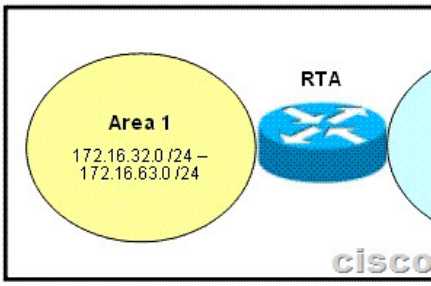
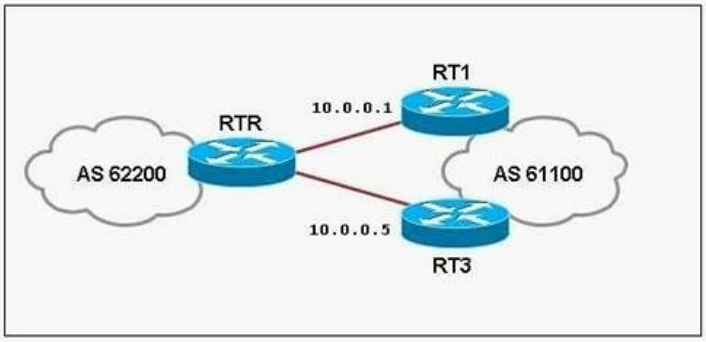
CCNP ROUTE(642-902) Questions (NEW)

1. What happens when an IPv6 enabled router running 6to4 must send a packet to a remote destination and the next hop is the address of 2002::/16? A.The packet is tagged with an IPv6 header and the IPv6 prefix is included. B.The IPv6 packet is encapsulated in an IPv4 packet using an IPv4 protocol type of 41. C.The IPv6 packet has its header removed and replaced with an IPv4 header. D.The IPv6 packet is dropped because that destination is unable to route IPv6 packets. **Correct Answers: B** 2. Router RTA is configured as follows: RTA (config)#router rip RTA(config-router)#network 10.0.0.0 RTA(config-router)#distribute-list 44 in interface BRI0 RTA(config-router)#exit RTA(config)#access-list 44 deny 172.16.1.0 0.0.0.255 RTA(config)#access-list 44 permit any What are the effects of this RIP configuration on router RTA? (Choose two.)

A.no routing updates will be sent from router RTA on interface BRI0 to router RTX B.router RTA will not advertise the 10.0.0.0 network to router RTX C.the route to network 172.16.1.0 will not be entered into the routing table on router RTA D.user traffic from the 172.16.1.0 network is denied by access-list 44 E.the routing table on router RTA will be updated with the route to router RTW **Correct Answers: C E Explanation:** Distribute list are used to filter routing updates and they are based on access lists. In this case, an access list of 44 was created to deny the route from network 172.16.1.0/24 so this route will not be entered into the routing table of RTA. But the route from RTW can be entered because it is not filtered by the access list A and B are not correct because the distribute list is applied to the inbound direction of interface BRI0 so outgoing routing updated will not be filtered. D is not correct because distribute list just filters routing updates so user traffic from network 172.16.1.0 will not be denied. 3. Refer to the exhibit. What must be configured on router RTA to summarize all routes from area 0 to area 1?

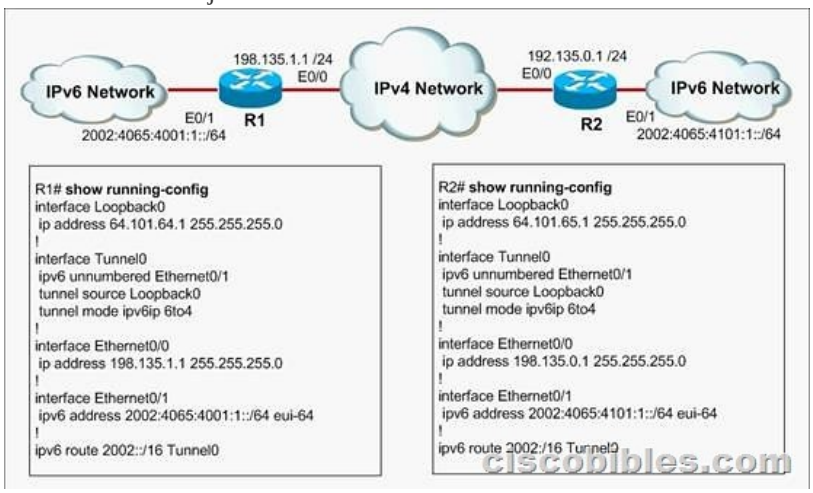


A.area 0 range 172.16.96.0 255.255.224.0 B.area 0 range 172.16.96.0 255.255.255.0 C.area 1 range 172.16.96.0 255.255.224.0 D.area 1 range 172.16.96.0 255.255.0.0 E.summary-address 172.16.96.0 255.255.224.0 F.summary-address 172.16.96.0 0.0.63.255 **Correct Answers: A** 4. Refer to the exhibit. Router RTR is attempting to establish BGP neighbor relationships with routers RT1 and RT3. On the basis of the information that is presented in the exhibit, which two statements are true? (Choose two.)




```
RTR# debug ip bgp
*Mar 1 03:27:00.879: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.1:179 to 10.0.0.2:11032
*Mar 1 03:27:00.883: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.1:179 to 10.0.0.2:11032
*Mar 1 03:27:04.311: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.1:11022 to 10.0.0.2:179
*Mar 1 03:27:12.315: %TCP-6-BADAUTH: No MD5 digest from 10.0.0.1:11022 to 10.0.0.2:179
*Mar 1 03:28:39.659: %TCP-6-BADAUTH: Invalid MD5 digest from 10.0.0.5:11026 to 10.0.0.6:179
*Mar 1 03:28:41.659: %TCP-6-BADAUTH: Invalid MD5 digest from 10.0.0.5:11026 to 10.0.0.6:179
```


A.RTR has a BGP password set but neighbor 10.0.0.1 does not. B.RTR has a BGP password set but neighbor 10.0.0.5 does not. C.RTR has a BGP password set but neighbor 10.0.0.1 has an incorrect password set. D.RTR has a BGP password set but neighbor 10.0.0.5 has an incorrect password set. E.Neighbor 10.0.0.1 has a BGP password set but RTR does not. F.Neighbor 10.0.0.5 has a BGP password set but RTR does not. **Correct Answers: A D Explanation:** You can configure MD5 authentication between two BGP peers, MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. If a router has a password configured for a peer, but the other peer does not, a message ?No MD5 digest from?? will appear on the console while the routers attempt to establish a Multicast Source Discovery Protocol (MSDP) session between them. Therefore A is correct because RT1 (with an ip address of 10.0.0.1) is not configured with a password. Similarly, if the two routers have different passwords configured, a message ?Invalid MD5 digest from?? will appear on the screen. 5. BGP contains two paths to a destination. Assuming both routes were originated locally and have an equal weight, what will be the next determining factor in choosing the best path? A.lowest MED B.highest local preference C.lowest neighbor IP address D.lowest origin code E.shortest AS-path **Correct Answers: B** 6. Refer to the exhibit. The 6to4 overlay tunnel configuration has been applied on each router to join isolated IPv6 networks over a IPv4 network. Which statements regarding the 6to4 overlay tunnel is true?

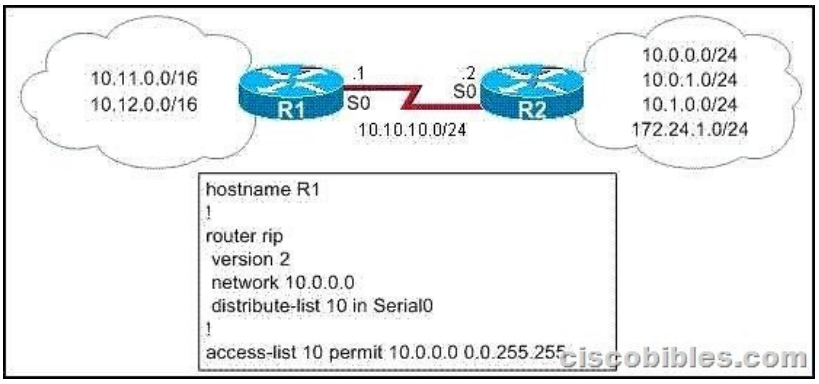



```
R1# show running-config
interface Loopback0
 ip address 64.101.64.1 255.255.255.0
!
interface Tunnel0
 ipv6 unnumbered Ethernet0/1
 tunnel source Loopback0
 tunnel mode ipv6ip 6to4
!
interface Ethernet0/0
 ip address 198.135.1.1 255.255.255.0
!
interface Ethernet0/1
 ipv6 address 2002:4065:4001:1::/64 eui-64
!
ipv6 route 2002::/16 Tunnel0
```

```
R2# show running-config
interface Loopback0
 ip address 64.101.65.1 255.255.255.0
!
interface Tunnel0
 ipv6 unnumbered Ethernet0/1
 tunnel source Loopback0
 tunnel mode ipv6ip 6to4
!
interface Ethernet0/0
 ip address 198.135.0.1 255.255.255.0
!
interface Ethernet0/1
 ipv6 address 2002:4065:4101:1::/64 eui-64
!
ipv6 route 2002::/16 Tunnel0
```


A.The least significant 32 bits in the address referenced by the ipv6 route 2002::/16 Tunnel0 command will correspond to the interface E0/0 IPv4 address. B.The least significant 32 bits in the address referenced by the ipv6 route 2002::/16 Tunnel0 command will correspond to the IPv4 address assigned to the tunnel source. C.The configuration is invalid since the tunnel source command must be configured with an IPv6 address. D.This is actually a configuration example of an IPv4-compatible tunnel and not a 6to4 tunnel. E.This is actually a configuration example of an ISATAP overlay tunnel and not a 6to4 tunnel. **Correct Answers: B Explanation:** 6to4 tunnels use IPv6 addresses that concatenate 2002::/16 with the 32-bit IPv4 address of the edge router, creating a

48-bit prefix. The tunnel interface on R1 has an IPv6 prefix of 2002:4065:4001:1::/64, where 4065:4001 is the hexadecimal equivalent of 64.101.64.1, the IPv4 address of its interface in the IPv4 network. The tunnel interface on R2 has an IPv6 prefix of 2002:4065:4101:1::/64, where 4065:4101 is the hexadecimal equivalent of 64.101.65.1, the IPv4 address of its interface in the IPv4 network. When R1 receives a packet with IPv6 destination address of 2002:4065:4101:1:: (from the left IPv6 network, for example) R1 will: * Take the IPv6 destination address of that packet (2002:4065:4101:1::) and convert it into an IPv4 address. In this case, the IPv4 address is 40.65.41.01 in hexa, which is 64.101.65.1 in decimal format. * R1 encapsulates the IPv6 packet in an IPv4 packet with a destination address of 64.101.65.1; the packet is routed normally through the IPv4 network to R2 * R2 receives the IPv4 packet, decapsulates and routes it normally to its final IPv6 destination. 7: Refer to the exhibit. What is the effect of the distribute-list command in the R1 configuration?



A.R1 will filter only the 172.24.1.0/24 route from the R2 RIP updates. B.R1 will permit only the 10.0.0.0/24 route in the R2 RIP updates. C.R1 will filter the 10.1.0.0/24 and the 172.24.1.0/24 routes from the R2 RIP updates. D.R1 will not filter any routes because there is no exact prefix match. **Correct Answers: C Explanation:** The command ?distribute-list 10 in Serial0? will create an incoming distribute list for interface serial 0 and refers to access list 10. So it will permit routing updates from 10.0.x.x network while other entries (in this case the 10.1.0.0/24 and 172.24.1.0/24 networks) will be filtered out from the routing update received on interface S0. 8. What are three IPv6 transition mechanisms? (Choose three) A.6to4 tunneling B.VPN tunneling C.GRE tunneling D.ISATAP tunneling E.PPP tunneling F.Teredo tunneling Answer: A D F **Explanation:** Below is a summary of IPv6 transition technologies: 6 to 4 tunneling: This mechanism allows IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup. The main advantage of this technology is that it requires no end-node reconfiguration and minimal router configuration but it is not intended as a permanent solution. ISATAP tunneling (Intra-Site Automatic Tunnel Addressing Protocol): is a mechanism for transmitting IPv6 packets over IPv4 network. The word ?automatic? means that once an ISATAP server/router has been set up, only the clients must be configured to connect to it. Teredo tunneling: This mechanism tunnels IPv6 datagrams within IPv4 UDP datagrams, allowing private IPv4 address and IPv4 NAT traversal to be used. In fact, GRE tunneling is also a IPv6 transition mechanism but is not mentioned in BSCI so we shouldn't choose it (there are 4 types of IPv6 transition mechanisms mentioned in BSCI; they are: manual, 6-to-4, Teredo and ISATAP).