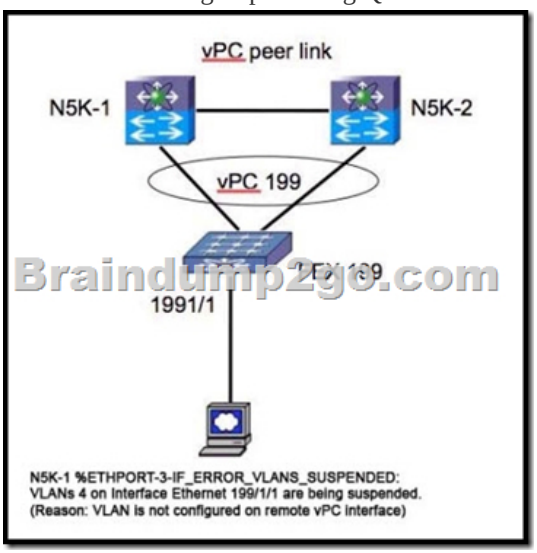
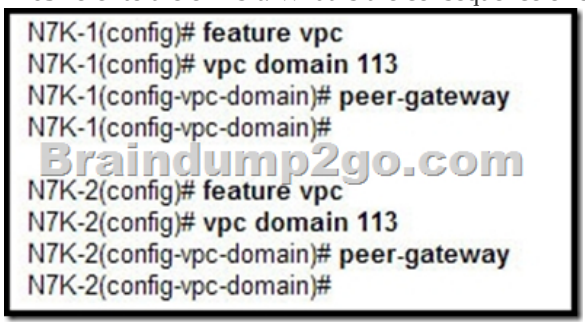
[2017-Aug.-Updated100% Exam Pass-300-165 VCE and 300-165 PDF Free from Braindump2go[61-70

2017 August New 300-165 Exam Dumps with PDF and VCE Free Updated Today! Following are some new 300-165 Questions:
1.|2017 New 300-165 Exam Dumps (PDF & VCE) 174Q&As Download:https://www.braindump2go.com/300-165.html 2.|2017 New 300-165 Exam Questions and Answers Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNRU9xWGk1cFJiaTg?usp=sharing QUESTION 61Refer to the exhibit. Which corrective action is taken to resolve the problem?

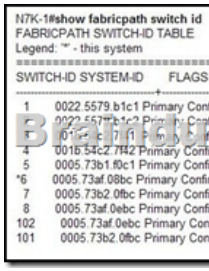


A. Trunk four VLANs on interface ethernet 199/1/1.B. Use the shut and no shut interface ethernet 199/1/1so that the VLANs come up.C. Place interface ethernet 199/1/1 in VLAN 4 in the N5K-2 configuration.D. Prune all but four VLANs from vPC 199. E. Add VLAN 4 to vPC 199. Answer: CExplanation:Place interface ethernet 199/1/1 in VLAN 4 in the N5K-2 configuration. QUESTION 62What is an Overlay Transport Virtualization extended VLAN? A. the VLAN used to locate other AEDsB. the VLAN used to access the overlay network by the join interfaceC. the user VLAN that exists in multiple sitesD. the VLAN that must contain the overlay interface Answer: C QUESTION 63Refer to the exhibit. 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: CExplanation: Beginning with Cisco NX-OS 4.2(1), you can configure vPC peer devices to act as the gateway even for packets that are destined to the vPC peer device's MAC address. Use the peer-gateway command to configure this feature.Some network-attached storage (NAS) devices or load-balancers may have features aimed to optimize the performances of particular applications. Essentially these features avoid performing a routing-table lookup when responding to a request that originated form a host not locally attached to the same subnet. Such devices may reply to traffic using the MAC address of the sender Cisco Nexus 7000 device rather than the common HSRP gateway. Such behavior is non-complaint with some basic Ethernet RFC standards. Packets reaching a vPC device for the non-local router MAC address are sent across the peer-link and could be dropped by the built in vPC loop avoidance mechanism if the final destination is behind another vPC. The vPC peer-gateway capability allows a vPC switch to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer. This feature enables local forwarding of such

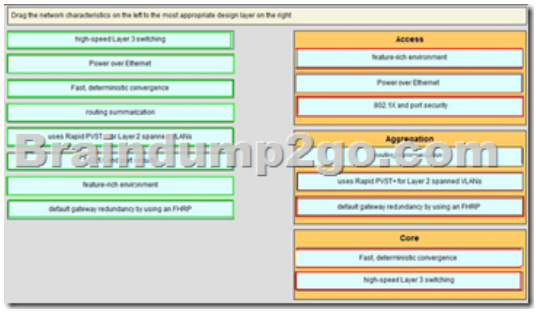
packets without the need to cross the vPC peer-link. In this scenario, the feature optimizes use of the peer-link and avoids potential traffic loss. Configuring the peer-gateway feature needs to be done on both primary and secondary vPC peers and is non-disruptive to the operations of the device or to the vPC traffic. The vPC peer-gateway feature can be configured globally under the vPC domain submode. When enabling this feature it is also required to disable IP redirects on all interface VLANs mapped over a vPC VLAN to avoid generation of IP redirect messages for packets switched through the peer gateway router. When the feature is enabled in the vPC domain, the user is notified of such a requirement through an appropriate message. Packets arriving at the peer-gateway vPC device will have their TTL decremented, so packets carrying TTL = 1 may be dropped in transit due to TTL expire. This needs to be taken into account when the peer-gateway feature is enabled and particular network protocols sourcing packets with TTL = 1 operate on a vPC VLAN.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_2/nx-os/interfaces/configuration/guide/if_nxos/if_vPC.html
QUESTION 64Refer to the exhibit. Which three statements about the Cisco Nexus 7000 switch are true? (Choose three.)



A. An emulated switch ID must be unique when the vPC+ feature is used.B. Switches with FabricPath and vPC+ consume two switch IDs.C. Emulated switch IDs must be numbered from 1 to 99.D. Each switch ID must be unique in the FabricPath topology.E. Switch IDs must be configured manually. Answer: BDEExplanation:To understand this feature, please refer to the link given below.
http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/guide_c07-690079.html#wp9000065
QUESTION 65Which statement about core-edge SAN topology is true? A. Converged FCoE links connect the core and edge MDS switches.B. The SAN core connects to the network aggregation layer.C. Separate links with the same I/O are used for SAN and LAN traffic.D. Storage devices are accessed via FCoE over the LAN network. Answer: BExplanation:The Aggregation layer of the data center provides connectivity for the Access layer switches in the server farm, an aggregates them into a smaller number of interfaces to be connected into the Core layer. In most data center environments, the Aggregation layer is the transition point between the purely Layer 3 routed Core layer, and the Layer 2-switched Access layer. 802.1Q trunks extend the server farm VLANs between Access and Aggregation layers. The Aggregation layer also provides a common connection point to insert services into the data flows between clients and servers, or between tiers of servers in a multi-tier application. QUESTION 66What configuration is required when implementing FCoE? A. disable LAN traffic on the interfaceB. configure PortFast on the access portC. permit all VLANs on the interfaceD. permit all VSANs on the interface Answer: AExplanation:DCBX allows the switch to send a LAN Logical Link Status (LLS) message to a directly-connected CNA. Enter the shutdown lan command to send an LLS-Down message to the CNA. This command causes all VLANs on the interface that are not enabled for FCoE to be brought down. If a VLAN on the interface is enabled for FCoE, it continues to carry SAN traffic without any interruption.
http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/fcoe/b_Cisco_Nexus_5000_Series_NX-OS_Fibre_Channel_over_Ethernet_Configuration_Guide_/Cisco_Nexus_5000_Series_NX-OS_Fibre_Channel_over_Ethernet_Configuration_Guide__chapter3.html QUESTION 67Drag and Drop QuestionDrag the network characteristics on the left to the most appropriate design layer on the right.



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. QUESTION 68Which topology is not supported when using vPC? A. a single-homed server to a single FEX that is connected to two Cisco Nexus 5500 Series SwitchesB. a dual-homed server to two FEXs, each connected to two Cisco Nexus 5500 Series SwitchesC. a dual-homed server to two FEXs that are connected to one Cisco Nexus 5500 Series SwitchD. a dual-homed server to a single FEX that is connected to two Cisco Nexus 5500 Series Switches Answer: CExplanation:The figure shows unsupported topology where a vPC is between hosts and two FEXs that are connected to one Cisco Nexus 5500 Series device. This topology does not provide a good high availability solution because the server loses the connectivity to the network when the Cisco Nexus 5000 Series device fails.If you need to connect a multi-homing server to a pair of FEXs when there is only one Cisco Nexus 5000 Series device, you have the option to run active or standby NIC teaming from the server.http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/mkt_ops_guides/513_n1_1/n5k_enhanced_vpc.html QUESTION 69Which protocol is the foundation for unified fabric as implemented in Cisco NX-OS? A. Fibre ChannelB. Data Center BridgingC. Fibre Channel over EthernetD. N proxy virtualizationE. N Port identifier virtualization Answer: CExplanation: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. http://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/white_paper_c11-495142.html QUESTION 70Drag and Drop QuestionDrag the description on the left to the most appropriate FCoE protocol or feature on the right.



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. !!!RECOMMEND!!! 1.|2017 New 300-165 Exam Dumps (PDF & VCE) 174Q&As Download:https://www.braindump2go.com/300-165.html 2.|2017 New 300-165 Study Guide Video: YouTube Video: YouTube.com/watch?v=IyG8YCqJDdc