[NEW-300-101-ROUTEBraindump2go CCNP 300-101 Exam PDF Dumps 230Q&As for 100% Passing 300-101 Exam[NQ11-NQ20

2016/11 New CCNP Routing and Switching 300-101 ROUTE: Implementing Cisco IP Routing (ROUTE) Exam Questions Updated Today! 1.|2016.Nov. 300-101 Exam Dumps (PDF & VCE) 230Q&As Download:http://www.braindump2go.com/300-101.html 2.|2016.Nov. 300-101 Exam Questions & Answers:https://1drv.ms/b/s!AvI7wzKf6QBjgQU3MiuxP2dJi8Wo QUESTION 11Refer to the following command:router(config)# ip http secure-port 4433Which 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 !!!RECOMMEND!!! 1.Braindump2go|2016.Nov. 300-101 Exam Dumps (PDF & VCE) 230Q&As Download:http://www.braindump2go.com/300-101.html2.Braindump2go|2016.Nov. 300-101 Exam Questions & Answers: https://1drv.ms/b/s!AvI7wzKf6QBjgQU3MiuxP2dJi8Wo