[2017 New Lead2pass 300-115 Exam Questions Free Download (126-150)

2017 July Cisco Official New Released 300-115 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
Amazing,100% candidates have passed the 300-115 exam by practising the preparation material of Lead2pass, because the braindumps are the latest and cover every aspect of 300-115 exam. Download the braindumps for an undeniable success in 300-115 exam. Following questions and answers are all new published by Cisco Official Exam Center:
https://www.lead2pass.com/300-115.html QUESTION 126Refer to the exhibit, which statement abort the current configuration on port GigabitEthernet2/0/1 is true? A. It is an access port configured for a phone and a PCB. It is a trunk port and the native VLAN is VLAN1C. It is a trunk port and the natrve VL AN m VLAN 700D. It is an access port in VLAN 700Answer: B QUESTION 127Which two options are advantages of deploying VTPv3? (Choose two) A. It stores the VTP domain password securely as a SHA-1 hashB. It adds on FCS field at the end of each VTP frame for consistency checkingC. It supports the propagation of private VLANs.D. It supports the use of AES to encrypt VTP messagingE. It can be configured to allow only one VTP server to make changes to the VTP domain Answer: CE QUESTION 128What percentage of bandwidth is reduced when a stack cable is broken? A. 0B. 25C. 50D. 75E. 100 Answer: CExplanation:Physical Sequential Linkage The switches are physically connected sequentially, as shown in Figure 3. A break in any one of the cables will result in the stack bandwidth being reduced to half of its full capacity. Subsecond timing mechanisms detect traffic problems and immediately institute failover. This mechanism restores dual path flow when the timing mechanisms detect renewed activity on the cable.Figure 3. Cisco StackWise Technology Resilient Cabling
http://www.cisco.com/c/en/us/products/collateral/switches/catalyst-3750-series-switches/prod_white_paper09186a00801b096a.html QUESTION 129Refer to the exhibit. Which set of configurations will result in all ports on both switches successfully bundling into an EtherChannel? A. switch1channel-group 1 mode activeswitch2channel-group 1 mode autoB. switch1channel-group 1 mode desirableswitch2channel-group 1 mode passiveC. switch1channel-group 1 mode onswitch2channel-group 1 mode autoD. switch1channel-group 1 mode desirableswitch2channel-group 1 mode auto Answer: DExplanation:The different etherchannel modes are described in the table below:Mode Descriptionactive Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending LACP packets.auto Places an interface into a passive negotiating state, in which the interface re-sponds to PAgP packets it receives but does not start PAgP packet negotiation.This setting minimizes the transmission of PAgP packets.desirable Places an interface into an active negotiating state, in which the interface starts negotiations with other interfaces by sending PAgP packets.on Forces the interface into an EtherChannel without PAgP or LACP. With the on mode, a usable EtherChannel exists only when an interface group in the on mode is connected to another interface group in the on mode.passive Places an interface into a passive negotiating state, in which the interface re- sponds to LACP packets that it receives, but does not start LACP packet ne-gotiation. This setting minimizes the transmission of LACP packets.Both the auto and desirable PAgP modes allow interfaces to negotiate with partner interfaces to determine if they can form an EtherChannel based on criteria suchas interface speed and, for Layer 2 EtherChannels, trunking state and VLAN numbers.Interfaces can form an EtherChannel when they are in different PAgP modes as long as the modes are compatible. For example:An interface in the desirable mode can form an EtherChannel with another interface that is in the desirable or auto mode.An interface in the auto mode can form an EtherChannel with another interface in the desirable mode.An interface in the auto mode cannot form an EtherChannel with another interface that is also in the auto mode because neither interface starts PAgP negotiation.An interface in the on mode that is added to a port channel is forced to have the same characteristics as the already existing on mode interfaces in the channel.
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3550/software/release/12-1_13_ea1/configuration/guide/3550scg/swethchl.html QUESTION 130Refer to the exhibit. How can the traffic that is mirrored out the GigabitEthernet0/48 port be limited to only traffic that is received or transmitted in VLAN 10 on the GigabitEthernet0/1 port? A. Change the configuration for GigabitEthernet0/48 so that it is a member of VLAN 10.B. Add an access list to GigabitEthernet0/48 to filter out traffic that is not in VLAN 10.C. Apply the monitor session filter globally to allow only traffic from VLAN 10.D. Change the monitor session source to VLAN 10 instead of the physical interface. Answer: CExplanation:To start a new flow-based SPAN (FSPAN) session or flow-based RSPAN (FRSPAN) source or destination session, or to limit (filter) SPAN source traffic to specific VLANs, use the monitor session filter global configuration command.Usage GuidelinesYou can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch or switch stack. You can monitor traffic on a single VLAN or on a series or range of ports or VLANs. You select a series or range of VLANs by using the [, | -] options.If you specify a series of VLANs, you must enter a space before and after the comma. If you specify a range of VLANs, you must enter a space before and after the hyphen (-). VLAN filtering refers to analyzing network traffic on a selected set of

VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the monitor session session_number filter vlan vlan-id command to limit SPAN traffic on trunk source ports to only the specified VLANs.VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/3se/network_managementcommand_reference/b_nm_3se_3850_cr/b_nm_3se_3850_cr_chapter_010.html#wp3875419997 QUESTION 131Refer to the exhibit. A network engineer wants to analyze all incoming and outgoing packets for an interface that is connected to an access switch. Which three items must be configured to mirror traffic to a packet sniffer that is connected to the distribution switch? (Choose three.) A. A monitor session on the distribution switch with a physical interface as the source and the remote SPAN VLAN as the destinationB. A remote SPAN VLAN on the distribution and access layer switchC. A monitor session on the access switch with a physical interface source and the remote SPAN VLAN as the destinationD. A monitor session on the distribution switch with a remote SPAN VLAN as the source and physical interface as the destinationE. A monitor session on the access switch with a remote SPAN VLAN source and the physical interface as the destinationF. A monitor session on the distribution switch with a physical interface as the source and a physical interface as the destination Answer: BCDExplanation:You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. RSPAN supports source ports, source VLANs, and destination ports on different switches (or different switch stacks), enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN. Each RSPAN source switch must have either ports or VLANs as RSPAN sources. The destination is always a physical port.
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/12-2_55_se/configuration/guide/3750xscg/swspan.html QUESTION 132After an EtherChannel is configured between two Cisco switches, interface port channel 1 is in the down/down state. Switch A is configured with channel-group 1 mode active, while Switch B is configured with channel-group 1 mode desirable. Why is the EtherChannel bundle not working? A. The switches are using mismatched EtherChannel negotiation modes.B. The switch ports are not configured in trunking mode.C. LACP priority must be configured on both switches.D. The channel group identifier must be different for Switch A and Switch B. Answer: AExplanation:Here we have a situation where one switch is using active mode, which is an LACP mode, and the other is using desirable, which is a PAGP mode.You can not mix the LACP and PAGP protocols to form an etherchannel. Here is a summary of the various etherchannel modes:EtherChannel PAgP ModesMode Descriptionauto Places a port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. This setting minimizes the transmission of PAgP packets.This mode is not supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).desirable Places a port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.This mode is not supported when the EtherChannel members are from different switches in the switch stack (cross-stack EtherChannel).EtherChannel LACP ModesMode Descriptionactive Places a port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.passive Places a port into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation. This setting minimizes the transmission of LACP packets.
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swethchl.html QUESTION 133Which feature must be enabled to eliminate the broadcasting of all unknown traffic to switches that are not participating in the specific VLAN? A. VTP pruningB. port-securityC. storm controlD. bpdguard Answer: AExplanation:VTP ensures that all switches in the VTP domain are aware of all VLANs. However, there are occasions when VTP can create unnecessary traffic. All unknown unicasts and broadcasts in a VLAN are flooded over the entire VLAN. All switches in the network receive all broadcasts, even in situations in which few users are connected in that VLAN. VTP pruning is a feature that you use in order to eliminate or prune this unnecessary traffic.Reference:
http://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/10558-21.html QUESTION 134Refer to the exhibit. The users in an engineering department that connect to the same access switch cannot access the network. The network engineer found that the engineering VLAN is missing from the database. Which action resolves this problem? A. Disable VTP pruning and disable 802.1q.B. Update the VTP revision number.C. Change VTP mode to server and enable 802.1q.D. Enable VTP pruning and disable 802.1q. Answer: CExplanation:Only VTP servers can add new VLANs to the switched network, so to enable vlan 10 on this

switch you will first need to change the VTP mode from client to server.Then, you will need to enable 802.1Q trunking to pass this new VLAN along to the other switches. QUESTION 135A network engineer wants to ensure Layer 2 isolation of customer traffic using a private VLAN. Which configuration must be made before the private VLAN is configured? A. Disable VTP and manually assign VLANs.B. Ensure all switches are configured as VTP server mode.C. Configure VTP Transparent Mode.D. Enable VTP version 3. Answer: CExplanation:You must configure VTP to transparent mode before you can create a private VLAN. Private VLANs are configured in the context of a single switch and cannot have members on other switches. Private VLANs also carry TLVs that are not known to all types of Cisco switches.Reference: http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=6 QUESTION 136Refer to the exhibit. The network switches for two companies have been connected and manually configured for the required VLANs, but users in company A are not able to access network resources in company B when DTP is enabled. Which action resolves this problem? A. Delete vlan.dat and ensure that the switch with lowest MAC address is the VTP server.B. Disable DTP and document the VTP domain mismatch.C. Manually force trunking with switchport mode trunk on both switches.D. Enable the company B switch with the vtp mode server command. Answer: CExplanation:Since the number of existing VLANs differ on the switches (9 on A and 42 on B) we know that there is a problem with VTP or the trunking interfaces. The VTP domain names do match and they are both VTP servers so there are no issues there. The only viable solution is that there is a DTP issues and so you must instead manually configure the trunk ports between these two switches so that the VLAN information can be sent to each switch. QUESTION 137A network engineer must implement Ethernet links that are capable of transporting frames and IP traffic for different broadcast domains that are mutually isolated. Consider that this is a multivendor environment. Which Cisco IOS switching feature can be used to achieve the task? A. PPP encapsulation with a virtual templateB. Link Aggregation Protocol at the access layerC. dot1q VLAN trunkingD. Inter-Switch Link Answer: CExplanation:Here the question asks for transporting "frames and IP traffic for different broadcast domains that are mutually isolated" which is basically a long way of saying VLANs so trunking is needed to carry VLAN information. There are 2 different methods for trunking, 802.1Q and ISL. Of these, only 802.1Q is supported by multiple vendors since ISL is a Cisco proprietary protocol. QUESTION 138Which statement about using native VLANs to carry untagged frames is true? A. Cisco Discovery Protocol version 2 carries native VLAN information, but version 1 does not.B. Cisco Discovery Protocol version 1 carries native VLAN information, but version 2 does not.C. Cisco Discovery Protocol version 1 and version 2 carry native VLAN information.D. Cisco Discovery Protocol version 3 carries native VLAN information, but versions 1 and 2 do not. Answer: AExplanation:Cisco Discovery Protocol (CDP) version 2 passes native VLAN information between Cisco switches. If you have a native VLAN mismatch, you will see CDP error messages on the console output.Reference: http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=3 QUESTION 139Refer to the exhibit. A multilayer switch has been configured to send and receive encapsulated and tagged frames. VLAN 2013 on the multilayer switch is configured as the native VLAN. Which option is the cause of the spanning-tree error? A. VLAN spanning-tree in SW-2 is configured.B. spanning-tree bpdu-filter is enabled.C. 802.1q trunks are on both sides, both with native VLAN mismatch.D. VLAN ID 1 should not be used for management traffic because its unsafe. Answer: CExplanation:Here we see that the native VLAN has been configured as 2013 on one switch, but 1 (the default native VLAN) on the other switch. If you use 802.1Q trunks, you must ensure that you choose a common native VLAN for each port in the trunk. Failure to do this causes Cisco switches to partially shut down the trunk port because having mismatched native VLANs can result in spanning-tree loops. Native VLAN mismatches are detected via spanning tree and Cisco Discovery Protocol (CDP), not via DTP messages. If spanning tree detects a native VLAN mismatch, spanning tree blocks local native VLAN traffic and the remote switch native VLAN traffic on the trunk; however, the trunk still remains up for other VLANs.Reference: http://www.informit.com/library/content.aspx? b=CCNP_Studies_Switching&seqNum=25 QUESTION 140A network engineer must improve bandwidth and resource utilization on the switches by stopping the inefficient flooding of frames on trunk ports where the frames are not needed. Which Cisco IOS feature can be used to achieve this task? A. VTP pruningB. access listC. switchport trunk allowed VLAND. VLAN access-map Answer: AExplanation:Cisco advocates the benefits of pruning VLANs in order to reduce unnecessary frame flooding. The?vtp pruning?command prunes VLANs automatically, which stops the inefficient flooding of frames where they are not needed. http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/24330-185.html QUESTION 141Refer to the exhibit. What is the result of the configuration? A. The EtherChannels would not form because the load-balancing method must match on the devices.B. The EtherChannels would form and function properly even though the load-balancing and EtherChannel modes do not match.C. The EtherChannels would form, but network loops would occur because the load- balancing methods do not match.D. The EtherChannels would form and both devices would use the dst-ip load-balancing method because Switch1 is configured with EtherChannel mode active. Answer: BExplanation:An etherchannel will form if one end is active and the other is

passive. Load balancing can only be configured globally. As a result, all channels (manually configured, PagP, or LACP) use the same load-balancing. This is true for the switch globally, although each switch involved in the etherchannel can have non matching parameters for load balancing.
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/54sg/configuration/guide/config/channel.html#wp1020804
QUESTION 142A network engineer tries to configure storm control on an EtherChannel bundle. What is the result of the configuration? A. The storm control settings will appear on the EtherChannel, but not on the associated physical ports.B. The configuration will be rejected because storm control is not supported for EtherChannel.C. The storm control configuration will be accepted, but will only be present on the physical interfaces.D. The settings will be applied to the EtherChannel bundle and all associated physical interfaces. Answer: DExplanation:After you configure an EtherChannel, any configuration that you apply to the port-channel interface affects the EtherChannel; any configuration that you apply to the physical interfaces affects only the interface where you apply the configuration. Storm Control is an exception to this rule. For example, you cannot configure Storm Control on some of the members of an EtherChannel; Storm Control must be configured on all or none of the ports.If you configure Storm Control on only some of the ports, those ports will be dropped from the EtherChannel interface (put in suspended state). Therefore, you should configure Storm Control at the EtherChannel Interface level, and not at the physical interface level. QUESTION 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. auditing Answer: 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 145Which 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 local Answer: 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 supervisors Answer: 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 track Answer: 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. 1024 Answer: 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#wp1044327 QUESTION 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.html QUESTION 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#ipsourceguard You can pass Cisco 300-115 exam if you get a complete hold of 300-115 braindumps in Lead2pass. What's more, all the 300-115 Certification exam Q and As provided by Lead2pass are the latest. 300-115 new questions on Google Drive:
https://drive.google.com/open?id=0B3Syig5i8gpDUFIySDhBLWlPcmc 2017 Cisco 300-115 exam dumps (All 401 Q&As) from

Lead2pass: https://www.lead2pass.com/300-115.html [100% Exam Pass Guaranteed]