[NEW-300-101-ROUTECCNP 300-101 VCE & PDF Free Download in Braindump2go[NQ21-NQ30

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 21Which statement is true about the PPP Session Phase of PPPoE? A.   PPP options are negotiated and authentication is not performed. Once the link setup is completed, PPPoE functions as a Layer 3 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.B.   PPP options are not negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 4 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.C.   PPP options are automatically enabled and authorization is performed.Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method that allows data to be encrypted over the PPP link within PPPoE headers.D.   PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers. Answer: DExplanation:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpn-cli/vpn-pppoe.html QUESTION 22Which type of traffic does DHCP snooping drop? A.   discover messagesB.   DHCP messages where the source MAC and client MAC do not matchC.   traffic from a trusted DHCP server to clientD.   DHCP messages where the destination MAC and client MAC do not match Answer: BExplanation:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html QUESTION 23Refer to the exhibit. Which command only announces the 1.2.3.0/24 network out of FastEthernet 0/0? A.   distribute list 1 outB.   distribute list 1 out FastEthernet0/0C.   distribute list 2 outD.   distribute list 2 out FastEthernet0/0 Answer: DExplanation:Access list 2 is more specific, allowing only 1.2.3.0/24, whereas access list 1 permits all 1.0.0.0/8 networks. This question also asks us to apply this distribute list only to the outbound direction of the fast Ethernet 0/0 interface, so the correct command is "distribute list 2 out FastEthernet0/0." QUESTION 24Which prefix is matched by the command ip prefix-list name permit 10.8.0.0/16 ge 24 le 24? A.   10.9.1.0/24B.   10.8.0.0/24C.   10.8.0.0/16D.   10.8.0.0/23 Answer: BExplanation:With prefix lists, the ge 24 term means greater than or equal to a /24 and the le 24 means less than or equal to /24, so only a /24 is both greater than or equal to 24 and less than or equal to 24. This translates to any prefix in the 10.8.x.0/24 network, where X is any value in the 0-255 range.Only the choice of 10.8.0.0.24 matches this. QUESTION 25Router A and Router B are configured with IPv6 addressing and basic routing capabilities using OSPFv3. The networks that are advertised from Router A do not show up in Router B's routing table. After debugging IPv6 packets, the message "not a router" is found in the output. Why is the routing information not being learned by Router B? A.   OSPFv3 timers were adjusted for fast convergence.B.   The networks were not advertised properly under the OSPFv3 process.C.   An IPv6 traffic filter is blocking the networks from being learned via the Router B interface that is connected to Router A.D.   IPv6 unicast routing is not enabled on Router A or Router B. Answer: DExplanation:
http://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_16.html QUESTION 26After you review the output of the command show ipv6 interface brief, you see that several IPv6 addresses have the 16-bit hexadecimal value of "FFFE" inserted into the address. Based on this information, what do you conclude about these IPv6 addresses? A.   IEEE EUI-64 was implemented when assigning IPv6 addresses on the device.B.   The addresses were misconfigured and will not function as intended. C.   IPv6 addresses containing "FFFE" indicate that the address is reserved for multicast.D.   The IPv6 universal/local flag (bit 7) was flipped.E.   IPv6 unicast forwarding was enabled, but IPv6 Cisco Express Forwarding was disabled. Answer: AExplanation: Extended Unique Identifier (EUI), as per RFC2373, allows a host to assign iteslf a unique 64-Bit IP Version 6 interface identify them EUI-64). This feature is a key benefit over IPv4 as it eliminates the need of manual configuration or DHCP as in the world of IPv4. The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The Mac address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific. The 16-bit 0xFFFE is then inserted between these two 24-bits to for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the EUI-48 MAC address.
https://supportforums.cisco.com/document/100566/understanding-ipv6-eui-64-bit-address QUESTION 27A packet capture log indicates that several router solicitation messages were sent from a local host on the IPv6 segment. What is the expected acknowledgment and its usage? A.   Router acknowledgment messages will be forwarded upstream, where the DHCP server will allocate addresses to the local host.B.   Routers on the IPv6 segment will respond with an advertisement that provides an external path from the local subnet, as well as certain data, such as prefix discovery.C.   Duplicate Address Detection will determine if any

other local host is using the same IPv6 address for communication with the IPv6 routers on the segment.D.   All local host traffic will be redirected to the router with the lowest ICMPv6 signature, which is statically defined by the network administrator. Answer: BExplanation:Router Advertisements (RA) are sent in response to router solicitation messages. Router solicitation messages, which have a value of 133 in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message. Given that router solicitation messages are usually sent by hosts at system startup (the host does not have a configured unicast address), the source address in router solicitation messages is usually the unspecified Ipv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When an RA is sent in response to a router solicitation, the destination address in the RA message is the unicast address of the source of the router solicitation message. RA messages typically include the following information:One or more onlink Ipv6 prefixes that nodes on the local link can use to automatically configure their Ipv6 addressesLifetime information for each prefix included in the advertisementSets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completedDefault router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time (in seconds) the router should be used as a default router)Additional information for hosts, such as the hop limit and MTU a host should use in packets that it originates http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-addrg_bsc_con.html QUESTION 28 A user is having issues accessing file shares on a network. The network engineer advises the user to open a web browser, input a prescribed IP address, and follow the instructions. After doing this, the user is able to access company shares. Which type of remote access did the engineer enable? A.   EZVPNB.   IPsec VPN client accessC.   VPDN client accessD.   SSL VPN client access Answer: DExplanation:The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100936-asa8x-split-tunnel-anyconnect-config.html QUESTION 29Which Cisco IOS VPN technology leverages IPsec, mGRE, dynamic routing protocol, NHRP, and Cisco Express Forwarding? A.   FlexVPNB.   DMVPNC.   GETVPND.   Cisco Easy VPN Answer: BExplanation:Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers and Unix-like Operating Systems based on the standard protocols, GRE, NHRP and Ipsec. This DMVPN provides the capability for creating a dynamic-mesh VPN network without having to pre-configure (static) all possible tunnel end-point peers, including Ipsec (Internet Protocol Security) and ISAKMP (Internet Security Association and Key Management Protocol) peers. DMVPN is initially configured to build out a hub-and-spoke network by statically configuring the hubs (VPN headends) on the spokes, no change in the configuration on the hub is required to accept new spokes. Using this initial hub- and-spoke network, tunnels between spokes can be dynamically built on demand (dynamic-mesh) without additional configuration on the hubs or spokes. This dynamic-mesh capability alleviates the need for any load on the hub to route data between the spoke networks.DMVPN is combination of the following technologies:http://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network QUESTION 30A network engineer is configuring a solution to allow failover of HSRP nodes during maintenance windows, as an alternative to powering down the active router and letting the network respond accordingly. Which action will allow for manual switching of HSRP nodes? A.   Track the up/down state of a loopback interface and shut down this interface during maintenance.B.   Adjust the HSRP priority without the use of preemption.C.   Disable and enable all active interfaces on the active HSRP node.D. Enable HSRPv2 under global configuration, which allows for maintenance mode. Answer: AExplanation:The standby track command allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority is reduced. This means that another HSRP router with higher priority can become the active router if that router has standby preempt enabled. Loopback interfaces can be tracked, so when this interface is shut down the HSRP priority for that router will be lowered and the other HSRP router will then become the active one.http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html !!!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