[February 2018 Lead2pass 2018 100% Real 300-115 Exam Questions 489q

Lead2pass 2018 New Cisco 300-115 Braindump Free Download: https://www.lead2pass.com/300-115.html QUESTION 11Which technique automatically limits VLAN traffic to only the switches that require it? A. access listsB. DTP in nonegotiateC. VTP pruningD. PBRAnswer: CExplanation:VTP pruning enhances network bandwidth use by reducing unnecessary flooded traffic, such as broadcast, multicast, unknown, and flooded unicast packets to only the switches that require it. VTP pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the appropriate network devices. By default, VTP pruning is disabled. QUESTION 12What effect does the mac address-table aging-time 180 command have on the MAC address-table? A. This is how long a dynamic MAC address will remain in the CAM table.B. The MAC address-table will be flushed every 3 minutes.C. The default timeout period will be 360 seconds.D. ARP requests will be processed less frequently by the switch.E. The MAC address-table will hold addresses 180 seconds longer than the default of 10 minutes. Answer: AExplanation:You can configure the amount of time that an entry (the packet source MAC address and port that packet ingresses) remain in the MAC table. To configure the aging time for all MAC addresses, perform this task: Command Purpose Step 1 switch# configure Enters configuration mode. terminal Step 2 switch(config)# mac-Specifies the time before an entry ages out address-table aging- and is discarded from the MAC address table. time seconds [vlan The range is from 0 to 1000000; the default is vlan_id] 300 seconds. Entering the value 0 disables the MAC aging. If a VLAN is not specified, the aging specification applies to all VLANs. This example shows how to set the aging time for entries in the MAC address table to 600 seconds (10 minutes): switch# configure terminal switch(config)# mac-address-table aging-time 600 QUESTION 13While working in the core network building, a technician accidently bumps the fiber connection between two core switches and damages one of the pairs of fiber. As designed, the link was placed into a non-forwarding state due to a fault with UDLD. After the damaged cable was replaced, the link did not recover. What solution allows the network switch to automatically recover from such an issue? A. macrosB. errdisable autorecoveryC. IP Event DampeningD. command aliasesE. Bidirectional Forwarding Detection Answer: B Explanation:There are a number of events which can disable a link on a Catalyst switch, such as the detection of a loopback, UDLD failure, or a broadcast storm. By default, manual intervention by an administrator is necessary to restore the interface to working order; this can be done by issuing shutdown followed by no shutdown on the interface. The idea behind requiring administrative action is so that a human engineer can intercede, assess, and (ideally) correct the issue. However, some configurations may be prone to accidental violations, and a steady recurrence of these can amount to a huge time sink for the administrative staff.This is where errdisable autorecovery can be of great assistance. We can configure the switch to automatically re-enable any error-disabled interfaces after a specified timeout period. This gives the offending issue a chance to be cleared by the user (for example, by removing an unapproved device) without the need for administrative intervention. QUESTION 14A network engineer deployed a switch that operates the LAN base feature set and decides to use the SDM VLAN template. The SDM template is causing the CPU of the switch to spike during peak working hours. What is the root cause of this issue? A. The VLAN receives additional frames from neighboring switches.B. The SDM VLAN template causes the MAC address-table to overflow.C. The VLAN template disables routing in hardware.D. The switch needs to be rebooted before the SDM template takes effect. Answer: CExplanation: SDM Template Notes:All templates are predefined. There is no way to edit template category individual values.The switch reload is required to use a new SDM template.The ACL merge algorithm, as opposed to the original access control entries (ACEs) configured by the user, generate the number of TCAM entries listed for security and QoS ACEs.The first eight lines (up to Security ACEs) represent approximate hardware boundaries set when a template is used. If the boundary is exceeded, all processing overflow is sent to the CPU which can have a major impact on the performance of the switch. Choosing the VLAN template will actually disable routing (number of entry for unicast or multicast route is zero) in hardware. QUESTION 15An access switch has been configured with an EtherChannel port. After configuring SPAN to monitor this port, the network administrator notices that not all traffic is being replicated to the management server. What is a cause for this issue? A. VLAN filters are required to ensure traffic mirrors effectively.B. SPAN encapsulation replication must be enabled to capture EtherChannel destination traffic.C. The port channel can be used as a SPAN source, but not a destination.D. RSPAN must be used to capture EtherChannel bidirectional traffic. Answer: CExplanation:A source port or EtherChannel is a port or EtherChannel monitored for traffic analysis. You can configure both Layer 2 and Layer 3 ports and EtherChannels as SPAN sources. SPAN can monitor one or more source ports or EtherChannels in a single SPAN session. You can configure ports or EtherChannels in any VLAN as SPAN sources. Trunk ports or EtherChannels can be configured as sources and mixed with nontrunk sources. A port-channel interface (an EtherChannel) can be a SPAN source, but not a destination. QUESTION 16A DHCP configured router is connected directly to a switch that has been provisioned with DHCP snooping. IP Source Guard with the ip verify source port-security command is configured under the interfaces that connect to

all DHCP clients on the switch. However, clients are not receiving an IP address via the DHCP server. Which option is the cause of this issue? A. The DHCP server does not support information option 82.B. The DHCP client interfaces have storm control configured.C. Static DHCP bindings are not configured on the switch.D. DHCP snooping must be enabled on all VLANs, even if they are not utilized for dynamic address allocation. Answer: AExplanation:When you enable both IP Source Guard and Port Security, using the ip verify source port- security interface configuration command, there are two caveats:The DHCP server must support option 82, or the client is not assigned an IP address.The MAC address in the DHCP packet is not learned as a secure address. The MAC address of the DHCP client is learned as a secure address only when the switch receives non-DHCP data traffic. Reference:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swdhcp82.html#wp1069615 QUESTION 17A switch is added into the production network to increase port capacity. A network engineer is configuring the switch for DHCP snooping and IP Source Guard, but is unable to configure ip verify source under several of the interfaces. Which option is the cause of the problem? A. The local DHCP server is disabled prior to enabling IP Source Guard.B. The interfaces are configured as Layer 3 using the no switchport command.C. No VLANs exist on the switch and/or the switch is configured in VTP transparent mode.D. The switch is configured for sdm prefer routing as the switched database management template.E. The configured SVIs on the switch have been removed for the associated interfaces. Answer: BExplanation:IP source guard is a security feature that restricts IP traffic on nonrouted, Layer 2 interfaces by filtering traffic based on the DHCP snooping binding database and on manually configured IP source bindings. You can use IP source guard to prevent traffic attacks caused when a host tries to use the IP address of its neighbor.You can enable IP source guard when DHCP snooping is enabled on an untrusted interface. After IP source guard is enabled on an interface, the switch blocks all IP traffic received on the interface, except for DHCP packets allowed by DHCP snooping. A port access control list (ACL) is applied to the interface. The port ACL allows only IP traffic with a source IP address in the IP source binding table and denies all other traffic.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.IP source guard is supported only on Layer 2 ports, including access and trunk ports. You can configure IP source guard with source IP address filtering or withsource IP and MAC address filtering.Reference:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swdhcp82.html#wp1069615 QUESTION 18The command storm-control broadcast level 75 65 is configured under the switch port connected to the corporate mail server. In which three ways does this command impact the traffic? (Choose three.) A. SNMP traps are sent by default when broadcast traffic reaches 65% of the lower-level threshold.B. The switchport is disabled when unicast traffic reaches 75% of the total interface bandwidth.C. The switch resumes forwarding broadcasts when they are below 65% of bandwidth.D. Only broadcast traffic is limited by this particular storm control configuration.E. Multicast traffic is dropped at 65% and broadcast traffic is dropped at 75% of the total interface bandwidth.F. The switch drops broadcasts when they reach 75% of bandwidth. Answer: CDFExplanation:storm-control {broad- Configure broadcast, multicast, or unicast storm control. By de- cast | multicast | uni- fault, storm control is disabled.cast} level {level [lev-The keywords have these meanings:el-low] | pps pps [pps-low]}For level, specify the rising threshold level for broadcast, multicast, or unicast traffic as a percentage (up to two decimal places) of the bandwidth. The port blocks traffic when the rising threshold is reached. The range is 0.00 to 100.00.(Optional) For level-low, specify the falling threshold level as a percentage (up to two decimal places) of the bandwidth. This value must be less than or equal to the rising suppression value. The port forwards traffic when traffic drops below this level. If you do not configure a falling suppression level, it is set to the rising suppression level. The range is 0.00 to 100.00.In this case, the broadcast keyword was used so only broadcast traffic is limited. http:// Reference:
www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-2_25_see/configuration/guide/3550SCG/swtrafc.html QUESTION 19After UDLD is implemented, a Network Administrator noticed that one port stops receiving UDLD packets. This port continues to reestablish until after eight failed retries. The port then transitions into the errdisable state. Which option describes what causes the port to go into the errdisable state? A. Normal UDLD operations that prevent traffic loops.B. UDLD port is configured in aggressive mode.C. UDLD is enabled globally.D. UDLD timers are inconsistent. Answer: BExplanation:With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor. After eight failed retries, the port is disabled. QUESTION 20After reviewing UDLD status on switch ports, an engineer notices that the current bidirectional state for an access port is "Unknown." Which statement describes what this indicates about the status of the port? A. The port is fully operational and no known issues are detected.B. The bidirectional status of "unknown" indicates that the port will go into the disabled state

because it stopped receiving UDLD packets from its neighbor.C. UDLD moved into aggressive mode after inconsistent acknowledgements were detected.D. The UDLD port is placed in the "unknown" state for 5 seconds until the next UDLD packet is received on the interface. Answer: AExplanation:By default, UDLD is disabled on all interfaces. We can enable UDLD globally on the device, or individually on specific interfaces with the command udld port. This enables UDLD in normal mode.It would be prohibitively difficult to coordinate the configuration of UDLD on both ends of a link at the same time, so when UDLD is first enabled and does not detect a neighbor the link state is considered unknown, which is not necessarily an error condition. The port will remain operational during this time. When UDLD is finally enabled on the other end, the status will transition to bidirectional. **300-115 dumps full version (PDF&VCE):** https://www.lead2pass.com/300-115.html **Large amount of free 300-115 exam questions on Google Drive:** https://drive.google.com/open?id=0B3Syig5i8gpDM0pqaFJWUXVuM2M Maybe you also need: 300-101 exam dumps: https://drive.google.com/open?id=0B3Syig5i8gpDakxVRXg3aUpmTE0 300-135 exam dumps: https://drive.google.com/open?id=0B3Syig5i8gpDZmFQVlZDZnpLejA