[2017 New Lead2pass 2017 100% Real 100-105 Exam Questions (181-200)

2017 June Cisco Official New Released 100-105 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed!
Lead2pass is one of the leading exam preparation material providers. Its updated 100-105 braindumps in PDF can ensure most candidates pass the exam without too much effort. If you are struggling for the 100-105 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/100-105.html QUESTION 181Some routers have been configured with default routes. What are some of the advantages of using default routes? (Choose two) A. They establish routes that will never go down.B. They keep routing tables small.C. They require a great deal of CPU power.D. They allow connectivity to remote networks that are not in the routing tableE. They direct traffic from the internet into corporate networks.Answer: BDExplanation: Cisco administration 101: What you need to know about default routes
http://www.techrepublic.com/article/cisco-administration-101-what-you-need-to-know-about-default-routes/ QUESTION 182Refer to the exhibit. PC1 pings PC2. What three things will CORE router do with the data that is received from PC1? (Choose three.) A. The data frames will be forwarded out interface FastEthernet0/1 of CORE router.B. The data frames will be forwarded out interface FastEthernet1/0 of CORE router.C. CORE router will replace the destination IP address of the packets with the IP address of PC2.D. CORE router will replace the MAC address of PC2 in the destination MAC address of the frames.E. CORE router will put the IP address of the forwarding FastEthernet interface in the place of the source IP address in the packets.F. CORE router will put the MAC address of the forwarding FastEthernet interface in the place of the source MAC address. Answer: BDF QUESTION 183Which three statements are correct about RIP version 2? (Choose three) A. It uses broadcast for its routing updates.B. It supports authentication.C. It is a classless routing protocol.D. It has a lower default administrative distance then RIP version 1.E. It has the same maximum hop count as RIP version 1.F. It does not send the subnet mask any updates. Answer: BCE QUESTION 184Refer to the exhibit. Why are two OSPF designated routers identified on Core-Router? A. Core-Router is connected to more than one multi-access network.B. The router at 208.149.23.130 is a secondary DR in case the primary fails.C. Two router IDs have the same OSPF priority and are therefore tied for DR electionD. The DR election is still underway and there are two contenders for the role. Answer: AExplanation: OSPF elects one DR per multi-access network. In the exhibit there are two DR so there must have more than one multi-access network. QUESTION 185What is the OSPF default frequency, in seconds, at which a Cisco router sends hello packets on a multi-access network? A. 10B. 40C. 30D. 20 Answer: AExplanation: On broadcast multiacess and point-to-point links, the default is 10 seconds. On NBMA, the default is 30 seconds. QUESTION 186What does the "Inside Global" address represent in the configuration of NAT? A. the summarized address for all of the internal subnetted addressesB. the MAC address of the router used by inside hosts to connect to the InternetC. a globally unique, private IP address assigned to a host on the inside networkD. a registered address that represents an inside host to an outside network Answer: DExplanation: NAT: Local and Global Definitions
http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094837.shtmlCisco defines these terms as:Inside local address--The IP address assigned to a host on the inside network. This is the address configured as a parameter of the computer OS or received via dynamic address allocation protocols such as DHCP. The address is likely not a legitimate IP address assigned by the Network Information Center (NIC) or service provider. Inside global address--A legitimate IP address assigned by the NIC or service provider that represents one or more inside local IP addresses to the outside world. Outside local address--The IP address of an outside host as it appears to the inside network. Not necessarily a legitimate address, it is allocated from an address space routable on the inside.Outside global address--The IP address assigned to a host on the outside network by the host owner.The address is allocated from a globally routable address or network space. These definitions still leave a lot to be interpreted. For this example, this document redefines these terms by first defining local address and global address. Keep in mind that the terms inside and outside are NAT definitions. Interfaces on a NAT router are defined as inside or outside with the NAT configuration commands, ip nat inside destination and ip nat outside source . Networks to which these interfaces connect can then be thought of as inside networks or outside networks, respectively. Local address--A local address is any address that appears on the inside portion of the network.Global address--A global address is any address that appears on the outside portion of the network. QUESTION 187Refer to the exhibit. A company wants to use NAT in the network shown. Which commands will apply the NAT configuration to the proper interfaces? (Choose two.) A. R1(config)# interface serial0/1R1(config-if)# ip nat insideB. R1(config)# interface serial0/1R1(config-if)# ip nat outsideC. R1(config)# interface fastethernet0/0R1(config-if)# ip nat insideD. R1(config)# interface fastethernet0/0R1(config-if)# ip nat outsideE. R1(config)# interface serial0/1R1(config-if)# ip nat outside source pool 200.2.2.18 255.255.255.252F. R1(config)# interface fastethernet0/0R1(config-if)# ip nat inside source 10.10.0.0 255.255.255.0 Answer: BC

QUESTION 188Which of the following statements are TRUE regarding Cisco access lists? (Choose two.) A. In an inbound access list, packets are filtered as they enter an interface.B. In an inbound access list, packets are filtered before they exit an interface.C. Extended access lists are used to filter protocol-specific packets.D. You must specify a deny statement at the end of each access list to filter unwanted traffic.E. When a line is added to an existing access list, it is inserted at the beginning of the access list. Answer: ACExplanation: In an inbound access list, packets are filtered as they enter an interface. Extended access lists are used to filter protocol specific packets. Access lists can be used in a variety of situations when the router needs to be given guidelines for decision-making. These situations include:Filtering traffic as it passes through the routerTo control access to the VTY lines (Telnet)To identify "interesting" traffic to invoke Demand Dial Routing (DDR) callsTo filter and control routing updates from one router to another There are two types of access lists, standard and extended. Standard access lists are applied as close to the destination as possible (outbound), and can only base their filtering criteria on the source IP address. The number used while creating an access list specifies the type of access list created. The range used for standard access lists is 1 to 99 and 1300 to 1999. Extended access lists are applied as close to the source as possible (inbound), and can base their filtering criteria on the source or destination IP address, or on the specific protocol being used. The range used for extended access lists is 100 to 199 and 2000 to 2699.Other features of access lists include:Inbound access lists are processed before the packet is routed. Outbound access lists are processed after the packet has been routed to an exit interface. An "implicit deny" is at the bottom of every access list, which means that if a packet has not matched any preceding access list condition, it will be filtered (dropped). Access lists require at least one permit statement, or all packets will be filtered (dropped). One access list may be configured per direction for each Layer 3 protocol configured on an interface The option stating that in an inbound access list, packets are filtered before they exit an interface is incorrect.Packets are filtered as they exit an interface when using an outbound access list. The option stating that a deny statement must be specified at the end of each access list in order to filter unwanted traffic is incorrect. There is an implicit deny at the bottom of every access list.When a line is added to an existing access list, it is not inserted at the beginning of the access list. It is inserted at the end. This should be taken into consideration. For example, given the following access list, executing the command access-list 110 deny tcp 192.168.5.0 0.0.0.255 any eq www would have NO effect on the packets being filtered because it would be inserted at the end of the list, AFTER the line that allows all traffic. access-list 110 permit ip host 192.168.5.1 anyaccess-list 110 deny icmp 192.168.5.0 0.0.0.255 any echo access-list 110 permit any any QUESTION 189From which of the following attacks can Message Authentication Code (MAC) shield your network? A. DoSB. DDoSC. spoofingD. SYN floods Answer: CExplanation: Message Authentication Code (MAC) can shield your network from spoofing attacks. Spoofing, also known as masquerading, is a popular trick in which an attacker intercepts a network packet, replaces the source address of the packets header with the address of the authorized host, and reinserts fake information which is sent to the receiver. This type of attack involves modifying packet contents. MAC can prevent this type of attack and ensure data integrity by ensuring that no data has changed. MAC also protects against frequency analysis, sequence manipulation, and ciphertext-only attacks. MAC is a secure message digest that requires a secret key shared by the sender and receiver, making it impossible for sniffers to change both the data and the MAC as the receiver can detect the changes.A denial-of-service (DoS) attack floods the target system with unwanted requests, causing the loss of service to users. One form of this attack generates a flood of packets requesting a TCP connection with the target, tying up all resources and making the target unable to service other requests. MAC does not prevent DoS attacks. Stateful packet filtering is the most common defense against a DoS attack.A Distributed Denial of Service attack (DDoS) occurs when multiple systems are used to flood the network and tax the resources of the target system. Various intrusion detection systems, utilizing stateful packet filtering, can protect against DDoS attacks. In a SYN flood attack, the attacker floods the target with spoofed IP packets and causes it to either freeze or crash. A SYN flood attack is a type of denial of service attack that exploits the buffers of a device that accept incoming connections and therefore cannot be prevented by MAC. Common defenses against a SYN flood attack include filtering, reducing the SYN-RECEIVED timer, and implementing SYN cache or SYN cookies. QUESTION 190Refer to the exhibit. After the power-on-self test (POST), the system LED of a Cisco 2950 switch turns amber. What is the status of the switch? A. The POST was successful.B. The switch has a problem with the internal power supply and needs an external power supply to be attached.C. POST failed and there is a problem that prevents the operating system from being loaded.D. The switch has experienced an internal problem but data can still be forwarded at a slower rate.E. The switch passed POST, but all the switch ports are busy. Answer: CExplanation: http://www.cisco.com/en/US/products/hw/switches/ps607/products_tech_note09186a00801
25913.shtmlEach time you power up the switch, eight Power-On Self Tests (POSTs) run automatically. POSTs check the most important system components before the switch begins to forward packets. When the switch begins the POST, the port status LEDs display amber for two seconds, and then display green. As each test runs, the port status LEDs go out. 1x is the first to go out. The port status LEDs for ports 2x through 8x go out sequentially as the system completes a test.When the POST completes successfully,

the port status LEDs go out. This indicates that the switch is operational. If a test fails, the port status LED associated with the test displays amber. The system LED also displays amber.NotE. From Cisco IOS Software Release 11.2(8.5) SA6 onwards, the port and system LEDs both remain amber after a POST failure. In the earlier Cisco IOS Software Releases, only the LEDs of failed linked ports remained amber. QUESTION 191Refer to the exhibit. A technician pastes the configurations in the exhibit into the two new routers shown. Otherwise, the routers are configured with their default configurations. A ping from Host1 to Host 2 fails, but the technician is able to ping the S0/0 interface of R2 from Host 1. The configurations of the hosts have been verified as correct. What could be the cause of the problem? A. The serial cable on R1 needs to be replaced.B. The interfaces on R2 are not configured properlyC. R1 has no route to the 192.168.1.128 network.D. The IP addressing scheme has overlapping subnetworks.E. The ip subnet-zero command must be configured on both routers. Answer: CExplanation: Without a static route pointing to host 2 network the router is unaware of the path to take to reach that network and reply traffic cannot be sent. QUESTION 192Refer to the exhibit. Why did the device return this message? A. The command requires additional options or parametersB. There is no show command that starts with ru.C. The command is being executed from the wrong router mode.D. There is more than one show command that starts with the letters ru. Answer: DExplanation: Answer D is correct because when you type the incomplete command having more same more command same up to types characters it shows display the ambiguous command error. QUESTION 193Refer to the exhibit. Serial 0/0 does not respond to a ping request from a host on the FastEthernet 0/0 LAN. How can this problem be corrected? A. Enable the Serial 0/0 interface.B. Correct the IP address for Serial 0/0.C. Correct the IP address for FastEthernet 0/0D. Change the encapsulation type on Serial 0/0E. Enable autoconfiguration on the Serial 0/0 interface Answer: AExplanation: Serial 0/0 interface is administratively down therefore, you will have to run the "no shutdown" command to enable the interface for data. QUESTION 194Refer to the exhibit. Why was this message received? A. No VTY password has been set.B. No enable password has been set.C. No console password has been set.D. No enable secret password has been set.E. The login command has not been set on CON 0F. The login command has not been set on the VTY ports. Answer: A QUESTION 195Refer to the exhibit. After configuring two interfaces on the HQ router, the network administrator notices an error message. What must be done to fix this error? A. The serial interface must be configured first.B. The serial interface must use the address 192.168.1.2C. The subnet mask of the serial interface should be changed to 255.255.255.0D. The subnet mask of the FastEthernet interface should be changed to 255.255.255.240E. The address of the FastEthernet interface should be changed to 192.168.1.66 Answer: D QUESTION 196Two routers named Atlanta and Brevard are connected by their serial interfaces as shown in the exhibit, but there is no data connectivity between them. The Atlanta router is known to have a correct configuration. Given the partial configurations shown in the exhibit, what is the problem on the Brevard router that is causing the lack of connectivity? A. A loopback is not set.B. The IP address is incorrect.C. The subnet mask is incorrect.D. The serial line encapsulations are incompatible.E. The maximum transmission unit (MTU) size is too large.F. The bandwidth setting is incompatible with the connected interface. Answer: B QUESTION 197What are two benefits of using a single OSPF area network design? (Choose two.) A. It is less CPU intensive for routers in the single area.B. It reduces the types of LSAs that are generated.C. It removes the need for virtual links.D. It increases LSA response times.E. It reduces the number of required OSPF neighbor adjacencies. Answer: BC QUESTION 198What command sequence will configure a router to run OSPF and add network 10.1.1.0 /24 to area 0? A. router ospf area 0network 10.1.1.0 255.255.255.0 area 0B. router ospfnetwork 10.1.1.0 0.0.0.255C. router ospf 1network 10.1.1.0 0.0.0.255 area 0D. router ospf area 0network 10.1.1.0 0.0.0.255 area 0E. router ospfnetwork 10.1.1.0 255.255.255.0 area 0F. router ospf 1network 10.1.1.0 0.0.0.255 Answer: C QUESTION 199Refer to the exhibit. If the router Cisco returns the given output and has not had its router ID set manually, what value will OSPF use as its router ID? A. 192.168.1.1B. 172.16.1.1C. 1.1.1.1D. 2.2.2.2 Answer: D QUESTION 200What OSPF command, when configured, will include all interfaces into area 0? A. network 0.0.0.0 255.255.255.255 area 0B. network 0.0.0.0 0.0.0.0 area 0C. network 255.255.255.255 0.0.0.0 area 0D. network all-interfaces area 0 Answer: A 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 100-105 exam braindumps in Lead2pass, and there would be no suspense to pass the exam. 100-105 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDSjRoR0JJWVA2ZDQ 2017 Cisco 100-105 exam dumps (All 321 Q&As) from Lead2pass: http://www.lead2pass.com/100-105.html [100% Exam Pass Guaranteed]