[Dec-2016-NewFree 200-105 Exam Dump PDF Offered by Braindump2go[31-40

2016/12 New Cisco 200-105: Interconnecting Cisco Networking Devices Part 2 (ICND2 v3.0) Exam Questions Updated Today! Free Instant Download 200-105 Exam Dumps (PDF & VCE) 346q from Braindump2go.com Today! 100% Real Exam Questions! 100% Exam Pass Guaranteed! 1.|2016/12 New 200-105 Exam Dumps (PDF & VCE) 346q Download: http://www.braindump2go.com/200-105.html2.|2016/12 New 200-105 Exam Questions & Answers: https://1drv.ms/f/s!AvI7wzKf6QBjgR8N2yzsALYPi7P6 QUESTION 31Refer 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 linkB. the preference of the linkC. the session count of the linkD. the number source-destination pairs on the link Answer: D QUESTION 32Which spanning-tree feature places a port immediately into a forwarding stated? A. BPDU guardB. PortFastC. loop guardD. UDLDE. Uplink Fast Answer: BExplanation: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 33Which protocol authenticates connected devices before allowing them to access the LAN? A. 802.1dB. 802.11C. 802.1wD. 802.1x Answer: DExplanation: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 34Which identification number is valid for an extended ACL? A. 1B. 64C. 99D. 100E. 299F. 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 interfaceC. the status of the physical layer of the interfaceD. the full configuration of the interfaceE. the interface's duplex settings Answer: ACExplanation: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 36Which EIGRP for IPv6 command can you enter to view the link-local addresses of the neighbors of a device? A. show ipv6 eigrp 20 interfacesB. show ipv6 route eigrpC. show ipv6 eigrp neighborsD. show ip eigrp traffic Answer: C QUESTION 37Which configuration can you apply to enable encapsulation on a subinterface? A. interface FastEthernet 0/0encapsulation dot1Q 30ip address 10.1.1.30 255.255.255.0B. interface FastEthernet 0/0.30ip address 10.1.1.30 255.255.255.0C. interface FastEthernet 0/0.30description subinterface vlan 30D. interface FastEthernet 0/0.30encapsulation dot1Q 30ip address 10.1.1.30 255.255.255.0 Answer: D QUESTION 38Which 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: EExplanation: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 CausesThe 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 SlownessPacket LossIn 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 IssuesWith 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 39Which 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: DExplanation: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 OperationThe 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 STEPS1. 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 40Which 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: DExplanation: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. !!!RECOMMEND!!!   1.|2016/12 New 200-105 Exam Dumps (PDF & VCE) 346q Download:http://www.braindump2go.com/200-105.html2.|2016/12 New 200-105 Study Guide: YouTube Video: YouTube.com/watch?v=MPVtnwlwW3E