[March-2019-New300-115 Free VCE Dumps from Braindump2go

2019/March Braindump2go 300-115 Exam Dumps with PDF and VCE New Updated Today! Following are some new 300-115 Real Exam Questions:1.|2019 Latest 300-115 Exam Dumps (VCE & PDF) Instant Download: https://www.braindump2go.com/300-115.html2.|2019 Latest 300-115 Exam Questions & Answers Instant Download: https://drive.google.com/drive/folders/0B75b5xYLjSSNYjV4eHQ4dTJoQXc?usp=sharing New QuestionWhen you design a switched network using VTPv2, how many VLANs can be used to carry user traffic?A. 1000B. 1001C. 1024D. 2048E. 4095F. 4096Answer: BExplanation:VTP versions 1 and 2 Supports normal VLAN numbers (1-1001).Only VTP version 3 supports extended VLANs (1-4095).New QuestionWhat does the command vlan dot1q tag native accomplish when configured under global configuration?A. All frames within the native VLAN are tagged, except when the native VLAN is set to 1.B. It allows control traffic to pass using the non-default VLAN.C. It removes the 4-byte dot1q tag from every frame that traverses the trunk interface(s).D. Control traffic is tagged.Answer: DExplanation:The "vlan dot1q tag native" will tag all untagged frames, including control traffic, with the defined native VLAN.New QuestionWhich private VLAN access port belongs to the primary VLAN and can communicate with all interfaces, including the community and isolated host ports?A. promiscuous portB. isolated portC. community portD. trunk portAnswer: AExplanation:The types of private VLAN ports are as follows:Promiscuous--A promiscuous port belongs to the primary VLAN. The promiscuous port can communicate with all interfaces, including the community and isolated host ports, that belong to those secondary VLANs associated to the promiscuous port and associated with the primary VLAN. You can have several promiscuous ports in a primary VLAN. Each promiscuous port can have several secondary VLANs, or no secondary VLANs, associated to that port. You can associate a secondary VLAN to more than one promiscuous port, as long as the promiscuous port and secondary VLANs are within the same primary VLAN. You may want to do this for load-balancing or redundancy purposes. You can also have secondary VLANs that are not associated to any promiscuous port.Isolated--An isolated port is a host port that belongs to an isolated secondary VLAN. This port has complete isolation from other ports within the same private VLAN domain, except that it can communicate with associated promiscuous ports. Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports. You can have more than one isolated port in a specified isolated VLAN. Each port is completely isolated from all other ports in the isolated VLAN.Community--A community port is a host port that belongs to a community secondary VLAN. Community ports communicate with other ports in the same community VLAN and with associated promiscuous ports.These interfaces are isolated from all other interfaces in other communities and from all isolated ports within the private VLAN domain.Reference: **http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html**New QuestionWhich private VLAN can have only one VLAN and be a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports and the gateway?A. isolated VLANB. primary VLANC. community VLAND. promiscuous VLANAnswer: AExplanation:Understanding Primary, Isolated, and Community Private VLANs Primary VLANs and the two types of secondary VLANs (isolated and community) have these characteristics:Primary VLAN--The primary VLAN carries traffic from the promiscuous ports to the host ports, both isolated and community, and to other promiscuous ports.Isolated VLAN--An isolated VLAN is a secondary VLAN that carries unidirectional traffic upstream from the hosts toward the promiscuous ports. You can configure multiple isolated VLANs in a private VLAN domain; all the traffic remains isolated within each one. Each isolated VLAN can have several isolated ports, and the traffic from each isolated port also remains completely separate.Community VLAN--A community VLAN is a secondary VLAN that carries upstream traffic from the community ports to the promiscuous port and to other host ports in the same community. You can configure multiple community VLANs in a private VLAN domain. The ports within one community can communicate, but these ports cannot communicate with ports in any other community or isolated VLAN in the private VLAN.Reference: **http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/PrivateVLANs.html**New QuestionWhich database is used to determine the validity of an ARP packet based on a valid IP-to- MAC address binding?A. DHCP snooping databaseB. dynamic ARP databaseC. dynamic routing databaseD. static ARP databaseAnswer: AExplanation:Information About Dynamic ARP Inspection DAI is used to validate ARP requests and responses as follows:Intercepts all ARP requests and responses on untrusted ports.Verifies that a packet has a valid IP-to-MAC address binding before updating the ARP cache or forwarding the packet.Drops invalid ARP packets.DAI can determine the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a DHCP snooping binding database. This database is built by DHCP snooping when it is enabled on the VLANs and on the device. It may also contain static entries that you have created.Reference:

http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus1000/hyperv/sw/5_2_1_s_m_1_5_2/troubleshooting/configuration/guide/n1000v_troubleshooting/n1000v_trouble_19dhcp.html New QuestionWhen IP Source Guard with source IP filtering is enabled on an interface, which feature must be enabled on the access VLAN for that interface?A. DHCP snoopingB. storm controlC. spanning-tree portfastD. private VLANAnswer: AExplanation:IP Source Guard Configuration GuidelinesYou can configure static IP bindings only on nonrouted ports. If you enter the ip source binding mac-address vlan vlan-id ip-address interface interface-id global configuration command on a routed interface, this error message appears:Static IP source binding can only be configured on switch port.When IP source guard with source IP filtering is enabled on an interface, DHCP snooping must be enabled on the access VLAN for that interface.If you are enabling IP source guard on a trunk interface with multiple VLANs and DHCP snooping is enabled on all the VLANs, the source IP address filter is applied on all the VLANs.You can enable this feature when 802.1x port-based authentication is enabled.Reference: **http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01110.html**New QuestionWhich switch feature prevents traffic on a LAN from being overwhelmed by continuous multicast or broadcast traffic?A. storm controlB. port securityC. VTP pruningD. VLAN trunkingAnswer: AExplanation:A traffic storm occurs when packets flood the LAN, which creates excessive traffic and degrades network performance. The traffic storm control feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces from either mistakes in network configurations or from users issuing a DoS attack. Reference: **http://3c3cc.com/c/en/us/td/docs/routers/7600/ios/122SR/configuration/guide/swcg/dos.pdf**New QuestionWhich command would a network engineer apply to error-disable a switchport when a packet-storm is detected?A. router(config-if)#storm-control action shutdownB. router(config-if)#storm-control action trapC. router(config-if)#storm-control action errorD. router(config-if)#storm-control action enableAnswer: AExplanation:Configuring the Traffic Storm Control Shutdown ModeTo configure the traffic storm control shutdown mode on an interface, perform this task:Command PurposeStep 1 Router(config)# interface {{type1 Selects an interface to configure.slot/port} | {port-channel num-ber}}Step 2 Router(config-if)# storm-control (Optional) Configures traffic storm control to action shutdown error- disable ports when a traffic storm occurs.? Enter the no storm-control action shut-down command to revert to the default action (drop).? Use the error disable detection and recov-ery feature, or the shutdown and no shut-down commands to reenable ports.Reference: **http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.html**New QuestionWhen a Cisco Catalyst switch that is configured in VTP server mode is first booted, which two VLAN ranges are loaded on the switch?A. all VLAN are in the VLAN database.B. VLANs greater than 1005 in the startup-config fileC. the first 1005 VLANs in the VLAN database fileD. the first 1005 VLANs in the startup-config fileE. VLANs greater than 1005 in the VLAN database fileAnswer: BCExplanation:If the startup VTP mode is server mode, or the startup VTP mode or domain names do not match the VLAN database, VTP mode and VLAN configuration for the first 1005 VLANs are selected by VLAN database information, such as the vlan.dat file. VLANs greater than 1005 are configured from the switch configuration file. **http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2940-series-switches/109304-manage-vlandat.html#bootup**New QuestionAn enterprise network has port security sticky enabled on all access ports. A network administrator moves a PC from one office desk to another.After the PC is moved, the network administrator clears the port security on the new network switch port connecting to the PC, but the port keeps going back into err-disabled mode.Which two factors are possible causes of this issue? (Choose two)A. Port security sticky exists on the new network switch port.B. Port security sticky is disabled on the new network switch port.C. Port security must be disabled on all access ports.D. Port security is still enabled on the older network switch port.E. Port security sticky is still enabled on the older network switch port.**Answer: AE**New QuestionOn which interface can port security be configured?A. static trunk portsB. destination port for SPANC. EtherChannel port groupD. dynamic access pointAnswer: AExplanation:Port Security and Port TypesYou can configure port security only on Layer 2 interfaces. Details about port security and different types of interfaces or ports are as follows:Access ports -- You can configure port security on interfaces that you have configured as Layer 2 access ports. On an access port, port security applies only to the access VLAN. Trunk ports -- You can configure port security on interfaces that you have configured as Layer 2 trunk ports. VLAN maximums are not useful for access ports. The device allows VLAN maximums only for VLANs associated with the trunk port.SPAN ports -- You can configure port security on SPAN source ports but not on SPAN destination ports.Ethernet Port Channels -- Port security is not supported on Ethernet port channels. **http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_portsec.html**These are some other guidelines for configuring port security:Port security can only be configured on static access ports. A secure port cannot be a dynamic access port or a trunk port. A secure port cannot be a destination port for Switch Port Analyzer

(SPAN). A secure port cannot belong to an EtherChannel port group. A secure port cannot be an 802.1X port. You cannot configure static secure MAC addresses in the voice VLAN.
https://supportforums.cisco.com/t5/network-infrastructure-documents/unable-to-configure-port-security-on-a-catalyst-2940-2950-2955/ta-p/3133064!!!RECOMMEND!!!**1.|2019 Latest 300-115 Exam Dumps (VCE & PDF) Instant Download: https://www.braindump2go.com/300-115.html2.|2019 Latest 300-115 Study Guide Video Instant Download:** YouTube Video: YouTube.com/watch?v=JSQMH1VFEwk