchport mode fex-fabric
C. switch(config-if)# switchport mode fabricpath
D. switch(config-if)# switchport mode vntag

Answer: B

NEW QUESTION 27
What is the Overlay Transport Virtualization site VLAN used for?

A. to facilitate communications between OTV edge devices within the site
B. to allow multiple site AEDs to communicate with each other
C. to detect devices at the site that are not capable of OTV
D. to allow the join interfaces at different sites to communicate

Answer: A

NEW QUESTION 31
Which Cisco MDS feature needs to be enabled for Cisco TrustSec FC Link Encryption to work?

A. feature Trust-Sec
B. feature ESP
C. feature FC-TSLE
D. feature FC-SP

Answer: D

NEW QUESTION 34
What is an Overlay Transport Virtualization extended VLAN?

A. the VLAN used to locate other AEDs
B. the VLAN used to access the overlay network by the join interface
C. the user VLAN that exists in multiple sites
D. the VLAN that must contain the overlay interface

Answer: C

Explanation:
Functions of OTV
Maintains a list of overlays
Maintains a list of configured overlay parameters such as name, multicast address, encapsulation type, authentication, and OTV feature sets
Maintains the state of the overlay interface
Maintains the status of OTV VLAN membership from Ethernet infrastructure and the state of the authoritative edge device (AED) from IS-IS
Maintains a database of overlay adjacencies as reported by IS-IS
Maintains IP tunnel information and manages the encapsulation for data sent on the overlay network
Manages delivery groups (DGs) for each overlay by snooping multicast traffic and monitoring traffic streams for active DGs
Configures, starts, and stops the OTV IS-IS instance
Interfaces with IP multicast to join provider multicast groups for each overlay

NEW QUESTION 37
Which statement accurately describes the implementation of FSPF on Cisco MDS 9700 Series switches?

A. FSPF is enabled on the Fibre Channel switches but must be enabled manually on a per-VSAN basis.
B. FSPF must be enabled manually on the switch and on each VSAN on the switch.
C. FSPF is enabled, by default, on the Fibre Channel switches for all VSANs.
D. FSPF is enabled on VSANs, but must be enabled manually on a per-FC switch basi

Answer: A

NEW QUESTION 39
You plan to implement the OSPF protocol whithin the data center network. Which two statements accurately describe OSPF on the Cisco NX-OS platform? (Choose two.)

A. The default reference bandwidth is 10 Gbps.
B. OSPF does nor require additional licenses.
C. The OSPF area can be configured by using decimal notation only.
D. Redistributing routes into OSPF requires a route map.
E. The secondary IP address is advertised by defaul

Answer: DE

NEW QUESTION 40
What can be identified by running the switch# show install all impact kickstart bootflash:n5000-uk9- kickstart.4.2.1.N.1.1a.bin system bootflash:n5000-uk9.4.2.1.N1.1a.bin command?

A. the impact of the specified kickstart image on the specified system image
B. whether the specified system image supports the kickstart image
C. whether bootflash is supported for the specified Cisco NX-OS images
D. whether ISSU is supported for the specified Cisco NX-OS images

Answer: D

NEW QUESTION 42
When you configure LISP, which two components must be configured at the site edge? (Choose two.)

A. AED
B. ELAN
C. ITR
D. EOBC
E. ETR

Answer: CE

NEW QUESTION 47
You have a Cisco Nexus 5000 Series switch. Port security is configured to use sticky learning. Where are the secured MAC addresses stored?

A. the running configuration
B. the startup configuration
C. NVRAM
D. RAM

Answer: C

NEW QUESTION 50
Which two issues explain why a packet is not being routed as desired in a policy-based routing configuration? (Choose two.)

A. The next hop that is configured in the route map has a higher metric than the default next hop.
B. The route map is not applied to the egress interface.
C. The next hop that is configured in the route map is not in the global routing table.
D. The route map is not applied to the ingress interface.
E. The next hop that is configured in the route map has a lower metric than the default next ho

Answer: CE

Explanation: The next hop that is configured in the route map is not in the global routing table then the packet will not be forwarded as desired. The next hop that is configured in the route map has a higher metric than the default next hop.

NEW QUESTION 51
Which features must be enabled to implement manual MACsec?

A. CTS and dot1x
B. MSDP and dot1x
C. CTS and MSDP
D. CTS and private VLAN

Answer: A

NEW QUESTION 56
Which two Nexus family line cards allow the configuration of features regarding LISP, OTV and MPLS? (Choose two.)

A. B1
B. F3
C. F2
D. F1
E. M2

Answer: BE

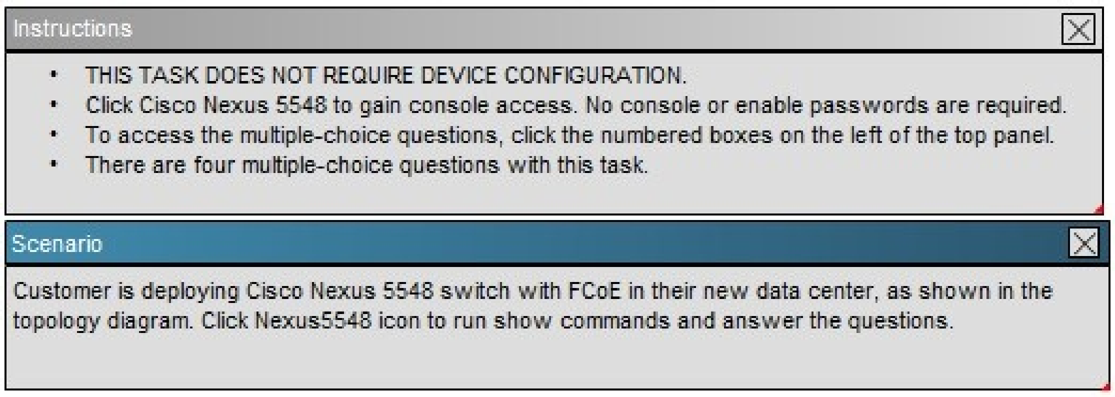
NEW QUESTION 57
After enabling strong, reversible 128-bit Advanced Encryption Standard password type-6 encryption on a Cisco Nexus 7000, which command would convert existing plain or weakly encrypted passwords to type-6 encrypted passwords?

A. switch# key config-key ascii
B. switch(config)# feature password encryption aes
C. switch# encryption re-encrypt obfuscated
D. switch# encryption decrypt type6

Answer: C

Explanation: This command converts existing plain or weakly encrypted passwords to type-6 encrypted passwords.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/security/configuration/guide/b_Cisco_Nexus_7000_NXOS_ Security_Configuration_Guide Release_5-x/b_Cisco_Nexus_7000_NXOS_ Security_Configuration_Guide Release_5-x_chapter_010101.html

NEW QUESTION 61
What is the status of FCoE license on Cisco Nexus 5548 switch?

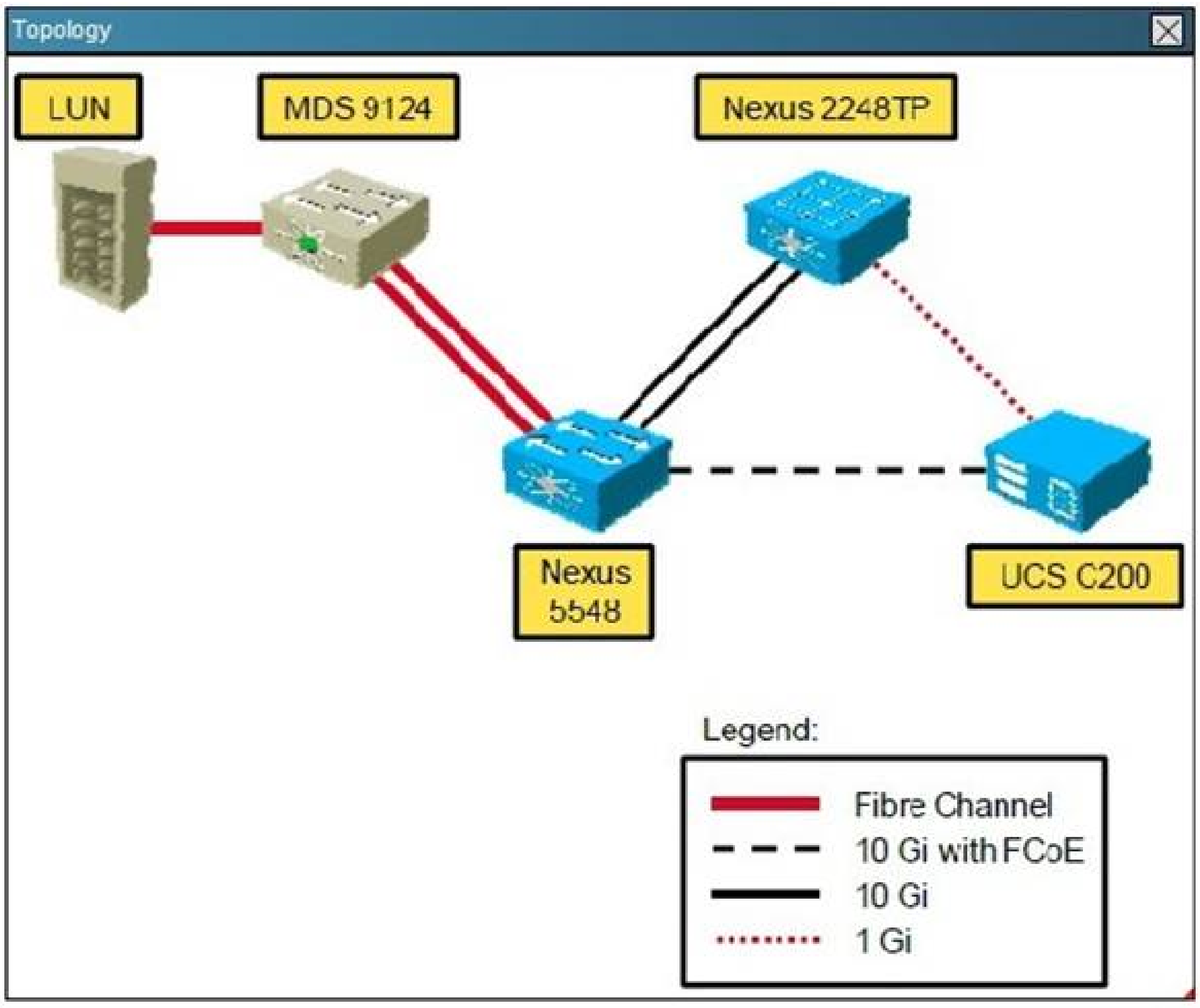


Instructions

- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- Click Cisco Nexus 5548 to gain console access. No console or enable passwords are required.
- To access the multiple-choice questions, click the numbered boxes on the left of the top panel.
- There are four multiple-choice questions with this task.

Scenario

Customer is deploying Cisco Nexus 5548 switch with FCoE in their new data center, as shown in the topology diagram. Click Nexus5548 icon to run show commands and answer the questions.

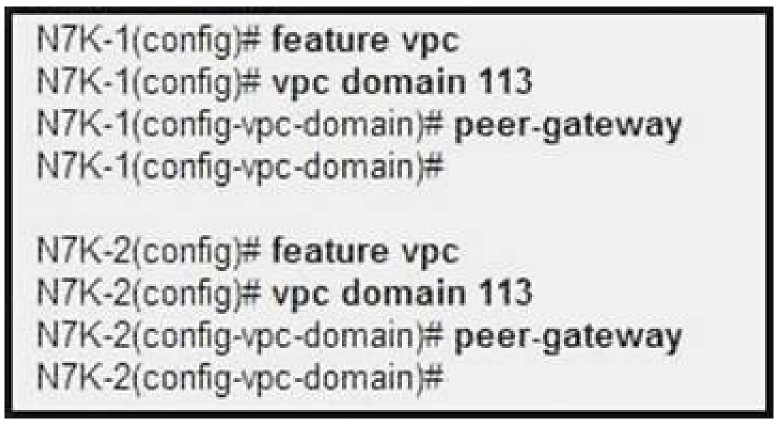


```
Nexus 5548#
```

A. FCoE license is not installed
B. FCoE license is installed, but it is expired
C. FCoE license is installed and status is enabled
D. FCoE license does not need to be installed because it is part of ENTERPRISE_PKG

Answer: C

NEW QUESTION 63
Refer to the exhibit.



```
N7K-1(config)# feature vpc
N7K-1(config)# vpc domain 113
N7K-1(config-vpc-domain)# peer-gateway
N7K-1(config-vpc-domain)#

N7K-2(config)# feature vpc
N7K-2(config)# vpc domain 113
N7K-2(config-vpc-domain)# peer-gateway
N7K-2(config-vpc-domain)#
```

What is the consequence of configuring peer-gateway on the two vPC peers N7K-1 and N7K-2?

A. Nothing, this is the standard vPC configuration to make the feature work.

B. The downstream device detects only one of the vPC peers as its gateway.
C. The downstream device can use DMAC of N7K-1 on the link to N7K-2, and N7K-2 forwards the packet.
D. This configuration enables the downstream device to use DHCP to obtain its default gatewa

Answer: C

Explanation: Beginning with Cisco NX-OS 4.2(1), you can configure vPC peer devices to act as the gateway even for packets that are destined to the vPC peer device's MAC address. Use the peer-gateway command to configure this feature.
Some network-attached storage (NAS) devices or load-balancers may have features aimed to optimize the performances of particular applications. Essentially these features avoid performing a routing-table lookup when responding to a request that originated form a host not locally attached to the same subnet. Such devices may reply to traffic using the MAC address of the sender Cisco Nexus 7000 device rather than the common HSRP gateway. Such behavior is non-complaint with some basic Ethernet RFC standards. Packets reaching a vPC device for the non-local router MAC address are sent across the peer-link and could be dropped by the built in vPC loop avoidance mechanism if the final destination is behind another vPC.
The vPC peer-gateway capability allows a vPC switch to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer. This feature enables local forwarding of such packets without the need to cross the vPC peer-link. In this scenario, the feature optimizes use of the peer-link and avoids potential traffic loss.
Configuring the peer-gateway feature needs to be done on both primary and secondary vPC peers and is non-disruptive to the operations of the device or to the vPC traffic. The vPC peer-gateway feature can be configured globally under the vPC domain submode.
When enabling this feature it is also required to disable IP redirects on all interface VLANs mapped over a vPC VLAN to avoid generation of IP redirect messages for packets switched through the peer gateway router. When the feature is enabled in the vPC domain, the user is notified of such a requirement through an appropriate message.
Packets arriving at the peer-gateway vPC device will have their TTL decremented, so packets carrying TTL = 1 may be dropped in transit due to TTL expire. This needs to be taken into account when the peer-gateway feature is enabled and particular network protocols sourcing packets with TTL = 1 operate on a vPC VLAN.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nxos/ interfaces/configuration/guide/if_nxos/if_vPC.html

NEW QUESTION 68
Which command should you run to limit IS-IS LSP flooding on a network?

A. isis hello-padding
B. isis passive-interface
C. is-type level-1
D. isis mesh-group ISIS-MESH

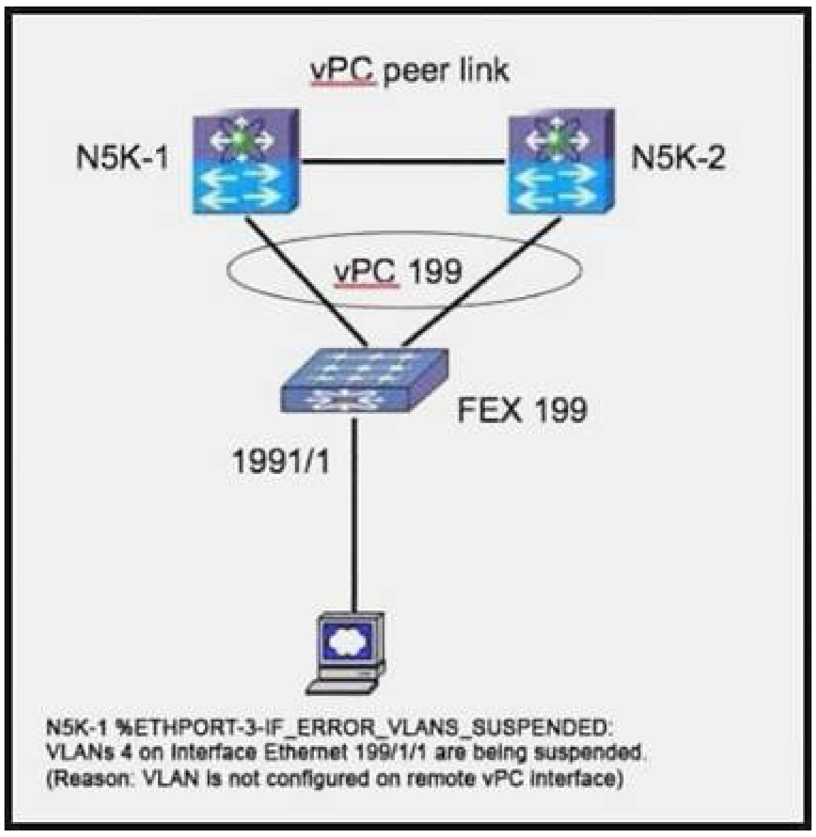
Answer: D

NEW QUESTION 71
What are two requirements for configuring SAN device aliases? (Choose two.)

A. The aliases are independent between fabric nodes.
B. The aliases can be assigned to WWPN and WWNN.
C. The aliases can be assigned to WWNN only.
D. The aliases can be assigned to WWPN only.
E. The aliases must be 64 characters or les

Answer: DE

NEW QUESTION 73
Refer to the exhibit.



```
N5K-1 %ETHPORT-3-IF_ERROR_VLANS_SUSPENDED:
VLANs 4 on Interface Ethernet 199/1/1 are being suspended.
(Reason: VLAN is not configured on remote vPC interface)
```

Which corrective action is taken to resolve the problem?

A. Trunk four VLANs on interface ethernet 199/1/1.
B. Use the shut and no shut interface ethernet 199/1/1so that the VLANs come up.
C. Place interface ethernet 199/1/1 in VLAN 4 in the N5K-2 configuration.
D. Prune all but four VLANs from vPC 199.
E. Add VLAN 4 to vPC 199.

Answer: C

Explanation: Place interface ethernet 199/1/1 in VLAN 4 in the N5K-2 configuration.

NEW QUESTION 75
What is the default Fibre Channel interface type for an FCIP virtual interface?

A. TF
B. E
C. TE
D. F

Answer: B

NEW QUESTION 79
You are configuring QoS on a Cisco Nexus 5000 Series switch. Which option is defined when configuring a CoPP policy?

A. network QoS
B. control plane
C. QoS
D. queuing

Answer: B

NEW QUESTION 81
Within the vPC configuration of the 7K's, the command peer switch is configured. What is the result of enabling the command?

A. Both vPC peers use the same STP root ID.
B. The Vpc primary switch (7k-4 in this case) also serves as the STP root to improve vPC convergence.
C. The vPC secondary switch (7k-3 in this case) server as the STP root to improve vPC performance
D. Allow 7k-3 to act as the active HSRP gateway for packets that are addressed to the MAC address of7K-4
E. Automatically disable IP redirects on all interface VLANs mapped over a vPC VLAN to avoid generation of IP redirect messages for packets switched though the vPC peer gateway router
F. Enable faster convergence of ARP tables after the vPC peer link flap
G. 9999

Answer: A

NEW QUESTION 85
Within the vPC configuration of the 7K's the command peer-gateway is configured as confirmed with the command show vpc. what is the result of enabling this command?

A. Enable 7k-3 to act as the active gateway for packet received on VLAN 101 that are addressed to the MAC address of 7k-4
B. Enables n7k-4 to use of the vpc peer link for forwarding packets received on VLAN 100 that are addressed to the MACRESS OF 7K-4
C. Generates IP redirect messages for packet switched though the peer-gateway router
D. Cause the HSRP active router to update the ARP table on the standby router for faster convergence after the vPC peer link has flapped
E. Allow the vpc peers to coordinate the IACP ID with must be the same on all links on all the port channel.

Answer: D

Explanation: The vPC peer gateway command allows either Nexus 7000 to intercept any packet (including HSRP packets) which is destined to the other peer's MAC address to prevent the packet from traversing the vPC peer link.

NEW QUESTION 86
Without having access to Fabric Path show commands, how can you confirm whether Fabric Path is configured on the two vPC peer 7K-3 and 7K-4?

A. Show vpc would not indicate any downstream virtual port channel vPC parameter with active VLANs
B. Show vpc role on both 7K-3 and 7K-4 would indicate their role as primary
C. Show interface would indicate port-channel 1 and 2 would use a port mode of Fabric path 0.
D. Show hsrp would be blank, since FHRP is not supported or required when using Fabric Path

Answer: A

NEW QUESTION 90
You have a vPC configuration with two functional peers. The peer link is up and the peer-link feature is restricted the spanning-tree operations in the configuration? (choose two)

A. vPC imposes a rule that the peer link is always blocking.
B. vPC removes some VLANs from the spanning tree for vPC use.
C. The primary and secondary switch generate and process BPDUs.
D. vPC requires the peer link to remain in the forwarding state.
E. The secondary switch processes BPDUs only if the peer-link fails.

Answer: CD

NEW QUESTION 92
What are two prerequisite to running the Smart Call Home feature on a Cisco nexus 6000 series switch? (Select two)

A. The switch must have SMTP access to an email server
B. The switch must have public management IP address
C. The switch must have SMTP access to a Cisco.com email server
D. The switch must have an active service contract
E. The switch must be configured to use an email address from the @cisco.com

Answer: AD

Explanation: Prerequisites for Smart Call Home
You must have e-mail server connectivity.
You must have access to contact name (SNMP server contact), phone, and street address information.
You must have IP connectivity between the switch and the e-mail server.
You must have an active service contract for the device that you are configuring.
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/
6x/b_6k_System_Mgmt_Config_6x/b_6k_System_Mgmt_Config_602N11_chapter_01010.html#con_ 1058068

NEW QUESTION 96
You have a Cisco Fabric Path network, you must extend the network to support more than 16 million segment, what should you do?

A. Enable the interface-vlan feature and configure the VLAN IDs
B. Enable the nv overlay feature and configure the segment IDs
C. Enable the vn-segment-vlan-based feature and configure segment IDs
D. Enable the FabricPath feature and configure the VLAN IDs.

Answer: C

Explanation: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-series-switches/whitepaper- c11-737022.html

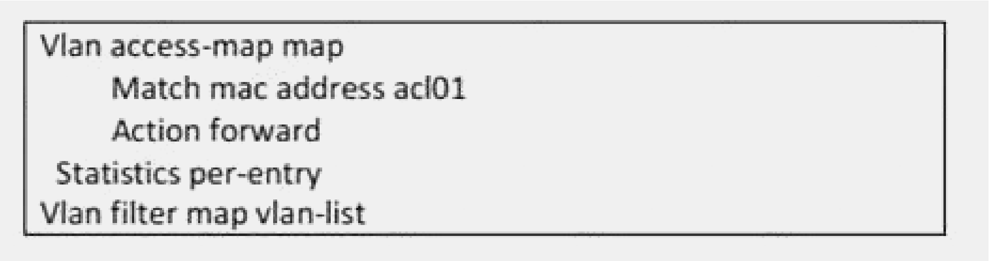
NEW QUESTION 98
When configuring PIM to support an OTV implementation, Which PIM configuration is supported in Cisco NX-OS?

A. Switch(config-if)tt ip pirn ssm default
B. switch(config-if)# ip pim sparse-mode
C. Switch(config-if)tf ip pim spase-mode
D. Switch(config-if)tf ip pim sparse-dense-mode

Answer: B

Explanation: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6- x/multicast/configuration/guide/b_Cisco_Nexus_9000_Series_NXOS_ Multicast_Routing_Configuration_Guide/b_Cisco_Nexus_9000_Series_NXOS_ Multicast_Routing_Configuration_Guide_chapter_011.html

NEW QUESTION 101
Refer to the exhibit.



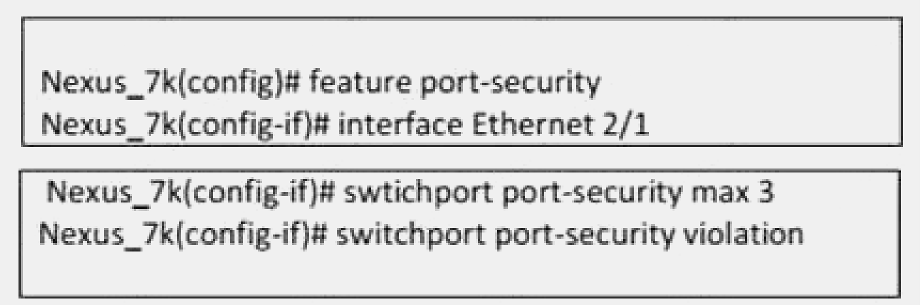
```
Vlan access-map map
        Match mac address acl01
        Action forward
  Statistics per-entry
Vlan filter map vlan-list
```

Which result of the configuration snippet is true?

A. A VACL map in applied to VLAN 101 and VLAN 200
B. VACL acl is applied to VLAN 100 through 200
C. Acl is applied to all of the VLANs on the switch
D. Global statistics are provided for the ACL map

Answer: B

NEW QUESTION 104
Refer to the exhibit.



```
Nexus_7k(config)# feature port-security
Nexus_7k(config-if)# interface Ethernet 2/1

 Nexus_7k(config-if)# swtichport port-security max 3
Nexus_7k(config-if)# switchport port-security violation
```

Which two options are results of the configuration on the Cisco Nexus switch are true? (Choose two.)

A. When the interface receives a packet triggering the violation, address learning is stopped and ingress traffic from the nonsecure MAC address is dropped
B. When the interface receives a packet triggering the violation, a syslog message is logged, address learning continues, and all traffic continues, and traffic continues to forwarded
C. Port security on the Ethernet 2/1 interface uses the dynamic method for MAC address learning
D. When the interface receives a packet triggering the volition, the interface is error disable
E. Port security on the Ethernet 2/1 interface users the sticky method for MAC address learning all traffic continue to be

Answer: AC

NEW QUESTION 105
Which option accurately describes the implementation of Fibre Channel domain IDs?

A. Are assigned on a peer-switch basis
B. Are assigned on a per-line card basis
C. Must be the dame on all on the Fabre Channel switch in the fabric
D. Must be unique on all the Fibre Channel switches in the fabric

Answer: A

NEW QUESTION 107
When configure HSPR on IPv6 enabled interface, which two configuration is correct.

A. switchA{config-if)» standbyt 6 preempt
B. switchA(config-if)» hsrp <group-number>
C. switchA(config-if)ff key 6
D. switchA{config-if)» hsrp version 2
E. switchA{config-if)B priority <level>

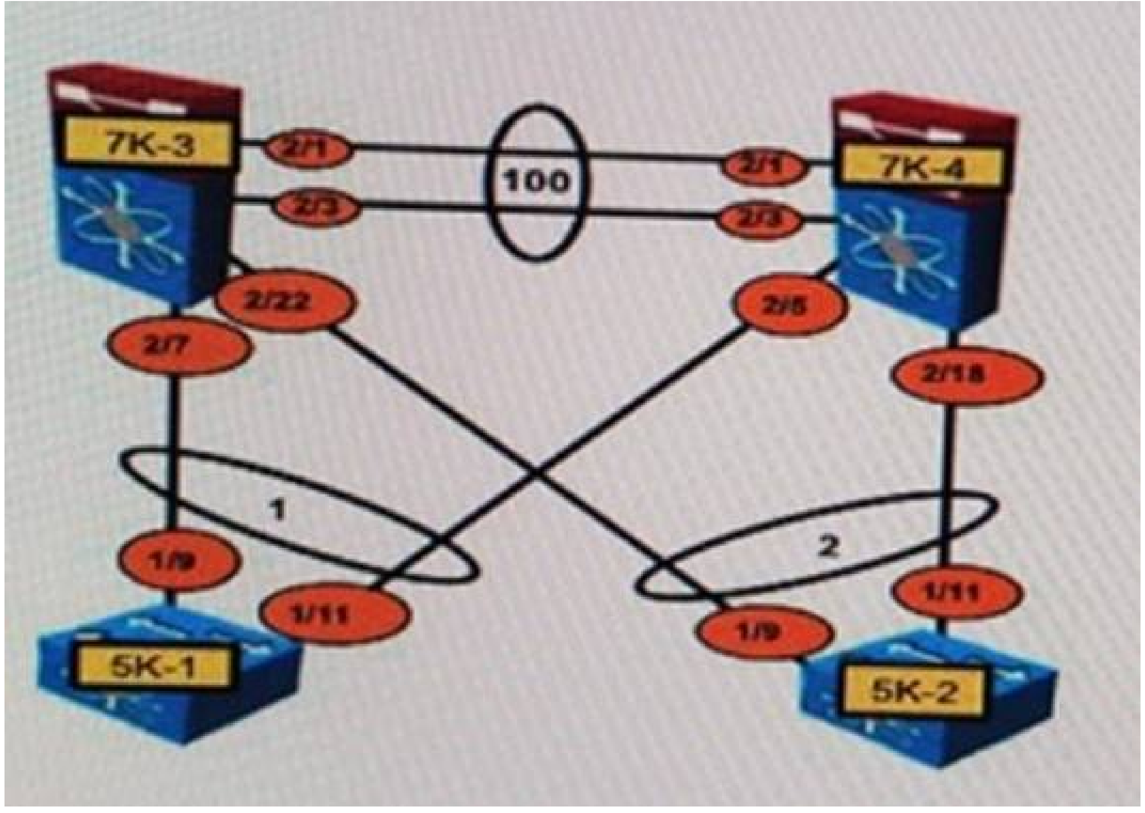
Answer: B

NEW QUESTION 111
You have a vPC configuration with two functional peers. The peer link is up and the peer-link feature is restricted the spanning-tree operations in the configuration? '(choose two)

A. vPC imposes a rule that the peer link is always blocking.
B. vPC removes some VLANs from the spanning tree for vPC use.
C. The primary and secondary switch generate and process BPDUs.
D. vPC requires the peer link to remain in the forwarding state.
E. The secondary switch processes BPDUs only if the peer-link fail

Answer: CD

NEW QUESTION 112
Scenario:
The following four questions concern the Nexus 7010' s which are configured as a vPC pair at the core of a Data Center network. You can utilize all the available show commands to answer the Questions Access to the running-configuration is not allowed.
Instructions:
Enter NX-OS commands on 7K-3 and 7K-4 to verity network operation and answer four multiplechoice questions
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the switch to gain access to the console of the switch. No console or enable passwords are required.
To access the multiple-choice questions, click on the numbered boxes on the loft of the top panel. There are four multiple-choice questions with this task Be sure to answer all four questions before selecting the Next button
Topology:



```
7K-4#
```

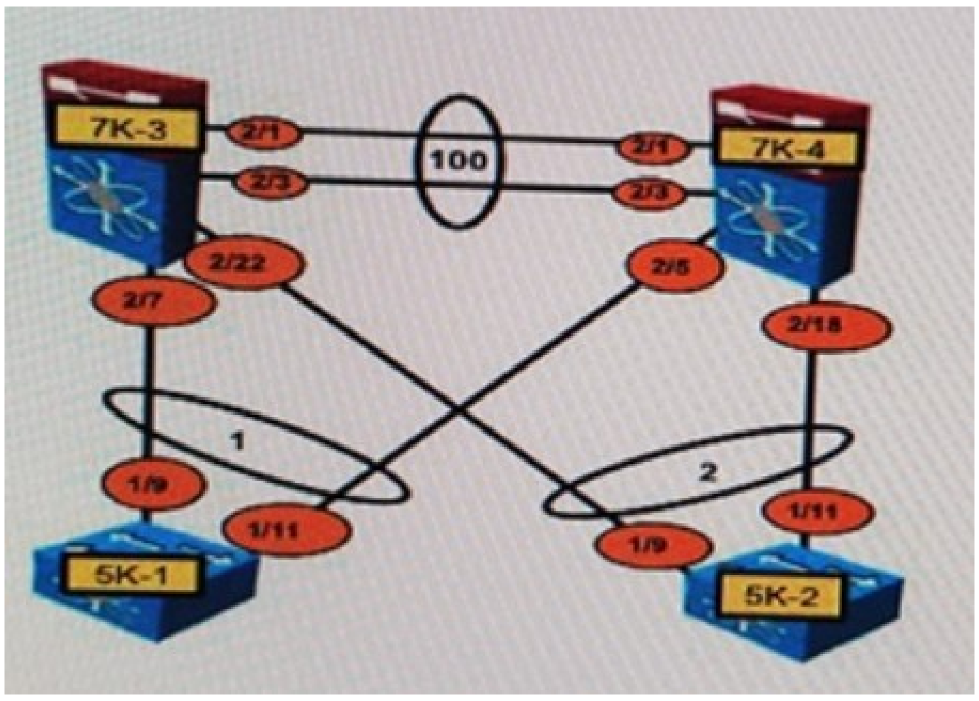
```
7K-3#
```

Which interface is used for the vPC peer keepalive on both 7000' s?

A. port-channel 1
B. port-channel 2
C. port-channel 100
D. mgmt 0
E. Ethernet 2/1
F. Ethernet 2/3

Answer: D

NEW QUESTION 117
Scenario:
The following four questions concern the Nexus 7010' s which are configured as a vPC pair at the core of a Data Center network. You can utilize all the available show commands to answer the Questions Access to the running-configuration is not allowed.
Instructions:
Enter NX-OS commands on 7K-3 and 7K-4 to verity network operation and answer four multiplechoice questions
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the switch to gain access to the console of the switch. No console or enable passwords are required.
To access the multiple-choice questions, click on the numbered boxes on the loft of the top panel. There are four multiple-choice questions with this task Be sure to answer all four questions before selecting the Next button
Topology:



```
7K-4#
```

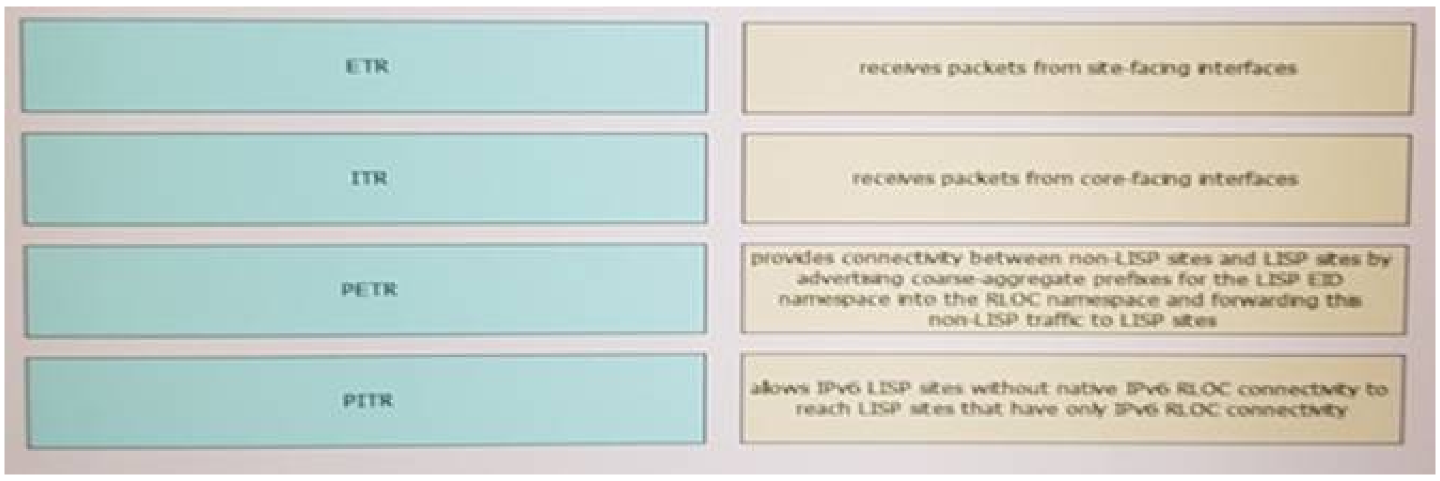
```
7K-3#
```

Within the vpc configuration of the 7K's. the command peer-switch is configured. What is the result of enabling this command'?

A. Both vPC peers use the same STP root ID
B. The vPC primary switch (7K-4 in this case) also serves as the STP root to improve vPC convergence
C. The vPC secondary switch (7K-3 in this case) serves as the STP root to improve vPC performance
D. Allows 7K-3 to act as the active HSRP gateway for packets that are addressed to the MAC address of 7K-4
E. Automatically disables IP redirects on all interface VUANs mapped over a vPC VLAN to avoid generation of IP redirect messages for packets switched through the vPC peer gateway router
F. Enables faster convergence of ARP tables after the vPC peer link flaps

Answer: B

NEW QUESTION 118
DRAG DROP
Drag and drop the LISP devices from the left onto the correct descriptions on the right.

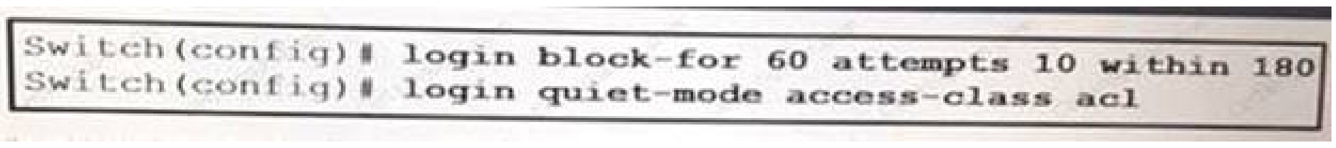


ETR	receives packets from site-facing interfaces
ITR	receives packets from core-facing interfaces
PETR	provides connectivity between non-LISP sites and LISP sites by advertising coarse-aggregate prefixes for the LISP EID namespace into the RLOC namespace and forwarding this non-LISP traffic to LISP sites
PITR	allows IPv6 LISP sites without native IPv6 RLOC connectivity to reach LISP sites that have only IPv6 RLOC connectivity

Answer:

Explanation: ITR = receives packets from site-facing interfaces ETR = receives packets from core-facing interfaces
PITR = provides connectivity between non-LISP sites and LISP sites by advertising coarse-aggregate prefixes for the LISP EID namespace into the Internet DFZ (RLOC namespace) and forwarding this non-LISP traffic to LISP sites
PETR = allows IPv6 LISP sites without native IPv6 RLOC connectivity to reach LISP sites that only have IPv6 RLOC connectivity

NEW QUESTION 120
Refer to Exhibit.



```
Switch(config)# login block-for 60 attempts 10 within 180
Switch(config)# login quiet-mode access-class acl
```

Which statement is true about the impact to login requests on a Cisco NX-OS switch that uses this configuration.

A. Hosts in the ACL are denied after 10 failed login attempts occur within 180 seconds.
B. Hosts in the ACL are allowed after 10 failed login attempts occur within 180 seconds.
C. All hosts are denied if 10 failed login attempts from hosts in the ACL occur in 180 seconds.
D. Hosts outside the ACL are allowed if more than 10 failed login attempts occu

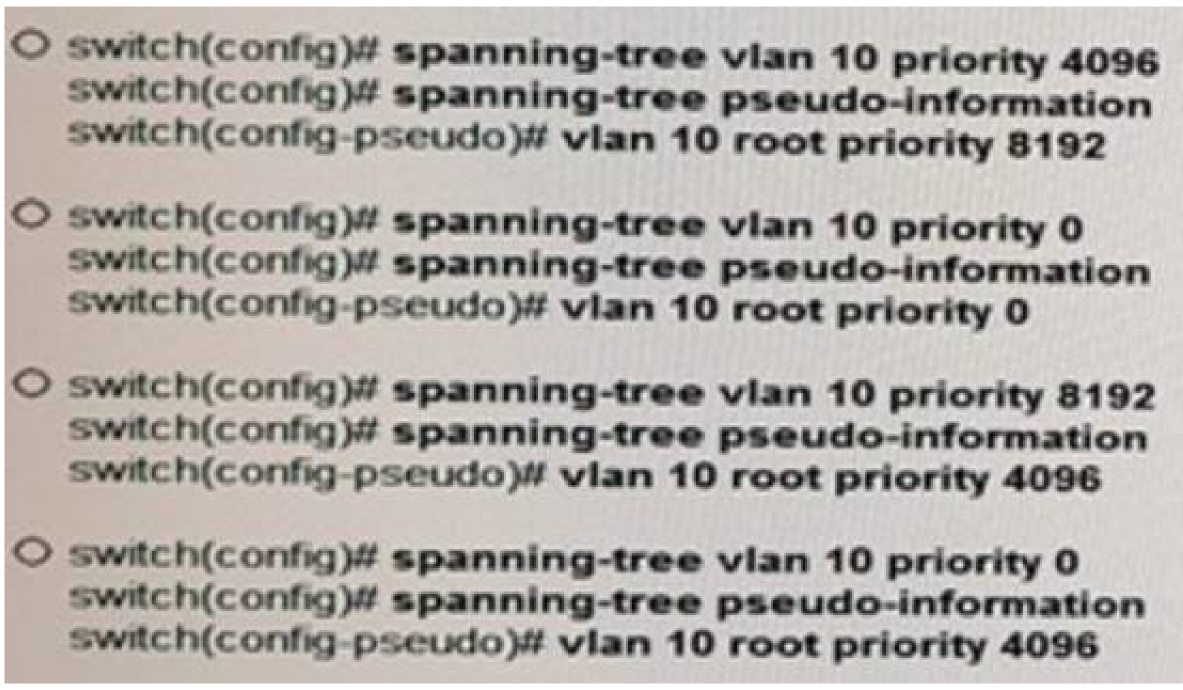
Answer: D

NEW QUESTION 125
When configuring OSPF, which two network types will avoid the DR and BDR election process between connected devices? (Choose Two)

A. non-broadcast
B. multi-access
C. point-to-multipoint
D. broadcast
E. point-to-point

Answer: CE

NEW QUESTION 126
You configure STP on a switch that is attached to a Cisco Fabric Path domain and that has the vPC feature deployed. How do you configure STP on the switch in the Cisco FabricPath domain on VL AN 10?



```
○ switch(config)# spanning-tree vlan 10 priority 4096
  switch(config)# spanning-tree pseudo-information
  switch(config-pseudo)# vlan 10 root priority 8192

○ switch(config)# spanning-tree vlan 10 priority 0
  switch(config)# spanning-tree pseudo-information
  switch(config-pseudo)# vlan 10 root priority 0

○ switch(config)# spanning-tree vlan 10 priority 8192
  switch(config)# spanning-tree pseudo-information
  switch(config-pseudo)# vlan 10 root priority 4096

○ switch(config)# spanning-tree vlan 10 priority 0
  switch(config)# spanning-tree pseudo-information
  switch(config-pseudo)# vlan 10 root priority 4096
```

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

Answer: C

NEW QUESTION 127
What is the purpose of the resequence command for ACLs?

A. to rearrange the order of the access lists in the running configuration
B. to assign new sequence numbers to the rules in an ACL
C. to refresh ACI programming in ASICs to apply the ACL changes
D. to rearrange ACL entries

Answer: B

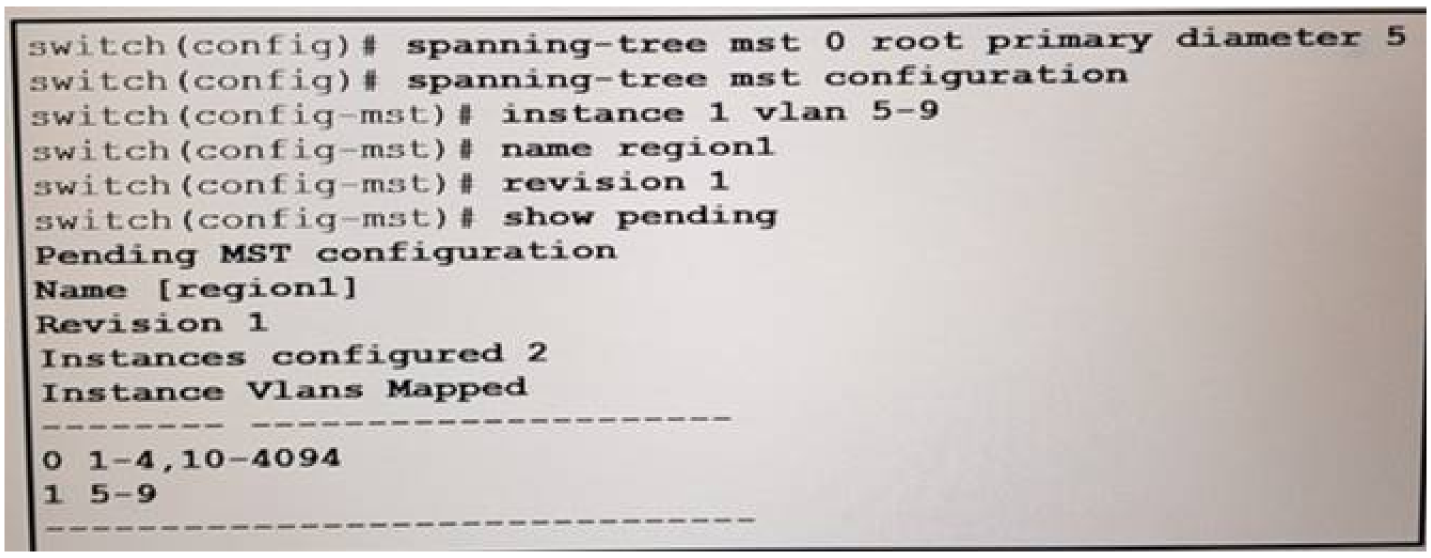
Explanation: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nxos/security/configuration/guide/sec_nx-os-cfg/sec_macacls.pdf

NEW QUESTION 128
What is the result when the configured RTT of an FCIP link is smaller than the measured RTT?

A. The minimum available bandwidth for the link must be increased
B. The link might be oversubscribed.
C. The TCP sliding window constantly resets
D. The link might not be fully utilize

Answer: B

NEW QUESTION 129
Refer to the exhibit.



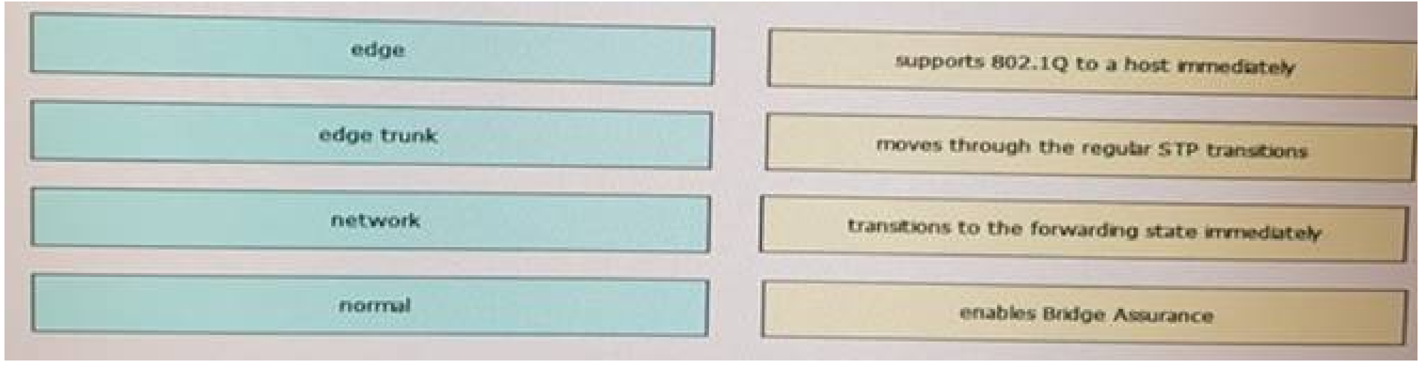
```
switch(config)# spanning-tree mst 0 root primary diameter 5
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 5-9
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name [region1]
Revision 1
Instances configured 2
Instance Vlans Mapped
-------- ---------------------
0 1-4,10-4094
1 5-9
-------------------------------
```

What does the diameter command specify?

A. the maximum number of hops between any two bridges on a network.
B. the number of VLANs that were removed from the MSTI.
C. the VLAN that becomes the root of the MSTI
D. the maximum number of hops between any two MST instances on a network

Answer: A

NEW QUESTION 130
DRAG DROP
Drag and drop the types of spanning tree ports from the left onto the correct descriptions on the right


edge
edge trunk
network
normal
supports 802.1Q to a host immediately
moves through the regular STP transitions
transitions to the forwarding state immediately
enables Bridge Assurance

Answer:

Explanation: Edge = edge port interface immediately transitions to the forwarding state Edge trunk = supports 802.1Q to a host immediately
Network = enables Bridge Assurance
Normal = moves through the regular STP transactions

NEW QUESTION 133
Which technology relies on STP as a failsafe mechanism?

A. vPC
B. VXLAN
C. FabricPath
D. MPLS

Answer: A

NEW QUESTION 136
Which information does the show fcns database command display?

A. FCID
B. port name
C. nWWN
D. interface

Answer: A

Explanation: https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/n5k/commands/show-fcnsdatabase. html

NEW QUESTION 137
Which two statements are true when implementing fabric binding? (Choose two.)

A. The MAINFRAME_PKG or the ENTERPRISE_PKG license must be installed on a switch
B. Cisco fabric Services must be enabled on a switch to distribute configuration information
C. Activation must be performed globally
D. Activation must be performed globally on a switch
E. Activation must be performed on a per-VSAN basis

Answer: AE

Explanation: https://www.cisco.com/en/US/products/ps5989/products_configuration_guide_chapter09186a0080 5ecf5c.html

NEW QUESTION 140
Which command allows a Cisco Nexus 7000 Series Switch to receive NTP configuration updates by using Cisco Fabric Services?

A. N7k (config) # feature ntp
B. N7k (config) # ntp distribute
C. N7k <config) # distribute
D. N7k (config) # ntp master

Answer: B

Explanation: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nxos/system_management/configuration/guide/sm_nx_os_cli/sm_3ntp.html
Enables the device to receive NTP configuration updates that are distributed through CFS.

NEW QUESTION 142
Which command configures the aging time for VLAN 100 to 50 minutes?

A. mac address-table aging-time 3000 vlan 100
B. mac address-table aging-time 50
C. mac address-table aging-time 300
D. mac address-table aging-time 50 vlan 100

Answer: A

NEW QUESTION 146
Which command should you use to apply a custom CoPP policy?

A. Nexus7000(config-cp)# service-policy input copp policy-moderate-policy
B. Nexus700Q(config)# class-map type control-plane match-any copp-system-p-policy
C. Nexus7000(config)# policy-map type control-plane copp-system-p-policy
D. Nexus7000(config)# copp profile strict

Answer: A

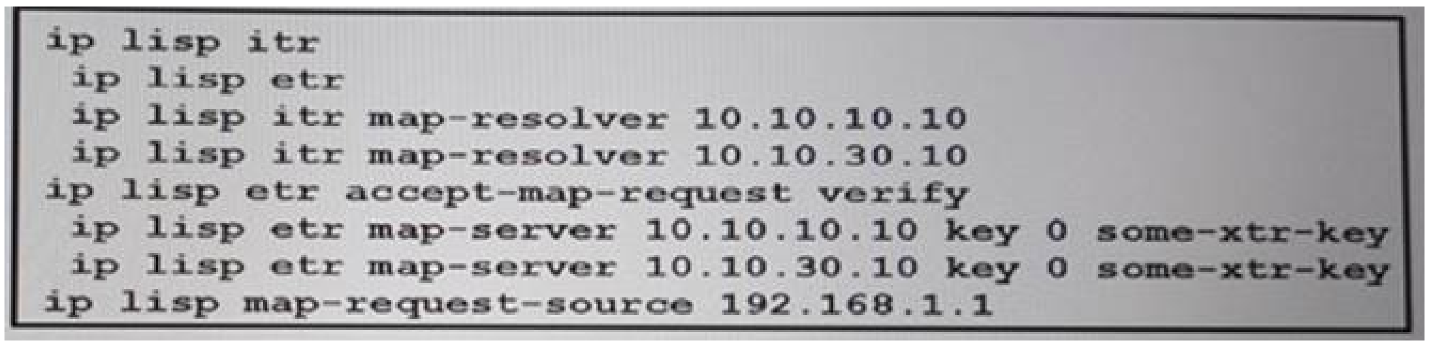
NEW QUESTION 149
You have two roles that are associated to the same user. Which statement is true about how the roles are evaluated to form the permissions of the user?

A. A combination of all commands that are permitted by the roles can be executed
B. A role that denies a command takes priority over a role that permits a command
C. An implicit permit is applied to both roles at the end of each rule set
D. Only the commands that are permitted by both roles can be executed

Answer: A

Explanation: Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nxos/security/configuration/guide/sec_nx-os-cfg/sec_rbac.html

NEW QUESTION 150
Refer to the exhibit.



```
ip lisp itr
 ip lisp etr
 ip lisp itr map-resolver 10.10.10.10
 ip lisp itr map-resolver 10.10.30.10
ip lisp etr accept-map-request verify
 ip lisp etr map-server 10.10.10.10 key 0 some-xtr-key
 ip lisp etr map-server 10.10.30.10 key 0 some-xtr-key
ip lisp map-request-source 192.168.1.1
```

Which two statements about the LISP implementation are true? (Choose two)

A. A LISP locator reachability algorithm is used
B. 192.168.1.1 is used as the map-request source
C. The address of the locator is used as the map-request source
D. LISP ETR caches the IPv4 mapping data contained in a map-request message
E. LISP ITR caches the IPv4 mapping data contained in a map-request message

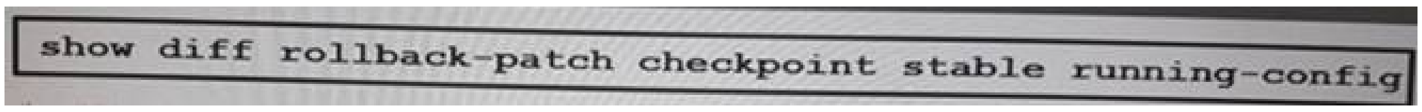
Answer: BD

NEW QUESTION 155
Which option accurately describes an EPLD upgrade on supervisor modules?

A. is disruptive in dual supervisor configurations
B. is disruptive in single supervisor configurations
C. requires an NX-OS image upgrade
D. can be performed during an ISSU

Answer: B

NEW QUESTION 159
Refer to the exhibit.



```
show diff rollback-patch checkpoint stable running-config
```

Which option is the result of the command when it is executed on a Cisco Nexus 9000 Series switch?

A. It implements a best-effort rollback to a stable user checkpoint.
B. It displays the differences between the latest rollback patch and the running configuration
C. It performs a rollback to the specified checkpoint name or file based on the current differences in the running configuration
D. It displays the differences between the source and the destination checkpoint selection

Answer: B

NEW QUESTION 160
Which two PIM modes on a Cisco Nexus 7000 Series switch require you to configure an RP? (Choose two)

A. SDM
B. DM
C. ASM
D. SSM
E. BIDIR

Answer: CE

Explanation: Any Source Multicast (ASM) provides discovery of multicast sources. It builds a shared tree between sources and receivers of a multicast group and supports switching over to a source tree when a new receiver is added to a group. ASM mode requires that you configure an RP.
Single Source Multicast (SSM) builds a source tree originating at the designated router on the LAN segment that receives a request to join a multicast source. SSM mode does not require you to configure RPs. Source discovery must be accomplished through other means.
Bidirectional shared trees (Bidir) build a shared tree between sources and receivers of a multicast group but do not support switching over to a source tree when a new receiver is added to a group. Bidir mode requires that you configure an RP. Bidir forwarding does not require source discovery because only the shared tree is used.
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/ multicast/configuration/guide/n7k_multic_cli_5x/pim.html

NEW QUESTION 163
Which feature does the spanning-tree port type network command enable?

A. TrustSec
B. Bridge Assurance

C. BPDU Guard
D. Rapid PVST+

Answer: B

Explanation: Network ports are connected only to switches or bridges. Bridge Assurance is enabled only on network ports.

NEW QUESTION 164
By default it will take 10 seconds for authentication to fail due to an unresponsive RADIUS server before a Cisco Nexus series switch reverts to another RADIUS server or local authentication. What is one efficient way to improve the reaction time to a RADIUS server failure?

A. Decrease the global RADIUS retransmission count to 1.
B. Decrease the global RADIUS timeout interval to 5 seconds.
C. Configure the RADIUS retransmission count and timeout interval per server, versus globally.
D. Configure per server a test idle timer, along with a username and passwor

Answer: D

Explanation: You can monitor the availability of RADIUS servers. These parameters include the username and password to use for the server and an idle timer. The idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. You can configure this option to test servers periodically. The test idle timer specifies the interval during which a RADIUS server receives no requests before the Nexus 5000 Series switch sends out a test packet. The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, the Nexus 5000 Series switch does not perform periodic RADIUS server monitoring.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_0_1a/CLIConfigurationGuide/sec_radius.html

NEW QUESTION 167
Which statement explains why a Cisco UCS 6200 Fabric Interconnect that is configured in end-host mode is beneficial to the unified fabric network?

A. There is support for multiple (power of 2) uplinks.
B. Upstream Layer 2 disjoint networks will remain separated.
C. The 6200 can connect directly via vPC to a Layer 3 aggregation device.
D. STP is not required on the uplink ports from the 6200.

Answer: D

Explanation: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unifiedcomputing/whitepaper_c11-701962.html

NEW QUESTION 172
Which two statements about Cisco Nexus 7000 line cards are true? (Choose two.)

A. M1, M2, and F1 cards are allowed in the same VDC.
B. M line cards are service-oriented and likely face the access layer and provide Layer 2 connectivity.
C. F line cards are performance-oriented and likely connect northbound to the core layer for Layer 3 connectivity.
D. M line cards support Layer 2, Layer 3, and Layer 4 with large forwarding tables and a rich feature set.
E. The F2 line card must reside in the admin VD

Answer: AD

Explanation: Cisco is introducing a new line card called as F3 Module which has rich feature set and offers high performance 40G/100G port density to the Nexus 7000 product family. Cisco also introduced a new feature in NX-OS 6.2(2) where the F2e line card can be in the same VDC as M1 or M2 Line Card. The objective of this session is to cover detailed steps and methodology of migrating Nexus 7000 with VDC types prior to NX-OS 6.2 to the newer F3 or M/F2e VDC types. The session also covers the effect of VDC migration with commonly used Network features, firewall and load balancer services.
M-Series XL modules support larger forwarding tables. M-Series modules are frequently required at network core, peering, and aggregation points. When used with the F1-Series, the M-Series modules provide inter-VLAN services and form a pool of Layer 3 resources for the system.
Reference: https://www.ciscolive2014.com/connect/sessionDetail.ww?SESSION_ID=2244
And http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/VMDC/2- 6/vmdctechwp.html

NEW QUESTION 174
Which statement about the Layer 3 card on the Cisco Nexus 5500 Series Switch is true?

A. BGP support is not provided, but RIP, EIGRP, and OSPF support is provided.
B. Up to two 4-port cards are supported with up to 160 Gb/s of Layer 3 forwarding capability.
C. Up to 16 FEX connections are supported.
D. Port channels cannot be configured as Layer 3 interface

Answer: C

Explanation: From the Cisco NX-OS 5.1(3)N1(1) release and later releases, each Cisco Nexus 5500 Series device can manage and support up to 24 FEXs without Layer 3. With Layer 3, the number of FEXs supported per Cisco Nexus 5500 Series device is 8. With Enhanced vPC and a dual-homed FEX topology each FEX is managed by both Cisco Nexus 5000 Series devices. As a result, one pair of Cisco Nexus 5500 Series devices can support up to 24 FEXs and 16 FEXs for Layer 2 and Layer 3.
Reference:
http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1
/n5k_enhanced_vpc.html

NEW QUESTION 179
Which three items must be configured in the port profile client in Cisco UCS Manager? (Choose three.)

A. port profile
B. DVS
C. data center
D. folder
E. vCenter IP address
F. VM port group

Answer: BCD

Explanation: After associating an ESX host to a DVS, you can migrate existing VMs from the vSwitch to the DVS, and you can create VMs to use the DVS instead of the vSwitch. With the hardware-based VN-Link implementation, when a VM uses the DVS, all VM traffic passes through the DVS and ASIC-based switching is performed by the fabric interconnect.
In Cisco UCS Manager, DVSes are organized in the following hierarchy: vCenter
Folder (optional) Datacenter Folder (required) DVS
At the top of the hierarchy is the vCenter, which represents a VMware vCenter instance. Each vCenter contains one or more datacenters, and optionally vCenter folders with which you can organize the
datacenters. Each datacenter contains one or more required datacenter folders. Datacenter folders contain the DVSes.
Reference: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/gui/config/guide/1-3-1/b_UCSM_GUI_Configuration_Guide_1_3_1/UCSM_GUI_Configuration_Guide_1_3_1_chapter28.h tml

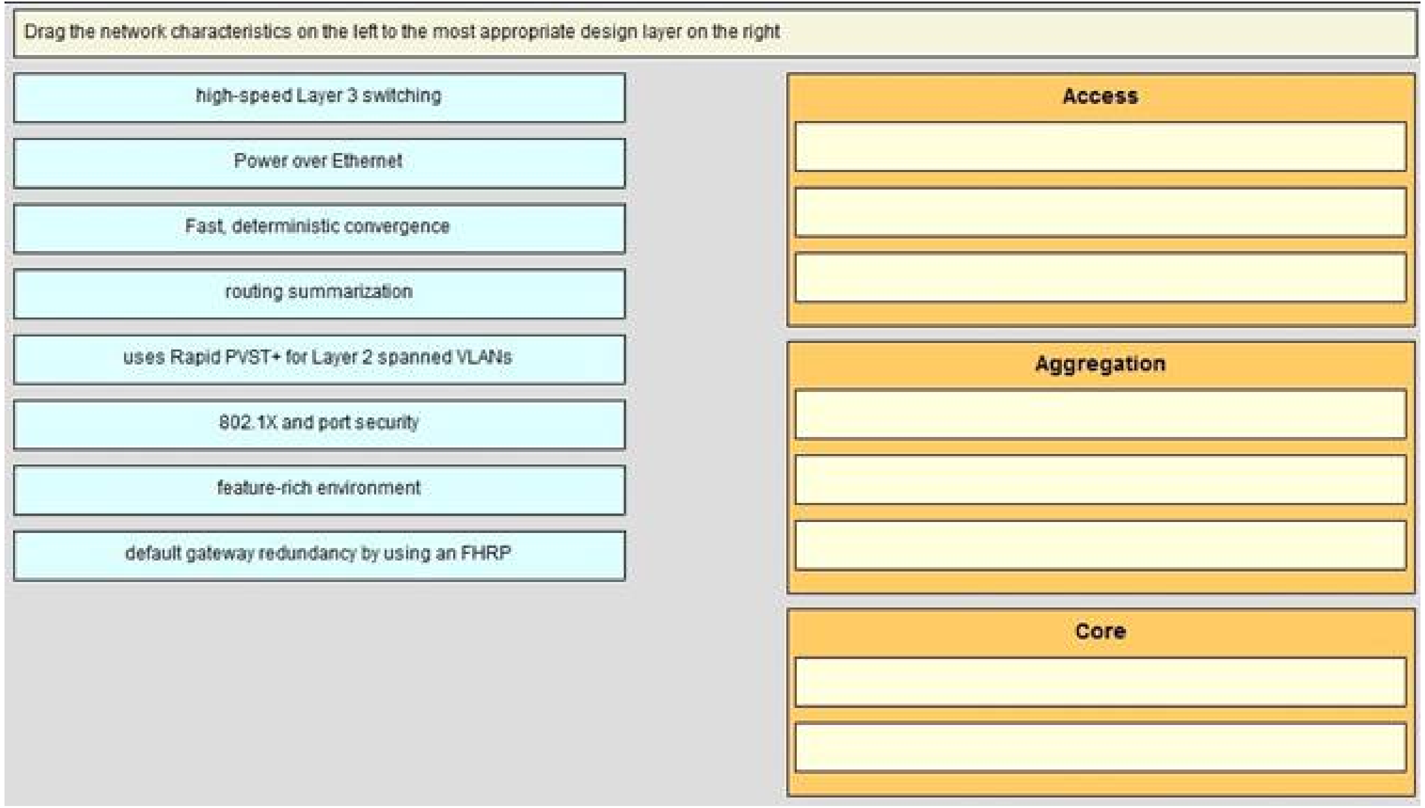
NEW QUESTION 181
Which protocol is the foundation for unified fabric as implemented in Cisco NX-OS?

A. Fibre Channel
B. Data Center Bridging
C. Fibre Channel over Ethernet
D. N proxy virtualization
E. N Port identifier virtualization

Answer: C

Explanation: Fibre Channel over Ethernet (FCoE) is one of the major components of a Unified Fabric. FCoE is a new technology developed by Cisco that is standardized in the Fibre Channel Backbone 5 (FC-BB-5) working group of Technical Committee T11 of the International Committee for Information Technology Standards (INCITS). Most large data centers have huge installed bases of Fibre Channel and want a technology that maintains the Fibre Channel model. FCoE assumes a lossless Ethernet, in which frames are never dropped (as in Fibre Channel) and that therefore does not use IP and TCP. Reference: http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-seriesswitches/white_paper_c11-495142.html

NEW QUESTION 182
DRAG DROP
Drag the network characteristics on the left to the most appropriate design layer on the right.



Drag the network characteristics on the left to the most appropriate design layer on the right

high-speed Layer 3 switching
Power over Ethernet
Fast, deterministic convergence
routing summarization
uses Rapid PVST+ for Layer 2 spanned VLANs
802.1X and port security
feature-rich environment
default gateway redundancy by using an FHRP

Answer:

Explanation: The access layer is the first tier or edge of the campus. It is the place where end devices (PCs, printers, cameras, and the like) attach to the wired portion of the campus network. It is also the place where devices that extend the network out one more level are attached—IP phones and wireless access points (APs) being the prime two key examples of devices that extend the connectivity out one more layer from the actual campus access switch. The wide variety of possible types of devices that can connect and the various services and dynamic configuration mechanisms that are necessary, make the access layer one of the most feature-rich parts of the campus network. You can enable an 802.1X port for port security by using the dot1x multiple-hosts interface configuration command.

You must also configure port security on the port by using the switchport port-security interface configuration command. With the multiple-hosts mode enabled, 802.1X authenticates the port, and port security manages network access for all MAC addresses, including that of the client. You can then limit the number or group of clients that can access the network through an 802.1X multiple-host port.

NEW QUESTION 184
Which statement about RBAC user roles on a Cisco Nexus switch is true?

A. If you belong to multiple roles, you can execute only the commands that are permitted by bothroles (logical AND).
B. Access to a command takes priority over being denied access to a command.
C. The predefined roles can only be changed by the network administrator (superuser).
D. The default SAN administrator role restricts configuration to Fibre Channel interfaces.
E. On a Cisco Nexus 7000 Series Switch, roles are shared between VDC

Answer: B

Explanation: If you belong to multiple roles, you can execute a combination of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose a user has RoleA, which denied access to the configuration commands. However, the users also have RoleB, which has access to the configuration commands. In this case, the users have access to the configuration commands.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/ CLIConfigurationGuide/sec_rbac.html

NEW QUESTION 185
Which two security features are only supported on the Cisco Nexus 7000 Series Switches? (Choose two.)

A. IP source guard
B. traffic storm control
C. CoPP
D. DHCP snooping
E. Dynamic ARP Inspection
F. NAC

Answer: BF

Explanation: A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces.
Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 10-millisecond interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends. Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/dcnm/security/configuration/g uide/b_Cisco_DCNM_Security_Configuration_Guide Release_5- x/Cisco_DCNM_Security_Configuration_Guide Release_5-x_chapter17.html
And http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/dcnm/security/configuration/g uide/b_Cisco_DCNM_Security_Configuration_Guide Release_5- x/Cisco_DCNM_Security_Configuration_Guide Release_5-x_chapter1.html

NEW QUESTION 190
Which statement about the implementation of Cisco TrustSec on Cisco Nexus 7000 Series Switches is true?

A. While SGACL enforcement and SGT propagation are supported on the M and F modules, 802.1AE (MACsec) support is available only on the M module.
B. SGT Exchange Protocol is required to propagate the SGTs across F modules that lack hardware support for Cisco TrustSec.
C. AAA authentication and authorization is supported using TACACS or RADIUS to a Cisco Secure Access Control Server.
D. Both Cisco TrustSec and 802.1X can be configured on an F or M module interfac

Answer: A

Explanation: The M-Series modules on the Nexus 7000 support 802.1AE MACSEC on all ports, including the new M2-series modules. The F2e modules will have this feature enabled in the future.
It is important to note that because 802.1AE MACSEC is a link-level encryption, the two MACSECenabled endpoints, Nexus 7000 devices in our case, must be directly L2 adjacent. This means we
direct fiber connection or one facilitated with optical gear is required. MACSEC has integrity checks for the frames and intermediate devices, like another switch, even at L2, will cause the integrity checks to fail. In most cases, this means metro-Ethernet services or carrier-provided label switched services will not work for a MACSEC connection.
Reference: http://www.ciscopress.com/articles/article.asp?p=2065720

NEW QUESTION 191
Which statement about implementation of Cisco TrustSec on Cisco Nexus 5546 or 5548 switches are true?

A. Cisco TrustSec support varies depending on Cisco Nexus 5500 Series Switch model.
B. The hardware is not able to support MACsec switch-port-level encryption based on IEEE 802.1AE.
C. The maximum number of RBACL TCAM user configurable entries is 128k.
D. The SGT Exchange Protocol must use the management (mgmt 0) interface.

Answer: B

Explanation: Reference:
https://scadahacker.com/library/Documents/Manuals/Cisco%20-%20TrustSec%20Solution%20Overview.pdf

NEW QUESTION 196
In the dynamic vNIC creation wizard, why are choices for Protection important?

A. They allow reserve vNICs to be allocated out of the spares pool.
B. They enable hardware-based failover.
C. They select the primary fabric association for dynamic vNICs.
D. They allow dynamic vNICs to be reserved for fabric failove

Answer: C

Explanation: Number of Dynamic vNICs – This is the number of vNICs that will be available for dynamic assignment to VMs. Remember that the VIC has a limit to the number of vNICs that it can support and this is based on the number of uplinks between the IOM and the FI. At least this is the case with
the 2104 IOM and the M81KR VIC, which supports ((# IOM Links * 15) – 2)). Also remember that your ESXi server will already have a number of vNICs used for other traffic such as Mgmt, vMotion,
storage, etc, and that these count against the limit.
Adapter Policy – This determines the vNIC adapter config (HW queue config, TCP offload, etc) and you must select VMWarePassThru to support VM-FEX in High Performance mode.
Protection – This determines the initial placement of the vNICs, either all of them are placed on fabric A or Fabric B or they are alternated between the two fabrics if you just select the “Protected” option. Failover is always enabled on these vNICs and there is no way to disable the protection. Reference:
http://infrastructureadventures.com/2011/10/09/deploying-cisco-ucs-vm-fex-for-vsphere-
%E2%80%93-part-2-ucsm-config-and-vmware-integration/

NEW QUESTION 199
How is a dynamic vNIC allocated?

A. Dynamic vNICs are assigned to VMs in vCenter.
B. Dynamic vNICs can only be bound to the service profile through an updating template.
C. Dynamic vNICs are bound directly to a service profile.
D. Dynamic vNICs are assigned by binding a port profile to the service profil

Answer: C

Explanation: The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.
Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.
For VM-FEX that has all ports on a blade in standard mode, you need to use the VMware adapter policy.
For VM-FEX that has at least one port on a blade in high-performance mode, use the VMwarePassThrough adapter policy or create a custom policy. If you need to create a custom policy, the resources provisioned need to equal the resource requirements of the guest OS that needs the most resources and for which you will be using high-performance mode.
Reference: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/vm_fex/vmware/gui/config_gui de/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide/b_GUI_VMware_VMFEX_ UCSM_Configuration_Guide_chapter_010.html

NEW QUESTION 202
Which Cisco Nexus feature is best managed with DCNM-SAN?

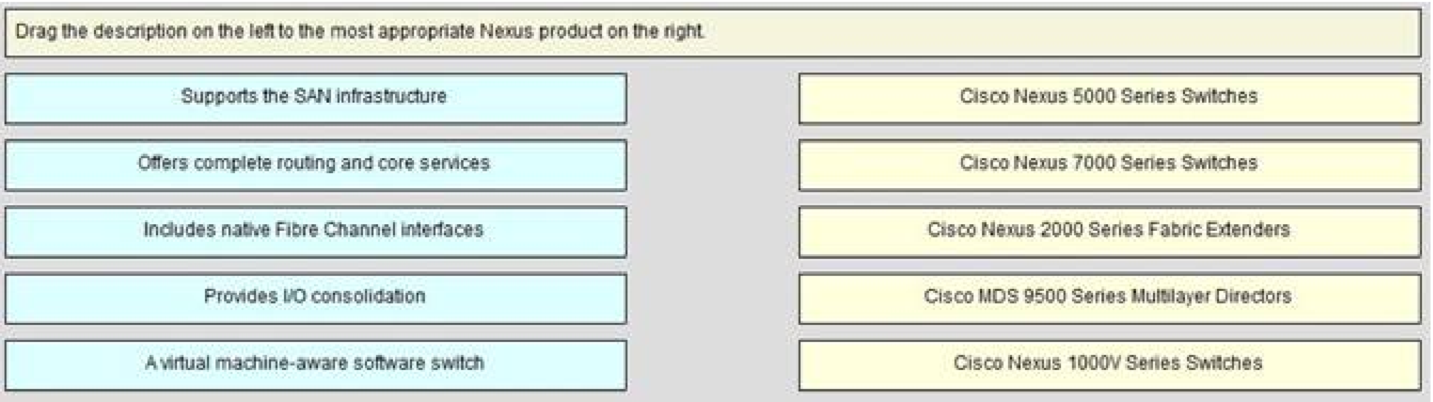
A. VSS
B. domain parameters
C. virtual switches
D. AAA

Answer: B

Explanation: The Fibre Channel domain (fcdomain) feature performs principal switch selection, domain ID distribution, FC ID allocation, and fabric reconfiguration functions as described in the FC-SW-2 standards. The domains are configured on a per VSAN basis. If you do not configure a domain ID, the local switch uses a random ID.
This section describes each fcdomain phase:
- Principal switch selection — This phase guarantees the selection of a unique principal switch across the fabric.
- Domain ID distribution — This phase guarantees each switch in the fabric obtains a unique domain ID.
- FC ID allocation — This phase guarantees a unique FC ID assignment to each device attached to the corresponding switch in the fabric.
- Fabric reconfiguration — This phase guarantees a resynchronization of all switches in the fabric to ensure they simultaneously restart a new principal switch selection phase.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_2/configuration/guides
/sysmgnt/DCNM-SAN/sysmgmt_dcnm/sysmgmt_overview.html#wp1051962

NEW QUESTION 207
DRAG DROP
Drag the description on the left to the most appropriate Nexus product on the right.



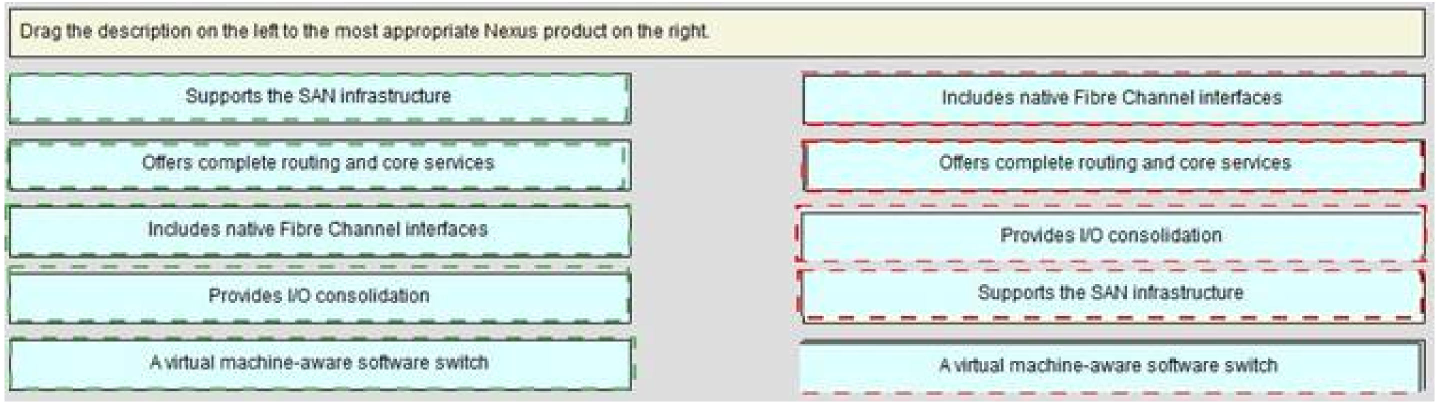
Drag the description on the left to the most appropriate Nexus product on the right.

Supports the SAN infrastructure
Offers complete routing and core services
Includes native Fibre Channel interfaces
Provides I/O consolidation
A virtual machine-aware software switch

Cisco Nexus 5000 Series Switches
Cisco Nexus 7000 Series Switches
Cisco Nexus 2000 Series Fabric Extenders
Cisco MDS 9500 Series Multilayer Directors
Cisco Nexus 1000V Series Switches

Answer:

Explanation:



Drag the description on the left to the most appropriate Nexus product on the right.

Supports the SAN infrastructure
Offers complete routing and core services
Includes native Fibre Channel interfaces
Provides I/O consolidation
A virtual machine-aware software switch

Includes native Fibre Channel interfaces
Offers complete routing and core services
Provides I/O consolidation
Supports the SAN infrastructure
A virtual machine-aware software switch

NEW QUESTION 209
Which two types of traffic are carried over a vPC peer link when no failure scenarios are present? (Choose two.)

A. multicast data traffic
B. unicast data traffic
C. broadcast data traffic
D. vPC keep-alive messages

Answer: AC

Explanation: The vPC peer link is the link used to synchronize states between the vPC peer devices. The vPC peer link carries control traffic between two vPC switches and also multicast, broadcast data traffic. In some link failure scenarios, it also carries unicast traffic. You should have at least two 10 Gigabit Ethernet interfaces for peer links.
Reference:
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-seriesswitches/ configuration_guide_c07-543563.html

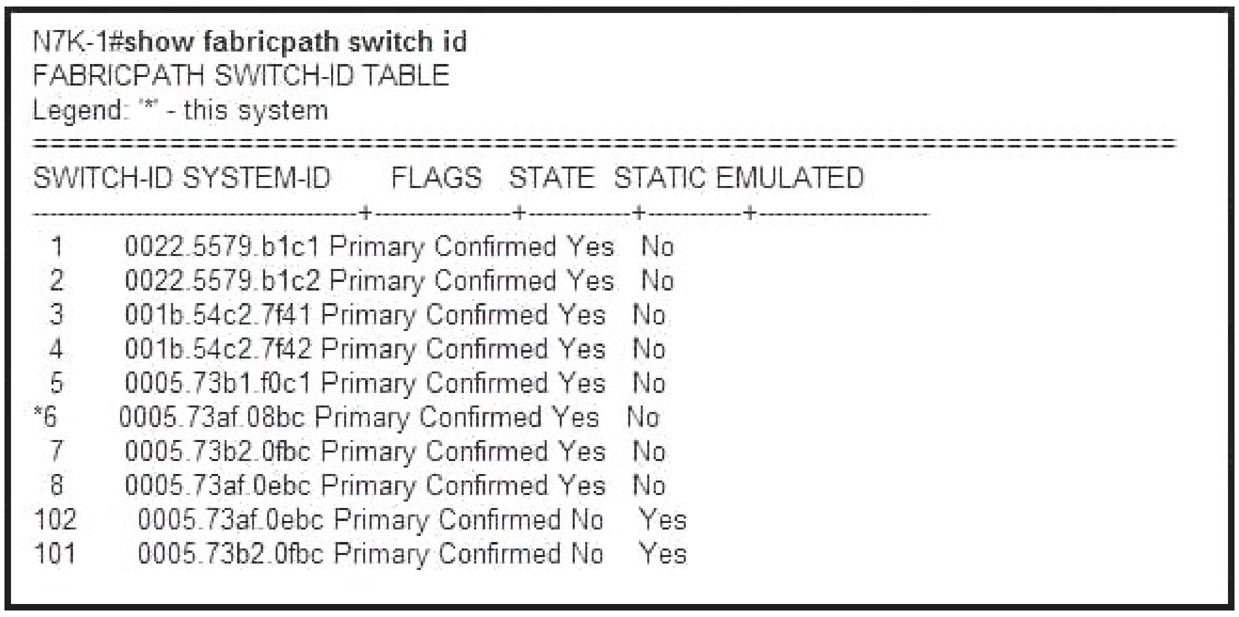
NEW QUESTION 210
Which SCSI terminology is used to describe source and destination nodes?

A. hosts and targets
B. initiators and targets
C. HBA and disks
D. initiators and disks
E. HBA and targets

Answer: B

Explanation: In computer data storage, a SCSI initiator is the endpoint that initiates a SCSI session, that is, sends a SCSI command. The initiator usually does not provide any Logical Unit Numbers (LUNs).
On the other hand, a SCSI target is the endpoint that does not initiate sessions, but instead waits for initiators' commands and provides required input/output data transfers. The target usually provides to the initiators one or more LUNs, because otherwise no read or write command would be possible. Reference:
http://en.wikipedia.org/wiki/SCSI_initiator_and_target

NEW QUESTION 213
Refer to the exhibit.



```
N7K-1#show fabricpath switch id
FABRICPATH SWITCH-ID TABLE
Legend: '*' - this system
=====================================================================
SWITCH-ID SYSTEM-ID       FLAGS   STATE  STATIC EMULATED
--------------------------------+-------------+----------+----------+-----------------
  1      0022.5579.b1c1 Primary Confirmed Yes   No
  2      0022.5579.b1c2 Primary Confirmed Yes   No
  3      001b.54c2.7f41 Primary Confirmed Yes   No
  4      001b.54c2.7f42 Primary Confirmed Yes   No
  5      0005.73b1.f0c1 Primary Confirmed Yes   No
*6      0005.73af.08bc Primary Confirmed Yes   No
  7      0005.73b2.0fbc Primary Confirmed Yes   No
  8      0005.73af.0ebc Primary Confirmed Yes   No
102       0005.73af.0ebc Primary Confirmed No    Yes
101       0005.73b2.0fbc Primary Confirmed No    Yes
```

Which three statements about the Cisco Nexus 7000 switch are true? (Choose three.)

A. An emulated switch ID must be unique when the vPC+ feature is used.
B. Switches with FabricPath and vPC+ consume two switch IDs.
C. Emulated switch IDs must be numbered from 1 to 99.
D. Each switch ID must be unique in the FabricPath topology.
E. Switch IDs must be configured manuall

Answer: BDE

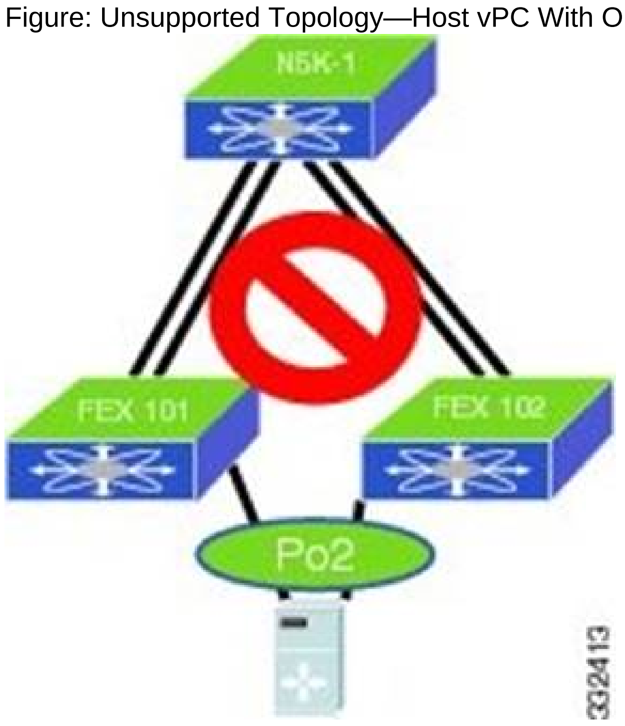
Explanation: To understand this feature, please refer to the link given below. Reference:
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/guide_c07-690079.html#wp9000065

NEW QUESTION 214
Which topology is not supported when using vPC?

A. a single-homed server to a single FEX that is connected to two Cisco Nexus 5500 Series Switches
B. a dual-homed server to two FEXs, each connected to two Cisco Nexus 5500 Series Switches
C. a dual-homed server to two FEXs that are connected to one Cisco Nexus 5500 Series Switch
D. a dual-homed server to a single FEX that is connected to two Cisco Nexus 5500 Series Switches

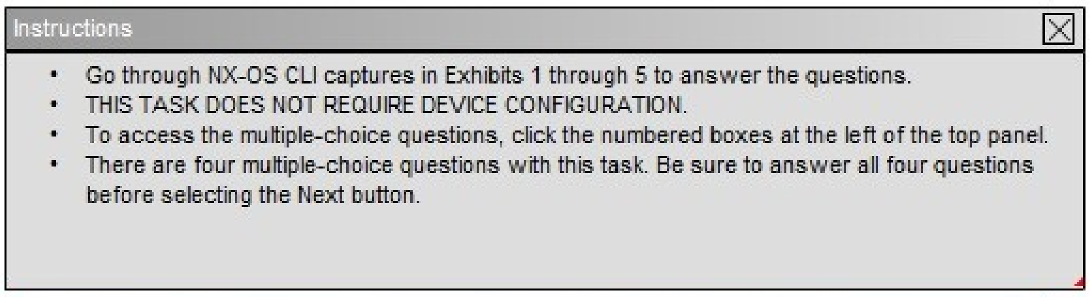
Answer: C

Explanation: The figure shows unsupported topology where a vPC is between hosts and two FEXs that are connected to one Cisco Nexus 5500 Series device. This topology does not provide a good high availability solution because the server loses the connectivity to the network when the Cisco Nexus 5000 Series device fails.
Figure: Unsupported Topology—Host vPC With One Cisco Nexus 5000 Series Device



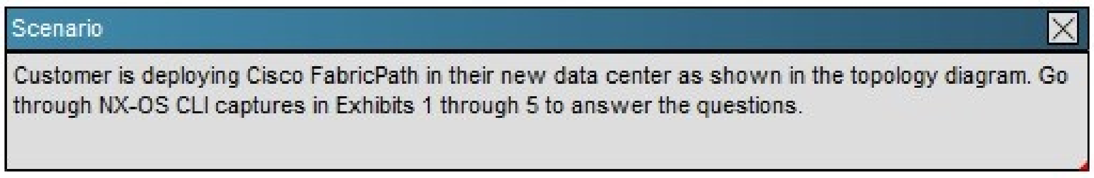
If you need to connect a multi-homing server to a pair of FEXs when there is only one Cisco Nexus 5000 Series device, you have the option to run active or standby NIC teaming from the server. Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1 /n5k_enhanced_vpc.html

NEW QUESTION 215
FabricPath switch-id is 25 and load-balance is configured for L3/L4 and rotate amount is 14 byte. What information is true about FabricPath switch-id?



Instructions

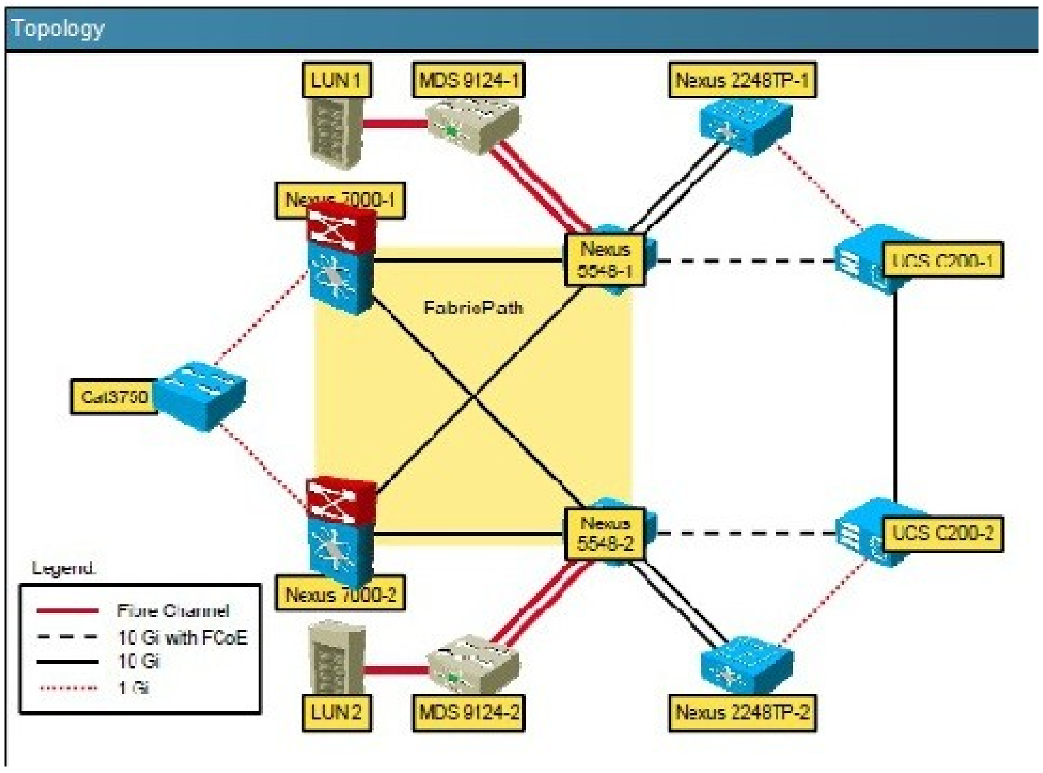
- Go through NX-OS CLI captures in Exhibits 1 through 5 to answer the questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- To access the multiple-choice questions, click the numbered boxes at the left of the top panel.
- There are four multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.



Scenario

Customer is deploying Cisco FabricPath in their new data center as shown in the topology diagram. Go through NX-OS CLI captures in Exhibits 1 through 5 to answer the questions.

Topology



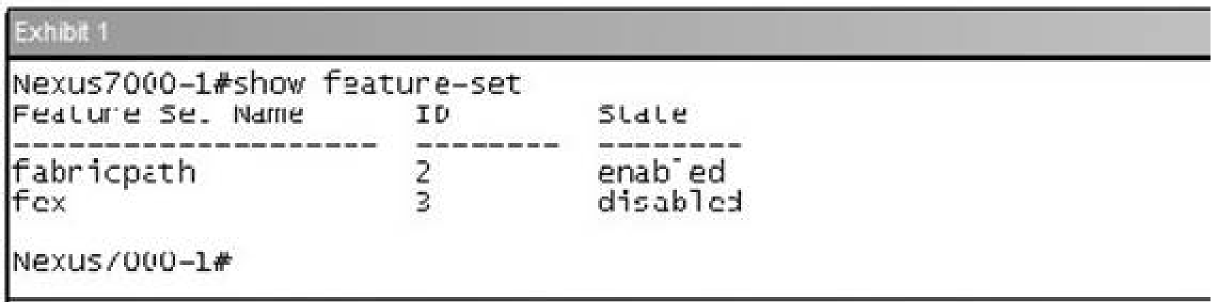


Exhibit 1

```
Nexus7000-1#show feature-set
Feature Set Name         ID         State
--------------------     --------   --------
fabricpath               2          enabled
fex                      3          disabled

Nexus7000-1#
```

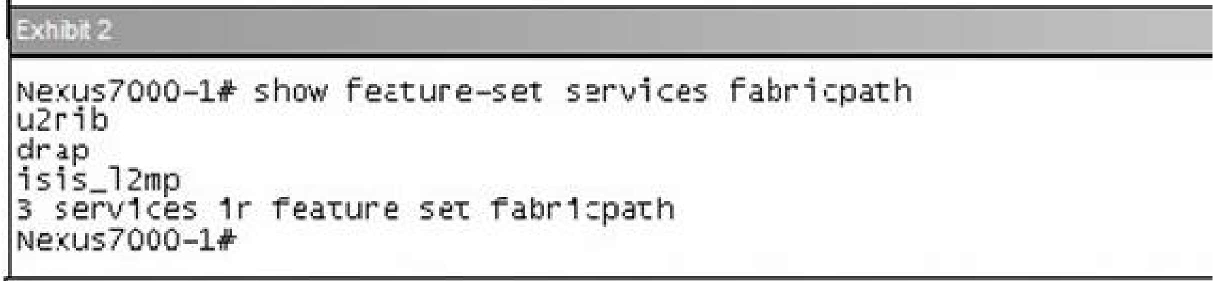


Exhibit 2

```
Nexus7000-1# show feature-set services fabricpath
u2rib
drap
isis_l2mp
3 services in feature set fabricpath
Nexus7000-1#
```

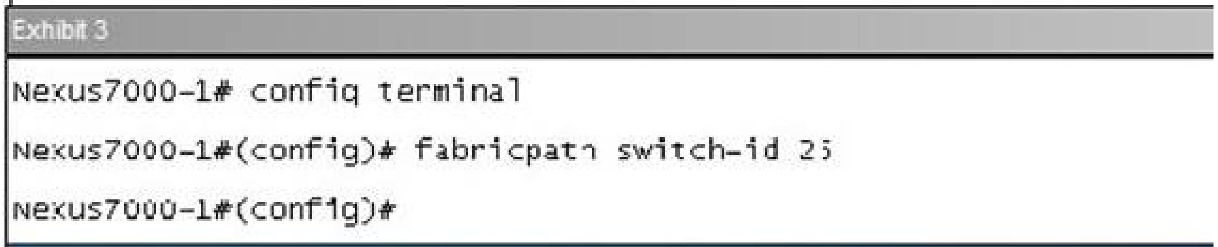


Exhibit 3

```
Nexus7000-1# config terminal

Nexus7000-1#(config)# fabricpath switch-id 25

Nexus7000-1#(config)#
```

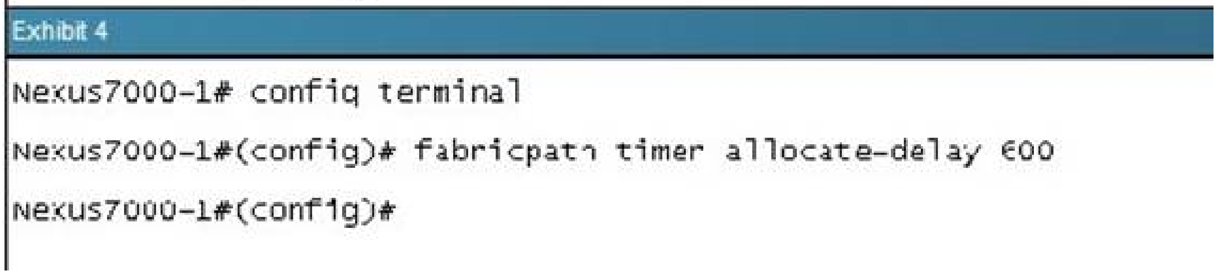


Exhibit 4

```
Nexus7000-1# config terminal

Nexus7000-1#(config)# fabricpath timer allocate-delay 600

Nexus7000-1#(config)#
```

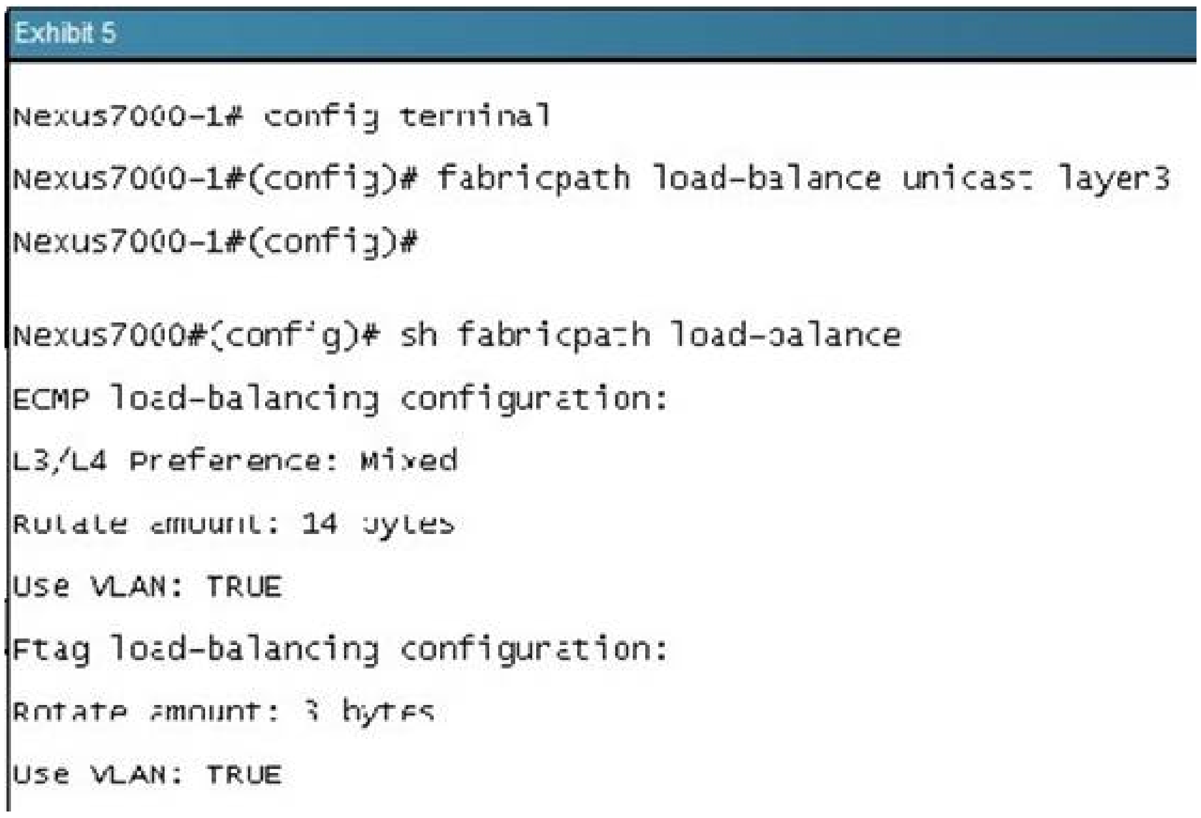


Exhibit 5

```
Nexus7000-1# config terminal
Nexus7000-1#(config)# fabricpath load-balance unicast layer3
Nexus7000-1#(config)#

Nexus7000#(config)# sh fabricpath load-balance
ECMP load-balancing configuration:
L3/L4 Preference: Mixed
Rotate amount: 14 bytes
Use VLAN: TRUE
Ftag load-balancing configuration:
Rotate amount: 3 bytes
Use VLAN: TRUE
```

A. FabricPath topology requires manual configuration of switch-id which has a range from 1 to 4095
B. Every FabricPath must have a manually configured switch-id for it to form a FabricPath topology
C. FabricPath topology requires manual configuration of switch-id which has a range from 1 to 4099
D. You do not have to manually assign a switch ID unless you are running a virtual port channel plus (vPC+) because the system assigns a switch ID for you when you enable FabricPath

Answer: D

Explanation: fabricpath switch-id (vPC)
To configure a virtual port channel plus (vPC+) switch ID, use the fabricpath switch-id command. To remove the FabricPath switch from a vPC domain, use the no form of this command.
fabricpath switch-id switch-id
no fabricpath switch-id [switch-id] Usage Guidelines
You do not have to manually assign a switch ID (unless you are running a vPC+); the system assigns a switch ID for you when you enable FabricPath.
Note You must assign the same vPC+ switch ID to each of the two vPC+ peer devices before they can form an adjacency.
This command requires an Enhanced Layer 2 license. Examples
This example shows how to configure a vPC+ switch ID on a FabricPath-enabled device: switch# configure terminal
switch(config)# vpc domain 1
switch(config-vpc-domain)# fabricpath switch-id 1
Configuring fabricpath switch id will flap vPCs. Continue (yes/no)? [no]

NEW QUESTION 218
Which statement about scalability in Cisco OTV is true?

A. The control plane avoids flooding by exchanging MAC reachability.
B. IP-based functionality provides Layer 3 extension over any transport.
C. Any encapsulation overhead is avoided by using IS-IS.
D. Unknown unicasts are handled by the authoritative edge devic

Answer: A

Explanation: Cisco calls the underlying concept of OTV traffic forwarding "MAC routing", since it behaves as if you are routing Ethernet frames over the DCI transport. OTV uses a control plane protocol to proactively propagate MAC address reachability before traffic is allowed to pass, which eliminates dependency on flooding mechanism to either learn MAC addresses or forward unknown unicasts. Reference:
http://www.computerworld.com/article/2515468/data-center/layer-2-data-center-interconnectoptions. html

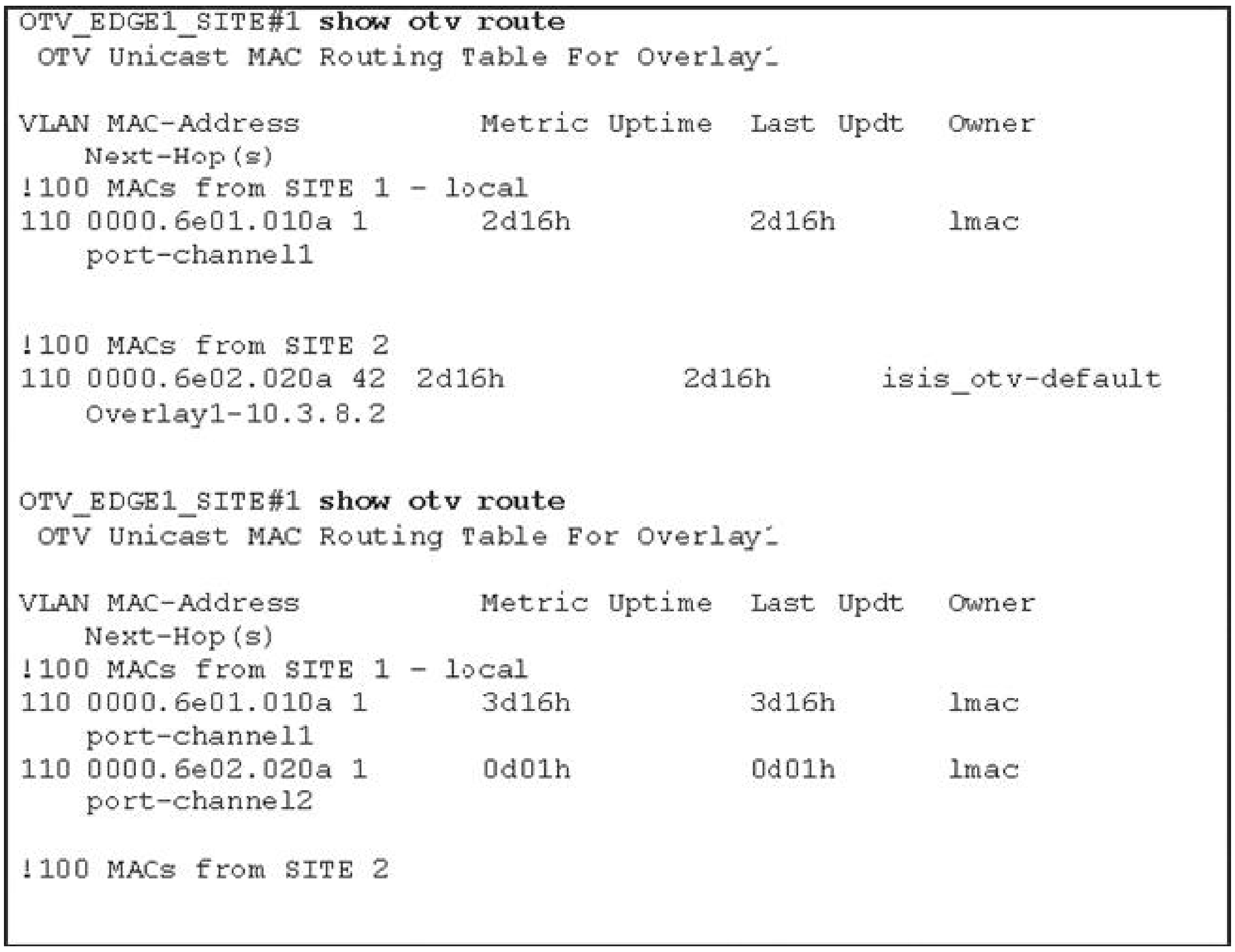
NEW QUESTION 222
Which policy-map action performs congestion avoidance?

A. priority
B. bandwidth
C. queue-limit
D. random-detect

Answer: D

Explanation: Congestion avoidance techniques monitor network traffic loads in an effort to anticipate and avoid congestion at common network bottlenecks. Congestion avoidance is achieved through packet dropping. Among the more commonly used congestion avoidance mechanisms is Random Early Detection (RED), which is optimum for high-speed transit networks. Cisco IOS QoS includes an implementation of RED that, when configured, controls when the router drops packets. If you do not configure Weighted Random Early Detection (WRED), the router uses the cruder default packet drop mechanism called tail drop.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfconav.html

NEW QUESTION 225
Refer to the exhibit.



```
OTV_EDGE1_SITE#1 show otv route
 OTV Unicast MAC Routing Table For Overlay1

VLAN MAC-Address           Metric Uptime   Last Updt   Owner
    Next-Hop(s)
!100 MACs from SITE 1 - local
110 0000.6e01.010a 1       2d16h           2d16h       lmac
    port-channel1


!100 MACs from SITE 2
110 0000.6e02.020a 42  2d16h           2d16h       isis_otv-default
    Overlay1-10.3.8.2


OTV_EDGE1_SITE#1 show otv route
 OTV Unicast MAC Routing Table For Overlay1

VLAN MAC-Address           Metric Uptime   Last Updt   Owner
    Next-Hop(s)
!100 MACs from SITE 1 - local
110 0000.6e01.010a 1       3d16h           3d16h       lmac
    port-channel1
110 0000.6e02.020a 1       0d01h           0d01h       lmac
    port-channel2

!100 MACs from SITE 2
```

Which statement based on these two outputs that were collected 24 hours apart is true?

A. The Site 2 OTV edge device has gone down.
B. The MAC address cannot be discovered on two separate port channel interfaces.
C. The MAC address that ends in 020a moved to the local site 23 hours ago.
D. The Overlay1 IP address should be a multicast IP addres

Answer: C

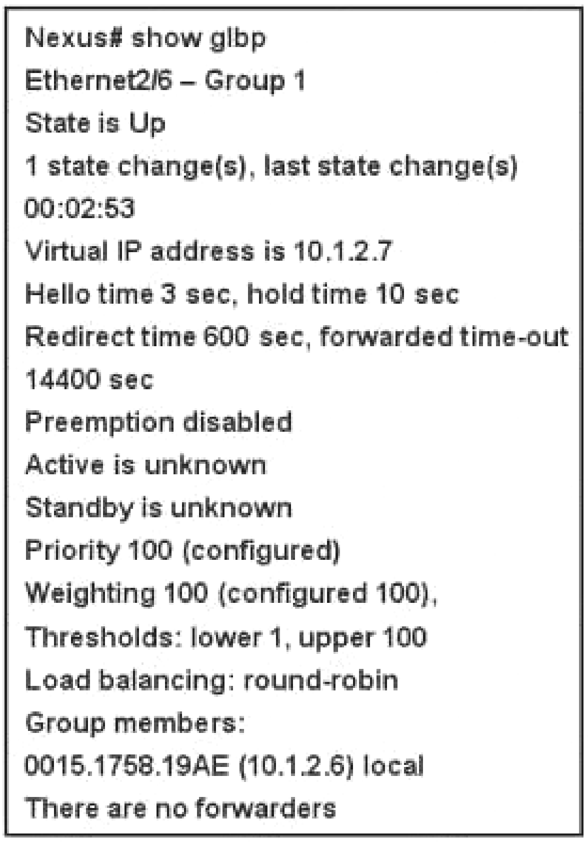
NEW QUESTION 228
What mode is required on a Cisco Nexus 7000 32-port 10-GB module port group to allow equal access to the 10-GB port controller?

A. dedicated
B. assigned
C. shared
D. community

Answer: C

Explanation: You can share 10 Gb of bandwidth among a group of ports (four ports) on a 32-port 10-Gigabit Ethernet module. To share the bandwidth, you must bring the dedicated port administratively down, specify the ports that are to share the bandwidth, change the rate mode to shared, and then bring the ports administratively up.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/ interfaces/configuration/guide/if_cli/if_basic.html#70242

NEW QUESTION 230
Refer to the exhibit.



```
Nexus# show glbp
Ethernet2/6 – Group 1
State is Up
1 state change(s), last state change(s)
00:02:53
Virtual IP address is 10.1.2.7
Hello time 3 sec, hold time 10 sec
Redirect time 600 sec, forwarded time-out
14400 sec
Preemption disabled
Active is unknown
Standby is unknown
Priority 100 (configured)
Weighting 100 (configured 100),
Thresholds: lower 1, upper 100
Load balancing: round-robin
Group members:
0015.1758.19AE (10.1.2.6) local
There are no forwarders
```

This multilayer Cisco Nexus switch had been the active virtual gateway for Group 1 before it became temporarily unavailable. What will happen to GLBP Group 1 when this device becomes available again?

A. The currently active router remains active.
B. It depends on the priority value that is configured active on the router.
C. The Cisco Nexus switch becomes the active virtual gateway after 600 seconds.
D. It depends on the weighting values that are configured active on the router.

Answer: A

Explanation: GLBP prioritizes gateways to elect an active virtual gateway (AVG). If multiple gateways have the same priority, the gateway with the highest real IP address becomes the AVG. The AVG assigns a virtual MAC address to each member of the GLBP group. Each member is the active virtual forwarder (AVF) for its assigned virtual MAC address, forwarding packets sent to its assigned virtual MAC address.
The AVG also answers Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved when the AVG replies to the ARP requests with different virtual MAC addresses. Note: Packets received on a routed port destined for the GLBP virtual IP address terminate on the local router, regardless of whether that router is the active GLBP router or a redundant GLBP router. This termination includes ping and Telnet traffic. Packets received on a Layer 2 (VLAN) interface destined for the GLBP virtual IP address terminate on the active router.

NEW QUESTION 233
What must be enabled on the interface of a multicast-enabled device to support the Source Specific Multicast feature?

A. IGMP version 3
B. IGMP version 2
C. IGMP version 1
D. PIM

Answer: A

Explanation: IGMP is the Internet Engineering Task Force (IETF) standards track protocol used for hosts to signal multicast group membership to routers. Version 3 of this protocol supports source filtering, which is required for SSM. To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself. IGMP v3lite and URD are two Ciscodeveloped transition solutions that enable the immediate development and deployment of SSM
services, without the need to wait for the availability of full IGMPv3 support in host operating systems and SSM receiver applications. IGMP v3lite is a solution for application developers that allows immediate development of SSM receiver applications switching to IGMPv3 as soon as it becomes available. URD is a solution for content providers and content aggregators that enables them to deploy receiver applications that are not yet SSM enabled (through support for IGMPv3). IGMPv3, IGMP v3lite, and URD interoperate with each other, so that both IGMP v3lite and URD can easily be used as transitional solutions toward full IGMPv3 support in hosts.
Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfssm.html

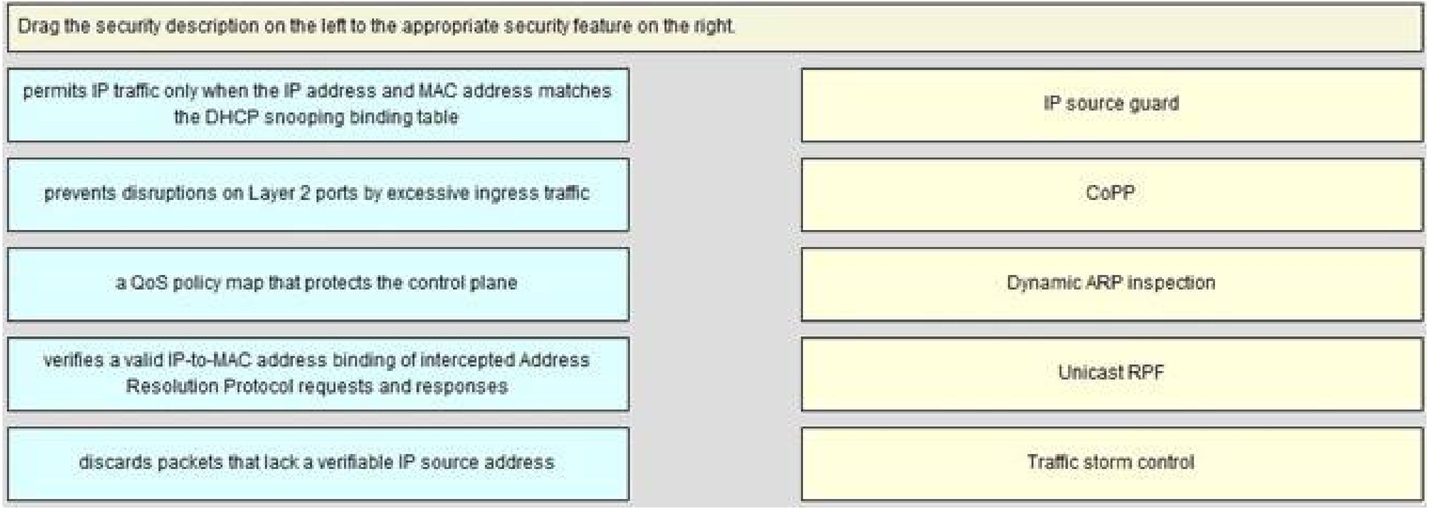
NEW QUESTION 235
Which two statements about implementing Cisco NPV and NPIV on a Cisco Nexus 5000 Series switch are true? (Choose two.)

A. STP must run inside the FP network.
B. All VLANs must be in the same mode, CE, or FP.
C. FP port can join the private and nonprivate VLANs.
D. Only F and M series modules can run FabricPath.
E. These require an enhanced Layer 2 license to ru

Answer: BE

Explanation: With the Nexus 5x00 switch, FCoE functionality is a licensed feature. After the license is installed, FCoE configuration can be completed.
Reference: http://www.ciscopress.com/articles/article.asp?p=2030048&seqNum=4

NEW QUESTION 238
DRAG DROP
Drag the security description on the left to the appropriate security feature on the right.



Drag the security description on the left to the appropriate security feature on the right.

permits IP traffic only when the IP address and MAC address matches the DHCP snooping binding table	IP source guard
prevents disruptions on Layer 2 ports by excessive ingress traffic	CoPP
a QoS policy map that protects the control plane	Dynamic ARP inspection
verifies a valid IP-to-MAC address binding of intercepted Address Resolution Protocol requests and responses	Unicast RPF
discards packets that lack a verifiable IP source address	Traffic storm control

Answer:

Explanation: IP Source guard: IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.
Initially, all IP traffic on the protected port is blocked except for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied. This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. IP Source Guard is a port-based feature that automatically creates an implicit port access control list (PACL).
CoPP: Control Plane Policing (CoPP) introduced the concept of early rate-limiting protocol specific traffic destined to the processor by applying QoS policies to the aggregate control-plane interface. Control Plane Protection extends this control plane functionality by providing three additional control-plane subinterfaces under the top-level (aggregate) control-plane interface. Each subinterface receives and processes a specific type of control-plane traffic.
Dynamic Arp Inspection: 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

Unicast RPF: The Unicast RPF feature reduces problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of Denial-of-Service (DoS) attacks, including Smurf and Tribal Flood Network (TFN) attacks, can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. Unicast RPF deflects attacks by forwarding only the packets that have source addresses that are valid
and consistent with the IP routing table.
When you enable Unicast RPF on an interface, the device examines all ingress packets received on that interface to ensure that the source address and source interface appear in the routing table and match the interface on which the packet was received. This examination of source addresses relies on the Forwarding Information Base (FIB).
Traffic Storm Control: A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. You can use the traffic storm control feature to prevent disruptions on Layer 2 ports by a broadcast, multicast, or unicast traffic storm on physical interfaces. Traffic storm control (also called traffic suppression) allows you to monitor the levels of the incoming broadcast, multicast, and unicast traffic over a 1-second interval. During this interval, the traffic level, which is a percentage of the total available bandwidth of the port, is compared with the traffic storm control level that you configured. When the ingress traffic reaches the traffic storm control level that is configured on the port, traffic storm control drops the traffic until the interval ends.

NEW QUESTION 241
Which three VDC resources can be constrained with a resource template? (Choose three.)

A. ACLs
B. NAT entries
C. IPv4 routes
D. IPv6 routes
E. SPAN sessions
F. RBAC users

Answer: CDE

Explanation: VDC resource templates set the minimum and maximum limits for shared physical device resources when you create the VDC. The Cisco NX-OS software reserves the minimum limit for the resource to the VDC. Any resources allocated to the VDC beyond the minimum are based on the maximum limit and availability on the device.
You can explicitly specify a VDC resource template, or you can use the default VDC template provided by the Cisco NX-OS software. VDC templates set limits on the following resources:
IPv4 multicast route memory IPv6 multicast route memory IPv4 unicast route memory IPv6 unicast route memory Port channels
Switch Port Analyzer (SPAN) sessions VLANs
Virtual routing and forwarding instances (VRFs) Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nxos/ virtual_device_context/configuration/guide/b-7k-Cisco-Nexus-7000-Series-NX-OS-Virtual-Device- Context-Configuration-Guide/vdc-res-template.html

NEW QUESTION 243
Which command sequence correctly enables Adapter FEX on Nexus 5000 Series Switches?

A. switch(config)# install feature-set virtualization switch(config)# feature-set virtualization
B. switch(config)# install feature-set adapter-fex switch(config)# feature-set adapter-fex
C. switch(config)# install feature-set adapter-fex switch(config)# feature-set virtualization
D. switch(config)# install feature-set virtualization switch(config)# feature-set adapter-fex

Answer: A

Explanation: install feature-set virtualization : installs the cisco virtual machine feature set on the switch. feature-set virtualization : enables the cisco virtual machine feature on the switch. Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/adapterfex/
513_n1_1/b_Configuring_Cisco_Nexus_5000_Series_AdapterQuestions
& Answers PDF P-100 FEX_rel_5_1_3_N1/b_Configuring_Cisco_Nexus_5000_Series_Adapter- FEX_rel_5_1_3_N1_chapter_010.pdf

NEW QUESTION 247
Which three Cisco UCS C-Series CNAs support Adapter FEX? (Choose three.)

A. Qlogic QLE8152
B. Broadcom BCM57712
C. Cisco UCS P81E
D. Cisco UCS VIC 1220
E. Emulex OCe10102-FX-C
F. Intel X520

Answer: BCD

Explanation: Reference:
http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c-series_integration/ucsm2- 1/b_UCSM2-1_C-Integration/b_UCSM2-1_CIntegration_
chapter_011.html#reference_D644111FC68046F0BEA49756A0834664

NEW QUESTION 250
Which two Cisco Nexus platforms support Adapter FEX? (Choose two.)

A. Cisco Nexus 7000 Series Switches
B. Cisco Nexus 5000 Series Switches
C. Cisco Nexus 5500 Series Switches
D. Cisco Nexus 4000 Series Switches
E. Cisco Nexus 2000 Series Fabric Extenders

Answer: CE

Explanation: At the access layer, the Adapter-FEX requires a FEX-enabled adapter on a server that connects to a parent device that supports virtualization of interfaces. The Adapter-FEX is supported on the following platforms:
• The Cisco Unified Computing System (UCS) platform supports Adapter-FEX between UCS servers and the UCS Fabric Interconnect.
• The Adapter-FEX is supported on the Cisco Nexus 5500 Series platform and on the Cisco Nexus 2200 Fabric Extender that is connected to a Cisco Nexus 5500 Series parent device. This implementation works on a variety of FEX-capable adapters, including the Cisco UCS P81E virtual interface card (VIC) adapter for the UCS C-Series platform and third party adapters such as the Broadcom BCM57712 Convergence Network Interface Card, that implement the virtual network tag (VNTag) technology.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/adapter_fex
/513_n1_1/ops_adapter_fex/ops_using_adapter_fex.html

NEW QUESTION 252
When connecting Cisco Nexus 5000 Series Switches to the VMware vCenter Server, which item must be configured before installing the extension keys?

A. configure vPC
B. configure DirectPath I/O support in vCenter
C. configure PTS on the VSM
D. configure dynamic vNICs

Answer: A

NEW QUESTION 255
Which three selections represent implementations of Cisco VN-Link technology? (Choose three.)

A. Cisco Nexus 1000V
B. Cisco Nexus 2000 FEX
C. Cisco VM-FEX
D. VMware PTS
E. vMotion

Answer: ACD

Explanation: The VM is powered on and resides on the ESX Host 1 with all the information stored on the shared storage.
The VM was connected to the PODy (where y is the number of your POD) PTS VDS by associating it to port group VLAN61 that was created on the Cisco Nexus 5548 device. The VM has been connected to the vPC system automatically using a VN-Link in the hardware in PTS mode or in VM-FEX mode.
The VEM bits are used in PTS mode to connect the VM VNIC to the VMNIC interface.
In this case, the VMNIC interface is not a real VMNIC but a dynamic VNIC that is presented as an interface to the ESX OS. The dynamic VNIC is enabled when the Cisco UCS VIC creates and configures the VNIC parameters inherited from port group VLAN61.

Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1 /n5k_ops_vmfex.html

NEW QUESTION 256
Which two items are required components of VN-Link in software? (Choose two.)

A. VDC
B. VEM
C. vPC
D. VSM
E. VRRP

Answer: BD

Explanation: The Cisco Nexus 1000V Series consists of two main types of components that can virtually emulate a 66-slot modular Ethernet switch with redundant supervisor functions:
• Virtual Ethernet module (VEM)-data plane: This lightweight software component runs inside the hypervisor. It enables advanced networking and security features, performs switching between directly attached virtual machines, provides uplink capabilities to the rest of the network, and effectively replaces the vSwitch. Each hypervisor is embedded with one VEM.
• Virtual supervisor module (VSM)-control plane: This standalone, external, physical or virtual appliance is responsible for the configuration, management, monitoring, and diagnostics of the
overall Cisco Nexus 1000V Series system (that is, the combination of the VSM itself and all the VEMs it controls) as well as the integration with VMware vCenter. A single VSM can manage up to 64 VEMs. VSMs can be deployed in an active-standby model, helping ensure high availability.
Reference:
http://www.cisco.com/c/en/us/solutions/collateral/switches/nexus-1000v-switch-vmwarevsphere/ white_paper_c11-525307.html

NEW QUESTION 260
What configuration is required when implementing FCoE?

A. disable LAN traffic on the interface
B. configure PortFast on the access port
C. permit all VLANs on the interface
D. permit all VSANs on the interface

Answer: A

Explanation: DCBX allows the switch to send a LAN Logical Link Status (LLS) message to a directly-connected CNA. Enter the shutdown lan command to send an LLS-Down message to the CN
A. This command causes
all VLANs on the interface that are not enabled for FCoE to be brought down. If a VLAN on the interface is enabled for FCoE, it continues to carry SAN traffic without any interruption. Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/fcoe/b_Cisco_Nexus_5 000_Series_NXOS_ Fibre_Channel_over_Ethernet_Configuration_Guide_/Cisco_Nexus_5000_Series_NXOS_ Fibre_Channel_over_Ethernet_Configuration_Guide chapter3.html

NEW QUESTION 262
Which protocol is responsible for the discovery of FCoE capabilities on a remote switch?

A. DCE
B. DCBx
C. CDP
D. LLDP

Answer: B

Explanation: Data Center Bridging Capabilities Exchange Protocol (DCBX): a discovery and capability exchange protocol that is used for conveying capabilities and configuration of the above features between neighbors to ensure consistent configuration across the network. This protocol leverages functionality provided by IEEE 802.1AB (LLDP). It is actually included in the 802.1az standard. Reference:
http://en.wikipedia.org/wiki/Data_center_bridging

NEW QUESTION 266
How does an FCoE end node acquire its FCoE MAC address?

A. server-provided MAC address
B. Fibre Channel name server
C. fabric-provided MAC address
D. FIP proxy

Answer: C

Explanation: The VN_Port is assigned a fabric-provided Mac address (FPMA) that is built by concatenating a 24-bit FCoE MAC address prefix (FC-MAP), ranging from 0x0E-FC-00 to 0x0E-FC-FF, to the 24-bit FCID. Being able to build a unique MAC address for the VN_Port directly from its FCID saves the switch from having to maintain a table that associates FCID and MAC addresses. Reference:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/UF_FCoE_final.html

NEW QUESTION 267
Which item represents the process that allows FCoE multihop using T11 standard FC-BB-5?

A. distributed FCF
B. FIP proxy
C. N Port proxy
D. FIP snooping

Answer: D

Explanation: FIP snooping is used in multi-hop FCoE environments. FIP snooping is a frame inspection method that can be used by FIP snooping capable DCB devices to monitor FIP frames and apply policies based on the information in those frames. This allows for:
Enhanced FCoE security (Prevents FCoE MAC spoofing.) Creates FC point-to-point links within the Ethernet LAN
Allows auto-configuration of ACLs based on name server information read in the FIP frames Reference:
http://www.definethecloud.net/fcoe-initialization-protocol-fip-deep-dive/

NEW QUESTION 272
Between which two types of ports does FIP establish Fibre Channel virtual links? (Choose two.)

A. VE Ports and VE Ports
B. N Ports and F Ports
C. VN Ports and VF Ports
D. VP Ports and VE Ports
E. VE Ports and VF Ports
F. E Ports and E Ports

Answer: AC

Explanation: FIP aims to establish virtual FC links between VN_Ports and VF_Ports (ENode to FCF), as well as between pairs of VE_Ports (FCF to FCF), since these are the only legal combinations supported by native Fibre Channel fabrics. Standards-compliant implementations are not required to support both forms of virtual FC links, and Cisco has decided to focus initially on implementing FIP only between ENodes and FCFs. FCF-to-FCF connectivity is considered a strategic direction for end-to-end FCoE deployments, but the short-term urgency is for FCoE adoption between CNAs and the Fibre Channel fabric perimeter, where unified fabric can offer the greatest capital expenditure (CapEx) savings today.
Reference:
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-7000-seriesswitches/ white_paper_c11-560403.html

NEW QUESTION 277
Which two reasons explain why a server on VLAN 10 is unable to join a multicast stream that originates on VLAN 20? (Choose two.)

A. IGMP snooping and mrouter are not enabled on VLAN 10.
B. VLAN 20 has no IGMP snooping querier defined and VLAN 10 has no mrouter.
C. The mrouter on VLAN 20 does not see the PIM join.
D. The mrouter must be on VLAN 10 and VLAN 20.

Answer: AC

Explanation: IGMP snooping is a mechanism to constrain multicast traffic to only the ports that have receivers attached. The mechanism adds efficiency because it enables a Layer 2 switch to selectively send out multicast packets on only the ports that need them. Without IGMP snooping, the switch floods the packets on every port. The switch "listens" for the exchange of IGMP messages by the router and the end hosts. In this way, the switch builds an IGMP snooping table that has a list of all the ports that have requested a particular multicast group.
The mrouter port is simply the port from the switch point of view that connects to a multicast router. The presence of at least one mrouter port is absolutely essential for the IGMP snooping operation to work across switches.
All Catalyst platforms have the ability to dynamically learn about the mrouter port. The switches passively listen to either the Protocol Independent Multicast (PIM) hellos or the IGMP query messages that a multicast router sends out periodically.
Reference:
http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/68131-catmulticast- prob.html

NEW QUESTION 278
Which two statements about SAN zoning on Cisco Nexus switches are true? (Choose two.)

A. Unlike configured zones, default zone information is not distributed to the other switches in the fabric.
B. Traffic can either be permitted or denied among members of the default zon
C. This information is not distributed to all switche
D. It must be configured in each switch.
E. The settings for default zone configurations cannot be changed.
F. To activate a zone set, you must copy the running configuration to the startup configuration after the zone set is configured.
G. Soft zoning restrictions will not prevent a source device from accessing a device outside its zone, if the source knows the Fibre Channel ID of the destination.
H. Hard zoning is enforced by the hardware on each FLOGI sent by an N Por

Answer: BE

Explanation: Each member of a fabric (in effect a device attached to an Nx port) can belong to any zone. If a member is not part of any active zone, it is considered to be part of the default zone. Therefore, if no zone set is active in the fabric, all devices are considered to be in the default zone. Even though a member can belong to multiple zones, a member that is part of the default zone cannot be part of any other zone. The switch determines whether a port is a member of the default zone when the attached port comes up. Unlike configured zones, default zone information is not distributed to the other switches in the fabric Traffic can either be permitted or denied among members of the default zone. This information is not distributed to all switches; it must be configured in each switch. Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_2/configuration/guides

/fabric/DCNM-SAN/fm_fabric/zone.html

NEW QUESTION 282
Which two statements about SAN zoning on Cisco Nexus switches are true? (Choose two.)

A. Zoning is enforced by examining the destination ID field.
B. Devices can only belong to one zone.
C. Only one zone set can be activated at any time.
D. A zone can only be a member one zone set.
E. Zoning must be administered from the primary SAN switch in the fabric.
F. Zone configuration changes are nondisruptiv

Answer: CF

Explanation: A zone set can be activated or deactivated as a single entity across all switches in the fabric. Only one zone set can be activated at any time. If zoning is not activated, all devices are members of the default zone. If zoning is activated, any device that is not in an active zone (a zone that is part of an active zone set) is a member of the default zone. Zoning can be administered from any switch in the fabric. When you activate a zone (from any switch), all switches in the fabric receive the active zone set. Additionally, full zone sets are distributed to all switches in the fabric, if this feature is enabled in the source switch.
Reference: http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/sanos/ quick/guide/qcg_zones.html

NEW QUESTION 286
Which three options are capabilities of the Cisco Nexus 7000 Series Switch? (Choose three.)

A. All interface and supervisor modules are accessible from the front.
B. All interface and supervisor modules are accessible from the rear.
C. single power supply only
D. multiple power supply option for redundancy
E. up to 180.7 Tbps forwarding capacity with Fabric-2 modules with 10-slot switches
F. up to 18.7 Tbps forwarding capacity with Fabric-2 modules with 18-slot switches

Answer: ADF

NEW QUESTION 291
Which three options are capabilities of the Cisco Nexus 7000 Series Supervisor Module? (Choose three.)

A. hardware forwarding on the supervisor module
B. fully decoupled control plane and data plane with no forwarding on the supervisor module
C. Sup2 requires Cisco NX-OS 5.1 or later.
D. Sup2 requires Cisco NX-OS 6.1 or later.
E. Sup2E supports 8+1 VDC with the N7K-VDC1K9 license per chassis.
F. Sup2 supports 8+1 VDCs with the N7K-VDC1K9 license per chassi

Answer: BDE

NEW QUESTION 295
Which feature must be enabled for Cisco TrustSec FC Link Encryption to work on a Cisco MDS 9000 Series Switch?

A. crypto IKE
B. port security
C. LDAP
D. FC-SP

Answer: D

NEW QUESTION 296
Which command ensures that a learned MAC address is stored within NVRAM?

A. switchport port-security mac-address address [vlan vlan-ID]
B. switchport port-security
C. switchport port-security mac-address sticky
D. feature port-security

Answer: C

NEW QUESTION 301
Which three parameters can be set when configuring a Cisco MDS 9000 Series Switch to use a TACACS+ server? (Choose three.)

A. group-size
B. deadtime
C. timeout
D. keep-alive
E. retransmit

Answer: BCE

NEW QUESTION 305
Which situation must you consider when you add a remote RADIUS server to a Cisco Nexus device?

A. If RADIUS authentication fails, the device falls back to local authentication automatically.
B. If RADIUS authentication fails, the user is denied access with no further authentication checks.
C. If the RADIUS server is unreachable, users are unable to log in.
D. If the RADIUS server is unreachable, all users are given access with the default rol

Answer: B

NEW QUESTION 310
Which three attributes encompass a local user account on a Cisco NX-OS device? (Choose three.)

A. expiration date
B. cisco-avpair
C. password
D. AAA server address
E. user roles
F. bind user DN
G. user privileges

Answer: ACE

NEW QUESTION 312
Which parameter is configurable when setting up logging on the Connectivity Management Processor?

A. the number of CMP messages to save in a single log file
B. the number of times the log can roll over
C. the directory to save the log file to
D. the severity threshold of the messages to log

Answer: D

NEW QUESTION 314
Which statement describes what happens if a new EPLD version is released with a new Cisco NX-OS version for a Cisco Nexus switch, but these EPLDs are not upgraded at the same time that NX-OS is upgraded?

A. Any new hardware or software feature that depends on the updated EPLD image is disabled until upgraded.
B. Modules that use an updated EPLD image remain offline until the EPLD is upgraded.
C. The EPLD image version mismatch is detected by the supervisor, which automatically initiates an upgrade.
D. The Cisco NX-OS upgrade fails as a result of the mismatch between EPLDs and NX-OS version

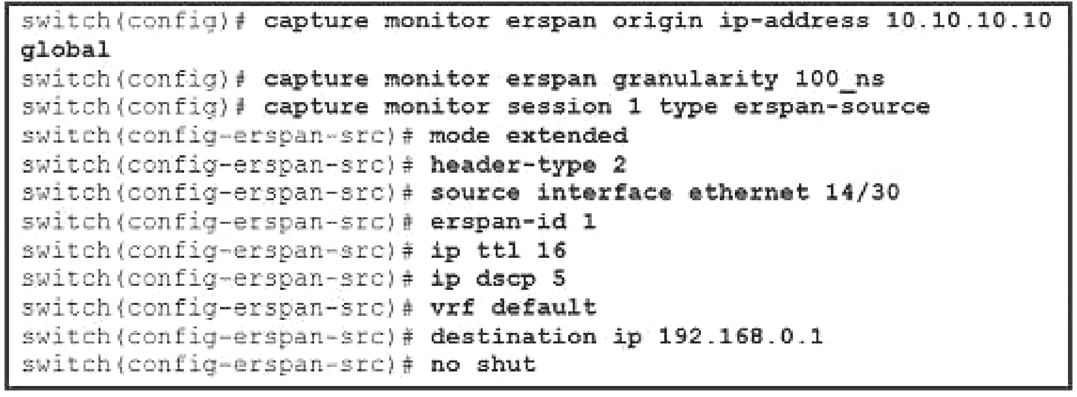
Answer: A

NEW QUESTION 317
Which two options are limitations of NetFlow Version 5? (Choose two.)

A. no support for IPv6, Layer 2, or MPLS fields
B. fixed field specifications
C. excessive network utilization
D. analyzes all packets on the interface

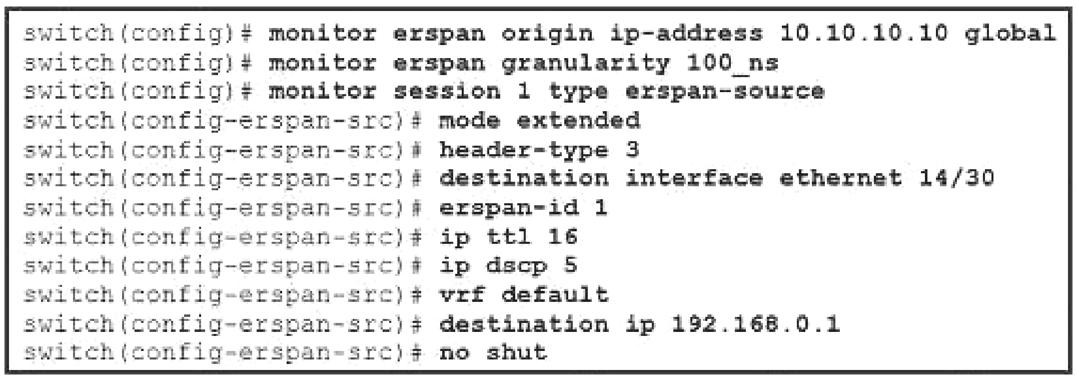
Answer: AB

NEW QUESTION 320
Which option shows how to configure an ERSPAN Type III source session in Cisco NX-OS 6.2?
A)



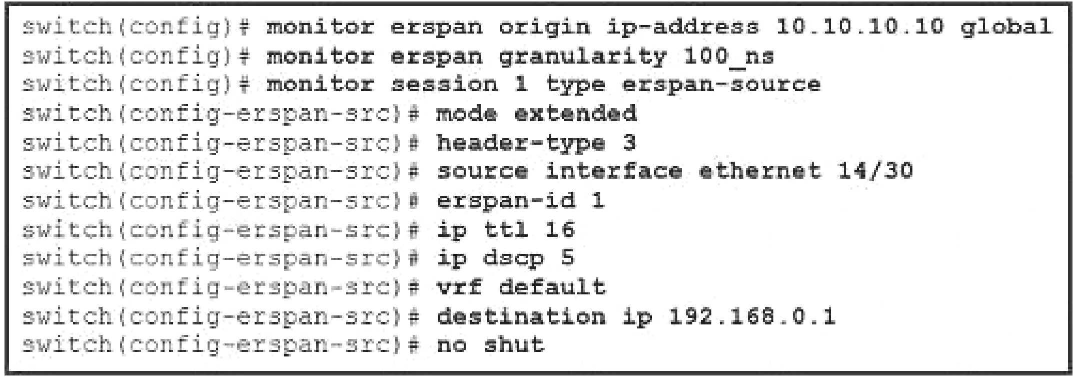
```
switch(config)# capture monitor erspan origin ip-address 10.10.10.10
global
switch(config)# capture monitor erspan granularity 100_ns
switch(config)# capture monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 2
switch(config-erspan-src)# source interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

B)



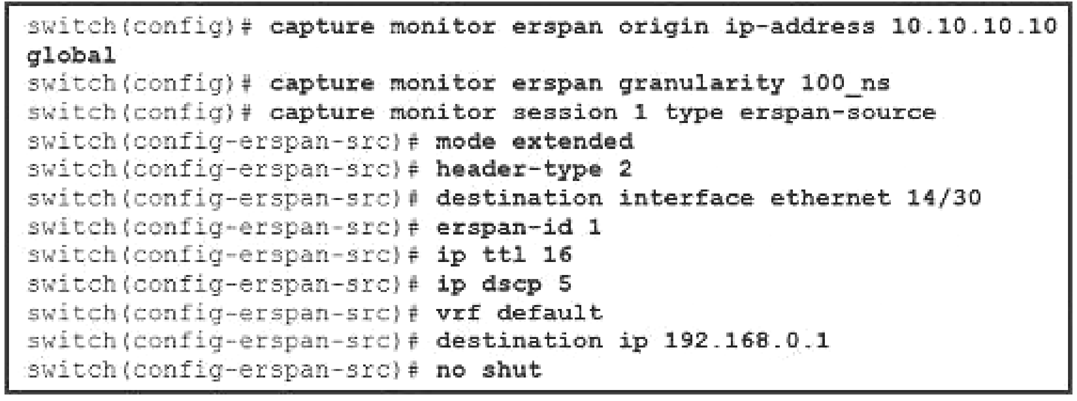
```
switch(config)# monitor erspan origin ip-address 10.10.10.10 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# destination interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

C)



```
switch(config)# monitor erspan origin ip-address 10.10.10.10 global
switch(config)# monitor erspan granularity 100_ns
switch(config)# monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 3
switch(config-erspan-src)# source interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

D)



```
switch(config)# capture monitor erspan origin ip-address 10.10.10.10
global
switch(config)# capture monitor erspan granularity 100_ns
switch(config)# capture monitor session 1 type erspan-source
switch(config-erspan-src)# mode extended
switch(config-erspan-src)# header-type 2
switch(config-erspan-src)# destination interface ethernet 14/30
switch(config-erspan-src)# erspan-id 1
switch(config-erspan-src)# ip ttl 16
switch(config-erspan-src)# ip dscp 5
switch(config-erspan-src)# vrf default
switch(config-erspan-src)# destination ip 192.168.0.1
switch(config-erspan-src)# no shut
```

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

Answer: C

NEW QUESTION 323
Which three options are CallHome predefined destination profiles that are supported on Cisco NXOS? (Choose three.)

A. CiscoTAC-1
B. full-text-destination
C. pager-xml-destination
D. short-text-destination
E. xml-text-destination
F. pager-json-destination

Answer: ABD

NEW QUESTION 327
If you are using NAT in your data center, which load balancing would you be likely to use within your GLBP configuration?

A. none
B. round-robin
C. host dependent
D. weighted

Answer: C

NEW QUESTION 330
Which command specifies a load-balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged?

A. load-balancing host-dependent
B. load-balancing mac-pinning
C. load-balancing round-robin
D. load-balancing weighted

Answer: A

NEW QUESTION 334
Which feature allows routing protocols to remain in the data path during a supervisor failover?

A. Cisco Nonstop Forwarding
B. Cisco Stateful Switchover
C. Cisco Express Forwarding
D. Cisco Route Processor Redundancy

Answer: A

NEW QUESTION 335
Which two functions are enabled when you set up vPC+ at the FabricPath edge? (Choose two.)

A. the ability to attach Cisco Fabric Extenders in FEX active/active mode
B. the ability to stop all Layer 3 egress traffic
C. the ability to attach servers to edge switches with port-channel teaming
D. the ability to attach additional Classic Ethernet switches in vPC+ mode

Answer: AC

NEW QUESTION 339
How does addition of bandwidth between spine and leaf switches in a FabricPath architecture get utilized?

A. Links between the same set of switches are automatically added to a port channel.
B. Adding additional bandwidth is handled dynamically using the 802.1AX protocol.
C. Traffic is load shared automatically across the available paths to the destination.
D. FabricPath uses hardware bonding of physical interfaces to form higher-speed link

Answer: C

NEW QUESTION 343
Which four statements about reserved VLANs in Cisco NX-OS are true? (Choose four.)

A. The range of reserved VLANs cannot be changed.
B. The number of reserved VLANs is 96.
C. A change to the range of reserved VLANs can be performed only in the VDC default.
D. A write-erase procedure restores the default reserved VLAN range.
E. The number of reserved VLANs is 128.
F. A reload is needed for changes to take place.
G. The configuration must be saved for changes to take plac

Answer: CEFG

NEW QUESTION 348
Which two RFCs are supported by Cisco NX-OS devices for OSPFv2? (Choose two.)

A. RFC 2238
B. RFC 1918
C. RFC 1583
D. RFC 2453
E. RFC 2740

Answer: AC

NEW QUESTION 351
Which three options of encryption are supported in PIM hello messages? (Choose three.)

A. cleartext
B. DES-SHA1
C. DES-CBC3-SHA
D. Cisco Type 7
E. RC4-SHA
F. 3DES

Answer: ADF

NEW QUESTION 356
Which command is used to associate EID-to-RLOC for a LISP site?

A. #feature lisp
B. #ipv6 lisp itr
C. #ip lisp database-mapping
D. #ip lisp itr map-resolver

Answer: C

NEW QUESTION 361
In OTV, how are the VLANs split when a site has two edge devices?

A. They are configured manually by user.
B. They are split in half among each edge device.
C. They are split as odd and even VLAN IDs on each edge device.
D. It is not possible to have two edge devices in same sit

Answer: C

NEW QUESTION 366
Which statement about the MPLS feature set is true?

A. It is not license dependent.
B. It can be installed from any VDC.
C. It can be enabled only in the default VDC.
D. It must be installed from the default VD

Answer: D

NEW QUESTION 370
When implementing Cisco Adapter FEX, which setting on the virtual interface card on the Cisco UCS C-Series Server must be configured?

A. uplink failover
B. PXE boot
C. network interface virtualization
D. VM-FEX

Answer: C

NEW QUESTION 375
Which standard has Cisco used to implement VM-FEX?

A. IEEE 802.1BR
B. IEEE 802.1Qbb
C. IEEE 802.1Qaz
D. IEEE 802.1p
E. IEEE 802.1x

Answer: A

NEW QUESTION 377
During the design of a new Cisco Data Center Network, a customer asked when VM-FEX would be used with Cisco Nexus 1000V Switch. Which scenario is most appropriate?

A. when a host must utilize a vSwitch and a distributed vSwitch
B. when using Non-UCS Servers to provide virtualization services with Nexus FEX modules
C. They are mutually exclusive of each other.
D. when a Cisco UCS C-Series server requires Cisco Nexus 1000V Switch to provide VM connectivity

Answer: C

NEW QUESTION 380
Which statement about FabricPath and private VLANs is true?

A. FabricPath ports can be put into a private VLAN.
B. All VLANs in the private VLAN must in the same mode.
C. Private VLANs are not supported with FabricPath.
D. FabricPath is the only mode supported for private VLAN

Answer: B

NEW QUESTION 383
If vPC peer keepalives are used between vPC peers, which VRF is used by default?

A. management
B. default
C. The user must dedicate a VRF for keepalives.
D. system

Answer: A

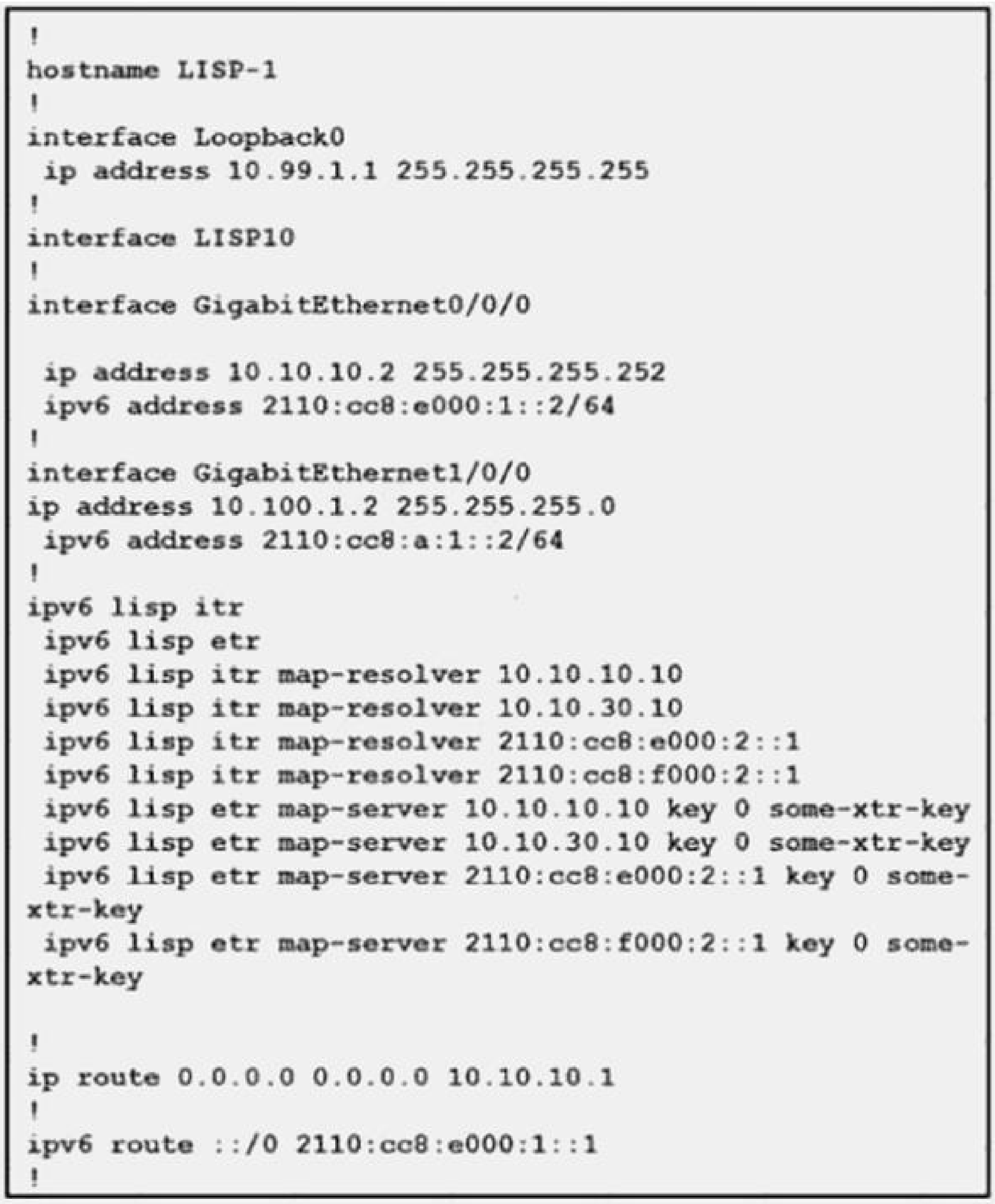
NEW QUESTION 385
Using the default VDC high-availability options in the Cisco Nexus 7010 switch, which event occurs after a VDC failure?

A. VDC restart occurs.
B. The VDC is deleted.
C. VDC bringdown occurs, and the VDC must be restarted manually.

D. VDC shutdown occurs, and the VDC must be restarted manuall

Answer: D

NEW QUESTION 389
Refer to the exhibit.



```
!
hostname LISP-1
!
interface Loopback0
 ip address 10.99.1.1 255.255.255.255
!
interface LISP10
!
interface GigabitEthernet0/0/0

 ip address 10.10.10.2 255.255.255.252
 ipv6 address 2110:cc8:e000:1::2/64
!
interface GigabitEthernet1/0/0
ip address 10.100.1.2 255.255.255.0
 ipv6 address 2110:cc8:a:1::2/64
!
ipv6 lisp itr
 ipv6 lisp etr
 ipv6 lisp itr map-resolver 10.10.10.10
 ipv6 lisp itr map-resolver 10.10.30.10
 ipv6 lisp itr map-resolver 2110:cc8:e000:2::1
 ipv6 lisp itr map-resolver 2110:cc8:f000:2::1
 ipv6 lisp etr map-server 10.10.10.10 key 0 some-xtr-key
 ipv6 lisp etr map-server 10.10.30.10 key 0 some-xtr-key
 ipv6 lisp etr map-server 2110:cc8:e000:2::1 key 0 some-
xtr-key
 ipv6 lisp etr map-server 2110:cc8:f000:2::1 key 0 some-
xtr-key

!
ip route 0.0.0.0 0.0.0.0 10.10.10.1
!
ipv6 route ::/0 2110:cc8:e000:1::1
!
```

Which statement about the configuration is true?

A. It provides an authoritative LISP site for IPv6 EID prefix 2110 cc8 a /48.
B. It configures a single map resolver system.
C. It creates a LISP site policy that requires active/standby service provider links for ingress traffic.
D. It configures PxTR services for IPv6 EID prefix 2110:ccB:a::/48.

Answer: A

NEW QUESTION 390
Which statement about vPC loop avoidance is true?

A. A vPC domain performs loop avoidance on the control plane layer
B. A vPC domain performs loop avoidance on the data plane layer
C. Up to four peer devices can be part of the same vPC domain
D. Traffic that comes from a vPC member port, and then crosses a vPC peer link can leave through any vPC member port

Answer: B

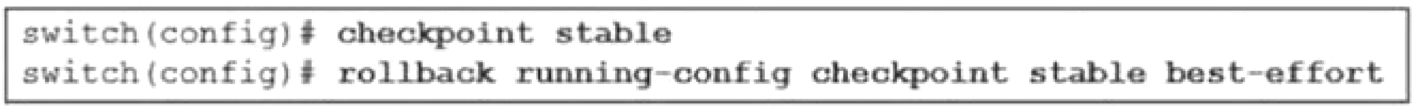
NEW QUESTION 395
You must configure Microsoft Network Load Balancing in unicast mode across OTV sites. Which OTV option do you enable?

A. selective unicast flooding
B. ARP local caching
C. multihoming
D. FHRP filtering

Answer: A

NEW QUESTION 397

Refer to the exhibit.



```
switch(config)# checkpoint stable
switch(config)# rollback running-config checkpoint stable best-effort
```

You are implementing a rollback of the configuration to a checkpoint. Which result of running the command is true?

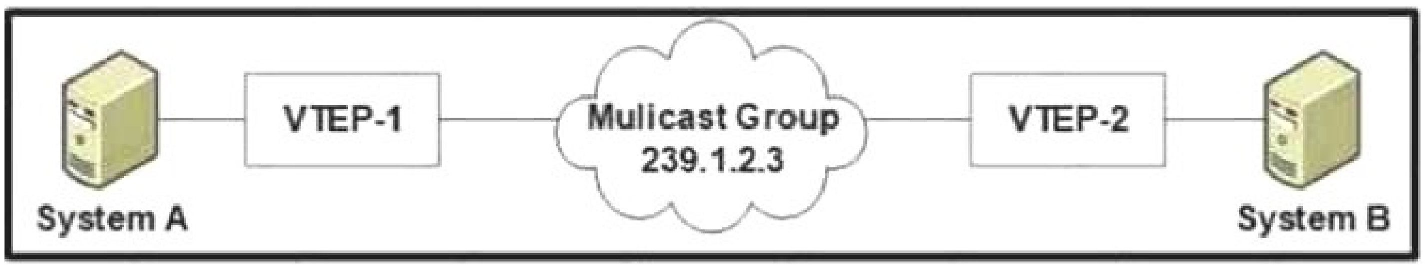
A. It stops a rollback if an error occurs.
B. It creates a rollback only if no errors occur.
C. It creates a rollback in a stable state.
D. It creates a rollback but skips any error

Answer: D

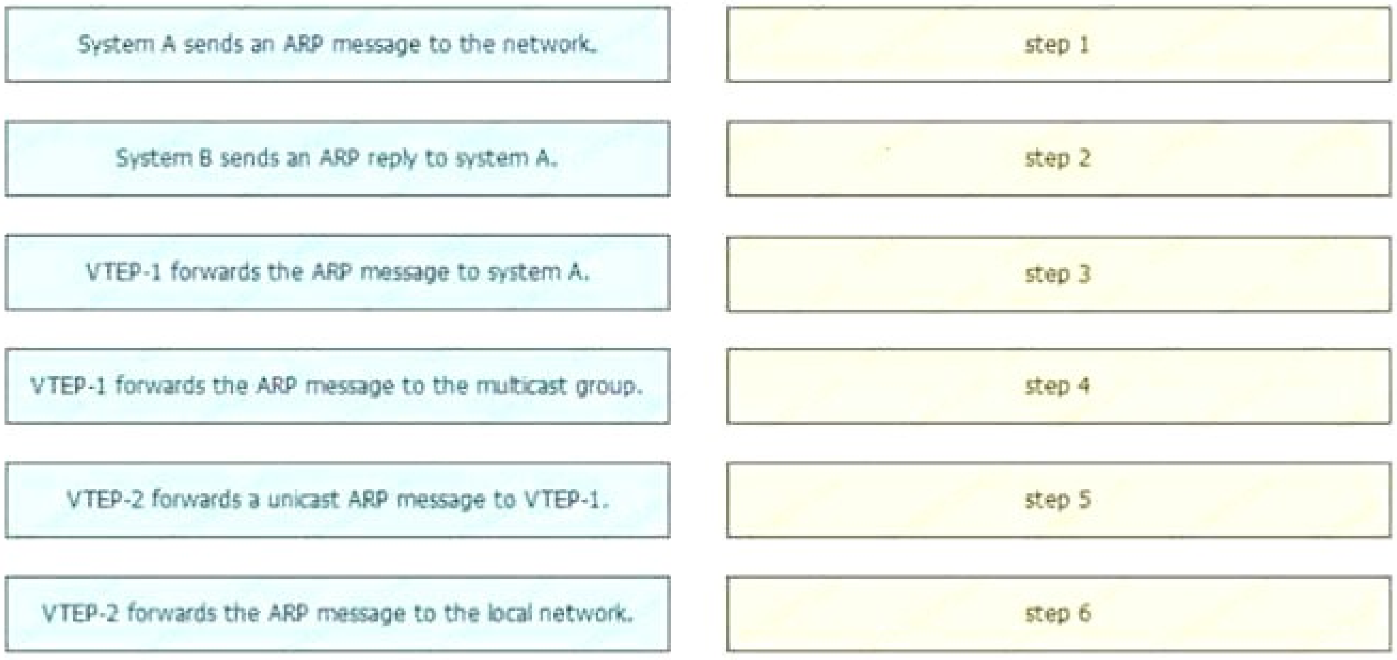
NEW QUESTION 401

DRAG DROP

Refer to the exhibit.



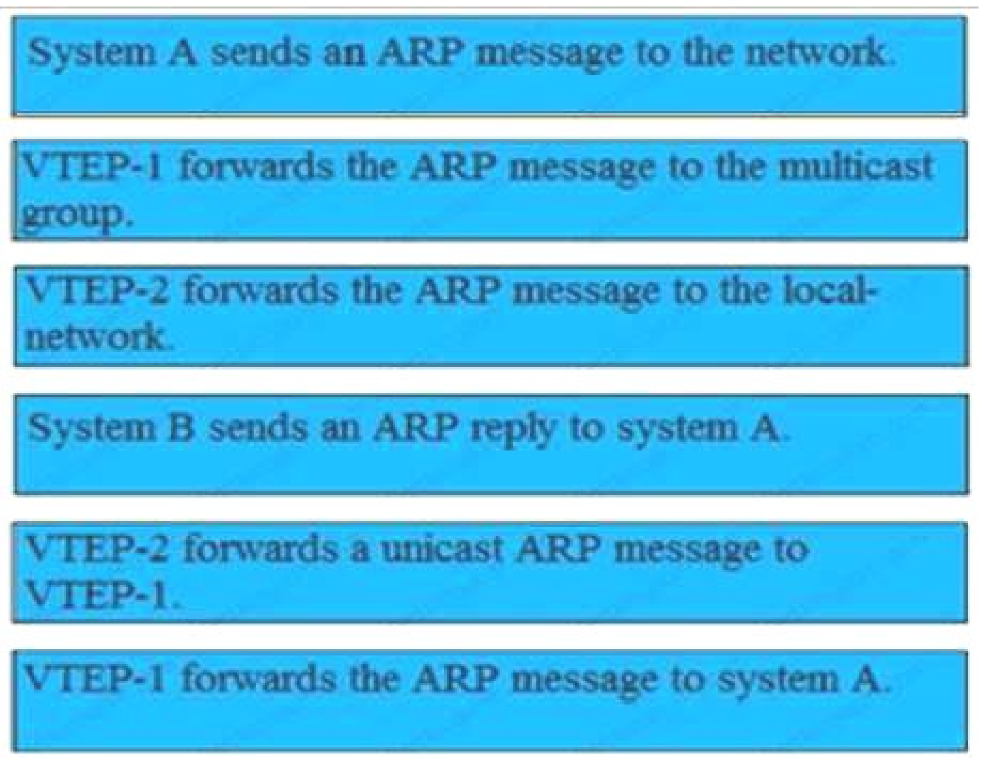
System A must be able to use VXLAN peer discovery to send a message to System B to receive a response. Drag and drop the peer discovery steps from the left into the correct order on the right.



System A sends an ARP message to the network.	step 1
System B sends an ARP reply to system A.	step 2
VTEP-1 forwards the ARP message to system A.	step 3
VTEP-1 forwards the ARP message to the multicast group.	step 4
VTEP-2 forwards a unicast ARP message to VTEP-1.	step 5
VTEP-2 forwards the ARP message to the local network.	step 6

Answer:

Explanation:



System A sends an ARP message to the network.

VTEP-1 forwards the ARP message to the multicast group.

VTEP-2 forwards the ARP message to the local-network.

System B sends an ARP reply to system A.

VTEP-2 forwards a unicast ARP message to VTEP-1.

VTEP-1 forwards the ARP message to system A.

NEW QUESTION 405

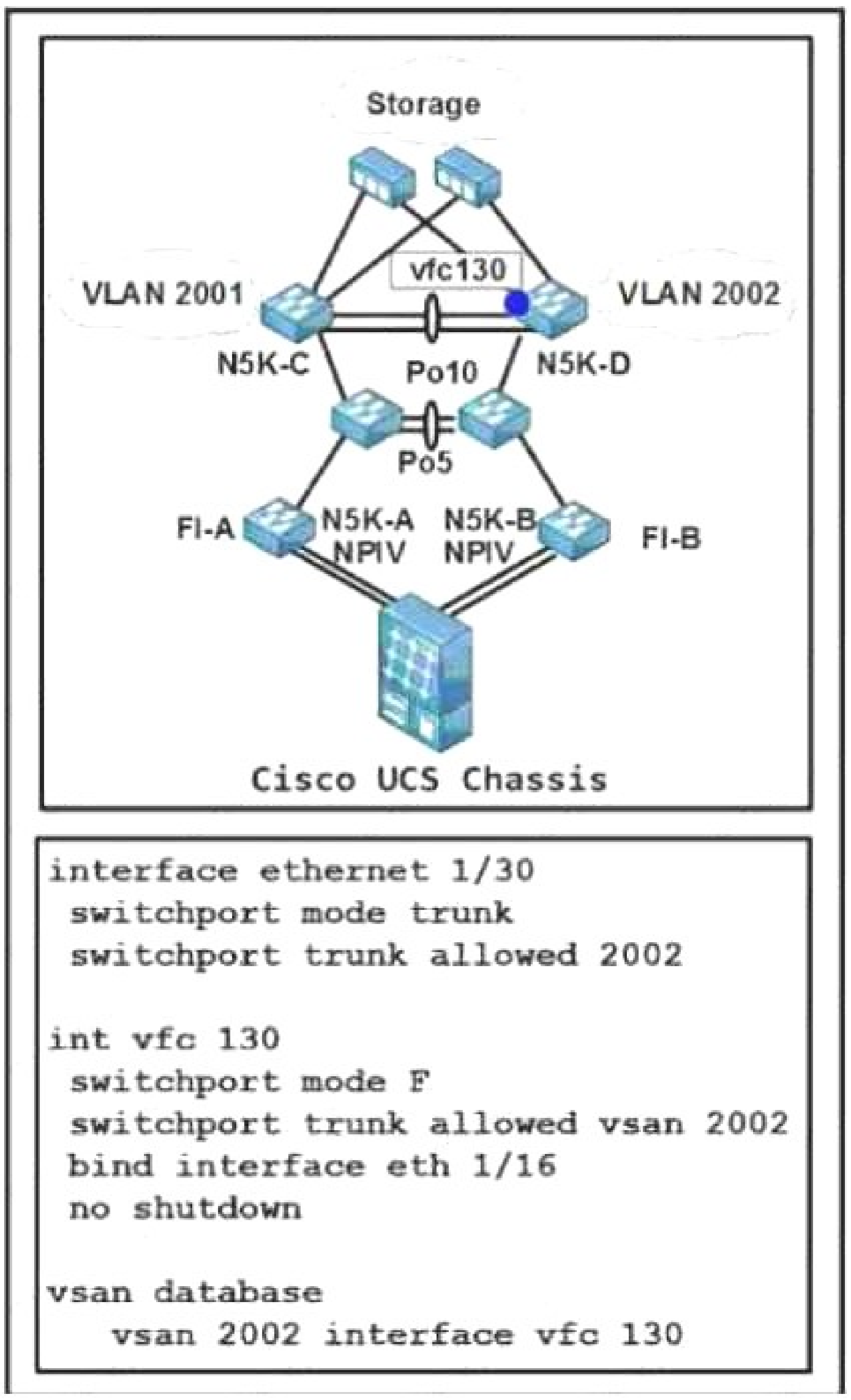
Which technology facilitates a nondisruptive upgrade on a Cisco Nexus 5000 Series Switch?

A. VSS
B. ITD

C. VDC
D. vPC

Answer: D

NEW QUESTION 410
Refer to the exhibit.



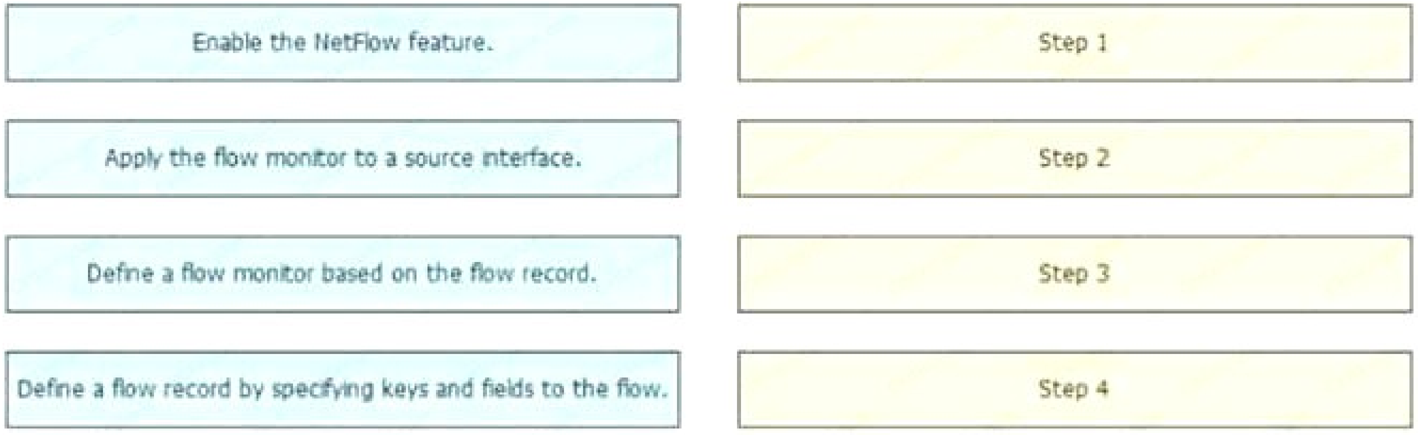
```
interface ethernet 1/30
 switchport mode trunk
 switchport trunk allowed 2002

int vfc 130
 switchport mode F
 switchport trunk allowed vsan 2002
 bind interface eth 1/16
 no shutdown

vsan database
   vsan 2002 interface vfc 130
```

What is the effect of the bind interface eth 1/16 command on the vfc 130 interface?

A. It transitions the port to the forwarding state of the spanning tree automatically.
B. It attaches the FCoE interface to the VSAN interface.
C. It attaches the virtual Fibre Channel interface to the physical interface.
D. It attaches the physical Fibre Channel interface to the virtual Fibre Channel interfac

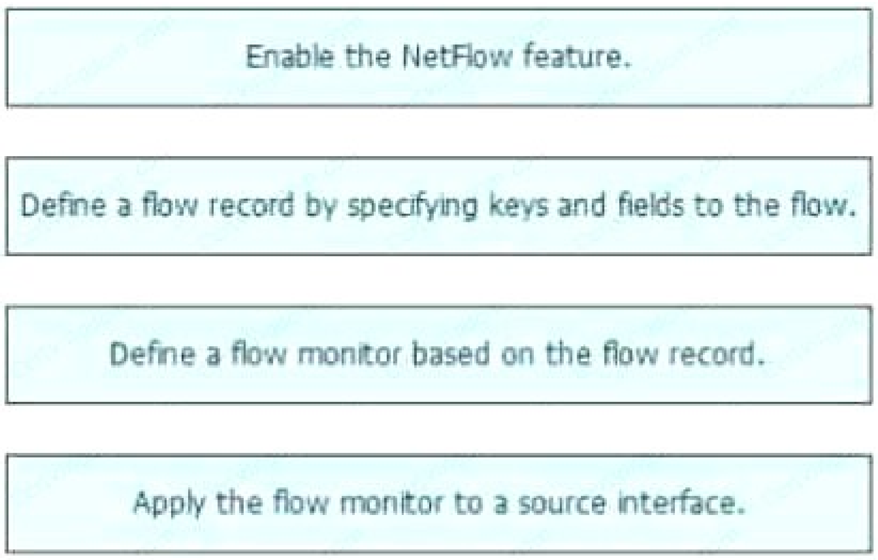
Answer: C

NEW QUESTION 414
DRAG DROP
You must configure NetFlow on a Cisco Nexus 7000 Series switch Drag and drop the configuration steps on the left to the correct order on the right.


Enable the NetFlow feature.
Apply the flow monitor to a source interface.
Define a flow monitor based on the flow record.
Define a flow record by specifying keys and fields to the flow.
Step 1
Step 2
Step 3
Step 4

Answer:

Explanation:



Enable the NetFlow feature.

Define a flow record by specifying keys and fields to the flow.

Define a flow monitor based on the flow record.

Apply the flow monitor to a source interface.

NEW QUESTION 419
Which description of Cisco zoning is true?

A. With enhanced zoning a single configuration session locks the entire fabric to implement achange.
B. In soft zoning individual frames are inspected on ingress.
C. Hard zoning is the most efficient method because it is enforced through software.
D. Soft zoning is implemented by using TCA

Answer: A

NEW QUESTION 424
Which issue does DCB address?

A. low bandwidth
B. latency
C. congestion
D. need for jumbo frames

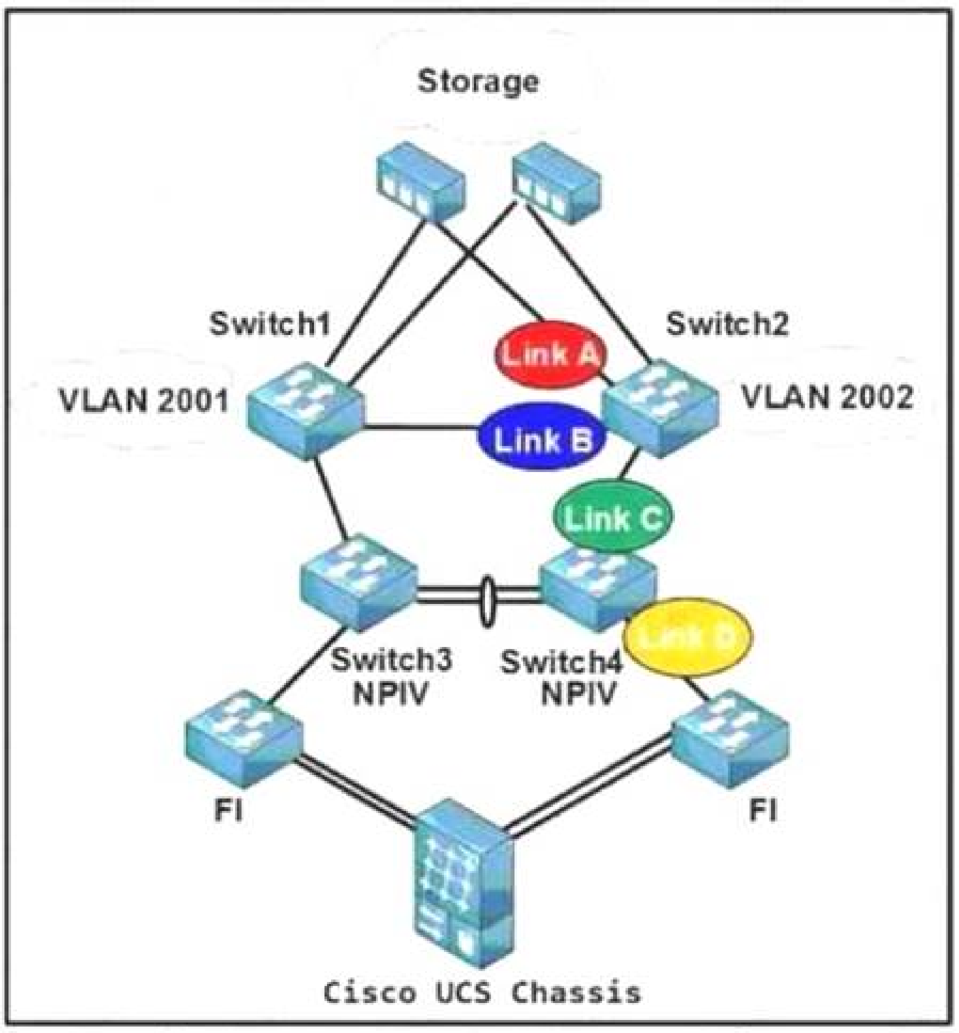
Answer: C

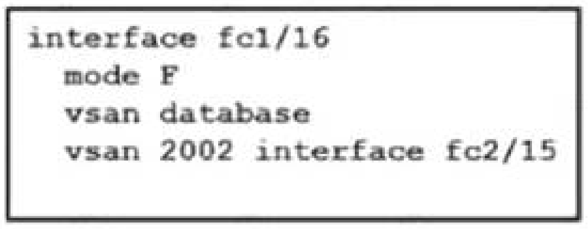
NEW QUESTION 429
You have multiple OTV edge devices in each OTV site. Which configuration prevents an end-to-end STP loop?

A. selective unicast flooding
B. AED election
C. FHRP filtering
D. ARP local caching

Answer: B

NEW QUESTION 432
Refer to the exhibit.





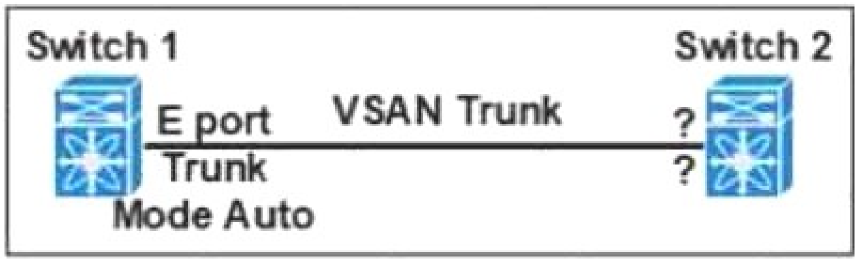
```
interface fc1/16
  mode F
  vsan database
  vsan 2002 interface fc2/15
```

The configuration belongs to which link?

A. Link A on Switch2
B. Link B on Switch2
C. Link C on Switch4
D. Link D on Switch4

Answer: D

NEW QUESTION 434
Refer to the exhibit.

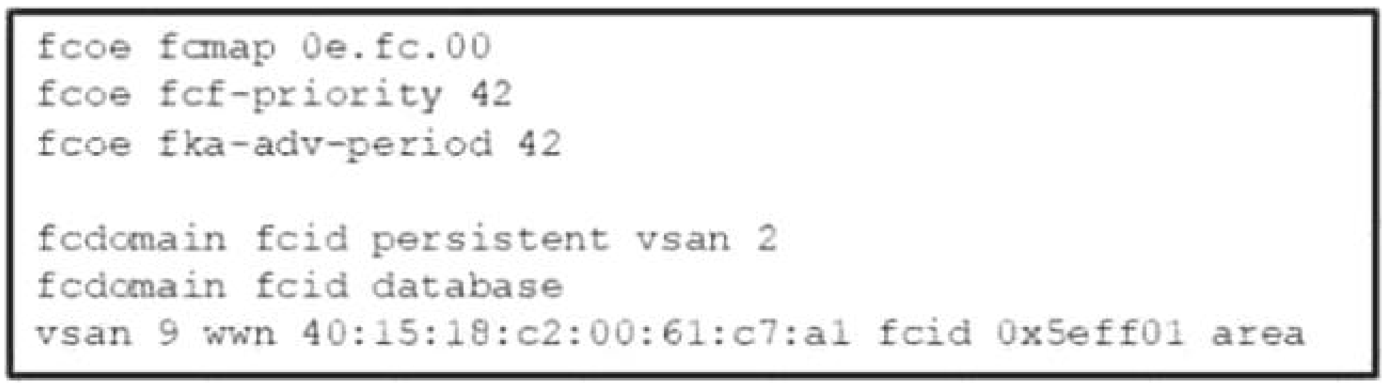


Which two features must you configure on Switch 2 to establish a VSAN trunk between Switch 1 and Switch 2? (Choose two.)

A. Trunk Mode On
B. F port
C. E port
D. NP port
E. Trunk Mode Auto

Answer: CE

NEW QUESTION 435
Refer to the exhibit.



```
fcoe fcmap 0e.fc.00
fcoe fcf-priority 42
fcoe fka-adv-period 42

fcdomain fcid persistent vsan 2
fcdomain fcid database
vsan 9 wwn 40:15:18:c2:00:61:c7:a1 fcid 0x5eff01 area
```

Which fabric -provided MAC address does the switch use when connecting to an end node on VSAN 9?

A. 5e.ff.01.0e.fc.00
B. 0e.fc.00.5e.ff.01
C. 40.15.18.oe.fc.00
D. 40.15.18.5e.ff.01

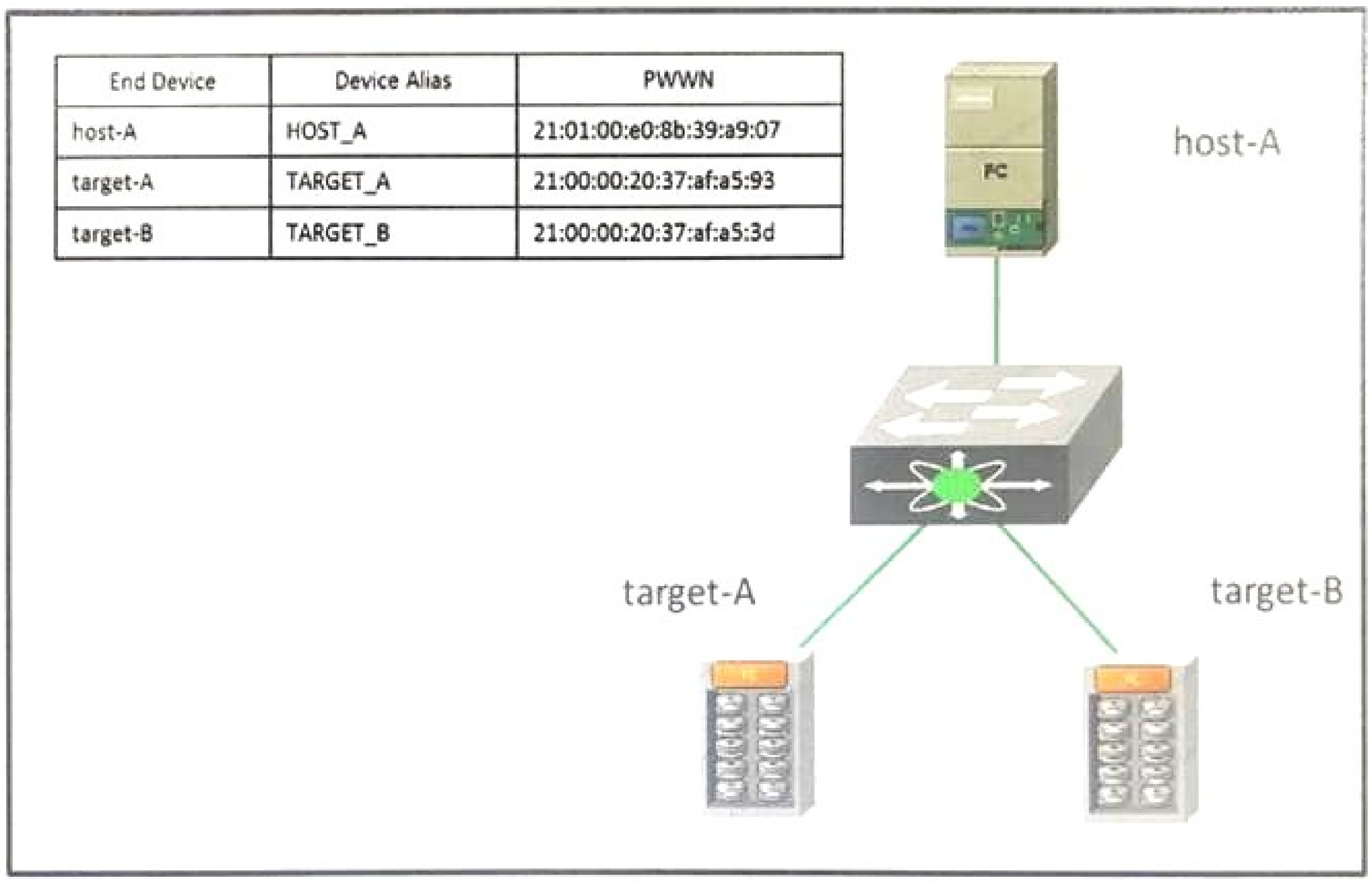
Answer: C

NEW QUESTION 437
When configuring PIM on a Cisco Nexus 7000 Series switch, which mode requires you to configure an RP?

A. SDM
B. SSM
C. DM
D. ASM

Answer: D

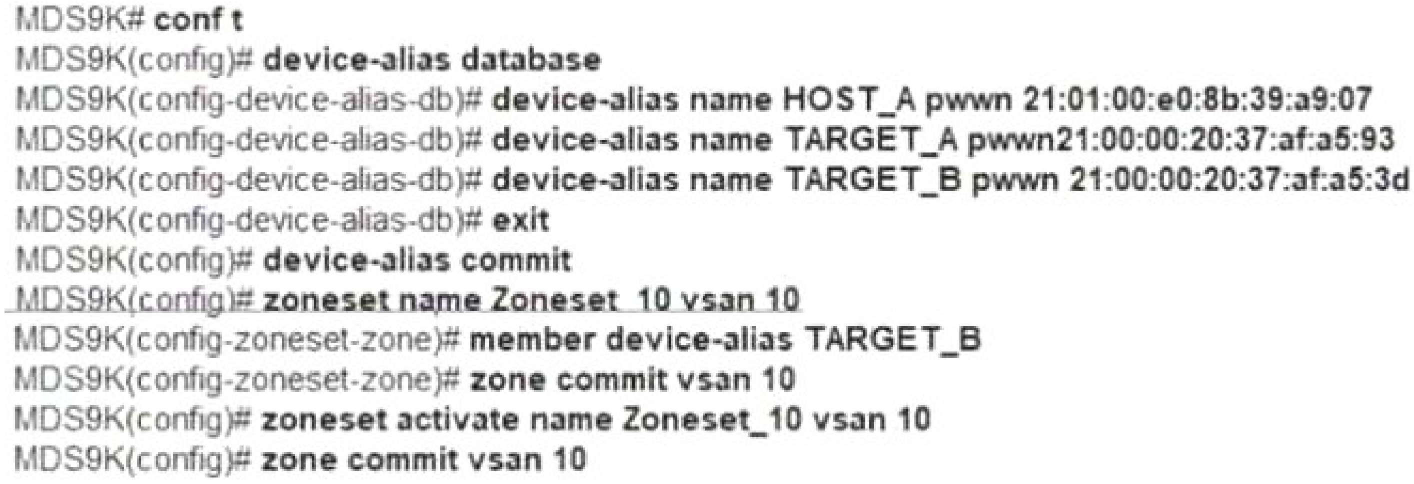
NEW QUESTION 440
Refer to the exhibit.



End Device	Device Alias	PWWN
host-A	HOST_A	21:01:00:e0:8b:39:a9:07
target-A	TARGET_A	21:00:00:20:37:af:a5:93
target-B	TARGET_B	21:00:00:20:37:af:a5:3d

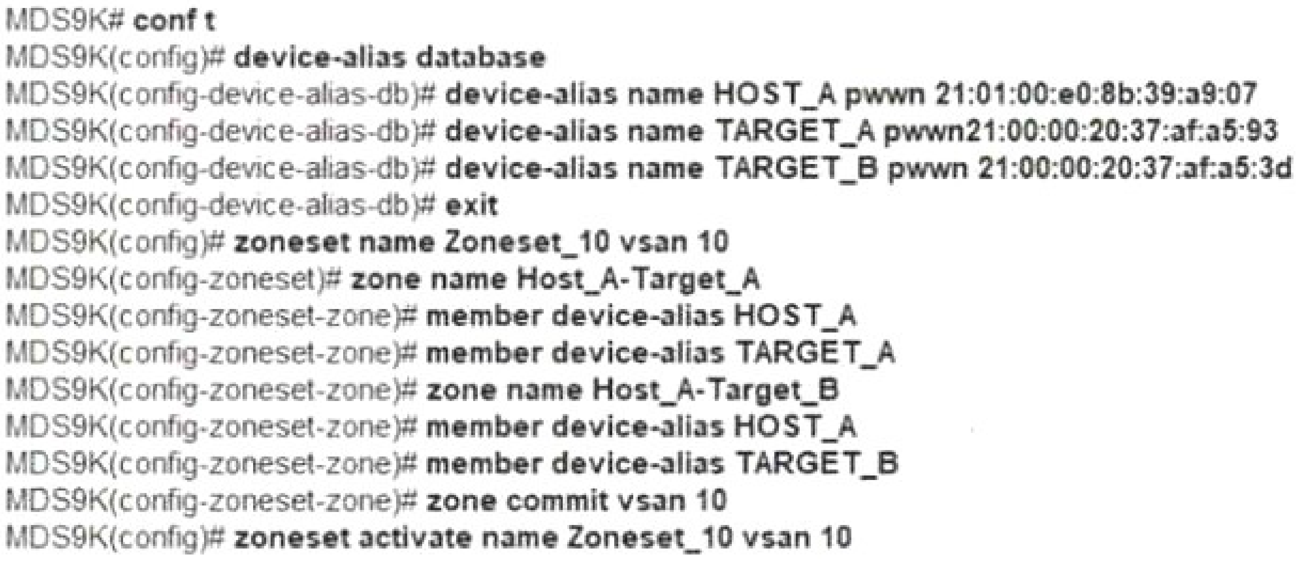
You must configure zones on a Cisco MDS 9000 Series SAN switch. Host_A must be able to communicate with target_A and with target_B in the Zoneset_10 active zone set in VSAN 10. Which command set should you use?

A)



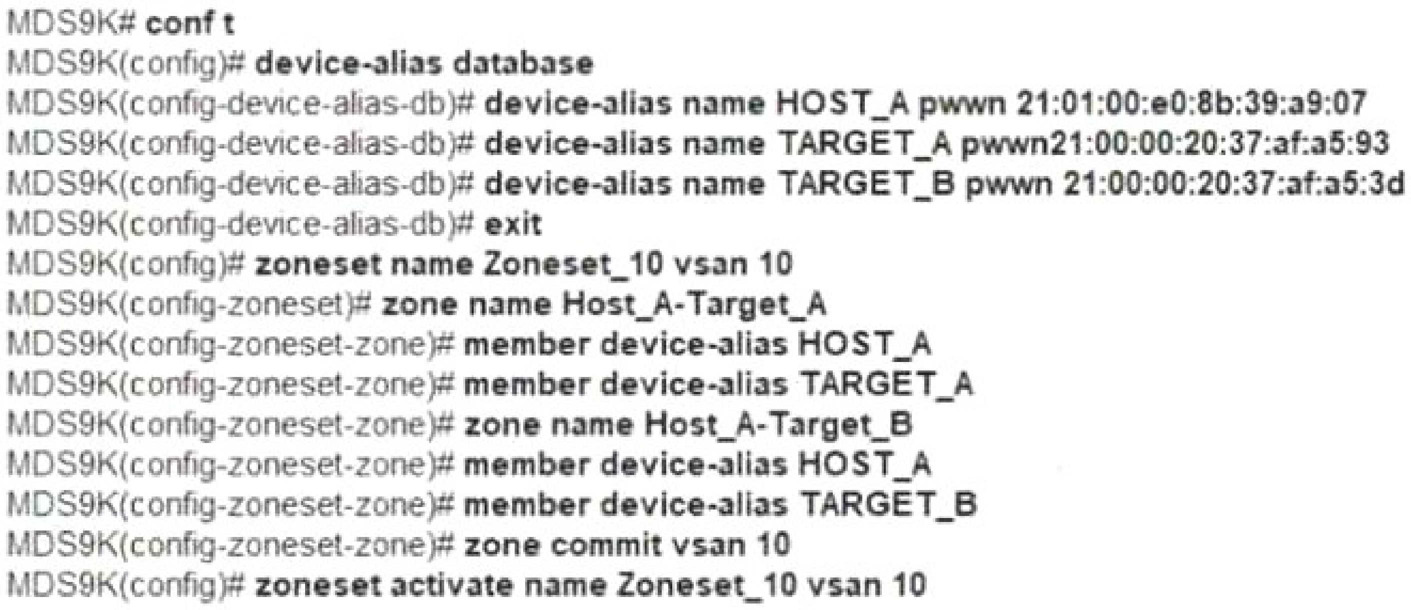
```
MDS9K# conf t
MDS9K(config)# device-alias database
MDS9K(config-device-alias-db)# device-alias name HOST_A pwwn 21:01:00:e0:8b:39:a9:07
MDS9K(config-device-alias-db)# device-alias name TARGET_A pwwn21:00:00:20:37:af:a5:93
MDS9K(config-device-alias-db)# device-alias name TARGET_B pwwn 21:00:00:20:37:af:a5:3d
MDS9K(config-device-alias-db)# exit
MDS9K(config)# device-alias commit
MDS9K(config)# zoneset name Zoneset_10 vsan 10
MDS9K(config-zoneset-zone)# member device-alias TARGET_B
MDS9K(config-zoneset-zone)# zone commit vsan 10
MDS9K(config)# zoneset activate name Zoneset_10 vsan 10
MDS9K(config)# zone commit vsan 10
```

B)



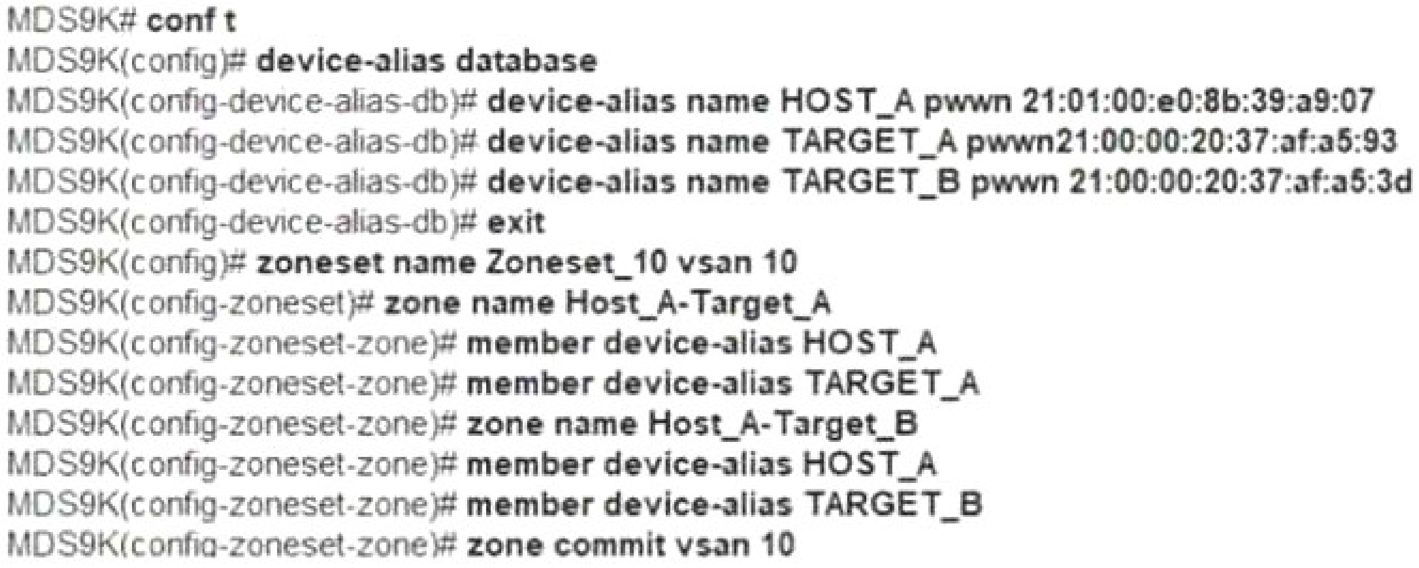
```
MDS9K# conf t
MDS9K(config)# device-alias database
MDS9K(config-device-alias-db)# device-alias name HOST_A pwwn 21:01:00:e0:8b:39:a9:07
MDS9K(config-device-alias-db)# device-alias name TARGET_A pwwn21:00:00:20:37:af:a5:93
MDS9K(config-device-alias-db)# device-alias name TARGET_B pwwn 21:00:00:20:37:af:a5:3d
MDS9K(config-device-alias-db)# exit
MDS9K(config)# zoneset name Zoneset_10 vsan 10
MDS9K(config-zoneset)# zone name Host_A-Target_A
MDS9K(config-zoneset-zone)# member device-alias HOST_A
MDS9K(config-zoneset-zone)# member device-alias TARGET_A
MDS9K(config-zoneset-zone)# zone name Host_A-Target_B
MDS9K(config-zoneset-zone)# member device-alias HOST_A
MDS9K(config-zoneset-zone)# member device-alias TARGET_B
MDS9K(config-zoneset-zone)# zone commit vsan 10
MDS9K(config)# zoneset activate name Zoneset_10 vsan 10
```

C)



```
MDS9K# conf t
MDS9K(config)# device-alias database
MDS9K(config-device-alias-db)# device-alias name HOST_A pwwn 21:01:00:e0:8b:39:a9:07
MDS9K(config-device-alias-db)# device-alias name TARGET_A pwwn21:00:00:20:37:af:a5:93
MDS9K(config-device-alias-db)# device-alias name TARGET_B pwwn 21:00:00:20:37:af:a5:3d
MDS9K(config-device-alias-db)# exit
MDS9K(config)# zoneset name Zoneset_10 vsan 10
MDS9K(config-zoneset)# zone name Host_A-Target_A
MDS9K(config-zoneset-zone)# member device-alias HOST_A
MDS9K(config-zoneset-zone)# member device-alias TARGET_A
MDS9K(config-zoneset-zone)# zone name Host_A-Target_B
MDS9K(config-zoneset-zone)# member device-alias HOST_A
MDS9K(config-zoneset-zone)# member device-alias TARGET_B
MDS9K(config-zoneset-zone)# zone commit vsan 10
MDS9K(config)# zoneset activate name Zoneset_10 vsan 10
```

D)

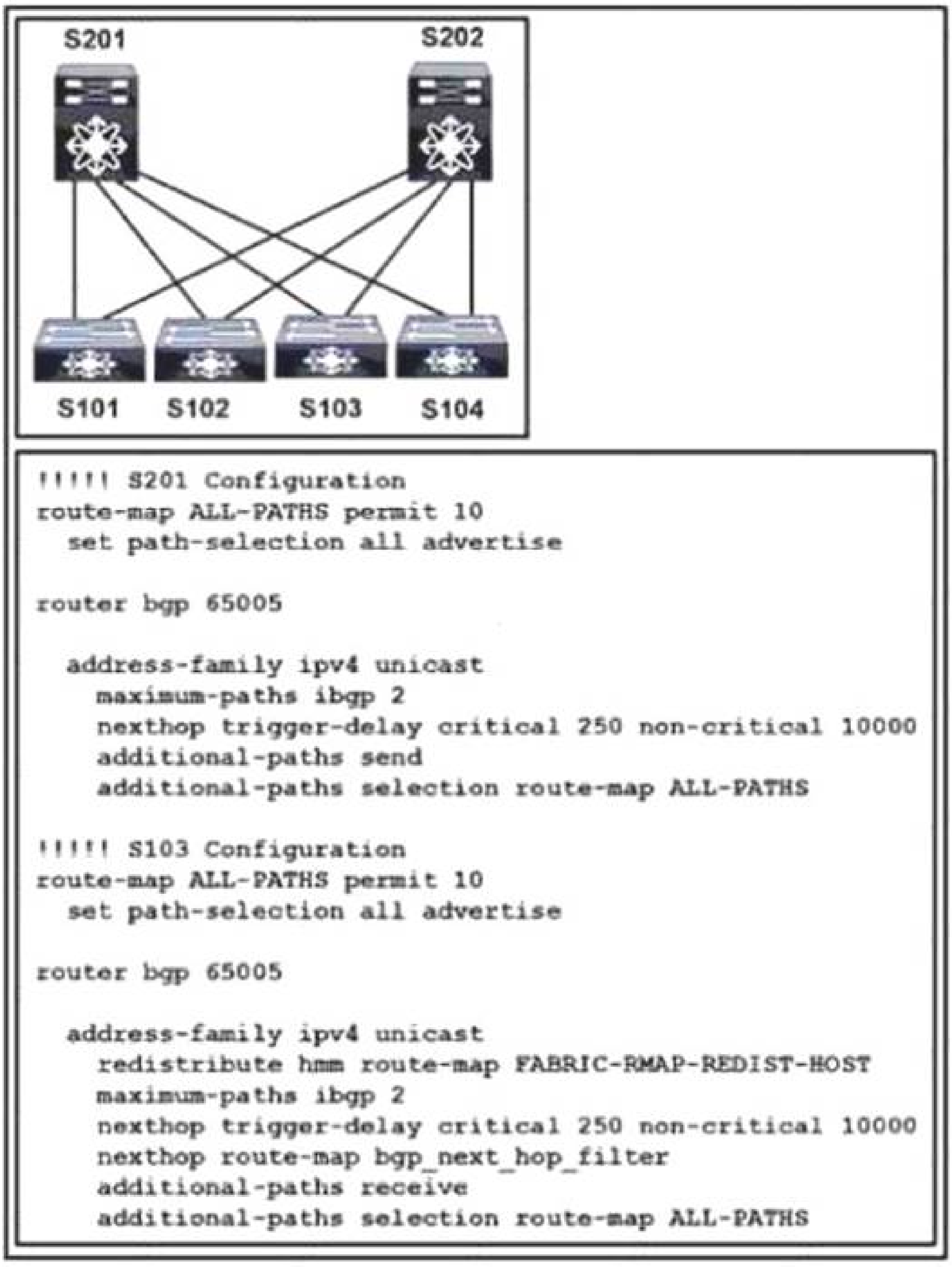


```
MDS9K# conf t
MDS9K(config)# device-alias database
MDS9K(config-device-alias-db)# device-alias name HOST_A pwwn 21:01:00:e0:8b:39:a9:07
MDS9K(config-device-alias-db)# device-alias name TARGET_A pwwn21:00:00:20:37:af:a5:93
MDS9K(config-device-alias-db)# device-alias name TARGET_B pwwn 21:00:00:20:37:af:a5:3d
MDS9K(config-device-alias-db)# exit
MDS9K(config)# zoneset name Zoneset_10 vsan 10
MDS9K(config-zoneset)# zone name Host_A-Target_A
MDS9K(config-zoneset-zone)# member device-alias HOST_A
MDS9K(config-zoneset-zone)# member device-alias TARGET_A
MDS9K(config-zoneset-zone)# zone name Host_A-Target_B
MDS9K(config-zoneset-zone)# member device-alias HOST_A
MDS9K(config-zoneset-zone)# member device-alias TARGET_B
MDS9K(config-zoneset-zone)# zone commit vsan 10
```

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

Answer: D

NEW QUESTION 442
Refer to the exhibit.



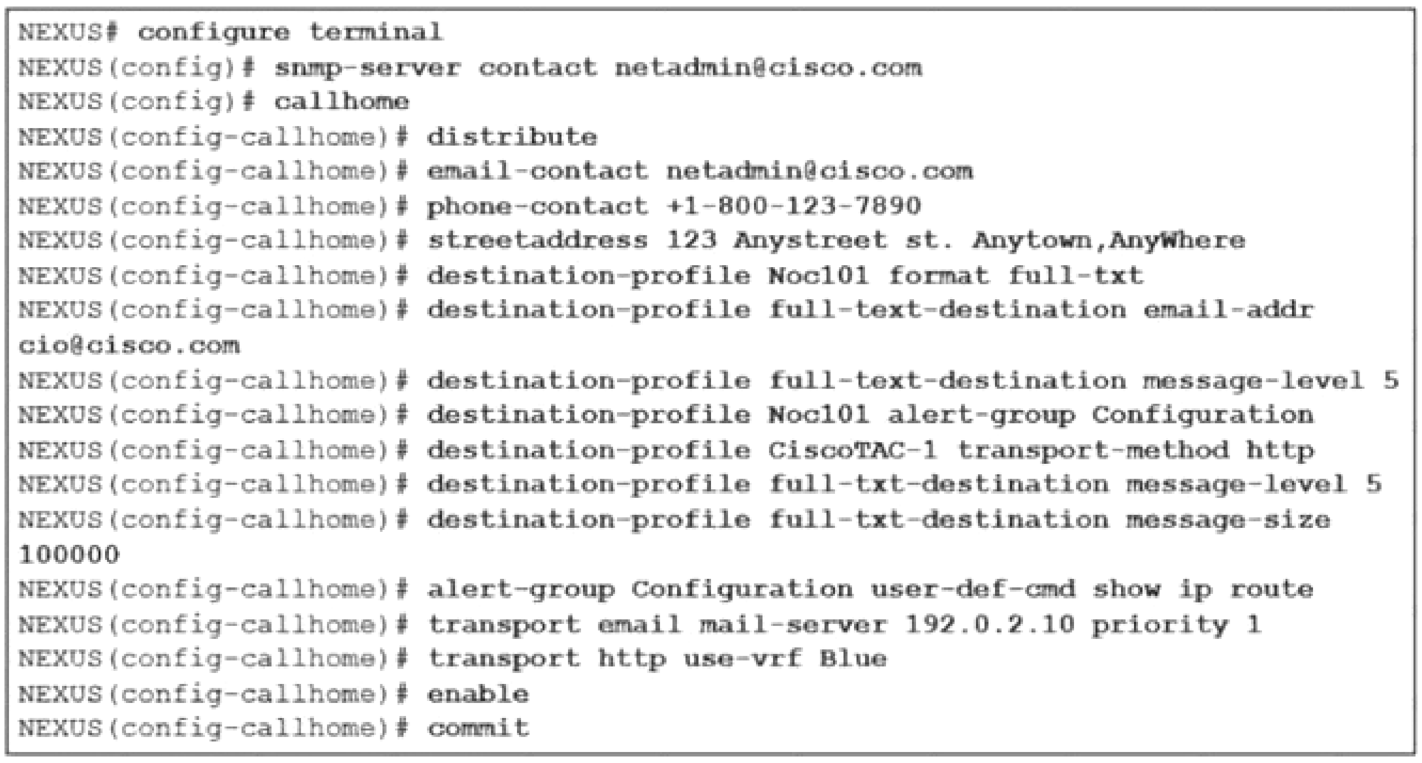
```
!!!!! S201 Configuration
route-map ALL-PATHS permit 10
  set path-selection all advertise

router bgp 65005

  address-family ipv4 unicast
    maximum-paths ibgp 2
    nexthop trigger-delay critical 250 non-critical 10000
    additional-paths send
    additional-paths selection route-map ALL-PATHS

!!!!! S103 Configuration
route-map ALL-PATHS permit 10
  set path-selection all advertise

router bgp 65005

  address-family ipv4 unicast
    redistribute hmm route-map FABRIC-RMAP-REDIST-HOST
    maximum-paths ibgp 2
    nexthop trigger-delay critical 250 non-critical 10000
    nexthop route-map bgp_next_hop_filter
    additional-paths receive
    additional-paths selection route-map ALL-PATHS
```

Which result does the configuration show?

A. border spine
B. tenant interface
C. SVI configuration
D. border leaf

Answer: D

NEW QUESTION 444
Refer to the exhibit.



```
NEXUS# configure terminal
NEXUS(config)# snmp-server contact netadmin@cisco.com
NEXUS(config)# callhome
NEXUS(config-callhome)# distribute
NEXUS(config-callhome)# email-contact netadmin@cisco.com
NEXUS(config-callhome)# phone-contact +1-800-123-7890
NEXUS(config-callhome)# streetaddress 123 Anystreet st. Anytown,AnyWhere
NEXUS(config-callhome)# destination-profile Noc101 format full-txt
NEXUS(config-callhome)# destination-profile full-text-destination email-addr
cio@cisco.com
NEXUS(config-callhome)# destination-profile full-text-destination message-level 5
NEXUS(config-callhome)# destination-profile Noc101 alert-group Configuration
NEXUS(config-callhome)# destination-profile CiscoTAC-1 transport-method http
NEXUS(config-callhome)# destination-profile full-txt-destination message-level 5
NEXUS(config-callhome)# destination-profile full-txt-destination message-size
100000
NEXUS(config-callhome)# alert-group Configuration user-def-cmd show ip route
NEXUS(config-callhome)# transport email mail-server 192.0.2.10 priority 1
NEXUS(config-callhome)# transport http use-vrf Blue
NEXUS(config-callhome)# enable
NEXUS(config-callhome)# commit
```

Which result of implementing the configuration is true?

A. The maximum message size is 2500000.
B. An alert is sent for a Major condition.
C. Email is used as the transport.
D. The minimum message seventy level is 9.

Answer: A

NEW QUESTION 445
Which two statements about the VRRP are true? (Choose two.)

A. VRRP allows the traffic load to be shared through the use of multiple VRRP groups.
B. When the VRRP is configured to track a Layer 2 interface, the VRRP priority instantly refilects the state of the Layer 2 interface.
C. The BFD for the VRRP can be configured only between two Cisco Nexus switches
D. vPC can forward traffic through both VRRP devices.
E. The VRRP can be configured on the management interfac

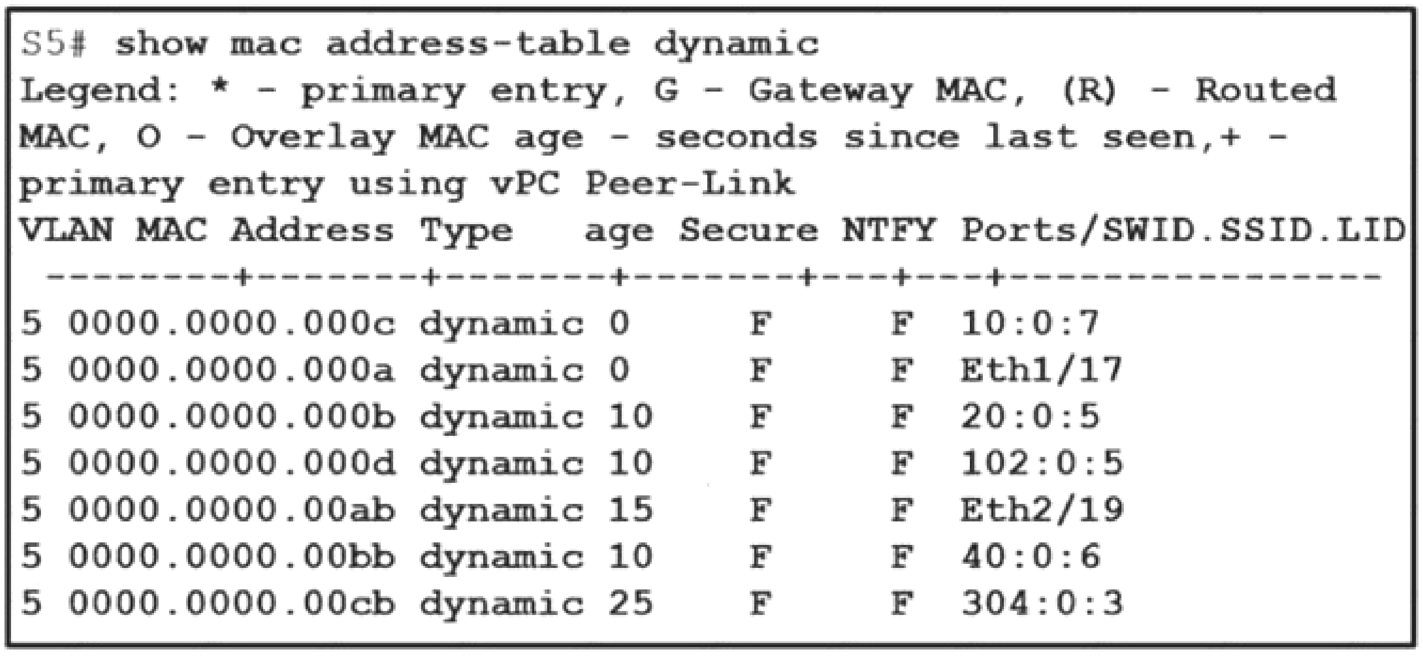
Answer: AD

NEW QUESTION 448
Which description of a MAC ACL is true?

A. It filters based on the DSCP value.
B. It is applied to egress traffic only.
C. It is applied when DHCP snooping is enabled.
D. It is applied to ingress traffic onl

Answer: A

NEW QUESTION 452
Refer to the exhibit.



```
S5# show mac address-table dynamic
Legend: * - primary entry, G - Gateway MAC, (R) - Routed
MAC, O - Overlay MAC age - seconds since last seen,+ -
primary entry using vPC Peer-Link
VLAN MAC Address Type   age Secure NTFY Ports/SWID.SSID.LID
 --------+--------+--------+--------+---+---+----------------
5 0000.0000.000c dynamic 0      F      F  10:0:7
5 0000.0000.000a dynamic 0      F      F  Eth1/17
5 0000.0000.000b dynamic 10     F      F  20:0:5
5 0000.0000.000d dynamic 10     F      F  102:0:5
5 0000.0000.00ab dynamic 15     F      F  Eth2/19
5 0000.0000.00bb dynamic 10     F      F  40:0:6
5 0000.0000.00cb dynamic 25     F      F  304:0:3
```

Which field identifies the ESID of a participating switch?

A. LID
B. NTFY
C. SSID
D. SWID

Answer: D

NEW QUESTION 453
Which feature does a vFC interface support?

A. port tracking
B. F Port mode
C. SAN port channels
D. buffer-to-buffer credits

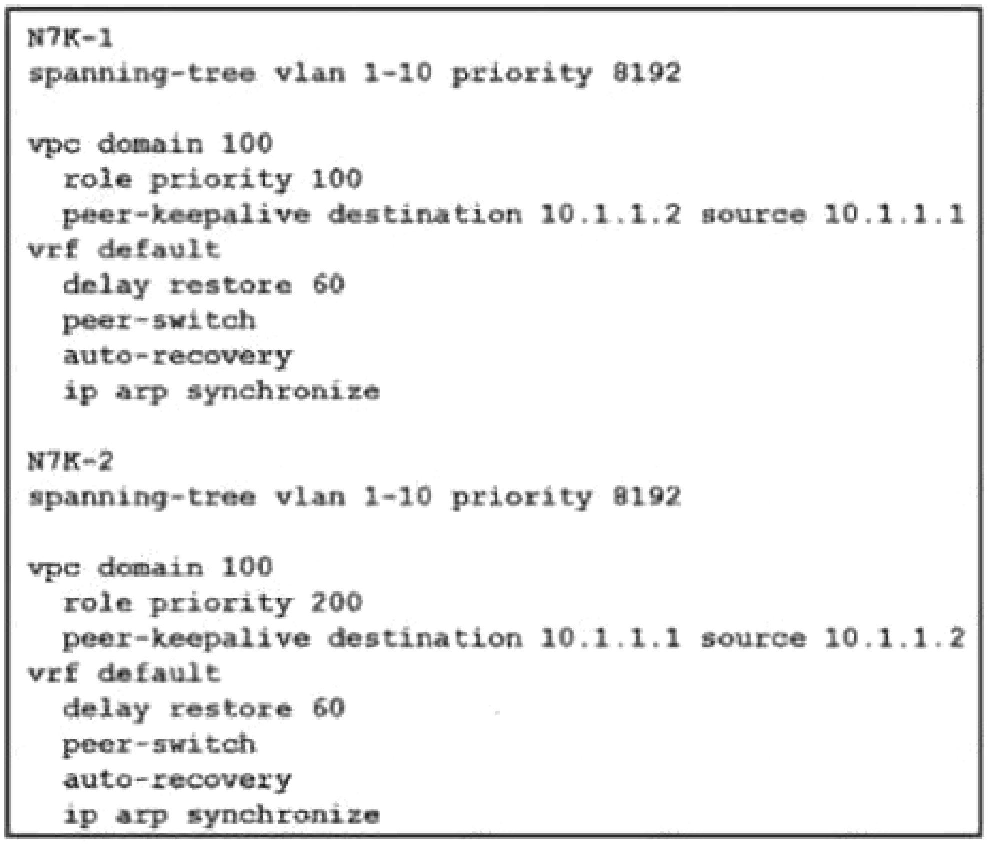
Answer: B

NEW QUESTION 456
Which three types of interfaces are required when implementing VXLAN on a Cisco Nexus 9000 Series Switch? (Choose three.)

A. overlay
B. NVE
C. management
D. Ethernet
E. ACI
F. loopback

Answer: BDF

NEW QUESTION 459
Refer to the exhibit.



```
N7K-1
spanning-tree vlan 1-10 priority 8192

vpc domain 100
  role priority 100
  peer-keepalive destination 10.1.1.2 source 10.1.1.1
vrf default
  delay restore 60
  peer-switch
  auto-recovery
  ip arp synchronize

N7K-2
spanning-tree vlan 1-10 priority 8192

vpc domain 100
  role priority 200
  peer-keepalive destination 10.1.1.1 source 10.1.1.2
vrf default
  delay restore 60
  peer-switch
  auto-recovery
  ip arp synchronize
```

Which statement about STP on the vPC is true?

A. N7K-1 and N7K-2 appear as a single STP bridge
B. N7K-2 appears as the STP root
C. N7K-1 preempts N7K-2 as the STP root
D. N7K-1 appears as the STP root

Answer: A

NEW QUESTION 463
A vPC fails a Type 2 consistency check during implementation. Which result is true?

A. The interfaces may forward packets using an undesirable path
B. The vPC algorithm selects a link to deactivate randomly until the condition is resolved
C. The interfaces are suspended
D. The link to the secondary vPC is suspended until the condition is resolved

Answer: D

NEW QUESTION 464
Which two actions are required when configuring LISP virtual machine mobility across subnets? (Choose two.)

A. Filter HSRP hello messages across data centers to create an active-active HSRP setup
B. Enable proxy ARP on the interfaces that allow virtual machine mobility
C. Configure different MAC addresses across all the HSRP groups
D. Ensure that all the HSRP virtual IP addresses are different in the extended LANs
E. Propagate ARP packets across all the broadcast domains of the data cente

Answer: AB

NEW QUESTION 465
......