[2017 New 2017 New 300-115 Exam PDF Ensure 300-115 Certification Exam Pass Successfully (76-100)

2017 July Cisco Official New Released 300-115 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Lead2pass is one of the leading exam preparation material providers. Its updated 300-115 braindumps in PDF can ensure most candidates pass the exam without too much effort. If you are struggling for the 300-115 exam, it will be a wise choice that get help from Lead2pass. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/300-115.html QUESTION 76Which two statements about default FHRP behavior are true? (Choose two) A. A backup GLBP active virtual gateway can become active only if the current active virtual gateway fails.B. Preemption is enabled by default.C. Unless specifically Configured, the priority of an HSRP router is 200.D. A standby HSRP router becomes active if it has a higher priority than the priority of the current active router.E. A VRRP backup virtual router becomes the master router if its priority is higher than the priority of the current master router.Answer: AE QUESTION 77What is the maximum number of 10 Gigabit Ethernet connections that can be utilized in an EtherChannel for the virtual switch link? A. 4B. 6C. 8D. 12 Answer: CExplanation:The VSS is made up of the following:Virtual switch members: Cisco Catalyst 6500 Series Switches (up to two switches with initial release) deployed with the Virtual Switching Supervisor 720 10GE Virtual switch link (VSL): 10 Gigabit Ethernet connections (up to eight using EtherChannel) between the virtual switch members.Reference: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_qas0900aecd806ed74b.html QUESTION 78Which statement describes what happens if all VSL connections between the virtual switch members are lost? A. Both virtual switch members cease to forward traffic.B. The VSS transitions to the dual active recovery mode, and both virtual switch members continue to forward traffic independently.C. The virtual switch members reload.D. The VSS transitions to the dual active recovery mode, and only the new active virtual switch continues to forward traffic. Answer: DExplanation:What happens if all VSL connections between the virtual switch members are lost?VSLs can be configured with up to eight links between the two switches across any combination of line cards or supervisor ports to provide a high level of redundancy. If for some rare reason all VSL connections are lost between the virtual switch members leaving both the virtual switch members up, the VSS will transition to the dual active recovery mode. The dual active state is detected rapidly (subsecond) by any of the following three methods:Enhancement to PAgP used in MEC with connecting Cisco switches L3 Bidirectional Forwarding Detection (BFD) configuration on a directly connected link (besides VSL) between virtual switch members or through an L2 link through an access layer switch L2 Fast-Hello Dual-Active Detection configuration on a directly connected link (besides VSL) between virtual switch members (supported with 12.2(33)SXI) In the dual active recovery mode, all interfaces except the VSL interfaces are in an operationally shut down state in the formerly active virtual switch member. The new active virtual switch continues to forward traffic on all links.Reference: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_qas0900aecd806ed74b.html QUESTION 79Which statement describes what happens when a switch enters dual active recovery mode? A. The switch shuts down and waits for the VSL link to be restored before sending traffic.B. All interfaces are shut down in the formerly active virtual switch member, but the new active virtual switch forwards traffic on all links.C. The switch continues to forward traffic out all links and enables spanning tree on VSL link and all other links to prevent loops.D. The VSS detects which system was last in active state and shuts down the other switch. Answer: BExplanation:In the dual active recovery mode, all interfaces except the VSL interfaces are in an operationally shut down state in the formerly active virtual switch member. The new active virtual switch continues to forward traffic on all links.Reference: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps9336/prod_qas0900aecd806ed74b.html QUESTION 80Which command globally enables AAA on a device? A. aaa new-modelB. aaa authenticationC. aaa authorizationD. aaa accounting Answer: AExplanation:To configure AAA authentication, enable AAA by using the aaa new-model global configuration command. AAA features are not available for use until you enable AAA globally by issuing the aaa new-model command.Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html QUESTION 81Which AAA Authorization type includes PPP, SLIP, and ARAP connections? A. networkB. IP mobileC. EXECD. auth-proxy Answer: A Explanation:Method lists for authorization define the ways that authorization will be performed and the sequence in which these methods will be performed. A method list is simply a named list describing the authorization methods to be queried (such as RADIUS or TACACS+), in sequence. Method lists enable you to designate one or more security protocols to be used for authorization, thus ensuring a backup system in case the initial method fails. Cisco IOS software uses the first method listed to authorize users for specific network services; if that method fails to respond, the Cisco IOS software selects the next method listed in the method list. This process continues until there is successful communication with a listed authorization method, or all methods

defined are exhausted. Method lists are specific to the authorization type requested:Auth-proxy--Applies specific security policies on a per-user basis. For detailed information on the authentication proxy feature, refer to the chapter "Configuring Authentication Proxy" in the "Traffic Filtering and Firewalls" part of this book.Commands--Applies to the EXEC mode commands a user issues. Command authorization attempts authorization for all EXEC mode commands, including global configuration commands, associated with a specific privilege level.EXEC--Applies to the attributes associated with a user EXEC terminal session. ·Network--Applies to network connections. This can include a PPP, SLIP, or ARAP connection.Reverse Access--Applies to reverse Telnet sessions.When you create a named method list, you are defining a particular list of authorization methods for the indicated authorization type.Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathor.html QUESTION 82Which authentication service is needed to configure 802.1x? A. RADIUS with EAP ExtensionB. TACACS+C. RADIUS with CoAD. RADIUS using VSA Answer: AExplanation:With 802.1x, the authentication server--performs the actual authentication of the client. The authentication server validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN and switch services. Because the switch acts as the proxy, the authentication service is transparent to the client. The Remote Authentication Dial-In User Service (RADIUS) security system with Extensible Authentication Protocol (EAP) extensions is the only supported authentication server.Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2940/software/release/121_19_ea1/configuration/guide/2940scg_1/sw8021x.pdf QUESTION 83Refer to the exhibit. Which login credentials are required when connecting to the console port in this output? A. none requiredB. username cisco with password ciscoC. no username with password linepassD. login authentication default Answer: AExplanation:Here the console has been configured with the NO_AUTH name, which lists none as the authentication method. None means no authentication, meaning that credentials are not required and all sessions are allowed access immediately. QUESTION 84Refer to the exhibit. When a network administrator is attempting an SSH connection to the device, in which order does the device check the login credentials? A. RADIUS server, local username, line passwordB. RADIUS server, line password, local usernameC. Line password, local username, RADIUS serverD. Line password, RADIUS server, local username Answer: AExplanation:SSH sessions use the vty lines, where the configured authentication method is named "default." The AAA default login preference is stated in order from first to last, so here the "aaa authentication login default group radius local line" means to use RADIUS first, then if that fails use the local user database. Finally, if that fails use the line password. QUESTION 85Which type of information does the DHCP snooping binding database contain? A. untrusted hosts with leased IP addressesB. trusted hosts with leased IP addressesC. untrusted hosts with available IP addressesD. trusted hosts with available IP addresses Answer: AExplanation:DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:Validates DHCP messages received from untrusted sources and filters out invalid messages.Rate-limits DHCP traffic from trusted and untrusted sources. · Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.pdf QUESTION 86 Which switch feature determines validity based on IP-to-MAC address bindings that are stored in a trusted database? A. Dynamic ARP InspectionB. storm controlC. VTP pruningD. DHCP snooping Answer: AExplanation: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. Reference: http://www.cisco.com/c/en/us/support/docs/switches/catalyst-3750-series-switches/72846-layer2-secftrs-catl3fixed.html QUESTION 87Which command is needed to enable DHCP snooping if a switchport is connected to a DHCP server? A. ip dhcp snooping trustB. ip dhcp snoopingC. ip dhcp trustD. ip dhcp snooping information Answer: AExplanation:When configuring DHCP snooping, follow these guidelines:DHCP snooping is not active until you enable the feature on at least one VLAN, and enable DHCP globally on the switch.Before globally enabling DHCP snooping on the switch, make sure that the devices acting as the DHCP server and the DHCP relay agent are configured and enabled.If a Layer 2 LAN port is connected to a DHCP server, configure the port as trusted by entering the "ip dhcp snooping trust" interface configuration command.If a Layer 2 LAN port is connected to a DHCP client, configure the port as untrusted by entering the no ip dhcp snooping trust interface configuration command.Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html QUESTION 88When you configure private VLANs on a switch, which port type connects the switch to the gateway router? A. promiscuousB.

communityC. isolatedD. trunked Answer: AExplanation:There are mainly two types of ports in a Private VLAN: Promiscuous port (P-Port) and Host port. Host port further divides in two types Isolated port (I-Port) and Community port (C-port). Promiscuous port (P-Port):The switch port connects to a router, firewall or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port on the VLAN.Host Ports:- Isolated Port (I-Port): Connects to the regular host that resides on isolated VLAN. This port communicates only with P-Ports.- Community Port (C-Port): Connects to the regular host that resides on community VLAN. This port communicates with P-Ports and ports on the same community VLAN. http://en.wikipedia.org/wiki/Private_VLAN. QUESTION 89When you configure a private VLAN, which type of port must you configure the gateway router port as? A. promiscuous portB. isolated portC. community portD. access port Answer: AExplanation:There are mainly two types of ports in a Private VLAN: Promiscuous port (P-Port) and Host port. Host port further divides in two types Isolated port (I-Port) and Community port (C-port). Promiscuous port (P-Port):The switch port connects to a router, firewall or other common gateway device. This port can communicate with anything else connected to the primary or any secondary VLAN. In other words, it is a type of a port that is allowed to send and receive frames from any other port on the VLAN.Host Ports:- Isolated Port (I-Port): Connects to the regular host that resides on isolated VLAN. This port communicates only with P-Ports.- Community Port (C-Port): Connects to the regular host that resides on community VLAN. This port communicates with P-Ports and ports on the same community VLAN.http://en.wikipedia.org/wiki/Private_VLAN QUESTION 90Which First Hop Redundancy Protocol is an IEEE Standard? A. GLBPB. HSRPC. VRRPD. OSPF Answer: CExplanation: http://cciethebeginning.wordpress.com/2008/08/23/router-high-availability-protocol-comparison-2/ QUESTION 91Refer to the exhibit. Which two statements about SW1 are true? (Choose two) A. InterfaceGi5/1 is using a Cisco proprietary trunking protocolB. On Interface Gi5/1, all untagged traffic is tagged with VLAN 113C. The device is configured with the default MST regionD. Interface Gi5/1 is using an industry-standard trunking protocolE. Interface Gi6/2 is the root port for VLAN 36F. On interface Gi6/2, all untagged traffic is tagged with VLAN 600 Answer: DF QUESTION 92Refer to the exhibit. Which two commands ensure that DSW1 becomes root bridge for VLAN 10 and 20? (Choose two.) A. spanning-tree mstp 1 priority 0B. spanning-tree mst1 root primaryC. spanning-tree mst vlan 10,20 priority rootD. spanning-tree mst1 priority 4096E. spanning-tree mst1 priority 1F. spanning-tree mstp vlan 10,20 root primary Answer: BD QUESTION 93Which gateway role is responsible for answering ARP requests for the virtual IP address in GLBP? A. active virtual forwarderB. active virtual routerC. active virtual gatewayD. designated router Answer: CExplanation:GLBP Active Virtual Gateway Members of a GLBP group elect one gateway to be the active virtual gateway (AVG) for that group. Other group members provide backup for the AVG in the event that the AVG becomes unavailable. The AVG assigns a virtual MAC address to each member of the GLBP group. Each gateway assumes responsibility for forwarding packets sent to the virtual MAC address assigned to it by the AVG. These gateways are known as active virtual forwarders (AVFs) for their virtual MAC address. The AVG is responsible for answering Address Resolution Protocol (ARP) requests for the virtual IP address. Load sharing is achieved by the AVG replying to the ARP requests with different virtual MAC addresses.http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_glbp.html QUESTION 94Which VRRP router is responsible for forwarding packets that are sent to the IP addresses of the virtual router? A. virtual router masterB. virtual router backupC. virtual router activeD. virtual router standby Answer: AExplanation:VRRP DefinitionsVRRP Router A router running the Virtual Router Redundancy Protocol. It may participate in one or more virtual routers.Virtual Router An abstract object managed by VRRP that acts as a default router for hosts on a shared LAN. It consists of a Virtual Router Identifier and a set of associated IP address(es) across a common LAN. A VRRP Router may backup one or more virtual routers.IP Address Owner The VRRP router that has the virtual router's IP address(es) as real interface address (es). This is the router that, when up, will respond to packets addressed to one of these IP addresses for ICMP pings, TCP connections, etc. Primary IP Address An IP address selected from the set of real interface addresses. One possible selection algorithm is to always select the first address. VRRP advertisements are always sent using the primary IP address as the source of the IP packet.Virtual Router Master The VRRP router that is assuming the responsibility of forwarding packets sent to the IP address(es) associated with the virtual router, and answering ARP requests for these IP addresses.Note that if the IP address owner is available, then it will always become the Master. http://www.ietf.org/rfc/rfc3768.txt QUESTION 95Which command correctly configures standby tracking for group 1 using the default decrement priority value? A. standby 1 track 100B. standby 1 track 100 decrement 1C. standby 1 track 100 decrement 5 D. standby 1 track 100 decrement 20 Answer: AExplanation:The default decrement value for HSRP standby tracking is 10. There is no need to explicitly state the value if the desired value is the default value. QUESTION 96Which command configures an HSRP group to become a slave of another HSRP group? A. standby slaveB. standby group trackC. standby followD. standby group backup Answer: CExplanation:Perform this task to configure multiple HSRP client groups. The "standby follow" command

configures an HSRP group to become a slave of another HSRP group.HSRP client groups follow the master HSRP with a slight, random delay so that all client groups do not change at the same time.
http://www.cisco.com/en/US/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-hsrp-mgo.html QUESTION 97Refer to the exhibit. Which option describes the reason for this message in a GLBP configuration? A. Unavailable GLBP active forwarderB. Incorrect GLBP IP addressC. HSRP configured on same interface as GLBPD. Layer 2 loop Answer: DExplanation:This section provides information you can use to troubleshoot your configuration.%GLBP-4-DUPADDR: Duplicate address The error message indicates a possible layer2 loop and STP configuration issues. In order to resolve this issue, issue the show interface command to verify the MAC address of the interface. If the MAC address of the interface is the same as the one reported in the error message, then it indicates that this router is receiving its own hello packets sent. Verify the spanning-tree topology and check if there is any layer2 loop. If the interface MAC address is different from the one reported in the error message, then some other device with a MAC address reports this error message.Note: GLBP members communicate between each other through hello messages sent every 3 seconds to the multicast address 224.0.0.102 and User DatagramProtocol (UDP) port 3222 (source and destination). When configuring the multicast boundary command, permit the Multicast address by permit 224.0.0.015.255.255.255.Reference: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_example09186a00807d2520.shtml#dr QUESTION 98Lab Simulation - LACP with STP Sim You work for SWITCH.com. They have just added a new switch (SwitchB) to the existing network as shown in the topology diagram. RouterA is currently configured correctly and is providing the routing function for devices on SwitchA and SwitchB. SwitchA is currently configured correctly, but will need to be modified to support the addition of SwitchB. SwitchB has a minimal configuration. You have been tasked with competing the needed configuring of SwitchA and SwitchB. SwitchA and SwitchB use Cisco as the enable password. Configuration Requirements for SwitchAThe VTP and STP configuration modes on SwitchA should not be modified. - SwitchA needs to be the root switch for vlans 11, 12, 13, 21, 22 and 23. All other vlans should be left are their default values. Configuration Requirements for SwitchB - Vlan 21Name: Marketing will support two servers attached to fa0/9 and fa0/10 - Vlan 22Name: Saleswill support two servers attached to fa0/13 and fa0/14 - Vlan 23Name: Engineeringwill support two servers attached to fa0/15 and fa0/16 - Access ports that connect to server should transition immediately to forwarding state upon detecting the connection of a device.- SwitchB VTP mode needs to be the same as SwitchA.- SwitchB must operate in the same spanning tree mode as SwitchA- No routing is to be configured on SwitchB- Only the SVI vlan 1 is to be configured and it is to use address 192.168.1.11/24 Inter-switch Connectivity Configuration Requirements - For operational and security reasons trunking should be unconditional and Vlans 1, 21, 22 and 23 should tagged when traversing the trunk link.- The two trunks between SwitchA and SwitchB need to be configured in a mode that allows for the maximum use of their bandwidth for all vlans. This mode should be done with a non-proprietary protocol, with SwitchA controlling activation.- Propagation of unnecessary broadcasts should be limited using manual pruning on this trunk link. Answer: SW-A (close to router) SW-A#configure terminal SW-A(config)#spanning-tree vlan 11-13,21-23 root primary SW-A(config)#vlan 21 SW-A(config-vlan)#name MarketingSW-A(config-vlan)#exit SW-A(config)#vlan 22SW-A(config-vlan)#name Sales SW-A(config-vlan)#exit SW-A(config)#vlan 23SW-A(config-vlan)#name EngineeringSW-A(config-vlan)#exit SW-A(config)#interface range Fa0/3 ? 4SW-A(config-if-range)#no switchport mode accessSW-A(config-if-range)#no switchport access vlan 98 (These two commands must be deleted to form a trunking link)SW-A(config-if-range)#switchport trunk encapsulation dot1q (cannot issued this command on this switch, but don?t worry coz I still got 100%) SW-A(config-if-range)#switchport mode trunkSW-A(config-if-range)#switchport trunk native vlan 99 SW-A(config-if-range)#switchport trunk allowed vlan 1,21-23SW-A(config-if-range)#channel-group 1 mode active SW-A(config-if-range)#channel-protocol lacpSW-A(config-if-range)#no shutdownSW-A(config-if-range)#end SW-B (far from router)SW-B#configure terminal SW-B(config)#vlan 21SW-B(config-vlan)#name MarketingSW-B(config-vlan)#exit SW-B(config)#vlan 22SW-B(config-vlan)#name SalesSW-B(config-vlan)#exit SW-B(config)#vlan 23SW-B(config-vlan)#name EngineeringSW-B(config-vlan)#exitSW-B(config)#vlan 99SW-B(config-vlan)#name TrunkNative // not necessary to name it but just name it same as SwitchASW-B(config-vlan)#exitSW-B(config)#interface range Fa0/9 ? 10SW-B(config-if-range)#switchport mode accessSW-B(config-if-range)#switchport access vlan 21SW-B(config-if-range)#spanning-tree portfast SW-B(config-if-range)#no shutdownSW-B(config-if-range)#exit SW-B(config)#interface range Fa0/13 ? 14 SW-B(config-if-range)#switchport mode accessSW-B(config-if-range)#switchport access vlan 22 SW-B(config-if-range)#spanning-tree portfastSW-B(config-if-range)#no shutdownSW-B(config-if-range)#exit SW-B(config)#interface range Fa0/15 ? 16SW-B(config-if-range)#switchport mode accessSW-B(config-if-range)#switchport access vlan 23SW-B(config-if-range)#spanning-tree portfastSW-B(config-if-range)#no shutdownSW-B(config-if-range)#exit SW-B(config)#vtp mode transparent SW-B(config)#spanning-tree mode rapid-pvst SW-B(config)#ip default-gateway 192.168.1.1

(you can get this IP from SW-A with command show cdp neighbour detail) // not sure about this command because the question says ?No routing is to be configured on SwitchB?. SW-B(config)#interface vlan 1SW-B(config-if)#ip address 192.168.1.11 255.255.255.0SW-B(config-if)#no shutdownSW-B(config-if)#exit SW-B(config)#interface range Fa0/3 ? 4 SW-B(config-if-range)#switchport trunk encapsulation dot1q (yes I can issued this command on this switch) SW-B(config-if-range)#switchport mode trunkSW-B(config-if-range)#switchport trunk native vlan 99 SW-B(config-if-range)#switchport trunk allowed vlan 1,21-23SW-B(config-if-range)#channel-group 1 mode passive //mode passive because ?SwitchA controlling activation?SW-B(config-if-range)#channel-protocol lacpSW-B(config-if-range)#no shutdown SW-B(config-if-range)#end Some guidelines for configuring SwitchA & SwitchB: Configuration Requirements for SwitchA- The VTP and STP configuration modes on SwitchA should not be modified.? SwitchA needs to be the root switch for vlans 11, 12, 13, 21, 22 and 23. All other vlans should be left are their default values SW-A(config)#spanning-tree vlan 11-13,21-23 root primary Configuration Requirements for SwitchB- Vlan 21, Name: Marketing, will support two servers attached to fa0/9 and fa0/10? Vlan 22, Name: Sales, will support two servers attached to fa0/13 and fa0/14? Vlan 23, Name: Engineering, will support two servers attached to fa0/15 and fa0/16? Access ports that connect to server should transition immediately to forwarding state upon detecting the connection of a device. vlan ?name ?(VLANs must be created on both switches if not exist)interface range Fa0/x ? xswitchport mode accessswitchport access vlanspanning-tree portfast- SwitchB VTP mode needs to be the same as SwitchA. vtp mode transparent- SwitchB must operate in the same spanning tree mode as SwitchA. spanning-tree mode rapid-pvst- No routing is to be configured on SwitchB.? Only the SVI vlan 1 is to be configured and it is to use address 192.168.1.11/24. interface vlan 1ip address 192.168.1.11 255.255.255.0Inter-switch Connectivity Configuration Requirements:- For operational and security reasons trunking should be unconditional and Vlans 1, 21, 22 and 23 should tagged when traversing the trunk link. SW-A(config)#interface range Fa0/3 ? 4SW-A(config-if)#no switchport mode accessSW-A(config-if)#no switchport access vlan 98 //These two commands must be deleted to form a trunking link.SW-A(config-if)#switchport mode trunkSW-A(config-if)#switchport trunk native vlan 99?????????????SW-B(config)#interface range Fa0/3 ? 4SW-B(config-if)#switchport trunk encapsulation dot1q (yes I can issued this command on this switch)SW-B(config-if)#switchport mode trunkSW-B(config-if)#switchport trunk native vlan 99- The two trunks between SwitchA and SwitchB need to be configured in a mode that allows for the maximum use of their bandwidth for all vlans. This mode should be done with a non-proprietary protocol, with SwitchA controlling activation. SW-A(config)#interface range Fa0/3 ? 4SW-A(config-if)#channel-group 1 mode activeSW-A(config-if)#channel-protocol lacp SW-A(config-if)#no shutdown?????????????SW-B(config)#interface range Fa0/3 ? 4SW-B(config-if)#channel-group 1 mode passiveSW-B(config-if)#channel-protocol lacpSW-B(config-if)#no shutdown?????????????Maybe the interface Port-channel 1 was configured on both switches so we don't configure it here. If not we have to configure them with ?interface port-channel 1? command. Also you have to turn them up.- Propagation of unnecessary broadcasts should be limited using manual pruning on this trunk link. SW-A(config)#interface range Fa0/3 ? 4SW-A(config-if)#switchport trunk allowed vlan 1,21-23????????????? SW-B(config)#interface range Fa0/3 ? 4SW-B(config-if)#switchport trunk allowed vlan 1,21-23 You may have to configure Interface Port-Channel on both switches. Check the configuration first, if it does not exist, use these commands: interface port-channel1switchport mode trunkswitchport trunk native vlan 99 //this command will prevent the ?Native VLAN mismatched? error on both switchesswitchport trunk allowed vlan 1,21-23,99 Some notes for this sim:+ You should check the initial status of both switches with these commands: show vtp status (transparent mode on switchA and we have to set the same mode on switchB), show spanning-tree [summary] (rapid-pvst mode on switchA and we have to set the same mode on switchB), show vlan (check the native vlan and the existence of vlan99), show etherchannel 1 port-channel and show ip int brief (check if Port-channel 1 has been created and make sure it is up), show run (to check everything again).+ When using ?int range f0/x - y? command hit space bar before and after ?-? otherwise the simulator does not accept it.+ You must create vlan 99 for the switchB. SwitchA already have vlan 99 configured.+ At the end, you can try to ping from SwitchB to RouterA (you can get the IP on RouterA via the show cdp neighbors detail on SwitchA), not sure if it can ping or not. If not, you can use the ?ip default-gateway 192.168.1.1? on SwitchB.+ The name of SwitchA and SwitchB can be swapped or changed so be careful to put your configuration into appropriate switch. QUESTION 99 Lab Simulation - AAA dot1x SWITCH.com is an IT company that has an existing enterprise network comprised of two layer 2 only switches; DSW1 and ASW1. The topology diagram indicates their layer 2 mapping. VLAN 20 is a new VLAN that will be used to provide the shipping personnel access to the server. Corporate polices do not allow layer 3 functionality to be enabled on the switches. For security reasons, it is necessary to restrict access to VLAN 20 in the following manner: - Users connecting to VLAN 20 via portfO/1 on ASW1 must be authenticated before they are given access to the network. Authentication is to be done via a Radius server:- Radius server host: 172.120.40.46- Radius key: rad123- Authentication should be implemented as close to the host as possible.- Devices on VLAN 20 are restricted to the subnet of 172.120.40.0/24.- Packets from devices in the subnet of

172.120.40.0/24 should be allowed on VLAN 20.- Packets from devices in any other address range should be dropped on VLAN 20. - Filtering should be implemented as close to the serverfarm as possible. The Radius server and application servers will be installed at a future date. You have been tasked with implementing the above access control as a pre-condition to installing the servers. You must use the available IOS switch features. Answer: 1. Verification of Pre-configuration:a. Check that the denoted vlan [vlan20] is created in both switches and ports [fa0/1 of ASW1] are assigned. b. Take down the radius-server ip [172.120.39.46] and the key [rad123].c. Take down the IP range [172.120.40.0/24] to be allowed the given vlan [vlan20]2. Configure the Port based authentication on ASW1:Enable AAA on the switch:ASW1> enable ASW1# conf tASW1(config)# aaa new-modelThe new-model keyword refers to the use of method lists, by which authentication methods and sources can be grouped or organized. De?ne the server along with its secret shared password:ASW1(config)# aaa authentication dot1x default group radius ASW1(config)# radius-server host 172.120.39.46 key rad123 This command causes the RADIUS server de?ned on the switch to be used for 802.1x authentication.Enable 802.1x on the switch: ASW1(config)# dot1x system-auth-controlCon?gure Fa0/1 to use 802.1x: ASW1(config)# interface fastEthernet 0/1ASW1(config-if)# switchport mode accessASW1(config-if)# dot1x port-control auto Notice that the word ?auto? will force connected PC to authenticate through the 802.1x exchange. ASW1(config-if)# exitASW1# copy running-config startup-config 3. Filter the traffic and create vlan access-map to restrict the traffic only for a range on DSW1 Define an access-list:DSW1> enable DSW1# conf tDSW1(config)# ip access-list standard 10 (syntax: ip access-list {standard | extended} acl-name)DSW1(config-ext-nacl)# permit 172.120.40.0 0.0.0.255DSW1(config-ext-nacl)# exitDefine an access-map which uses the access-list above:DSW1(config)# vlan access-map MYACCMAP 10 (syntax: vlan access-map map_name [0-65535])DSW1(config-access-map)# match ip address 10 (syntax: match ip address {acl_number | acl_name})DSW1(config-access-map)# action forwardDSW1(config-access-map)# exitDSW1(config)# vlan access-map MYACCMAP 20DSW1(config-access-map)# action drop (drop other networks)DSW1(config-access-map)# exit Apply a vlan-map into a vlan: DSW1(config)# vlan filter MYACCMAP vlan-list 20 (syntax: vlan filter mapname vlan-list list)DSW1# copy running-config startup-config 4. Note:It is not possible to verify the configuration in this lab. All we have do the correct configurations. Most of the exam takers report that ?copy running-config startup-config? is not working. It does not a matter. Do not try unwanted/wrong commands in the consoles. They are not real switches. QUESTION 100Hotspot - HSRPFerris Plastics, Inc. is a medium sized company, with an enterprise network (access, distribution and core switches) that provides LAN connectivity from user PCs to corporate servers. The distribution switches are configured to use HSRPto provide a high availability solution. - DSW1 -primary device for VLAN 101 VLAN 102 andVLAN 105- DSW2 - primary device for VLAN 103 and VLAN 104- A failure of GigabitEthemet1/0/1 on primary device should cause the primary device to release its status as the primary device, unless GigabitEthernet1/0/1 on backup device has also failed. Troubleshooting has identified several issues. Currently all interfaces are up. Using the running configurations and show commands, you have been asked to investigate and respond to the following question. During routine maintenance, GigabitEthernet1/0/1 on DSW1 was shut down. All other interfaces were up. DSW2 became the active HSRP device for VLAN 101 as desired. However, after GigabitEthemet1/0/1 on DSW1 was reactivated, DSW1 did not become the active router for VLAN 101 as desired. What needs to be done to make the group for VLAN 101 function properly? A. Enable preempt in the VLAN 101 HSRP group on DSW1.B. Disable preempt in the VLAN 101 HSRP group on DSW2's.C. In the VLAN 101 HSRP group on DSW1, decrease the priority value to avaluethatis less ' than the priority value configured in the VLAN 101 HSRP group on DSW2.D. Decrease the decrement value in the track command for the VLAN 101 HSRP group on U DSWTs to a values less than the value in the track command for the VLAN 101 HSRP group on DSW2. Answer: AExplanation: A is correct. All other answers is incorrect. Because Vlan101 on DS1 (left) disable preempt. We need enable preempt to after it reactive, it will be active device. If not this command, it never become active device. There is no doubt that Lead2pass is the top IT certificate exam material provider. All the braindumps are the latest and tested by senior Cisco lecturers and experts. Get the 300-115 exam braindumps in Lead2pass, and there would be no suspense to pass the exam. 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]