

Exam Questions 300-165

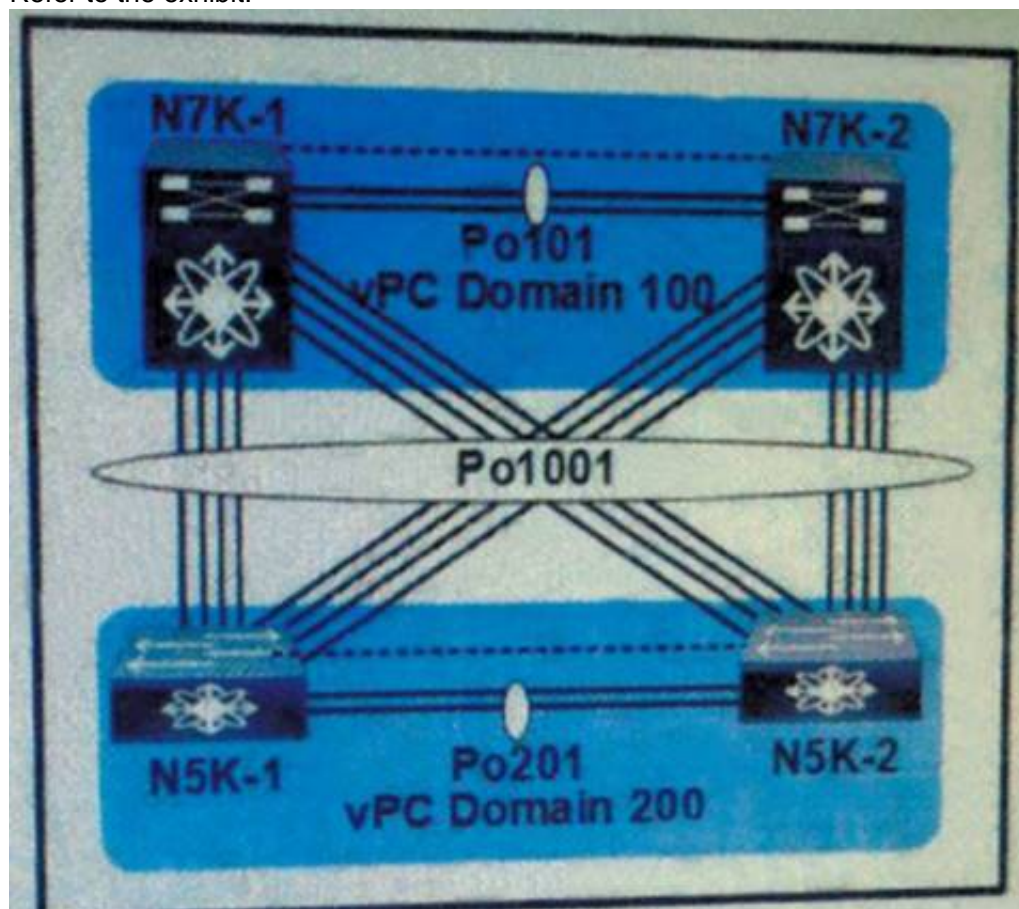
DCII Implementing Cisco Data Center Infrastructure (DCII)

<https://www.2passeasy.com/dumps/300-165/>



NEW QUESTION 1

Refer to the exhibit.



You must ensure that the vPC Domain 100 controls the LACP Po1001 link. Which feature do you configure?

- A. peer switch
- B. role priority
- C. system priority
- D. peer gateway

Answer: C

NEW QUESTION 2

DRAG DROP

Drag and drop the configuration management commands on the left to their correct definitions on the right.

atomic	type of rollback that occurs if no errors occur
best-effort	type of rollback that stops if an error occurs
checkpoint	saved state of the running configuration
stop-at-first-failure	type of rollback that skips any errors

Answer:

Explanation:

atomic	atomic
best-effort	stop-at-first-failure
checkpoint	checkpoint
stop-at-first-failure	best-effort

NEW QUESTION 3

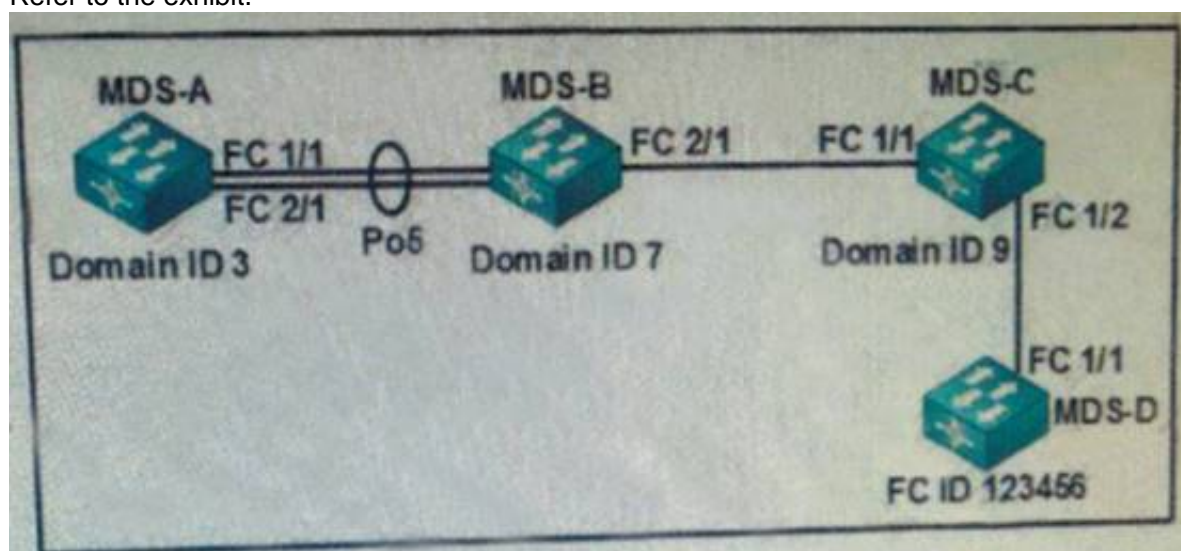
Which option describes the atomic rollback feature in Cisco NX-OS?

- 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 4

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 5

DRAG DROP

Drag and drop the types of PTP clocks on the left to their correct descriptions on the right.

boundary	has a single PTP port in a domain and communicates with the network
end-to-end transparent	has multiple PTP ports in a domain, and each port communicates with the network
ordinary	measures the residence time of a PTP message and accumulates the times in a follow-up message
peer-to-peer transparent	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

Which statement about the configuration of a VXLAN is true?

- A. The source interface must be a loopback interface.
- B. The VNI must be shared across multiple NVE interfaces.
- C. The source interface must be a physical interface
- D. Static MAC addresses must be configured on the interfac

Answer: A

NEW QUESTION 7

You create a checkpoint on a Cisco Nexus 7700 Series switch. You plan to roll back the running configuration by using the checkpoint. You must ensure that changes are made only if the entire rollback can be applied successfully. Which rollback option should you use?

- A. atomic
- B. stop-at-first-failure
- C. best-effort
- D. verbose

Answer: A

NEW QUESTION 8

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 9

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.html

NEW QUESTION 10

You plan to configure authentication for OSPF. In which mode should you configure OSPF authentication to use a specific key chain?

- A. router ospf
- B. global configuration
- C. vPC
- D. interface

Answer: D

NEW QUESTION 10

ipv6 access-list MY_ACL

permit tcp 2001:cc1e:aaaa::/64 2001:cc1e:befe:cccc::/64 permit udp 2001:cc1e:bbbb::/64 2001:cc1e:befe:cccc::/64 interface ethernet 1/1

ipv6 address 2001:cc1e:befe:cccc::1/64 ipv6 traffic-filter MY_ACL in

Refer to the exhibit. Only the ACL in the exhibit is applied on a VDC, and only the default VRF is used. In which two scenarios is traffic permitted? (Choose two.)

- A. TCP traffic from 2001:cc1e:aaaa::/64 to 2001:cc1e:befe:cccc:abcd/64
- B. GRE traffic from 2001:cc1e:befe:cccc::abcd/64 to 2001:cc1e:aaaa/64
- C. UDP traffic from 2001:cc1e:aaaa::/64 to 2001::cc1e:befe:cccc::abcd/64
- D. GRE traffic from 2001:cc1e:bbbb::/64 to 2001:cc1e:befe:cccc::abcd/64
- E. TCP traffic from 2001:cc1e:bbbb::/64 to 2001:cc1e:befe:cccc:abcd/64

Answer: AD

NEW QUESTION 13

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 14

Which technology is required in the underlay to facilitate remote VTEP discovery?

- A. multicast
- B. VXLAN
- C. OSPF
- D. BGR

Answer: A

NEW QUESTION 16

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 17

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 20

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 23

On a Cisco Nexus 7000 Series router, which statement about HSRP and VRRP is true?

- A. When VDCs are in use, only VRRP is supported.
- B. HSRP and VRRP both use the same multicast IP address with different port numbers.
- C. HSRP has shorter default hold and hello times.
- D. The VRRP group IP address can be the same as the router-specific IP address

Answer: D

Explanation: VRRP allows for transparent failover at the first-hop IP router by configuring a group of routers to share a virtual IP address. VRRP selects a master router in that group to handle all packets for the virtual IP address. The remaining routers are in standby and take over if the master router fails. Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/unicast/configuration/guide/l3_cli_nxos/l3_vrrp.html

NEW QUESTION 25

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 30

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 32

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 35

Which protocol is used to exchange MAC address reachability between OTV-enabled switches?

- A. EIGRP
- B. IS-IS
- C. iBGP
- D. RIPv2

Answer: B

NEW QUESTION 40

Which command should you run to enforce SNMP message encryption for all SNMPv3 communications?

- A. snmp-server globalEnforceAuth
- B. snmp-server user Admin enforcePriv
- C. snmp-server globalEnforcePriv
- D. snmp-server user Admin enforceAuth

Answer: C

NEW QUESTION 45

You plan to implement the OSPF protocol within 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 not 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 default

Answer: DE

NEW QUESTION 46

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 48

A Cisco Nexus 2000 Series Fabric Extender is connected to two Cisco Nexus 5000 Series switches via a vPC link. After both Cisco Nexus 5000 Series switches lose power, only one switch is able to power back up. At this time, the Cisco Nexus 2000 Series Fabric Extender is not active and the vPC ports are unavailable to the network.

Which action will get the Cisco Nexus 2000 Series Fabric Extender active when only one Cisco Nexus 5000 Series switch is up and active?

- A. Move the line from the failed Cisco Nexus 5000 Series switch to the switch that is powered on, so the port channel forms automatically on the switch that is powered on.
- B. Shut down the peer link on the Cisco Nexus 5000 Series switch that is powered on.
- C. Configure reload restore or auto-recovery reload-delay on the Cisco Nexus 5000 Series switch that is powered on.
- D. Power off and on the Cisco Nexus 2000 Series Fabric Extender so that it can detect only one Cisco Nexus 5000 Series switch at power up.

Answer: C

Explanation: The vPC consistency check message is sent by the vPC peer link. The vPC consistency check cannot be performed when the peer link is lost. When the vPC peer link is lost, the operational secondary switch suspends all of its vPC member ports while the vPC member ports remain on the operational primary switch. If the vPC member ports on the primary switch flaps afterwards (for example, when the switch or server that connects to the vPC primary switch is reloaded), the ports remain down due to the vPC consistency check and you cannot add or bring up more vPCs.

Beginning with Cisco NX-OS Release 5.0(2)N2(1), the auto-recovery feature brings up the vPC links when one peer is down. This feature performs two operations:

- If both switches reload, and only one switch boots up, auto-recovery allows that switch to assume the role of the primary switch. The vPC links come up after a configurable period of time if

the vPC peer-link and the peer-keepalive fail to become operational within that time. If the peer-link comes up but the peer-keepalive does not come up, both peer switches keep the vPC links down. This feature is similar to the reload restore feature in Cisco NX-OS Release 5.0(2)N1(1) and earlier releases. The reload delay period can range from 240 to 3600 seconds.

- When you disable vPCs on a secondary vPC switch because of a peer-link failure and then the primary vPC switch fails, the secondary switch reenables the vPCs. In this scenario, the vPC waits for three consecutive keepalive failures before recovering the vPC links.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/n5k_vpc_ops.html

NEW QUESTION 53

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 56

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 hop

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 61

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 62

Which two protocols can be used to back up the configuration of a Cisco Nexus 5600 Series switch to a remote location? (Choose two.)

- A. NFS
- B. SCP
- C. SMB
- D. CIFS
- E. SFTP

Answer: BE

NEW QUESTION 66

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 70

Which security feature is only supported on the Cisco Nexus 7000 Series Switch?

- A. Dynamic ARP Inspection
- B. NAC
- C. CoPP
- D. IP source guard

Answer: B

NEW QUESTION 73

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 74

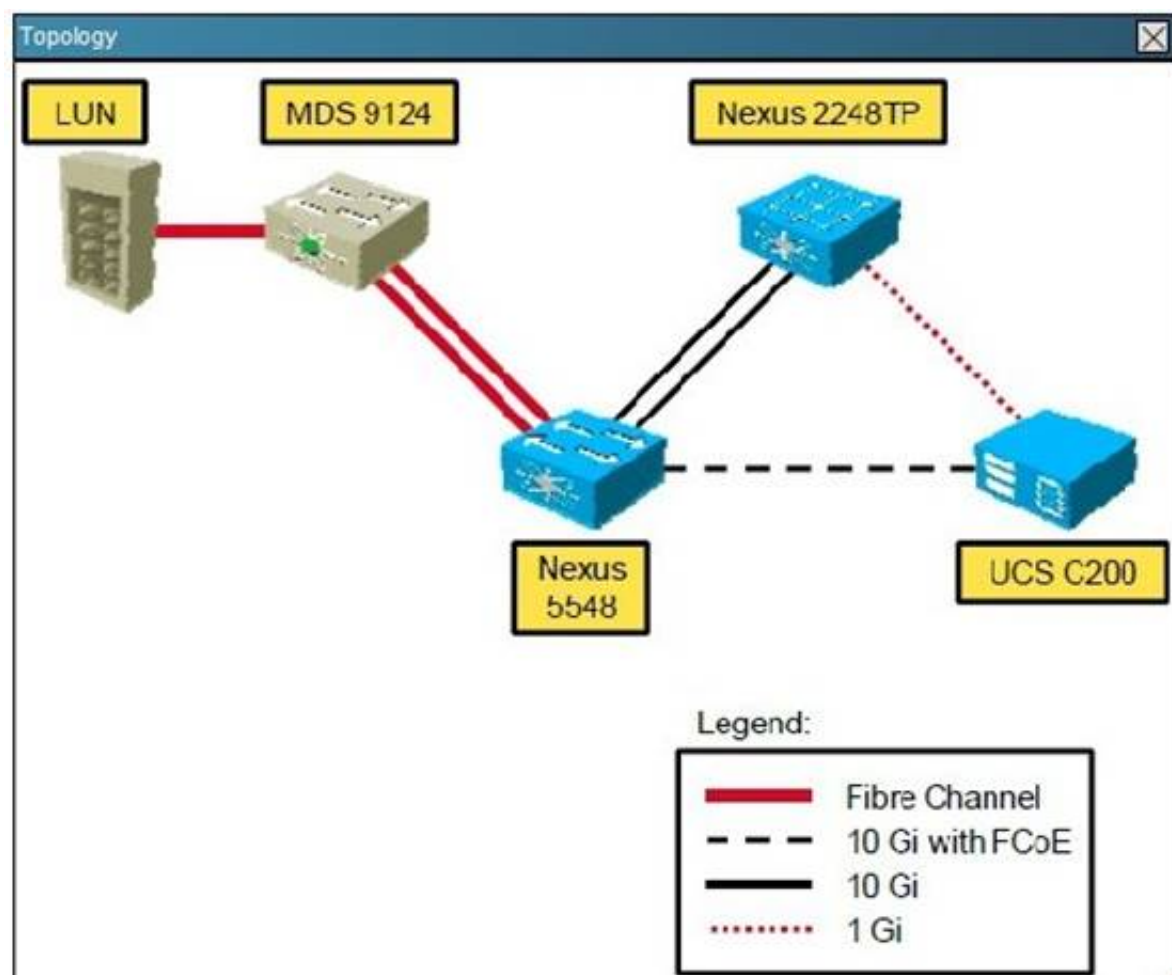
Ethernet interface 1/5 on Cisco Nexus 5548 is connected to Cisco UCS C220 rack server. What is the status of Ethernet 1/5 interface for FCoE functionality?

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.



- A. Interface reset on Ethernet 1/5 is preventing the FCoE connection from coming up
- B. MTU size of 1500 on Ethernet interface 1/5 needs to be changed for FCoE to come UP
- C. Cisco Nexus 5548 needs a layer 3 daughter card for FCoE to come UP on the Ethernet interface 1/5
- D. Ethernet interface 1/5 is operational for FCoE and the status is UP

Answer: D

NEW QUESTION 76

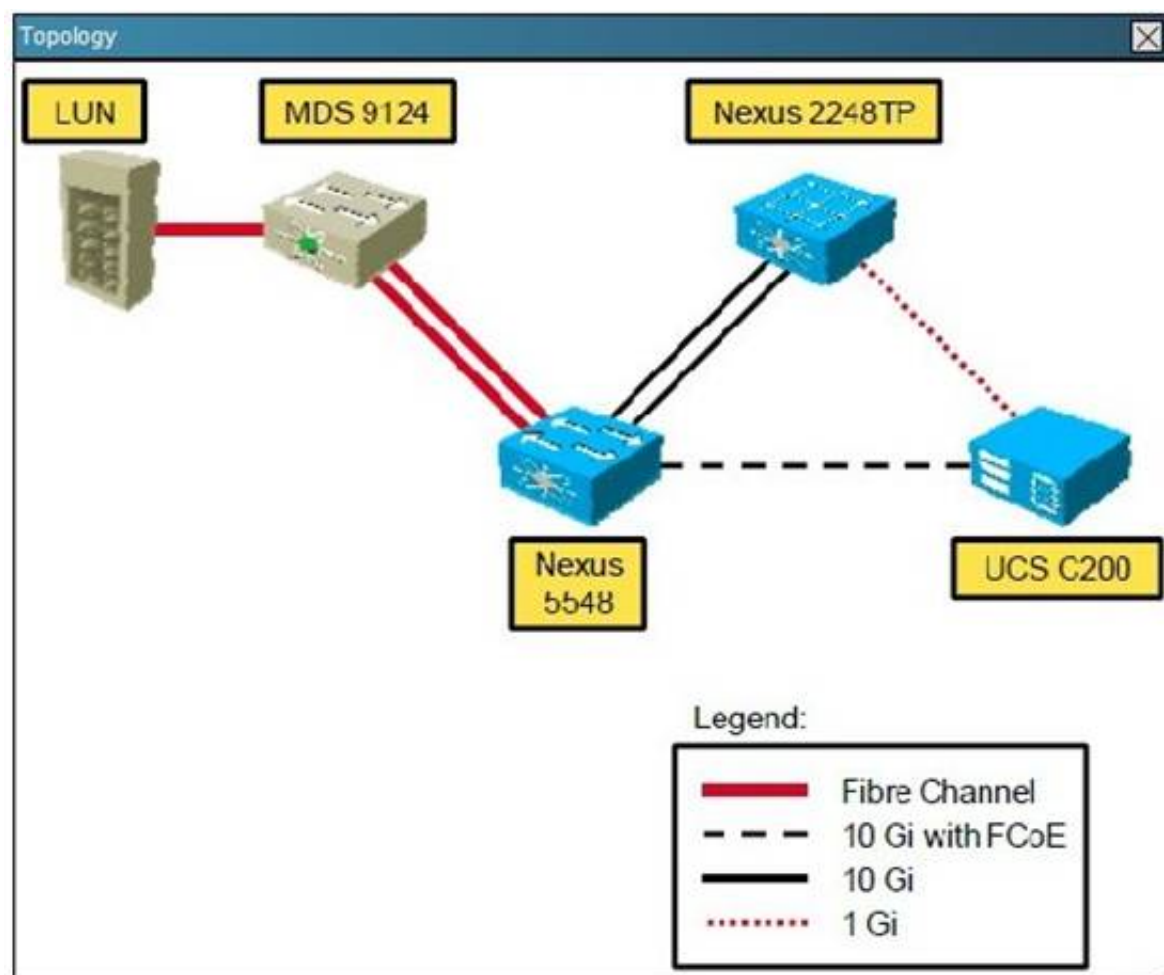
When configuring FCoE VLANs and Virtual Fiber Channel (vFC) Interfaces, what guidelines must be followed?

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.



- A. Each vFC interface must be bound to an FCoE-enabled Ethernet or EtherChannel interface or to the MAC address of a remotely connected adapter
- B. Each FC interface must be bound to an FCoE-enabled Ethernet or EtherChannel interface or to the MAC address of a remotely connected adapter
- C. Each vFC interface must be bound to an FC enabled Ethernet or EtherChannel interface or to the MAC address of a remotely connected adapter
- D. Each vFC interface must be bound to an FCoE-enabled vFC or EtherChannel interface or to the MAC address of a remotely connected adapter

Answer: A

NEW QUESTION 77

Which action limits the maximum number of routes that are allowed in the routing table?

- A. Use a BGP filter.
- B. Use only static routes.
- C. Use the maximum routes command inside address family.
- D. Use a route map to filter route

Answer: C

NEW QUESTION 78

You have two Fibre Channel switches that are connected via EISL. You discover that the fabrics are isolated. What are two possible causes of the fabric isolation? (Choose two.)

- A. mismatched SAN port channel group modes
- B. mismatched VSANs on either switch
- C. mismatched active zone set databases
- D. mismatched line card types
- E. mismatched switch series

Answer: BC

NEW QUESTION 83

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 88

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 less

Answer: DE

NEW QUESTION 89

Which implicit rules are applied to all IPv6 ACLs?

- A. deny icmp any any nd-na deny icmp any any nd-ns permit icmp any any router-advertisement permit icmp any any router-solicitation deny ipv6 any any
- B. deny icmp any any nd-na log deny icmp any any nd-ns log deny ipv6 any any log
- C. deny icmp any any router-advertisement log deny icmp any any router-solicitation log deny ipv6 any any log
- D. permit icmp any any nd-na permit icmp any any nd-ns permit icmp any any router-advertisement permit icmp any any router-solicitation deny ipv6 any any

Answer: D

NEW QUESTION 92

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 94

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 99

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 103

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.

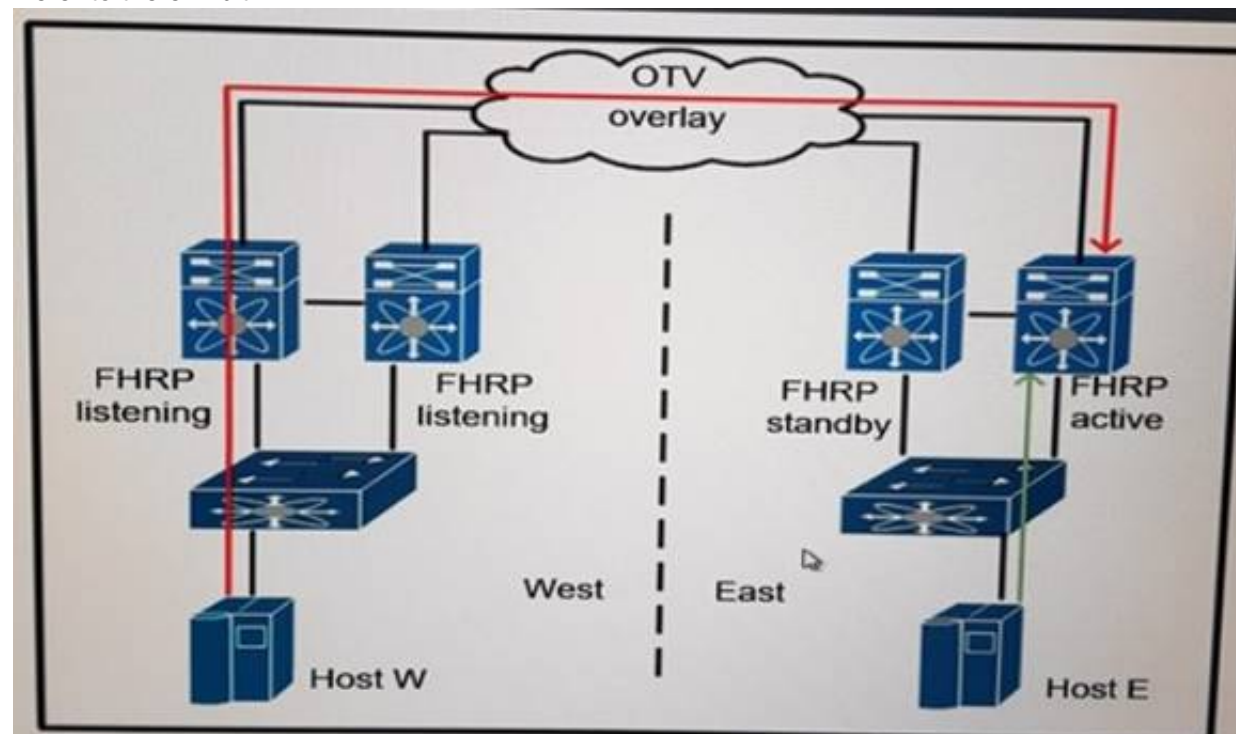
You must have an active service contract for the device that you are configuring.

[https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/](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)

[6x/b_6k_System_Mgmt_Config_6x/b_6k_System_Mgmt_Config_602N11_chapter_01010.html#con_1058068](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 105

Refer to the exhibit.



You have a suboptimal outbound routing issue in the datacenter. Which two options you can use to resolve the issue? (Choose two)

- A. On the OTV VDC, configure an OTV MAC route filter that prevents the virtual FHRP MAC address from being announced to other sites.
- B. On the OTV edge devices, configure a VACL that prevents FHRP hellos from being forwarded on the overlay
- C. Configure the same FHRP priority on all the OTV edge devices in both sites
- D. Remove the VLAN from which FHRP hellos are sent from the extended VLAN range
- E. On the OTV edge devices, configure an IP ACL that prevents hosts from reaching the FHRP master router on the other site

Answer: AB

NEW QUESTION 109

You have a Cisco MDS switch that uses port channel. You must ensure that frames between the source and the destination follow the same links for a specific flow. Subsequent flows can use a different link, which load-balancing method do you use?

- A. Source-destination-ip
- B. Source-destination-port
- C. Flow
- D. Source id-destination id-oxid

Answer: C

NEW QUESTION 111

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

- A. Switch(config-if)# ip pim ssm default
- B. switch(config-if)# ip pim sparse-mode
- C. Switch(config-if)# ip pim sparse-mode
- D. Switch(config-if)# 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 115

You have a Cisco Nexus 7700 Series switch on which the graceful which the graceful restart feature is disable, you are configuring BGP, which command should you run to enable the graceful restart feature?

- A. Switch(config-router)# graceful-restart restart-time
- B. Switch(config-router)** graceful-restart grace-period
- C. Switch(config-router)ff graceful-restart-helper
- D. Switch(config-router)» graceful-restart

Answer: D

NEW QUESTION 117

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 is 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 122

Refer to the exhibit.

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

Nexus_7k(config-if)# switchport 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 be 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 violation, the interface is error disabled
- E. Port security on the Ethernet 2/1 interface uses the sticky method for MAC address learning all traffic continues to be forwarded

Answer: AC

NEW QUESTION 127

Fibre Channel IDs are dynamically assigned to which object?

- A. FSPF packets
- B. FEXs
- C. WWPNs
- D. VSANs
- E. Cisco Fabric Services packets

Answer: D

NEW QUESTION 129

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 same on all of the Fibre Channel switches in the fabric
- D. Must be unique on all the Fibre Channel switches in the fabric

Answer: A

NEW QUESTION 134

Refer to the exhibit.

```
Switch(config)# snmp-server user all enforcePriv
```

Which option is the expected outcome on the configured switch?

- A. The switch enforces SNMP message encryption for all users
- B. The switch responds with an authorization error for any SNMPv3 PDU requests that use a security level parameter.
- C. SNMP requires encryption for all incoming requests
- D. The switch enforces SNMP message encryption for the user all

Answer: D

NEW QUESTION 138

Refer to the exhibit.

```
N7k-1# show runing-config fabricpath
...
Fabricpath switch-id 11
Vpc domain 11
Fabricpath switch-id 1100
```

You have a Cisco Nexus 7010 switch named N7k-1

Which command set should you run on a neighboring Cisco Nexus 7010 switch to establish a vPC+ environment that includes N7k-1?

- A. fabricpath switch-id 11 vpc domain 11 fabricpath switch-id 1100
- B. fabricpath switch-id 12 vpc domain 11 fabricpath switch-id 1100
- C. fabricpath switch-id 11 vpc domain 11 fabricpath switch-id 1200
- D. fabricpath switch-id 11 vpc domain 12 fabricpath switch-id 1101

Answer: B

NEW QUESTION 140

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 142

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:

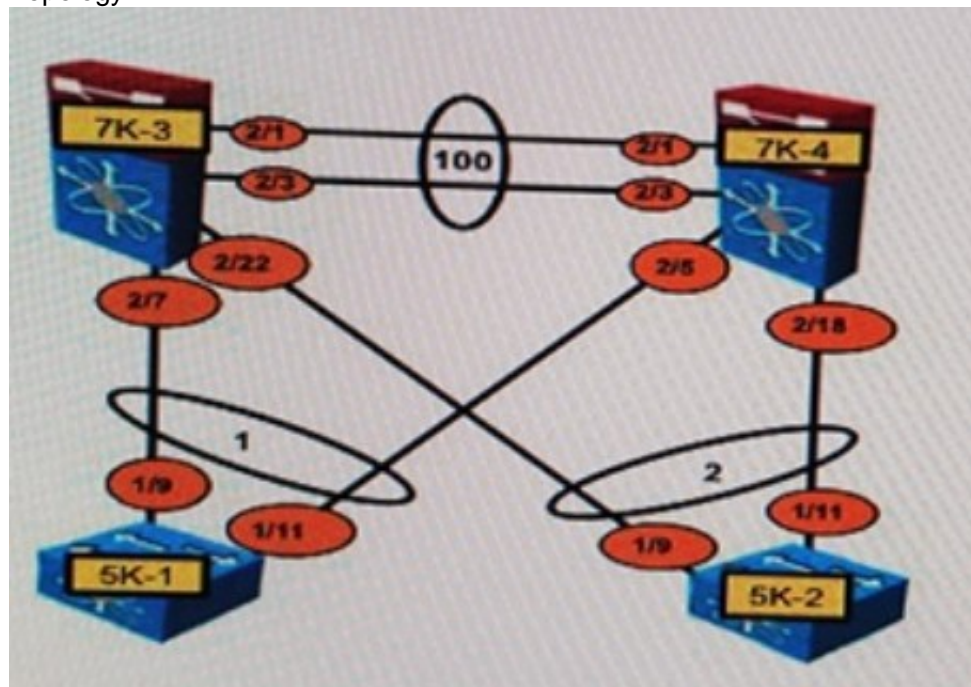
Enter NX-OS commands on 7K-3 and 7K-4 to verity network operation and answer four multiplechoice questions

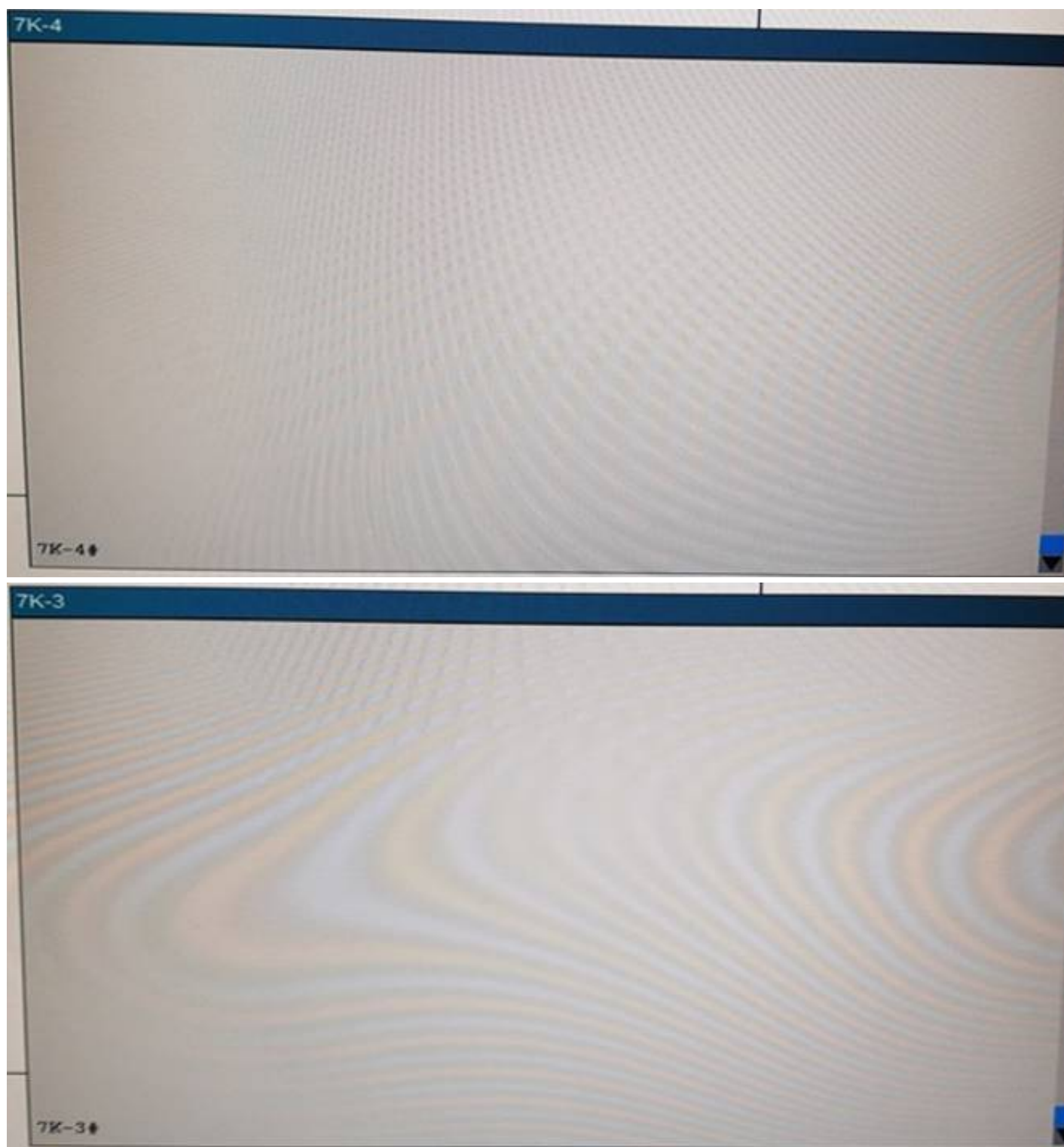
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.

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:





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 147

Refer to Exhibit.



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 occur

Answer: D

NEW QUESTION 152

When configuring HSRP on IPv6-enabled interfaces, which two commands are required? (Choose two)

- A. SwitchA(config-if)# hsrp version 2
- B. SwitchA(config-if)# hsrp <group-number> ipv6
- C. SwitchA(config-if)# key 6
- D. SwitchA(config-if)# standby 6 preempt
- E. SwitchA(config-if)#priority <level>

Answer: AB

Explanation: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-sy/fhp-15-sybook/ip6-fhrp-hsrp.html#topic_BC3E645261274DE6B46AA7F2A8E70048

NEW QUESTION 156

Refer to the exhibit.

```
switch(config)# spanning-tree port type edge
bpdupfilter default
switch(config)# interface ethernet 1/1-24
switch(config-if)# spanning-tree bpduguard enable
```

Which two descriptions of the switch are true? (Choose two)

- A. It shuts down any edge port that receives a BPDU
- B. It shuts down any port that receives a BPDU
- C. If a port in the range of e1/1-24 receives a BPDU, the port is moved to the errdisable state.
- D. It prevents edge devices from sending or receiving BPDUs globally
- E. It prevents edge devices from sending or receiving BPDUs on e1/1-24 only

Answer: CD

NEW QUESTION 161

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 ACL 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_macacis.pdf

NEW QUESTION 164

DRAG DROP

Drag and drop the types of spanning tree ports from the left onto the correct descriptions on the right

edge	supports 802.1Q to a host immediately
edge trunk	moves through the regular STP transitions
network	transitions to the forwarding state immediately
normal	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 167

Refer to the exhibit.

```
SW3# rollback running-config checkpoint
user-checkpoint-1 atomic
```

What is the result?

- A. The switch implements a rollback file that is named running-config
- B. The switch implements a rollback and skips any errors
- C. The switch implements a rollback that stops if an error occurs
- D. The switch implements a rollback only if no errors occur

Answer: D

NEW QUESTION 168

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 169

Refer to the exhibit. What is the result of the configuration?

```
mac access-list mac-01
  permit 11c0.0000.0000 0000.ffff.ffff any

vlan access-map acl mac
  match mac address mac-01
  action forward
vlan filter acl-mac vlan-list 100-120
```

- A. A MAC address of 11c0.adaa.3213 is denied.
- B. The MAC ACL is applied to VLANs 10-120.
- C. The MAC ACL denies a MAC address of 1122.2847.4591 on VLAN 101.
- D. A MAC address of 11c0.adaa.3213 is permitte

Answer: D

NEW QUESTION 170

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 172

Assuming hello PDU authentication has been disabled, which command re-enables the feature on a FabricPath interface?

- A. switch (config-if) # fabricpath isis authentication-type cleartext
- B. switch (config-if) # fabricpath isis authentication-type md5
- C. switch (config-if) # fabricpath isis authentication check
- D. switch (config-if) # fabricpath isis hello-interval

Answer: C

NEW QUESTION 176

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 181

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 186

Which two events automatically generate Cisco NX OS checkpoints? (Choose two)

- A. The license of a feature expires
- B. The NX-OS software is upgraded.
- C. The switch reboots.
- D. An enabled feature is disabled by using the no feature command
- E. A system crash occur

Answer: AD

Explanation: The Cisco NX-OS software automatically generates system checkpoints to help you avoid a loss of configuration information. System checkpoints are generated by the following events:

Disabling an enabled feature with the no feature command

Removing an instance of a Layer 3 protocol, such as with the no router bgp command or the no ip pim sparse-mode command

License expiration of a feature Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/systemmanagement/guide/b_Cisco_Nexus_7000_Series_NXOS_System_Management_Configuration_Guide-RI/configuring_rollback.html

NEW QUESTION 189

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 193

You have a Switch that is operating NPV mode. The interfaces of the switch use which port type to connect to the core network?

- A. TE Port
- B. NP Port
- C. E Port
- D. F Port

Answer: B

NEW QUESTION 195

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 197

You enable the HSRP feature on a Cisco Nexus 7000 Series switch. You must ensure that the switch manages packets that are sent to the local vPC MAC address, remote vPC MAC address, and HSRP virtual MAC address. Which command should you run?

- A. Peer-gateway
- B. hsrp preempt
- C. map-server
- D. peer-switch

Answer: A

NEW QUESTION 198

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 203

Which statement about RADIUS configuration distribution using Cisco Fabric Services on a Cisco Nexus 7000 Series Switch is true?

- A. Cisco Fabric Services does not distribute the RADIUS server group configuration or server and global keys.
- B. Enabling Cisco Fabric Services causes the existing RADIUS configuration on your Cisco NX-OS device to be immediately distributed.
- C. When the RADIUS configuration is being simultaneously changed on more than one device in a Cisco Fabric Services region, the most recent changes will take precedence.
- D. Only the Cisco NX-OS device with the lowest IP address in the Cisco Fabric Services region can lock the RADIUS configuration.

Answer: A

Explanation: CFS does not distribute the RADIUS server group configuration or server and global keys. The keys are unique to the Cisco NX-OS device and are not shared with other Cisco NX-OS devices. Reference:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/6_x/nxos/security/configuration/guide/b_Cisco_Nexus_7000_NXOS_Security_Configuration_Guide_Release_6-x/b_Cisco_Nexus_7000_NXOS_Security_Configuration_Guide_Release_6-x_chapter_0101.html

NEW QUESTION 207

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 210

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 214

Which GLBP load-balancing algorithm ensures that a client is always mapped to the same VMAC address?

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

Answer: D

Explanation: Host dependent—GLBP uses the MAC address of the host to determine which virtual MAC address to direct the host to use. This algorithm guarantees that a host gets the same virtual MAC address if the number of virtual forwarders does not change.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/unicast/configuration/guide/l3_cli_nxos/l3_glb主.html

NEW QUESTION 215

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	<div style="background-color: #f9a825; padding: 5px; text-align: center;">Access</div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div>
Power over Ethernet	
Fast, deterministic convergence	
routing summarization	
uses Rapid PVST+ for Layer 2 spanned VLANs	<div style="background-color: #f9a825; padding: 5px; text-align: center;">Aggregation</div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div>
802.1X and port security	
feature-rich environment	
default gateway redundancy by using an FHRP	<div style="background-color: #f9a825; padding: 5px; text-align: center;">Core</div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div> <div style="background-color: #fff9c4; height: 20px; margin: 2px;"></div>

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 216

Which statement is true if password-strength checking is enabled?

- A. Short, easy-to-decipher passwords will be rejected.
- B. The strength of existing passwords will be checked.
- C. Special characters, such as the dollar sign (\$) or the percent sign (%), will not be allowed.
- D. Passwords become case-sensitiv

Answer: A

Explanation: If a password is trivial (such as a short, easy-to-decipher password), the cisco NX_OS software will reject your password configuration if password-strength checking is enabled. Be sure to configure a strong password. Passwords are case sensitive.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/security/configuration/guide/b_Cisco_Nexus_9000_Series_NXOS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NXOS_Security_Configuration_Guide_7x_chapter_01000.pdf

NEW QUESTION 219

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 222

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_guide/b_GUI_VMware_VM-FEX_UCSM_Configuration_Guide/b_GUI_VMware_VMFEX_UCSM_Configuration_Guide_chapter_010.html

NEW QUESTION 225

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/sysmgmt/DCNM-SAN/sysmgmt_dcnm/sysmgmt_overview.html#wp1051962

NEW QUESTION 229

Which option is a restriction of the unified ports on the Cisco UCS 6200 Series Fabric Interconnect when connecting to the unified fabric network?

- A. Direct FC connections are not supported to Cisco MDS switches
- B. The FCoE or Fibre Channel port allocations must be contiguous on the 6200.
- C. 10-G Fibre Channel ports only use SFP+ interfaces.
- D. vPC is not supported on the Ethernet port

Answer: B

Explanation: When you configure the links between the Cisco UCS 2200 Series FEX and a Cisco UCS 6200 series fabric interconnect in fabric port channel mode, the available VIF namespace on the adapter varies depending on where the FEX uplinks are connected to the fabric interconnect ports.

Inside the 6248 fabric interconnect there are six sets of eight contiguous ports, with each set of ports managed by a single chip. When uplinks are connected such that all of the uplinks from an FEX are connected to a set of ports managed by a single chip, Cisco UCS Manager maximizes the number of VIFs used in service profiles deployed on the blades in the chassis. If uplink connections from an IOM are distributed across ports managed by separate chips, the VIF count is decreased.

Reference:

http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/hw/6200-installguide/6200_HIG/6200_HIG_chapter_01.html

NEW QUESTION 232

The Connectivity Management Processor monitors the active supervisor module on a Cisco Nexus 7000 switch and will reboot the device in the event of a lights-out management issue. However, which option includes features that provide similar benefits in the absence of the Connectivity Management Processor?

- A. high-availability functionality from features such as vPC and NSF
- B. traditional system connectivity models like SNMP, GUI, or SSH
- C. Cisco FabricPath
- D. VDC failover

Answer: A

Explanation: vPC uses the vPC peer-keepalive link to run hello messages that are used to detect a dual-active scenario. A Gigabit Ethernet port can be used to carry the peer-keepalive messages. A dedicated VRF is recommended to isolate these control messages from common data packets. When an out-of-band network infrastructure is present, the management interfaces of the Cisco Nexus 7000 supervisor could be also used to carry keep-alive connectivity using the dedicated management VRF. When the vPC peer-link is no longer detected, a dual-active situation occurs, and the system disables all vPC port channel member on the "secondary" vPC peer (lower vPC role priority value). Also SVI interfaces associated to a vPC VLAN are suspended on the secondary switch. As a result, in this condition only the "primary" vPC peer actively forwards traffic on the vPC VLANs. Multiple peerkeepalive links can be used to increase resiliency of the dual-active detection mechanism.

Both the Cisco Catalyst 6500 and the Cisco Nexus 7000 offer a variety of high-availability features. Some of the primary features to highlight are In Service Software Upgrade (ISSU), Stateful Switchover (SSO), and Nonstop Forwarding (NSF). The operation and the behavior of these features are unique to the respective platform and can be independently executed without affecting the interoperability between the two platforms.

Reference:

http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6500-seriesswitches/white_paper_c11_589890.html

NEW QUESTION 233

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	Cisco Nexus 5000 Series Switches
Offers complete routing and core services	Cisco Nexus 7000 Series Switches
Includes native Fibre Channel interfaces	Cisco Nexus 2000 Series Fabric Extenders
Provides I/O consolidation	Cisco MDS 9500 Series Multilayer Directors
A virtual machine-aware software switch	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	Includes native Fibre Channel interfaces
Offers complete routing and core services	Offers complete routing and core services
Includes native Fibre Channel interfaces	Provides I/O consolidation
Provides I/O consolidation	Supports the SAN infrastructure
A virtual machine-aware software switch	A virtual machine-aware software switch

NEW QUESTION 238

Which statement about Cisco FabricPath is true?

- A. It is the best solution for interconnecting multiple data centers.
- B. It optimizes STP throughout the Layer 2 network.
- C. It is a simplified extension of Layer 3 networks across a single data center.
- D. The Cisco FabricPath domain appears as a single STP bridge, where each edge port uses the same MAC address.

Answer: D

Explanation: To have a loop-free topology for the CE/FabricPath hybrid network, the FabricPath network automatically displays as a single bridge to all connected CE devices. The STP domains do not cross into the FabricPath network. If multiple STP domains are defined, BPDUs and topology change notifications (TCNs) are localized to the domain. If a connected STP domain is multihomed to the FabricPath domain, a TCN must be able to reach to all devices in the STP domain through the FabricPath domain. As a result, the TCN is sent to the FabricPath domain through the IS-IS protocol data unit (PDU) by default.

Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1/n5k_ops_fabricpath.html

NEW QUESTION 242

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-series/switches/configuration_guide_c07-543563.html

NEW QUESTION 243

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 247

Which function does the graceful restart feature allow a Cisco Nexus 7000 Series router to perform?

- A. Perform a rapid route convergence.
- B. Initialize a standby supervisor transparently when one is present.
- C. Remain in the data forwarding path through a process restart.
- D. Maintain a management connection throughout a router restart

Answer: C

Explanation: Graceful Restart and Non Stop Routing both allow for the forwarding of data packets to continue along known routes while the routing protocol information is being restored (in the case of Graceful Restart) or refreshed (in the case of Non Stop Routing) following a processor switchover. When Graceful Restart is used, peer networking devices are informed, via protocol extensions prior to the event, of the SSO capable routers ability to perform graceful restart. The peer device must have the

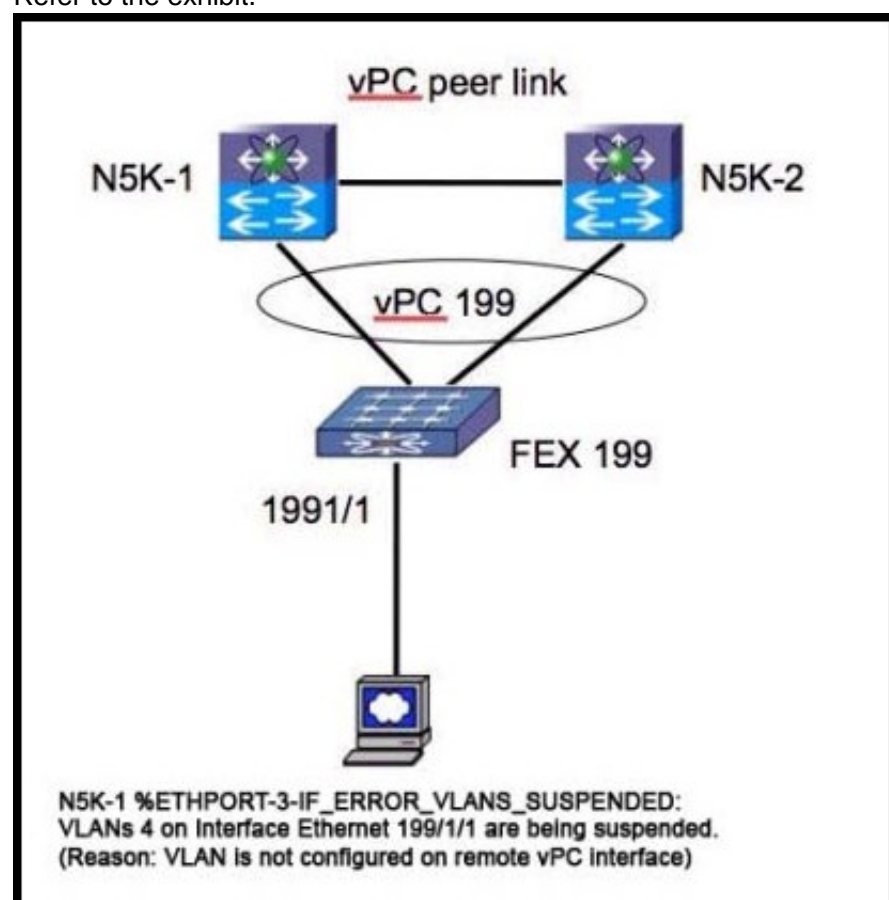
ability to understand this messaging. When a switchover occurs, the peer will continue to forward to the switching over router as instructed by the GR process for each particular protocol, even though in most cases the peering relationship needs to be rebuilt. Essentially, the peer router will give the switching over router a "grace" period to re-establish the neighbor relationship, while continuing to forward to the routes from that peer.

Reference:

http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/highavailability/solution_overview_c22-487228.html

NEW QUESTION 252

Refer to the exhibit.



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 199/1/1 so 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 257

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 manually.

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 259

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 260

On a Cisco Nexus7000 switches what is true regarding Cisco FabricPath requirements?

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

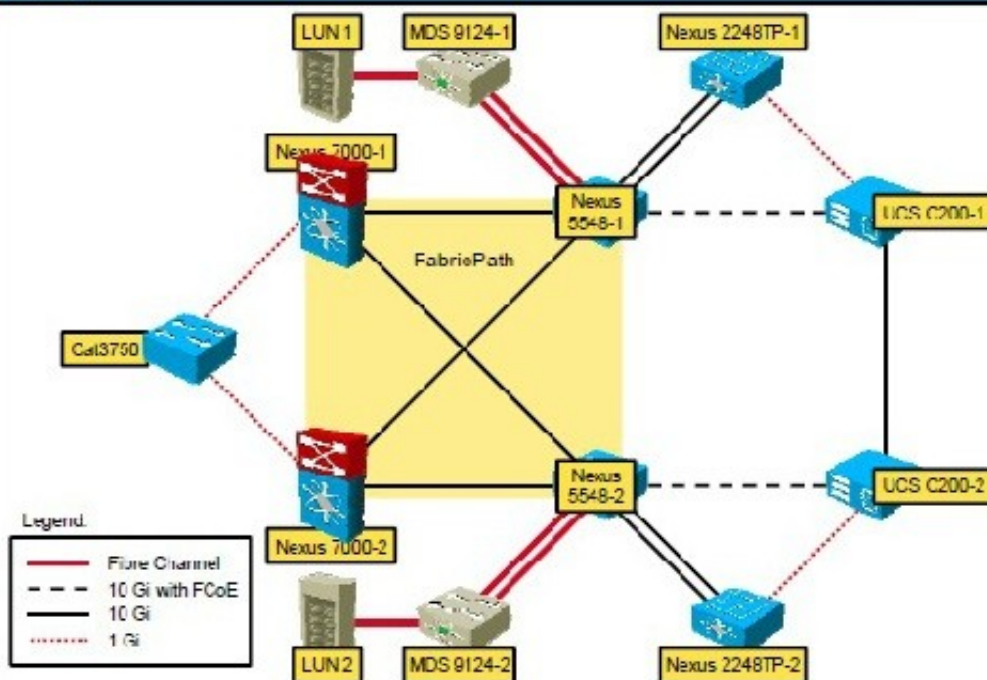


Exhibit 1

```
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 1r 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. Ensure that you have installed the Enhanced Layer 2 license and that you have installed an F Series module
- B. Ensure that you have installed the Enhanced Layer 2 license and that you have installed an M Series module
- C. Ensure that you have installed the Enhanced Layer 3 license and that you have installed an M Series module
- D. Ensure that you have installed the Scalable Feature License license and that you have installed an F Series module

Answer: A

Explanation: FabricPath switching has the following prerequisites:

- You should have a working knowledge of Classical Ethernet Layer 2 functioning.
- You must install the FabricPath feature set on the default and nondefault VDC before you enable FabricPath on the switch. See Configuring Feature Set for FabricPath for information on installing the FabricPath feature set.
- You are logged onto the device.
- Ensure that you have installed the Enhanced Layer 2 license.
- You are in the correct virtual device context (VDC). A VDC is a logical representation of a set of system resources. You can use the switchto vdc command with a VDC number.
- You are working on the F Series module. Reference:

http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nxos/fabricpath/configuration/guide/fp_switching.html

NEW QUESTION 263

Customer has configured fabricpath allocate-delay to 600. What is the effect of this?

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.

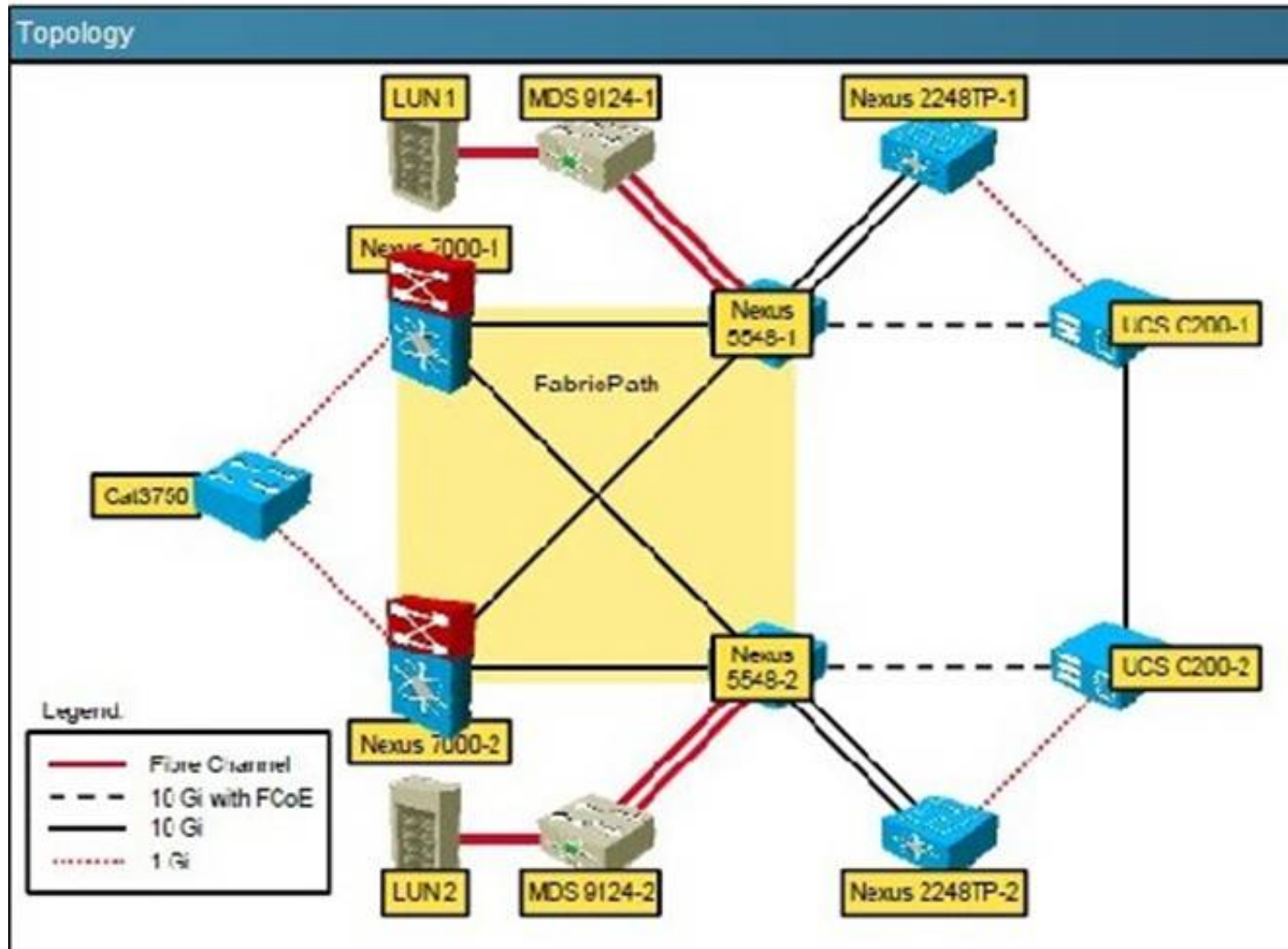


Exhibit 1

```
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 1r 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. The allocate-delay is the time for FP to go into forwarding state
- B. It specifies the time delay for a transitioned value to be propagated throughout the network
- C. It specifies the time delay for a link bringup to detect conflicts
- D. The allocate-delay is the time delay for a new resource to be propagated throughout the network

Answer: D

Explanation: Specifies the time delay for a new resource to be propagated throughout the network. Reference:
http://www.cisco.com/web/techdoc/dc/reference/cli/nxos/commands/fpath/fabricpath_timers.html

NEW QUESTION 268

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

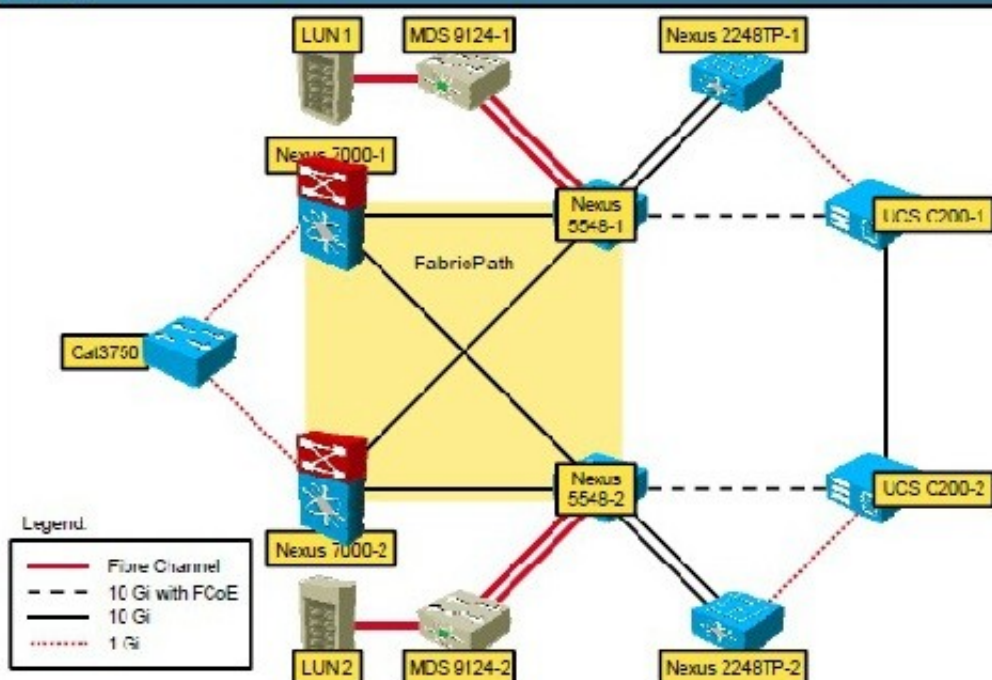


Exhibit 1

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

Nexus/000-1#
```

Exhibit 2

```
Nexus7000-1# show feature-set services fabricpath
u2rib
drap
isis_l2mp
3 services 1r 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#(conf'g)# 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 272

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/qcfcnav.html

NEW QUESTION 277

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 281

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 Cisco-developed 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 283

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 285

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 defilects 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 286

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](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 290

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 294

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 295

Which feature enables NIV?

- A. EHV
- B. vPC
- C. Cisco FabricPath
- D. Cisco OTV
- E. VN-Tag

Answer: A

Explanation: EHV is the feature that enables NIV.

NEW QUESTION 298

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 303

Which statement about core-edge SAN topology is true?

- A. Converged FCoE links connect the core and edge MDS switches.
- B. The SAN core connects to the network aggregation layer.
- C. Separate links with the same I/O are used for SAN and LAN traffic.
- D. Storage devices are accessed via FCoE over the LAN network

Answer: B

Explanation: The Aggregation layer of the data center provides connectivity for the Access layer switches in the server farm, and aggregates them into a smaller number of interfaces to be connected into the Core layer. In most data center environments, the Aggregation layer is the transition point between the purely Layer 3 routed Core layer, and the Layer 2-switched Access layer. 802.1Q trunks extend the server farm VLANs between Access and Aggregation layers. The Aggregation layer also provides a common connection point to insert services into the data flows between clients and servers, or between tiers of servers in a multi-tier application.

NEW QUESTION 306

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 307

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 312

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 nondisruptive

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 316

DRAG DROP

Drag the description on the left to the most appropriate FCoE protocol or feature on the right.

Drag the description on the left to the most appropriate FCoE protocol or feature on the right.

processes FLOGIs	ENodes
replaces lower Fibre Channel layers with unified fabric I/O	FIP
control plane protocol used to establish virtual links	FCF
Fibre Channel interfaces in the form of VN Ports	FCoE

Answer:

Explanation: ENODES: During FLOGI or FDISC, the ENode advertises the addressing modes it supports. If the FC switch supports an addressing mode that the ENode uses, the virtual link can be established, and the devices can communicate.

FIP: FIP is the set of control plane functions that enable discovery of FCoE-capable devices across FCoE passthrough switches and establishment of legal combinations of virtual links.

FCF: FCoE Initialization Protocol (FIP) is the FCoE control protocol responsible for establishing and maintaining Fibre Channel virtual links between pairs of FCoE devices (ENodes or FCFs). During the virtual link establishment phase, FIP first discovers FCoE VLANs and remote virtual FC interfaces; then it performs virtual link initialization functions (fabric login [FLOGI] and fabric discovery [FDISC], or exchange link parameters [ELP]) similar to their native Fibre Channel equivalents. After the virtual link is established, Fibre Channel payloads can be exchanged on the virtual link, and FIP remains in the background to perform virtual link maintenance functions; it continuously verifies reachability between the two virtual FC interfaces on the Ethernet network, and it offers primitives to delete the virtual link in response to administrative actions to that effect. This document does not describe the virtual link maintenance functions of FIP.

NEW QUESTION 319

DRAG DROP

VSANs and SAN Zoning have similar security goals, but also have different qualities. Drag the characteristic on the left to the appropriate column heading (VSAN or Zoning) on the right.

VSANs and SAN Zoning have similar security goals, but also have different qualities. Drag the characteristic on the left to the appropriate column heading (VSAN or Zoning) on the right.

Limits unicast, multicast, and broadcast traffic	VSANs
Endpoints can only belong to one	
Shared routing and name space	
Limits unicast traffic	
Separate routing and name space	Zoning
Endpoints can belong to multiple	
Configured at fabric edge	
Encompass the entire fabric	

Answer:

Explanation:

VSAN Characteristic	Zone Characteristic
VSANs equal SANs with routing, naming, and zoning protocols.	Routing, naming, and zoning protocols are not available on a per-zone basis.
VSANs limit unicast, multicast, and broadcast traffic.	Zones limit unicast traffic.
Membership is typically defined using the VSAN ID to F ports.	Membership is typically defined by the pWWN.
An HBA or a storage device can belong only to a single VSAN (the VSAN associated with the F port).	An HBA or storage device can belong to multiple zones.
VSANs enforce membership at each E port, source port, and destination port.	Zones enforce membership only at the source and destination ports.
VSANs are defined for larger environments (storage service providers).	Zones are defined for a set of initiators and targets not visible outside the zone.
VSANs encompass the entire fabric.	Zones are configured at the fabric edge.

NEW QUESTION 320

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 324

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 328

Which Cisco NX-OS feature allows transparent Layer 2 extension between sites?

- A. FabricPath
- B. ETV
- C. OTV
- D. vPC
- E. LISP
- F. TrustSec

Answer: C

NEW QUESTION 329

Which two elements must be configured correctly for Cisco TrustSec Fibre Channel Link Encryption to work on a Cisco MDS 9000 Series Switch? (Choose two.)

- A. AES-GMAC
- B. key
- C. salt
- D. AAA
- E. group

Answer: BC

NEW QUESTION 334

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 337

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 338

Which task must be done before a zone set takes effect?

- A. Add a member to the zone.
- B. Enter the exit config t command.
- C. Enter the copy running-config startup-config command.
- D. Enter the zoneset activate name <zone-name> vsan <vsan-#> comman

Answer: D

NEW QUESTION 342

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 343

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 344

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 349

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 351

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 353

Which two advantages does FabricPath have over Spanning Tree in implementing a loop-free network topology design? (Choose two.)

- A. Blocked links can be brought in to service if active links fail.
- B. Convergence times are faster.
- C. Multipath forwarding is supported for unicast and multicast Layer 2 and Layer 3 traffic.
- D. Unknown unicast addresses are flooded in through the originating port

Answer: BC

NEW QUESTION 357

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 360

When creating a VDC on a Cisco Nexus 7000 switch, which command in the VDC designates that only 10 port channels can be created in that VDC?

- A. allocate resource port-channel 10
- B. limit-resource port-channel minimum 0 maximum 10
- C. allow-resource port-channel maximum 10
- D. port-channel maximum 10

Answer: B

NEW QUESTION 365

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 367

Which example creates an Embedded Event Manager policy allowing the CLI command to execute, and triggers an SNMP notification when a user enters configuration mode?

A)

```
event manager applet TRACK_CONFIG
event cli match "conf t"
action 1.0 snmp-trap strdata "Configuration change"
action 2.0 event-default
```

B)

```
event manager applet TRACK_CONFIG
event cli match "conf t"
action 1.0 snmp-trap strdata "Configuration change"
```

C)

```
event manager applet TRACK_CONFIG
event cli "conf t"
action 1.0 snmp-trap strdata "Configuration change"
```

D)

```
event manager applet TRACK_CONFIG
event command "conf t"
action 1.0 snmp-trap strdata "Configuration change"
action 2.0 event-default
```

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

Answer: A

NEW QUESTION 369

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 manually.

Answer: D

NEW QUESTION 374

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 375

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 378

DRAG DROP

Drag and drop the optional OSPF parameters from the left onto the correct functions on the right.

area range	creates a type 5 LSA
default information originate	converts type 7 LSAs to type 5
default metric	summarizes routes between areas
route map	sets all redistributed routes to the same metric
translate	filters select external routes flooded throughout the NSSA

Answer:

Explanation:

default metric
route map
area range
translate
default information originate

NEW QUESTION 383

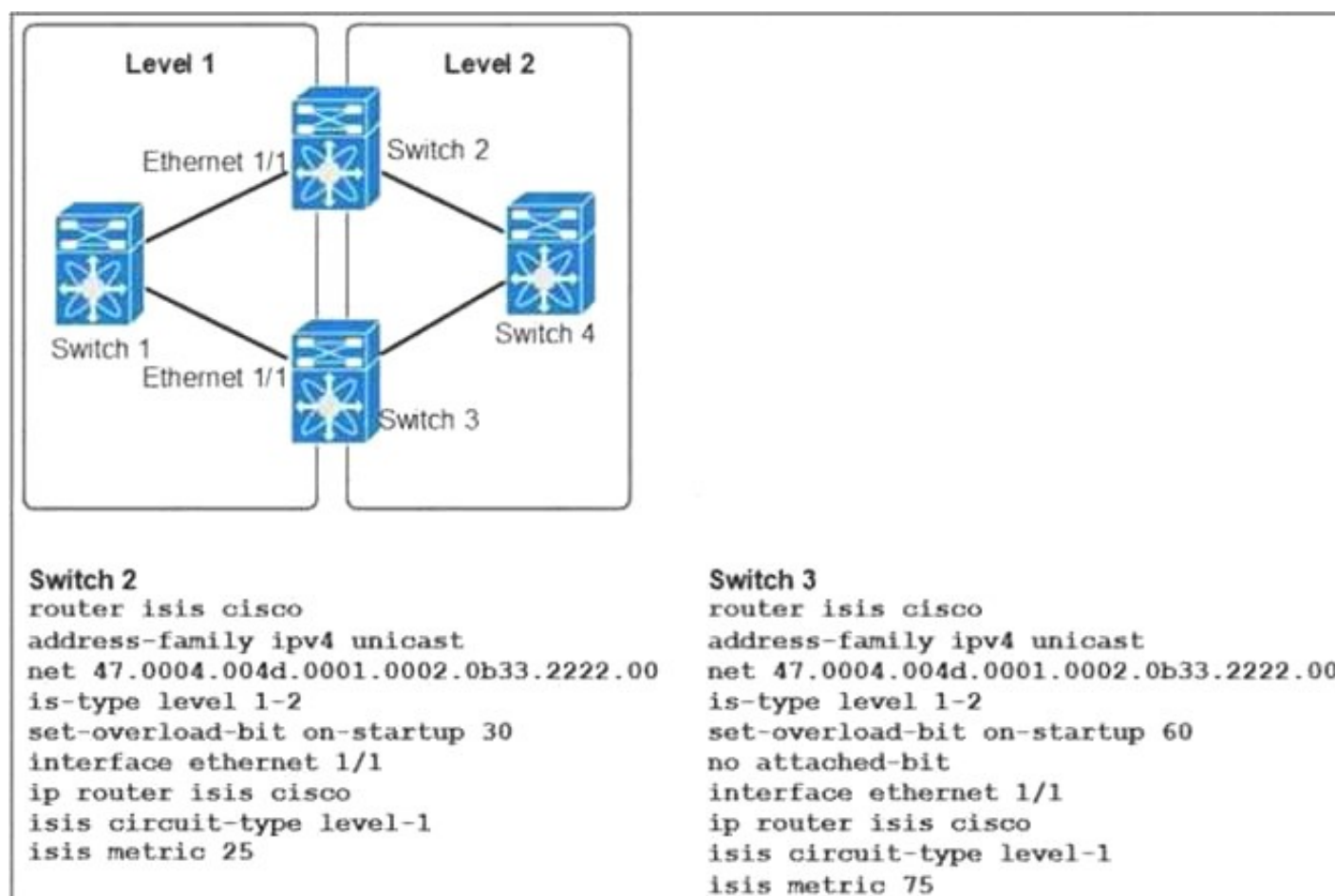
You are implementing a Cisco Fabric Path network. Which statement accurately describes the VNSegment feature?

- A. The VN-Segment feature must be enabled on all leaf switches.
- B. Up to 16,000 VN segments are supported on a leaf switch.
- C. The VN-Segment feature must be enabled on all switches.
- D. The VN-Segment tag is added to VN-Segment edge port

Answer: A

NEW QUESTION 384

Refer to the exhibit.



How does Switch 1 route traffic to the Level 2 network?

- A. Switch 1 prefers Switch 2 as the path to the Level 2 network.
- B. Switch 1 load balances traffic destined for Level 2 between Switch 2 and Switch 3.
- C. Switch 1 sends 75 percent of the traffic destined for Level 2 to Switch 3 and 25 percent to Switch 2.
- D. Switch 1 prefers Switch 3 as the path to the Level 2 network.

Answer: A

NEW QUESTION 387

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 390

Refer to the exhibit.

```

NEXUS# configure terminal
NEXUS(config)# interface eth 1/23
NEXUS(config-if)# no shut
NEXUS(config-if)# exit
NEXUS(config)# no monitor session 1
NEXUS(config)# monitor session 1 rx
NEXUS(config-erspan-src)# source interface ethernet 1/1-3 rx
NEXUS(config-erspan-src)# erspan-id 1
NEXUS(config-erspan-src)# ip ttl 10
NEXUS(config-erspan-src)# vrf default
NEXUS(config-erspan-src)# destination ip 1.1.1.2
NEXUS(config-erspan-src)# no shut
NEXUS(config-erspan-src)# exit
  
```

Which result of implementing the configuration is true?

- A. It creates a bidirectional ERSPAN session.
- B. It sets the IP TTL to 5.
- C. It sets the IP DSCP to 42.
- D. It creates a unidirectional ERSPAN session.

Answer: D

NEW QUESTION 391

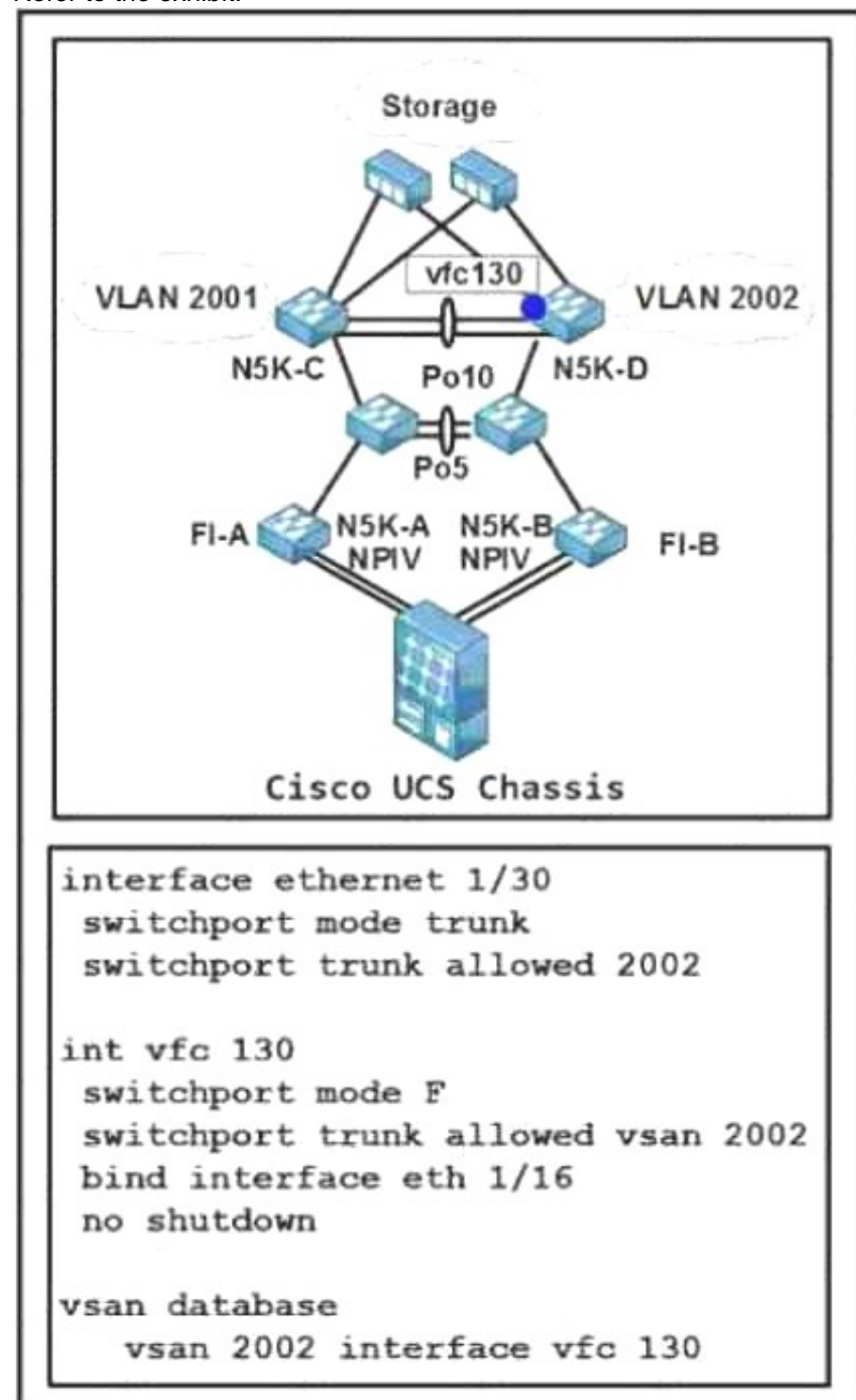
Which technology facilitates a nondisruptive upgrade on a Cisco Nexus 5000 Series Switch?

- A. VSS
- B. ITD
- C. VDC
- D. vPC

Answer: D

NEW QUESTION 395

Refer to the exhibit.



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 interface.

Answer: C

NEW QUESTION 398

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.	Step 1
Apply the flow monitor to a source interface.	Step 2
Define a flow monitor based on the flow record.	Step 3
Define a flow record by specifying keys and fields to the flow.	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 399

Which description of Cisco zoning is true?

- A. With enhanced zoning a single configuration session locks the entire fabric to implement a change.
- 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 402

Which issue does DCB address?

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

Answer: C

NEW QUESTION 407

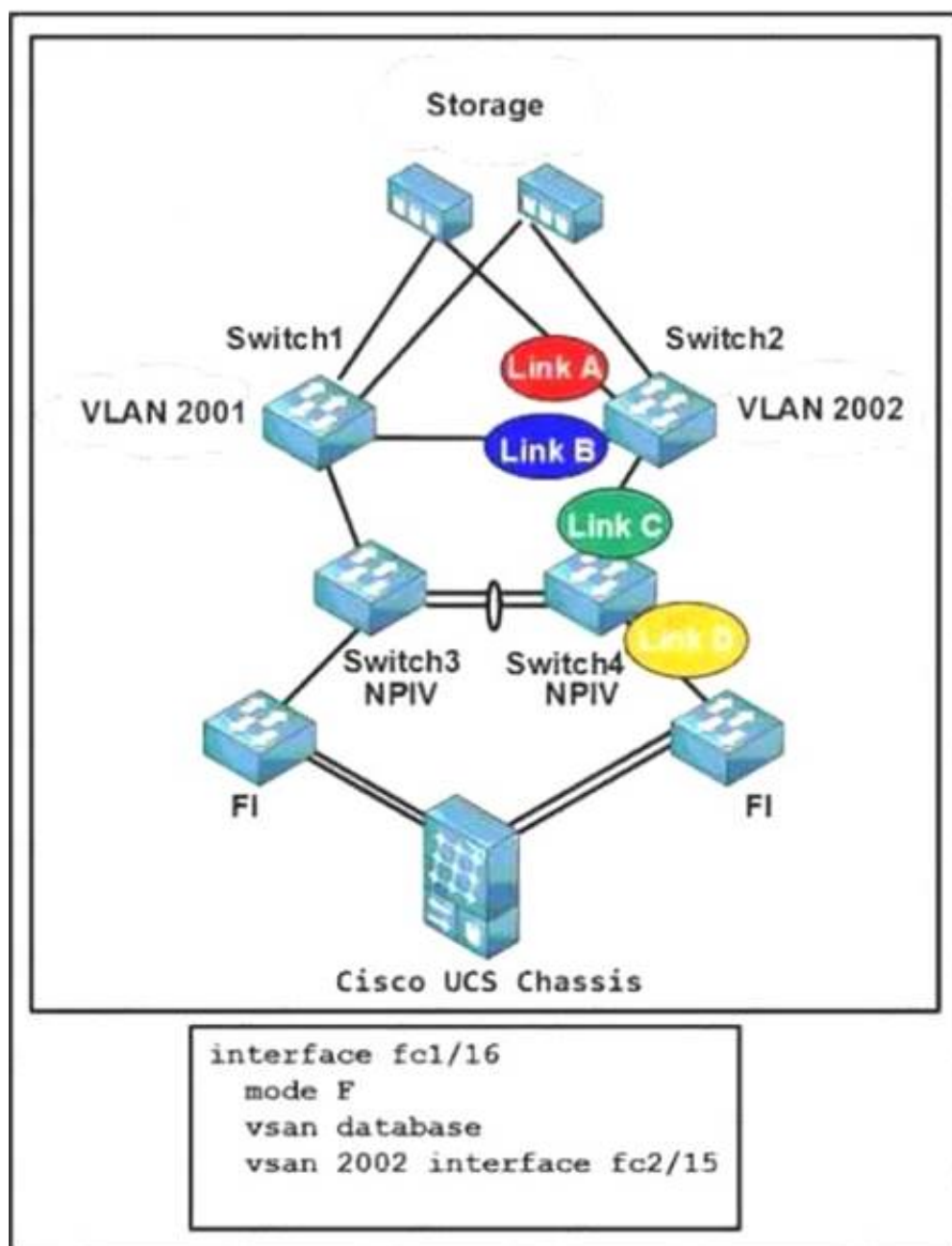
You have multiple OTV edge devices in each OTV site. Which configuration prevents an end-to-end STP loop?

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

Answer: B

NEW QUESTION 411

Refer to the exhibit.



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 416

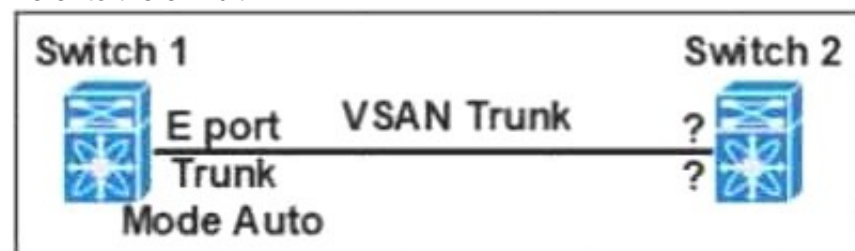
Which statement about implementing fabric binding is true?

- A. Cisco Fabric Services must be enabled on a switch to distribute configuration information
- B. Activation must be performed globally
- C. Activation must be performed on a per-VSAN basis
- D. Activation must be performed globally on a switch

Answer: C

NEW QUESTION 420

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 423

Refer to the exhibit.

```
fcoe fcmmap 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
```

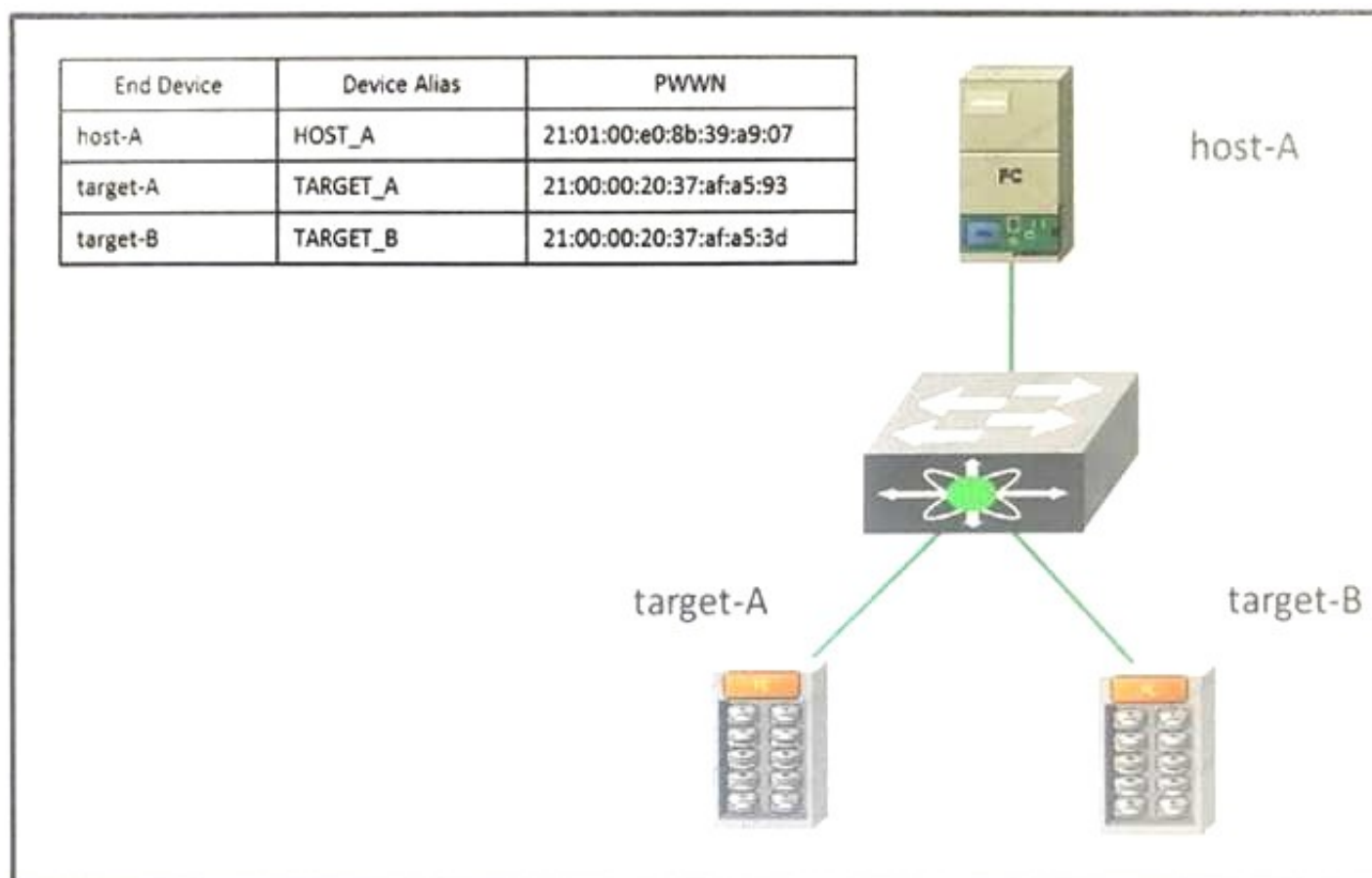
Which fabric -provided MAC address does the switch use when connecting to an end node on VSAN 9?

- A. 5e.ff.01.0e.fc.00
- B. 0e.fc.00.5e.ff.01
- C. 40.15.18.0e.fc.00
- D. 40.15.18.5e.ff.01

Answer: C

NEW QUESTION 425

Refer to the exhibit.



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)

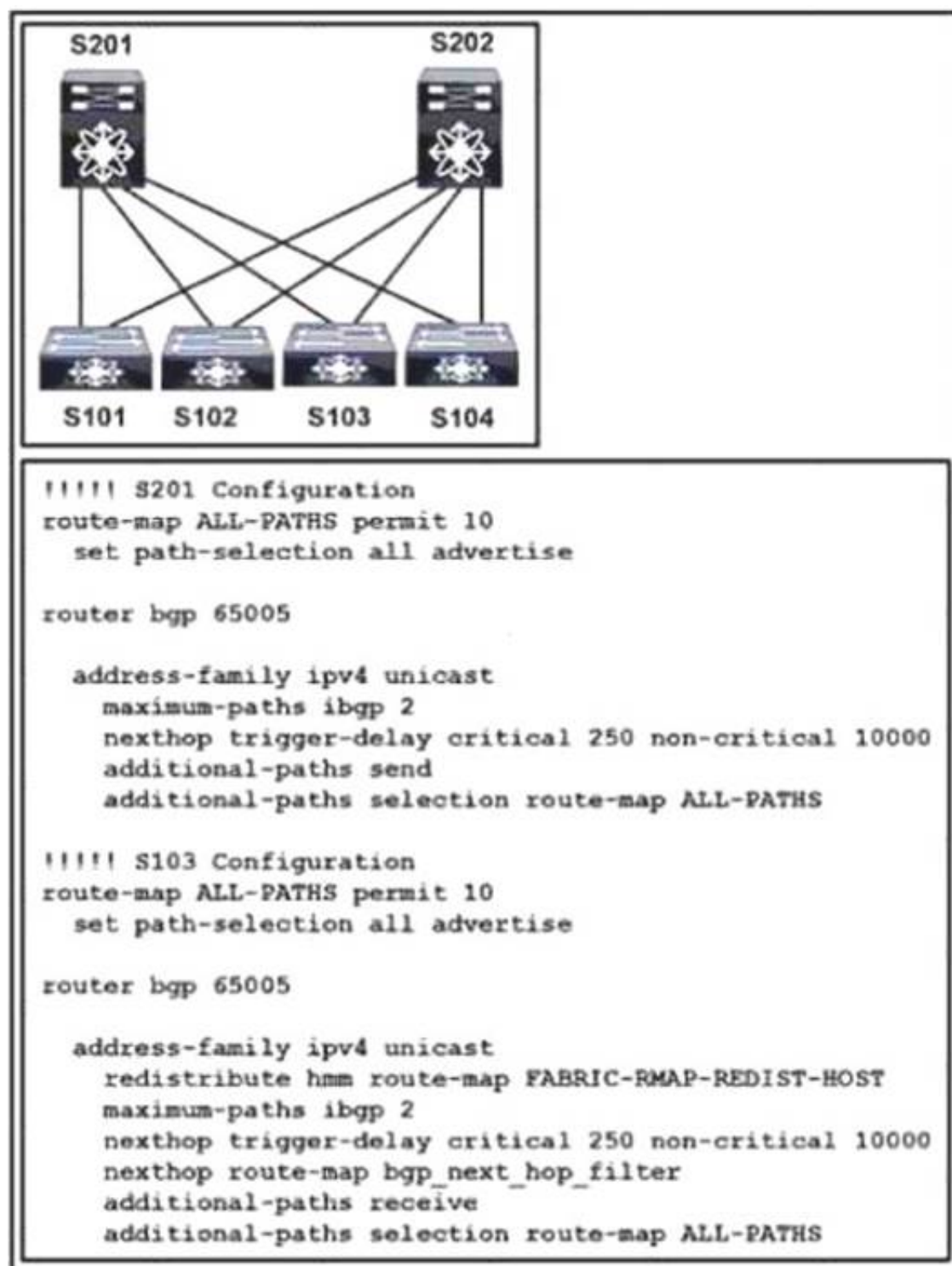
```
MDS9K# conf t
MDS9K(config)# device-alias database
MDS9K(config-device-alias-db)# device-alias name HOST_A pwwn 21:01:00:e0:8b:39:a9:07
MDS9K(config-device-alias-db)# device-alias name TARGET_A pwwn21:00:00:20:37:af:a5:93
MDS9K(config-device-alias-db)# device-alias name TARGET_B pwwn 21:00:00:20:37:af:a5:3d
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 427

Refer to the exhibit.



Which result does the configuration show?

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

Answer: D

NEW QUESTION 431

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 reflects 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 436

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 438

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 442

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 446

Refer to the exhibit.

```
switch# configure terminal
switch(config)# install feature-set fabricpath
switch(config)# feature-set fabricpath
switch(config)# feature vn-segment-vlan-based

switch# configure terminal
switch(config)# vlan 90
switch(config-vlan)# mode fabricpath
switch(config-vlan)# vn-segment 4096
```

Which type of domain does the configuration create?

- A. Layer 3 local
- B. Layer 3 global
- C. Layer 2 local
- D. Layer 2 global

Answer: C

NEW QUESTION 447

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 450

You have a Fibre Channel switch with one of its ports connected to a host. The host remains in the initializing state. What is the most likely cause of this issue?

- A. The FLOGI packet was dropped somewhere on the data path
- B. The ELP process failed after the FLOGI occurred

- C. The host is not powered on
- D. The vFC interface on the host is configured to use an incorrect mode

Answer: A

NEW QUESTION 451

Refer to the exhibit.

```
scheduler job name nexus-core-a-cfg
cli var name timestamp $(TIMESTAMP) ;copy running-config
bootflash:/$ (SWITCHNAME) -cfg.$ (timestamp) ;copy
bootflash:/$ (SWITCHNAME) -cfg.$ (timestamp)
tftp://10.10.10.1/ vrf admin
scheduler schedule name daily
job name nexus-core-a-cfg
time daily 1:00 switch
```

What is the result of running the command?

- A. The running config is backed up to the TFTP server by using a file named nexus-core-a-cfg.
- B. The default VRF is used to establish a connection to the TFTP server.
- C. The startup config file is backed up.
- D. A timestamp is included in the name of the file that is backed up to the TFTP server

Answer: A

NEW QUESTION 456

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 458

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 300-165 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 300-165 Product From:

<https://www.2passeasy.com/dumps/300-165/>

Money Back Guarantee

300-165 Practice Exam Features:

- * 300-165 Questions and Answers Updated Frequently
- * 300-165 Practice Questions Verified by Expert Senior Certified Staff
- * 300-165 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 300-165 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year