[PDF&VCE Lead2pass 100-101 Exam Questions Guarantee 200-105 Certification Exam 100% Success (31-50)

2016 September Cisco Official New Released **200-105** Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Lead2pass is ready to provide Cisco candidates with 200-105 exam dumps which can be very helpful for getting Cisco certification, which means that candidates can easily get access to the services of Cisco 200-105 exam dumps, which will assure them 100% passing success rate. With Lead2pass 200-105 exam dumps, it will be easy to pass your 200-105 exam at your first time. Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/200-105.html QUESTION 31 Refer to the exhibit. While troubleshooting a switch, you executed the show interface port-channel 1 etherchannel command and it returned this output. Which information is provided by the Load value?

A. the percentage of use of the link B. the preference of the link C. the session count of the link D. the number source-destination pairs on the link Answer: D QUESTION 32 Which spanning-tree feature places a port immediately into a forwarding stated? A. BPDU guard B. PortFast C. loop guard D. UDLD E. Uplink Fast Answer: B Explanation: PortFast causes a switch or trunk port to enter the spanning tree forwarding state immediately, bypassing the listening and learning states. You can use PortFast on switch or trunk ports that are connected to a single workstation, switch, or server to allow those devices to connect to the network immediately, instead of waiting for the port to transition from the listening and learning states to the forwarding state. QUESTION 33 Which protocol authenticates connected devices before allowing them to access the LAN? A. 802.1d B. 802.11 C. 802.1w D. 802.1x Answer: D Explanation: 802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The term 'supplicant' is also used interchangeably to refer to the software running on the client that provides credentials to the authenticator. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols. The authenticator acts like a security guard to a protected network. The supplicant (i.e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. An analogy to this is providing a valid visa at the airport's arrival immigration before being allowed to enter the country. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network. QUESTION 34 Which identification number is valid for an extended ACL? A. 1 B. 64 C. 99 D. 100 E. 299 F. 1099 Answer: D QUESTION 35 Which two pieces of information are provided by the show controllers serial 0 command? (Choose two.) A. the type of cable that is connected to the interface. B. The uptime of the interface C. the status of the physical layer of the interface D. the full configuration of the interface E. the interface's duplex settings Answer: AC Explanation: The show controller command provides hardware-related information useful to troubleshoot and diagnose issues with Cisco router interfaces. The Cisco 12000 Series uses a distributed architecture with a central command-line interface (CLI) at the Gigabit Route Processor (GRP) and a local CLI at each line card. QUESTION 36 Which EIGRP for IPv6 command can you enter to view the link-local addresses of the neighbors of a device? A. show ipv6 eigrp 20 interfaces B. show ipv6 route eigrp C. show ipv6 eigrp neighbors D. show ip eigrp traffic Answer: C QUESTION 37 Which configuration can you apply to enable encapsulation on a subinterface? A. interface FastEthernet 0/0 encapsulation dot1Q 30 ip address 10.1.1.30 255.255.255.0 B. interface FastEthernet 0/0.30 ip address 10.1.1.30 255.255.255.0 C. interface FastEthernet 0/0.30 description subinterface vlan 30 D. interface FastEthernet 0/0.30 encapsulation dot1Q 30 ip address 10.1.1.30 255.255.255.0 Answer: D QUESTION 38 Which statement about slow inter VLAN forwarding is true? A. The VLAN is experiencing slowness in the point-to-point collisionless connection. B. The VLANs are experiencing slowness because multiple devices are connected to the same hub. C. The local VLAN is working normally, but traffic to the alternate VLAN is forwarded slower than expected. D. The entire VLAN is experiencing slowness. E. The VLANs are experiencing slowness due to a duplex mismatch. Answer: E Explanation: Common Causes of Slow IntraVLAN and InterVLAN

Connectivity The symptoms of slow connectivity on a VLAN can be caused by multiple factors on different network layers. Commonly the network speed issue may be occurring on a lower level, but symptoms can be observed on a higher level as the problem masks itself under the term "slow VLAN". To clarify, this document defines the following new terms: "slow collision domain", "slow broadcast domain" (in other words, slow VLAN), and "slow interVLAN forwarding". These are defined in the section Three Categories of Causes, below. In the following scenario (illustrated in the network diagram below), there is a Layer 3 (L3) switch performing interVLAN routing between the server and client VLANs. In this failure scenario, one server is connected to a switch, and the port duplex mode is configured half- duplex on the server side and full-duplex on the switch side. This misconfiguration results in a packet loss and slowness, with increased packet loss when higher traffic rates occur on the link where the server is connected. For the clients who communicate with this server, the problem looks like slow interVLAN forwarding because they do not have a problem communicating to other devices or clients on the same VLAN. The problem occurs only when communicating to the server on a different VLAN. Thus, the problem occurred on a single collision domain, but is seen as slow interVLAN forwarding. Three Categories of Causes The causes of slowness can be divided into three categories, as follows: Slow Collision Domain Connectivity Collision domain is defined as connected devices configured in a half-duplex port configuration, connected to each other or a hub. If a device is connected to a switch port and full-duplex mode is configured, such a point-to-point connection is collisionless. Slowness on such a segment still can occur for different reasons. Slow Broadcast Domain Connectivity (Slow VLAN) Slow broadcast domain connectivity occurs when the whole VLAN (that is, all devices on the same VLAN) experiences slowness. Slow InterVLAN Connectivity (Slow Forwarding Between VLANs) Slow interVLAN connectivity (slow forwarding between VLANs) occurs when there is no slowness on the local VLAN, but traffic needs to be forwarded to an alternate VLAN, and it is not forwarded at the expected rate. Causes for Network Slowness Packet Loss In most cases, a network is considered slow when higher-layer protocols (applications) require extended time to complete an operation that typically runs faster. That slowness is caused by the loss of some packets on the network, which causes higher-level protocols like TCP or applications to time out and initiate retransmission. Hardware Forwarding Issues With another type of slowness, caused by network equipment, forwarding (whether Layer 2 [L2] or L3) is performed slowly. This is due to a deviation from normal (designed) operation and switching to slow path forwarding. An example of this is when Multilayer Switching (MLS) on the switch forwards L3 packets between VLANs in the hardware, but due to misconfiguration, MLS is not functioning properly and forwarding is done by the router in the software (which drops the interVLAN forwarding rate significantly). QUESTION 39 Which statement about the IP SLAs ICMP Echo operation is true? A. The frequency of the operation .s specified in milliseconds. B. It is used to identify the best source interface from which to send traffic. C. It is configured in enable mode. D. It is used to determine the frequency of ICMP packets. Answer: D Explanation: This module describes how to configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) Echo operation to monitor end-to-end response time between a Cisco router and devices using IPv4 or IPv6. ICMP Echo is useful for troubleshooting network connectivity issues. This module also demonstrates how the results of the ICMP Echo operation can be displayed and analyzed to determine how the network IP connections are performing. ICMP Echo Operation The ICMP Echo operation measures end-to-end response time between a Cisco router and any devices using IP. Response time is computed by measuring the time taken between sending an ICMP Echo request message to the destination and receiving an ICMP Echo reply. In the figure below ping is used by the ICMP Echo operation to measure the response time between the source IP SLAs device and the destination IP device. Many customers use IP SLAs ICMP-based operations, in-house ping testing, or ping-based dedicated probes for response time measurements. The IP SLAs ICMP Echo operation conforms to the same IETF specifications for ICMP ping testing and the two methods result in the same response times. Configuring a Basic ICMP Echo Operation on the Source Device SUMMARY STEPS 1. enable 2. configure terminal 3. ip sla operation-number 4. icmp-echo {destination-ip-address | destination-hostname} [source-ip {ip-address | hostname} | source-interface interface-name] 5. frequency seconds 6. end QUESTION 40 Which option describes how a switch in rapid PVST+ mode responds to a topology change? A. It immediately deletes dynamic MAC addresses that were learned by all ports on the switch. B. It sets a timer to delete all MAC addresses that were learned dynamically by ports in the same STP instance. C. It sets a timer to delete dynamic MAC addresses that were learned by all ports on the switch. D. It immediately deletes all MAC addresses that were learned dynamically by ports in the same STP instance. Answer: D Explanation: Rapid PVST+This spanning-tree mode is the same as PVST+ except that is uses a rapid convergence based on the IEEE 802.1w standard. To provide rapid convergence, the rapid PVST+ immediately deletes dynamically learned MAC address entries on a per-port basis upon receiving a topology change. By contrast, PVST+ uses a short aging time for dynamically learned MAC address entries. The rapid PVST+ uses the same configuration as PVST+ (except where noted), and the switch needs only minimal extra configuration. The benefit of rapid PVST+ is that you can migrate a large PVST+ install base to rapid PVST+ without having to learn the complexities of the MSTP configuration and without having to reprovision

your network. In rapid-PVST+ mode, each VLAN runs its own spanning-tree instance up to the maximum supported. QUESTION 41 Which type of topology is required by DMVPN? A. ring B. full mesh C. hub-and-spoke D. partial mesh Answer: C QUESTION 42 Refer to the exhibit. Router edge-1 is unable to establish OSPF neighbor adjacency with router ISP-1. Which two configuration changes can you make on edge-1 to allow the two routers to establish adjacency? (Choose two.)

A. Set the subnet mask on edge-1 to 255 255.255.252. B. Reduce the MTU on edge-1 to 1514. C. Set the OSPF cost on edge-1 to 1522. D. Reduce the MTU on edge-1 to 1500. E. Configure the ip ospf mtu-ignore command on the edge-1 Gi0/0 interface. Answer: DE Explanation: A situation can occur where the interface MTU is at a high value, for example 9000, while the real value of the size of packets that can be forwarded over this interface is 1500. If there is a mismatch on MTU on both sides of the link where OSPF runs, then the OSPF adjacency will not form because the MTU value is carried in the Database Description (DBD) packets and checked on the other side. QUESTION 43 Which statement about switch access ports is true? A. They drop packets with 802.1Q tags. B. A VLAN must be assigned to an access port before it is created. C. They can receive traffic from more than one VLAN with no voice support D. By default, they carry traffic for VLAN 10. Answer: A Explanation: "If an access port receives a packet with an 802.1Q tag in the header other than the access VLAN value, that port drops the packet without learning its MAC source address." QUESTION 44 Which option is a benefit of switch stacking? A. It provides redundancy with no impact on resource usage. B. It simplifies adding and removing hosts. C. It supports better performance of high-needs applications. D. It provides higher port density with better resource usage. Answer: D Explanation: A stackable switch is a network switch that is fully functional operating standalone but which can also be set up to operate together with one or more other network switches, with this group of switches showing the characteristics of a single switch but having the port capacity of the sum of the combined switches. QUESTION 45 What is the first step you perform to configure an SNMPv3 user? A. Configure server traps. B. Configure the server group. C. Configure the server host. D. Configure the remote engine ID. Answer: B Explanation: The first task in configuring SNMPv3 is to define a view. To simplify things, we'll create a view that allows access to the entire internet subtree: router(config)#snmp-server view readview internet included This command creates a view called readview. If you want to limit the view to the system tree, for example, replace internet with system. The included keyword states that the specified tree should be included in the view; use excluded if you wanted to exclude a certain subtree. Next, create a group that uses the new view. The following command creates a group called readonly ; v3 means that SNMPv3 should be used. The auth keyword specifies that the entity should authenticate packets without encrypting them; read readview says that the view named readview should be used whenever members of the readonly group access the router. router(config)#snmp-server group readonly v3 auth read readview QUESTION 46 Which statement about named ACLs is true? A. They support standard and extended ACLs. B. They are used to filter usernames and passwords for Telnet and SSH. C. They are used to filter Layer 7 traffic. D. They support standard ACLs only. E. They are used to rate limit traffic destined to targeted networks. Answer: A Explanation: Named Access Control Lists (ACLs) allows standard and extended ACLs to be given names instead of numbers. Unlike in numbered Access Control Lists (ACLs), we can edit Named Access Control Lists. Another benefit of using named access configuration mode is that you can add new statements to the access list, and insert them wherever you like. With the legacy syntax, you must delete the entire access list before reapplying it using the updated rules. QUESTION 47 Which two switch states are valid for 802.1w? (Choose two.) A. listening B. backup C. disabled D. learning E. discarding Answer: DE Explanation: Port States There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state. QUESTION 48 Which statement about MPLS is true? A. It operates in Layer 1. B. It operates between Layer 2 and Layer 3. C. It operates in Layer 3. D. it operates in Layer 2. Answer: B Explanation: MPLS belongs to the family of packet-switched networks. MPLS operates at a layer that is generally considered to lie between traditional definitions of OSI Layer 2 (data link layer) and Layer 3 (network layer), and thus is often referred to as a layer 2.5 protocol. QUESTION 49 Which Cisco platform can verify ACLs? A. Cisco Prime Infrastructure B. Cisco Wireless LAN Controller C.

Cisco APIC-EM D.   Cisco IOS-XE Answer: B QUESTION 50 Which three options are the HSRP states for a router? (Choose three.) A.   initialize B.   learn C.   secondary D.   listen E.   speak F.   primary Answer: BDE Lead2pass are committed on providing you with the latest and most accurate 200-105 exam dumps. Our 200-105 dump is rich in variety. We offer 200-105 PDF dumps and 200-105 VCE dumps. We ensure you can pass the 200-105 easily. Welcome to Lead2pass.com. **200-105** new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDY2V1UExCV21ZUHM 2016 Cisco **200-105** exam dumps (All 346 Q&As) from Lead2pass: http://www.lead2pass.com/200-105.html [100% Exam Pass Guaranteed]