[2017 New Easily Pass 300-101 Exam With Lead2pass Updated Cisco 300-101 Dumps (1-20)

2017 July Cisco Official New Released 300-101 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! Lead2pass updates Cisco 300-101 exam questions, adds some new changed questions from Cisco Official Exam Center. Want to know 2017 300-101 exam test points? Download the following free Lead2pass latest exam questions today! Following questions and answers are all new published by Cisco Official Exam Center: http://www.lead2pass.com/300-101.html QUESTION 1A network engineer has been asked to ensure that the PPPoE connection is established and authenticated using an encrypted password. Which technology, in combination with PPPoE, can be used for authentication in this manner? A. PAPB. dot1xC. IPsecD. CHAPE. ESPAnswer: DExplanation:With PPPoE, the two authentication options are PAP and CHAP. When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or "challenges" the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router. When the remote device receives the challenge packet, it concatenates the ID, the remote device's password, and the random number, and then encrypts all of it using the remote device's password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process. When the access server receives the response, it uses the name it received to retrieve a password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password--if the result matches the result sent in the response packet, authentication succeeds. The benefit of using CHAP authentication is that the remote device's password is never transmitted in clear text (encrypted). This prevents other devices from stealing it and gaining illegal access to the ISP's network. http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html QUESTION 2A corporate policy requires PPPoE to be enabled and to maintain a connection with the ISP, even if no interesting traffic exists. Which feature can be used to accomplish this task? A. TCP AdjustB. Dialer PersistentC. PPPoE GroupsD. half-bridgingE. Peer Neighbor Route Answer: BExplanation:A new interface configuration command, dialer persistent, allows a dial-on-demand routing (DDR) dialer profile connection to be brought up without being triggered by interesting traffic. When configured, the dialer persistent command starts a timer when the dialer interface starts up and starts the connection when the timer expires. If interesting traffic arrives before the timer expires, the connection is still brought up and set as persistent. The command provides a default timer interval, or you can set a custom timer interval. QUESTION 3Which encapsulation supports an interface that is configured for an EVN trunk? A. 802.1QB. ISLC. PPPD. Frame RelayE. MPLSF. HDLC Answer: AExplanation:Restrictions for EVNAn EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.A single IP infrastructure can be virtualized to provide up to 32 virtual networks end-to-end. If an EVN trunk is configured on an interface, you cannot configure VRF-Lite on the same interface.OSPFv3 is not supported; OSPFv2 is supported. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.pdf QUESTION 4Which three characteristics are shared by subinterfaces and associated EVNs? (Choose three.) A. IP addressB. routing tableC. forwarding tableD. access control listsE. NetFlow configuration Answer: ABCExplanation:runk interface can carry traffic for multiple EVNs. To simplify the configuration process, all the subinterfaces and associated EVNs have the same IP address assigned. In other words, the trunk interface is identified by the same IP address in different EVN contexts. This is accomplished as a result of each EVN having a unique routing and forwarding table, thereby enabling support for overlapping IP addresses across multiple EVNs.http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/xe-3sg/evn-overview.pdf QUESTION 5Which traffic does the following configuration allow? ipv6 access-list ciscopermit ipv6 host 2001:DB8:0:4::32 any eq sshline vty 0 4ipv6 access-class cisco in A. all traffic to vty 0 4 from source 2001:DB8:0:4::32B. only ssh traffic to vty 0 4 from source allC. only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32D. all traffic to vty 0 4 from source all Answer: CExplanation:Here we see that the Ipv6 access list called "cisco" is being applied to incoming VTY connections to the router. Ipv6 access list has just one entry, which allows only the single Ipv6 IP address of 2001:DB8:0:4::32 to connect using SSH only. QUESTION 6For troubleshooting purposes, which method can you use in combination with the debug ip packet command to limit the amount of output data? A. You can disable the IP route cache globally.B. You can use the KRON scheduler.C. You can use an extended access list.D. You can use an IOS parser.E. You can use the RITE traffic exporter. Answer: CExplanation:The "debug ip packet" command generates a substantial amount of output and uses a substantial amount of system resources. This command should be used with caution in production networks. Always use with the access-list command to apply an extended ACL to the debug output. http://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

QUESTION 7Refer to the following access list. access-list 100 permit ip any any log After applying the access list on a Cisco router, the network engineer notices that the router CPU utilization has risen to 99 percent. What is the reason for this? A. A packet that matches access-list with the "log" keyword is Cisco Express Forwarding switched.B. A packet that matches access-list with the "log" keyword is fast switched.C. A packet that matches access-list with the "log" keyword is process switched.D. A large amount of IP traffic is being permitted on the router. Answer: CExplanation:ging-enabled access control lists (ACLs) provide insight into traffic as it traverses the network or is dropped by network devices. Unfortunately, ACL logging can be CPU intensive and can negatively affect other functions of the network device. There are two primary factors that contribute to the CPU load increase from ACL logging: process switching of packets that match log-enabled access control entries (ACEs) and the generation and transmission of log messages.http://www.cisco.com/web/about/security/intelligence/acl-logging.html#4 QUESTION 8Which address is used by the Unicast Reverse Path Forwarding protocol to validate a packet against the routing table? A. source address B. destination addressC. router interfaceD. default gateway Answer: AExplanation:The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribal Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet. http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html QUESTION 9What are the three modes of Unicast Reverse Path Forwarding? A. strict mode, loose mode, and VRF modeB. strict mode, loose mode, and broadcast modeC. strict mode, broadcast mode, and VRF modeD. broadcast mode, loose mode, and VRF mode Answer: AExplanation:Network administrators can use Unicast Reverse Path Forwarding (Unicast RPF) to help limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode. Note that not all network devices support all three modes of operation. Unicast RPF in VRF mode will not be covered in this document.When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.When administrators use Unicast RPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode.Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be of concern when deploying this feature, Unicast RPF loose mode is a scalable option for networks that contain asymmetric routing paths.http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html QUESTION 10What does the following access list, which is applied on the external interface FastEthernet 1/0 of the perimeter router, accomplish? router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any logrouter (config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any logrouter (config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any logrouter (config)#access-list 101 permit ip any anyrouter (config)#interface fastEthernet 1/0router (config-if)#ip access-group 101 in A. It prevents incoming traffic from IP address ranges 10.0.0.0-10.0.0.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 and logs any intrusion attempts.B. It prevents the internal network from being used in spoofed denial of service attacks and logs any exit to the Internet.C. It filters incoming traffic from private addresses in order to prevent spoofing and logs any intrusion attempts.D. It prevents private internal addresses to be accessed directly from outside. Answer: CExplanation:The private IP address ranges defined in RFC 1918 are as follows:10.0.0.0 -- 10.255.255.255172.16.0.0 -- 172.31.255.255192.168.0.0 -- 192.168.255.255These IP addresses should never be allowed from external networks into a corporate network as they would only be able to reach the network from the outside via routing problems or if the IP addresses were spoofed. This ACL is used to prevent all packets with a spoofed reserved private source IP address to enter the network. The log keyword also enables logging of this intrusion attempt. QUESTION 11Refer to the following command: router(config)# ip http secure-port 4433 Which statement is true? A. The router will listen on port 4433 for HTTPS traffic.B. The router will listen on port 4433 for HTTP traffic.C. The router will never accept any HTTP and HTTPS traffic.D. The router will listen to HTTP and HTTP traffic on port 4433. Answer: AExplanation:To set the secure HTTP (HTTPS) server port number for listening, use the ip http secure-port command in global configuration mode. To return the HTTPS server port number to the default, use the no form of this command.Ip http secure-port port-numberno ip http secure-portSyntax Description port-numberInteger in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.http://www.cisco.com/en/US/docs/ios-xml/ios/https/command/nm-https-cr-cl-sh.html#wp3612805529 QUESTION 12A network engineer is configuring SNMP on network devices to utilize one-way SNMP notifications. However, the engineer is not concerned with authentication or encryption. Which command satisfies the requirements of this scenario? A. router(config)#snmp-server host 172.16.201.28 traps version 2c CISCOROB. router(config)#snmp-server host 172.16.201.28 informs version 2c CISCOROC. router(config)#snmp-server host 172.16.201.28 traps version 3 auth CISCOROD. router(config)#snmp-server host 172.16.201.28 informs version 3 auth CISCORO Answer: AExplanation:Most network admins and engineers are familiar with SNMPv2c which has become the dominant SNMP version of the past decade. It's simple to configure on both the router/switch-side and just as easy on the network monitoring server. The problem of course is that the SNMP statistical payload is not encrypted and authentication is passed in cleartext. Most companies have decided that the information being transmitted isn't valuable enough to be worth the extra effort in upgrading to SNMPv3, but I would suggest otherwise.Like IPv4 to Ipv6, there are some major changes under the hood. SNMP version 2 uses community strings (think cleartext passwords, no encryption) to authenticate polling and trap delivery. SNMP version 3 moves away from the community string approach in favor of user-based authentication and view-based access control. The users are not actual local user accounts, rather they are simply a means to determine who can authenticate to the device. The view is used to define what the user account may access on the IOS device. Finally, each user is added to a group, which determines the access policy for its users. Users, groups, views. http://www.ccnpguide.com/snmp-version-3/ QUESTION 13When using SNMPv3 with NoAuthNoPriv, which string is matched for authentication? A. usernameB. passwordC. community-stringD. encryption-key Answer: AExplanation:The following security models exist: SNMPv1, SNMPv2, SNMPv3. The following security levels exits: "noAuthNoPriv" (no authentiation and no encryption ?noauth keyword in CLI), "AuthNoPriv109thernet109ationre authenticated but not encrypted ?auth keyword in CLI), "AuthPriv" (messages are authenticated and encrypted ?priv keyword in CLI). SNMPv1 and SNMPv2 models only support the "noAuthNoPriv" model since they use plain community string to match the incoming packets. The SNMPv3 implementations could be configured to use either of the models on per-group basis (in case if "noAuthNoPriv" is configured, username serves as a replacement for community string).http://blog.ine.com/2008/07/19/snmpv3-tutorial/ QUESTION 14After a recent DoS attack on a network, senior management asks you to implement better logging functionality on all IOS-based devices. Which two actions can you take to provide enhanced logging results? (Choose two.) A. Use the msec option to enable service time stamps.B. Increase the logging history.C. Set the logging severity level to 1.D. Specify a logging rate limit.E. Disable event logging on all noncritical items. Answer: ABExplanation:The optional msec keyword specifies the date/time format should include milliseconds. This can aid in pinpointing the exact time of events, or to correlate the order that the events happened. To limit syslog messages sent to the router's history table and to an SNMP network management station based on severity, use the logging history command in global configuration mode. By default, Cisco devices Log error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, "saving level warnings or higher." By increasing the severity level, more granular monitoring can occur, and SNMP messages will be sent by the less sever (5-7) messages. QUESTION 15A network engineer finds that a core router has crashed without warning. In this situation, which feature can the engineer use to create a crash collection? A. secure copy protocolB. core dumpsC. warm reloadsD. SNMPE. NetFlow Answer: BExplanation:When a router crashes, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the crash. Core dumps are generally very useful to your technical support representative.Four basic ways exist for setting up the router to generate a core dump: Using Trivial File Transfer Protocol (TFTP)Using File Transfer Protocol (FTP)Using remote copy protocol (rcp)Using a Flash disk http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr19aa.html QUESTION 16A network engineer is trying to implement broadcast-based NTP in a network and executes the ntp broadcast client command. Assuming that an NTP server is already set up, what is the result of the command? A. It enables receiving NTP broadcasts on the interface where the command was executed.B. It enables receiving NTP broadcasts on all interfaces globally.C. It enables a device to be an NTP peer to another device.D. It enables a device to receive NTP broadcast and unicast packets. Answer: AExplanation:The NTP service can be activated by entering any ntp command. When you use the ntp broadcast client command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously. CommandDescriptionntp broadcast clientAllows the system to receive NTP broadcast packets on an interface. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-xe-3se-3850-cr-book/bsm-xe-3se-3850-cr-book_chapter_00.html QUESTION 17Which three TCP enhancements can be used with TCP selective acknowledgments? (Choose three.) A. header compressionB. explicit congestion notificationC. keepaliveD. time stampsE. TCP path discoveryF. MTU window Answer: BCDExplanation:TCP Selective AcknowledgmentThe TCP Selective Acknowledgment feature improves performance if multiple packets are lost from one TCP window of data.Prior to this feature, because of limited information available from cumulative acknowledgments, a TCP sender could learn about only one lost packet per-round-trip time. An aggressive sender could choose to resend packets early, but such re-sent segments might have already been successfully received.The TCP selective acknowledgment mechanism helps improve performance. The receiving TCP host returns selective acknowledgment packets to the sender, informing the sender of data that has been received. In other words, the receiver can acknowledge packets received out of order. The sender can then resend only missing data segments (instead of everything since the first missing packet).Prior to selective acknowledgment, if TCP lost packets 4 and 7 out of an 8-packet window, TCP would receive acknowledgment of only packets 1, 2, and 3. Packets 4 through 8 would need to be re-sent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 must be re-sent.TCP selective acknowledgment is used only when multiple packets are dropped within one TCP window. There is no performance impact when the feature is enabled but not used. Use the ip tcp selective-ack command in global configuration mode to enable TCP selective acknowledgment. Refer to RFC 2018 for more details about TCP selective acknowledgment.TCP Time StampThe TCP time-stamp option provides improved TCP round-trip time measurements. Because the time stamps are always sent and echoed in both directions and the time-stamp value in the header is always changing, TCP header compression will not compress the outgoing packet. To allow TCP header compression over a serial link, the TCP time-stamp option is disabled. Use the ip tcp timestamp command to enable the TCP time-stamp option.TCP Explicit Congestion NotificationThe TCP Explicit Congestion Notification (ECN) feature allows an intermediate router to notify end hosts of impending network congestion. It also provides enhanced support for TCP sessions associated with applications, such as Telnet, web browsing, and transfer of audio and video data that are sensitive to delay or packet loss. The benefit of this feature is the reduction of delay and packet loss in data transmissions. Use the ip tcp ecn command in global configuration mode to enable TCP ECN.TCP Keepalive TimerThe TCP Keepalive Timer feature provides a mechanism to identify dead connections. When a TCP connection on a routing device is idle for too long, the device sends a TCP keepalive packet to the peer with only the Acknowledgment (ACK) flag turned on. If a response packet (a TCP ACK packet) is not received after the device sends a specific number of probes, the connection is considered dead and the device initiating the probes frees resources used by the TCP connection. QUESTION 18A network administrator uses IP SLA to measure UDP performance and notices that packets on one router have a higher one-way delay compared to the opposite direction. Which UDP characteristic does this scenario describe? A. latencyB. starvationC. connectionless communicationD. nonsequencing unordered packetsE. jitter Answer: AExplanation:Cisco IOS IP SLAs provides a proactive notification feature with an SNMP trap. Each measurement operation can monitor against a pre-set performance threshold. Cisco IOS IP SLAs generates an SNMP trap to alert management applications if this threshold is crossed. Several SNMP traps are available: round trip time, average jitter, one-way latency, jitter, packet loss, MOS, and connectivity tests.Here is a partial sample output from the IP SLA statistics that can be seen:router#show ip sla statistics 1Round Trip Time (RTT) for Index 55Latest RTT: 1 msLatest operation start time: *23:43:31.845 UTC Thu Feb 3 2005 Latest operation return code: OKRTT Values:Number Of RTT: 10 RTT Min/Avg/Max: 1/1/1 milliseconds Latency one-way time:Number of Latency one-way Samples: 0Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html QUESTION 19 Under which condition does UDP dominance occur? A. when TCP traffic is in the same class as UDPB. when UDP flows are assigned a lower priority queueC. when WRED is enabledD. when ACLs are in place to block TCP traffic Answer: A Explanation:Mixing TCP with UDPIt is a general best practice to not mix TCP-based traffic with UDP-based traffic (especially Streaming-Video) within a single service-provider class because of the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters throttle back flows when drops are detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely oblivious to drops and, thus, never lower transmission rates because of dropping. When TCP flows are combined with UDP flows within a single service-provider class and the class experiences congestion, TCP flows continually lower their transmission rates, potentially giving up their bandwidth to UDP flows that are oblivious to drops. This effect is called TCP starvation/UDP dominance.TCP starvation/UDP dominance likely occurs if (TCP-based) Mission-Critical Data is assigned to the same service-provider class as (UDP-based) Streaming-Video and the class experiences sustained congestion. Even if WRED is enabled on the service-provider class, the same behavior would be observed because WRED (for the most part) manages congestion only on TCP-based flows. http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/VPNQoS.html QUESTION 20PPPoE is composed of which two phases? A. Active Authentication Phase and PPP Session PhaseB. Passive

Discovery Phase and PPP Session PhaseC. Active Authorization Phase and PPP Session PhaseD. Active Discovery Phase and PPP Session Phase Answer: D Lead2pass promise that all 300-101 exam questions are the latest updated, we aim to provide latest and guaranteed questions for all certifications. You just need to be braved in trying then we will help you arrange all later things! 100% pass all exams you want or full money back! Do you want to have a try on passing 300-101? 300-101 new questions on Google Drive: https://drive.google.com/open?id=0B3Syig5i8gpDX0QwYXF1aXFINmM 2017 Cisco 300-101 exam dumps (All 403 Q&As) from Lead2pass: http://www.lead2pass.com/300-101.html [100% Exam Pass Guaranteed]