

CCNP ENARSI v8 (300-410) Certification Practice Exam Answers

 itexamanswers.net/ccnp-enarsi-v8-300-410-certification-practice-exam-answers.html

April 8, 2021

CCNP Enterprise: Advanced Routing (Version 8.0) – CCNP ENARSI (300-410) Certification Practice Exam

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**.

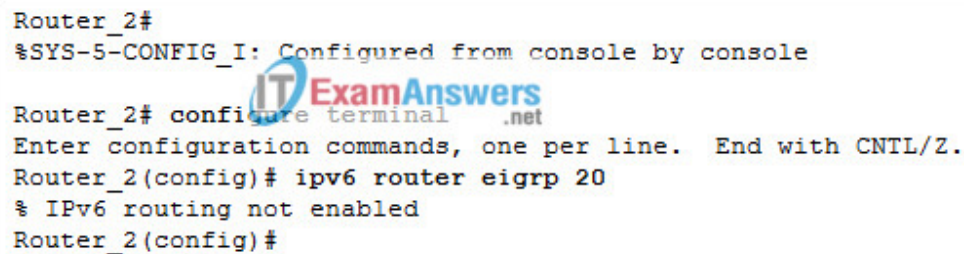
NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. 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.)

- 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.

2. Refer to the exhibit. A network administrator is configuring EIGRP AS 20 on Router_2 and has received the error that is shown. What is the cause of the error?



```
Router_2#
%SYS-5-CONFIG_I: Configured from console by console

Router_2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router_2(config)# ipv6 router eigrp 20
% IPv6 routing not enabled
Router_2(config)#
```

- The autonomous system (AS) number is not the same as the number on other routers in this network.
- The EIGRPv6 interface configuration is incomplete.
- The passive-interface default command has been implemented for EIGRPv6.
- **The IPv6 routing process cannot be implemented until IPv6 routing is enabled.**

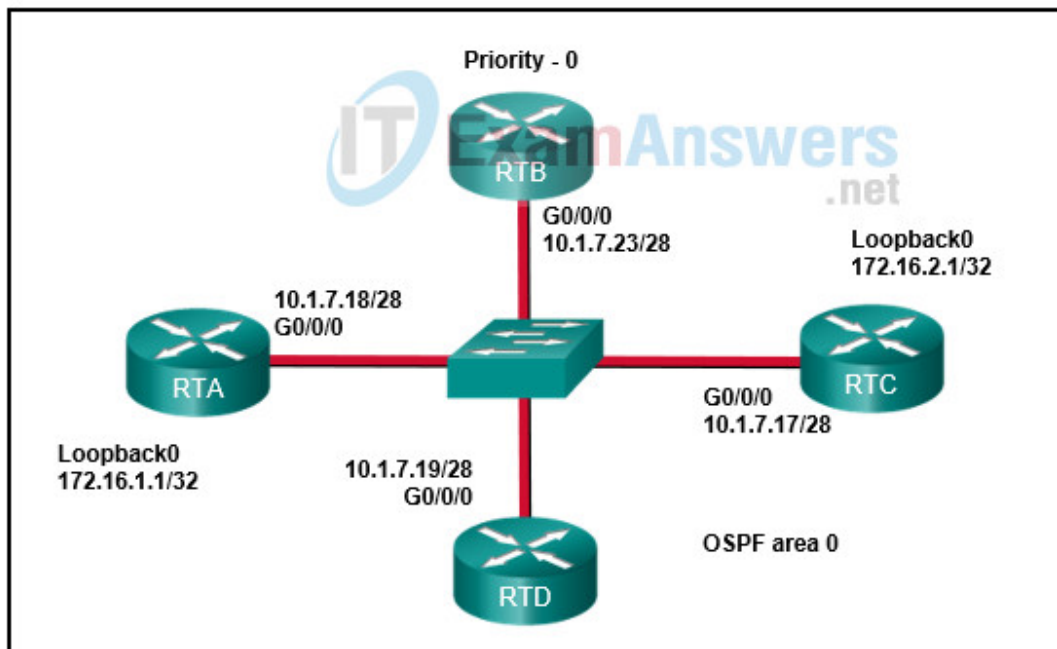
Explanation: The EIGRPv6 configuration is causing an error because the command **ipv6 unicast-routing** has not been implemented yet in global configuration mode. This command enables IPv6 routing on the Cisco router. Without this command, no IPv6 protocols will be enabled.

3. An administrator is troubleshooting an adjacency issue between two OSPF routers. Which two neighbor states indicate a stable adjacency between the routers? (Choose two.)

- exstart
- **2way**
- **full**
- exchange
- loading

Explanation: The full and 2way states are two stable OSPF adjacency types. The 2way stay occurs after two adjacent routers have received hello messages from each other and each router saw its own RID in the received hello message. The full state indicates that OSPF routers have successfully formed an adjacency.

4. Refer to the exhibit. What destination address will RTB use to advertise LSAs?



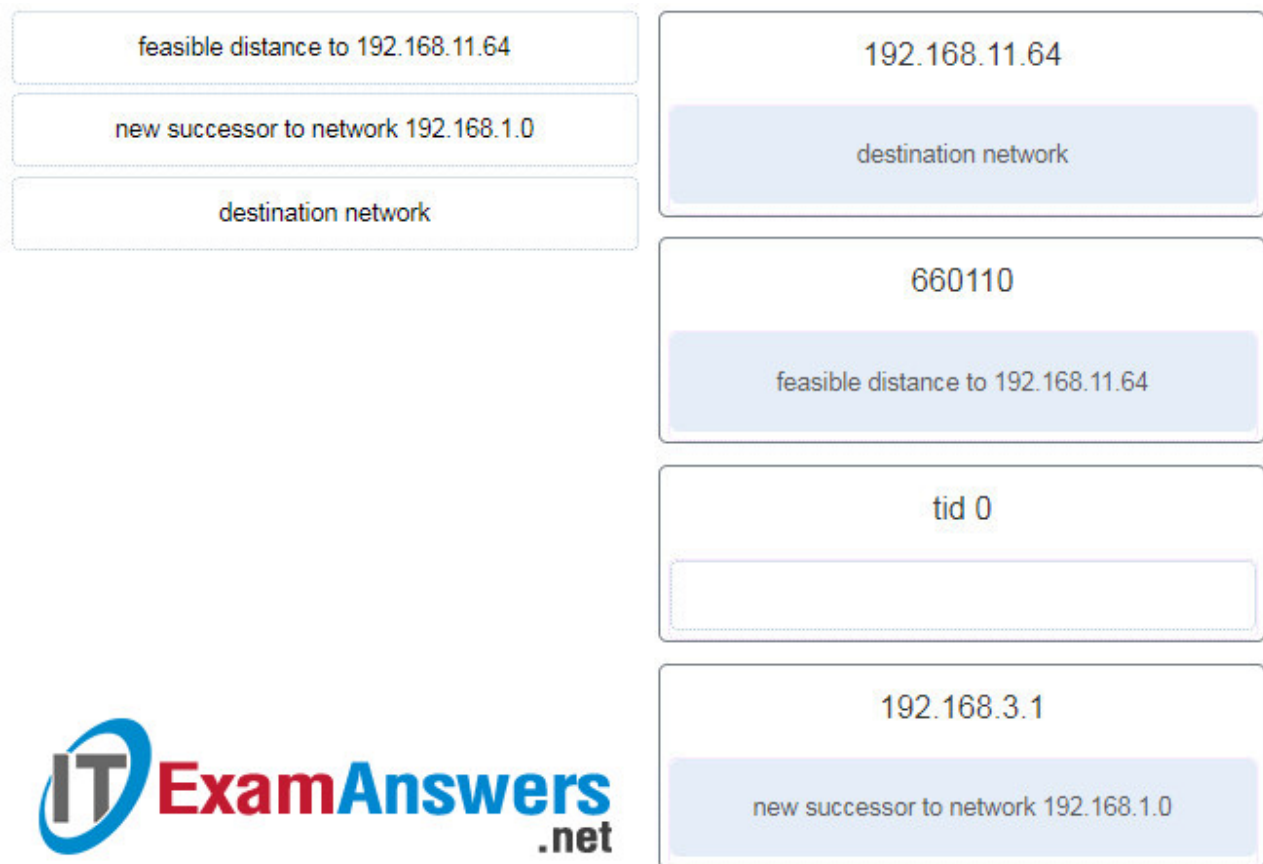
- 255.255.255.255
- **224.0.0.6**
- 172.16.1.1
- 224.0.0.5
- 10.1.7.17/28
- 172.16.2.1

Explanation: A DR and BDR are elected on multiaccess networks to reduce the number of OSPF adjacencies formed. Non-DR routers will form adjacencies with the DR and BDR and send LSU packets to the AllDR-Routers multicast address of 224.0.0.6

5. Refer to the exhibit. Match the description to the corresponding value used by the DUAL FSM. (Not all options are used.)

```
R1# debug eigrp fsm
EIGRP Finite State Machine debugging is on
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface serial0/0/0
R1(config-if)# shutdown
```

EIGRP-IPv4(1):Find FS for dest 192.168.11.64/26. FD is 660110, RD is 660110 on tid 0
DUAL: AS(1) Removing dest 192.168.1.0/24, nexthop 172.16.1.1
DUAL: AS(1) RT installed 192.168.1.0/24 via 192.168.3.1



6. Refer to the exhibit. After configuring two-way redistribution, an administrator notices that none of the EIGRP routes are being advertised in the OSPF network. What is a possible reason that the routes are not being advertised?

```
router1# show run

<output omitted>

router eigrp 100
network 10.0.0.0
redistribute ospf 5 10000 100 255 1 1500
!
router ospf 5
network 209.165.200.224 0.0.0.31 area 0
redistribute eigrp 5 metric 100

<output omitted>
```

- The wrong EIGRP AS is being redistributed.
- The metric value is wrong for the redistribute command under OSPF.
- The metric value is wrong for the redistribute command under EIGRP.
- The subnets keyword is missing on the redistribute command under OSPF.

Explanation: The **redistribute** command under the OSPF 5 process should indicate an EIGRP AS of 100 instead of 5.

7. A network administrator is teaching a junior network engineer about EIGRP stub routers. Which two explanations can be given to the junior engineer about the subject? (Choose two.)

- An EIGRP stub router advertises only connected routes by default.
- An EIGRP stub router receives queries from EIGRP when a route goes active.
- **An EIGRP stub router does not advertise routes that it learns from other EIGRP peers.**
- An EIGRP stub router announces that it is a stub router within the EIGRP query packet.
- **An EIGRP stub router can be configured only to receive routes.**

Explanation: An EIGRP stub router does not advertise routes that it learns from other EIGRP peers. By default, EIGRP stubs advertise only connected and summary routes, but they can be configured only to receive routes or advertise any combination of redistributed routes, connected routes, or summary routes. The EIGRP stub router announces that it is a stub router within the EIGRP hello packet. If a route goes active, EIGRP does not send EIGRP queries to an EIGRP stub router.

8. A boundary router is performing mutual redistribution between OSPF and EIGRP. What process should be taken to have an external EIGRP route preferred over an OSPF route to the same destination network?

- **Modify the administrative distance parameter for the external EIGRP routes to be set to 100.**
- Modify the default seed metric to 21 for the source information from OSPF.
- Modify the administrative distance parameter for the internal EIGRP routes to be set to 180.
- Modify the default seed metric to 19 for the source information from OSPF.

Explanation: In order to have an external EIGRP route with a default AD of 170 preferred over an OSPF route with a default AD of 110 to the same destination network, the administrative distance value should be modified to a lower value.

9. Which two statements describe OSPF? (Choose two.)

- OSPF must be implemented in a three-layer area hierarchy.
- **OSPF routers may have large routing tables if routes are not summarized.**
- OSPF uses the SPF algorithm, which requires few CPU cycles.
- **OSPF routers within an area have the same link-state information.**
- OSPF performs automatic route summarization by default.

Explanation: OSPF routers within the same area will have the same link-state databases. Without route summarization, OSPF routers may have large routing tables. There is no automatic summarization of routes with OSPF. OSPF can be implemented in a single area or in a two-layer multiarea hierarchy. SPF recalculation, especially in larger networks, is processor intensive.

10. Refer to the exhibit. Which two conclusions can be derived from the output? (Choose two.)

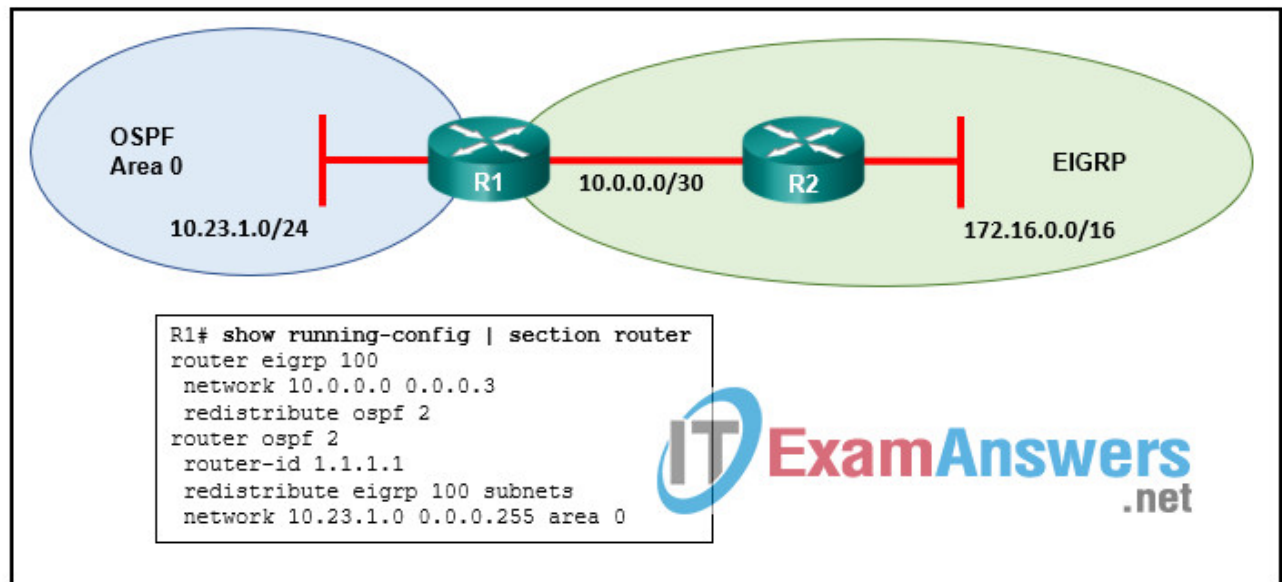
```
R1# show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(2.2.2.2)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply, r - reply
Status, s - sia Status

P 172.16.3.0/24, 1 successors, FD is 1315
   via Connected, GigabitEthernet0/1
P 192.168.1.8/30, 1 successors, FD is 452141
   via 192.168.11.1 (452141/216956), Serial0/0/1
   via 172.16.6.1 (68024000/216956), Serial0/0/0
P 192.168.1.0/24, 1 successors, FD is 3012096
   via 192.168.11.1 (3012096/28116), Serial0/0/1
   via 172.16.6.1 (41024256/2170112), Serial0/0/0
P 192.168.10.8/30, 1 successors, FD is 3011840
   via Connected, Serial0/0/1
```

- Router R1 has two successors to the 172.16.3.0/24 network
- There is one feasible successor to network 192.168.1.8/30.
- The reported distance to network 192.168.1.0/24 is 41024256
- The neighbor 172.16.6.1 meets the feasibility condition to reach the 192.168.1.0/24 network.
- The network 192.168.10.8/30 can be reached through 192.168.11.1.

Explanation: The second entry in the table indicates that there is one feasible successor (“1 successors”) for network 192.168.1.8/30. The last entry in the table shows that network 192.168.10.8/30 is directly connected, so it is not reachable through network 192.168.11.1. The third entry indicates that the reported distances for network 192.168.1.0 are 28116 and 2170112, not 41024256. This same entry shows that neighbor 172.16.6.1 is a feasible successor for network 192.168.1.0. The first entry indicates that R1 has only one successor, not two to network 172.16.3.0/24.

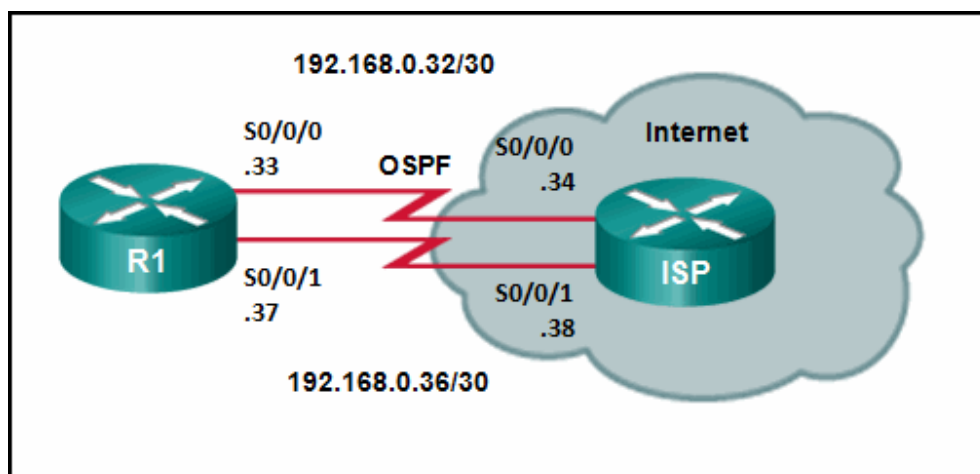
11. Refer to the exhibit. A network administrator has configured two-way redistribution on router R1. However, OSPF routes are not being redistributed into the EIGRP domain. What is causing this issue?



- The EIGRP process ID is incorrect and should be set to 2.
- The subnets keyword from the OSPF configuration should be removed.
- **A seed metric is not provided for OSPF routes.**
- An OSPF metric type has not been defined.

Explanation: The redistribution configuration exists under the destination protocol and identifies the source protocol. Unless a seed metric is defined, routes redistributed into EIGRP will have a default seed metric of infinity and will not be included in the EIGRP topology table.

12. Refer to the exhibit. Router R1 has an OSPF neighbor relationship with the ISP router over the 192.168.0.32 network. The 192.168.0.36 network link should serve as a backup when the OSPF link goes down. The floating static route command `ip route 0.0.0.0 0.0.0.0 S0/0/1 100` was issued on R1 and now traffic is using the backup link even when the OSPF link is up and functioning. Which change should be made to the static route command so that traffic will only use the OSPF link when it is up?



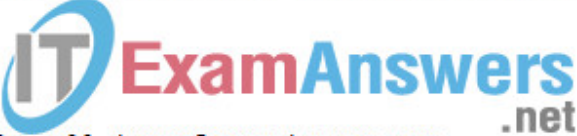
- Change the administrative distance to 120.
- Add the next hop neighbor address of 192.168.0.36.
- Change the destination network to 192.168.0.34.
- Change the administrative distance to 1.

Explanation: The problem with the current floating static route is that the administrative distance is set too low. The administrative distance will need to be higher than that of OSPF, which is 110, so that the router will only use the OSPF link when it is up.

13. Refer to the exhibit. OSPFv2 has been configured on router R1, and the router-id command has not been manually configured. When the network administrator reboots router R1, what will be the value of the OSPF router ID?

```
R1# show ip interface brief
Interface                IP-Address      OK? Method Status        Protocol
FastEthernet0/0          192.168.2.254   YES manual up            up
FastEthernet0/1          unassigned      YES unset  up            down
Serial10/0/0              10.0.10.2       YES manual up            up
Serial10/0/1              unassigned      YES unset  down          down
Loopback10                10.15.15.1      YES manual up            up
Loopback15                172.16.1.1      YES manual up            up
Vlan1                     unassigned      YES unset  administratively down down

R1# show ip protocols
Routing Protocol is "ospf 10"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.2.254
<output omitted>
```



- 10.0.10.2
- 10.15.15.1
- **172.16.1.1**
- 192.168.2.254

Explanation: If the router ID is not exactly specified by the router-id command, then the highest IPv4 address on any configured loopback interface(s) would become the router ID.

14. Refer to the exhibit. Based on the output shown, how are the OSPFv3 address families configured this router?

```

R1# show ospfv3 interface | include Instance
      Area 1,      Process ID 1,      Instance ID 64,      Router ID 172.16.0.1
      Area 0,      Process ID 1,      Instance ID 0,      Router ID 172.16.0.1
<output omitted>

```



- The IPv6 address family is configured for both Area 0 and Area 1.
- **The IPv4 address family is configured for Area 1, IPv6 for Area 0.**
- The IPv4 address family is configured for Area 0, IPv6 for Area 1.
- The IPv4 address family is configured for both Area 0 and Area 1.

Explanation: The instance ID 0 is for IPv6 unicast and instance ID 64 is for IPv4 unicast. OSPFv3 runs on top of IPv6 and uses IPv6 link-local scope (FE80::/10) for control packets. As a consequence, it is required that IPv6 be enabled on an OSPFv3 link although the link may not be participating in any IPv6 routing. For OSPFv3 AFs, both OSPF for IPv4 and OSPF for IPv6 use IPv6 to exchange routing information. Therefore, IPv6 unicast routing must be enabled on the routers.

15. 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

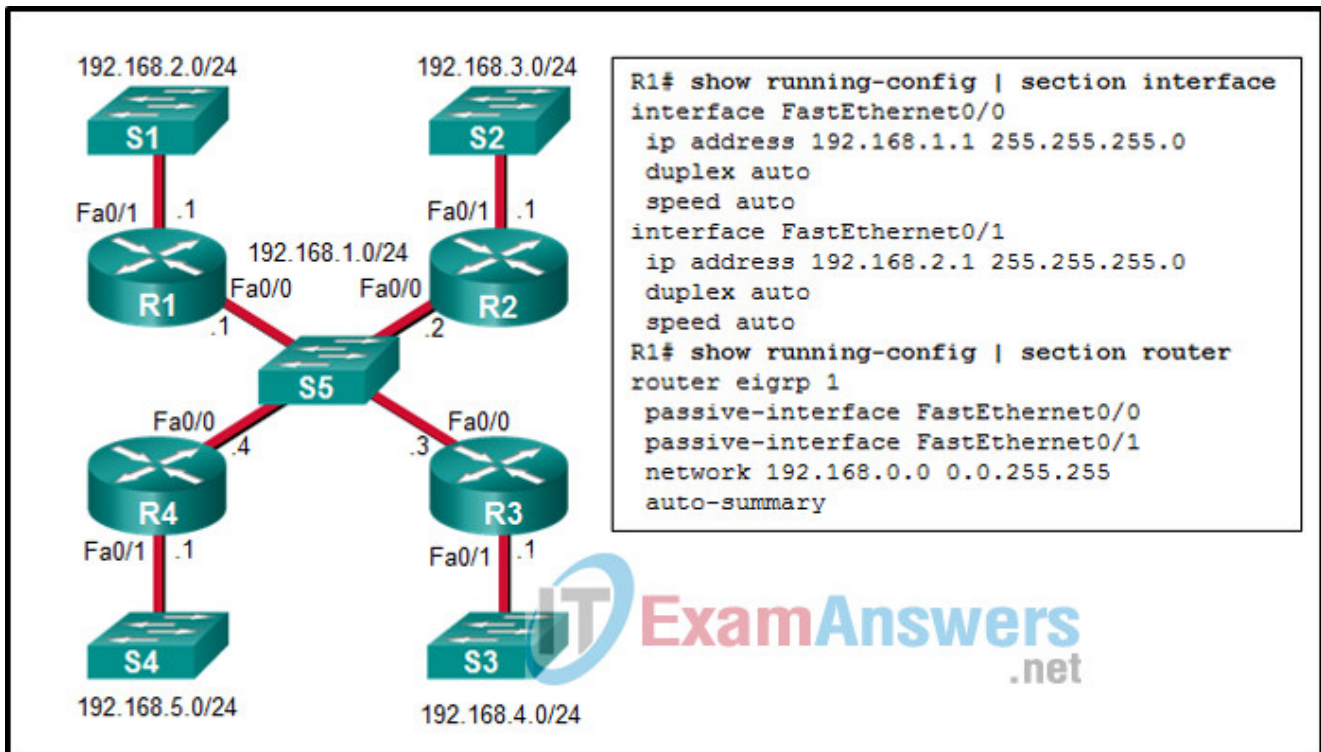
Explanation: A variance of 11 is needed to load balance across the second route. The metric of the existing successor route is 25000. The metric of the second route is 264000. The first metric needs to be multiplied by 11, which is 275000, in order for the route to be put into the routing table.

16. An administrator is troubleshooting failing EIGRP route exchanges on routers R1 and R2. On further investigation it is discovered that the route exchanges were failing because the routers had duplicate router IDs. The router ID for R1 is changed using the `eigrp router-id` command, but the problem persists. Which additional action must be taken to enable the routers to exchange routes?

- Change the timers on both routers to be the same.
- Change the router ID on R2.
- **Clear the EIGRP process.**
- Change the link-local address on R1 to a multicast address.

Explanation: Both routers on an adjoining EIGRP must belong to the same router process ID. However, the router IDs must be unique. In the event one router ID is changed, the EIGRP process must be cleared for the router to start exchanging EIGRP routes again.

17. 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?

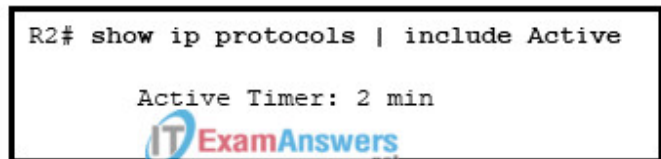


- because the automatic summarization is enabled on R1
- because the IPv4 address on Fa0/0 interface of R1 is incorrect
- **because the Fa0/0 interface of R1 is declared as passive for EIGRP**
- because there is no network command for the network 192.168.1.0/24 on R1

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 Fa0/0 of the router R1 is declared as passive, so R1 will not send hello packets over its interface Fa0/0.

18. Refer to the exhibit. A network administrator verifies on an enterprise network that EIGRP query packets are delayed because of packet loss. The administrator issues the show ip protocols | include Active command to see the EIGRP active timer on a router. What can the administrator conclude from this output?

- EIGRP waits 120 seconds before sending a SIA query to neighbors that did not respond.
- The SIA state is declared for a neighbor without receiving an SIA reply after 4 minutes.
- **Upon receipt of an SIA query from a neighbor router, the router needs to respond within 60 seconds to avoid being SIA state.**
- This is the default value of the active timer.



```
R2# show ip protocols | include Active
Active Timer: 2 min
```

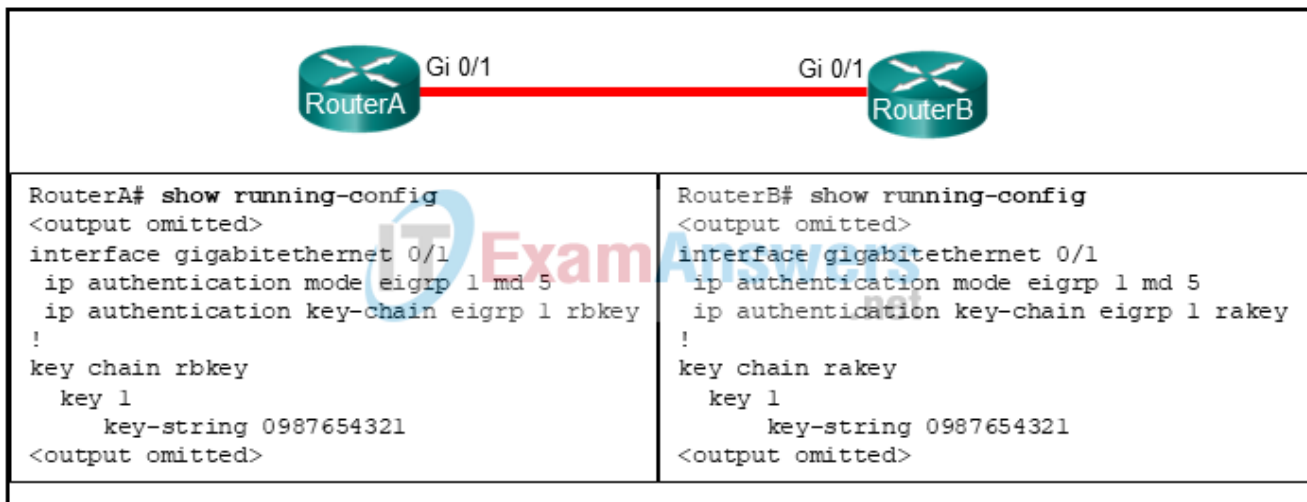
Explanation: Occasionally, an EIGRP query is delayed because of packet loss, slow neighbors, or a large hop count. EIGRP maintains an active timer, which has a default value of 3 minutes (180 seconds). According to the output, the active timer was set to 2 minutes (120 seconds). EIGRP then waits half of the active timer value that was set (60 seconds) for a reply. If the router does not receive a response within 60 seconds, the originating router sends a SIA query to EIGRP neighbors that did not respond.

19. When the `distribute-list 1 in serial 0/0` command is used, which EIGRP routing updates would be permitted?

- Routing updates that are received on the serial 0/0 interface and permitted by ACL 1.
- Routing updates that are received on the serial 0/0 interface and permitted by prefix-list 1.
- Routing updates that are received on the serial 0/0 interface and permitted by route-map 1.
- Routing updates that are received on the serial 0/0 interface and permitted by offset-list 1.

Explanation: EIGRP supports filtering of routes as they are received or advertised from an interface. Filtering of routes can be matched against ACLs (named or numbered), IP prefix lists, route maps, and gateway IP addresses. It is accomplished with the distribute-list {acl-number | acl-name | prefix prefix-list-name | route-map route-map-name | gateway prefix-list-name} {in | out} [interface-id] command.

20. Refer to the exhibit. What can the field engineer conclude about the EIGRP authentication between RouterA and RouterB?



- **Authentication will succeed and EIGRP updates can be exchanged.**
- Authentication will fail because the key chain names do not match.
- Authentication will fail because the key chain names must match the router names.
- Authentication will fail because only one key is configured.

Explanation: Authentication ensures that only authorized routers are eligible to become EIGRP neighbors. A precomputed password hash is encrypted by using a MD5 authentication and it is included with all EIGRP packets. The hash is computed using the key number and the key string. The receiving router decrypts the hash. If the passwords do not match for a packet, the routers will not become neighbors. In this scenario, the key number and the key string are the same on both routers. Therefore, they will become neighbors.


21. In which situation would a company implement an OSPF NSSA?

- when external routes need to connect to an OSPF area
- **when one or more non-OSPF networks connect to an OSPF stub area**
- when external routes need to be suppressed throughout all of the OSPF areas
- when one or more non-OSPF networks need to connect to the OSPF backbone

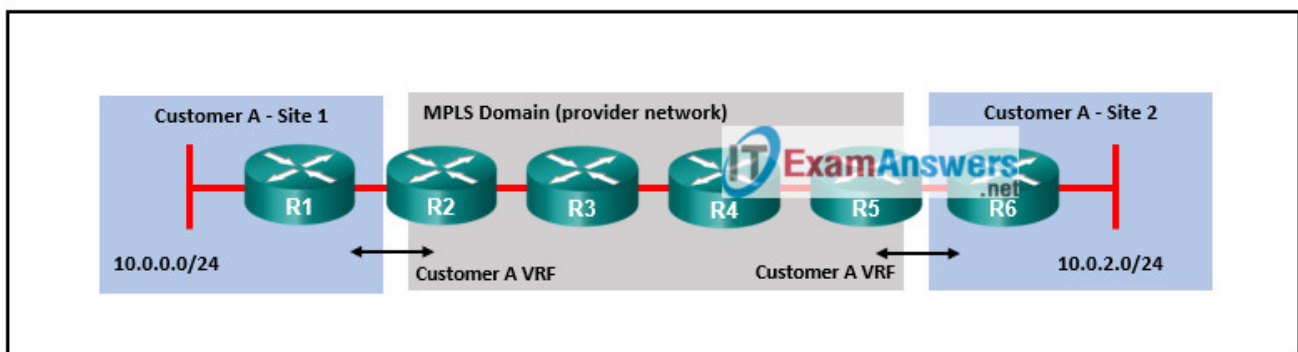
Explanation: When an OSPF not-so-stubby area (NSSA) is implemented, external routes are allowed to travel through a stub area that has other external routes prohibited. The way this is accomplished is through the use of type 7 LSAs which are used to carry the external routes

across the stub area, but still keep other type 5 external routes out of the area. When the type 7 LSAs reach the ABR for the stub area, the ABR changes these LSAs to type 5s for transmission through the rest of the OSPF areas that allow type 5 LSAs.

22. Match the LSR component with the description. (Not all options are used.)

FIB		makes forwarding decisions on labeled packets <input style="width: 100%; background-color: #e6f2ff;" type="text" value="LFIB"/>
LIB		the cumulative label path through an MPLS domain <input style="width: 100%; height: 30px;" type="text"/>
LDP		makes forwarding decisions on unlabeled packets <input style="width: 100%; background-color: #e6f2ff;" type="text" value="FIB"/>
LFIB		stores label information <input style="width: 100%; background-color: #e6f2ff;" type="text" value="LIB"/>
		generates and exchanges labels <input style="width: 100%; background-color: #e6f2ff;" type="text" value="LDP"/>

23. Refer to the exhibit. Which two routers would perform penultimate hop popping? (Choose two.)



- R5
- **R3**
- R6
- R1
- R2
- **R4**

Explanation: With penultimate hop popping the last intermediate LSR removes the label and then forwards the unlabeled packet to the edge PE router. In this example routers R3 and R4 are intermediate routers. They will perform penultimate hop popping as they forward packets to the edge PE routers R2 and R5.

24. Which three protocols are involved in the establishment of an IPsec VPN tunnel? (Choose three.)

- **Authentication Header**
- Generic Routing Encapsulation
- **Internet Key Exchange**
- Tunnel Profile
- **Encapsulating Security Payload**
- Secure Socket Layer

Explanation: IPsec is composed of security protocols, security associations, and key management functions. Authentication header (AH) and encapsulating security payload (ESP) are security protocols. Internet key exchange (IKE) is a key management protocol.

25. A network administrator is teaching a junior engineer about MPLS Layer 3 VPNs. The administrator is explaining that a label stack is required for an MPLS domain to forward traffic. Which statement is accurate about a label stack?

- The LDP label is used by the egress router to determine customer specifics about the packet.
- **VPN labels are learned from PE routers over the MP-IBGP peering.**
- When the IP packet leaves the egress PE router, the VPN and LDP labels are attached to the IP packet.
- There are two labels attached to the IP packet; the first one is an LDP label, and the second one is the VPN label.

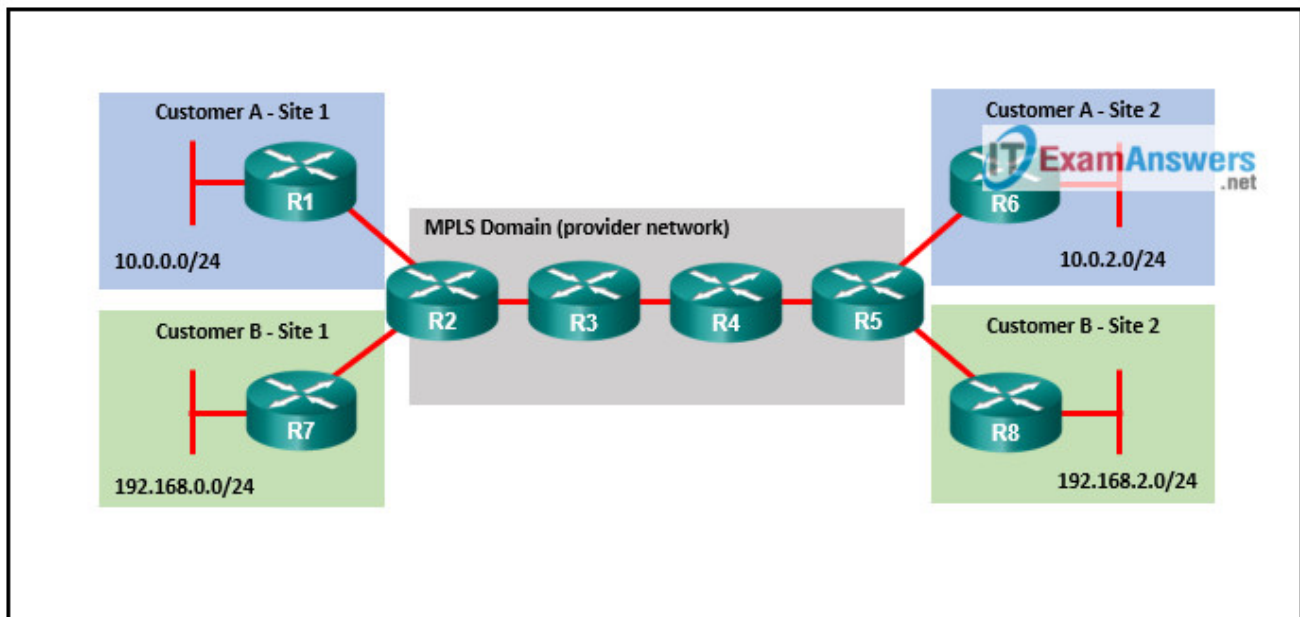
Explanation: Specifically, two labels are required for traffic to be successfully forwarded through the MPLS domain. The VPN label is the first label attached to the packet, and the LDP label is the second. The PE router attaches both labels when the IP packet arrives at the ingress PE router. The egress router uses the VPN label to determine customer specifics about the packet and what should be done with it. The LDP label is used for label switching from PE to PE in the MPLS domain. VPN labels are learned from PE routers over the MP-IBGP peering.

26. An administrator has chosen IPsec to encrypt DMVPN tunnels used to connect remote sites. How does the IPsec AH protocol differ from the IPsec ESP protocol?

- The AH protocol supports the DES and 3DES algorithms, but the ESP protocol only supports the AES algorithm.
- **The AH protocol does not support encryption, but the ESP protocol does.**
- The AH protocol does not support authentication, but the ESP protocol does.
- The AH protocol uses MD5, while the ESP protocol uses the SHA algorithm.

Explanation: IPsec uses two protocols to provide data integrity and confidentiality, the IP authentication header (AH) and the encapsulating security payload (ESP). AH provides integrity and authentication but does not provide encryption. AH ensures that the original data packet has not been modified during transport but it does not encrypt data to ensure it is viewable only by authorized users. ESP provides confidentiality, integrity, and authentication. ESP maintains data confidentiality by encrypting the payload and adding a new set of headers during transport across a public network.

27. Refer to the exhibit. What is used on router R2 and router R5 to isolate the routes of customer A and B?



- BGP communities
- **VRF instances**
- DMVPN tunnels
- MP-BGP address families

Explanation: When multiple customers are supported, a VRF instance needs to be created for each customer on the PE routers. This will isolate customer information and traffic from other customers.

28. A network administrator is configuring the tunnel interfaces for an IPv6 DMVPN implementation where IPv6 is going to be the tunneling protocol. What type of IPv6 address should the administrator configure on the tunnel interfaces?

- anycast
- unique local
- **link-local**
- unique global

Explanation: Because IPv6 routing protocols use IPv6 link-local addresses for neighbor discovery, IPv6 DMVPN configuration must assign IPv6 link-local addresses on the tunnel interfaces.

29. Match the secure transport element to the description. (Not all options are used.)

confidentiality	ensures user activity information is collected and logged once they are authenticated
integrity	ensures data is viewable to only authorized users
availability	ensures data can only be modified by authorized users and has not been changed
	ensures that the network is always available to allow the secure transport of data

30. What happens to an unlabeled IP packet that arrives at an LSR router and the intended outgoing interface is MPLS-enabled?

- **A label is added and the packet is forwarded.**
- The packet is sent to the LFIB for a forwarding decision.
- The packet is forwarded without a label to the next hop LSR.
- An error code is sent to the source CE router and the packet is dropped.

Explanation: The data plane of an LSR consists of an IP forwarding table (FIB) and a label forwarding table (LFIB). The FIB makes forwarding decisions for unlabelled packets. The LFIB makes forwarding decisions for labeled packets. When an unlabeled IP packet arrives on an interface, if the outgoing interface is MPLS enabled, a label is added and the packet forwarded out the MPLS-enabled interface.

31. A network administrator reviewing the output of the show dmvpn command notes that the tunnel is in the IKE state. What is indicated by the IKE state?

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

Explanation: The IKE state indicates that IPsec has not successfully established an IKE session over the tunnel.

32. What is an IPsec protocol that provides data confidentiality and authentication for IP packets?

- IKE
- RSA
- **ESP**
- AH

Explanation: AH (Authentication Header) does not provide confidentiality for IP packets but rather provides data authentication and integrity. ESP (Encapsulating Security Payload) does provide confidentiality and authentication by encrypting the IP packet. RSA is a cryptosystem used in IKE (Internet Key Exchange) .

33. A network administrator is assigned the task of configuring front door VRF on a spoke router. What is the first configuration step the administrator needs to perform?

- Associate the FVRF instance with the DMVPN tunnel.
- **Create the FVRF instance.**
- Associate an interface with the VRF instance.
- Initialize the IP address family.

Explanation: There are five configuration steps to perform when configuring FVRF:

- Create the FVRF instance.
- Initialize the IP address family.
- Associate an interface with the VRF instance.
- Assign an IP address to the interface.
- Associate the FVRF instance with the DMVPN tunnel.

34. Refer to the exhibit. Router R1 is configured as shown. An administrative user attempts to use Telnet from router R2 to R1 using the interface IP address 10.10.10.1. However, Telnet access is denied. Which conclusion can be drawn from this scenario?

```
R1(config)# enable algorithm-type scrypt
R1(config)# enable secret 9 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
R1(config)# username Admin algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local enable
R1#

R2# telnet 10.10.10.1
Trying 10.10.10.1 ... Open
User Access Verification

Username: admin
Password: Str0ngPa55w0rd

% Authentication failed

[Connection to 10.10.10.1 closed by foreign host]
R2#
```

- The vty lines must be configured with the login authentication default command.
- **The password was mistyped.**
- The administrative user should use the username Admin .
- The aaa local authentication attempts max-fail command must be set to 2 or higher.

Explanation: The AAA authentication is defined with the list default with two methods. The first method is to use the local database and the second method is to use the enable password. The local keyword indicates that the username and password are not case-sensitive, so the username can be typed as “admin”. The problem is that the password is “Strong5rPa55word” and the user typed “StrongPa55word”.

35. 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.

36. Which IPv6 First-Hop Security feature can block IPv6 traffic if this traffic is from an unknown origin?

- RA Guard
- **Source Guard**
- DHCPv6 Guard
- IPv6 ND inspection/snooping

Explanation: IPv6 Source Guard is a Layer 2 snooping interface feature for validating the source of IPv6 traffic. If the traffic arriving on an interface is from an unknown source, IPv6 Source Guard can block it.

37. Which mitigation technique would prevent rogue servers from providing false IPv6 configuration parameters to clients?

- **enabling DHCPv6 Guard**
- enabling RA Guard
- implementing port security on edge ports
- disabling CDP on edge ports

Explanation: DHCPv6 Guard is a feature designed to ensure that rogue DHCPv6 servers are not able to hand out addresses to clients, redirect client traffic, or starve out the DHCPv6 server and cause a DoS attack. DHCPv6 Guard requires a policy to be configured in DHCP Guard configuration mode, and DHCPv6 Guard is enabled on an interface-by-interface basis.

38. A network administrator is configuring a prefix list with the command

```
ipv6 prefix-list IPV6-1 seq 5 permit 2001:db8:abcd:20::/59 ge 62
```

Which network matches the prefix match specification?

- 2001:db8:ab:20::/62
- 2001:db8:abcd:2::/59
- 2001:db8:abcd:36::/62
- 2001:db8:abcd:60::/64

Explanation: The prefix matching logic works exactly the same for IPv6 networks as for IPv4 networks. The third hexadecimal group of the match specification is 0x0020, which is 00000000 00100000 in binary. To match /59 prefix length, the third hexadecimal group of a network must match 00000000 001, that is, between 0x0020 and 0x003F. The prefix length must be /62 or higher.

39. Which network prefix matches the prefix match pattern 2001:db8:cafe::/48 ge 48 le 52

- 2001:db80:cafe:12::/52
- **2001:db8:cafe:1001:/48**
- 2001:db8:feed::/48
- 2001:db8::/52

Explanation: To match the criteria in the given example, the prefix must have the same 48 high-order bits as 2001:db8:cafe::/48 and also have a prefix length that is equal to or greater than /48 and also less than or equal to /52.

40. A network administrator wants to verify the number of packets that have conformed to a specific class map used for CoPP. Which command should the administrator use?

- show class-map
- show access-list
- show policy-map
- **show policy-map control-plane**

Explanation: The **show policy-map control-plane** command provides a large amount of information such as the applied policy map, the class maps in the order they will be applied, the match conditions of the class maps, and the policies that are applied to the traffic that is matched. In addition, values for cir, bc, and be, as well the number of conformed, exceeded, and violated packets can be verified.

41. Which two UDP port numbers may be used for server-based AAA RADIUS authentication? (Choose two.)

- **1812**

- **1645**
- 1813
- 1646
- 49

Explanation: RADIUS authentication and accounting utilize the following UDP port numbers:
 UDP port 1645 or 1812 for authentication
 UDP port 1646 or 1813 for accounting
 TACACS+ uses TCP port 49.

42. A junior network engineer needs to configure uRPF on a Cisco router interface to eliminate spoofed IP packets on a network. Which command should be used to configure uRPF mode when using asymmetric routing?

- **ip verify unicast source reachable-via any**
- ip verify unicast source reachable-via rx
- ip verify unicast source reachable-via rx allow-self-ping
- ip verify unicast source reachable-via rx allow-default

Explanation: When uRPF is configured on an interface, the uRPF mode should be chosen according to the type of routing. With asymmetric routing, a different path ends up being used for return traffic. Where asymmetric routing occurs, the uRPF loose mode should be configured. The **ip verify unicast source reachable-via any** command configures uRPF in loose mode.

43. A network administrator is configuring a prefix list with the command

```
ipv6 prefix-list IPV6-1 seq 5 permit 2001:db8:abcd:30::/60 ge 61 le 63
```

Which two networks match the prefix match specification? (Choose two.)

- 2001:db8:abcd:30::/60
- **2001:db8:abcd:34::/62**
- 2001:db8:abcd:20::/62
- **2001:db8:abcd:36::/63**
- 2001:db8:abcd:60::/64

Explanation: The prefix matching logic works the same for IPv6 networks as for IPv4 networks. The fourth hexadecimal group of the match specification is 0x0030, which is 00000000 00110000 in binary. To match /60 prefix length, the fourth hexadecimal group of a network must be between 00000000 00110000 and 00000000 00111111, that is, between 0x0030 and 0x003F. The prefix length must be between /61 and /63.

44. Which is the correct order of the four steps to configure CoPP on a Cisco router?

- 1) Configure extended ACLs to identify specific granular traffic.**
- 2) Configure the class map to define interesting traffic.**
- 3) Configure a policy map to apply actions to the identified traffic.**
- 4) Configure a service policy to identify which interface should be activated for the service.**

- 1) Configure a service policy to identify which interface should be activated for the service.
- 2) Configure extended ACLs to identify specific granular traffic.
- 3) Configure the class map to define interesting traffic.
- 4) Configure a policy map to apply actions to the identified traffic.

- 1) Configure extended ACLs to identify specific granular traffic.
- 2) Configure the class map to define interesting traffic.
- 3) Configure a service policy to identify which interface should be activated for the service.
- 4) Configure a policy map to apply actions to the identified traffic.

- 1) Configure a policy map to apply actions to the identified traffic.
- 2) Configure a service policy to identify which interface should be activated for the service.
- 3) Configure extended ACLs to identify specific granular traffic.
- 4) Configure the class map to define interesting traffic.

Explanation: Control Plane Policing (CoPP) varies based on IOS version and platform version. Therefore, there are general elements that apply to all versions. When configuring CoPP, the steps are as follows:

Create ACLs to identify the traffic.

Create class maps to define a traffic class.

Create policy maps to define a service policy.

Apply the service policy to the control plane.

45. Which IPv6 First-Hop security feature learns and populates the binding table for stateless autoconfiguration addresses?

- DHCPv6 Guard
- **IPv6 neighbor discovery inspection**
- RA Guard
- Source Guard

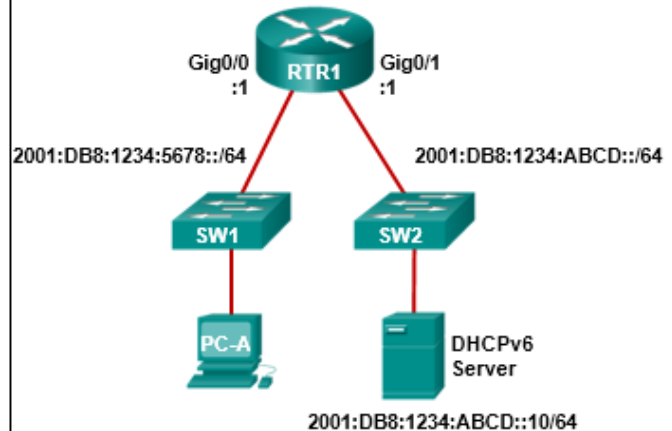
Explanation: IPv6 neighbor discovery inspection/snooping is a feature that learns and populates the binding table for stateless autoconfiguration addresses. It analyzes ND (neighbor discovery) messages and places valid bindings in the binding table and drops all messages that do not have valid bindings.

46. Refer to the exhibit. PC-A is unable to receive an IPv6 address from the stateful DHCPv6 server. What is the problem?

```

RTR1# show running-config
<output omitted>
!
interface GigabitEthernet0/0
  no ip address
  duplex auto
  speed auto
  ipv6 address 2001:DB8:1234:5678::1/64
  ipv6 enable
  ipv6 nd managed-config-flag
!
interface GigabitEthernet0/1
  no ip address
  duplex auto
  speed auto
  ipv6 address 2001:DB8:1234:ABCD::1/64
  ipv6 enable
  ipv6 dhcp relay destination 2001:DB8:1234:ABCD::10
GigabitEthernet0/1
<output omitted>

```



- The `ipv6 dhcp relay` command should be applied to interface Gig0/0.
- The `ipv6 nd managed-config-flag` should be applied to interface Gig0/1.
- The `ipv6 dhcp relay` command should use the link-local address of the DHCP server.
- The `ipv6 nd managed-config-flag` command should be `ipv6 nd other-config-flag`.

Explanation: The **ipv6 dhcp relay** command must be applied to the interface where the clients are located. The **ipv6 dhcp relay** command can use either the link-local or global unicast address of the DHCPv6 server, or even a multicast address. The **ipv6 nd managed-config-flag** indicates to the clients that they should use stateful DHCPv6 and is also applied to the interface where the clients are located.

47. Refer to the exhibit. A network administrator is implementing stateful DHCPv6 operation for the company. However, the clients are not using the prefix and prefix-length information that is configured in the DHCP pool. The administrator issues a `show ipv6 interface` command. What could be the cause of the problem?

```

R1# show ipv6 interface gigabitEthernet 0/0
GigabitEthernet0/0 is up, line protocol is up
  IPv6 is enabled, link-local address is
FE80::523D:E5FF:FEAA:COA0
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:DB8:ACAD:1::1, subnet is 2001:DB8:ACAD:1::/64

<output omitted>

  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
  Hosts use DHCP to obtain other configuration.
R1#

```

- No virtual link-local address is configured
- The Duplicate Address Detection feature is disabled
- The router is configured for SLAAC DHCPv6 operation
- **The router is configured for stateless DHCPv6 operation**

Explanation: The router is configured for stateless DHCPv6 operation, which is shown by the last two lines of the show command output. Hosts will configure their IPv6 addresses by using the prefix information that is provided by RA messages. They will also obtain additional configuration information from a DHCPv6 server. The “No virtual link-local address” option and the “Duplicate Address Detection” option are irrelevant to DHCP configuration. Option “SLAAC configuration” is incorrect because by definition SLAAC will use only the information that is provided by RA messages to configure IPv6 settings.

48. A network administrator is configuring SSH on a router. When verifying the configuration, the administrator notices that the SSH connection requests fail, but the Telnet connection requests from the same workstation are successful. Which two parts of the router configuration should be checked to try to locate the problem? (Choose two.)

- **The transport input command is incorrect on the vty lines.**
- **An extended ACL that is referencing the port argument for SSH is misconfigured.**
- The ip access-class command is missing.
- The password is misconfigured on the console line.
- A standard ACL is possibly blocking the workstation from access to the router.

Explanation: There are several possible configuration issues to account for why SSH connections are failing. Among them are (1) the VTY lines should accept SSH connections by the transport input all or transport input ssh command; and (2) if there is an extended ACL to protect access to the vty lines, the port (either by the word ssh or the numeric number) should be included in the permit ACE. Because Telnet works, the connectivity to the vty line can be established, and thus the option that the standard ACL is blocking the workstation from access to the router does not apply. The option that the ip access-class command is missing does not apply because if the command is missing, no ACL will be applied to filter the access to vty lines. (Although the statement might be true in the router configuration, it is not a reason why SSH is not successful.) Finally the option that the password is misconfigured on the console line does not apply because SSH connects to vty lines, not to the console line.

49. Refer to the exhibit. Which two conclusions can be drawn from the syslog message that was generated by the router? (Choose two.)

```
Mar 01 07:23:03.2323: %LINEPROTO-5-UPDOWN: Line protocol on Interface  
Serial0/0, changed state to up
```

- This message resulted from an unusual error requiring reconfiguration of the interface
- **This message indicates that service timestamps have been configured**
- This message indicates that the interface changed state five times
- **This message is a level 5 notification message**
- This message indicates that the interface should be replaced

Explanation: The message is a level 5 notification message as shown in the %LINEPROTO-5 section of the output. Messages reporting the link status are common and do not require replacing the interface or reconfiguring the interface. The date and time displayed at the beginning of the message indicates that service timestamps have been configured on the router.

50. Refer to the exhibit. A SNMP manager has IP address 172.16.1.120. The SNMP manager is unable to change configuration variables on the R1 SNMP agent. What could be the problem?

```
R1(config)# snmp-server community snmpenable ro ACL_SNMP  
R1(config)# snmp-server location Not_Here  
R1(config)# snmp-server contact John Doe  
R1(config)# snmp-server host 172.16.1.1 version 2c snmpenable  
R1(config)# snmp-server enable traps  
R1(config)# ip access-list standard ACL_SNMP  
R1(config-std-nacl)# permit 172.16.1.0 0.0.0.255  
R1(config-std-nacl)# deny any
```

- The ACL of ACL_SNMP has not been implemented on an interface yet.
- The SNMP agent should have traps disabled.
- The IP address of the SNMP manager must be 172.16.1.1.

- **The SNMP agent is not configured for write access.**

Explanation: Because the SNMP manager is able to access the SNMP agent, the problem is not related to the ACL configuration. The SNMP agent configuration should have an access level configured of rw to support the SNMP manager set requests. The SNMP manager cannot change configuration variables on the SNMP agent R1 with only ro access. The IP address of the SNMP manager does not have to be 172.16.1.1 to make changes to the SNMP agent. The SNMP agent does not have to have traps disabled.

51. 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.

52. A host PC is attempting to lease an address through DHCP. What message is sent by the server to let the client know it is able to use the provided IP information?

- DHCPDISCOVER
- DHCPOFFER
- DHCPREQUEST
- DHCPACK
- DHCPNACK

Explanation: When a host uses DHCP to automatically configure an IP address, the typically sends two messages: the DHCPDISCOVER message and the DHCPREQUEST message. These two messages are usually sent as broadcasts to ensure that all DHCP servers receive them. The servers respond to these messages using DHCPOFFER, DHCPACK, and DHCPNACK messages, depending on the circumstance.

53. A network technician opens PuTTY to connect to a Cisco switch. The technician sets PuTTY with the IP address of the switch and port 23. However, connections to the switch are always declined. What is a possible cause for this issue?

- **The transport input ssh command has been configured on vty lines.**
- Only Telnet is allowed to connect to the switch.
- The domain name of the switch should be used in PuTTY.
- An ACL is applied on the console port that blocks the PC that the technician uses.

Explanation: Telnet uses TCP port 23 and SSH uses TCP port 22. If vty lines are configured with the **transport input ssh** command, only SSH connections are allowed.

54. Which two types of probes can be configured to monitor traffic by IP SLA within a network environment? (Choose two.)

- **voice quality scores**
- website upload time
- SNMP traps
- **packet loss**
- syslog messages

Explanation: IP SLA is a tool that allows for the continuous monitoring of various aspects of the network. Different types of probes can be configured to monitor traffic within a network environment:

Delay

Jitter (directional)

Packet loss (directional)

Packet sequencing (packet ordering)

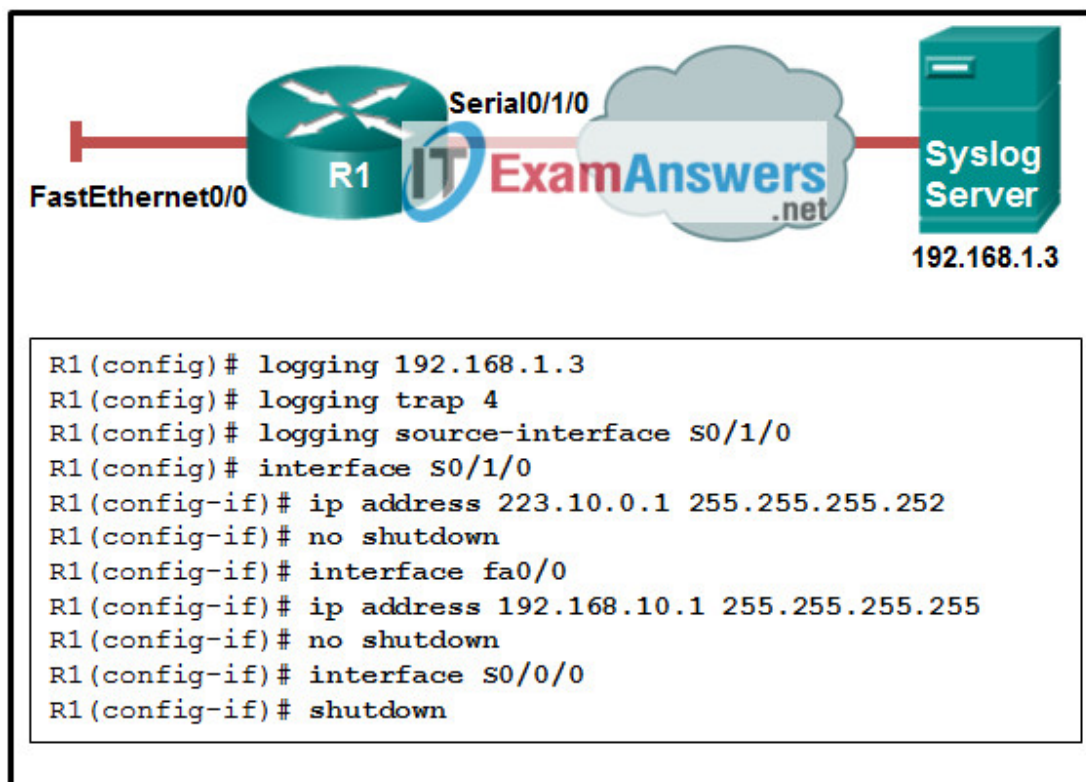
Path (per hop)
Connectivity (directional)
Server or website download time
Voice quality scores

55. A network administrator has verified that timestamps are not appearing with syslog messages on a router. What is the most likely reason for this?

- The router has the wrong time set, according to the output of the show clock command.
- The terminal monitor command was not issued on the router.
- **The no service timestamps command was executed on the router.**
- Syslog was not correctly configured.

Explanation: When troubleshooting, it is important that syslog generates the right type of messages at the right time. If no timestamps are included with either log messages or debug messages, it is because the **no service timestamps** command has been executed.

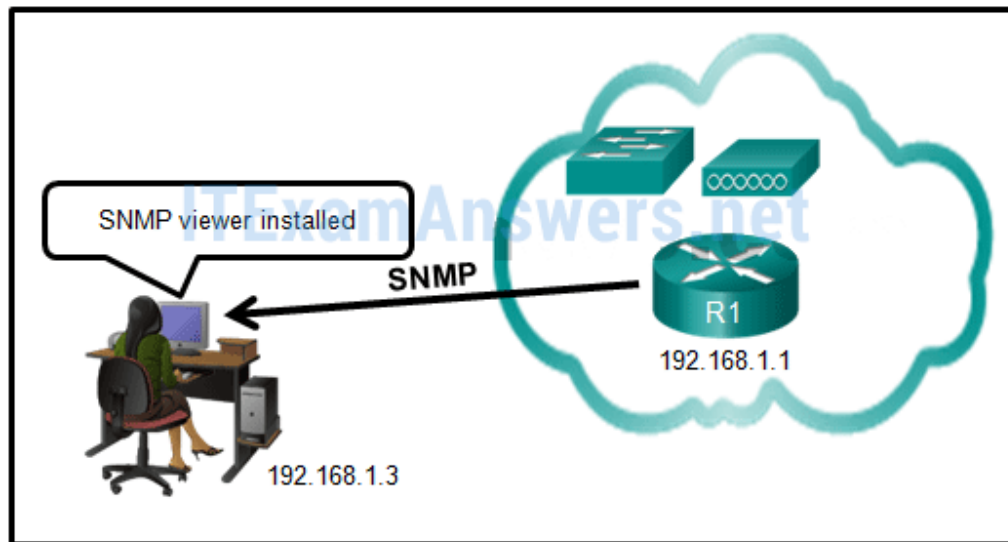
56. Refer to the exhibit. A network administrator has configured router R1 to send syslog messages to the syslog server. Why is the syslog server unable to receive any logging messages?



- The IP address of the server is not configured properly.
- **The source interface is not configured correctly.**
- The syslog server should be directly connected.
- The logging level should be set to 5.

Explanation: The source interface that is configured to send the messages to the server is not configured and is shut down. The logging level has no influence on the ability to send or receive syslog messages. The server IP address is set properly, and the syslog server does not need to be directly connected to the equipment to be monitored.

57. 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.

58. A company uses the method SLAAC to configure IPv6 addresses for the workstations of the employees. A network administrator configured the IPv6 address on the LAN interface of the router. The interface status is UP. However, the workstations on the LAN segment did not obtain the correct prefix and prefix length. What else should be configured on the router that is attached to the LAN segment for the workstations to obtain the information?

- R1(config)# ipv6 dhcp pool
- R1(config-if)# ipv6 enable
- R1(config)# ipv6 unicast-routing
- R1(config-if)# ipv6 nd other-config-flag

Explanation: A PC that is configured to use the SLAAC method obtains the IPv6 prefix and prefix length from a router. When the PC boots, it sends an RS message to inform the routers that it needs the information. A router sends an RA message that includes the required information. For a router to be able to send RA messages, it must be enabled as an IPv6 router by the unicast ipv6-routing command in global configuration mode. The other options are not used to enable IPv6 routing on a router.

59. Refer to the exhibit. A SNMP manager is using the community string of snmpenable and is configured with the IP address 172.16.10.1. The SNMP manager is unable to read configuration variables on the R1 SNMP agent. What could be the problem?

```
R1(config)# snmp-server community snmpenable rw ACL_SNMP
R1(config)# snmp-server location Over_There
R1(config)# snmp-server contact Jane_Doe
R1(config)# snmp-server host 172.16.10.1 version 2c snmpenable2
R1(config)# snmp-server enable traps
R1(config)# ip access-list standard ACL_SNMP
R1(config-std-nacl)# permit 172.16.10.10 0.0.0.0
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
R1(config)# interface FastEthernet 0/1
R1(config-if)# ip access-group ACL_SNMP in
R1(config-if)# exit
R1(config)#
```



- The incorrect community string is configured on the SNMP manager.
- The community of snmpenable2 is incorrectly configured on the SNMP agent.
- **The ACL is not permitting access by the SNMP manager.**
- The SNMP agent is not configured for read-only access.

Explanation: ACLs are used to prevent SNMP messages from going beyond the required devices. The ACL_SNMP is permitting only the host IP of 172.16.10.10 to access the SNMP agent. The actual IP of the SNMP manager is 172.16.10.1. The SNMP agent is configured for

read-write access for reading and setting variables. The community string of **snmpenable2** is only affecting connectivity for trap messages.

60. A network student intern is asked to clean the system settings and upgrade the IOS on a Cisco router. The student uses a Windows 10 laptop and a rollover cable to connect to the console port of the router. The student powers on the router and opens the TeraTerm program. However, the program does not receive any response from the router. What are two possible causes for this problem? (Choose two.)

- The IP address was misconfigured in TeraTerm.
- **The communication settings were misconfigured on TeraTerm.**
- The wrong password was used to connect to the console port.
- The student entered an incorrect enable password.
- **The wrong COM port was selected in TeraTerm.**

Explanation: When troubleshooting console port access, there are a few items to look for:

Has the correct COM port been selected in the terminal program?

Are the settings of the terminal program configured correctly?

Is a line password used to authenticate to the console?

Are a local username and password used to authenticate to the console?

In this case, because there is no response from the router after it is powered on, the problem is most likely that the wrong COM port was selected or the communication settings were misconfigured.

61. A network administrator has configured a router for stateless DHCPv6 operation. However, users report that workstations are not receiving DNS server information. Which two router configuration lines should be verified to ensure that stateless DHCPv6 service is properly configured? (Choose two.)

- The domain-name line is included in the `ipv6 dhcp pool` section.
- The dns-server line is included in the `ipv6 dhcp pool` section.
- The `ipv6 nd other-config-flag` is entered for the interface that faces the LAN segment.
- The address prefix line is included in the `ipv6 dhcp pool` section.
- The `ipv6 nd managed-config-flag` is entered for the interface that faces the LAN segment.

Explanation: To use the stateless DHCPv6 method, the router must inform DHCPv6 clients to configure a SLAAC IPv6 address and contact the DHCPv6 server for additional configuration parameters, such as the DNS server address. This is done through the command **ipv6 nd other-config-flag** entered at the interface configuration mode. The DNS server address is indicated in the **ipv6 dhcp pool** configuration.

62. Refer to the exhibit. From what location have the syslog messages been retrieved?

```
R1# show logging | include changed state to up
*Jun 12 17:46:26.143: %LINK-3-UPDOWN: Interface
GigabitEthernet0/1, changed state to up
*Jun 12 17:16:26.143: %LINK-3-UPDOWN: Interface Serial0/0/1,
changed state to up
*Jun 12 17:25:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/1, changed state to up
*Jun 12 17:55:27.263: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Serial0/0/1, changed state to up
*Jun 12 20:28:43.427: %LINK-3-UPDOWN: Interface
GigabitEthernet0/0, changed state to up
```

```
R1# show logging
<output omitted>
Buffer logging: level debugging, 32 messages logged, xml
disabled, filtering disabled
Exception Logging: size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
```

- syslog server
- syslog client
- **router RAM**
- router NVRAM

Explanation: The output is captured from a virtual terminal connection on a router. The syslog messages are stored in the RAM of the monitored router.

63. 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 RADIUSRV
  address ipv4 10.0.10.51 auth-port 1812 acct-port 1813
  key RADIUSPASSWORD
aaa group server radius RADIUSMETHOD
  server name RADIUSRV
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].

64. Which IPv6 First-Hop Security feature is used to block unwanted advertisement messages from unauthorized routers?

- IPv6 ND inspection
- DHCPv6 Guard
- Source Guard
- **RA Guard**

Explanation: RA Guard is a feature that analyzes RAs and can filter out unwanted RAs from unauthorized devices. RA requires a policy to be configured in RA Guard policy configuration mode, and enabled on an interface-by-interface basis.

65. An administrator is configuring an extended ACL for BGP route selection. Which ACE should the administrator issue to permit only 10.0.0.0 networks with a /16 through /32 prefix?

- permit ip 10.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255
- permit ip 10.0.0.0 0.0.255.255 255.255.255.0 0.0.0.255
- permit ip 10.0.0.0 0.0.0.255 0.0.0.255 255.255.255.0
- **permit ip 10.0.0.0 0.0.255.255 255.255.0.0 0.0.0.255**

Explanation: When an ACL is used for BGP network selection, the ACE source field matches against the network portion of the network, and the destination field matches against the network mask. In this example, the ACE source field and wildcard-mask of 10.10.0.0 0.0.255.255 will match the first 16 bits of network 10.0.0.0. The destination field and wildcard-mask of 255.255.0.0 0.0.255.255 will match prefix lengths of /16 through /32.

66. Refer to the exhibit. The administrator can ping the So/o/1 interface of RouterB but is unable to gain Telnet access to the router by using the password cisco123. What is a possible cause of the problem?

- AAA authorization is not configured.
- The administrator does not have enough rights on the PC that is being used.
- **The administrator has used the wrong password.**
- The wrong vty lines are configured.

Explanation: To authenticate and log in using a Telnet vty line, the network administrator is required to use the local username and password that has been configured on the local router. This is evidenced by the application of the **aaa authentication login telnet local-case** command. The administrator must use a capital C in Cisco123 to match the applied configuration.

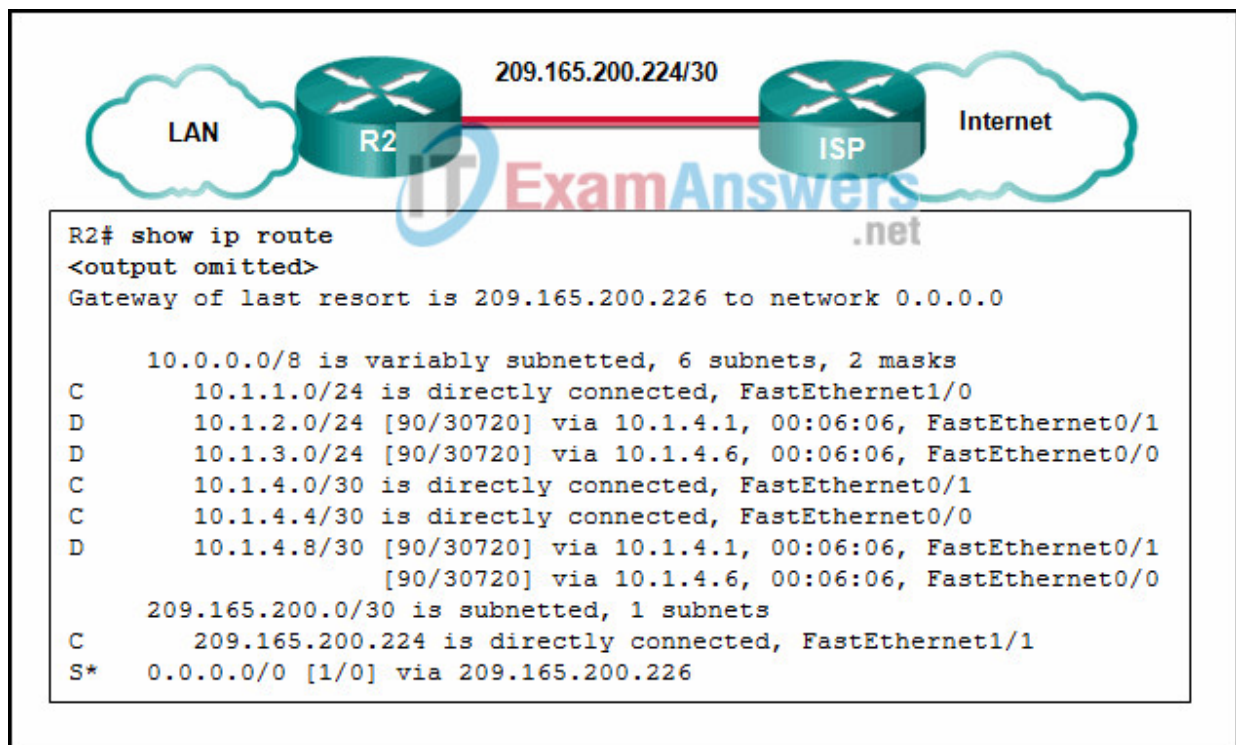
67. Which command, if applied on an OSPF router, would give a Gigabit Ethernet interface a lower cost than a Fast Ethernet interface?

- **(config-router)# auto-cost reference-bandwidth 1000**

- (config-if)# bandwidth 100
- (config-if)# ip ospf priority 1
- (config-if)# ip ospf cost 100

Explanation: OSPF uses the formula; $\text{Cost} = 100,000,000 / \text{bandwidth}$. Because OSPF will only use integers as cost, any bandwidth of 100 Mb/s or greater will all equal a cost of 1. To change this behavior, a new reference bandwidth can be configured. The new reference bandwidth will need to be larger than 100,000,000. In this case it needs to be 1,000,000,000. This is accomplished with the command `auto-cost reference-bandwidth 1000`, which means multiply the unit Mb/s by 1000. The result is 1,000,000,000.

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




- 10.1.0.0/16
- **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.

69. 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 and the

path through the neighbor 1.1.1.1 is the best-path. Which configuration step will allow the administrator to change the best path to use neighbor 3.3.3.3?

```
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
```



- Set the multi-exit discriminator to 75 for the path through 3.3.3.3.
- Set the origin code to i for the path through 3.3.3.3.
- **Set the local preference to 200 for the path through 3.3.3.3.**
- Change the metric value from 131072 to 32768 for the path through 3.3.3.3.

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.

70. The show ip eigrp topology command output on a router displays a successor route and a feasible successor route to network 192.168.1.0/24. In order to improve network convergence, what does EIGRP do when the primary route to this network fails?

- The router sends query packets to all EIGRP neighbors for a better route to network 192.168.1.0/24.
- DUAL immediately recomputes the algorithm to calculate the next backup route.
- Packets that are destined for network 192.168.1.0/24 are sent out the default gateway instead.
- **The backup route to network 192.168.1.0/24 is installed in the routing table.**

Explanation: When EIGRP detects that it has lost a successor for a path, the feasible successor instantly becomes the successor route, providing a backup route. This route is installed in the routing table and the router sends out an update packet for that path because of the new EIGRP path metrics.

71. Refer to the exhibit. A network engineer has issued the verification command while troubleshooting a routing loop on the network. What is the error in the configuration?

```
BR1# show running-config

ip prefix-list TAG_10.44.0.0 seq 5 permit 10.44.100.0/24
!
route-map REDIS_EIGRP_TO_OSPF permit 10
  match ip address prefix-list 10.44.100.0
  set tag 10
route-map REDIS_EIGRP_TO_OSPF permit 20
!
router ospf 10
  redistribute eigrp 44 subnets route-map REDIS_EIGRP_TO_OSPF
!
<output omitted>
```

- The route-map is dropping all other routes that do not match the prefix list TAG_10.44.100.0.
- **The match ip address command refers to the incorrect prefix list.**
- The redistribute command is configured to filter routes using the route map instead of the prefix list.
- The route-map sequence 20 is missing the match and set statements.

Explanation: Router BR1 is configured to set a tag of 10 for the routes identified by the prefix list of 10.44.100.0. However, the prefix list being referenced is incorrect and does not exist.

72. Refer to the exhibit. An administrator is trying to configure R1 to run OSPFv3 but the neighbor adjacency is not forming with the router connected to Fa0/o. What is the cause of the problem?

<pre> R1# show ip interface brief Interface IP-Address OK? Method Status Protocol FastEthernet0/0 unassigned YES unset up up FastEthernet0/1 unassigned YES unset administratively down down Serial0/0/0 unassigned YES unset administratively down down Serial0/0/1 unassigned YES unset administratively down down </pre>		<pre> R1# show running-config <output omitted> interface FastEthernet0/0 no ip address duplex auto speed auto ipv6 address 2001:DB8:C5C0:1::1/64 ipv6 ospf 1 area 0 <output omitted> ipv6 router ospf 1 log-adjacency-changes default-information originate <output omitted> </pre>	
		<pre> R1# show ipv6 ospf interface fa0/0 %OSPFv3: OSPF not enabled on FastEthernet0/0 </pre>	

- **No router ID has been configured.**
- FastEthernet0/0 has been configured as a passive interface.
- A link-local address has not been configured on interface FastEthernet0/0.
- The OSPF process ID and area values are backwards in the interface configuration.

Explanation: The output of show ipv6 ospf interface fa0/0 shows that OSPFv3 is not enabled on the interface even though the command is in the running configuration. This is because no router ID has been configured on this router. The router ID in OSPFv3 is a 32 bit number, similar to the ID in OSPFv2. If the router ID is not manually specified then an IPv4 address from one of the interfaces is used instead. This router has no IPv4 addresses configured on it so a router ID cannot be automatically chosen. The router-id command must be configured under ipv6 router ospf 1 in order to fix this problem.


73. A network administrator is configuring a BGP router with the neighbor 10.12.1.2 maximum-prefix 20 75 command. What will happen when the peer at 10.12.1.2 advertises 15 routes?

- The router moves the peer to the Idle state and closes the BGP session.
- The router transitions to listening mode and does not install any new routes into the BGP table.
- The router drops any further advertisements from the peer.
- **The router sends a warning message to the peer.**

Explanation: The prefix restrictions can be put on a BGP neighbor by using the BGP address family configuration command `neighbor ip-address maximum-prefix prefix-count [warning-percentage] [restart time] [warning-only]`. When a peer advertises more routes than the maximum prefix count, the router moves the neighbor to the Idle (PfxCt) state in the finite-state machine (FSM), closes the BGP session, and sends out the appropriate syslog message. A warning is not generated before the prefix limit is reached. By adding a warning percentage (set to 1 to 100) after the maximum prefix count, a warning message will be sent when the percentage is reached.

74. 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.

75. A router is participating in an OSPFv2 domain. What will always happen if the dead interval expires before the router receives a hello packet from an adjacent DROTHER OSPF router?

- OSPF will run a new DR/BDR election.
- SPF will run and determine which neighbor router is “down”.
- A new dead interval timer of 4 times the hello interval will start.
- **OSPF will remove that neighbor from the router link-state database.**

Explanation: On Cisco routers the default dead interval is 4 times the hello interval, and this timer has expired in this case. SPF does not determine the state of neighbor routers; it determines which routes become routing table entries. A DR/DBR election will not always automatically run; this depends on the type of network and on whether or not the router no longer up was a DR or BDR.

76. Which type of OSPF LSA(s) can be represented with the label O*E2 in a routing table?

- type 1 and type 2 LSAs
- type 3 and type 4 LSAs
- **type 5 LSA only**
- type 4 and type 5 LSAs

Explanation: Each router uses the SPF tree to determine the best paths to destination networks. The method that is used to calculate these paths is outlined below:

1. All routers calculate the best paths to destinations within their area, adding these entries to the routing table. They are the type 1 and type 2 LSAs, and are represented with a routing designator of O.
2. All routers calculate the best paths to the other areas within the internetwork. They are type 3 and type 4 LSAs, and are represented with a routing designator of O IA.
3. All routers (except those that are in a stub area) calculate the best paths to the external autonomous system (type 5) destinations. They are represented with either an O E1 or an O E2 route designator, depending on the configuration.

77. In addition to configuring an IPv4 address and mask, and issuing the no shutdown command, which two additional commands does a network technician have to issue on the interface of a Cisco router to enable OSPFv3 address families for IPv4 on that interface? (Choose two.)

- router ospfv3 1
- ipv6 ospf 1
- **ipv6 enable**
- ipv6 router ospf 1
- **ospfv3 1 area 0 ipv4**
- router ospf 1

Explanation: The **ipv6 enable** command initializes IPv6 and a link-local address on the interface so that OSPFv3 address families can form an adjacency with a neighbor router. Alternatively, an IPv6 global unicast address can be configured on the interface. The **ospfv3 1 area 0 ipv4** command initializes OSPv3 process ID 1 on the interface and puts it in IPv4 area 0. The **ipv6 ospf 1** command configures OPSFv3 for IPv6 only, not address families, on an interface. The **ipv6 router ospf 1** command globally initializes the OSPFv3 address families process on the router. The **router ospf 1** command globally starts OSPFv2 on the router. The router ospfv3 1 command initializes the OSPFv3 address families process globally.

78. Which two statements correctly describe OSPF type 3 LSAs? (Choose two.)

- Type 3 LSAs are known as autonomous system external LSA entries.
- Type 3 LSAs are known as router link entries.
- Type 3 LSAs are used for routes to networks outside the OSPF autonomous system.

- **Type 3 LSAs are used to update routes between OSPF areas.**
- **Type 3 LSAs are generated without requiring a full SPF calculation.**

Explanation: Type 4 LSAs are known as autonomous system external LSA entries. Type 4 LSAs are generated by an ABR to inform other areas of next-hop information for the ASBR. Type 1 LSAs are known as router link entries. Type 3 LSAs can be generated without requiring a full SPF calculation. Type 3 LSAs are used to carry routes between OSPF areas.

79. Which two OSPFv3 LSA types are used to advertise IPv6 prefixes to neighbors? (Choose two.)

- LSA type 4 – interarea router
- LSA type 5 – AS-external
- LSA type 7 – NSSA
- **LSA type 8 – link-local LSA**
- **LSA type 9 – intra-area prefix LSA**

Explanation: Two new LSA types are added to OSPFv3, type 8, link-local LSA, and type 9, intra-area prefix LSA. These two LSAs advertise unicast prefixes and prevent the need for OSPF calculations when interface addresses are added or changed.

80. Refer to the exhibit. What is the function of the Null0 route in the outputs displayed for R1 and R2?

```
R1# show ipv6 route eigrp
<Output omitted>
D 2001:DB8:1::/48 [5/2816]
via Null0, directly connected
D 2001:DB8:2::/48 [90/2848]
via FF84::2, GigabitEthernet0/1
```

```
R2# show ipv6 route eigrp
<Output omitted>
D 2001:DB8:1::/48 [90/2841]
via FF84::1, GigabitEthernet0/1
D 2001:DB8:2::/48 [5/2816]
via Null0, directly connected
```

- **to advertise the local /48 summary route**
- to force advertisements of only the /64 route entries to the neighbor routers
- to force advertisements of only the /128 route entries to the neighbor routers
- to invoke the split horizon rule to prevent routing loops

Explanation: In EIGRPv6, a Null0 route with an administrative distance of 5 is added to the routing table as a loop-prevention mechanism. Only the /48 summary prefix is received from the neighbor router and any of the more specific /64 and /128 route entries are suppressed. In this instance a Null0 route is populated on the router for the local /48 summary route advertisement.

81. Which technology creates a mapping of public IP addresses for remote tunnel spokes in a DMVPN configuration?

- **NHRP**
- IPsec
- NAT
- ARP

Explanation: The Next Hop Resolution Protocol (NHRP) creates a distributed mapping of IP addresses and tunnel spokes in a DMVPN deployment.

82. A network administrator needs to learn information about EIGRP load balancing to configure an EIGRP network. Which piece of information is accurate about this subject?

- The variance multiplier is obtained by dividing the successor route metric by the feasible successor metric.
- Any feasible distance of a feasible successor with a metric above the EIGRP variance value is installed into the RIB.
- The maximum equal-cost multipathing routing for EIGRP is four routes.
- **The EIGRP variance value is the feasible distance for a route multiplied by the EIGRP variance multiplier.**

Explanation: EIGRP allows multiple successor routes (with the same metric) to be installed into the EIGRP RIB. This is called equal-cost multipathing (ECMP) routing. The actual default maximum ECMP is four routes, but this value can be changed with the maximum-paths maximum-paths command. EIGRP also supports unequal-cost load balancing changing the EIGRP variance multiplier. The EIGRP variance value is the feasible distance (FD) for a route multiplied by the EIGRP variance multiplier. Any FD of a feasible successor with a metric below the EIGRP variance value is installed into the RIB. Dividing the feasible successor metric by the successor route metric provides the variance multiplier.

83. Refer to the exhibit. Directly connected networks configured on router R1 are not being shared with neighboring routers through OSPFv3. What is the cause of the issue?


```
R1# show running-config
```

```
<output omitted>
```

```
ipv6 unicast-routing
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address 2001:DB8:CAFE:A001::1/64
!
interface GigabitEthernet0/1
 no ip address
 ipv6 address 2001:DB8:CAFE:1::1/64
!
ipv6 router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
!
```



- IPv6 OSPF routing is not enabled.
- **The routes are not enabled in the OSPF advertisement.**
- There are no IPv4 addresses configured on the interfaces.
- There are no network statements for the routes in the OSPF configuration.

Explanation: Unlike OSPFv2, OSPFv3 does not use the network command to advertise directly attached networks. OSPFv3 is enabled directly on the interface. Once the command `ipv6 ospf process_id area area_id` is entered on the interface, that particular network will be included in OSPFv3 advertisements.

84. Refer to the exhibit. R2 uses loopback0 interface 2.2.2.2 and R5 uses loopback0 interface 5.5.5.5 in the neighbor ip_address remote-as as_number statement in their respective configurations. A network administrator issues the `show bgp ipv4 unicast summary` command on R2. Which statement describes the adjacency state of R5?

```
R2# show bgp ipv4 unicast summary
```

```
BGP router identifier 2.2.2.2, local AS number 65502
```

```
BGP table version is 1, main routing table version 1
```

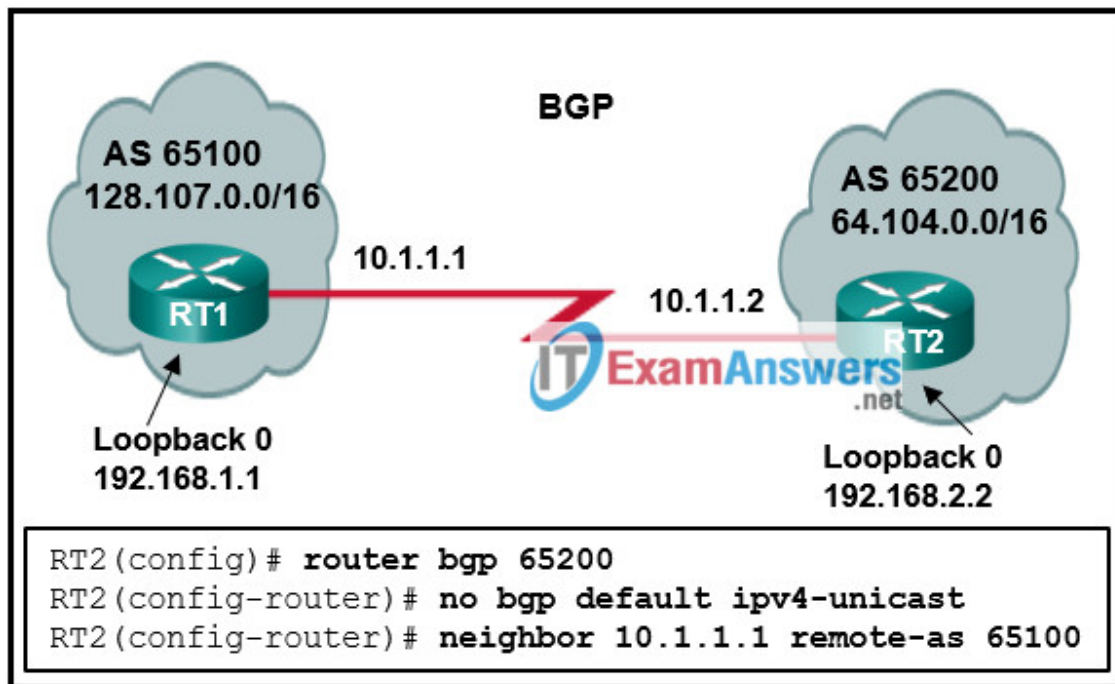


Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
5.5.5.5	4	65502	0	0	1	0	0	00:00:13	Active
10.1.12.1	4	65501	2	2	1	0	0	00:00:12	0

- R2 uses the default route to reach R5.
- There is no route in the routing table of R2 to reach R5.
- An adjacency is formed between R2 and R5, but there is no message transmitted.
- **An open message is sent to R5, but no response is received.**

Explanation: If there is no route for the IP address or a router uses the default route to reach a neighbor, the state is Idle. If a route is found in the routing table and a three-way TCP handshake is complete, an open message is sent. If there is no response to the open message, the state is Active.

85. Refer to the exhibit. A network administrator is configuring BGP on router RT2, but RT2 cannot establish a peer relationship with RT1. What is the cause of the problem?



- An IPv4 multicast address should be used in the neighbor statement.
- The network statement for the network 192.168.2.2/32 is missing.
- The network statement for the network 17.0.0.0/16 is missing.
- **The IPv4 address family has not been activated.**

Explanation: In order to establish BGP neighbor and allow BGP communications, the address family needs to be activated. Cisco IOS activates the IPv4 address family by default. The BGP router configuration command **no bgp default ipv4-unicast** disables the automatic activation of the IPv4 AFI. Thus it is necessary to initialize the address family with the BGP router configuration command **address-family** afi safi before activating the address family for the BGP neighbor with the the command **neighbor ip-address activate** .

86. In order to limit spoofed packets on a network, a network administrator is configuring uRPF on a Cisco router interface with the ip verify unicast source reachable-via rx command. After the configuration is completed, the administrator observes that valid packets are being dropped. What may be causing this packet discard?

- The uRPF is configured with loose mode and asymmetric routing occurs.

- The uRPF is configured with strict mode and symmetric routing occurs.
- **The return traffic used a different path to that used by the source traffic.**
- The same path is used for the source traffic and the return traffic.

Explanation: When uRPF is configured on an interface, the uRPF mode should be chosen according to the type of routing. With symmetric routing, the same path is used for the source and the return traffic. With asymmetric routing, a different path ends up being used for return traffic. The `ip verify unicast reachable-via rx` command configures uRPF in strict mode. If strict mode is used when asymmetric routing occurs, the legitimate traffic is dropped. Where symmetric routing is guaranteed to occur, uRPF should be configured in strict mode.