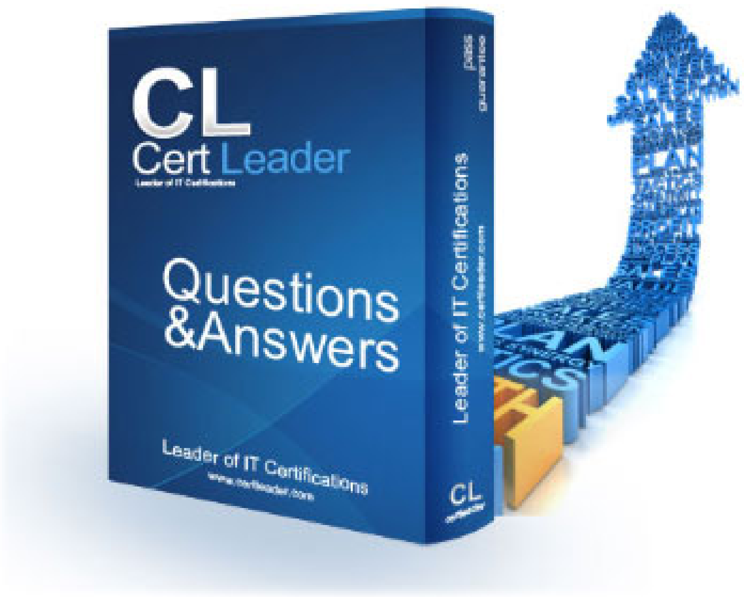
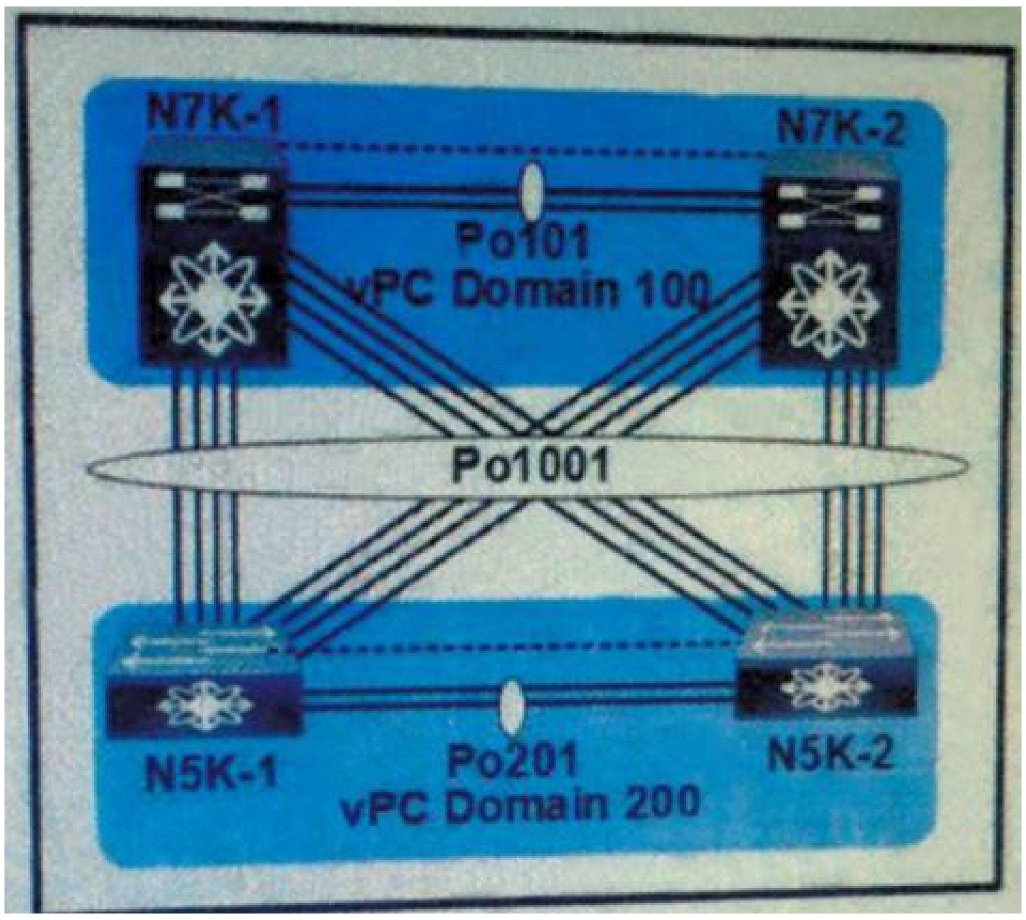
300-165 Dumps

DCII Implementing Cisco Data Center Infrastructure (DCII)

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



NEW QUESTION 1
Refer to the exhibit.

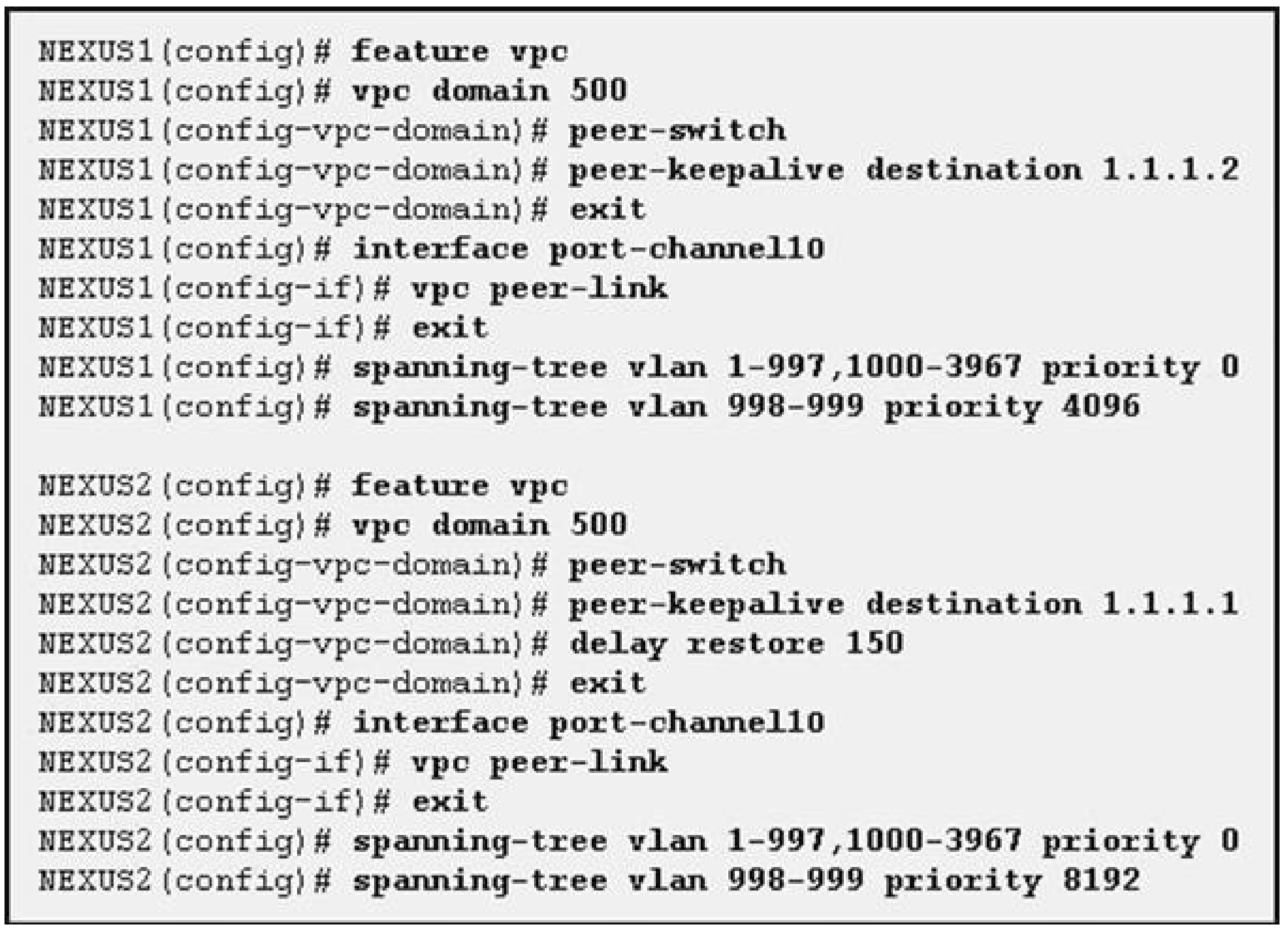


You must ensure that the vPC Domain 100 controls the LACP Po1001 link. Which feature do you configure?

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

Answer: C

NEW QUESTION 2
Refer to the exhibit.



```
NEXUS1(config)# feature vpc
NEXUS1(config)# vpc domain 500
NEXUS1(config-vpc-domain)# peer-switch
NEXUS1(config-vpc-domain)# peer-keepalive destination 1.1.1.2
NEXUS1(config-vpc-domain)# exit
NEXUS1(config)# interface port-channel10
NEXUS1(config-if)# vpc peer-link
NEXUS1(config-if)# exit
NEXUS1(config)# spanning-tree vlan 1-997,1000-3967 priority 0
NEXUS1(config)# spanning-tree vlan 998-999 priority 4096

NEXUS2(config)# feature vpc
NEXUS2(config)# vpc domain 500
NEXUS2(config-vpc-domain)# peer-switch
NEXUS2(config-vpc-domain)# peer-keepalive destination 1.1.1.1
NEXUS2(config-vpc-domain)# delay restore 150
NEXUS2(config-vpc-domain)# exit
NEXUS2(config)# interface port-channel10
NEXUS2(config-if)# vpc peer-link
NEXUS2(config-if)# exit
NEXUS2(config)# spanning-tree vlan 1-997,1000-3967 priority 0
NEXUS2(config)# spanning-tree vlan 998-999 priority 8192
```

You configure two switches named NEXUS1 and NEXUS2. Which two results of implementing the configuration are true? (Choose two.)

A. NEXUS1 is the spanning-tree root for VLAN 100.
B. NEXUS1 is the spanning-tree root for VLAN 998.
C. NEXUS2 is the spanning-tree root for VLAN 100.
D. Both switches are the spanning-tree root for VLAN 998.
E. Both switches are the spanning-tree root for VLAN 100.

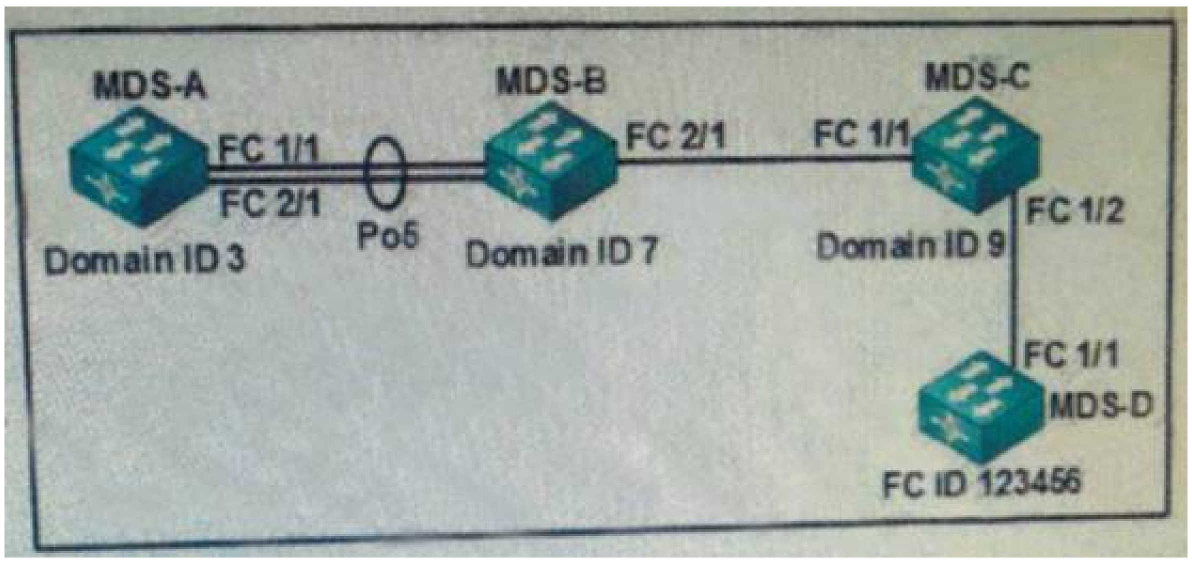
Answer: BE

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.



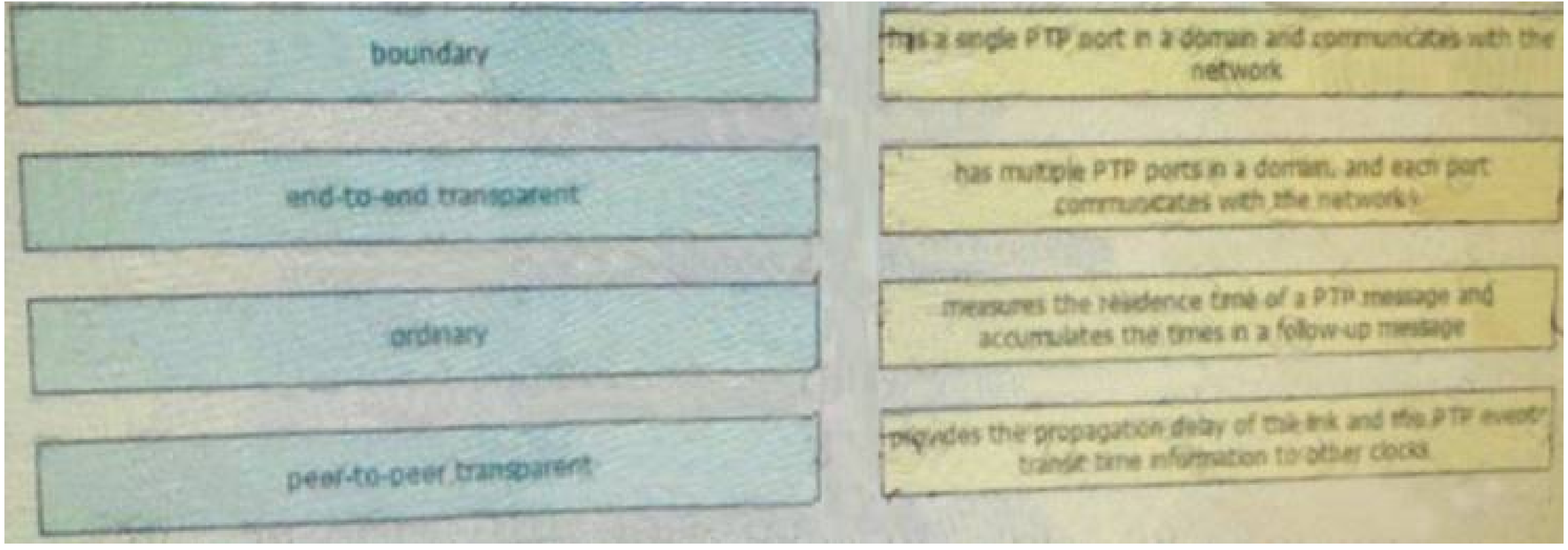
Which command configures a static FSPF route from MDS-A to FC ID 123456?

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

end-to-end transparent

ordinary

peer-to-peer transparent

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

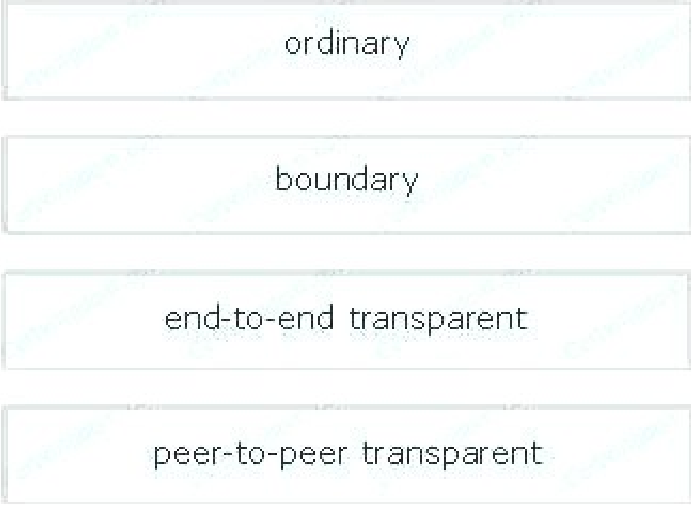
has multiple PTP ports in a domain, and each port communicates with the network

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

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

Answer:

Explanation:



ordinary

boundary

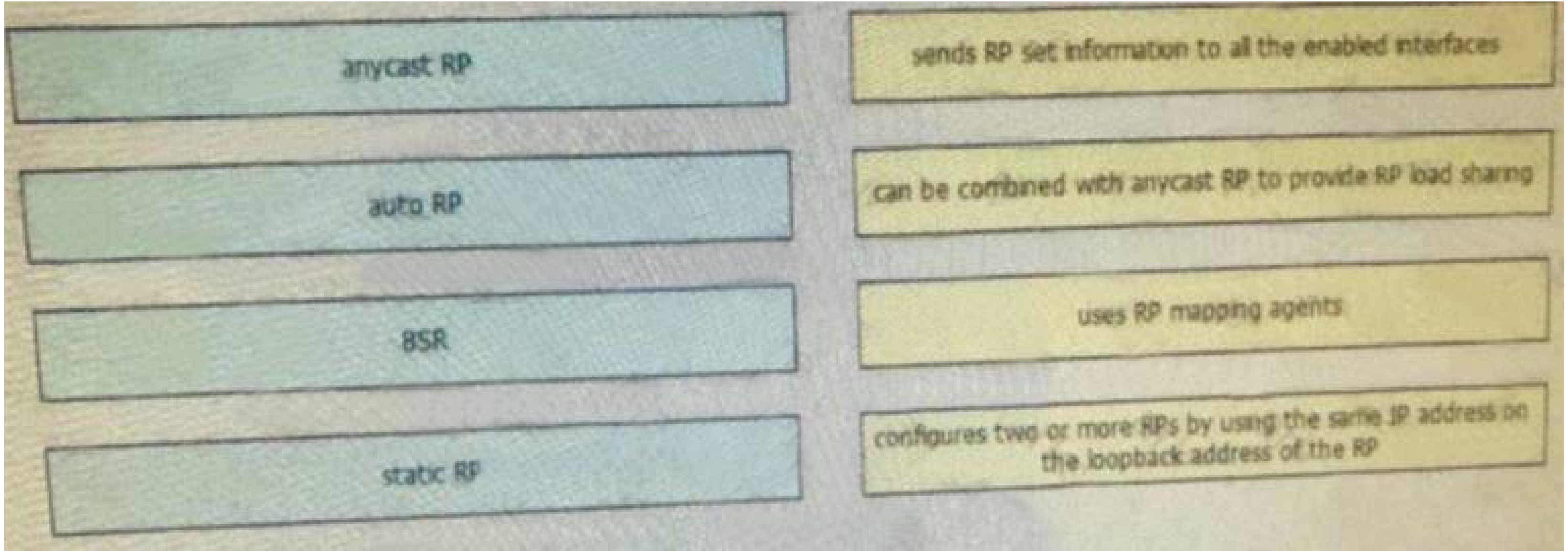
end-to-end transparent

peer-to-peer transparent

NEW QUESTION 6

DRAG DROP

Drag and drop the RP mechanisms on the left to their correct redundancy implementations on the right.



anycast RP

auto RP

BSR

static RP

sends RP set information to all the enabled interfaces

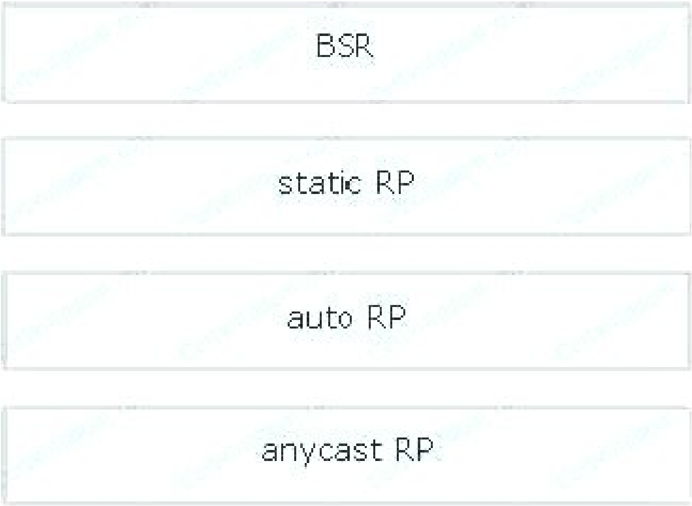
can be combined with anycast RP to provide RP load sharing

uses RP mapping agents

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

Answer:

Explanation:



BSR

static RP

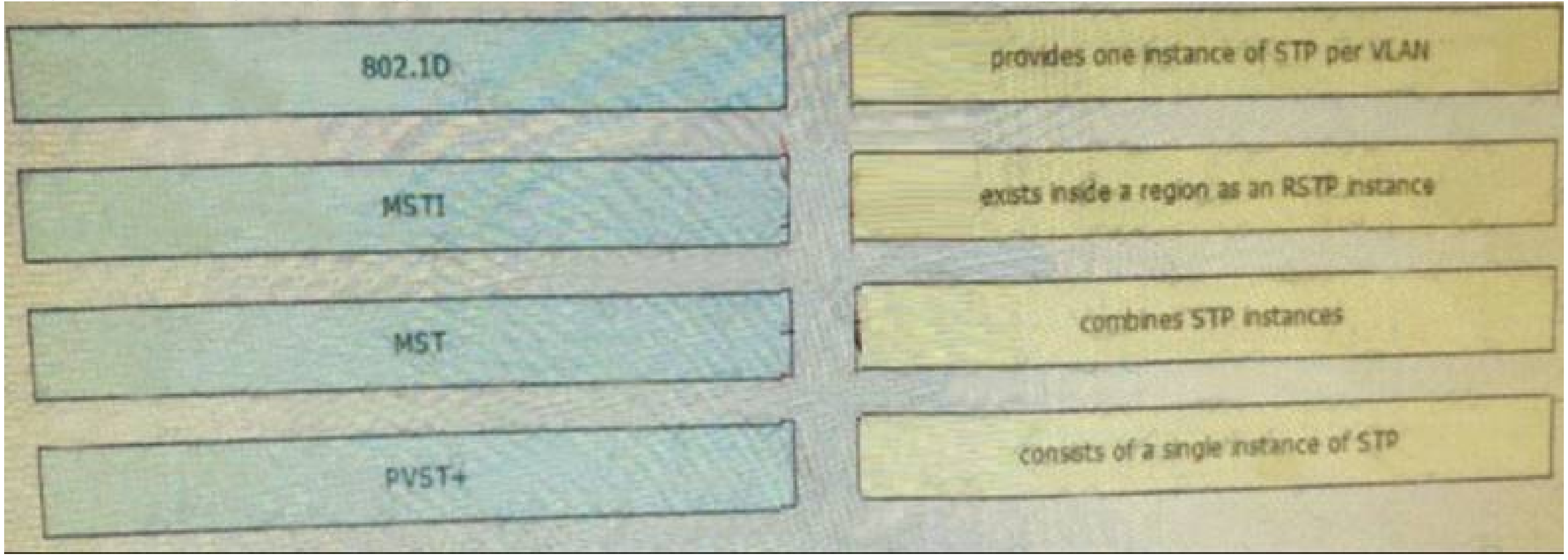
auto RP

anycast RP

NEW QUESTION 7

DRAG DROP

Drag and drop the spanning tree types on the left to their correct descriptions on the right



802.1D

MSTI

MST

PVST+

provides one instance of STP per VLAN

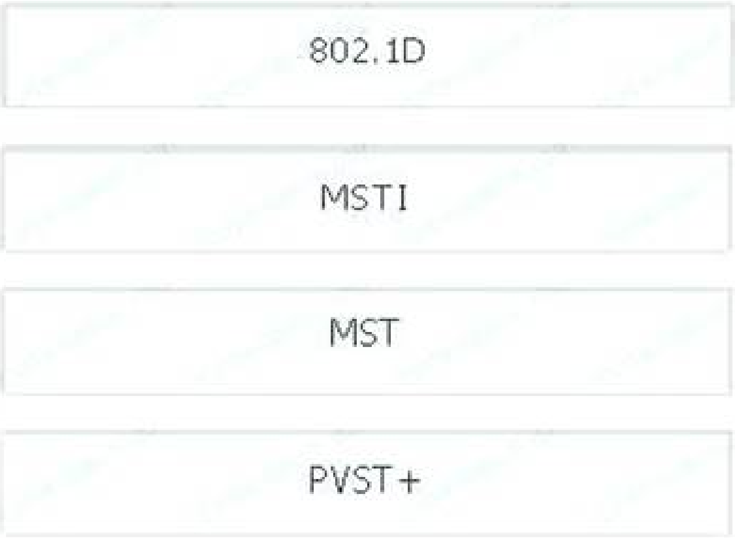
exists inside a region as an RSTP instance

combines STP instances

consists of a single instance of STP

Answer:

Explanation:



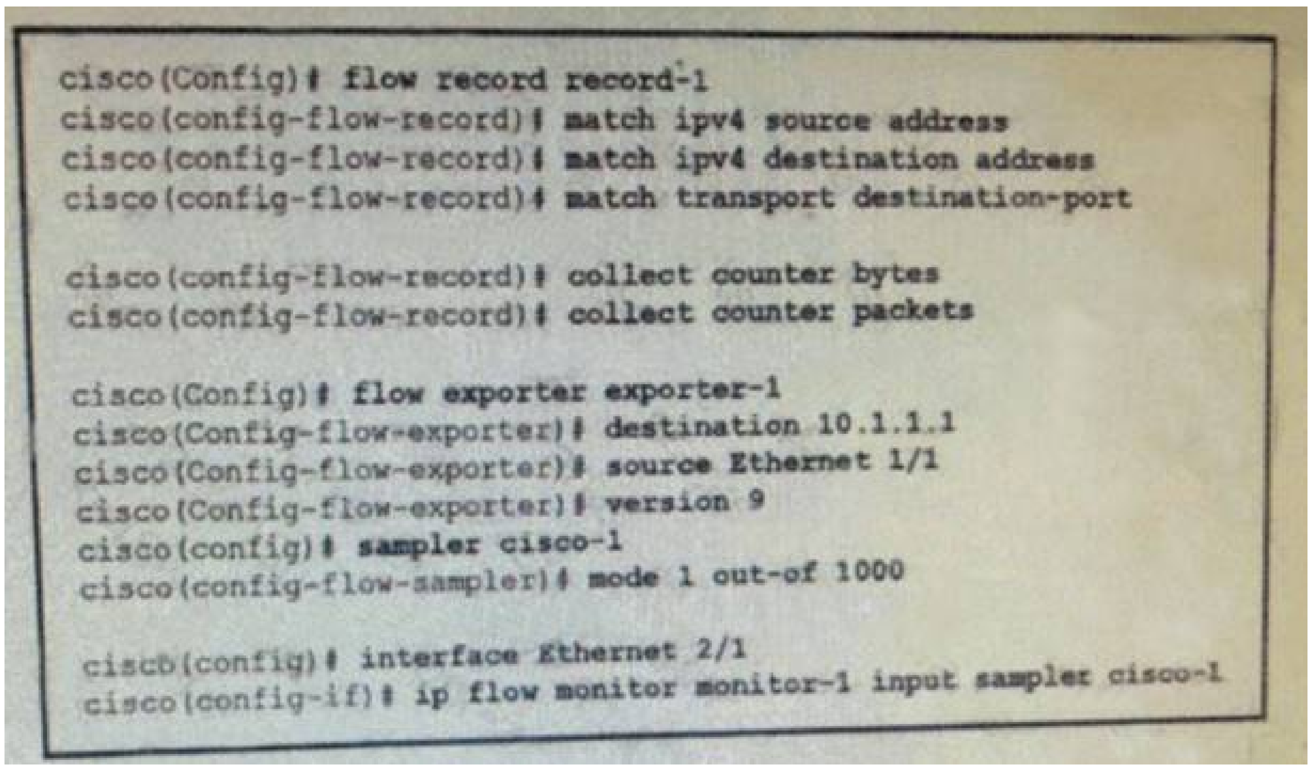
802.1D

MSTI

MST

PVST+

NEW QUESTION 8
Refer to the exhibit.



```
cisco(Config)# flow record record-1
cisco(config-flow-record)# match ipv4 source address
cisco(config-flow-record)# match ipv4 destination address
cisco(config-flow-record)# match transport destination-port

cisco(config-flow-record)# collect counter bytes
cisco(config-flow-record)# collect counter packets

cisco(Config)# flow exporter exporter-1
cisco(Config-flow-exporter)# destination 10.1.1.1
cisco(Config-flow-exporter)# source Ethernet 1/1
cisco(Config-flow-exporter)# version 9
cisco(config)# sampler cisco-1
cisco(config-flow-sampler)# mode 1 out-of 1000

cisco(config)# interface Ethernet 2/1
cisco(config-if)# ip flow monitor monitor-1 input sampler cisco-1
```

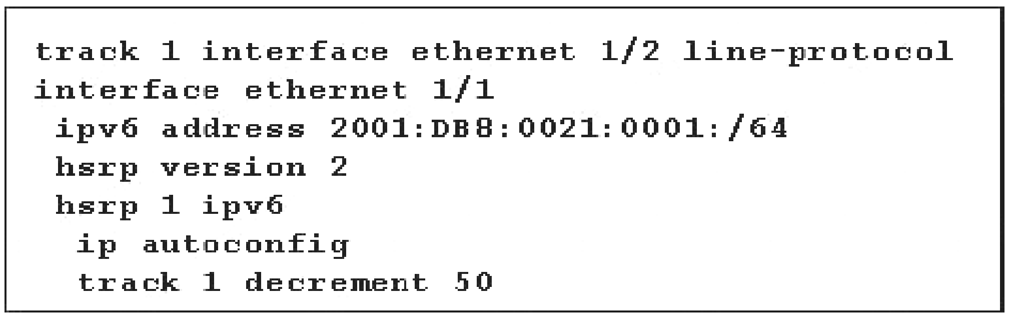
Which statement about the NetFlow implementation is true?

A. It samples inbound IPv6 traffic on Ethernet 2/1
B. It uses TCP for data export.
C. It samples outbound traffic on Ethernet 2/1
D. It samples inbound traffic on Ethernet 2/1

Answer: D

Explanation: Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fnetflow/configuration/15-mt/fnf-15-mtbook/use-fnflow-redce-cpu.html

NEW QUESTION 9
Refer to the exhibit.



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

Which statement about the result of the configuration is true?

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

Answer: D

NEW QUESTION 10
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 10
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 13

```
switch# configure terminal
switch (config) # interface ethernet 1/4 switch (config-if) # switchport mode trunk
switch (config-if) # channel-group 1 mode active
```

Refer to the exhibit. Which type of port channel was created?

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

Answer: A

NEW QUESTION 18
Which statement about electronic programmable logic device image upgrades is true?

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

Answer: D

Explanation: You can upgrade (or downgrade) EPLDs using CLI commands on the Nexus 7000 Series device. Follow these guidelines when you upgrade or downgrade EPLDs:
- You can execute an upgrade from the active supervisor module only. All the modules, including the active supervisor module, can be updated individually.
- You can individually update each module whether it is online or offline as follows:

– If you upgrade EPLD images on an online module, only the EPLD images with version numbers that differ from the new EPLD images are upgraded.
– If you upgrade EPLD images on an offline module, all of the EPLD images are upgraded.
- On a system that has two supervisor modules, upgrade the EPLDs for the standby supervisor and then switch the active supervisor to standby mode to upgrade its EPLDs. On a system that has only one supervisor module, you can upgrade the active supervisor, but this will disrupt its operations during the upgrade.
- If you interrupt an upgrade, you must upgrade the module that is being upgraded again.
- The upgrade process disrupts traffic on the targeted module.
- Do not insert or remove any modules while an EPLD upgrade is in progress. Reference:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_0/epld/release/notes/epld_rn.ht ml

NEW QUESTION 19
Which command configures the aging for VLAN 100 to 500 minutes?

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

Answer: C

NEW QUESTION 20
You experience an issue on a Cisco Nexus 7700 Series switch. You must gather detailed information about the system state and the configuration of the switch. Which command should you run?

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

Answer: B

NEW QUESTION 23

```
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 24
Which two options can be used for link aggregation when you configure vPC member interfaces? (Choose two.)

A. a static EtherChannel
B. the Cisco Fabric Services protocol
C. the LACP protocol
D. the VSL control link
E. the PAgP protocol

Answer: AC

NEW QUESTION 26
Which technology is required in the underlay to facilitate remote VTEP discovery?

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

Answer: A

NEW QUESTION 28
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 29
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 34
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 addres

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 37
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 38

Which option must be configured when you implement a vPC?

A. the CCL link, peer link, and vPC member interfaces
B. the peer keepalive link, peer link, and vPC member interfaces
C. the VSL link, peer link, and vPC member interfaces
D. the VSS link, peer link, and vPC member interfaces

Answer: B

NEW QUESTION 39
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 40
You plan to implement the OSPF protocol whithin the data center network. Which two statements accurately describe OSPF on the Cisco NX-OS platform? (Choose two.)

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

Answer: DE

NEW QUESTION 45
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_op s.html

NEW QUESTION 47
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 51
You have a Cisco Nexus 5000 Series switch. Port security is configured to use sticky learning. Where are the secured MAC addresses stored?

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

Answer: C

NEW QUESTION 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 ho

Answer: CE

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

NEW QUESTION 58
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 63
Which two options accurately describe the implementation of Fibre Channel domain IDs? (Choose two.)

A. are assigned on a per-line card basis
B. must be unique on all of the Fibre Channel switches in the fabric
C. are assigned on a per switch basis
D. are assigned on a per-VSAN basis
E. must be the same on all of the Fibre Channel switches in the fabric

Answer: BC

NEW QUESTION 65
Which LISP component provides connectivity between LISP and non-LISP sites?

A. a map resolver
B. a proxy ETR
C. a proxy ITR
D. an ALT

Answer: C

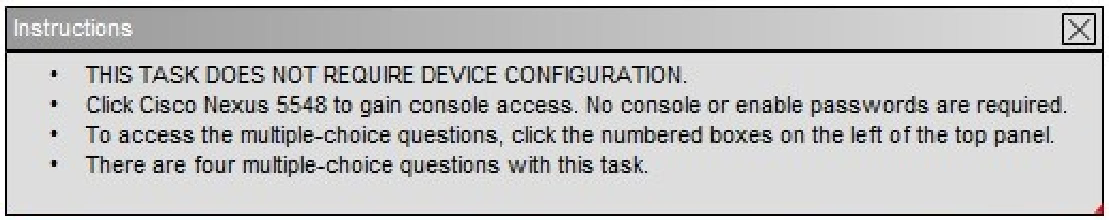
NEW QUESTION 69
After enabling strong, reversible 128-bit Advanced Encryption Standard password type-6 encryption on a Cisco Nexus 7000, which command would convert existing plain or weakly encrypted passwords to type-6 encrypted passwords?

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

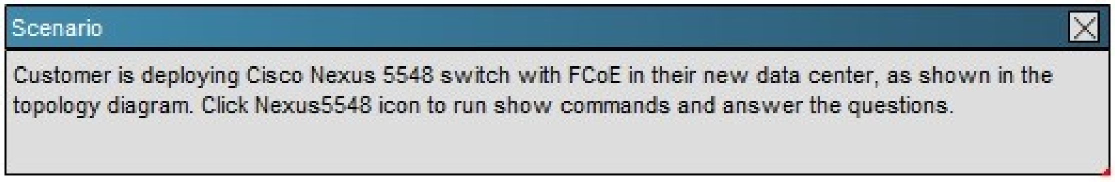
Explanation: This command converts existing plain or weakly encrypted passwords to type-6 encrypted passwords.
Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nxos/security/configuration/guide/b_Cisco_Nexus_7000_NXOS_ Security_Configuration_Guide Release_5-x/b_Cisco_Nexus_7000_NXOS_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

NEW QUESTION 72
What is the status of FCoE license on Cisco Nexus 5548 switch?



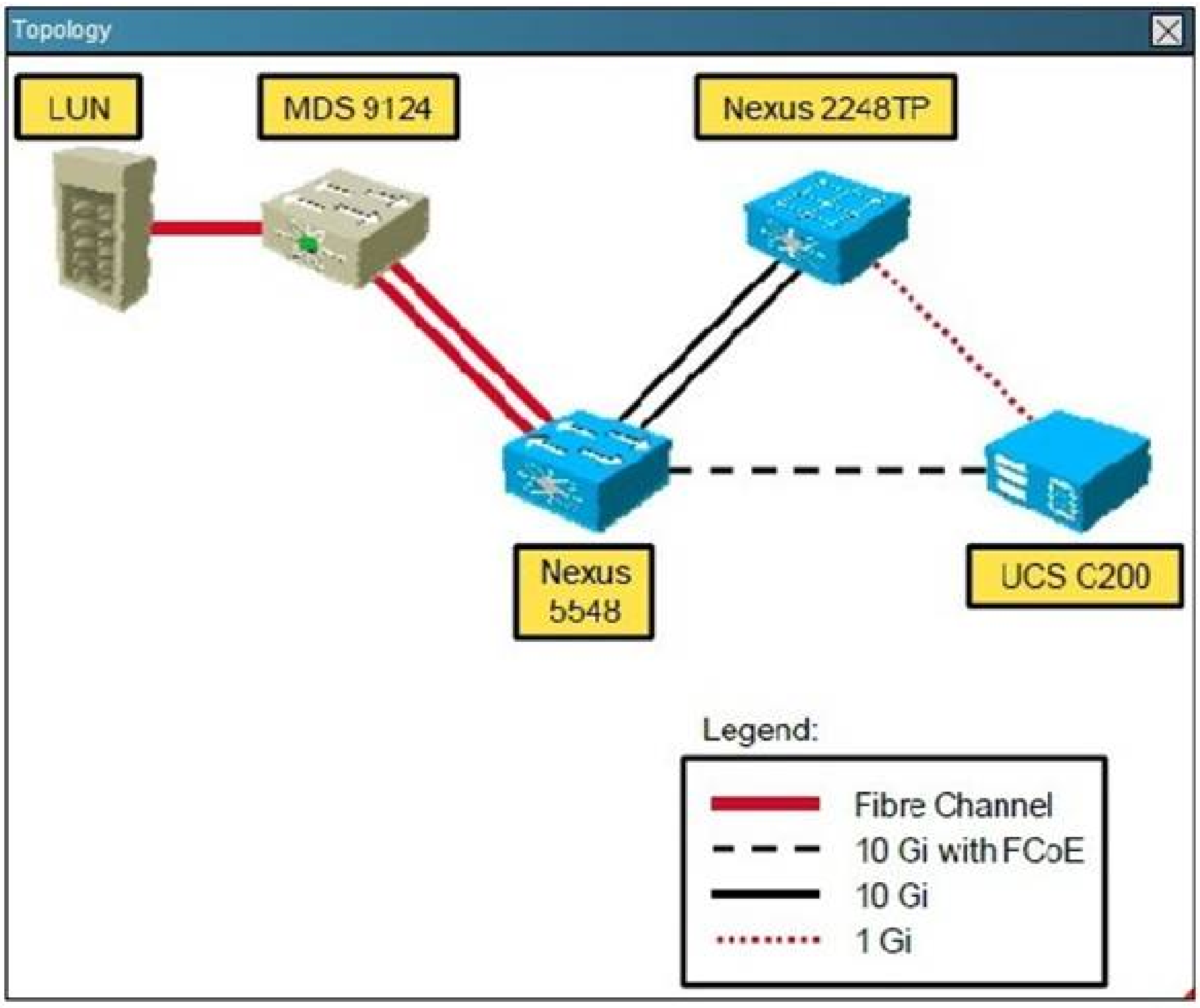
Instructions

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



Scenario

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

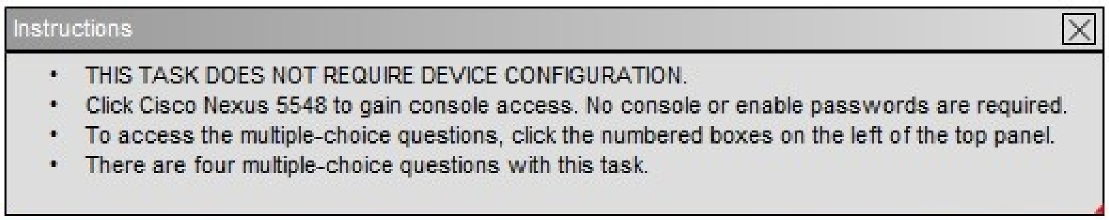


```
Nexus 5548#
```

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

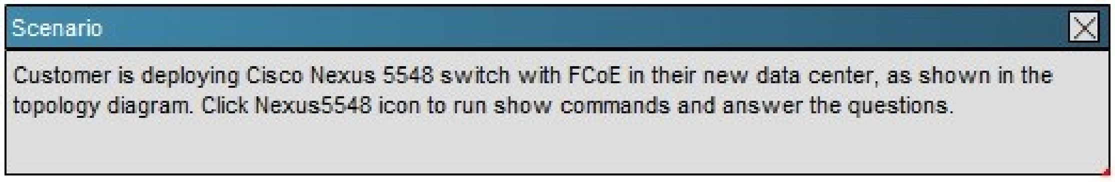
Answer: C

NEW QUESTION 76
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?



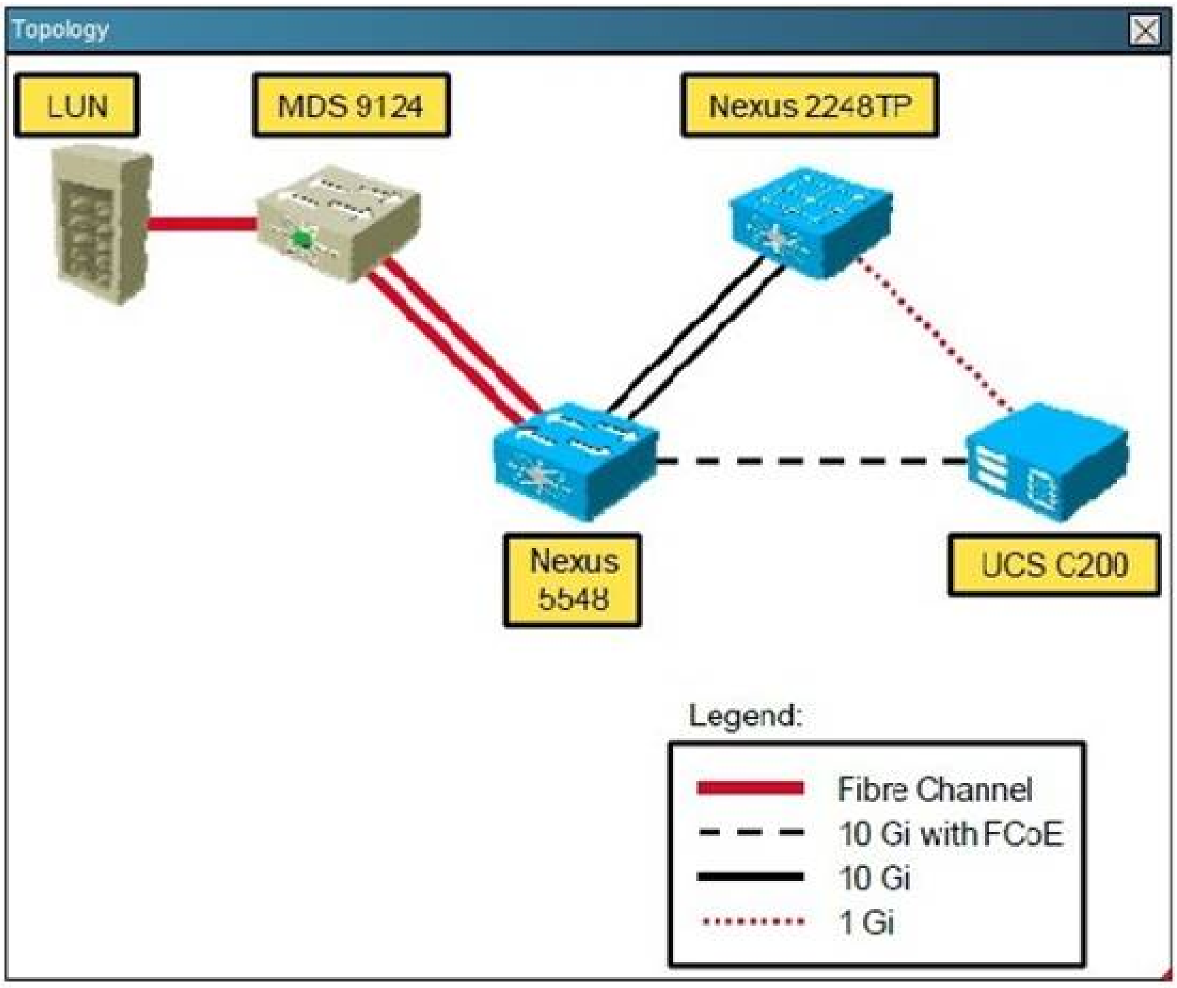
Instructions

- 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.



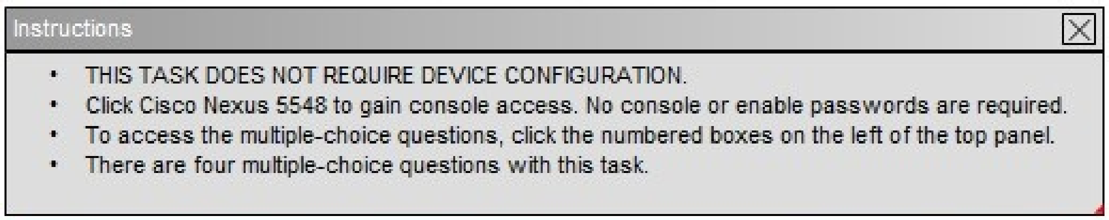
Nexus 5548

```
Nexus 5548#
```

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

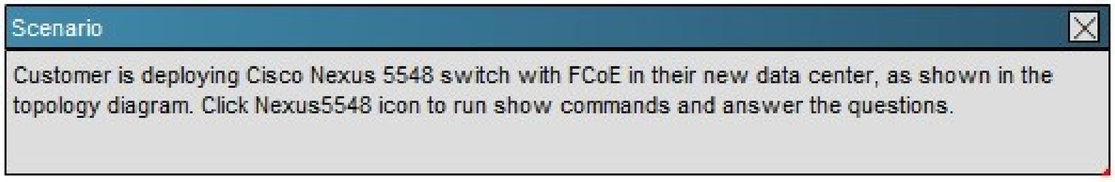
Answer: D

NEW QUESTION 80
What is the status of FC interface associated with ethernet 1/5 indicate?



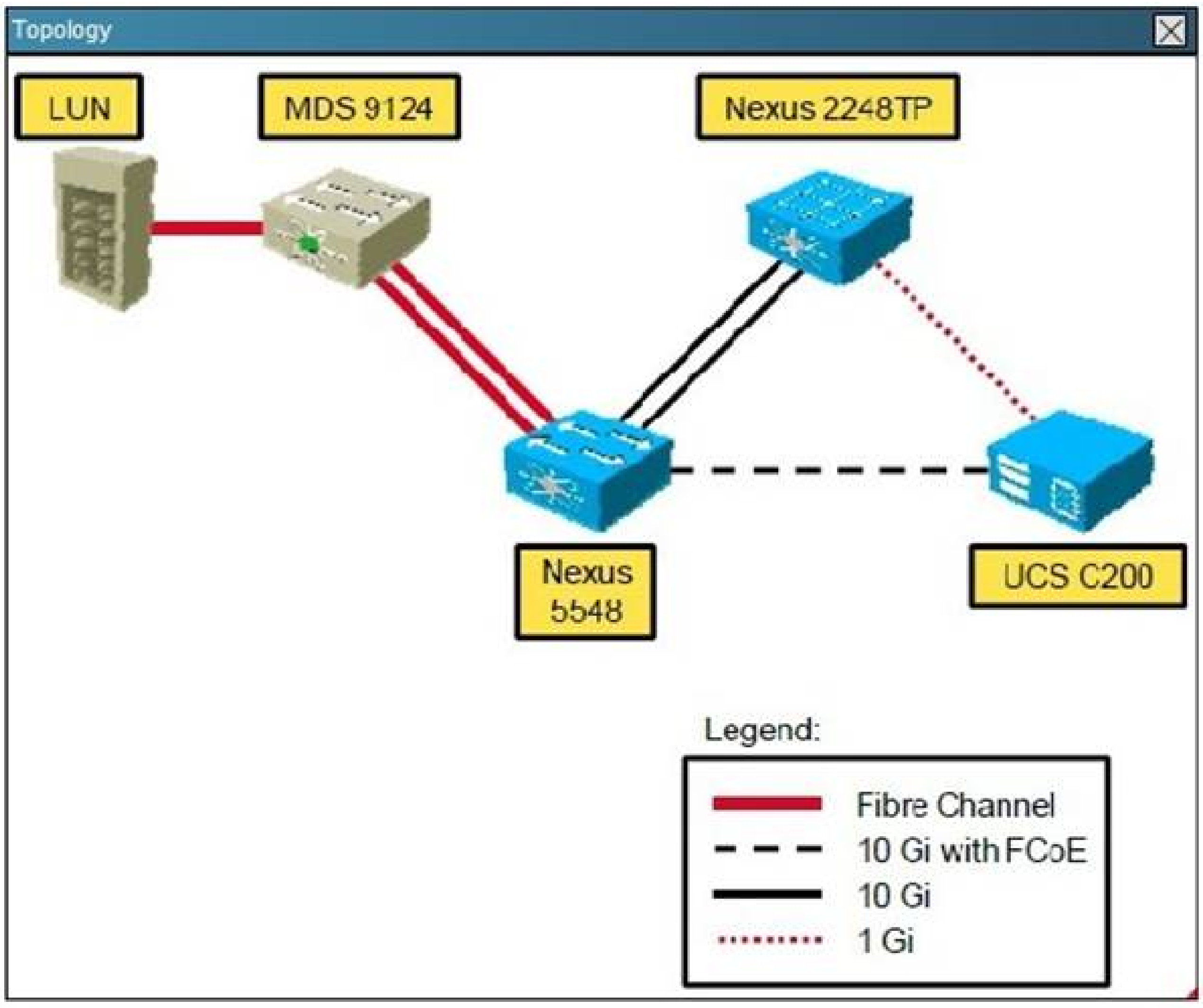
Instructions

- 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.



Topology

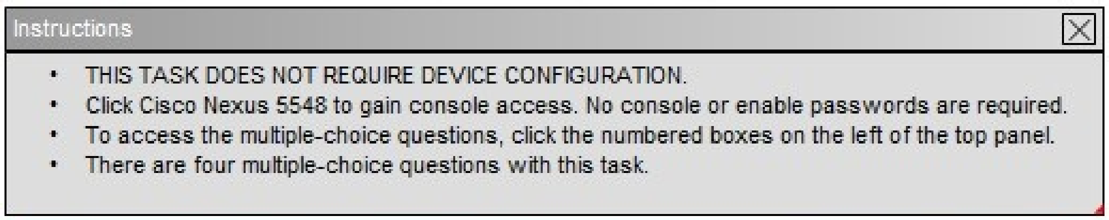
Nexus 5548

```
Nexus 5548#
```

A. Trunk VSAN 11 is isolated
B. Inteface vfc 5 is up and running for the assigned VSAN
C. Trunk VSAN 11 is intializing
D. VSAN to FC mapping is not working as expected

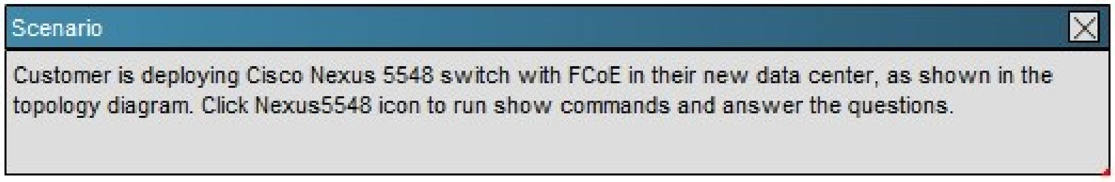
Answer: B

NEW QUESTION 81
When configuring FCoE VLANs and Virtual Fiber Channel (vFC) Interfaces, what guidelines must be followed?



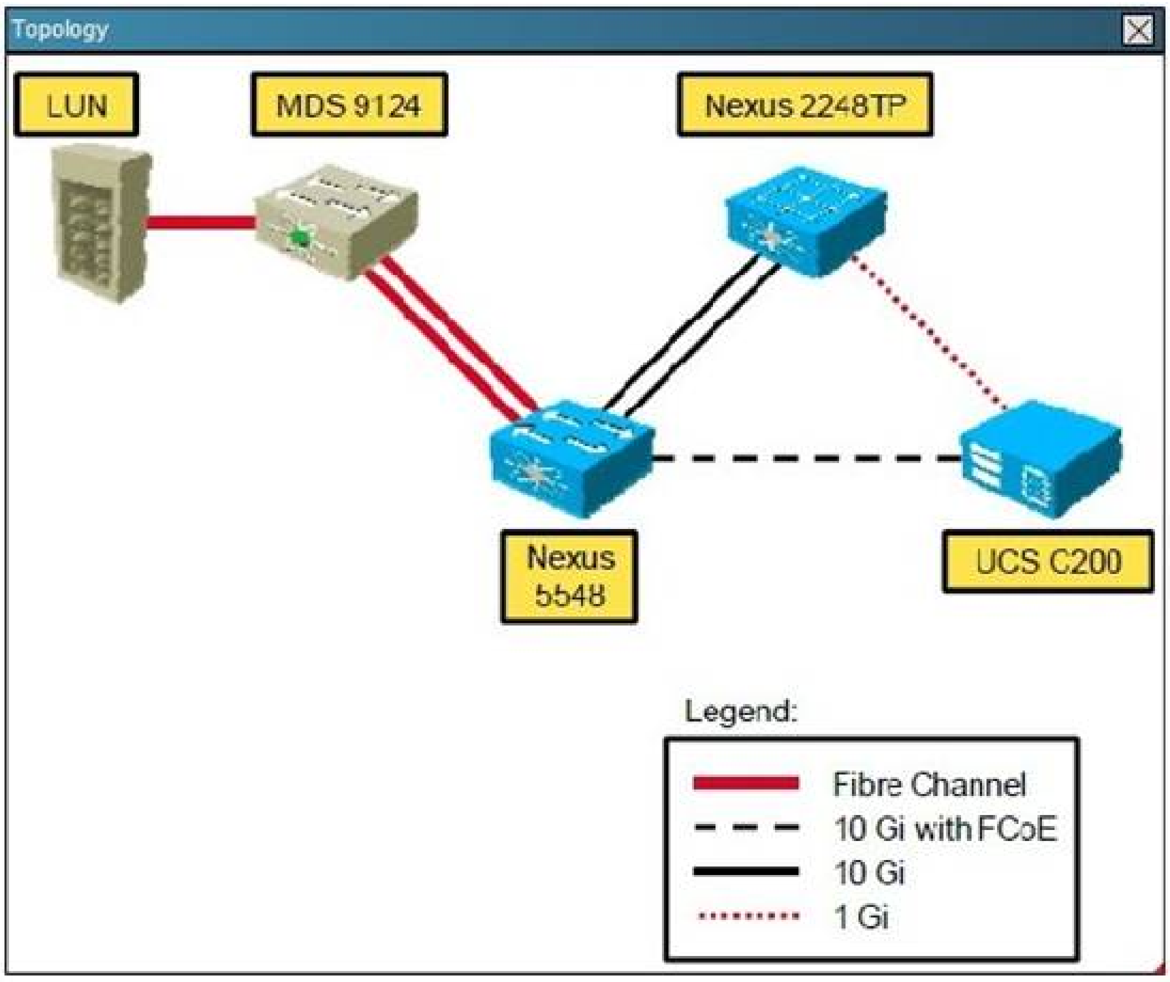
Instructions

- 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.



Nexus 5548

```
Nexus 5548#
```

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 85
You have two Cisco Nexus 7700 Series switches named SwitchA and SwitchB. You use the Rapid PVST+ protocol. You must configure the switches as the STP root switches for VLANs 100 to 200. Which command set should you run?

A. SwitchA(config-if)#spanning-tree cost 100 SwitchB(config-if)#spanning-tree cost 100
B. SwitchA(config-if)#spanning-tree guard root SwitchB(config-if)#spanning-tree guard root
C. SwitchA(config)#spanning-tree vlan 100-200 priority 61440SwitchB(config)#spanning-tree vlan 100-200 priority 61440
D. SwitchA(config)#spanning-tree vlan 100-200 root primary SwitchB(config)#spanning-tree vlan 100-200 root secondary

Answer: D

NEW QUESTION 90
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 92
Which two items are services that are provided by Cisco Fabric Services? (Choose two.)

A. device alias distribution
B. VLAN database distribution
C. Kerberos proxy distribution
D. RSA key pair distribution
E. DPVM configuration distribution

Answer: AE

Explanation: The device alias application uses the Cisco Fabric Services (CFS) infrastructure to enable efficient database management and distribution. Device aliases use the coordinated distribution mode and the fabric-wide distribution scope.
DPVM can use CFS to distribute the database to all switches in the fabric. This allows devices to move anywhere and keep the same VSAN membership. You should enable CFS distribution on all switches in the fabric. Using the CFS infrastructure, each DPVM server learns the DPVM database from each of its neighboring switches during the ISL bring-up process. If you change the database locally, the DPVM server notifies its neighboring switches, and that database is updated by all switches in the fabric.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/ CLIConfigurationGuide/ddas.html and http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nxos/ san_switching/configuration/guide/b_Cisco_Nexus_7000_NXOS_ SAN_Switching_Configuration_Guide/Cisco_Nexus_7000_NXOS_ SAN_Switching_Configuration_Guide_chapter4.html#concept_2B83E16506C845B39BDF96F9CA FFAEC3

NEW QUESTION 97
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 101
What are two requirements for configuring SAN device aliases? (Choose two.)

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

Answer: DE

NEW QUESTION 104
Which two statements are true when performing a SPAN capture of traffic reaching the Supervisor CPU in order to troubleshoot control plane protocols in the tenant VDC? (Choose two.)

A. The destination interface will also receive control plane traffic from other VDCs.
B. The SPAN configuration must be added to the default or administrative VDC.
C. SPAN only supports monitoring of ingress traffic to the supervisor.
D. Captured traffic from the supervisor can be shown directly on the terminal.
E. Only monitoring of egress traffic from the supervisor is possibl

Answer: BD

NEW QUESTION 106
Which implicit rules are applied to all IPv6 ACLs?

A. deny icmp any any nd-na deny icmp any any nd-nspermit 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-nspermit icmp any any router-advertisement permit icmp any any router-solicitation deny ipv6 any any

Answer: D

NEW QUESTION 107
What are two ways to configure the switch ID for Cisco FabricPath? (Choose two.)

A. manually by using the vPC domain configuration
B. manually by using global configuration mode
C. dynamically by using the POAP protocol
D. dynamically by using the DRAP protocol
E. dynamically by using the SNMPv2 protocol

Answer: BD

NEW QUESTION 112
Within the vPC configuration of the 7K's, the command peer switch is configured. What is the result of enabling the command?

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

Answer: A

NEW QUESTION 113
Within the vPC configuration of the 7K's the command peer-gateway is configured as confirmed with the command show vpc. what is the result of enabling this command?

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

Answer: D

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

NEW QUESTION 114
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 115
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

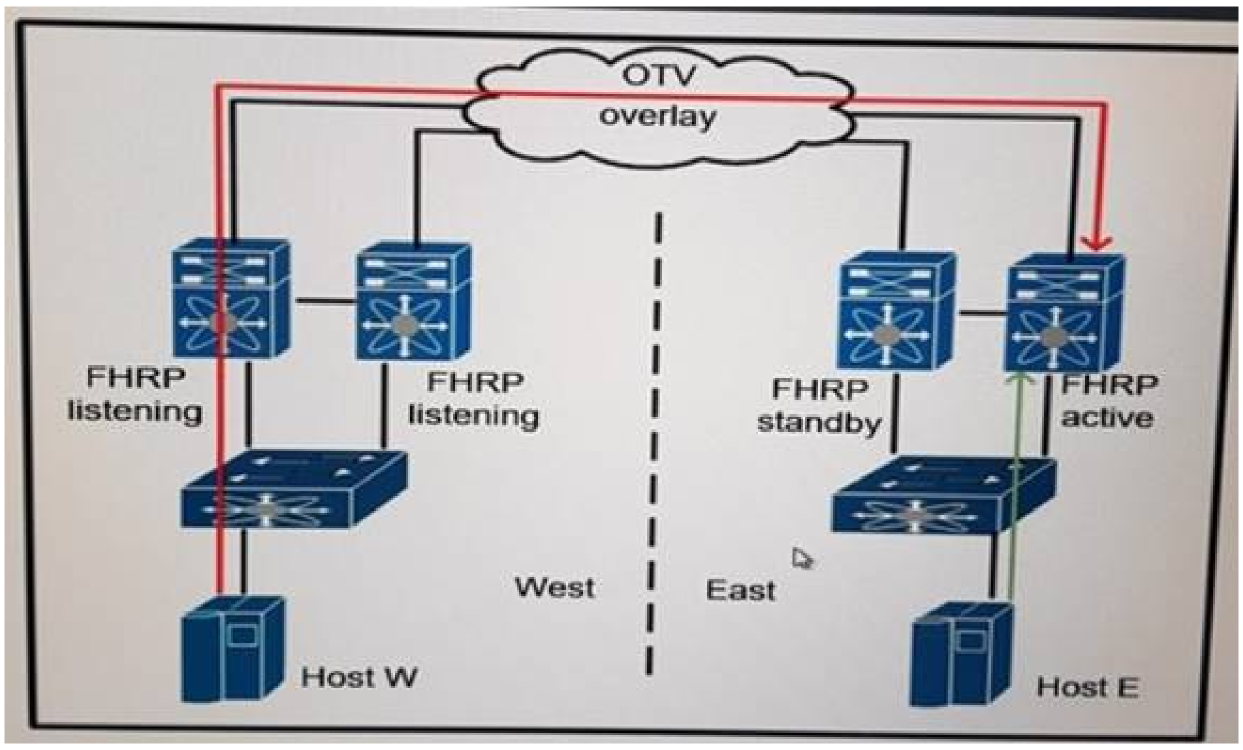
NEW QUESTION 119
What are two prerequisite to running the Smart Call Home feature on a Cisco nexus 6000 series switch? (Select two)

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

Answer: AD

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

NEW QUESTION 124
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 126
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-destioation-port
C. Flow
D. Source id-destination id-oxid

Answer: C

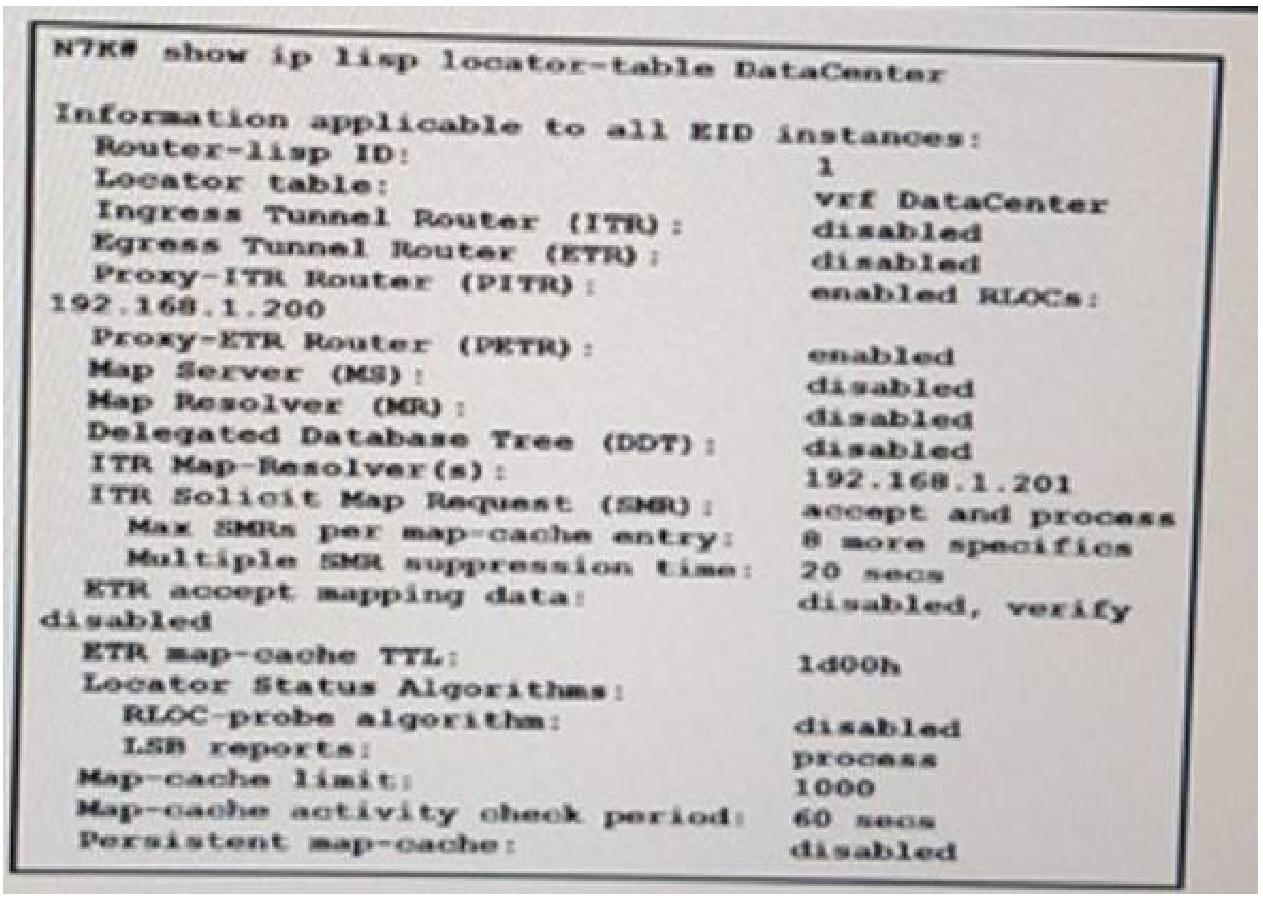
NEW QUESTION 129
You have a Cisco Fabric Path network, you must extend the network to support more than 16 million segment, what should you do?

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

Answer: C

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

NEW QUESTION 131
Refer to the exhibit,



```
N7K# show ip lisp locator-table DataCenter

Information applicable to all EID instances:
   Router-lisp ID:                               1
   Locator table:                                vrf DataCenter
   Ingress Tunnel Router (ITR):                  disabled
   Egress Tunnel Router (ETR):                   disabled
   Proxy-ITR Router (PITR):                      enabled RLOCs:
192.168.1.200
   Proxy-ETR Router (PETR):                      enabled
   Map Server (MS):                              disabled
   Map Resolver (MR):                            disabled
   Delegated Database Tree (DDT):                disabled
   ITR Map-Resolver(s):                          192.168.1.201
   ITR Solicit Map Request (SMR):                accept and process
     Max SMRs per map-cache entry:               8 more specifics
     Multiple SMR suppression time:              20 secs
   ETR accept mapping data:                      disabled, verify
disabled
   ETR map-cache TTL:                            1d00h
   Locator Status Algorithms:
     RLOC-probe algorithm:                       disabled
     LSB reports:                                process
   Map-cache limit:                              1000
   Map-cache activity check period:              60 secs
   Persistent map-cache:                         disabled
```

Which description of the output is true?

A. The default map-cache limit is used.
B. PETR is disable
C. The table output apply to the default VRF
D. The switch acts as an IPv4 LISP ETR

Answer: A

NEW QUESTION 132
When configuring PIM to support an OTV implementation, Which PIM configuration is supported in Cisco NX-OS?

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

Answer: B

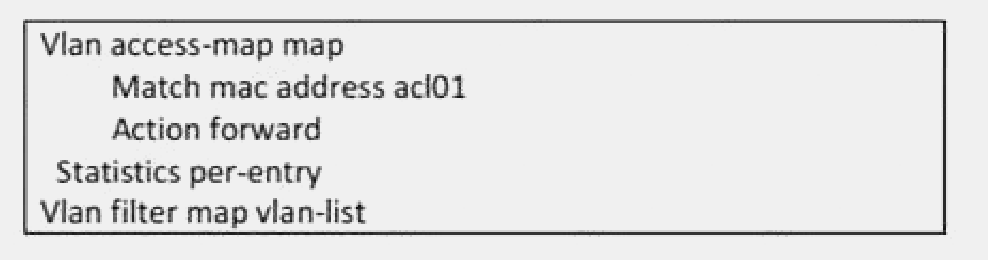
Explanation: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6- x/multicast/configuration/guide/b_Cisco_Nexus_9000_Series_NXOS_ Multicast_Routing_Configuration_Guide/b_Cisco_Nexus_9000_Series_NXOS_ Multicast_Routing_Configuration_Guide_chapter_011.html

NEW QUESTION 135
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 140
Refer to the exhibit.



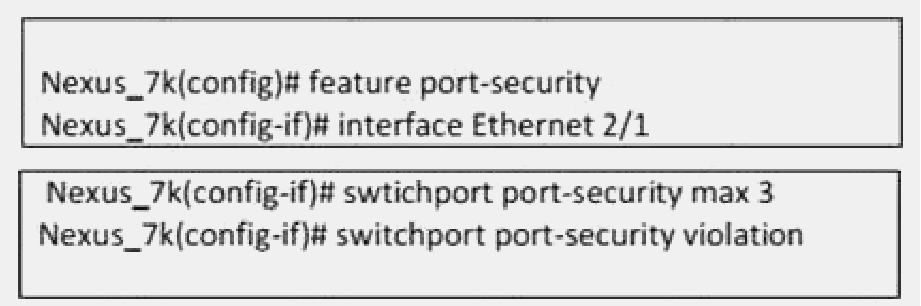
```
Vlan access-map map
        Match mac address acl01
        Action forward
  Statistics per-entry
Vlan filter map vlan-list
```

Which result of the configuration snippet is true?

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

Answer: B

NEW QUESTION 143
Refer to the exhibit.



```
Nexus_7k(config)# feature port-security
Nexus_7k(config-if)# interface Ethernet 2/1
Nexus_7k(config-if)# swtichport port-security max 3
Nexus_7k(config-if)# switchport port-security violation
```

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

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

Answer: AC

NEW QUESTION 148
Fibre Chanel IDs are dynamically assigned to which object?

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

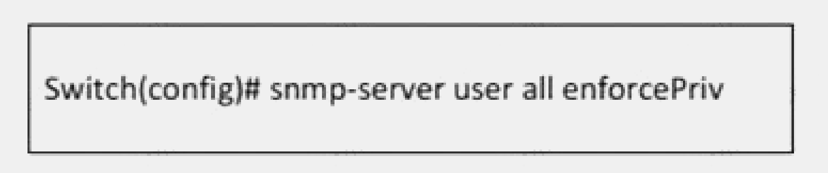
Answer: D

NEW QUESTION 151
Which option accurately describes the implementation of Fibre Channel domain IDs?

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

Answer: A

NEW QUESTION 153
Refer to the exhibit.



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

Which option is 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 al

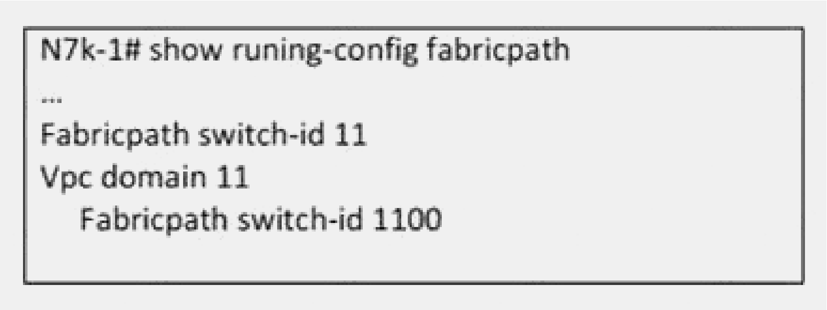
Answer: D

NEW QUESTION 155
You have a Cisco FabricPath network. You must implement Vpc+ for a downstream switch. Which three actions should you preform? (Choose three)

A. Configure the downstream switch to use PAgP on EtherChannel.
B. Configure the switch ID on the peer switches.
C. Establish a peer link between the peer switches.
D. Configure the upstream switch to use PAgP on EtherChannel.
E. Configure a peer keepalive between the peer switches.
F. Connect the downstream switch to a 1-0Gb por

Answer: ABC

NEW QUESTION 159
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 namedN7k-l
Which command set should you run on a neighboring Cisco Nexus 7010 swith to estabish a vPC+ environment that includes N7k-1?

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

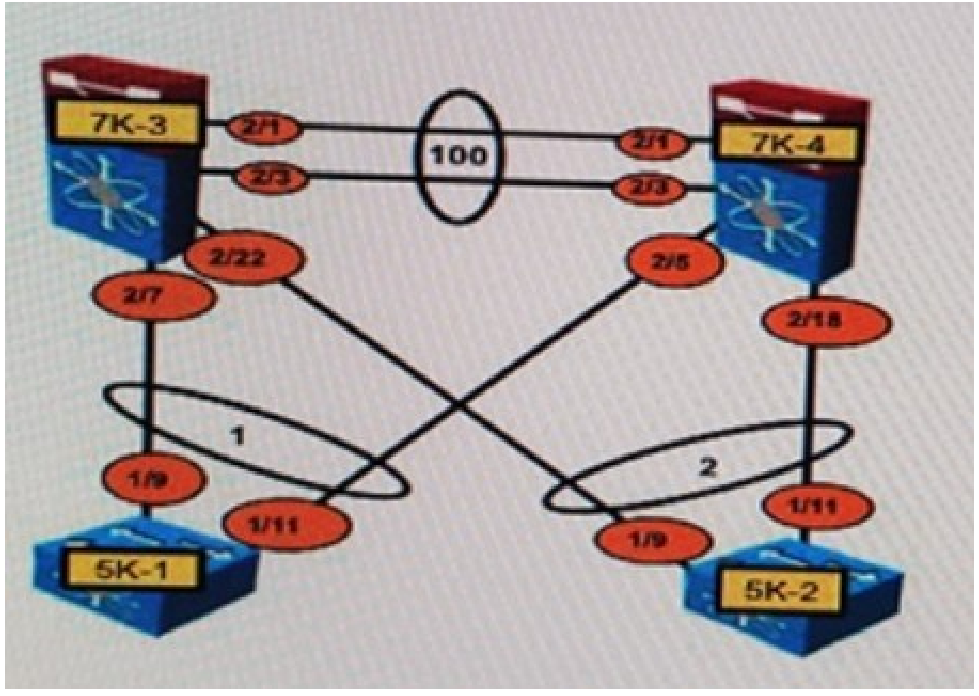
Answer: B

NEW QUESTION 164
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 167
Scenario:
The following four questions concern the Nexus 7010' s which are configured as a vPC pair at the core of a Data Center network. You can utilize all the available show commands to answer the Questions Access to the running-configuration is not allowed.
Instructions:
Enter NX-OS commands on 7K-3 and 7K-4 to verity network operation and answer four multiplechoice questions
THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
Click on the switch to gain access to the console of the switch. No console or enable passwords are required.
To access the multiple-choice questions, click on the numbered boxes on the loft of the top panel. There are four multiple-choice questions with this task Be sure to answer all four questions before selecting the Next button
Topology:



```
7K-4#
```

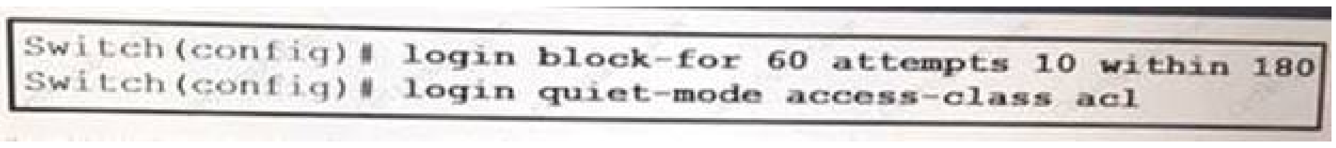
```
7K-3#
```

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

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

Answer: B

NEW QUESTION 171
Refer to Exhibit.



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

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

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

Answer: D

NEW QUESTION 172
When configuring OSPF, which two network types will avoid the DR and BDR election process between connected devices? (Choose Two)

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

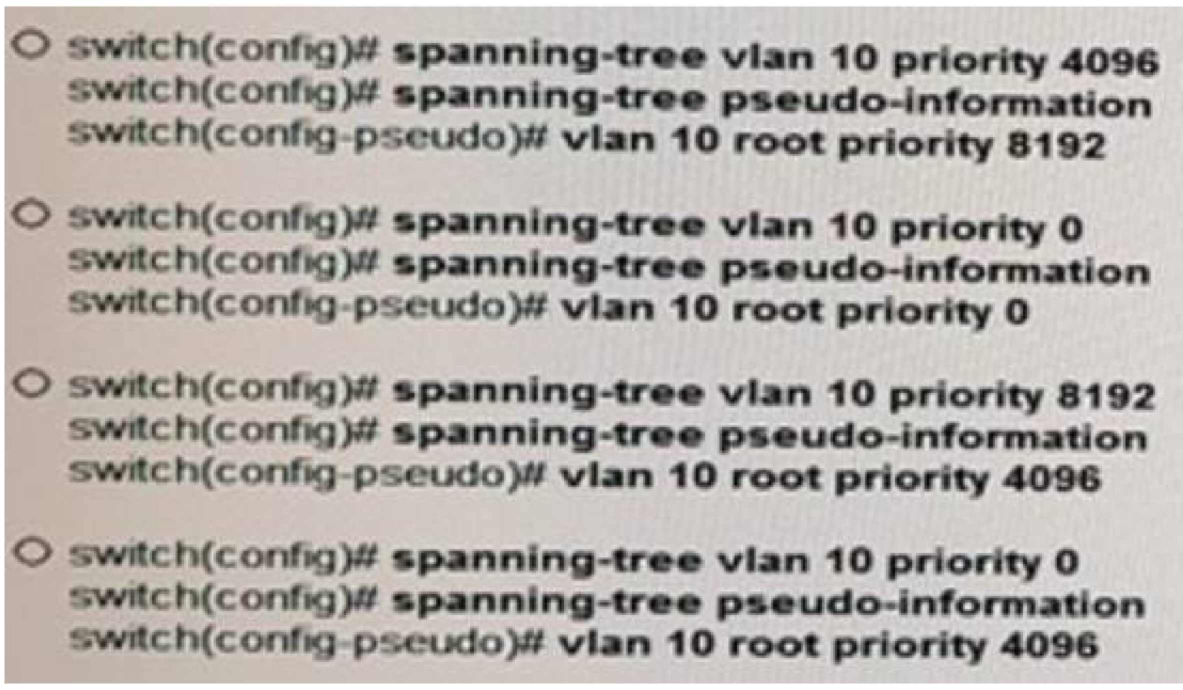
Answer: CE

NEW QUESTION 176
You are configuring OTV between two data centers. On which interfaces should the site VLAN allowed?

A. the interfaces that connect to the aggregation switches
B. the OTV overlay interfaces
C. the interfaces that connect to the join interfaces
D. the mgmt0 interfaces

Answer: A

NEW QUESTION 179
You configure STP on a switch that is attached to a Cisco Fabric Path domain and that has the vPC feature deployed. How do you configure STP on the switch in the Cisco FabricPath domain on VL AN 10?



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

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

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

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

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

Answer: C

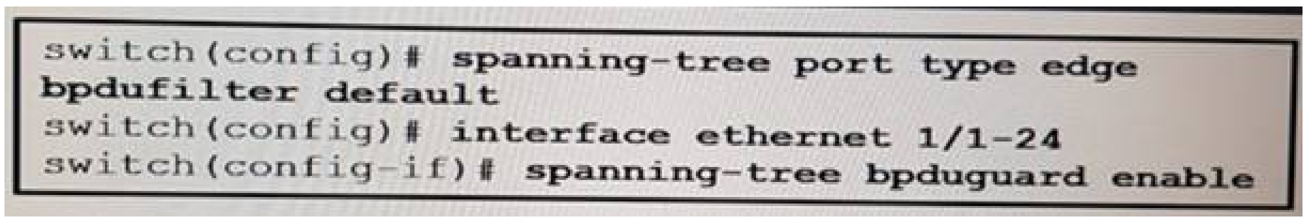
NEW QUESTION 184
When configuring HSRP on IPv6-enabled interfaces, which two commands are required? (Choose two)

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 189
Refer to the exhibit.



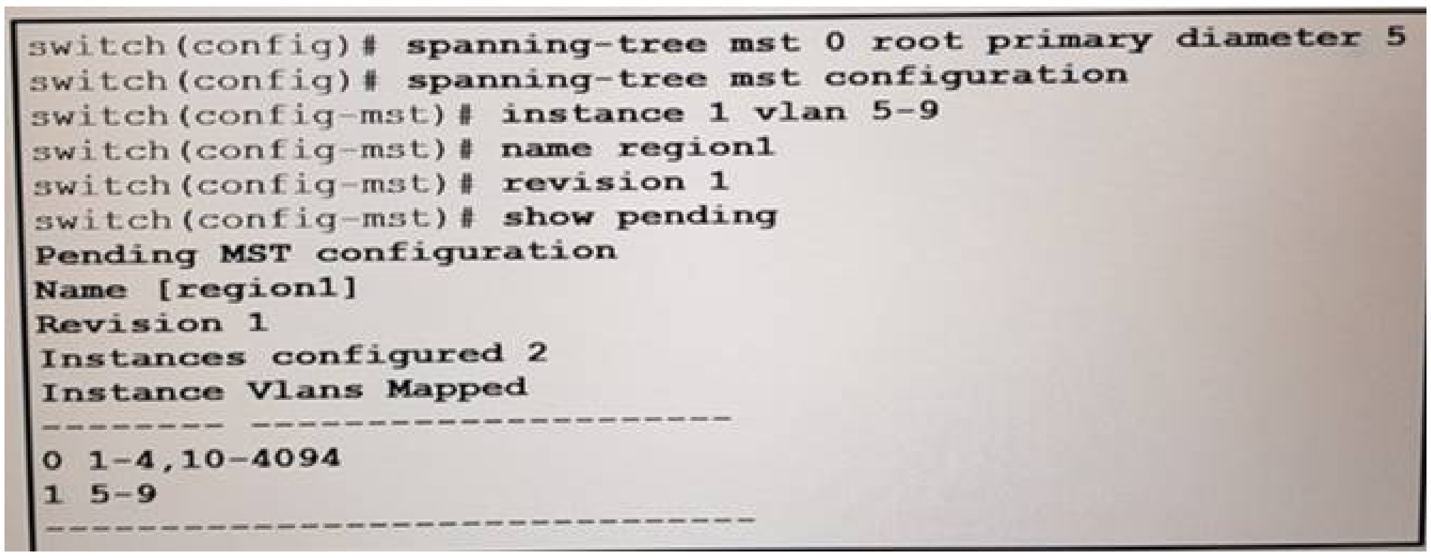
```
switch(config)# spanning-tree port type edge
bpdufilter default
switch(config)# interface ethernet 1/1-24
switch(config-if)# spanning-tree bpduguard enable
```

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 192
Refer to the exhibit.



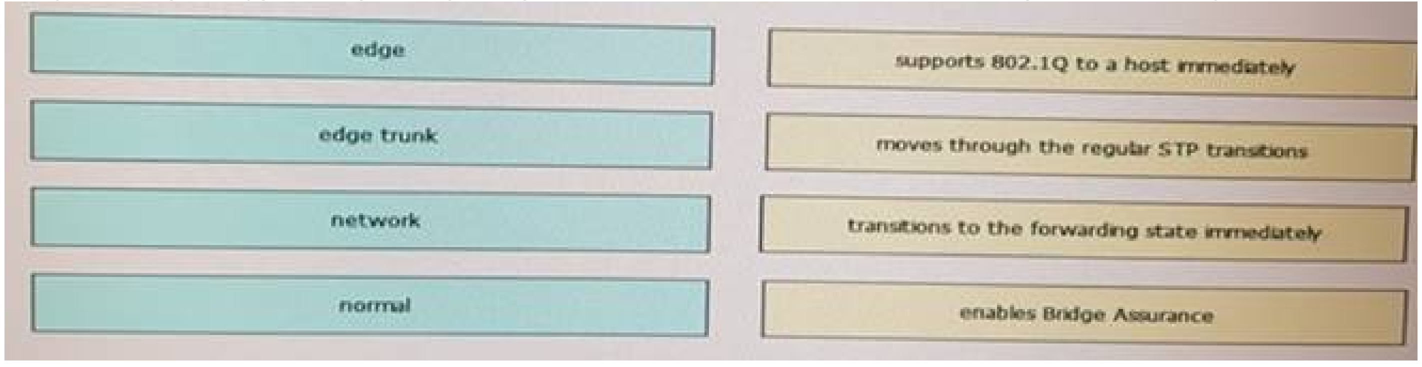
```
switch(config)# spanning-tree mst 0 root primary diameter 5
switch(config)# spanning-tree mst configuration
switch(config-mst)# instance 1 vlan 5-9
switch(config-mst)# name region1
switch(config-mst)# revision 1
switch(config-mst)# show pending
Pending MST configuration
Name [region1]
Revision 1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

What does the diameter command specify?

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

Answer: A

NEW QUESTION 193
DRAG DROP
Drag and drop the types of spanning tree ports from the left onto the correct descriptions on the right



edge
edge trunk
network
normal

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

Answer:

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

NEW QUESTION 197
Which technology relies on STP as a failsafe mechanism?

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

Answer: A

NEW QUESTION 200
Which information does the show fcns database command display?

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

Answer: A

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

NEW QUESTION 205
Which command allows a Cisco Nexus 7000 Series Switch to receive NTP configuration updates by using Cisco Fabric Services?

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

Answer: B

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

NEW QUESTION 210
Which command configures the aging time for VLAN 100 to 50 minutes?

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

Answer: A

NEW QUESTION 211
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 212
You plan to configure a SAN zone set. Which two facts should you consider before you configure the 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: BE

NEW QUESTION 217
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 222
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 224
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

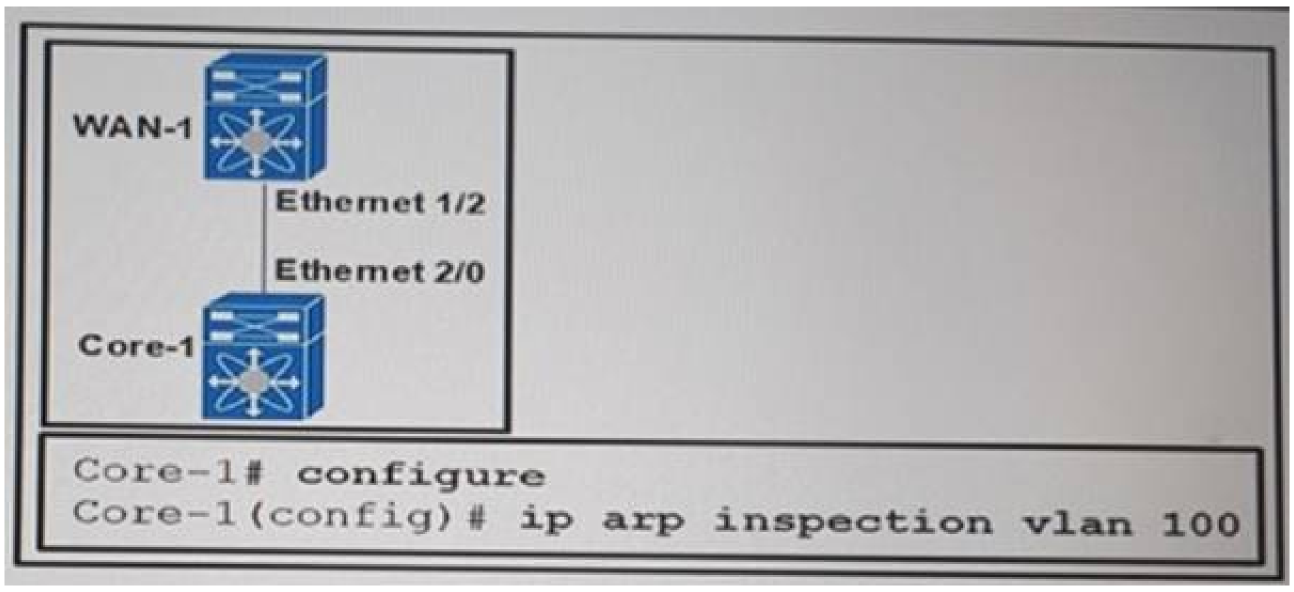
License expiration of a feature Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/systemmanagement/guide/b_Cisco_Nexus_7000_Series_NXOS_System_Management_Configuration_Guide-RI/configuring_rollback.html

NEW QUESTION 227
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 230
Refer to the exhibit.



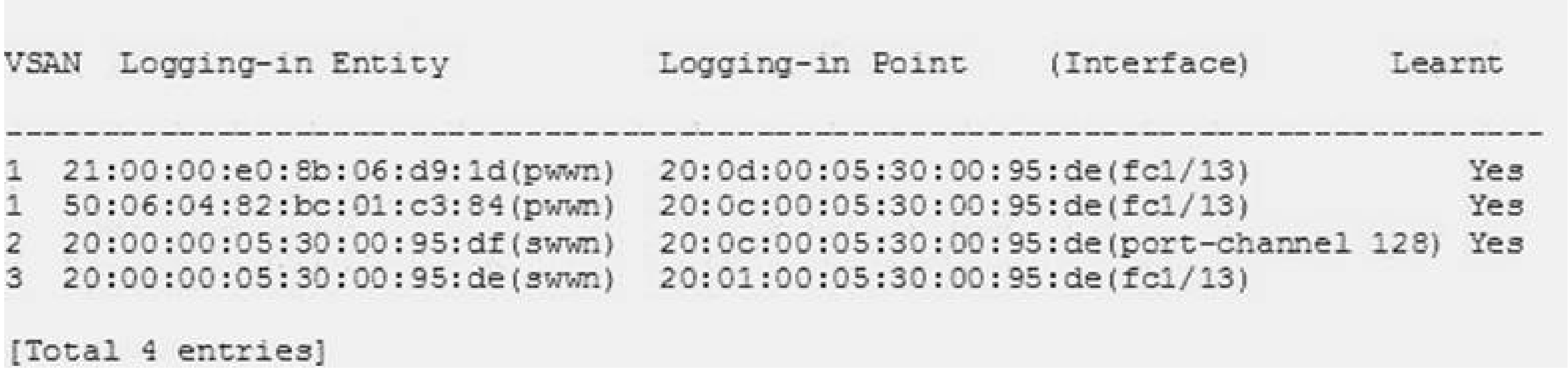
```
Core-1# configure
Core-1(config)# ip arp inspection vlan 100
```

Which action do you take to prevent DAI from inspecting packets on Ethernet 2/0?

A. Configure a DHCP snooping entry.
B. Create a VLAN ACL
C. Create a MAC ACL
D. Configure Ethernet 2/0 as a trusted interfac

Answer: D

NEW QUESTION 233
Refer to the exhibit.



```
VSAN  Logging-in Entity           Logging-in Point     (Interface)      Learnt
-------------------------------------------------------------------------------
1   21:00:00:e0:8b:06:d9:1d(pwwn)  20:0d:00:05:30:00:95:de(fc1/13)           Yes
1   50:06:04:82:bc:01:c3:84(pwwn)  20:0c:00:05:30:00:95:de(fc1/13)           Yes
2   20:00:00:05:30:00:95:df(swwn)  20:0c:00:05:30:00:95:de(port-channel 128) Yes
3   20:00:00:05:30:00:95:de(swwn)  20:01:00:05:30:00:95:de(fc1/13)

[Total 4 entries]
```

Which command should you run on a Cisco MDS 9000 Series switch to produce the output?

A. show fabric-binding database active
B. show port-security database active
C. show fabric-binding database
D. show port-security database

Answer: B

NEW QUESTION 234
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 237
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 242
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 246
Which statement about the Layer 3 card on the Cisco Nexus 5500 Series Switch is true?

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

Answer: C

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

NEW QUESTION 247
Refer to the command below. When configuring an SVS connection on the Cisco Nexus 5000 Series Switch, which device is being referenced as the remote IP address?
nexus5500-2(config-svs-conn)# remote ip address 10.10.1.15 port 80 vrf management

A. ESX or ESXi host
B. vCenter
C. vPC peer switch
D. Cisco IMC management

Answer: B

Explanation: This command specifies the hostname or IP address for the vCenter Server. Optionally, specifies the port number and VRF.
Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/layer2/6x/b_5500_Laye
r2_Config_6x/b_5500_Layer2_Config_602N12_chapter_010000.html

NEW QUESTION 250
Which protocol is the foundation for unified fabric as implemented in Cisco NX-OS?

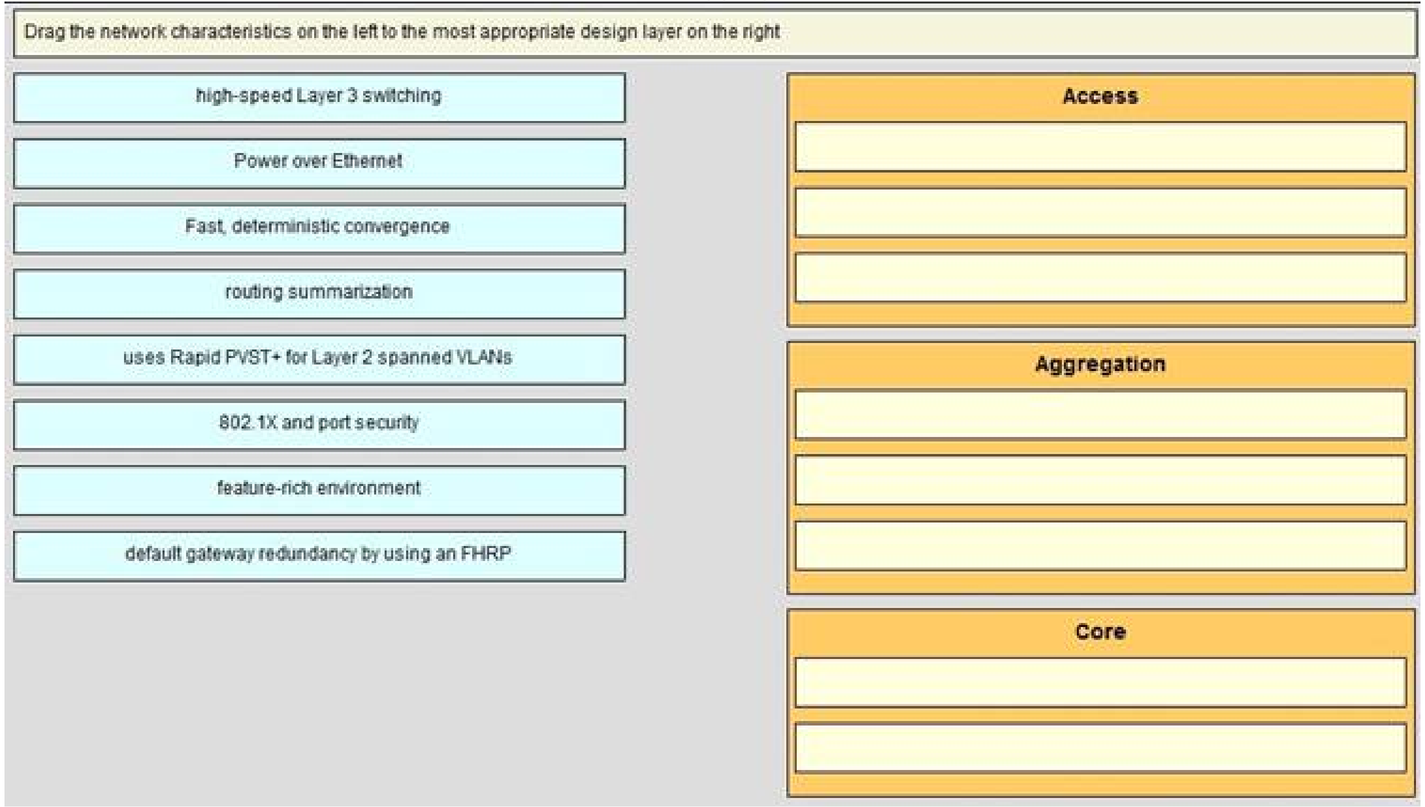
A. Fibre Channel

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

Answer: C

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

NEW QUESTION 251
DRAG DROP
Drag the network characteristics on the left to the most appropriate design layer on the right.



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

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

Access

Aggregation

Core

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 252
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 255
Which two security features are only supported on the Cisco Nexus 7000 Series Switches? (Choose two.)

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

Answer: BF

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

NEW QUESTION 257
Which statement about the implementation of Cisco TrustSec on Cisco Nexus 7000 Series Switches is true?

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

Answer: A

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

NEW QUESTION 260
In the dynamic vNIC creation wizard, why are choices for Protection important?

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

Answer: C

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

NEW QUESTION 263
How is a dynamic vNIC allocated?

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

Answer: C

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

NEW QUESTION 266

Which of the following Cisco Nexus features is best managed with DCNM-LAN?

A. VSS
B. Domain parameters
C. Virtual switches
D. AAA

Answer: C

Explanation: DCNM-LAN supports the following platforms:
• Cisco Nexus 1000V switches
• Cisco Nexus 2000 Fabric Extenders
• Cisco Nexus 3000 Series switches
• Cisco Nexus 4000 Series switches
• Cisco Nexus 5000 Series switches
• Catalyst 6500
DCNM-LAN provides limited support for the Catalyst 6500 Series switches that runs classic IOS version 12.2(33)SXI or higher.
– DCNM-LAN supports the viewing of the current configuration attributes of the device.
– DCNM-LAN does not support changing the configuration of the device.
– DCNM-LAN supports the Firewall Service Module (FWSM) version 4.0 or higher for the Catalyst 6500 Series switches.
• Cisco Nexus 7000 Series switches Reference:
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/5_2/configuration/guides
/fund/DCNM-SAN-LAN_5_2/DCNM_Fundamentals/fund_overview.html

NEW QUESTION 267
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 268
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-ofband 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 269
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 271
What is the grace period in a graceful restart situation?

A. how long the supervisor waits for NSF replies
B. how often graceful restart messages are sent after a switchover
C. how long NSF-aware neighbors should wait after a graceful restart has started before tearing down adjacencies
D. how long the NSF-capable switches should wait after detecting that a graceful restart has started, before verifying that adjacencies are still valid

Answer: C

Explanation: Graceful restart (GR) refers to the capability of the control plane to delay advertising the absence of a peer (going through control-plane switchover) for a "grace period," and thus help minimize disruption during that time (assuming the standby control plane comes up). GR is based on extensions per routing protocol, which are interoperable across vendors. The downside of the grace period is huge when the peer completely fails and never comes up, because that slows down the overall network convergence, which brings us to the final concept: nonstop routing (NSR).
NSR is an internal (vendor-specific) mechanism to extend the awareness of routing to the standby routing plane so that in case of failover, the newly active routing plane can take charge of the already established sessions.
Reference: http://www.ciscopress.com/articles/article.asp?p=1395746&seqNum=2

NEW QUESTION 274
Which two types of traffic are carried over a vPC peer link when no failure scenarios are present? (Choose two.)

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

Answer: AC

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

NEW QUESTION 279
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 282
Which function does the graceful restart feature allow a Cisco Nexus 7000 Series router to perform?

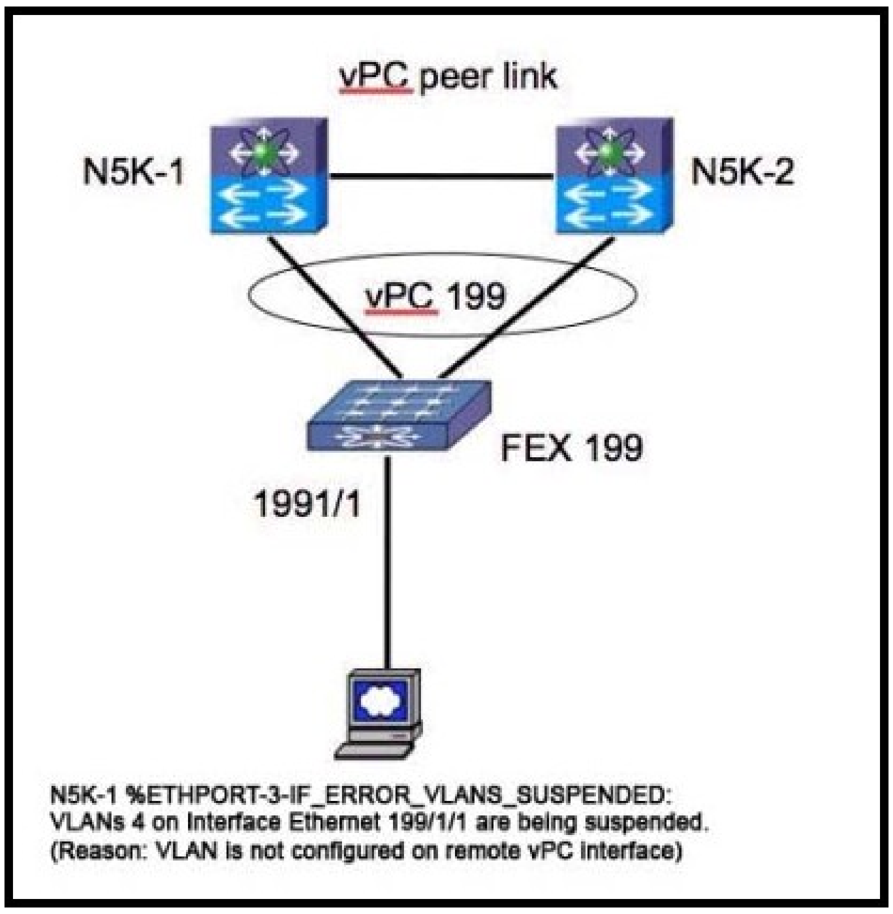
A. Perform a rapid route convergence.
B. Initialize a standby supervisor transparently when one is present.
C. Remain in the data forwarding path through a process restart.
D. Maintain a management connection throughout a router restar

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 286
Refer to the exhibit.



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

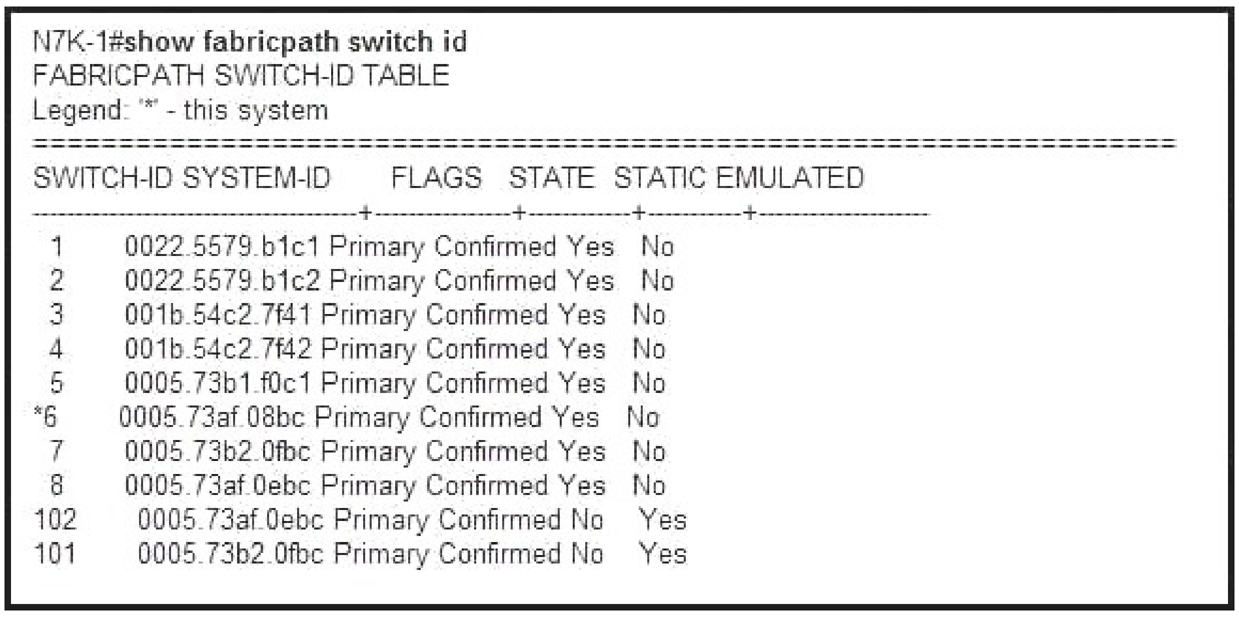
Which corrective action is taken to resolve the problem?

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

Answer: C

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

NEW QUESTION 290
Refer to the exhibit.



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

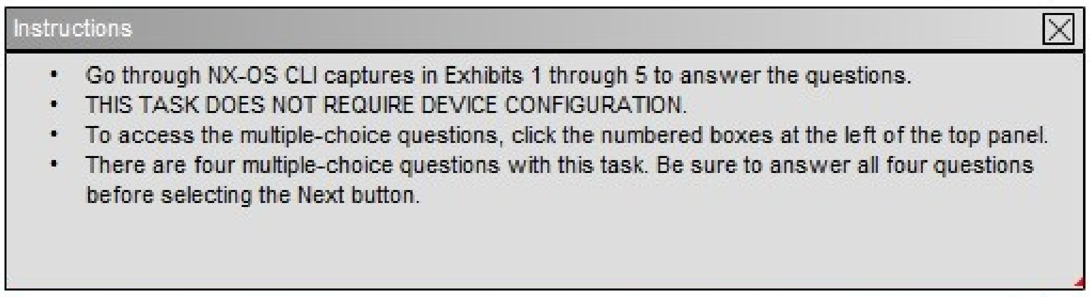
Which three statements about the Cisco Nexus 7000 switch are true? (Choose three.)

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

Answer: BDE

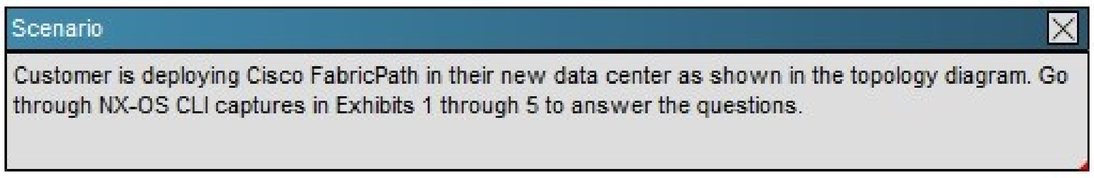
Explanation: To understand this feature, please refer to the link given below. Reference:
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/guide_c07-690079.html#wp9000065

NEW QUESTION 291
On a Cisco Nexus7000 switches what is true regarding Cisco FabricPath requirements?



Instructions

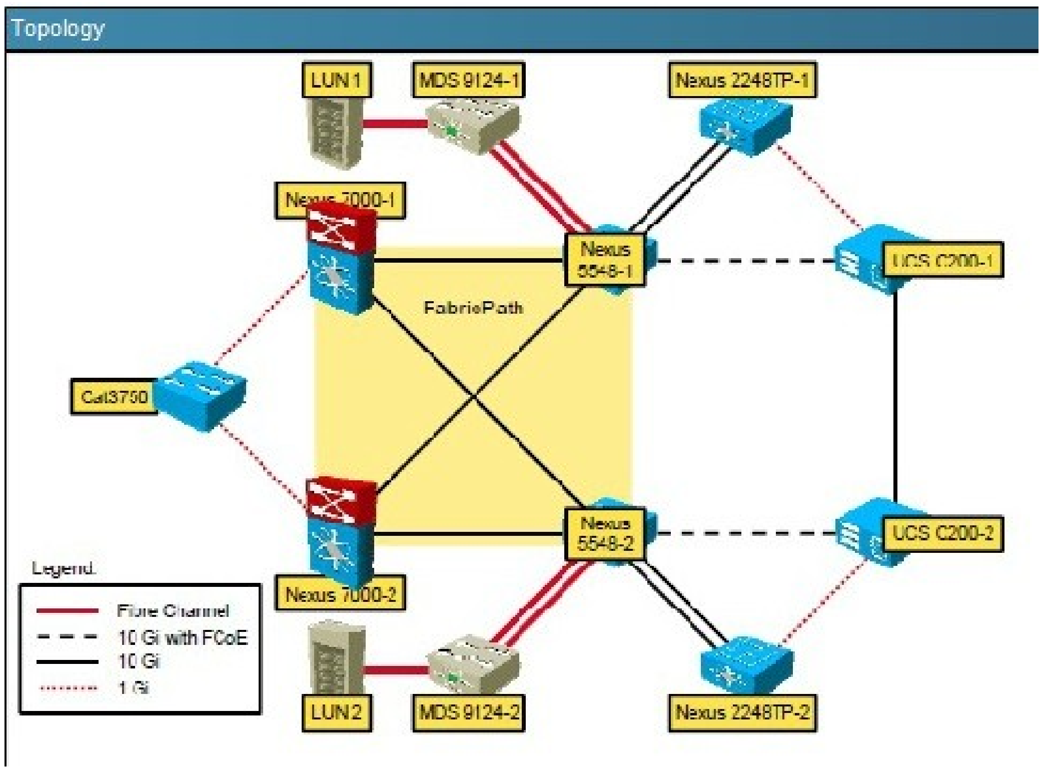
- Go through NX-OS CLI captures in Exhibits 1 through 5 to answer the questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- To access the multiple-choice questions, click the numbered boxes at the left of the top panel.
- There are four multiple-choice questions with this task. Be sure to answer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



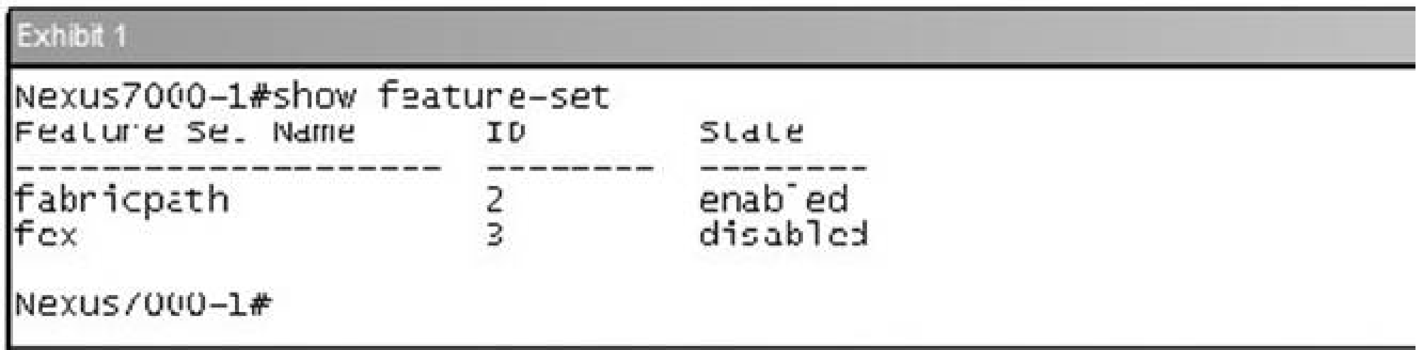


Exhibit 1

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

Nexus7000-1#
```

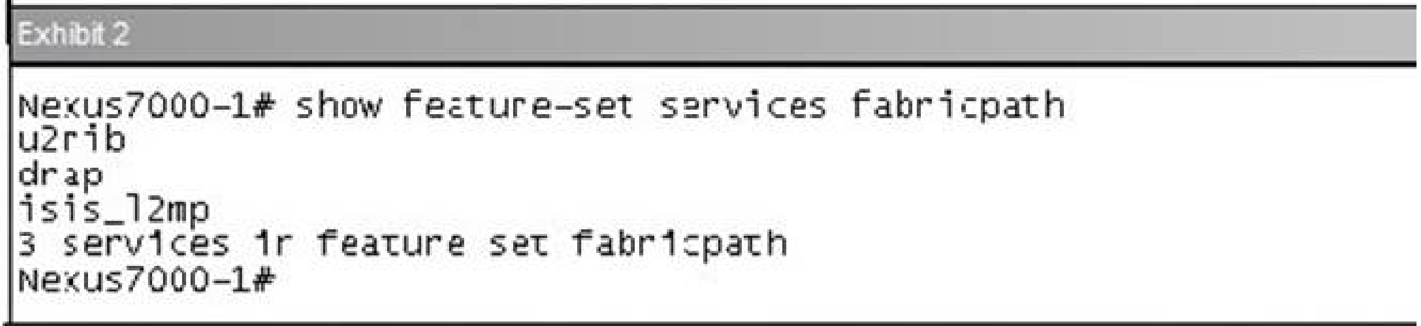


Exhibit 2

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

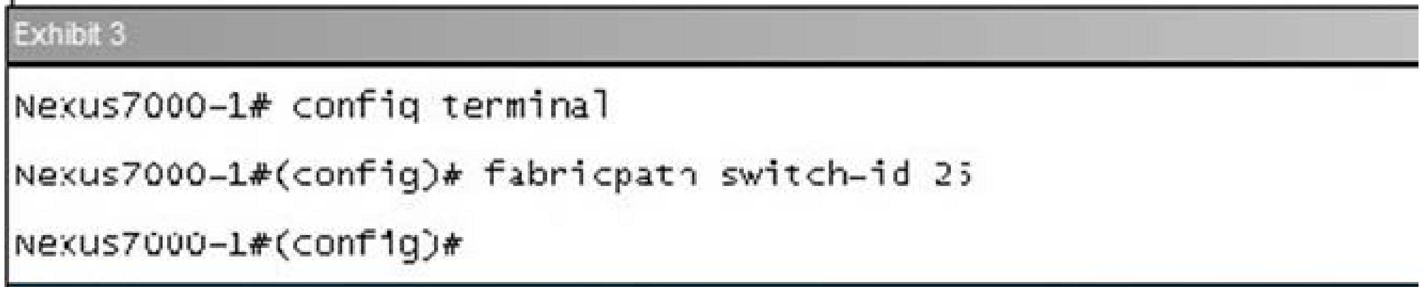


Exhibit 3

```
Nexus7000-1# config terminal

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

Nexus7000-1#(config)#
```

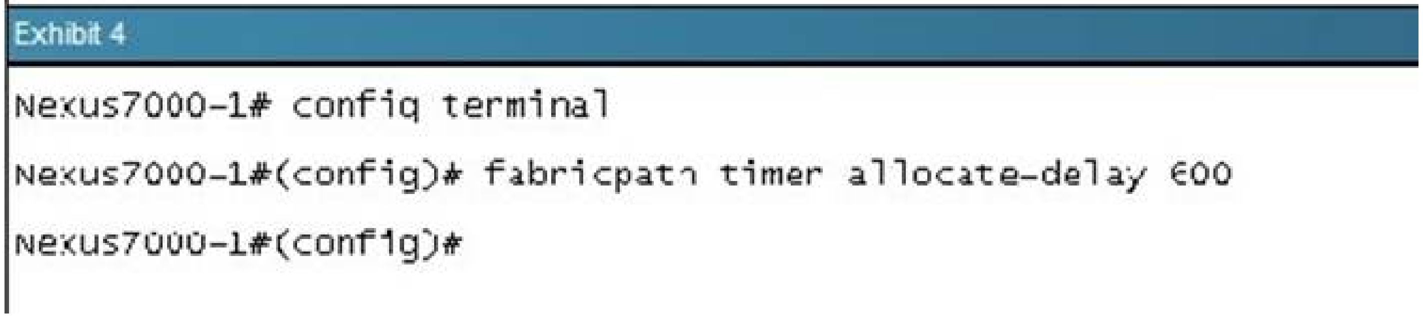


Exhibit 4

```
Nexus7000-1# config terminal

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

Nexus7000-1#(config)#
```

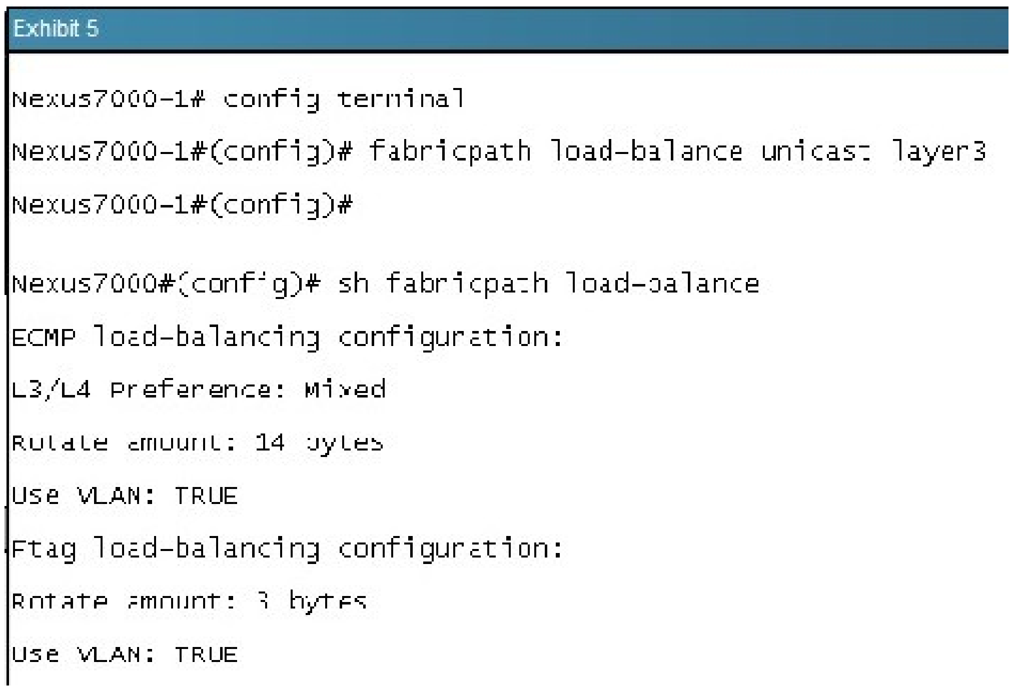


Exhibit 5

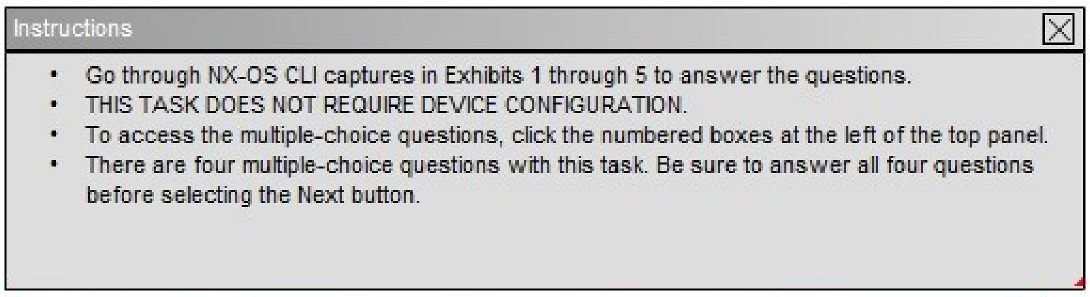
```
Nexus7000-1# config terminal
Nexus7000-1#(config)# fabricpath load-balance unicast layer3
Nexus7000-1#(config)#

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

A. 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

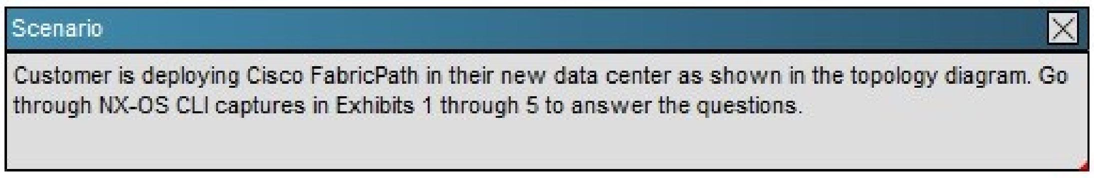
Explanation: FabricPath switching has the following prerequisites:
- You should have a working knowledge of Classical Ethernet Layer 2 functioning.
- You must install the FabricPath feature set on the default and nondefault VDC before you enable FabricPath on the switch. See Configuring Feature Set for 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 295
What is effect of the command “fabricpath load-balance unicast layer3”?



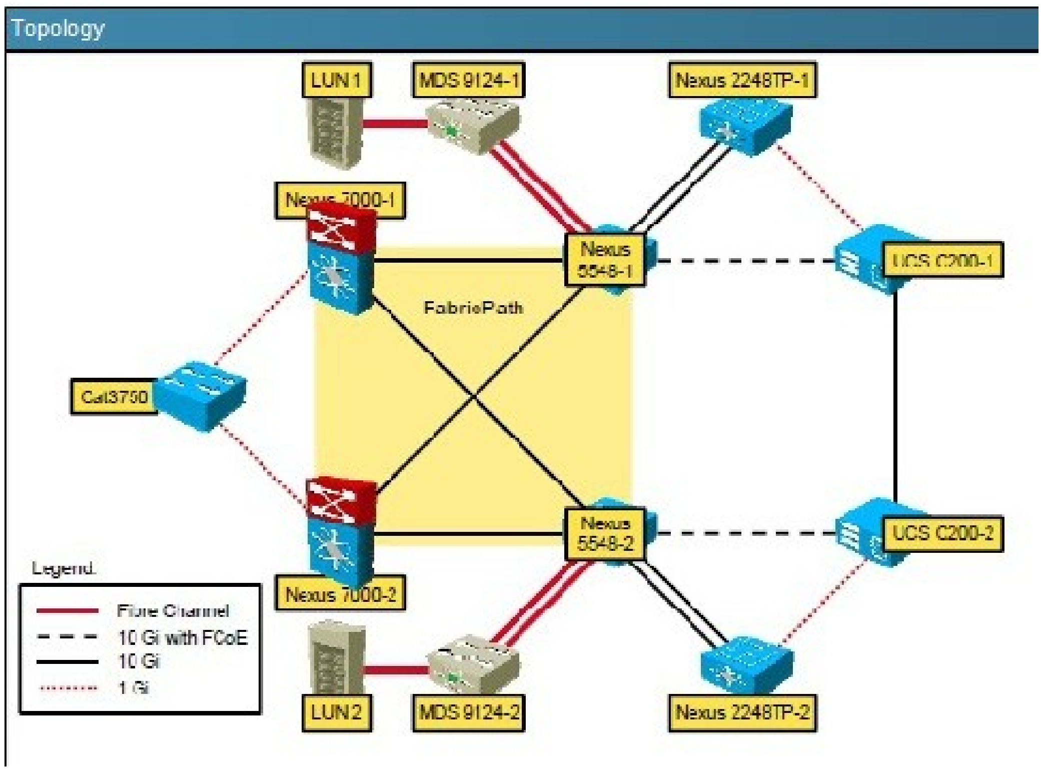
Instructions

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



Scenario

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



Topology

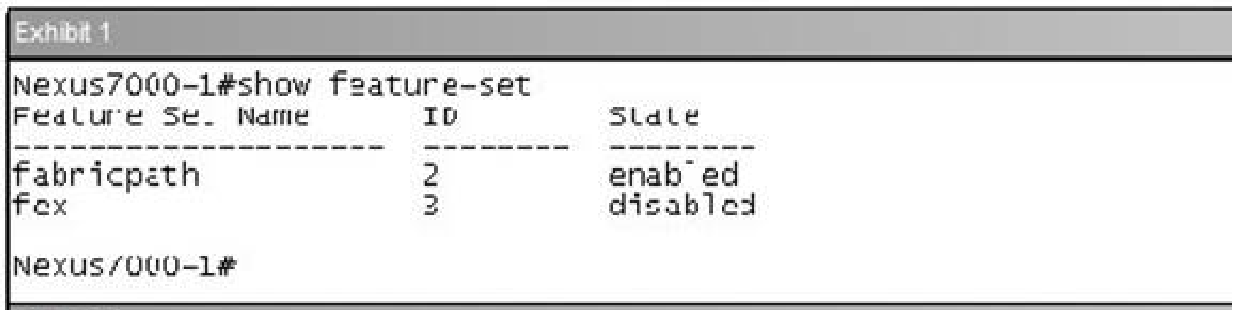


Exhibit 1

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

Nexus7000-1#
```

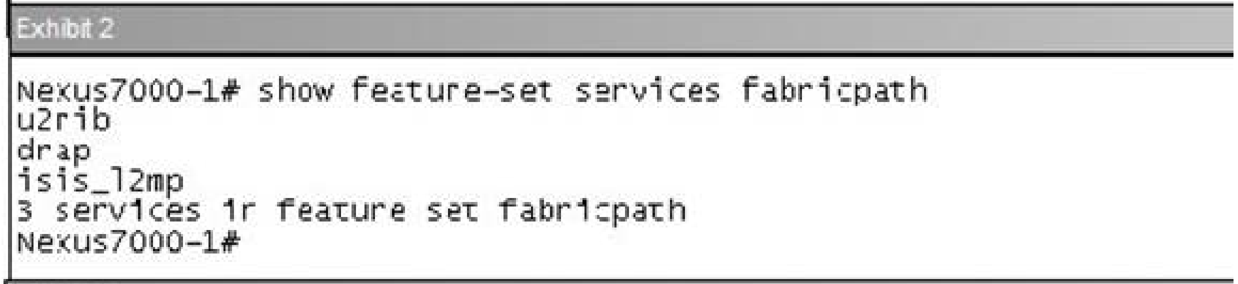


Exhibit 2

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

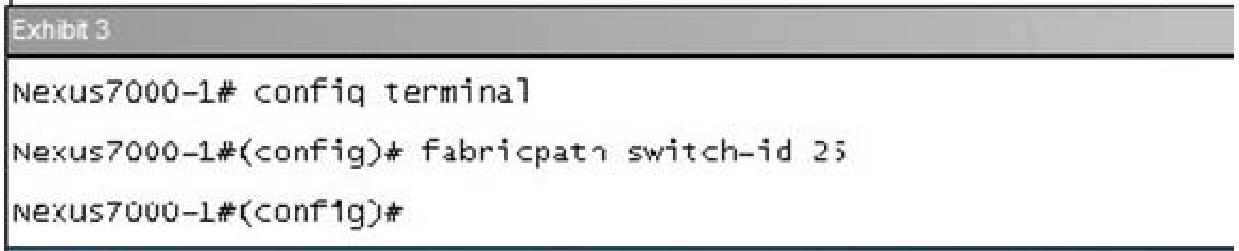


Exhibit 3

```
Nexus7000-1# config terminal

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

Nexus7000-1#(config)#
```

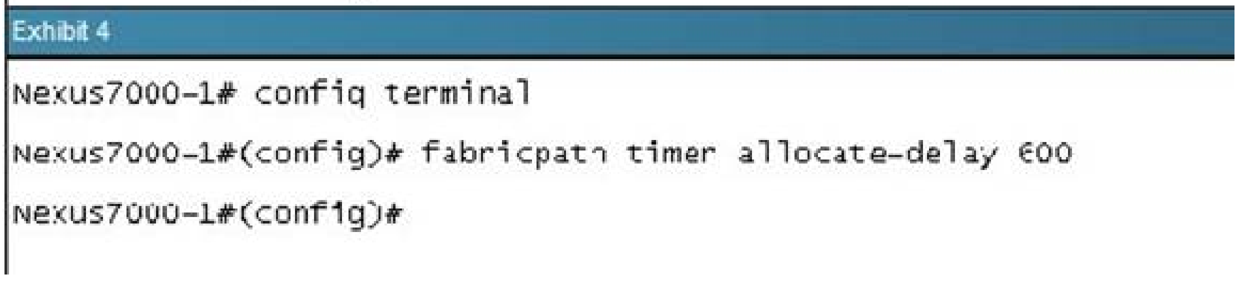


Exhibit 4

```
Nexus7000-1# config terminal

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

Nexus7000-1#(config)#
```

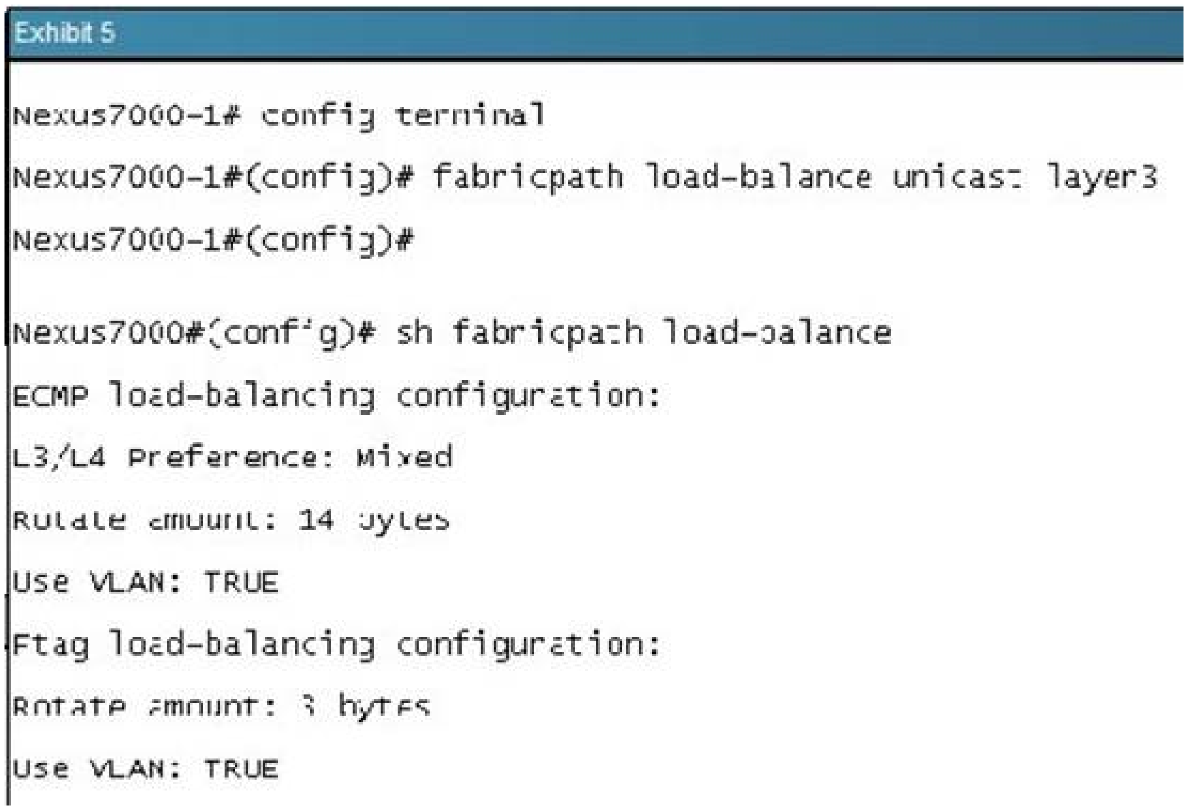


Exhibit 5

```
Nexus7000-1# config terminal

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

Nexus7000-1#(config)#


Nexus7000#(config)# sh fabricpath load-balance

ECMP load-balancing configuration:

L3/L4 Preference: Mixed

Rotate amount: 14 bytes

Use VLAN: TRUE

Ftag load-balancing configuration:

Rotate amount: 3 bytes

Use VLAN: TRUE
```

A. It configures F2 VDC FabricPath unicast load balancing
B. The command automatically load balances broadcast traffic
C. It configures F1/MI VDC FabricPath unicast load balancing
D. It configures M1 VDC FabricPath unicast load balancing

Answer: C

Explanation: The F1 cards are complemented by M1 card for routing purposes. When using M1 cards in the same virtual device context (VDC) as the F1 card, routing is offloaded to the M1 cards, and more routing capacity is added to the F1 card by putting more M1 ports into the same VDC as the F1 card.

NEW QUESTION 297
Which statement about scalability in Cisco OTV is true?

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

Answer: A

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

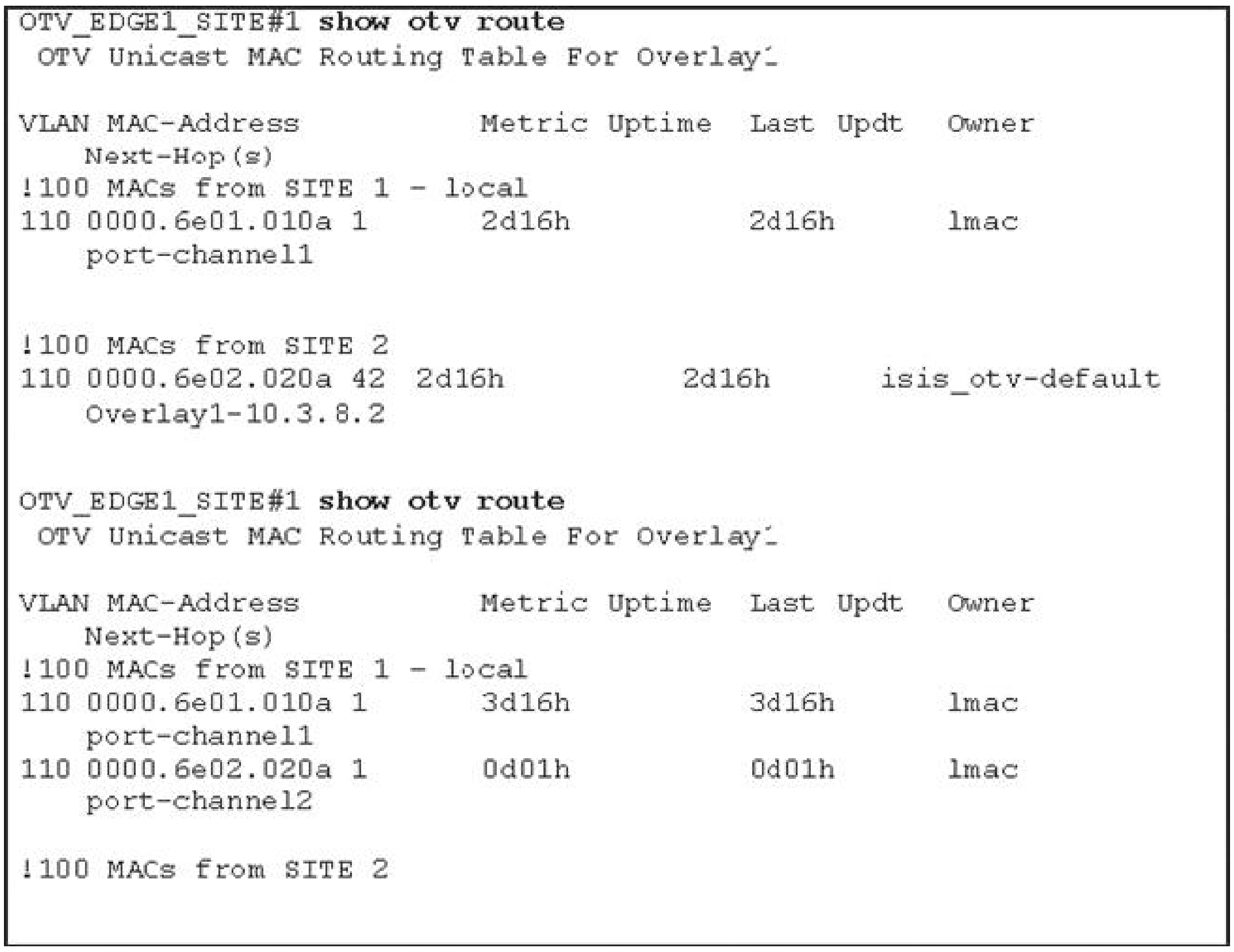
NEW QUESTION 299
Which policy-map action performs congestion avoidance?

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

Answer: D

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

NEW QUESTION 304
Refer to the exhibit.



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

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


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


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

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

!100 MACs from SITE 2
```

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

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

Answer: C

NEW QUESTION 308
What mode is required on a Cisco Nexus 7000 32-port 10-GB module port group to allow equal access to the 10-GB port controller?

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

Answer: C

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

NEW QUESTION 310
What must be enabled on the interface of a multicast-enabled device to support the Source Specific Multicast feature?

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

Answer: A

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

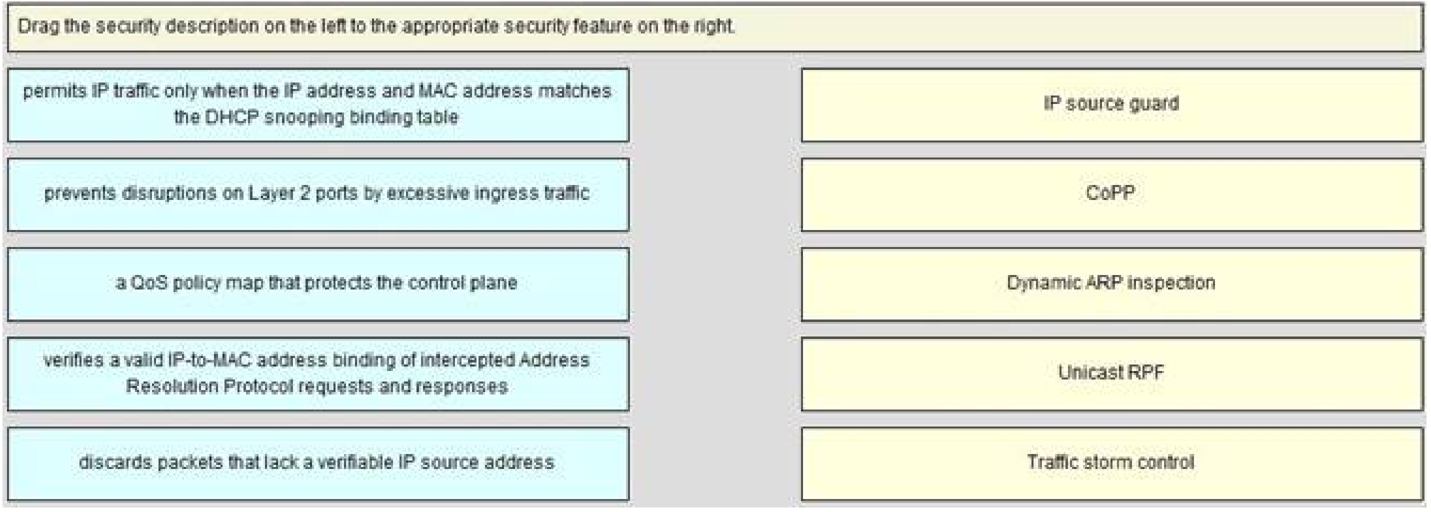
NEW QUESTION 312
Which two statements about implementing Cisco NPV and NPIV on a Cisco Nexus 5000 Series switch are true? (Choose two.)

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 313
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

prevents disruptions on Layer 2 ports by excessive ingress traffic

a QoS policy map that protects the control plane

verifies a valid IP-to-MAC address binding of intercepted Address Resolution Protocol requests and responses

discards packets that lack a verifiable IP source address

IP source guard

CoPP

Dynamic ARP inspection

Unicast RPF

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 317
Which three VDC resources can be constrained with a resource template? (Choose three.)

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

Answer: CDE

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

NEW QUESTION 322
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 327
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 332
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 335
Which three selections represent implementations of Cisco VN-Link technology? (Choose three.)

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

Answer: ACD

Explanation: The VM is powered on and resides on the ESX Host 1 with all the information stored on the shared storage.
The VM was connected to the PODy (where y is the number of your POD) PTS VDS by associating it to port group VLAN61 that was created on the Cisco Nexus 5548 device. The VM has been connected to the vPC system automatically using a VN-Link in the hardware in PTS mode or in VM-FEX mode.
The VEM bits are used in PTS mode to connect the VM VNIC to the VMNIC interface.
In this case, the VMNIC interface is not a real VMNIC but a dynamic VNIC that is presented as an interface to the ESX OS. The dynamic VNIC is enabled when the Cisco UCS VIC creates and configures the VNIC parameters inherited from port group VLAN61.
Reference: http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1
/n5k_ops_vmfex.html

NEW QUESTION 338
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 342
How does an FCoE end node acquire its FCoE MAC address?

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

Answer: C

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

NEW QUESTION 343
Which FCoE component is responsible for the encapsulation and de-encapsulation of Fibre Channel frames in Ethernet?

A. distributed FCF
B. FCoE node
C. FCoE logical endpoint
D. Fibre Channel forwarder
E. FCoE forwarder

Answer: C

Explanation: The FCoE Logical Endpoint (FCoE_LEP) is responsible for the encapsulation and deencapsulation functions of the FCoE traffic. FCoE_LEP has the

standard Fibre Channel layers, starting with FC-2 and continuing up the Fibre Channel Protocol stack.
Reference:
https://www.safaribooksonline.com/library/view/ccna-dataQuestions& Answers PDF P-106 center/9780133860429/ch11lev3sec5.html

NEW QUESTION 346
Between which two types of ports does FIP establish Fibre Channel virtual links? (Choose two.)

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

Answer: AC

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

NEW QUESTION 347
Which two reasons explain why a server on VLAN 10 is unable to join a multicast stream that originates on VLAN 20? (Choose two.)

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

Answer: AC

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

NEW QUESTION 348
Which two statements about SAN zoning on Cisco Nexus switches are true? (Choose two.)

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

Answer: BE

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

NEW QUESTION 351
Which two statements about SAN zoning on Cisco Nexus switches are true? (Choose two.)

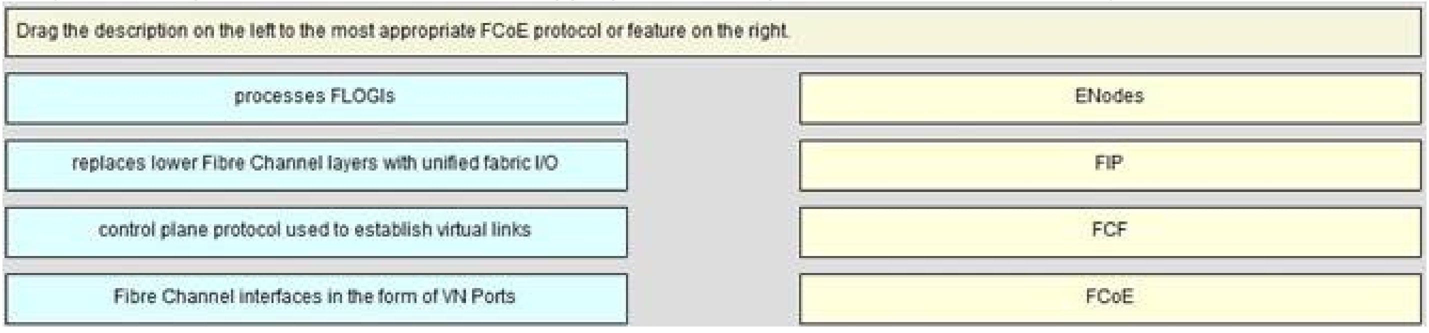
A. Zoning is enforced by examining the destination ID field.
B. Devices can only belong to one zone.
C. Only one zone set can be activated at any time.
D. A zone can only be a member one zone set.
E. Zoning must be administered from the primary SAN switch in the fabric.

F. Zone configuration changes are nondisruptiv

Answer: CF

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

NEW QUESTION 353
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
replaces lower Fibre Channel layers with unified fabric I/O
control plane protocol used to establish virtual links
Fibre Channel interfaces in the form of VN Ports

ENodes
FIP
FCF
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 354
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 359
Which four options are capabilities of the Cisco Nexus 5000 and 5500 Series Switch? (Choose four.)

A. line rate
B. managed by a parent switch
C. lossless 10 Gigabit Ethernet
D. lossless 100 Gigabit Ethernet
E. low latency
F. extremely low latency
G. hosts a virtual supervisor module

Answer: ACEG

NEW QUESTION 362
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 364
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 368
Which configuration is specific to Cisco TelePresence System seed devices?

A. radius server radius-server-name
B. aaa session-id common
C. radius-server vsa send authentication
D. aaa new-model

Answer: A

NEW QUESTION 373
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 375
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 380
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 382
Which three options are CallHome predefined destination profiles that are supported on Cisco NXOS? (Choose three.)

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

Answer: ABD

NEW QUESTION 383
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 386
Which command specifies a load-balancing method based on the MAC address of a host where the same forwarder is always used for a particular host while the number of GLBP group members remains unchanged?

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

Answer: A

NEW QUESTION 387
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 391
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 por

Answer: BC

NEW QUESTION 394
Which four statements about reserved VLANs in Cisco NX-OS are true? (Choose four.)

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

Answer: CEFG

NEW QUESTION 399
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 400
In OTV, how are the VLANs split when a site has two edge devices?

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

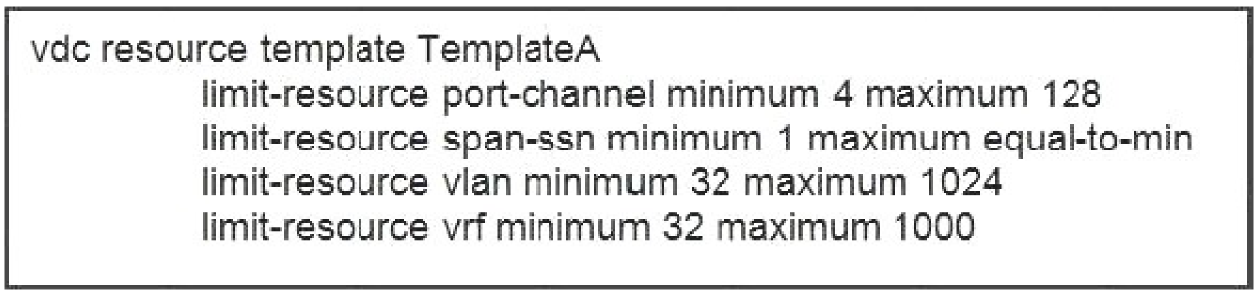
Answer: C

NEW QUESTION 404
Which statement about the MPLS feature set is true?

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

Answer: D

NEW QUESTION 407
Refer to the exhibit.



```
vdc resource template TemplateA
          limit-resource port-channel minimum 4 maximum 128
          limit-resource span-ssn minimum 1 maximum equal-to-min
          limit-resource vlan minimum 32 maximum 1024
          limit-resource vrf minimum 32 maximum 1000
```

What is the maximum IPv6 unicast route memory allocated?

A. 4 MB
B. 8 MB
C. 1024 MB
D. 1 GB
E. 5 MB

Answer: A

NEW QUESTION 412
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 416
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 420
Which standard has Cisco used to implement VM-FEX?

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

Answer: A

NEW QUESTION 424
During the design of a new Cisco Data Center Network, a customer asked when VM-FEX would be used with Cisco Nexus 1000V Switch. Which scenario is most appropriate?

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

Answer: C

NEW QUESTION 428
Which two actions are required before FIPS is configured in Cisco MDS? (Choose two.)

A. Passwords must be a minimum of 10 characters in length.
B. SNMP v2 or v3 must be enabled.
C. Remote authentication must occur utilizing RADIUS/TACACS+.
D. Disable VRRP.
E. Delete all SSH server RSA key pairs.
F. Delete all IKE policies utilizing MD5 or DES for encryption.
G. Enable the FC-FIPS feature.
H. Disable SS

Answer: DF

NEW QUESTION 430
If vPC peer keepalives are used between vPC peers, which VRF is used by default?

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

Answer: A

NEW QUESTION 433
Using the default VDC high-availability options in the Cisco Nexus 7010 switch, which event occurs after a VDC failure?

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

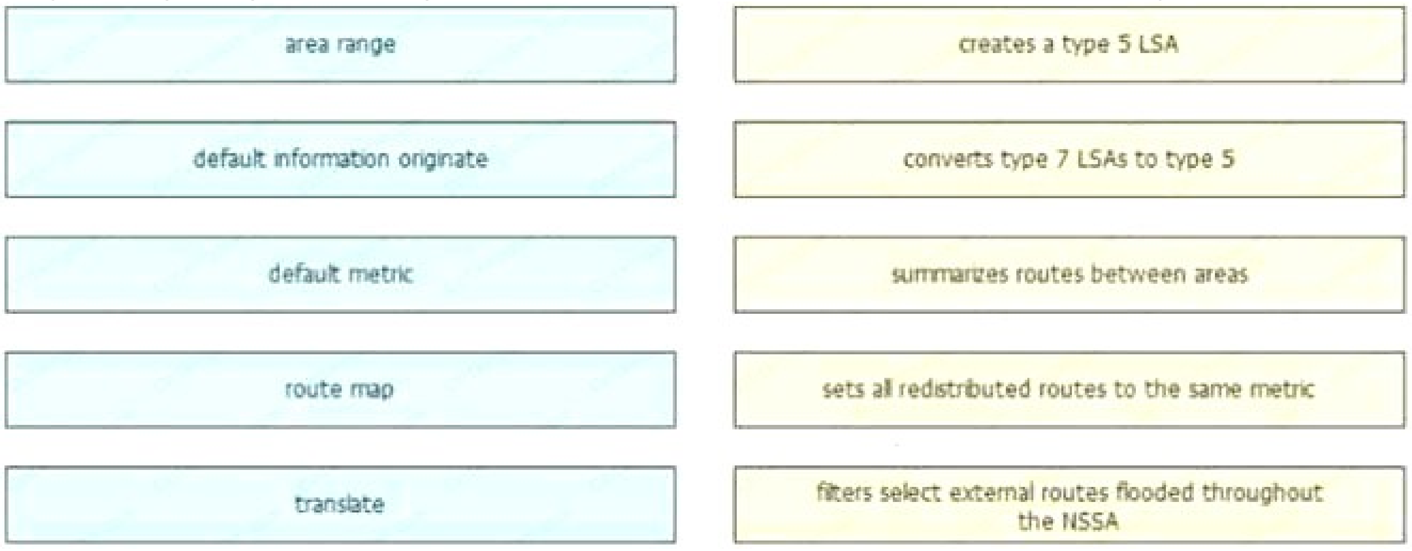
Answer: D

NEW QUESTION 434
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

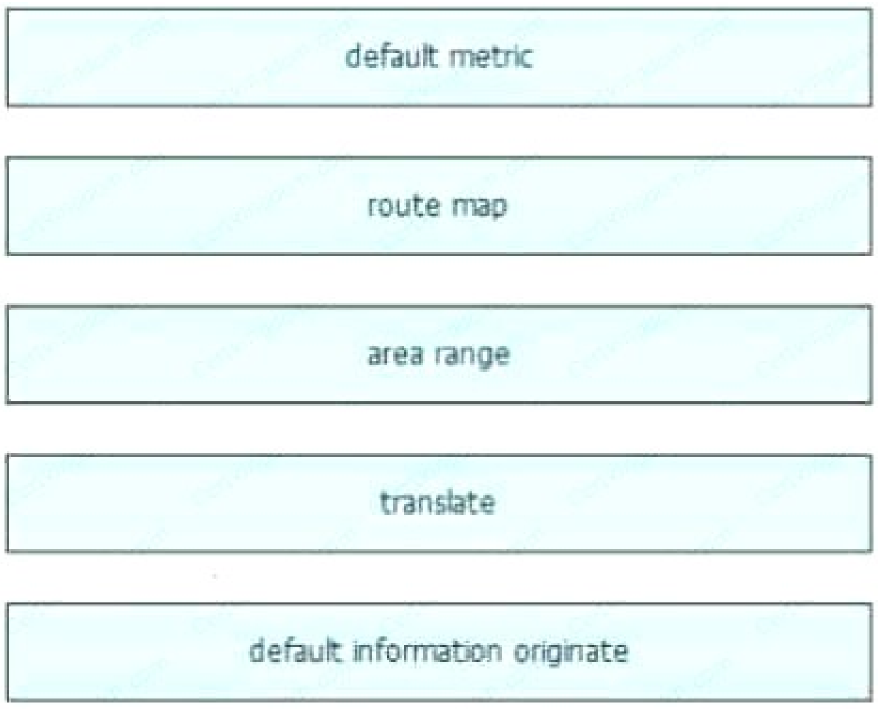
NEW QUESTION 435
DRAG DROP
Drag and drop the optional OSPF parameters from the left onto the correct functions on the right.



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

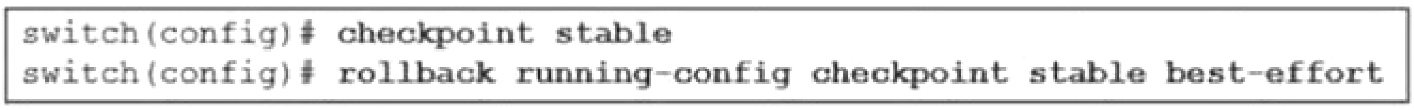
default information originate

NEW QUESTION 440
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 441
Refer to the exhibit.



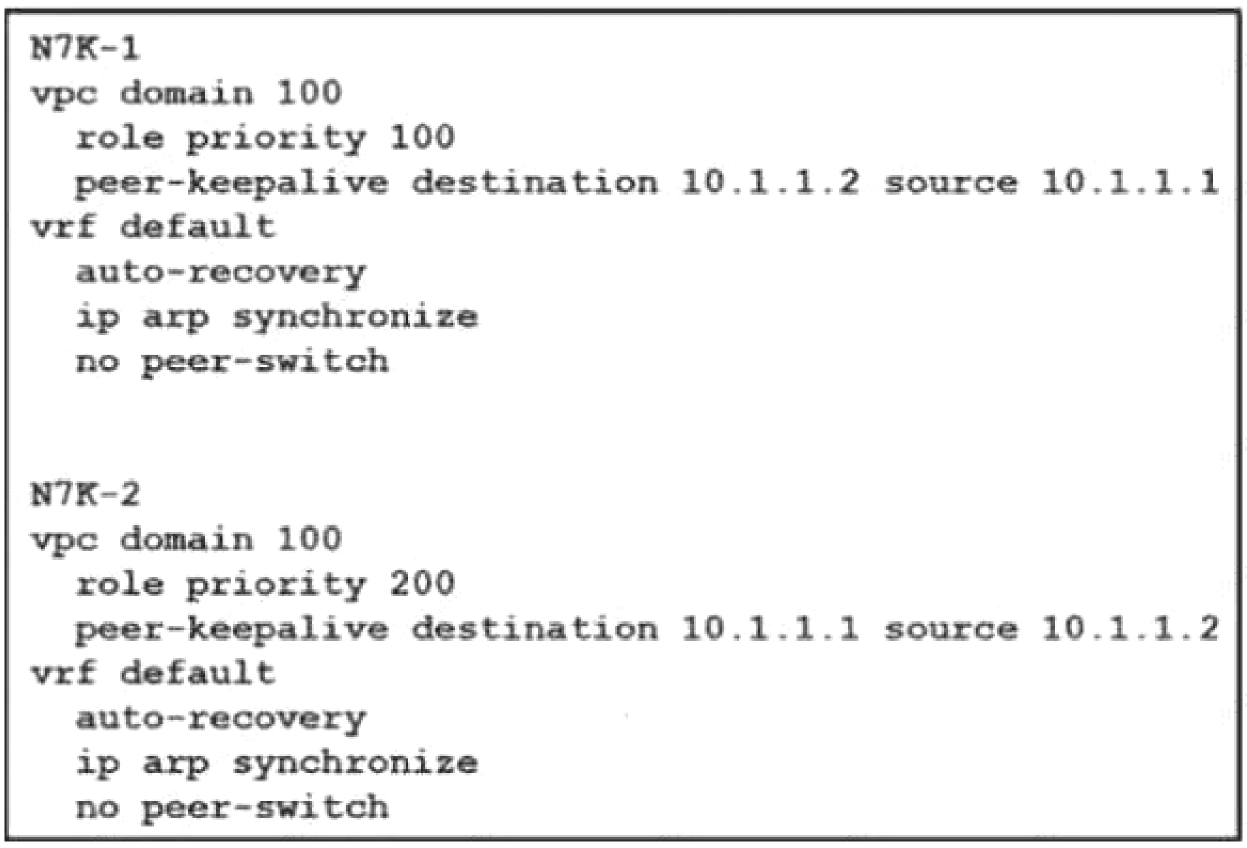
```
switch(config)# checkpoint stable
switch(config)# rollback running-config checkpoint stable best-effort
```

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 446
Refer to the exhibit.



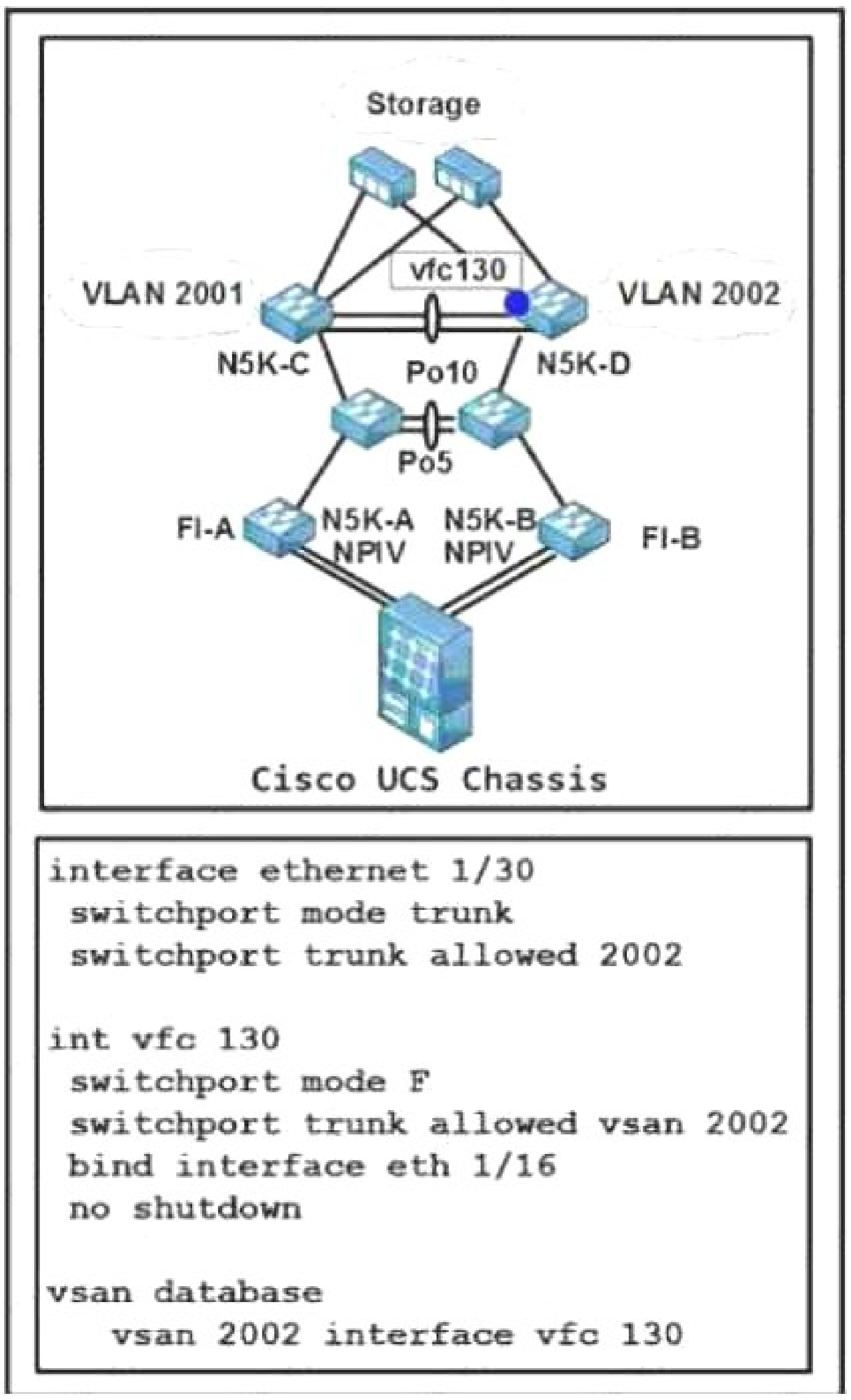
```
N7K-1
vpc domain 100
  role priority 100
  peer-keepalive destination 10.1.1.2 source 10.1.1.1
vrf default
  auto-recovery
  ip arp synchronize
  no peer-switch


N7K-2
vpc domain 100
  role priority 200
  peer-keepalive destination 10.1.1.1 source 10.1.1.2
vrf default
  auto-recovery
  ip arp synchronize
  no peer-switch
```

Which result occurs if N7K-2 fails and then recovers?

A. The vPC on N7K-2 requires additional time to come back online.
B. N7K-1 performs a local replication of the MAC address of the interface VLAN defined on N7K-2.
C. N7K-2 attempts to become the primary vPC peer
D. An ARP bulk synchronization is performed by using CF

Answer: D

NEW QUESTION 447
Refer to the exhibit.



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

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

vsan database
   vsan 2002 interface vfc 130
```

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

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

Answer: C

NEW QUESTION 450
......