

PDFVCE



Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarantee in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

<http://www.pdfvce.com>

Highly Efficiently Exam Tool and Effective Exam Practice Materials

Exam : **642-997**

Title : **Implementing Cisco Data
Center Unified Fabric (DCUFI)**

Vendor : **Cisco**

Version : **DEMO**

NO.1 Which two options are limitations of NetFlow Version 5? (Choose two.)

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

Answer: A,B

NO.2 Which item is gathered in the Cisco DCNM initial discovery process?

- A. response time from the device
- B. only Cisco NXOS devices on the network
- C. running configuration
- D. show tech-support output from discovery devices

Answer: C

NO.3 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 interfaces.

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

NO.4 Which management feature provides these functions?

- * Direct paging of network support engineers
- * Email notifications to a network operations center
- * Direct Service Request generation with the Cisco TAC

- A. scripting along with the scheduler feature
- B. RSA
- C. Call Home
- D. SNMP traps

Answer: C

NO.5 What is the Overlay Transport Virtualization site VLAN used for?

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

Answer: D

NO.6 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: A,C

NO.7 Refer to the exhibit.

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

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

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

- A. Nothing, this is the standard vPC configuration to make the feature work.
- B. The downstream device detects only one of the vPC peers as its gateway.
- C. The downstream device can use DMAC of N7K-1 on the link to N7K-2, and N7K-2 forwards the packet.
- D. This configuration enables the downstream device to use DHCP to obtain its default gateway.

Answer: C

Explanation:

Beginning with Cisco NX-OS 4.2(1), you can configure vPC peer devices to act as the gateway even for packets that are destined to the vPC peer device's MAC address. Use the peer-gateway command to configure this feature.

Some network-attached storage (NAS) devices or load-balancers may have features aimed to optimize the performances of particular applications. Essentially these features avoid performing a routing-table lookup when responding to a request that originated from a host not locally attached to the same subnet. Such devices may reply to traffic using the MAC address of the sender Cisco Nexus 7000 device rather than the common HSRP gateway.

Such behavior is non-complaint with some basic Ethernet RFC standards. Packets reaching a vPC device for the non-local router MAC address are sent across the peer-link and could be dropped by the built in vPC loop avoidance mechanism if the final destination is behind another vPC.

The vPC peer-gateway capability allows a vPC switch to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer. This feature enables local forwarding of such packets without the need to cross the vPC peer-link. In this scenario, the feature optimizes use of the peer-link and avoids potential traffic loss.

Configuring the peer-gateway feature needs to be done on both primary and secondary vPC peers and is non-disruptive to the operations of the device or to the vPC traffic. The vPC peer-gateway feature can be configured globally under the vPC domain submodule.

When enabling this feature it is also required to disable IP redirects on all interface VLANs mapped over a vPC VLAN to avoid generation of IP redirect messages for packets switched through the peer gateway router. When the feature is enabled in the vPC domain, the user is notified of such a requirement through an appropriate message.

Packets arriving at the peer-gateway vPC device will have their TTL decremented, so packets carrying TTL = 1 may be dropped in transit due to TTL expire. This needs to be taken into account when the peer-gateway feature is enabled and particular network protocols sourcing packets with TTL = 1 operate on a vPC VLAN.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/interfaces/configuration/guide/if_nxos/if_vPC.html

NO.8 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

NO.9 Which task must be done before a zone set takes effect?

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

Answer: D

NO.10 DRAG DROP

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

Drag the description on the left to the most appropriate Nexus product on the right.	
Supports the SAN infrastructure	Cisco Nexus 5000 Series Switches
Offers complete routing and core services	Cisco Nexus 7000 Series Switches
Includes native Fibre Channel interfaces	Cisco Nexus 2000 Series Fabric Extenders
Provides I/O consolidation	Cisco MDS 9500 Series Multilayer Directors
A virtual machine-aware software switch	Cisco Nexus 1000V Series Switches

Answer:

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

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

NO.11 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

NO.12 Which feature allows routing protocols to remain in the data path during a supervisor failover?

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

Answer: A

NO.13 Which three options are CallHome predefined destination profiles that are supported on Cisco NX-OS? (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: A,B,D

NO.14 Which command is used to associate EID-to-RLOC for a LISP site?

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

Answer: C

NO.15 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-sensitive.

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_NX-OS_Security_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_Security_Configuration_Guide_7x_chapter_01000.pdf

NO.16 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 device.

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-interconnect-options.html>