[2018-April-New100% Real Exam Questions-Braindump2go 300-115 Dumps 478Q Download[154-164

2018 April New Cisco 300-115 Exam Dumps with PDF and VCE Just Updated Today! Following are some new 300-115 Real Exam Questions:1.|2018 Latest 300-115 Exam Dumps (PDF & VCE) 478Q Download:https://www.braindump2go.com/300-115.html2.|2018 Latest 300-115 Exam Questions & Answers Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNYjV4eHQ4dTJoQXc?usp=sharingQUESTION 154A network is running VTPv2. After verifying all VTP settings, the network engineer notices that the new switch is not receiving the list of VLANs from the server. Which action resolves this problem?A.   Reload the new switch.B.   Restart the VTP process on the new switch.C.   Reload the VTP server.D.   Verify connected trunk ports.Answer: DExplanation:VTP should never need to have the switch reloaded or the VTP process to restart in order for it to work.The first thing that should be done is to verify that the trunk ports are connected and up.QUESTION 155After configuring new data VLANs 1020 through 1030 on the VTP server, a network engineer notices that none of the VTP clients are receiving the updates. What is the problem?A.   The VTP server must be reloaded.B.   The VTP version number must be set to version 3.C.   After each update to the VTP server, it takes up to 4 hours propagate.D.   VTP must be stopped and restarted on the server.E.   Another switch in the domain has a higher revision number than the server.Answer: BExplanation:VTP version 3 supports these features that are not supported in version 1 or version 2:Enhanced authentication--You can configure the authentication as hidden or secret. When hidden, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain.When you enter the secret keyword, you can directly configure the password secret key.Support for extended range VLAN (VLANs 1006 to 4094) database propagation.VTP versions 1 and 2 propagate only VLANs 1 to 1005. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2. QUESTION 156A network engineer is extending a LAN segment between two geographically separated data centers. Which enhancement to a spanning-tree design prevents unnecessary traffic from crossing the extended LAN segment?A.   Modify the spanning-tree priorities to dictate the traffic flow.B.   Create a Layer 3 transit VLAN to segment the traffic between the sites.C.   Use VTP pruning on the trunk interfaces.D.   Configure manual trunk pruning between the two locations.Answer: CExplanation:Pruning unnecessary VLANs from the trunk can be performed with one of two methods:? Manual pruning of the unnecessary VLAN on the trunk - This is the best method, and it avoids the use of the spanning tree. Instead, the method runs the pruned VLAN on trunks.? VTP pruning - Avoid this method if the goal is to reduce the number of STP instances.VTP-pruned VLANs on a trunk are still part of the spanning tree. Therefore, VTP-pruned VLANs do not reduce the number of spanning tree port instances.Since the question asked for the choice that is an enhancement to the STP design, VTP pruning is the best choice.

http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtmlQUESTION 157The network manager has requested that several new VLANs (VLAN 10, 20, and 30) are allowed to traverse the switch trunk interface. After the command switchport trunk allowed vlan 10,20,30 is issued, all other existing VLANs no longer pass traffic over the trunk. What is the root cause of the problem?A.   The command effectively removed all other working VLANs and replaced them with the new VLANs.B.   VTP pruning removed all unused VLANs.C.   ISL was unable to encapsulate more than the already permitted VLANs across the trunk.D.   Allowing additional VLANs across the trunk introduced a loop in the network.Answer: AExplanation:The "switchport trunk allowed vlan" command will only allow the specified VLANs, and overwrite any others that were previously defined. You would also need to explicitly allow the other working VLANs to this configuration command, or use the "issue the switchport trunk allowed vlan add vlan-list" command instead to add these 3 VLANS to the other defined allowed VLANs. QUESTION 158When 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).QUESTION 159What 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.QUESTION 160Which 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.htmlQUESTION 161Which 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.htmlQUESTION 162Which 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.htmlQUESTION 163When 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.htmlQUESTION 164Which 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!!!RECOMMEND!!!1.|2018 Latest 300-115 Exam Dumps (PDF & VCE) 478Q Download:https://www.braindump2go.com/300-115.html2.|2018 Latest 300-115 Study Guide Video: YouTube Video: YouTube.com/watch?v=Uf0h4fpiP74