[2018-April-New100% Exam Pass-300-115 VCE and PDF Free from Braindump2go[143-153

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 143A Cisco Catalyst switch that is prone to reboots continues to rebuild the DHCP snooping database. What is the solution to avoid the snooping database from being rebuilt after every device reboot?A. A DHCP snooping database agent should be configured.B. Enable DHCP snooping for all VLANs that are associated with the switch.C. Disable Option 82 for DHCP data insertion.D. Use IP Source Guard to protect the DHCP binding table entries from being lost upon rebooting.E. Apply ip dhcp snooping trust on all interfaces with dynamic addresses.Answer: AExplanation:Minimum DHCP Snooping ConfigurationThe minimum configuration steps for the DHCP snooping feature are as follows:1.Define and configure the DHCP server.2.Enable DHCP snooping on at least one VLAN.By default, DHCP snooping is inactive on all VLANs.3.Ensure that DHCP server is connected through a trusted interface. By default, the trust state of all interfaces is untrusted.4.Configure the DHCP snooping database agent.This step ensures that database entries are restored after a restart or switchover.5.Enable DHCP snooping globally.The feature is not active until you complete this step.Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SX/configuration/guide/snoodhcp.html#wp1090479
QUESTION 144Which portion of AAA looks at what a user has access to?A. authorizationB. authenticationC. accountingD. auditingAnswer: AExplanation:AAA consists of the following three elements:Authentication: Identifies users by login and password using challenge and response methodology before the user even gains access to the network. Depending on your security options, it can also support encryption. Authorization: After initial authentication, authorization looks at what that authenticated user has access to do. RADIUS or TACACS+ security servers perform authorization for specific privileges by defining attribute-value (AV) pairs, which would be specific to the individual user rights. In the Cisco IOS, you can define AAA authorization with a named list or authorization method.Accounting: The last "A" is for accounting. It provides a way of collecting security information that you can use for billing, auditing, and reporting. You can use accounting to see what users do once they are authenticated and authorized. For example, with accounting, you could get a log of when users logged in and when they logged out.Reference:
http://www.techrepublic.com/blog/data-center/what-is-aaa-and-how-do-you-configure-it-in-the-cisco-ios/QUESTION 145 Which command creates a login authentication method named "login" that will primarily use RADIUS and fail over to the local user database?A. (config)# aaa authentication login default radius localB. (config)# aaa authentication login login radius localC. (config)# aaa authentication login default local radiusD. (config)# aaa authentication login radius localAnswer: BExplanation:In the command "aaa authentication login login radius local" the second login is the name of the AAA method. It also lists radius first then local, so it will primarily use RADIUS for authentication and fail over to the local user database only if the RADIUS server is unreachable.QUESTION 146What is the function of NSF?A. forward traffic simultaneously using both supervisorsB. forward traffic based on Cisco Express ForwardingC. provide automatic failover to back up supervisor in VSS modeD. provide nonstop forwarding in the event of failure of one of the member supervisorsAnswer: DExplanation:VSS is network system virtualization technology that pools multiple Cisco Catalyst 6500 Series Switches into one virtual switch, increasing operational efficiency, boosting nonstop communications, and scaling system bandwidth capacity to 1.4 Tbps. Switches would operate as a single logical virtual switch called a virtual switching system 1440 (VSS1440). VSS formed by two Cisco Catalyst 6500 Series Switches with the Virtual Switching Supervisor 720-10GE. In a VSS, the data plane and switch fabric with capacity of 720 Gbps of supervisor engine in each chassis are active at the same time on both chassis, combining for an active 1400-Gbps switching capacity per VSS. Only one of the virtual switch members has the active control plane. Both chassis are kept in sync with the inter-chassis Stateful Switchover (SSO) mechanism along with Nonstop Forwarding (NSF) to provide nonstop communication even in the event of failure of one of the member supervisor engines or chassis. QUESTION 147Which configuration command ties the router hot standby priority to the availability of its interfaces?A. standby groupB. standby priorityC. backup interfaceD. standby trackAnswer: DExplanation:The standby track interface configuration command ties the router hot standby priority to the availability of its interfaces and is useful for tracking interfaces that are not configured for HSRP. When a tracked interface fails, the hot standby priority on the device on which tracking has been configured decreases by 10. If an interface is not tracked, its state changes do not affect the hot standby priority of the configured device. For each interface configured for hot standby, you can configure a separate list of interfaces to be tracked.

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/configuration/guide/swhsrp.html
QUESTION 148What is the default HSRP priority?A. 50B. 100C. 120D. 1024Answer: BExplanation:standby [group-num-Set a priority value used in choosing the active router. The ber] priority priority range is 1 to 255; the default priority is 100. The highest [preempt [delay delay]] number represents the highest priority.(Optional) group-number--The group number to whichthe command applies.(Optional)preempt--Select so that when the local router has a higher priority than the active router, it assumes control as the active router.(Optional)delay--Set to cause the local router to post-pone taking over the active role for the shown number of sec- onds. The range is 0 to 36000 (1 hour); the default is 0 (no de- lay before taking over).Use the no form of the command to restore the default values.Reference:
http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/configuration/guide/swhsrp.html#wp1044327QUESTION 149A server with a statically assigned IP address is attached to a switch that is provisioned for DHCP snooping. For more protection against malicious attacks, the network team is considering enabling dynamic ARP inspection alongside DHCP snooping. Which solution ensures that the server maintains network reachability in the future?A. Disable DHCP snooping information option.B. Configure a static DHCP snooping binding entry on the switch.C. Trust the interface that is connected to the server with the ip dhcp snooping trust command.D. Verify the source MAC address of all untrusted interfaces with ip dhcp snooping verify mac-address command.Answer: BExplanation:Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:Intercepts all ARP requests and responses on untrusted ports Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.Drops invalid ARP packets Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without any checks. On untrusted interfaces, the switch forwards the packet only if it is valid. To ensure network reachability to the server, configure a static DHCP snooping binding entry on the switch. Reference:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swdynarp.htmlQUESTION 150DHCP snooping and IP Source Guard have been configured on a switch that connects to several client workstations. The IP address of one of the workstations does not match any entries found in the DHCP binding database. Which statement describes the outcome of this scenario?A. Packets from the workstation will be rate limited according to the default values set on the switch.B. The interface that is connected to the workstation in question will be put into the errdisabled state.C. Traffic will pass accordingly after the new IP address is populated into the binding database.D. The packets originating from the workstation are assumed to be spoofed and will be discarded.Answer: DExplanation:The IP source binding table has bindings that are learned by DHCP snooping or are manually configured (static IP source bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number. The switch uses the IP source binding table only when IP source guard is enabled. You can configure IP source guard with source IP address filtering, or with source IP and MAC address filtering. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP address. The switch forwards IP traffic when the source IP address matches an entry in the DHCP snooping binding database or a binding in the IP source binding table. When IP source guard is enabled with this option, IP traffic is filtered based on the source IP and MAC addresses. The switch forwards traffic only when the source IP and MAC addresses match an entry in the IP source binding table. If there is no match, the packets are assumed to be spoofed and will be discarded.Reference:
http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html#ipsourceguardQUESTION 151Which technique allows specific VLANs to be strictly permitted by the administrator?A. VTP pruning B. transparent bridgingC. trunk-allowed VLANsD. VLAN access-listE. L2P tunnelingAnswer: CExplanation: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 152For 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: ABExplanation: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 153Which two protocols can be automatically negotiated between switches for trunking? (Choose two.)A. PPPB. DTPC. ISLD. HDLCE. DLCIF. DOT1QAnswer: 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.
!!!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