CCNP ENARSI v8 Final Exam Answers Full – Advanced Routing

itexamanswers.net/ccnp-enarsi-v8-final-exam-answers-full-advanced-routing.html

April 15, 2021

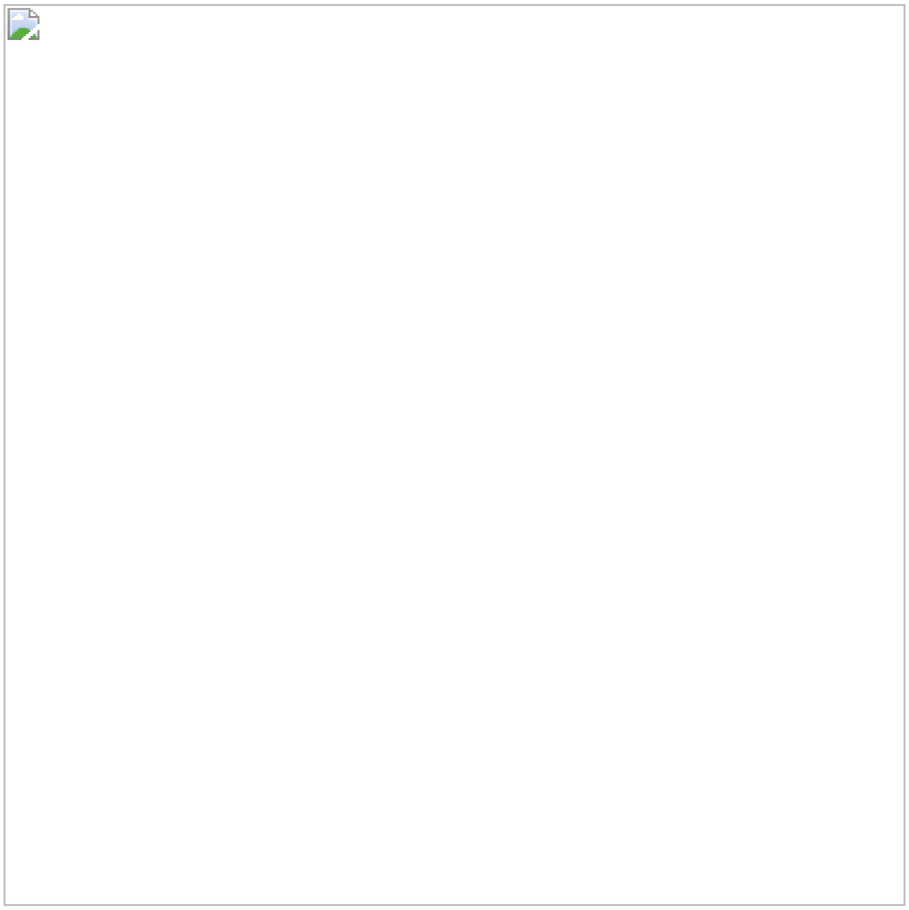
How to find: Press **“Ctrl + F”** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

Note: Some questions have no answers yet

CCNP Enterprise: Advanced Routing (Version 8.0) – CCNP ENARSI 8 Final Exam

1. Refer to the exhibit. A network engineer has performed a partial configuration to prevent routes from being reinjected. What is the next configuration that should be issued?

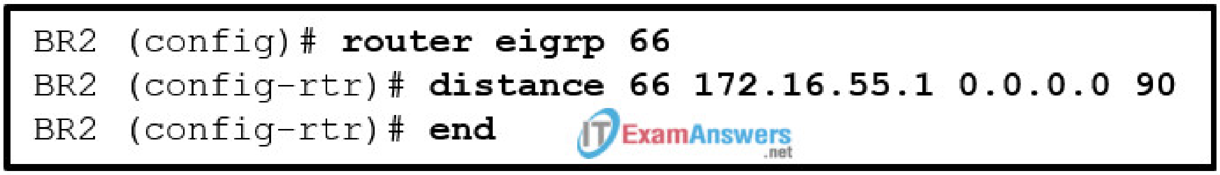


- An access list with a deny statement must be created and used with redistribution.
- **A distribute list with a deny statement must be created and used with redistribution.**
- A route map with a deny statement must be created and used with redistribution.
- A prefix list with a deny statement must be created and used with redistribution.

2. In which two situations is a metric not required for performing redistribution into the EIGRP routing process? (Choose two.)

- when redistributing routes from OSPF
- when redistributing routes from RIP
- **when redistributing static routes**
- when redistributing routes from BGP
- **when redistributing routes from another EIGRP autonomous system**

3. Refer to the exhibit. A network engineer has issued the commands shown on a boundary router. What are two results of the network engineer issuing this command? (Choose two.)



```
BR2 (config)# router eigrp 66
BR2 (config-rtr)# distance 66 172.16.55.1 0.0.0.0 90
BR2 (config-rtr)# end
```

- The internal administrative distance for EIGRP AS 66 has been changed to 66.
- The internal administrative distance has changed to 66 and the external administrative distance has changed to 90 for routes sourced from the router with IP 172.16.55.1.
- **The router has created the EIGRP autonomous system of 66.**
- The network 172.16.55.0 has a modified internal metric of 66.
- **The internal administrative distance has been changed to 66 for routes sourced from the router with IP 172.16.55.1 and matching ACL 90.**

Explanation: The EIGRP command **distance 66 172.16.55.1 0.0.0.0 90** changes the AD to 66 for all EIGRP routes learned from neighbor 172.16.55.1 that match the specific network prefix of ACL 90.

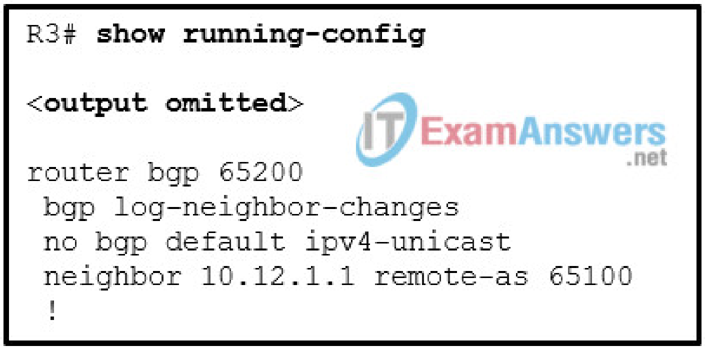
4. What type of BGP message precedes the successful formation of a BGP peering session?

- keepalive
- established
- withdraw
- **open**
- update

Explanation: A BGP open message is used to establish a BGP adjacency. Both peer sides negotiate session capabilities before BGP peering is established.

5. Refer to the exhibit. A network administrator is configuring BGP on a router. Which configuration step is needed in order to establish the BGP session with the neighbor router?

- Configure the keepalive timer.
- **Initialize and activate the address family.**
- Advertise the networks attached to the router.
- Restart the BGP process.



```
R3# show running-config

<output omitted>

router bgp 65200
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
 neighbor 10.12.1.1 remote-as 65100
 !
```

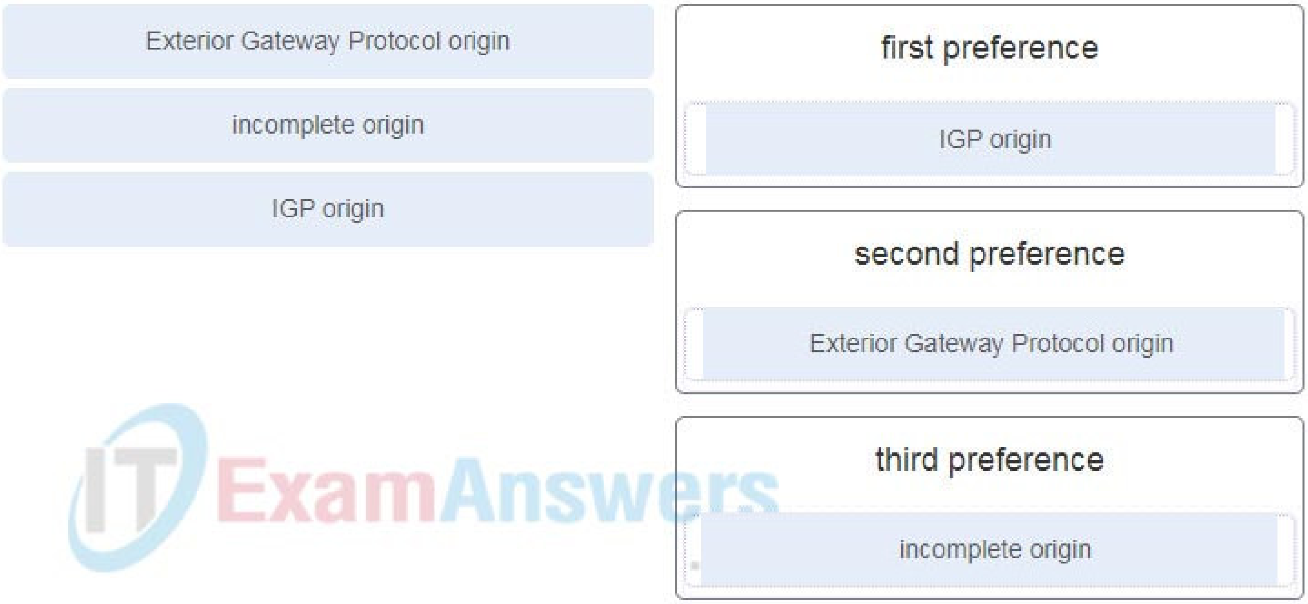
Explanation: For a BGP session to initiate, one address family for a neighbor must be activated. On Cisco routers the IPv4 address family is activated by default; however, it may cause confusion when working with other address families. The BGP router configuration command no bgp default ip4-unicast disables the automatic activation of the IPv4 AFI.

6. Which two statements describe the BGP weight attribute? (Choose two.)

- It is advertised to neighbor routers.
- It correlates to the AS hop count.
- It is an 8-bit value.
- **It is the first step in selecting the BGP best path.**
- **It is a Cisco-defined attribute.**

Explanation: BGP weight is a Cisco-defined attribute and the first step in selecting the BGP best path. Weight is a 16-bit value (0 through 65,535) assigned locally on the router; it is not advertised to other routers

7. Match the preference, that is used by the BGP origin attribute in best path calculation, to the order.



Exterior Gateway Protocol origin

incomplete origin

IGP origin

first preference

IGP origin

second preference

Exterior Gateway Protocol origin

third preference

incomplete origin

8. A network administrator is configuring BGP multipathing for paths learned from iBGP advertisement. What is a condition for additional paths to be considered equal to the best path?

- The AIGP attribute must match.
- The neighbor IP address must match.
- The originated attribute must match.
- **The IGP cost must match for IBGP and EBGP.**

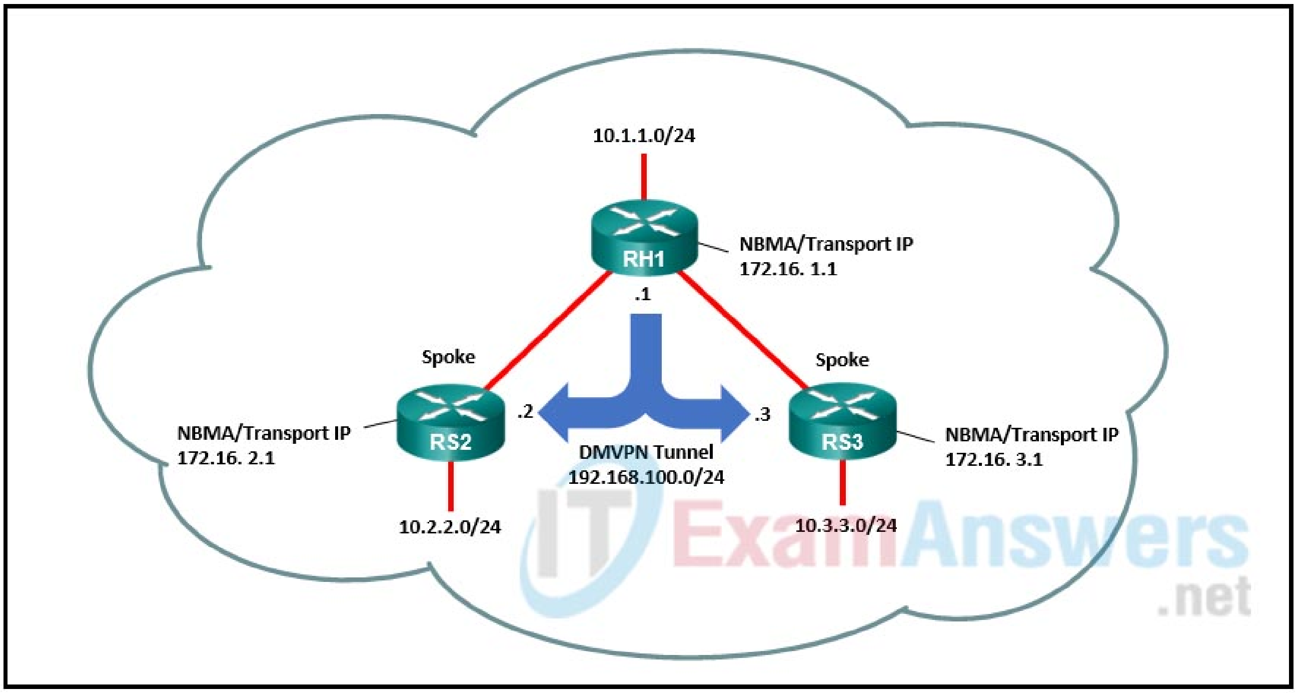
Explanation: When you configure BGP multipathing, the additional paths need to match the following best-path BGP path attributes:
– Weight
– Local preference
– AS_Path length
– AS_Path content (although confederations can contain a different AS_CONFED_SEQ path)
– Origin
– MED
– Advertisement method (iBGP or eBGP) (If the prefix is learned from an iBGP advertisement, the IGP cost must match for iBGP and eBGP to be considered equal.)

9. A network administrator is troubleshooting an issue with a DMVPN tunnel. From the output of the show dmvpn command, the administrator notes that the tunnel is in the IPsec state. What problem does this state indicate?

- The line protocol of the DMVPN tunnel is down.
- The DMVPN spoke router has not registered.
- **IPsec tunnels have not established IKE sessions.**
- IPsec security associations are not established.

Explanation: The command **show dmvpn [detail]** provides the tunnel interface, tunnel role, tunnel state, and tunnel peers with uptime. When the DMVPN tunnel interfaceis administratively shut down, there are no entries associated to that tunnel interface. The tunnel states are, in order of establishment:
– INTF: The line protocol of the DMVPN tunnel is down.
– IKE: DMVPN tunnels configured with IPsec have not yet successfully established an Internet key exchange (IKE) session.
– IPsec: An IKE session is established but an IPsec security association (SA) has not yet been established.
– NHRP: The DMVPN spoke router has not yet successfully registered.
– Up: The DMVPN spoke router has registered with the DMVPN hub and received an ACK (positive registration reply) from the hub.

10. Refer to the exhibit. A network administrator is configuring Phase 1 DMVPN. The hub router RH1 and the spoke router RS2 are already configured and the administrator is finalizing configurations on spoke router RS3 by mapping the NHRP and NHS addresses for the DMVPN hub. Which configuration should the administrator use for the ip nhrp map command?



- **ip nhrp map 192.168.100.1 172.16.1.1**
- ip nhrp map 192.168.100.1 172.16.3.1
- ip nhrp map 192.168.100.3 172.16.3.1
- ip nhrp map 192.168.100.3 172.16.1.1

11. Which NHRP message type notifies routers of routes used by NHRP that are no longer available?

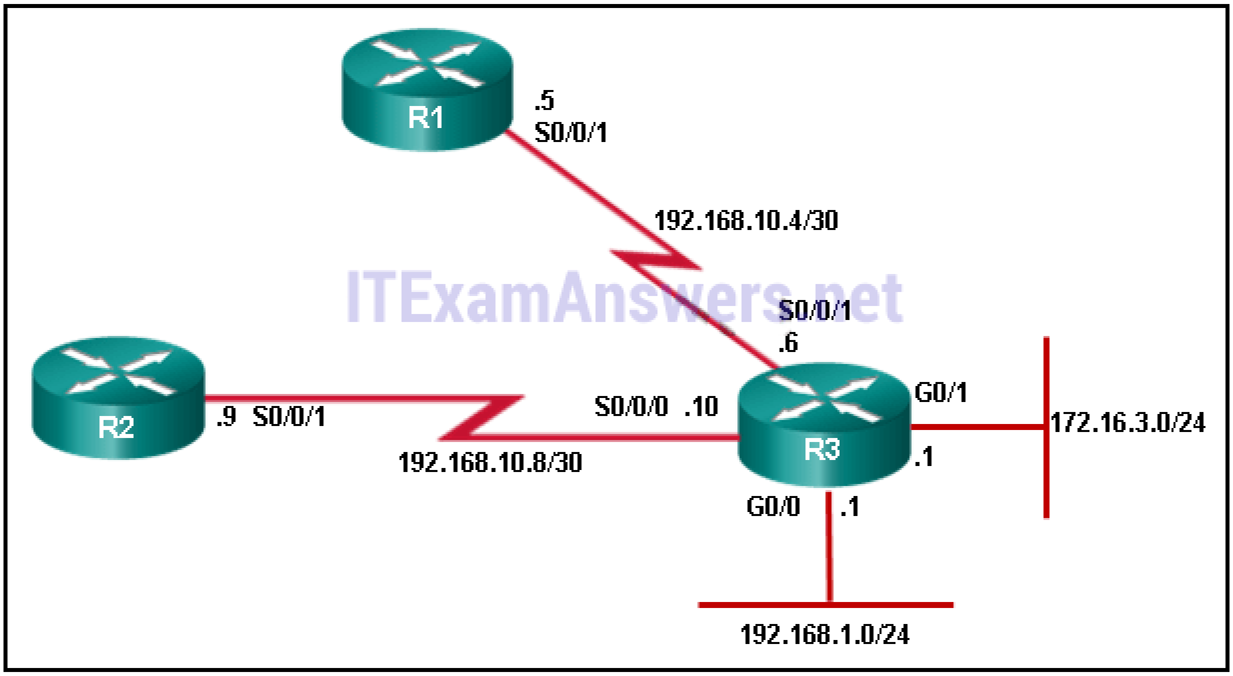
- **purge**
- registration
- redirect
- resolution

Explanation: Purge messages are sent to remove a cached NHRP entry. Purge messages notify routers of the loss of a route used by NHRP. Purges are typically sent by an NHS to NHCs (which it answered) to indicate that the mapping for an address/network that it answered is not valid anymore (for example, if the network is unreachable from the original station or has moved). Purge messages take the most direct path (spoke-to-spoke tunnel) if feasible. If a spoke-to-spoke tunnel is not established, purge messages are forwarded via the hub.

12. What information is maintained in the CEF adjacency table?

- MAC address to IPv4 address mappings
- the IP addresses of all neighboring routers
- IP address to interface mappings
- **Layer 2 next hops**

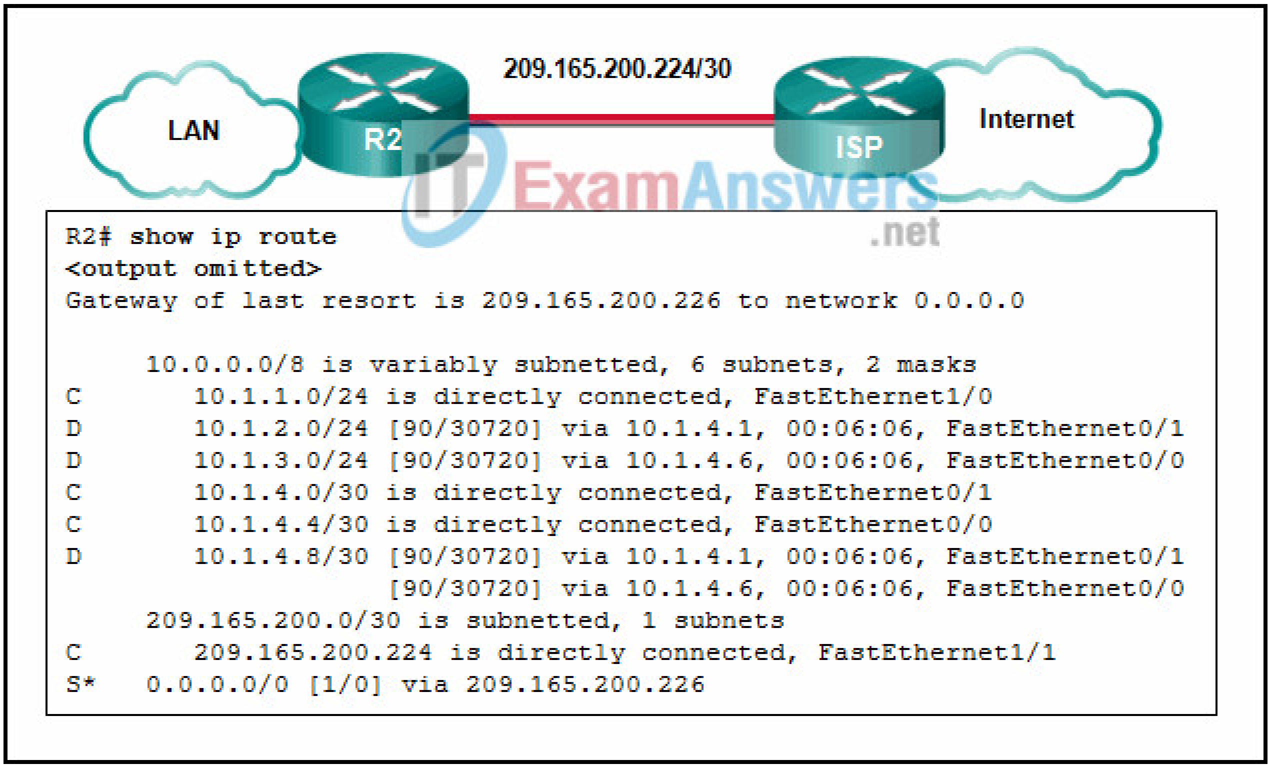
13. Refer to the exhibit. All networks are active in the same EIGRP routing domain. When the auto-summary command is issued on R3, which two summary networks will be calculated on R3? (Choose two.)



- **172.16.0.0/16**
- 172.16.3.0/24
- 192.168.1.0/30
- 192.168.10.0/30
- **192.168.10.0/24**

Explanation: As a result of implementing EIGRP automatic summarization, router R3 uses a classful network addressing scheme to group networks together based on their classful network mask. 192.168.10.4/30 and 192.168.10.8/30 are shortened to 192.168.10.0/24 and 172.16.3.0/24 is summarized to 172.16.0.0/16. 192.168.1.0/24 is already using its classful mask and is not summarized.

14. Refer to the exhibit. Which two routes will be advertised to the router ISP if autosummarization is disabled? (Choose two.)



```
R2# show ip route
<output omitted>
Gateway of last resort is 209.165.200.226 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.1.1.0/24 is directly connected, FastEthernet1/0
D       10.1.2.0/24 [90/30720] via 10.1.4.1, 00:06:06, FastEthernet0/1
D       10.1.3.0/24 [90/30720] via 10.1.4.6, 00:06:06, FastEthernet0/0
C       10.1.4.0/30 is directly connected, FastEthernet0/1
C       10.1.4.4/30 is directly connected, FastEthernet0/0
D       10.1.4.8/30 [90/30720] via 10.1.4.1, 00:06:06, FastEthernet0/1
                    [90/30720] via 10.1.4.6, 00:06:06, FastEthernet0/0
     209.165.200.0/30 is subnetted, 1 subnets
C       209.165.200.224 is directly connected, FastEthernet1/1
S*   0.0.0.0/0 [1/0] via 209.165.200.226
```

- 10.1.0.0/1
- **10.1.2.0/24**
- 10.1.4.0/24
- 10.1.4.0/28
- **10.1.4.0/30**

Explanation: If the no auto-summary command was issued disabling the autosummarization, all subnetworks will be advertised, without summarization.

15. Which is a characteristic of policy based routing (PBR)?

- Packets originating from a router can be identified through local PBR policies.
- PBR examines packets as they exit a router interface.
- PBR policies are universal for all packets and modify the RIB.
- **Next-hop addresses defined in set statements are automatically placed in the routing table.**

16. Which two statements are true of policy-based routing (PBR) as a path control tool? (Choose two.)

- It can be applied only to link-state routing protocols.
- **It is applied only in the inbound direction.**
- Configured route map entries will have default sequence number increments of 5.
- Packets that do not match any match statements will be dropped.

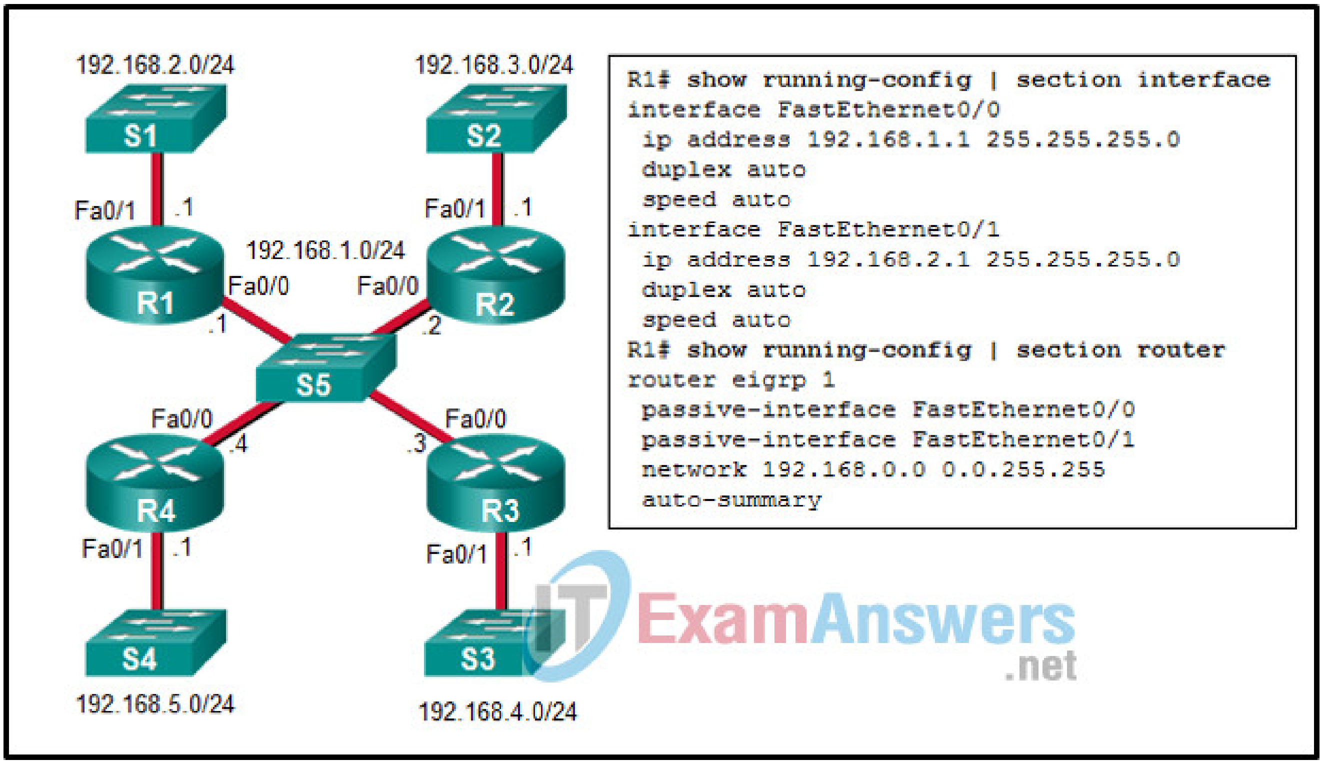
- **It provides a mechanism to specify one or more next hops for packets that match criteria.**

17. A network administrator is writing a standard ACL that will deny any traffic from the 172.16.0.0/16 network, but permit all other traffic. Which two commands should be used? (Choose two.)

- Router(config)# access-list 95 deny 172.16.0.0 255.255.0.0
- **Router(config)# access-list 95 permit any**
- Router(config)# access-list 95 host 172.16.0.0
- **Router(config)# access-list 95 deny 172.16.0.0 0.0.255.255**
- Router(config)# access-list 95 172.16.0.0 255.255.255.255
- Router(config)# access-list 95 deny any

Explanation: To deny traffic from the 172.16.0.0/16 network, the **access-list 95 deny 172.16.0.0 0.0.255.255** command is used. To permit all other traffic, the **access-list 95 permit any** statement is added.

18. Refer to the exhibit. Considering that R2, R3, and R4 are correctly configured, why did R1 not establish an adjacency with R2, R3, and R4?

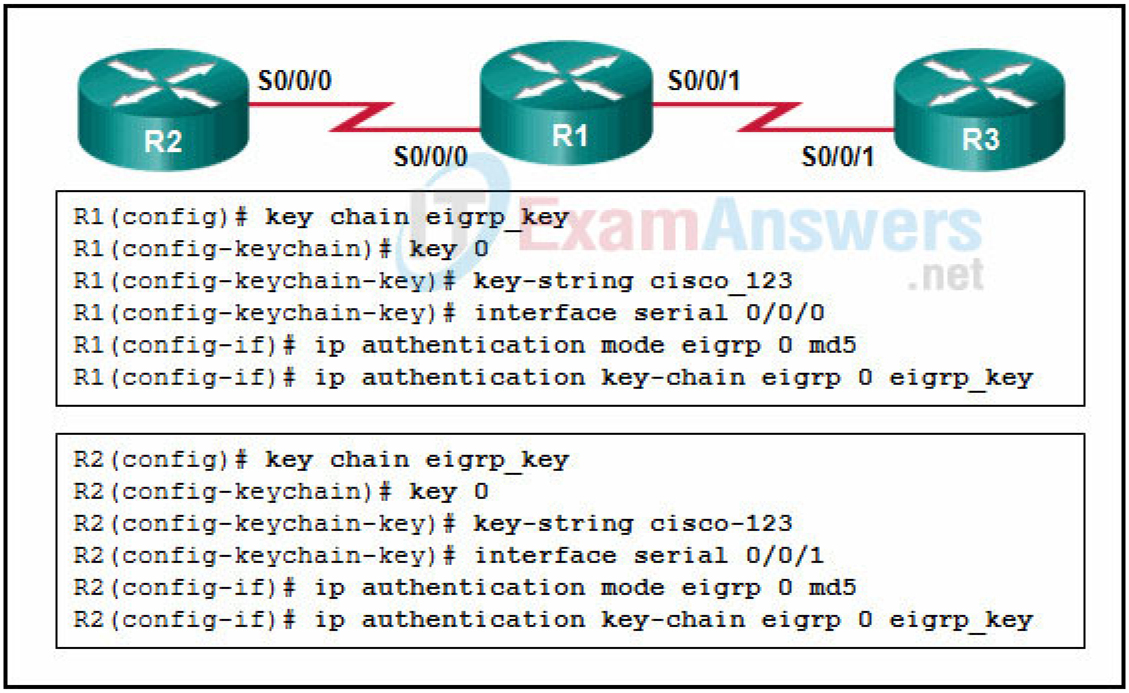


```
R1# show running-config | section interface
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
interface FastEthernet0/1
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
R1# show running-config | section router
router eigrp 1
 passive-interface FastEthernet0/0
 passive-interface FastEthernet0/1
 network 192.168.0.0 0.0.255.255
 auto-summary
```

- because the automatic summarization is enabled on R1
- because the IPv4 address on Fa0/0 interface of R1 is incorrect
- **because the Fa0/0 interface of R1 is declared as passive for EIGRP**
- because there is no network command for the network 192.168.1.0/24 on R1

Explanation: The missing routes are the result of there not being an EIGRP adjacency between R1 and R2, R3, and R4.To establish adjacency, a router must send and receive hello packets over an interface to and from its neighbors. The interface Fa0/ of the router R1 is declared as passive, so R1 will not send hello packets over its interface Fa0/0.

19. Refer to the exhibit. Routers R1 and R2 were configured with EIGRP message authentication, but the routers cannot exchange EIGRP messages. Which two problems are causing the EIGRP authentication failure between R1 and R2 in this configuration? (Choose two.)

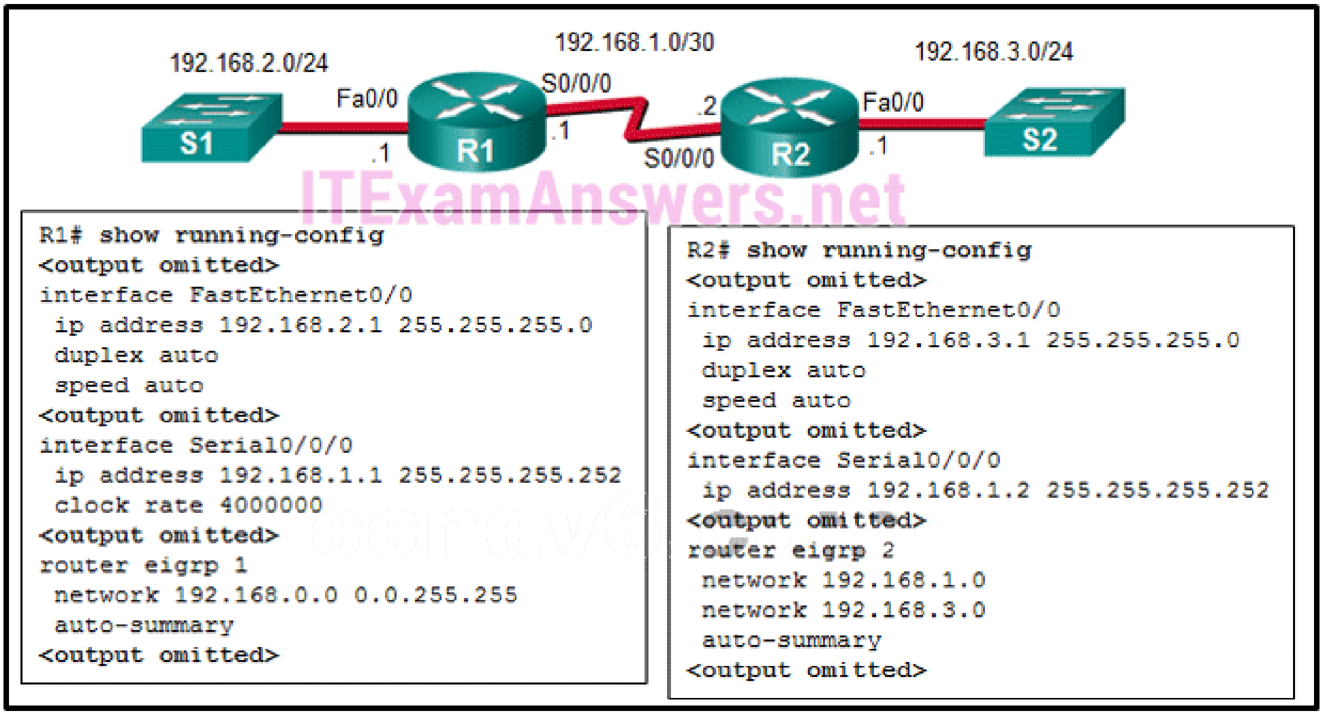


```
R1(config)# key chain eigrp_key
R1(config-keychain)# key 0
R1(config-keychain-key)# key-string cisco_123
R1(config-keychain-key)# interface serial 0/0/0
R1(config-if)# ip authentication mode eigrp 0 md5
R1(config-if)# ip authentication key-chain eigrp 0 eigrp_key
```

```
R2(config)# key chain eigrp_key
R2(config-keychain)# key 0
R2(config-keychain-key)# key-string cisco-123
R2(config-keychain-key)# interface serial 0/0/1
R2(config-if)# ip authentication mode eigrp 0 md5
R2(config-if)# ip authentication key-chain eigrp 0 eigrp_key
```

- The key ID is invalid, because its value has to be in the range from 1 to 2147483647.
- **The EIGRP message authentication is being configured on the wrong interface on R2.**
- The key chain name must be in upper case.
- **The routers have a different value for the key-string.**
- **At least two keys had to be created for each key chain.**

20. Refer to the exhibit. Why did R1 and R2 not establish an adjacency?



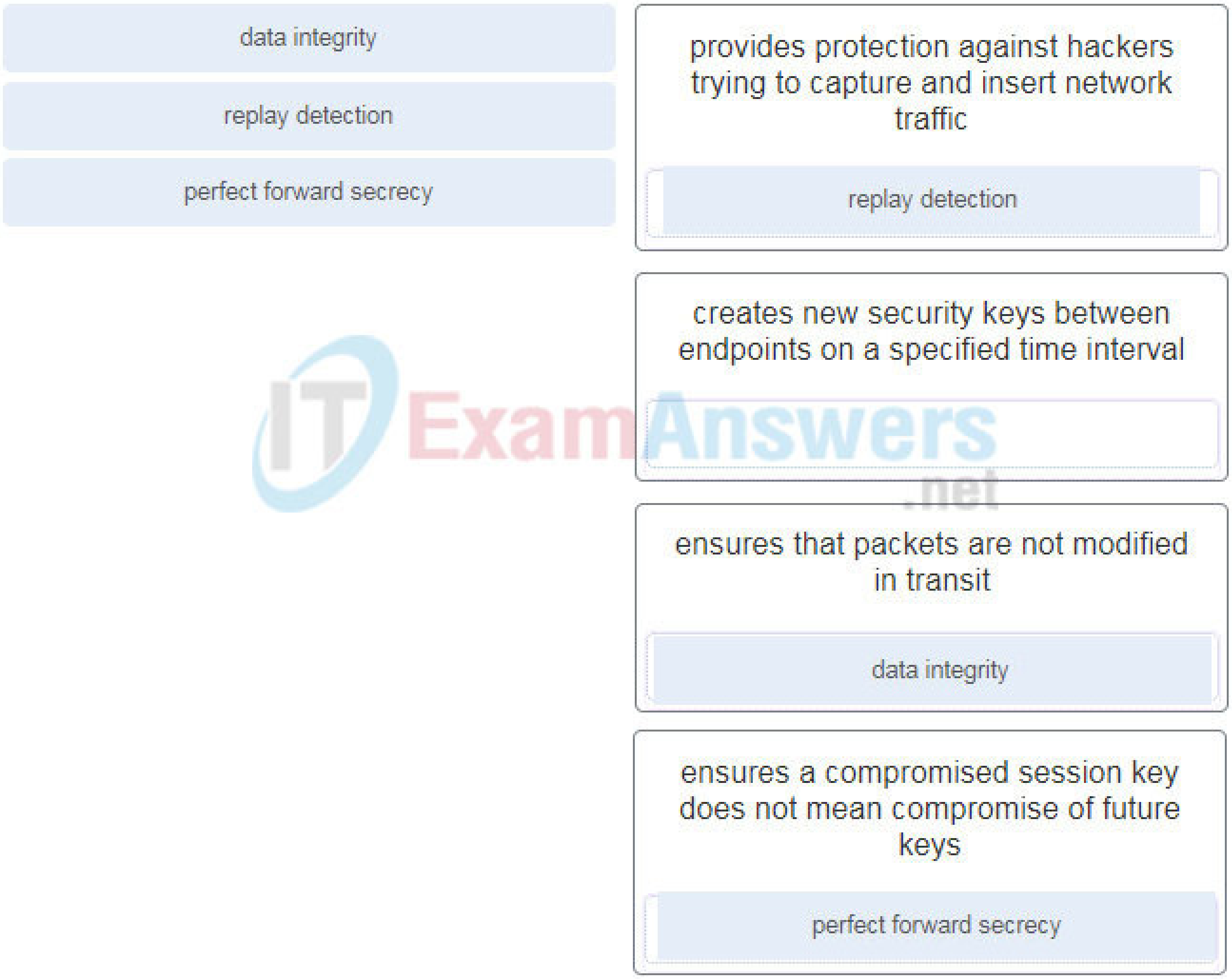
```
R1# show running-config
<output omitted>
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
<output omitted>
interface Serial0/0/0
 ip address 192.168.1.1 255.255.255.252
 clock rate 4000000
<output omitted>
router eigrp 1
 network 192.168.0.0 0.0.255.255
 auto-summary
<output omitted>
```

```
R2# show running-config
<output omitted>
interface FastEthernet0/0
 ip address 192.168.3.1 255.255.255.0
 duplex auto
 speed auto
<output omitted>
interface Serial0/0/0
 ip address 192.168.1.2 255.255.255.252
<output omitted>
router eigrp 2
 network 192.168.1.0
 network 192.168.3.0
 auto-summary
<output omitted>
```

- The IPv4 address of Fa0/0 interface of R1 has a wrong IP address.
- **The AS number does not match on R1 and R2.**
- The automatic summarization is enabled on R1 and R2.
- There is no network command for the network 192.168.1.0/24 on R1.

Explanation: To establish adjacency, both routers must be configured with the same AS number. The network 192.168.0.0 .0.0.255.255 command issued on R1 includes all networks from 192.168.0.0 to 192.168.255.255. Therefore, the network 192.168.1.0/24 is also included.

21. Match the IPsec function with its description. (Not all options are used.)



data integrity

replay detection

perfect forward secrecy

provides protection against hackers trying to capture and insert network traffic

replay detection

creates new security keys between endpoints on a specified time interval

ensures that packets are not modified in transit

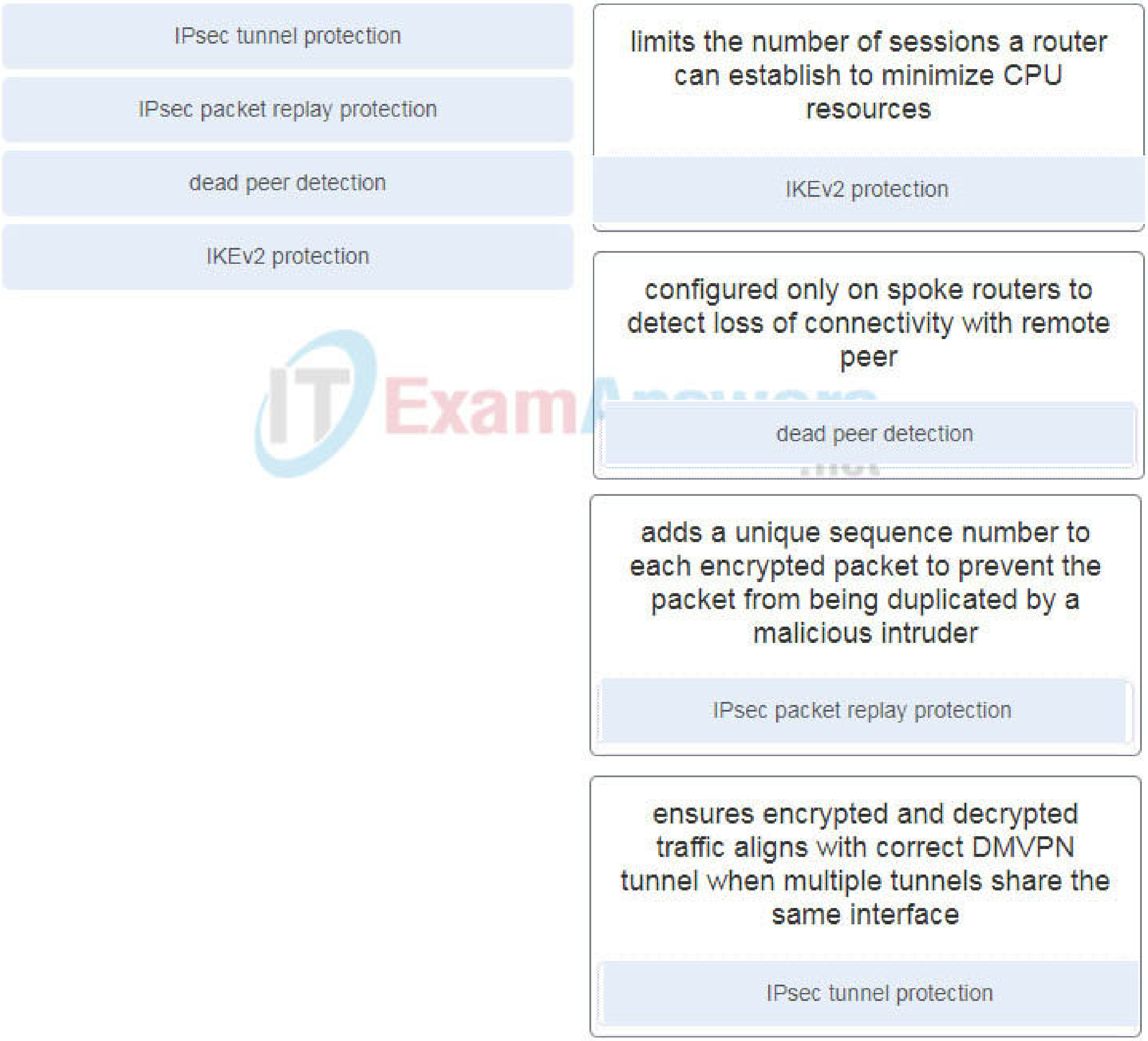
data integrity

ensures a compromised session key does not mean compromise of future keys

perfect forward secrecy

Explanation: – Data integrity: Hashing algorithms ensure that packets are not modified in transit.
– Replay detection: This provides protection against hackers trying to capture and insert network traffic.
– Perfect forward secrecy: Each session key isderived independently of the previous key. A compromise of one key does not compromise future keys.

22. Match the IPsec function with the description.



IPsec tunnel protection

IPsec packet replay protection

dead peer detection

IKEv2 protection

limits the number of sessions a router can establish to minimize CPU resources

IKEv2 protection

configured only on spoke routers to detect loss of connectivity with remote peer

dead peer detection

adds a unique sequence number to each encrypted packet to prevent the packet from being duplicated by a malicious intruder

IPsec packet replay protection

ensures encrypted and decrypted traffic aligns with correct DMVPN tunnel when multiple tunnels share the same interface

IPsec tunnel protection

23. Which three statements describe the IPsec protocol framework? (Choose three.)

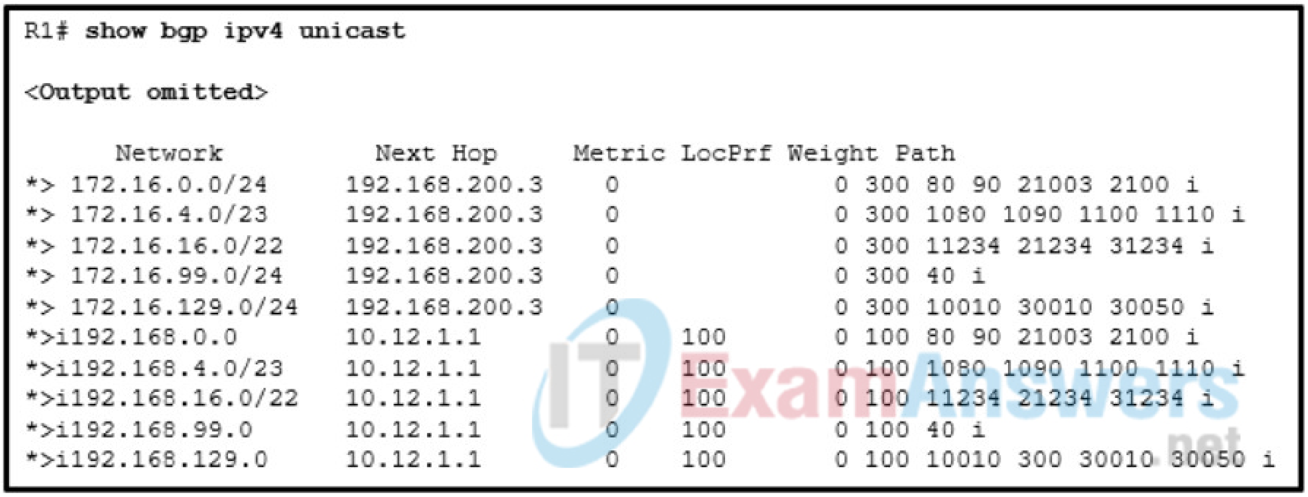
- **AH provides integrity and authentication.**
- **ESP provides encryption, authentication, and integrity.**
- **AH uses IP protocol 51.**
- AH provides encryption and integrity.
- ESP uses UDP protocol 50.
- ESP requires both authentication and encryption.

Explanation: The two primary protocols used with IPsec are AH and ESP. AH is protocol number 51 and provides data authentication and integrity for IP packets that are exchanged between the peers. ESP, which is protocol number 50, performs packet encryption.

24. A network administrator is configuring an ACL to match networks for BGP route filtering. The administrator creates an ACE permit ip 10.0.32.0 0.0.31.0 255.255.255.0 0.0.0.192 . Which network matches the ACE?

- 10.0.32.0/27
- 10.0.66.0/24
- **10.0.62.0/25**
- 10.0.31.0/26

25. Refer to the exhibit. A network administrator is troubleshooting BGP configuration and wants to display only routes that originated in AS 40. Which regular expression should the administrator use in the command show bgp ipv4 unicast regex regex-pattern ?



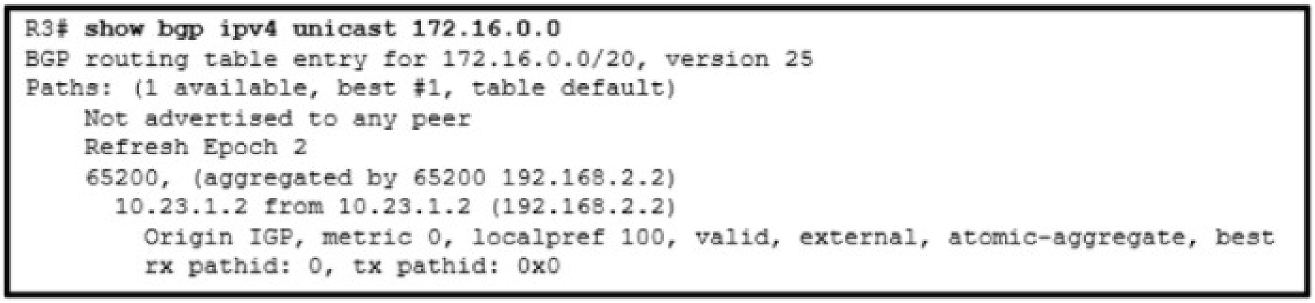
```
R1# show bgp ipv4 unicast

<Output omitted>

      Network          Next Hop      Metric LocPrf Weight Path
*> 172.16.0.0/24     192.168.200.3    0               0 300 80 90 21003 2100 i
*> 172.16.4.0/23     192.168.200.3    0               0 300 1080 1090 1100 1110 i
*> 172.16.16.0/22    192.168.200.3    0               0 300 11234 21234 31234 i
*> 172.16.99.0/24    192.168.200.3    0               0 300 40 i
*> 172.16.129.0/24   192.168.200.3    0               0 300 10010 30010 30050 i
*>i192.168.0.0       10.12.1.1        0     100       0 100 80 90 21003 2100 i
*>i192.168.4.0/23    10.12.1.1        0     100       0 100 1080 1090 1100 1110 i
*>i192.168.16.0/22   10.12.1.1        0     100       0 100 11234 21234 31234 i
*>i192.168.99.0      10.12.1.1        0     100       0 100 40 i
*>i192.168.129.0     10.12.1.1        0     100       0 100 10010 300 30010 30050 i
```

- **show bgp ipv4 unicast regex ^40_**
- show bgp ipv4 unicast regex *40_
- show bgp ipv4 unicast regex _40$????
- show bgp ipv4 unicast regex .40.

Explanation: In troubleshooting BGP, regular expressions (regex) can be used to parse through the large number of available ASNs. Regular expressions are based on query modifiers used to select the appropriate content. The regex pattern 100_ indicates to only include the lines that contain the exact phrase of 100. Some regex query modifiers are as follows:

(underscore) – Matches a space
^ (caret) – Indicates the start of a string
$ (dollar sign) – Indicates the end of a string
. (period) – Matches a single character, including a space

26. Refer to the exhibit. A network administrator issues the `show bgp ipv4 unicast 172.16.0.0` command to check the route information in the BGP table. Which statement describes the characteristic of the advertisement of this route?



```
R3# show bgp ipv4 unicast 172.16.0.0
BGP routing table entry for 172.16.0.0/20, version 25
Paths: (1 available, best #1, table default)
    Not advertised to any peer
    Refresh Epoch 2
    65200, (aggregated by 65200 192.168.2.2)
      10.23.1.2 from 10.23.1.2 (192.168.2.2)
        Origin IGP, metric 0, localpref 100, valid, external, atomic-aggregate, best
        rx pathid: 0, tx pathid: 0x0
```

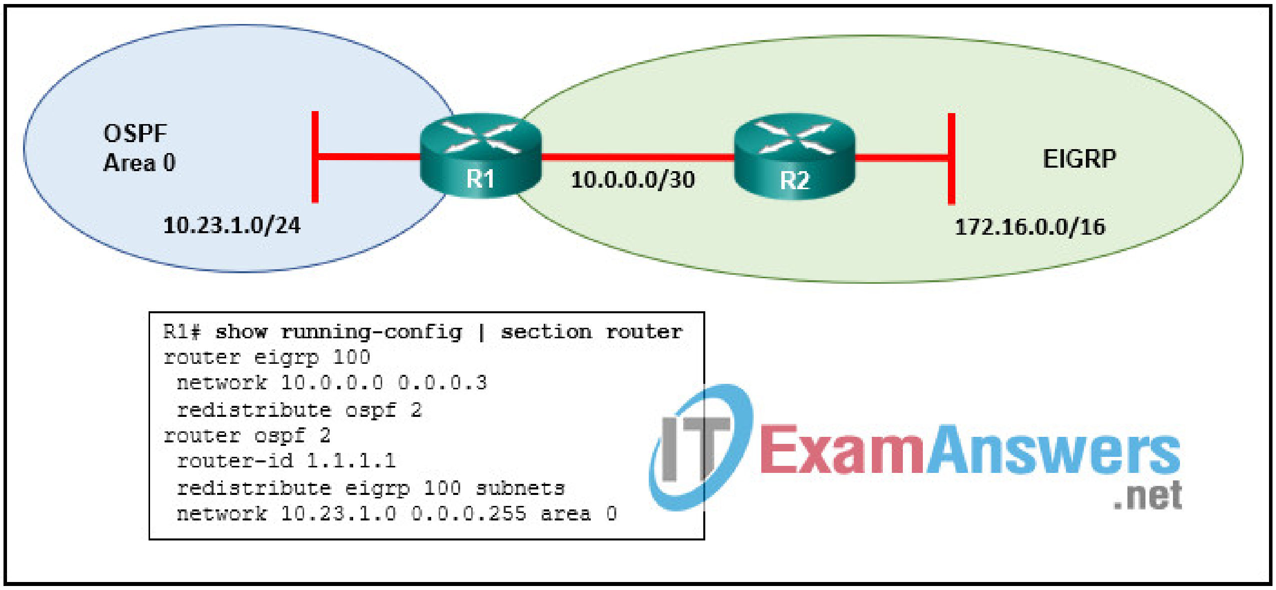
- The route is advertised for networks directly connected to the BGP router 192.168.2.2.
- **The route is advertised with the aggregate-address 172.16.0.0 255.255.240.0 summary-only command.**
- The route is advertised through an IGP.
- The route is advertised through a static route.

27. What OSPF LSA type is used to advertise routes redistributed into an OSPF domain?

- type 3
- type 4
- **type 5**
- type 7

Explanation: OSPF uses six LSA types for IPv4 routing:
– Type 1, router: LSAs that advertise network prefixes within an area
– Type 2, network: LSAs that indicate the routers attached to broadcast segment within an area
– Type 3, summary: LSAs that advertises network prefixes that originate from a different area
– Type 4, ASBR summary: LSA used to locate the ASBR from a different area
– Type 5, AS external: LSA that advertises network prefixes that were redistributed in to OSPF
– Type 7, NSSA external: LSA for external network prefixes that were redistributed in a local NSSA area

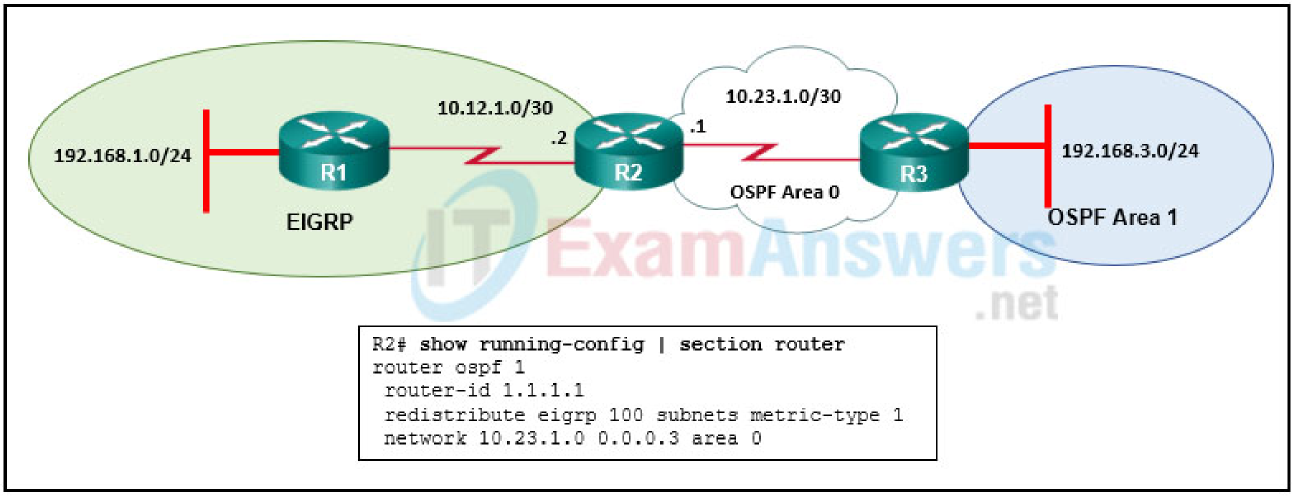
28. Refer to the exhibit. A network administrator has configured two-way redistribution on router R1. What metrics will be used for redistributed routes?



```
R1# show running-config | section router
router eigrp 100
 network 10.0.0.0 0.0.0.3
 redistribute ospf 2
router ospf 2
 router-id 1.1.1.1
 redistribute eigrp 100 subnets
 network 10.23.1.0 0.0.0.255 area 0
```

- EIGRP routes will have a metric of 1 and OSPF routes will have a metric of infinity.
- **EIGRP routes will have a metric of infinity and OSPF routes will have a metric of 20.**
- EIGRP routes will have a metric of 170 and OSPF routes will have a metric of 20.
- EIGRP routes will have a metric of infinity and OSPF routes will have a metric of 1.

29. Refer to the exhibit. Which route will appear in the routing table of R3 as a result of the redistribution configuration issued on R2?



```
R2# show running-config | section router
router ospf 1
 router-id 1.1.1.1
 redistribute eigrp 100 subnets metric-type 1
 network 10.23.1.0 0.0.0.3 area 0
```

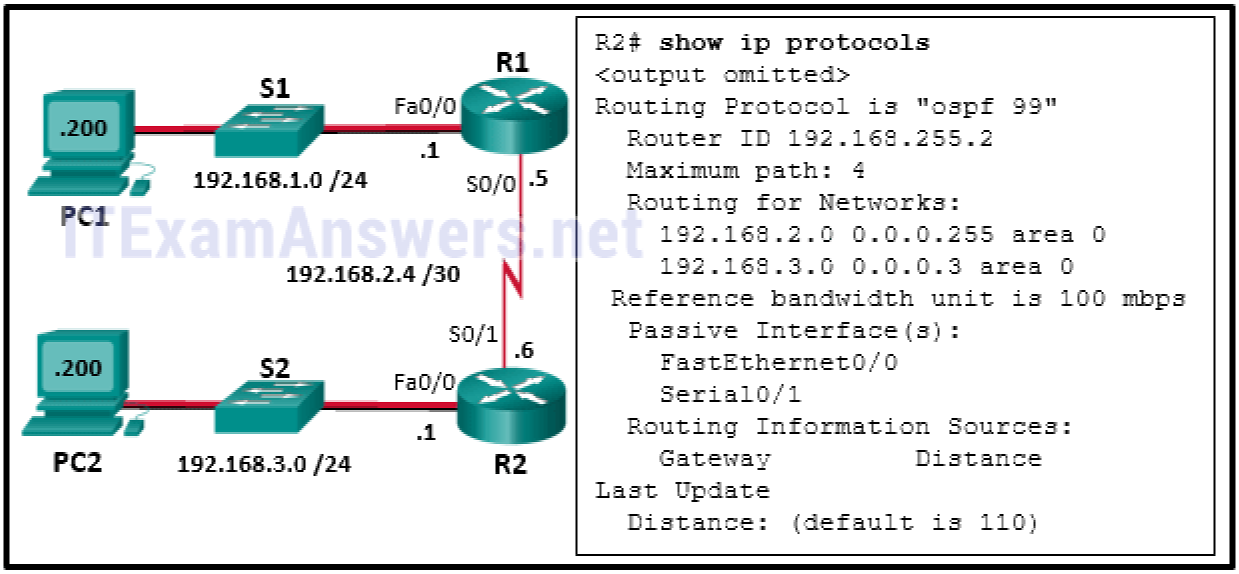
- O E2 192.168.1.0/24 [110/20] via 10.23.1.1, 00:04:42, Serial0/0/1
- O IA 10.23.1.0/30 [110/20] via 10.23.1.1, 00:04:42, Serial0/0/1
- O E1 192.168.1.0/24 [110/86] via 10.23.1.1, 00:04:42, Serial0/0/1
- D EX 10.23.1.0/30 [170/3072] via 10.12.1.2, 00:09:07, Serial0/0/1

Explanation: Route redistribution has been configured on router R2 according to the provided exhibit. EIGRP is now being utilized as the routing protocol. Router R2 will redistribute routes from EIGRP into OSPF based on the configuration that was given to it. R2 has a process number of 11, which is used by OSPF. The network statement notifies OSPF that the 10.23.1.0/30 network is included in the OSPF area 0 and that it belongs to that area. OSPF is instructed to redistribute routes from EIGRP AS 11 into OSPF when the redistribute eigrp 11 command is executed. The cost metric is always used by default. OSPF is instructed to use the external metric type while redistributing routes from EIGRP when the metric-type type-1 command is executed.

OSPF is instructed by the match internal external 1 external 2 command to only redistribute routes that are both internal to EIGRP (routes that have been learned from EIGRP neighbors) and that are external to OSPF. The match internal external 1 external 2 command is used (routes that are not learned from any OSPF neighbors).

The route to 10.23.1.0/30 can now be seen in the routing table on router R3 thanks to the show ip route command. The route is being advertised as being an OSPF route. R2 is required to learn the route, which has an associated cost of 86.

30. Refer to the exhibit. A network administrator has configured OSPFv2 on the two Cisco routers. The routers are unable to form a neighbor adjacency. What should be done to fix the problem on router R2?

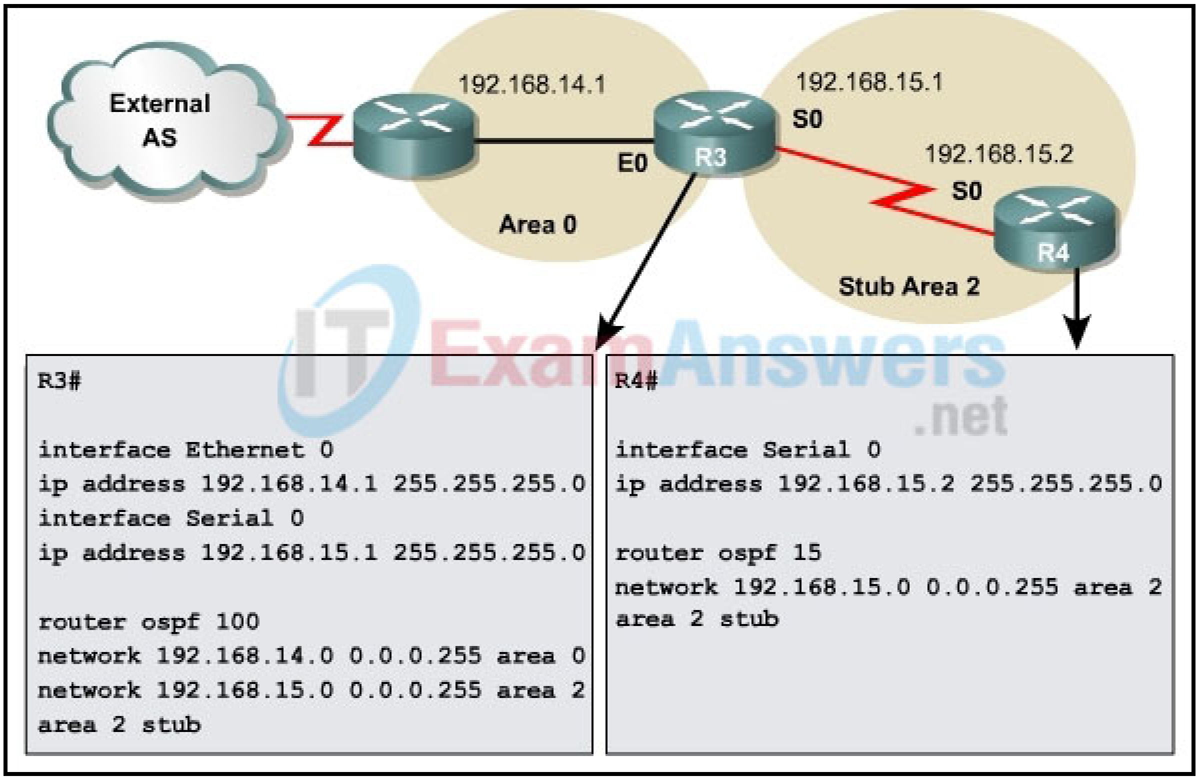


```
R2# show ip protocols
<output omitted>
Routing Protocol is "ospf 99"
  Router ID 192.168.255.2
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.3 area 0
 Reference bandwidth unit is 100 mbps
  Passive Interface(s):
    FastEthernet0/0
    Serial0/1
  Routing Information Sources:
    Gateway         Distance
Last Update
  Distance: (default is 110)
```

- **Implement the command no passive-interface Serial0/1.**
- Implement the command network 192.168.2.6 0.0.0.0 area 0 on router R2.
- Change the router-id of router R2 to 2.2.2.2.
- Implement the command network 192.168.3.1 0.0.0.0 area 0 on router R2.

31. Refer to the exhibit. A network administrator is troubleshooting a recent OSPF stub configuration between R3 and R4. The only routes that should appear on the routing table for R4 are intra-area routes and the default route.

However, interarea routes are also appearing. What must the administrator do to fix this problem?



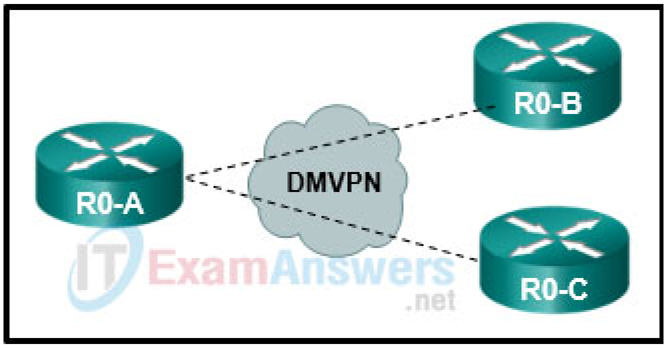
```
R3#

interface Ethernet 0
ip address 192.168.14.1 255.255.255.0
interface Serial 0
ip address 192.168.15.1 255.255.255.0

router ospf 100
network 192.168.14.0 0.0.0.255 area 0
network 192.168.15.0 0.0.0.255 area 2
area 2 stub
```

```
R4#

interface Serial 0
ip address 192.168.15.2 255.255.255.0

router ospf 15
network 192.168.15.0 0.0.0.255 area 2
area 2 stub
```

- Issue the keyword nssa on R3.
- Issue the keyword nssa on R4.
- Issue the keyword stub on R4.
- Issue the keyword no-summary on R4.
- **Issue the keyword no-summary on R3.**
- Issue the keyword stub on R3.

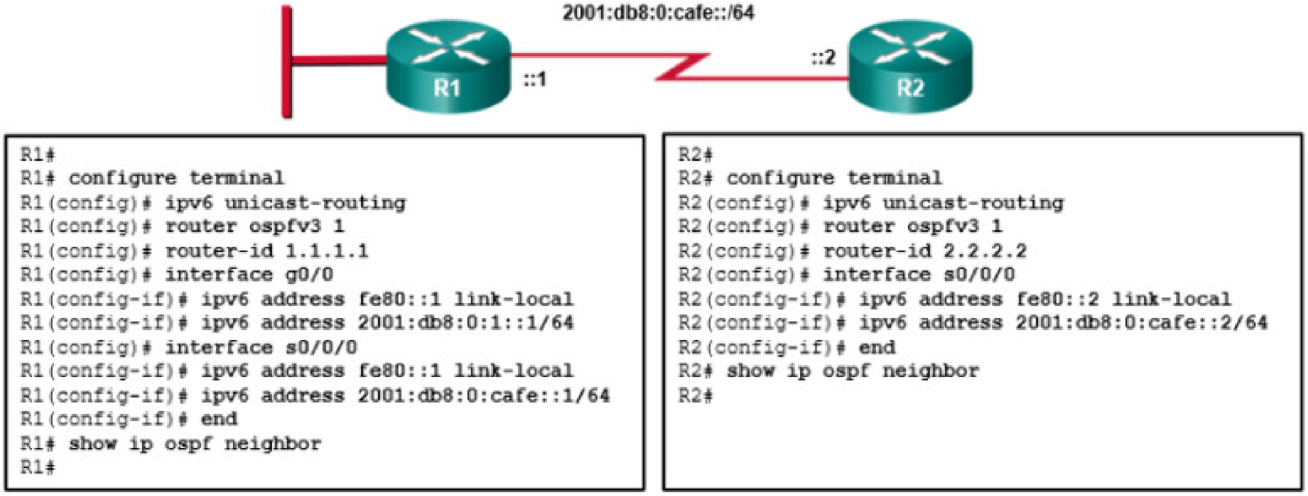
32. Refer to the exhibit. Router R0-A is not learning all of the OSPF routes from the remote sites that connect to router R0-B and R0-C. What are two issues the network engineer should consider? (Choose two.)

- routes not going from the LSDB to the routing table because of ACL
- DR selection
- missing default route(s)
- neighbor adjacency
- SSH misconfiguration



33. Refer to the exhibit. Routers R1 and R2 are configured as shown. However, the `show ipv6 ospf`

`neighbor` command reveals that there are no OSPFv3 neighbors established. What error in the configuration is preventing neighbor relationship from forming between the two routers?



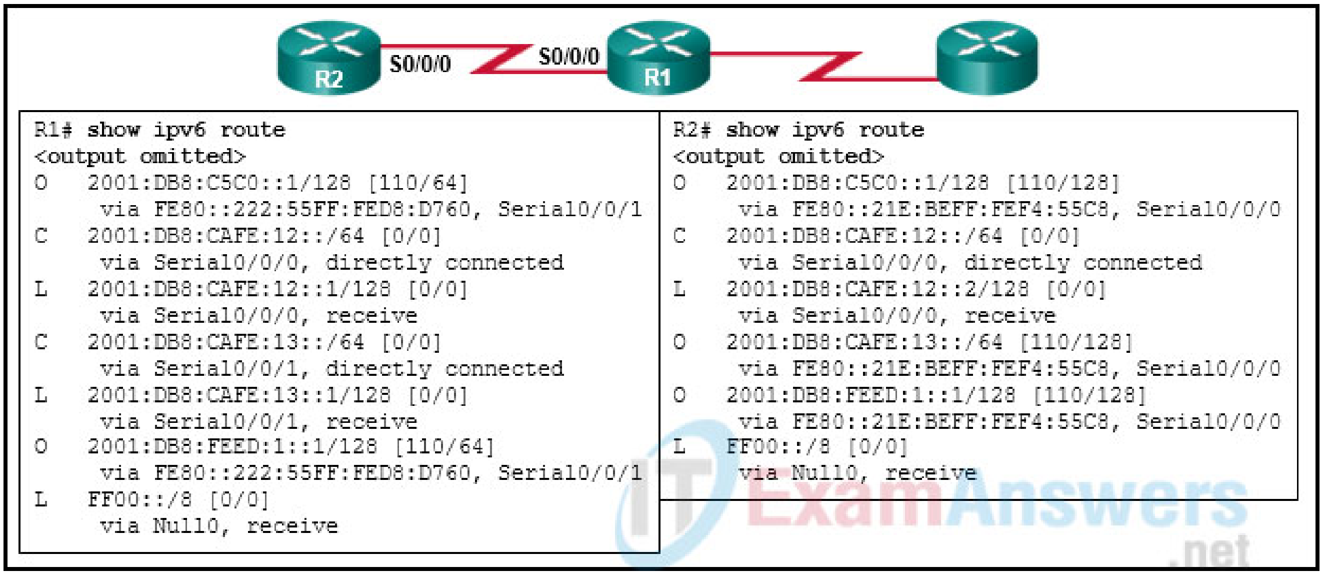
```
R1#
R1# configure terminal
R1(config)# ipv6 unicast-routing
R1(config)# router ospfv3 1
R1(config)# router-id 1.1.1.1
R1(config)# interface g0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:0:1::1/64
R1(config)# interface s0/0/0
R1(config-if)# ipv6 address fe80::1 link-local
R1(config-if)# ipv6 address 2001:db8:0:cafe::1/64
R1(config-if)# end
R1# show ip ospf neighbor
R1#
```

```
R2#
R2# configure terminal
R2(config)# ipv6 unicast-routing
R2(config)# router ospfv3 1
R2(config)# router-id 2.2.2.2
R2(config)# interface s0/0/0
R2(config-if)# ipv6 address fe80::2 link-local
R2(config-if)# ipv6 address 2001:db8:0:cafe::2/64
R2(config-if)# end
R2# show ip ospf neighbor
R2#
```

- OSPFv3 is not enabled on the interfaces.
- The IPv6 routing process is not enabled.
- There is a link-local address conflict between the serial and gigabit interfaces on R1.
- The IPv6 address family is not initialized on either router.

Explanation: The routers are unable to form an OSPFv3 adjacency because OSPFv3 has not been enabled on the interfaces with the `ospfv3 1 ipv6 area 0` command.

34. Refer to the exhibit. An administrator has entered the command default-information originate in OSPFv3 global configuration mode on R1, but R2 is not receiving a default route. What is the problem?



```
R1# show ipv6 route
<output omitted>
O   2001:DB8:C5C0::1/128 [110/64]
     via FE80::222:55FF:FED8:D760, Serial0/0/1
C   2001:DB8:CAFE:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:12::1/128 [0/0]
     via Serial0/0/0, receive
C   2001:DB8:CAFE:13::/64 [0/0]
     via Serial0/0/1, directly connected
L   2001:DB8:CAFE:13::1/128 [0/0]
     via Serial0/0/1, receive
O   2001:DB8:FEED:1::1/128 [110/64]
     via FE80::222:55FF:FED8:D760, Serial0/0/1
L   FF00::/8 [0/0]
     via Null0, receive
```

```
R2# show ipv6 route
<output omitted>
O   2001:DB8:C5C0::1/128 [110/128]
     via FE80::21E:BEFF:FEF4:55C8, Serial0/0/0
C   2001:DB8:CAFE:12::/64 [0/0]
     via Serial0/0/0, directly connected
L   2001:DB8:CAFE:12::2/128 [0/0]
     via Serial0/0/0, receive
O   2001:DB8:CAFE:13::/64 [110/128]
     via FE80::21E:BEFF:FEF4:55C8, Serial0/0/0
O   2001:DB8:FEED:1::1/128 [110/128]
     via FE80::21E:BEFF:FEF4:55C8, Serial0/0/0
L   FF00::/8 [0/0]
     via Null0, receive
```

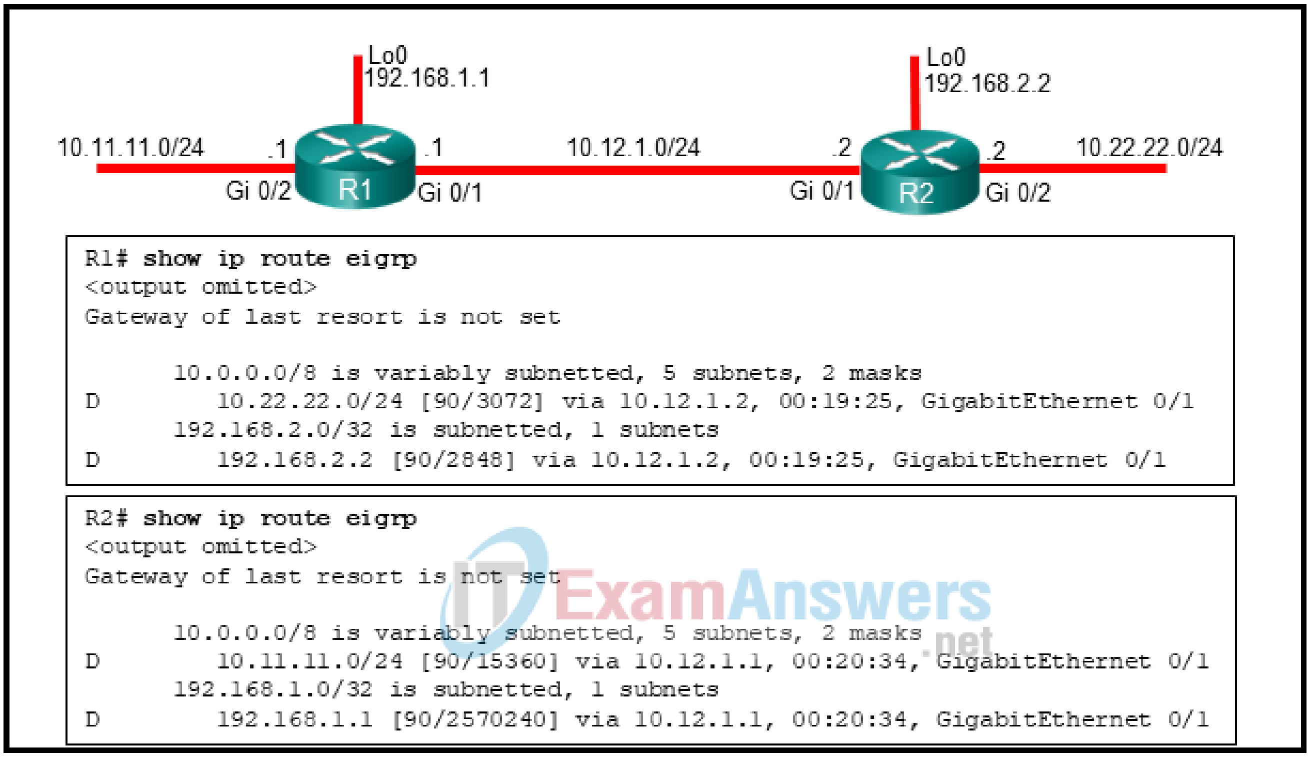
- The default-information originate command is only used for OSPFv2.

- R1 and R2 are on different subnets.
- OSPFv3 is not running on R2.
- **R1 does not have a default route configured.**

35. An administrator is troubleshooting an OSPFv3 network. Router A and router B are configured with IPv6 addressing and basic routing capabilities using OSPFv3. While debugging the routing process, the administrator discovers that the networks that are advertised from router A do not show in the routing table of router B. Why is the routing information not being learned by router B?

- Router A has a stub interface.
- **IPv6 unicast routing is not enabled on Router B.**
- The OSPFv3 timers on both routers were adjusted for fast convergence.
- An IPv6 traffic filter is blocking the networks from entering the interface on router B that is connected.

36. Refer to the exhibit. Routers R1 and R2 enable EIGRP on all of their interfaces. Which two conclusions can the field engineer draw from the outputs of the show ip route eigrp command on each router? (Choose two.)



```
R1# show ip route eigrp
<output omitted>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D        10.22.22.0/24 [90/3072] via 10.12.1.2, 00:19:25, GigabitEthernet 0/1
      192.168.2.0/32 is subnetted, 1 subnets
D        192.168.2.2 [90/2848] via 10.12.1.2, 00:19:25, GigabitEthernet 0/1
```

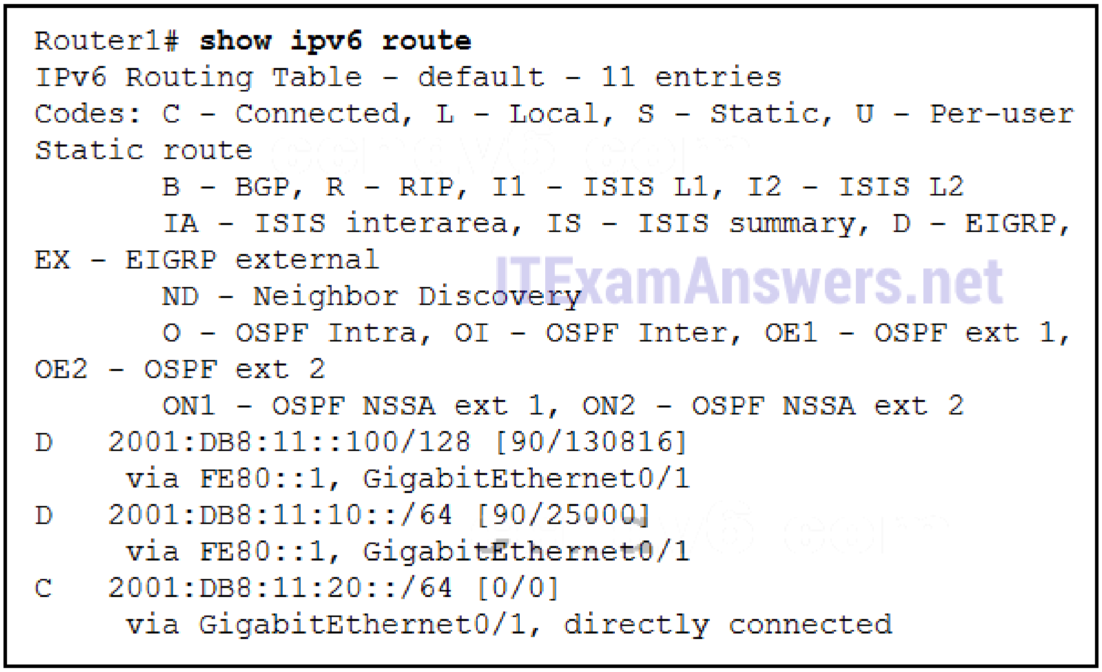
```
R2# show ip route eigrp
<output omitted>
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
D        10.11.11.0/24 [90/15360] via 10.12.1.1, 00:20:34, GigabitEthernet 0/1
      192.168.1.0/32 is subnetted, 1 subnets
D        192.168.1.1 [90/2570240] via 10.12.1.1, 00:20:34, GigabitEthernet 0/1
```

- Both routers are using the same path metric calculation method.
- **The path metric calculation used in R2 addresses the scalability with higher-capacity interfaces.**
- R1 and R2 are using the same K factors to calculate the path metric.

- **An adjacency will be allowed between the routers, as long as all the K factors in both routers are set to default values.**
- The EIGRP configuration mode of R1 uses wide metrics calculation.
- R2 is using EIGRP classic configuration mode.

Explanation: The metrics for R2 routes are different from the metrics from R1 routes. This is because R1 is using EIGRP classic configuration mode that uses classic metrics, and R2 is using EIGRP named mode configuration that uses wide metrics by default. The EIGRP classic metric calculation uses 5 K values (K1 to K5) to calculate the metric, whereas the EIGRP wide metric calculation uses 6 K values (K1 to K6). The two metric styles will allow adjacency between the two routers, as long as K1 through K5 are the same, and K6 is not set. The wide metrics calculation addresses the issues of scalability with higher-capacity interfaces.

37. Refer to the exhibit. An administrator wants EIGRP on Router1 to load balance traffic to network 2001:db8:11:10::/64 across two interfaces. Currently traffic is using only interface GigabitEthernet0/1. A second route, not in the routing table, is available with a metric of 264000. What value is needed in the variance command to make EIGRP put the second route into the routing table?

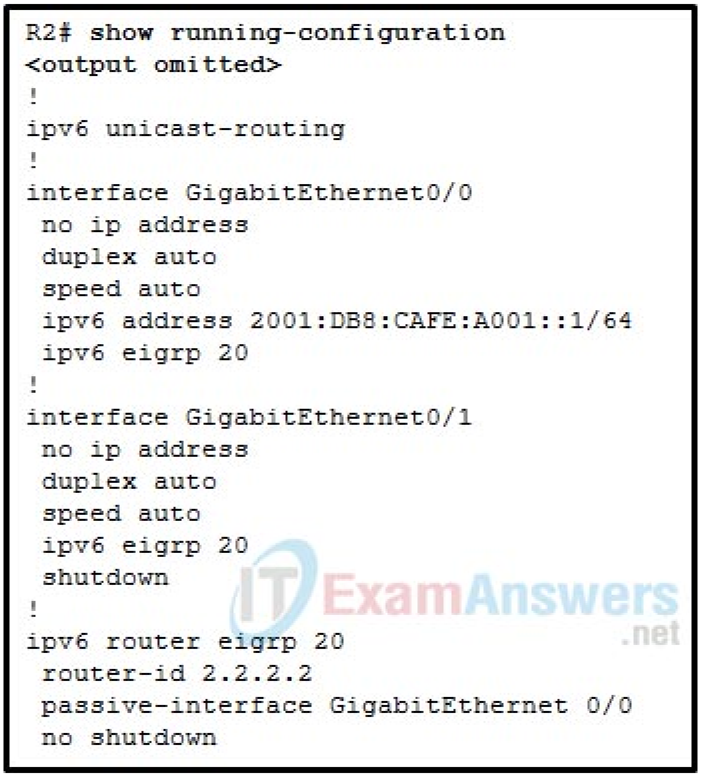


```
Router1# show ipv6 route
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user
Static route
       B - BGP, R - RIP, I1 - ISIS L1, I2 - ISIS L2
       IA - ISIS interarea, IS - ISIS summary, D - EIGRP,
EX - EIGRP external
       ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1,
OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D   2001:DB8:11::100/128 [90/130816]
     via FE80::1, GigabitEthernet0/1
D   2001:DB8:11:10::/64 [90/25000]
     via FE80::1, GigabitEthernet0/1
C   2001:DB8:11:20::/64 [0/0]
     via GigabitEthernet0/1, directly connected
```

- 4
- 10
- 1
- **11**

Explanation: A variance of 11 is needed to load balance across the second route. The metric of the existing successor route is 25000. The metric of the second route is 264000. The first metric needs to be multiplied by 11, which is 275000, in order for the route to be put into the routing table.

38. Refer to the exhibit. Router R2 has recently been configured and connected via interface Gigabit Ethernet 0/0 to router R1. R1 is configured correctly, but fails to establish a neighbor relationship with R2. What is the problem?



```
R2# show running-configuration
<output omitted>
!
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address 2001:DB8:CAFE:A001::1/64
 ipv6 eigrp 20
!
interface GigabitEthernet0/1
 no ip address
 duplex auto
 speed auto
 ipv6 eigrp 20
 shutdown
!
ipv6 router eigrp 20
 router-id 2.2.2.2
 passive-interface GigabitEthernet 0/0
 no shutdown
```

- The EIGRPv6 process has not been activated on interface Gigabit Ethernet 0/0.
- **The passive-interface command is preventing hello packets from being sent.**
- The command ipv6 unicast-routing should be implemented in the router configuration mode.
- The command ipv6 unicast-routing has not been implemented.

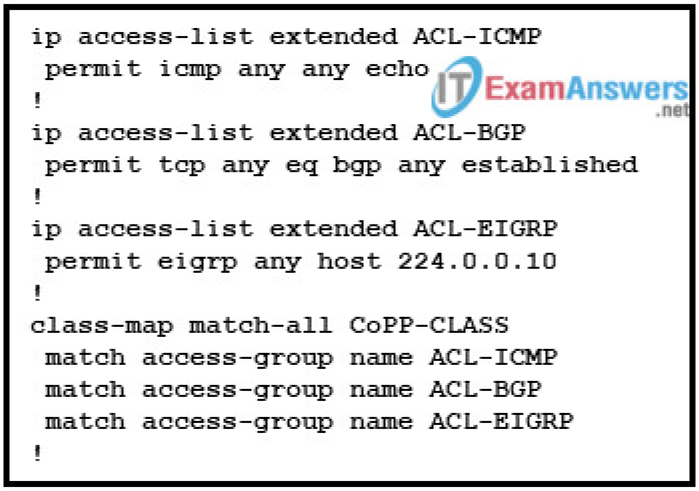
39. An administrator wants to configure EIGRPv6 in an IPv6 network. Which three statements are valid for the configuration of EIGRPv6? (Choose three.)

- Split horizon needs to be enabled on all EIGRPv6 hub routers.
- The network statement must be configured for the EIGRPv6 process.
- **EIGRPv6 has to be directly configured on the interfaces over which it runs.**
- **There is no network statement configuration for EIGRPv6.**
- **When using a passive-interface configuration, EIGRPv6 does not have to be configured for that interface.**
- EIGRPv6 needs to be directly configured on an interface that has been made passive.

40. Refer to the exhibit. A network administrator configured a class map as shown, but the traffic is not being classified as desired. Which conclusion can be drawn from this configuration?

- The traffic would be subject to the implicit default class.
- The ACL-EIGRP is permitting the wrong IP multicast address.

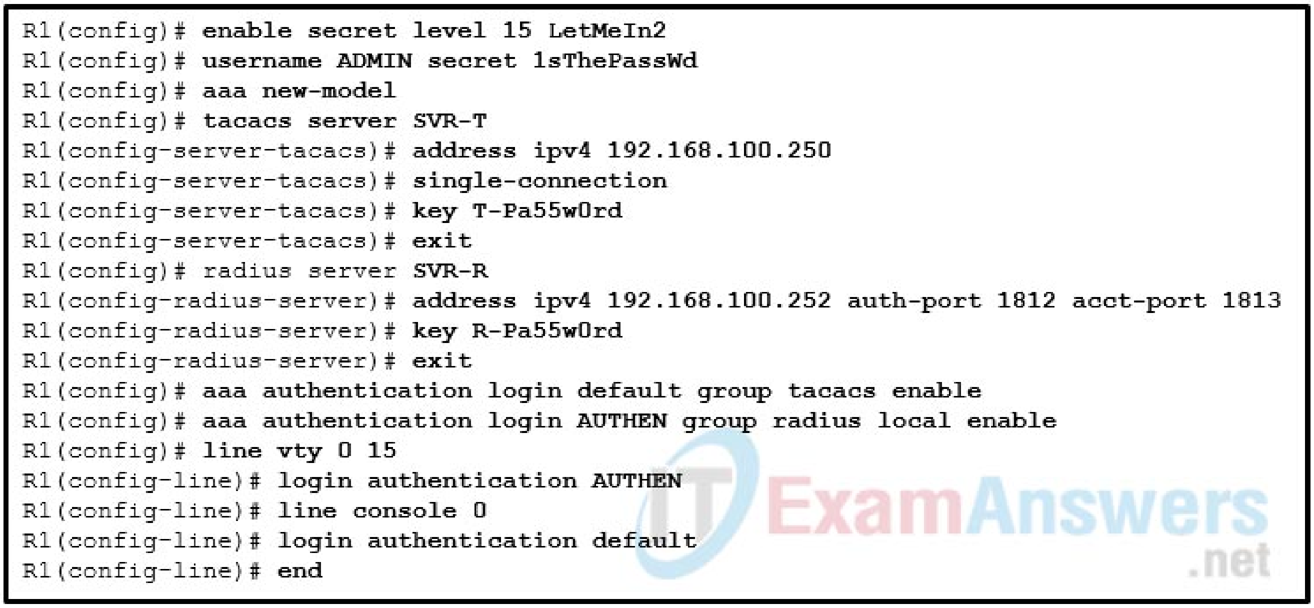
- **The traffic would never match the CoPP-CLASS class map.**
- The ACL-ICMP access-list should be in a separate class map because it is not a routing protocol.



```
ip access-list extended ACL-ICMP
 permit icmp any any echo
!
ip access-list extended ACL-BGP
 permit tcp any eq bgp any established
!
ip access-list extended ACL-EIGRP
 permit eigrp any host 224.0.0.10
!
class-map match-all CoPP-CLASS
 match access-group name ACL-ICMP
 match access-group name ACL-BGP
 match access-group name ACL-EIGRP
!
```

Explanation: A class map may contain one of two instructions: **match-any** or **match-all** . If you have multiple **match** commands in a single class map and **match-any** is used, it means the traffic must match one of the match commands to be classified as part of the traffic class. If you use **match-all** , the traffic must match all the **match** commands to be part of the traffic class. Considering the exhibit, it is not possible for a packet to be ICMP, BGP, and EIGRP at the same time. Therefore, the traffic would never match the CoPP-CLASS class map and would never be subject to the implicit default class.

41. Refer to the exhibit. A network administrator configures AAA authentication on router R1. The ACS servers are configured and running. The administrator tests the configuration by telneting to R1. What will happen if the administrator attempts to authenticate through the RADIUS server using incorrect credentials?



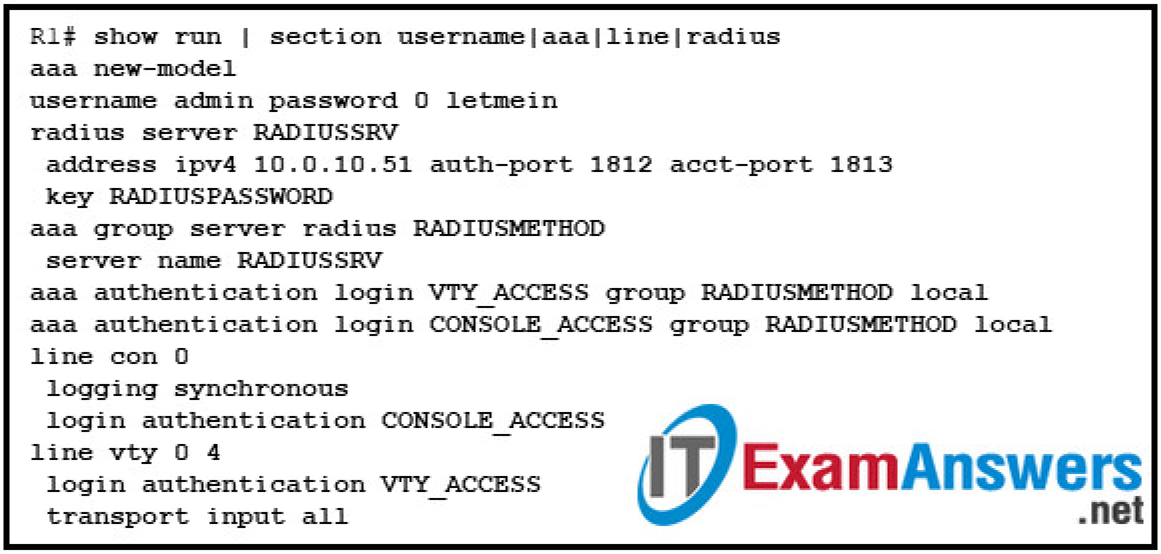
```
R1(config)# enable secret level 15 LetMeIn2
R1(config)# username ADMIN secret 1sThePassWd
R1(config)# aaa new-model
R1(config)# tacacs server SVR-T
R1(config-server-tacacs)# address ipv4 192.168.100.250
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key T-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)# radius server SVR-R
R1(config-radius-server)# address ipv4 192.168.100.252 auth-port 1812 acct-port 1813
R1(config-radius-server)# key R-Pa55w0rd
R1(config-radius-server)# exit
R1(config)# aaa authentication login default group tacacs enable
R1(config)# aaa authentication login AUTHEN group radius local enable
R1(config)# line vty 0 15
R1(config-line)# login authentication AUTHEN
R1(config-line)# line console 0
R1(config-line)# login authentication default
R1(config-line)# end
```

- The enable secret password and a random username could be used in the next login attempt.
- **The authentication process stops.**

- The enable secret password could be used in the next login attempt.
- The username and password of the local user database could be used in the next login attempt.

Explanation: The authentication for Telnet connections is defined by AAA method list AUTHEN. The AUTHEN list defines that the first authentication method is through an ACS server using the RADIUS protocol (or RADIUS server), the second authentication method is to use the local user database, and the third method is to use the enable password. In this scenario, however, because the administrator fails to pass the authentication by the first method, the authentication process stops and no other authentication methods are allowed.

42. Refer to the exhibit. A network administrator issues the show run | section username|aaa|line|radius command to verify an AAA configuration on a Cisco router. Which two conclusions can be drawn from the command output? (Choose two.)



```
R1# show run | section username|aaa|line|radius
aaa new-model
username admin password 0 letmein
radius server RADIUSSRV
 address ipv4 10.0.10.51 auth-port 1812 acct-port 1813
 key RADIUSPASSWORD
aaa group server radius RADIUSMETHOD
 server name RADIUSSRV
aaa authentication login VTY_ACCESS group RADIUSMETHOD local
aaa authentication login CONSOLE_ACCESS group RADIUSMETHOD local
line con 0
 logging synchronous
 login authentication CONSOLE_ACCESS
line vty 0 4
 login authentication VTY_ACCESS
 transport input all
```

- The router must use Cisco default ports for authentication and accounting to connect to a RADIUS server.
- Authentication for the vty lines is using the default authentication method.
- **Authentication for the console line will use local authentication as a fallback method if the RADIUS server is not available.**
- **A missing ip radius source-interface command on RADIUS server settings may prevent the router from using the services of the server.**
- The Cisco router can use the radiuspassword pre-shared key to connect to a RADIUS server.

Explanation: The conclusions that can be drawn from the command output are:
According to the **aaa authentication login VTY_ACCESS group RADIUSMETHOD local** command the first method to be used is the group of servers in the

RADIUSMETHOD group.
According to the **aaa authentication login CONSOLE_ACCESS group RADIUSMETHOD local** command, the first method to be used is the group of servers in the **RADIUSMETHOD** group, and the second method to be used if the servers are not available is the local username and password database.
RADIUS server is using ports 1812 and 1813 for authentication and accounting, so the port numbers on the Cisco router should be the same, not the Cisco default ports (1645 and 1646).
The router needs to be configured with the same pre-shared key for the RADIUS server, **RADIUSPASSWORD** .
When a router sources packets, it uses the exit interface as the source of the packet. If the exit interface is not configured with the IP address that the AAA server is expecting, the client cannot use the AAA server and the services it provides. It is recommended that the IP address of a loopback interface be used for the source of packets and as the client IP address that is configured on the AAA server. Therefore, the router should be configured with the ip radius source-interface [loopback] [number].

43. From the routing tables shown from routers within a multiarea OSPF network, which routing table would be from an internal router that is within a totally stub area?

A.

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 8 subnets, 4 masks
O IA 10.0.0.0/30 [110/4] via 10.1.1.1, 01:17:40, GigabitEthernet0/1
O IA 10.0.0.4/30 [110/3] via 10.1.1.1, 01:17:50, GigabitEthernet0/1
O IA 10.0.0.8/30 [110/66] via 10.1.1.1, 01:17:50, GigabitEthernet0/1
O 10.1.0.0/24 [110/2] via 10.1.1.1, 01:18:00, GigabitEthernet0/1
C 10.1.1.0/24 is directly connected, GigabitEthernet0/1
L 10.1.1.2/32 is directly connected, GigabitEthernet0/1
O IA 10.2.0.0/25 [110/5] via 10.1.1.1, 01:17:40, GigabitEthernet0/1
O IA 10.2.0.128/25 [110/6] via 10.1.1.1, 01:17:40, GigabitEthernet0/1
O*IA 0.0.0.0/0 [110/3] via 10.1.1.1, 01:17:50, GigabitEthernet0/1
```

B.

```
Gateway of last resort is 10.1.1.1 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
O 10.1.0.0/24 [110/2] via 10.1.1.1, 01:26:37, GigabitEthernet0/1
C 10.1.1.0/24 is directly connected, GigabitEthernet0/1
L 10.1.1.2/32 is directly connected, GigabitEthernet0/1
O*IA 0.0.0.0/0 [110/3] via 10.1.1.1, 01:26:27, GigabitEthernet0/1
```

C.

```
Gateway of last resort is 10.0.0.5 to network 0.0.0.0

10.0.0.0/8 is variably subnetted, 10 subnets, 4 masks
O 10.0.0.0/30 [110/2] via 10.0.0.5, 01:42:33, GigabitEthernet0/1
C 10.0.0.4/30 is directly connected, GigabitEthernet0/1
L 10.0.0.6/32 is directly connected, GigabitEthernet0/1
C 10.0.0.8/30 is directly connected, Serial0/0/0
L 10.0.0.9/32 is directly connected, Serial0/0/0
C 10.1.0.0/24 is directly connected, GigabitEthernet0/0
L 10.1.0.1/32 is directly connected, GigabitEthernet0/0
O 10.1.1.0/24 [110/2] via 10.1.0.2, 01:42:38, GigabitEthernet0/0
O IA 10.2.0.0/25 [110/3] via 10.0.0.5, 01:42:33, GigabitEthernet0/1
O IA 10.2.0.128/25 [110/4] via 10.0.0.5, 01:42:33, GigabitEthernet0/1
192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
O E2 192.168.0.0/30 [110/20] via 10.0.0.5, 01:42:33, GigabitEthernet0/1
O E2 192.168.0.64/26 [110/20] via 10.0.0.5, 00:47:20, GigabitEthernet0/1
O*E2 0.0.0.0/0 [110/1] via 10.0.0.5, 01:42:33, GigabitEthernet0/1
```

D.

```
Gateway of last resort is not set

1.0.0.0/32 is subnetted, 1 subnets
C 1.1.1.1/32 is directly connected, Loopback0
S 10.0.0.0/8 is directly connected, Serial0/0/0
203.0.113.0/24 is variably subnetted, 2 subnets, 2 masks
C 203.0.113.0/30 is directly connected, Serial0/0/0
L 203.0.113.1/32 is directly connected, Serial0/0/0
```

44. How does Cisco implement interarea OSPF summarization?

- **It must be configured manually on ASBRs.**
- The summarized route metric is equal to the lowest cost of all subnets within the summary address range.
- Multiple routes inside the area are summarized by more than one LSA.
- It is performed automatically by OSPF.

45. What are the two purposes of an OSPF router ID? (Choose two.)

- to uniquely identify the router within the OSPF domain
- to facilitate router participation in the election of the designated router
- to enable the SPF algorithm to determine the lowest cost path to remote networks
- to facilitate the establishment of network convergence
- to facilitate the transition of the OSPF neighbor state to Full

Explanation: OSPF router ID does not contribute to SPF algorithm calculations, nor does it facilitate the transition of the OSPF neighbor state to Full. Although the router ID is contained within OSPF messages when router adjacencies are being established, it has no bearing on the actual convergence process.

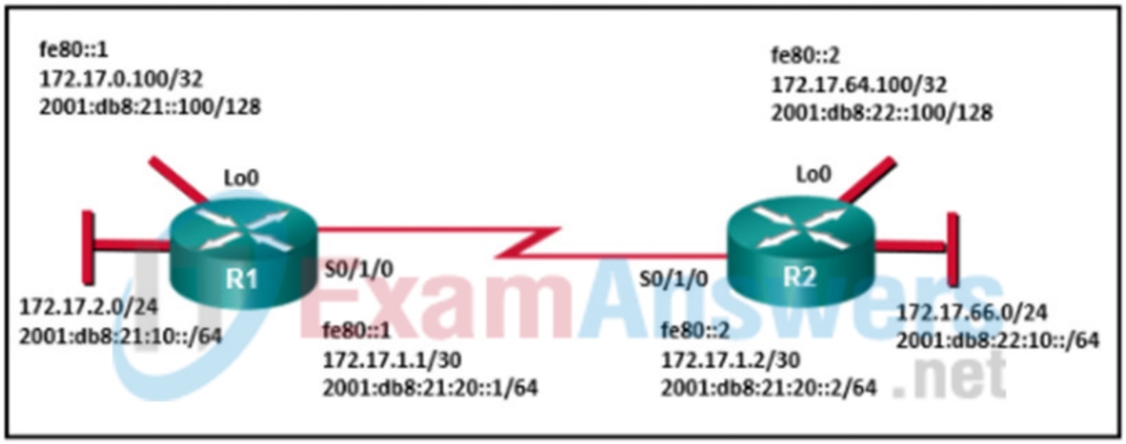
46. How is the flooding scope of link state advertisements denoted within OSPFv3 LSAs?

- The outer IPv6 OSPFv3 header uses three bits to determine LSA scope.
- **Three bits of the 16-bit LS type field of OSPFv3 LSAs set the scope.**
- ABR LSAs include scope information as part of the routing information payload.
- LSA scope is specified by the area area-ID range prefix-length command.

47. A network technician is verifying the OPSFv3 address families configuration on a Cisco router. What would the technician expect to see displayed when the show ospfv3 database router adv-router 4.4.4.4 command is issued?

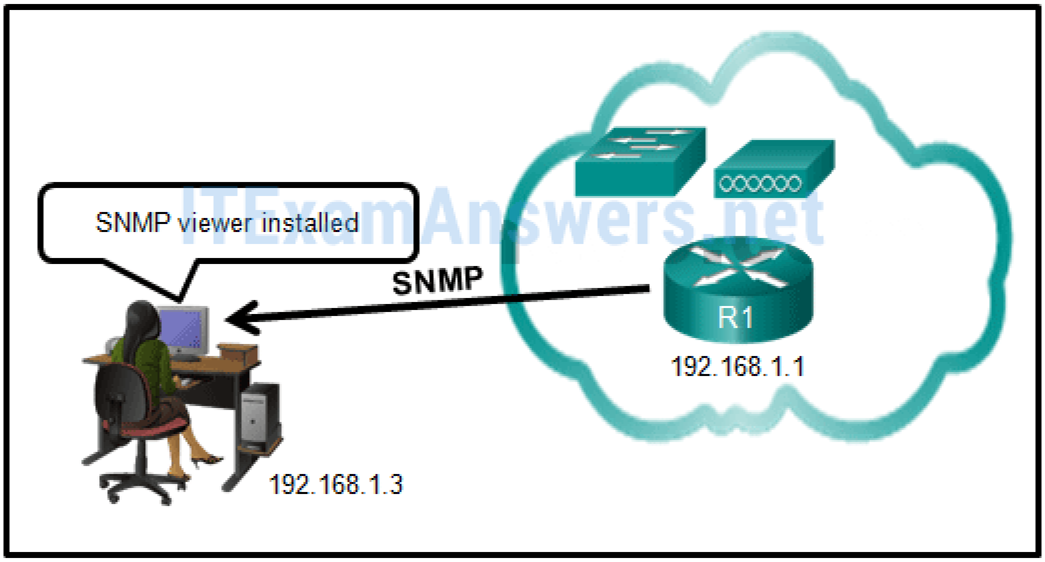
- the LSAs created by the router on which the command is executed and sent to the router with RID 4.4.4.4
- all area LSAs in the LSDB of the DR router on which the command is executed with RID 4.4.4.4
- **all LSAs in the LSDB of the router with RID 4.4.4.4**
- the LSAs received from the router with RID 4.4.4.4 that exist in the LSDB of the local router

48. Refer to the exhibit. Both routers R1 and R2 are configured for OSPFv3 and are routing for both IPv4 and IPv6 address families. Which two destination addresses will R1 use to establish a full adjacency with R2? (Choose two.)



- ff02::5
- fe80::2
- 2001:db8:22::100
- 172.17.66.1
- 2001:db8:21:20::2

49. Refer to the exhibit. Router R1 was configured by a network administrator to use SNMP version 2. The following commands were issued:



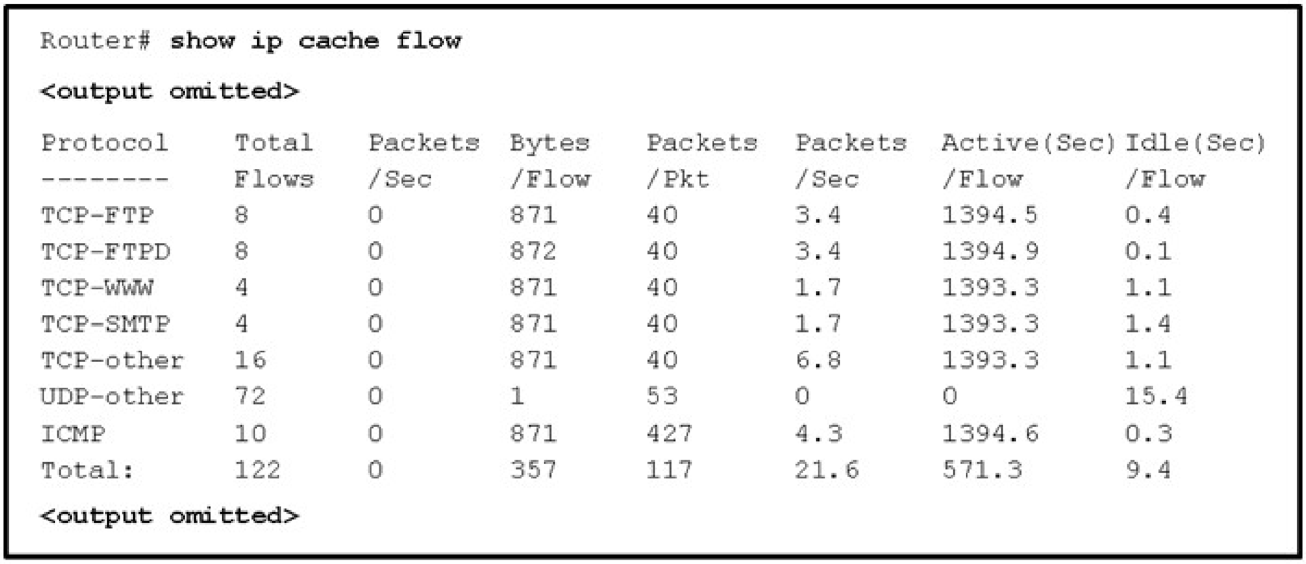
R1(config)# snmp-server community batonaug ro SNMP_ACL
R1(config)# snmp-server contact Wayne World
R1(config)# snmp-server host 192.168.1.3 version 2c batonaug
R1(config)# ip access-list standard SNMP_ACL
R1(config-std-nacl)# permit 192.168.10.3

Why is the administrator not able to get any information from R1?

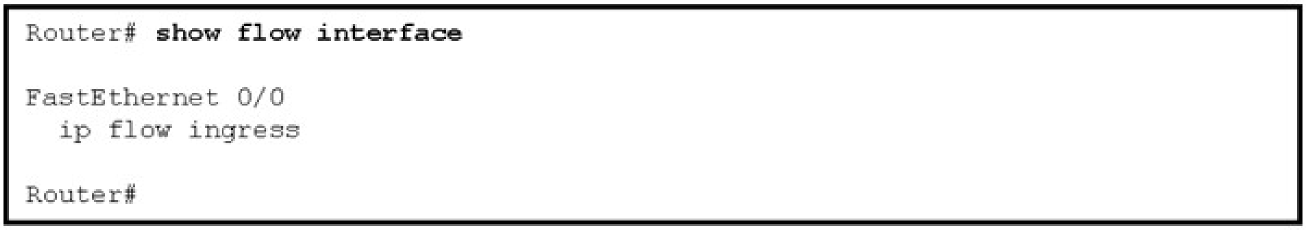
- The snmp-server enable traps command is missing.
- **There is a problem with the ACL configuration.**
- The snmp-server community command needs to include the rw keyword.
- The snmp-server location command is missing.

Explanation: The permit statement with the incorrect IP address is the reason why the administrator is not able to access router R1. The correct statement should be permit 192.168.1.3. The snmp-server location and snmp-server enable traps commands are optional commands and have no relation to the access restriction to router R1. The rw keyword does not need to be included in this case because the administrator just wants to obtain information, not change any configuration.

50. Refer to the exhibit. The total number of packet flows is not consistent with what is expected by the network administrator. The results show only half of the flows that are typically captured for the interface. Pings between the router and the collector are successful. What is the reason for the unexpected results?



```
Router# show ip cache flow

<output omitted>

Protocol     Total    Packets  Bytes    Packets  Packets  Active(Sec) Idle(Sec)
--------     Flows    /Sec     /Flow    /Pkt     /Sec     /Flow       /Flow
TCP-FTP      8        0        871      40       3.4      1394.5      0.4
TCP-FTPD     8        0        872      40       3.4      1394.9      0.1
TCP-WWW      4        0        871      40       1.7      1393.3      1.1
TCP-SMTP     4        0        871      40       1.7      1393.3      1.4
TCP-other    16       0        871      40       6.8      1393.3      1.1
UDP-other    72       0        1        53       0        0           15.4
ICMP         10       0        871      427      4.3      1394.6      0.3
Total:       122      0        357      117      21.6     571.3       9.4

<output omitted>
```

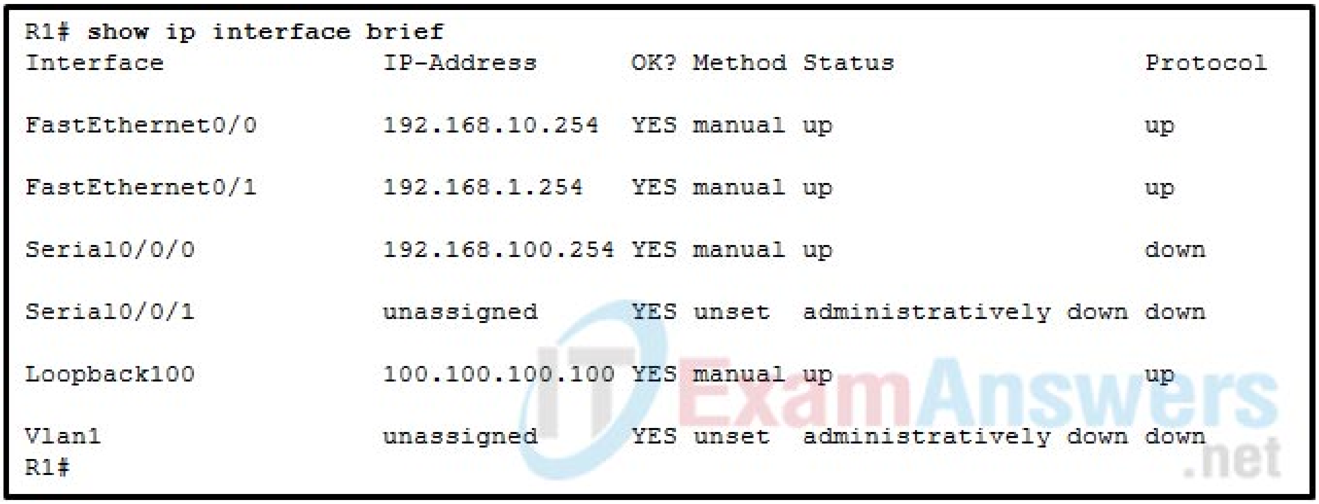


```
Router# show flow interface

FastEthernet 0/0
  ip flow ingress

Router#
```

- Interface Fa0/0 is not configured as the source of the packets sent to the collector.
- The interface is shutdown.
- The Netflow collector IP address and UDP port number are not configured on the router.
- **The router is not configured to monitor outgoing packets on the interface.**

Explanation: NetFlow flows are unidirectional. One user connection exists as two flows. The flow in each direction must be captured. This is done by using both the ip flow ingress and ip flow egress command on the interface.

51. Refer to the exhibit. A network administrator is configuring the syslog service on a Cisco router. Which command should be used to configure an IPv4 address of 192.168.10.254 as the source address on the syslog packets as they exit the router R1?



```
R1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.10.254  YES manual up                    up

FastEthernet0/1        192.168.1.254   YES manual up                    up

Serial0/0/0            192.168.100.254 YES manual up                    down

Serial0/0/1            unassigned      YES unset  administratively down down

Loopback100            100.100.100.100 YES manual up                    up

Vlan1                  unassigned      YES unset  administratively down down
R1#
```

- **R1(config)#logging host 192.168.10.254**
- R1(config)#logging origin-id ip
- R1(config)#logging source-interface fa0/0
- R1(config)# logging 192.168.10.254

52. Which three implicit access control entries are automatically added to the end of an IPv6 ACL? (Choose three.)

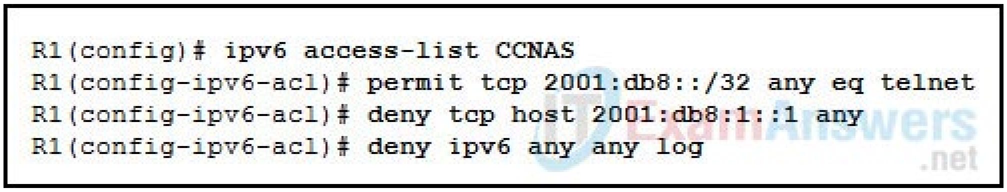
- deny ip any any
- **deny ipv6 any any**
- permit ipv6 any any
- deny icmp any any
- **permit icmp any any nd-ns**
- **permit icmp any any nd-na**

53. Which two networks would match the following prefix list? (Choose two.)

```
ip prefix-list MATCHTHIS seq 5 deny 10.1.0.0/16 ge 24 le 30
```

- 10.0.0.0/16
- **10.1.1.0/30**
- **10.1.0.0/24**
- 10.1.0.0/16
- 10.0.0.0/24

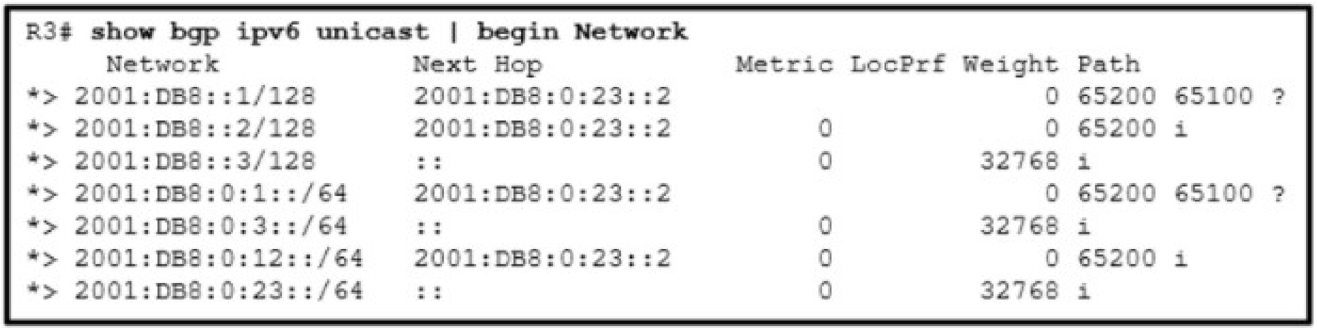
54. Refer to the exhibit. An administrator has configured the IPv6 ACL that is in the exhibit to permit outbound Telnet traffic to any destination, and block TCP connections from 2001:db8:1::1 to any destination. All other packets should be denied and logged. After implementing the ACL, all IPv6 traffic, including Telnet from the 2001:db8::/32 subnet is denied. What is the problem?



```
R1(config)# ipv6 access-list CCNAS
R1(config-ipv6-acl)# permit tcp 2001:db8::/32 any eq telnet
R1(config-ipv6-acl)# deny tcp host 2001:db8:1::1 any
R1(config-ipv6-acl)# deny ipv6 any any log
```

- **The deny ipv6 any any log ACE is preventing NDP from functioning.**
- The eq telnet parameter should appear immediately after the IPv6 address in the first ACE.
- The ACEs are in the wrong order.
- The wildcard mask is missing from the first ACE.

55. Refer to the exhibit. A network administrator issues the command `show bgp ipv6 unicast | begin Network` to check the BGP table. Which statement describes the routes with an unspecified address (::) in the Next Hop column?

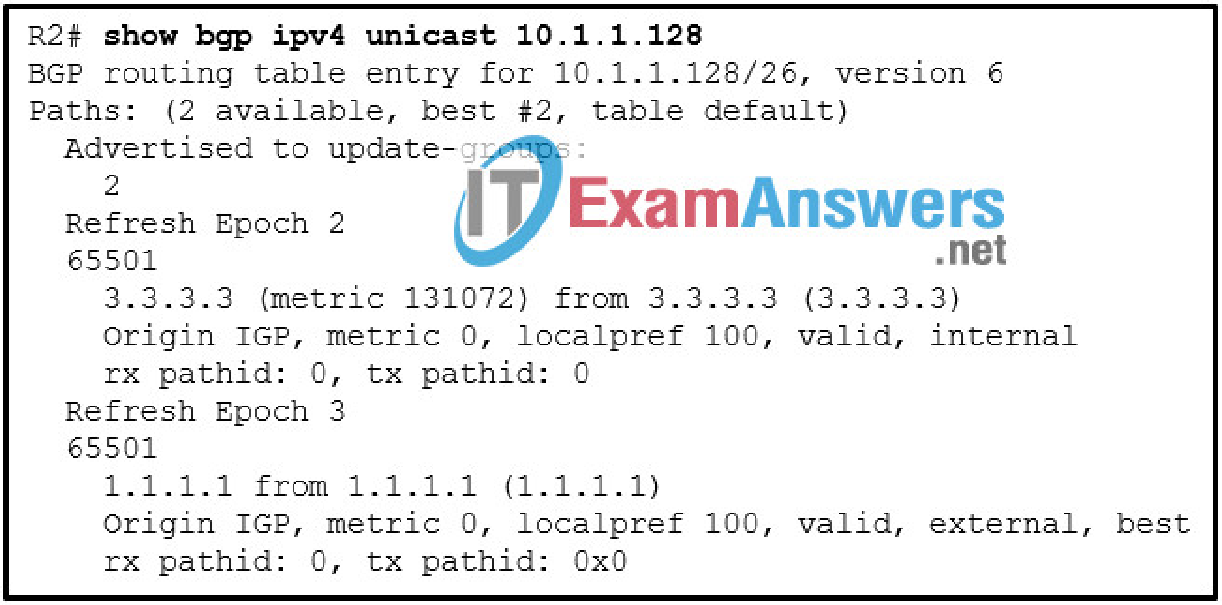


```
R3# show bgp ipv6 unicast | begin Network
     Network              Next Hop            Metric LocPrf Weight Path
*> 2001:DB8::1/128      2001:DB8:0:23::2                        0 65200 65100 ?
*> 2001:DB8::2/128      2001:DB8:0:23::2          0             0 65200 i
*> 2001:DB8::3/128      ::                        0         32768 i
*> 2001:DB8:0:1::/64    2001:DB8:0:23::2                        0 65200 65100 ?
*> 2001:DB8:0:3::/64    ::                        0         32768 i
*> 2001:DB8:0:12::/64   2001:DB8:0:23::2          0             0 65200 i
*> 2001:DB8:0:23::/64   ::                        0         32768 i
```

- They are learned through an IGP.
- They are locally generated network prefixes.
- They indicate routes created by static route configuration.
- They are learned through BGP advertisements from the next neighbor.

Explanation: An unspecified address in the BGP table indicates that the local router is generating the prefix for the BGP table. The weight value 32,768 also indicates that the prefix is locally originated by the router.

56. Refer to the exhibit. A network administrator issues the show bgp ipv4 unicast 10.1.1.128 command on router R2 to verify the network 10.1.1.128 in the BGP table. The administrator notices that there are two paths to reach the network. Which BGP factor is used to determine the best-path?



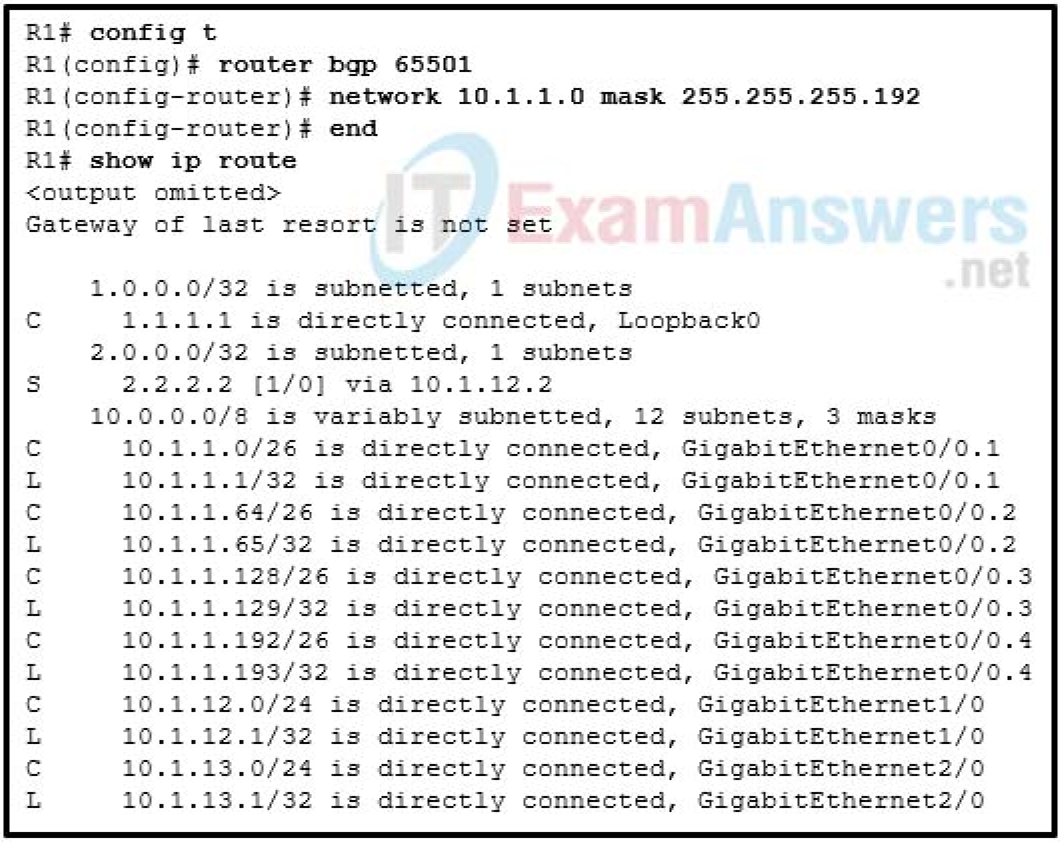
```
R2# show bgp ipv4 unicast 10.1.1.128
BGP routing table entry for 10.1.1.128/26, version 6
Paths: (2 available, best #2, table default)
  Advertised to update-groups:
    2
  Refresh Epoch 2
  65501
    3.3.3.3 (metric 131072) from 3.3.3.3 (3.3.3.3)
      Origin IGP, metric 0, localpref 100, valid, internal
      rx pathid: 0, tx pathid: 0
  Refresh Epoch 3
  65501
    1.1.1.1 from 1.1.1.1 (1.1.1.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      rx pathid: 0, tx pathid: 0x0
```

- the value of the BGP RID
- the value of the lowest multi-exit discriminator attribute
- whether the path is being learned via IBGP or EBGP
- **the value of the weight attribute**

Explanation: Cisco routers review BGP attributes in the following ranked order when deciding which path is the best-path:
– Prefer the highest weight .
– Prefer the highest local preference .
– Prefer the route originated by the local router.
– Prefer the path with the shorter Accumulated Interior Gateway Protocol (AIGP) metric attribute.
– Prefer the shortest AS_Path .
– Prefer the lowest origin code.
– Prefer the lowest multi-exit discriminator (MED).
– Prefer an external path over an internal path.
– Prefer the path through the closest IGP neighbor .
– Prefer the oldest route for EBGP paths.
– Prefer the path with the lowest neighbor BGP RID .
– Prefer the path with the lowest neighbor IP address .
The first path attribute to be checked is the weight. In this case, no weight is listed because both routes are using the default value 0. The next path attribute to be checked is the local preference. A higher value is better. Therefore, setting the local preference to 200 will make the path through 3.3.3.3 the best-path.

57. Refer to the exhibit. A network administrator is configuring BGP route advertisement on router R1. The network 10.1.0.0/24 is subnetted into four 10.1.0.0/26 subnets that are attached to the 4 interfaces of R1 respectively. The

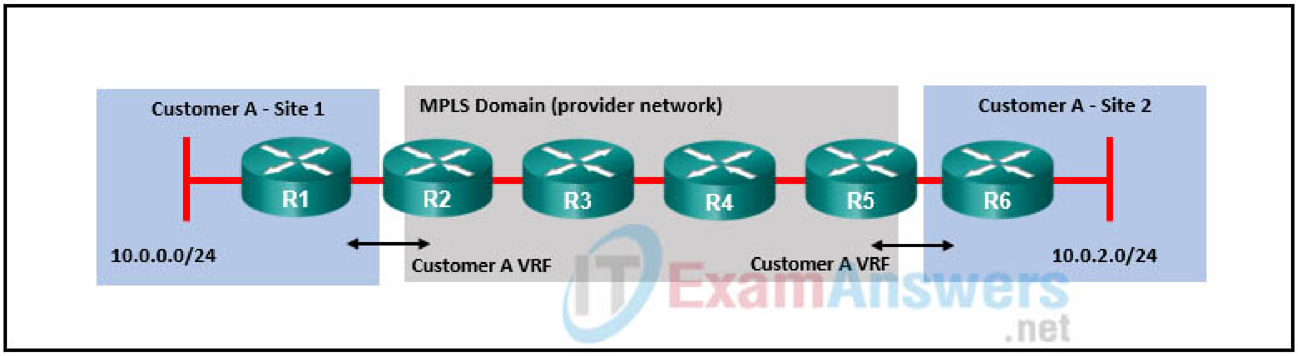
administrator issues the show ip route command and notices that the network 10.1.0.0/24 is not advertised by BGP. What is a possible cause for this issue?



```
R1# config t
R1(config)# router bgp 65501
R1(config-router)# network 10.1.1.0 mask 255.255.255.192
R1(config-router)# end
R1# show ip route
<output omitted>
Gateway of last resort is not set

    1.0.0.0/32 is subnetted, 1 subnets
C     1.1.1.1 is directly connected, Loopback0
    2.0.0.0/32 is subnetted, 1 subnets
S     2.2.2.2 [1/0] via 10.1.12.2
    10.0.0.0/8 is variably subnetted, 12 subnets, 3 masks
C     10.1.1.0/26 is directly connected, GigabitEthernet0/0.1
L     10.1.1.1/32 is directly connected, GigabitEthernet0/0.1
C     10.1.1.64/26 is directly connected, GigabitEthernet0/0.2
L     10.1.1.65/32 is directly connected, GigabitEthernet0/0.2
C     10.1.1.128/26 is directly connected, GigabitEthernet0/0.3
L     10.1.1.129/32 is directly connected, GigabitEthernet0/0.3
C     10.1.1.192/26 is directly connected, GigabitEthernet0/0.4
L     10.1.1.193/32 is directly connected, GigabitEthernet0/0.4
C     10.1.12.0/24 is directly connected, GigabitEthernet1/0
L     10.1.12.1/32 is directly connected, GigabitEthernet1/0
C     10.1.13.0/24 is directly connected, GigabitEthernet2/0
L     10.1.13.1/32 is directly connected, GigabitEthernet2/0
```

- Not all four interfaces are up/up.
- **The network mask command does not match the network/prefix in the routing table.**
- The BGP slit-horizon rule prevents the network from being advertised.
- The network command is missing the summary-only keyword.

58. Refer to the exhibit. Which protocol is used by R2 and R5 to exchange Layer 3 routes?



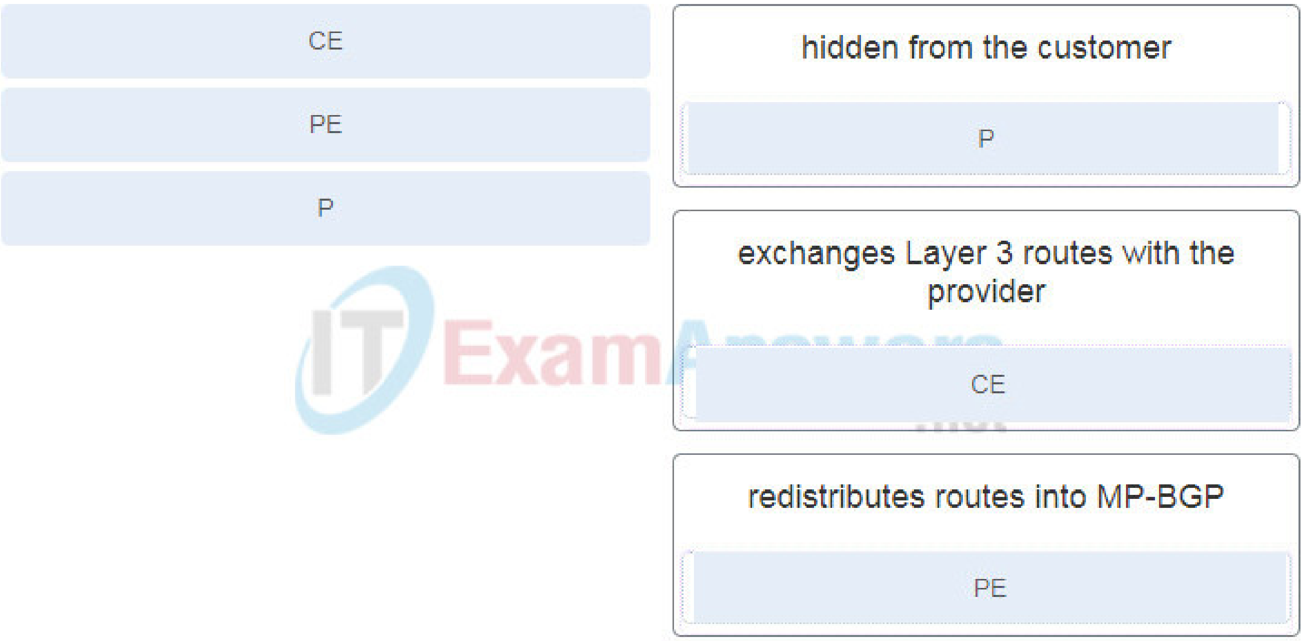
- EIGRP
- MP-BGP

- LDP
- **OSPF**

59. When an unlabeled packet arrives at an MPLS-enabled router interface, which database is used to make a forwarding decision on the packet?

- IP routing table (RIB)
- **IP forwarding table (FIB)**
- label information base (LIB)
- label forwarding table (LFIB)

60. Match the MPLS router type to its characteristic.



CE

PE

P

hidden from the customer

P

exchanges Layer 3 routes with the provider

CE

redistributes routes into MP-BGP

PE

61. What is the order in determining the BGP router ID?

- statically defined, the highest IP address of any active interfaces, and the highest IP address of any active loopback interfaces
- **statically defined, the highest IP address of any active loopback interfaces, and the highest IP address of any active interfaces**
- the highest IP address of any active interfaces, statically defined, and the highest IP address of any active loopback interfaces
- the highest IP address of any active loopback interfaces, statically defined, and the highest IP address of any active interfaces

Explanation: Statically configuring the BGP router ID (RID) is a best practice to ensure RID stability. If the RID is not statically configured, the dynamic RID allocation logic uses the highest IP address of any active loopback interfaces. If there is not an active loopback interface, then the highest IP address of any active interfaces becomes the RID when the BGP process initializes.