[2017 New Free 300-115 Exam Dumps With PDF And VCE Download (1-25)

2017 July Cisco Official New Released 300-115 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
300-115 exam questions and answers provided by Lead2pass will guarantee you pass 300-115 exam, because Lead2pass is the top IT Certification study training materials vendor. Many candidates have passed exam with the help of Lead2pass. We offer the latest 300-115 PDF and VCE dumps with new version VCE player for free download, you can pass the exam beyond any doubt. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/300-115.html QUESTION 1An EtherChannel bundle has been established between a Cisco switch and a corporate web server. The network administrator noticed that only one of the EtherChannel links is being utilized to reach the web server. What should be done on the Cisco switch to allow for better EtherChannel utilization to the corporate web server? A. Enable Cisco Express Forwarding to allow for more effective traffic sharing over the EtherChannel bundle.B. Adjust the EtherChannel load-balancing method based on destination IP addresses.C. Disable spanning tree on all interfaces that are participating in the EtherChannel bundle.D. Use link-state tracking to allow for improved load balancing of traffic upon link failure to the server.E. Adjust the EtherChannel load-balancing method based on source IP addresses.Answer: EExplanation:EtherChannel load balancing can use MAC addresses, IP addresses, or Layer 4 port numbers, and either source mode, destination mode, or both. The mode you select applies to all EtherChannels that you configure on the switch. Use the option that provides the greatest variety in your configuration. For example, if the traffic on a channel only goes to a single MAC address (which is the case in this example, since all traffic is going to the same web server), use of the destination MAC address results in the choice of the same link in the channel each time. Use of source addresses or IP addresses can result in a better load balance. http://www.cisco.com/c/en/us/support/docs/lan-switching/ etherchannel/12023-4.html QUESTION 2Interface FastEthernet0/1 is configured as a trunk interface that allows all VLANs. This command is configured globally: monitor session 2 filter vlan 1 - 8, 39, 52 What is the result of the implemented command? A. All VLAN traffic is sent to the SPAN destination interface.B. Traffic from VLAN 4 is not sent to the SPAN destination interface.C. Filtering a trunked SPAN port effectively disables SPAN operations for all VLANs.D. The trunk's native VLAN must be changed to something other than VLAN 1.E. Traffic from VLANs 1 to 8, 39, and 52 is replicated to the SPAN destination port. Answer: E Explanation:The "monitor session filter" command is used to specify which VLANS are to be port mirrored using SPAN. This example shows how to monitor VLANs 1 through 5 and VLAN 9 when the SPAN source is a trunk interface: Switch(config)# monitor session 2 filter vlan 1 - 5 , 9http://www.cisco.com/ c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/span.html/ index.html#wp1066836 QUESTION 3A network engineer notices inconsistent Cisco Discovery Protocol neighbors according to the diagram that is provided. The engineer notices only a single neighbor that uses Cisco Discovery Protocol, but it has several routing neighbor relationships. What would cause the output to show only the single neighbor? A. The routers are connected via a Layer 2 switch.B. IP routing is disabled on neighboring devices.C. Cisco Express Forwarding is enabled locally.D. Cisco Discovery Protocol advertisements are inconsistent between the local and remote devices. Answer: AExplanation:If all of the routers are connected to each other using a layer 2 switch, then each router will only have the single switch port that it connects to as its neighbor. Even though multiple routing neighbors can be formed over a layer 2 network, only the physical port that it connects to will be seen as a CDP neighbor. CDP can be used to determine the physical topology, but not necessarily the logical topology. QUESTION 4After the implementation of several different types of switches from different vendors, a network engineer notices that directly connected devices that use Cisco Discovery Protocol are not visible. Which vendor-neutral protocol could be used to resolve this issue? A. Local Area MobilityB. Link Layer Discovery ProtocolC. NetFlowD. Directed Response Protocol Answer: BExplanation:The Link Layer Discovery Protocol (LLDP) is a vendor-neutral link layer protocol in the Internet Protocol Suite used by network devices for advertising their identity, capabilities, and neighbors on an IEEE 802 local area network, principally wired Ethernet. LLDP performs functions similar to several proprietary protocols, such as the Cisco Discovery Protocol (CDP).http://en.wikipedia.org/wiki/ Link_Layer_Discovery_Protocol QUESTION 5Several new switches have been added to the existing network as VTP clients. All of the new switches have been configured with the same VTP domain, password, and version. However, VLANs are not passing from the VTP server (existing network) to the VTP clients. What must be done to fix this? A. Remove the VTP domain name from all switches with "null" and then replace it with the new domain name.B. Configure a different native VLAN on all new switches that are configured as VTP clients.C. Provision one of the new switches to be the VTP server and duplicate information from the existing network.D. Ensure that all switch interconnects are configured as trunks to allow VTP information to be transferred. Answer: DExplanation:VTP allows switches to advertise VLAN information between other members of the same VTP domain.VTP allows a consistent view of the switched network across all switches. There are several reasons why the VLAN information can fail

to be exchanged. Verify these items if switches that run VTP fail to exchange VLAN information:VTP information only passes through a trunk port. Make sure that all ports that interconnect switches are configured as trunks and are actually trunking. Make sure that if EtherChannels are created between two switches, only Layer 2 EtherChannels propagate VLAN information.Make sure that the VLANs are active in all the devices.One of the switches must be the VTP server in a VTP domain. All VLAN changes must be done on this switch in order to have them propagated to the VTP clients. The VTP domain name must match and it is case sensitive. CISCO and cisco are two different domain names.Make sure that no password is set between the server and client. If any password is set, make sure that the password is the same on both sides.
http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a0080890613.shtml QUESTION 6After implementing VTP, the extended VLANs are not being propagated to other VTP switches. What should be configured for extended VLANs? A. VTP does not support extended VLANs and should be manually added to all switches.B. Enable VTP version 3, which supports extended VLAN propagation.C. VTP authentication is required when using extended VLANs because of their ability to cause network instability.D. Ensure that all switches run the same Cisco IOS version. Extended VLANs will not propagate to different IOS versions when extended VLANs are in use. Answer: BExplanation:VTP version 1 and VTP version 2 do not propagate configuration information for extended- range VLANs (VLAN numbers 1006 to 4094). You must configure extended-range VLANs manually on each network device.VTP version 3 supports extended-range VLANs (VLAN numbers 1006 to 4094). If you convert from VTP version 3 to VTP version 2, the VLANs in the range 1006 to 4094 are removed from VTP control. QUESTION 7Refer to the exhibit. Switch A, B, and C are trunked together and have been properly configured for VTP. Switch C receives VLAN information from the VTP server Switch A, but Switch B does not receive any VLAN information. What is the most probable cause of this behavior? A. Switch B is configured in transparent mode.B. Switch B is configured with an access port to Switch A, while Switch C is configured with a trunk port to Switch B.C. The VTP revision number of the Switch B is higher than that of Switch A.D. The trunk between Switch A and Switch B is misconfigured. Answer: AExplanation:VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2. QUESTION 8Refer to the exhibit. Switch A, B, and C are trunked together and have been properly configured for VTP. Switch B has all VLANs, but Switch C is not receiving traffic from certain VLANs. What would cause this issue? A. A VTP authentication mismatch occurred between Switch A and SwitchB. B. The VTP revision number of Switch B is higher than that of Switch A.C. VTP pruning is configured globally on all switches and it removed VLANs from the trunk interface that is connected to Switch C.D. The trunk between Switch A and Switch B is misconfigured. Answer: CExplanation: VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices.Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default. VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. The best explanation for why switch C is not seeing traffic from only some of the VLANs, is that VTP pruning has been configured. QUESTION 9After the recent upgrade of the switching infrastructure, the network engineer notices that the port roles that were once "blocking" are now defined as "alternate" and "backup." What is the reason for this change? A. The new switches are using RSTP instead of legacy IEEE 802.1D STP.B. IEEE 802.1D STP and PortFast have been configured by default on all newly implemented Cisco Catalyst switches.C. The administrator has defined the switch as the root in the STP domain.D. The port roles have been adjusted based on the interface bandwidth and timers of the new Cisco Catalyst switches. Answer: AExplanation:RSTP works by adding an alternative port and a backup port compared to STP. These ports are allowed to immediately enter the forwarding state rather than passively wait for the network to converge.RSTP bridge port roles:Root port A forwarding port that is the closest to the root bridge in terms of path costDesignated port A forwarding port for every LAN segment Alternate port A best alternate path to the root bridge. This path is different than using the root port. The alternative port moves to the forwarding state if there is a failure on the designated port for the segment.Backup port A backup/redundant path to a segment where another bridge port already connects. The backup port applies only when a single switch has two links to the same segment (collision domain). To have two links to the same collision domain, the switch must be attached to a hub.Disabled port Not strictly part of STP, a network administrator can manually disable a port. QUESTION 10An administrator recently configured all ports for rapid transition using PortFast. After testing, it has been determined that several ports are not transitioning as they should. What is the reason for this? A. RSTP has been enabled per interface and not globally.B. The STP root bridge selection is forcing key ports to remain in non-rapid transitioning mode.C. STP is unable to achieve rapid transition for trunk links.D. The switch does not have the processing power to ensure rapid transition for all ports. Answer: CExplanation:RSTP can only achieve rapid transition to the forwarding state on edge ports and on

point-to- point links, not on trunk links. The link type is automatically derived from the duplex mode of a port. A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port by default.This automatic link type setting can be overridden by explicit configuration. In switched networks today, most links operate in full-duplex mode and are treated as point-to-point links by RSTP. This makes them candidates for rapid transition to the forwarding state. QUESTION 11 Which technique automatically limits VLAN traffic to only the switches that require it? A. access listsB. DTP in nonegotiateC. VTP pruningD. PBR Answer: 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. QUESTION 21Pilot testing of the new switching infrastructure finds that when the root port is lost, STP immediately replaces the root port with an alternative root port. Which spanning-tree technology is used to accomplish backup root port selection? A. PVST+B. PortFastC. BackboneFastD. UplinkFastE. Loop GuardF. UDLD Answer: DExplanation: If a switch loses connectivity, it begins using the alternate paths as soon as the spanning tree selects a new root port. By enabling UplinkFast with the spanning-tree uplinkfast global configuration command, you can accelerate the choice of a new root port when a link or switch fails or when the spanning tree reconfigures itself. The root port transitions to the forwarding state immediately without going through the listening and learning states, as it would with the normal spanning-tree procedures. UplinkFast provides fast convergence after a direct link failure and achieves load balancing between redundant Layer 2 links using uplink groups. An uplink group is a set of Layer 2 interfaces (per VLAN), only one of which is forwarding at any given time. Specifically, an uplink group consists of the root port (which is forwarding) and a set of blocked ports, except for self-looping ports. The uplink group provides an alternate path in case the currently forwarding link fails. QUESTION 22A network engineer must adjust the STP interface attributes to influence root port selection. Which two elements are used to accomplish this? (Choose two.) A. port-priorityB. costC. forward-timersD. link typeE. root guard Answer: ABExplanation:Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment. When two ports on a switch are part of a loop, the spanning-tree port priority and path cost settings control which port is put in the forwarding state and which is put in the blocking state. The spanning-tree port priority value represents the location of a port in the network topology and how well it is located to pass traffic. The path cost value represents the media speed. QUESTION 23A network engineer must set the load balance method on an existing port channel. Which action must be done to apply a new load balancing method? A. Configure the new load balancing method using port-channel load-balance.B. Adjust the switch SDM back to "default".C. Ensure that IP CEF is enabled globally to support all load balancing methods.D. Upgrade the PFC to support the latest load balancing methods. Answer: AExplanation:EtherChannel balances the traffic load across the links in a channel through the reduction of part of the binary pattern that the addresses in the frame form to a numerical value that selects one of the links in the channel. EtherChannel load balancing can use MAC addresses or IP addresses, source or destination addresses, or both source and destination addresses. The mode applies to all EtherChannels that are configured on the switch. You configure the load balancing and forwarding method with use of the port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac} global configuration command. QUESTION 24Refer to the exhibit. A network engineer investigates a recent network failure and notices that one of the interfaces on the switch is still down. What is causing the line protocol on this interface to be shown as down? A. There is a layer 1 physical issue.B. There is a speed mismatch on the interface.C. The interface is configured as the target of the SPAN session.D. The interface is configured as the source of the SPAN session.E. There is a duplex mismatch on the interface. Answer: CExplanation:With the SAPN destination port, the state of the destination port is up/down by design. The interface shows the port in this state in order to make it evident that the port is currently not usable as a production port. This is the normal operational state for SPAN destinations. QUESTION 25While doing network discovery using Cisco Discovery Protocol, it is found that rapid error tracking is not currently enabled. Which option must be enabled to allow for enhanced reporting mechanisms using Cisco Discovery Protocol? A. Cisco Discovery Protocol version 2B. Cisco IOS Embedded Event ManagerC. logging bufferedD. Cisco Discovery Protocol source interfaceE. Cisco Discovery Protocol logging options Answer: AExplanation:CDP Version 1 -- This is the first version of CDP which was used for the discovery of Cisco devices in the network. This version is mainly used for backward compatibility.CDP Version 2 -- This is the most recent version of CDP which has enhanced features such as rapid reporting mechanism, which is used to track down errors and minimize

costly downtime. It allows you to track instances even if the native VLAN ID or port duplex states do not match between connecting devices.This is the default version on all switches. Lead2pass is the leader in supplying candidates with current and up-to-date training materials for Cisco certification and exam preparation. Comparing with others, our 300-115 exam questions are more authoritative and complete. We offer 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=0B3Syig5i8gpDUFIySDhBLWlPcmc 2017 Cisco 300-115 exam dumps (All 401 Q&As) from Lead2pass: http://www.lead2pass.com/300-115.html [100% Exam Pass Guaranteed]