

## [2017 New Best Lead2pass Cisco 300-115 PDF Dumps With New Update Exam Questions (151-175)]

2017 July Cisco Official New Released 300-115 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Are you worrying about the 300-115 exam? Lead2pass provides the latest 300-115 braindumps and guarantees you passing 300-115 exam beyond any doubt. Following questions and answers are all new published by Cisco Official Exam Center:

<https://www.lead2pass.com/300-115.html> QUESTION 151 Which technique allows specific VLANs to be strictly permitted by the administrator? A. VTP pruning B. transparent bridging C. trunk-allowed VLANs D. VLAN access-list E. L2P tunneling Answer: C Explanation: By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk. To restrict the traffic a trunk carries, use the "switchport trunk allowed vlan remove vlan-list" interface configuration command to remove specific VLANs from the allowed list. QUESTION 152 For security reasons, the IT manager has prohibited users from dynamically establishing trunks with their associated upstream switch. Which two actions can prevent interface trunking? (Choose two.) A. Configure trunk and access interfaces manually. B. Disable DTP on a per interface basis. C. Apply BPDU guard and BPDU filter. D. Enable switchport block on access ports. Answer: AB Explanation: The Dynamic Trunking Protocol (DTP) is used to negotiate forming a trunk between two Cisco devices. DTP causes increased traffic, and is enabled by default, but may be disabled. To disable DTP, configure "switchport nonegotiate." This prevents the interface from generating DTP frames. You can use this command only when the interface switchport mode is access or trunk. You must manually configure the neighboring interface as a trunk interface to establish a trunk link, otherwise the link will be a non-trunking link. QUESTION 153 Which two protocols can be automatically negotiated between switches for trunking? (Choose two.) A. PPP B. DTP C. ISL D. HDLC E. DLCI F. DOT1Q Answer: CF Explanation: Switches such as the Catalyst 3550 that are capable of either 802.1Q or ISL trunking encapsulation, the switchport trunk encapsulation [dot1q | isl | negotiate] interface command must be used prior to the switchport mode trunk command. QUESTION 154 A 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: D Explanation: 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 155 After 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: B Explanation: 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 156 A 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: C Explanation: 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.shtml](http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml) QUESTION 157 The 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. 4096 Answer: 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 port Answer: 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> QUESTION 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 VLAN. D. promiscuous VLAN Answer: 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> QUESTION 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 database Answer: 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](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) QUESTION 163 When 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 snooping B. storm control C. spanning-tree portfast D. private VLAN Answer: A Explanation: IP Source Guard Configuration Guidelines You 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](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) QUESTION 164 Which switch feature prevents traffic on a LAN from being overwhelmed by continuous multicast or broadcast traffic? A. storm control B. port security C. VTP pruning D. VLAN trunking Answer: A Explanation: 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> QUESTION 165 Which command would a network engineer apply to error-disable a switchport when a packet-storm is detected? A. router(config-if)#storm-control action shutdown B. router(config-if)#storm-control action trap C. router(config-if)#storm-control action error D. router(config-if)#storm-control action enable Answer: A Explanation: Configuring the Traffic Storm Control Shutdown Mode To configure the traffic storm control shutdown mode on an interface, perform this task: Command Purpose Step 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 recovery feature, or the shutdown and no shut-down commands to reenabling ports. Reference: <http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/storm.html> QUESTION 166 When 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 file C. the first 1005 VLANs in the VLAN database file D. the first 1005 VLANs in the startup-config file E. VLANs greater than 1005 in the VLAN database file Answer: BD QUESTION 167 An 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 QUESTION 168 On which interface can port security be configured? A. static trunk ports B. destination port for SPAN C. EtherChannel port group D. dynamic access point Answer: A Explanation: Port Security and Port Types You 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](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) QUESTION 169 Based on the show spanning-tree vlan 200 output shown in the exhibit, which two statements about the STP process for VLAN 200 are true? (Choose two.) A. BPDUs will be sent out every two seconds. B. The time spent in the listening state will be 30 seconds. C. The time spent in the learning state will be 15 seconds. D. The maximum length of time that the BPDU information will be saved is 30 seconds. E. This switch is the root bridge for VLAN 200. F. BPDUs will be sent out every 10 seconds. Answer: BF QUESTION 170 Which three statements are correct with regard to the IEEE 802.1Q standard? (Choose three) A. The IEEE 802.1Q frame format adds a 4 byte field to a Ethernet frame B. The packet is encapsulated with a 26 byte

header and a 4 byte FCSC. The protocol uses point-to-multipoint connectivityD. The protocol uses point-to-point connectivityE. The IEEE 802.1Q frame uses multicast destination of 0x01-00-0c-00-00f. The IEEE 802.1Q frame retains the original MAC destination address Answer: ADF QUESTION 171Refer to the exhibit. Based upon the output of show vlan on switch CAT2, what can we conclude about interfaces Fa0/13 and Fa0/14? A. That interfaces Fa0/13 and Fa0/14 are in VLAN 1 B. That interfaces Fa0/13 and Fa0/14 are down C. That interfaces Fa0/13 and Fa0/14 are trunk interfacesD. That interfaces Fa0/13 and Fa0/14 have a domain mismatch with another switch E. That interfaces Fa0/13 and Fa0/14 have a duplex mismatch with another switch Answer: C QUESTION 172VLAN maps have been configured on switch R1. Which of the following actions are taken in a VLAN map that does not contain a match clause? A. Implicit deny feature at end of list.B. Implicit deny feature at start of list.C. Implicit forward feature at end of listD. Implicit forward feature at start of list. Answer: A QUESTION 173Given the configuration on a switch interface, what happens when a host with the MAC address of 0003.0003.0003 is directly connected to the switch port? switchport mode accessswitchport port-securityswitchport port-security maximum 2switchport port-security mac-address 0002.0002.0002 switchport port-security violation shutdown A. The host will be allowed to connect.B. The port will shut down.C. The host can only connect through a hub/switch where 0002.0002.0002 is already connected.D. The host will be refused access. Answer: A QUESTION 174Refer to the exhibit. Switch 15 is configured as the root switch for VLAN 10 but not for VLAN 20. If the STP configuration is correct, what will be true about Switch 15? A. All ports will be in forwarding mode.B. All ports in VLAN 10 will be in forwarding mode.C. All ports in VLAN 10 will be in forwarding mode and all ports in VLAN 20 will be in blocking mode.D. All ports in VLAN 10 will be in forwarding mode and all ports in VLAN 20 will be in standby mode. Answer: B QUESTION 175Which of the following HSRP router states does an active router enter when it is preempted by a higher priority router? (Select the best answer.) A. activeB. speakC. learnD. listenE. initF. standby Answer: B Lead2pass offers the latest 300-115 PDF and VCE dumps with new version VCE player for free download, and the new 300-115 dump ensures your exam 100% pass. 300-115 new questions on Google Drive: <https://drive.google.com/open?id=0B3Syig5i8gpDUFIySDhBLWIPcmc> 2017 Cisco 300-115 exam dumps (All 401 Q&As) from Lead2pass: <https://www.lead2pass.com/300-115.html> [100% Exam Pass Guaranteed]