300-101.prepaway.premium.exam.847q

Number: 300-101
Passing Score: 800
Time Limit: 120 min
File Version: 25.0

300-101

Implementing Cisco IP Routing

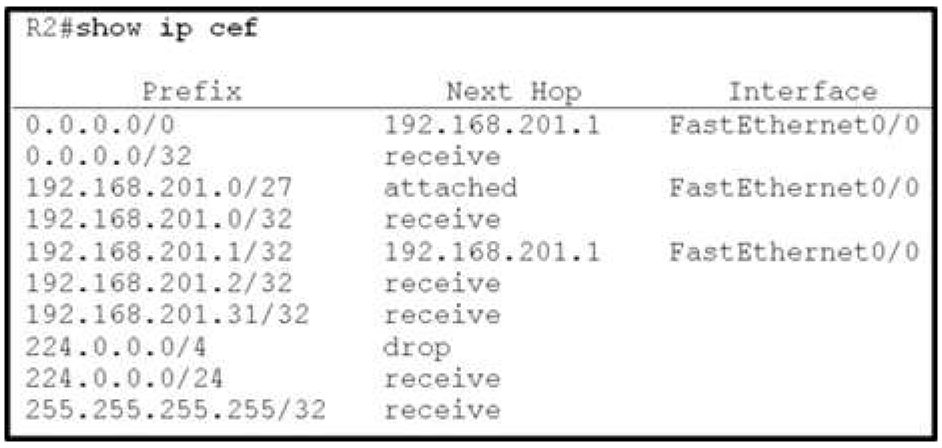
Version 25.0

Sections

1. Network Principles
2. Layer 2 Technologies
3. Layer 3 Technologies
4. VPN Technologies
5. Infrastructure Security
6. Infrastructure Services
7. Mix Questions

Exam A

QUESTION 1
Refer to the exhibit.



```
R2#show ip cef

      Prefix                  Next Hop          Interface
0.0.0.0/0                 192.168.201.1    FastEthernet0/0
0.0.0.0/32                receive
192.168.201.0/27          attached         FastEthernet0/0
192.168.201.0/32          receive
192.168.201.1/32          192.168.201.1    FastEthernet0/0
192.168.201.2/32          receive
192.168.201.31/32         receive
224.0.0.0/4               drop
224.0.0.0/24              receive
255.255.255.255/32        receive
```

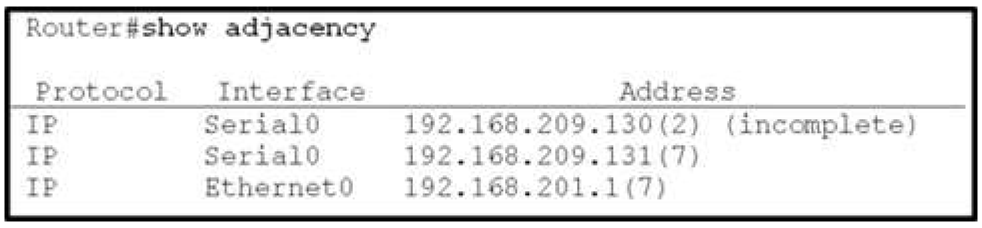
Based on this FIB table, which statement is correct?

A. There is no default gateway.
B. The IP address of the router on FastEthernet is 209.168.201.1.
C. The gateway of last resort is 192.168.201.1.
D. The router will listen for all multicast traffic.

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The 0.0.0.0/0 route is the default route and is listed as the first CEF entry. Here we see the next hop for this default route lists 192.168.201.1 as the default router (gateway of last resort).

QUESTION 2
Refer to the exhibit.



```
Router#show adjacency

 Protocol   Interface              Address
IP         Serial0     192.168.209.130(2) (incomplete)
IP         Serial0     192.168.209.131(7)
IP         Ethernet0   192.168.201.1(7)
```

A network administrator checks this adjacency table on a router. What is a possible cause for the incomplete marking?

A. incomplete ARP information
B. incorrect ACL
C. dynamic routing protocol failure
D. serial link congestion

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
To display information about the Cisco Express Forwarding adjacency table or the hardware Layer 3-switching adjacency table, use the show adjacency command.
Reasons for Incomplete Adjacencies
There are two known reasons for an incomplete adjacency:

- The router cannot use ARP successfully for the next-hop interface.
- After a clear ip arp or a clear adjacency command, the router marks the adjacency as incomplete. Then it fails to clear the entry.
- In an MPLS environment, IP CEF should be enameled for Label Switching. Interface level command ip route-cache cef

No ARP Entry
When CEF cannot locate a valid adjacency for a destination prefix, it punts the packets to the CPU for ARP resolution and, in turn, for completion of the adjacency.

Reference: http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/17812-cef-incomp.html#t4

QUESTION 3
A network engineer notices that transmission rates of senders of TCP traffic sharply increase and decrease simultaneously during periods of congestion. Which condition causes this?

A. global synchronization
B. tail drop
C. random early detection
D. queue management algorithm

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:

Explanation:
TCP global synchronization in computer networks can happen to TCP/IP flows during periods of congestion because each sender will reduce their transmission rate at the same time when packet loss occurs.
Routers on the Internet normally have packet queues, to allow them to hold packets when the network is busy, rather than discarding them.
Because routers have limited resources, the size of these queues is also limited. The simplest technique to limit queue size is known as tail drop. The queue is allowed to fill to its maximum size, and then any new packets are simply discarded, until there is space in the queue again.
This causes problems when used on TCP/IP routers handling multiple TCP streams, especially when bursty traffic is present. While the network is stable, the queue is constantly full, and there are no problems except that the full queue results in high latency. However, the introduction of a sudden burst of traffic may cause large numbers of established, steady streams to lose packets simultaneously.

Reference: http://en.wikipedia.org/wiki/TCP_global_synchronization

QUESTION 4
Which three problems result from application mixing of UDP and TCP streams within a network with no QoS? (Choose three.)

A. starvation
B. jitter
C. latency
D. windowing
E. lower throughput

Correct Answer: ACE
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
It is a general best practice not to mix TCP-based traffic with UDP-based traffic (especially streaming video) within a single service provider class due to the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters will throttle-back flows when drops have been detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely oblivious to drops and thus never lower transmission rates due to dropping. When TCP flows are combined with UDP flows in a single service provider class and the class experiences congestion, then TCP flows will continually lower their rates, potentially giving up their bandwidth to drop-oblivious UDP flows. This effect is called *TCP-starvation/UDP-dominance*. This can increase latency and lower the overall throughput.
TCP-starvation/UDP-dominance likely occurs if (TCP-based) mission-critical data is assigned to the same service provider class as (UDP-based) streaming video and the class experiences sustained congestion. Even if WRED is enabled on the service provider class, the same behavior would be observed, as WRED (for the most part) only affects TCP-based flows.
Granted, it is not always possible to separate TCP-based flows from UDP-based flows, but it is beneficial to be aware of this behavior when making such application-mixing decisions.

Reference: http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/spqsd_wp.htm

QUESTION 5
Which method allows IPv4 and IPv6 to work together without requiring both to be used for a single connection during the migration process?

A. dual-stack method
B. 6to4 tunneling
C. GRE tunneling
D. NAT-PT

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Dual stack means that devices are able to run IPv4 and IPv6 in parallel. It allows hosts to simultaneously reach IPv4 and IPv6 content, so it offers a very flexible coexistence strategy. For sessions that support IPv6, IPv6 is used on a dual stack endpoint. If both endpoints support Ipv4 only, then IPv4 is used.
Benefits:

- Native dual stack does not require any tunneling mechanisms on internal networks
- Both IPv4 and IPv6 run independent of each other
- Dual stack supports gradual migration of endpoints, networks, and applications.

Reference: http://www.cisco.com/web/strategy/docs/gov/IPV6at_a_glance_c45-625859.pdf

QUESTION 6
Which statement about the use of tunneling to migrate to IPv6 is true?

A. Tunneling is less secure than dual stack or translation.
B. Tunneling is more difficult to configure than dual stack or translation.
C. Tunneling does not enable users of the new protocol to communicate with users of the old protocol without dual-stack hosts.
D. Tunneling destinations are manually determined by the IPv4 address in the low-order 32 bits of IPv4-compatible IPv6 addresses.

Correct Answer: C
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Using the tunneling option, organizations build an overlay network that tunnels one protocol over the other by encapsulating IPv6 packets within IPv4 packets and IPv4 packets within IPv6 packets. The advantage of this approach is that the new protocol can work without disturbing the old protocol, thus providing connectivity between users of the new protocol.
Tunneling has two disadvantages, as discussed in RFC 6144:

- Users of the new architecture cannot use the services of the underlying infrastructure.
- **Tunneling does not enable users of the new protocol to communicate with users of the old protocol without dual-stack hosts, which negates interoperability.**

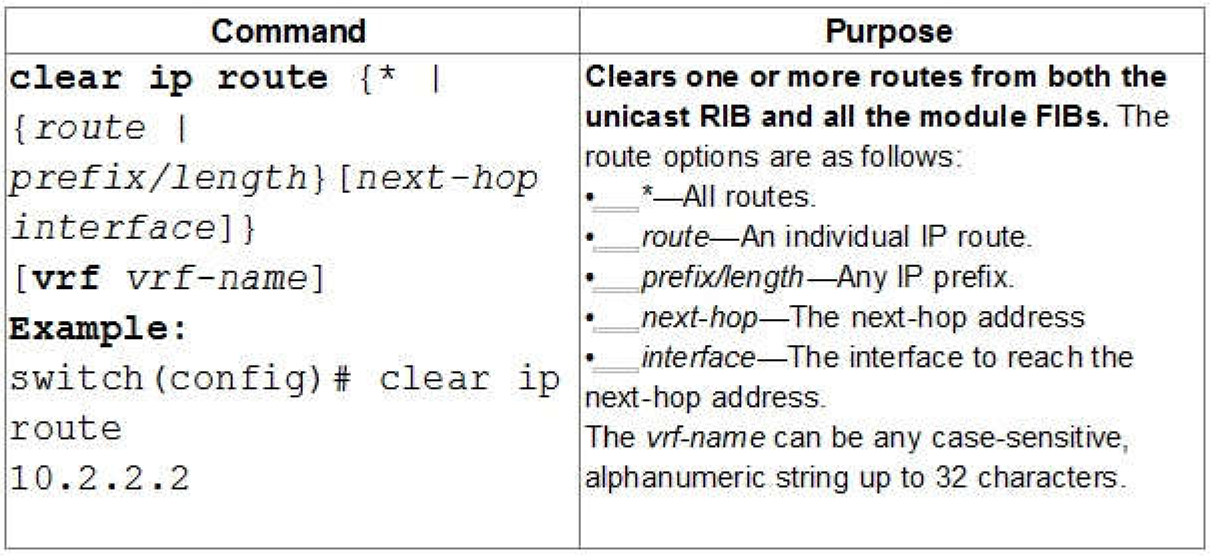
Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

QUESTION 7
A network administrator executes the command clear ip route. Which two tables does this command clear and rebuild? (Choose two.)

A. IP routing
B. FIB
C. ARP cache
D. MAC address table
E. Cisco Express Forwarding table
F. topology table

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
To clear one or more entries in the IP routing table, use the following commands in any mode:



Command	Purpose
clear ip route {* | {*route* | *prefix/length*}[*next-hop interface*]} [**vrf** *vrf-name*] **Example:** switch(config)# clear ip route 10.2.2.2	**Clears one or more routes from both the unicast RIB and all the module FIBs.** The route options are as follows: • *—All routes. • *route*—An individual IP route. • *prefix/length*—Any IP prefix. • *next-hop*—The next-hop address • *interface*—The interface to reach the next-hop address. The *vrf-name* can be any case-sensitive, alphanumeric string up to 32 characters.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/unicast/5_0_3_N1_1/Cisco_n5k_layer3_ucast_cfg_rel_503_N1_1/l3_manage-routes.html

QUESTION 8
Which switching method is used when entries are present in the output of the command show ip cache?

A. fast switching
B. process switching
C. Cisco Express Forwarding switching
D. cut-through packet switching

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Fast switching allows higher throughput by switching a packet using a cache created by the initial packet sent to a particular destination. Destination addresses are stored in the high-speed cache to expedite forwarding. Routers offer better packet-transfer performance when fast switching is enabled. Fast switching is enabled by default on all interfaces that support fast switching.
To display the routing table cache used to fast switch IP traffic, use the “show ip cache” EXEC command.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/command/reference/fswtch_r/xrfscmd5.html#wp1038133

QUESTION 9
Which two actions must you perform to enable and use window scaling on a router? (Choose two.)

A. Execute the command ip tcp window-size 65536.
B. Set window scaling to be used on the remote host.
C. Execute the command ip tcp queuemax.
D. Set TCP options to "enabled" on the remote host.
E. Execute the command ip tcp adjust-mss.

Correct Answer: AB
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
The TCP Window Scaling feature adds support for the Window Scaling option in RFC 1323, TCP Extensions for High Performance. A larger window size is recommended to improve TCP performance in network paths with large bandwidth-delay product characteristics that are called Long Fat Networks (LFNs). The TCP Window Scaling enhancement provides that support.
The window scaling extension in Cisco IOS software expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit window field of the TCP header. The window size can increase to a scale factor of 14. Typical applications use a scale factor of 3 when deployed in LFNs.
The TCP Window Scaling feature complies with RFC 1323. The larger scalable window size will allow TCP to perform better over LFNs. Use **the ip tcp**

window-size command in global configuration mode to configure the TCP window size. In order for this to work, the remote host must also support this feature and its window size must be increased.

QUESTION 10
Which three TCP enhancements can be used with TCP selective acknowledgments? (Choose three.)

A. header compression
B. explicit congestion notification
C. keepalive
D. time stamps
E. TCP path discovery
F. MTU window

Correct Answer: BCD
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
TCP Selective Acknowledgment
The TCP Selective Acknowledgment feature improves performance if multiple packets are lost from one TCP window of data.
Prior to this feature, because of limited information available from cumulative acknowledgments, a TCP sender could learn about only one lost packet per-round-trip time. An aggressive sender could choose to resend packets early, but such re-sent segments might have already been successfully received.
The TCP selective acknowledgment mechanism helps improve performance. The receiving TCP host returns selective acknowledgment packets to the sender, informing the sender of data that has been received. In other words, the receiver can acknowledge packets received out of order. The sender can then resend only missing data segments (instead of everything since the first missing packet).
Prior to selective acknowledgment, if TCP lost packets 4 and 7 out of an 8-packet window, TCP would receive acknowledgment of only packets 1, 2, and 3. Packets 4 through 8 would need to be re-sent. With selective acknowledgment, TCP receives acknowledgment of packets 1, 2, 3, 5, 6, and 8. Only packets 4 and 7 must be re-sent.
TCP selective acknowledgment is used only when multiple packets are dropped within one TCP window. There is no performance impact when the feature is enabled but not used. Use the ip tcp selective-ack command in global configuration mode to enable TCP selective acknowledgment.
Refer to RFC 2018 for more details about TCP selective acknowledgment.
TCP Time Stamp
The TCP time-stamp option provides improved TCP round-trip time measurements. Because the time stamps are always sent and echoed in both directions and the time-stamp value in the header is always changing, TCP header compression will not compress the outgoing packet. To allow TCP header compression over a serial link, the TCP time-stamp option is disabled. Use the ip tcp timestamp command to enable the TCP time-stamp option.
TCP Explicit Congestion Notification
The TCP Explicit Congestion Notification (ECN) feature allows an intermediate router to notify end hosts of impending network congestion. It also provides enhanced support for TCP sessions associated with applications, such as Telnet, web browsing, and transfer of audio and video data that are sensitive to delay or packet loss. The benefit of this feature is the reduction of delay and packet loss in data transmissions. Use the ip tcp ecn command in global configuration mode to enable TCP ECN.
TCP Keepalive Timer
The TCP Keepalive Timer feature provides a mechanism to identify dead connections.
When a TCP connection on a routing device is idle for too long, the device sends a TCP keepalive packet to the peer with only the Acknowledgment (ACK) flag turned on. If a response packet (a TCP ACK packet) is not received after the device sends a specific number of probes, the connection is considered dead and the device initiating the probes frees resources used by the TCP connection.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp/configuration/xe-3s/asr1000/iap-xe-3s-asr1000-book/iap-tcp.html#GUID-22A82C5F-631F-4390-9838-F2E48FFEEA01

QUESTION 11
A network administrator uses IP SLA to measure UDP performance and notices that packets on one router have a higher one-way delay compared to the opposite direction. Which UDP characteristic does this scenario describe?

A. latency
B. starvation
C. connectionless communication
D. nonsequencing unordered packets
E. jitter

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Cisco IOS IP SLAs provides a proactive notification feature with an SNMP trap. Each measurement operation can monitor against a pre-set performance threshold. Cisco IOS IP SLAs generates an SNMP trap to alert management applications if this threshold is crossed. Several SNMP traps are available: round trip time, average jitter, **one-way latency**, jitter, packet loss, MOS, and connectivity tests.
Here is a partial sample output from the IP SLA statistics that can be seen:

```
router#show ip sla statistics 1
Round Trip Time (RTT) for Index 55
Latest RTT: 1 ms
Latest operation start time: *23:43:31.845 UTC Thu Feb 3 2005
Latest operation return code: OK
RTT Values:
Number Of RTT: 10 RTT Min/Avg/Max: 1/1/1 milliseconds
Latency one-way time:
Number of Latency one-way Samples: 0
Source to Destination Latency one way Min/Avg/Max: 0/0/0 milliseconds
Destination to Source Latency one way Min/Avg/Max: 0/0/0 milliseconds
```

Reference: http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html

QUESTION 12
Under which condition does UDP dominance occur?

A. when TCP traffic is in the same class as UDP

B. when UDP flows are assigned a lower priority queue
C. when WRED is enabled
D. when ACLs are in place to block TCP traffic

Correct Answer: A
Section: Network Principles
Explanation

Explanation/Reference:
Explanation:
Mixing TCP with UDP
It is a general best practice to not mix TCP-based traffic with UDP-based traffic (especially Streaming-Video) within a single service-provider class because of the behaviors of these protocols during periods of congestion. Specifically, TCP transmitters throttle back flows when drops are detected. Although some UDP applications have application-level windowing, flow control, and retransmission capabilities, most UDP transmitters are completely oblivious to drops and, thus, never lower transmission rates because of dropping.
When TCP flows are combined with UDP flows within a single service-provider class and the class experiences congestion, TCP flows continually lower their transmission rates, potentially giving up their bandwidth to UDP flows that are oblivious to drops. This effect is called TCP starvation/UDP dominance.
TCP starvation/UDP dominance likely occurs if (TCP-based) Mission-Critical Data is assigned to the same service-provider class as (UDP-based) Streaming-Video and the class experiences sustained congestion. Even if WRED is enabled on the service-provider class, the same behavior would be observed because WRED (for the most part) manages congestion only on TCP-based flows.

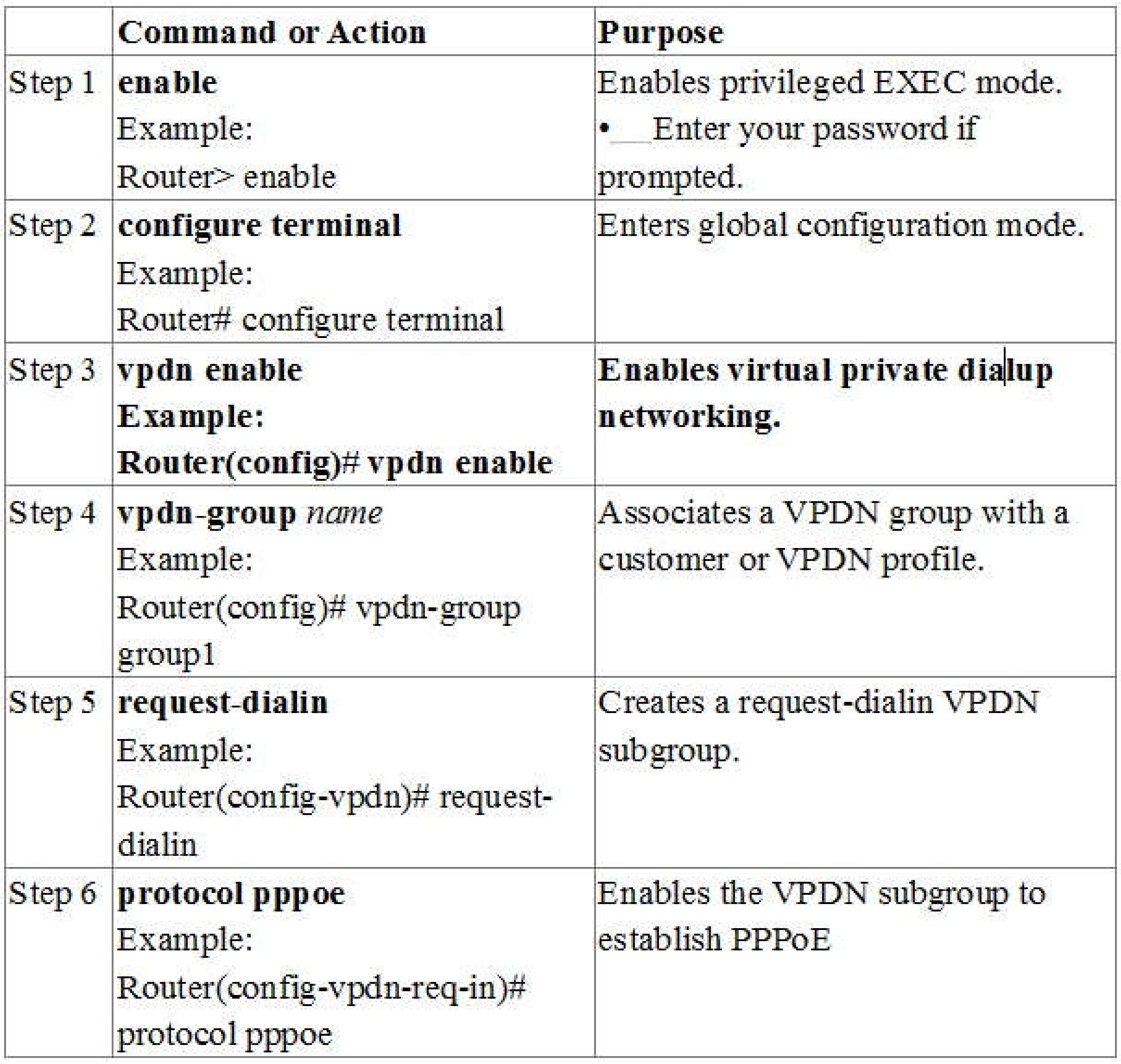
Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/VPNQoS.html

QUESTION 13
Prior to enabling PPPoE in a virtual private dialup network group, which task must be completed?

A. Disable CDP on the interface.
B. Execute the vpdn enable command.
C. Execute the no switchport command.
D. Enable QoS FIFO for PPPoE support.

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Enabling PPPoE in a VPDN Group
Perform this task to enable PPPoE in a virtual private dial-up network (VPDN) group.
Restrictions
This task applies only to releases prior to Cisco IOS Release 12.2(13)T.
SUMMARY STEPS
1. enable
2. configure terminal
3. vpdn enable
4. vpdn-group *name*
5. request-dialin
6. protocol pppoe
DETAILED STEPS



	Command or Action	Purpose
Step 1	**enable** Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** Example: Router# configure terminal	Enters global configuration mode.
Step 3	**vpdn enable** **Example:** **Router(config)# vpdn enable**	**Enables virtual private dialup networking.**
Step 4	**vpdn-group** *name* Example: Router(config)# vpdn-group group1	Associates a VPDN group with a customer or VPDN profile.
Step 5	**request-dialin** Example: Router(config-vpdn)# request-dialin	Creates a request-dialin VPDN subgroup.
Step 6	**protocol pppoe** Example: Router(config-vpdn-req-in)# protocol pppoe	Enables the VPDN subgroup to establish PPPoE

Reference: http://www.cisco.com/en/US/docs/ios/12_2t/12_2t2/feature/guide/ftpppoec_support_TSD_Island_of_Content_Chapter.html

QUESTION 14
A network engineer has been asked to ensure that the PPPoE connection is established and authenticated using an encrypted password. Which technology, in combination with PPPoE, can be used for authentication in this manner?

A. PAP
B. dot1x
C. Ipsec
D. CHAP
E. ESP

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
With PPPoE, the two authentication options are PAP and CHAP. When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or “challenges” the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router.
When the remote device receives the challenge packet, it concatenates the ID, the remote device’s password, and the random number, and then encrypts all of it using the remote device’s password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process.
When the access server receives the response, it uses the name it received to retrieve a password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password — if the result matches the result sent in the response packet, authentication succeeds.
The benefit of using CHAP authentication is that the remote device’s password is never transmitted in clear text (encrypted). This prevents other devices from stealing it and gaining illegal access to the ISP’s network.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html

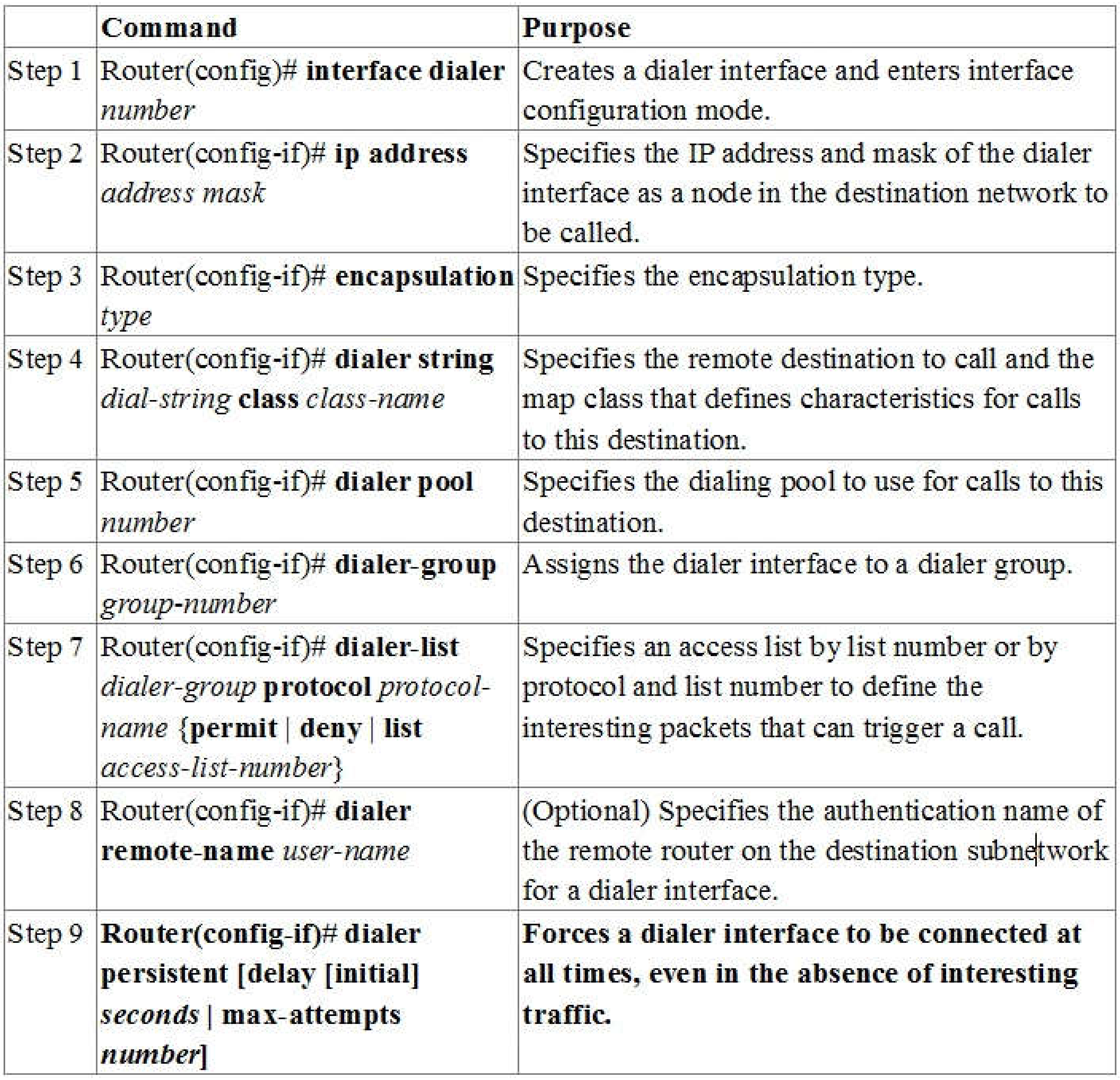
QUESTION 15
A corporate policy requires PPPoE to be enabled and to maintain a connection with the ISP, even if no interesting traffic exists. Which feature can be used to accomplish this task?

A. TCP Adjust
B. Dialer Persistent
C. PPPoE Groups
D. half-bridging
E. Peer Neighbor Route

Correct Answer: B
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
A new interface configuration command, **dialer persistent**, allows a dial-on-demand routing (DDR) dialer profile connection to be brought up without being triggered by *interesting* traffic. When configured, the **dialer persistent** command starts a timer when the dialer interface starts up and starts the connection when the timer expires. If interesting traffic arrives before the timer expires, the connection is still brought up and set as persistent. The command provides a default timer interval, or you can set a custom timer interval.

To configure a dialer interface as persistent, use the following commands beginning in global configuration mode:



	Command	Purpose
Step 1	Router(config)# **interface dialer** *number*	Creates a dialer interface and enters interface configuration mode.
Step 2	Router(config-if)# **ip address** *address mask*	Specifies the IP address and mask of the dialer interface as a node in the destination network to be called.
Step 3	Router(config-if)# **encapsulation** *type*	Specifies the encapsulation type.
Step 4	Router(config-if)# **dialer string** *dial-string* **class** *class-name*	Specifies the remote destination to call and the map class that defines characteristics for calls to this destination.
Step 5	Router(config-if)# **dialer pool** *number*	Specifies the dialing pool to use for calls to this destination.
Step 6	Router(config-if)# **dialer-group** *group-number*	Assigns the dialer interface to a dialer group.
Step 7	Router(config-if)# **dialer-list** *dialer-group* **protocol** *protocol-name* {**permit** | **deny** | **list** *access-list-number*}	Specifies an access list by list number or by protocol and list number to define the interesting packets that can trigger a call.
Step 8	Router(config-if)# **dialer remote-name** *user-name*	(Optional) Specifies the authentication name of the remote router on the destination subnetwork for a dialer interface.
Step 9	**Router(config-if)# dialer persistent [delay [initial]** ***seconds*** **| max-attempts** ***number*****]**	**Forces a dialer interface to be connected at all times, even in the absence of interesting traffic.**

QUESTION 16
Which PPP authentication method sends authentication information in clear text?

A. MS CHAP
B. CDPCP
C. CHAP
D. PAP

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
PAP authentication involves a two-way handshake where the username and password are sent across the link in clear text; hence, PAP authentication does not provide any protection against playback and line sniffing.
CHAP authentication, on the other hand, periodically verifies the identity of the remote node using a three-way handshake. After the PPP link is established, the host sends a "challenge" message to the remote node. The remote node responds with a value calc“lated usi”g a one-way hash function. The host checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is terminated.

Reference: http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/10241-ppp-callin-hostname.html

QUESTION 17
Which protocol uses dynamic address mapping to request the next-hop protocol address for a specific connection?

A. Frame Relay inverse ARP
B. static DLCI mapping
C. Frame Relay broadcast queue
D. dynamic DLCI mapping

Correct Answer: A
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
Dynamic address mapping uses Frame Relay Inverse ARP to request the next-hop protocol address for a specific connection, given its known DLCI. Responses to Inverse ARP requests are entered in an address-to-DLCI mapping table on the router or access server; the table is then used to supply the next-hop protocol address or the DLCI for outgoing traffic.

QUESTION 18
Which statement is true about the PPP Session Phase of PPPoE?

A. PPP options are negotiated and authentication is not performed. Once the link setup is completed, PPPoE functions as a Layer 3 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.

B. PPP options are not negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 4 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.

C. PPP options are automatically enabled and authorization is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method that allows data to be encrypted over the PPP link within PPPoE headers.

D. PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method that allows data to be transferred over the PPP link within PPPoE headers.

Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
PPPoE is composed of two main phases:

- Active Discovery Phase — In this phase, the PPPoE client locates a PPPoE server, called an access concentrator. During this phase, a Session ID is assigned and the PPPoE layer is established.
- **PPP Session Phase — In this phase, PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method, allowing data to be transferred over the PPP link within PPPoE headers.**

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpn-cli/vpn-pppoe.html

QUESTION 19
PPPoE is composed of which two phases?

A. Active Authentication Phase and PPP Session Phase

B. Passive Discovery Phase and PPP Session Phase

C. Active Authorization Phase and PPP Session Phase

D. Active Discovery Phase and PPP Session Phase

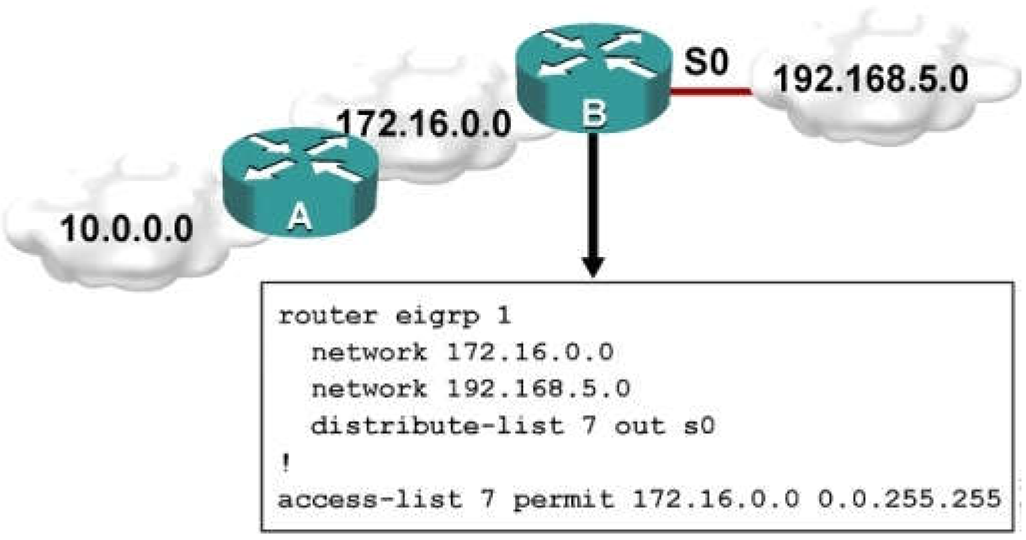
Correct Answer: D
Section: Layer 2 Technologies
Explanation

Explanation/Reference:
Explanation:
PPPoE is composed of two main phases:

- Active Discovery Phase — In this phase, the PPPoE client locates a PPPoE server, called an access concentrator. During this phase, a Session ID is assigned and the PPPoE layer is established.
- PPP Session Phase — In this phase, PPP options are negotiated and authentication is performed. Once the link setup is completed, PPPoE functions as a Layer 2 encapsulation method, allowing data to be transferred over the PPP link within PPPoE headers.

Reference: http://www.cisco.com/c/en/us/td/docs/security/asa/asa92/configuration/vpn/asa-vpn-cli/vpn-pppoe.html

QUESTION 20
Refer to the exhibit.



```
router eigrp 1
  network 172.16.0.0
  network 192.168.5.0
  distribute-list 7 out s0
!
access-list 7 permit 172.16.0.0 0.0.255.255
```

Which one statement is true?

A. Traffic from the 172.16.0.0/16 network will be blocked by the ACL.

B. The 10.0.0.0/8 network will not be advertised by Router B because the network statement for the 10.0.0.0/8 network is missing from Router B.

C. The 10.0.0.0/8 network will not be in the routing table on Router B.

D. Users on the 10.0.0.0/8 network can successfully ping users on the 192.168.5.0/24 network, but users on the 192.168.5.0/24 cannot successfully ping users on the 10.0.0.0/8 network.

E. Router B will not advertise the 10.0.0.0/8 network because it is blocked by the ACL.

Correct Answer: E
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
You can filter what individual routes are sent (out) or received (in) to any interface within your EIGRP configuration.
One example is noted above. If you filter outbound, the next neighbor(s) will not know about anything except the 172.16.0.0/16 route and therefore won't send it to anyone else downstream. If you filter inbound, YOU won't know about the route and therefore won't send it to anyone else downstream.

QUESTION 21
A router with an interface that is configured with ipv6 address autoconfig also has a link-local address assigned. Which message is required to obtain a global unicast address when a router is present?

A. DHCPv6 request
B. router-advertisement
C. neighbor-solicitation
D. redirect

Correct Answer: B
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Autoconfiguration is performed on multicast-enabled links only and begins when a multicast-enabled interface is enabled (during system startup or manually). Nodes (both, hosts and routers) begin the process by generating a link-local address for the interface. It is formed by appending the interface identifier to well-known link-local prefix **FE80::0.** The interface identifier replaces the right-most zeroes of the link-local prefix.
Before the link-local address can be assigned to the interface, the node performs the Duplicate Address Detection mechanism to see if any other node is using the same link-local address on the link. It does this by sending a Neighbor Solicitation message with target address as the "tentative" address and destination address as the solicited-node multicast address corresponding to this tentative address. If a node responds with a Neighbor Advertisement message with tentative address as the target address, the address is a duplicate address and must not be used. Hence, manual configuration is required.
Once the node verifies that its tentative address is unique on the link, it assigns that link-local address to the interface. At this stage, it has IP-connectivity to other neighbors on this link.
The autoconfiguration on the routers stop at this stage, further tasks are performed only by the hosts. The routers will need manual configuration (or stateful configuration) to receive site-local or global addresses.
The next phase involves obtaining Router Advertisements from routers if any routers are present on the link. If no routers are present, a stateful configuration is required. If routers are present, the Router Advertisements notify what sort of configurations the hosts need to do and the hosts receive a global unicast IPv6 address.

Reference: https://sites.google.com/site/amitsciscozone/home/important-tips/ipv6/ipv6-stateless-autoconfiguration

QUESTION 22
An engineer has configured a router to use EUI-64, and was asked to document the IPv6 address of the router. The router has the following interface parameters:

mac address 2201.420A.0004
subnet 2001:DB8:0:1::/64

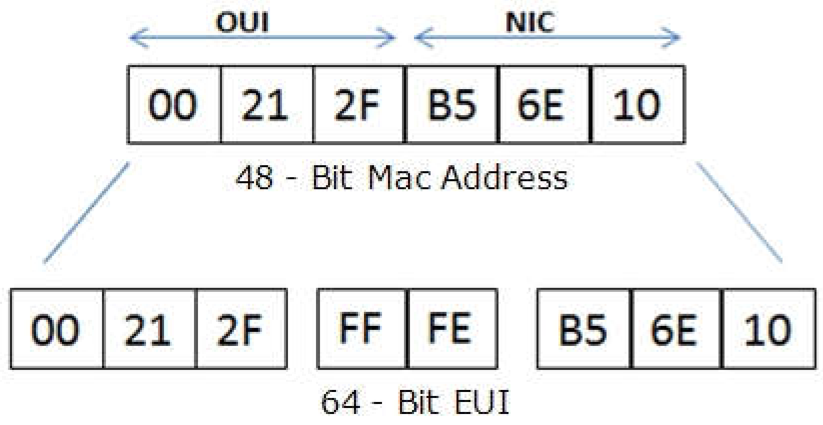
Which IPv6 addresses should the engineer add to the documentation?

A. 2001:DB8:0:1:01:42AF:FE0F:4
B. 2001:DB8:0:1:FFFF:2201:420F:4
C. 2001:DB8:0:1:FE80:2201:420F:4
D. 2001:DB8:0:1:C601:42AE:800F:4

Correct Answer: A
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Extended Unique Identifier (EUI), as per RFC2373, allows a host to assign iteslf a unique 64-Bit IP Version 6 interface identifier (EUI-64). This feature is a key benefit over IPv4 as it eliminates the need of manual configuration or DHCP as in the world of IPv4. The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The Mac address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific. The 16-bit 0xFFFE is then inserted between these two 24-bits to for the 64-bit EUI address. IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the EUI-48 MAC address.

Here is an example showing how the Mac Address is used to generate EUI.



Next, the seventh bit from the left, or the universal/local (U/L) bit, needs to be inverted. This bit identifies whether this interface identifier is universally or locally administered. If 0, the address is locally administered and if 1, the address is globally unique. It is worth noticing that in the OUI portion, the globally unique addresses assigned by the IEEE has always been set to 0 whereas the locally created addresses has 1 configured. Therefore, when the bit is inverted, it maintains its original scope (global unique address is still global unique and vice versa). The reason for inverting can be found in RFC4291 section 2.5.1.

Reference: https://supportforums.cisco.com/document/100566/understanding-ipv6-eui-64-bit-address

QUESTION 23
For security purposes, an Ipv6 traffic filter was configured under various interfaces on the local router. However, shortly after implementing the traffic filter, OSPFv3 neighbor adjacencies were lost. What caused this issue?

A. The traffic filter is blocking all ICMPv6 traffic.

B. The global anycast address must be added to the traffic filter to allow OSPFv3 to work properly.
C. The link-local addresses that were used by OSPFv3 were explicitly denied, which caused the neighbor relationships to fail.
D. Ipv6 traffic filtering can be implemented only on SVIs.

Correct Answer: C
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
OSPFv3 uses link-local Ipv6 addresses for neighbor discovery and other features, so if any Ipv6 traffic filters are implemented be sure to include the link local address so that it is permitted in the filter list.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_ospfv3.html

QUESTION 24
What is the purpose of the autonomous-system {autonomous-system-number} command?

A. It sets the EIGRP autonomous system number in a VRF.
B. It sets the BGP autonomous system number in a VRF.
C. It sets the global EIGRP autonomous system number.
D. It sets the global BGP autonomous system number.

Correct Answer: A
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
To configure the autonomous-system number for an Enhanced Interior Gateway Routing Protocol (EIGRP) routing process to run within a VPN routing and forwarding (VRF) instance, use the **autonomous-system** command in address-family configuration mode. To remove the autonomous-system for an EIGRP routing process from within a VPN VRF instance, use the **no** form of this command.
Autonomous-system *autonomous-system-number*
no autonomous-system *autonomous-system-number*

Reference: http://www.cisco.com/c/en/us/td/docs/ios/iproute_eigrp/command/reference/ire_book/ire_a1.html#wp1062796

QUESTION 25
What is the default OSPF hello interval on a Frame Relay point-to-point network?

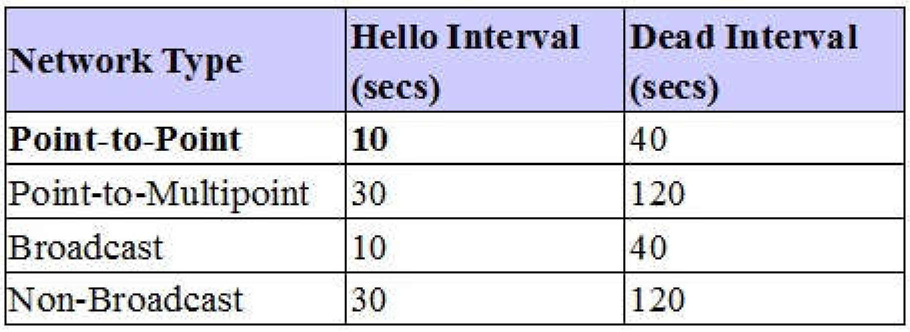
A. 10
B. 20
C. 30
D. 40

Correct Answer: A
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Before you troubleshoot any OSPF neighbor-related issues on an NBMA network, it is important to remember that an NBMA network can be configured in these modes of operation with the **ip ospf network** command:

- Point-to-Point
- Point-to-Multipoint
- Broadcast
- NBMA

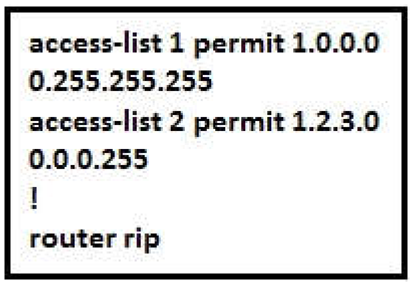
The Hello and Dead Intervals of each mode are described in this table:



Network Type	Hello Interval (secs)	Dead Interval (secs)
Point-to-Point	**10**	40
Point-to-Multipoint	30	120
Broadcast	10	40
Non-Broadcast	30	120

Reference: http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13693-22.html

QUESTION 26
Refer to the exhibit.



```
access-list 1 permit 1.0.0.0
0.255.255.255
access-list 2 permit 1.2.3.0
0.0.0.255
!
router rip
```

Which command only announces the 1.2.3.0/24 network out of FastEthernet 0/0?

A. distribute list 1 out
B. distribute list 1 out FastEthernet0/0
C. distribute list 2 out
D. distribute list 2 out FastEthernet0/0

Correct Answer: D
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Access list 2 is more specific, allowing only 1.2.3.0/24, whereas access list 1 permits all 1.0.0.0/8 networks. This question also asks us to apply this distribute list only to the outbound direction of the fast Ethernet 0/0 interface, so the correct command is “distribute list 2 out FastEthernet0/0.”

QUESTION 27
Which prefix is matched by the command ip prefix-list name permit 10.8.0.0/16 ge 24 le 24?

A. 10.9.1.0/24
B. 10.8.0.0/24
C. 10.8.0.0/16
D. 10.8.0.0/23

Correct Answer: B
Section: Layer 3 Technologies
Explanation

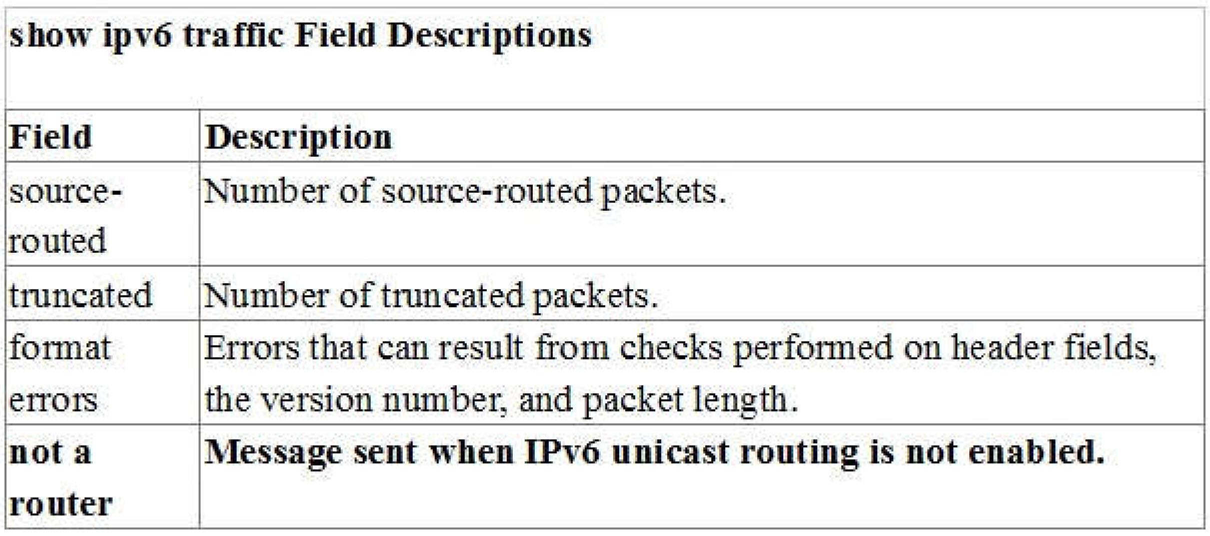
Explanation/Reference:
Explanation:
With prefix lists, the ge 24 term means greater than or equal to a /24 and the le 24 means less than or equal to /24, so only a /24 is both greater than or equal to 24 and less than or equal to 24. This translates to any prefix in the 10.8.x.0/24 network, where X is any value in the 0-255 range. Only the choice of 10.8.0.0.24 matches this.

QUESTION 28
Router A and Router B are configured with IPv6 addressing and basic routing capabilities using oSPFv3. The networks that are advertised from Router A do not show up in Router B's routing table. After debugging IPv6 packets, the message "not a router" is found in the output. Why is the routing information not being learned by Router B?

A. OSPFv3 timers were adjusted for fast convergence.
B. The networks were not advertised properly under the OSPFv3 process.
C. An IPv6 traffic filter is blocking the networks from being learned via the Router B interface that is connected to Router A.
D. IPv6 unicast routing is not enabled on Router A or Router B.

Correct Answer: D
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:



show ipv6 traffic Field Descriptions

Field	Description
source-routed	Number of source-routed packets.
truncated	Number of truncated packets.
format errors	Errors that can result from checks performed on header fields, the version number, and packet length.
not a router	**Message sent when IPv6 unicast routing is not enabled.**

Reference: http://www.cisco.com/c/en/us/td/docs/ios/ipv6/command/reference/ipv6_book/ipv6_16.html

QUESTION 29
After you review the output of the command show ipv6 interface brief, you see that several IPv6 addresses have the 16-bit hexadecimal value of "fFFE" inserted into the address. Based on this information, what do you conclude about these IPv6 addresses?

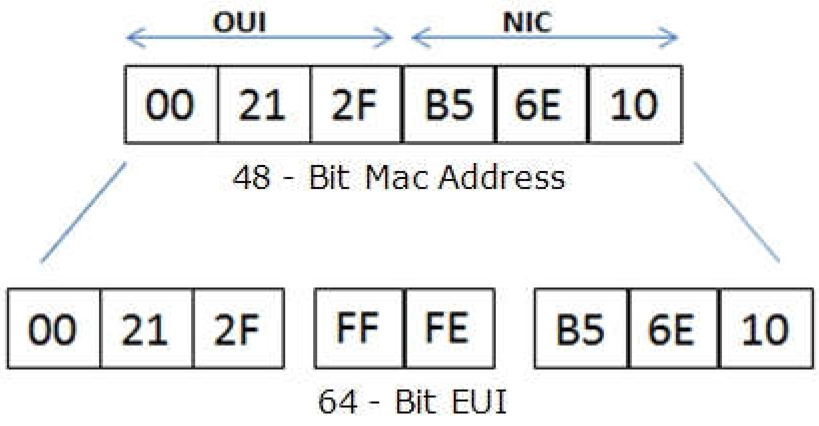
A. IEEE EUI-64 was implemented when assigning IPv6 addresses on the device.

B. The addresses were misconfigured and will not function as intended.
C. IPv6 addresses containing "FFFE" indicate that the address is reserved for multicast.
D. The IPv6 universal/local flag (bit 7) was flipped.
E. IPv6 unicast forwarding was enabled, but IPv6 Cisco Express Forwarding was disabled.

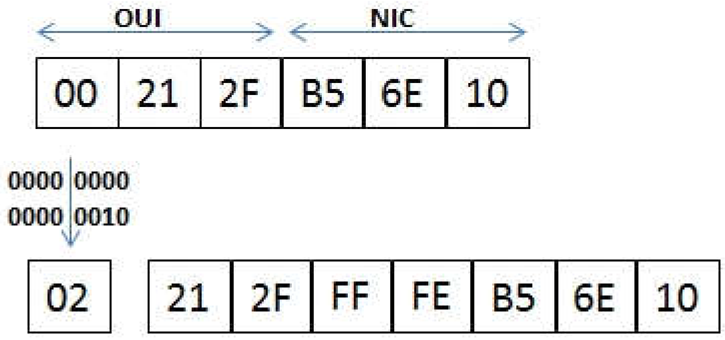
Correct Answer: A
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Extended Unique Identifier (EUI), as per RFC2373, allows a host to assign iteslf a unique 64-Bit IP Version 6 interface identify them EUI-64). This feature is a key benefit over IPv4 as it eliminates the need of manual configuration or DHCP as in the world of IPv4. The IPv6 EUI-64 format address is obtained through the 48-bit MAC address. The Mac address is first separated into two 24-bits, with one being OUI (Organizationally Unique Identifier) and the other being NIC specific. The 16-bit 0xFFFE is then inserted between these two 24-bits to for the 64-bit EUI address. **IEEE has chosen FFFE as a reserved value which can only appear in EUI-64 generated from the EUI-48 MAC address**.

Here is an example showing how the Mac Address is used to generate EUI.



Next, the seventh bit from the left, or the universal/local (U/L) bit, needs to be inverted. This bit identifies whether this interface identifier is universally or locally administered. If 0, the address is locally administered and if 1, the address is globally unique. It is worth noticing that in the OUI portion, the globally unique addresses assigned by the IEEE have always been set to 0 whereas the locally created addresses have 1 configured. Therefore, when the bit is inverted, it maintains its original scope (global unique address is still global unique and vice versa). The reason for inverting can be found in RFC4291 section 2.5.1.



Once the above is done, we have a fully functional EUI-64 format address.

Reference: https://supportforums.cisco.com/document/100566/understanding-ipv6-eui-64-bit-address

QUESTION 30
A packet capture log indicates that several router solicitation messages were sent from a local host on the Ipv6 segment. What is the expected acknowledgment and its usage?

A. Router acknowledgment messages will be forwarded upstream, where the DHCP server will allocate addresses to the local host.
B. Routers on the Ipv6 segment will respond with an advertisement that provides an external path from the local subnet, as well as certain data, such as prefix discovery.
C. Duplicate Address Detection will determine if any other local host is using the same Ipv6 address for communication with the Ipv6 routers on the segment.
D. All local host traffic will be redirected to the router with the lowest ICMPv6 signature, which is statically defined by the network administrator.

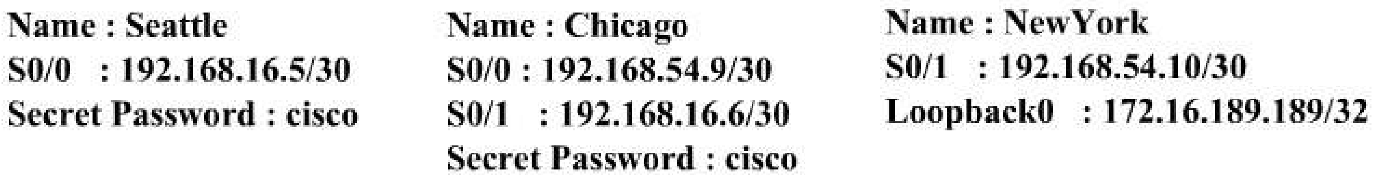
Correct Answer: B
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Router Advertisements (RA) are sent in response to router solicitation messages. Router solicitation messages, which have a value of 133in the Type field of the ICMP packet header, are sent by hosts at system startup so that the host can immediately autoconfigure without needing to wait for the next scheduled RA message. Given that router solicitation messages are usually sent by hosts at system startup (the host does not have a configured unicast address), the source address in router solicitation messages is usually the unspecified Ipv6 address (0:0:0:0:0:0:0:0). If the host has a configured unicast address, the unicast address of the interface sending the router solicitation message is used as the source address in the message. The destination address in router solicitation messages is the all-routers multicast address with a scope of the link. When an RA is sent in response to a router solicitation, the destination address in the RA message is the unicast address of the source of the router solicitation message.
RA messages typically include the following information:
- One or more on link Ipv6 prefixes that nodes on the local link can use to automatically configure their Ipv6 addresses
- Lifetime information for each prefix included in the advertisement
- Sets of flags that indicate the type of autoconfiguration (stateless or stateful) that can be completed
- Default router information (whether the router sending the advertisement should be used as a default router and, if so, the amount of time (in seconds) the

router should be used as a default router)
• Additional information for hosts, such as the hop limit and MTU a host should use in packets that it originates

QUESTION 31
SIMULATION
Route.com is a small IT corporation that is attempting to implement the network shown in the exhibit. Currently the implementation is partially completed. OSPF has been configured on routers Chicago and NewYork. The SO/O interface on Chicago and the SO/1 interface on NewYork are in Area 0. The loopbackO interface on NewYork is in Area 1. However, they cannot ping from the serial interface of the Seattle router to the loopback interface of the NewYork router. You have been asked to complete the implementation to allow this ping.
ROUTE.com's corporate implementation guidelines require:
• The OSPF process ID for all routers must be 10.
• The routing protocol for each interface must be enabled under the routing process.
• The routing protocol must be enabled for each interface using the most specific wildcard mask possible.
• The serial link between Seattle and Chicago must be in OSPF area 21.
• OSPF area 21 must not receive any inter-area or external routes.

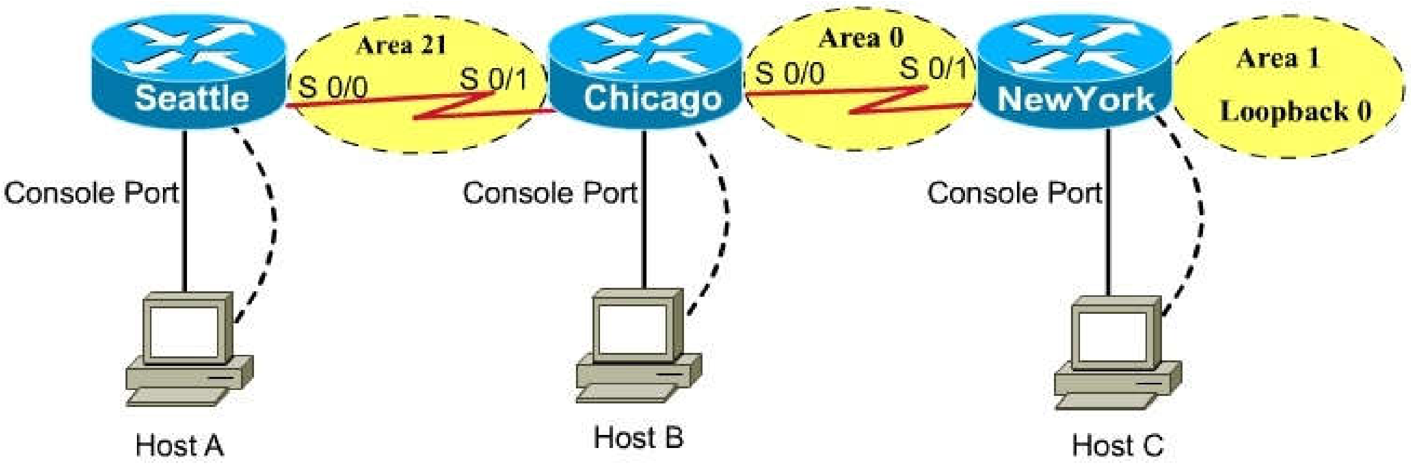
Network Information
Seattle
S0/0 192.168.16.5/30 — Link between Seattle and Chicago
Secret Password: cisco
Chicago
S0/0 192.168.54.9/30 — Link between Chicago and New York
S0/1 192.168.16.6/30 — Link between Seattle and Chicago
Secret Password: cisco
New York
S0/1 192.168.54.10/30 — Link between Chicago and New York
Loopback0 172.16.189.189
Secret Password: cisco

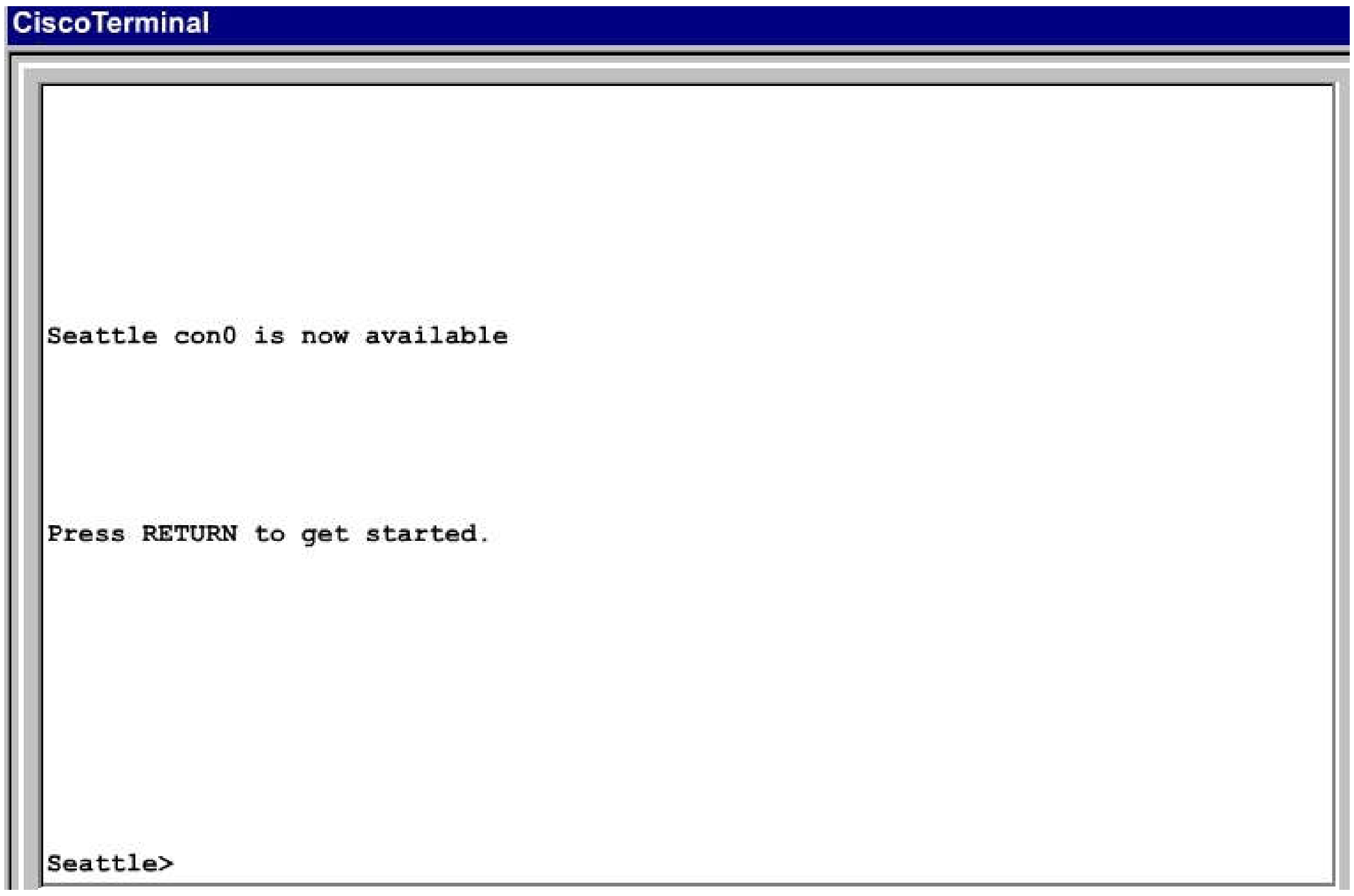


Name : Seattle
S0/0 : 192.168.16.5/30
Secret Password : cisco

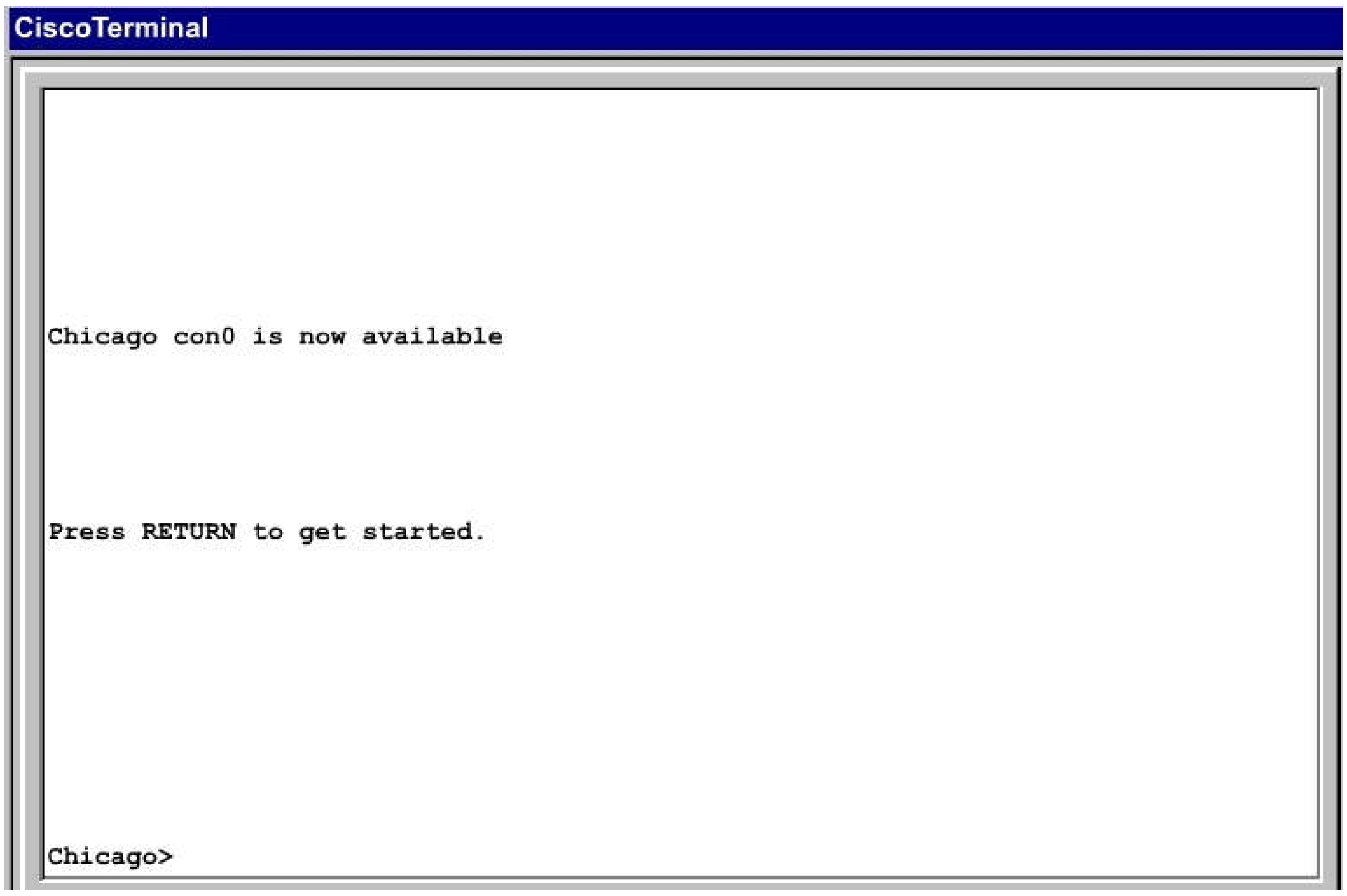
Name : Chicago
S0/0 : 192.168.54.9/30
S0/1 : 192.168.16.6/30
Secret Password : cisco

Name : NewYork
S0/1 : 192.168.54.10/30
Loopback0 : 172.16.189.189/32

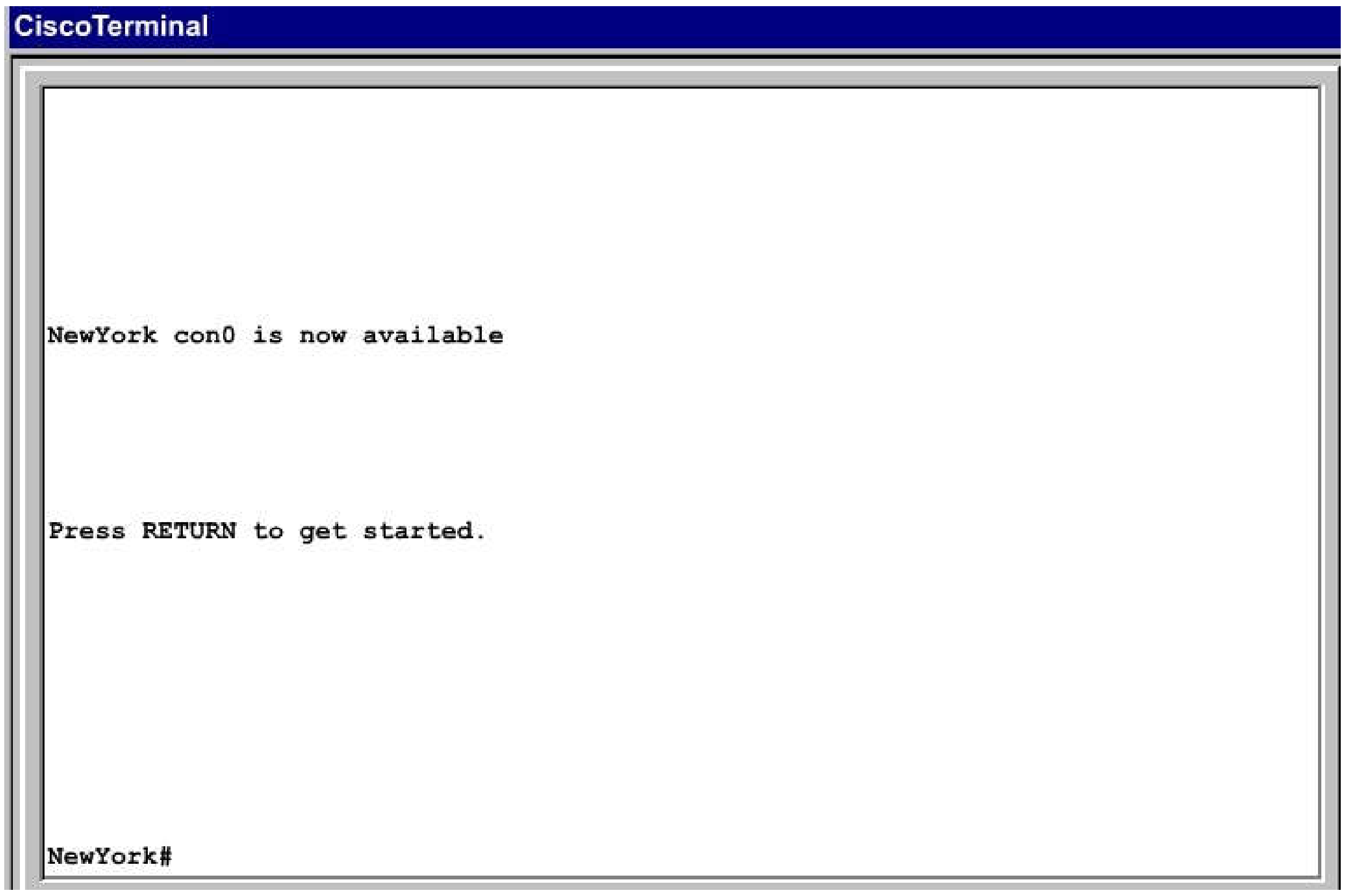




```
Seattle con0 is now available



Press RETURN to get started.





Seattle>
```



```
Chicago con0 is now available


Press RETURN to get started.



Chicago>
```



```
NewYork con0 is now available


Press RETURN to get started.



NewYork#
```

Correct Answer: See explanation below
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:

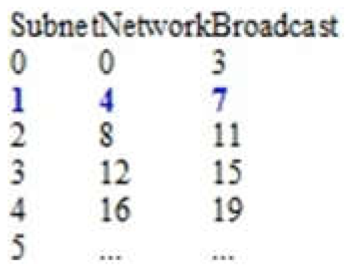
Note: In actual exam, the IP addressing, OSPF areas and process ID, and router hostnames may change, but the overall solution is the same.

Seattle’s S0/0 IP Address is 192.168.16.5/30. So, we need to find the network address and wildcard mask of 192.168.16.5/30 in order to configure the OSPF.

IP Address: 192.168.16.5 /30
Subnet Mask: 255.255.255.252

Here subtract 252 from 2565, 256-252 = 4, hence the subnets will increment by 4.

First, find the 4thoctet of the Network Address:



Subnet	Network	Broadcast
0	0	3
1	4	7
2	8	11
3	12	15
4	16	19
5	...	...

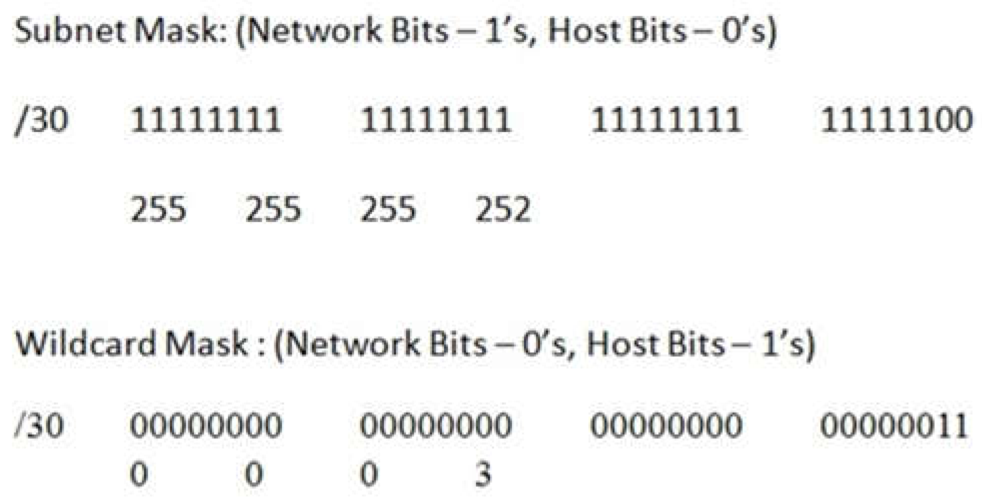
The 4thoctet of IP address (192.168.16.5) belongs to subnet 1 (4 to 7).

Network Address: 192.168.16.4
Broadcast Address: 192.168.16.7

Let's find the wildcard mask of /30.

Subnet Mask: (Network Bits – 1's, Host Bits – 0's)

Let's find the wildcard mask of /30:



Subnet Mask: (Network Bits – 1's, Host Bits – 0's)

```
/30   11111111   11111111   11111111   11111100

      255   255   255   252
```

Wildcard Mask : (Network Bits – 0's, Host Bits – 1's)

```
/30   00000000   00000000   00000000   00000011
      0     0     0     3
```

Now we configure OSPF using process ID 10 (note the process ID may change to something else in real exam).

```
Seattle>enable
Password:
Seattle#conf t
Seattle(config)#router ospf 10

Seattle(config-router)#network 192.168.16.4 0.0.0.3 area 21
```

One of the tasks states that area 21 should not receive any external or inter-area routes (except the default route).

```
Seattle(config-router)#area 21 stub
Seattle(config-router)#end
Seattle#copy run start
```

Chicago Configuration:

```
Chicago>enable
Password: cisco
Chicago#conf t
Chicago(config)#router ospf10
```

We need to add Chicago's S0/1 interface to Area 21

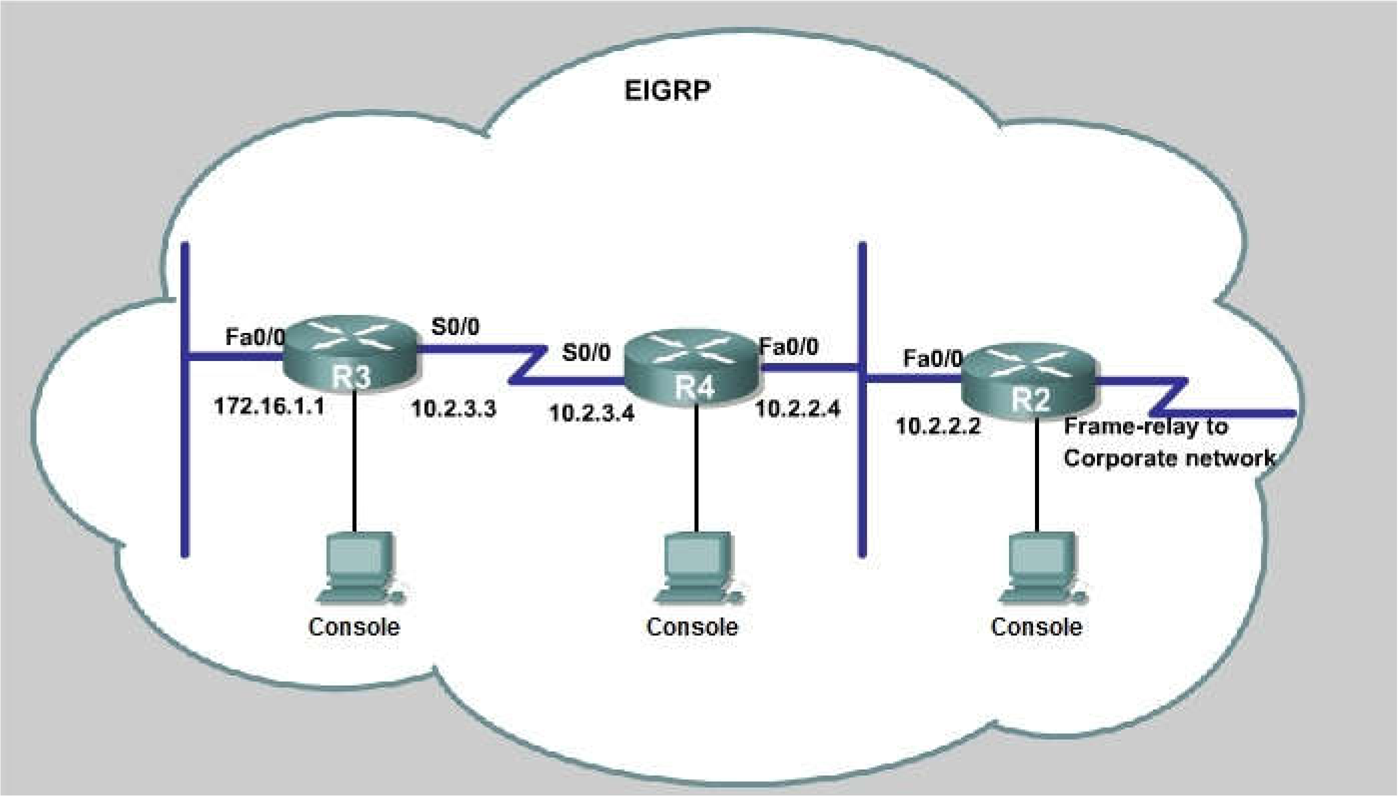
```
Chicago(config-router)#network 192.168.16.4 0.0.0.3 area 21
```

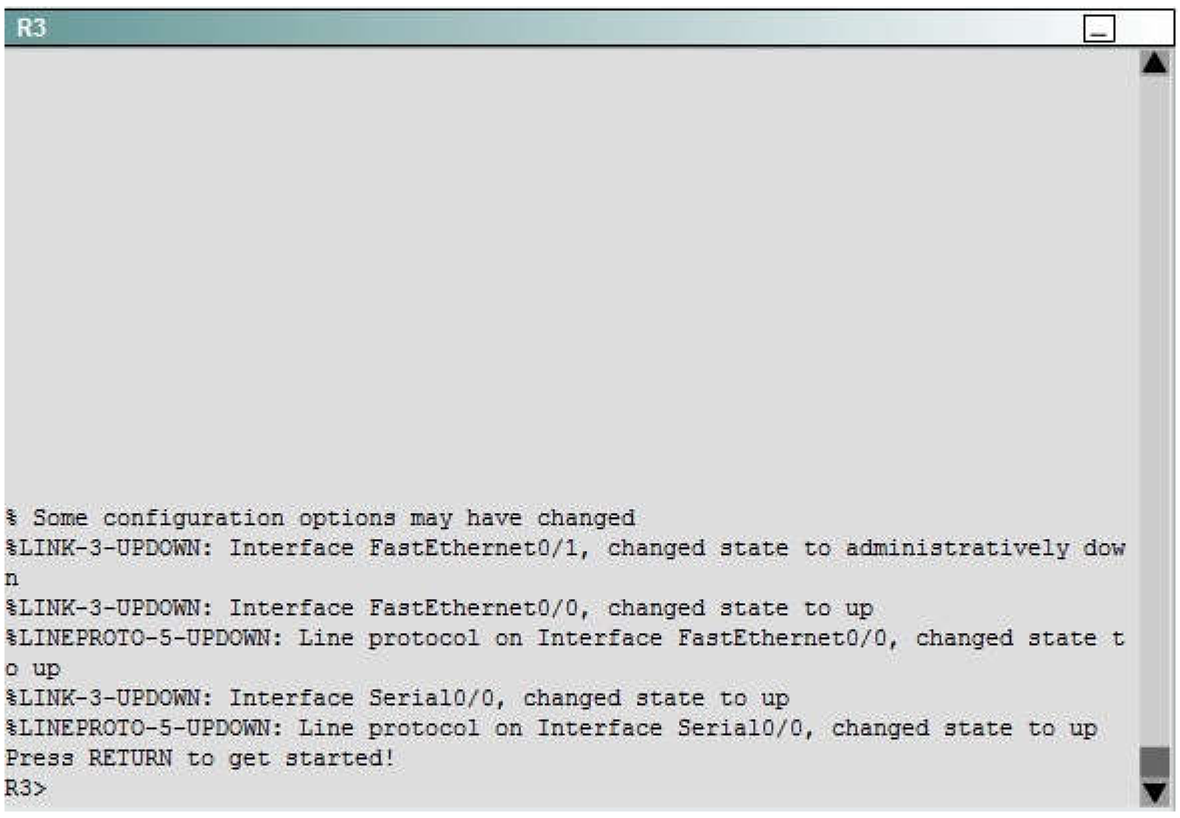
Again, area 21 should not receive any external or inter-area routes (except the default route).
In order to accomplish this, we must stop LSA Type 5 if we don't want to send external routes. And if we don't want to send inter-area routes, we have to stop LSA Type 3 and Type 4. There fore we want to configure area 21 as a totally stubby area.

```
Chicago(config-router)#area 21 stub no-summary

Chicago(config-router)#end
Chicago#copy run start
```

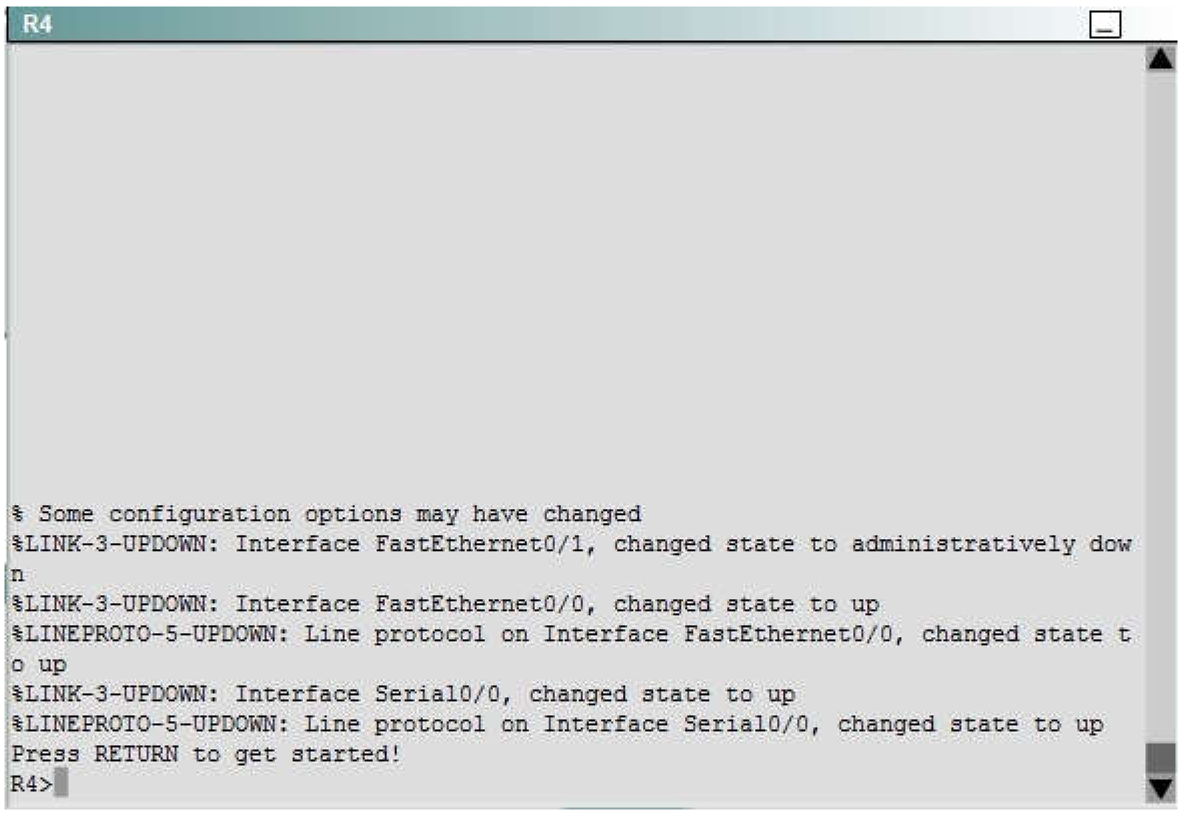
The other interface on the Chicago router is already configured correctly in this scenario, as well as the New York router so there is nothing that needs to be done on that router.

QUESTION 32
SIMULATION
JS Industries has expanded their business with the addition of their first remote office. The remote office router (R3) was previously configured and all corporate subnets were reachable from R3. JS Industries is interested in using route summarization along with the EIGRP Stub Routing feature to increase network stability while reducing the memory usage and bandwidth utilization to R3. Another network professional was tasked with implementing this solution. However, in the process of configuring EIGRP stub routing connectivity with the remote network devices off of R3 has been lost.
Currently EIGRP is configured on all routers R2, R3, and R4 in the network. Your task is to identify and resolve the cause of connectivity failure with the remote office router R3. Once the issue has been resolved you should complete the task by configuring route summarization only to the remote office router R3.
You have corrected the fault when pings from R2 to the R3 LAN interface are successful, and the R3 IP routing table only contains 2 10.0.0.0 subnets.

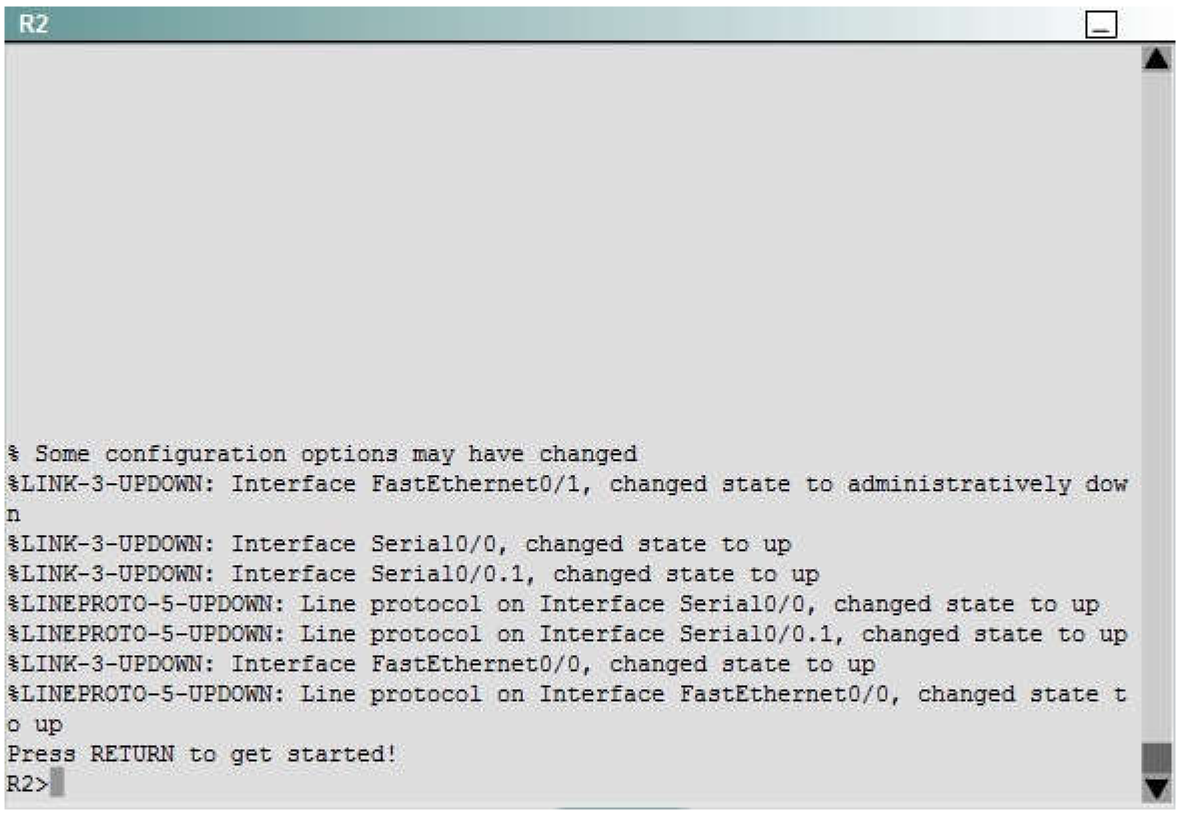




```
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
Press RETURN to get started!
R3>
```



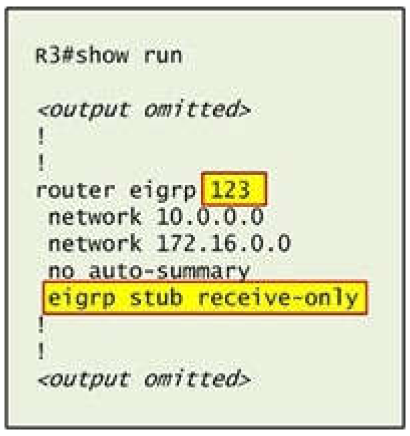
```
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
Press RETURN to get started!
R4>
```



```
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
%LINK-3-UPDOWN: Interface Serial0/0, changed state to up
%LINK-3-UPDOWN: Interface Serial0/0.1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0.1, changed state to up
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
Press RETURN to get started!
R2>
```

Correct Answer: See explanation below
Section: Layer 3 Technologies
Explanation

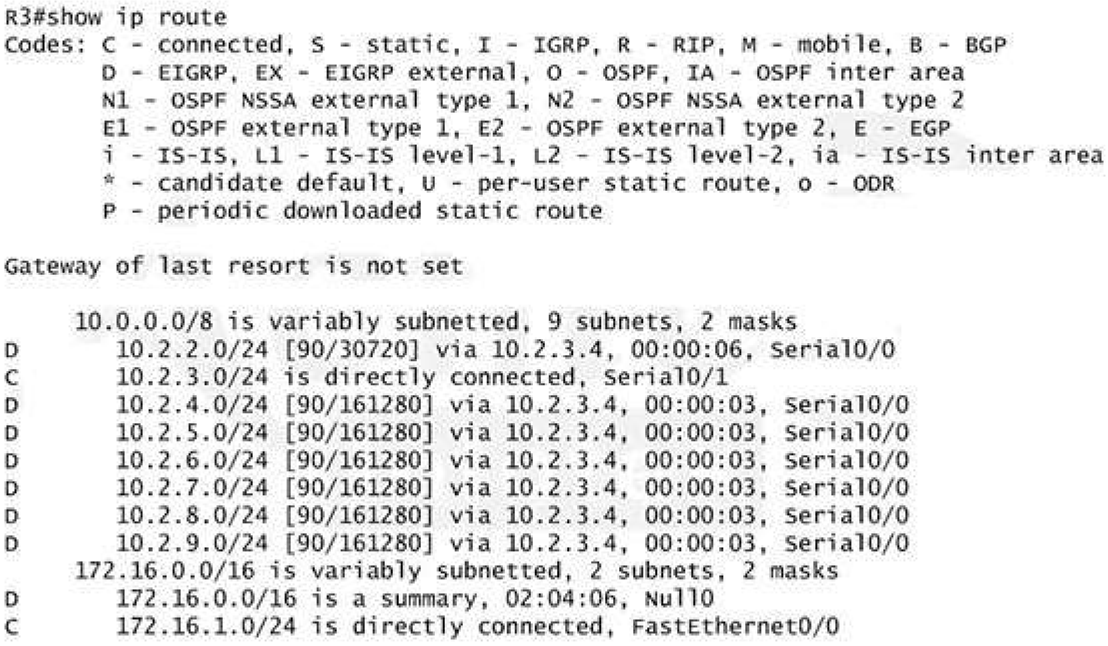
Explanation/Reference:
Explanation:
First we have to figure out why R3 and R4 can not communicate with each other. Use the show running-config command on router R3.



```
R3#show run

<output omitted>
!
!
router eigrp 123
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
 eigrp stub receive-only
!
!
<output omitted>
```

Notice that R3 is configured as a stub receive-only router. The receive-only keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system. This keyword will also prevent any type of route from being sent. Therefore we will remove this command and replace it with the eigrp stub command:
R3# configure terminal R3(config)# router eigrp 123 R3(config-router)# no eigrp stub receive-only R3(config-router)# eigrp stub
R3(config-router)# end

Now R3 will send updates containing its connected and summary routes to other routers. Notice that the eigrp stub command equals to the eigrp stub connected summary because the connected and summary options are enabled by default.
Next we will configure router R3 so that it has only 2 subnets of 10.0.0.0 network. Use the show ip route command on R3 to view its routing table:



```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
D       10.2.2.0/24 [90/30720] via 10.2.3.4, 00:00:06, Serial0/0
C       10.2.3.0/24 is directly connected, Serial0/1
D       10.2.4.0/24 [90/161280] via 10.2.3.4, 00:00:03, Serial0/0
D       10.2.5.0/24 [90/161280] via 10.2.3.4, 00:00:03, Serial0/0
D       10.2.6.0/24 [90/161280] via 10.2.3.4, 00:00:03, Serial0/0
D       10.2.7.0/24 [90/161280] via 10.2.3.4, 00:00:03, Serial0/0
D       10.2.8.0/24 [90/161280] via 10.2.3.4, 00:00:03, Serial0/0
D       10.2.9.0/24 [90/161280] via 10.2.3.4, 00:00:03, Serial0/0
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 02:04:06, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
```

Because we want the routing table of R3 only have 2 subnets so we have to summary sub-networks at the interface which is connected with R3, the s0/0 interface of R4.

There is one interesting thing about the output of the show ip route shown above: the 10.2.3.0/24, which is a directly connected network of R3. We can’t get rid of it in the routing table no matter what technique we use to summary the networks. Therefore, to make the routing table of R3 has only 2 subnets we have to summary other subnets into one subnet.

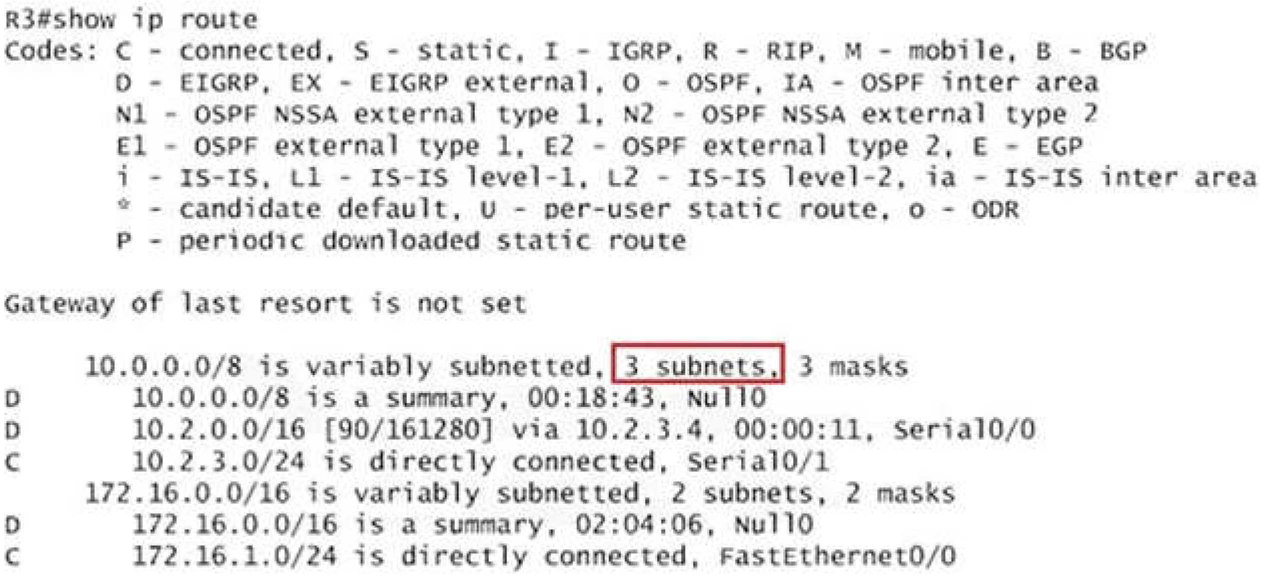
In the output if we don’t see the summary line (like 10.0.0.0/8 is a summary…) then we should use the command ip summary-address eigrp 123 10.2.0.0

255.255.0.0 so that all the ping can work well.

In conclusion, we will use the ip summary-address eigrp 123 10.2.0.0 255.255.0.0 at the interface s0/0 of R4 to summary.

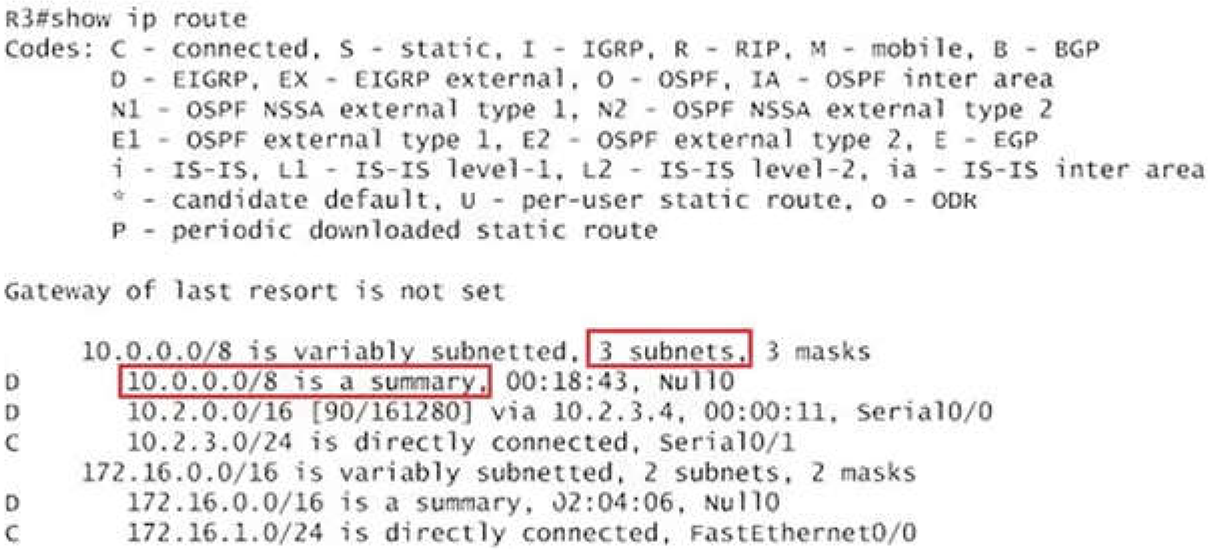
R4> enable R4# conf t
R4(config)# interface s0/0 R4(config-if)# ip summary-address eigrp 123 10.2.0.0 255.255.0.0

Now we jump back to R3 and use the show ip route command to verify the effect, the output is shown below:



```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
D       10.0.0.0/8 is a summary, 00:18:43, Null0
D       10.2.0.0/16 [90/161280] via 10.2.3.4, 00:00:11, Serial0/0
C       10.2.3.0/24 is directly connected, Serial0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 02:04:06, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
```

Note: Please notice that the IP addresses and the subnet masks in your real exam might be different so you might use different ones to solve this question.
Just for your information, notice that if you use another network than 10.0.0.0/8 to summary, for example, if you use the command ip summary-address eigrp 123 10.2.0.0 255.255.0.0 you will leave a /16 network in the output of the show ip route command.



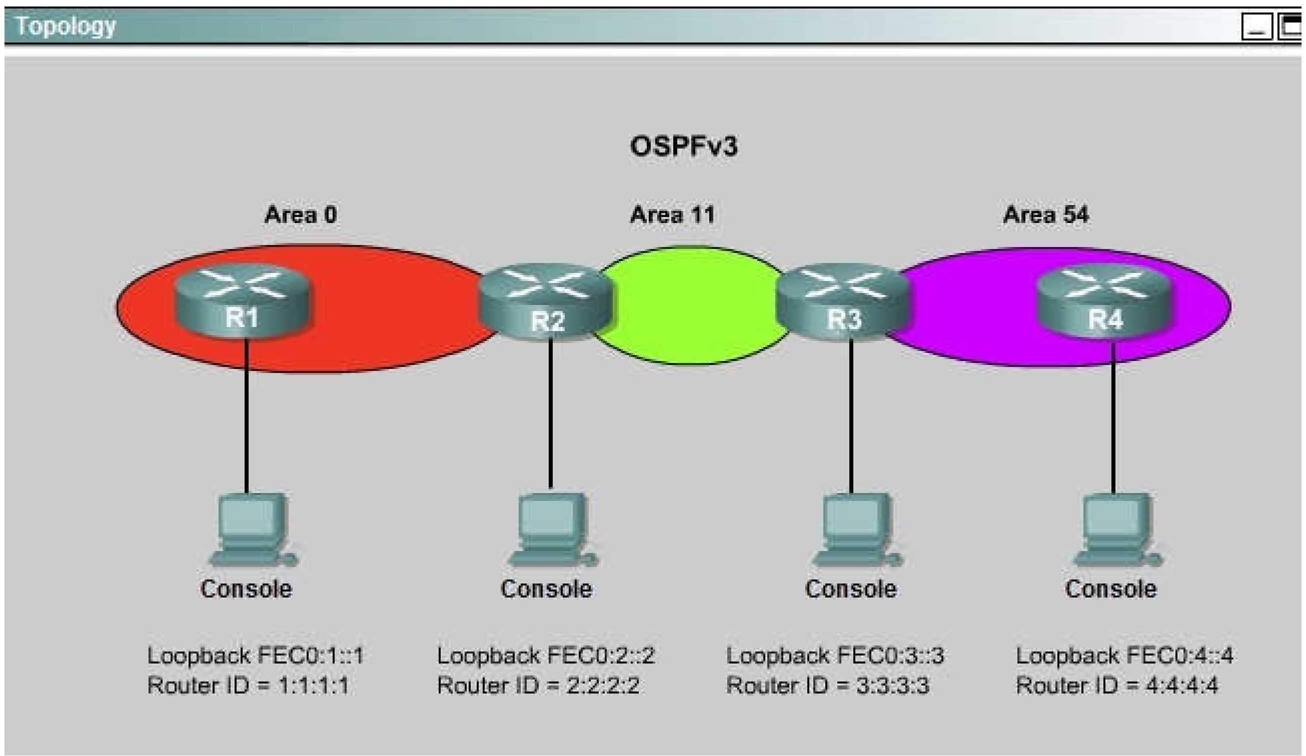
```
R3#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 3 subnets, 3 masks
D       10.0.0.0/8 is a summary, 00:18:43, Null0
D       10.2.0.0/16 [90/161280] via 10.2.3.4, 00:00:11, Serial0/0
C       10.2.3.0/24 is directly connected, Serial0/1
     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
D       172.16.0.0/16 is a summary, 02:04:06, Null0
C       172.16.1.0/24 is directly connected, FastEthernet0/0
```

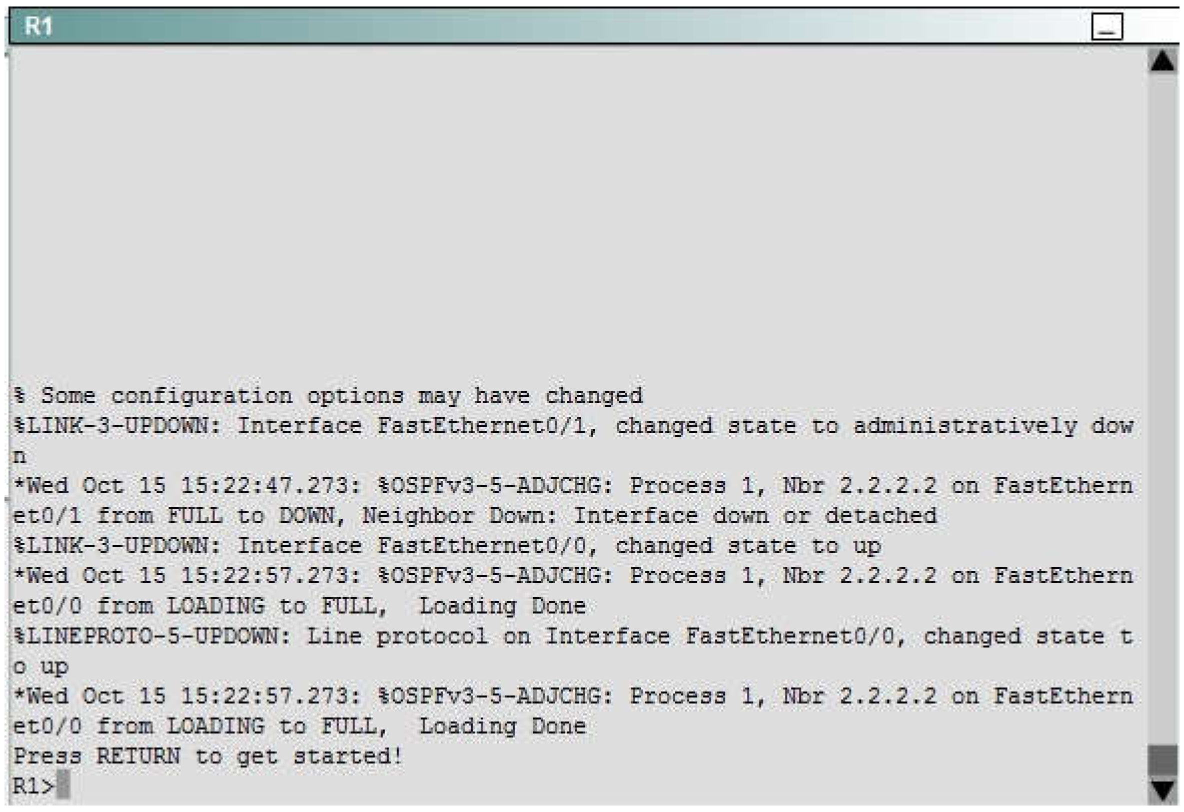
But in your real exam, if you don’t see the line “10.0.0.0/8 is a summary, Null0” then you can summarize using the network 10.2.0.0/16. This summarization is better because all the pings can work well.
Finally don’t forget to use the copy run start command on routers R3 and R4 to save the configurations.
R3(config-if)# end
R3# copy run start
R4(config-if)# end
R4# copy run start

If the “copy run start” command doesn’t work then use “write memory.”

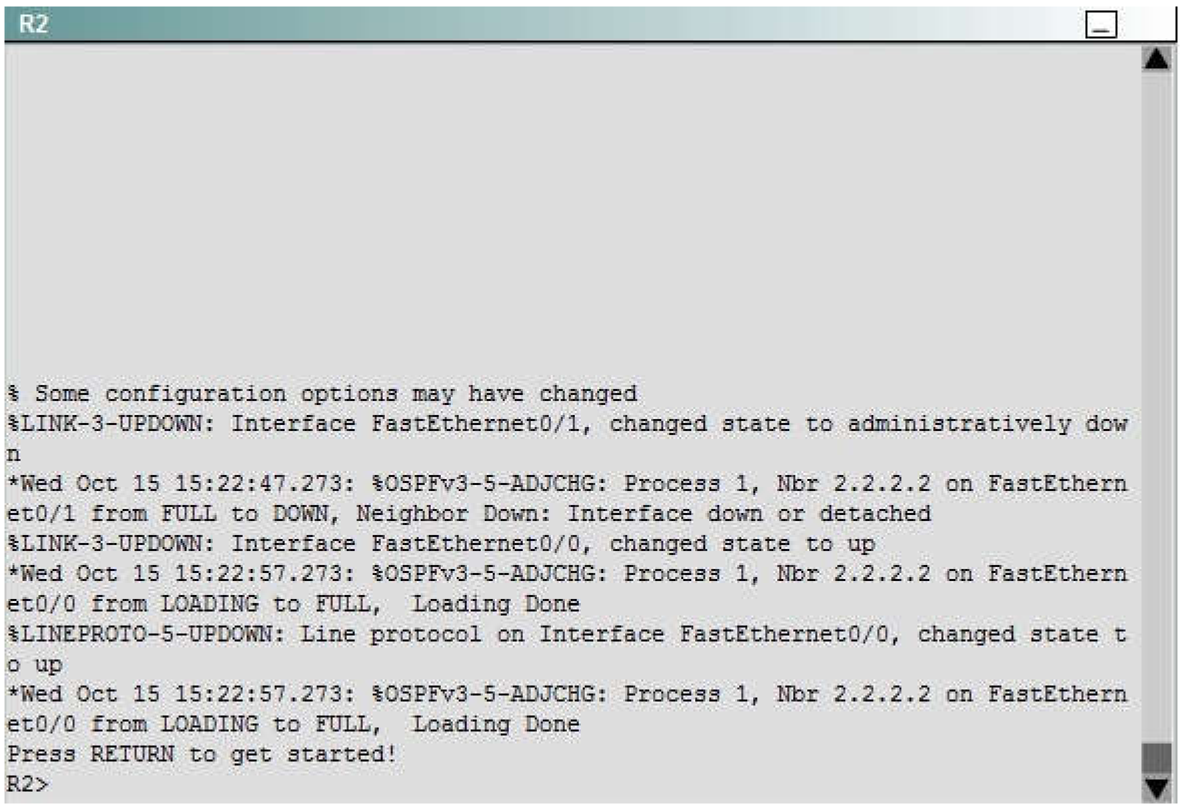
QUESTION 33
SIMULATION
ROUTE.com is a small IT corporation that has an existing enterprise network that is running Ipv6 0SPFv3. Currently OSPF is configured on all routers. However, R4’s loopback address (FEC0:4:4) cannot be seen in R1’s Ipv6 routing table. You are tasked with identifying the cause of this fault and implementing the needed corrective actions that uses OPSF features and does not change the current area assignments. You will know that you have corrected the fault when R4’s loopback address (FEC0:4:4) can be seen in RTs Ipv6 routing table.

Special Note: To gain the maximum number of points you must remove all incorrect or unneeded configuration statements related to this issue.

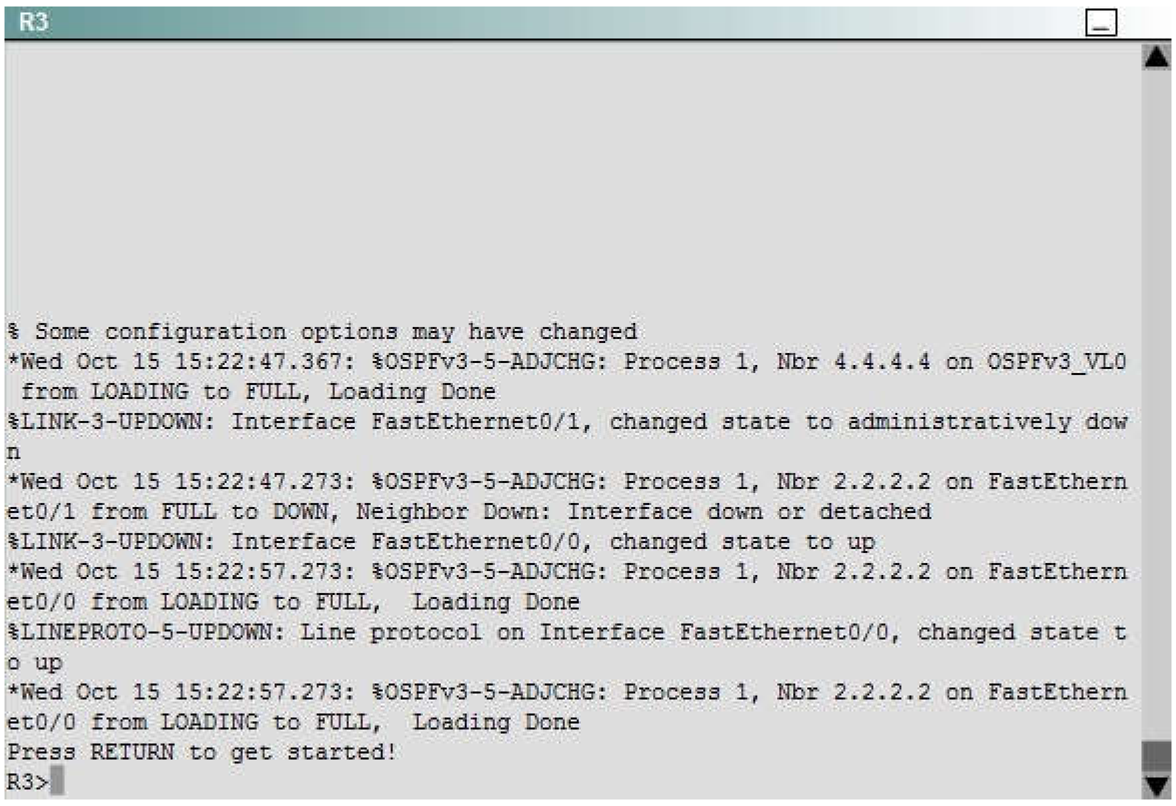




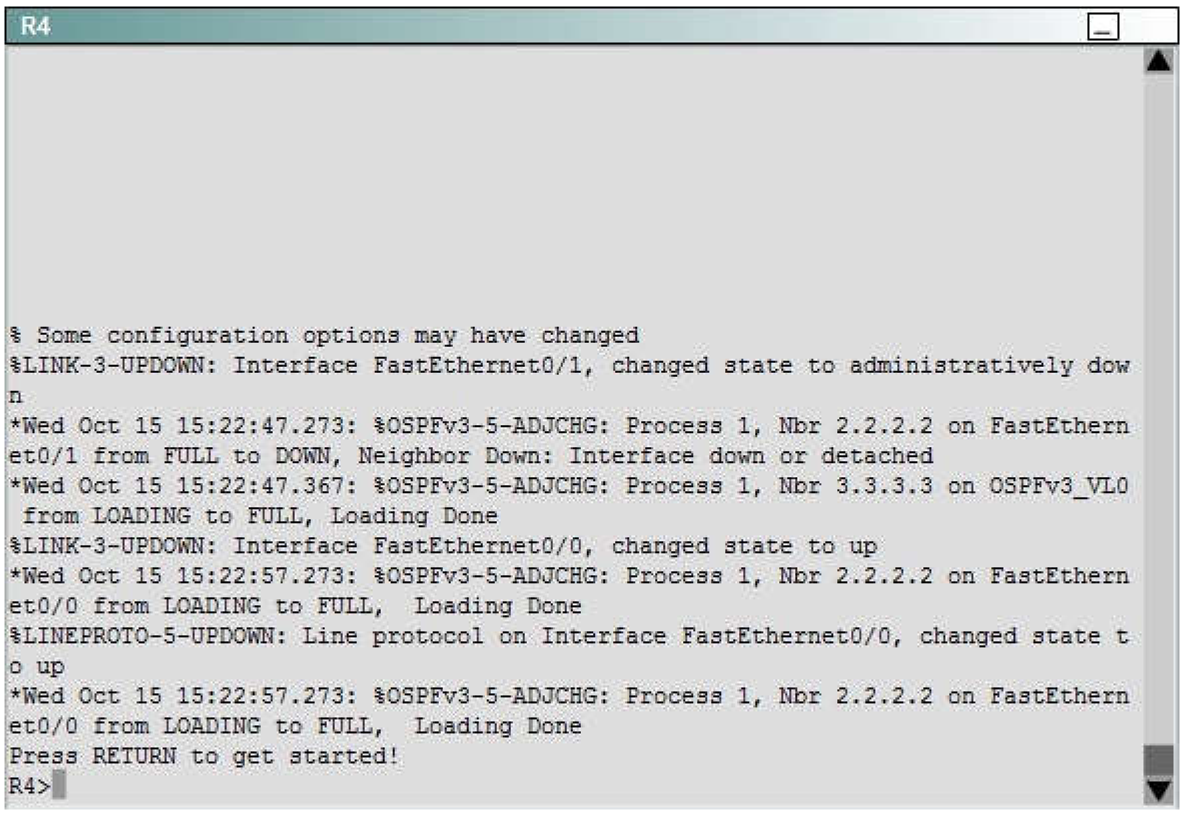
```
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
Press RETURN to get started!
R1>
```



```
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
Press RETURN to get started!
R2>
```



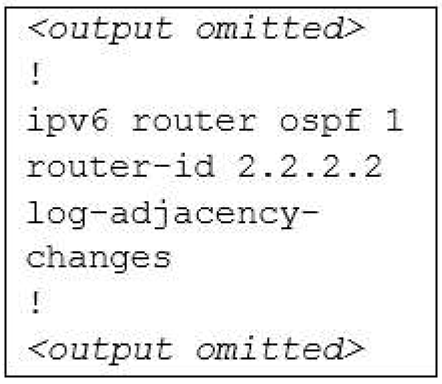
```
% Some configuration options may have changed
*Wed Oct 15 15:22:47.367: %OSPFv3-5-ADJCHG: Process 1, Nbr 4.4.4.4 on OSPFv3_VL0
 from LOADING to FULL, Loading Done
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
Press RETURN to get started!
R3>
```



```
% Some configuration options may have changed
%LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to administratively dow
n
*Wed Oct 15 15:22:47.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/1 from FULL to DOWN, Neighbor Down: Interface down or detached
*Wed Oct 15 15:22:47.367: %OSPFv3-5-ADJCHG: Process 1, Nbr 3.3.3.3 on OSPFv3_VL0
 from LOADING to FULL, Loading Done
%LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state t
o up
*Wed Oct 15 15:22:57.273: %OSPFv3-5-ADJCHG: Process 1, Nbr 2.2.2.2 on FastEthern
et0/0 from LOADING to FULL,  Loading Done
Press RETURN to get started!
R4>
```

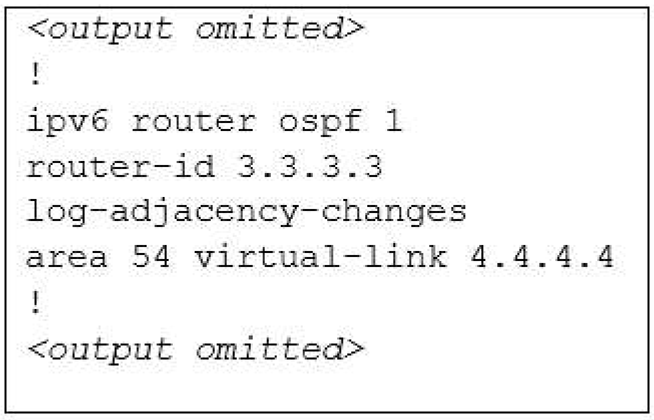
Correct Answer: See explanation below
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
To troubleshoot the problem, first issue the show running-config on all of 4 routers. Pay more attention to the outputs of routers R2 and R3 The output of the "show running-config" command of R2:



```
<output omitted>
!
ipv6 router ospf 1
router-id 2.2.2.2
log-adjacency-
changes
!
<output omitted>
```

The output of the "show running-config" command of R3:

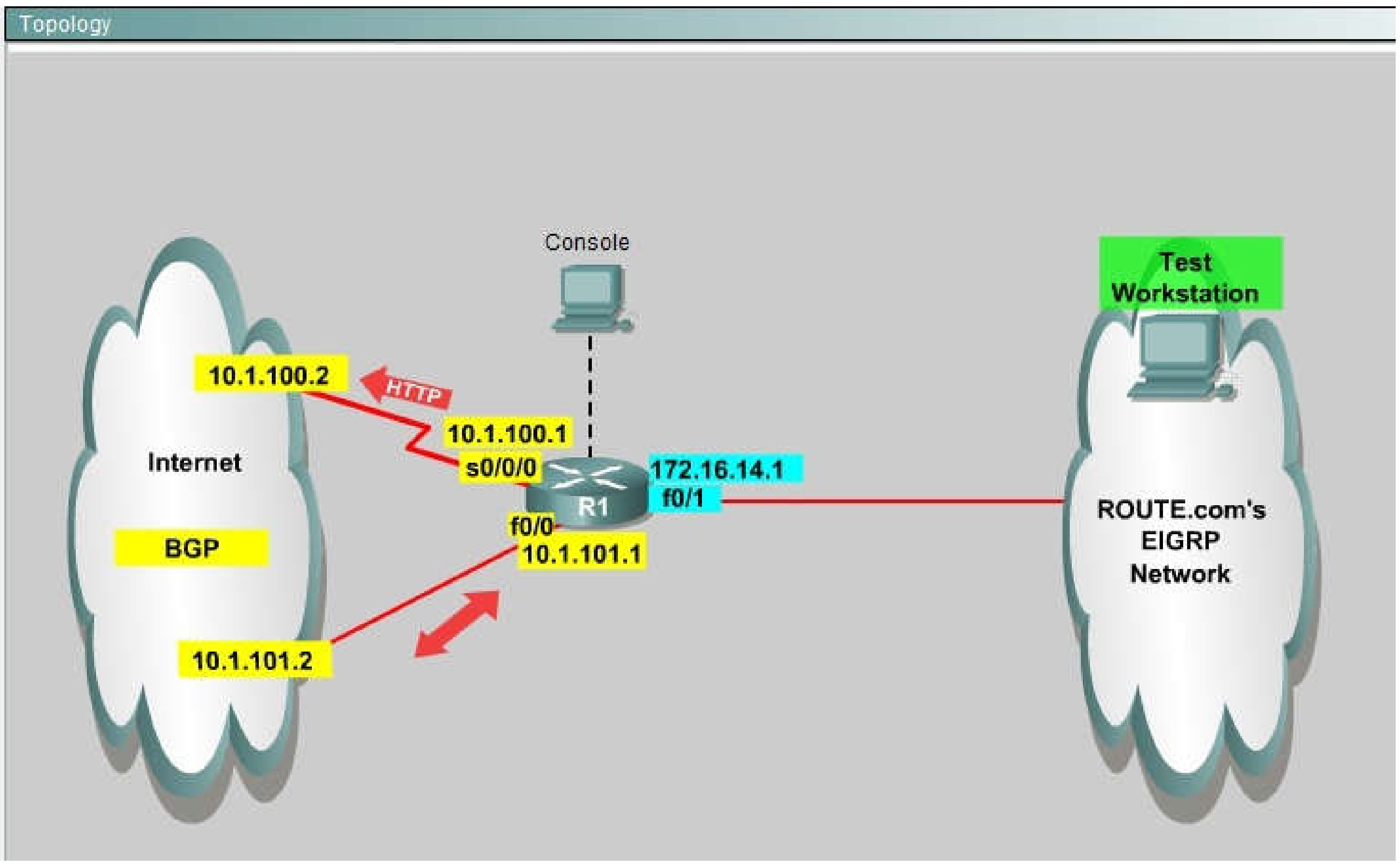


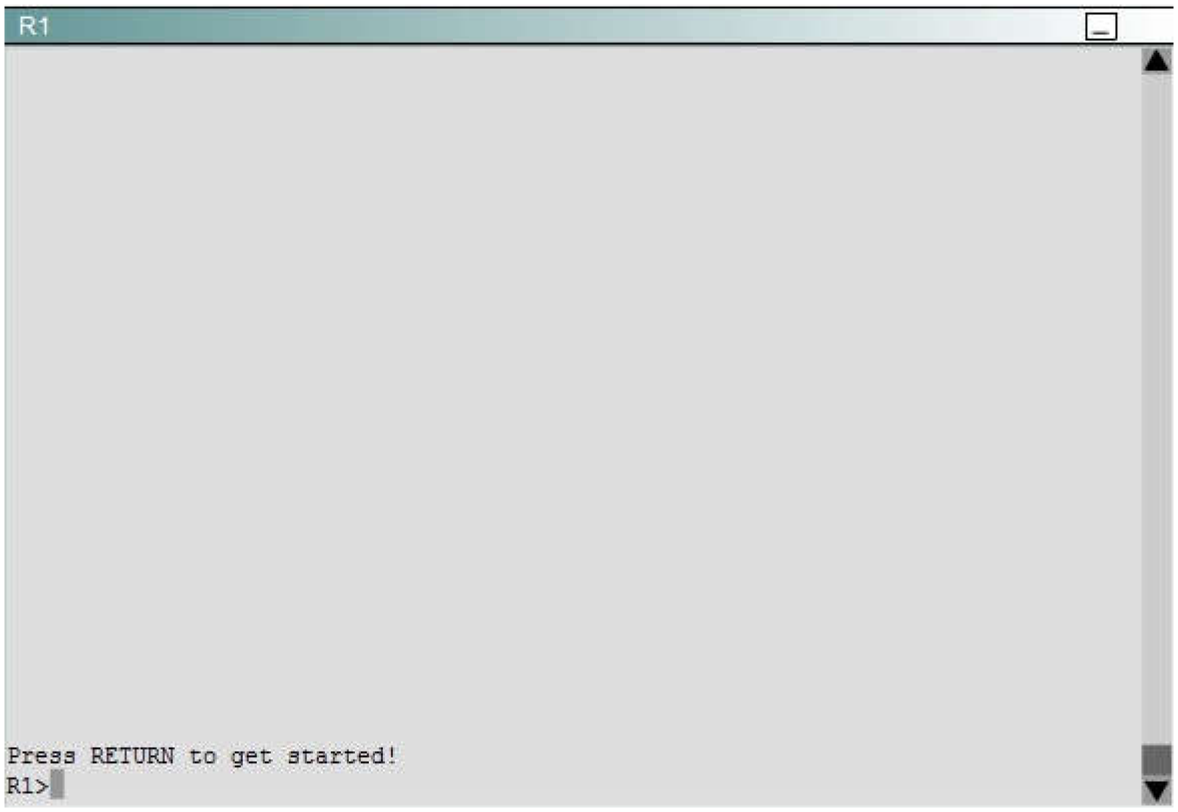
```
<output omitted>
!
ipv6 router ospf 1
router-id 3.3.3.3
log-adjacency-changes
area 54 virtual-link 4.4.4.4
!
<output omitted>
```

We knew that all areas in an Open Shortest Path First (OSPF) autonomous system must be physically connected to the backbone area (Area 0). In some cases, where this is not possible, we can use a virtual link to connect to the backbone through a non-backbone area. The area through which you configure the virtual link is known as a transit area. In this case, the area 11 will become the transit area. Therefore, routers R2 and R3 must be configured with the area <area id> virtual-link <neighbor router-id>command. + Configure virtual link on R2 (from the first output above, we learned that the OSPF process ID of R2 is 1):
R2>enable
R2#configure terminal
R2(config)#ipv6 router ospf 1
R2(config-rtr)#area 11 virtual-link 3.3.3.3
Save the configuration:
R2(config-rtr)#end
R2#copy running-config startup-config
(Notice that we have to use neighbor router-id 3.3.3.3, not R2's router-id 2.2.2.2) + Configure virtual link on R3 (from the second output above, we learned that the OSPF process ID of R3 is 1 and we have to disable the wrong configuration of "area 54 virtual-link 4.4.4.4"):
R3>enable
R3#configure terminal
R3(config)#ipv6 router ospf 1
R3(config-rtr)#no area 54 virtual-link 4.4.4.4
R3(config-rtr)#area 11 virtual-link 2.2.2.2
Save the configuration:
R3(config-rtr)#end
R3#copy running-config startup-config
You should check the configuration of R4, too. Make sure to remove the incorrect configuration statements to get the full points.
R4(config)#ipv6 router ospf 1
R4(config-router)#no area 54 virtual-link 3.3.3.3
R4(config-router)#end
After finishing the configuration doesn't forget to ping between R1 and R4 to make sure they work.
Note. If you want to check the routing information, use the show ipv6 route command, not "show ip route".

QUESTION 34
SIMULATION
You are a network engineer with ROUTE.com, a small IT company. ROUTE.com has two connections to the Internet; one via a frame relay link and one via an EoMPLS link. IT policy requires that all outbound HTTP traffic use the frame relay link when it is available. All other traffic may use either link. No static or default routing is allowed.

Choose and configure the appropriate path selection feature to accomplish this task. You may use the Test Workstation to generate HTTP traffic to validate your solution.





```
Press RETURN to get started!
R1>
```

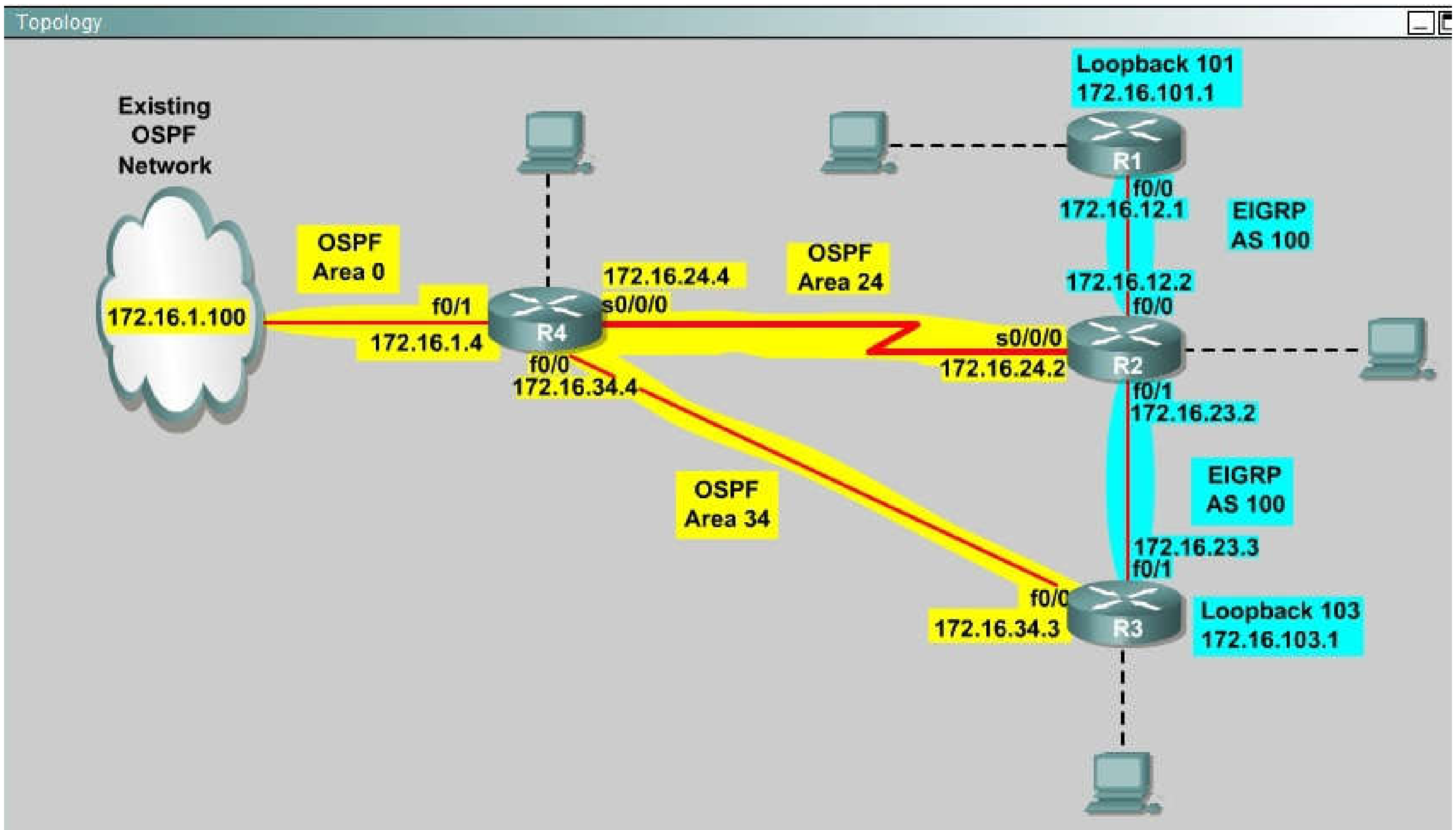
Correct Answer: See explanation below
Section: Layer 3 Technologies
Explanation

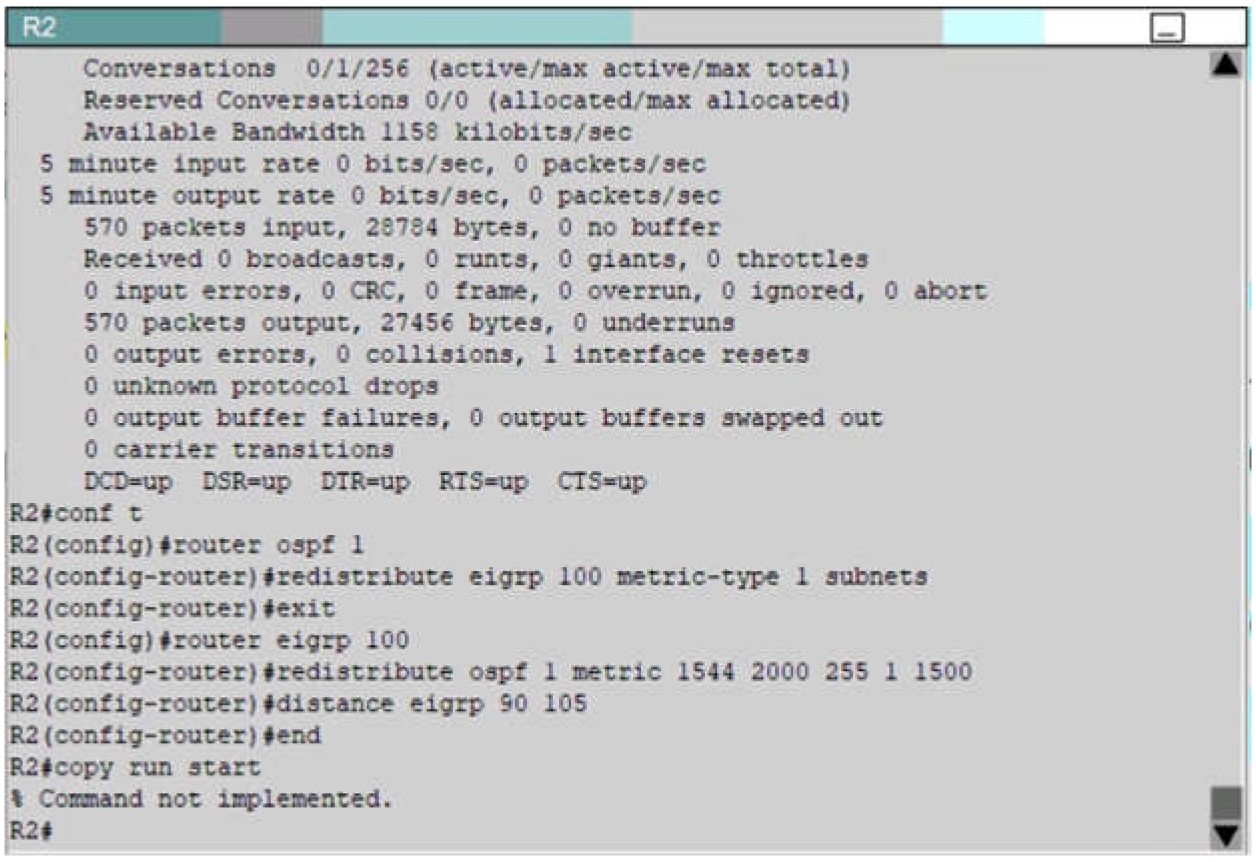
Explanation/Reference:
Explanation:
First you need to configure access list to HTTP traffic and then configure that access list. After that configure the route map and then apply it on the interface to the server in EIGRP network.

QUESTION 35
SIMULATION
You are a network engineer with ROUTE.com, a small IT company. They have recently merged two organizations and now need to merge their networks as shown in the topology exhibit. One network is using OSPF as its IGP and the other is using EIGRP as its IGP. R4 has been added to the existing OSPF network to provide the interconnect between the OSPF and EIGRP networks. Two links have been added that will provide redundancy.

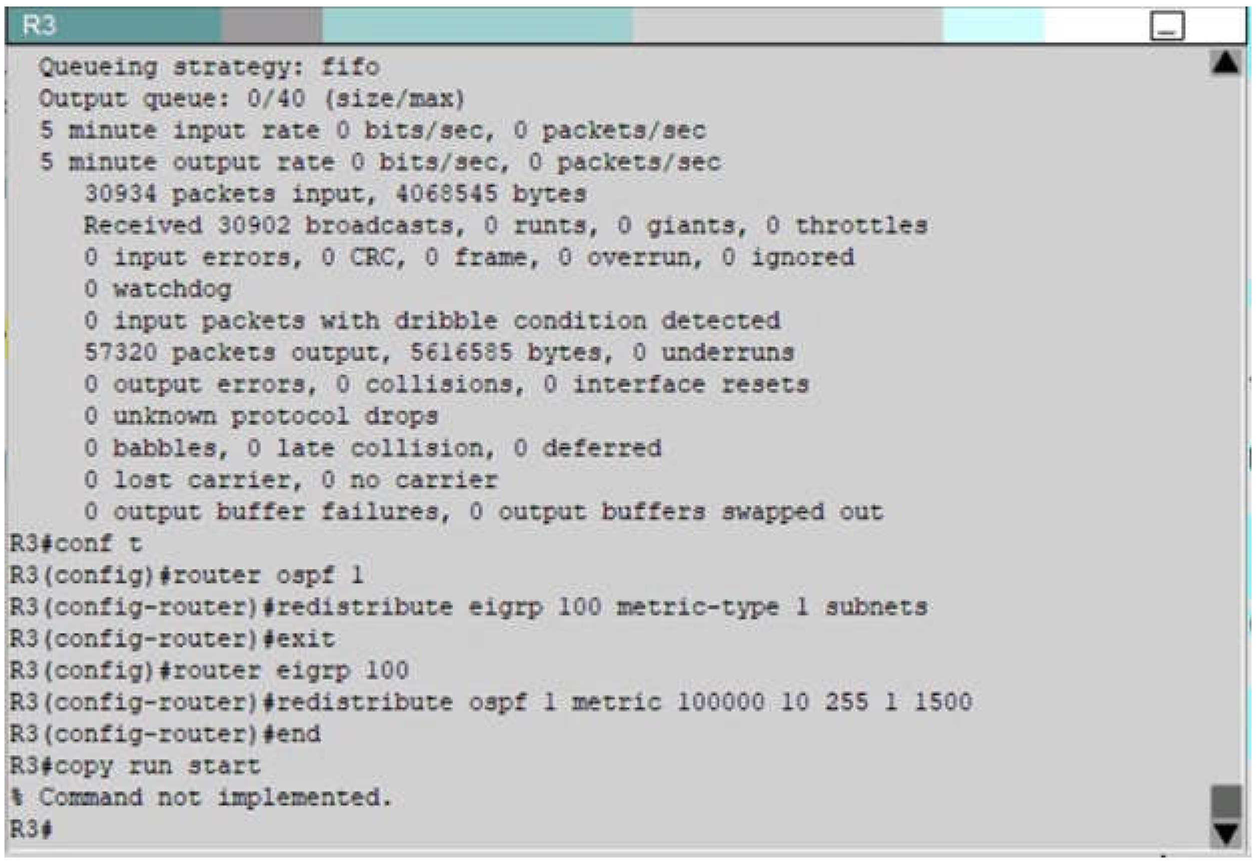
The network requirements state that you must be able to ping and telnet from loopback 101 on R1 to the OPSF domain test address of 172.16.1.100. All traffic must use the shortest path that provides the greatest bandwidth. The redundant paths from the OSPF network to the EIGRP network must be available in case of a link failure. No static or default routing is allowed in either network.

A previous network engineer has started the merger implementation and has successfully assigned and verified all IP addressing and basic IGP routing. You have been tasked with completing the implementation and ensuring that the network requirements are met. You may not remove or change any of the configuration commands currently on any of the routers. You may add new commands or change default values.





```
     Conversations  0/1/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 1158 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     570 packets input, 28784 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     570 packets output, 27456 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
R2#conf t
R2(config)#router ospf 1
R2(config-router)#redistribute eigrp 100 metric-type 1 subnets
R2(config-router)#exit
R2(config)#router eigrp 100
R2(config-router)#redistribute ospf 1 metric 1544 2000 255 1 1500
R2(config-router)#distance eigrp 90 105
R2(config-router)#end
R2#copy run start
% Command not implemented.
R2#
```



```
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     30934 packets input, 4068545 bytes
     Received 30902 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     57320 packets output, 5616585 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
R3#conf t
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 100 metric-type 1 subnets
R3(config-router)#exit
R3(config)#router eigrp 100
R3(config-router)#redistribute ospf 1 metric 100000 10 255 1 1500
R3(config-router)#end
R3#copy run start
% Command not implemented.
R3#
```

Correct Answer: Please see explanation
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
First we need to find out 5 parameters (Bandwidth, Delay, Reliability, Load, MTU) of the s0/0/0 interface (the interface of R2 connected to R4) for redistribution:

```
R2#show interface s0/0/0
```

Write down these 5 parameters, notice that we have to divide the Delay by 10 because the metric unit is in tens of microsecond. For example, we get Bandwidth=1544 Kbit, Delay=20000 us, Reliability=255, Load=1, MTU=1500 bytes then we would redistribute as follows:

```
R2#config terminal
R2(config)# router ospf 1
R2(config-router)# redistribute eigrp 100 metric-type 1 subnets
R2(config-router)#exit
R2(config-router)#router eigrp 100
R2(config-router)#redistribute ospf 1 metric 1544 2000 255 1 1500
```

Note: In fact, these parameters are just used for reference and we can use other parameters with no problem.
If the delay is 20000us then we need to divide it by 10, that is 20000 / 10 = 2000)
For R3 we use the show interface fa0/0 to get 5 parameters too

```
R3#show interface fa0/0
```

For example we get Bandwidth=10000 Kbit, Delay=1000 us, Reliability=255, Load=1, MTU=1500 bytes

```
R3#config terminal
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 100 metric-type 1 subnets
R3(config)#exit
R3(config-router)#router eigrp 100
R3(config-router)#redistribute ospf 1 metric 10000 100 255 1 1500
```

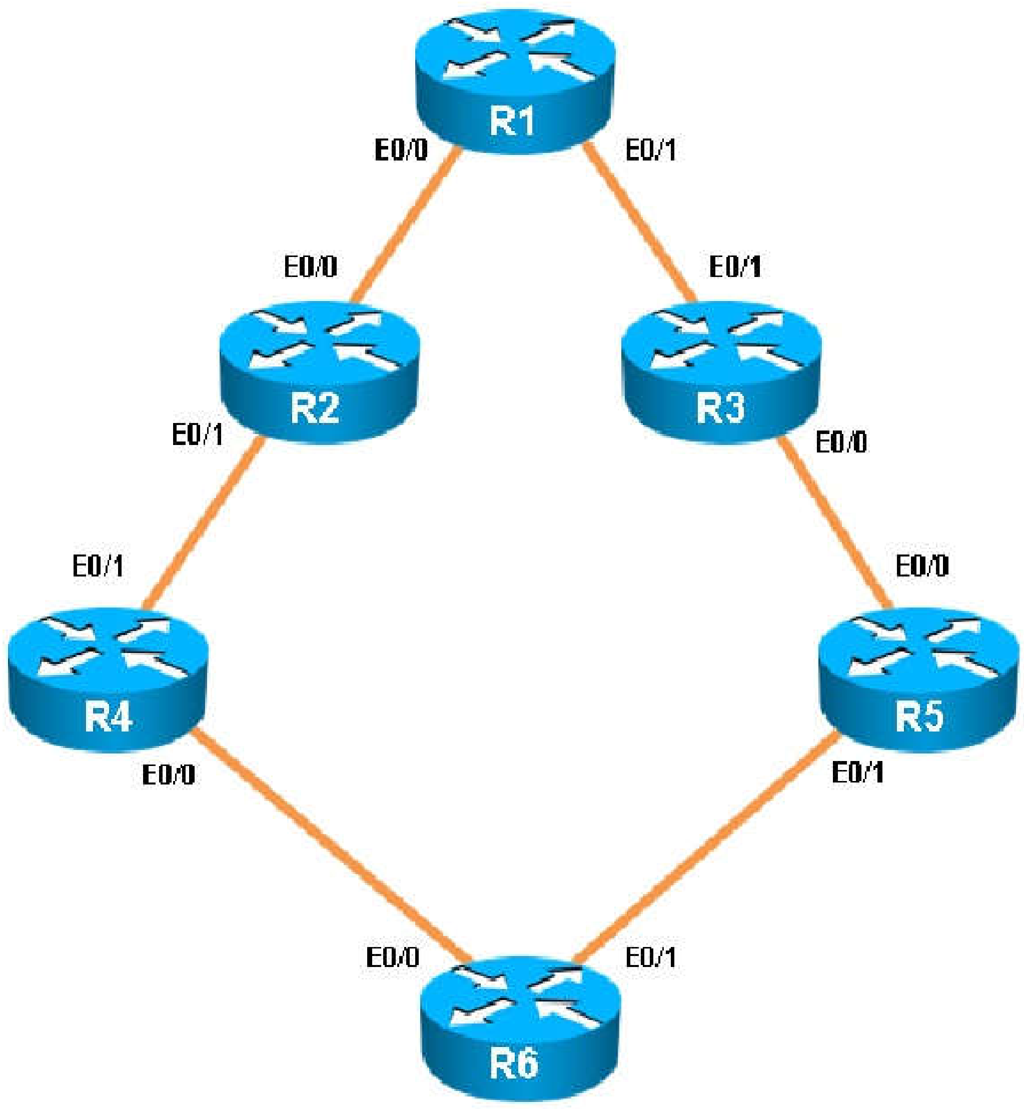
Finally you should try to "show ip route" to see the 172.16.100.1 network (the network behind R4) in the routing table of R1 and make a ping from R1 to this network.
Note: If the link between R2 and R3 is FastEthernet link, we must put the command below under EIGRP process to make traffic from R1 to go through R3 (R1 -> R2 -> R3 -> R4), which is better than R1 -> R2 -> R4.

```
R2(config-router)# distance eigrp 90 105
```

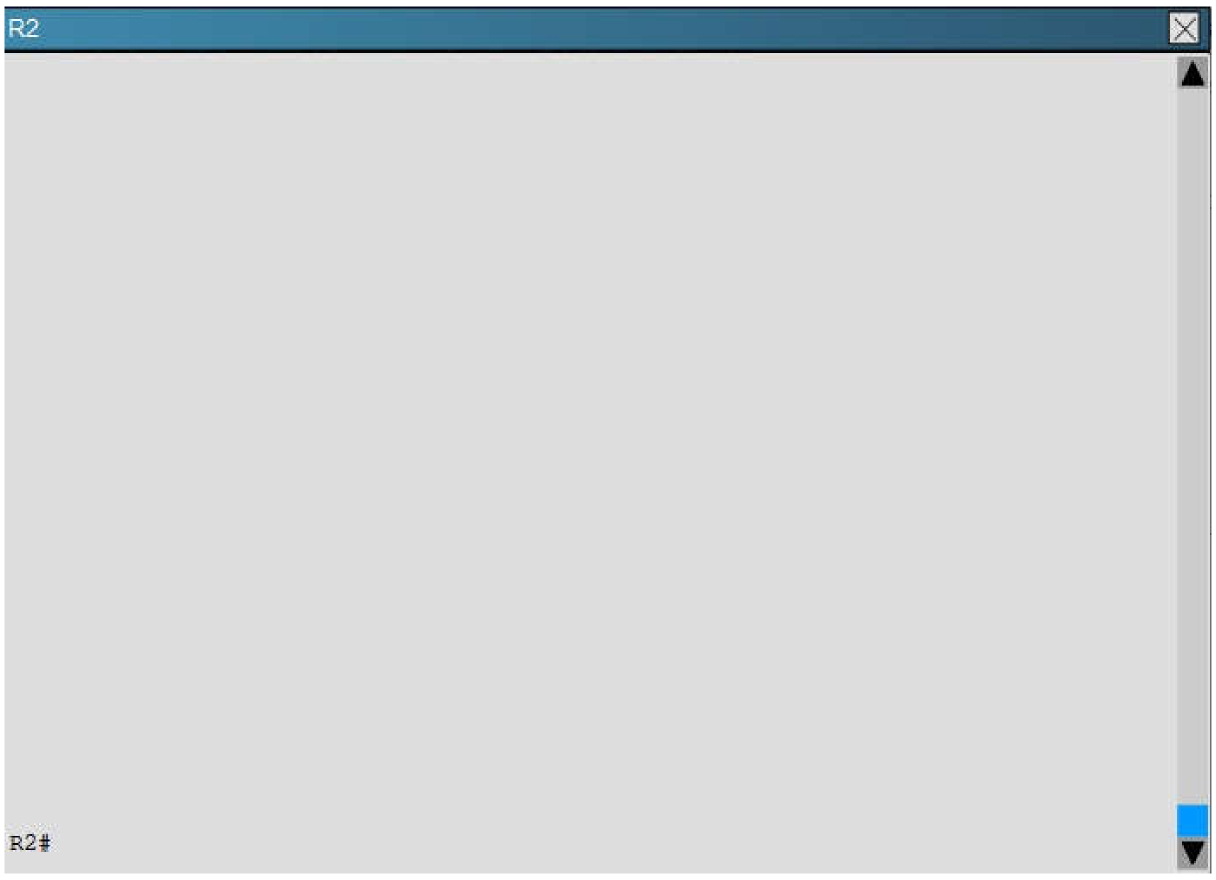
This command sets the Administrative Distance of all EIGRP internal routes to 90 and all EIGRP external routes to 105, which is smaller than the Administrative Distance of OSPF (110) -> the link between R2 & R3 will be preferred to the serial link between R2 & R4.
Note: The actual OPSF and EIGRP process numbers may change in the actual exam so be sure to use the actual correct values, but the overall solution is the same.

QUESTION 36
Scenario
You have been asked to evaluate how EIGRP is functioning in a customer network. Access the device consoles to answer the questions.

Instructions
- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- Click on the individual device icons or use the tab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are five multiple-choice questions with this task. Be sure to answer all five questions before selecting the Next button.

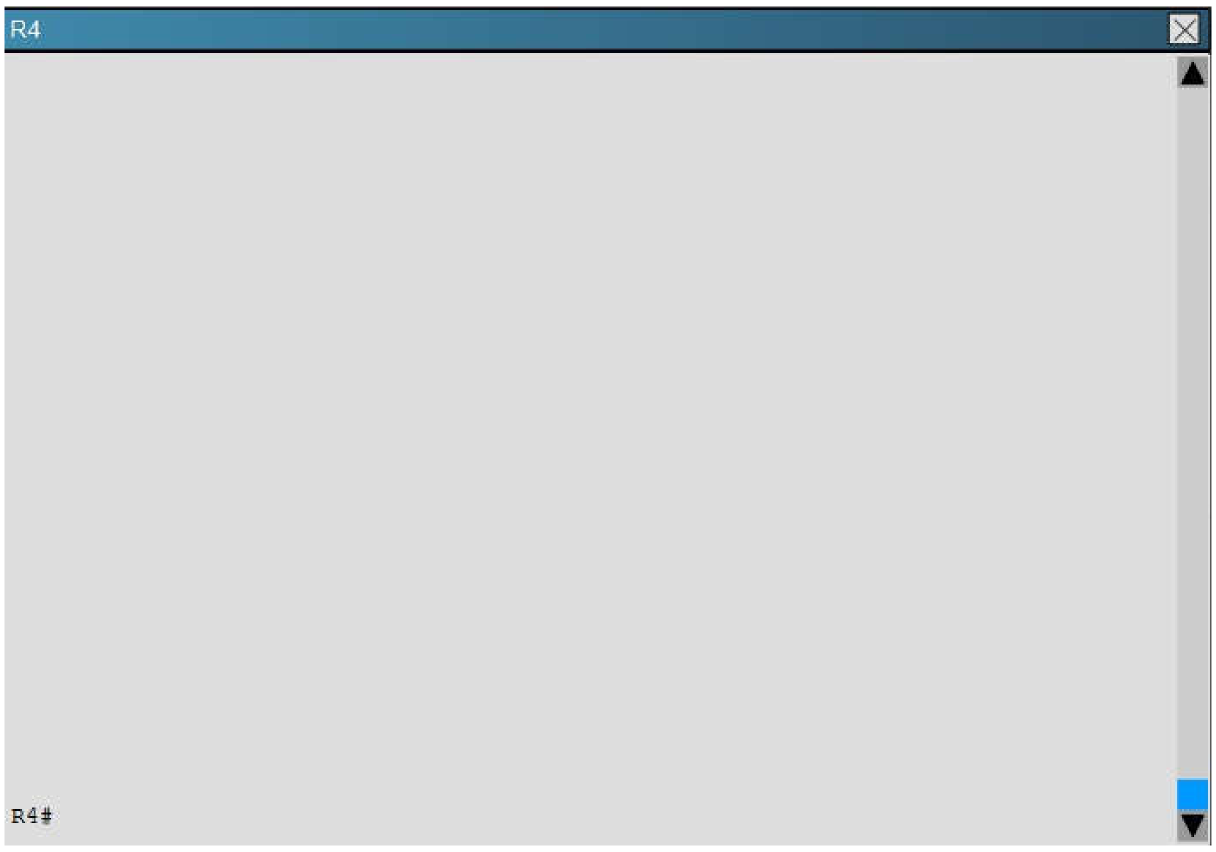


```
R1#
```



```
R2#
```

```
R3#
```



```
R4#
```

```
R5#
```

```
R6#
```

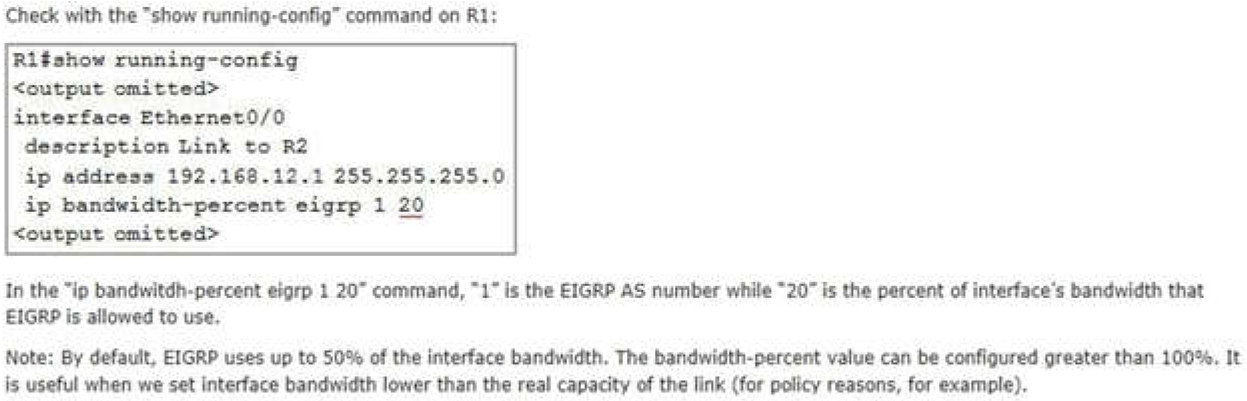
What percent of R1’s interfaces bandwidth is EIGRP allowed to use?

A. 10

B. 20
C. 30
D. 40

Correct Answer: B
Section: Layer 3 Technologies
Explanation

Explanation/Reference:



Check with the "show running-config" command on R1:

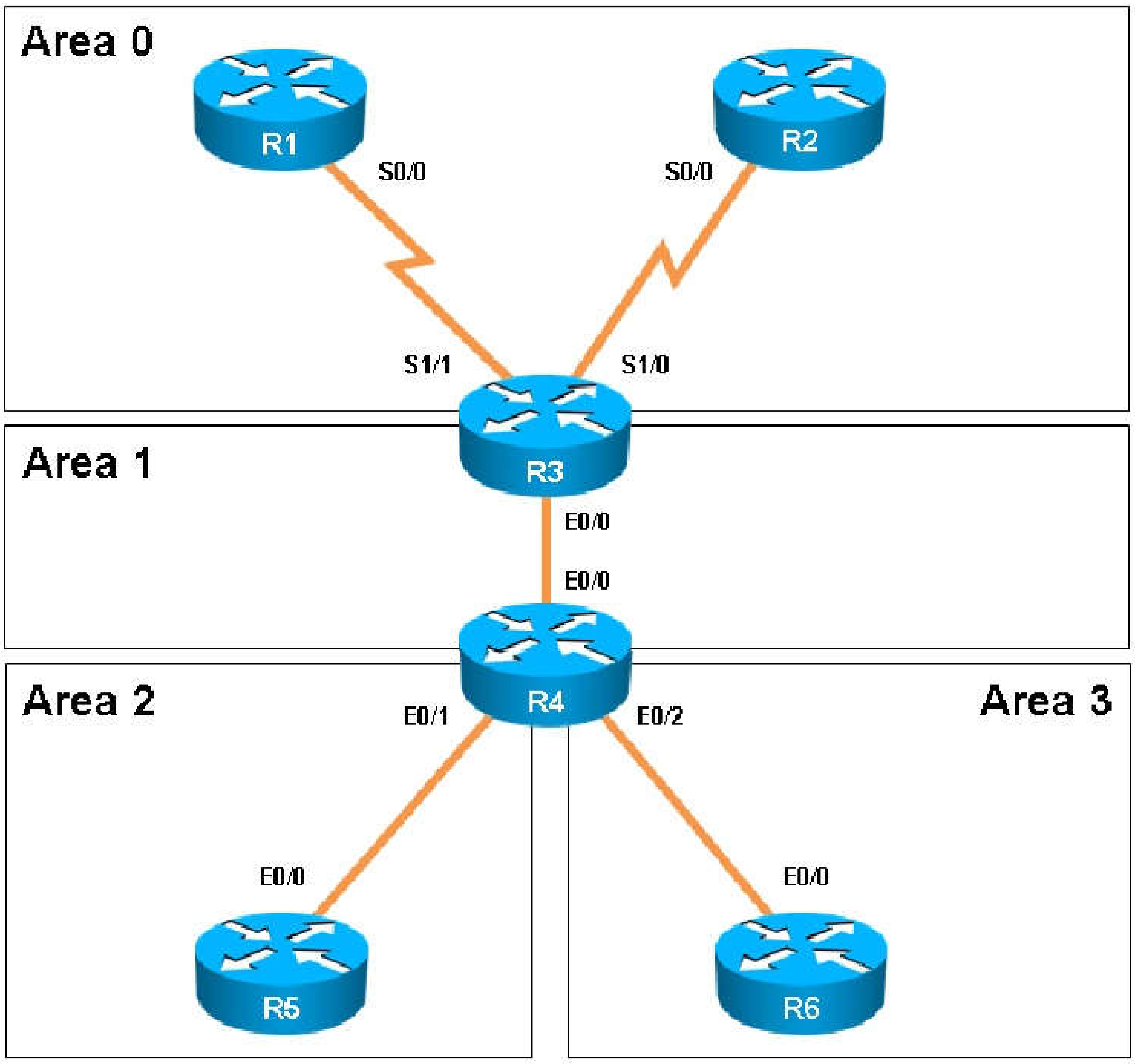
```
R1#show running-config
<output omitted>
interface Ethernet0/0
 description Link to R2
 ip address 192.168.12.1 255.255.255.0
 ip bandwidth-percent eigrp 1 20
<output omitted>
```

In the "ip bandwitdh-percent eigrp 1 20" command, "1" is the EIGRP AS number while "20" is the percent of interface's bandwidth that EIGRP is allowed to use.

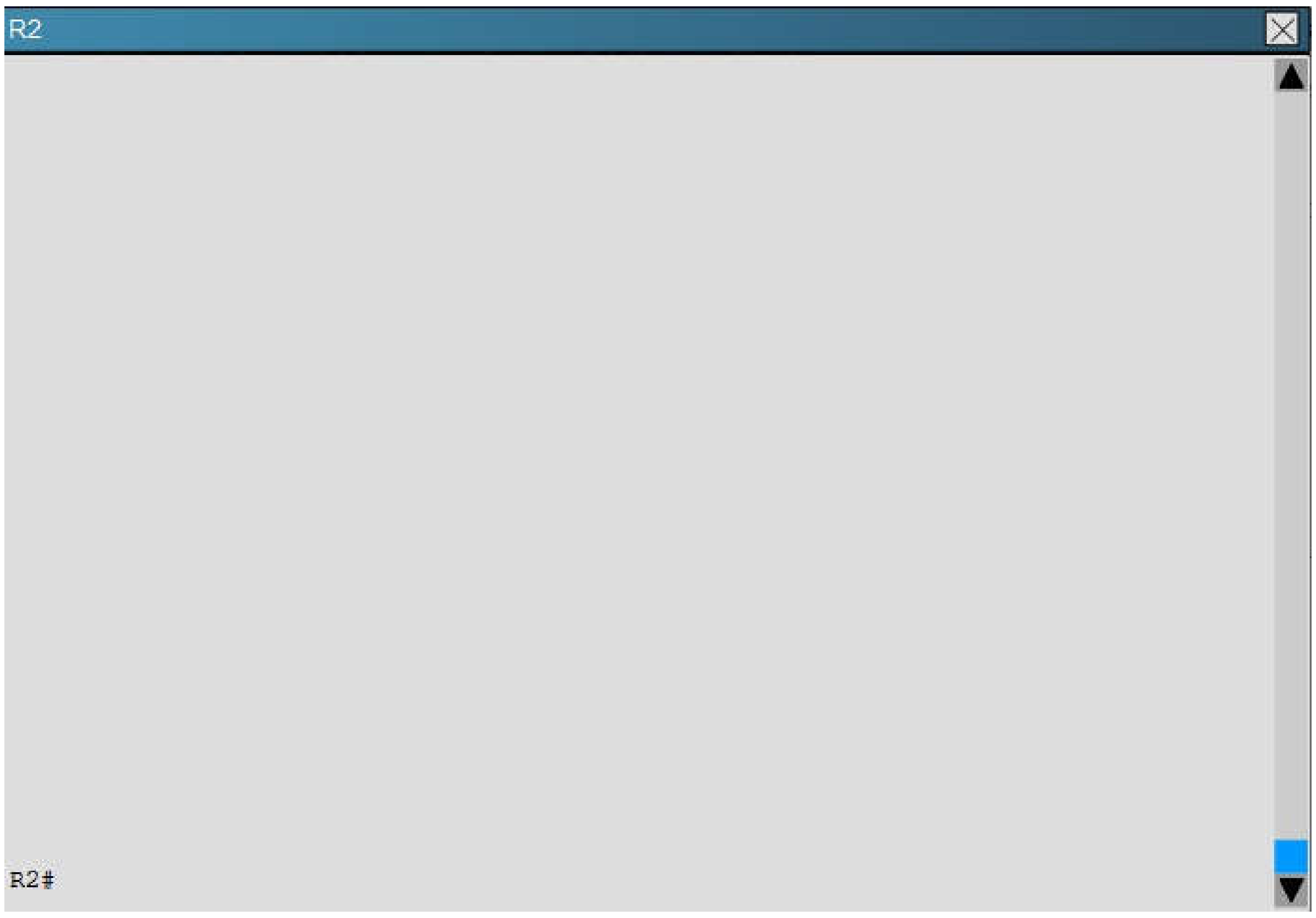
Note: By default, EIGRP uses up to 50% of the interface bandwidth. The bandwidth-percent value can be configured greater than 100%. It is useful when we set interface bandwidth lower than the real capacity of the link (for policy reasons, for example).

QUESTION 37
Scenario
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.

Instructions
- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION**.
- Click on the icon or the lab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.

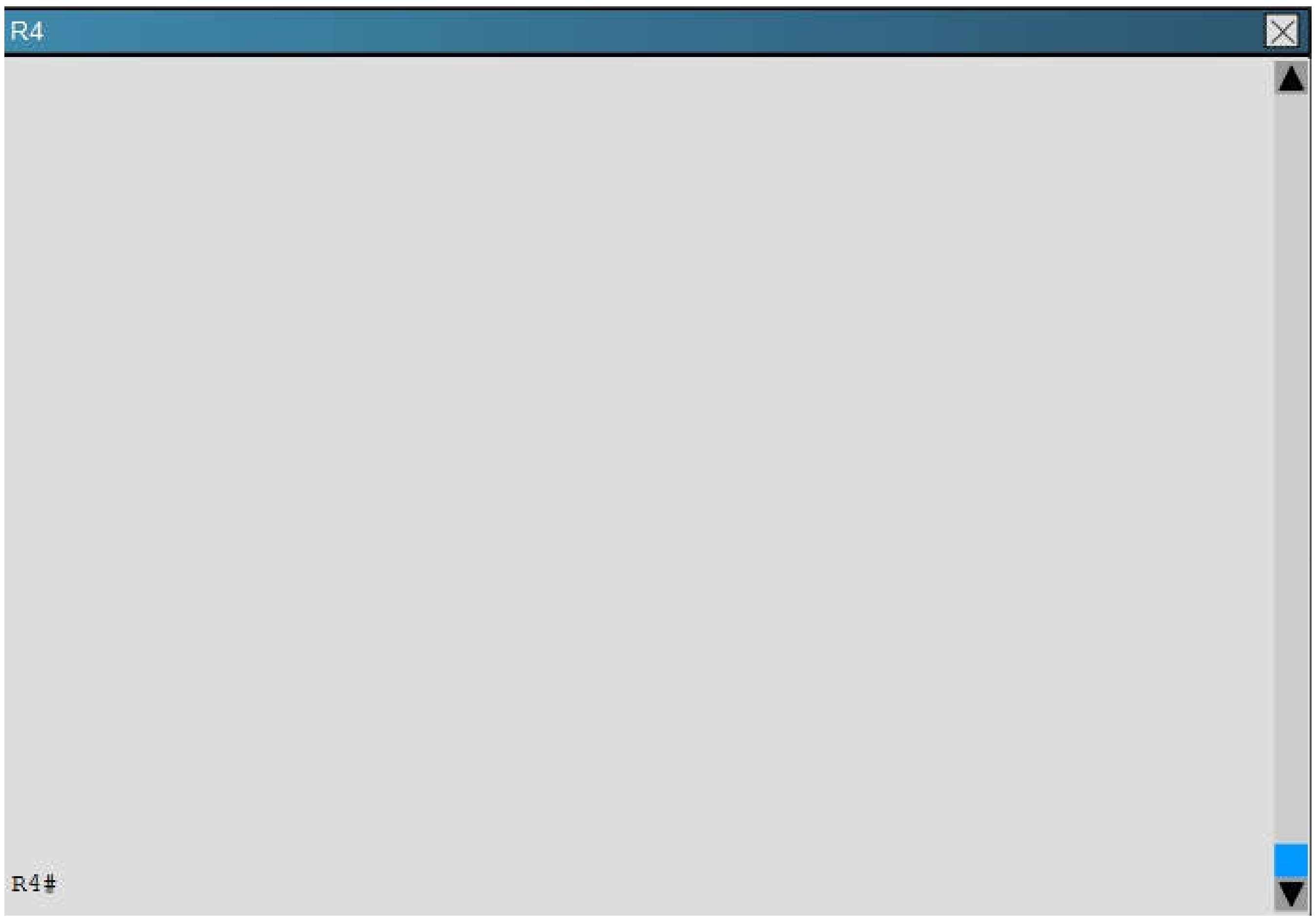


```
R1#
```

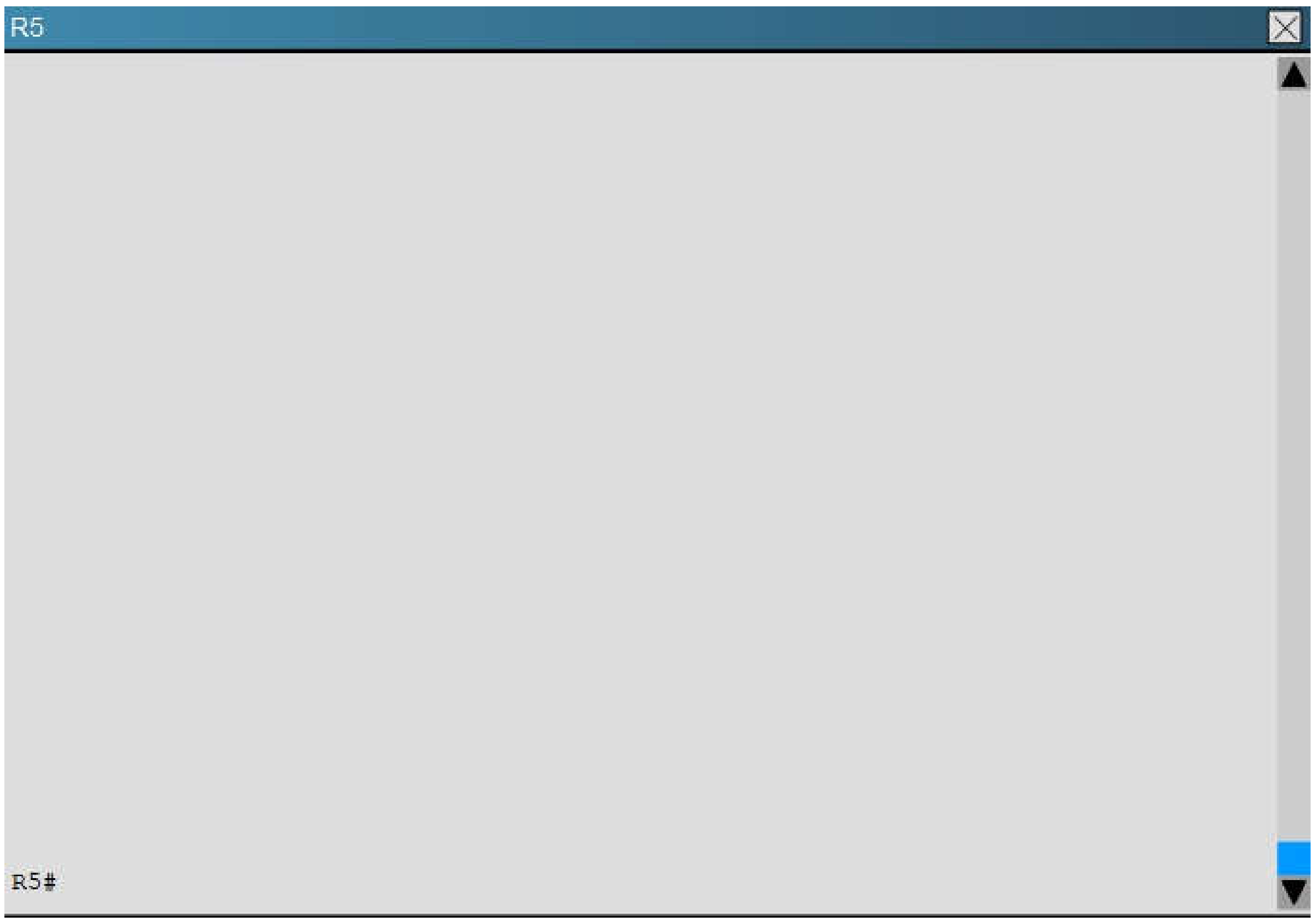


```
R2#
```

```
R3#
```



```
R4#
```



```
R5#
```

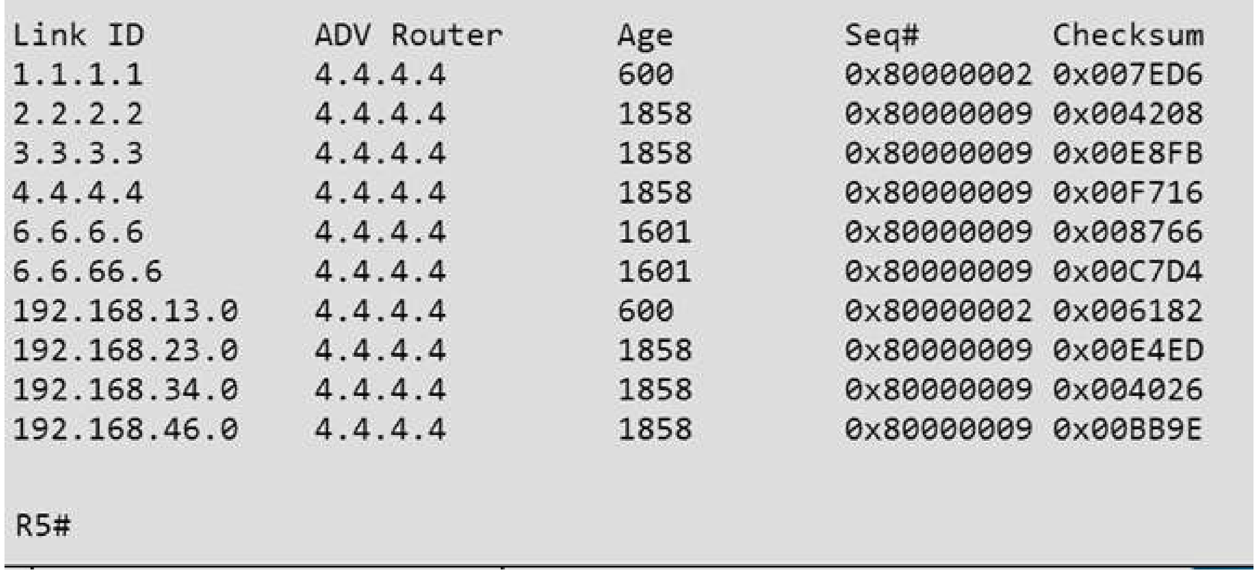
```
R6#
```

How old is the Type 4 LSA from Router 3 for area 1 on the router R5, based on the output you have examined?

A. 1858
B. 1601
C. 600
D. 1569

Correct Answer: A
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Part of the “show ip ospf topology” command on R5 shows this:

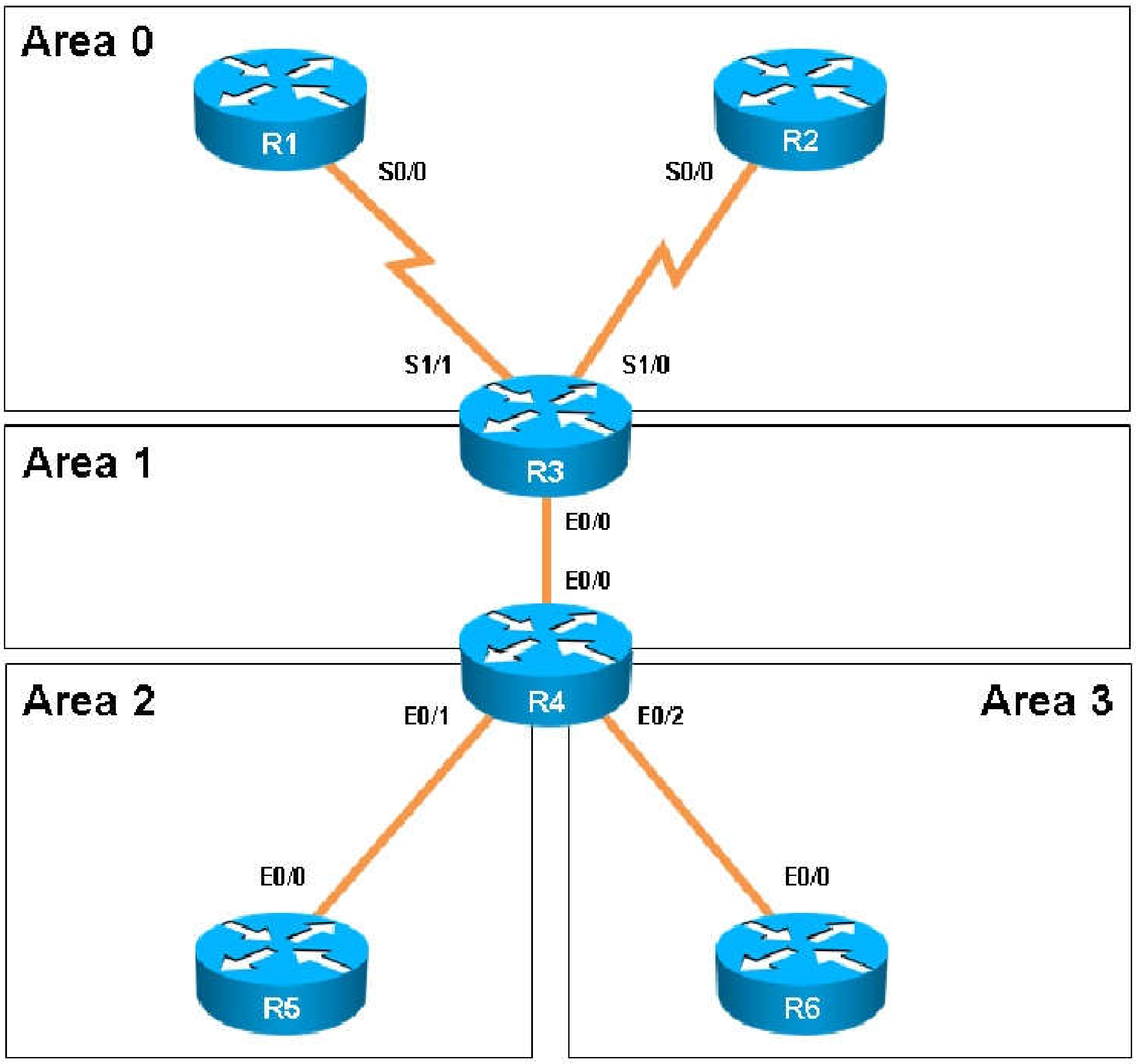


```
Link ID         ADV Router      Age         Seq#       Checksum
1.1.1.1         4.4.4.4         600         0x80000002 0x007ED6
2.2.2.2         4.4.4.4         1858        0x80000009 0x004208
3.3.3.3         4.4.4.4         1858        0x80000009 0x00E8FB
4.4.4.4         4.4.4.4         1858        0x80000009 0x00F716
6.6.6.6         4.4.4.4         1601        0x80000009 0x008766
6.6.66.6        4.4.4.4         1601        0x80000009 0x00C7D4
192.168.13.0    4.4.4.4         600         0x80000002 0x006182
192.168.23.0    4.4.4.4         1858        0x80000009 0x00E4ED
192.168.34.0    4.4.4.4         1858        0x80000009 0x004026
192.168.46.0    4.4.4.4         1858        0x80000009 0x00BB9E

R5#
```

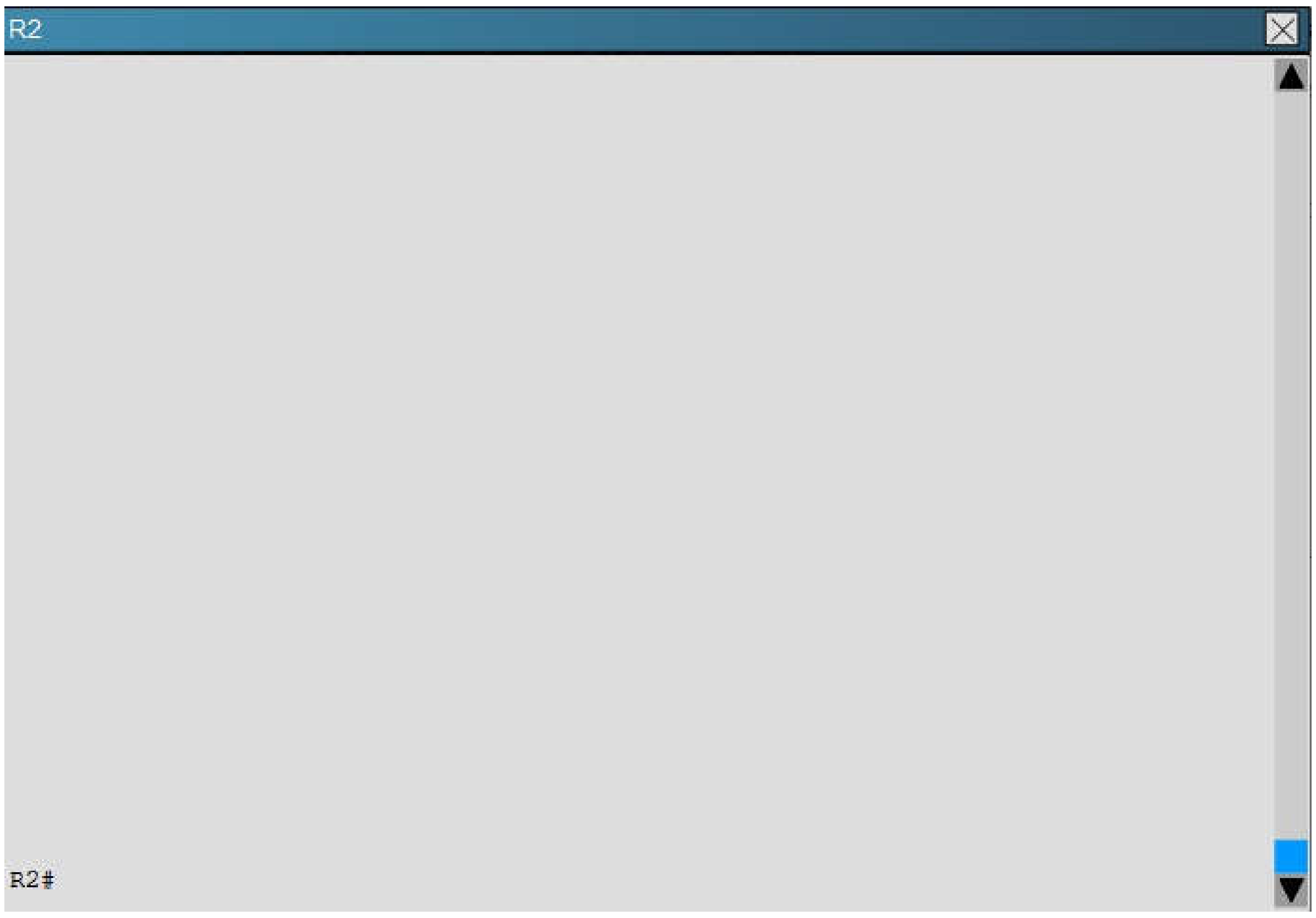
The Link ID of R3 (3.3.3.3) shows the age is 1858.

QUESTION 38
Scenario
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.

Instructions
- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION**.
- Click on the icon or the lab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all **four** questions before selecting the Next button.

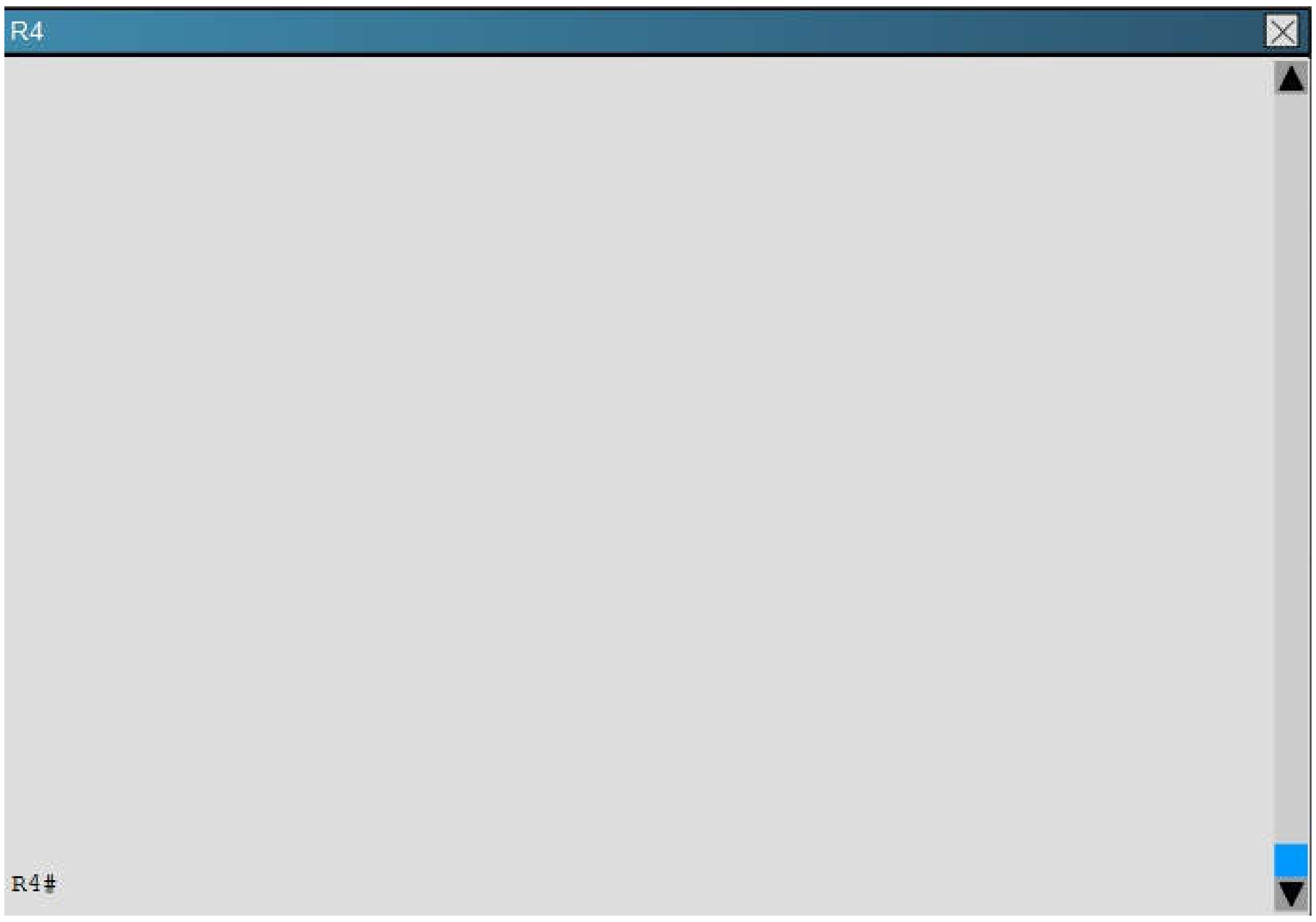


```
R1#
```

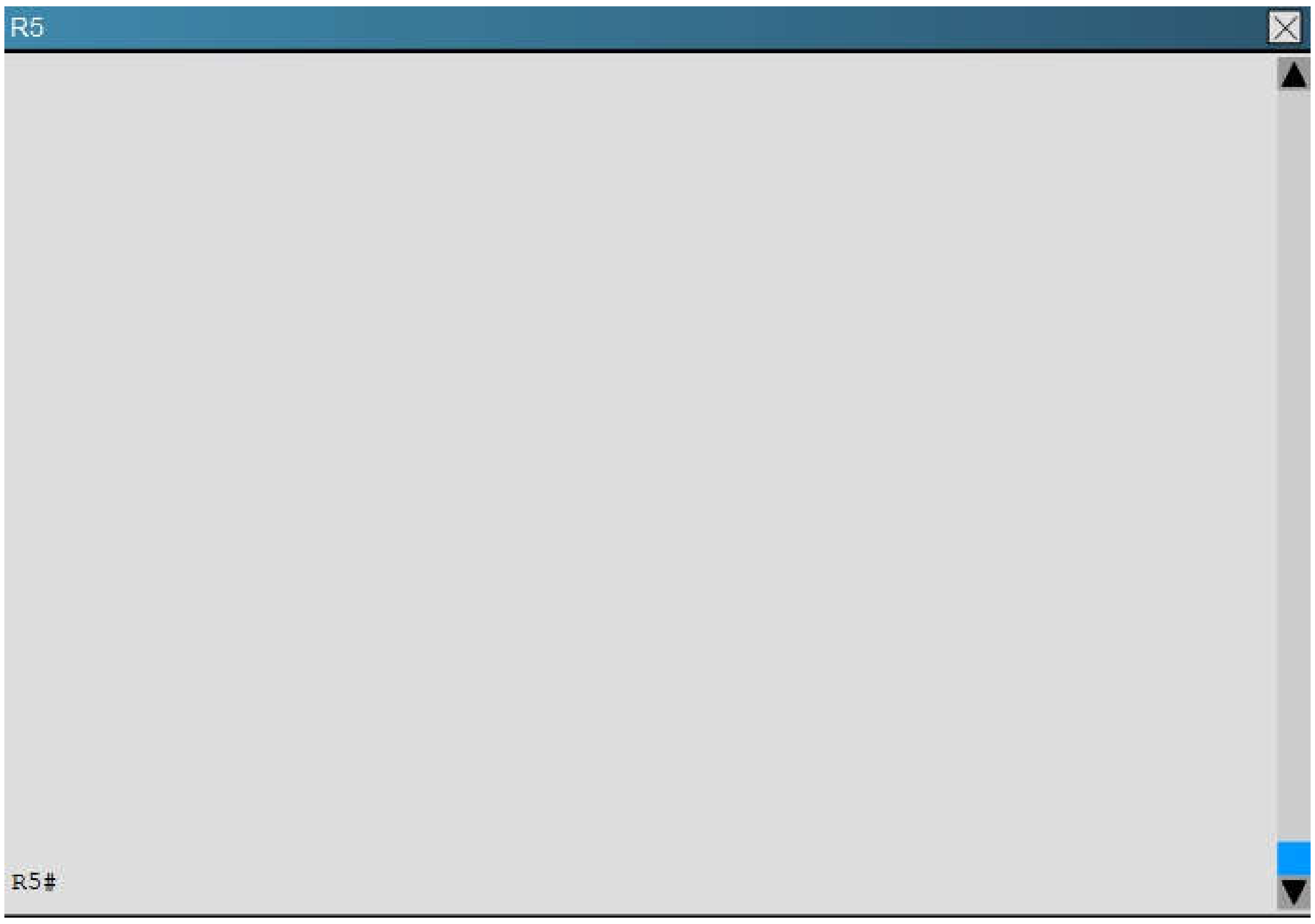


```
R2#
```

```
R3#
```



```
R4#
```



```
R5#
```

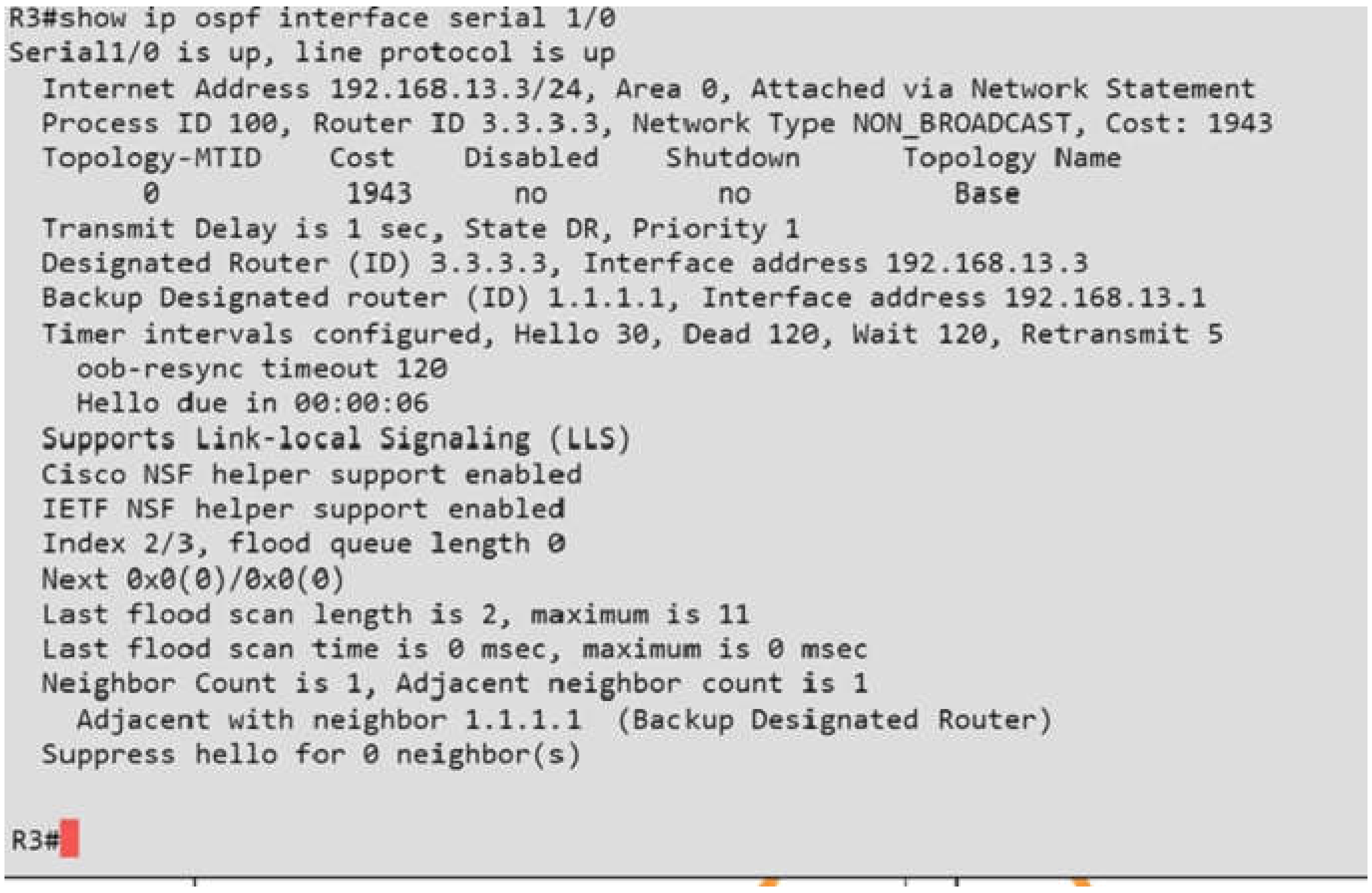
```
R6#
```

Which of the following statements is true about the serial links that terminate in R3?

A. The R1-R3 link needs the neighbor command for the adjacency to stay up
B. The R2-R3 link OSPF timer values are 30, 120, 120
C. The R1-R3 link OSPF timer values should be 10, 40, 40
D. R3 is responsible for flooding LSUs to all the routers on the network

Correct Answer: B
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
We can see the configured timers using the following command:



```
R3#show ip ospf interface serial 1/0
Serial1/0 is up, line protocol is up
  Internet Address 192.168.13.3/24, Area 0, Attached via Network Statement
  Process ID 100, Router ID 3.3.3.3, Network Type NON_BROADCAST, Cost: 1943
  Topology-MTID    Cost    Disabled    Shutdown      Topology Name
        0           1943      no          no            Base
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.13.3
  Backup Designated router (ID) 1.1.1.1, Interface address 192.168.13.1
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:06
  Supports Link-local Signaling (LLS)
  Cisco NSF helper support enabled
  IETF NSF helper support enabled
  Index 2/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 11
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 1.1.1.1  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)

R3#
```

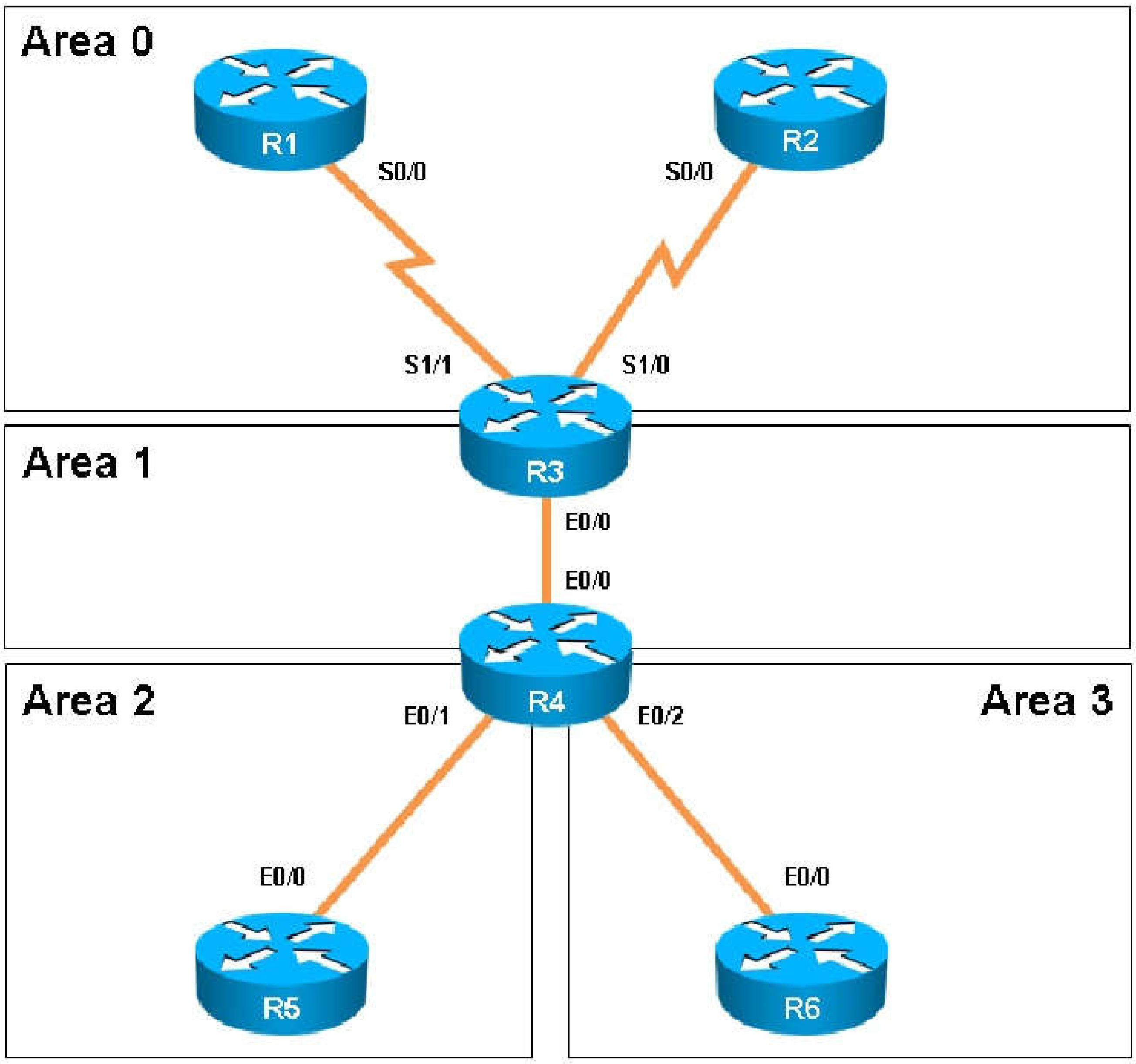
QUESTION 39

Scenario

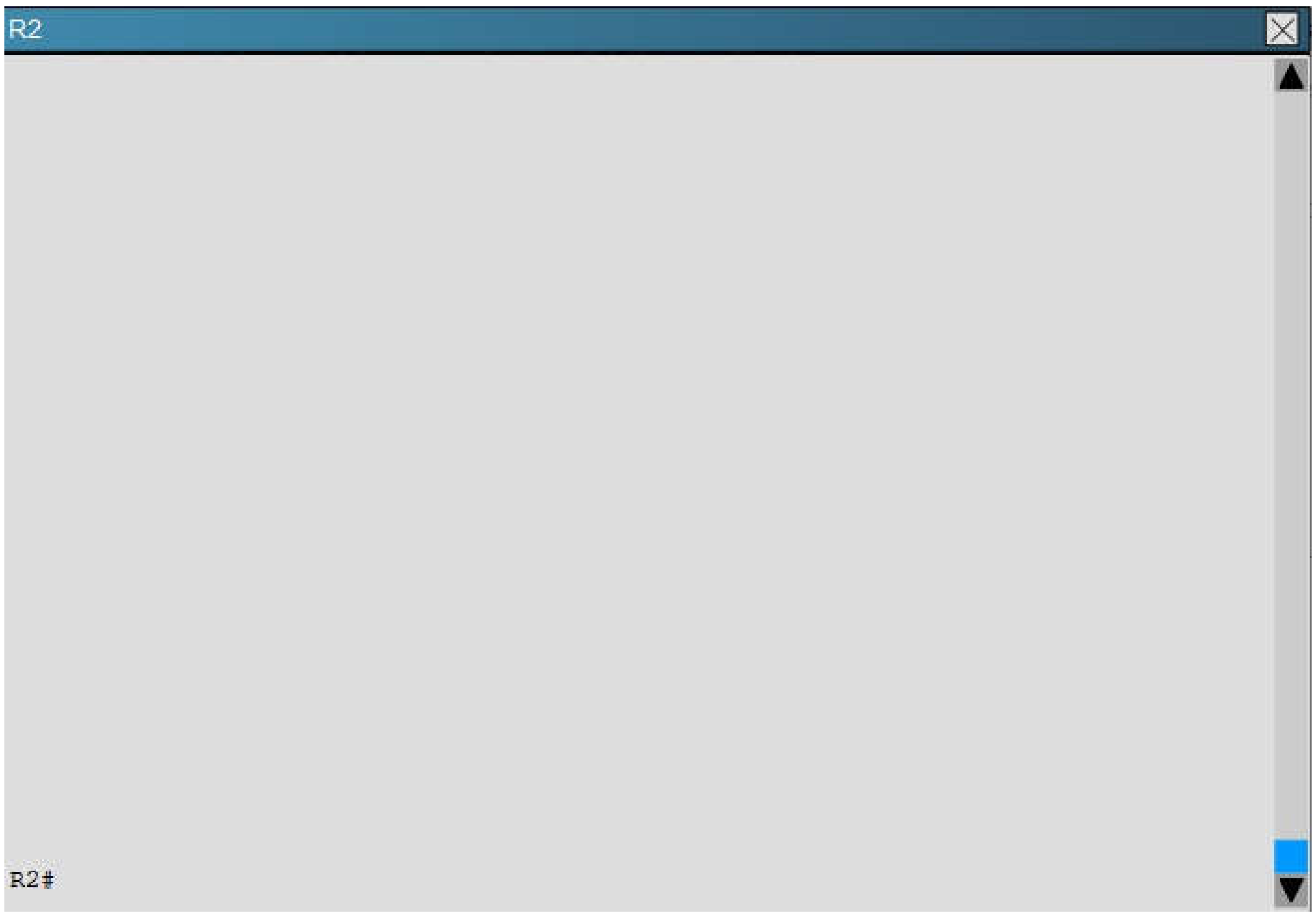
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.

Instructions

- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION**.
- Click on the icon or the lab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all **four** questions before selecting the Next button.

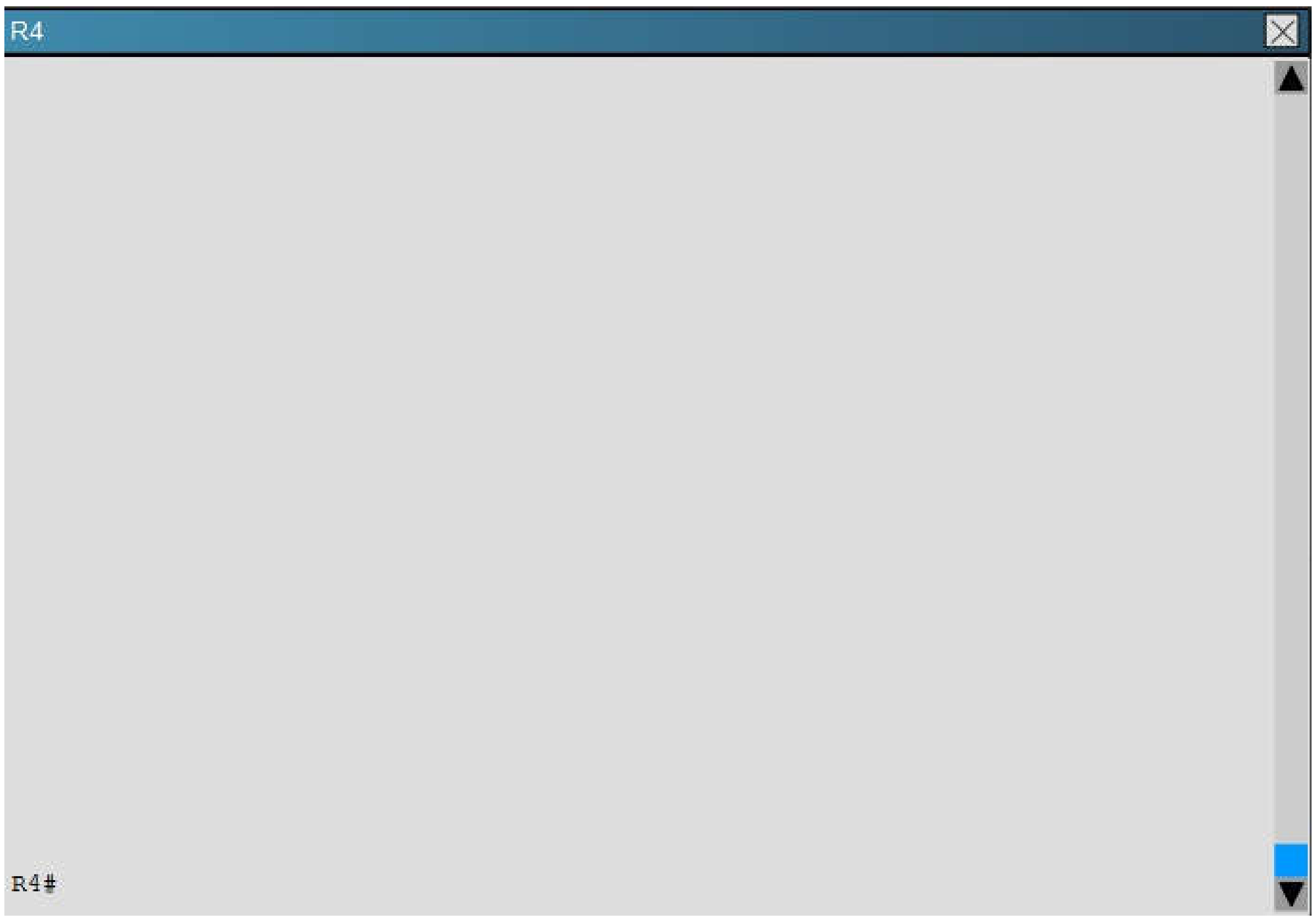


```
R1#
```

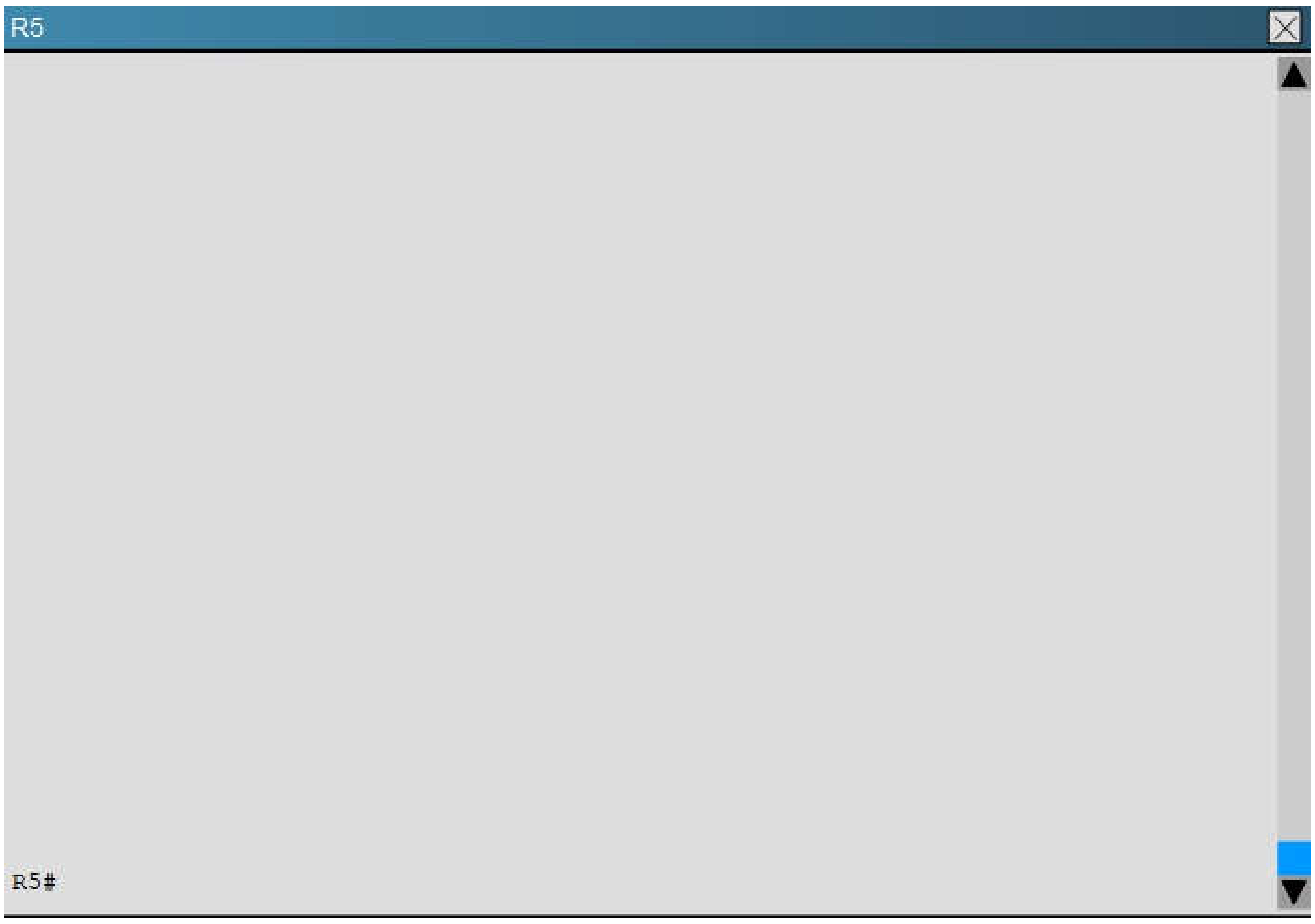


```
R2#
```

```
R3#
```



```
R4#
```



```
R5#
```

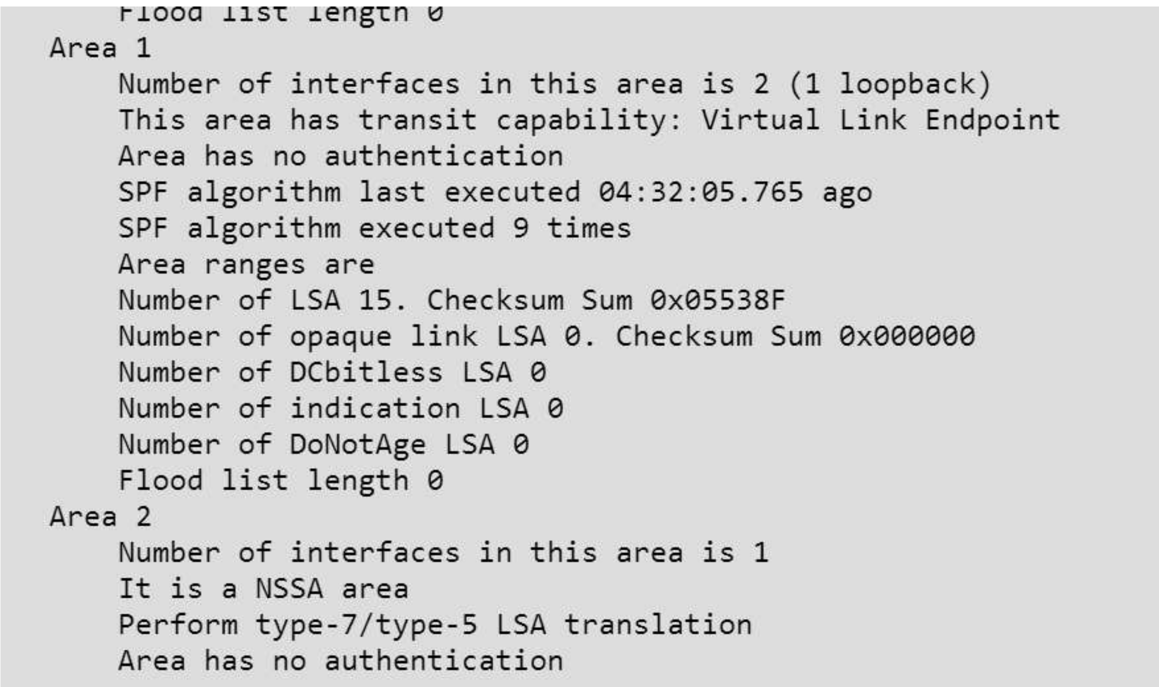
```
R6#
```

How many times was SPF algorithm executed on R4 for Area 1?

A. 1
B. 5
C. 9
D. 20
E. 54
F. 224

Correct Answer: C
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
This can be found using the “show ip ospf” command on R4. Look for the Area 1 stats which shows this:



```
        Flood list length 0
    Area 1
        Number of interfaces in this area is 2 (1 loopback)
        This area has transit capability: Virtual Link Endpoint
        Area has no authentication
        SPF algorithm last executed 04:32:05.765 ago
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 15. Checksum Sum 0x05538F
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
    Area 2
        Number of interfaces in this area is 1
        It is a NSSA area
        Perform type-7/type-5 LSA translation
        Area has no authentication
```

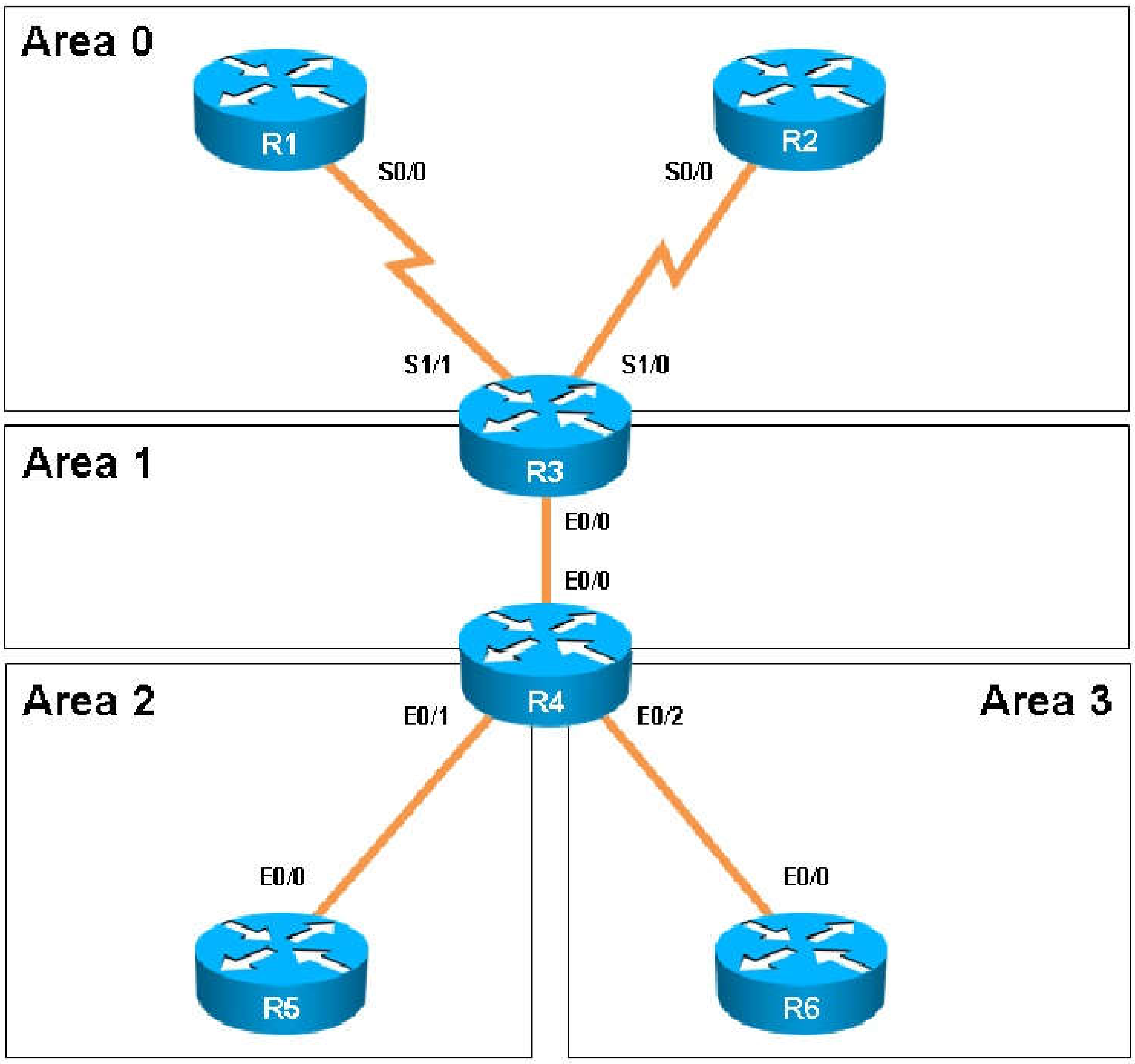
QUESTION 40

Scenario

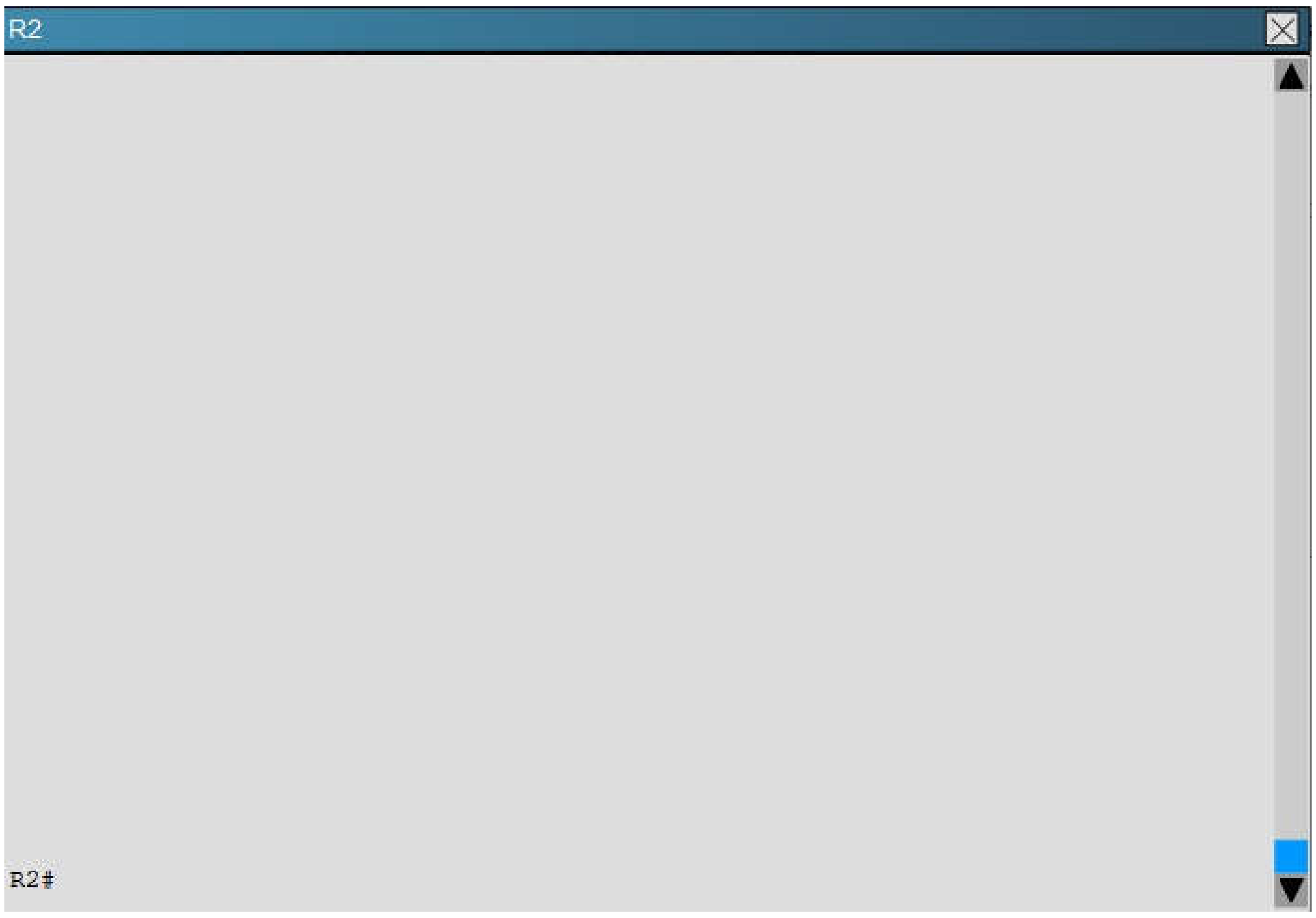
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.

Instructions

- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION**.
- Click on the icon or the lab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all **four** questions before selecting the Next button.

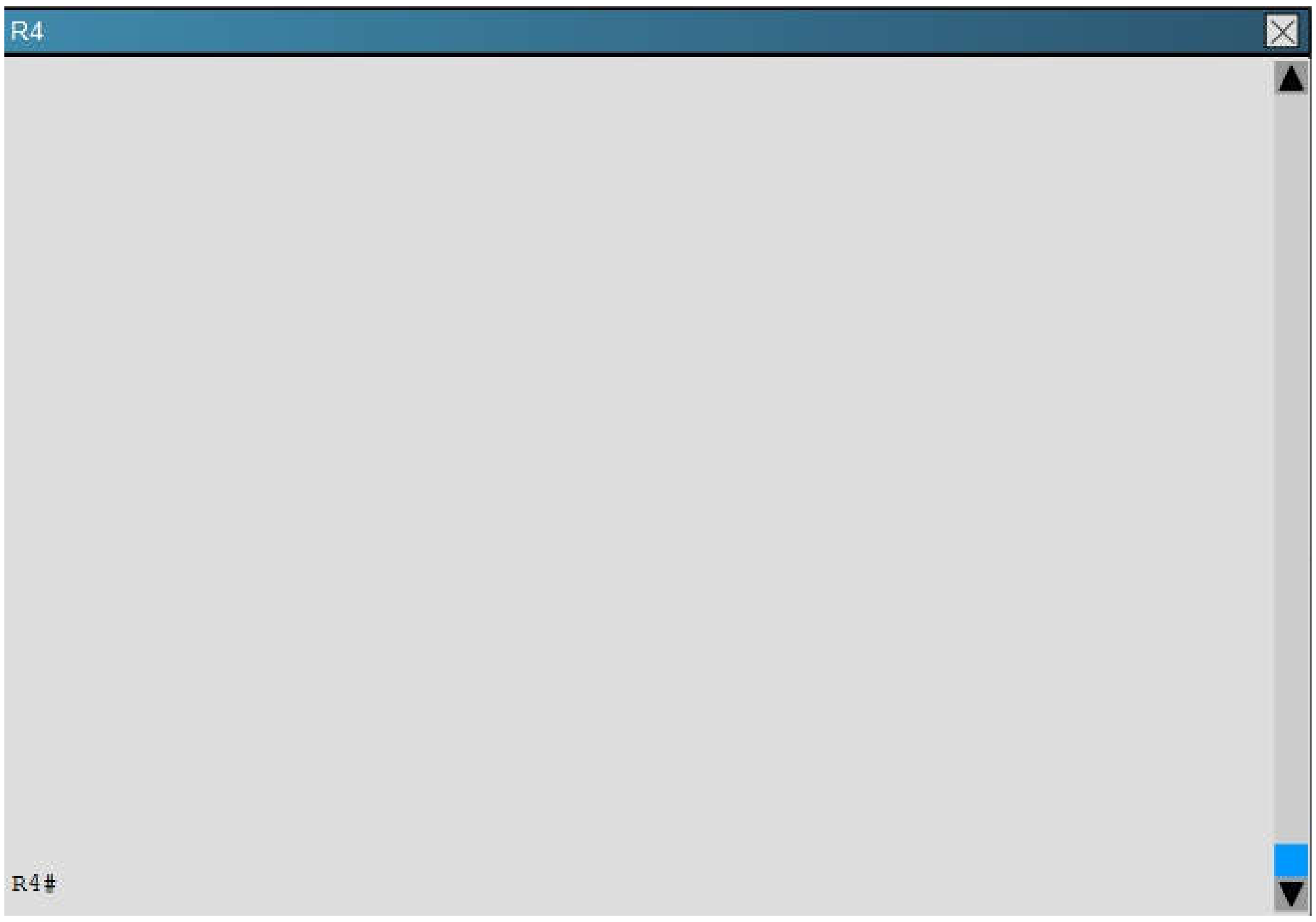


```
R1#
```

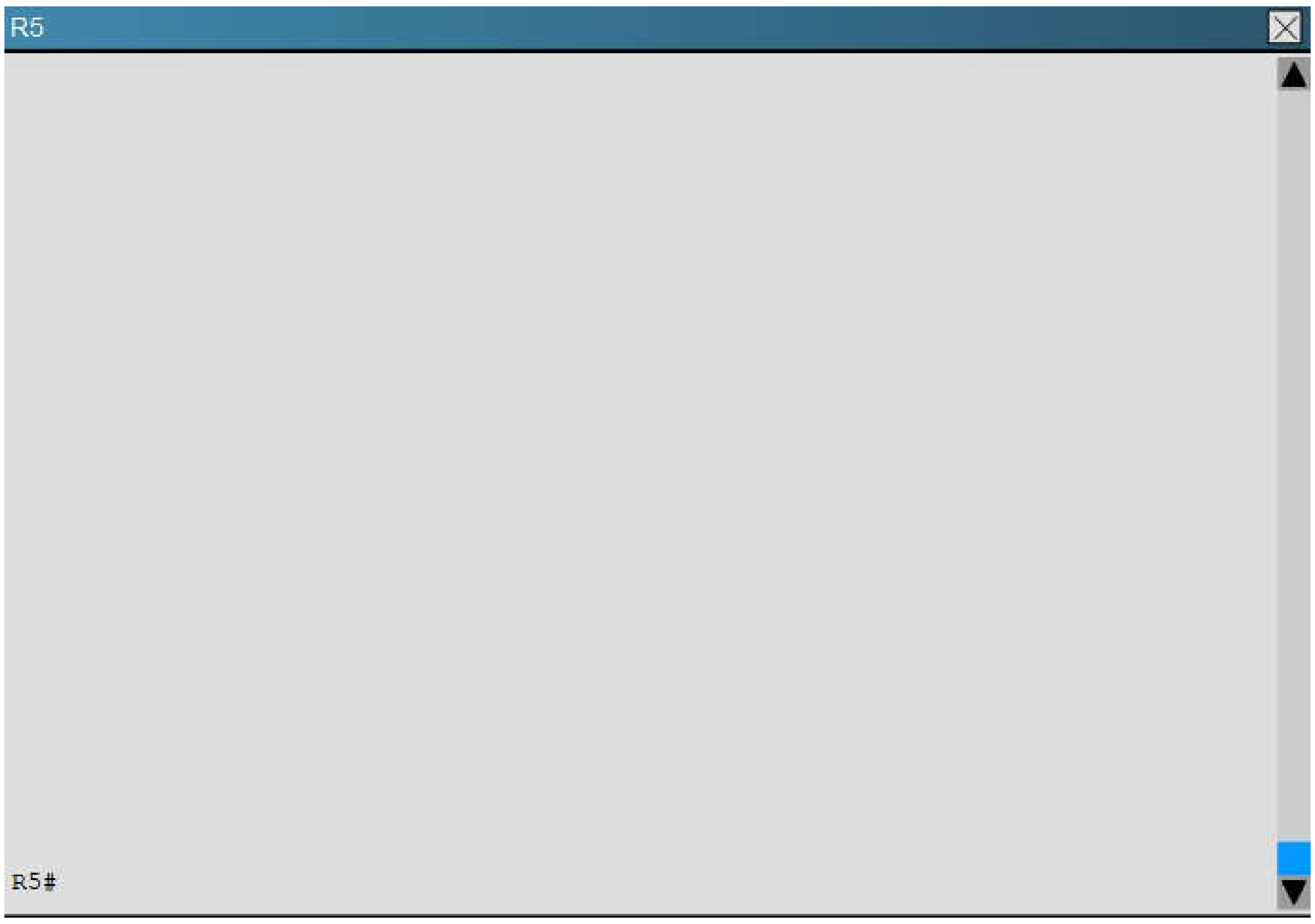


```
R2#
```

```
R3#
```



```
R4#
```



```
R5#
```

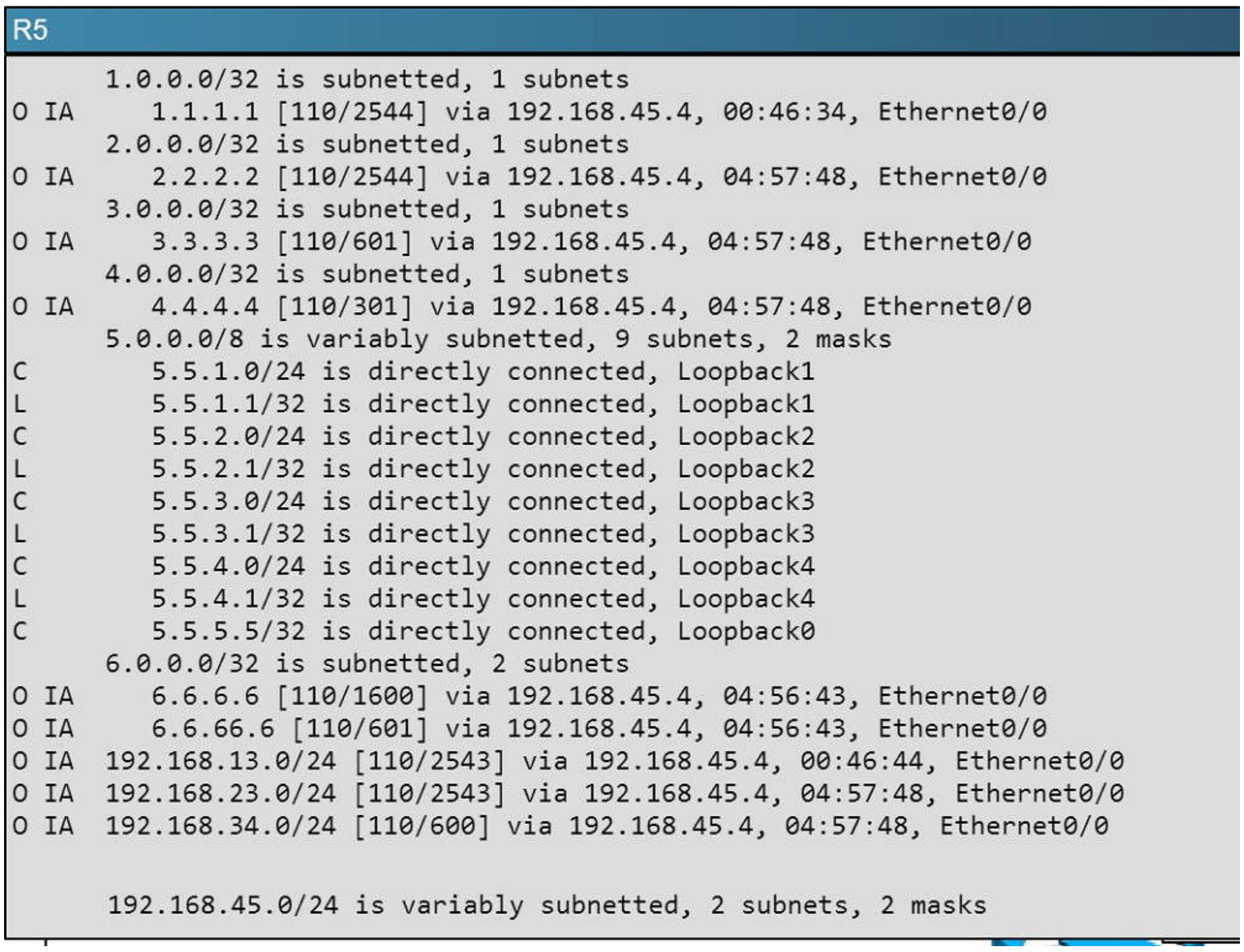
```
R6#
```

Areas of Router 5 and 6 are not normal areas. Inspect their routing tables and determine which statement is true.

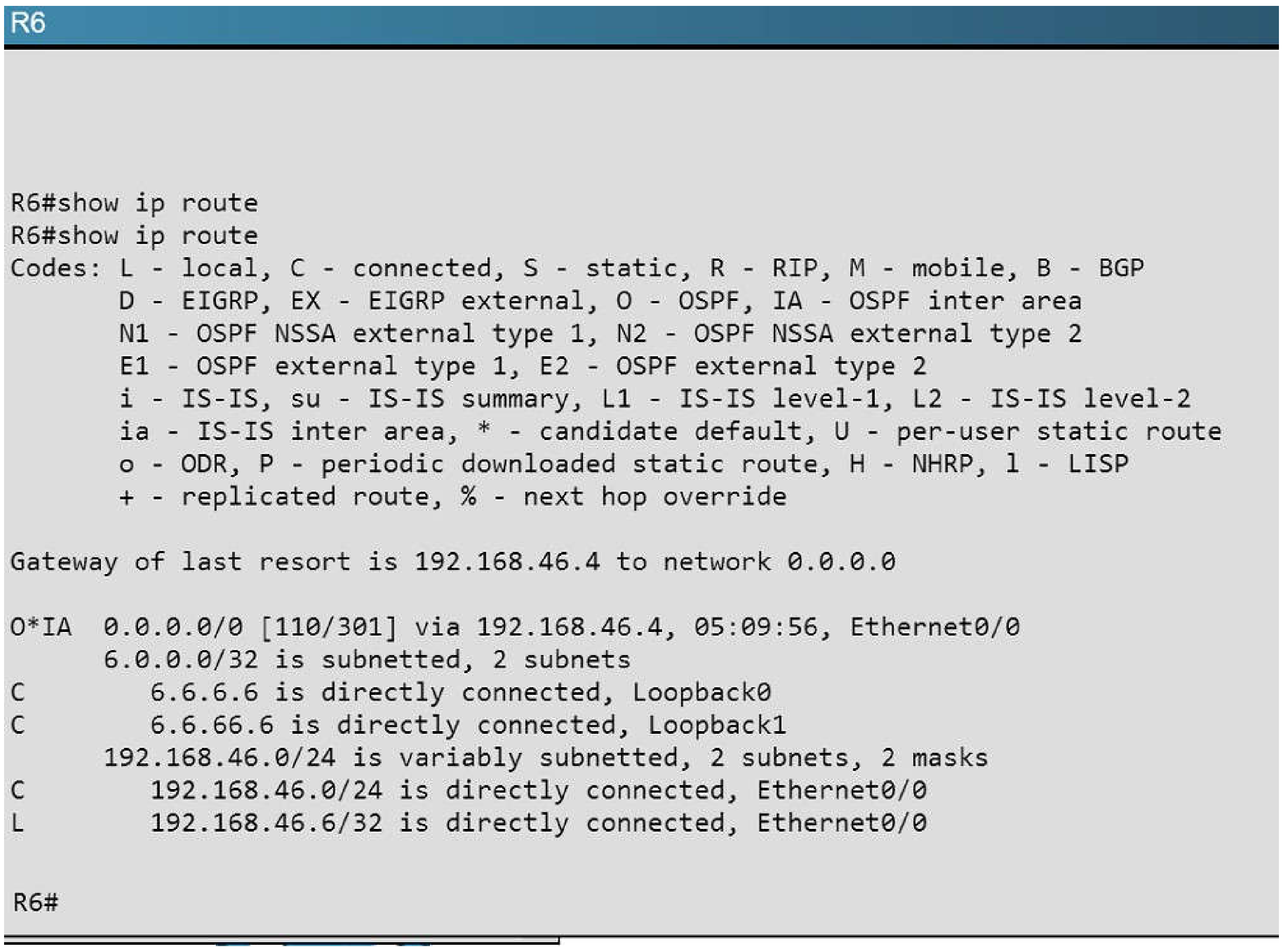
A. R5’s Loopback and R6’s Loopback are both present in R5’s Routing table
B. R5’s Loopback and R6’s Loopback are both present in R6’s Routing table
C. Only R5’s loopback is present in R5’s Routing table
D. Only R6’s loopback is present in R5’s Routing table
E. Only R5’s loopback is present in R6’s Routing table

Correct Answer: A
Section: Layer 3 Technologies
Explanation

Explanation/Reference:
Explanation:
Here are the routing tables of R5 and R6:


R5

```
      1.0.0.0/32 is subnetted, 1 subnets
O IA     1.1.1.1 [110/2544] via 192.168.45.4, 00:46:34, Ethernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O IA     2.2.2.2 [110/2544] via 192.168.45.4, 04:57:48, Ethernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O IA     3.3.3.3 [110/601] via 192.168.45.4, 04:57:48, Ethernet0/0
      4.0.0.0/32 is subnetted, 1 subnets
O IA     4.4.4.4 [110/301] via 192.168.45.4, 04:57:48, Ethernet0/0
      5.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        5.5.1.0/24 is directly connected, Loopback1
L        5.5.1.1/32 is directly connected, Loopback1
C        5.5.2.0/24 is directly connected, Loopback2
L        5.5.2.1/32 is directly connected, Loopback2
C        5.5.3.0/24 is directly connected, Loopback3
L        5.5.3.1/32 is directly connected, Loopback3
C        5.5.4.0/24 is directly connected, Loopback4
L        5.5.4.1/32 is directly connected, Loopback4
C        5.5.5.5/32 is directly connected, Loopback0
      6.0.0.0/32 is subnetted, 2 subnets
O IA     6.6.6.6 [110/1600] via 192.168.45.4, 04:56:43, Ethernet0/0
O IA     6.6.66.6 [110/601] via 192.168.45.4, 04:56:43, Ethernet0/0
O IA  192.168.13.0/24 [110/2543] via 192.168.45.4, 00:46:44, Ethernet0/0
O IA  192.168.23.0/24 [110/2543] via 192.168.45.4, 04:57:48, Ethernet0/0
O IA  192.168.34.0/24 [110/600] via 192.168.45.4, 04:57:48, Ethernet0/0

      192.168.45.0/24 is variably subnetted, 2 subnets, 2 masks
```


R6

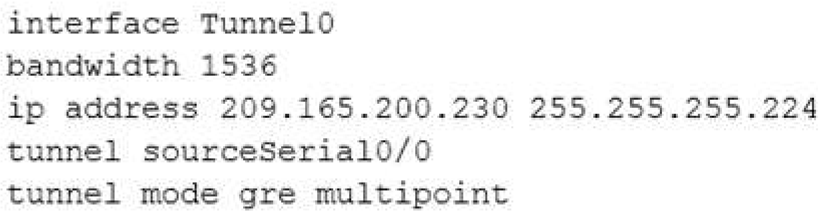
```
R6#show ip route
R6#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.46.4 to network 0.0.0.0

O*IA  0.0.0.0/0 [110/301] via 192.168.46.4, 05:09:56, Ethernet0/0
      6.0.0.0/32 is subnetted, 2 subnets
C        6.6.6.6 is directly connected, Loopback0
C        6.6.66.6 is directly connected, Loopback1
      192.168.46.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.46.0/24 is directly connected, Ethernet0/0
L        192.168.46.6/32 is directly connected, Ethernet0/0

R6#
```

Here we see R5's loopbacks in the routing table shown as connected, and the 6.6.6.6 loopback IP address of R6 is also seen as an OSPF route in R5's routing table.

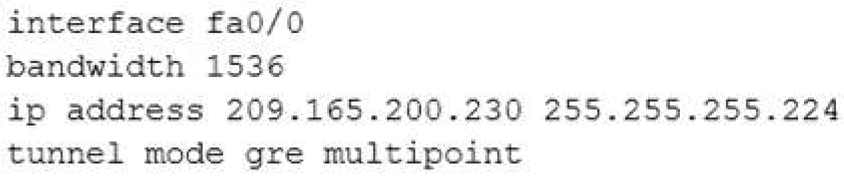
QUESTION 41

A company has just opened two remote branch offices that need to be connected to the corporate network. Which interface configuration output can be applied to the corporate router to allow communication to the remote sites?

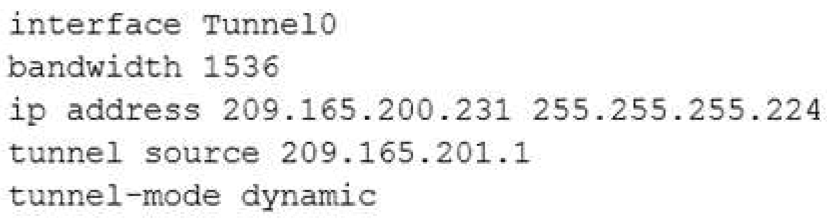
A.



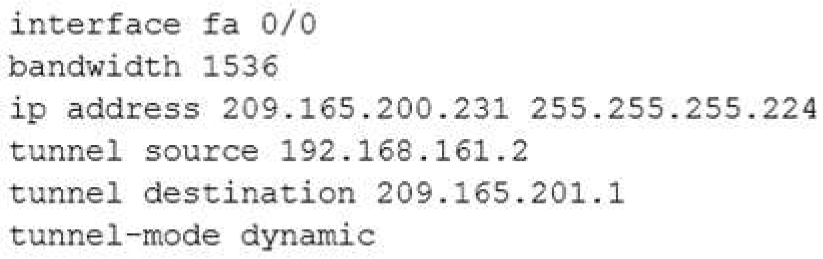
```
interface Tunnel0
bandwidth 1536
ip address 209.165.200.230 255.255.255.224
tunnel sourceSerial0/0
tunnel mode gre multipoint
```

B. 

```
interface fa0/0
bandwidth 1536
ip address 209.165.200.230 255.255.255.224
tunnel mode gre multipoint
```

C. 

```
interface Tunnel0
bandwidth 1536
ip address 209.165.200.231 255.255.255.224
tunnel source 209.165.201.1
tunnel-mode dynamic
```

D. 

```
interface fa 0/0
bandwidth 1536
ip address 209.165.200.231 255.255.255.224
tunnel source 192.168.161.2
tunnel destination 209.165.201.1
tunnel-mode dynamic
```

Correct Answer: A
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
The configuration of mGRE allows a tunnel to have multiple destinations. The configuration of mGRE on one side of a tunnel does not have any relation to the tunnel properties that might exist at the exit points. This means that an mGRE tunnel on the hub may connect to a p2p tunnel on the branch. Conversely, a p2p GRE tunnel may connect to an mGRE tunnel. The distinguishing feature between an mGRE interface and a p2p GRE interface is the tunnel destination. An mGRE interface does not have a configured destination. Instead the GRE tunnel is configured with the command **tunnel mode gre multipoint**. This command is used instead of the **tunnel destination** x.x.x.x found with p2p GRE tunnels. Besides allowing for multiple destinations, an mGRE tunnel requires NHRP to resolve the tunnel endpoints. Note, tunnel interfaces by default are point-to-point (p-p) using GRE encapsulation, effectively they have the **tunnel mode gre** command, which is not seen in the configuration because it is the default.
The mGRE configuration is as follows:

```
!
interface Tunnel0
 bandwidth 1536
 ip address 10.62.1.10 255.255.255.0
 tunnel source Serial0/0
 tunnel mode gre multipoint
```

Reference: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/DMVPDG/DMVPN_2_Phase2.html

QUESTION 42
A network engineer executes the show crypto ipsec sa command. Which three pieces of information are displayed in the output? (Choose three.)

A. inbound crypto map
B. remaining key lifetime
C. path MTU
D. tagged packets
E. untagged packets
F. invalid identity packets

Correct Answer: ABC
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
show crypto ipsec sa
This command shows IPsec SAs built between peers. The encrypted tunnel is built between 12.1.1.1 and 12.1.1.2 for traffic that goes between networks 20.1.1.0 and 10.1.1.0. You can see the two Encapsulating Security Payload (ESP) SAs built inbound and outbound. Authentication Header (AH) is not used since there are no AH SAs.
This output shows an example of the show crypto ipsec sa command (bolded ones found in answers for this question).

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 12.1.1.1
   local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
   current_peer: 12.1.1.2
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
    #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #Recv errors 0
     local crypto endpt.: 12.1.1.1, remote crypto endpt.: 12.1.1.2
     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound esp sas:
      spi: 0x136A010F(325714191)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4608000/52)
        IV size: 8 bytes
      replay detection support: Y
    inbound ah sas:
    inbound pcp sas:
inbound pcp sas:
outbound esp sas:
   spi: 0x3D3(979)
    transform: esp-3des esp-md5-hmac ,
    in use settings ={Tunnel, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test
    sa timing: remaining key lifetime (k/sec): (4608000/52)
    IV size: 8 bytes
    replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

QUESTION 43
Refer to the following output:

```
Router#show ip nhrp detail
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
TypE. Dynamic, Flags: authoritative unique nat registered used
NBMA address: 10.12.1.2
```

What does the authoritative flag mean in regards to the NHRP information?

A. It was obtained directly from the next-hop server.
B. Data packets are process switches for this mapping entry.
C. NHRP mapping is for networks that are local to this router.
D. The mapping entry was created in response to an NHRP registration request.
E. The NHRP mapping entry cannot be overwritten.

Correct Answer: A
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
Show NHRP: Examples
The following is sample output from the show ip nhrp command:

```
Router# show ip nhrp
10.0.0.2 255.255.255.255, tunnel 100 created 0:00:43 expire 1:59:16
 Type: dynamic Flags: authoritative
 NBMA address: 10.1111.1111.1111.1111.1111.1111.1111.1111.1111.11
10.0.0.1 255.255.255.255, Tunnel0 created 0:10:03 expire 1:49:56
 Type: static Flags: authoritative
 NBMA address: 10.1.1.2
```

The fields in the sample display are as follows:

- The IP address and its network mask in the IP-to-NBMA address cache. The mask is always 255.255.255.255 because Cisco does not support aggregation of NBMA information through NHRP.
- The interface type and number and how long ago it was created (hours:minutes:seconds).
- The time in which the positive and negative authoritative NBMA address will expire (hours:minutes:seconds). This value is based on the **ip nhrp holdtime** command.
- Type of interface:
  – dynamic — NBMA address was obtained from the NHRP Request packet.
  – static — NBMA address was statically configured.
- Flags:
  – authoritative — Indicates that the NHRP information was obtained from the Next Hop Server or router that maintains the NBMA-to-IP address mapping for a particular destination.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nhrp/configuration/xe-16/nhrp-xe-16-book/config-nhrp.html

QUESTION 44
Which common issue causes intermittent DMVPN tunnel flaps?

A. a routing neighbor reachability issue
B. a suboptimal routing table
C. interface bandwidth congestion
D. that the GRE tunnel to hub router is not encrypted

Correct Answer: A
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
DMVPN Tunnel Flaps Intermittently
Problem
DMVPN tunnel flaps intermittently.
Solution
When DMVPN tunnels flap, check the neighborship between the routers as issues with neighborship formation between routers may cause the DMVPN tunnel to flap. In order to resolve this problem, make sure the neighborship between the routers is always up.

Reference: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dcmvpn.html#Prblm1

QUESTION 45
Which encapsulation supports an interface that is configured for an EVN trunk?

A. 802.1Q
B. ISL
C. PPP
D. Frame Relay
E. MPLS
F. HDLC

Correct Answer: A
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
Restrictions for EVN

- An EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.
- A single IP infrastructure can be virtualized to provide up to 32 virtual networks end-to-end.
- If an EVN trunk is configured on an interface, you cannot configure VRF-Lite on the same interface.
- OSPFv3 is not supported; OSPFv2 is supported.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.pdf

QUESTION 46
Which three characteristics are shared by subinterfaces and associated EVNs? (Choose three.)

A. IP address
B. routing table
C. forwarding table
D. access control lists
E. NetFlow configuration

Correct Answer: ABC
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
A trunk interface can carry traffic for multiple EVNs. To simplify the configuration process, all the subinterfaces and associated EVNs have the same IP address assigned. In other words, the trunk interface is identified by the same IP address in different EVN contexts. This is accomplished as a result of each EVN having a unique routing and forwarding table, thereby enabling support for overlapping IP addresses across multiple EVNs.

Reference: http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/xe-3sg/evn-overview.pdf

QUESTION 47
A user is having issues accessing file shares on a network. The network engineer advises the user to open a web browser, input a prescribed IP address, and follow the instructions. After doing this, the user is able to access company shares. Which type of remote access did the engineer enable?

A. EZVPN
B. Ipsec VPN client access
C. VPDN client access
D. SSL VPN client access

Correct Answer: D
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
The Cisco AnyConnect VPN Client provides secure SSL connections to the security appliance for remote users. Without a previously installed client, remote users enter the IP address in their browser of an interface configured to accept SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<address>.
After entering the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it downloads the client that matches the operating system of the remote computer. After downloading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

Reference: http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100936-asa8x-split-tunnel-anyconnect-config.html

QUESTION 48
Which Cisco IOS VPN technology leverages Ipsec, mGRE, dynamic routing protocol, NHRP, and Cisco Express Forwarding?

A. FlexVPN
B. DMVPN
C. GETVPN
D. Cisco Easy VPN

Correct Answer: B
Section: VPN Technologies
Explanation

Explanation/Reference:
Explanation:
Dynamic Multipoint Virtual Private Network (DMVPN) is a dynamic tunneling form of a virtual private network (VPN) supported on Cisco IOS-based routers and Unix-like Operating Systems based on the standard protocols, GRE, NHRP and Ipsec. This DMVPN provides the capability for creating a dynamic-mesh

VPN network without having to pre-configure (static) all possible tunnel end-point peers, including Ipsec (Internet Protocol Security) and ISAKMP (Internet Security Association and Key Management Protocol) peers. DMVPN is initially configured to build out a hub-and-spoke network by statically configuring the hubs (VPN headends) on the spokes, no change in the configuration on the hub is required to accept new spokes. Using this initial hub-and-spoke network, tunnels between spokes can be dynamically built on demand (dynamic-mesh) without additional configuration on the hubs or spokes. This dynamic-mesh capability alleviates the need for any load on the hub to route data between the spoke networks.
DMVPN is combination of the following technologies:

- Multipoint GRE (mGRE)
- Next-Hop Resolution Protocol (NHRP)
- Dynamic Routing Protocol (EIGRP, RIP, OSPF, BGP)
- Dynamic Ipsec encryption
- Cisco Express Forwarding (CEF)

Reference: http://en.wikipedia.org/wiki/Dynamic_Multipoint_Virtual_Private_Network

QUESTION 49
Which traffic does the following configuration allow?

```
Ipv6 access-list cisco
permit ipv6 host 2001:DB8:0:4::32 any eq ssh
line vty 0 4
ipv6 access-class cisco in
```

A. all traffic to vty 0 4 from source 2001:DB8:0:4::32

B. only ssh traffic to vty 0 4 from source all

C. only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32

D. all traffic to vty 0 4 from source all

Correct Answer: C
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
Here we see that the Ipv6 access list called “cisco” is being applied to incoming VTY connections to the router. Ipv6 access list has just one entry, which allows only the single Ipv6 IP address of 2001:DB8:0:4::32 to connect using SSH only.

QUESTION 50
For troubleshooting purposes, which method can you use in combination with the “debug ip packet” command to limit the amount of output data?

A. You can disable the IP route cache globally.

B. You can use the KRON scheduler.

C. You can use an extended access list.

D. You can use an IOS parser.

E. You can use the RITE traffic exporter.

Correct Answer: C
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
The “debug ip packet” command generates a substantial amount of output and uses a substantial amount of system resources. This command should be used with caution in production networks. Always use with the access-list command to apply an extended ACL to the debug output.

Reference: http://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html

QUESTION 51
Refer to the following access list.

```
Access-list 100 permit ip any any log
```

After applying the access list on a Cisco router, the network engineer notices that the router CPU utilization has risen to 99 percent. What is the reason for this?

A. A packet that matches access-list with the “log” keyword is Cisco Express Forwarding switched.

B. A packet that matches access-list with the "log" keyword is fast switched.

C. A packet that matches access-list with the "log" keyword is process switched.

D. A large amount of IP traffic is being permitted on the router.

Correct Answer: C
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
Logging-enabled access control lists (ACLs) provide insight into traffic as it traverses the network or is dropped by network devices. Unfortunately, ACL logging can be CPU intensive and can negatively affect other functions of the network device. There are two primary factors that contribute to the CPU load increase from ACL logging: process switching of packets that match log-enabled access control entries (ACEs) and the generation and transmission of log messages.

Reference: http://www.cisco.com/web/about/security/intelligence/acl-logging.html#4

QUESTION 52
Which address is used by the Unicast Reverse Path Forwarding protocol to validate a packet against the routing table?

A. source address

B. destination address
C. router interface
D. default gateway

Correct Answer: A
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribal Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.

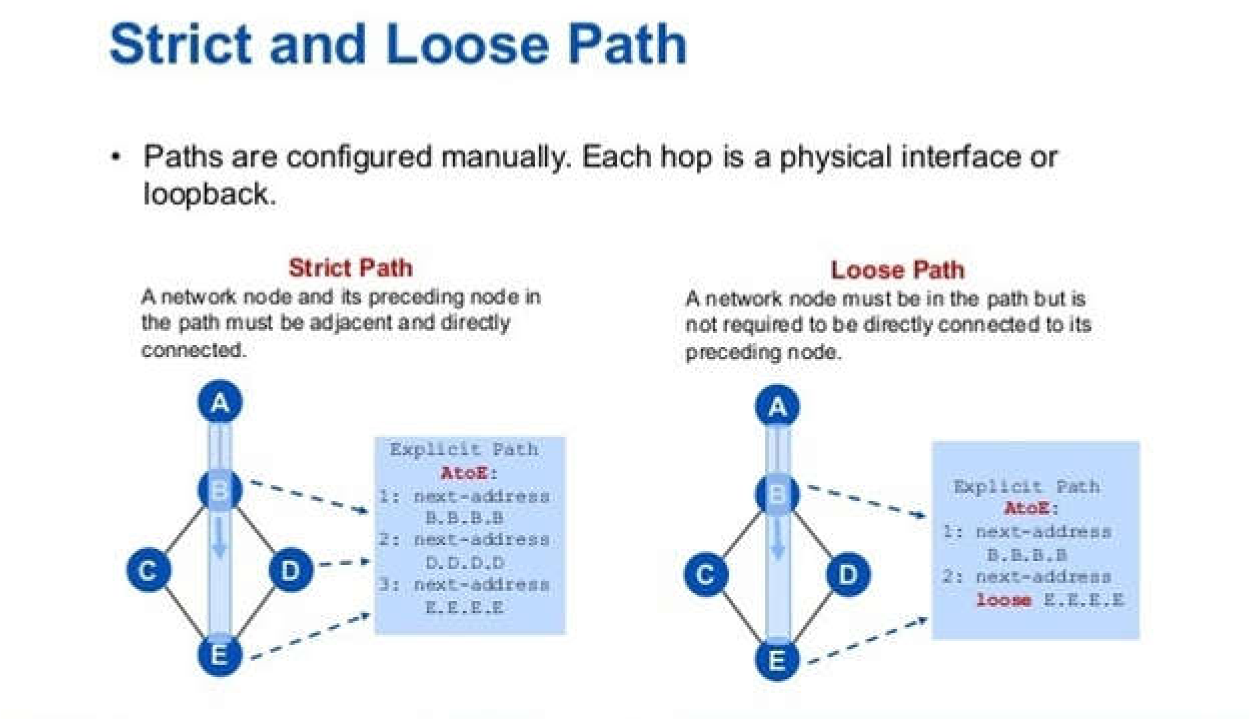
Reference: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html

QUESTION 53
What are the three modes of Unicast Reverse Path Forwarding?

A. strict mode, loose mode, and VRF mode
B. strict mode, loose mode, and broadcast mode
C. strict mode, broadcast mode, and VRF mode
D. broadcast mode, loose mode, and VRF mode

Correct Answer: A
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:



Strict and Loose Path

- Paths are configured manually. Each hop is a physical interface or loopback.

Strict Path
A network node and its preceding node in the path must be adjacent and directly connected.

```
Explicit Path
AtoE:
1: next-address
   B.B.B.B
2: next-address
   D.D.D.D
3: next-address
   E.E.E.E
```

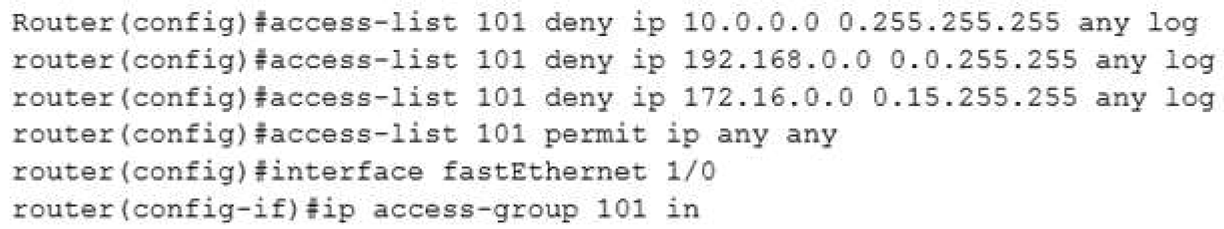
Loose Path
A network node must be in the path but is not required to be directly connected to its preceding node.

```
Explicit Path
AtoE:
1: next-address
   B.B.B.B
2: next-address
   loose E.E.E.E
```

Network administrators can use Unicast Reverse Path Forwarding (Unicast RPF) to help limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. **Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode.** Note that not all network devices support all three modes of operation. Unicast RPF in VRF mode will not be covered in this document.
When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.
When administrators use Unicast RPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the **allow-default** option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode.
Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be of concern when deploying this feature, Unicast RPF loose mode is a scalable option for networks that contain asymmetric routing paths.

Reference: http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html

QUESTION 54
What does the following access list, which is applied on the external interface FastEthernet 1/0 of the perimeter router, accomplish?



```
Router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any log
router(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any log
router(config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any log
router(config)#access-list 101 permit ip any any
router(config)#interface fastEthernet 1/0
router(config-if)#ip access-group 101 in
```

A. It prevents incoming traffic from IP address ranges 10.0.0.0-10.0.0.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 and logs any intrusion attempts.
B. It prevents the internal network from being used in spoofed denial of service attacks and logs any exit to the Internet.
C. It filters incoming traffic from private addresses in order to prevent spoofing and logs any intrusion attempts.
D. It prevents private internal addresses to be accessed directly from outside.

Correct Answer: C
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
The private IP address ranges defined in RFC 1918 are as follows:
10.0.0.0 — 10.255.255.255
172.16.0.0 — 172.31.255.255
192.168.0.0 — 192.168.255.255
These IP addresses should never be allowed from external networks into a corporate network as they would only be able to reach the network from the outside via routing problems or if the IP addresses were spoofed. This ACL is used to prevent all packets with a spoofed reserved private source IP address to enter the network. The log keyword also enables logging of this intrusion attempt.

QUESTION 55
Refer to the following command:

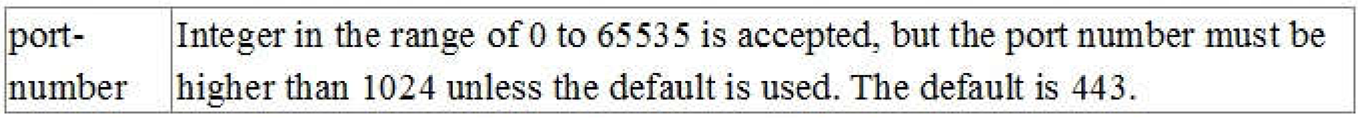
```
router(config)# ip http secure-port 4433
```

Which statement is true?

A. The router will listen on port 4433 for HTTPS traffic.
B. The router will listen on port 4433 for HTTP traffic.
C. The router will never accept any HTTP and HTTPS traffic.
D. The router will listen to HTTP and HTTP traffic on port 4433.

Correct Answer: A
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
To set the secure HTTP (HTTPS) server port number for listening, use the ip http secure-port command in global configuration mode. To return the HTTPS server port number to the default, use the no form of this command.
Ip http secure-port port-number
no ip http secure-port
Syntax Description



port-number	Integer in the range of 0 to 65535 is accepted, but the port number must be higher than 1024 unless the default is used. The default is 443.

Reference: http://www.cisco.com/en/US/docs/ios-xml/ios/https/command/nm-https-cr-cl-sh.html#wp3612805529

QUESTION 56
A network engineer is configuring a routed interface to forward broadcasts of UDP 69, 53, and 49 to 172.20.14.225. Which command should be applied to the configuration to allow this?

A. router(config-if)#ip helper-address 172.20.14.225
B. router(config-if)#udp helper-address 172.20.14.225
C. router(config-if)#ip udp helper-address 172.20.14.225
D. router(config-if)#ip helper-address 172.20.14.225 69 53 49

Correct Answer: A
Section: Infrastructure Security
Explanation

Explanation/Reference:
Explanation:
To let a router forward broadcast packet the command ip helper-address can be used. The broadcasts will be forwarded to the unicast address which is specified with the ip helper command.

ip helper-address {ip address}

When configuring the ip helper-address command, the following broadcast packets will be forwarded by the router by default:
- TFTP — UDP port 69
- Domain Name System (DNS) – UDP port 53
- Time service — port 37
- NetBIOS Name Server — port 137
- NetBIOS Datagram Server — port 138
- Bootstrap Protocol (BOOTP) — port 67
- TACACS – UDP port 49

QUESTION 57
A network engineer is configuring SNMP on network devices to utilize one-way SNMP notifications. However, the engineer is not concerned with authentication or encryption. Which command satisfies the requirements of this scenario?

A. router(config)#snmp-server host 172.16.201.28 traps version 2c CISCORO
B. router(config)#snmp-server host 172.16.201.28 informs version 2c CISCORO

C. router(config)#snmp-server host 172.16.201.28 traps version 3 auth CISCORO
D. router(config)#snmp-server host 172.16.201.28 informs version 3 auth CISCORO

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Most network admins and engineers are familiar with SNMPv2c which has become the dominant SNMP version of the past decade. It's simple to configure on both the router/switch-side and just as easy on the network monitoring server. The problem of course is that the SNMP statistical payload is not encrypted and authentication is passed in cleartext. Most companies have decided that the information being transmitted isn't valuable enough to be worth the extra effort in upgrading to SNMPv3, but I would suggest otherwise.
Like IPv4 to Ipv6, there are some major changes under the hood. SNMP version 2 uses community strings (think clear text passwords, no encryption) to authenticate polling and trap delivery. SNMP version 3 moves away from the community string approach in favor of user-based authentication and view-based access control. The users are not actual local user accounts, rather they are simply a means to determine who can authenticate to the device. The view is used to define what the user account may access on the IOS device. Finally, each user is added to a group, which determines the access policy for its users. Users, groups, views.

QUESTION 58
When using SNMPv3 with NoAuthNoPriv, which string is matched for authentication?

A. username
B. password
C. community-string
D. encryption-key

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
The following security models exist: SNMPv1, SNMPv2, SNMPv3. The following security levels exits: "noAuthNoPriv" (no authentiation and no encryption – noauth keyword in CLI), "AuthNoPriv109thernet109ationre authenticated but not encrypted – auth keyword in CLI), "AuthPriv" (messages are authenticated and encrypted – priv keyword in CLI). SNMPv1 and SNMPv2 models only support the "noAuthNoPriv" model since they use plain community string to match the incoming packets. The SNMPv3 implementations could be configured to use either of the models on per-group basis (**in case if "noAuthNoPriv" is configured, username serves as a replacement for community string**).

Reference: http://blog.ine.com/2008/07/19/snmpv3-tutorial/

QUESTION 59
After a recent DoS attack on a network, senior management asks you to implement better logging functionality on all IOS-based devices. Which two actions can you take to provide enhanced logging results? (Choose two.)

A. Use the msec option to enable service time stamps.
B. Increase the logging history
C. Set the logging severity level to 1.
D. Specify a logging rate limit.
E. Disable event logging on all noncritical items.

Correct Answer: AB
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
The optional **msec** keyword specifies the date/time format should include milliseconds. This can aid in pinpointing the exact time of events, or to correlate the order that the events happened. To limit syslog messages sent to the router's history table and to an SNMP network management station based on severity, use the logging history command in global configuration mode. By default, Cisco devices Log error messages of severity levels 0 through 4 (emergency, alert, critical, error, and warning levels); in other words, "saving level warnings or higher." By increasing the severity level, more granular monitoring can occur, and SNMP messages will be sent by the less sever (5-7) messages.

QUESTION 60
A network engineer finds that a core router has crashed without warning. In this situation, which feature can the engineer use to create a crash collection?

A. secure copy protocol
B. core dumps
C. warm reloads
D. SNMP
E. NetFlow

Correct Answer: B
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
When a router crashes, it is sometimes useful to obtain a full copy of the memory image (called a core dump) to identify the cause of the crash. Core dumps are generally very useful to your technical support representative.
Four basic ways exist for setting up the router to generate a core dump:

- Using Trivial File Transfer Protocol (TFTP)
- Using File Transfer Protocol (FTP)
- Using remote copy protocol (rcp)
- Using a Flash disk

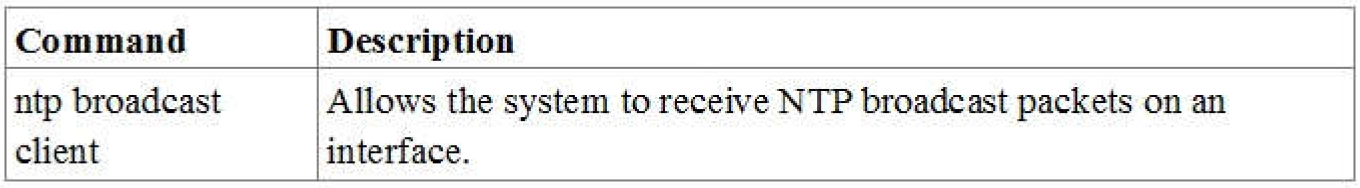
Reference: http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr19aa.html

QUESTION 61
A network engineer is trying to implement broadcast-based NTP in a network and executes the ntp broadcast client command. Assuming that an NTP server is already set up, what is the result of the command?

A. It enables receiving NTP broadcasts on the interface where the command was executed.
B. It enables receiving NTP broadcasts on all interfaces globally.
C. It enables a device to be an NTP peer to another device.
D. It enables a device to receive NTP broadcast and unicast packets.

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
The NTP service can be activated by entering any ntp command. When you use the ntp broadcast client command, the NTP service is activated (if it has not already been activated) and the device is configured to receive NTP broadcast packets on a specified interface simultaneously.



Command	Description
ntp broadcast client	Allows the system to receive NTP broadcast packets on an interface.

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/command/bsm-xe-3se-3850-cr-book/bsm-xe-3se-3850-cr-book_chapter_00.html

QUESTION 62
What is a function of NPTv6?

A. It interferes with encryption of the full IP payload.
B. It maintains a per-node state.
C. It is checksum-neutral.
D. It rewrites transport layer headers.

Correct Answer: C
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
RFC 6296 describes a stateless Ipv6-to-Ipv6 Network Prefix Translation (NPTv6) function, designed to provide address independence to the edge network. It is transport-agnostic with respect to transports that do not checksum the IP header, such as SCTP, and to transports that use the TCP/UDP/DCCP (Datagram Congestion Control Protocol) pseudo-header and checksum
NPTv6 provides a simple and compelling solution to meet the address-independence requirement in Ipv6. The address-independence benefit stems directly from the translation function of the network prefix translator. To avoid as many of the issues associated with NAPT44 as possible, NPTv6 is defined to include a two-way, checksum-neutral, algorithmic translation function, and nothing else.

Reference: http://tools.ietf.org/html/rfc6296

QUESTION 63
Ipv6 has just been deployed to all of the hosts within a network, but not to the servers. Which feature allows Ipv6 devices to communicate with Ipv4 servers?

A. NAT
B. NATng
C. NAT64
D. dual-stack NAT
E. DNS64

Correct Answer: C
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
NAT64 is a mechanism to allow Ipv6 hosts to communicate with Ipv4 servers. The NAT64 server is the endpoint for at least one Ipv4 address and an Ipv6 network segment of 32-bits (for instance 64:ff9b::/96, see RFC 6052, RFC 6146). The Ipv6 client embeds the Ipv4 address it wishes to communicate with using these bits, and sends its packets to the resulting address. The NAT64 server then creates a NAT-mapping between the Ipv6 and the Ipv4 address, allowing them to communicate.

Reference: http://en.wikipedia.org/wiki/NAT64

QUESTION 64
A network engineer initiates the ip sla responder tcp-connect command in order to gather statistics for performance gauging. Which type of statistics does the engineer see?

A. connectionless-oriented
B. service-oriented
C. connection-oriented
D. application-oriented

Correct Answer: C

Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Configuration Examples for IP SLAs TCP Connect Operations
The following example shows how to configure a TCP Connection-oriented operation from Device B to the Telnet port (TCP port 23) of IP Host 1 (IP address 10.0.0.1), as shown in the “TCP Connect Operation” figure in the “Information About the IP SLAs TCP Connect Operation” section. The operation is scheduled to start immediately. In this example, the control protocol is disabled on the source (Device B). IP SLAs uses the control protocol to notify the IP SLAs responder to enable the target port temporarily. This action allows the responder to reply to the TCP Connect operation. In this example, because the target is not a Cisco device and a well-known TCP port is used, there is no need to send the control message.
Device A (target device) Configuration
configure terminal
 ip sla responder tcp-connect ipaddress 10.0.0.1 port 23

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_tcp_conn.html

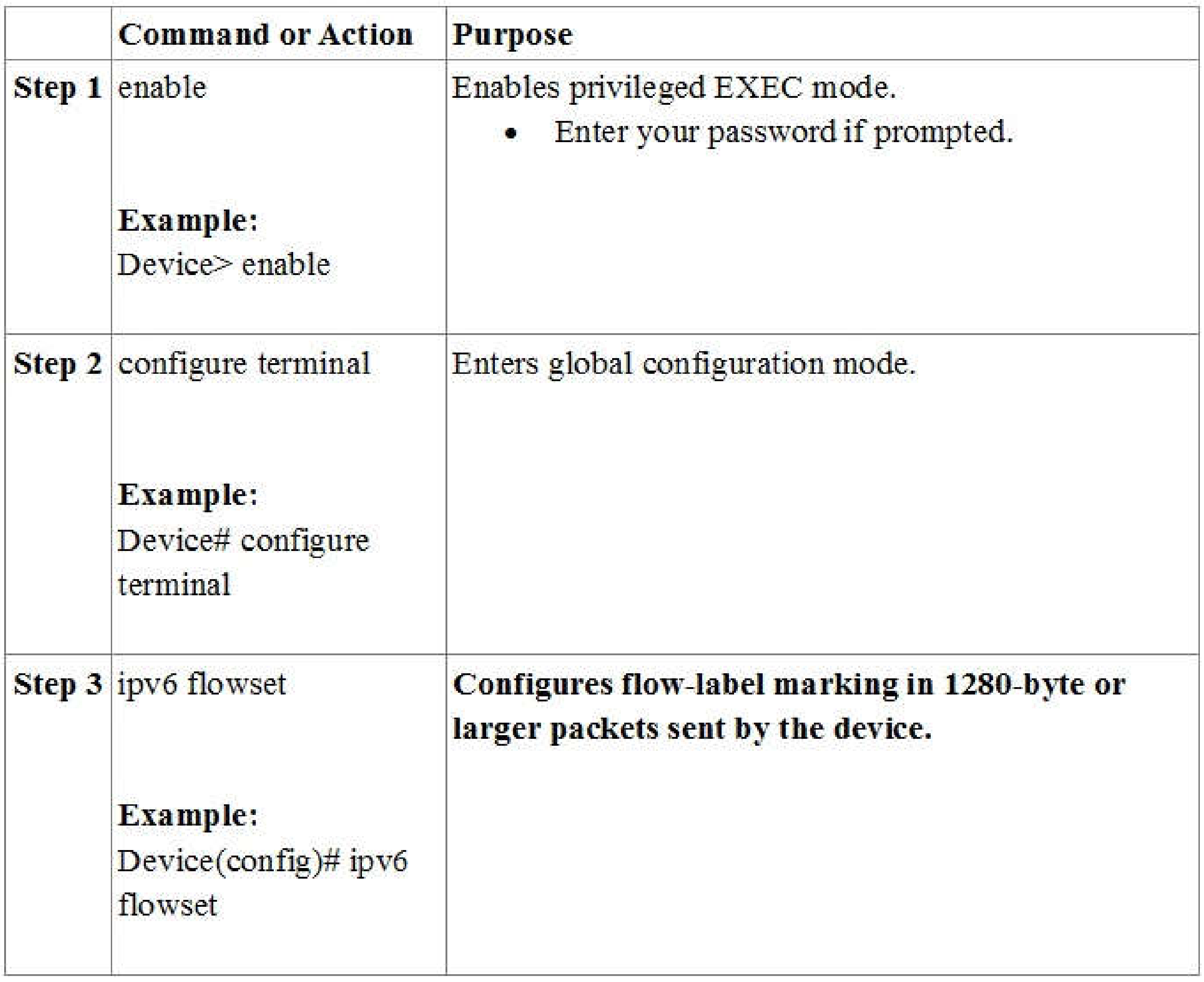
QUESTION 65
A network engineer executes the “ipv6 flowset” command. What is the result?

A. Flow-label marking in 1280-byte or larger packets is enabled.
B. Flow-set marking in 1280-byte or larger packets is enabled.
C. Ipv6 PMTU is enabled on the router.
D. Ipv6 flow control is enabled on the router.

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Enabling Flow-Label Marking in Packets that Originate from the Device
This feature allows the device to track destinations to which the device has sent packets that are 1280 bytes or larger.
SUMMARY STEPS
1. enable
2. configure terminal
3. ipv6 flowset
4. exit
5. clear ipv6 mtu

DETAILED STEPS



	Command or Action	**Purpose**
Step 1	enable **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	ipv6 flowset **Example:** Device(config)# ipv6 flowset	**Configures flow-label marking in 1280-byte or larger packets sent by the device.**

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/15-mt/ip6b-15-mt-book/ip6-mtu-path-disc.html

QUESTION 66
A network engineer executes the show ip flow export command. Which line in the output indicates that the send queue is full and export packets are not being sent?

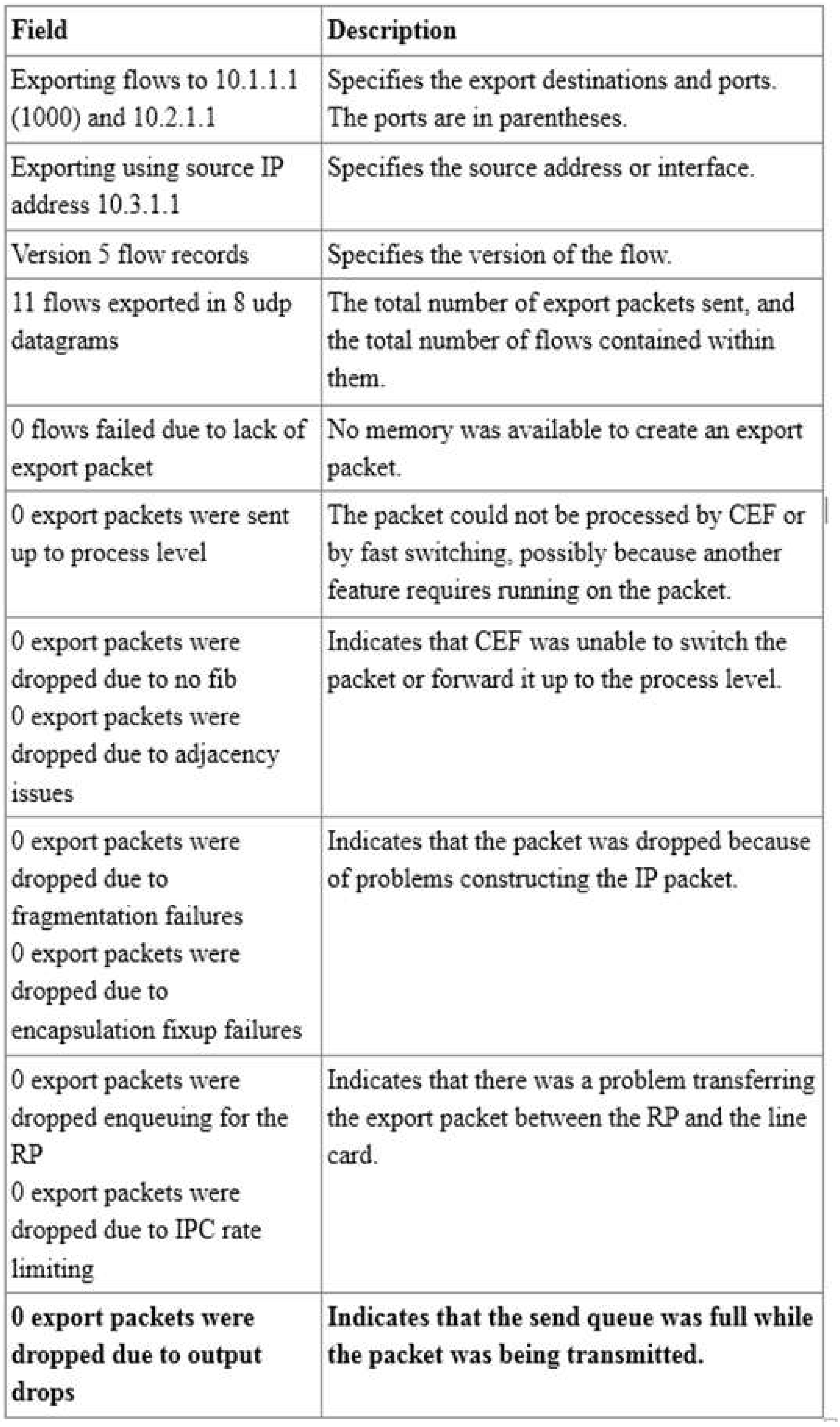
A. output drops
B. enqueuing for the RP
C. fragmentation failures

D. adjacency issues

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:

Table 5 show ip flow export Field Descriptions



Field	Description
Exporting flows to 10.1.1.1 (1000) and 10.2.1.1	Specifies the export destinations and ports. The ports are in parentheses.
Exporting using source IP address 10.3.1.1	Specifies the source address or interface.
Version 5 flow records	Specifies the version of the flow.
11 flows exported in 8 udp datagrams	The total number of export packets sent, and the total number of flows contained within them.
0 flows failed due to lack of export packet	No memory was available to create an export packet.
0 export packets were sent up to process level	The packet could not be processed by CEF or by fast switching, possibly because another feature requires running on the packet.
0 export packets were dropped due to no fib 0 export packets were dropped due to adjacency issues	Indicates that CEF was unable to switch the packet or forward it up to the process level.
0 export packets were dropped due to fragmentation failures 0 export packets were dropped due to encapsulation fixup failures	Indicates that the packet was dropped because of problems constructing the IP packet.
0 export packets were dropped enqueuing for the RP 0 export packets were dropped due to IPC rate limiting	Indicates that there was a problem transferring the export packet between the RP and the line card.
0 export packets were dropped due to output drops	**Indicates that the send queue was full while the packet was being transmitted.**

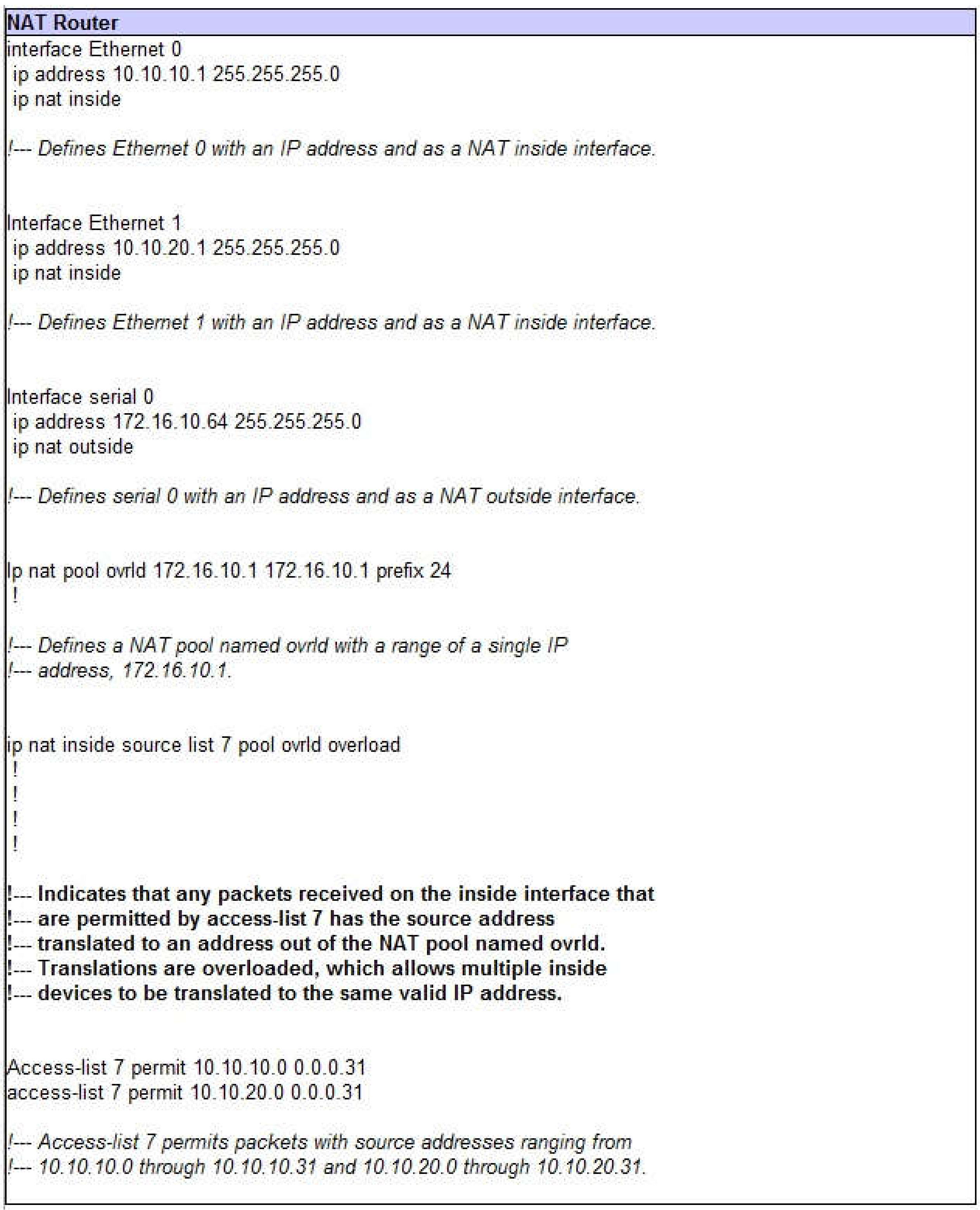
References:
http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/oaggnf.html

QUESTION 67
A network engineer is asked to configure a “site-to-site” Ipsec VPN tunnel. One of the last things that the engineer does is to configure an access list (access-list 1 permit any) along with the command ip nat inside source list 1 int s0/0 overload. Which functions do the two commands serve in this scenario?

A. The command access-list 1 defines interesting traffic that is allowed through the tunnel.
B. The command ip nat inside source list 1 int s0/0 overload disables “many-to-one” access for all devices on a defined segment to share a single IP address upon exiting the external interface.
C. The command access-list 1 permit any defines only one machine that is allowed through the tunnel.
D. The command ip nat inside source list 1 int s0/0 overload provides “many-to-one” access for all devices on a defined segment to share a single IP address upon exiting the external interface.

Correct Answer: D
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Configuring NAT to Allow Internal Users to Access the Internet Using Overloading



NAT Router

```
interface Ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 0 with an IP address and as a NAT inside interface.


Interface Ethernet 1
 ip address 10.10.20.1 255.255.255.0
 ip nat inside

!--- Defines Ethernet 1 with an IP address and as a NAT inside interface.


Interface serial 0
 ip address 172.16.10.64 255.255.255.0
 ip nat outside

!--- Defines serial 0 with an IP address and as a NAT outside interface.


Ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24
 !

!--- Defines a NAT pool named ovrld with a range of a single IP
!--- address, 172.16.10.1.


ip nat inside source list 7 pool ovrld overload
 !
 !
 !
 !

!--- Indicates that any packets received on the inside interface that
!--- are permitted by access-list 7 has the source address
!--- translated to an address out of the NAT pool named ovrld.
!--- Translations are overloaded, which allows multiple inside
!--- devices to be translated to the same valid IP address.


Access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Access-list 7 permits packets with source addresses ranging from
!--- 10.10.10.0 through 10.10.10.31 and 10.10.20.0 through 10.10.20.31.
```

Note in the previous second configuration, the NAT pool “ovrld”only has a range of one address. The keyword **overload** used in the **ip nat inside source list 7 pool ovrld overload** command allows NAT to translate multiple inside devices to the single address in the pool.

Reference: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094e77.shtml

QUESTION 68
A network engineer is configuring a solution to allow failover of HSRP nodes during maintenance windows, as an alternative to powering down the active router and letting the network respond accordingly. Which action will allow for manual switching of HSRP nodes?

A. Track the up/down state of a loopback interface and shut down this interface during maintenance.
B. Adjust the HSRP priority without the use of preemption.
C. Disable and enable all active interfaces on the active HSRP node.
D. Enable HSRPv2 under global configuration, which allows for maintenance mode.

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
The **standby track** command allows you to specify another interface on the router for the HSRP process to monitor in order to alter the HSRP priority for a given group. If the line protocol of the specified interface goes down, the HSRP priority is reduced. This means that another HSRP router with higher priority can become the active router if that router has **standby preempt** enabled. Loopback interfaces can be tracked, so when this interface is shut down the HSRP priority for that router will be lowered and the other HSRP router will then become the active one.

Reference: http://www.cisco.com/c/en/us/support/docs/ip/hot-standby-router-protocol-hsrp/13780-6.html

QUESTION 69
A network engineer is notified that several employees are experiencing network performance related issues, and bandwidth-intensive applications are identified as the root cause. In order to identify which specific type of traffic is causing this slowness, information such as the source/destination IP and Layer 4 port numbers is required. Which feature should the engineer use to gather the required information?

A. SNMP
B. Cisco IOS EEM
C. NetFlow
D. Syslog
E. WCCP

Correct Answer: C
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
NetFlow Flows Key Fields
A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and transport-layer source and des—nation port numbers. Specifically, a flow is identified as the combination of the following key fields:

- Source IP address
- Destination IP address
- Source Layer 4 port number
- Destination Layer 4 port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

QUESTION 70
An organization decides to implement NetFlow on its network to monitor the fluctuation of traffic that is disrupting core services. After reviewing the output of NetFlow, the network engineer is unable to see OUT traffic on the interfaces. What can you determine based on this information?

A. Cisco Express Forwarding has not been configured globally.
B. NetFlow output has been filtered by default.
C. Flow Export version 9 is in use.
D. The command ip flow-capture fragment-offset has been enabled.

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
We came across a recent issue where a user setup a router for NetFlow export but was unable to see the OUT traffic for the interfaces in NetFlow Analyzer. Every NetFlow configuration aspect was checked and nothing incorrect was found. That is when we noticed the 'no ip cef' command on the router. CEF was enabled at the global level and within seconds, NetFlow Analyzer started showing OUT traffic for the interfaces. This is why this topic is about Cisco Express Forwarding.
What is switching?
A Router must make decisions about where to forward the packets passing through. This decision-making process is called "switching". Switching is what a router does when it makes the following decisions:
1. Whether to forward or not forward the packets after checking that the destination for the packet is reachable.
2. If the destination is reachable, what is the next hop of the router and which interface will the router use to get to that destination.
What is CEF?
CEF is one of the available switching options for Cisco routers. Based on the routing table, CEF creates its own table, called the Forwarding Information Base (FIB). The FIB is organized differently than the routing table and CEF uses the FIB to decide which interface to send traffic from. CEF offers the following benefits:
1. Better performance than fast-switching (the default) and takes less CPU to perform the same task.
2. When enabled, allows for advanced features like NBAR
3. Overall, CEF can switch traffic faster than route-caching using fast-switching
How to enable CEF?
CEF is disabled by default on all routers except the 7xxx series routers. Enabling and Disabling CEF is easy. To enable CEF, go into global configuration mode and enter the CEF command.
Router# config t
Router(config)# ip cef
Router(config)#
To disable CEF, simply use the 'no' form of the command, ie. '**no ip cef**'.
Why CEF Needed when enabling NetFlow?
CEF is a prerequisite to enable NetFlow on the router interfaces. CEF decides through which interface traffic is exiting the router. Any NetFlow analyzer product will calculate the OUT traffic for an interface based on the **Destination Interface** value present in the NetFlow packets exported from the router. If the CEF is disabled on the router, the NetFlow packets exported from the router will have "Destination interface" as "null" and this leads NetFlow Analyzer to show no OUT traffic for the interfaces. Without enabling the CEF on the router, the NetFlow packets did not mark the destination interfaces and so NetFlow Analyzer was not able to show the OUT traffic for the interfaces.

Reference: https://blogs.manageengine.com/network-2/netflowanalyzer/2010/05/19/need-for-cef-in-netflow-data-export.html

QUESTION 71
A network engineer has left a NetFlow capture enabled over the weekend to gather information regarding excessive bandwidth utilization. The following command is entered:

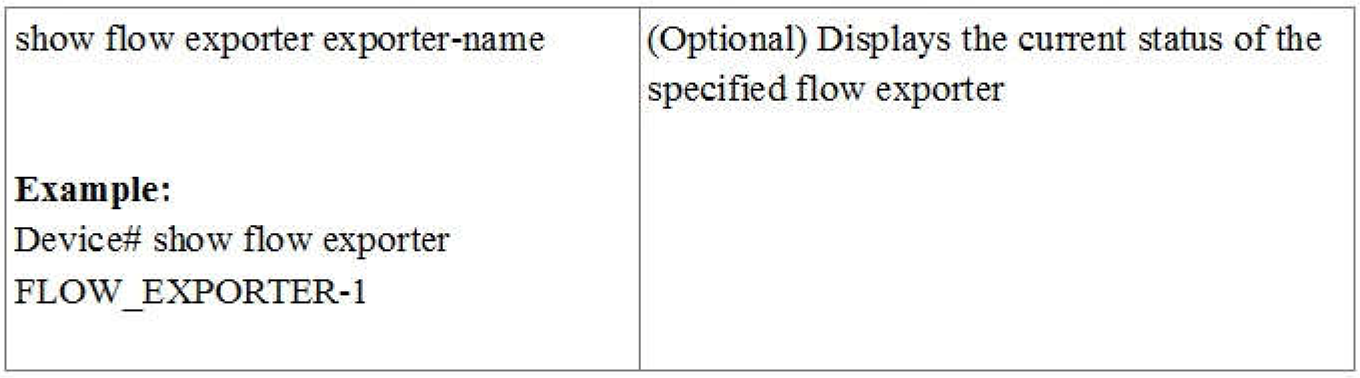
```
switch#show flow exporter Flow_Exporter-1
```

What is the expected output?

A. configuration of the specified flow exporter
B. current status of the specified flow exporter
C. status and statistics of the specified flow monitor
D. configuration of the specified flow monitor

Correct Answer: B
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:



show flow exporter exporter-name **Example:** Device# show flow exporter FLOW_EXPORTER-1	(Optional) Displays the current status of the specified flow exporter

Reference: http://www.cisco.com/en/US/docs/ios-xml/ios/fnetflow/configuration/15-mt/cfg-de-fnflow-exprts.html

QUESTION 72
A company's corporate policy has been updated to require that stateless, 1-to-1, and Ipv6 to Ipv6 translations at the Internet edge are performed. What is the best solution to ensure compliance with this new policy?

A. NAT64
B. NAT44
C. NATv6
D. NPTv4
E. NPTv6

Correct Answer: E
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
NPTv6 provides a mechanism to translate the private internal organization prefixes to public globally reachable addresses. The translation mechanism is stateless and provides a 1:1 relationship between the internal addresses and external addresses. The use cases for NPTv6 outlined in the RFC include peering with partner networks, multi homing, and redundancy and load sharing.

Reference: http://www.cisco.com/c/dam/en/us/td/docs/solutions/SBA/August2012/Cisco_SBA_BN_IPv6AddressingGuide-Aug2012.pdf

QUESTION 73
Which two functions are completely independent when implementing NAT64 over NAT-PT? (Choose two.)

A. DNS
B. NAT
C. port redirection
D. stateless translation
E. session handling

Correct Answer: AB
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Work Address Translation IPv6 to IPv4, or NAT64, technology facilitates communication between IPv6-only and IPv4-only hosts and networks (whether in a transit, an access, or an edge network). This solution allows both enterprises and ISPs to accelerate IPv6 adoption while simultaneously handling IPv4 address depletion. The DnS64 and NAT64 functions are completely separated, which is essential to the superiority of NAT64 over NAT-PT.

Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

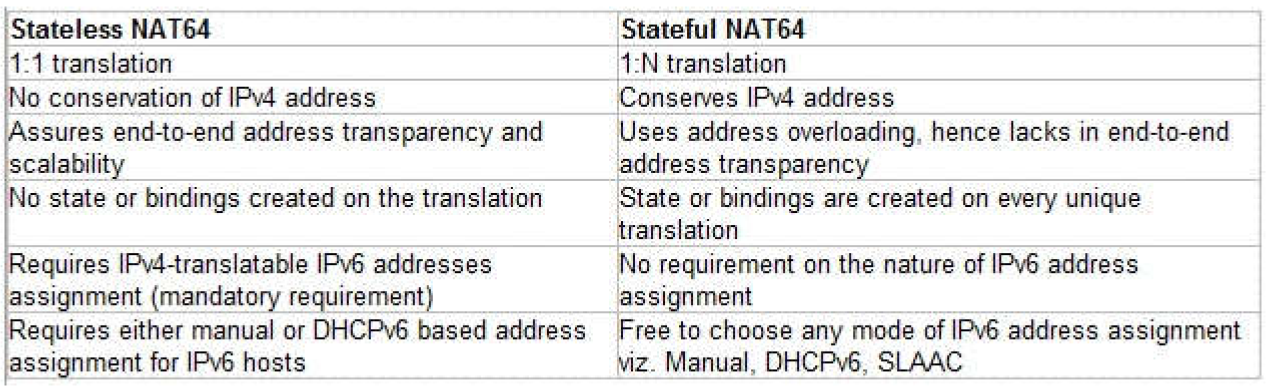
QUESTION 74
Which two methods of deployment can you use when implementing NAT64? (Choose two.)

A. stateless
B. stateful
C. manual
D. automatic
E. static
F. functional
G. dynamic

Correct Answer: AB
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
While stateful and stateless NAT64 perform the task of translating IPv4 packets into IPv6 packets and vice versa, there are important differences. The following table provides a high-level overview of the most relevant differences.

Table 2. Differences Between Stateless NAT64 and Stateful NAT64



Stateless NAT64	Stateful NAT64
1:1 translation	1:N translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment (mandatory requirement)	No requirement on the nature of IPv6 address assignment
Requires either manual or DHCPv6 based address assignment for IPv6 hosts	Free to choose any mode of IPv6 address assignment viz. Manual, DHCPv6, SLAAC

Reference: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676277.html

QUESTION 75
Which NetFlow component is applied to an interface and collects information about flows?

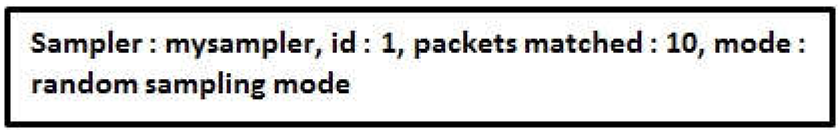
A. flow monitor
B. flow exporter
C. flow sampler
D. flow collector

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
Flow monitors are the NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the record, which is configured for the flow monitor and stored in the flow monitor cache.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/fnetflow/command/reference/fnf_book/fnf_01.html#wp1314030

QUESTION 76
Refer to the exhibit.



```
Sampler : mysampler, id : 1, packets matched : 10, mode :
random sampling mode
```

Which statement about the output of the show flow-sampler command is true?

A. The sampler matched 10 packets, each packet randomly chosen from every group of 100 packets.
B. The sampler matched 10 packets, one packet every 100 packets.
C. The sampler matched 10 packets, each one randomly chosen from every 100-second interval.
D. The sampler matched 10 packets, one packet every 100 seconds.

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
The sampling mode determines the algorithm that selects a subset of traffic for NetFlow processing. In the random sampling mode that Random Sampled NetFlow uses, incoming packets are randomly selected so that one out of each n sequential packets is selected on average for NetFlow processing. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th, 120th, 199th, 302nd, and so on packets. This sample configuration provides NetFlow data on 1 percent of total traffic. The n value is a parameter from 1 to 65535 packets that you can configure.

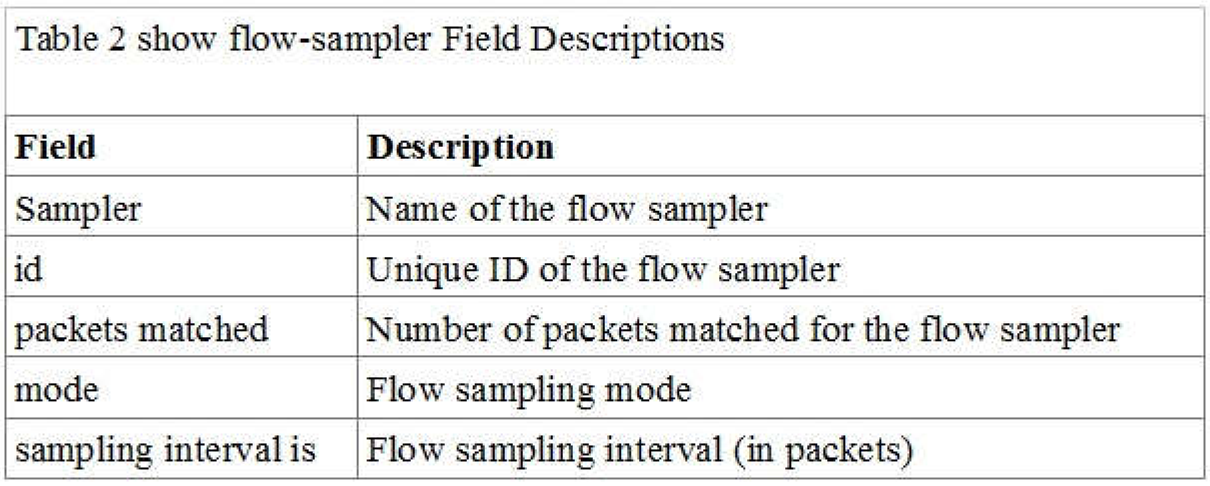


Table 2 show flow-sampler Field Descriptions

Field	Description
Sampler	Name of the flow sampler
id	Unique ID of the flow sampler
packets matched	Number of packets matched for the flow sampler
mode	Flow sampling mode
sampling interval is	Flow sampling interval (in packets)

References:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/xe-16-6/nf-xe-16-6-book/nflow-filt-samp-traff-xe.html

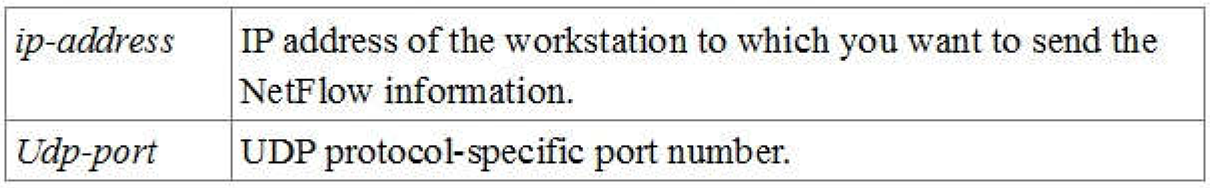
QUESTION 77
What is the result of the command ip flow-export destination 10.10.10.1 5858?

A. It configures the router to export cache flow information to IP 10.10.10.1 on port UDP/5858.

B. It configures the router to export cache flow information about flows with destination IP 10.10.10.1 and port UDP/5858.
C. It configures the router to receive cache flow information from IP 10.10.10.1 on port UDP/5858.
D. It configures the router to receive cache flow information about flows with destination IP 10.10.10.1 and port UDP/5858.

Correct Answer: A
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
To enable the exporting of information in NetFlow cache entries, use the **ip flow-export destination** command in global configuration mode.
Syntax Description



ip-address	IP address of the workstation to which you want to send the NetFlow information.
Udp-port	UDP protocol-specific port number.

Reference: http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html#wp1023091

QUESTION 78
Which type of traffic does DHCP snooping drop?

A. discover messages
B. DHCP messages where the source MAC and client MAC do not match
C. traffic from a trusted DHCP server to client
D. DHCP messages where the destination MAC and client MAC do not match

Correct Answer: B
Section: Infrastructure Services
Explanation

Explanation/Reference:
Explanation:
The switch validates DHCP packets received on the untrusted interfaces of VLANs with DHCP snooping enabled. The switch forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

1. The switch receives a packet (such as a DHCPOFFER, DHCPACK, DHCPNAK, or DHCPLEASEQUERY packet) from a DHCP server outside the network or firewall.
2. The switch receives a packet on an untrusted interface, and the source MAC address and the DHCP client hardware address do not match. This check is performed only if the DHCP snooping MAC address verification option is turned on.
3. The switch receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.
4. The switch receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0.
To support trusted edge switches that are connected to untrusted aggregation-switch ports, you can enable the DHCP option-82 on untrusted port feature, which enables untrusted aggregation-switch ports to accept DHCP packets that include option-82 information. Configure the port on the edge switch that connects to the aggregation switch as a trusted port.

Reference: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SX/configuration/guide/book/snoodhcp.html

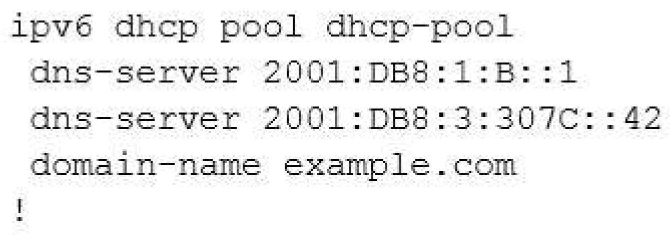
QUESTION 79
Which two commands would be used to troubleshoot high memory usage for a process? (Choose two.)

A. router#show memory allocating-process table
B. router#show memory summary
C. router#show memory dead
D. router#show memory events
E. router#show memory processor statistics

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 80
The following configuration is applied to a router at a branch site:



```
ipv6 dhcp pool dhcp-pool
 dns-server 2001:DB8:1:B::1
 dns-server 2001:DB8:3:307C::42
 domain-name example.com
!
```

If IPv6 is configured with default settings on all interfaces on the router, which two dynamic IPv6 addressing mechanisms could you use on end hosts to provide end-to-end connectivity? (Choose two.)

A. EUI-64
B. SLAAC
C. DHCPv6

D. BOOTP

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 81
The enterprise network WAN link has been receiving several denial of service attacks from both IPv4 and IPv6 sources. Which three elements can you use to identify an IPv6 packet via its header, in order to filter future attacks? (Choose three.)

A. Traffic Class
B. Source address
C. Flow Label
D. Hop Limit
E. Destination Address
F. Fragment Offset

Correct Answer: BCE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Because flows are identified by the 3-tuple of the Flow Label and the Source and Destination Addresses, the risk of theft or denial of service introduced by the Flow Label is related to the risk of theft or denial of service by address spoofing.

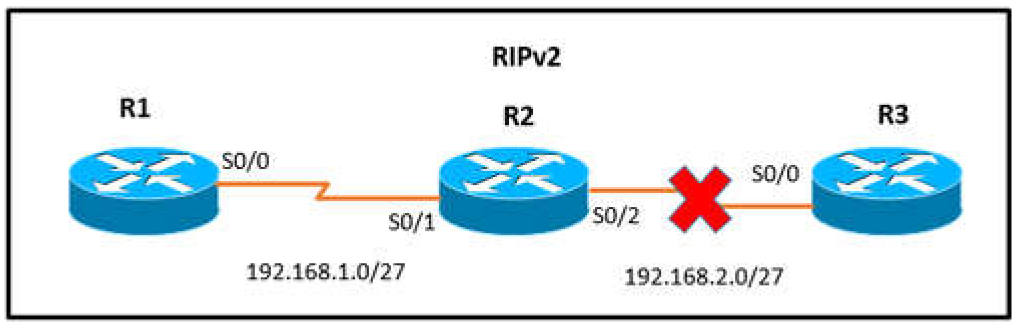
QUESTION 82
A network engineer has set up VRF-Lite on two routers where all the interfaces are in the same VRF. At a later time, a new loopback is added to Router 1, but it cannot ping any of the existing interfaces. Which two configurations enable the local or remote router to ping the loopback from any existing interface? (Choose two.)

A. adding a static route for the VRF that points to the global route table
B. adding the loopback to the VRF
C. adding dynamic routing between the two routers and advertising the loopback
D. adding the IP address of the loopback to the export route targets for the VRF
E. adding a static route for the VRF that points to the loopback interface
F. adding all interfaces to the global and VRF routing tables

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 83
Refer to the exhibit. The network setup is running the RIP routing protocol. Which two events will occur following link failure between R2 and R3? (Choose two.)



A. R2 will advertise network 192.168.2.0/27 with a hop count of 16 to R1.
B. R2 will not send any advertisements and will remove route 192.168.2.0/27 from its routing table.
C. R1 will reply to R2 with the advertisement for network 192.168.2.0/27 with a hop count of 16.
D. After communication fails and after the hold-down timer expires, R1 will remove the 192.168.2.0/27 route from its routing table.
E. R3 will not accept any further updates from R2, due to the split-horizon loop prevention mechanism.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 84
Which three benefits does the Cisco Easy Virtual Network provide to an enterprise network? (Choose three.)

A. simplified Layer 3 network virtualization
B. improved shared services support
C. enhanced management, troubleshooting, and usability
D. reduced configuration and deployment time for dot1q trunking
E. increased network performance and throughput
F. decreased BGP neighbor configurations

Correct Answer: ABC
Section: Mix Questions
Explanation

Explanation/Reference:

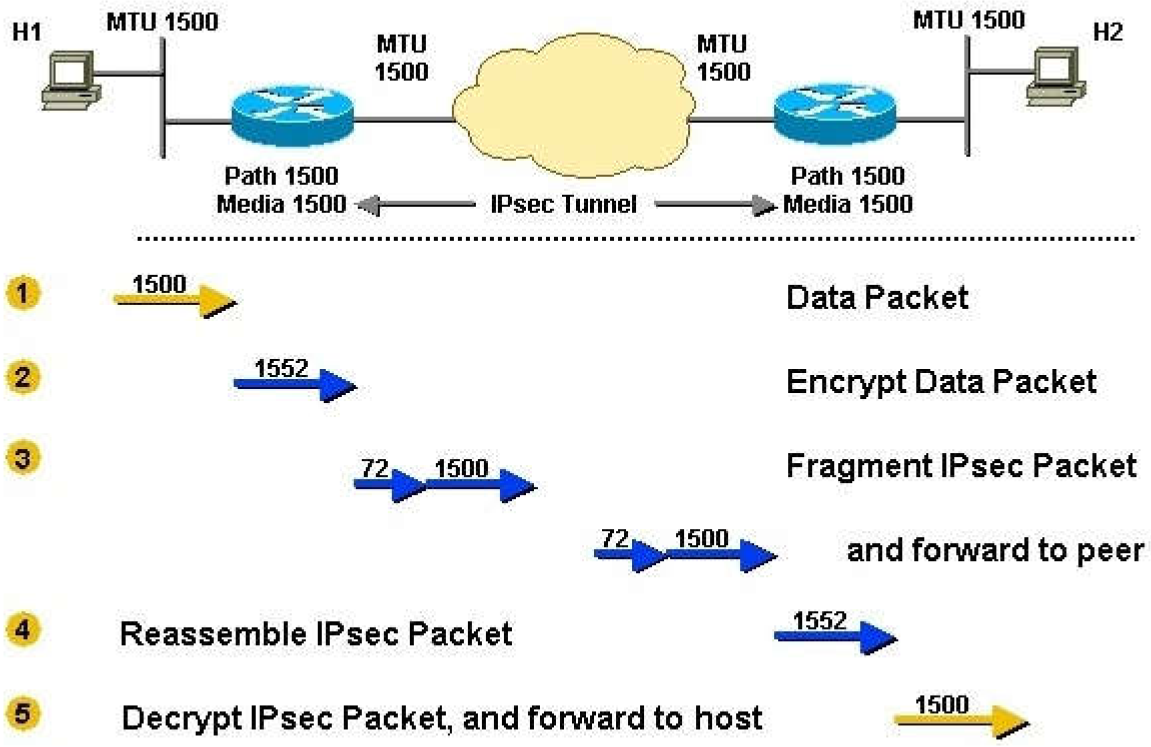
QUESTION 85
Which technology was originally developed for routers to handle fragmentation in the path between end points?

A. PMTUD
B. MSS
C. windowing
D. TCP
E. global synchronization

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Path **MTU D**iscovery (**PMTUD**) is a standardized technique in computer networking for determining the maximum transmission unit (MTU) size on the network path between two Internet Protocol (IP) hosts, usually with the goal of avoiding IP fragmentation. PMTUD was originally intended for routers in Internet Protocol Version 4 (IPv4).[1] However, all modern operating systems use it on endpoints. In IPv6, this function has been explicitly delegated to the end points of a communications session.[2]

PMTUD is standardized for IPv4 in RFC 1191 and for IPv6 in RFC 1981. RFC 4821 describes an extension to the techniques that works without support from Internet Control Message Protocol.



QUESTION 86
Which traffic characteristic is the reason that UDP traffic that carries voice and video is assigned to the queue only on a link that is at least 768 kbps?

A. typically is not fragmented
B. typically is fragmented
C. causes windowing
D. causes excessive delays for video traffic

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 87
A network administrator is troubleshooting a DMVPN setup between the hub and the spoke. Which action should the administrator take before troubleshooting the IPsec configuration?

A. Verify the GRE tunnels.
B. Verify ISAKMP.
C. Verify NHRP.
D. Verify crypto maps.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 88
To configure SNMPv3 implementation, a network engineer is using the AuthNoPriv security level. What effect does this action have on the SNMP messages?

A. They become unauthenticated and unencrypted.
B. They become authenticated and unencrypted.
C. They become authenticated and encrypted.
D. They become unauthenticated and encrypted.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

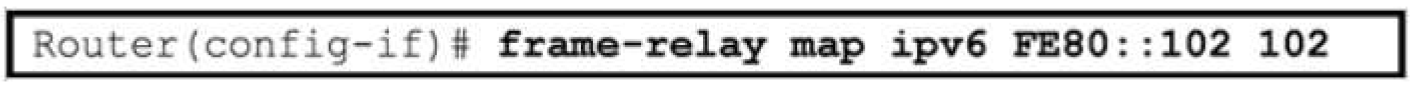
QUESTION 89
A network engineer is investigating the cause of a service disruption on a network segment and executes the debug condition interface fastethernet f0/0 command. In which situation is the debugging output generated?

A. when packets on the interface are received and the interface is operational
B. when packets on the interface are received and logging buffered is enabled
C. when packets on the interface are received and forwarded to a configured syslog server
D. when packets on the interface are received and the interface is shut down

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 90
Refer to the exhibit. The command is executed while configuring a point-to-multipoint Frame Relay interface. Which type of IPv6 address is portrayed in the exhibit?



```
Router(config-if)# frame-relay map ipv6 FE80::102 102
```

A. link-local
B. site-local
C. global
D. multicast

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 91
An engineer executes the ip flow ingress command in interface configuration mode. What is the result of this action?

A. It enables the collection of IP flow samples arriving to the interface.
B. It enables the collection of IP flow samples leaving the interface.
C. It enables IP flow while disabling IP CEF on the interface.
D. It enables IP flow collection on the physical interface and its subinterfaces.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 92
What is the primary service that is provided when you implement Cisco Easy Virtual Network?

A. It requires and enhances the use of VRF-Lite.
B. It reduces the need for common services separation.
C. It allows for traffic separation and improved network efficiency.
D. It introduces multi-VRF and label-prone network segmentation.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 93
How does an IOS router process a packet that should be switched by Cisco Express Forwarding without an FIB entry?

A. by forwarding the packet

B. by dropping the packet
C. by creating a new FIB entry for the packet
D. by looking in the routing table for an alternate FIB entry

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 94
Which statement about dual stack is true?

A. Dual stack translates IPv6 addresses to IPv4 addresses.
B. Dual stack means that devices are able to run IPv4 and IPv6 in parallel.
C. Dual stack translates IPv4 addresses to IPv6 addresses.
D. Dual stack changes the IP addresses on hosts from IPv4 to IPv6 automatically.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 95
Which PPP authentication method sends authentication information in cleartext?

A. MS CHAP
B. CDPCP
C. CHAP
D. PAP

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
PAP authentication involves a two-way handshake where the username and password are sent across the link in clear text; hence, PAP authentication does not provide any protection against playback and line sniffing.
CHAP authentication, on the other hand, periodically verifies the identity of the remote node using a three-way handshake. After the PPP link is established, the host sends a "challenge" message to the remote node. The remote node responds with a value calc"lated usi"g a one-way hash function. The host checks the response against its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise, the connection is terminated.

Reference:
http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/10241-ppp-callin-hostname.html

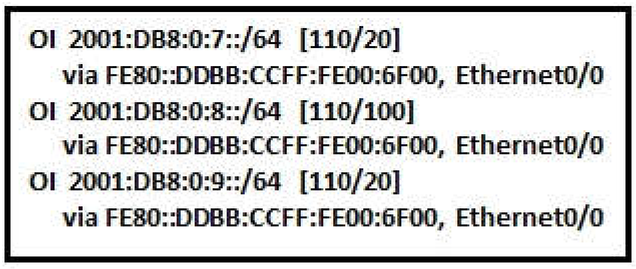
QUESTION 96
A router receives a routing advertisement for the same prefix and subnet from four different routing protocols. Which advertisement is installed in the routing table?

A. RIP
B. OSPF
C. iBGP
D. EIGRP

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 97
Refer to the exhibit. When summarizing these routes, which route is the summarized route?



```
OI 2001:DB8:0:7::/64  [110/20]
   via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0
OI 2001:DB8:0:8::/64  [110/100]
   via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0
OI 2001:DB8:0:9::/64  [110/20]
   via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0
```

A. OI 2001:DB8::/48 [110/100] via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0
B. OI 2001:DB8::/24 [110/100] via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0
C. OI 2001:DB8::/32 [110/100] via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0
D. OI 2001:DB8::/64 [110/100] via FE80::DDBB:CCFF:FE00:6F00, Ethernet0/0

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

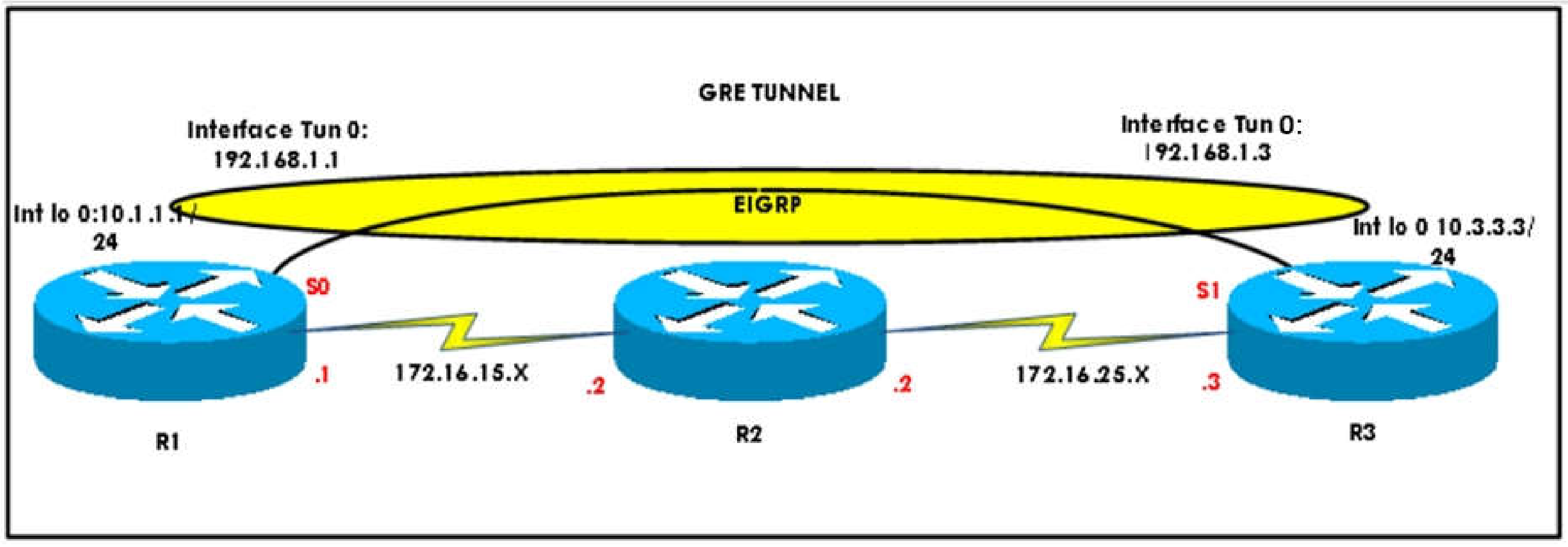
QUESTION 98
Which type of BGP AS number is 64591?

A. a private AS number
B. a public AS number
C. a private 4-byte AS number
D. a public 4-byte AS number

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 99
Refer to the exhibit. After configuring GRE between two routers running EIGRP that are connected to each other via a WAN link, a network engineer notices that the two routers cannot establish the GRE tunnel to begin the exchange of routing updates. What is the reason for this?



A. Either a firewall between the two routers or an ACL on the router is blocking IP protocol number 47.
B. Either a firewall between the two routers or an ACL on the router is blocking UDP 57.
C. Either a firewall between the two routers or an ACL on the router is blocking TCP 47.
D. Either a firewall between the two routers or an ACL on the router is blocking IP protocol number 57.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 100
Which Cisco VPN technology can use multipoint tunnel, resulting in a single GRE tunnel interface on the hub, to support multiple connections from multiple spoke devices?

A. DMVPN
B. GETVPN
C. Cisco Easy VPN
D. FlexVPN

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 101
Which Cisco VPN technology uses AAA to implement group policies and authorization and is also used for the XAUTH authentication method?

A. DMVPN
B. Cisco Easy VPN
C. GETVPN
D. GREVPN

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 102

Which parameter in an SNMPv3 configuration offers authentication and encryption?

A. auth
B. noauth
C. priv
D. secret

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 103
Refer to the following configuration command.

router (config-line)# ntp master 10

Which statement about this command is true?

A. The router acts as an authoritative NTP clock and allows only 10 NTP client connections.
B. The router acts as an authoritative NTP clock at stratum 10.
C. The router acts as an authoritative NTP clock with a priority number of 10.
D. The router acts as an authoritative NTP clock for 10 minutes only.

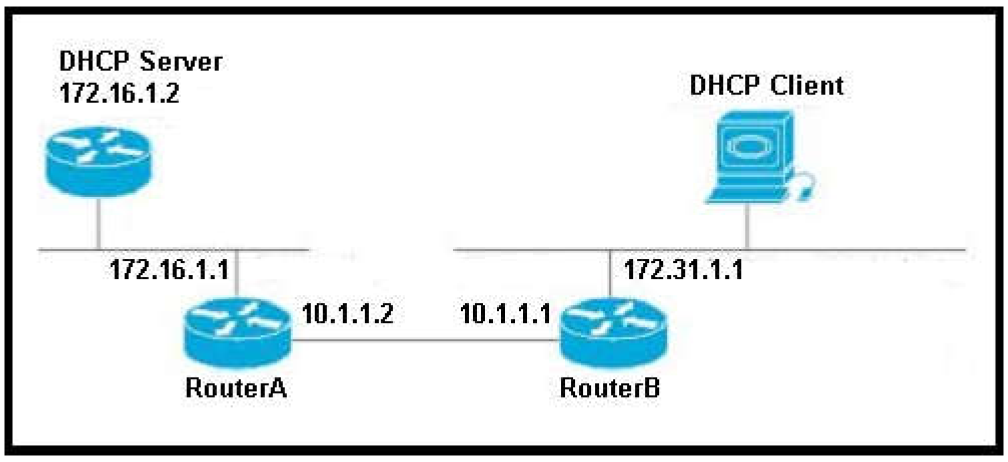
Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 104
Refer to the exhibit. The DHCP client is unable to receive a DHCP address from the DHCP server. Consider the following output:

```
hostname RouterB
!
interface fastethernet 0/0
 ip address 172.31.1.1 255.255.255.0
interface serial 0/0
 ip address 10.1.1.1 255.255.255.252
!
ip route 172.16.1.0 255.255.255.0 10.1.1.2
```

Which configuration is required on the Router B fastEthernet 0/0 port in order to allow the DHCP client to successfully receive an IP address from the DHCP server?



A. RouterB(config-if)# ip helper-address 172.16.1.2
B. RouterB(config-if)# ip helper-address 172.16.1.1
C. RouterB(config-if)# ip helper-address 172.31.1.1
D. RouterB(config-if)# ip helper-address 255.255.255.255

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 105
Which statement about the NPTv6 protocol is true?

A. It is used to translate IPv4 prefixes to IPv6 prefixes.
B. It is used to translate an IPv6 address prefix to another IPv6 prefix.
C. It is used to translate IPv6 prefixes to IPv4 subnets with appropriate masks.
D. It is used to translate IPv4 addresses to IPv6 link-local addresses.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
NPT stands for Network Prefix Translation.

IPv6-to-IPv6 Network Prefix Translation (NPTv6) performs a stateless, static translation of one IPv6 prefix to another IPv6 prefix thereby allowing private Unique Local Addresses (ULA) to be able to access the Internet, by translating it to Global Routable Addresses

NPTv6 does not do a port translation, hence, the ports remain the same for incoming and outgoing packets.

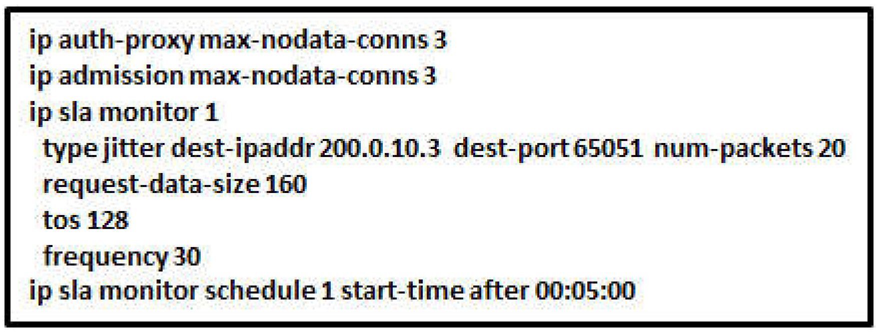
QUESTION 106
Two aspects of an IP SLA operation can be tracked: state and reachability. Which statement about state tracking is true?

A. When tracking state, an OK return code means that the track's state is up; any other return code means that the track's state is down.
B. When tracking state, an OK or over threshold return code means that the track's state is up; any other return code means that the track's state is down.
C. When tracking state, an OK return code means that the track's state is down; any other return code means that the track's state is up.
D. When tracking state, an OK or over threshold return code means that the track's state is down; any other return code means that the track's state is up.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 107
Refer to the exhibit. Which statement about the configuration is true?



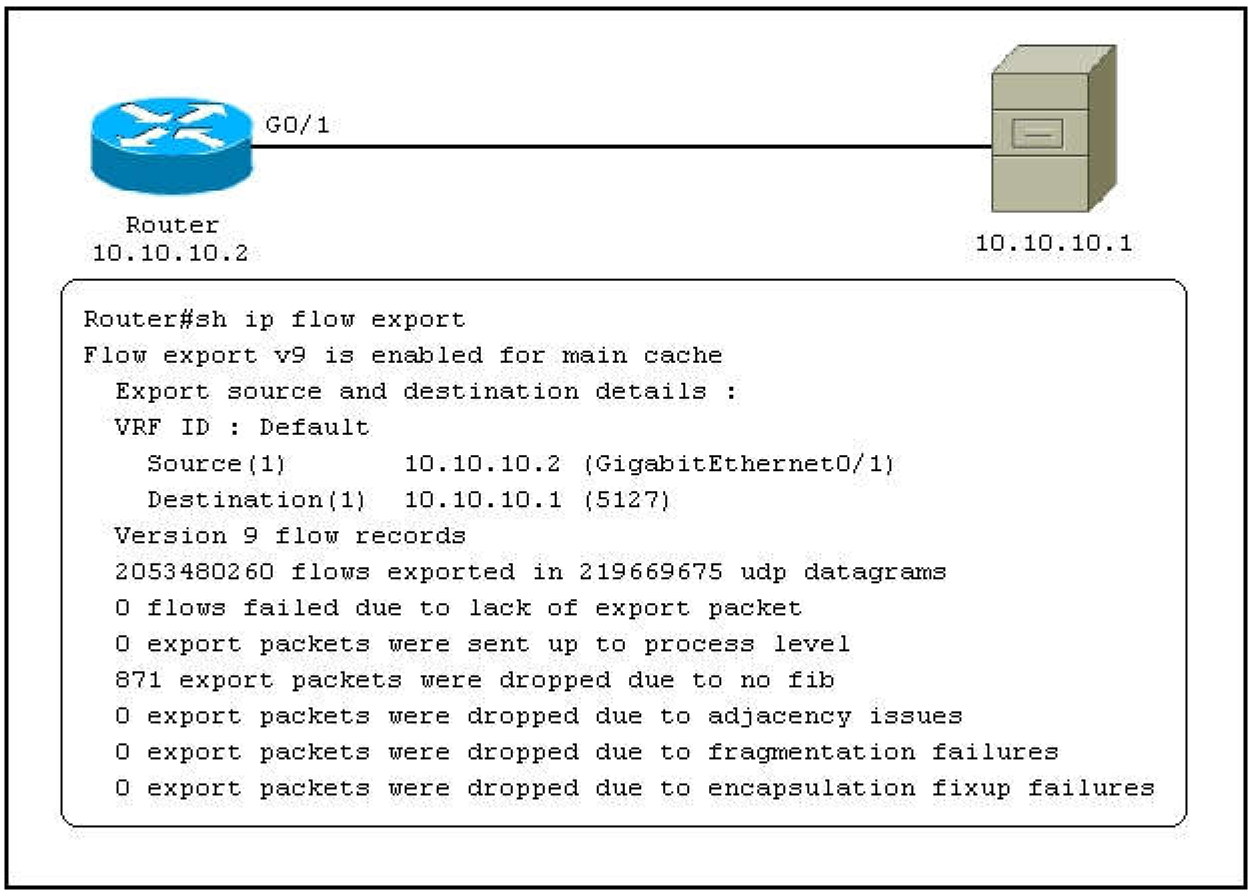
```
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip sla monitor 1
 type jitter dest-ipaddr 200.0.10.3  dest-port 65051  num-packets 20
 request-data-size 160
 tos 128
 frequency 30
ip sla monitor schedule 1 start-time after 00:05:00
```

A. 20 packets are being sent every 30 seconds.
B. The monitor starts at 12:05:00 a.m.
C. Jitter is being tested with TCP packets to port 65051.
D. The packets that are being sent use DSCP EF.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 108
Refer to the exhibit. Which statement about the command output is true?



```
Router#sh ip flow export
Flow export v9 is enabled for main cache
  Export source and destination details :
  VRF ID : Default
    Source(1)       10.10.10.2 (GigabitEthernet0/1)
    Destination(1)  10.10.10.1 (5127)
  Version 9 flow records
  2053480260 flows exported in 219669675 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  871 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

A. The router exports flow information to 10.10.10.1 on UDP port 5127.
B. The router receives flow information from 10.10.10.2 on UDP port 5127.
C. The router exports flow information to 10.10.10.1 on TCP port 5127.
D. The router receives flow information from 10.10.10.2 on TCP port 5127.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 109
A network engineer is trying to modify an existing active NAT configuration on an IOS router by using the following command:

(config)# no ip nat pool dynamic-nat-pool 192.1.1.20 192.1.1.254 netmask 255.255.255.0

Upon entering the command on the IOS router, the following message is seen on the console:

%Dynamic Mapping in Use, Cannot remove message or the %Pool outpool in use, cannot destroy

What is the least impactful method that the engineer can use to modify the existing IP NAT configuration?

A. Clear the IP NAT translations using the clear ip nat traffic * " command, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.
B. Clear the IP NAT translations using the clear ip nat translation * " command, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.
C. Clear the IP NAT translations using the reload command on the router, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.
D. Clear the IP NAT translations using the clear ip nat table * " command, then replace the NAT configuration quickly, before any new NAT entries are populated into the translation table due to active NAT traffic.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 110
Which IPv6 address type is seen as the next-hop address in the output of the show ipv6 rip RIPng database command?

A. link-local
B. global
C. site-local
D. anycast
E. multicast

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 111
Which three items can you track when you use two time stamps with IP SLAs? (Choose three.)

A. delay
B. jitter
C. packet loss
D. load
E. throughput
F. path

Correct Answer: ABC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 112
If the total bandwidth is 64 kbps and the RTT is 3 seconds, what is the bandwidth delay product?

A. 8,000 bytes
B. 16,000 bytes
C. 24,000 bytes
D. 32,000 bytes
E. 62,000 bytes

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Bandwidth delay product is defined as capacity of a pipe = bandwidth (bits/ sec) * RTT (s) where capacity is specific to TCP and is a bi-product of how the protocol itself operates.

64 kbps = 64.000bps
1byte=8bit

64.000/8=8.000*3=24.000
Reference:
https://supportforums.cisco.com/t5/wan-routing-and-switching/tcp-performance-bandwidth-delay-product/td-p/765376

QUESTION 113
What are the default timers for RIPng?

A. Update: 30 seconds Expire: 180 seconds Flush: 240 seconds
B. Update: 20 seconds Expire: 120 seconds Flush: 160 seconds
C. Update: 10 seconds Expire: 60 seconds Flush: 80 seconds
D. Update: 5 seconds Expire: 30 seconds Flush: 40 seconds

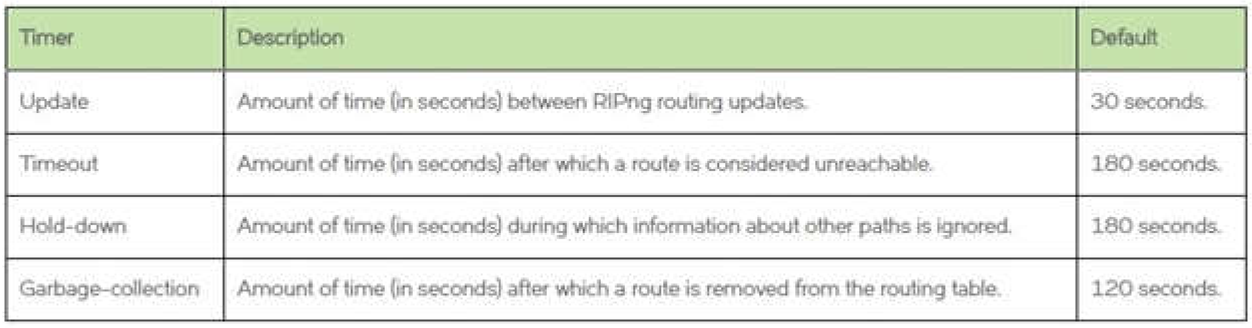
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Update Timer
The update timer controls the interval between two gratuitous Response Messages. By default the value is **30** seconds. The response message is broadcast to all its RIP enabled interface.[8]

Invalid Timer
The invalid timer specifies how long a routing entry can be in the routing table without being updated. This is also called as expiration Timer. By default, the value is **180** seconds. After the timer expires the hop count of the routing entry will be set to 16, marking the destination as unreachable.

Flush Timer
The flush timer controls the time between the route is invalidated or marked as unreachable and removal of entry from the routing table. By default the value is **240** seconds. This is 60 seconds longer than Invalid timer. So for 60 seconds the router will be advertising about this unreachable route to all its neighbours. This timer must be set to a higher value than the invalid timer.[8]

Hold-down Timer
The hold-down timer is started per route entry, when the hop count is changing from lower value to higher value. This allows the route to get stabilized. During this time no update can be done to that routing entry. This is not part of the RFC 1058. This is Cisco's implementation. The default value of this timer is **180** seconds.



Timer	Description	Default
Update	Amount of time (in seconds) between RIPng routing updates.	30 seconds.
Timeout	Amount of time (in seconds) after which a route is considered unreachable.	180 seconds.
Hold-down	Amount of time (in seconds) during which information about other paths is ignored.	180 seconds.
Garbage-collection	Amount of time (in seconds) after which a route is removed from the routing table.	120 seconds.

Reference:
http://www.brocade.com/content/html/en/configuration-guide/fastiron-08030b-l3guide/GUID-97023AC1-C034-40EA-B02D-1E3E9DACCAC7.html

QUESTION 114
What is the purpose of the route-target command?

A. It extends the IP address to identify which VRF instance it belongs to.
B. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities.
C. It manages the import and export of routes between two or more VRF instances.
D. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 115
A network engineer has configured a tracking object to monitor the reachability of IP SLA 1. In order to update the next hop for the interesting traffic, which feature must be used in conjunction with the newly created tracking object to manipulate the traffic flow as required?

A. SNMP
B. PBR
C. IP SLA
D. SAA
E. ACLs
F. IGP

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 116
A route map uses an ACL, if the required matching is based on which criteria?

A. addressing information
B. route types
C. AS paths
D. metrics

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 117
Various employees in the same department report to the network engineer about slowness in the network connectivity to the Internet. They are also having latency issues communicating to the network drives of various departments. Upon monitoring, the engineer finds traffic flood in the network. Which option is the problem?

A. network outage
B. network switching loop
C. router configuration issue
D. wrong proxy configured

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 118
Which type of handshake does CHAP authentication use to establish a PPP link?

A. one-way
B. two-way
C. three-way
D. four-way

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 119
Which two authentication protocols does PPP support? (Choose two.)

A. WAP
B. PAP
C. CHAP
D. EAP
E. RADIUS

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 120
Which statement is a restriction for PPPoE configuration?

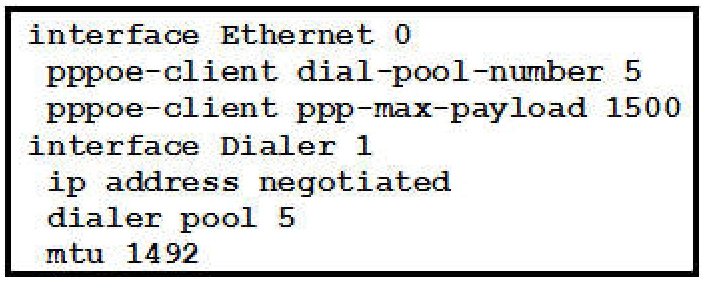
A. Multiple PPPoE clients can use the same dialer interface.
B. Multiple PPPoE clients can use the same dialer pool.
C. A PPPoE session can be initiated only by the client.
D. A PPPoE session can be initiated only by the access concentrator.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Restrictions for PPPoE on Ethernet

The following restrictions apply when the PPPoE on Ethernet feature is used:
• PPPoE is not supported on Frame Relay.
• PPPoE is not supported on any other LAN interfaces such as FDDI and Token Ring.
• Fast switching is supported. PPP over Ethernet over RFC 1483 fibswitching is supported for IP. All other protocols are switched over process switching.

QUESTION 121
Refer to the exhibit.



```
interface Ethernet 0
 pppoe-client dial-pool-number 5
 pppoe-client ppp-max-payload 1500
interface Dialer 1
 ip address negotiated
 dialer pool 5
 mtu 1492
```

Which statement about the configuration is true?

A. This configuration is incorrect because the MTU must match the ppp-max-payload that is defined.
B. This configuration is incorrect because the dialer interface number must be the same as the dialer pool number.
C. This configuration is missing an IP address on the dialer interface.
D. This configuration represents a complete PPPoE client configuration on an Ethernet connection.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 122
A company has their headquarters located in a large city with a T3 frame relay link that connects 30 remote locations that each have T1 frame relay connections. Which technology must be configured to prevent remote sites from getting overwhelmed with traffic and prevent packet drops from the headquarters?

A. traffic shaping
B. IPsec VPN
C. GRE VPN
D. MPLS

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 123
On which two types of interface is Frame Relay switching supported? (Choose two.)

A. serial interfaces
B. Ethernet interfaces
C. fiber interfaces
D. ISDN interfaces
E. auxiliary interfaces

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

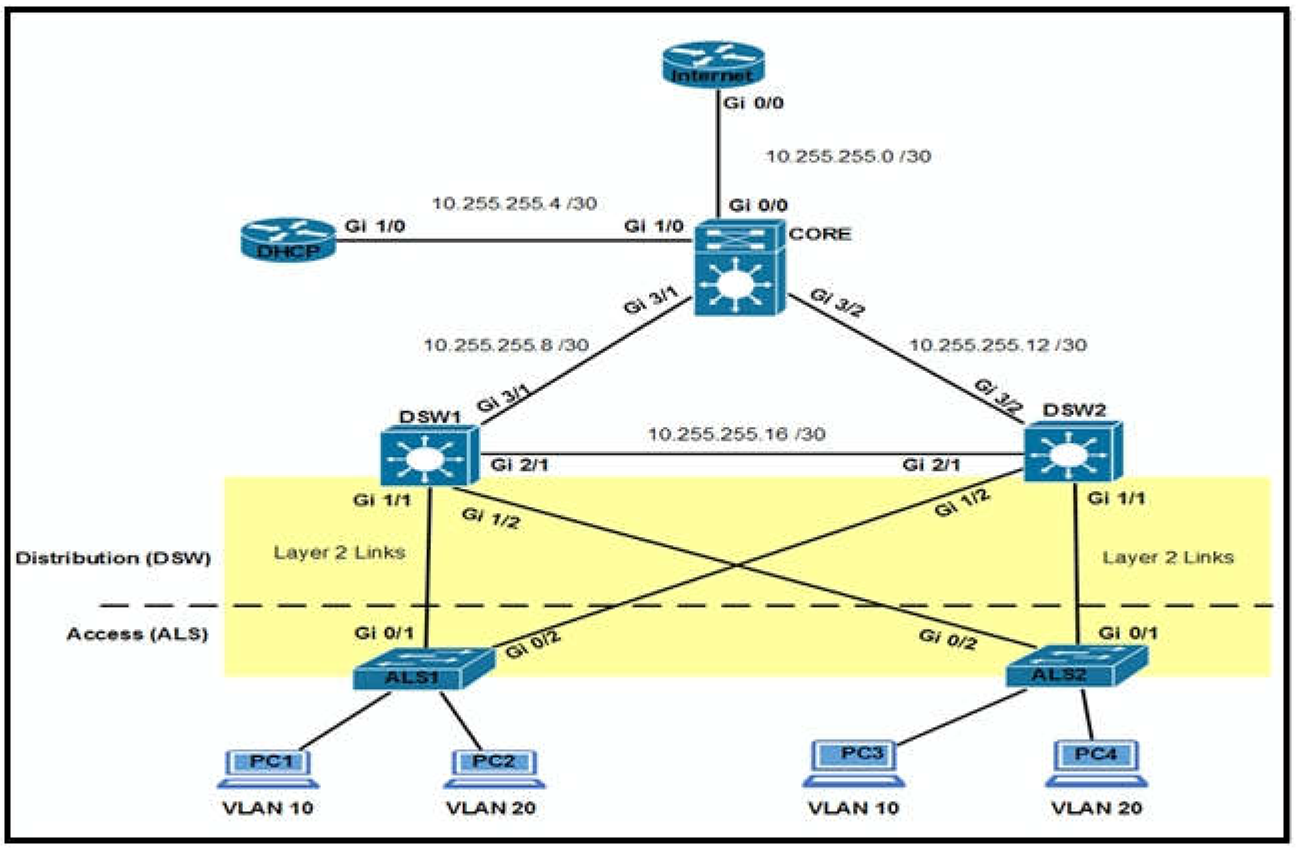
QUESTION 124
In IPv6, SLAAC provides the ability to address a host based on a network prefix that is advertised from a local network router. How is the prefix advertised?

A. routing table
B. router advertisements
C. routing protocol
D. routing type

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 125
Refer to the exhibit.



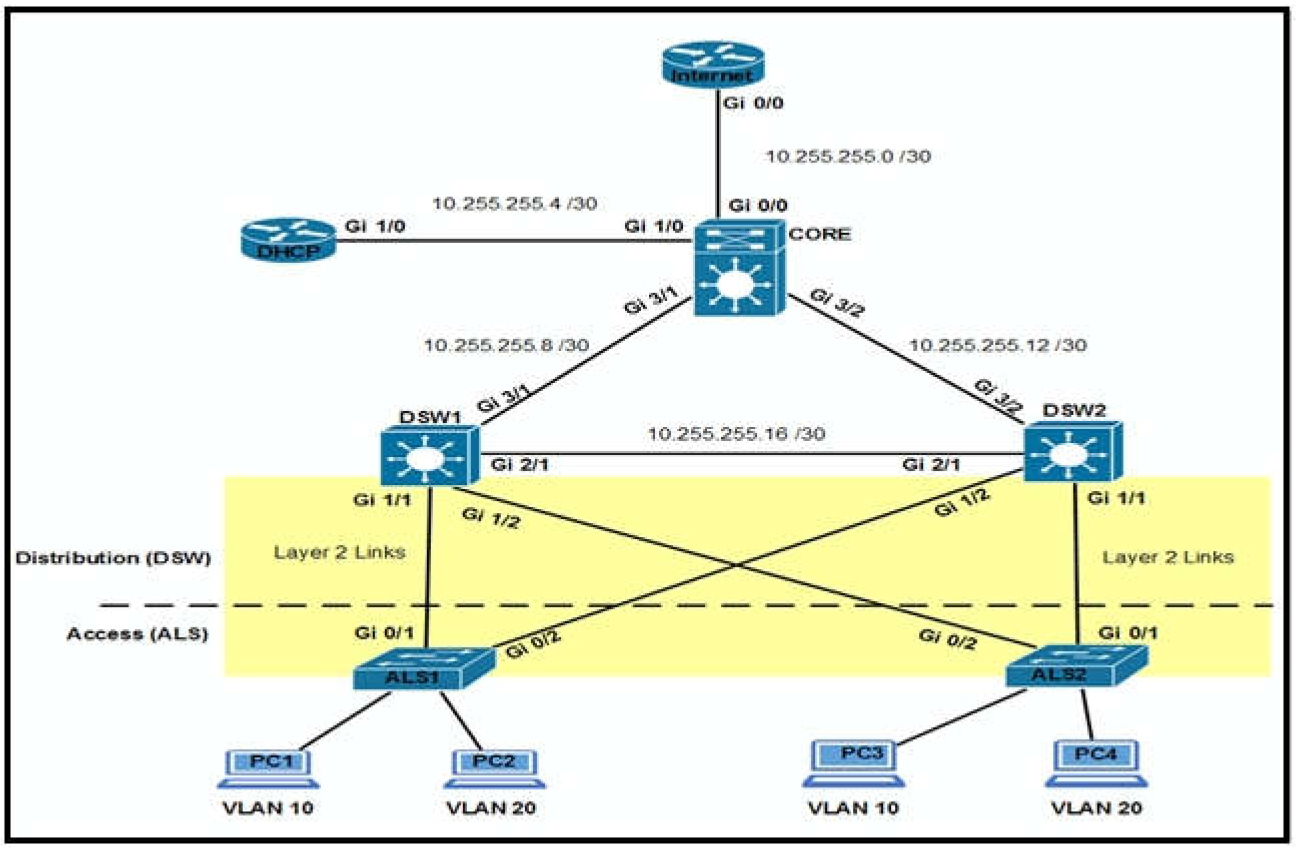
Which option prevents routing updates from being sent to the access layer switches?

A. DWS1(config-router)# passive-interface default DWS2(config-router)# passive-interface default
B. ALS1(config-router)# passive-interface default ALS2(config-router)# passive-interface default
C. DWS1(config-router)# passive-interface gi1/1 DWS1(config-router)# passive-interface gi1/2 DWS2(config-router)# passive-interface gi1/1 DWS2(config-router)# passive-interface gi1/2
D. ALS1(config-router)# passive-interface gi0/1 ALS1(config-router)# passive-interface gi0/2 ALS2(config-router)# passive-interface gi0/1 ALS2(config-router)# passive-interface gi0/2

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 126
Refer to the exhibit.



Which option prevents routing updates from being sent to the DHCP router, while still allowing routing update messages to flow to the Internet router and the distribution switches?

A. DHCP(config-router)# passive-interface default DHCP(config-router)# no passive-interface Gi1/0 Internet(config-router)# passive-interface Gi0/1 Internet (config-router)# passive-interface Gi0/2
B. Core(config-router)# passive-interface Gi0/0 Core(config-router)# passive-interface Gi3/1 Core(config-router)# passive-interface Gi3/2 DHCP(config-router)# no passive-interface Gi1/0
C. Core(config-router)# passive-interface default Core(config-router)# no passive-interface Gi0/0 Core(config-router)# no passive-interface Gi3/1 Core (config-router)# no passive-interface Gi3/2
D. Internet(config-router)# passive-interface default Core(config-router)# passive-interface default DSW1(config-router)# passive-interface default DSW2 (config-router)# passive-interface default

Correct Answer: C

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 127
A network engineer is considering enabling load balancing with EIGRP. Which consideration should be analyzed?

A. EIGRP allows a maximum of four paths across for load balancing traffic.
B. By default, EIGRP uses a default variance of 2 for load balancing.
C. EIGRP unequal path load balancing can result in routing loops.
D. By default, EIGRP performs equal cost load balancing at least across four equal cost paths.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 128
The OSPF database of a router shows LSA types 1, 2, 3, and 7 only. Which type of area is this router connected to?

A. stub area
B. totally stubby area
C. backbone area
D. not-so-stubby area

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 129
An engineer is configuring a GRE tunnel interface in the default mode. The engineer has assigned an IPv4 address on the tunnel and sourced the tunnel from an Ethernet interface. Which option also is required on the tunnel interface before it is operational?

A. tunnel destination address
B. keepalives
C. IPv6 address
D. tunnel protection

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 130
Which protocol is used in a DMVPN network to map physical IP addresses to logical IP addresses?

A. BGP
B. LLDP
C. EIGRP
D. NHRP

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 131
Which two routing protocols are supported by Easy Virtual Network? (Choose two.)

A. RIPv2
B. OSPFv2
C. BGP
D. EIGRP
E. IS-IS

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 132
Which statement is true?

A. RADIUS uses TCP, and TACACS+ uses UDP.
B. RADIUS encrypts the entire body of the packet.
C. TACACS+ encrypts only the password portion of a packet.
D. TACACS+ separates authentication and authorization.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 133
Which two statements about AAA implementation in a Cisco router are true? (Choose two.)

A. RADIUS is more flexible than TACACS+ in router management.
B. RADIUS and TACACS+ allow accounting of commands.
C. RADIUS and TACACS+ encrypt the entire body of the packet.
D. RADIUS and TACACS+ are client/server AAA protocols.
E. Neither RADIUS nor TACACS+ allow for accounting of commands.

Correct Answer: BD
Section: Mix Questions
Explanation

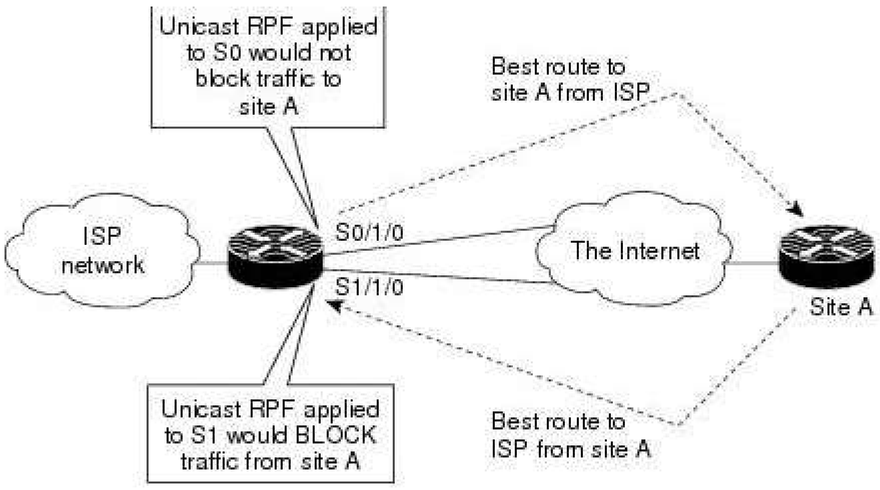
Explanation/Reference:

QUESTION 134
Which option is invalid when configuring Unicast Reverse Path Forwarding?

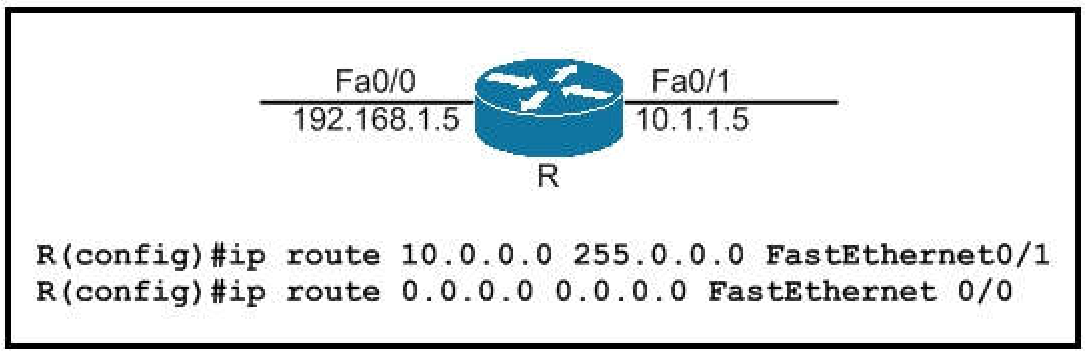
A. allow self ping to router
B. allow default route
C. allow based on ACL match
D. source reachable via both

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:


Unicast RPF applied to S0 would not block traffic to site A
Best route to site A from ISP
ISP network
S0/1/0
The Internet
S1/1/0
Site A
Unicast RPF applied to S1 would BLOCK traffic from site A
Best route to ISP from site A

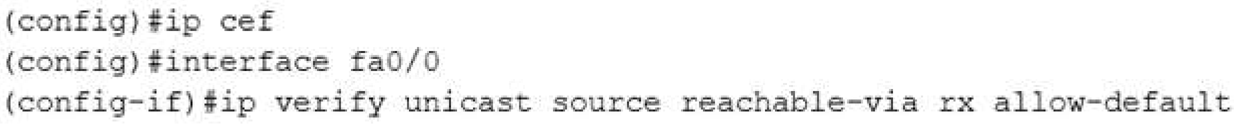
QUESTION 135
Refer to the exhibit.



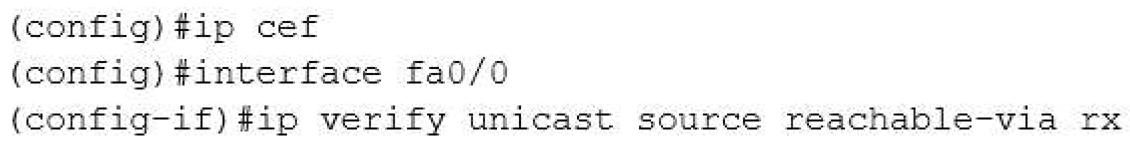
```
R(config)#ip route 10.0.0.0 255.0.0.0 FastEthernet0/1
R(config)#ip route 0.0.0.0 0.0.0.0 FastEthernet 0/0
```

Which option represents the minimal configuration that allows inbound traffic from the 172.16.1.0/24 network to successfully enter router R, while also limiting spoofed 10.0.0.0/8 hosts that could enter router R?

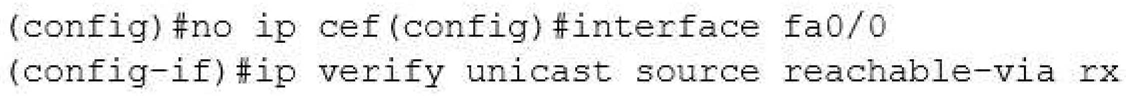
A.



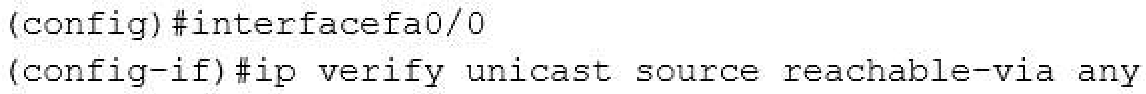
```
(config)#ip cef
(config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via rx allow-default
```

B. 

```
(config)#ip cef
(config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via rx
```

C. 

```
(config)#no ip cef(config)#interface fa0/0
(config-if)#ip verify unicast source reachable-via rx
```

D. 

```
(config)#interfacefa0/0
(config-if)#ip verify unicast source reachable-via any
```

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 136
Which outbound access list, applied to the WAN interface of a router, permits all traffic except for http traffic sourced from the workstation with IP address 10.10.10.1?

A. ip access-list extended 200
deny tcp host 10.10.10.1 eq 80 any
permit ip any any
B. ip access-list extended 10
deny tcp host 10.10.10.1 any eq 80
permit ip any any
C. ip access-list extended NO_HTTP
deny tcp host 10.10.10.1 any eq 80
D. ip access-list extended 100
deny tcp host 10.10.10.1 any eq 80
permit ip any any

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

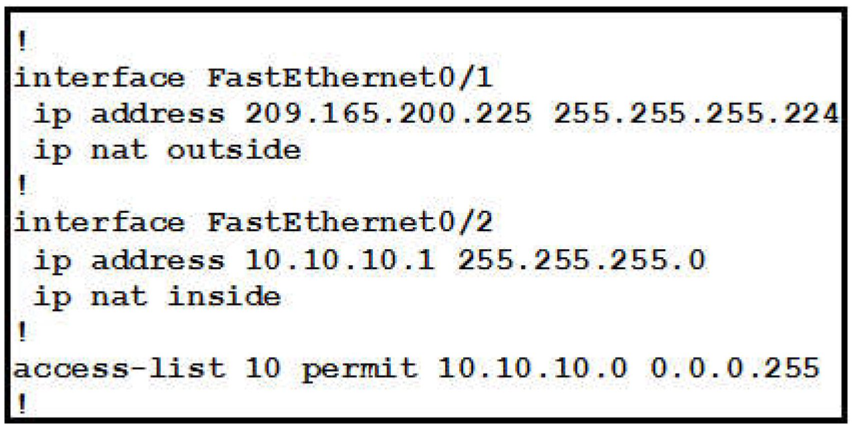
QUESTION 137
Which two statements indicate a valid association mode for NTP synchronization? (Choose two.)

A. The client polls NTP servers for time.
B. The client broadcasts NTP requests.
C. The client listens to NTP broadcasts.
D. The client creates a VPN tunnel to an NTP server.
E. The client multicasts NTP requests.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 138
Refer to the exhibit.



```
!
interface FastEthernet0/1
 ip address 209.165.200.225 255.255.255.224
 ip nat outside
!
interface FastEthernet0/2
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
!
access-list 10 permit 10.10.10.0 0.0.0.255
!
```

Which command allows hosts that are connected to FastEthernet0/2 to access the Internet?

A. ip nat inside source list 10 interface FastEthernet0/1 overload
B. ip nat outside source static 209.165.200.225 10.10.10.0 overload
C. ip nat inside source list 10 interface FastEthernet0/2 overload
D. ip nat outside source list 10 interface FastEthernet0/2 overload

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 139
Which statement describes what this command accomplishes when inside and outside interfaces are correctly identified for NAT?

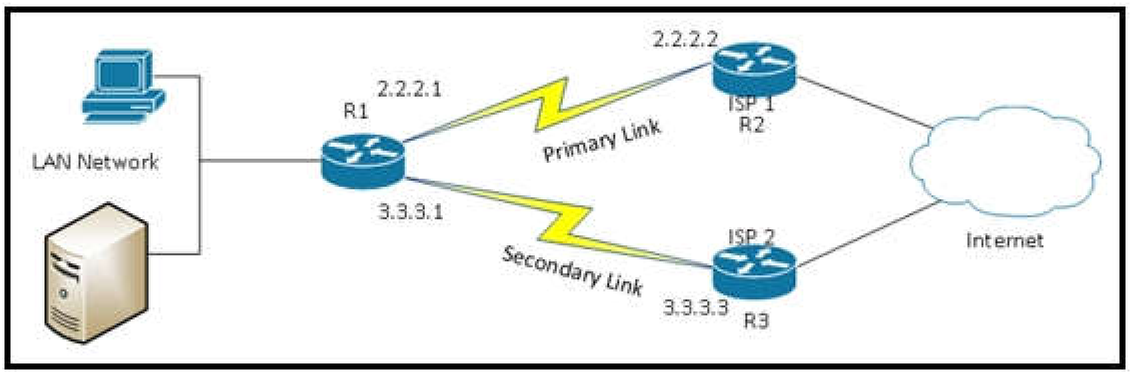
ip nat inside source static tcp 192.168.1.50 80 209.165.201.1 8080 extendable

A. It allows host 192.168.1.50 to access external websites using TCP port 8080.
B. It allows external clients coming from public IP 209.165.201.1 to connect to a web server at 192.168.1.50.
C. It allows external clients to connect to a web server hosted on 192.168.1.50.
D. It represents an incorrect NAT configuration because it uses standard TCP ports.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 140
Refer to the exhibit.



Which technology can be employed to automatically detect a WAN primary link failure and failover to the secondary link?

A. HSRP
B. VRRP
C. IP SLA
D. multicast

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 141
In which two ways can NetFlow data be viewed? (Choose two.)

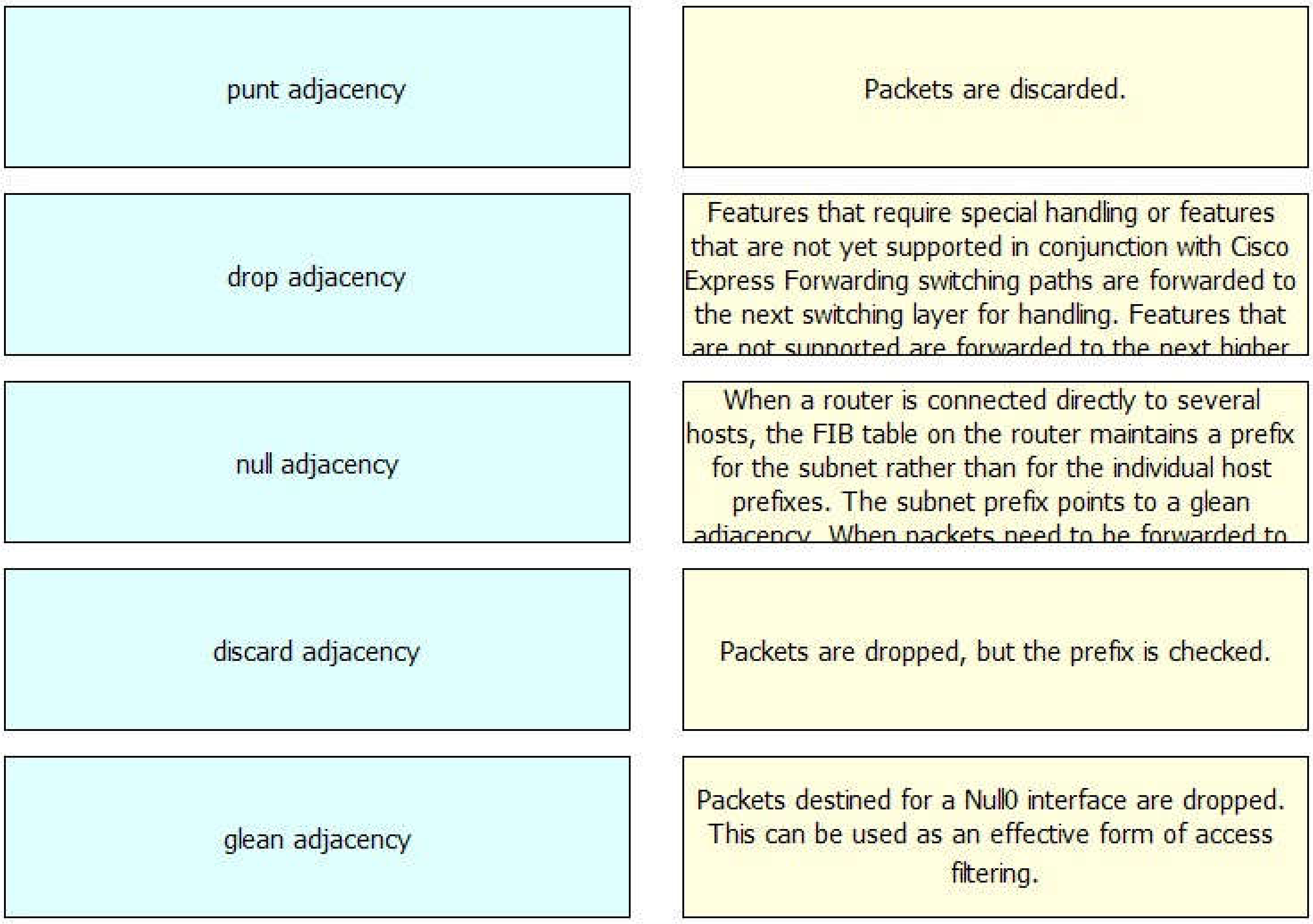
A. CLI
B. NetFlow
C. built-in GUI
D. syslog server interface
E. web interface

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

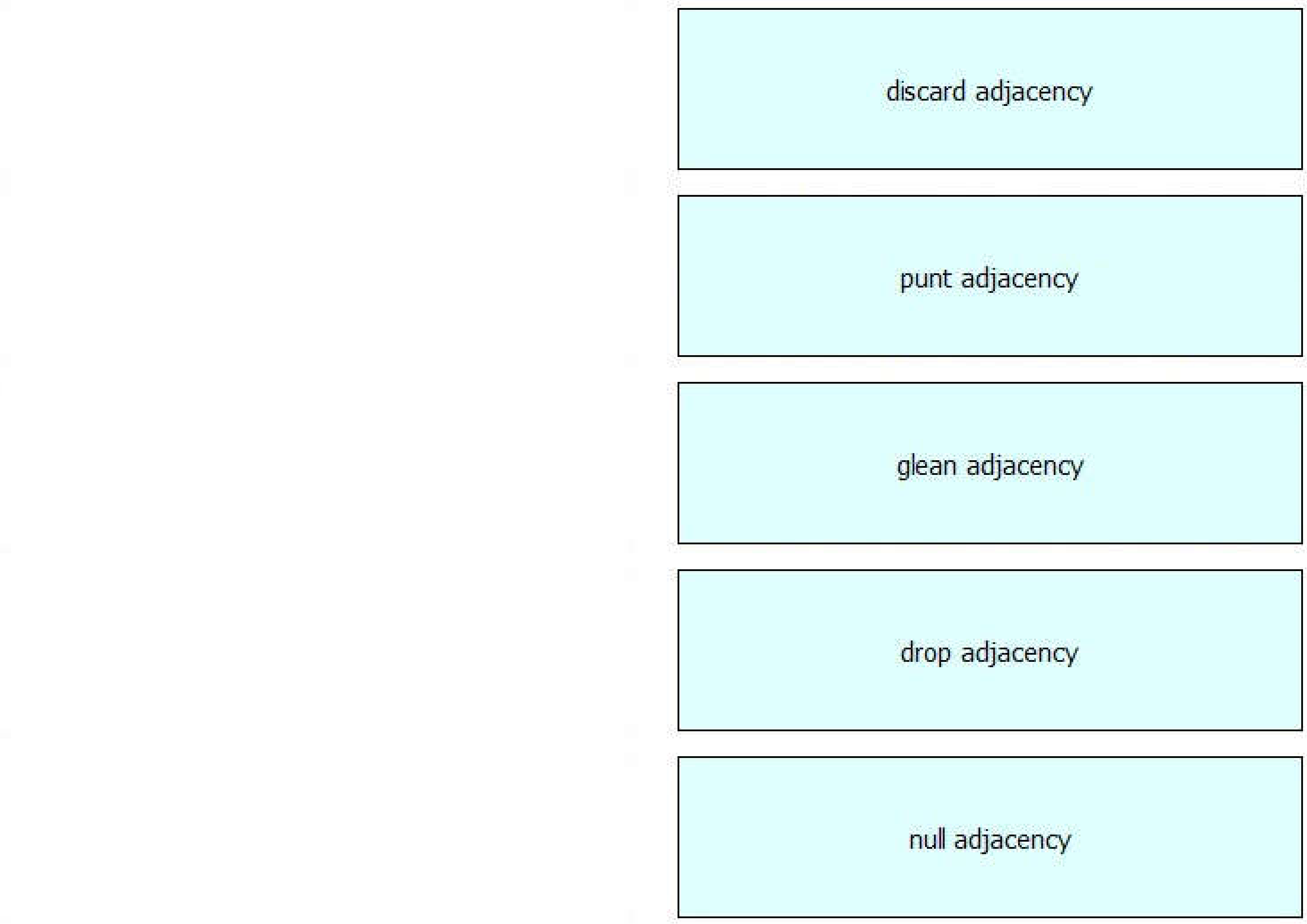
QUESTION 142
DRAG DROP
Drag and drop the Cisco Express Forwarding adjacency types from the left to the correct type of processing on the right.

Select and Place:



punt adjacency	Packets are discarded.
drop adjacency	Features that require special handling or features that are not yet supported in conjunction with Cisco Express Forwarding switching paths are forwarded to the next switching layer for handling. Features that are not supported are forwarded to the next higher
null adjacency	When a router is connected directly to several hosts, the FIB table on the router maintains a prefix for the subnet rather than for the individual host prefixes. The subnet prefix points to a glean adjacency. When packets need to be forwarded to
discard adjacency	Packets are dropped, but the prefix is checked.
glean adjacency	Packets destined for a Null0 interface are dropped. This can be used as an effective form of access filtering.

Correct Answer:



discard adjacency

punt adjacency

glean adjacency

drop adjacency

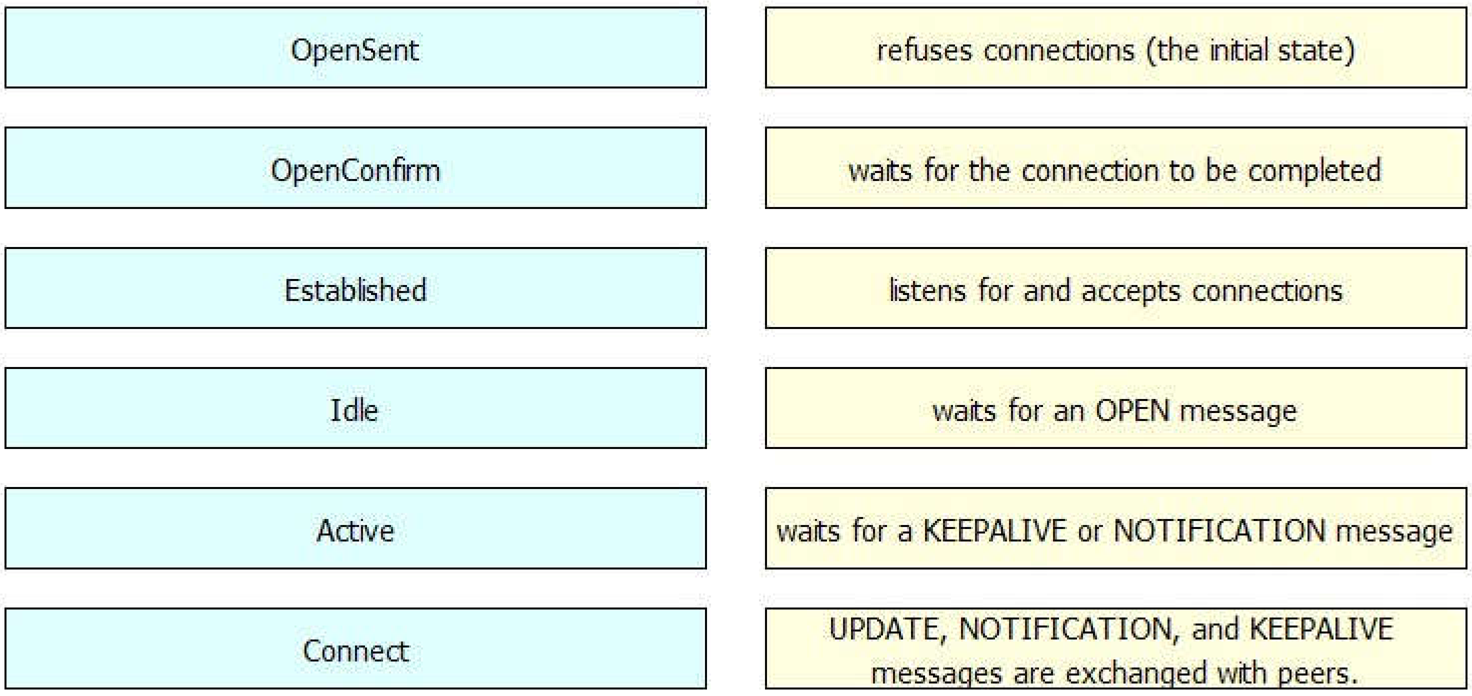
null adjacency

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 143
DRAG DROP
Drag and drop the BGP states from the left to the matching definitions on the right.

Select and Place:



OpenSent

OpenConfirm

Established

Idle

Active

Connect

refuses connections (the initial state)

waits for the connection to be completed

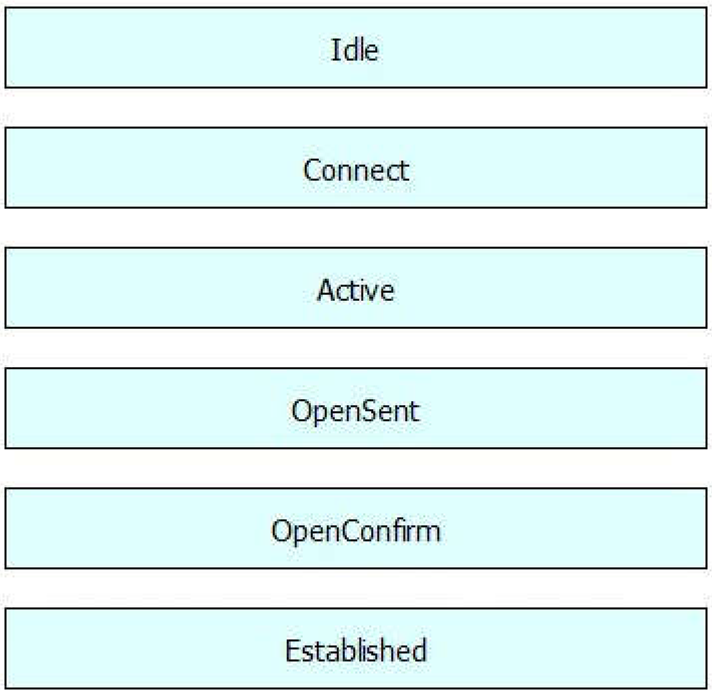
listens for and accepts connections

waits for an OPEN message

waits for a KEEPALIVE or NOTIFICATION message

UPDATE, NOTIFICATION, and KEEPALIVE messages are exchanged with peers.

Correct Answer:



Idle

Connect

Active

OpenSent

OpenConfirm

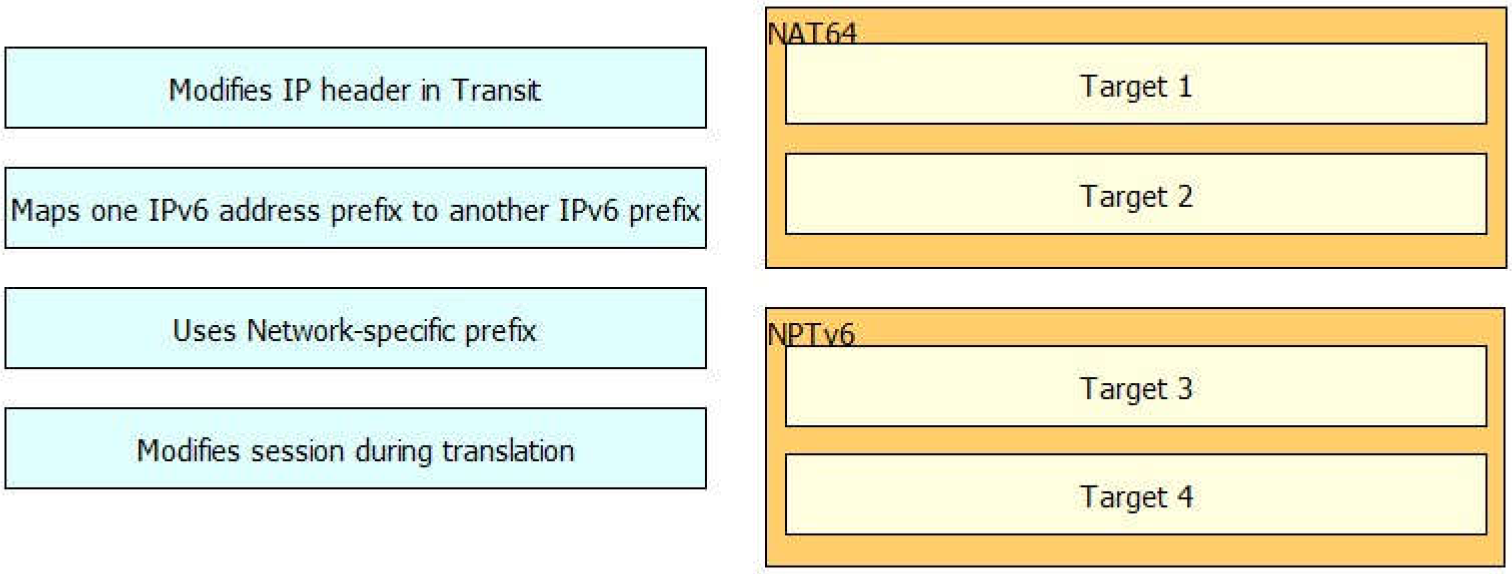
Established

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 144
DRAG DROP
Drag and drop the IPv6 NAT characteristic from the left to the matching IPv6 NAT category on the right.

Select and Place:



Modifies IP header in Transit

Maps one IPv6 address prefix to another IPv6 prefix

Uses Network-specific prefix

Modifies session during translation

NAT64

Target 1

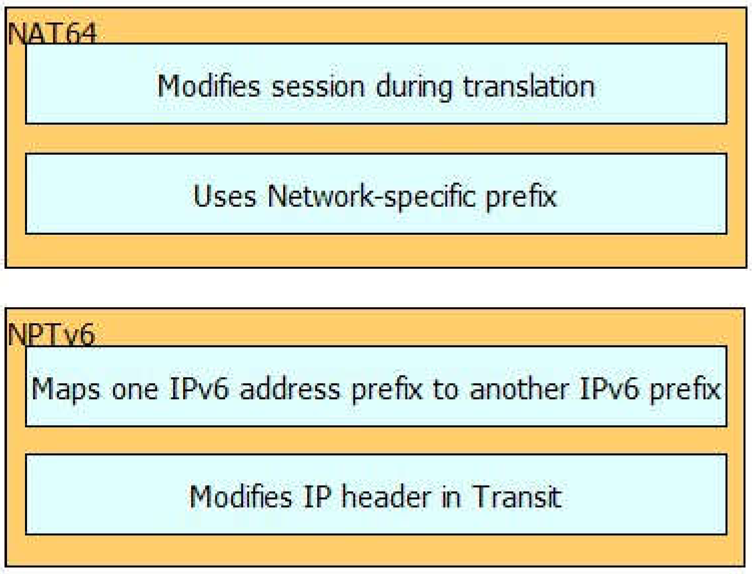
Target 2

NPTv6

Target 3

Target 4

Correct Answer:



NAT64

Modifies session during translation

Uses Network-specific prefix

NPTv6

Maps one IPv6 address prefix to another IPv6 prefix

Modifies IP header in Transit

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 145
An engineer is asked to monitor the availability of the next-hop IP address of 172.16.201.25 every 3 seconds using an ICMP echo packet via an ICMP echo probe. Which two commands accomplish this task? (Choose two.)

A. router(config-ip-sla)#icmp-echo 172.16.201.25 source-interface FastEthernet 0/0
B. router(config-ip-sla-echo)#timeout 3
C. router(config-ip-sla)#icmp-jitter 172.16.201.25 interval 100
D. router(config-ip-sla-echo)#frequency 3
E. router(config-ip-sla)#udp-echo 172.16.201.25 source-port 23
F. router(config-ip-sla-echo)#threshold 3

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 146
What is the function of the snmp-server manager command?

A. to enable the device to send and receive SNMP requests and responses
B. to disable SNMP messages from getting to the SNMP engine
C. to enable the device to send SNMP traps to the SNMP server
D. to configure the SNMP server to store log data

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The SNMP manager process sends SNMP requests to agents and receives SNMP responses and notifications from agents. When the SNMP manager process is enabled, the router can query other SNMP agents and process incoming SNMP traps.
Most network security policies assume that routers will be accepting SNMP requests, sending SNMP responses, and sending SNMP notifications. With the SNMP manager functionality enabled, the router may also be sending SNMP requests, receiving SNMP responses, and receiving SNMP notifications. The security policy implementation may need to be updated prior to enabling this functionality.
SNMP requests are typically sent to UDP port 161. SNMP responses are typically sent from UDP port 161. SNMP notifications are typically sent to UDP port 162

QUESTION 147
Refer to the following configuration command.:

router(config)# ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80

Which statement about the command is true?

A. Any packet that is received in the inside interface with a source IP port addresses of 172.16.10.8:80 is translated to 172.16.10.8:8080.
B. Any packet that is received in the inside interface with a source IP address of 172.16.10.8is redirected to port 8080 or port 80.
C. The router accepts only a TCP connection from port 8080 and port 80 on IP address 172.16.10.8.
D. Any packet that is received in the inside interface with a source IP port address of 172.16.10.8:8080 is translatedto 172.16.10.8:80.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html#topic9

QUESTION 148

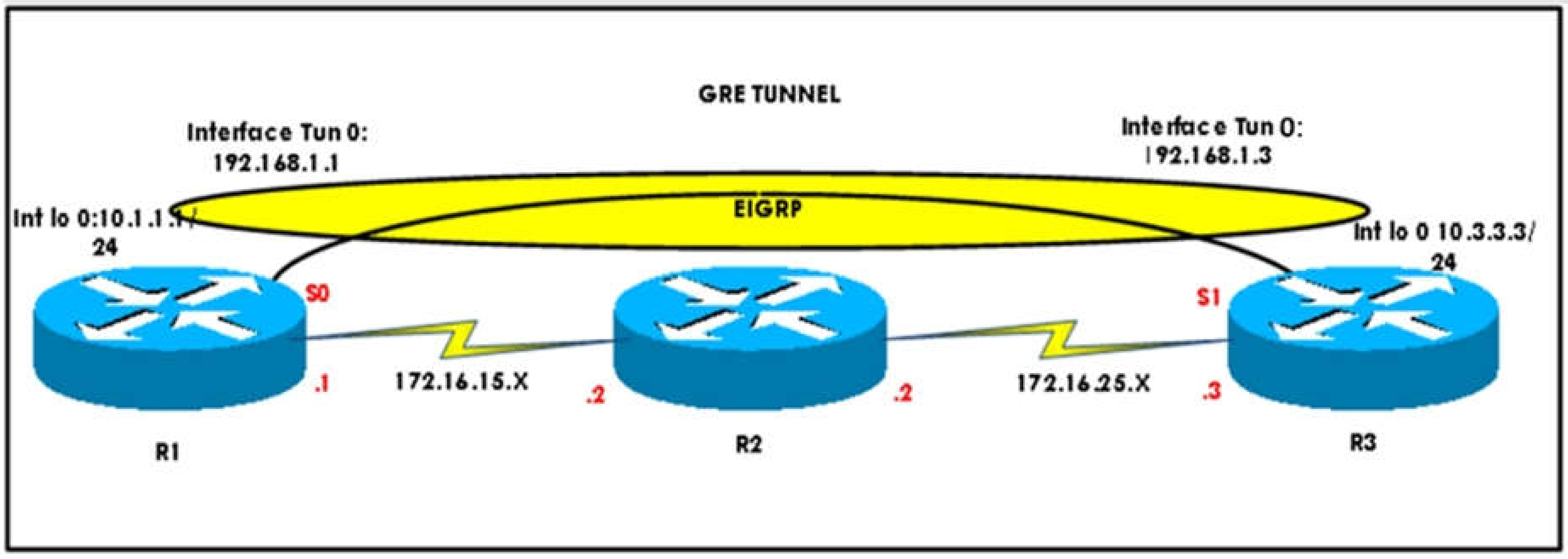
When a tunnel interface is configured in the default mode, which statement about routers and the tunnel destination address is true?

A. The router must have WCCP redirects enabled inbound from the tunnel destination.
B. The router must have redirects enabled outbound toward the tunnel destination.
C. The router must have a route installed toward the tunneldestination.
D. The router must have Cisco Discovery Protocol enabled on the tunnel to form a CDP neighborship with the tunnel destination.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 149



Refer to the exhibit. A network engineer has configured GRE between two IOS routers. The state of the tunnel interface is continuously oscillating between up and down. What is the solution to this problem?

A. Create a more specific ARP entry to define how to reach the remote router.
B. Save the configuration and reload the router.
C. Create a more specific static route to define how to reach the remote router.
D. Check whether the Internet service provider link is stable,

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
References:
http://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/22327-gre-flap.html

QUESTION 150
Other than a working EIGRP configuration, which option must be the same on all routers for EIGRP authentication key role over to work correctly?

A. SMTP
B. SNMP
C. passwords
D. time

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Requirements for EIGRP authentication

- The time must be properly configured on all routers. Refer to Configuring NTP for more information.
- A working EIGRP configuration is recommended.

If we have option "Key-Chain", instead of "Passwords" then option C would also be correct.

References: https://www.cisco.com/c/en/us/support/docs/ip/enhanced-interior-gateway-routing-protocol-eigrp/82110-eigrp-authentication.html

QUESTION 151
Which two statements about NTP operation are true? (Choose two.)

A. Locally configured time overrides time received from an NTP server.
B. If multiple NTP servers are configured, the one with the lowest stratum is preferred.
C. If multiple NTP servers are configured, the one with the highest stratum is preferred.
D. “Stratum” refers to the number of hops between the NTP client and the NTP server.
E. By default, NTP communications use UDP port 123.

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
NTP is designed to synchronize the time on a network of machines. NTP runs over the User Datagram Protocol (UDP), using port 123 as both the source and destination, which in turn runs over IP. NTP Version 3 RFC 1305 leavingcisco.com is used to synchronize timekeeping among a set of distributed time servers and clients. A set of nodes on a network are identified and configured with NTP and the nodes form a synchronization subnet, sometimes referred to as an overlay network. While multiple masters (primary servers) may exist, there is no requirement for an election protocol.
An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. An NTP client makes a transaction with its server over its polling interval (from 64 to 1024 seconds) which dynamically changes over time depending on the network conditions between the NTP server and the client. The other situation occurs when the router communicates to a bad NTP server (for example, NTP server with large dispersion); the router also increases the poll interval. No more than one NTP transaction per minute is needed to synchronize two machines. It is not possible to adjust the NTP poll interval on a router.
NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. For example, a stratum 1 time server has a radio or atomic clock directly attached to it. It then sends its time to a stratum 2 time server through NTP, and so on. A machine running NTP automatically chooses the machine with the lowest stratum number that it is configured to communicate with using NTP as its time source. This strategy effectively builds a self-organizing tree of NTP speakers. NTP performs well over the non-deterministic path lengths of packet-switched networks, because it makes robust estimates of the following three key variables in the relationship between a client and a time server

Reference:
http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntpm.html

QUESTION 152
Which type of IPv6 address is an identifier for a single interface on a single node?

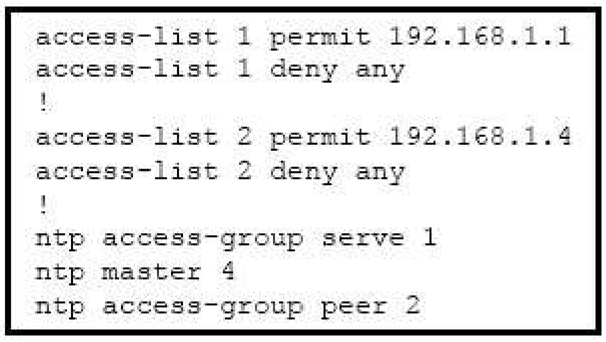
A. broadcast
B. multicast
C. anycast
D. unicast

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

An IPv6 unicast address is an identifier for a single interface,on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.
References:

QUESTION 153
Refer to the exhibit. Which three NTP features can be deduced on the router? (Choose three.)



```
access-list 1 permit 192.168.1.1
access-list 1 deny any
!
access-list 2 permit 192.168.1.4
access-list 2 deny any
!
ntp access-group serve 1
ntp master 4
ntp access-group peer 2
```

A. only updates its time from 192.168.1.4
B. only accepts time requests from 192.168.1.1
C. only updates its time from 192.168.1.1
D. only accepts time requests from 192.168.1.4
E. only handles four requests at a time
F. only is in stratum 4

Correct Answer: ABF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The access group options are scanned in the following order, from least restrictive to most restrictive. However, if NTP matches a deny ACL rule in a configured peer, ACL processing stops and does not continue to the next access group option.
- The peer keyword enables the device to receive time requests and NTP control queries and to synchronize itself to the servers specified in the access list.
- The serve keyword enables the device to receivetime requests and NTP control queries from the servers specified in the access list but not to synchronize itself to the specified servers.
- The serve-only keyword enables the device to receive only time requests from servers specified in the access list.
- The query-only keyword enables the device to receive only NTP control queries from the servers specified in the access list.

QUESTION 154
What command can you enter to configure an enable password that users an encrypted password from another configuration?

A. enable secret $abc%!#.Cd34$!ao0
B. enable secret 7 $abc%!#.Cd34$!ao0
C. enable secret 0 $abc%!#.Cd34$!ao0

D. enable secret 5 $abc%!#.Cd34$!ao0
E. enable secret 15 $abc%!#.Cd34$!ao0
F. enable secret 6 $abc%!#.Cd34$!ao0

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
References:

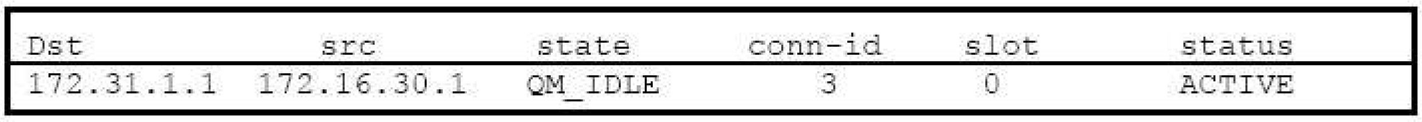
QUESTION 155
A network engineer receives reports about poor voice quality issues at a remote site. The network engineer does a packet capture and sees out-of-order packets being delivered. Which option can cause the VoIP quality to suffer?

A. speed duplex link issues
B. misconfigured voice VLAN
C. load balancing over redundant links
D. traffic over backup redundant links

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
In traditional packet forwarding systems, using different paths have varying latencies that cause out of order packets, eventually resulting in far lower performance for the network application. Also , if some packets are process switched quickly by the routing engine of the router while others are interrupt switched (which takes more time) then it could result in out of order packets. The other options would cause packet drops or latency, but not out of order packets.

QUESTION 156



```
Dst          src          state      conn-id   slot   status
172.31.1.1   172.16.30.1  QM_IDLE       3        0     ACTIVE
```

Refer to the exhibit. A network engineer is troubleshooting a DMVPN setup between the hub and the spoke. The engineer executes the command show crypto isakmp sa and observes the output that is displayed. What is the problem?

A. that ISAKMP is using default settings
B. an incompatible ISAKMP policy
C. an incompatible IPsec transform set
D. that ISAKMP is not enabled

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Reference:
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

QUESTION 157
Which two attributes describe UDP within a TCP/IP network? (Choose two.)

A. acknowledgments
B. unreliable delivery
C. connection-oriented communication
D. increased headers
E. connectionless communication

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
UDP Characteristics
presents the structure of a UDP segment header. Because UDP is considered to be an unreliable protocol, it lacks the sequence numbering, window size, and connectionless acknowledgment numbering present in the header of a TCP segment.
Rather the UDP segment's
Because a UDP segment header is so much smaller than a TCP segment header, UDP becomes a good candidate for the transport layer protocol serving applications that need to maximize bandwidth and do not require acknowledgments.

QUESTION 158
Which three IP SLA performance metrics can you use to monitor enterprise-class networks? (Choose three.)

A. packet loss
B. delay
C. bandwidth
D. connectivity
E. reliability

F. traps

Correct Answer: ABD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Cisco IOS IP SLAs collects a unique subset of the following performance metrics:
• Delay (both round-trip and one-way)
• Jitter (directional)
• Packet loss (directional)
• Packet sequencing (packet ordering)
• Path(per hop)
• Connectivity (directional)
• Server or website download time
• Voice quality scores

QUESTION 159
A network administrator notices that the BGP state and logs are generated for missing BGP hello keepalives. What is the potential problem?

A. hello timer mismatch
B. MTU mismatch
C. incorrect neighbor options
D. BGP path MTU enabled

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Introduction
This document describes how to determine if internal or external Border Gateway Protocol (BGP) neighbor flaps are caused by maximum transmission unit (MTU) issues.
Problem
BGP neighbors form; however, at the time of prefix exchange, the BGP state drops and the logsgenerate missing BGP hello keepalives or the other peer terminates the session.
References:

QUESTION 160
A network engineer wants to notify a manager in the event that the IP SLA connection loss threshold is reached. Which two features are needed to implement this functionality? (Choose two.)

A. Cisco IOS EEM
B. SNMP traps
C. threshold action
D. MOS
E. logging local

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:
References:

QUESTION 161
Which Easy Virtual Networking configuration component significantly decreases network configuration?

A. MBGP
B. VNET tags
C. VNET Trunk List
D. VirtualNetwork Trunk
E. dot1e

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

EVN reduces network virtualization configuration significantly across the entire network infrastructure with the Virtual Network Trunk. The traditional VRF-Lite solution requires creating one subinterface perVRF on all switches and routers involved in the data path, creating a lot of burden in configuration management. EVN removes the need of per VRF subinterface by using “vnet trunk” command.
References:
http://www.cisco.com/c/en/us/products/ios-nx-os-software/easy-virtual-network-evn/index.html

QUESTION 162
A network engineer wants to display the statistics of an active tunnel on a DMVPN network. Which command should the administrator execute to accomplish this task?

A. router#show crypto isakmp peers
B. router#show crypto isakmp sa

C. router#show crypto ipsec transform-set
D. router#show crypto engine connections active
E. router#show crypto ipsec sa

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Certain show commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of show command output.

- show crypto isakmp sa—Displays the state for the ISAKMP security association (SA).
- show crypto engine connections active —Displays the total encrypts/decrypts per SA.
- show crypto ipsec sa—Displays the statistics on the active tunnels.
- show ip route—Displays the routing table.
- show ip eigrp neighbor—Displays the EIGRP neighbors.
- show ip nhrp—Displays the IP Next Hop Resolution Protocol (NHRP) cache, optionally limited to dynamic or static cache entries for a specific interface.
- show crypto socket—Displays the cryptosocket table between NHRP and IPSec.

References:
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/29240-dcmvpn.html#veri

QUESTION 163
Which IP SLA operation can be used to measure round-trip delay for the full path and hop-by hop round-trip delay on the network?

A. HTTP
B. ICMP echo
C. TCP connect
D. ICMP path echo

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The ICMP Path Echo operation computes hop-by-hop response time between a Cisco router and any IP device on the network.

References:
http://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper09186a00802d5efe.html

QUESTION 164
In which form does PAP Authentication send the user name and password across the link?

A. clear text
B. hashed
C. encrypted
D. password protected

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 165
What is the administrative distance for EBGP?

A. 200
B. 20
C. 30
D. 70

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 166
Considering the IPv6 address independence requirement, which process do you avoid when you use NPTv6 for translation?

A. IPv6 duplication and conservation
B. IPsec AH header modification
C. checksum verification
D. rewriting of higher layer information

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

Explanation:

The IPv6-to-IPv6 Network Prefix Translation (NPTv6) serves as a useful mechanism for implementing address independence in an IPv6 environment. A major benefit associated with NPTv6 is the fact that it avoids the requirement for an NPTv6 Translator to rewrite the transport layer headers which reduces the load on network devices. NPTv6 also does not interfere with encryption of the full IP payload.
References:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-asr1k-nptv6.html

QUESTION 167
What is the optimal location from which to execute a debug command that produces an excessive amount of information?

A. vty lines
B. a console port
C. SNMP commands
D. an AUX port

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Excessive debugs to the console port of a router can cause it to hang. This is because the router automatically prioritizes console output ahead of other router functions. Hence if the router is processing a large debug outputto the console port, it may hang. Hence, if the debug output is excessive use the vty (telnet) ports or the log buffers to obtain your debugs. More information is provided below.
References:
http://www.cisco.com/c/en/us/support/docs/dial-access/integrated-services-digital-networks-isdn-channel-associated-signaling-cas/10374-debug.html

QUESTION 168
A network engineer is configuring the router for NetFlow data exploring. What is required in order for NDE to begin exporting data?

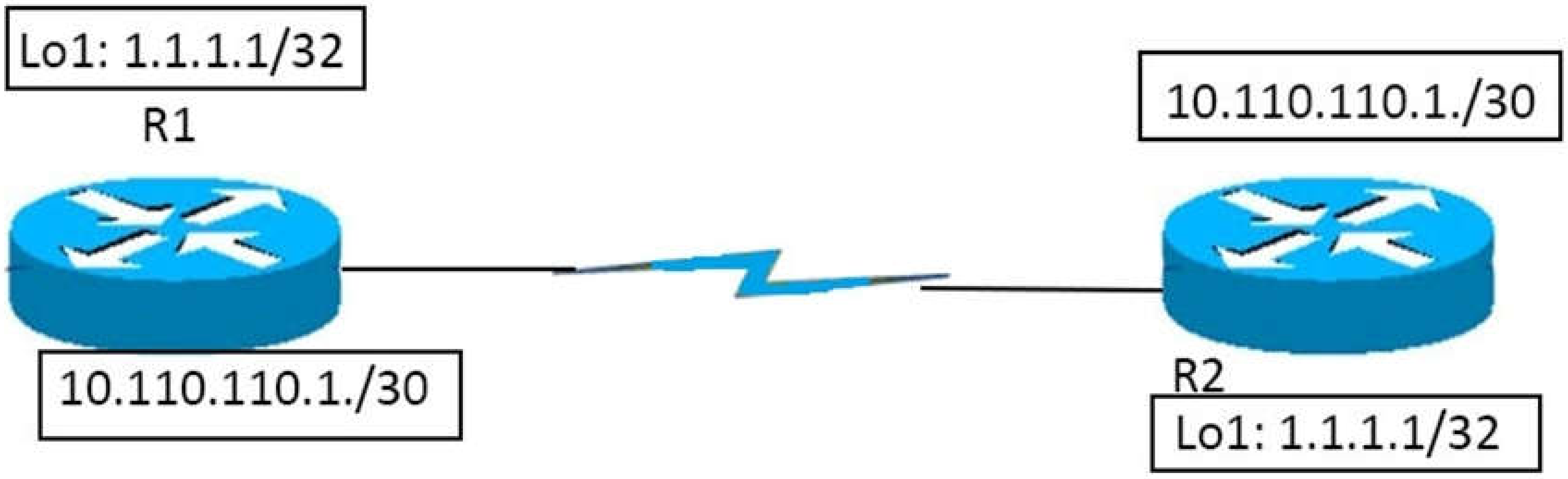
A. destination
B. flowmask
C. source
D. traffic type
E. interface type
F. NetFlow version

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
NetFlow Multiple Export Destinations--To configure redundant NDE data streams, which improves the probability of receiving complete NetFlow data, you can enter the ip flow-export destination command twice and configure a different destination IP address in each command. Configuring two destinations increases the RP CPU utilization, as you are exporting the data records twice.

References:
http://www.cisco.com/en/US/docs/general/Test/dwerblo/broken_guide/nde.html#wp1139278

QUESTION 169



Refer to the exhibit. Router 1 cannot ping router 2 via the Frame Relay between them. Which two statements describe the problems? (Choose two.)

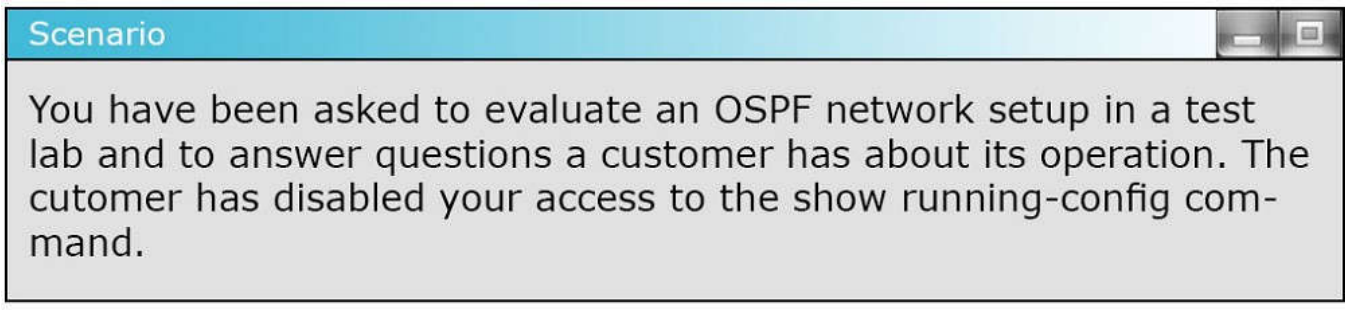
A. Frame Relay map is configured.
B. DLCI is active.
C. DLCI isinactive or deleted.
D. Encapsulation is mismatched.
E. An access list is needed to allow ping.

Correct Answer: CD
Section: Mix Questions

Explanation

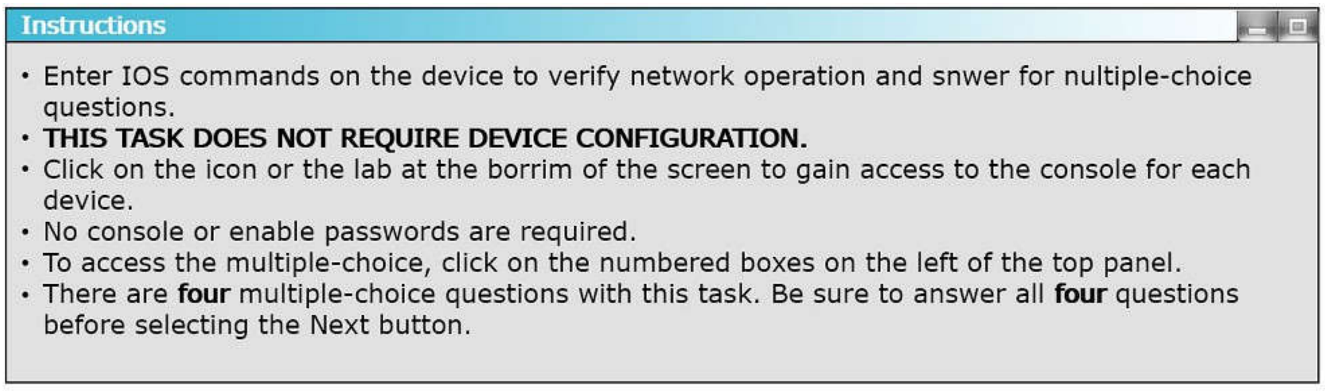
Explanation/Reference:
Explanation:

QUESTION 170



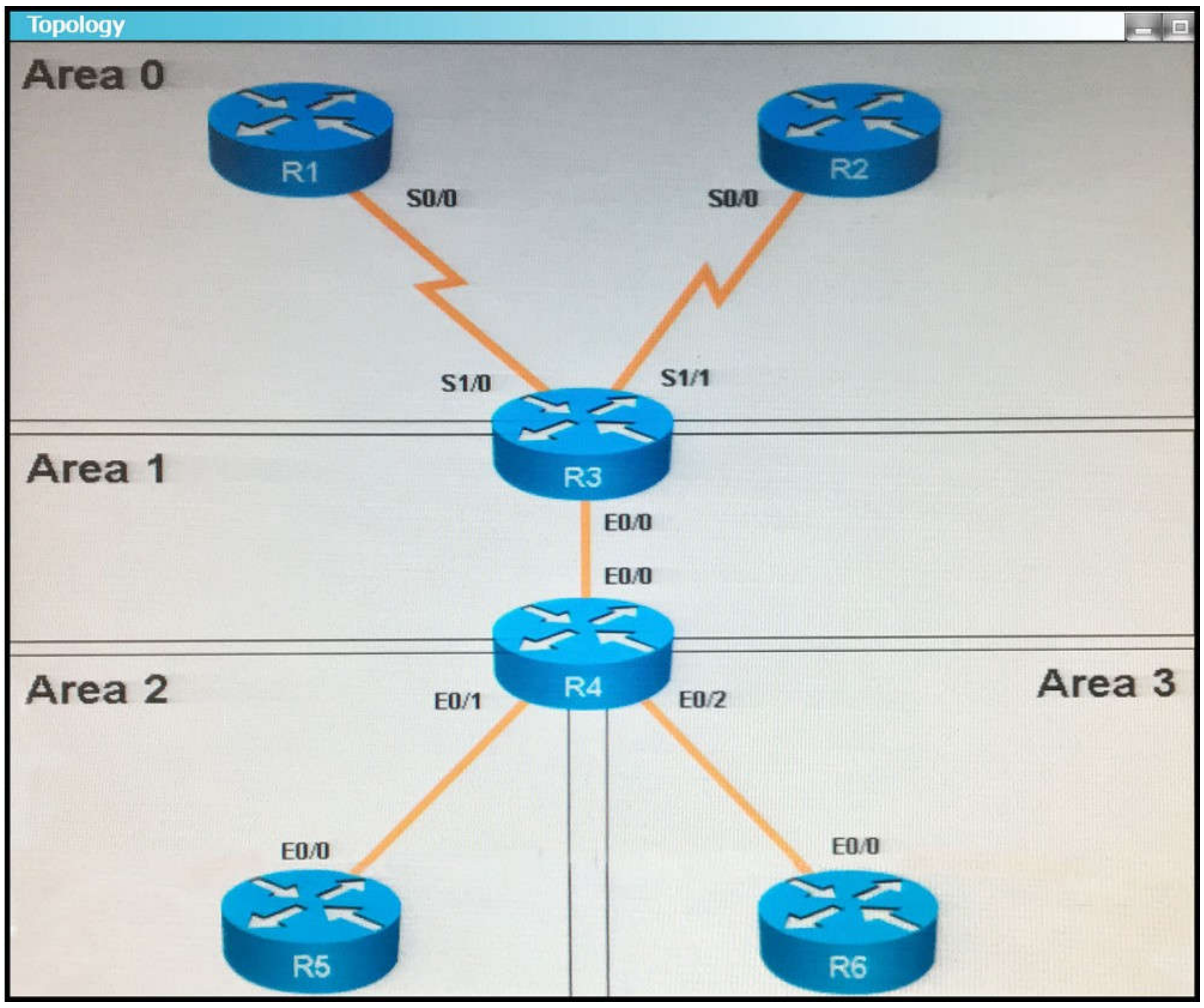
Scenario

You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The cutomer has disabled your access to the show running-config command.



Instructions

- Enter IOS commands on the device to verify network operation and snwer for nultiple-choice questions.
- **THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.**
- Click on the icon or the lab at the borrim of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice, click on the numbered boxes on the left of the top panel.
- There are **four** multiple-choice questions with this task. Be sure to answer all **four** questions before selecting the Next button.

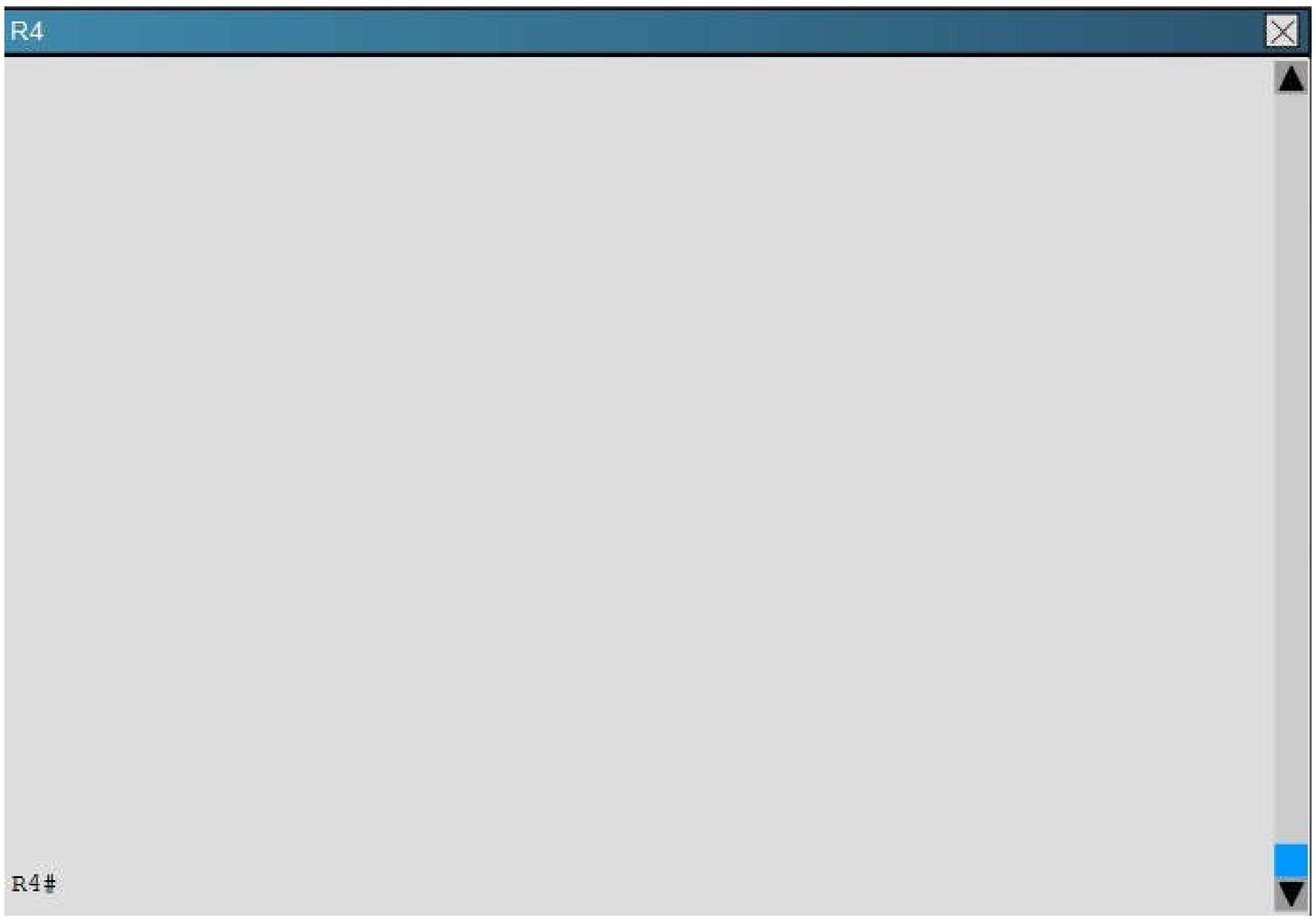


Topology

```
R1#
```

```
R2#
```

```
R3#
```



```
R4#
```

```
R5#
```

```
R5#
```

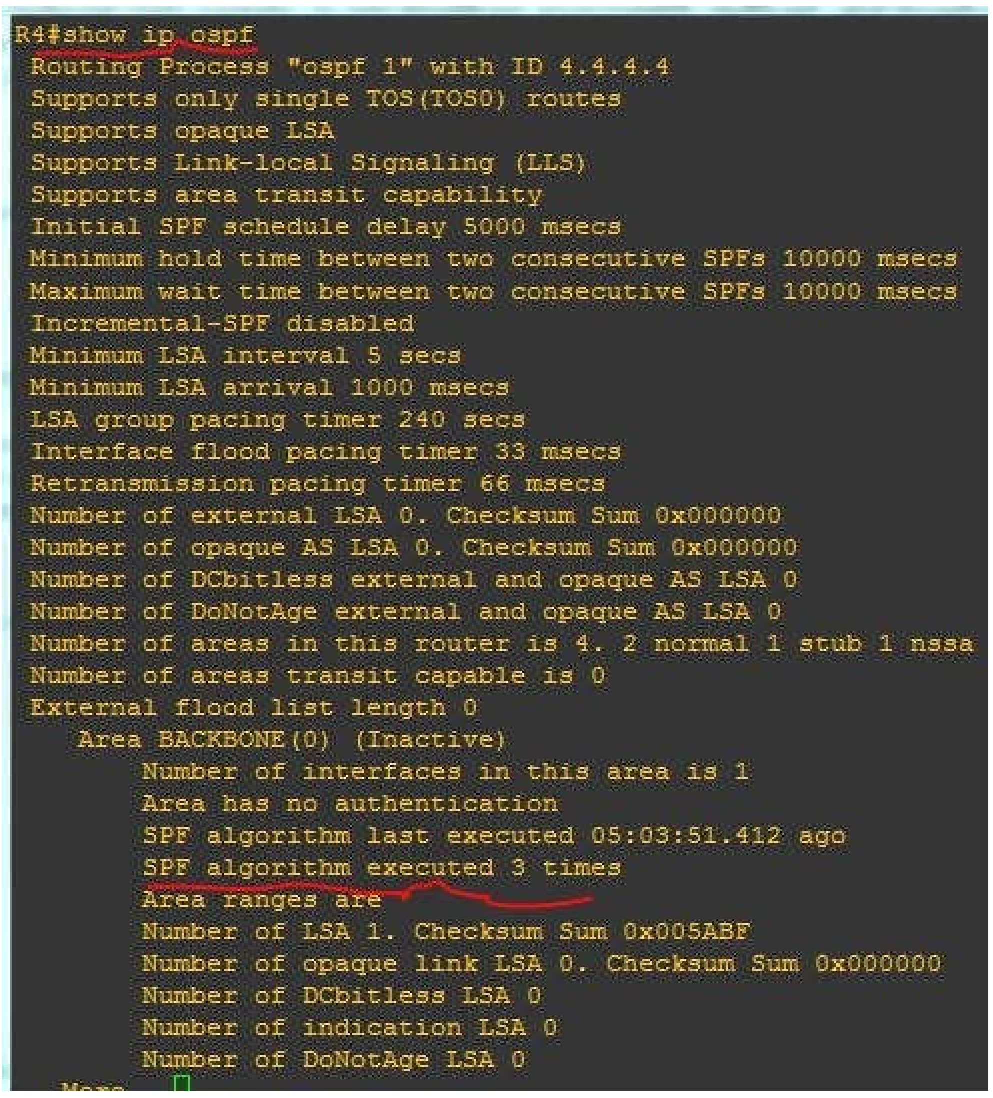
How many times was SPF alrogithm executed on R4 for Area 1?

A. 1
B. 5
C. 9
D. 20
E. 54
F. 224

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Answers vary, some answers will be 3. To find the answer, you can check the number of times the execcuted SPF algorithm ran via the “show ip ospf”command on R4:



```
R4#show ip ospf
 Routing Process "ospf 1" with ID 4.4.4.4
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Supports Link-local Signaling (LLS)
 Supports area transit capability
 Initial SPF schedule delay 5000 msecs
 Minimum hold time between two consecutive SPFs 10000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Incremental-SPF disabled
 Minimum LSA interval 5 secs
 Minimum LSA arrival 1000 msecs
 LSA group pacing timer 240 secs
 Interface flood pacing timer 33 msecs
 Retransmission pacing timer 66 msecs
 Number of external LSA 0. Checksum Sum 0x000000
 Number of opaque AS LSA 0. Checksum Sum 0x000000
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 4. 2 normal 1 stub 1 nssa
 Number of areas transit capable is 0
 External flood list length 0
    Area BACKBONE(0) (Inactive)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm last executed 05:03:51.412 ago
        SPF algorithm executed 3 times
        Area ranges are
        Number of LSA 1. Checksum Sum 0x005ABF
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
   --More--
```

In this case it was 3. Again, answers will vary.

QUESTION 171
An engineer is using a network sniffer to troubleshoot DHCPv6 between a router and hosts on the LAN with the following configuration:

```
interface Ethernet0
ipv6 dhcp server DHCPSERVERPOOL rapid-commit
!
```

Which two DHCP messages will appear in the sniffer logs? (Choose two.)

A. reply
B. request
C. advertise
D. Acknowledge
E. solicit
F. accept

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The DHCPv6 client can obtain configuration parameters from a server either through a rapid two-message exchange (solicit, reply) or through a four-message exchange (solicit, advertise, request, and reply). By default, the four-message exchange is used. When the rapid-commit option is enabled by both the client and the server, the two-message exchange is used.
References:

QUESTION 172
At which layer does Cisco Express Forwarding use adjacency tables to populate addressing information?

A. Layer 4
B. Layer 3
C. Layer 2
D. Layer 1

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation: Adjacency table - Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.
References:
http://www.cisco.com/c/en/us/support/docs/routers/12000-series-routers/47321-ciscoef.html

QUESTION 173
A network engineer wants to ensure an optimal end-to-end delay bandwidth product. The delay is less than 64 ms. Which TCP feature ensures steady state throughput?

A. network buffers
B. TCP acknowledgments
C. widows scaling
D. round-trip timers

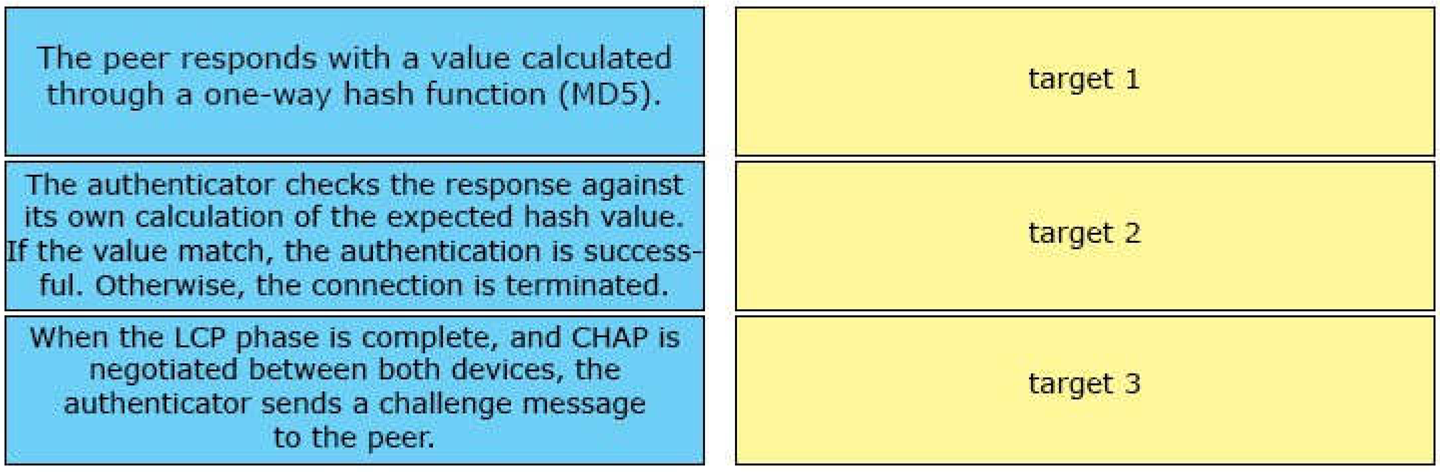
Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Options can be carried in a TCP header. Those relevant to TCP performance include Window- scale option : This option is intended to address the issue of the maximum window size in the face of paths that exhibit a high-delay bandwidth product. This option allows the window size advertisement to be right-shifted by the amount specified (in binary arithmetic, a right-shift corresponds to a multiplication by 2). Without this option, the maximum window size that can be advertised is 65,535 bytes (the maximum value obtainable in a 16-bit field). The limit of TCP transfer speed is effectively one window size in transit between the sender and the receiver. For high-speed, long-delay networks, this performance limitation is a significant factor, because it limits the transfer rate to at most 65,535 bytes per round-trip interval, regardless of available network capacity. Use of the window- scale option allows the TCP sender to effectively adapt to high-band-width, high-delay network paths, by allowing more data to be held in flight.
The maximum window size with this option.
Reference:
http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-5/ipj-archive/article09186a00800c8417.html

QUESTION 174
DRAG DROP

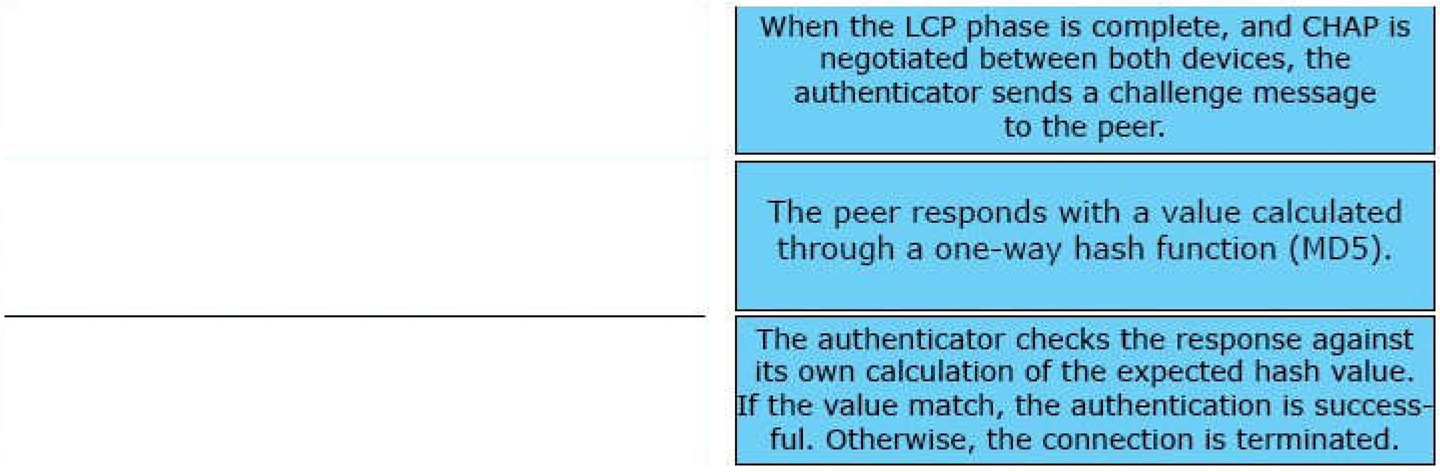
Drag and drop the Challenge Handshake Authentication Protocol steps from the left into the correct order in which they occur on the right.

Select and Place:



The peer responds with a value calculated through a one-way hash function (MD5).	target 1
The authenticator checks the response against its own calculation of the expected hash value. If the value match, the authentication is successful. Otherwise, the connection is terminated.	target 2
When the LCP phase is complete, and CHAP is negotiated between both devices, the authenticator sends a challenge message to the peer.	target 3

Correct Answer:



	When the LCP phase is complete, and CHAP is negotiated between both devices, the authenticator sends a challenge message to the peer.
	The peer responds with a value calculated through a one-way hash function (MD5).
	The authenticator checks the response against its own calculation of the expected hash value. If the value match, the authentication is successful. Otherwise, the connection is terminated.

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The Challenge Handshake Authentication Protocol (CHAP) verifies the identity of the peer by means of a three-way handshake. These are the general steps performed in CHAP:
1. After the LCP (Link Control Protocol) phase is complete, and CHAP is negotiated between both devices,the authenticator sends a challenge message to the peer.
2. The peer responds with a value calculated through a one-way hash function (Message Digest 5 (MD5)).
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication is successful. Otherwise, the connection is terminated.
References:
http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

QUESTION 175
Which two functionalities are specific to stateless NAT64? (Choose two.)

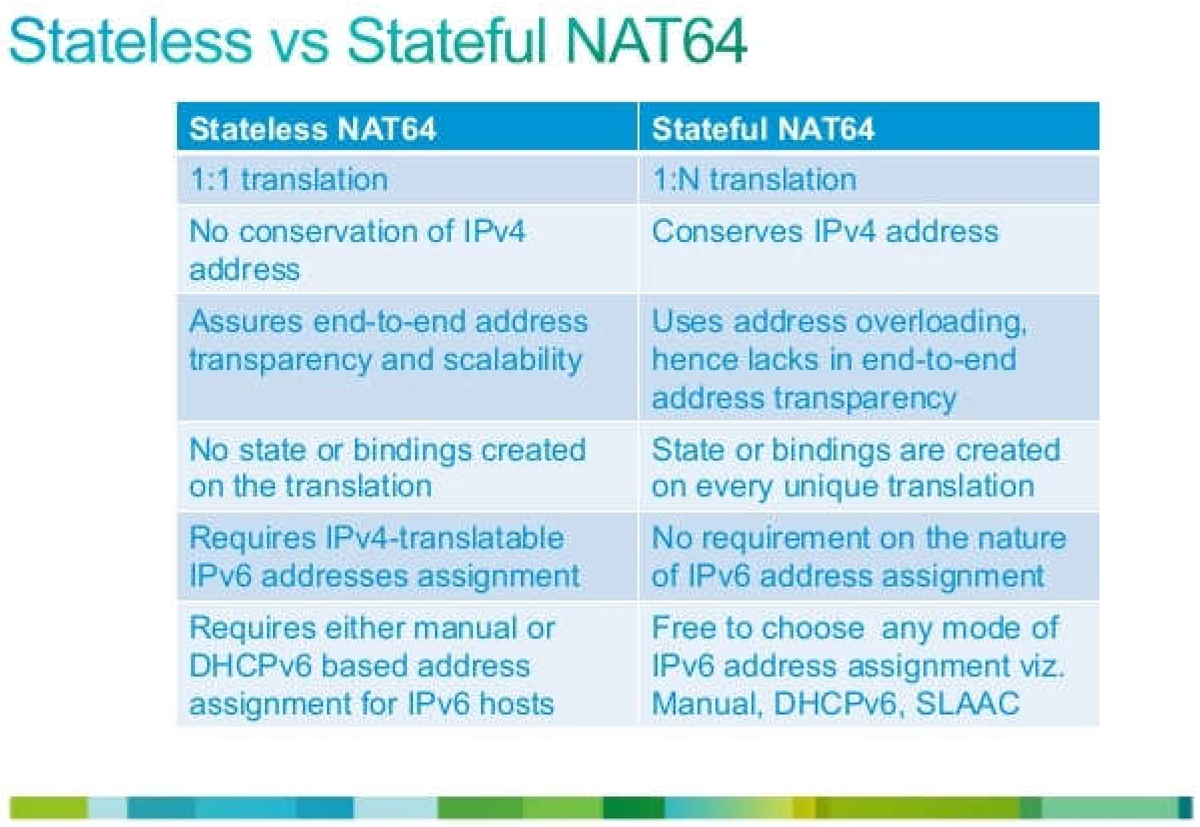
A. It does not conserve IPv4 addresses.
B. No requirement exists for the characteristics of IPv6 address assignment.

C. It uses address overloading.
D. State or bindings are created on the translation.
E. It provides 1-to-1 translation.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Comparison Between Stateless and Stateful NAT64
Stateless NAT64
Stateful NAT64
1:1 translation, hence applicable for limited number of endpoints
1: N translation, hence no constraint on thenumber of end points therefore, also applicable for carrier grade NAT (CGN)
No conservation of IPv4 address
Conserves IPv4 address
Helps ensure end-to-end address transparency and scalability
Uses address overloading; hence lacks end-to-end address transparency
No state or bindings created on the translation
State or bindings created on every unique translation
Requires IPv4-translatable IPv6 address assignment (mandatory requirement)
No requirement for the characteristics of IPv6 address assignment
Requires either manual or Domain Host Configuration Protocol Version 6 (DHCPv6)-based address assignment for IPv6 hosts
Capability to choose any mode of IPv6 address assignment: manual, DHCPv6, or stateless address autoconfiguration (SLAAC)



Stateless vs Stateful NAT64

Stateless NAT64	Stateful NAT64
1:1 translation	1:N translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment	No requirement on the nature of IPv6 address assignment
Requires either manual or DHCPv6 based address assignment for IPv6 hosts	Free to choose any mode of IPv6 address assignment viz. Manual, DHCPv6, SLAAC

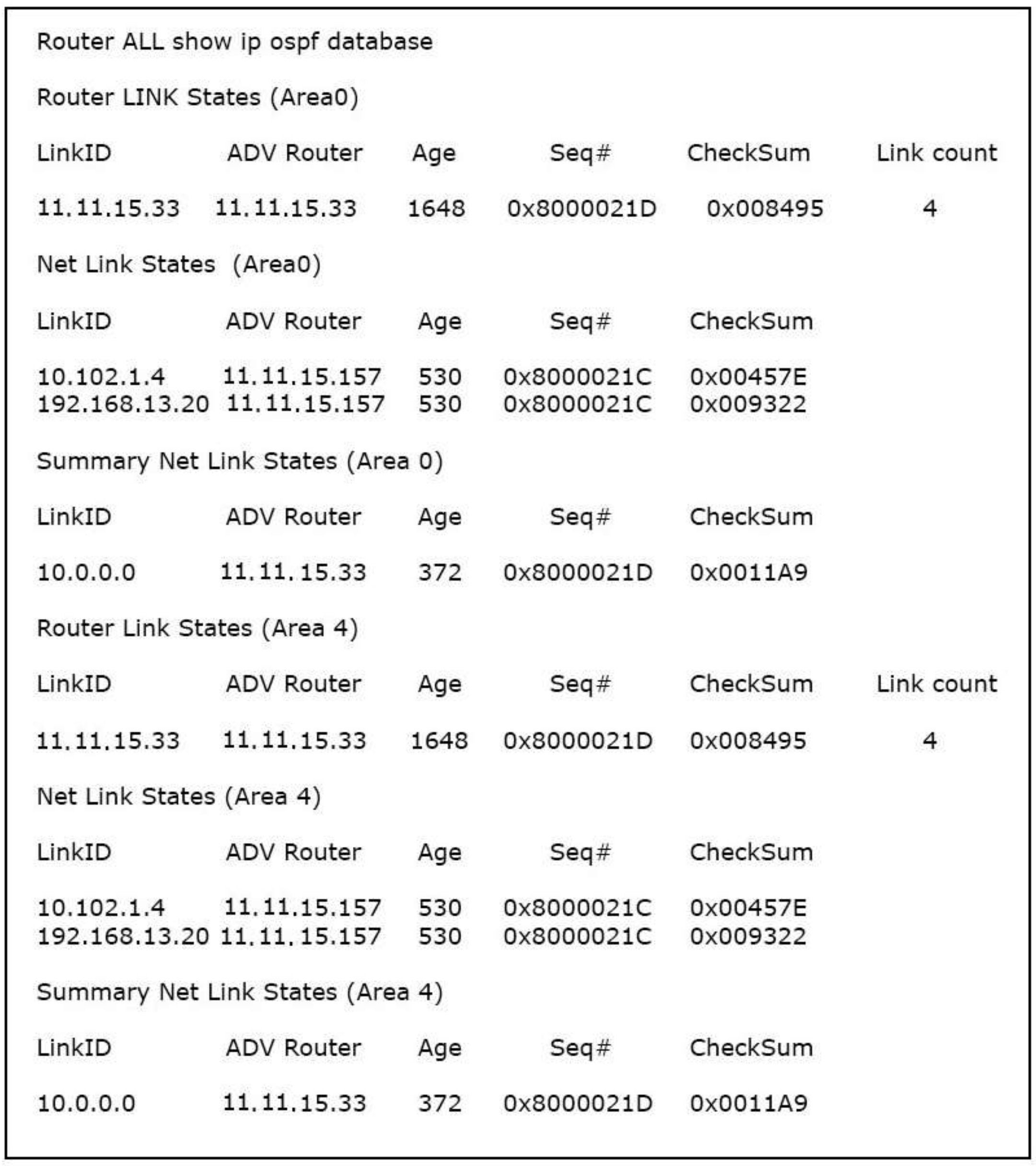
QUESTION 176
A network administrator creates a static route that points directly to a multi-access interface, instead of the next-hop IP address. The administrator notices that Cisco Express Forwarding ARP requests are being sent to all destinations. Which issue might this configuration create?

A. Cisco Express Forwarding routing loop
B. IP route interference
C. high memory usage
D. high bandwidth usage
E. low bandwidth usage

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:
http://www.cisco.com/c/en/us/support/docs/ip/express-forwarding-cef/26083-trouble-cef.html

QUESTION 177



```
Router ALL show ip ospf database

Router LINK States (Area0)

LinkID          ADV Router     Age       Seq#        CheckSum      Link count

11.11.15.33   11.11.15.33     1648    0x8000021D     0x008495          4

Net Link States  (Area0)

LinkID          ADV Router      Age       Seq#        CheckSum

10.102.1.4      11.11.15.157    530    0x8000021C    0x00457E
192.168.13.20  11.11.15.157    530    0x8000021C    0x009322

Summary Net Link States (Area 0)

LinkID          ADV Router      Age       Seq#        CheckSum

10.0.0.0        11.11.15.33     372    0x8000021D    0x0011A9

Router Link States (Area 4)

LinkID          ADV Router      Age       Seq#        CheckSum      Link count

11.11.15.33     11.11.15.33    1648    0x8000021D    0x008495          4

Net Link States (Area 4)

LinkID          ADV Router      Age       Seq#        CheckSum

10.102.1.4      11.11.15.157    530    0x8000021C    0x00457E
192.168.13.20 11.11.15.157    530    0x8000021C    0x009322

Summary Net Link States (Area 4)

LinkID          ADV Router      Age       Seq#        CheckSum

10.0.0.0        11.11.15.33     372    0x8000021D    0x0011A9
```

Refer to the exhibit showing complete command output. What type of OSPF router is router A?

A. internal router
B. ASBR
C. ABR
D. edge router

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
An area is interface specific. A router that has all of its interfaces within the same area is called an internal router (IR). A router that has interfaces in multiple areas is called an area border router (ABR).

Reference:
http://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#t8

QUESTION 178
You are configuring a Microsoft client to call a PPP server using CHAP. Only the client will be authenticated, but the client's password has expired and must be changed. Which PPP server configuration allows the call to be completed?

A. ppp authentication ms-chap-v2
B. ppp authentication chap callin
C. ppp authentication chap
D. ppp authentication ms-chap-v2 callin
E. ppp authentication ms-chap callin

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 179
During which DMVPN phase is spoke-to-spoke communication enabled?

A. Phase 1
B. Phase 6
C. Phase 2
D. Phase 5
E. Phase 4

Correct Answer: C

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 180
Which two tasks does a DHCP relay agent perform? (Choose two.)

A. It forwards DHCPHELLO and DHCPREQUEST messages to the DHCP server.
B. It forwards DHCPREQUEST and DHCPACK messages to the DHCP server.
C. It forwards DHCPOFFER and DHCPCOMPLETE messages to the DHCP client.
D. It forwards DHCPDISCOVER and DHCPREQUEST messages to the DHCP server.
E. It forwards DHCPOFFER and DHCPACK messages to the DHCP client.

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/rtg_brdg/guide/rtbrgdgd/dhcp.pdfpage 3

QUESTION 181
Which command enables NAT-PT on an IPv6 interface?

A. ipv6 nat enable
B. ipv6 nat
C. ipv6nat-pt enable
D. ipv6 nat-pt

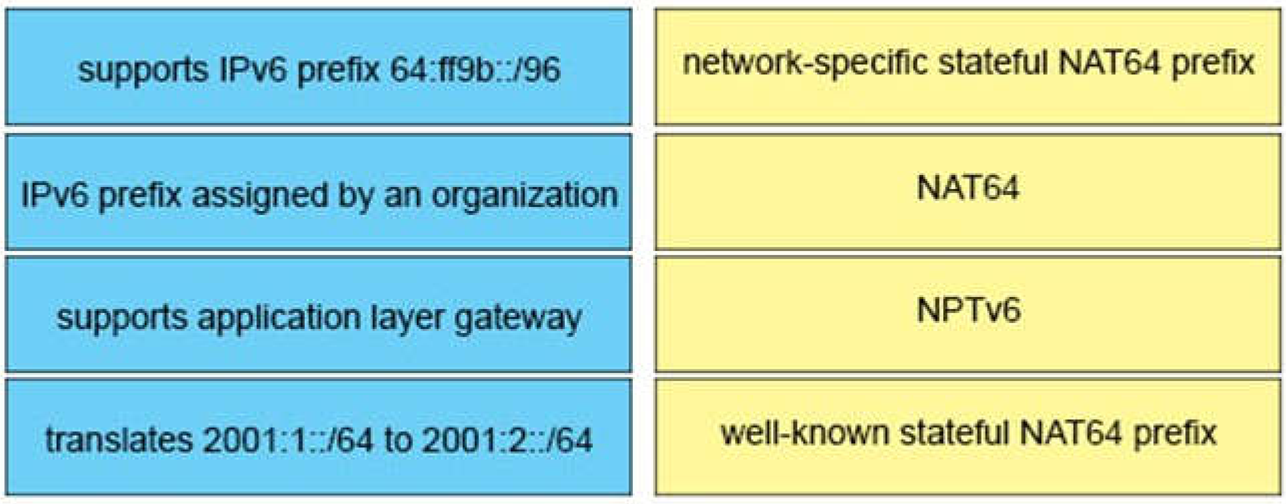
Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/ip6-natpt.html

QUESTION 182
DRAG DROP

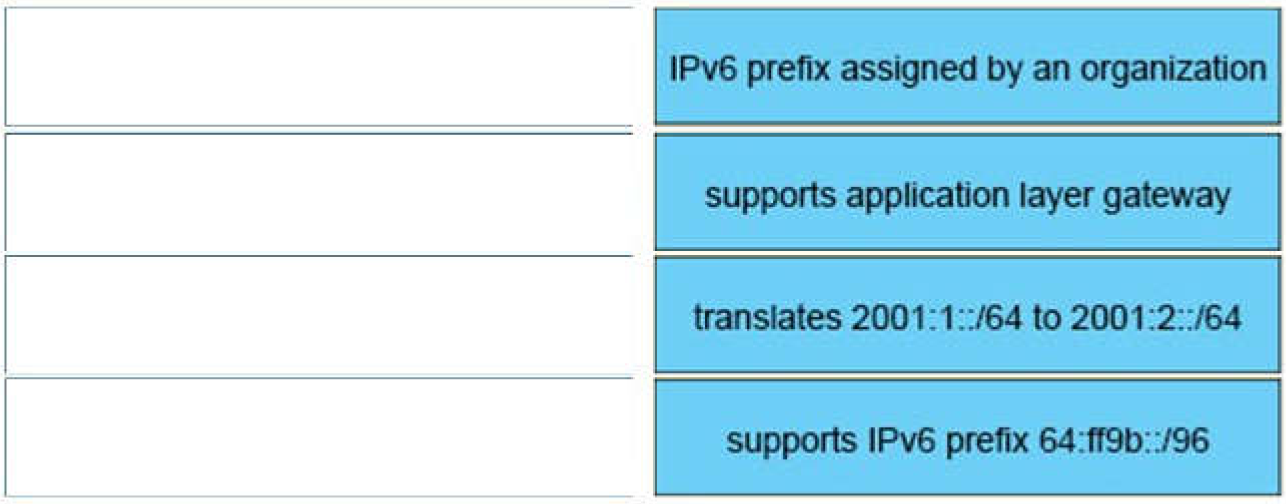
Drag and drop the IPv6 NAT characteristic from the left onto the correct IPv6 NAT category on the right.

Select and Place:



supports IPv6 prefix 64:ff9b::/96	network-specific stateful NAT64 prefix
IPv6 prefix assigned by an organization	NAT64
supports application layer gateway	NPTv6
translates 2001:1::/64 to 2001:2::/64	well-known stateful NAT64 prefix

Correct Answer:



	IPv6 prefix assigned by an organization
	supports application layer gateway
	translates 2001:1::/64 to 2001:2::/64
	supports IPv6 prefix 64:ff9b::/96

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 183
Which two address types are included in NAT? (Choose two.)

A. outside Internet
B. outside local
C. inside global
D. global outside
E. inside Internet

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/4606-8.html

QUESTION 184
A network engineer is modifying RIPng timer configuration. Which configuration mode should the engineer use?

A. router(config-if)#
B. router(config-rtr)#
C. router(config)#
D. router(config-ripng)#

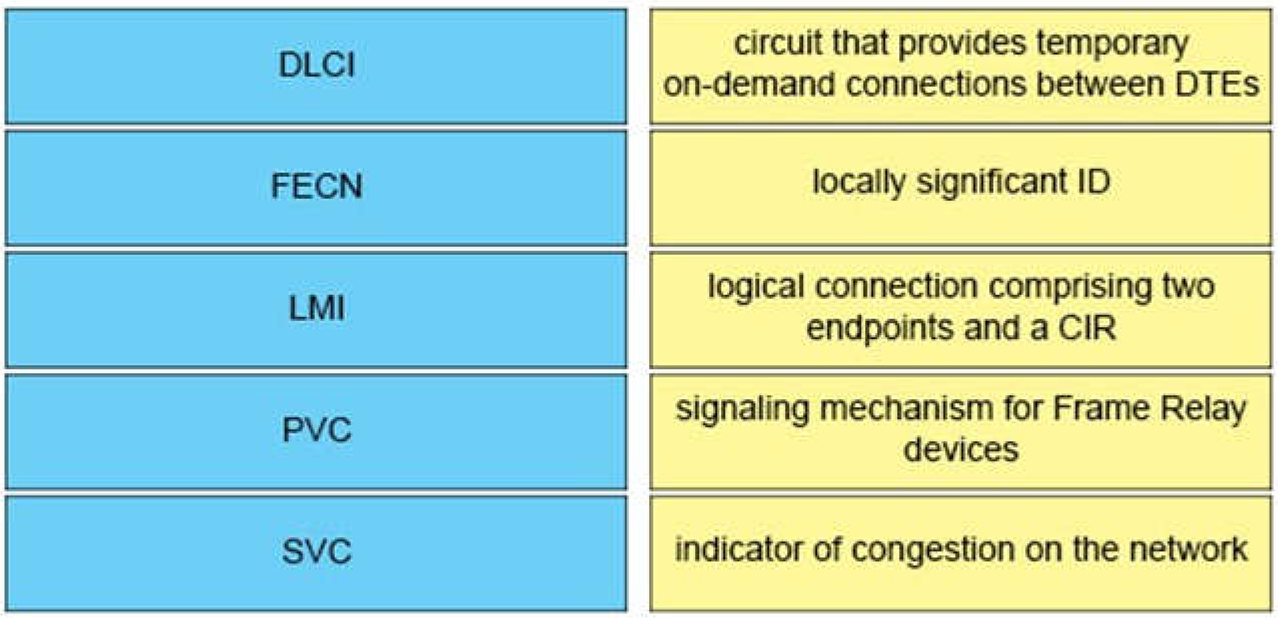
Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
This is how to change the timers for RIPng:
R1(config)#ipv6 router rip test
R1(config-rtr)#timers 5 15 10 30 (5: Update period; 15: Route timeout period; 10: Route holddown period; 30: Route garbage collection period)

QUESTION 185
DRAG DROP

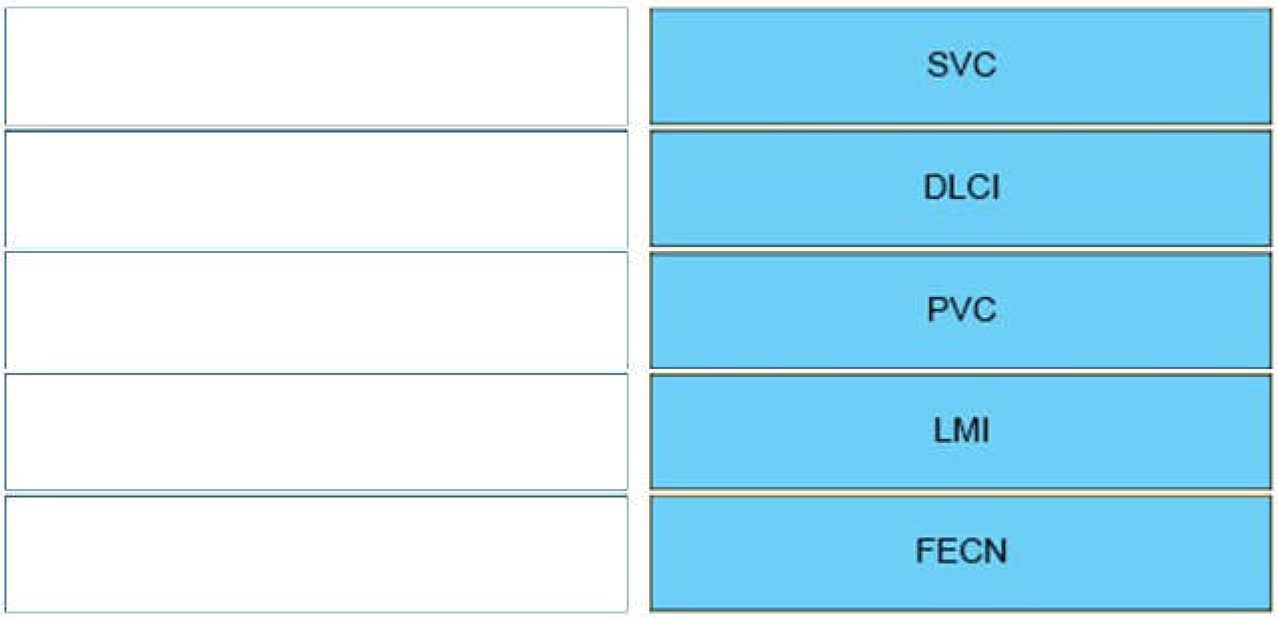
Drag and drop the Frame Relay components from the left onto the correct descriptions on the right.

Select and Place:



DLCI	circuit that provides temporary on-demand connections between DTEs
FECN	locally significant ID
LMI	logical connection comprising two endpoints and a CIR
PVC	signaling mechanism for Frame Relay devices
SVC	indicator of congestion on the network

Correct Answer:



	SVC
	DLCI
	PVC
	LMI
	FECN

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 186
Which two statements about IP access lists are true? (Choose two.)

A. IP access lists without at least one deny statement permit all traffic by default.
B. They support wildcard masks to limit the address bits to which entries are applied.
C. Extended access lists must include port numbers.
D. They end with an implicit permit.
E. Entries are applied to traffic in the order in which they appear.

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 187
Which option is one way to mitigate asymmetric routing on an active/active firewall setup for TCP-based connections?

A. disabling asr-group commands on interfaces that are likely to receive asymmetric traffic
B. disabling stateful TCP checks
C. performing packet captures
D. replacing them with redundant routers and allowing load balancing

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 188
A network engineer executes the show ip cache flow command. Which two types of information are displayed in the report that is generated? (Choose two.)

A. flow samples for specific protocols
B. IP packet distribution
C. top talkers
D. flow export statistics
E. MLS flow traffic

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 189
Which two statements about NetFlow version 9 are true? (Choose two.)

A. It is IEEE standards based.
B. It is a Cisco proprietary technology.
C. It is IETF standards based.
D. It supports egress flows only.
E. It supports ingress flows only.
F. It supports ingress and egress flows.

Correct Answer: CF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 190
Which CLI command can you enter to permit or deny IPv6 traffic travelling through an interface?

A. ipv6 access-class
B. access-list
C. access-group
D. ipv6 traffic-filter

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 191
Which three statements about SNMP are true? (Choose three.)

A. The manager polls the agent using UDP port 161.
B. SNMPv3 supports authentication and encryption.
C. The manager configures and send traps to the agent.
D. The manager sends GET and SET messages.
E. The MIB database can be altered only by the SNMP agent.
F. The agent is the monitoring device.

Correct Answer: ABD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
"A manager can send the agent requests to get and set MIB values."
" The security features provided in SNMPv3 are as follows: Message integrity, Authentication, Encryption."
"SNMP requests typically are sent to User Datagram Protocol (UDP) port 161."

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/configuration/guide/ffun_c/fcf014.html

QUESTION 192
Which two OSPF network types can operate without a DR/BDR relationship? (Choose two.)

A. point-to-multipoint
B. nonbroadcast multiaccess
C. nonbroadcast
D. point-to-point
E. broadcast

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 193
Which three algorithms can you configure with the **ip cef load-sharing algorithm** command? (Choose three.)

A. per-packet
B. include-ports
C. universal
D. per-destination
E. tunnel
F. per-source

Correct Answer: BCE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The following load-balancing algorithms are provided for use with Cisco Express Forwarding traffic. You select a load-balancing algorithm with the **ip cef load-sharing algorithm** command.

- Original algorithm--The original Cisco Express Forwarding load-balancing algorithm produces distortions in load sharing across multiple routers because the same algorithm was used on every router. Depending on your network environment, you should select either the universal algorithm (default) or the tunnel algorithm instead.
- Universal algorithm--The universal load-balancing algorithm allows each router on the network to make a different load sharing decision for each source-destination address pair, which resolves load-sharing imbalances. The router is set to perform universal load sharing by default.
- Tunnel algorithm--The tunnel algorithm is designed to balance the per-packet load when only a few source and destination pairs are involved.
- Include-ports algorithm--The include-ports algorithm allows you to use the Layer 4 source and destination ports as part of the load-balancing decision. This method benefits traffic streams running over equal cost paths that are not load shared because the majority of the traffic is between peer addresses

that use different port numbers, such as Real-Time Protocol (RTP) streams. The include-ports algorithm is available in Cisco IOS Release 12.4(11)T and later releases.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/15-mt/isw-cef-15-mt-book/isw-cef-load-balancing.html

QUESTION 194
Which interface type does a PPPoE client use to establish a session?

A. dialer
B. virtual-template
C. physical
D. loopback

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bbdsl/configuration/xe-3s/bba-pppoe-client.html

QUESTION 195
DHCPv6 can obtain configuration parameters from a server through rapid two-way message exchange. Which two steps are involved in this process? (Choose two.)

A. reply
B. auth
C. advertise
D. request
E. solicit

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
When a server has IPv6 addresses and other configuration information committed to a client, the client and server may be able to complete the exchange using only two messages, instead of four messages as described in the next section. In this case, the client sends a Solicit message to the All_DHCP_Relay_Agents_and_Servers requesting the assignment of addresses and other configuration information.
The server that is willing to commit the assignment of addresses to the client immediately responds with a Reply message.

QUESTION 196
In a point-to-multipoint Frame Relay topology, which two methods ensure that all routing updates are received by all EIGRP routers within the Frame Relay network? (Choose two.)

A. Use subinterfaces.
B. Create separate address families.
C. Disable EIGRP auto summary.
D. Use statically defined EIGRP neighbors on the hub site.
E. Disable split horizon.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 197
In which two areas does OSPF send a summary route by default? (Choose two.)

A. NSSA
B. totally stubby
C. normal
D. backbone
E. stub

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

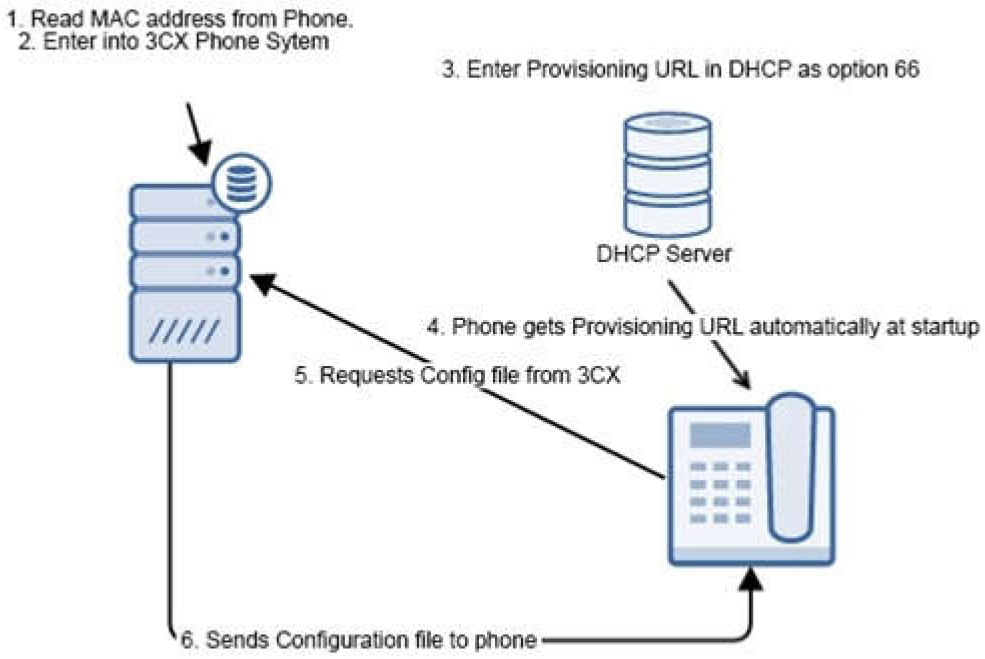
QUESTION 198
Which DHCP options provides a TFTP server that Cisco phones can use to download a configuration?

A. DHCP Option 57
B. DHCP Option 66
C. DHCP Option 82
D. DHCP Option 68

Correct Answer: B
Section: Mix Questions

Explanation

Explanation/Reference:
Explanation:


1. Read MAC address from Phone.
2. Enter into 3CX Phone Sytem
3. Enter Provisioning URL in DHCP as option 66
DHCP Server
4. Phone gets Provisioning URL automatically at startup
5. Requests Config file from 3CX
6. Sends Configuration file to phone

QUESTION 199
Which two commands must you configure on a DMVPN hub to enable phase 3? (Choose two.)

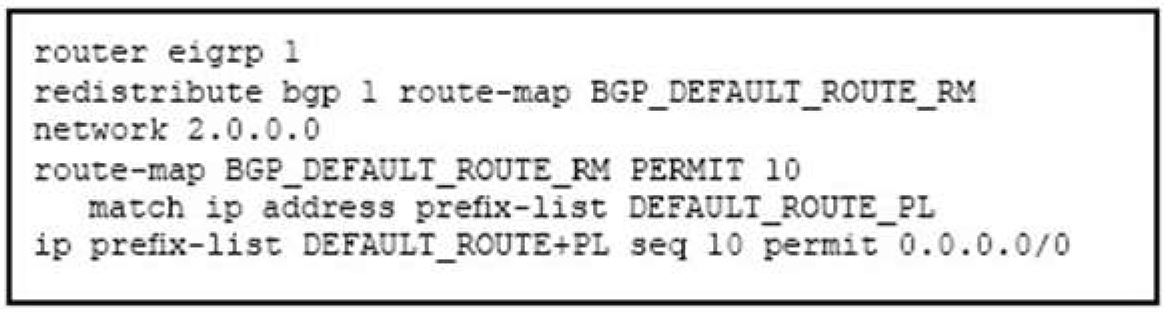
A. ip nhrp map
B. ip redirects
C. ip nhrp shortcut
D. ip nhrp interest
E. ip nhrp redirect
F. ip network-id

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
DMVPN in Phase 3
--ip nhrp shortcut is require only to the Spoke,
--ip nhrp shortcut and ip nhrp redirect are both requires to the Hub

Reference: http://blog.ine.com/2008/12/23/dmvpn-phase-3/

QUESTION 200
Refer to the exhibit.



```
router eigrp 1
redistribute bgp 1 route-map BGP_DEFAULT_ROUTE_RM
network 2.0.0.0
route-map BGP_DEFAULT_ROUTE_RM PERMIT 10
   match ip address prefix-list DEFAULT_ROUTE_PL
ip prefix-list DEFAULT_ROUTE+PL seq 10 permit 0.0.0.0/0
```

For which reason is EIGRP failing to redistribute the default route?

A. The EIGRP process is missing the no auto-summary command.
B. The EIGRP process is missing the default metric.
C. The route-map statement is missing the match any keyword.
D. The EIGRP process is missing the router ID.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 201
By default, which type of IPv6 address is used to build the EUI-64 bit format?

A. IPv4-compatible IPv6 address
B. aggregatable-local address
C. unique-local address
D. link-local address

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
https://howdoesinternetwork.com/2013/slaac-ipv6-stateless-address-autoconfiguration

QUESTION 202
Which two statements about GRE tunnel interfaces are true? (Choose two.)

A. To establish a tunnel, the source interface must be a loopback.
B. To establish a tunnel, the source interface must be in the up/up state.
C. A tunnel destination must be a physical interface that is in the up/up state.
D. A tunnel can be established when the source interface is in the up/down state.
E. A tunnel destination must be routable, but it can be unreachable.

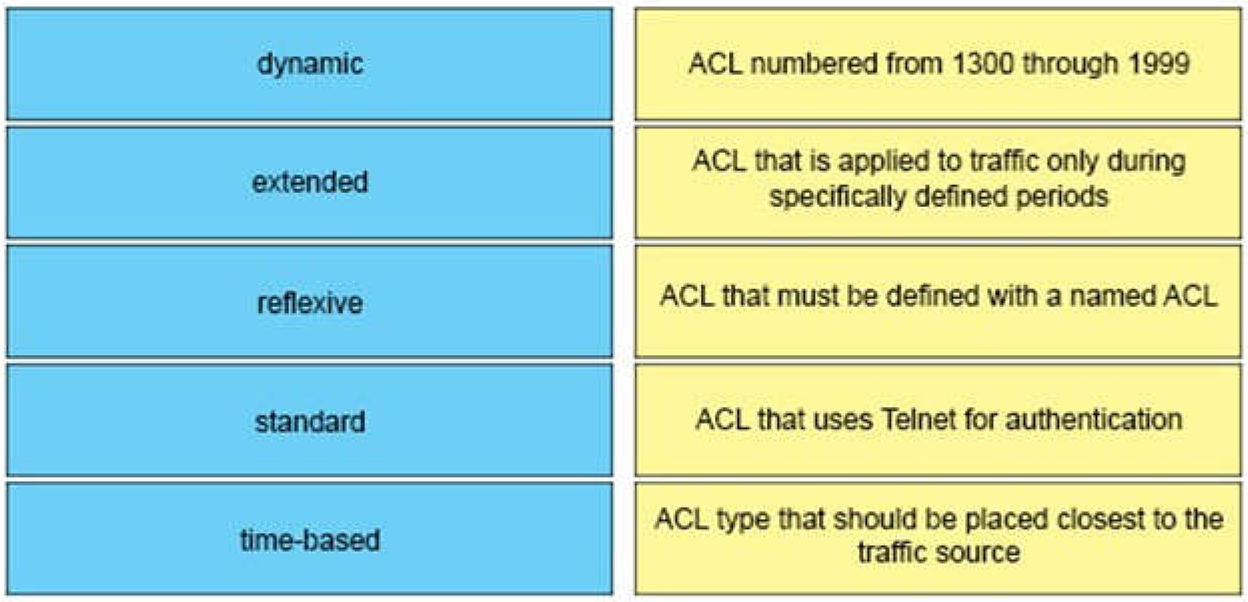
Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html

QUESTION 203
DRAG DROP

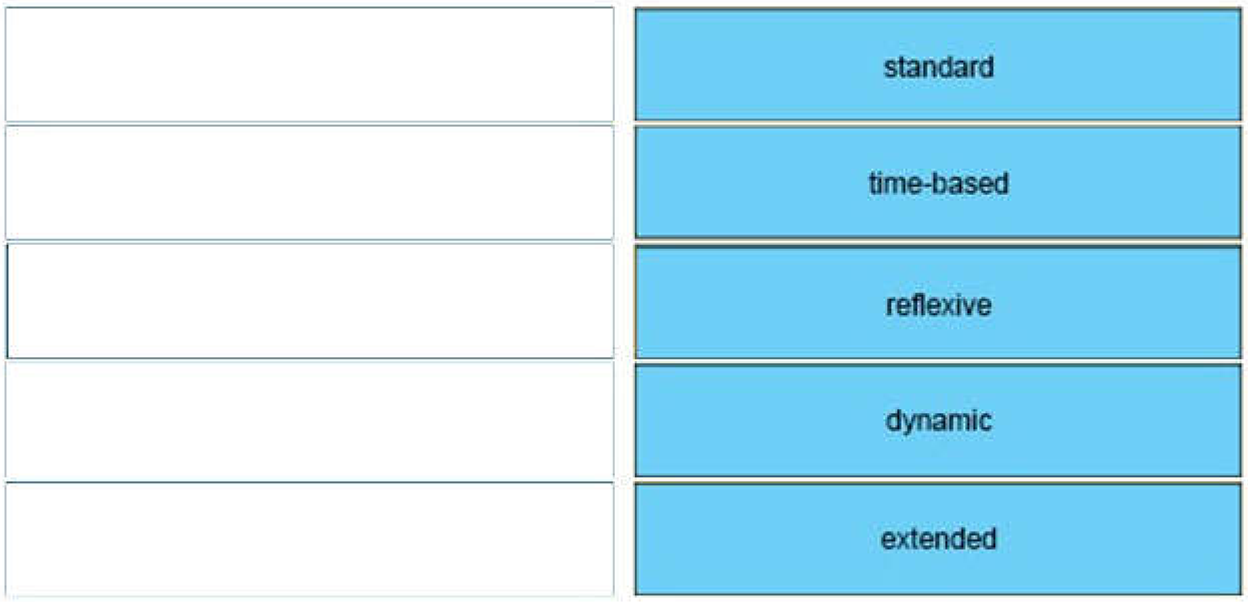
Drag and drop the ACL types from the left onto the correct descriptions on the right.

Select and Place:



dynamic	ACL numbered from 1300 through 1999
extended	ACL that is applied to traffic only during specifically defined periods
reflexive	ACL that must be defined with a named ACL
standard	ACL that uses Telnet for authentication
time-based	ACL type that should be placed closest to the traffic source

Correct Answer:



	standard
	time-based
	reflexive
	dynamic
	extended

Section: Mix Questions

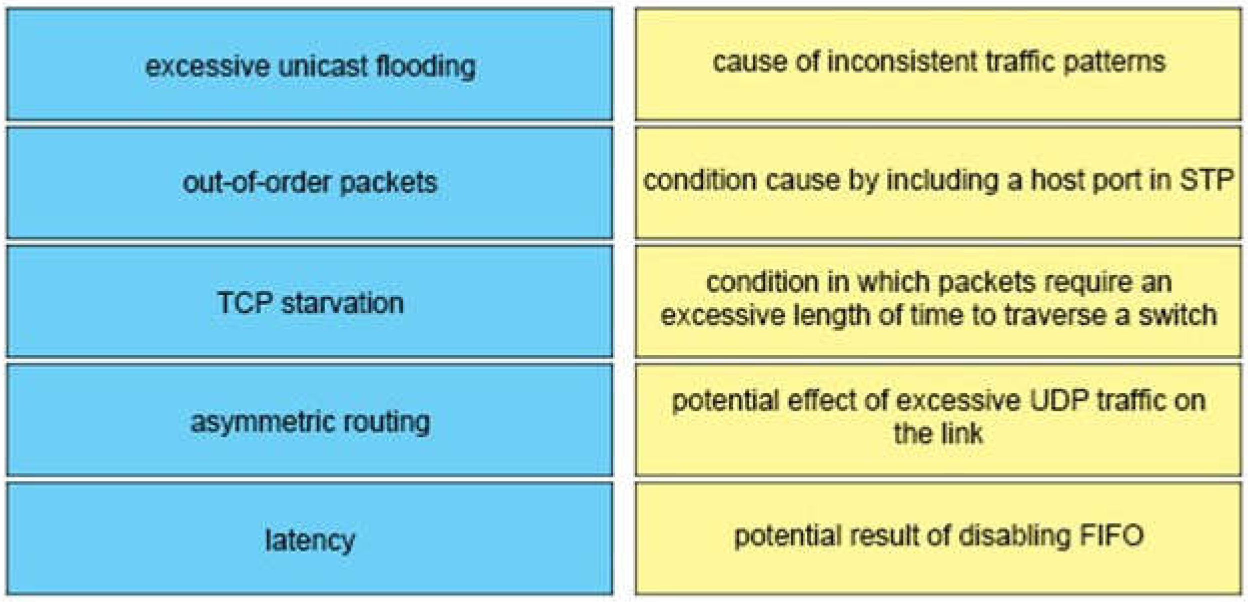
Explanation

Explanation/Reference:

QUESTION 204
DRAG DROP

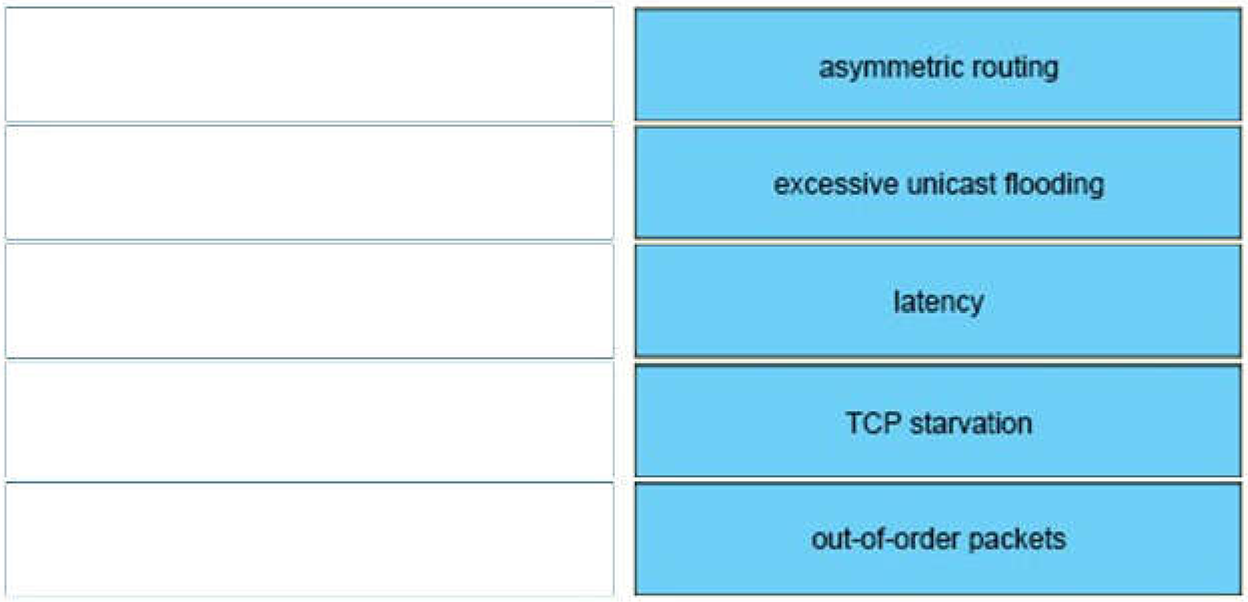
Drag and drop the adverse network conditions from the left onto the correct descriptions on the right.

Select and Place:



excessive unicast flooding	cause of inconsistent traffic patterns
out-of-order packets	condition cause by including a host port in STP
TCP starvation	condition in which packets require an excessive length of time to traverse a switch
asymmetric routing	potential effect of excessive UDP traffic on the link
latency	potential result of disabling FIFO

Correct Answer:



	asymmetric routing
	excessive unicast flooding
	latency
	TCP starvation
	out-of-order packets

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 205
A network engineer executes the commands logging host 172.16.200.225 and logging trap 5. Which action results when these two commands are executed together?

A. Logging messages that have a debugging severity level are sent to the remote server 172.16.200.225.
B. Logged information is stored locally, showing the source as 172.16.200.225.
C. Logging messages that have any severity level are sent to the remote server 172.16.200.225.
D. Logging messages that have a severity level of “notifications” and above (numerically lower) are sent to the remote server 172.16.200.225.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 206
Which problem can be caused by latency on a UDP stream?

A. The device that sends the stream is forced to hold data in the buffer for a longer period of time.
B. The device that receives the stream is forced to hold data in the buffer for a longer period of time.
C. The devices at each end of the stream are forced to negotiate a smaller windows size.
D. The overall throughput of the stream is decreased.

Correct Answer: B

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 207
Which Cisco Express Forwarding components maintains Layer 2 addressing information?

A. adjacency table
B. RIB
C. FIB
D. fast switching

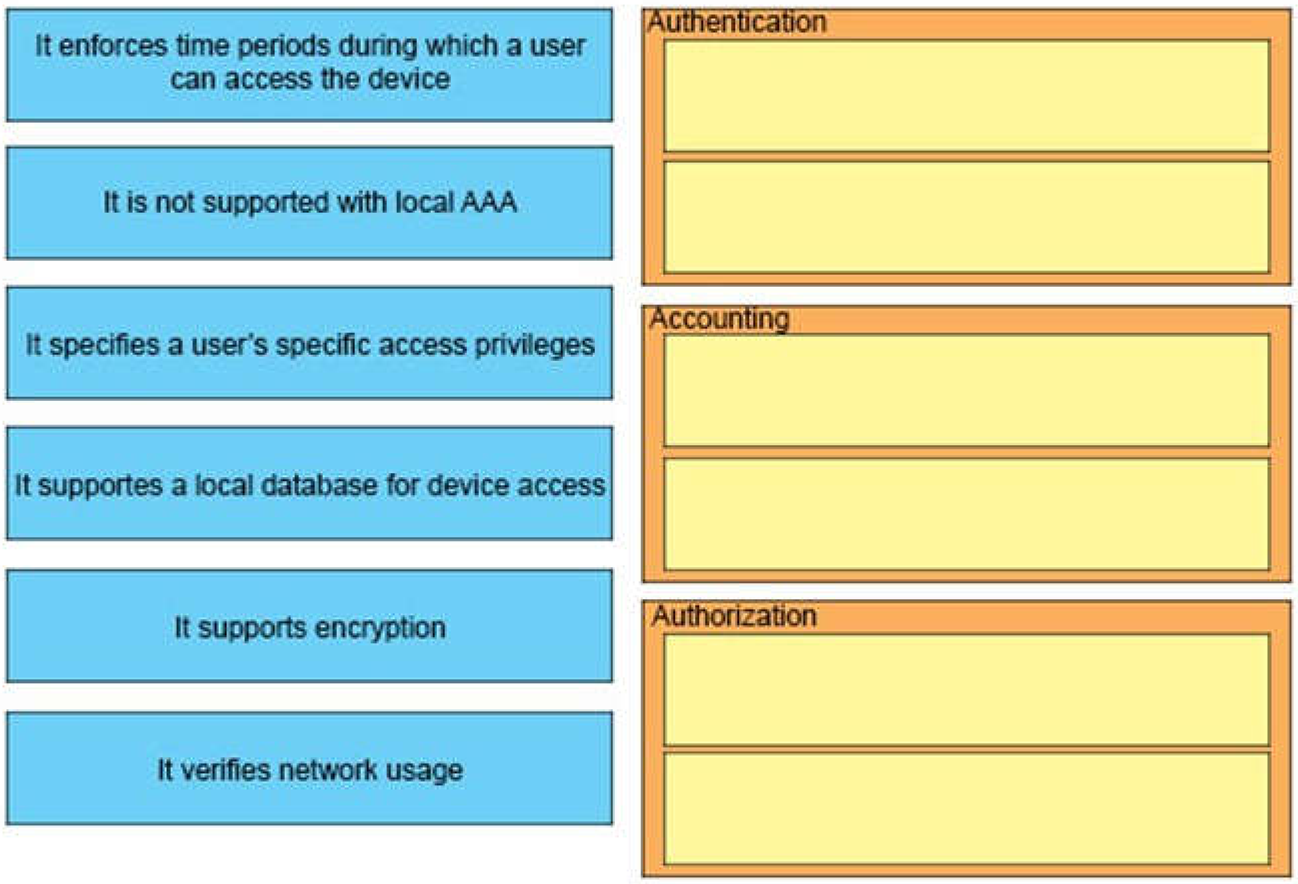
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 208
DRAG DROP

Drag and drop the statements about authentication, authorization and accounting from the left into the correct categories on the right.

Select and Place:



It enforces time periods during which a user can access the device

It is not supported with local AAA

It specifies a user's specific access privileges

It supportes a local database for device access

It supports encryption

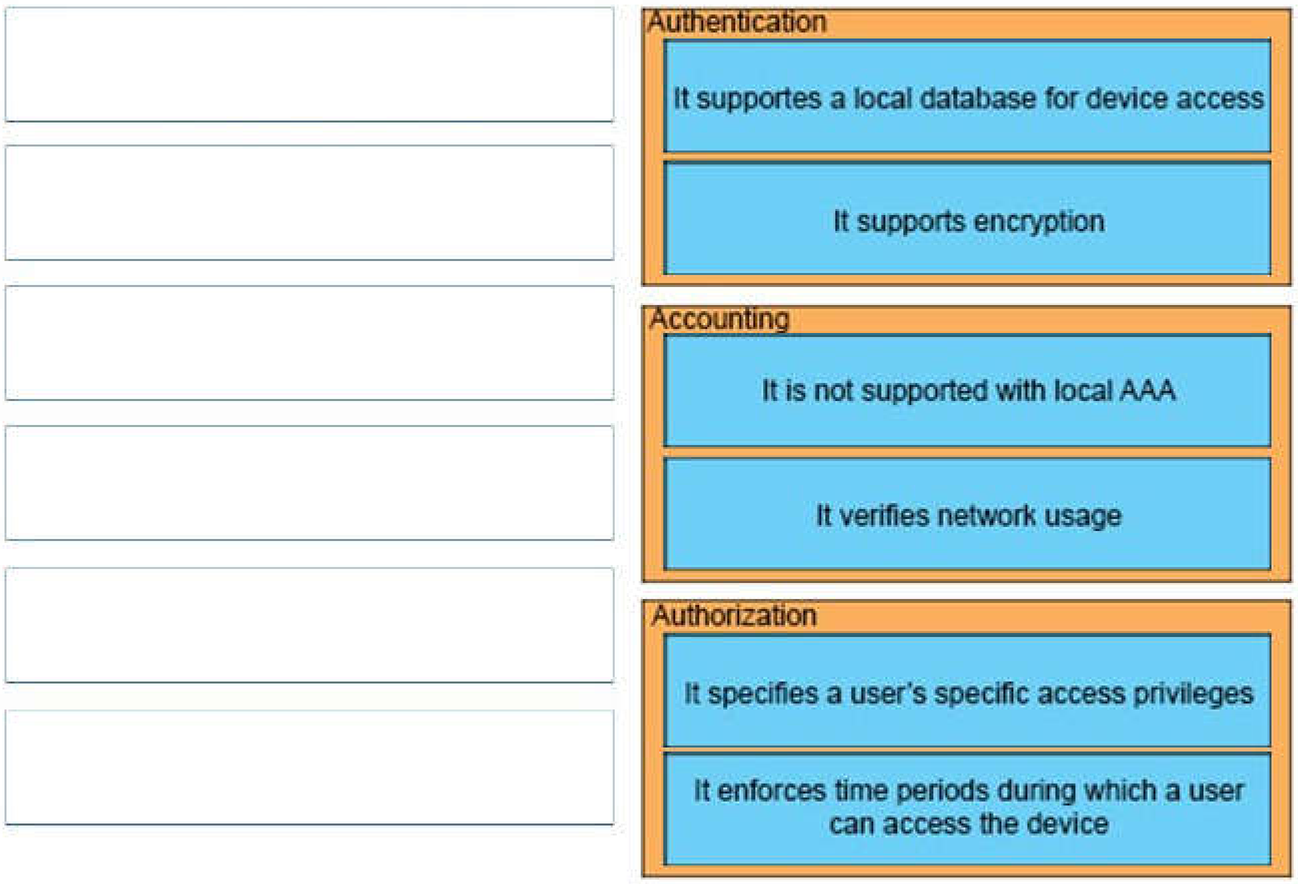
It verifies network usage

Authentication

Accounting

Authorization

Correct Answer:



Authentication

It supportes a local database for device access

It supports encryption

Accounting

It is not supported with local AAA

It verifies network usage

Authorization

It specifies a user's specific access privileges

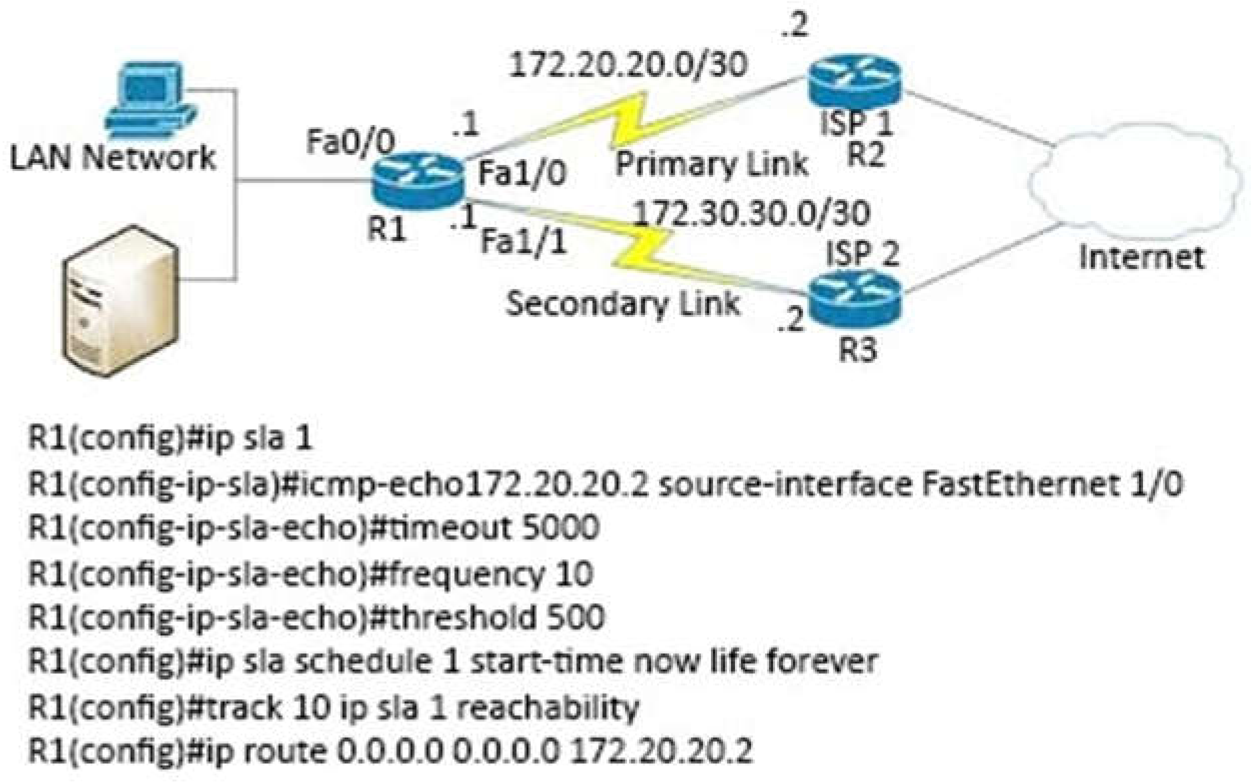
It enforces time periods during which a user can access the device

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

AAA offers different solutions that provide access control to network devices. The following services are included within its modular architectural framework:
+ Authentication – The process of validating users based on their identity and predetermined credentials, such as passwords and other mechanisms like digital certificates. Authentication controls access by requiring valid user credentials, which are typically a username and password. With RADIUS, the ASA supports PAP, CHAP, MS-CHAP1, MS-CHAP2, that means Authentication supports encryption.
+ Authorization – The method by which a network device assembles a set of attributes that regulates what tasks the user is authorized to perform. These attributes are measured against a user database. The results are returned to the network device to determine the user's qualifications and restrictions. This database can be located locally on Cisco ASA or it can be hosted on a RADIUS or Terminal Access Controller Access-Control System Plus (TACACS+) server. In summary, Authorization controls access per user after users authenticate.
+ Accounting – The process of gathering and sending user information to an AAA server used to track login times (when the user logged in and logged off) and the services that users access. This information can be used for billing, auditing, and reporting purposes.

QUESTION 209
Refer to the exhibit.



```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo172.20.20.2 source-interface FastEthernet 1/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

Why is the default route not removed when 172.20.20.2 stops replying to ICMP echos?

A. The source-interface is configured incorrectly.
B. The default route is missing the track feature.
C. The destination must be 172.30.30.2 for icmp-echo.
D. The threshold value is wrong.

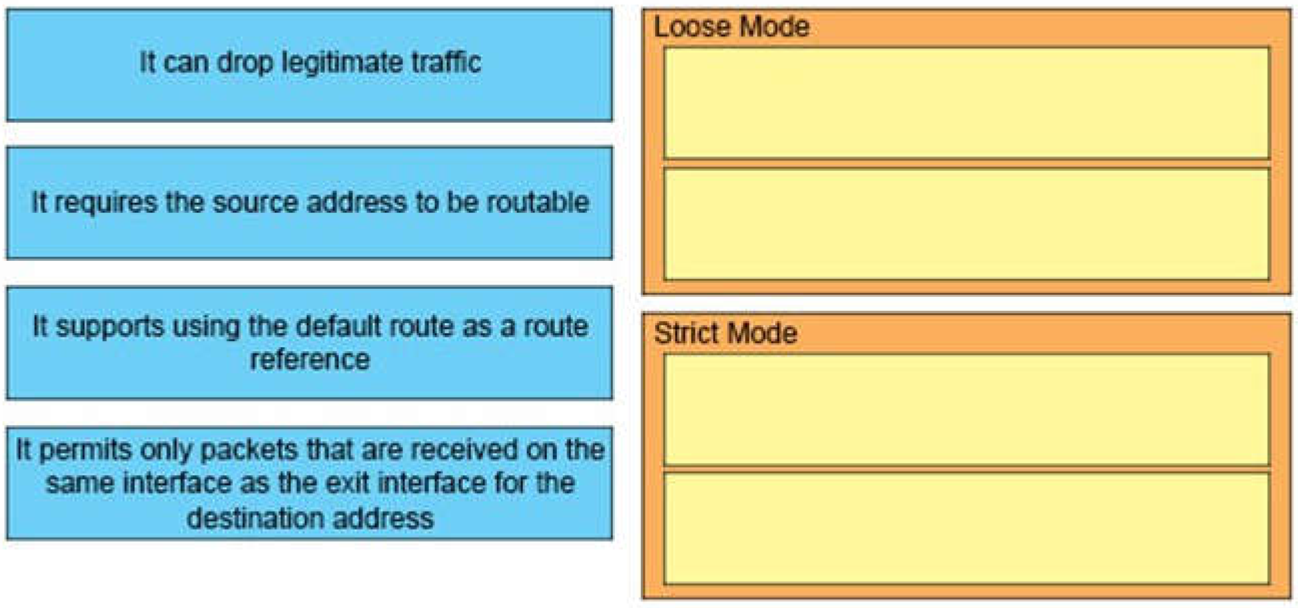
Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 210
DRAG DROP

Drag and drop the statements from the left onto the correct uRPF modes on the right.

Select and Place:



It can drop legitimate traffic

It requires the source address to be routable

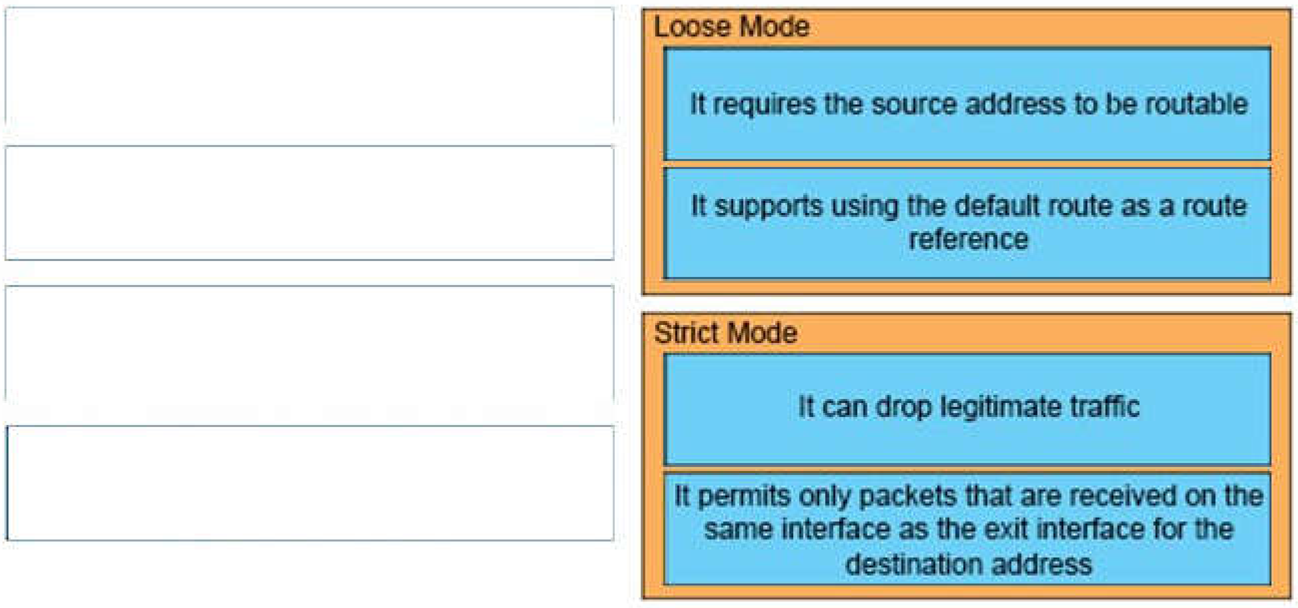
It supports using the default route as a route reference

It permits only packets that are received on the same interface as the exit interface for the destination address

Loose Mode

Strict Mode

Correct Answer:



Loose Mode

It requires the source address to be routable

It supports using the default route as a route reference

Strict Mode

It can drop legitimate traffic

It permits only packets that are received on the same interface as the exit interface for the destination address

Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

QUESTION 211
In which scenario can asymmetric routing occur?

A. active/active firewall setup
B. redundant routers running VRRP
C. active/standby firewall setup
D. single path in and out of the network

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
What is Asymmetric Routing?
In Asymmetric routing, a packet traverses from a source to a destination in one path and takes a different path when it returns to the source. This is commonly seen in Layer-3 routed networks.

Asymmetric routing is when a packet returns on a patch that is different from a path that the traffic was sent. This can be seen in normal situations when there are multiple paths to/from a destination. It can also be seen in misconfiguration situations such as a server having two NIC's for load balancing and it's instead routing between them.

QUESTION 212
Which feature can mitigate fragmentation issues within network segments that are between GRE endpoints?

A. TCP Flow Control

B. TCP MSS
C. PMTU
D. ICMP DF bit

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 213
After reviewing the EVN configuration, a network administrator notices that a predefined EVN, which is known as “vnet global”, was configured. What is the purpose of this EVN?

A. It aggregates and carries all dot1qtagged traffic.
B. It refers to the global routing context and corresponds to the default RIB.
C. It safeguards the virtual network that is preconfigured to avoid mismatched routing instances.
D. It defines the routing scope for each particular EVN edge interface.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.html

QUESTION 214
Which two debug commands can you use to view issues with CHAP and PAP authentication? (Choose two.)

A. debug radius
B. debug tacacs
C. debug aaa authentication
D. debug ppp negotiation
E. debug ppp authentication

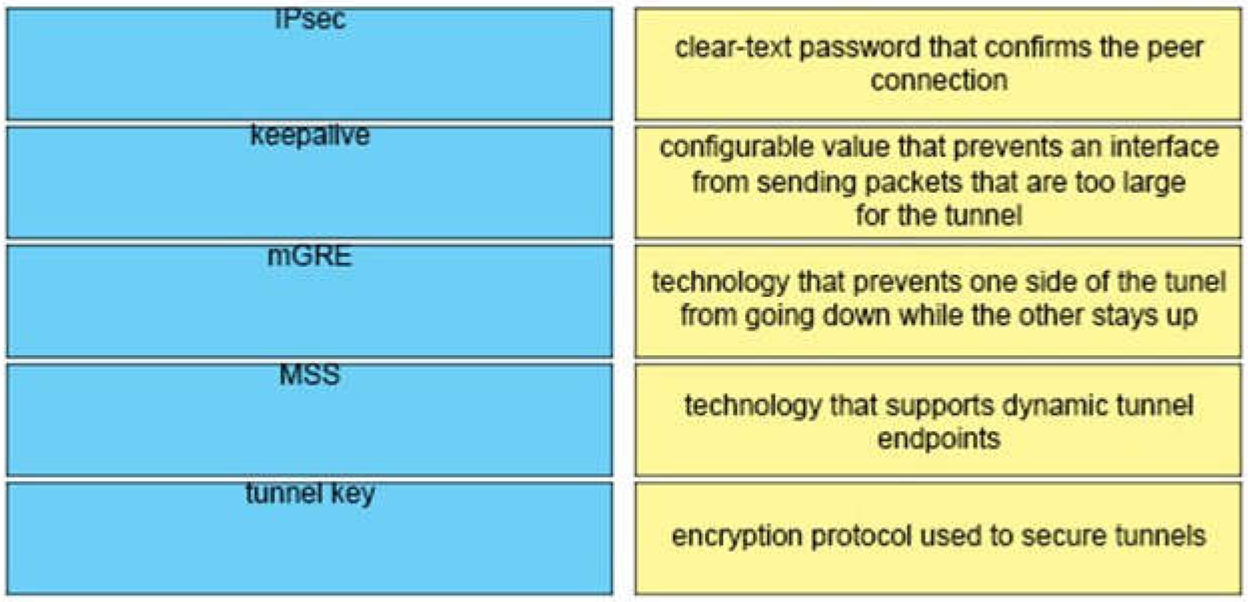
Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Reference:
http://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

QUESTION 215
DRAG DROP

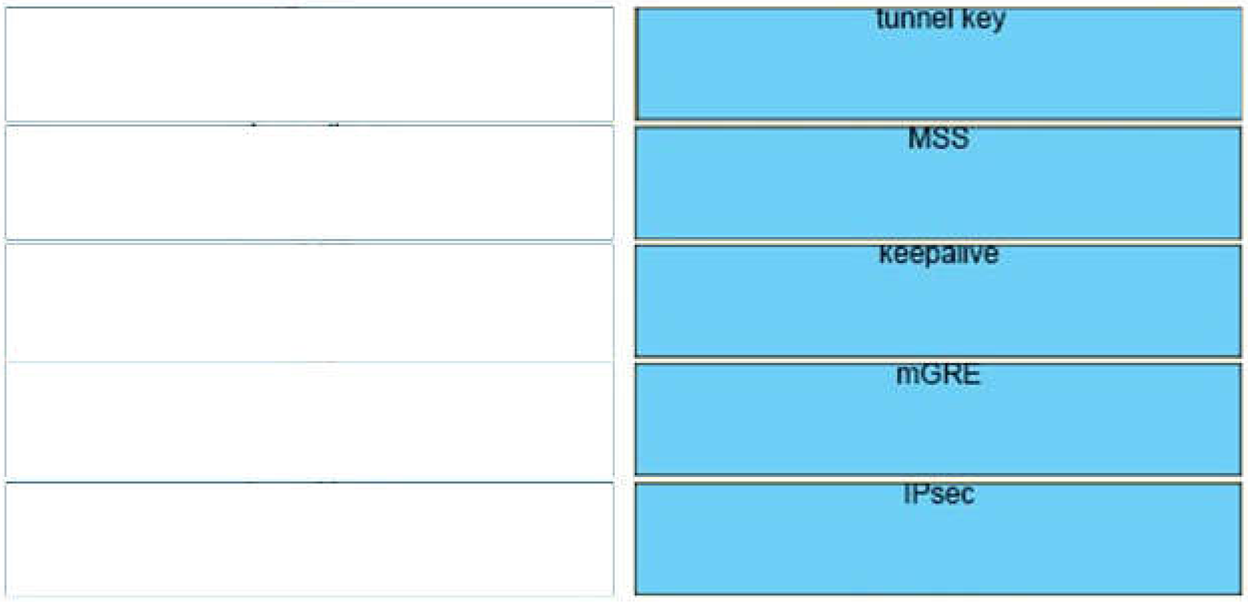
Drag and drop the GRE features from the left onto the correct descriptions on the right.

Select and Place:



IPsec	clear-text password that confirms the peer connection
keepalive	configurable value that prevents an interface from sending packets that are too large for the tunnel
mGRE	technology that prevents one side of the tunel from going down while the other stays up
MSS	technology that supports dynamic tunnel endpoints
tunnel key	encryption protocol used to secure tunnels

Correct Answer:



tunnel key

MSS

keepalive

mGRE

IPsec

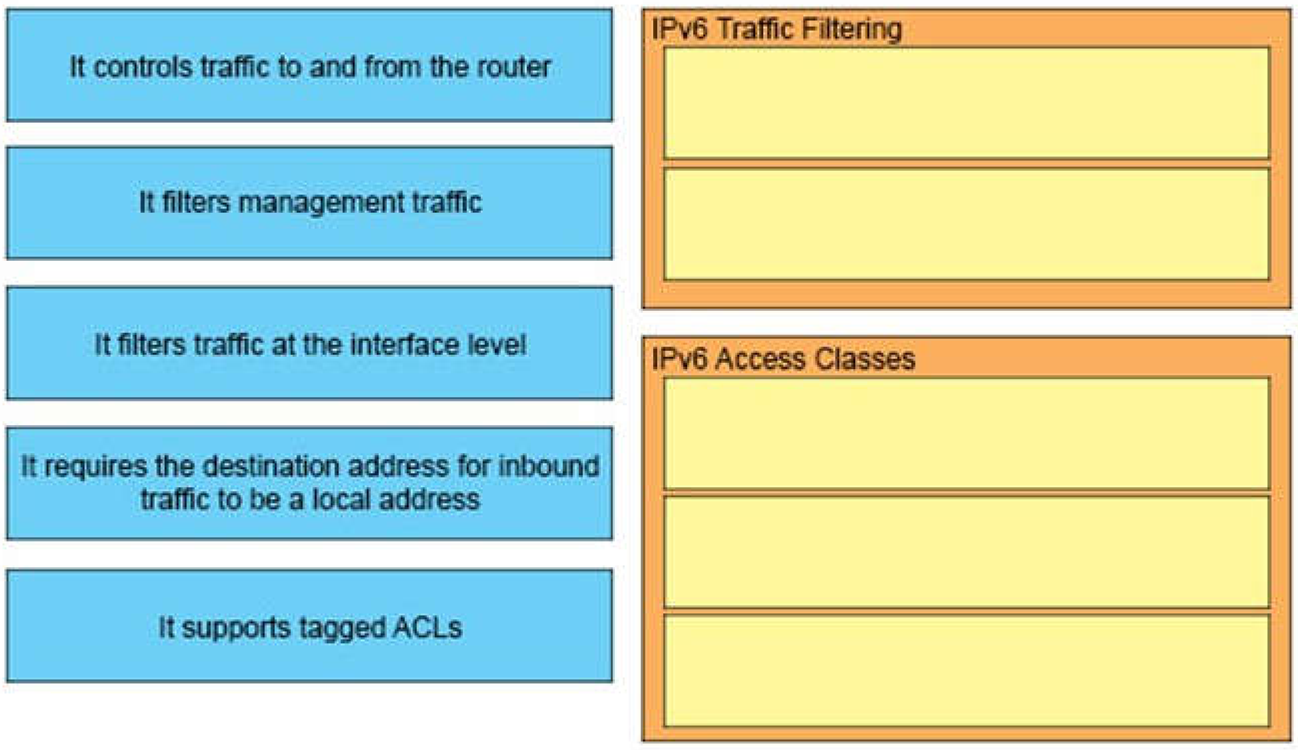
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 216
DRAG DROP

Drag and drop the statements from the left onto the correct IPv6 router security features on the right.

Select and Place:



It controls traffic to and from the router

It filters management traffic

It filters traffic at the interface level

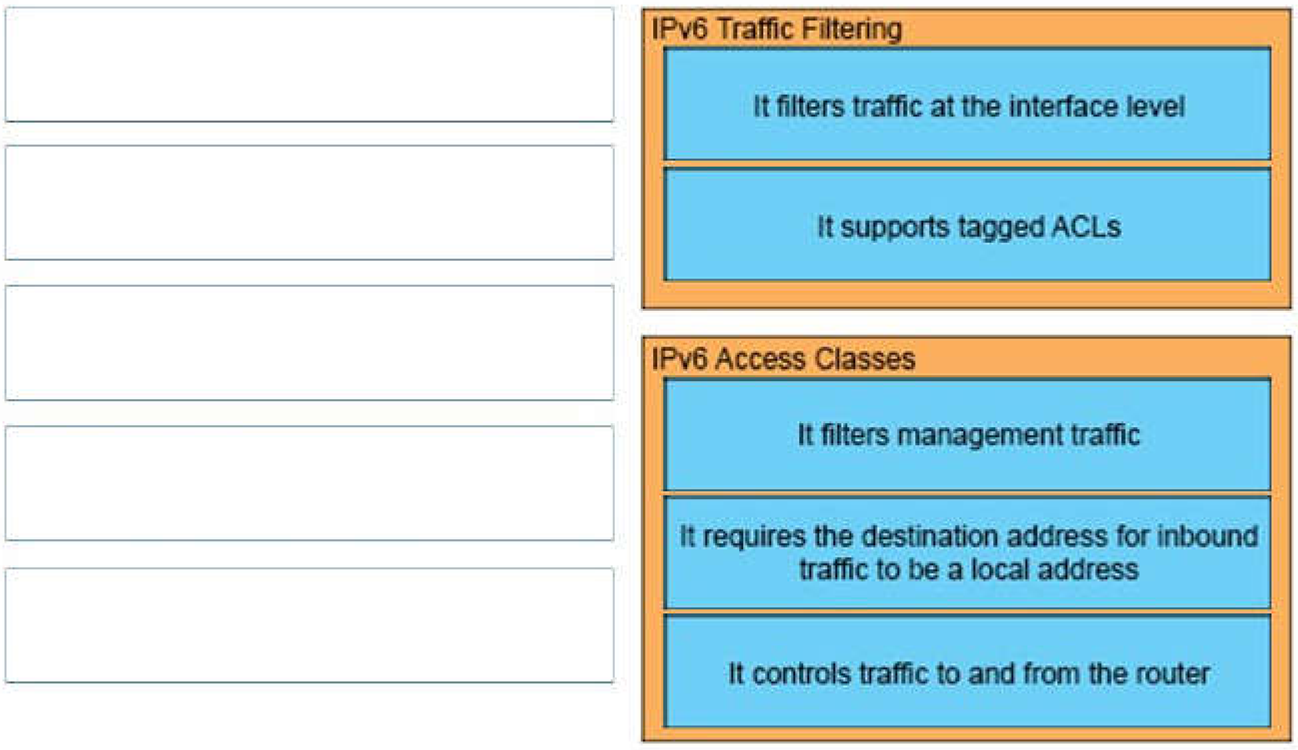
It requires the destination address for inbound traffic to be a local address

It supports tagged ACLs

IPv6 Traffic Filtering

IPv6 Access Classes

Correct Answer:



IPv6 Traffic Filtering

It filters traffic at the interface level

It supports tagged ACLs

IPv6 Access Classes

It filters management traffic

It requires the destination address for inbound traffic to be a local address

It controls traffic to and from the router

Section: Mix Questions

Explanation

Explanation/Reference:

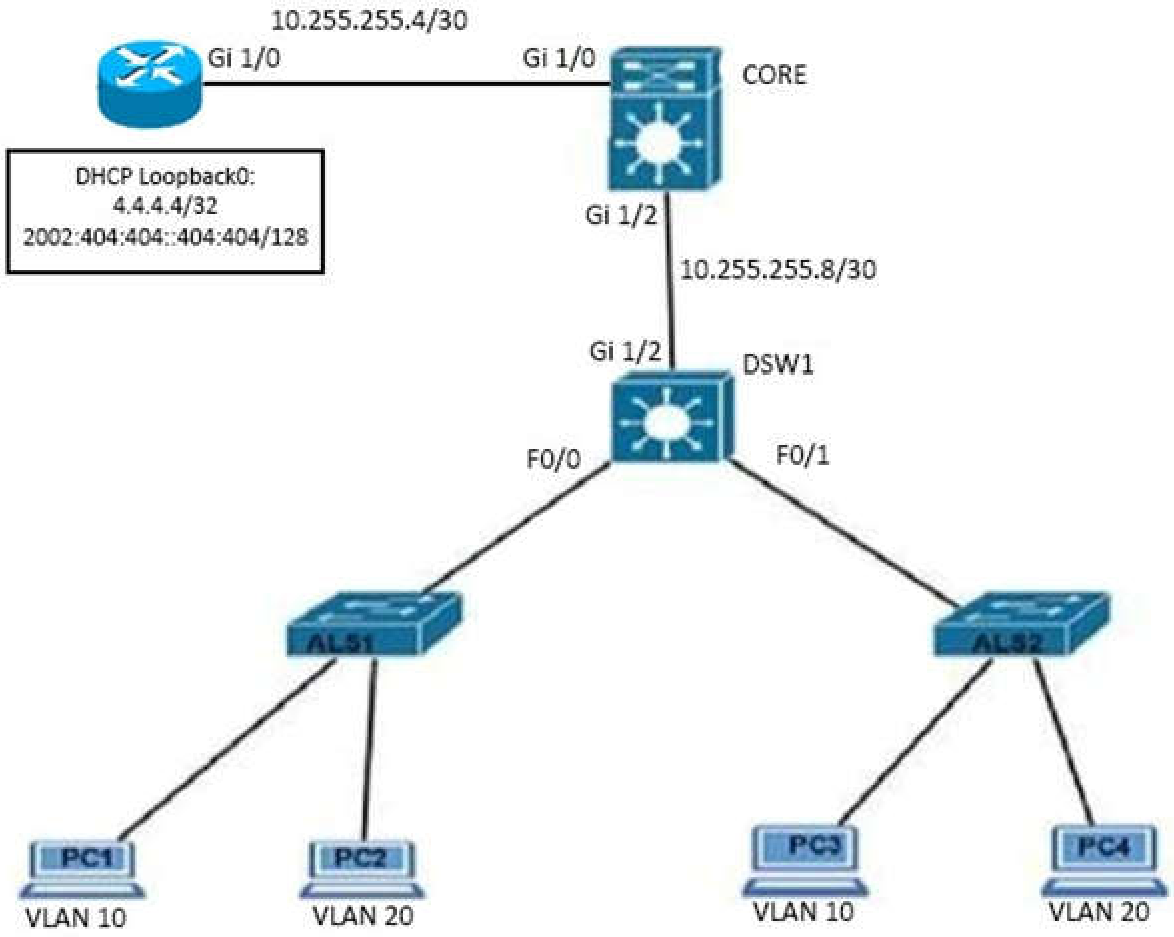
QUESTION 217
Which option is the minimum privilege level that allows the user to execute all user-level commands but prohibits enable-level commands by default?

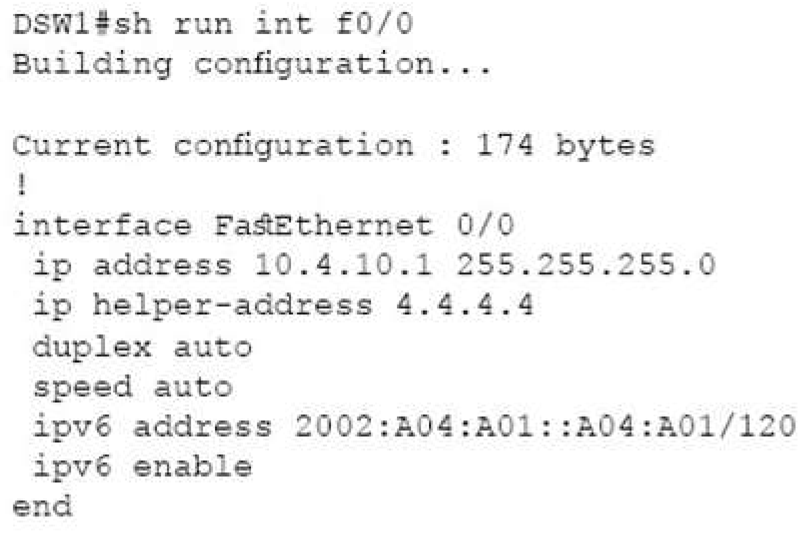
A. level 0
B. level 1
C. level 14
D. level 15
E. level 16

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/terminal-access-controller-access-control-system-tacacs-/23383-showrun.html#priv

QUESTION 218





```
DSW1#sh run int f0/0
Building configuration...

Current configuration : 174 bytes
!
interface FastEthernet 0/0
 ip address 10.4.10.1 255.255.255.0
 ip helper-address 4.4.4.4
 duplex auto
 speed auto
 ipv6 address 2002:A04:A01::A04:A01/120
 ipv6 enable
end
```

Refer to the exhibit. Router DHCP is configured to lease IPv4 and IPv6 addresses to clients on ALS1 and ALS2. Clients on ALS2 receive IPv4 and IPv6 addresses. Clients on ALS1 receive IPv4 addresses. Which configuration on DSW1 allows clients on ALS1 to receive IPv6 addresses?

A. DSW1(config-if)# ipv6 dhcp relay destination2002:404:404::404:404 GigabitEthernet1/2
B. DSW1(config-if)# ipv6 helper address 2002:404:404::404:404
C. DSW1(config)# ipv6 route 2002:404:404::404:404/128 FastEthernet1/0
D. DSW1(dhcp-config)# default-router 2002:A04:A01::A04:A01

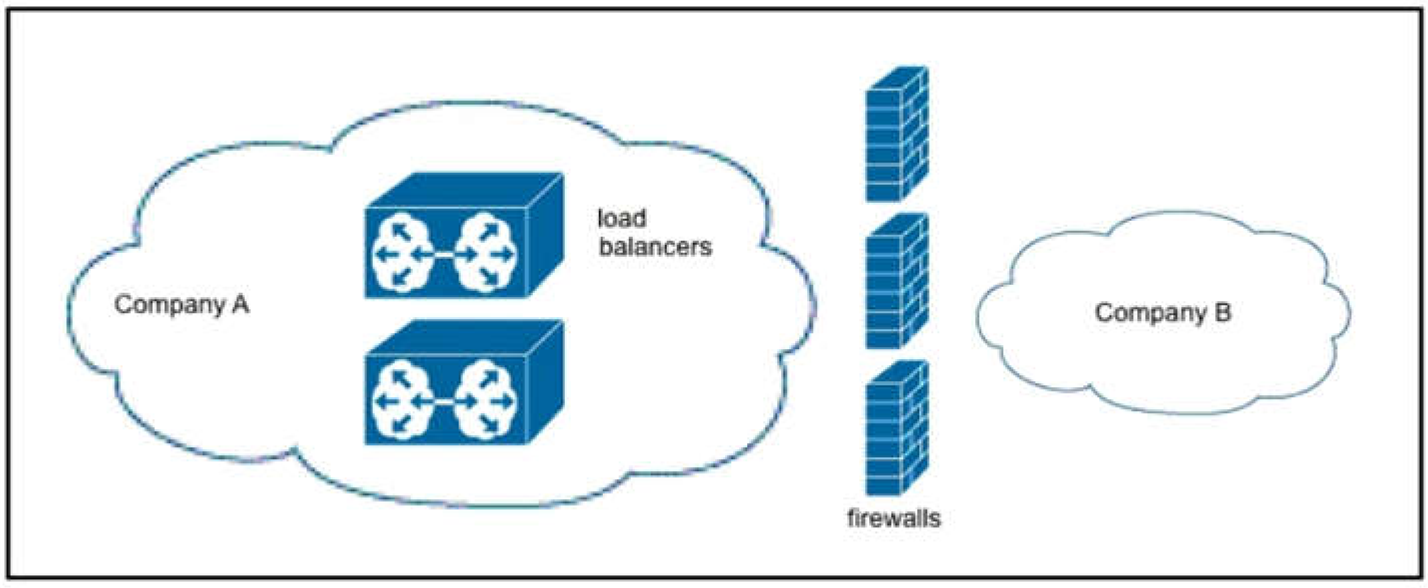
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Specifies a destination address to which client packets are forwarded and enables DHCPv6 relay service on the interface.

ipv6 dhcp relay destination ipv6-address[interface-type interface-number]

Example:
Router(config-if) ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 ethernet 4/3

QUESTION 219



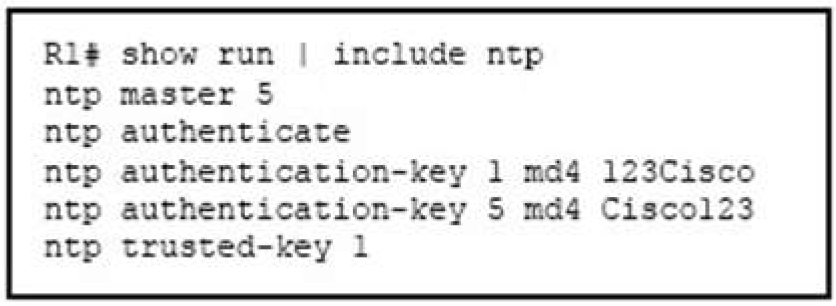
Refer to the exhibit. Which networking challenge is the most important issue to address to enable optimal communication between the networks at company A and company B?

A. IPv4 fragmentation
B. asymmetric routing
C. unicast flooding
D. UDP latency
E. IPV4 MTU

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 220



```
R1# show run | include ntp
ntp master 5
ntp authenticate
ntp authentication-key 1 md4 123Cisco
ntp authentication-key 5 md4 Cisco123
ntp trusted-key 1
```

Refer to the exhibit. Which effect of this configuration is true?

A. R1 acts as an authoritative clock at stratum 5.
B. R1 acts as an authoritative clock with a priority ID of 1.
C. R1 synchronizes with systems that include authentication key 5 in their packets.
D. R1 is the NTP client for a stratum 1 server.

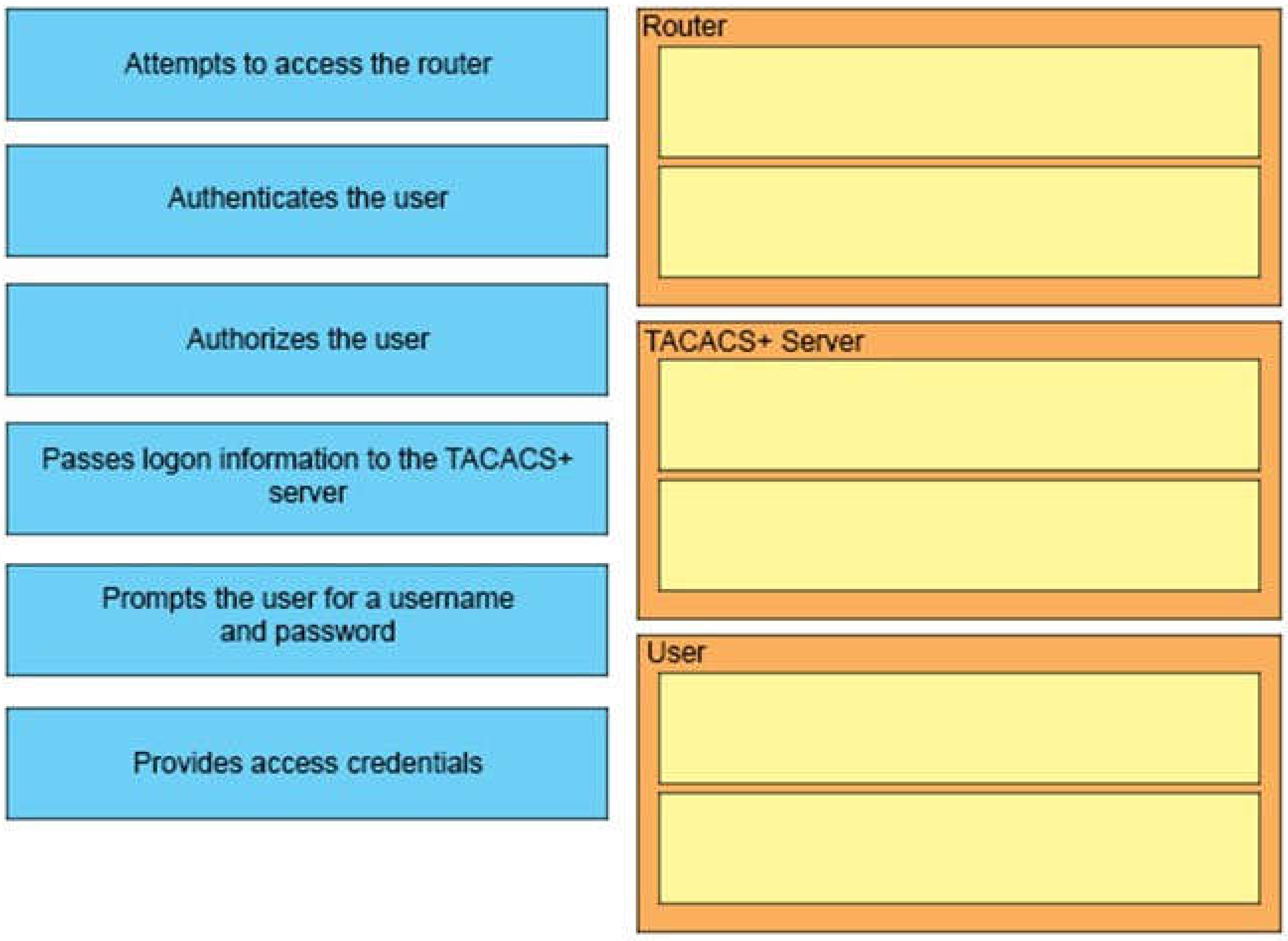
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 221
DRAG DROP

Drag and drop the steps in the TACACS+ authentication process from the left onto the actors that perform them on the right.

Select and Place:



Attempts to access the router

Authenticates the user

Authorizes the user

Passes logon information to the TACACS+ server

Prompts the user for a username and password

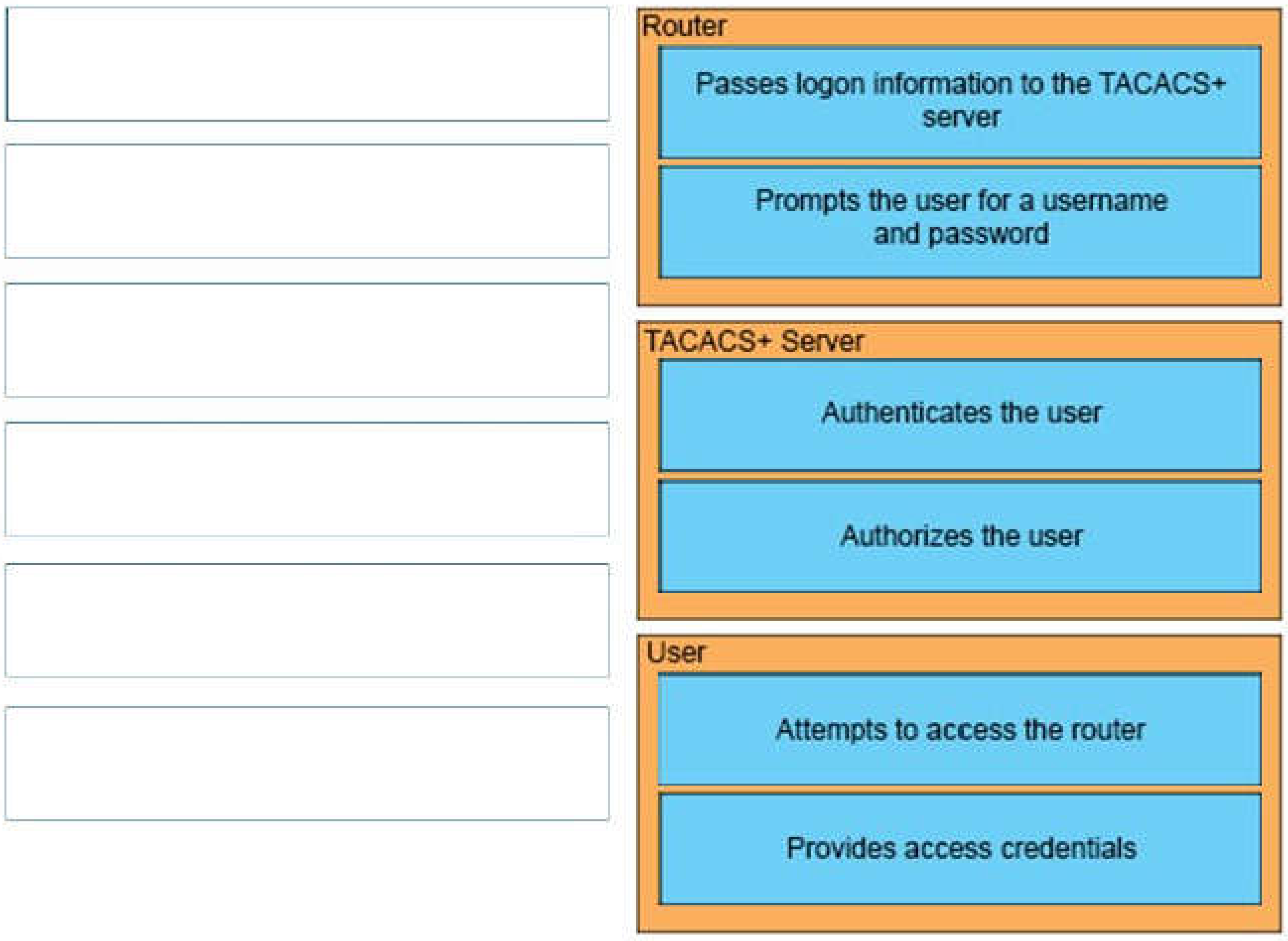
Provides access credentials

Router

TACACS+ Server

User

Correct Answer:



Router

- Passes logon information to the TACACS+ server
- Prompts the user for a username and password

TACACS+ Server

- Authenticates the user
- Authorizes the user

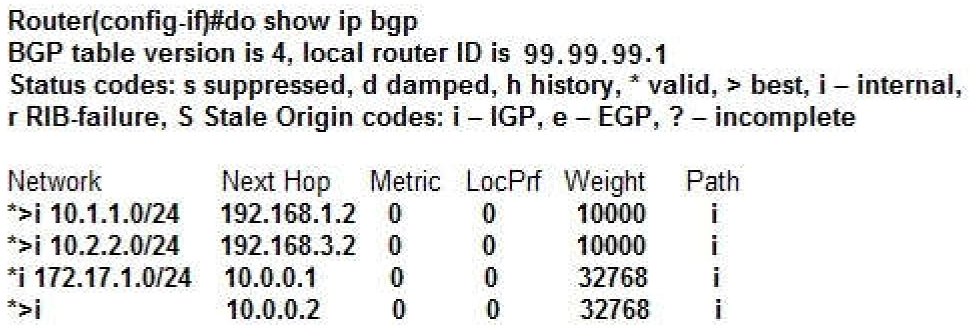
User

- Attempts to access the router
- Provides access credentials

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 222
Which next hop is going to be used for 172.17.1.0/24 ?



```
Router(config-if)#do show ip bgp
BGP table version is 4, local router ID is 99.99.99.1
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal,
r RIB-failure, S Stale Origin codes: i – IGP, e – EGP, ? – incomplete

Network          Next Hop     Metric  LocPrf  Weight   Path
*>i 10.1.1.0/24  192.168.1.2   0       0      10000     i
*>i 10.2.2.0/24  192.168.3.2   0       0      10000     i
*i 172.17.1.0/24  10.0.0.1     0       0      32768     i
*>i               10.0.0.2     0       0      32768     i
```

A. 10.0.0.1
B. 192.168.1.2
C. 10.0.0.2
D. 192.168.3.2

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The > indicates the best route to the destination 172.17.1.0/24
Reference: https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp5.html#wp1156281

QUESTION 223
Which two OSPF router types can perform summarization in an OSPF network? (Choose two.)

A. autonomous system boundary router
B. backbone router
C. internal router
D. summary router
E. area border router

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 224
Which option is the minimum logging level that displays a log message when an ACL drops an incoming packet?

A. Level 5
B. Level 7
C. Level 3
D. Level 6

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

When the ACL logging feature is configured, the system monitors ACL flows and logs dropped packets and statistics for each flow that matches the deny conditions of the ACL entry.

The log and log-input options apply to an individual ACE and cause packets that match the ACE to be logged.
The sample below illustrates the initial message and periodic updates sent by an IOS device with a default configuration using the log ACE option.

```
*May 1 22:12:13.243: %SEC-6-IPACCESSLOGP: list ACL-IPv4-E0/0-IN permitted tcp 192.168.1.3(1024) -> 192.168.2.1(22), 1 packet
```

From the example above we can see when an ACL drops a packet, it generates a level 6 Syslog (%SEC-6-)

Reference: https://www.cisco.com/c/en/us/about/security-center/access-control-list-logging.html

QUESTION 225
Which condition can cause unicast reverse path forwarding to fail?

A. PortFast security violation
B. split horizon
C. asymmetric routing
D. STP convergence

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.

https://www.cisco.com/c/en/us/about/security-center/unicast-reverse-path-forwarding.html

QUESTION 226
Which two protocols can be affected by MPP? (Choose two.)

A. HTTP
B. POP
C. SFTP
D. SSH

E. SMTP

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Examples of protocols processed in the management plane are **Simple Network Management Protocol (SNMP), Telnet, HTTP, Secure HTTP (HTTPS), and SSH**. These management protocols are used for monitoring and for CLI access. Restricting access to devices to internal sources (trusted networks) is critical.

The Management Plane Protection (MPP) feature in Cisco IOS software provides the capability to restrict the interfaces on which network management packets are allowed to enter a device. The MPP feature allows a network operator to designate one or more router interfaces as management interfaces. Device management traffic is permitted to enter a device only through these management interfaces. After MPP is enabled, no interfaces except designated management interfaces will accept network management traffic destined to the device.

Restricting management packets to designated interfaces provides greater control over management of a device, providing more security for that device. Other benefits include improved performance for data packets on nonmanagement interfaces, support for network scalability, need for fewer access control lists (ACLs) to restrict access to a device, and management packet floods on switching and routing interfaces are prevented from reaching the CPU.

QUESTION 227
How does an EVN provide end-to-end virtualization and separation for data traffic from multiple networks?

A. It tags traffic with an 802.1q tag at the trunk interface.
B. It tags traffic with a virtual network tag at the edge interface.
C. It tags traffic with an 802.1q tag at the edge interface.
D. It tags traffic with a virtual network tag at the trunk interface.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 228
When a packet is denied by an IPv6 traffic filter, which additional action does the device perform?

A. It scans the rest of the ACL for a **permit** entry matching the destination.
B. It generates an ICMP unreachable message for the frame.
C. It generates a TCP Fin bit and sends it to the source.
D. A creates a null route for the destination and adds it to the route table.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 229
Which two features does RADIUS combine? (Choose two.)

A. SSH
B. authorization
C. Telnet
D. authentication
E. accounting

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 230
After testing various dynamic IPv6 address assignment methods, an engineer decides that more control is needed when distributing addresses to clients. Which two advantages does DHCPv6 have over EUI-64? (Choose two.)

A. DHCPv6 requires less planning and configuration than EUI-64 requires.
B. DHCPv6 does not require the configuration of prefix pools.
C. DHCPv6 provides tighter control over the IPv6 addresses that are distributed to clients.
D. DHCPv6 does not require neighbor and router discovery on the network segment.
E. DHCPv6 allows for additional parameters to be sent to the client, such as the domain name and DNS server.

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 231
What does stateful NAT64 do that stateless NAT64 does not do?

A. Stateful NAT64 maintains bindings or session state while performing translation
B. Stateful NAT64 maintains bindings of IPv4 to IPv6 link-local addresses
C. Stateful NAT64 translates IPv4 to IPv6
D. Stateful NAT64 translates IPv6 to IPv4

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676278.html

QUESTION 232
Which version or versions of NetFlow support MPLS?

A. NetFlow version 9
B. NetFlow version 8
C. all versions of NetFlow
D. NetFlow versions 8 and 9
E. NetFlow version 5

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
MPLS-aware NetFlow uses the NetFlow Version 9 export format. MPLS-aware NetFlow exports up to three labels of interest from the incoming label stack, the IP address associated with the top label, as well as traditional NetFlow data.

Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fsmnf24.html

QUESTION 233
A network engineer needs to verify IP SLA operations on an interface that shows an indication of excessive traffic. Which command should the engineer use to complete this action?

A. show reachability
B. show threshold
C. show frequency
D. show track

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 234
Which value does a Cisco router use as its default username for CHAP authentication?

A. ppp
B. its own hostname
C. cisco
D. chap

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:
https://www.cisco.com/c/en/us/support/docs/wan/point-to-point-protocol-ppp/25647-understanding-ppp-chap.html

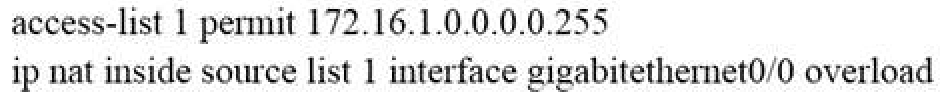
QUESTION 235
A network engineer wants an NTP client to be able to update the local system without updating or synchronizing with the remote system. Which option for the **ntp access-group** command is needed to accomplish this?

A. peer
B. query-only
C. serve-only
D. serve

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 236
Refer to the exhibit. You have correctly identified the inside and outside interfaces in the NAT configuration of this device. Which effect of this configuration is true?



```
access-list 1 permit 172.16.1.0.0.0.0.255
ip nat inside source list 1 interface gigabitethernet0/0 overload
```

A. NAT64
B. dynamic NAT
C. PAT
D. static NAT

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 237
The Neighbor Discovery Protocol in ipv6 is replaced with which discovery protocol in ipv4?

A. ARP
B. ICMP
C. UDP
D. TCP
E. RFC

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Neighbor Discovery -- or ND -- is the protocol used by IPv6 to determine neighboring hosts, and will replace ARP which was used in IPv4. It will perform similar tasks of the Address Resolution Protocol (ARP) and ICMP Router Discovery Protocol. It's purpose remains to get the MAC/Link Layer addresses of available hosts, and the connection information of available routers in the network.

QUESTION 238
Fill in the Blank.
How to minimize Unicast flooding?
____

Correct Answer: By decreasing the ARP time compared to CAM table time
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 239
Which two protocols can cause TCP starvation? (Choose two)

A. TFTP
B. SNMP
C. SMTP
D. HTTPS
E. FTP

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation: TFTP (69) and SNMP (161) are UDP protocols

QUESTION 240
What is the international standard for transmitting data over a cable system?

A. PPPoE
B. DOCSIS
C. CMTS
D. AAL5

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 241
You have a router that has some interfaces configured with 10Gbps and 1Gbps interfaces. Which command you use to optimize higher bandwidth?

A. auto-cost reference-bandwidth 10000
B. auto-cost reference-bandwidth 1000
C. auto-cost reference-bandwidth 100

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 242
The company network is in the process of migrating the IP address scheme to use IPv6. Which of the following address types are associated with IPv6? (Select three)

A. Unicast
B. Private
C. Broadcast
D. Public
E. Multicast
F. Anycast

Correct Answer: AEF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 243
ALWAYS block the outbound web traffic on Saturdays and Sunday between 1:00 to 23:59

A. periodic Saturday Sunday 01:00 to 23:59 and IN
B. periodic Saturday Sunday 01:00 to 23:59 and OUT
C. periodic Saturday Sunday 01:00 to 11:59 and IN
D. Absolute Saturday Sunday 01:00 to 11:59 and IN

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 244
What is IPv6 router solicitation?

A. A request made by a node to join a specified multicast group
B. A request made by a node for its IP address
C. A request made by a node for the IP address of the DHCP server
D. A request made by a node for the IP address of the local router

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 245
What is the default value of TCP maximum segment size?

A. 536
B. 1492
C. 1500
D. 1508
E. 3340
F. 4096

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
THE TCP MAXIMUM SEGMENT SIZE IS THE IP MAXIMUM DATAGRAM SIZE MINUS FORTY.
The default IP Maximum Datagram Size is 576.
The default TCP Maximum Segment Size is 536.
http://www.ietf.org/rfc/rfc879.txt?referring_site=bodynav

QUESTION 246
Congestion in the network. What is the effect on UDP?

A. Sender will have to buffer more data.
B. Receiver will have to buffer more data before sending packets to higher layers
C. There will be latency.

Correct Answer: C

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 247
If routers in a single area are configured with the same priority value, what value does a router use for the OSPF Router ID in the absence of a loopback interface?

A. The lowest IP address of any physical interface
B. The highest IP address of any physical interface
C. The lowest IP address of any logical interface
D. The highest IP address of any logical interface

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

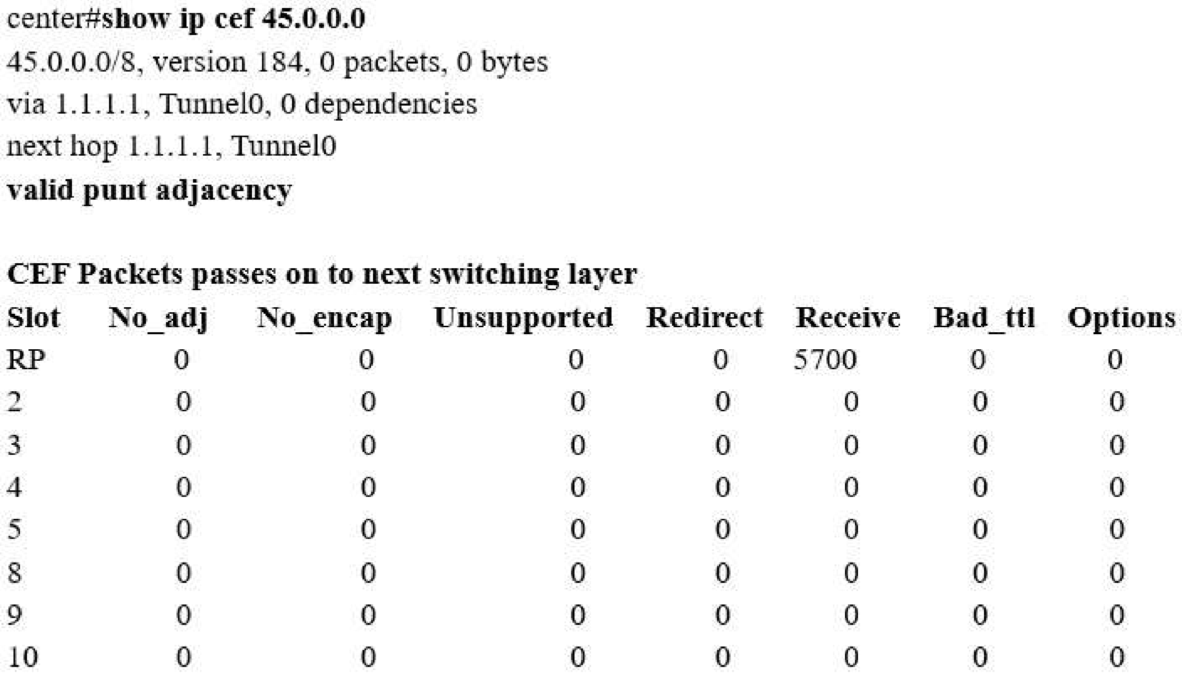
QUESTION 248
Which security feature can you enable to control access to the vty lines on a router?

A. Exec-time out
B. Logging
C. Username and password
D. Transport output

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 249
Refer to exhibit. What is indicated by the show ip cef command for an address?



```
center#show ip cef 45.0.0.0
45.0.0.0/8, version 184, 0 packets, 0 bytes
via 1.1.1.1, Tunnel0, 0 dependencies
next hop 1.1.1.1, Tunnel0
valid punt adjacency

CEF Packets passes on to next switching layer
Slot  No_adj  No_encap  Unsupported  Redirect  Receive  Bad_ttl  Options
RP       0        0          0           0       5700      0        0
2        0        0          0           0          0      0        0
3        0        0          0           0          0      0        0
4        0        0          0           0          0      0        0
5        0        0          0           0          0      0        0
8        0        0          0           0          0      0        0
9        0        0          0           0          0      0        0
10       0        0          0           0          0      0        0
```

A. CEF is unable to get routing information for this route.
B. CEF cannot switch packet for this route and passes it to the next best switching method.
C. A valid entry and is pointed to hardware based forwarding.
D. CEF cannot switch packet for this route and drops it.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Glean adjacency in short when the router is directly connected to hosts the FIB table on the router will maintain a prefix for the subnet rather than for the individual host prefix. This subnet prefix points to a GLEAN adjacency. Punt adjacency When packets to a destination prefix can't be CEF Switched, or the feature is not supported in the CEF Switching path, the router will then use the next slower switching mechanism configured on the router.

QUESTION 250
Which two options are causes of out-of-order packets? (Choose two.)

A. A routing loop
B. A router in the packet flow path that is intermittently dropping packets
C. High latency
D. Packets in a flow traversing multiple paths through the network.
E. Some packets in a flow being process-switched and others being interrupt-switched on a transit Router

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
In traditional packet forwarding systems, using different paths have varying latencies that cause out of order packets, eventually resulting in far lower performance for the network application. Also, if some packets are process switched quickly by the routing engine of the router while others are interrupt switched (which takes more time) then it could result in out of order packets. The other options would cause packet drops or latency, but not out of order packets.

QUESTION 251
A network engineer applies the command ip tcp adjust-mss <bytes> under interface configuration mode. What is the result?

A. The probability of SYN packet truncation is increased.
B. The UDP session is inversely affected.
C. The probability of dropped or segmented TCP packets is decreased.
D. The optimum MTU value for the interface is set.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 252
Which two commands do you need to implement on the CALLING router to support the PPPoE client? (choose Two)

A. peer default ip address pool
B. mtu
C. bba-group pppoe
D. pppoe enable group
E. pppoe-client dialer-pool-number

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Configuration at **Client side** (PPPoE Client):

```
interface Dialer 2
encapsulation ppp
ip address negotiated
ppp chap hostname TUT
ppp chap password MyPPPoE
ip mtu 1492
dialer pool 1
```

Then the next page: http://www.digitaltut.com/ppp-over-ethernet-pppoe-tutorial/2

Configuration at **Server side** (PPPoE Server)
1. First we configure a broadband aggregation (BBA) group
```
bba-group pppoe MyPPPoEProfile
virtual-template 1
```
2. Now we will create the virtual template 1 interface
```
interface Virtual-Template 1
ip address 10.0.0.1 255.255.255.0
peer default ip address pool PPPoE_Pool
ppp authentication chap
```
3. Finally link the PPPoE profile to the physical E0/0 interface, which is connected to the PPPoE client.
```
interface Ethernet0/0
pppoe enable group MyPPPoEProfile
```

For the above we ca see that **mtu** and **pppoe-client dialer-pool-number** are commands to pppoe **CLIENT**

and

peer default ip address pool, **bba-group pppoe**, and **pppoe enable group** are commands to pppoe **SERVER**

QUESTION 253
Which two commands must you configure in the calling router to support the PPPoE client? (Choose two.)

A. **pppoe enable group**
B. **peer default ip address pool**
C. **pppoe-client-dial-pool-number**
D. **bba-group pppoe**
E. **mtu**

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 254
Frame Relay LMI autosense. Which statements are true? (Choose two.)

A. Line should be up and protocol should be down
B. Protocol must be up
C. It only works on DTEs
D. It only works on DCEs

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
LMI autosense is active in the following situations:
-The router is powered up or the interface changes state to up.
-The line protocol is down but the line is up.
-The interface is a Frame Relay DTE.
-The LMI type is not explicitly configured.

QUESTION 255
Which value does Frame Relay use to identify a connection between a DTE and DCE?

A. DLCI
B. IP address
C. MAC address
D. VLAN ID

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 256
Which two statements about configuring Frame Relay point-to-multipoint connections are true? (Choose two)

A. They ignore the broadcast keyword in the frame-relay DLCI mapping
B. They require the same DLCI on each side of the link.
C. Changing a point-to-multipoint subinterface to a different type requires the interface to be deleted and recreated.
D. They require the frame-relay mapping command to be configured.
E. They require inverse ARP.

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 257
Which two statements about Frame Relay Point-to-Point connections are true? (Choose two.)

A. Changing a point-to-point sub interface to a different type requires the device to be reloaded.
B. They use two DLCIs to communicate with multiple endpoints over the Frame Relay cloud.
C. The device can establish a point-to-point connection to the cloud without a DLCI.
D. They can operate normally without a DLCI map.
E. Each physical interface that extends to the Frame Relay cloud can support a single SVC.

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 258
Which DSL encapsulation method requires client software running on the end-user PC that is directly connected to a DSL modem?

A. PPPoA
B. PPPoE
C. PPP
D. L2TP
E. ATM

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 259
Which cisco Express Forwarding component maintains Layer 2 addressing information?

A. dCEF
B. Adjacency table
C. FIB
D. Fast switching
E. RIB

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Adjacency TablesNodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 addressing information. The adjacency table maintains Layer 2 next-hop addresses for all FIB entries.

Reference:
http://www.cisco.com/c/en/us/td/docs/ios/12_2/switch/configuration/guide/fswtch_c/xcfcef.html

QUESTION 260
What configurations does PPPoE allow? (Choose two.)

A. Client can be installed on the same network devices as server
B. 8 clients can be configured on 1 CPE
C. Clients can connect to multiple hosts over DMVPN
D. Client connecting over ATM PVC
E. Client installed on native IPv6 network

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 261
What are characteristics of PAP and CHAP? (Choose two.)

A. PAP provides a challenge to the client
B. CHAP provides a challenge to the client
C. PAP can be used by TACACS+ to verify access credentials
D. PAP requires a username and optional password
E. CHAP requires a username and optional password

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 262
What is the purpose of configuring the router as a PPPoE client? Select the best response.

A. To provide VPN access over L2TP
B. To enable PPP session from the router to the termination device at the headend for metro Ethernet connectivity
C. For DSL connectivity and removing the need for the end-user PC to run the PPPoE client software
D. For connecting the router to a cable modem, which bridges the Ethernet frames from the router to the cable modem termination system

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 263
In which form does PAP authentication send the username and password across the link?

A. Encrypted
B. Password protected
C. Clear text
D. Hashed

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
(Password Authentication Protocol)
PAP
In this protocol, password is sent in clear text format that makes it less secure in comparison with CHAP.

Reference:

http://www.computernetworkingnotes.com/ccna-study-guide/ppp-protocol-and-encapsulation-method-explained.html

QUESTION 264
Which command configures a PPPoE client and specifies dial-on-demand routing functionality?

A. pppoe-client dial-pool-number <#>
B. PPPoE enable.
C. interface dialer 1
D. encapsulation PPP

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

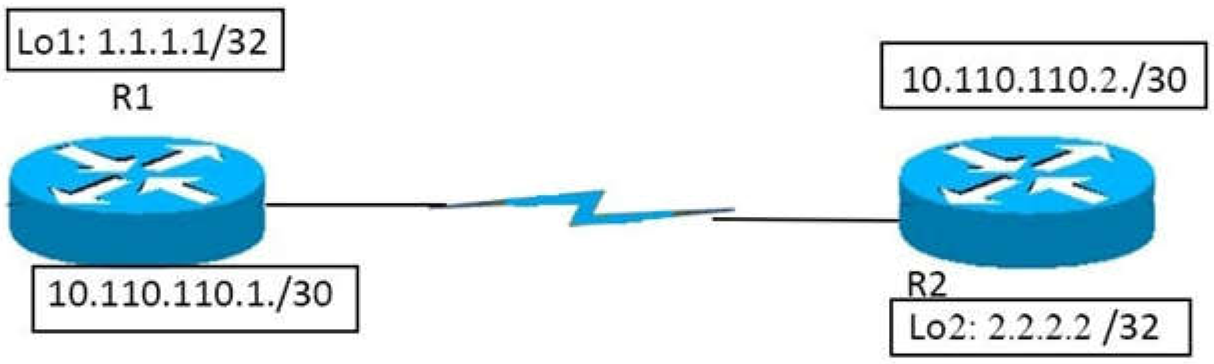
QUESTION 265
Which command instruct a PPPoE client to obtain its IP address from the PPPoe server?

A. Interface dialer
B. IP address negotiated
C. PPPoE enable
D. IP address DHCP
E. IP address dynamic

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 266
Refer to the exhibit. Router 1 cannot ping router 2 via the Frame Relay between them.
Which two statements describe the problems? (Chooses two.)



A. Encapsulation is mismatched.
B. Frame Relay map is configured.
C. DLCI is active.
D. DLCI is inactive or deleted.
E. An access list is needed to allow ping

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Frame Relay: Cannot ping Remote Router:
1-Encapsulation mismatch has occurred.
2-DLCI is inactive or has been deleted.
3-DLCI is assigned to the wrong subinterface.
4-An access list was misconfigured.
5-The frame-relay map command is missing.
6-No broadcast keyword is found in frame-relay map statements.

QUESTION 267
How should a router that is being used in a Frame Relay network be configured to keep split horizon issues from preventing routing updates?

A. Configure a separate subinterface for each PVC with a unique DLCI and subnet assigned to the subinterface
B. Configure each Frame Relay circuit as a point-to-point line to support multicast and broadcast traffic
C. Configure many subinterfaces in the same subnet.
D. Configure a single subinterface to establish multiple PVC connections to multiple remote router interfaces

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

If you have a serial port configured with multiple DLCIs connected to multiple remote sites, split horizon rules, stop route updates received on an interface from being sent out the same interface. By creating subinterfaces for each PVC, you can avoid the split horizon issues when using Frame Relay.
http://www.indiabix.com/networking/wide-area-networks/015004

QUESTION 268
In which two ways can split horizon issues be overcome in a Frame Relay network environment? (Choose two.)

A. Configuring one physical serial interface with Frame Relay to various remote sites.
B. Configure a loopback interface with Frame Relay to various remote sites
C. Configuring multiple subinterfaces on a single physical interface to various remote sites.
D. Enabling split horizon.
E. Disabling split horizon.

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
1/ IP split horizon checking is disabled by default for Frame Relay encapsulation to allow routing updates to go in and out of the same interface. An exception is the Enhanced Interior Gateway Routing Protocol (EIGRP) for which split horizon must be explicitly disabled. 2/Configuring Frame Relay subinterfaces ensures that a single physical interface is treated as multiple virtual interfaces. This capability allows you to overcome split horizon rules so packets received on one virtual interface can be forwarded to another virtual interface, even if they are configured on the same physical interface.

Reference:
http://www.cisco.com/c/en/us/support/docs/wan/frame-relay/14168-fr-faq.html

QUESTION 269
Your network consists of a large hub-and-spoke Frame Relay network with a CIR of 56 kb/s for each spoke.

Which statement about the selection of a dynamic protocol is true? Choose the best response.

A. EIGRP would be appropriate if LMI type ANSI is NOT used.
B. EIGRP would be appropriate, because the Frame Relay spokes could be segmented into their own areas.
C. EIGRP would be appropriate, because by default, queries are not propagated across the slow speed Frame Relay links.
D. EIGRP would be appropriate, because you can manage how much bandwidth is consumed over the Frame Relay interface.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
By default, EIGRP will limit itself to using no more than 50% of the interface bandwidth. The primary benefit of controlling EIGRP's bandwidth usage is to avoid losing EIGRP packets, which could occur when EIGRP generates data faster than the interface line can absorb it. This is of particular benefit on Frame Relay networks, where the access interface bandwidth and the PVC capacity may be very different.

QUESTION 270
A network engineer enables OSPF on a Frame Relay WAN connection to various remote sites, but no OSPF adjacencies come up.

Which two actions are possible solutions for this issue? (Choose two)

A. Change the network type to point-to-multipoint under WAN interface.
B. Enable virtual links.
C. Change the network type to nonbroadcast multipoint access.
D. Configure the neighbor command under OSPF process for each remote site.
E. Ensure that the OSPF process number matches among all remote sites.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 271
Which of the following SNMPv2 uses for authentication?

A. HMAC-MD5
B. HMAC-SHA
C. CBC-DES
D. Community strings

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 272
Which statement about stateless and stateful IPv6 autoconfiguration are true?

A. Both stateless and stateful autoconfiguration require additional setup
B. Stateless autoconfiguration requires no additional setup, whereas stateful autoconfiguration requires additional setup

C. Stateless autoconfiguration requires additional setup, whereas stateful autoconfiguration requires no additional setup
D. Both stateless and stateful autoconfiguration require no additional setup

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Stateful autoconfiguration is the IPv6 equivalent of DHCP. A new protocol, called DHCPv6 (and based closely on DHCP), is used to pass out addressing and service information in the same way that DHCP is used in IPv4. This is called "stateful" because the DHCP server and the client must both maintain state information to keep addresses from conflicting, to handle leases, and to renew addresses over time.

Stateless Autoconfiguration allows an interface to automatically "lease" an IPv6 address and does not require the establishment of an server to delve out address space. Stateless autoconfiguration allows a host to propose an address which will probably be unique (based on the network prefix and its Ethernet MAC address) and propose its use on the network. Because no server has to approve the use of the address, or pass it out, stateless autoconfiguration is simpler. This is the default mode of operation for most IPv6 systems, including servers

QUESTION 273
In IPv6, the interfaces running OSPF can be configured with multiple address prefixes. Which statement is true about the IPv6 addresses that can be included into the OSPF process?

A. Specific addresses can be selected using a route map.
B. Specific addresses can be selected using an ACL
C. Specific addresses cannot be selected for importation into the OSPF process.
D. Specific addresses can be selected using a prefix list.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 274
What is true about peer groups? (Choose two.)

A. Optimize backdoor routes.
B. If you change configuration then it effects all peers in the group.
C. Peer groups can send soft updates to all.
D. Updates can be sent with multicast.

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 275
IP CEF load-sharing options (Choose three.)

A. Tunnel
B. Universal
C. Include-ports
D. Source
E. Destination

Correct Answer: ABC
Section: Mix Questions
Explanation

Explanation/Reference:

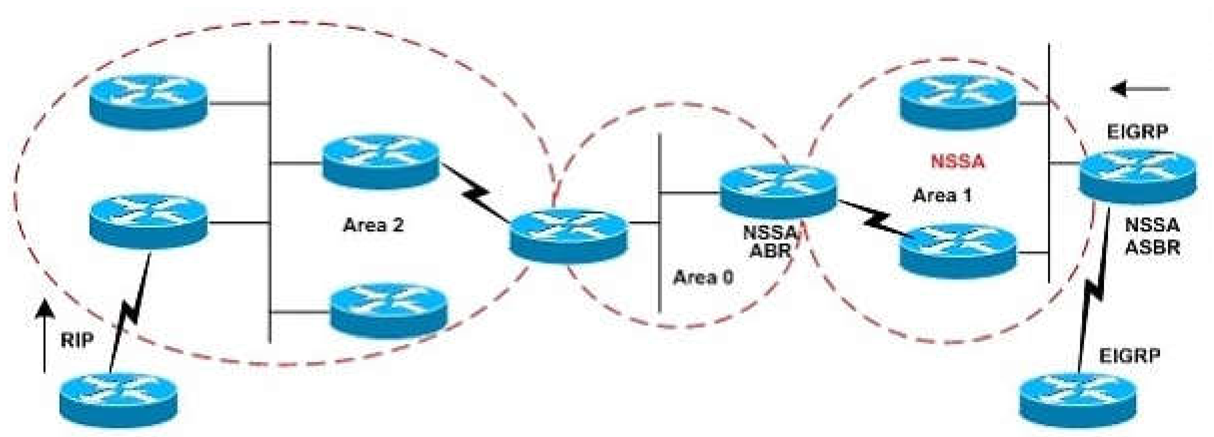
QUESTION 276
If you want to migrate an IS-IS network to another routing protocol with _____. (Choose two)

A. UDP
B. Internal BGP
C. TCP/IP
D. EIGRP
E. OSPF
F. RIP

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 277
Refer to the exhibit. In the network diagram, Area 1 is defined as a stub area. Because redistribution is not allowed in the stub area, EIGRP routes cannot be propagated into the OSPF domain. How does defining area 1 as a not-so-stubby area (NSSA) make it possible to inject EIGRP routes into the OSPF NSSA domain?



A. By creating type 5 LSAs
B. By creating type 7 LSAs
C. By creating a link between the EIGRP domain and the RIP domain, and redistributing EIGRP into RIP
D. By manually changing the routing metric of EIGRP so that it matches the routing metric of OSPF

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 278
What is a valid ipv6 multicast address?

A. FF02::2
B. FFFF::FF
C. FE80::FF
D. 0::/128

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 279
What attribute is used to influce traffic form AS200 and AS300 so that it uses link1 to reach AS100?

A. MED
B. AS_path
C. Weight
D. Local preference

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 280
What is true about EIGRP's redistributed static routes and summarized routes? (Choose two.)

A. Summary routes have AD of 5
B. Static redistributed routes have AD of 190
C. Summary routes have AD of 20
D. Static redistributed routes have AD of 200

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 281
How route tags can be set? (Choose two.)

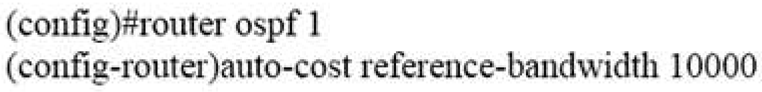
A. Only with route-maps
B. Only with taglists
C. Can be set with route-maps
D. Can be set with taglist.
E. Only used on link state RPs.

Correct Answer: CD
Section: Mix Questions
Explanation

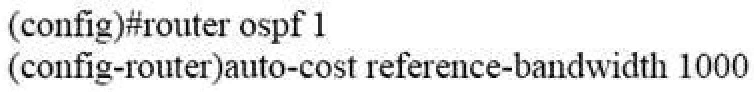
Explanation/Reference:

QUESTION 282
You have a router has some interface configured with 10Gb interface and giga interface.

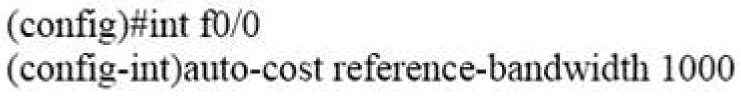
Which command you use to optimize higher BW?

A. 

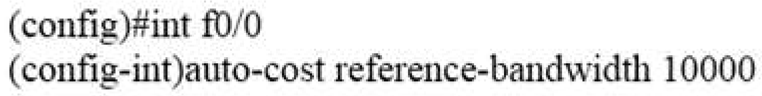
```
(config)#router ospf 1
(config-router)auto-cost reference-bandwidth 10000
```

B. 

```
(config)#router ospf 1
(config-router)auto-cost reference-bandwidth 1000
```

C. 

```
(config)#int f0/0
(config-int)auto-cost reference-bandwidth 1000
```

D. 

```
(config)#int f0/0
(config-int)auto-cost reference-bandwidth 10000
```

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 283
RIPv2 uses _____________.

A. Port UDP 520
B. Port TCP 520
C. Port UDP 502
D. Port TCP 502

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 284
RIPng ____________.

A. Firewall Port block UDP 520
B. Firewall Port block TCP 520
C. Firewall Port block UDP 521
D. Firewall Port block TCP 521

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 285
Which are new LSA types in OSPF for IPv6 (OSPFv3)? (Choose two.)

A. LSA Type 8
B. LSA Type 9
C. LSA Type 10
D. LSA Type 12

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 286
Which of the below mentioned conditions form a neighbor relationship in EIGRP? (Choose three.)

A. Hello or ACK received
B. AS number match
C. Hello timer match
D. Identical metric (k values
E. Dead Timer Match

Correct Answer: ABD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 287
A network engineer is disabling split horizon on a point-to-multipoint interface that is running RIPng. Under which configuration mode can split horizon be disabled?

A. router(config-riping)#
B. router(config-rtr)#
C. router(config-if)#
D. router(config)#

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 288
A network engineer configures two connected routers to run OSPF in Area 0; however, the routers fail to establish adjacency. Which option is one of the caused for this issue?

A. Area numbers match.
B. OSPF process numbers do not match on both neighbor routers.
C. The Same MTU sizes are configured on both sides.
D. The Same OSPF router IDs are configured on both routers.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 289
Which item does EIGRP IPv6 require before it can start running?

A. Router ID
B. DHCP server
C. Subnet mask
D. Default gateway

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Reference:
http://www.ciscopress.com/articles/article.asp?p=2137516&seqNum=4

QUESTION 290
An EUI-64-bit address is formed by adding a reserved 16-bit value in which position of the Mac address?

A. Between the vendor OID and the NIC-specific part of the MAC address.
B. After the NIC-specific part of the MAC address.
C. Before the vendor OID part of the MAC address.
D. Anywhere in the Mac address, because the value that is added is reserved.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 291
An EUI-64 bit address is formed by inserting which 16-bit value into the MAC address of a device?

A. 3FFE
B. FFFE
C. FF02
D. 2001

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 292
Which IPV6 address type does RIPng use for next-hop addresses?

A. Anycast
B. Global
C. Multicas
D. Site-local
E. Link-local

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 293
Which type of message does a device configured with the eigrp stub command send in response to EIGRP queries?

A. Invalid request
B. Unavailable
C. Stuck in active
D. Stub-only
E. Reject
F. Inaccessible

Correct Answer: F
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
When using the EIGRP Stub Routing feature, you need to configure the distribution and remote routers to use EIGRP, and to configure only the remote router as a stub. Only specified routes are propagated from the remote (stub) router. The router responds to queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message "**inaccessible**." A router that is configured as a stub will send a special peer information packet to all neighboring routers to report its status as a stub router.

QUESTION 294
Which two statements about route targets that are configured with VRF-Lite are true? (Choose two.)

A. Route targets uniquely identify the customer routing table
B. Route targets control the import and export of routes into a customer routing table
C. Route targets are supported only when BGP is configured
D. When IS-IS is configured, route targets identify the circuit level in which the customer resides
E. When BGP is configured, route targets are transmitted as BGP standard communities
F. Route targets allos customers to be assigned overlapping adresses

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 295
Redistributing BGP into OSPF what statement is correct?

```
route-map deny 10
match ip address 10
route-map permit 20
access-list 10 permit 172.16.0.0 0.0.0.255
```

A. 172.16.0.0/24 will NOT be redistributed into OSPF.
B. 172.16.0.0/24 will be redistributed into OSPF.
C. Routes permitted by ACL 10 will be redistributed.
D. All routes will be filtered.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 296
What is the output of the following command:

```
show ip vrf
```

A. Show's default RD values.
B. Displays IP routing table information associated with a VRF.
C. Show's routing protocol information associated with a VRF.
D. Displays the ARP table (static and dynamic entries) in the specified VRF.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 297
What command would you use to set EIGRP routes to be prioritized?

A. Distance 100
B. Distance 89
C. Distance eigrp 100
D. Distance eigrp 89

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 298
A route map was configured and it was distributing OSPF external routes __________.

A. Distributing E1 only
B. Distributing E1 and E2 using prefix list
C. Distributing E1 and E2 using access list
D. Distributing E2 routes

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Access list is for traffic filtering & prefix list is for route filtering

QUESTION 299
Which routing protocol does DMVPN support? (Choose three.)

A. ISIS
B. RIP
C. EIGRP
D. OSPF
E. BGP

Correct Answer: CDE
Section: Mix Questions
Explanation

Explanation/Reference:

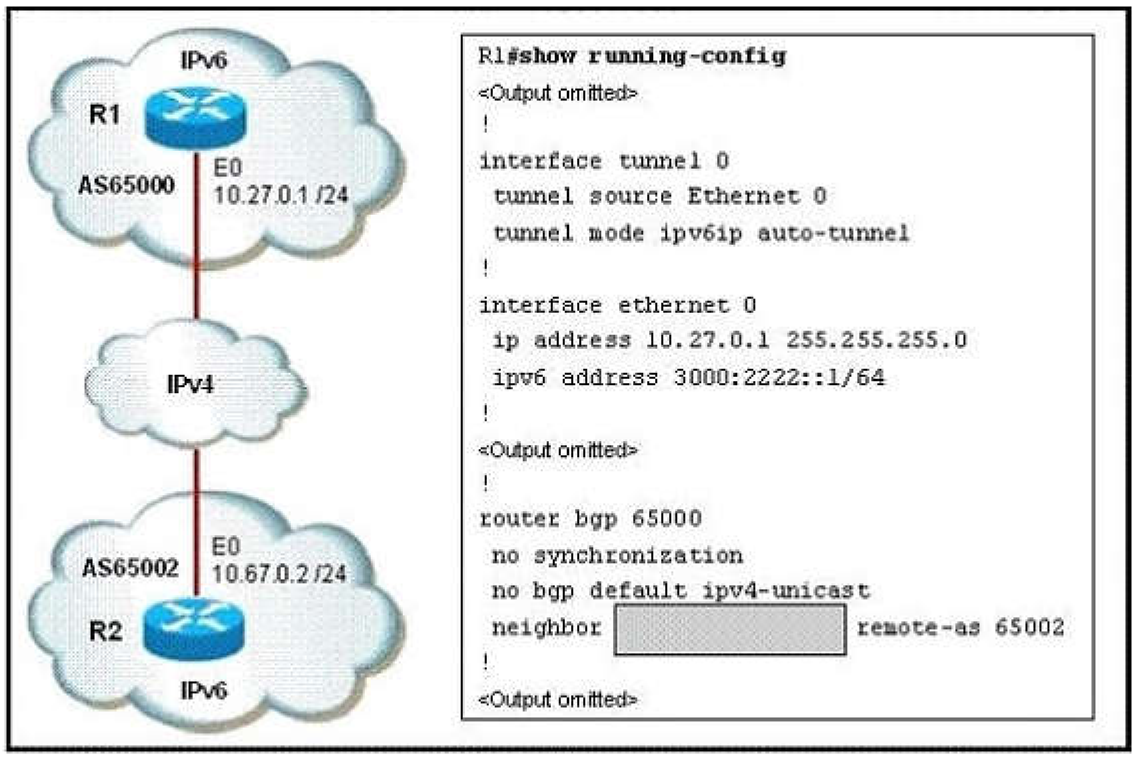
QUESTION 300
What is used in EIGRP metric calculation?

A. Maximum delay
B. Minimum delay
C. Average delay
D. Minimum interface bandwidth

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 301
Refer to the exhibit.



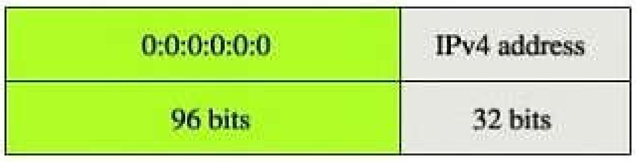
```
R1#show running-config
<Output omitted>
!
interface tunnel 0
 tunnel source Ethernet 0
 tunnel mode ipv6ip auto-tunnel
!
interface ethernet 0
 ip address 10.27.0.1 255.255.255.0
 ipv6 address 3000:2222::1/64
!
<Output omitted>
!
router bgp 65000
 no synchronization
 no bgp default ipv4-unicast
 neighbor                remote-as 65002
!
<Output omitted>
```

Routers R1 and R2 are IPv6 BGP peers that have been configured to support a neighbor relationship over an IPv4 internet work. Which three neighbor IP addresses are valid choices to use in the highlighted section of the exhibit? (Choose three.)

A. ::0A43:0002
B. 0A43:0002::
C. ::10.67.0.2
D. 10.67.0.2::
E. 0:0:0:0:0:0:10.67.0.2
F. 10.67.0.2:0:0:0:0:0:0

Correct Answer: ACE
Section: Mix Questions
Explanation

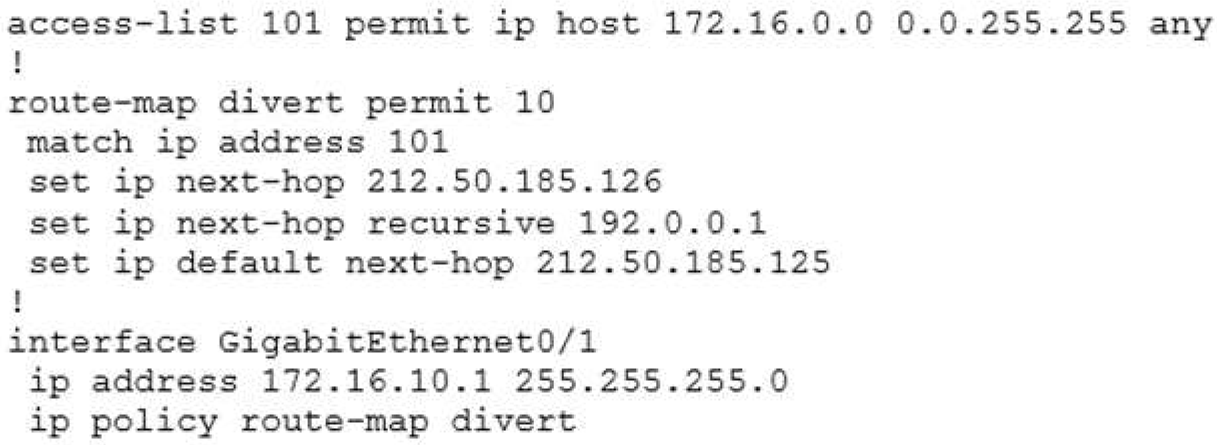
Explanation/Reference:
Explanation:
The automatic tunneling mechanism uses a special type of IPv6 address, termed an "IPv4- compatible" address. An IPv4-compatible address is identified by an all-zeros 96-bit prefix, and holds an IPv4 address in the low-order 32-bits. IPv4-compatible addresses are structured as follows:



0:0:0:0:0:0	IPv4 address
96 bits	32 bits

Therefore, an IPv4 address of 10.67.0.2 will be written as ::10.67.0.2 or
0:0:0:0:0:0:10.67.0.2 or ::0A43:0002 (with 10[decimal] = 0A[hexa] ; 67[decimal] = 43[hexa] ; 0[hexa] = 0[decimal] ; 2[hexa] = 2[decimal])

QUESTION 302
Refer to the exhibit. Which command would verify if PBR reacts to packets sourced from 172.16.0.0/16?

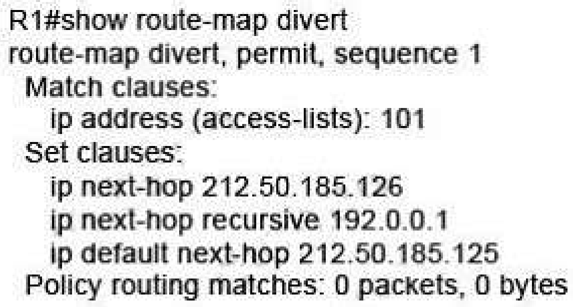


```
access-list 101 permit ip host 172.16.0.0 0.0.255.255 any
!
route-map divert permit 10
 match ip address 101
 set ip next-hop 212.50.185.126
 set ip next-hop recursive 192.0.0.1
 set ip default next-hop 212.50.185.125
!
interface GigabitEthernet0/1
 ip address 172.16.10.1 255.255.255.0
 ip policy route-map divert
```

A. show ip route
B. show policy-map
C. show access-lists
D. show route-map

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The "show route-map "route-map name" displays the policy routing match counts so we can learn if PBR reacts to packets sourced from 172.16.0.0/16 or not.



```
R1#show route-map divert
route-map divert, permit, sequence 1
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 212.50.185.126
    ip next-hop recursive 192.0.0.1
    ip default next-hop 212.50.185.125
  Policy routing matches: 0 packets, 0 bytes
```

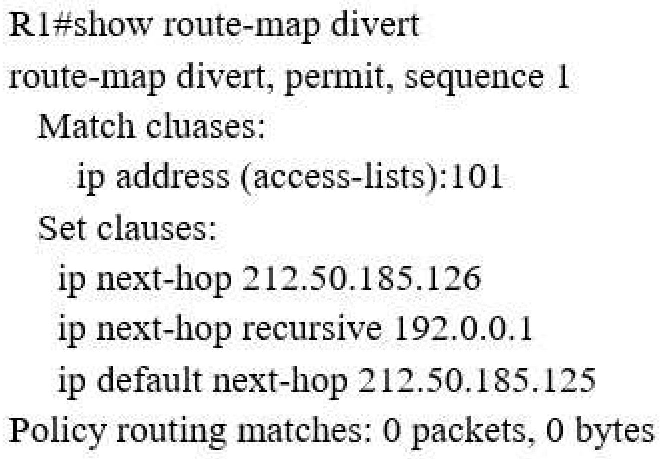
QUESTION 303
What are three reasons to control routing updates via route filtering? (Choose three).

A. To hide certain networks from the rest of the organization
B. For easier implementation
C. To control network overhead on the wire
D. For simple security
E. To prevent adjacencies from forming

Correct Answer: ACD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Route filtering hide certain networks from the rest of the organization and it also controls network overhead. Not only this, it also provides security to the routing updates.

QUESTION 304
Refer to the exhibit. Based upon the configuration, you need to understand why the policy routing match counts are not increasing. Which would be the first logical step to take?



```
R1#show route-map divert
route-map divert, permit, sequence 1
  Match cluases:
    ip address (access-lists):101
  Set clauses:
   ip next-hop 212.50.185.126
   ip next-hop recursive 192.0.0.1
   ip default next-hop 212.50.185.125
Policy routing matches: 0 packets, 0 bytes
```

A. Confirm if there are other problematic route-map statements that precede divert.
B. Check the access list for log hits.
C. Check the routing table for 212.50.185.126.
D. Remove any two of the set clauses. (Multiple set clause entries will cause PBR to use the routing table.)

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
First we should check the access-list log, if the hit count does not increase then no packets are matched the access-list -> the policy based routing match counts will not increase.

QUESTION 305
Which statement describes the difference between a manually configured IPv6 in IPv4 tunnel versus an automatic 6to4 tunnel?

A. A manually configured IPv6 in IPv4 tunnel allows multiple IPv4 destinations.
B. An automatic 6to4 tunnel allows multiple IPv4 destinations.
C. A manually configured IPv6 in IPv4 tunnel does not require dual-stack (IPv4 and IPv6) routers at the tunnel endpoints.
D. An automatic 6to4 tunnel does not require dual-stack (IPv4 and IPv6) routers at the tunnel endpoints.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. The key difference between automatic 6to4 tunnels and manually configured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint -> it allows multiple IPv4 destinations. Manually 6to4 is point-to-point -> only allows one IPv4 destination. Configuring 6to4 (manually and automatic) requires dual-stack routers (which supports both IPv4 & IPv6) at the tunnel endpoints because they are border routers between IPv4 & IPv6 networks.

QUESTION 306
Which two statements are true about using IPv4 and IPv6 simultaneously on a network segment? (Choose two.)

A. Hosts can be configured to receive both IPv4 and IPv6 addresses via DHCP.

B. Host configuration options for IPv4 can be either statically assigned or assigned via DHCP.Host configuration options for IPv6 can be statically assigned only.
C. IPv6 allows a host to create its own IPv6 address that will allow it to communicate to other devices on a network configured via DHCP. IPv4 does not provide a similar capability for hosts.
D. IPv4 and IPv6 addresses can be simultaneously assigned to a host but not to a router interface.
E. IPv6 provides for more host IP addresses but IPv4 provides for more network addresses.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Like DHCP in IPv4, IPv6 hosts can also be configured to acquire connectivity parameters from DHCPv6 servers. IPv4 clients use DHCP broadcasts to locate DHCP servers, and since broadcasts are extinct in IPv6, clients use specialized multicasts to locate DHCPv6 servers. These multicasts use the reserved address FF02::1:2. One notable difference between DHCP and DHCPv6 is that while DHCP can inform clients which node to use as the default gateway, DHCPv6 does not do this.

QUESTION 307
To enable BGP tunneling over an IPv4 backbone, the IPv4 address 192.168.30.1 is converted into a valid IPv6 address.

Which three IPv6 addresses are acceptable formats for the IPv4 address? (Choose three.)

A. 192.168.30.1:0:0:0:0:0:0
B. 0:0:0:0:0:0:192.168.30.1
C. ::192.168.30.1
D. C0A8:1E01::
E. 192.168.30.1::
F. ::C0A8:1E01

Correct Answer: BCF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 308
Which two among the following are used to indicate external type of route in routing table? (Choose two.)

A. D EX
B. IA
C. O E2
D. R E2
E. i L2

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 309
The OSPF which type of Router CAN BE aggregated? (Choose two.)

A. the ABR
B. the ASBR
C. Backbone Router
D. Intra Router

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 310
You need the IP address of the devices with which the router has established an adjacency. Also, the retransmit interval and the queue counts for the adjacent routers need to be checked. What command will display the required information?

A. show ip eigrp adjacency
B. show ip eigrp topology
C. show ip eigrp interfaces
D. show ip eigrp neighbor

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 311
You get a call from a network administrator who tells you that he typed the following into his router:

```
Router(config)#router ospf 1
Router(config-router)#network 10.0.0.0 255.0.0.0 area 0
```

He tells you he still can't see any routes in the routing table. What configuration error did the administrator make?

A. The wildcard mask is incorrect.
B. The OSPF area is wrong.
C. The OSPF Process ID is incorrect.
D. The AS configuration is wrong.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 312
Which is an “invalid” option when redistributing from EIGRP into OSPF?

A. ACL
B. Tag
C. Metric
D. Route map

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 313
Engineer has to enable RIP on a link. Where he will issue the command?

A. Ipv6
B. Global
C. Router sub command
D. Interface subcommand

Correct Answer: C
Section: Mix Questions
Explanation

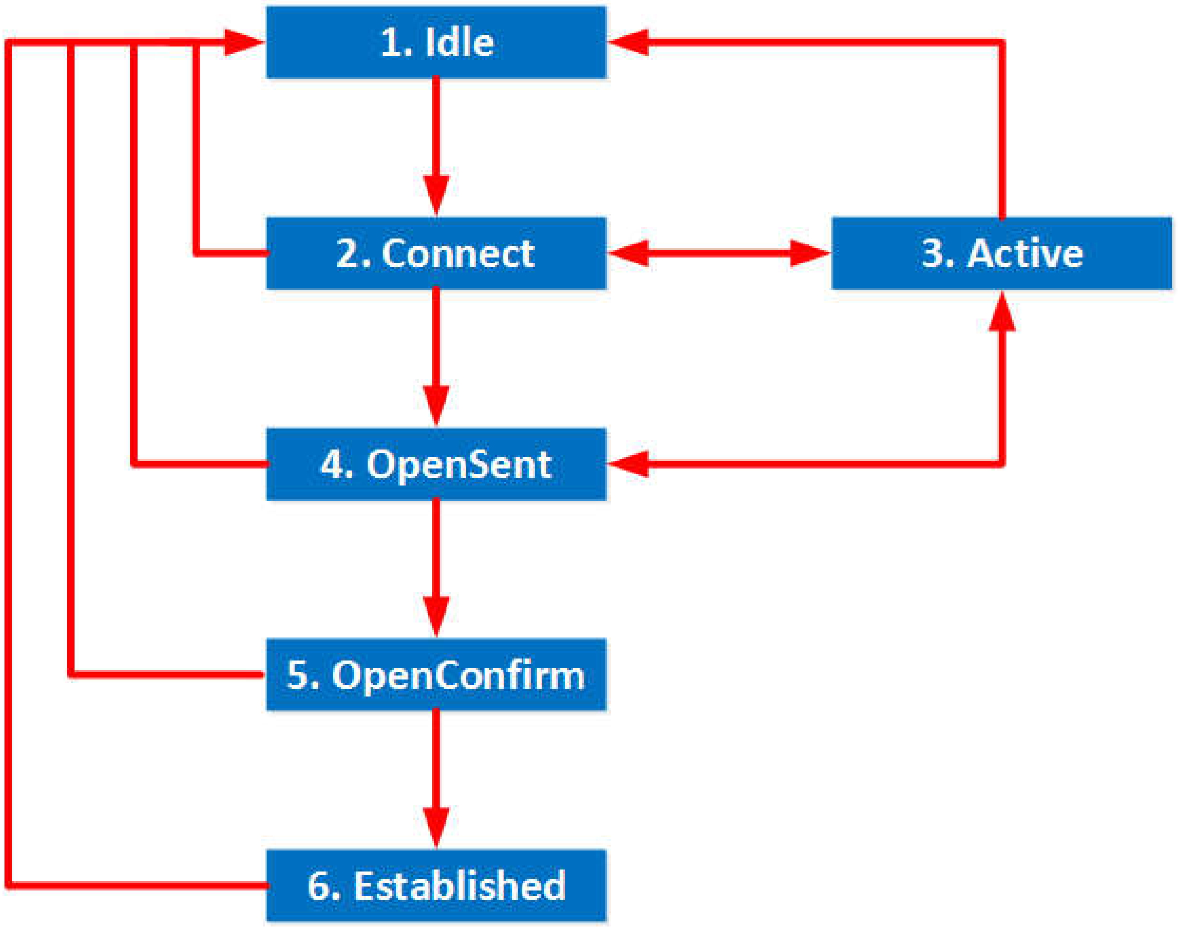
Explanation/Reference:

QUESTION 314
Which two BGP neighbor states are valid? (Choose two.)

A. Established
B. Active
C. Stuck in active
D. 2-WAY
E. Unknown
F. DROTHER

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



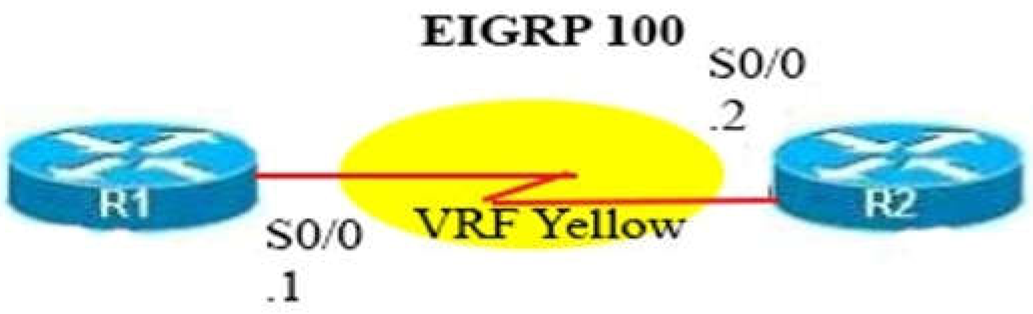
QUESTION 315
What does the show ip route vrf CISCO command display?

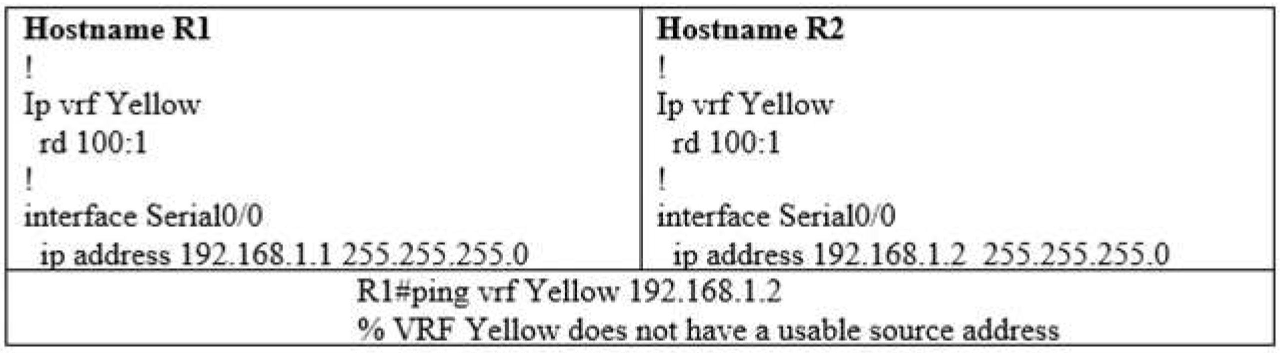
A. Directly connected routes for VRF CISCO
B. The routing table for VRF CISCO
C. The global routing table.
D. All routing tables that start with VRF CISCO.
E. The route distinguisher for VRF CISCO

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 316
Refer to Exhibit.
R1 is unable to ping interface S0/0 of R2.
What is the issue the configuration that is shown here?





```
Hostname R1
!
Ip vrf Yellow
 rd 100:1
!
interface Serial0/0
 ip address 192.168.1.1 255.255.255.0
```

```
Hostname R2
!
Ip vrf Yellow
 rd 100:1
!
interface Serial0/0
 ip address 192.168.1.2  255.255.255.0
```

```
R1#ping vrf Yellow 192.168.1.2
% VRF Yellow does not have a usable source address
```

A. The route-target configuration command is missing.
B. The interface IP addresses are not in the same subnet.
C. the syntax of the ping command is wrong.
D. The default route configuration is missing.
E. The serial interfaces belong to the global table instead of vrf Yellow.

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

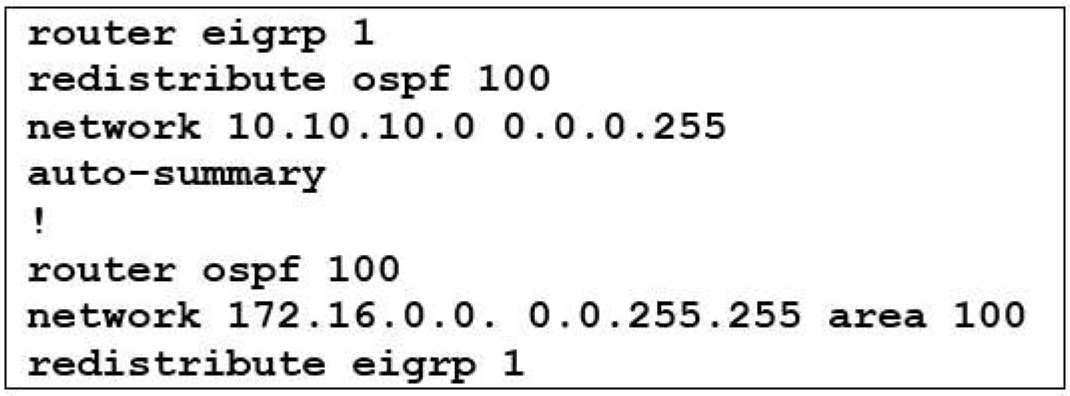
QUESTION 317
Which LSA type can exist only in an OSPF NSSA area?

A. Type 7 LSA
B. Type 1 LSA
C. Type 5 LSA
D. Type 3 LSA

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 318
Which option describes why the EIGRP neighbors of this router are not learning routes that are received from OSPF?



```
router eigrp 1
redistribute ospf 100
network 10.10.10.0 0.0.0.255
auto-summary
!
router ospf 100
network 172.16.0.0. 0.0.255.255 area 100
redistribute eigrp 1
```

A. The subnet defined in OSPF is not part of area 0.
B. Default metrics are not configured under EIGRP.
C. There is no overlap in the subnets advertised.
D. The routing protocols do not have the same AS number.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 319
What is the hop count that is advertised for an unreachable network by a RIP router that uses poison reverse?

A. 15
B. 255
C. 0
D. 16

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 320
By default, which statement is correct regarding the redistribution of routes from other routing protocols into OSPF? Select the best response.

A. They will appear in the OSPF routing table as type E1 routes.
B. They will appear in the OSPF routing table as type E2 routes
C. Summarized routes are not accepted.
D. All imported routes will be automatically summarized when possible.
E. Only routes with lower administrative distances will be imported.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Type E1 external routes calculate the cost by adding the external cost to the internal cost of each link that the packet crosses while the external cost of E2 packet routes is always the external cost only. E2 is useful if you do not want internal routing to determine the path. E1 is useful when internal routing should be included in path selection. E2 is the default external metric when redistributing routes from other routing protocols into OSPF.

QUESTION 321
Which authentication methods are EIGRP uses?

A. sha
B. md5
C. xda

D. chap
E. cisco

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 322
Which statement about local policy routing is true?

A. It is used to policy route packets that are generated by the device.
B. It requires all packets to be packet switched.
C. It is used to policy route packets that pass through the device.
D. It requires all packets to be CEF switched.
E. It supports IPv4 packets only.
F. It requires an ip address or access list as the matching criteria.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 323
What appears in the other router routing table?

#loopback EIGRP STUB

A. loopback of the stub router advertised
B. loopback of the stub router was not advertised

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 324
Which three configuration parameters can a DHCPV6 pool contain? (Choose three.)

A. Domain search list
B. Router IP
C. Default gateway
D. Prefix delegation
E. DNS servers
F. Subnet mask

Correct Answer: ADE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Each configuration pool can contain the following configuration parameters and operational information:
-Prefix delegation information, which includes:
-A prefix pool name and associated preferred and valid lifetimes
-A list of available prefixes for a particular client and associated preferred and valid lifetimes
-A list of IPv6 addresses of DNS servers
-A domain search list, which is a string containing domain names for the DNS resolution

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_dhcp/configuration/xe-3s/dhcp-xe-3s-book/ip6-dhcp-prefix-xe.pdf

QUESTION 325
What are two BGP neigborship states? (Choose two.)

A. Full
B. Open Sent
C. 2WAY
D. Connect
E. DROTHER
F. Stuck in active

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 326
What is the effect of the following two commands? (Choose two.)

area 1 range 10.1.0.0 255.255.0.0
summary address 10.1.0.0 255.255.0.0

A. area 1 range: command applied to summarize internal OSPF routes (ABR)
B. area 1 range: command applied to summarize external OSPF routes (ASBR)
C. Summary address: command applied to summarize external OSPF routes (ASBR)
D. Summary address: command applied to summarize internal OSPF routes (ABR)

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 327
Which access list entry checks for an ACK within a packet TCP header?

A. access-list 49 permit ip any any eq 21 tcp-ack
B. access-list 49 permit tcp any any eq 21 tcp-ack
C. access-list 149 permit tcp any any eq 21 established
D. access-list 49 permit tcp any any eq 21 established

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 328
Which TCP port for BGP?

A. port 161
B. port 123
C. port 179
D. port 47

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 329
Which type of access list allows granular session filtering for upper-level protocols?

A. Content-based access lists
B. Context-based access lists
C. Reflexive access lists
D. Extended access lists

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 330
Which two options are requirements for EIGRP authentication? (Choose two.)

A. A crypto map must be configured.
B. The Authentication key must be configured under the interface running EIGRP.
C. The authentication key must be configured within the EIGRP routing configuration.
D. The authentication key IDs must match between two neighbors.
E. A separate key chain must be configured.
F. AN IPsec profile must be configured.

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 331
Which command prevents routers from sending routing updates through a router interface?

A. default-metric 0
B. distribute-list in

C. passive-interface
D. distribute-list out

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
To prevent routing updates through a specified interface, use the passive-interface type number command in router configuration mode.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/xe-3s/iri-xe-3s-book/iri-default-passive-interface.html

QUESTION 332
Which three options are valid DHCPv6 functions? (Choose three.)

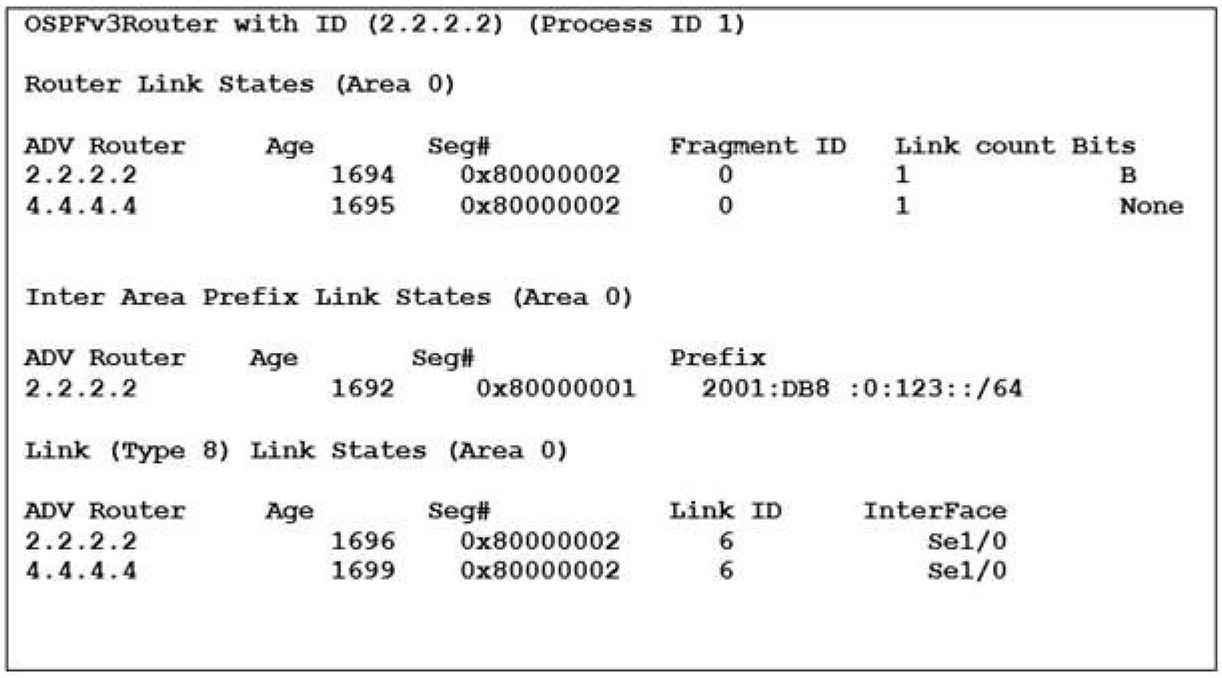
A. Server
B. Client
C. Approver
D. Requester
E. Repeater
F. ACK
G. Relay

Correct Answer: ABG
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 333
Refer to the exhibit. A network engineer executes the show ipv6 ospf database command and is presented with the output that is shown.

Which flooding scope is referenced in the link-state type?



```
OSPFv3Router with ID (2.2.2.2) (Process ID 1)

Router Link States (Area 0)

ADV Router     Age       Seg#           Fragment ID   Link count Bits
2.2.2.2            1694    0x80000002       0          1             B
4.4.4.4            1695    0x80000002       0          1             None


Inter Area Prefix Link States (Area 0)

ADV Router    Age       Seg#            Prefix
2.2.2.2            1692     0x80000001    2001:DB8 :0:123::/64

Link (Type 8) Link States (Area 0)

ADV Router     Age       Seg#           Link ID     InterFace
2.2.2.2            1696    0x80000002       6            Se1/0
4.4.4.4            1699    0x80000002       6            Se1/0
```

A. Link-local
B. Area
C. As (OSPF domain)
D. Reserved

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

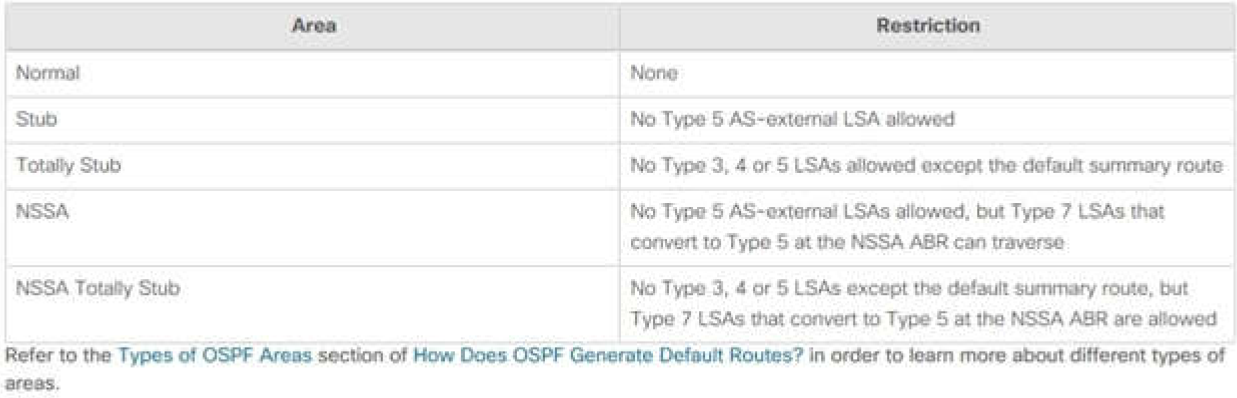
QUESTION 334
Which ospf area prevent LSA type 4, LSA type 5? (Choose two.)

A. Not so stubby
B. Total stubby
C. Stubby area
D. Totally Not-So-Stubby Area

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Tottaly NSSA and NSSA convert LSA 7 into LSA 5 so in this case LSA 5 is permitting
Tottaly Stub and Stub DO NOT allow LSA 4,5 instead they inject default route



Area	Restriction
Normal	None
Stub	No Type 5 AS-external LSA allowed
Totally Stub	No Type 3, 4 or 5 LSAs allowed except the default summary route
NSSA	No Type 5 AS-external LSAs allowed, but Type 7 LSAs that convert to Type 5 at the NSSA ABR can traverse
NSSA Totally Stub	No Type 3, 4 or 5 LSAs except the default summary route, but Type 7 LSAs that convert to Type 5 at the NSSA ABR are allowed

Refer to the Types of OSPF Areas section of How Does OSPF Generate Default Routes? in order to learn more about different types of areas.

Reference:
https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13703-8.html#anc2

QUESTION 335
Which type of address does OSPFv3 use to form neighbor adjacencies and to send LSAs?

A. Unicast IPv6 addresses
B. Link-local addresses
C. Multicast address FF02::5
D. Unicast IPv4 addresses

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 336
What following parameters for the EIGRP authentication need to match in order for EIGRP neighbors to establish a neighbor relationship?

A. Autonomous System number.
B. K-Values
C. If authentication is used both: the key number, the password, and the date/time.
D. The neighbors must be on common subnet (all IGPs follow this rule).

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 337
Which value does GRE tunnel use to identify the end points or destination?

A. IP address
B. MAC address
C. DLCI
D. Tunnel

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
For Frame Relay the answer would be DLCI but here it is asking about GRE tunnel so the best choice here is “IP address”.

QUESTION 338
FILL BLANK
What is the function of the command redistribute ospf 1 match internal?

Correct Answer: Redistribute ospf 1 match internal means that just inter and intra will be redistributed
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Router(config-router)#redistribute ospf 1 match internal external 1 external 2

Redistributes routes learned from OSPF process ID 1. The keywords match internal external 1 and external 2 instruct EIGRP to only redistribute internal, external type 1 and type 2 OSPF routes.

NOTE: The default behavior when redistributing OSPF routes is to redistribute all routes—internal, external 1, and external 2. The keywords match internal external 1 and external 2 are required only if router behavior is to be modified.

QUESTION 339
Which the Valid range for BGP private ASNs?

A. 64512-65535
B. 62464-65024

C. 64512-65024
D. 62464-64511

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 340
OSPF chooses routes in which order, regardless of route's administrative distance and metric? (Choose all that apply.)

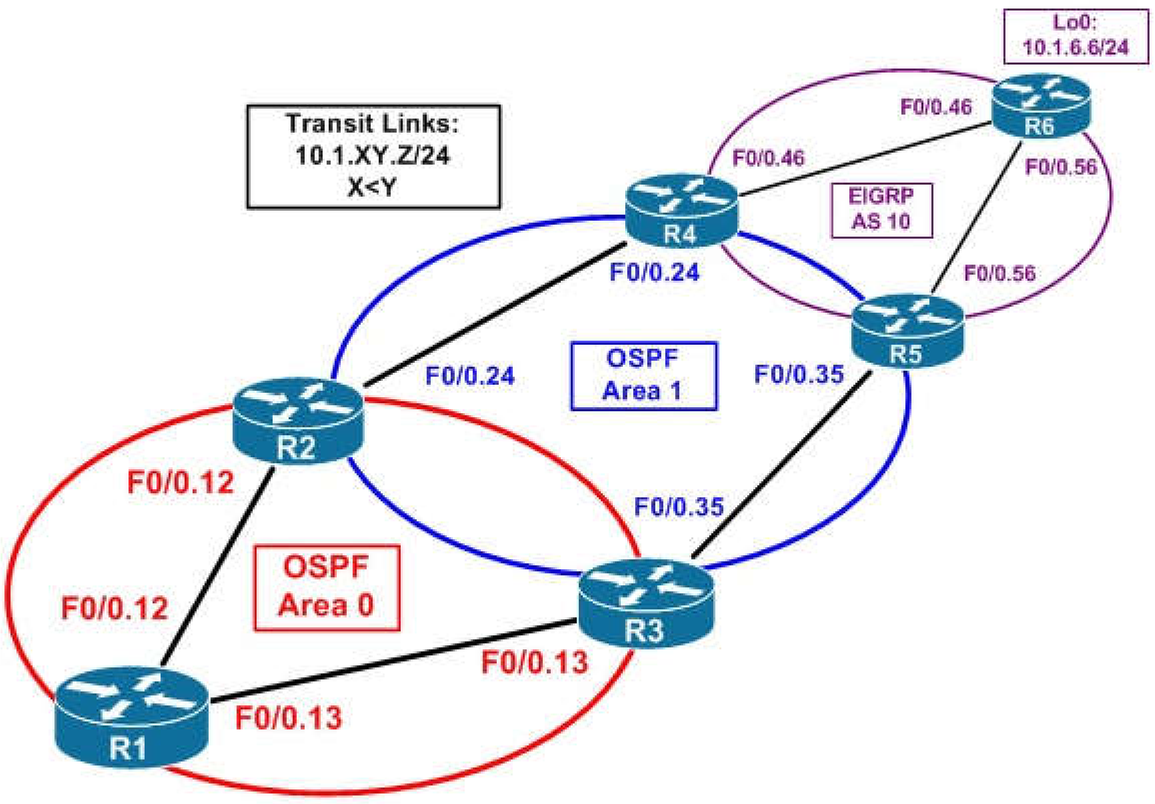
A. Intra-Area (O)
B. Inter-Area (O IA)
C. External Type 1 (E1)
D. External Type 2 (E2)
E. NSSA Type 1 (N1)
F. NSSA Type 2 (N2)

Correct Answer: ABCDEF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Regardless of a route's metric or administrative distance, OSPF will choose routes in the following order:

Intra-Area (O)
Inter-Area (O IA)
External Type 1 (E1)
External Type 2 (E2)
NSSA Type 1 (N1)
NSSA Type 2 (N2)

To demonstrate this, take the following topology:



QUESTION 341
When ospf is forming an adjacency, in which state does the actual exchange of information in the link-state database occur?

A. INIT
B. Loading
C. Exstart
D. Exchange

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Down
This is the first OSPF neighbor state. It means that no information (hellos) has been received from this neighbor, but hello packets can still be sent to the neighbor in this state.

During the fully adjacent neighbor state, if a router doesn't receive hello packet from a neighbor within the RouterDeadInterval time (RouterDeadInterval = 4*HelloInterval by default) or if the manually configured neighbor is being removed from the configuration, then the neighbor state changes from Full to Down.

Attempt
This state is only valid for manually configured neighbors in an NBMA environment. In Attempt state, the router sends unicast hello packets every poll interval to the neighbor, from which hellos have not been received within the dead interval.

Init
This state specifies that the router has received a hello packet from its neighbor, but the receiving router's ID was not included in the hello packet. When a router receives a hello packet from a neighbor, it should list the sender's router ID in its hello packet as an acknowledgment that it received a valid hello packet.

2-Way
This state designates that bi-directional communication has been established between two routers. Bi-directional means that each router has seen the other's hello packet. This state is attained when the router receiving the hello packet sees its own Router ID within the received hello packet's neighbor field. At this state, a router decides whether to become adjacent with this neighbor. On broadcast media and non-broadcast multiaccess networks, a router becomes full only with the designated router (DR) and the backup designated router (BDR); it stays in the 2-way state with all other neighbors. On Point-to-point and Point-to-multipoint networks, a router becomes full with all connected routers.

At the end of this stage, the DR and BDR for broadcast and non-broadcast multi-acess networks are elected. For more information on the DR election process, refer to DR Election.

Note: Receiving a Database Descriptor (DBD) packet from a neighbor in the init state will also a cause a transition to 2-way state.

Exstart
Once the DR and BDR are elected, the actual process of exchanging link state information can start between the routers and their DR and BDR.

In this state, the routers and their DR and BDR establish a master-slave relationship and choose the initial sequence number for adjacency formation. The router with the higher router ID becomes the master and starts the exchange, and as such, is the only router that can increment the sequence number. Note that one would logically conclude that the DR/BDR with the highest router ID will become the master during this process of master-slave relation. Remember that the DR/BDR election might be purely by virtue of a higher priority configured on the router instead of highest router ID. Thus, it is possible that a DR plays the role of slave. And also note that master/slave election is on a per-neighbor basis.

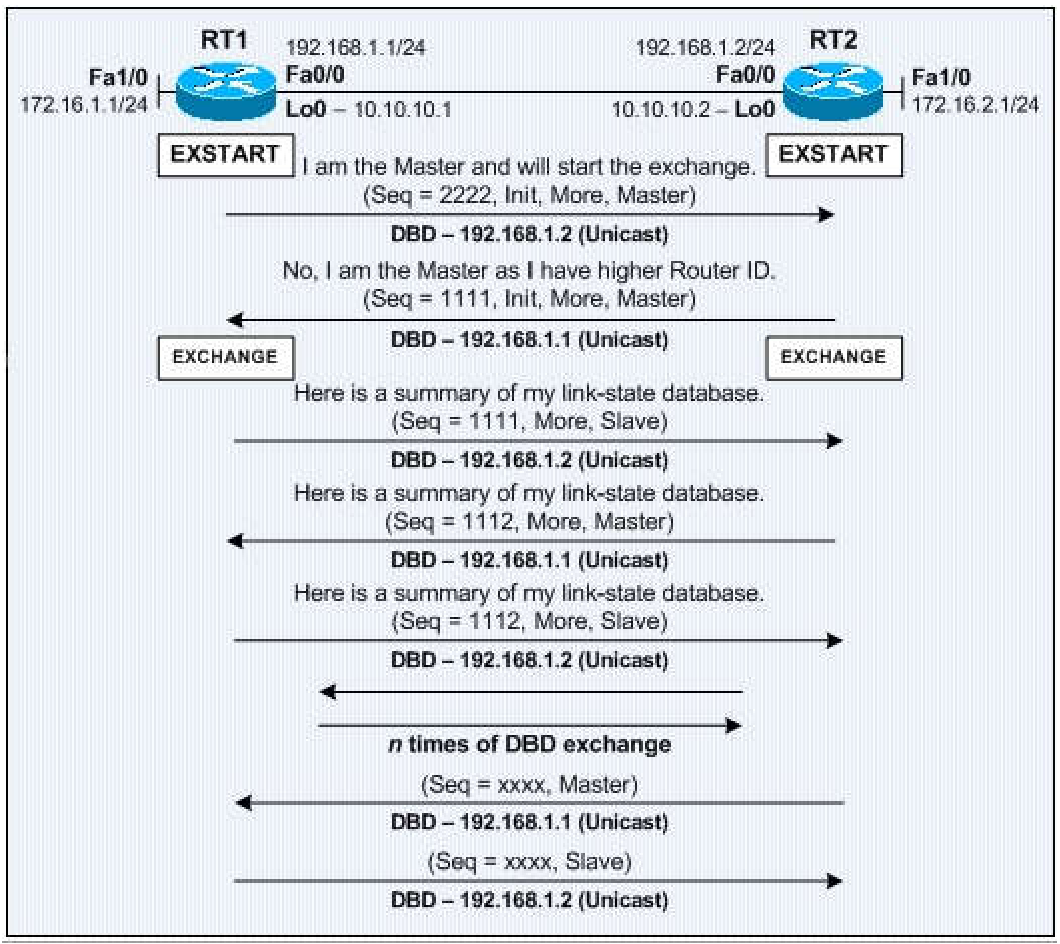
Exchange
In the exchange state, OSPF routers exchange database descriptor (DBD) packets. Database descriptors contain link-state advertisement (LSA) headers only and describe the contents of the entire link-state database. Each DBD packet has a sequence number which can be incremented only by master which is explicitly acknowledged by slave. Routers also send link-state request packets and link-state update packets (which contain the entire LSA) in this state. The contents of the DBD received are compared to the information contained in the routers link-state database to check if new or more current link-state information is available with the neighbor.

Loading
In this state, the actual exchange of link state information occurs. Based on the information provided by the DBDs, routers send link-state request packets. The neighbor then provides the requested link-state information in link-state update packets. During the adjacency, if a router receives an outdated or missing LSA, it requests that LSA by sending a link-state request packet. All link-state update packets are acknowledged.

Full
In this state, routers are fully adjacent with each other. All the router and network LSAs are exchanged and the routers' databases are fully synchronized.

Full is the normal state for an OSPF router. If a router is stuck in another state, it is an indication that there are problems in forming adjacencies. The only exception to this is the 2-way state, which is normal in a broadcast network. Routers achieve the FULL state with their DR and BDR in NBMA/broadcast media and FULL state with every neighbor in the remaining media such as point-to-point and point-to-multipoint.

Note: The DR and BDR that achieve FULL state with every router on the segment will display FULL/DROTHER when you enter the show ip ospf neighbor command on either a DR or BDR. This simply means that the neighbor is not a DR or BDR, but since the router on which the command was entered is either a DR or BDR, this shows the neighbor as FULL/DROTHER.


RT1
192.168.1.1/24
Fa0/0
Lo0 – 10.10.10.1
Fa1/0
172.16.1.1/24
RT2
192.168.1.2/24
Fa0/0
10.10.10.2 – Lo0
Fa1/0
172.16.2.1/24
EXSTART
EXSTART
I am the Master and will start the exchange.
(Seq = 2222, Init, More, Master)
DBD – 192.168.1.2 (Unicast)
No, I am the Master as I have higher Router ID.
(Seq = 1111, Init, More, Master)
DBD – 192.168.1.1 (Unicast)
EXCHANGE
EXCHANGE
Here is a summary of my link-state database.
(Seq = 1111, More, Slave)
DBD – 192.168.1.2 (Unicast)
Here is a summary of my link-state database.
(Seq = 1112, More, Master)
DBD – 192.168.1.1 (Unicast)
Here is a summary of my link-state database.
(Seq = 1112, More, Slave)
DBD – 192.168.1.2 (Unicast)
n times of DBD exchange
(Seq = xxxx, Master)
DBD – 192.168.1.1 (Unicast)
(Seq = xxxx, Slave)
DBD – 192.168.1.2 (Unicast)

QUESTION 342
Using new backup router in spite of faulty one in ospf domain but relationship with neighbor in one interface only not working, what is the reason of this problem? (Choose two)

A. area Id match
B. authentication mismatch
C. process id of ospf not match

D. ospf timers not match
E. MTU mismatch

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 343
Which two statements are true of the OSPF link-state routing protocol? (Choose two.)

A. Using the Bellman-Ford algorithm, each OSPF router independently calculates its best paths to all destinations in the network.
B. Using the DUAL algorithm, each OSPF router independently calculates its best paths to all destinations in the network.
C. OSPF sends summaries of individual link-state entries every 30 minutes to ensure LSDB synchronization.
D. OSPF sends triggered updates when a network change occurs.
E. OSPF sends updates every 10 seconds.
F. When a link changes state, the router that detected the change creates a link-state advertisement (LSA) and propagates it to all OSPF devices using the 224.0.0.6 multicast address.

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The point of this question is the basis of OSPF.
Incorrect answer A. OSPF send hello packets every 10 seconds, not the updates, OSPF sends triggered updates when a network change occurs. For OSPF, D Rother use the multicast address 224.0.0.6 to send packets to DR and BDR, only DR and BDR can get the information from this multicast address.

QUESTION 344
What type of IPv6 packet will indicate traffic from single host and single node?

A. Multicast
B. Unicast
C. Broadcast
D. Anycast

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
IPv6 has three types of addresses, which can be categorized by type and scope:
Unicast addresses. A packet is delivered to one interface Multicast addresses. A packet is delivered to multiple interfaces. Anycast addresses. A packet is delivered to the nearest of multiple interfaces (in terms of routing distance).

QUESTION 345
A network administrator notices that the BGP state drops and logs are generated for missing BGP hello keepalives. What is the potential problem?

A. Incorrect neighbor options
B. Hello timer mismatch
C. BGP path MTU enabled
D. MTU mismatch

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
BGP neighbors form; however, at the time of prefix exchange, the BGP state drops and the logs generate missing BGP hello keepalives or the other peer terminates the session.
Here are some possible causes:
*The interface MTU on both routers do not match.
*The interface MTU on both routers match, but the Layer 2 domain over which the BGP session is formed does not match.
*Path MTU discovery determined the incorrect max datasize for the TCP BGP session. *The BGP Path Maximum Transmission Unit Discovery (PMTUD) could be failing due to PMTUD ICMP packets blocked (firewall or ACL)
http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/116377-troubleshoot-bgp-mtu.html

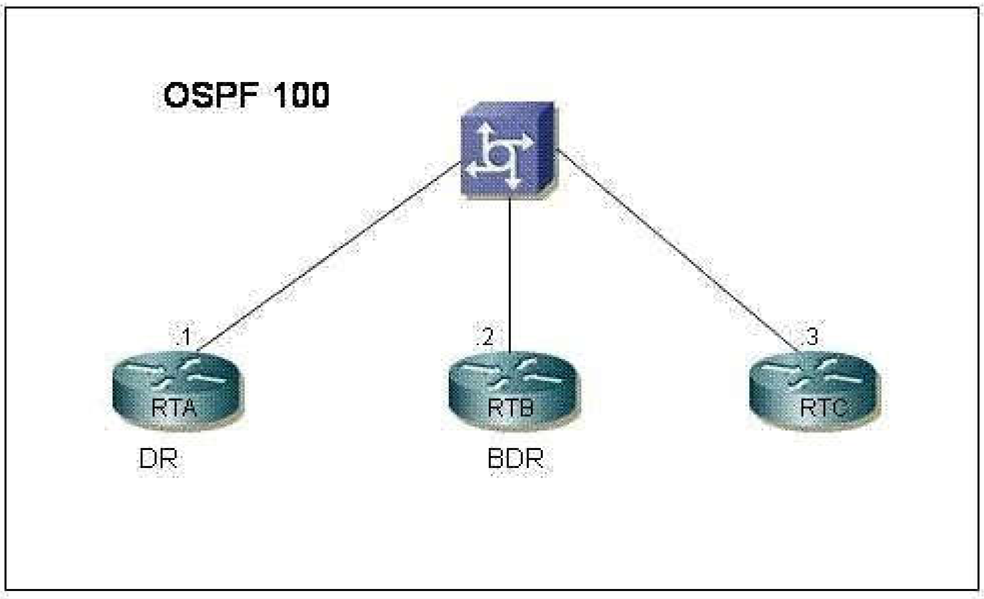
QUESTION 346
Which BGP option is required when load sharing over multiple equal-bandwidth parallel links from a single CE router to a single ISP router over eBGP? Select the best response.

A. eBGP Multipath
B. eBGP Multihop
C. BGP Synchronization
D. Public AS numbers

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 347
During a recent OSPF election among three routers, RTA was elected the DR and RTB was elected the BDR, as seen in the graphic. Assume that RTA fails, and that RTB takes the place of the DR while RTC becomes the new BDR. What will happen when RTA comes back online?



A. RTA will take the place of DR immediately upon establishing its adjacencies
B. RTA will take the place of DR only if RTB fails.
C. RTA will take the place of DR only if both RTB and RTC fail.
D. A new election will take place establishing an all new DR and BDR based on configured priority levels and MAC addresses.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
If a router with a higher priority value gets added to the network, it does not preempt the DR and BDR. The only time a DR and BDR changes is if one of them is out of service. If the DR is out of service, the BDR becomes the DR, and a new BDR is selected. If the BDR is out of service, a new BDR is elected. In a multi-access network, the router that is powered on first will generally become the DR, since the DR/BDR process is not pre-emptive.

CCNP Self-Study Second Edition P.243

QUESTION 348
What is the IPv6 address FF02::2 used for? Select the best response.

A. All hosts in a local segment
B. All routers in a local segment
C. All hosts in a particular multicast group
D. All routers in an autonomous system

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

To identify all nodes for the node-local and link-local scopes, the following multicast addresses are defined:
· FF01::1 (node-local scope all-nodes address)
· FF02::1 (link-local scope all-nodes address)

To identify all routers for the node-local, link-local, and site-local scopes, the following multicast addresses are defined:
· FF01::2 (node-local scope all-routers address)
· FF02::2 (link-local scope all-routers address)
· FF05::2 (site-local scope all-routers address)

QUESTION 349
When an IPv6 enabled host boots, it sends a router solicitation (RS) message. An IPv6 router responds with a router advertisement (RA). Which two items are contained in the RA? (Choose two.)

A. IPv6 address for the host
B. Lifetime of the prefix
C. Prefixes for the link
D. Keepalive timers
E. Request for the local host IP address
F. Any route advertisements it has received

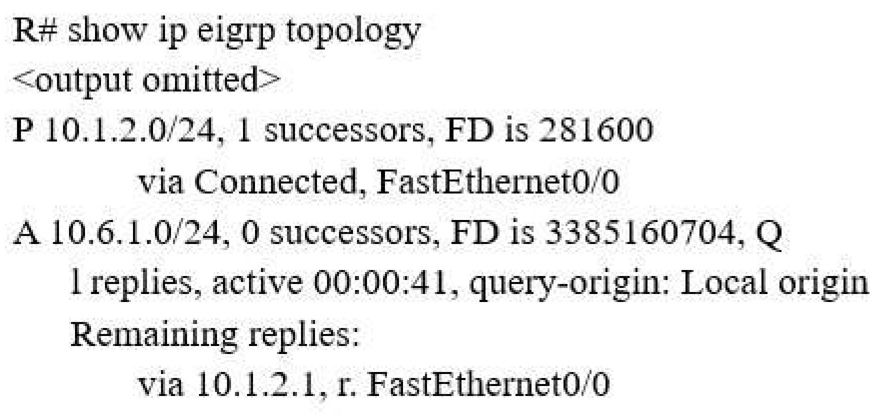
Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In IP Version 6, Router Advertisements have the following attributes:

1. Routers advertise periodically
-- Max. time between advertisements can be in the range from 4 and 1800 seconds
-- The advertisement has a lifetime (= 0 if not a default router)
2. Advertisement contains one or more prefixes
-- Prefixes have a lifetime
3. Preferred lifetime
4. Valid lifetime
5. Specifies if stateful or stateless autoconfiguration is to be used
6. Plays a key role in site renumbering

QUESTION 350
Refer to the exhibit. EIGRP is configured on all routers in the network. On a basis of the show ip eigrp topology output provided, what conclusion can be derived? Select the best response.



```
R# show ip eigrp topology
<output omitted>
P 10.1.2.0/24, 1 successors, FD is 281600
        via Connected, FastEthernet0/0
A 10.6.1.0/24, 0 successors, FD is 3385160704, Q
    1 replies, active 00:00:41, query-origin: Local origin
    Remaining replies:
        via 10.1.2.1, r. FastEthernet0/0
```

A. Router R1 can send traffic destined for network 10.6.1.0/24 out of interface FastEthernet0/0.
B. Router R1 is waiting for a reply from the neighbor 10.1.2.1 to the hello message sent out before it declares the neighbor unreachable.
C. Router R1 is waiting for a reply from the neighbor 10.1.2.1 to the hello message sent out inquiring for a second successor to network 10.6.1.0/24.
D. Router R1 is waiting for a reply from the neighbor 10.1.2.1 in response to the query sent out about network 10.6.1.0/24.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 351
An administrator types in the command router ospf 1 and receives the error message:

"OSPF process 1 cannot start." (Output is omitted.)

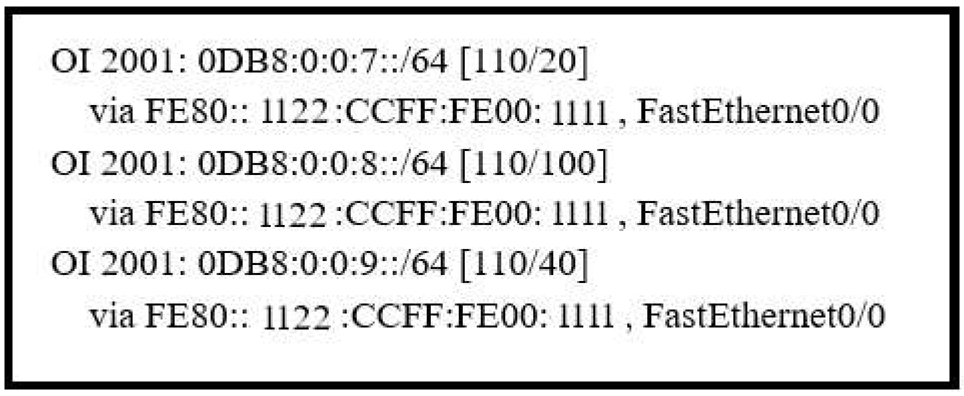
What should be done to correctly set up OSPF? Select the best response.

A. Ensure that an interface has been configured with an IP address.
B. Ensure that an interface has been configured with an IP address and is up.
C. Ensure that IP classless is enabled.
D. Ensure that the interfaces can ping their directly connected neighbors.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 352
The following exhibit shows ipv6 route output. What would the metric be for a summary route that summarizes all three OSPFv3 routes displayed?



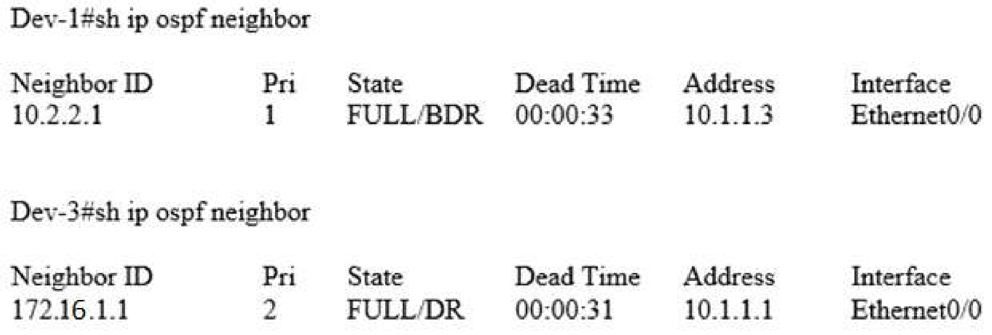
```
OI 2001: 0DB8:0:0:7::/64 [110/20]
   via FE80:: 1122 :CCFF:FE00: 1111 , FastEthernet0/0
OI 2001: 0DB8:0:0:8::/64 [110/100]
   via FE80:: 1122 :CCFF:FE00: 1111 , FastEthernet0/0
OI 2001: 0DB8:0:0:9::/64 [110/40]
   via FE80:: 1122 :CCFF:FE00: 1111 , FastEthernet0/0
```

A. 160
B. 140
C. 120
D. 100

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 353
The Dev-1 and Dev-3 routers are OSPF neighbors over the Ethernet 0/0 connection. Based on the show ip ospf neighbor output from the Dev-1 and Dev-3 routers, which statement is true? Select the best response.



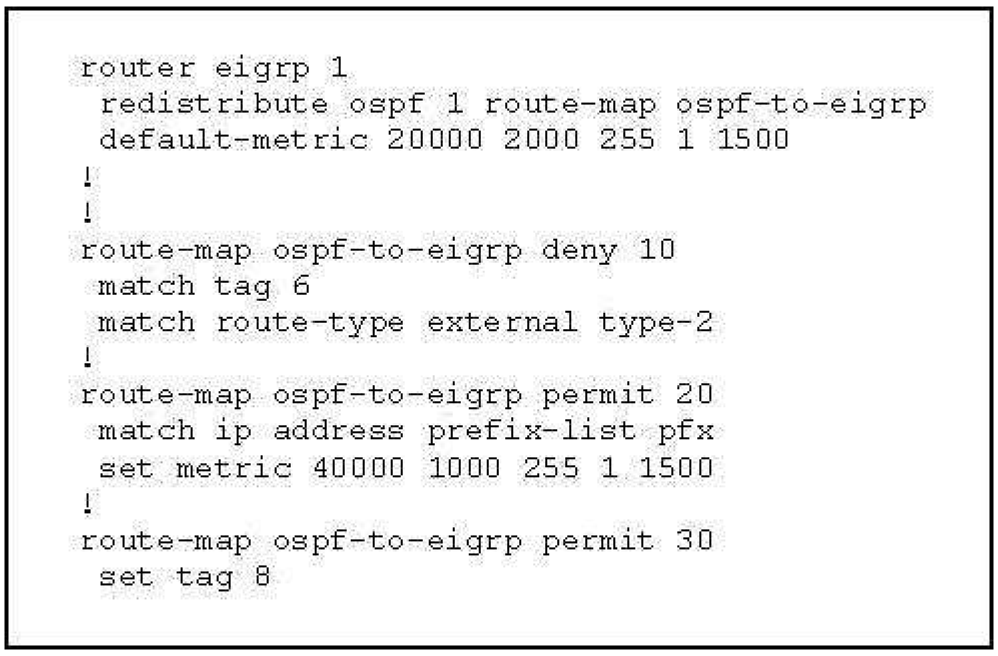
```
Dev-1#sh ip ospf neighbor

Neighbor ID     Pri   State      Dead Time   Address    Interface
10.2.2.1        1     FULL/BDR   00:00:33    10.1.1.3   Ethernet0/0


Dev-3#sh ip ospf neighbor

Neighbor ID     Pri   State      Dead Time   Address    Interface
172.16.1.1      2     FULL/DR    00:00:31    10.1.1.1   Ethernet0/0
```

A. Dev-1 is the DR because it has a higher OSPF router priority.
B. Dev-1 is the DR because it has a lower OSPF router ID.
C. Dev-3 is the DR because it has a higher OSPF router priority.
D. Dev-3 is the DR because it has a lower OSPF router ID.
E. Both Dev-1 and Dev-3 are using the default OSPF router priority.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 354
Refer to the exhibit. Which three statements accurately describe the result of applying the exhibited route map? (Choose three.)



```
router eigrp 1
 redistribute ospf 1 route-map ospf-to-eigrp
 default-metric 20000 2000 255 1 1500
!
!
route-map ospf-to-eigrp deny 10
 match tag 6
 match route-type external type-2
!
route-map ospf-to-eigrp permit 20
 match ip address prefix-list pfx
 set metric 40000 1000 255 1 1500
!
route-map ospf-to-eigrp permit 30
 set tag 8
```

A. The map prohibits the redistribution of all type 2 external OSPF routes with tag 6 set.
B. The map prohibits the redistribution of all type 2 external OSPF routes.
C. The map redistributes into EIGRP all routes that match the pfx prefix list and the five metric values 40000, 1000, 255, 1, and 1500.
D. The map prohibits the redistribution of all external OSPF routes with tag 6 set.
E. All routes that do no match clauses 10 and 20 of the route map are redistributed with their tags set to 8.
F. The map permits the redistribution of all type 1 external OSPF routes.

Correct Answer: AEF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
In the route-map:

route-map ospf-to-eigrp deny 10
match tag 6
match route-type external type-2

The deny clause rejects route matches from redistribution. If several match commands are present in a clause, all must succeed for a given route in order for that route to match the clause (in other words, the logical AND algorithm is applied for multiple match commands). In this question, both the “match tag 6” and “match route-type external type-2” must be matched for this route to be denied -> A is correct.

If a match command is not present, all routes match the clause. In this question, all routes that reach clause 30 match and their tags are set to 8 -> E is correct.

If a route is not matched with clause 10 or 20 then it will be matched with clause 30 for sure -> F is correct.

Option C is incorrect because it says the route will be redistributed if it matches the prefix-list pfx AND the metric values. This is not true.

The route-map statement 20 SETS the seed metric for the prefixes identified by the prefix-list pfx. So the statement in option C is missing the "SET" keyword.

Option F is correct because the only deny statement in route-map is statement 10 which only denies Type-2 External routes that have a tag value of 6. This means all Type-1 External routes will be redistributed because they will match either permit statement 20 or 30.

Note: Route-maps that are applied to redistribution behave the same way as ACLs: if the route does not match any clause in a route-map then the route redistribution is denied, as if the route-map contained deny statement at the end.

Reference:
http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a008047915d.shtml

QUESTION 355
Which IPv4-mapped IPv6 address is equivalent to IPv6 address ::ffff:AC11:AC11? Choose the best response.

A. ::ffff:10.12.10.12
B. ::ffff:10.14.10.14
C. ::ffff44.49.44.49
D. ::ffff161.193.161.193
E. ::ffff 172.17.172.17
F. ::ffff193.11.193.11

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 356
What are three key concepts that apply when configuring the EIGRP stub routing feature in a hub and spoke network? (Choose three.)

A. A hub router prevents routes from being advertised to the remote router.
B. Only remote routers are configured as stubs.
C. Stub routers are not queried for routes.
D. Spoke routers connected to hub routers answer the route queries for the stub router.
E. A stub router should have only EIGRP hub routers as neighbors.
F. EIGRP stub routing should be used on hub routers only.

Correct Answer: BCE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 357
What is the difference between the IPv6 addresses ::/0 and ::/128? Choose the best response.

A. ::/0 is the unspecified address, and ::/128 is the multicast address.
B. ::/0 is the unicast address, and ::/128 is the anycast address.
C. ::/0 is the unicast address, and ::/128 is the multicast address.
D. ::/0 is the anycast address, and ::/128 is the multicast address.
E. ::/0 is the default route, and ::/128 is the unspecified address.
F. ::/0 is the anycast address, and ::/128 is the default address.

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 358
Which statement is true about IPv6? Choose the best response.

A. Only one IPv6 address is assigned per node.
B. Only one IPv6 address can be assigned to each interface.
C. Each host can autoconfigure its address without the aid of a DHCP server.
D. IPv6 hosts use anycast addresses to assign IP addresses to interfaces.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 359
Using the rules for IPv6 addressing, how can the address 2031:0000:240F:0000:0000:09C0:123A:121B be rewritten? Select the best response.

A. 2031:0:240F::09C0:123A:121B
B. 2031::240F::09C0:123A:121B
C. 2031::240F:9C0::123A:121B
D. 2031::240F:::09C0:123A:121B

Correct Answer: A
Section: Mix Questions

Explanation

Explanation/Reference:
Explanation:
Leading zeros can be truncated.
For example "0000" can be be just written as empty. In the above example :: indicates that it has multiple 0's in that location.
Typically the IPv6 format can be written down in three ways 1) compressed, 2) uncompressed and 3) fully uncompressed as shown below. All of the following are the same:

QUESTION 360
Which statement is true about EBGP? Select the best response.

A. An internal routing protocol can be used to reach an EBGP neighbor.
B. The next hop does not change when BGP updates are exchanged between EBGP neighbors.
C. A static route can be used to form an adjacency between neighbors.
D. EBGP requires a full mesh.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 361
Which three are characteristics of IPv6? (Choose three.)

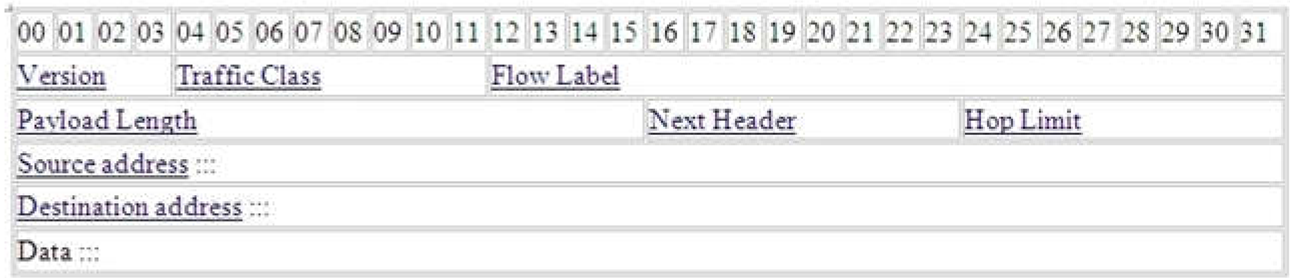
A. An IPv6 address is 128 bits long.
B. An IPv6 header is 20 bits long.
C. An IPv6 header contains the next header field.
D. An IPv6 header contains the protocol field.
E. IPv6 routers send RA messages.
F. An IPv6 header contains the header checksum field.

Correct Answer: ACE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

All IPv6 addresses are 128 bits long to accommodate a far larger number of stations than what was possible with the 32 bit IPv4 addresses.
The following displays the IPv6 header field in detail:

IPv6 header:



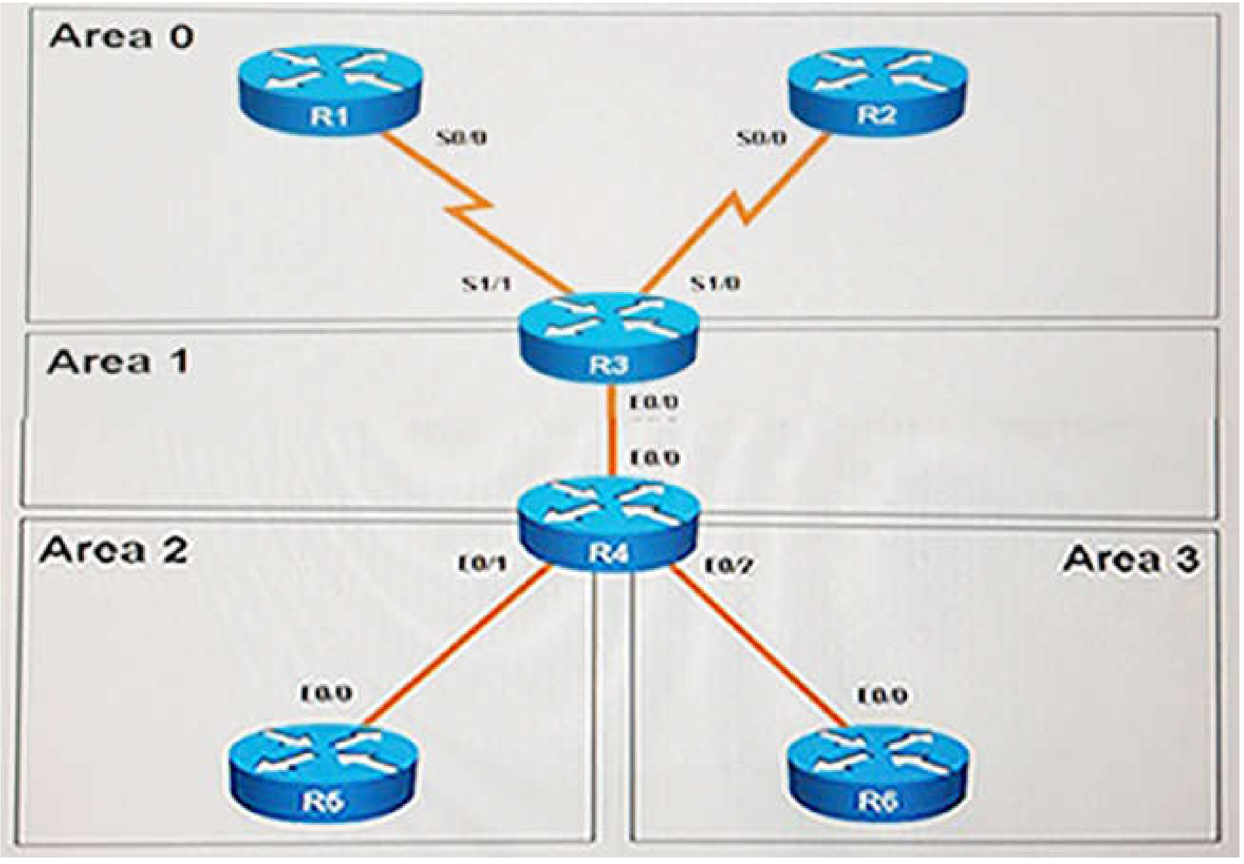
<table>
<tr><td>00</td><td>01</td><td>02</td><td>03</td><td>04</td><td>05</td><td>06</td><td>07</td><td>08</td><td>09</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td colspan="4">Version</td><td colspan="8">Traffic Class</td><td colspan="20">Flow Label</td></tr>
<tr><td colspan="16">Payload Length</td><td colspan="8">Next Header</td><td colspan="8">Hop Limit</td></tr>
<tr><td colspan="32">Source address :::</td></tr>
<tr><td colspan="32">Destination address :::</td></tr>
<tr><td colspan="32">Data :::</td></tr>
</table>

Version. 4 bits.IPv6 version number.
Traffic Class.8 bits.Internet traffic priority delivery value.
Flow Label. 20 bits.Used for specifying special router handling from source to destination(s) for a sequence of packets.
Payload Length. 16 bits unsigned.Specifies the length of the data in the packet. When cleared to zero, the option is a hop-by-hop Jumbo payload.
Next Header. 8 bits.Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.
Hop Limit. 8 bits unsigned.For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.
Source address. 16 bytes.The IPv6 address of the sending node.
Destination address. 16 bytes.The IPv6 address of the destination node.

QUESTION 362
Instructions:
- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- Click on icon or the tab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are four multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.

Scenario
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.

Topology:

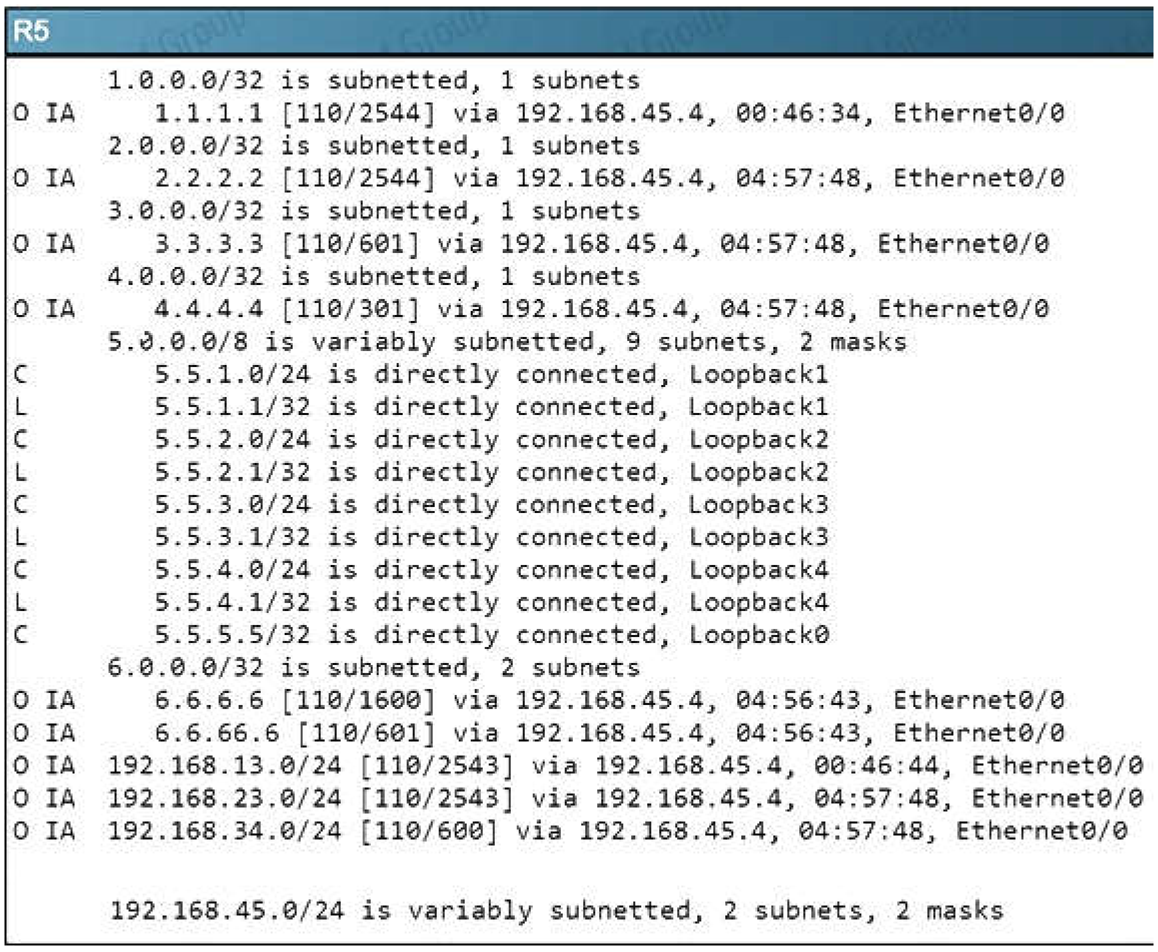


Areas of Router 5 and Router 6 are not normal areas. Which statement is true based on their routing tables?

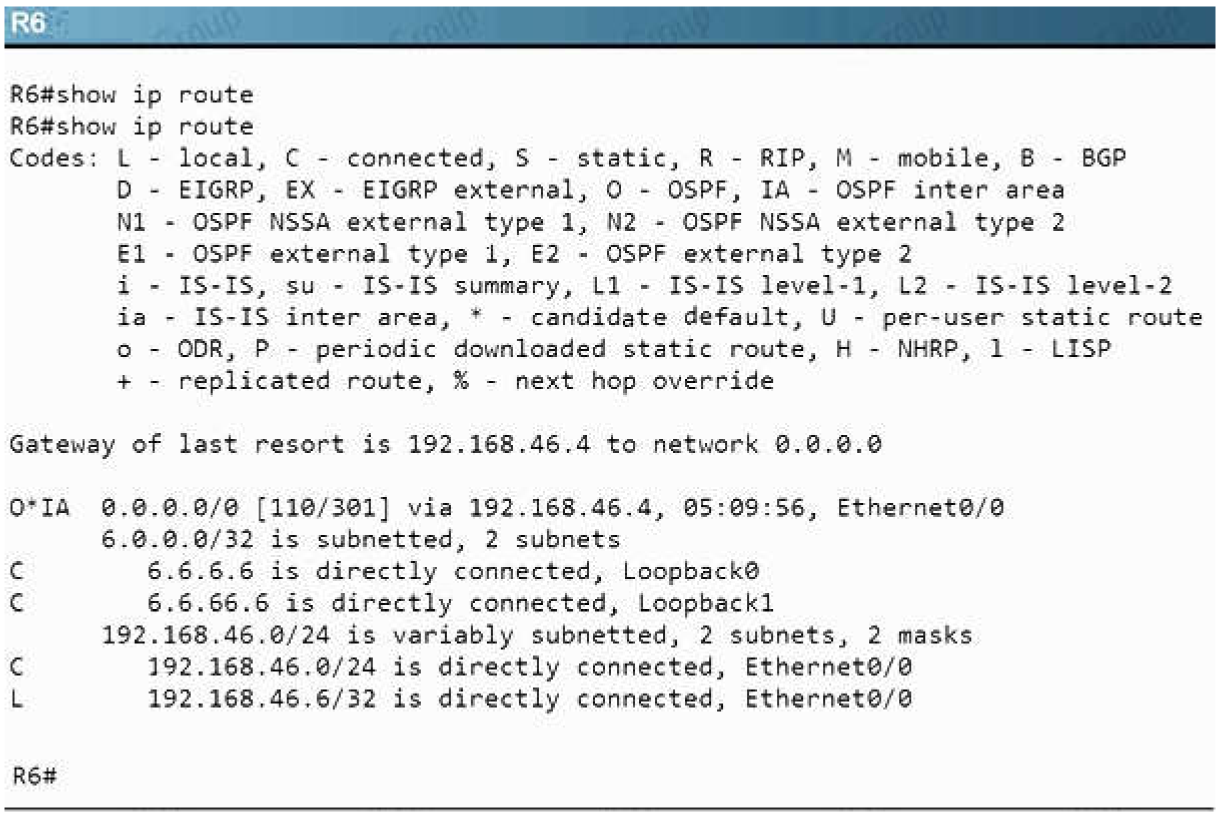
A. R5's Loopback and R6's Loopback are both present in R5's Routing table.
B. R5's Loopback and R6's Loopback are both present in R6's Routing table.
C. Only R5's Loopback is present in R5's Routing table.
D. Only R6's Loopback is present in R5's Routing table.
E. Only R5's Loopback is present in R6's Routing table.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Here are the routing tables of R5 and R6:

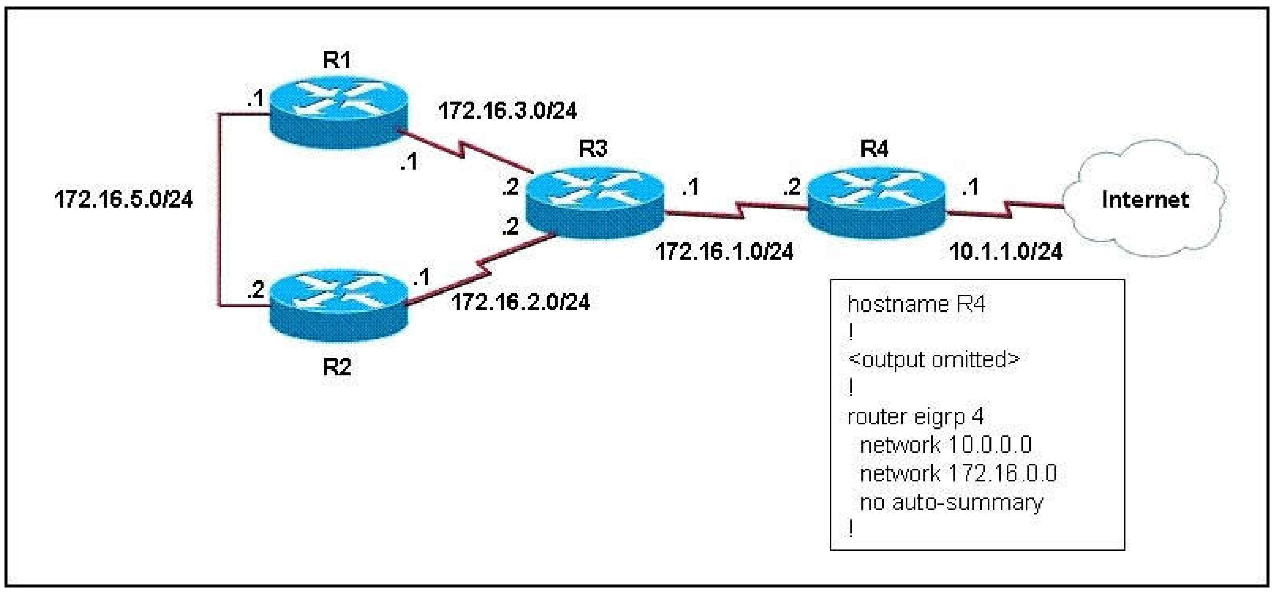


```
      1.0.0.0/32 is subnetted, 1 subnets
O IA     1.1.1.1 [110/2544] via 192.168.45.4, 00:46:34, Ethernet0/0
      2.0.0.0/32 is subnetted, 1 subnets
O IA     2.2.2.2 [110/2544] via 192.168.45.4, 04:57:48, Ethernet0/0
      3.0.0.0/32 is subnetted, 1 subnets
O IA     3.3.3.3 [110/601] via 192.168.45.4, 04:57:48, Ethernet0/0
      4.0.0.0/32 is subnetted, 1 subnets
O IA     4.4.4.4 [110/301] via 192.168.45.4, 04:57:48, Ethernet0/0
      5.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
C        5.5.1.0/24 is directly connected, Loopback1
L        5.5.1.1/32 is directly connected, Loopback1
C        5.5.2.0/24 is directly connected, Loopback2
L        5.5.2.1/32 is directly connected, Loopback2
C        5.5.3.0/24 is directly connected, Loopback3
L        5.5.3.1/32 is directly connected, Loopback3
C        5.5.4.0/24 is directly connected, Loopback4
L        5.5.4.1/32 is directly connected, Loopback4
C        5.5.5.5/32 is directly connected, Loopback0
      6.0.0.0/32 is subnetted, 2 subnets
O IA     6.6.6.6 [110/1600] via 192.168.45.4, 04:56:43, Ethernet0/0
O IA     6.6.66.6 [110/601] via 192.168.45.4, 04:56:43, Ethernet0/0
O IA  192.168.13.0/24 [110/2543] via 192.168.45.4, 00:46:44, Ethernet0/0
O IA  192.168.23.0/24 [110/2543] via 192.168.45.4, 04:57:48, Ethernet0/0
O IA  192.168.34.0/24 [110/600] via 192.168.45.4, 04:57:48, Ethernet0/0

      192.168.45.0/24 is variably subnetted, 2 subnets, 2 masks
```



```
R6#show ip route
R6#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is 192.168.46.4 to network 0.0.0.0

O*IA  0.0.0.0/0 [110/301] via 192.168.46.4, 05:09:56, Ethernet0/0
      6.0.0.0/32 is subnetted, 2 subnets
C        6.6.6.6 is directly connected, Loopback0
C        6.6.66.6 is directly connected, Loopback1
      192.168.46.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.46.0/24 is directly connected, Ethernet0/0
L        192.168.46.6/32 is directly connected, Ethernet0/0

R6#
```

QUESTION 363
Refer to the exhibit.



```
hostname R4
!
<output omitted>
!
router eigrp 4
 network 10.0.0.0
 network 172.16.0.0
 no auto-summary
!
```

EIGRP has been configured on all routers in the network. What additional configuration statement should be included on router R4 to advertise a default route to its neighbors?

A. R4(config)# ip default-network 10.0.0.0
B. R4(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1
C. R4(config)# ip route 10.0.0.0 255.0.0.0 10.1.1.1
D. R4(config-router)# default-information originate

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The “ip default-network ” command will direct other routers to send its unknown traffic to this network. Other router (R1,R2,R3) will indicate this network as the “Gateway of last resort”.

There is another way to route unknown traffic to 10.1.1.0/24 network: create a static route using “ip route 0.0.0.0 0.0.0.0 10.1.1.2” command then inject this route using the “network 0.0.0.0” command, or using “redistribute static” command.

Note: In EIGRP, default routes cannot be directly injected (as they can in OSPF with the default-information originate command. Also, EIGRP does not have the “default-information originate” command).

QUESTION 364
Which two statements are true about 6to4 tunnels? (Choose two.)

A. In a 6to4 tunnel, the first two bytes of the IPv6 address will be 2002 and the next four bytes will be the hexadecimal equivalent of the IPv4 address.
B. In a 6to4 tunnel, the first two bytes of the IPv6 address will be locally derived and the next two bytes will be the hexadecimal equivalent of the IPv4 address.
C. In a 6to4 tunnel, the IPv4 address 192.168.99.1 would be converted to the 2002:c0a8:6301::/48 IPv6 address.
D. In a 6to4 tunnel, the IPv4 address 192.168.99.1 would be converted to the 2002:c0a8:6301::/16 IPv6 address.
E. In a 6to4 tunnel, the IPv4 address 192.168.99.1 would be converted to the 2002:1315:4463:1::/64 IPv6 address.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
In a 6to4 tunnel, the first two bytes of the IPv6 address will be 0x2002 and the next four bytes will be the hexadecimal equivalent of the IPv4 address. The IPv4 address 192.168.99.1 would be converted to the 2002:c0a8:6301::/48 IPv6 address.

QUESTION 365
What does the command clear ipv6 ospf process accomplish? Select the best response.

A. The OSPF adjacencies are cleared and initiated again.
B. The route table is cleared. Then the OSPF neighbors are reformed.
C. The shortest path first (SPF) algorithm is performed on the LSA database.
D. The OSPF database is repopulated. Then the shortest path first (SPF) algorithm is performed.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The command "clear ipv6 ospf" will clear the present routing table and force the OSPFv3 process to build a new one. This command is often used when something in the network was changed or for debugging purpose.

When the "process" keyword is added, which means "clear ipv6 ospf process", the OSPF database is cleared and repopulated then the SPF algorithm is performed.

QUESTION 366
When implementing OSPFv3, which statement describes the configuration of OSPF areas? Select the best response.

A. In interface configuration mode, the OSPFv3 area ID combination assigns interfaces to OSPFv3 areas.
B. In router configuration mode, the network wildcard area ID combination assigns networks to OSPFv3 areas.
C. In interface configuration mode, the IPv6 OSPF process area ID combination assigns interfaces to OSPFv3 areas.
D. In router configuration mode, the IPv6 OSPF interface area ID combination assigns interfaces to OSPFv3 areas.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 367
How is authentication handled with OSPFv3? Select the best response.

A. OSPFv3 for IPv6 authentication is supported by SHA-1 authentication.
B. OSPFv3 for IPv6 authentication is supported by MD5 authentication.
C. OSPFv3 for IPv6 authentication is supported by IPv6 IPsec.
D. OSPFv3 for IPv6 authentication is supported by IPv4 IPsec.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 368
You have implemented mutual route redistribution between OSPF and EIGRP on a border router. When checking the routing table on one of the OSPF routers within the OSPF routing domain, you are seeing some, but not all of the expected routes. Which two things should you verify to troubleshoot this problem? (Choose two.)

A. The border router is using a proper seed metric for OSPF.
B. The border router is using a proper seed metric for EIGRP.
C. The administrative distance is set for OSPF and EIGRP.
D. The missing EIGRP routes are present in the routing table of the border router.
E. The subnet keyword on the border router in the redistribute EIGRP command.

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
We are checking the routing table on EIGRP routers not OSPF so we don't need to check the seed metric for OSPF. Besides OSPF doesn't need to specify seed metric as all external routes get a default metric of 20 (except for BGP, which is 1) -> A is not correct.

We must specify seed metrics when redistributing into EIGRP (and RIP). If not all the redistributed routes will not be seen but the question says only some routes are missing -> B is not correct.

The default administrative distance for external routes redistributed into EIGRP is 170 so we don't need to set it -> C is not correct.

We should check the routing table of the border router to see the missing OSPF routes are there or not. An incorrect distribute-list can block some routes and we can't see it in other EIGRP routers -> D is correct.

Answer D is obvious that we should check all the routes we want to redistribute are present in the routing table of the border router. Let's discuss about answer E.

A rule of thumb when redistributing into OSPF is we should always include the “subnets” keyword after the redistributed route. For example:

```
router ospf 1
redistribute eigrp 100 subnets
```

This keyword makes sure all of the routes, including subnets are redistributed correctly into OSPF. For example these routes are learned via EIGRP:

+ 192.168.1.0/24
+ 192.168.2.0/25
+ 192.168.3.0/26

Then without the keyword “subnets”, only 192.168.1.0/24 network is redistributed into OSPF.

QUESTION 369
Which three restrictions apply to OSPF stub areas? (Choose three)

A. No virtual links are allowed.
B. The area cannot be a backbone area.
C. Redistribution is not allowed unless the packet is changed to a type 7 packet.
D. The area has no more than 10 routers.
E. No autonomous system border routers are allowed.
F. Inter area routes are suppressed.

Correct Answer: ABE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 370
What is EIGRP Summary Route Administrative Distance?

A. 90
B. 170
C. 5
D. 110

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 371
What is the NHRP role in DMVPN? (Choose two.)

A. Obtains the next-hop to be used for routing
B. Routes the packet through the tunnel
C. Identifies the PIM-SM RP used to route the packet
D. Can authenticate VPN endpoints
E. It requires each tunnel endpoint to have a unique network ID

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 372
How does an EVN provide end-to-end virtualization and separation of data traffic from multiple networks?

A. It tags traffic with an 802.1q tag at the edge interface.
B. it tags traffic with an 802.1q tag at trunk interface.
C. it tags traffic with a virtual network tag at the trunk interface.
D. it tags traffic with a virtual network tag at the edge interface

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 373
Which two statements about EVNs are true? (Choose two.)

A. VRFs using MPLS require a trunk interface that uses EVN
B. VRF-Lite requires a trunk interface that uses EVN
C. All EVNs within a trunk interface can share the same IP infrastructure
D. Each EVN within a trunk interface must be configured separately
E. Commands that are specified once under a trunk interface can be inherited by all EVNs

Correct Answer: CE

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 374
Which two protocols are required for DMVPN? (Choose two.)

A. IPsec
B. PPTP
C. mGRE
D. NHRP
E. Open VPN

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
IPsec in DMVPN is Optional
required are mGRE and NHRP

DMVPN is not a protocol, it is the combination of the following technologies:
+ Multipoint GRE (mGRE)
+ Next-Hop Resolution Protocol (NHRP)
+ Dynamic Routing Protocol (EIGRP, RIP, OSPF, BGP…) (optional)
+ Dynamic IPsec encryption (optional)
+ Cisco Express Forwarding (CEF)

DMVPN combines multiple GRE (mGRE) Tunnels, IPSec encryption and NHRP (Next Hop Resolution Protocol) to perform its job and save the administrator the need to define multiple static crypto maps and dynamic discovery of tunnel endpoints.

QUESTION 375
A network administrator uses GRE over IPSec to connect two branches together via VPN tunnel. Which one of the following is the reason for using GRE over IPSec?

A. GRE over IPSec provides better QoS mechanism and is faster than other WAN technologies
B. GRE over IPSec decreases the overhead of the header.
C. GRE supports use of routing protocol, while IPSec supports encryption.
D. GRE supports encryption, while IPSec supports use of routing protocol.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Following are the management protocols that the MPP feature supports.
These management protocols are also the only protocols affected when MPP is enabled.

QUESTION 376
Which statement is true about an IPsec/GRE tunnel?

A. The GRE tunnel source and destination addresses are specified within the IPsec transform set.
B. An IPsec/GRE tunnel must use IPsec tunnel mode.
C. GRE encapsulation occurs before the IPsec encryption process.
D. Crypto map ACL is not needed to match which traffic will be protected.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 377
For a GRE tunnel to be up between two routers, which of the following must be configured?

A. Loopback Interface
B. IP reachability between the loopback interfaces
C. Dynamic Routing between routers.
D. Tunnel interfaces must be in the same subnet.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 378
Which values identifies VPNs in an EVN environment?

A. DLCI
B. Route target

C. Virtual network tag
D. VLAN ID

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:
https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/layer-3-vpns-l3vpn/whitepaper_c11-638769.html

QUESTION 379
What are the four main steps in configuring a GRE tunnel over IPsec on Cisco routers? (Choose four.)

A. Configure a physical interface or create a loopback interface to use as the tunnel endpoint.
B. Create the GRE tunnel interfaces.
C. Add the tunnel interfaces to the routing process so that it exchanges routing updates across that interface.
D. Add the tunnel subnet to the routing process so that it exchanges routing updates across that interface.
E. Add all subnets to the crypto access-list, so that IPsec encrypts the GRE tunnel traffic.
F. Add GRE traffic to the crypto access-list, so that IPsec encrypts the GRE tunnel traffic.

Correct Answer: ABDF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Four steps to configure GRE tunnel over IPsec are:

1. Create a physical or loopback interface to use as the tunnel endpoint. Using a loopback rather than a physical interface adds stability to the configuration.
2. Create the GRE tunnel interfaces.
3. Add the tunnel subnet to the routing process so that it exchanges routing updates across that interface.
4. Add GRE traffic to the crypto access list, so that IPsec encrypts the GRE tunnel traffic.

An example of configuring GRE Tunnel is shown below:

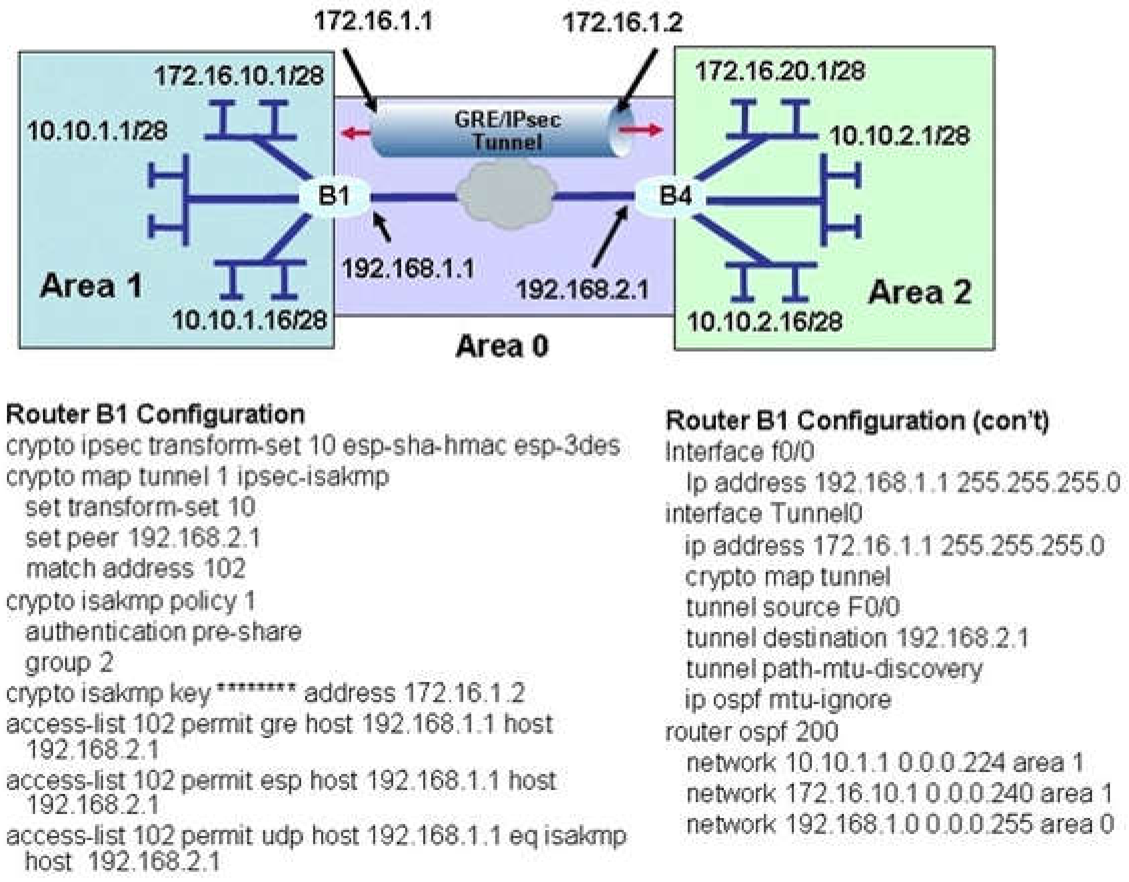
```
interface Tunnel0
ip address 192.168.16.2 255.255.255.0
tunnel source FastEthernet1/0
tunnel destination 14.38.88.10
tunnel mode gre ip
```

Note: The last command is enabled by default so we can ignore it in the configuration)

(Reference: CCNP Routing and Switching Quick Reference)

QUESTION 380
Refer to the exhibit. A new TAC engineer came to you for advice. A GRE over IPsec tunnel was configured, but the tunnel is not coming up.

What did the TAC engineer configure incorrectly?



Router B1 Configuration

```
crypto ipsec transform-set 10 esp-sha-hmac esp-3des
crypto map tunnel 1 ipsec-isakmp
  set transform-set 10
  set peer 192.168.2.1
  match address 102
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp key ******** address 172.16.1.2
access-list 102 permit gre host 192.168.1.1 host
  192.168.2.1
access-list 102 permit esp host 192.168.1.1 host
  192.168.2.1
access-list 102 permit udp host 192.168.1.1 eq isakmp
  host  192.168.2.1
```

Router B1 Configuration (con't)

```
Interface f0/0
  Ip address 192.168.1.1 255.255.255.0
interface Tunnel0
  ip address 172.16.1.1 255.255.255.0
  crypto map tunnel
  tunnel source F0/0
  tunnel destination 192.168.2.1
  tunnel path-mtu-discovery
  ip ospf mtu-ignore
router ospf 200
  network 10.10.1.1 0.0.0.224 area 1
  network 172.16.10.1 0.0.0.240 area 1
  network 192.168.1.0 0.0.0.255 area 0
```

A. The crypto isakmp configuration is not correct.
B. The crypto map configuration is not correct.
C. The interface tunnel configuration is not correct.
D. The network 172.16.1.0 is not included in the OSPF process

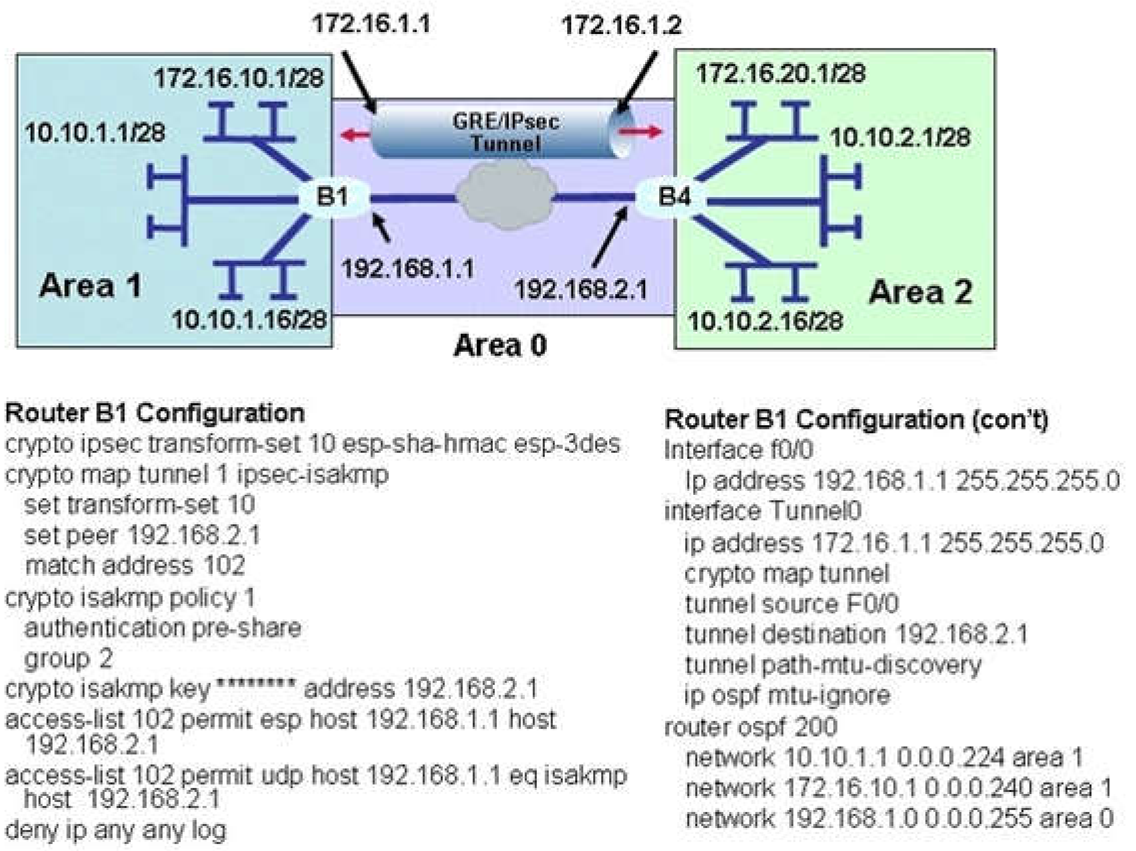
Correct Answer: A

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The address of the crypto isakmp key should be 192.168.1.2, not 172.16.1.2 -> A is correct.

QUESTION 381
Refer to the exhibit. A new TAC engineer came to you for advice. A GRE over IPsec tunnel was configured, but the tunnel is not coming up.

What did the TAC engineer configure incorrectly?



Router B1 Configuration

```
crypto ipsec transform-set 10 esp-sha-hmac esp-3des
crypto map tunnel 1 ipsec-isakmp
  set transform-set 10
  set peer 192.168.2.1
  match address 102
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp key ******** address 192.168.2.1
access-list 102 permit esp host 192.168.1.1 host
  192.168.2.1
access-list 102 permit udp host 192.168.1.1 eq isakmp
  host  192.168.2.1
deny ip any any log
```

Router B1 Configuration (con't)

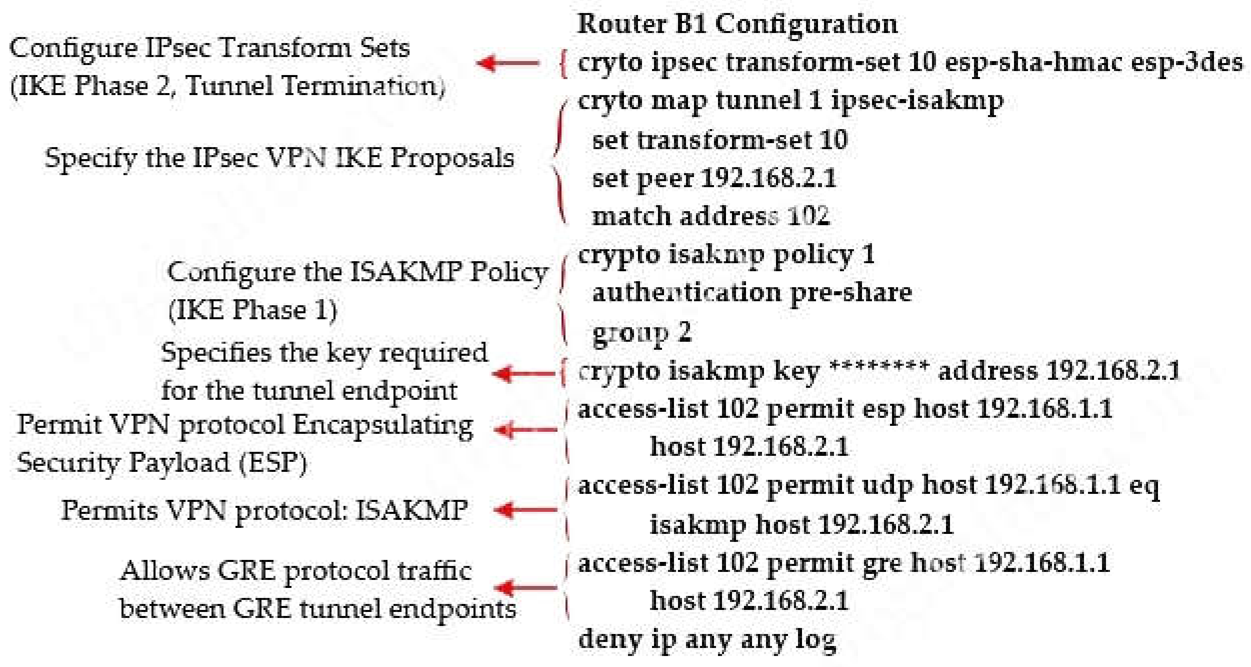
```
Interface f0/0
  Ip address 192.168.1.1 255.255.255.0
interface Tunnel0
  ip address 172.16.1.1 255.255.255.0
  crypto map tunnel
  tunnel source F0/0
  tunnel destination 192.168.2.1
  tunnel path-mtu-discovery
  ip ospf mtu-ignore
router ospf 200
  network 10.10.1.1 0.0.0.224 area 1
  network 172.16.10.1 0.0.0.240 area 1
  network 192.168.1.0 0.0.0.255 area 0
```

A. The crypto map is not configured correctly
B. The crypto ACL is not configured correctly.
C. The crypto map is not applied to the correct interface.
D. The OSPF network is not configured correctly.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The access-list must also support GRE traffic with the “access-list 102 permit gre host 192.168.1.1 host 192.168.2.1” command -> B is correct.

Below is the correct configuration for GRE over IPsec on router B1 along with descriptions.



Configure IPsec Transform Sets (IKE Phase 2, Tunnel Termination)

Specify the IPsec VPN IKE Proposals

Configure the ISAKMP Policy (IKE Phase 1)

Specifies the key required for the tunnel endpoint

Permit VPN protocol Encapsulating Security Payload (ESP)

Permits VPN protocol: ISAKMP

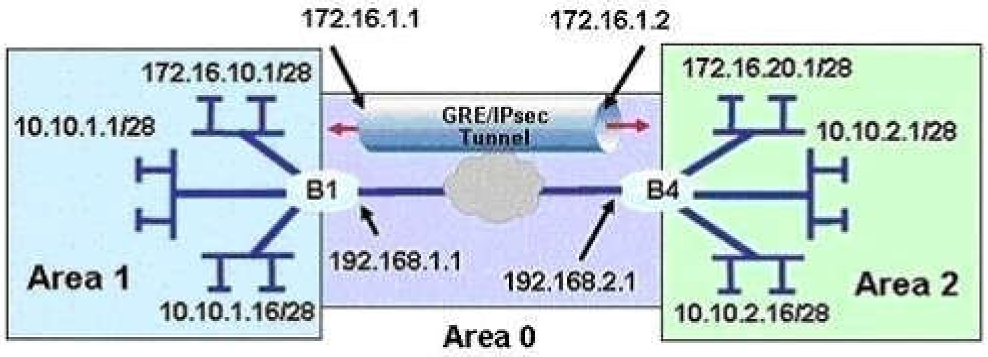
Allows GRE protocol traffic between GRE tunnel endpoints

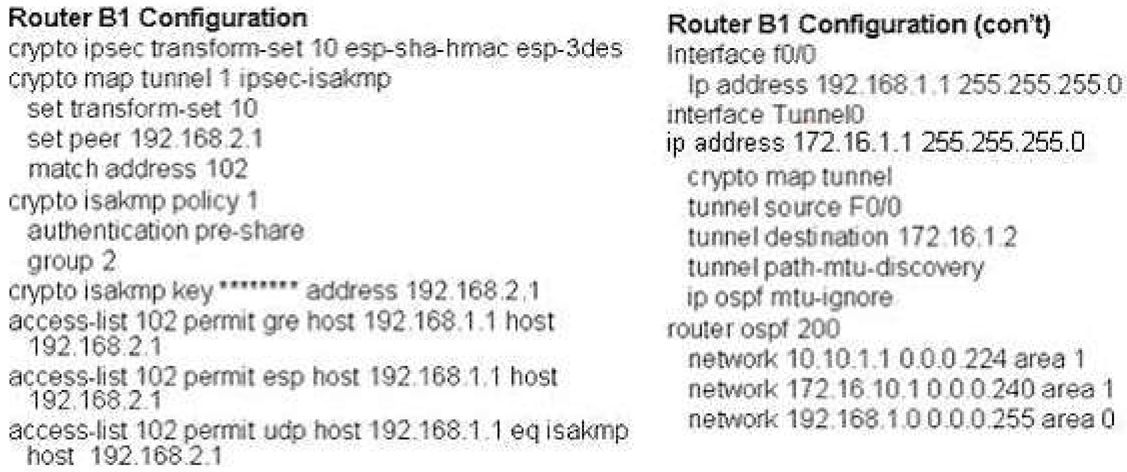
Router B1 Configuration

```
cryto ipsec transform-set 10 esp-sha-hmac esp-3des
cryto map tunnel 1 ipsec-isakmp
  set transform-set 10
  set peer 192.168.2.1
  match address 102
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp key ******** address 192.168.2.1
access-list 102 permit esp host 192.168.1.1
      host 192.168.2.1
access-list 102 permit udp host 192.168.1.1 eq
      isakmp host 192.168.2.1
access-list 102 permit gre host 192.168.1.1
      host 192.168.2.1
deny ip any any log
```

QUESTION 382
Refer to the exhibit. A new TAC engineer came to you for advice. A GRE over IPsec tunnel was configured, but the tunnel is not coming up.

What did the TAC engineer configure incorrectly?





Router B1 Configuration

```
crypto ipsec transform-set 10 esp-sha-hmac esp-3des
crypto map tunnel 1 ipsec-isakmp
  set transform-set 10
  set peer 192.168.2.1
  match address 102
crypto isakmp policy 1
  authentication pre-share
  group 2
crypto isakmp key ******** address 192.168.2.1
access-list 102 permit gre host 192.168.1.1 host
  192.168.2.1
access-list 102 permit esp host 192.168.1.1 host
  192.168.2.1
access-list 102 permit udp host 192.168.1.1 eq isakmp
  host  192.168.2.1
```

Router B1 Configuration (con't)

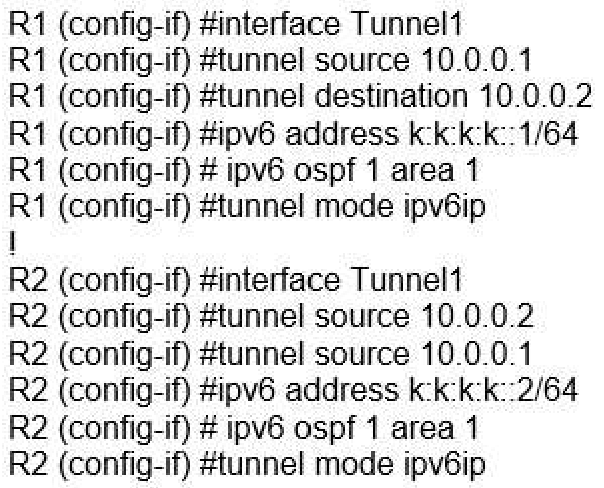
```
Interface f0/0
  Ip address 192.168.1.1 255.255.255.0
interface Tunnel0
ip address 172.16.1.1 255.255.255.0
  crypto map tunnel
  tunnel source F0/0
  tunnel destination 172.16.1.2
  tunnel path-mtu-discovery
  ip ospf mtu-ignore
router ospf 200
  network 10.10.1.1 0.0.0.224 area 1
  network 172.16.10.1 0.0.0.240 area 1
  network 192.168.1.0 0.0.0.255 area 0
```

A. The crypto isakmp configuration is not correct.
B. The crypto map configuration is not correct.
C. The network 172.16.1.0 is not included in the OSPF process.
D. The interface tunnel configuration is not correct.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The “tunnel destination” in interface tunnel should be 192.168.1.2, not 172.16.1.2 -> D is correct.

QUESTION 383
Refer to exhibit. A user calls from another branch office with a request to establish a simple VPN tunnel to test a new router's tunneling capability Based on the configuration in the exhibit, which type of tunnel was configured?



```
R1 (config-if) #interface Tunnel1
R1 (config-if) #tunnel source 10.0.0.1
R1 (config-if) #tunnel destination 10.0.0.2
R1 (config-if) #ipv6 address k:k:k:k::1/64
R1 (config-if) # ipv6 ospf 1 area 1
R1 (config-if) #tunnel mode ipv6ip
!
R2 (config-if) #interface Tunnel1
R2 (config-if) #tunnel source 10.0.0.2
R2 (config-if) #tunnel source 10.0.0.1
R2 (config-if) #ipv6 address k:k:k:k::2/64
R2 (config-if) # ipv6 ospf 1 area 1
R2 (config-if) #tunnel mode ipv6ip
```

A. PPTP
B. IPsec site-to-site
C. 6to4
D. EZVPN

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 384
What two features are benefits of using GRE tunnels with IPsec over using an IPsec tunnel alone in building-to-building site-to-site VPNs? (Choose two.)

A. Allows dynamic routing securely over the tunnel
B. IKE keepalives are unidirectional and sent every ten seconds
C. Reduces IPsec headers overhead since tunnel mode is used
D. Supports non-IP traffic over the tunnel
E. uses Virtual Tunnel Interface (VTI) to simplify the IPsec VPN configuration

Correct Answer: AD
Section: Mix Questions

Explanation

Explanation/Reference:
Explanation:
A drawback of IPSec is it does not support multicast traffic. But most popular routing protocols nowadays rely on multicast (like OSPF, EIGRP, RIP… except BGP) to send their routing updates. A popular solution to this is using GRE tunnels. GRE tunnels do support transporting IP multicast and broadcast packets to the other end of the GRE tunnel -> A is correct.

Non-IP traffic (such as IPX, AppleTalk) can be wrapped inside GRE encapsulation and then this packet is subjected to IPSec encapsulation so all traffic can be routed -> D is correct.

QUESTION 385
Which of the following is a GRE Tunnel characteristic?

A. GRE impose more CPU overhead than IPSec on VPN gateways
B. GRE tunnels can run through IPsec tunnels.
C. GRE Tunnel doesn't have support for IPv6
D. GRE consists of two sub-protocols: Encapsulated Security Payload (ESP) and Authentication Header (AH).

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
If you run an IPsec tunnel through a GRE tunnel, then we call it as "IPsec over GRE"

QUESTION 386
Router R1, a branch router, connects to the Internet using DSL. Some traffic flows through a GRE and IPsec tunnel, over the DSL connection, destined for an Enterprise network. Which of the following answers best describes the router's logic that tells the router, for a given packet, to apply GRE encapsulation to the packet?

A. When the packet received on the LAN interface is permitted by the ACL listed on the tunnel gre acl command under the incoming interface
B. When routing the packet, matching a route whose outgoing interface is the GRE tunnel interface
C. When routing the packet, matching a route whose outgoing interface is the IPsec tunnel interface
D. When permitted by an ACL that was referenced in the associated crypto map

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
As for the correct answer: the process of routing a packet out a GRE tunnel interface triggers the GRE encapsulation action.

As for the incorrect answers: There is no tunnel gre acl command. There is no IPsec tunnel interface. Finally, one answer refers to logic that would describe a router's logic when determining whether to encapsulate a packet into an IPsec tunnel.

QUESTION 387
What is a key benefit of using a GRE tunnel to provide connectivity between branch offices and headquarters?

A. Authentication, integrity checking, and confidentiality
B. Less overhead
C. Dynamic routing over the tunnel
D. Granular QoS support
E. Open standard
F. Scalability

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Generic routing encapsulation. Tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork.

QUESTION 388
Which two statement about GRE tunnel interface are true? (Choose two.)

A. A tunnel can be established when a source the source interface is in the up/down state
B. A tunnel Destination must be Routable, but it can be unreachable
C. To establish a tunnel the source interface must be a loopback
D. To Establish a tunnel the source interface must be up/up state
E. A tunnel destination must be a physical interface that is on up/up state

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Reference:
http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/118361-technote-gre-00.html

QUESTION 389

Which two statements about EVN are true? (Choose two.)

A. Virtual network tags are assigned per-VRF.
B. It is supported only on access ports.
C. Virtual network tags are assigned globally.
D. Routing metrics can be manipulated only from directly within the routing-context configuration.
E. The VLAN ID in the 802.1q frame carries the virtual network tag.
F. The VLAN ID is the ISL frame carries the virtual network tag.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 390
A network engineer recently deployed Easy Virtual Networking in the enterprise network.
Which feature improves shared services support?

A. Route replication
B. Edge interfacing
C. Tunnel feedback
D. Route distinguishers

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Route Replication. It allows shared services between VRF in a more powerful way than BGP. It allows routes to be shared between the Global route table and other VRFs without limitations. BGP can only share 5 VRFs with 1000 routes per VRF in this situation.

QUESTION 391
Which two phases of DMVPN allow to spoke sites to create dynamic tunnels to one another? (Choose two.)

A. Phase1
B. Phase 2
C. Phase 3
D. Phase 4
E. Phase 5

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 392
Which two GRE features can you configure to prevent fragmentation? (Choose two.)

A. TCP MSS
B. DF Bit Clear
C. IP MTU
D. PMTUD
E. MTU ignore
F. UDP windows sizes

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html

QUESTION 393
When the tunnel interface is configured in default mode, which statement about routers and the tunnel destination address is true?

A. The router must have a route installed towards the tunnel destination
B. The router must have wccp redirects enabled inbound from the tunnel destination
C. The router must have cisco discovery protocol enabled on the tunnel to form a CDP neigborship with the tunnel destination
D. The router must have redirects enabled outbound towards the tunnel destination

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 394
One of the AAA Authentication PPP Methods if PAP used ____.

A. krb5
B. ssl
C. transliteration methods
D. UPN

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Uses Kerberos 5 for authentication (can only be used for PAP authentication)

QUESTION 395
What to configure on routes if TACACS+ authentication fails? (Choose two.)

A. Configure local username and password
B. Include 'local' keyword in AAA config
C. aaa accounting exec default start-stop tacacs+
D. ip ssl certificate-data-file tftp 192.168.9.210 certfile

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
device(config)#enable telnet authentication
device(config)#aaa authentication login default tacacs local

The commands above cause TACACS/TACACS+ to be the primary authentication method for securing Telnet/SSH access to the CLI. If TACACS/TACACS+ authentication fails due to an error with the server, authentication is performed using local user accounts instead.

Reference:
http://www.brocade.com/content/html/en/configuration-guide/FI_08030_SECURITY/GUID-162894DA-A189-4A10-AE28-BD31214D62BA.html

QUESTION 396
Which two statements about password-protecting device access are true? (Choose two.)

A. The more system: running-config command displays encrypted passwords in clear text
B. The service password-encryption command forces a remote device to encrypt the password before transmitting it
C. A network administrator can recover an encrypted password
D. The privilege level command controls the commands a specific user can execute
E. The password can be encrypted in the running configuration

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 397
What is the minimum privilege level to enter all commands in user mode?

A. Level14
B. Level0
C. Level1
D. Level15

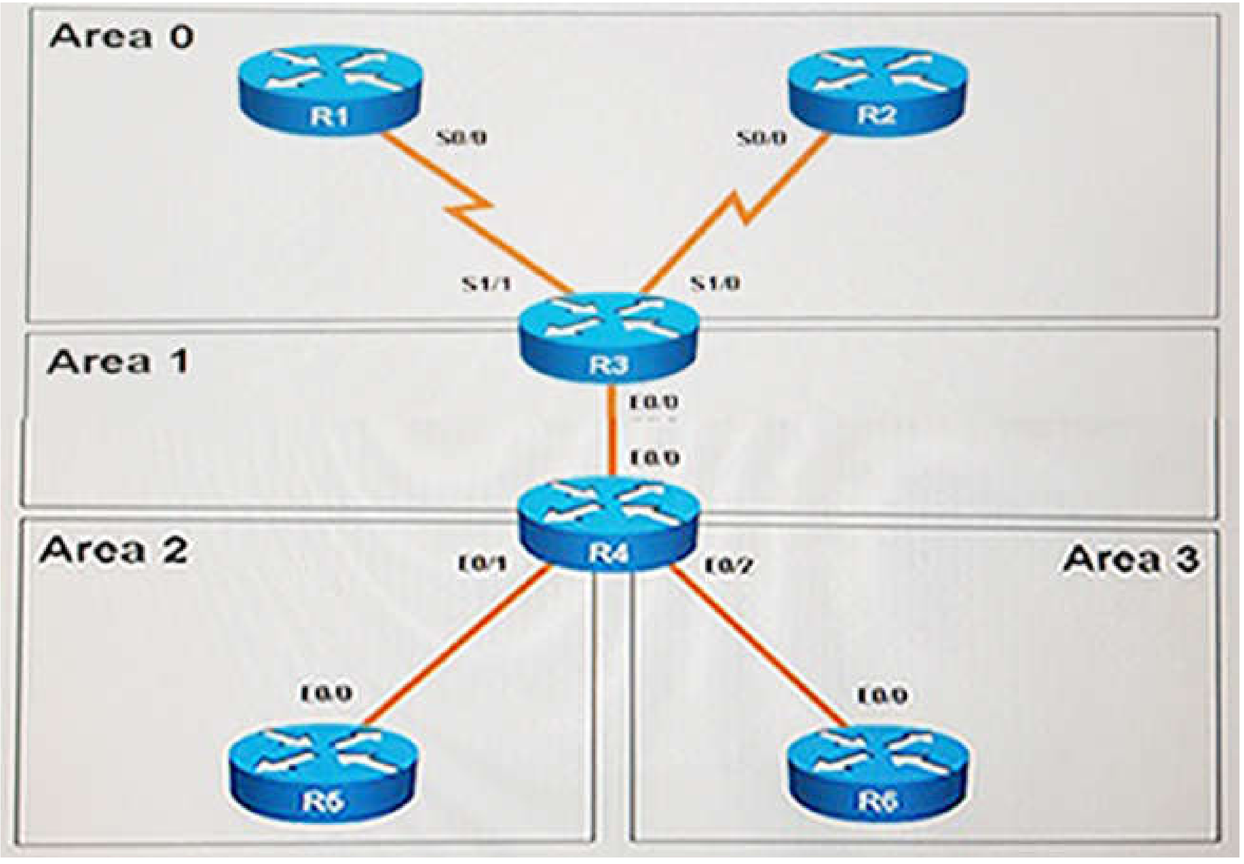
Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 398
Instructions:
- Enter IOS commands on the device to verify network operation and answer for multiple-choice questions.
- THIS TASK DOES NOT REQUIRE DEVICE CONFIGURATION.
- Click on icon or the tab at the bottom of the screen to gain access to the console for each device.
- No console or enable passwords are required.
- To access the multiple-choice questions, click on the numbered boxes on the left of the top panel.
- There are four multiple-choice questions with this task. Be sure to answer all four questions before selecting the Next button.

Scenario
You have been asked to evaluate an OSPF network setup in a test lab and to answer questions a customer has about its operation. The customer has disabled your access to the show running-config command.

Topology:

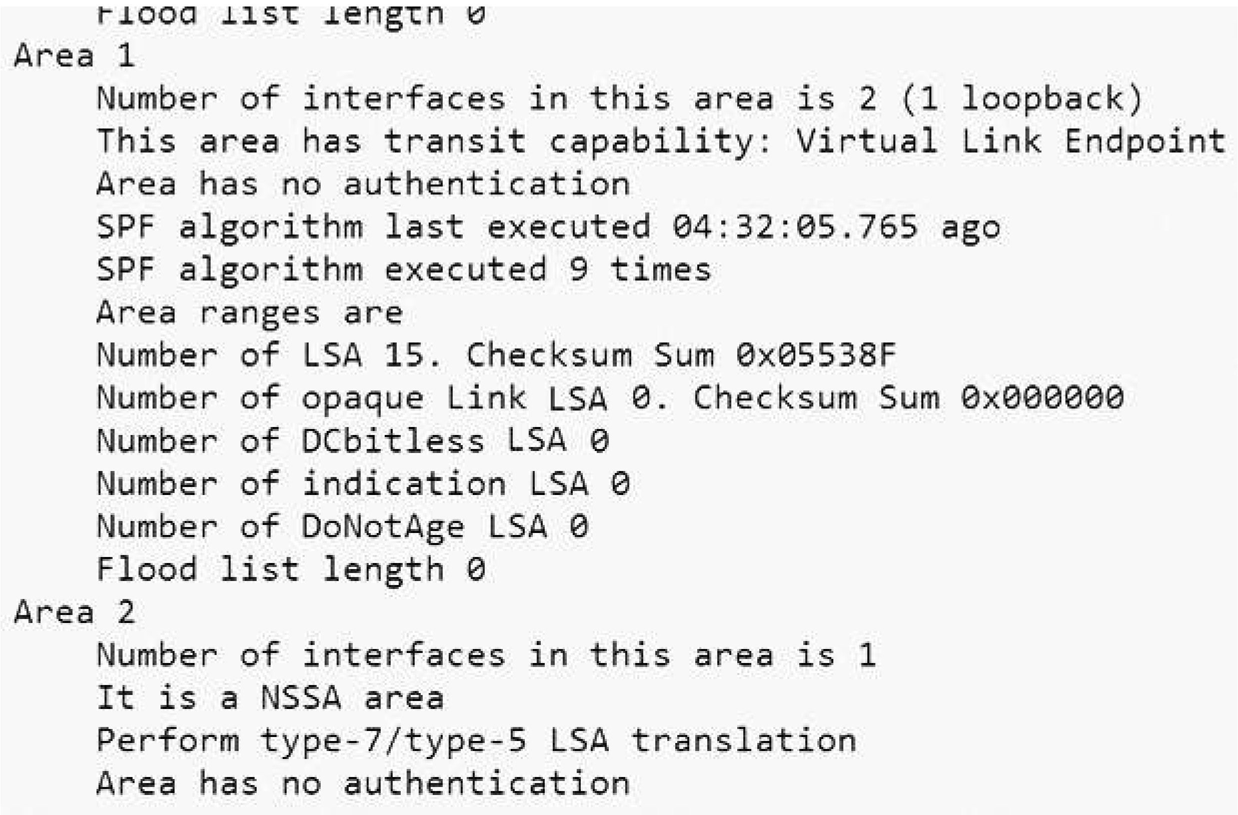


How many times was SPF algorithm executed on R4 for Area 1?

A. 1
B. 5
C. 9
D. 20
E. 54
F. 224

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
This can be found using the “show ip ospf” command on R4. Look for the Area 1 stats which shows this:



```
    Flood list length 0
Area 1
    Number of interfaces in this area is 2 (1 loopback)
    This area has transit capability: Virtual Link Endpoint
    Area has no authentication
    SPF algorithm last executed 04:32:05.765 ago
    SPF algorithm executed 9 times
    Area ranges are
    Number of LSA 15. Checksum Sum 0x05538F
    Number of opaque Link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
Area 2
    Number of interfaces in this area is 1
    It is a NSSA area
    Perform type-7/type-5 LSA translation
    Area has no authentication
```

QUESTION 399
The Cisco SA 500 Series Security Appliances are built specifically for businesses with less than 100 employees. What are three important benefits of this device? (Choose three.)

A. Business-grade firewall
B. Premium support via SMART net
C. Site-to-site VPN for remote offices
D. Cisco IOS software-based
E. Email security
F. XML support

Correct Answer: ACE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 400
Which two methods use IPsec to provide secure connectivity from the branch office to the headquarters office? (Choose two.)

A. DMVPN
B. MPLS VPN
C. Virtual Tunnel Interface (VTI)
D. SSL VPN
E. PPPoE

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The Dynamic Multipoint VPN (DMVPN) feature allows users to better scale large and small IPSec VPNs by combining generic routing encapsulation (GRE) tunnels, IPSec encryption, and Next Hop Resolution Protocol (NHRP) to provide users with easy configuration through crypto profiles, which override the requirement for defining static crypto maps, and dynamic discovery of tunnel endpoints.

The use of VTI greatly simplifies the configuration process when you need to configure IPsec. A major benefit associated with IPsec VTIs is that the configuration does not require a static mapping of IPsec sessions to a physical interface.

Reference:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008014bcd7.shtml

QUESTION 401
What is the command to enable IPv6 access list?

A. ipv6 traffic-filter access-list-name { in | out }
B. ipv6 access-list [access-list-name]
C. access-list ipv6 [access-list-name]
D. ipv6 access-group [access-list-name] { in | out }

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 402
When unicast reverse path forwarding is configured on an interface, which action does the interface take first when it receives a packet?

A. It verifies that the source has a valid CEF adjacency.
B. It checks the egress access lists.
C. It verifies a reverse path via the FIB to the source.
D. It checks the ingress access lists.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 403
What are 2 protocols used for user with authentication on network device?

A. CHAP
B. Radius
C. 802.1x
D. PAP
E. TACACS+

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 404
Other than a working EIGRP configuration, which components must be the same on all routers for EIGRP authentication key rollover to work correctly?

A. SMTP
B. time
C. SNMP
D. passwords

Correct Answer: B
Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 405
Which of the following are characteristics of TACACS+? (Choose two.)

A. Uses UDP
B. Encrypts an entire packet
C. Offers robust accounting
D. Cisco-proprietary

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
CHARACTERISTICS O TACACS+
1-TACACS+ encrypts the entire body of the packet
2- TACACS+ uses TCP
3-TACACS+ uses the AAA architecture, which separates AAA 4-TACACS+ offers multiprotocol support.
5-TACACS+ is Cisco proprietary protocol
6-TACACS+ is a heavy-weight protocol consuming more resources 7-TACACS+ uses TCP port 8-Mainly used for Device Administration
9-TACACS+ supports 15 privilege levels

Reference:
http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html

QUESTION 406
Which command sequence can you enter a router to configure Unicast Reverse Path Forwarding in loose mode?

A. interface GigabitEthernet0/0
ip verify unicast source reachable-via loose.
B. interface GigabitEthernet0/0
ip verify unicast source reachable-via all.
C. interface GigabitEthernet0/0
ip verify unicast source reachable-via any.
D. interface GigabitEthernet0/0
ip verify unicast source reachable-via rx.

Correct Answer: C
Section: Mix Questions
Explanation

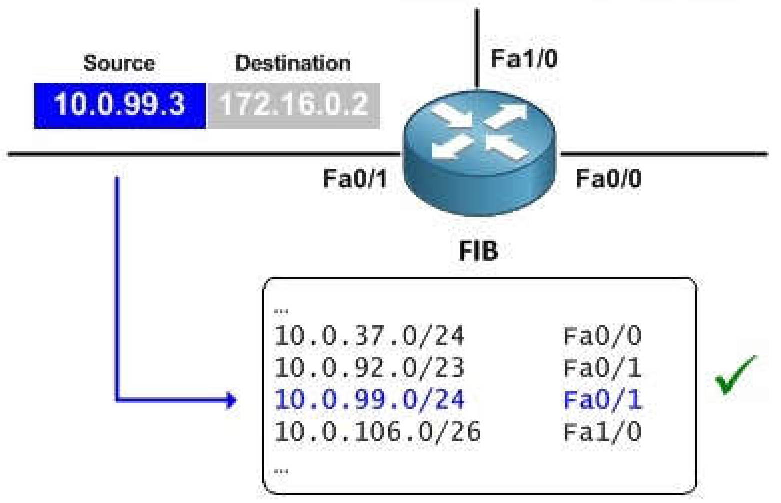
Explanation/Reference:

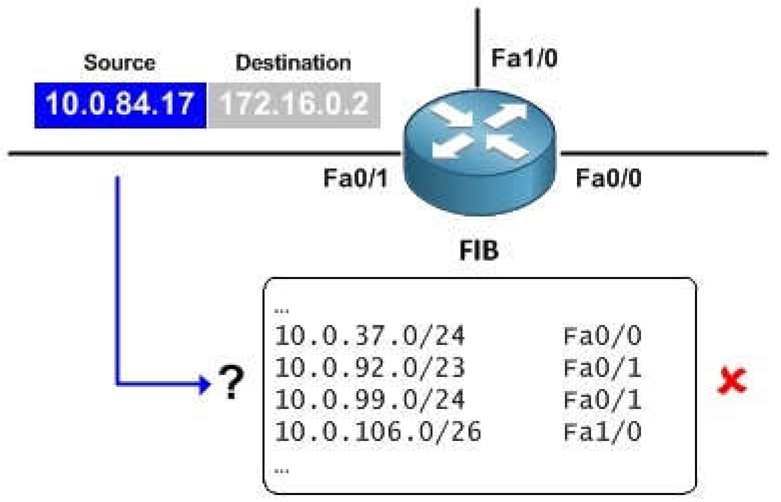
QUESTION 407
Which mode of uRPF causes a router interface to accept a packet, if the network to which the packet's source IP address belongs is found in the router's FIB?

A. Strict mode
B. Loose mode
C. Auto mode
D. Desirable mode

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:





A number of common types of DoS attacks take advantage of forged or rapidly changing source IP addresses, allowing attackers to thwart efforts by ISPs to locate or filter these attacks. Unicast RPF was originally created to help mitigate such attacks by providing an automated, scalable mechanism to implement the Internet Engineering Task Force (IETF) Best Common Practices 38/Request for Comments 2827 (BCP 38/RFC 2827) anti-spoofing filtering on the customer-to- ISP network edge. By taking advantage of the information stored in the Forwarding Information Base (FIB) that is created by the Unicast RPF can determine whether IP packets are spoofed or malformed by CEF switching process matching the IP source address and ingress interface against the FIB entry that reaches back to this source (a so-called reverse lookup). Packets that are received from one of the best reverse path routes back out of the same interface are forwarded as normal. If there is no reverse path route on the same interface from which the packet was received, it might mean that the source address was modified, and the packet is dropped (by default).

Reference: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_urpf/configuration/xe-3s/sec-data-urpf-xe-3s-book/sec-unicast-rpf-loose-mode.html?referring_site=RE&pos=1&page=http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/srpf_gsr.html#GUID-FFFA94D5-EEFB-4215-9EE1-DB37CD01C2CA

QUESTION 408
Which access list used to filter upper layer protocol?

A. Extended acl
B. Standart acl
C. Reflexive acl
D. Time based acl
E. Dynamic acl

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Remember the three Ps **P**er protocol, **P**er direction, and **P**er interface

One ACL per protocol- To control traffic flow on an interface an ACL must be defined for each protocol enabled on the interface (example IP, IPX, AppleTalk)
One ACL per direction- ACLs control traffic in one direction at one time on an interface. You must create two separate ACLs to control traffic in both inbound and outbound connections.
One ACL per interface- ACLs control traffic for an interface such as Fast Ethernet.

Dynamic ACLs

Dynamic or lock-and-key ACLs are available for Internet Protocol traffic only. Dynamic ACLs starts with the application of an extended ACL to block traffic through the router.

Common reasons to use Dynamic ACLs are:

When you want a specific remote user or group of remote users to access a host within your network.
Connecting to the outside of your network (Internet) Lock-and-key authenticates the user and then permits limited access through your firewall router.
You want a subset of hosts on a local network to access a host from a remote network that is protected by a firewall.
Lock-and-key requires users to authenticate through an AAA, TACACS server or other security server before it allows access.

Reflexive ACLs

Reflexive ACLs allow IP packets to be filtered based on upper-layer session information. Generally are used to allow outbound traffic and to limit inbound traffic by using sessions that originate inside the router. When a router sees a new outbound connection it adds an entry to a temporary ACL to allow replies back into the network. Reflexive ACLs can be defined only with an extended named IP ACL. They cannot be defined with numbered or standard named ACLs or with other protocols.

Time-Based ACLs

Time-Based ACLs are like extended ACLs in function, but they allow access control based on time. To use time-based ACLs you create a time range that defines specific times of the day and days of the week. You use the time range with a name and then refer to it by a function. The time range relies on the router system clock. This feature works with NTP (Network Time Protocol) synchronization, but the router clock can also be used.

Numbered ACL

You can assign a number based on whether your ACL is standard or extended

1 to 99 and 1300 to 1999 are Standard IP ACL
100 to 199 and 2000 to 2699 are Extended IP ACL
You cannot add or delete entries within the ACL (You have to totally delete the ACL in order to edit it)

Named ACL

You can assign names to the ACL instead of numbers.

Names can contain alphanumeric characters
Recommended to type the name in all CAPITAL LETTERS
Names cannot contain spaces or punctuation and must begin with an alphabetic character
You can add or delete entries within the ACL
You can specify whether the ACL is standard or extended

QUESTION 409
Which option is one way to mitigate symmetric routing on an active/active firewall setup for TCP-based connections?

A. Performing packet captures
B. Disabling asr-group commands on interfaces that are likely to receive asymmetric traffic
C. Replacing them with redundant routers and allowing load balancing
D. Disabling stateful TCP checks

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 410
Which allowing website access between certain times?

A. Filters using Time-Based ACLs
B. Standard ACL
C. Extended ACL
D. Reflexive ACL

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

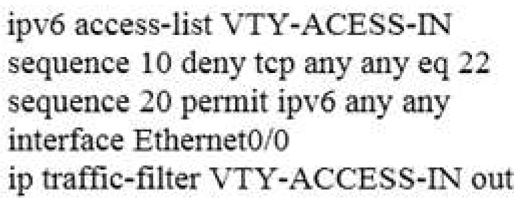
QUESTION 411
Which configuration is applied to a device so that it blocks outbound web traffic on Saturdays and Sundays between the hours of 1:00 AM and 11:59 PM?

A.
```
time-range SATSUN absolute Saturday Sunday 1:00 to 23:59
access-list 102 deny tcp any any eq 80 time-range SATSUN
access-list 102 deny tcp any any eq 443 time-range SATSUN
interface Vlan303
ip address 10.9.5.3 255.255.255.0
ip access-group 102 in
```
B.
```
time-range SATSUN periodic Saturday Sunday 1:00 to 23:59
access-list 102 deny tcp any any eq 80 time-range SATSUN
access-list 102 deny tcp any any eq 443 time-range SATSUN
interface VLAN303
ip address 10.9.5.3 255.255.255.0
ip access-group 102 in
```
C.
```
time-range SATSUN periodic Saturday Sunday 1:00 to 11:59
access-list 102 deny tcp any any eq 80 time-range SATSUN
access-list 102 deny tcp any any eq 443 time-range SATSUN
interface Vlan303
ip address 10.9.5.3 255.255.255.0
ip access-group 102 in
```
D.
```
time-range SATSUN periodic Saturday Sunday 1:00 to 23:59
access-list 102 deny udp any any eq 80 time-range SATSUN
access-list 102 deny tcp any any eq 443 time-range SATSUN
interface Vlan303
ip address 10.9.5.3 255.255.255.0
ip access-group 102 out
```

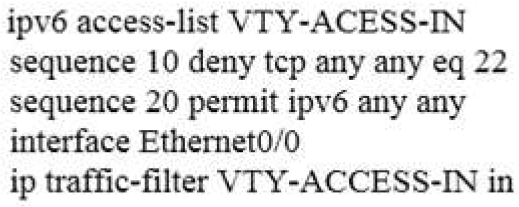
Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

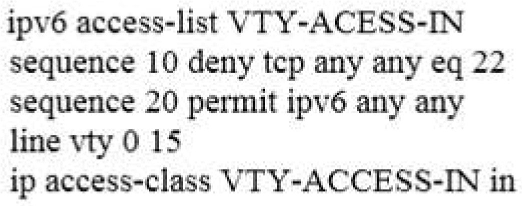
QUESTION 412
Which two different configurations can you apply to a device to block incoming SSH access? (Choose two.)

A. 

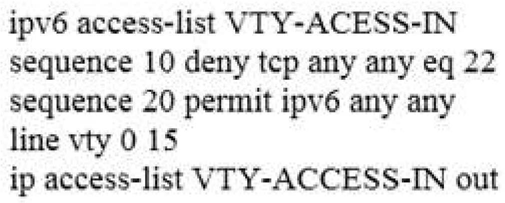
```
ipv6 access-list VTY-ACESS-IN
sequence 10 deny tcp any any eq 22
sequence 20 permit ipv6 any any
interface Ethernet0/0
ip traffic-filter VTY-ACCESS-IN out
```

B. 

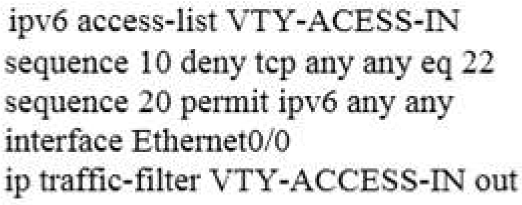
```
ipv6 access-list VTY-ACESS-IN
sequence 10 deny tcp any any eq 22
sequence 20 permit ipv6 any any
interface Ethernet0/0
ip traffic-filter VTY-ACCESS-IN in
```

C. 

```
ipv6 access-list VTY-ACESS-IN
sequence 10 deny tcp any any eq 22
sequence 20 permit ipv6 any any
line vty 0 15
ip access-class VTY-ACCESS-IN in
```

D. 

```
ipv6 access-list VTY-ACESS-IN
sequence 10 deny tcp any any eq 22
sequence 20 permit ipv6 any any
line vty 0 15
ip access-list VTY-ACCESS-IN out
```

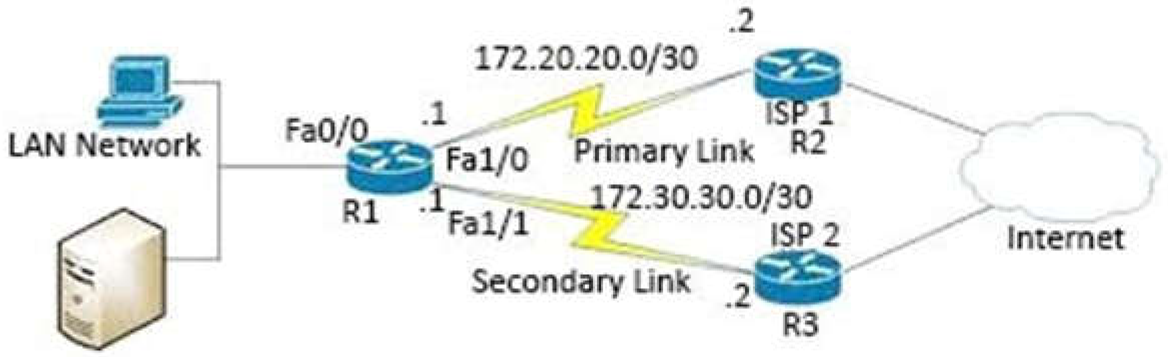
E. 

```
ipv6 access-list VTY-ACESS-IN
sequence 10 deny tcp any any eq 22
sequence 20 permit ipv6 any any
interface Ethernet0/0
ip traffic-filter VTY-ACCESS-IN out
```

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 413
Refer to Exhibit.



```
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo172.20.20.2 source-interface FastEthernet 1/0
R1(config-ip-sla-echo)#timeout 5000
R1(config-ip-sla-echo)#frequency 10
R1(config-ip-sla-echo)#threshold 500
R1(config)#ip sla schedule 1 start-time now life forever
R1(config)#track 10 ip sla 1 reachability
R1(config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2  track 10
R1(config)#no ip route 0.0.0.0.0.0.0.0 172.20.20.2
R1(config)#ip route 0.0.0.0.0.0.0.0 172.30.30.2.5
```

Which two reasons for IP SLA tracking failure are likely true? (Choose two.)

A. The source-interface is configured incorrectly.
B. The destination must be 172.30.30.2 for icmp-echo.
C. A route back to the R1 LAN network is missing in R2.
D. The default route has wrong next hop IP address.
E. The threshold value is wrong.

Correct Answer: AC
Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 414
What is the minimum level that displays a log message when an ACL drops an incoming packet?

A. 4
B. 5
C. 3
D. 7
E. 6

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 415
Which Netflow version supports MPLS?

A. None
B. All of them
C. Version 8 and 9
D. Version 9

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
MPLS-aware NetFlow uses the NetFlow Version 9 export format. If you are exporting MPLS data to a NetFlow collector or a data analyzer, the collector must support NetFlow Version 9 flow export format, and you must configure NetFlow export in Version 9 format on the router.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fsmnf25.html

QUESTION 416
Which option is a prerequisite for stateful NAT64?

A. IPsec for IPv6
B. DNS64
C. Application Layer Gateway
D. ICMP64

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 417
Which of the following are features of Netflow version 9?

A. Cisco proprietary
B. IEEE standard
C. IETF standard
D. ingress
E. egress
F. ingress/egress

Correct Answer: CF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 418
What do we prioritize with LLQ?

A. Voice
B. Data
C. Video
D. Queues

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

Explanation:
Low Latency Queueing with Priority Percentage Support

Specifying the Bandwidth Percentage: Example
The following example uses the priority percent command to specify a bandwidth percentage of 10 percent for the class called voice-percent. Then the bandwidth remaining percent command is used to specify a bandwidth percentage of 30 percent for the class called data1, and a bandwidth percentage of 20 percent for the class called data2.

```
Router> enable
 Router# configure terminal
 Router(config)# policy-map policy1
 Router(config-pmap)# class voice-percent
 Router(config-pmap-c)# priority percent 10
 Router(config-pmap-c)# class data1
 Router(config-pmap-c)# bandwidth remaining percent 30
 Router(config-pmap-c)# class data2
 Router(config-pmap-c)# bandwidth remaining percent 20
 Router(config-pmap-c)# end
```

As a result of this configuration, 10 percent of the interface bandwidth is guaranteed for the class called voice-percent. The classes called data1 and data2 get 30 percent and 20 percent of the remaining bandwidth, respectively.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12sllqpc.html

QUESTION 419
Refer to the exhibit.

```
configure terminal
ip flow-export destination 192.168.10.1 9991
ip flow-export version 9
```

How can you configure a second export destination for IP address 192.168.10.1?

A. Specify a different TCP port
B. Specify a different UDP port
C. Specify a VRF
D. Configure a version 5 flow-export to the same destination
E. Specify a different flow ID

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Note Do not enter the same ip address twice. However, entering two different ip addresses with the same udp port number is configurable

Reference:
https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/12s_mdnf.html

QUESTION 420
Which two statements about VRRP object tracking are true? (Choose two.)

A. VRRP supports only interface tracking.
B. A VRRP group can track only one object at a time.
C. The priority of a VRRP device can change in accordance with the up or down status of a VRRP object.
D. VRRP can track the status of interfaces and routes.
E. The VRRP interface priority must be manually configured by the administrator.

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 421
If you configure one router in your network with the auto-cost reference bandwidth 100 command, which effect on the data path is true?

A. The data path remains the same for all links.
B. The data path changes for 10 Mbps links only.
C. The data path changes for all links
D. The data path changes for 10 Gbps links only.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 422
Router R1, a branch router, connects to the Internet using DSL. Some traffic flows through a GRE and IPsec tunnel, over the DSL connection, and into the core of an Enterprise network. The branch also allows local hosts to communicate directly with public sites in the Internet over this same DSL connection. Which of the following answers defines how the branch NAT config avoids performing NAT for the Enterprise directed traffic but does perform NAT for the Internet-directed traffic?

A. By not enabling NAT on the IPsec tunnel interface
B. By not enabling NAT on the GRE tunnel interface
C. By configuring the NAT-referenced ACL to not permit the Enterprise traffic
D. By asking the ISP to perform NAT in the cloud

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The NAT configuration acts only on packets permitted by a referenced ACL. As a result, the ACL can permit packets destined for the Internet, performing NAT on those packets. The ACL also denies packets going to the Enterprise, meaning that the router does not apply NAT to those packets.

QUESTION 423
Which two addresses types are included in NAT?

A. Inside global
B. Global outside
C. Outside internet
D. Inside internet
E. Outside local

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 424
Which two statements about NetFlow templates are true? (Choose two.)

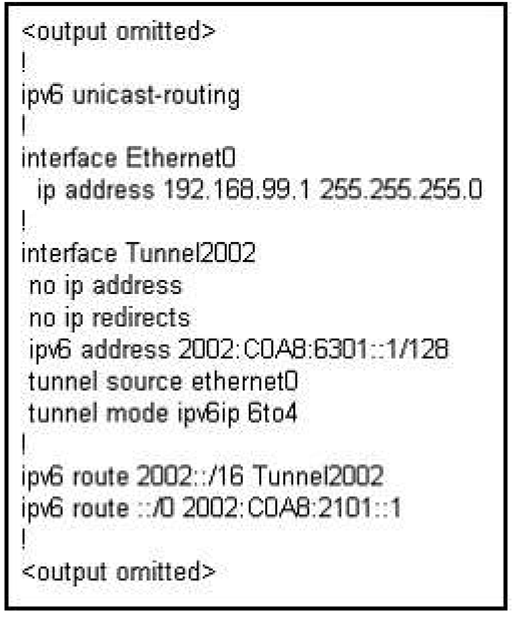
A. Only NetFlow version 9 is template based.
B. NetFlow Version 5 and version 9 are template based.
C. Only NetFlow version 5 is template based.
D. Template can increase bandwidth usage.
E. They can increase overall performance.
F. They can reduce bandwidth usage.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Reference:
https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html

QUESTION 425
Refer to the exhibit. Given the partial configuration in the exhibit, which IPv6 statement is true?



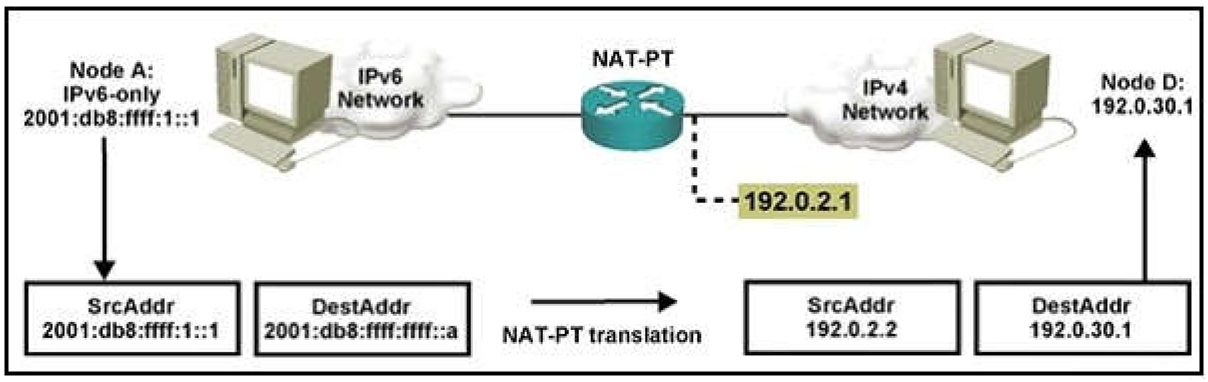
```
<output omitted>
!
ipv6 unicast-routing
!
interface Ethernet0
  ip address 192.168.99.1 255.255.255.0
!
interface Tunnel2002
 no ip address
 no ip redirects
 ipv6 address 2002:C0A8:6301::1/128
 tunnel source ethernet0
 tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 Tunnel2002
ipv6 route ::/0 2002:C0A8:2101::1
!
<output omitted>
```

A. The configuration is an example of an encrypted IPv6 VPN tunnel.
B. The configuration is an example of a one to one IPv6 tunnel.
C. The configuration is an example of a 6to4 tunnel.
D. The configuration is an example of a 4to6 tunnel.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 426
Refer to the exhibit.



Which statement is correct regarding the operation of NAT-PT between the IPv4 and IPv6 networks shown?

A. The router will determine the IPv4 destination address.
B. The source IPv6 host can use DNS to determine the IPv6-to-IPv4 address mapping.
C. The host is statically configured with the IPv6-to-IPv4 address mapping.
D. ICMP can be used to determine the IPv6-to-IPv4 address mapping.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 427
The network engineer types the follow commands in a router:

```
logging host 172.16.10.12
logging trap 5
```

What do these commands do?

A. Export messages of notifications for an external server
B. Show notifications in cli
C. Sends info to host 172.16.10.12 with notifications less than or equal to 5
D. Sends info to host 172.16.10.12 with notifications greater than or equal to 5

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 428
A packet capture indicates that the router is not forwarding the DHCP packets that it receives on interface FastEthernet0/0.

Which command needs to be entered in global configuration mode to resolve this issue?

A. ip helper-address
B. ip DHCP relay
C. service DHCP
D. ip forward-protocol

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 429
Which SNMP version provides both encryption and authentication?

A. SNMPv4
B. SNMPv2c
C. SNMPv3
D. SNMPv1

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

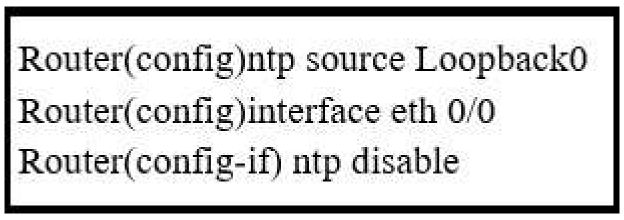
QUESTION 430
A network engineer wants to verify the status of a recently configured NTP setup on one of the routers. The engineer executes the show ntp associations command.
What does the output indicate?

A. The synchronized NTP servers that are configured on the device.
B. The authentication mode that is used with the NTP server.
C. The security key value for the configured NTP server.
D. The facility that is configured for the NTP server.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 431
Refer to the Exhibit.



```
Router(config)ntp source Loopback0
Router(config)interface eth 0/0
Router(config-if) ntp disable
```

Which statement about the configuration on the Cisco router is true?

A. The router sends only NTP traffic using the loopback interface, and it disables eth0/0 from sending NTP traffic.
B. Eth0/0 sends NTP traffic on behalf of the loopback interface
C. The router sends only NTP traffic, using the eth0/0 interface, and it disables loopback0 from sending NTP traffic.
D. The router never sends NTP traffic, as using the loopback interface for NTP traffic is not supported on IOS routers.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 432
Which option to the command service timestamps debug enables the logging server to capture the greatest amount of information from the router?

A. Uptime
B. Show-timezone
C. Year
D. msec

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The “msec” keyword enables millisecond (msec) timestamps for the debug, which indicates the date and time according to the system clock in the format MMM DD HH:MM:SS.

Reference:
https://www.cisco.com/c/en/us/support/docs/dial-access/integrated-services-digital-networks-isdn-channel-associated-signaling-cas/10374-debug.html

QUESTION 433
NPTv6 restrictions? (Choose all that apply.)

A. Virtual Routing and Forwarding (VRF)
B. NAT64 on the same interface.
C. Multicast and Firewall is not supported.
D. Payload address or port translation is not supported.
E. Syslog is not supported.

Correct Answer: ABCDE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Restrictions for NPTv6 support on ASR1k/CSR1k/ISR4k

Virtual Routing and Forwarding (VRF) is not supported by NPTv6 support on ASR1k/CSR1k/ISR4k feature.
NPTv6 support on ASR1k/CSR1k/ISR4k does not support configuring NAT64 on the same interface.
Multicast is not supported.
Firewall is not supported.
Application Level Gateways (ALG) is not supported by NPTv6 support on ASR1k/CSR1k/ISR4k feature. **Payload** address or port translation is not supported.
High Speed Logging (HSL) and **syslog** is not supported.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-16/nat-xe-16-book/iadnat-asr1k-nptv6.html

QUESTION 434
Which option can you use to monitor voice traffic when configuring an IP SLA?

A. udp-jitter
B. tcp-jitter
C. ip sla logging traps
D. ip sla reaction-configuration

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 435
Technologies used in preparing Service Provider IPv6? (Choose two.)

A. 6ND
B. 6RD
C. 6VPE
D. VRF-Lite
E. DS-Lite
F. Dual-stackA

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 436
What show command is used here?

```
TCB Local Address Foreign Address (state)
6523A4FC 10.1.25.3.11000 10.1.25.3.23 ESTAB
65239A84 10.1.25.3.23 10.1.25.3.11000 ESTAB
653FCBBC *.1723 *.* LISTEN
```

A. show tcp brief
B. show tcp brief all
C. show tcp brief numeric
D. show tcp brief ip

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The following example shows the IP activity and the addresses in DNS hostname format.

```
Router# show tcp brief all

TCB          Local Address            Foreign Address        (state)
36AE9520     a00.lsanca04.us..37888   a02.lsanca04.us..179    ESTAB
36B861F8     a00.lsanca04.us..23      gnat.cisco.com.33908    ESTAB
32F0A0A4     a00.lsanca04.us..179     a01.lsanca04.us..11002  ESTAB
369CEAD4     a00.lsanca04.us..23      gnat.cisco.com.33948    ESTAB
36B873A8     ge-1-2.a00.lsanc.11266   d3-0-1-0.r01.roc.23     ESTAB
35C918A4     a00.lsanca04.us..179     a03.lsanca04.us..1035   ESTAB
```

The following example shows the IP activity by using the numeric keyword to display the addresses in IP format.

```
Router# show tcp brief numeric

TCB           Local Address         Foreign Address     (state)
6523A4FC      10.1.25.3.11000       10.1.25.3.23        ESTAB
65239A84      10.1.25.3.23          10.1.25.3.11000     ESTAB
653FCBBC      *.1723 *.* LISTEN
```

QUESTION 437
Under which circumstance will a branch ISR router contain interface vlan configurations?

A. Performing inter-VLAN routing
B. Performing 802.1Q trunking
C. Performing ISL trunking
D. Ethernet Switch Module installed
E. ADSL WIC installed
F. Running Call Manager Express

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
In smaller offices, a single ISR may be used for a both remote connectivity and inter-VLAN routing. In that case, know that an Ethernet Switch Module would

be required for the ISR router

QUESTION 438
A Network engineer wants to configure logging to compile and send information to an external server. Which type of logging must be configured?

A. Terminal
B. Syslog
C. Buffer
D. Console

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 439
How to set up IP SLA to monitor Bandwidth between the certain limits?

A. Timer
B. Frequency
C. Threshold
D. Queue-limit

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 440
Which location is traffic from IP SLAs?

A. Core edge
B. Access edge
C. WAN edge
D. Distribution edge
E. User edge

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Maybe this question wants to ask “which location IP SLAs are usually used to monitor the traffic?” then the answer should be WAN edge as IP SLA is usually used to track a remote device or service (usually via ping).

QUESTION 441
What is the reasons of command:

```
router(config)# snmp-server host 192.168.1.3 traps version 2c CISCORO
```

A. for network system to management server
B. allow 192.168.1.3 only

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 442
Which command is used to check IP SLA when an interface is suspected to receive lots of traffic with options?

A. Show track
B. Show threshold
C. Show timer
D. Show delay

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 443
Where the output will be shown of the command debug condition interface fa0/1?

A. It will show on interface f0/1
B. It will show on interface f0/0
C. Both interfaces will show debugging output

D. An interface cannot be used as condition

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The command “debug condition interface <interface>” command is used to disable debugging messages for all interfaces except the specified interface so in this case the debug output will be shown on Fa0/1 interface only.

Note: If in this question there was another “debug condition interface fa0/0” command configured then the answer should be C (both interfaces will show debugging ouput).

QUESTION 444
A network engineer executes the show ip sla statistics command.
What does the output of this command show?

A. Operation availability
B. Device CPU utilization
C. Interface packet statistics
D. Packet sequencing

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 445
What is the most security snmp version?

A. v2c auth
B. v2c
C. v3
D. v1

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 446
Which alerts will be seen on the console when running the command: logging console warnings?

A. Warnings only
B. Warnings, notifications, error, debugging, informational
C. Warnings, errors, critical, alerts, emergencies
D. Notifications, warnings, errors
E. Warnings, errors, critical, alerts

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 447
A network engineer is asked to create an SNMP-enabled proactive monitoring solution to ensure that jitter levels remain between particular boundaries.
Which IP SLA option should the engineer use?

A. Threshold
B. Frequency
C. Verify-data
D. Timeout

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 448
Which IP SLA operation requires Cisco endpoints?

A. UDP Jitter for VoIP
B. ICMP Path Echo
C. ICMP Echo
D. UDP Jitter

Correct Answer: A

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
With the addition of real-time traffic (ie: VoIP), the focus shifts not just in the reliability of the network, but also on the delays involved in transmitting the data. Real-time traffic is delay sensitive. For Voice data, packet loss is manageable to some extent, but frequent losses impair communication between endpoints.

The UDP jitter operation is the most popular operation because the user can obtain packet loss, jitter and latency from one operation. This also includes unidirectional measurements as well. The Jitter operation is designed to measure the delay, delay variance and packet loss in IP networks by generating active UDP traffic. It sends N packets, each of size S, from source router to a target router (which requires Cisco IOS IP SLAs responder enabled) each T milliseconds apart. All these parameters are user configurable.

Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_udp_jitter.pdf

QUESTION 449
IP SLA network with a configuration snippet

A. Apply the ipv6 acl under a vty
B. Ip access-class
C. Ipv6 access class
D. Access-list IN
E. Access-list OUT

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
http://www.firewall.cx/cisco-technical-knowledgebase/cisco-routers/813-cisco-router-ipsla-basic.html

QUESTION 450
Given ((diagram with R1 SLA config)) with configuration written on Picture as

```
R(Config)#ip sla 1
R1(Config-ip-sla)#icmp-echo 172.20.20.2 source-interface f1/0
R1(Config-ip-sla)#frequency 10
R1(Config-ip-sla)#threshold 100
R1(Config)#ip sla schedule 1 start-time now life forever
R1(Config)#track 10 ip sla ???-
R1(Config)#ip route 0.0.0.0 0.0.0.0 172.20.20.2
```

What make default route not removed when SLA state down or failed?

A. The destination must be 172.30.30.2 for icmp-echo
B. The threshold value is wrong
C. Missing of track feature on default static route command

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Remember: If you want to use the “state”, remember that the “track state” will be down also if the the threshold is reached.

Note: with Cisco IOS Release 12.4(20)T, 12.2(33)SXI1, 12.2(33)SRE and Cisco IOS XE Release 2.4, the track rtr command is replaced by the track ip sla command. See the track ip sla command for more information.

Reference:
http://www.ciscozine.com/using-ip-sla-to-change-routing/

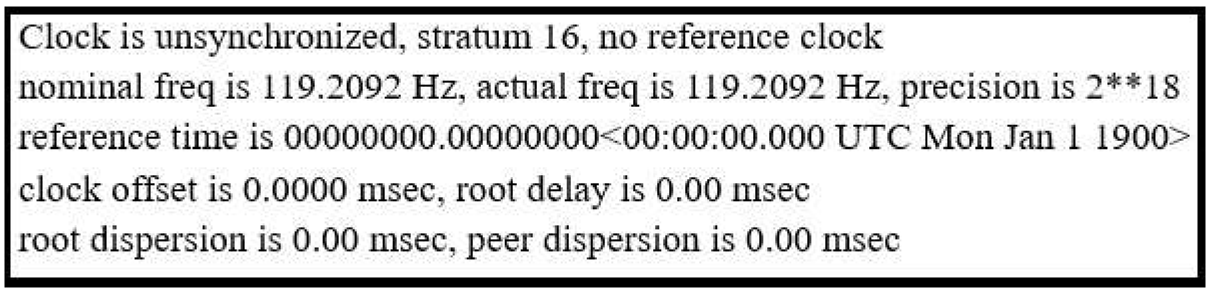
QUESTION 451
Which option must be configured on a target device to use time stamping to accurately represent response times using IP SLA?

A. Responder
B. Jitter value
C. TCP Connect
D. ICMP Echo

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 452
Refer to the exhibit.



```
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 119.2092 Hz, actual freq is 119.2092 Hz, precision is 2**18
reference time is 00000000.00000000<00:00:00.000 UTC Mon Jan 1 1900>
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
```

A network engineer receives a command output from a customer that indicates an issue with. What are two reasons for the output? (Choose two.)

A. NTP traffic is blocked.
B. NTP is not configured.
C. The router is the NTP master.
D. NTP update-calendar is missing.
E. There is an NTP authentication failure.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
NTP uses a value, called a stratum value, to indicate the believability of a time source.
Valid stratum values are in the range 0-15, with a value of 16 being used to indicate that a device does not have its time synchronized. However, Cisco IOS only permits you to set stratum values in the range 1-15.

QUESTION 453
Which type of information is displayed when a network engineer executes the show track 1 command on the router?

A. Information about tracking list 1
B. Time to next poll for track object 1
C. Information about the IP route track table.
D. Tracking information statistics.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 454
A network engineer is notified that several employees are experiencing network performance related issues, and bandwidth-intensive applications are identified as the root cause. In order to identify which specific type of traffic is causing this slowness, information such as the source/destination IP and Layer 4 port numbers is required. Which feature should the engineer use to gather the required information?

A. SNMP
B. Cisco IOS EEM
C. NetFlow
D. Syslog
E. WCCP

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
NetFlow Flows Key Fields
A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and transport-layer source and des--nation port numbers. Specifically, a flow is identified as the combination of the following key fields: http://www.cisco.com/en/US/docs/ios-xml/ios/netflow/configuration/12-4t/cfg-nflow-data-expt.html

QUESTION 455
Where can NetFlow export data for long term storage and analysis?

A. Syslog
B. Collector
C. Another network device
D. Flat file

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 456
What is the viable successor of NAT_PT?

A. NAT44
B. NAT64

C. NPTv6
D. NATng

Correct Answer: B
Section: Mix Questions
Explanation

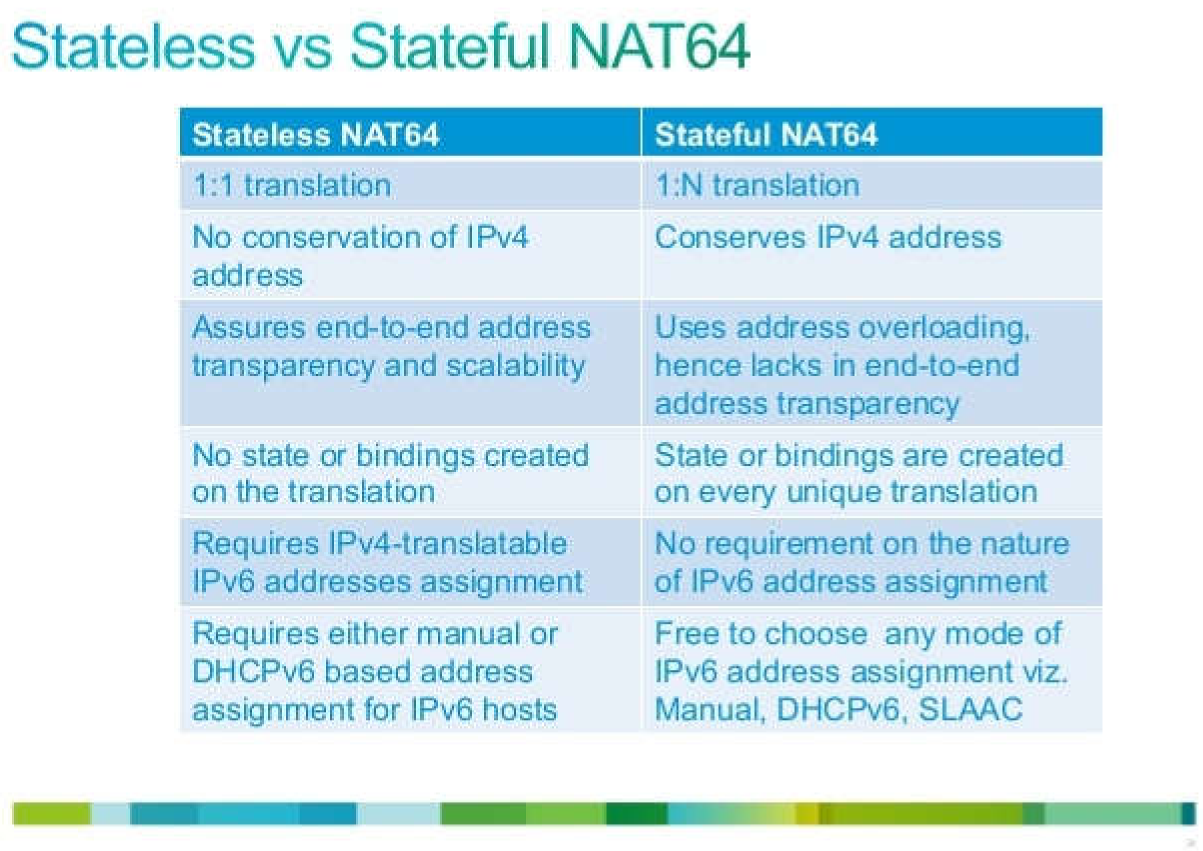
Explanation/Reference:

QUESTION 457
Which three functionalities are specific to stateful NAT64? (Choose three.)

A. 1:N translation
B. Conserves IPv4 address
C. Uses address overloading, hence lacks in end-to-end address transparency
D. No state or bindings created on the translation
E. Requires IPv4-translatable IPv6 addresses assignment (mandatory requirement)
F. Requires either manual or DHCPv6 based address assignment for IPv6 hosts

Correct Answer: ABC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



Stateless vs Stateful NAT64

Stateless NAT64	Stateful NAT64
1:1 translation	1:N translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment	No requirement on the nature of IPv6 address assignment
Requires either manual or DHCPv6 based address assignment for IPv6 hosts	Free to choose any mode of IPv6 address assignment viz. Manual, DHCPv6, SLAAC

QUESTION 458
Which option is the first task that a device that is configured with NAT64 performs when it receives an incoming IPv6 packet that matches the stateful NAT64 prefix?

A. It translates the IPv6 header into an IPv4 header.
B. It checks the IPv6 packet against the NAT64 stateful prefix.
C. It translates the IPv6 source address to an IPv4 header.
D. It translates the^ IPv4 destination address into a new NAT64 state.
E. It performs an IPv6 route lookup.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 459
When use NPTv6 for IPV6 to IPV6 Address translation? (Choose two.)

A. Stateful address translation
B. A limit of 32 1-to-1 translations
C. Lack of overloading functionality
D. Identify all interface NAT inside or outside
E. One-to-one prefix rewrite
F. Mismatched prefix allocations

Correct Answer: CE

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 460
Which command do you enter to display log messages with a timestamp that includes the length of time since the device was last rebooted?

A. Service timestamps log uptime
B. Logging facility 20
C. Service timestamps debugging localtime msec
D. Logging console errors
E. Logging monitor 7
F. Service timestamps log datetime msec

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 461
Which SNMP verification command shows the encryption and authentication protocols that are used in SNMPV3?

A. Show snmp group
B. Show snmp user
C. Show snmp
D. Show snmp view

Correct Answer: B
Section: Mix Questions
Explanation

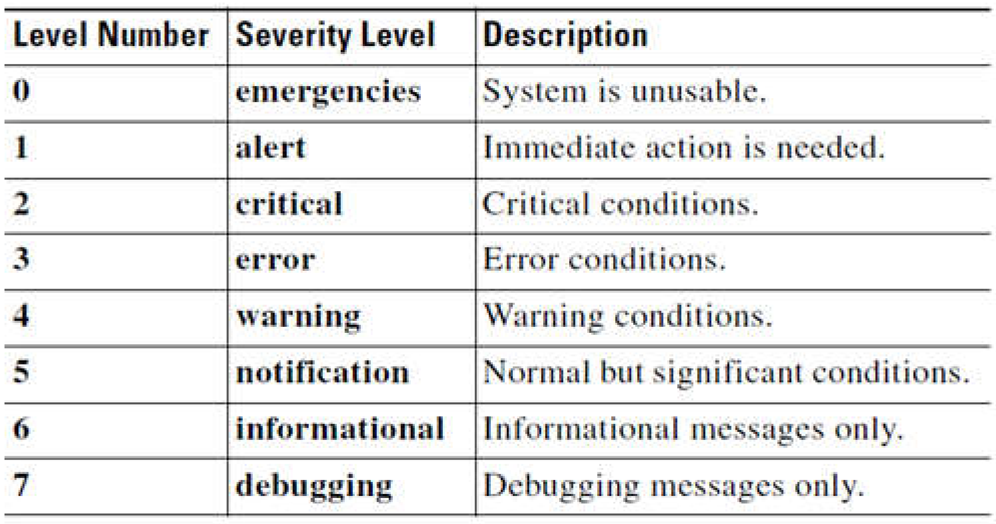
Explanation/Reference:

QUESTION 462
A network engineer enables a trunk port and encounters the following message:%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet 1/1, changed state to up. What is the severity level of this message?

A. Alert
B. Critical
C. Notification
D. Informational

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



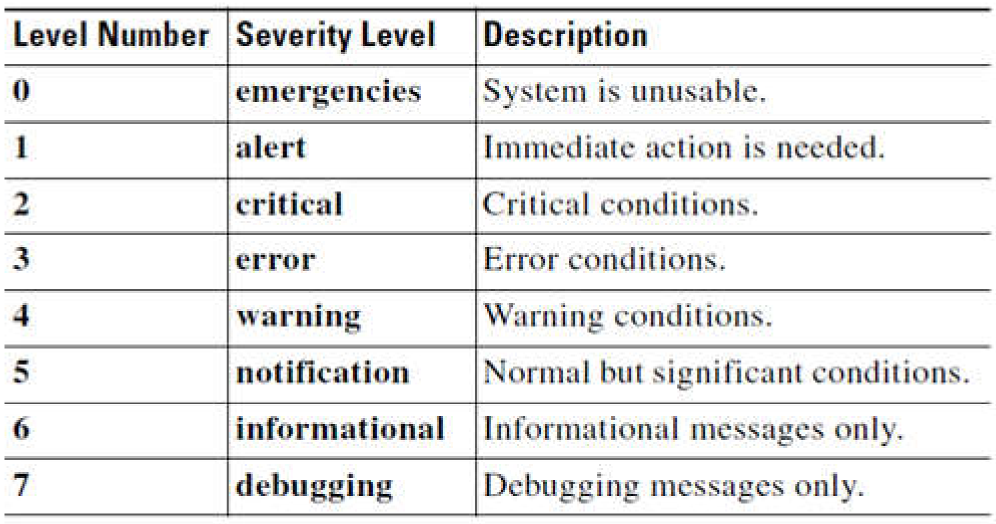
Level Number	Severity Level	Description
0	emergencies	System is unusable.
1	alert	Immediate action is needed.
2	critical	Critical conditions.
3	error	Error conditions.
4	warning	Warning conditions.
5	notification	Normal but significant conditions.
6	informational	Informational messages only.
7	debugging	Debugging messages only.

QUESTION 463
Up/down interface... what is the log severity level?

A. Level 3
B. Level 4
C. Level 5
D. Level 0

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



Level Number	Severity Level	Description
0	**emergencies**	System is unusable.
1	**alert**	Immediate action is needed.
2	**critical**	Critical conditions.
3	**error**	Error conditions.
4	**warning**	Warning conditions.
5	**notification**	Normal but significant conditions.
6	**informational**	Informational messages only.
7	**debugging**	Debugging messages only.

QUESTION 464
Which NAT Command do you enter to disable dynamic ARP learning on an interface?

A. R(config-if) # ip nat enable
B. R(config-if) # ip nat inside
C. R(config-if)# ip nat outside
D. R(config)# ip nat allow-static-host
E. R(config)# ip nat service

Correct Answer: D
Section: Mix Questions
Explanation

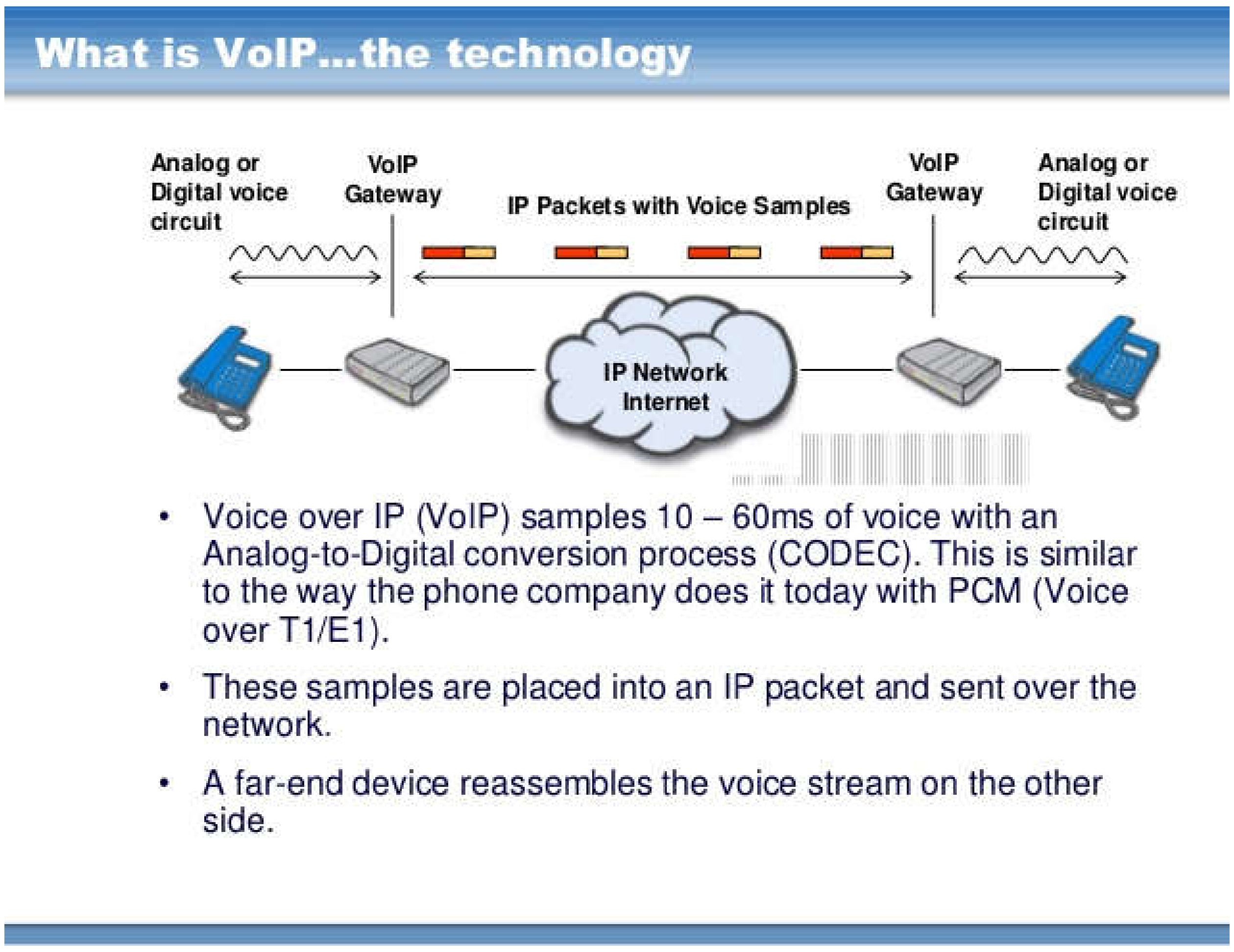
Explanation/Reference:

QUESTION 465
Your company uses Voice over IP (VoIP). The system sends UDP datagrams containing the voice data between communicating hosts. When areas of the network become busy, some of the datagrams arrive at their destination out of order. What happens when this occurs?

A. UDP will send an ICMP Information request message to the source host.
B. UDP will pass the information in the datagrams up to the next OSI layer in the order in which they arrive.
C. UDP will drop the datagrams that arrive out of order.
D. UDP will use the sequence numbers in the datagram headers to reassemble the data into the correct order.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



What is VoIP...the technology

Analog or Digital voice circuit
VoIP Gateway
IP Packets with Voice Samples
VoIP Gateway
Analog or Digital voice circuit
IP Network Internet

- Voice over IP (VoIP) samples 10 – 60ms of voice with an Analog-to-Digital conversion process (CODEC). This is similar to the way the phone company does it today with PCM (Voice over T1/E1).
- These samples are placed into an IP packet and sent over the network.
- A far-end device reassembles the voice stream on the other side.

QUESTION 466
Which command will display all the EIGRP feasible successor routes known to a router?

A. Show ip routes

B. Show ip eigrp summary
C. Show ip eigrp topology
D. Show ip eigrp adjacencies

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 467
Where are EIGRP successor routes stored?

A. In the routing table only
B. In the neighbor table only
C. In the topology table only
D. In the routing table and the topology table
E. In the routing table and the neighbor table

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 468
A network engineer is troubleshooting connectivity issues with a directly connected RIPng neighbor. Which command should directly connected RIPng neighbor adjacencies only?

A. Router#show ipv6 rip next-hops
B. Router#show ip rip neighbors
C. Router#show ipv6 routers
D. Router#show ipv6 rip database

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 469
Which three NTP operating modes must the trusted-Key command be configured on for authentication to operate properly? (Choose three.)

A. Interface
B. Client
C. Peer
D. Server
E. Broadcast
F. Stratum

Correct Answer: BCE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Client/Server Mode
Configuring an association in client mode, usually indicated by a server declaration in the configuration file, indicates that one wishes to obtain time from the remote server, but that one is not willing to provide time to the remote server.

Symmetric Active/Passive Mode (Peer)
A peer is configured in symmetric active mode by using the peer command and specifying the DNS name or address of the other peer. The other peer is also configured in symmetric active mode in this way.
Note: If the other peer is not specifically configured in this way, a symmetric passive association is activated upon arrival of a symmetric active message. Since an intruder can impersonate a symmetric active peer and inject false time values, symmetric mode should always be authenticated.

Broadcast and/or Multicast Mode
Broadcast mode is intended for configurations involving one or a few servers and a potentially large client population. A broadcast server is configured using the broadcast command and a local subnet address. A broadcast client is configured using the broadcastclient command, allowing the broadcast client to respond to broadcast messages received on any interface. Since an intruder can impersonate a broadcast server and inject false time values, this mode should always be authenticated

QUESTION 470
Which two types of threshold can you configure for tracking objects? (Choose two.)

A. Percentage
B. MTU
C. Bandwidth
D. Weight
E. Delay
F. Administrative distance

Correct Answer: AD

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Object Track List

An object track list allows you to track the combined states of multiple objects. Object track lists support the following capabilities:

-Boolean "and" function — Each object defined within the track list must be in an up state so that the track list object can become up.

-Boolean "or" function — At least one object defined within the track list must be in an up state so that the tracked object can become up.

-Threshold percentage — The percentage of up objects in the tracked list must be greater than the configured up threshold for the tracked list to be in the up state. If the percentage of down objects in the tracked list is above the configured track list down threshold, the tracked list is marked as down.

-Threshold weight — Assign a weight value to each object in the tracked list, and a weight threshold for the track list. If the combined weights of all up objects exceeds the track list weight up threshold, the track list is in an up state. If the combined weights of all the down objects exceeds the track list weight down threshold, the track list is in the down state.

QUESTION 471
A router was configured with the eigrp stub command.
The router advertises which types of routes?

A. Connected, static, and summary
B. Static and summary
C. Connected and static
D. Connected and summary

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 472
Consider this scenario. TCP traffic is blocked on port 547 between a DHCPv6 relay agent and a DHCPv6 server that is configured for prefix delegation. Which two outcomes will result when the relay agent is rebooted? (Choose two.)

A. Routers will not obtain DHCPv6 prefixes.
B. DHCPv6 clients will be unreachable.
C. Hosts will not obtain DHCPv6 addresses.
D. The DHCPv6 relay agent will resume distributing addresses.
E. DHCPv6 address conflicts will occur on downstream clients.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The DHCPv6 use UDP protocol for distribution IPv6 addresses and prefixes. The routers dont need in the DHCPv6 prefixes from DHCPv6 server, its work for network administrator. DHCPv6 messages are exchanged over UDP port 546 and 547. Clients listen for DHCP messages on UDP port 546 while servers and relay agents listen for DHCP messages on UDP port 547.

DHCPv6 messages are exchanged over UDP port 546 and 547. Clients listen for DHCP messages on UDP port 546 while servers and relay agents listen for DHCP messages on UDP port 547. The basic message format is as follows:

dhcpv6-client	546/tcp	DHCPv6 Client
dhcpv6-client	546/udp	DHCPv6 Client
dhcpv6-server	547/tcp	DHCPv6 Server
dhcpv6-server	547/udp	DHCPv6 Server

Client -> Server messages (msg-type):
Solicit, Request, Confirm, Renew, Rebind, Release, Decline, Information-Request
Server -> Client messages (msg-type):
Advertise, Reply, Reconfigure
Relay -> Relay/Server messages (msg-type):
Relay-Forw
Server/Relay -> Relay (msg-type):
Relay-Reply

SOLICIT (1)
A DHCPv6 client sends a Solicit message to locate DHCPv6 servers.

ADVERTISE (2)
A server sends an Advertise message to indicate that it is available for DHCP service, in response to a Solicit message received from a client.

REQUEST (3)
A client sends a Request message to request configuration parameters, including IP addresses or delegated prefixes, from a specific server.

CONFIRM (4)
A client sends a Confirm message to any available server to determine whether the addresses it was assigned are still appropriate to the link to which the client is connected. This could happen when the client detects either a link-layer connectivity change or if it is powered on and one or more leases are still valid. The confirm message is used to confirm whether the client is still on the same link or whether it has been moved. The actual lease(s) are not validated; just the prefix portion of the addresses or delegated prefixes.

RENEW (5)
A client sends a Renew message to the server that originally provided the client's addresses and configuration parameters to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters.

REBIND (6)
A client sends a Rebind message to any available server to extend the lifetimes on the addresses assigned to the client and to update other configuration parameters; this message is sent after a client receives no response to a Renew message.

REPLY (7)
A server sends a Reply message containing assigned addresses and configuration parameters in response to a Solicit, Request, Renew, Rebind message received from a client. A server sends a Reply message containing configuration parameters in response to an Information-request message. A server sends a Reply message in response to a Confirm message confirming or denying that the addresses assigned to the client are appropriate to the link to which the client is connected. A server sends a Reply message to acknowledge receipt of a Release or Decline message.

RELEASE (8)
A client sends a Release message to the server that assigned addresses to the client to indicate that the client will no longer use one or more of the assigned addresses.

DECLINE (9)
A client sends a Decline message to a server to indicate that the client has determined that one or more addresses assigned by the server are already in use on the link to which the client is connected.

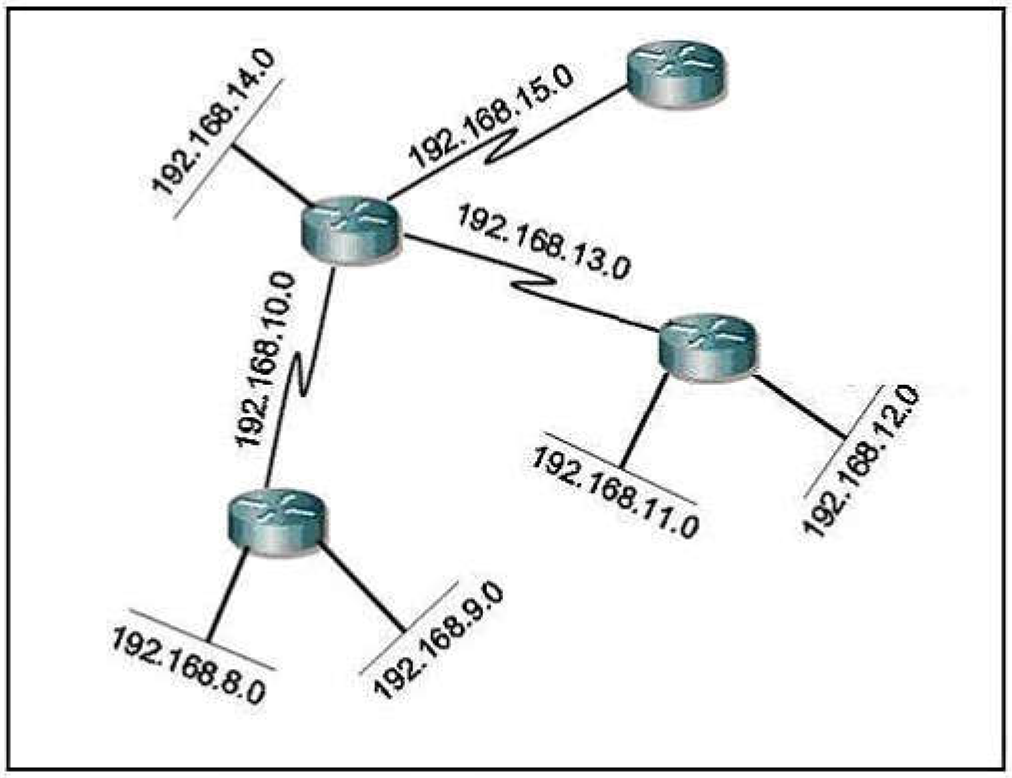
RECONFIGURE (10)
A server sends a Reconfigure message to a client to inform the client that the server has new or updated configuration parameters, and that the client is to initiate a Renew/Reply or Information-request/Reply transaction with the server in order to receive the updated information.

INFORMATION-REQUEST (11)
A client sends an Information-request message to a server to request configuration parameters without the assignment of any IP addresses to the client.

RELAY-FORW (12)
A relay agent sends a Relay-forward message to relay messages to servers, either directly or through another relay agent. The received message, either a client message or a Relay-forward message from another relay agent, is encapsulated in an option in the Relay-forward message.

RELAY-REPL (13)
A server sends a Relay-reply message to a relay agent containing a message that the relay agent delivers to a client. The Relay-reply message may be relayed by other relay agents for delivery to the destination relay agent. The server encapsulates the client message as an option in the Relay-reply message, which the relay agent extracts and relays to the client.

QUESTION 473
When policy-based routing (PBR) is being configured, which three criteria can the set command specify? (Choose three.)

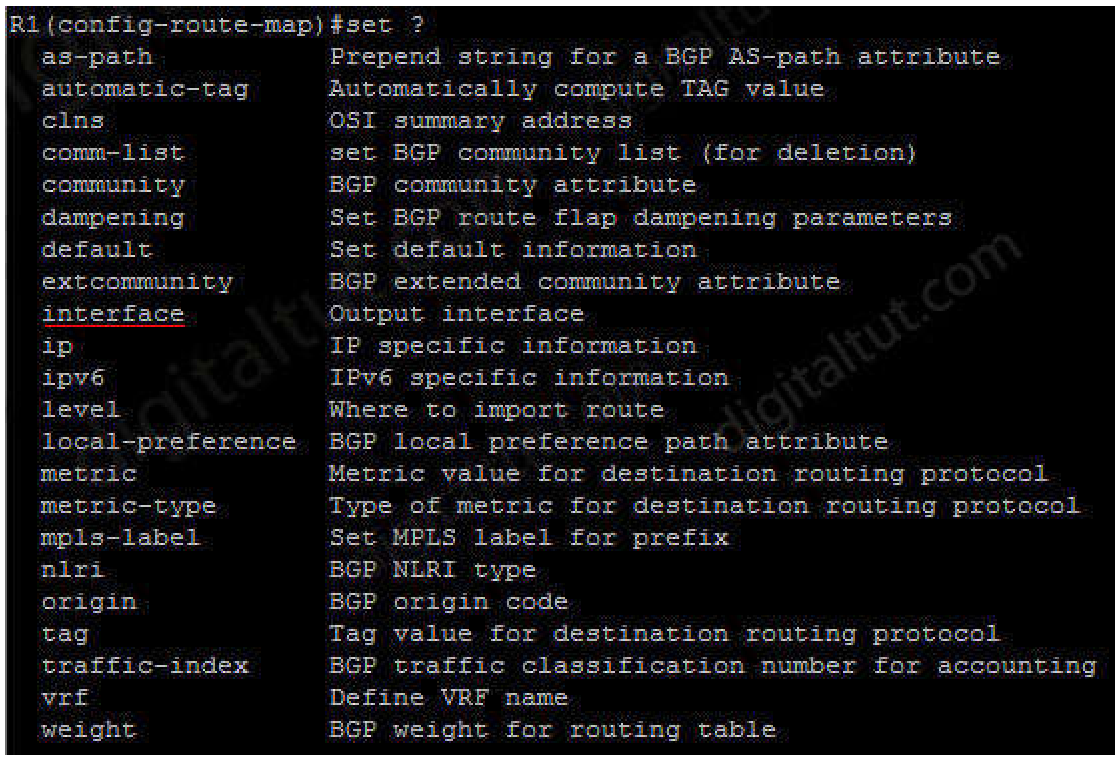


A. All interfaces through which the packets can be routed
B. All interfaces in the path toward the destination
C. Adjacent next hop router in the path toward the destination
D. All routers in the path toward the destination
E. All networks in the path toward the destination
F. Type of service and precedence in the IP packets

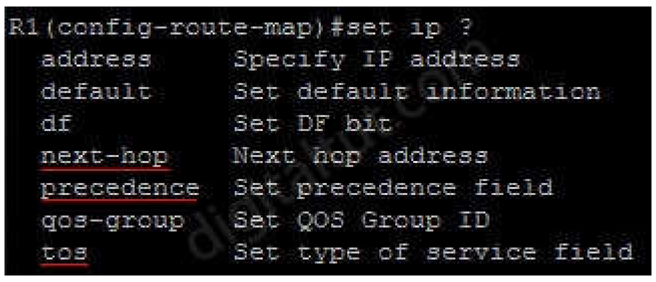
Correct Answer: ACF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The set command specifies the action(s) to take on the packets that match the criteria. You can specify any or all of the following:

* **precedence**: Sets precedence value in the IP header. You can specify either the precedence number or name.
* df: Sets the “Don’t Fragment” (DF) bit in the ip header.
* vrf: Sets the VPN Routing and Forwarding (VRF) instance.
* next-hop: Sets next hop to which to route the packet.
* next-hop recursive: Sets next hop to which to route the packet if the hop is to a router which is not adjacent.
* interface: Sets output interface for the packet.
* default next-hop: Sets next hop to which to route the packet if there is no explicit route for this destination.
* default interface: Sets output interface for the packet if there is no explicit route for this destination.



```
R1(config-route-map)#set ?
  as-path            Prepend string for a BGP AS-path attribute
  automatic-tag      Automatically compute TAG value
  clns               OSI summary address
  comm-list          set BGP community list (for deletion)
  community          BGP community attribute
  dampening          Set BGP route flap dampening parameters
  default            Set default information
  extcommunity       BGP extended community attribute
  interface          Output interface
  ip                 IP specific information
  ipv6               IPv6 specific information
  level              Where to import route
  local-preference   BGP local preference path attribute
  metric             Metric value for destination routing protocol
  metric-type        Type of metric for destination routing protocol
  mpls-label         Set MPLS label for prefix
  nlri               BGP NLRI type
  origin             BGP origin code
  tag                Tag value for destination routing protocol
  traffic-index      BGP traffic classification number for accounting
  vrf                Define VRF name
  weight             BGP weight for routing table
```

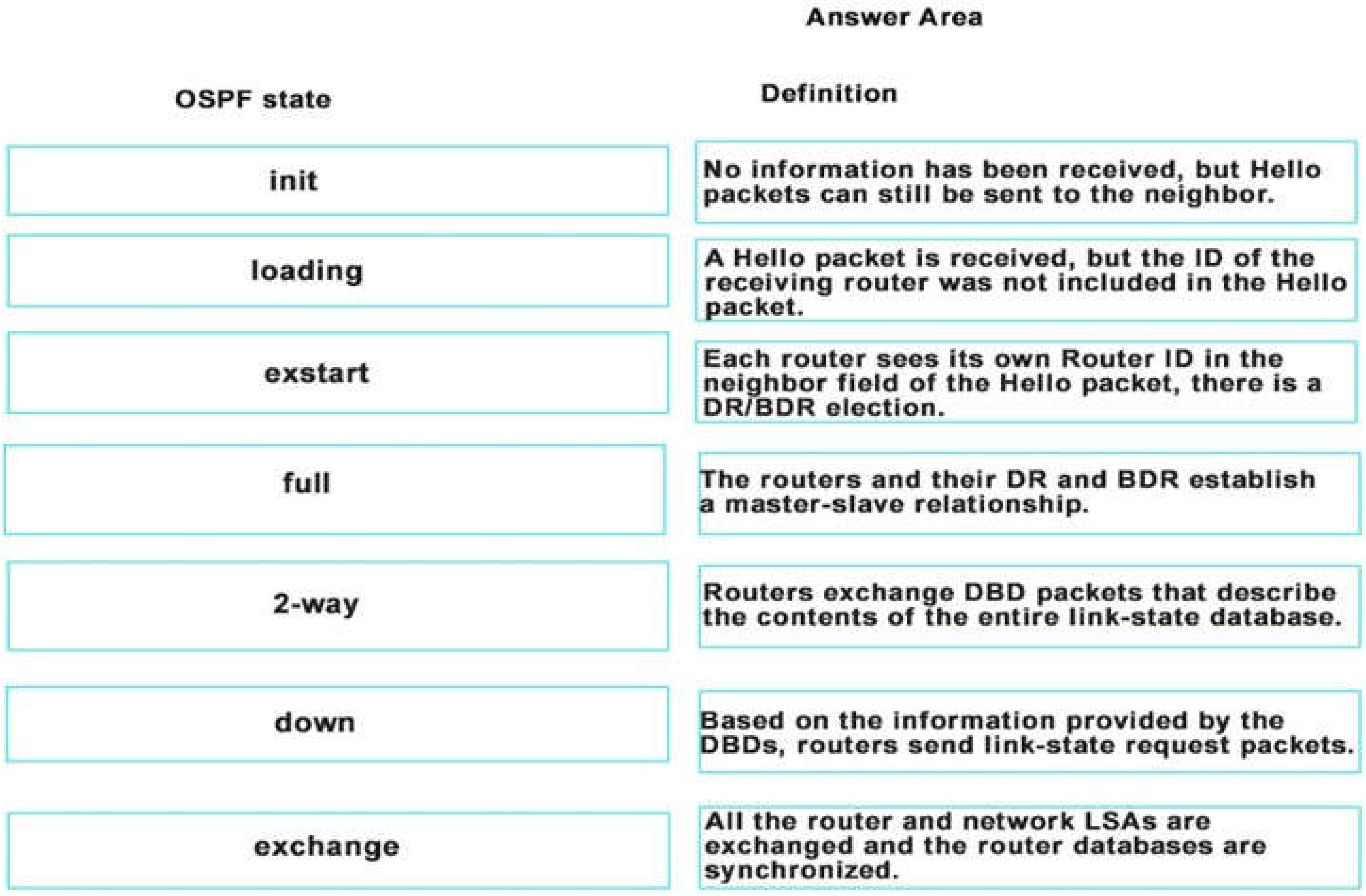


```
R1(config-route-map)#set ip ?
  address      Specify IP address
  default      Set default information
  df           Set DF bit
  next-hop     Next hop address
  precedence   Set precedence field
  qos-group    Set QOS Group ID
  tos          Set type of service field
```

Reference:
http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpbr_ps1835_TSD_Products_Configuration_Guide_Chapter.html

QUESTION 474
DRAG DROP
Drag each OSPF state to the correct definition.

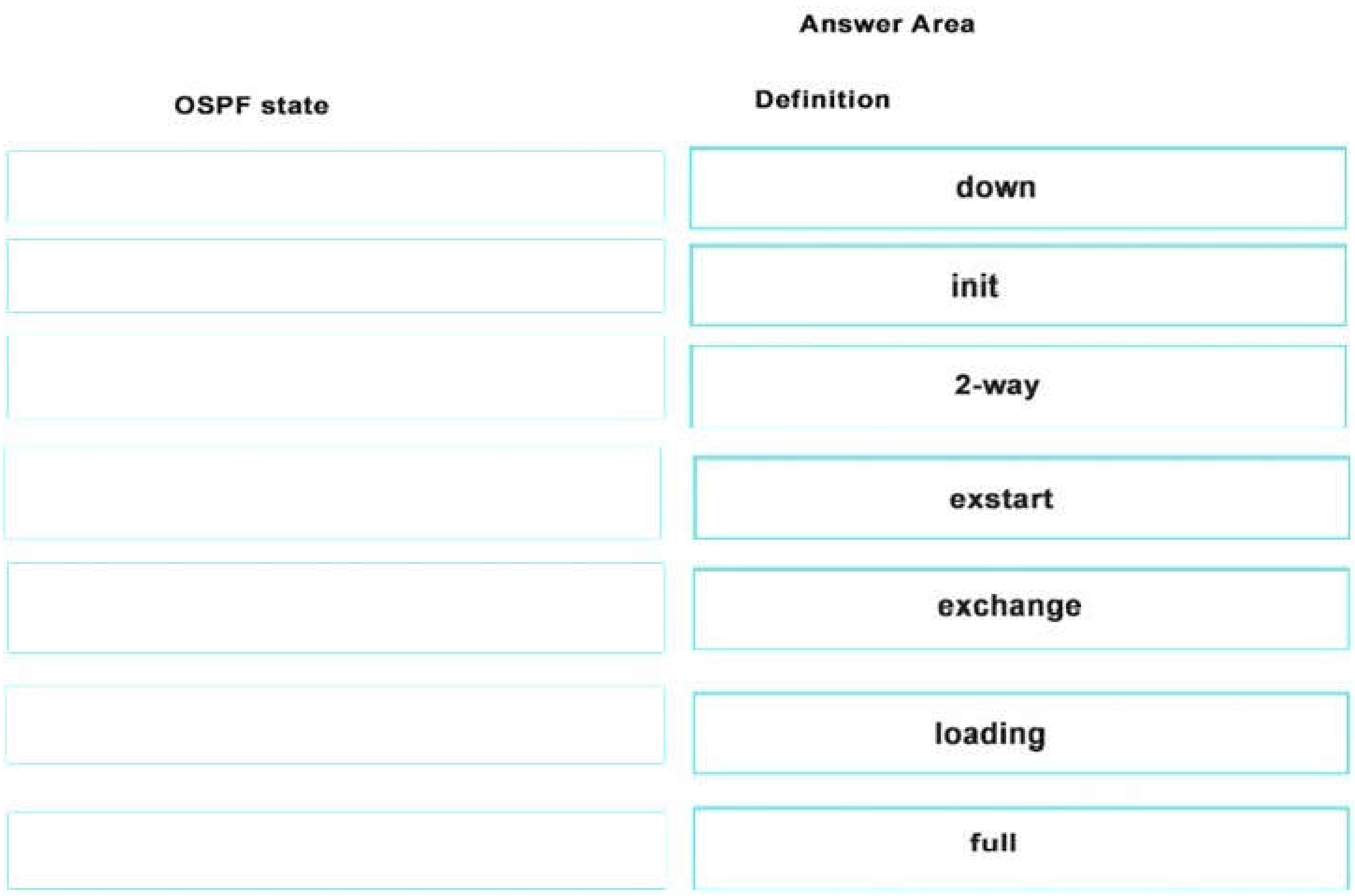
Select and Place:



Answer Area

OSPF state	Definition
init	No information has been received, but Hello packets can still be sent to the neighbor.
loading	A Hello packet is received, but the ID of the receiving router was not included in the Hello packet.
exstart	Each router sees its own Router ID in the neighbor field of the Hello packet, there is a DR/BDR election.
full	The routers and their DR and BDR establish a master-slave relationship.
2-way	Routers exchange DBD packets that describe the contents of the entire link-state database.
down	Based on the information provided by the DBDs, routers send link-state request packets.
exchange	All the router and network LSAs are exchanged and the router databases are synchronized.

Correct Answer:



Answer Area

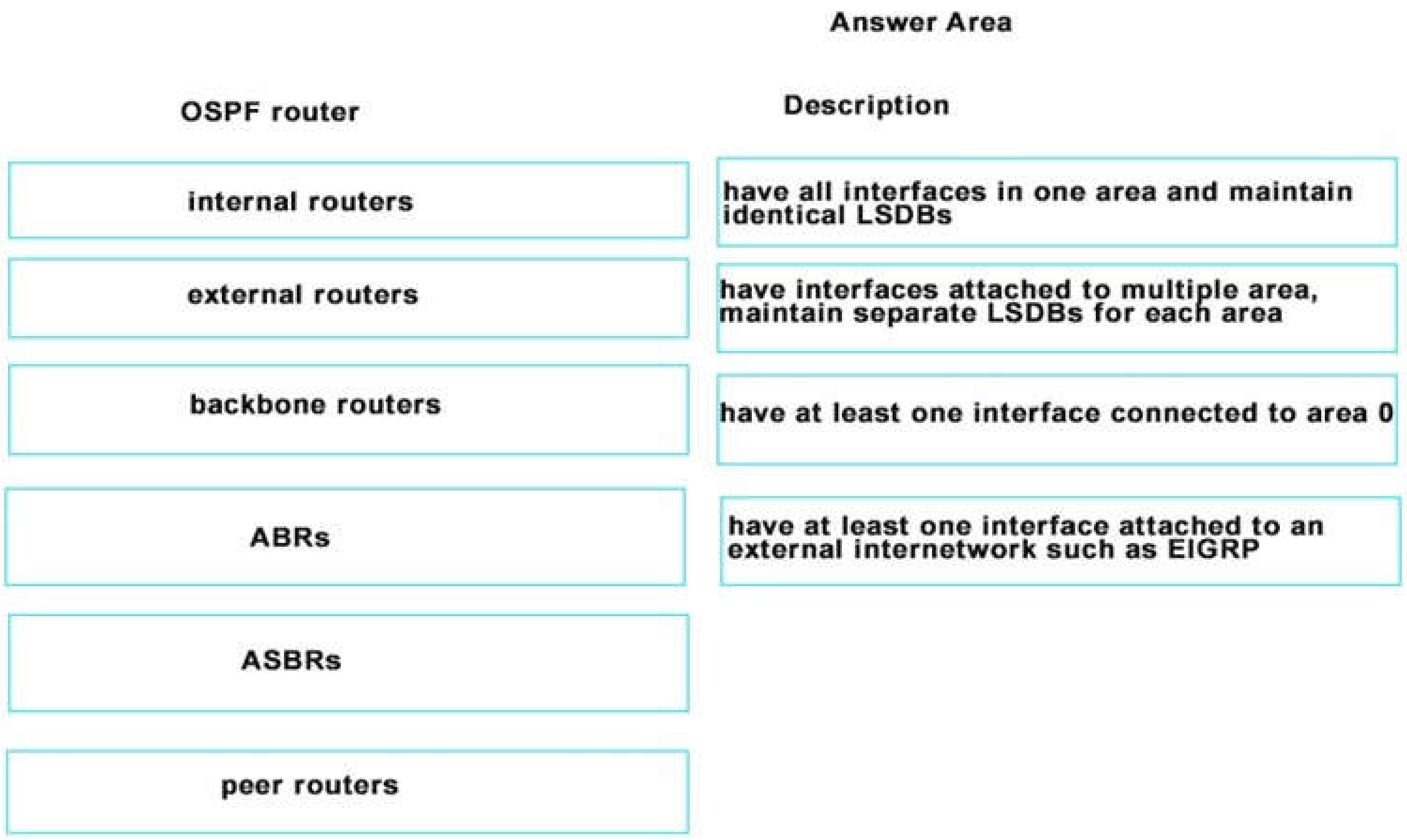
OSPF state	Definition
	down
	init
	2-way
	exstart
	exchange
	loading
	full

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 475
QUESTION NO: 483 DRAG DROP
Drag each OSPF router type to the approximate description on the left. Not all types are used.

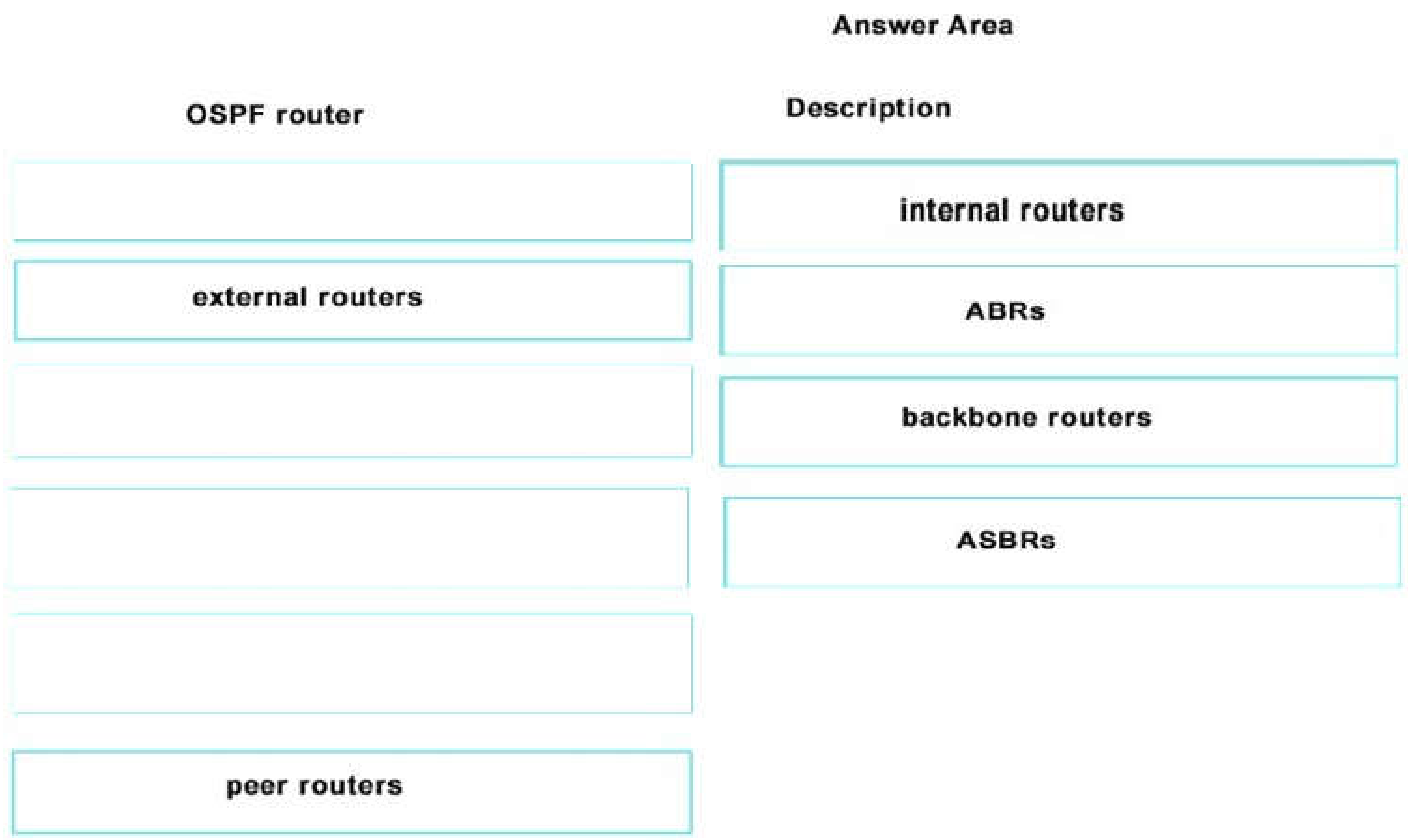
Select and Place:



Answer Area

OSPF router	Description
internal routers	have all interfaces in one area and maintain identical LSDBs
external routers	have interfaces attached to multiple area, maintain separate LSDBs for each area
backbone routers	have at least one interface connected to area 0
ABRs	have at least one interface attached to an external internetwork such as EIGRP
ASBRs	
peer routers	

Correct Answer:


Answer Area

OSPF router

external routers

peer routers

Description

internal routers

ABRs

backbone routers

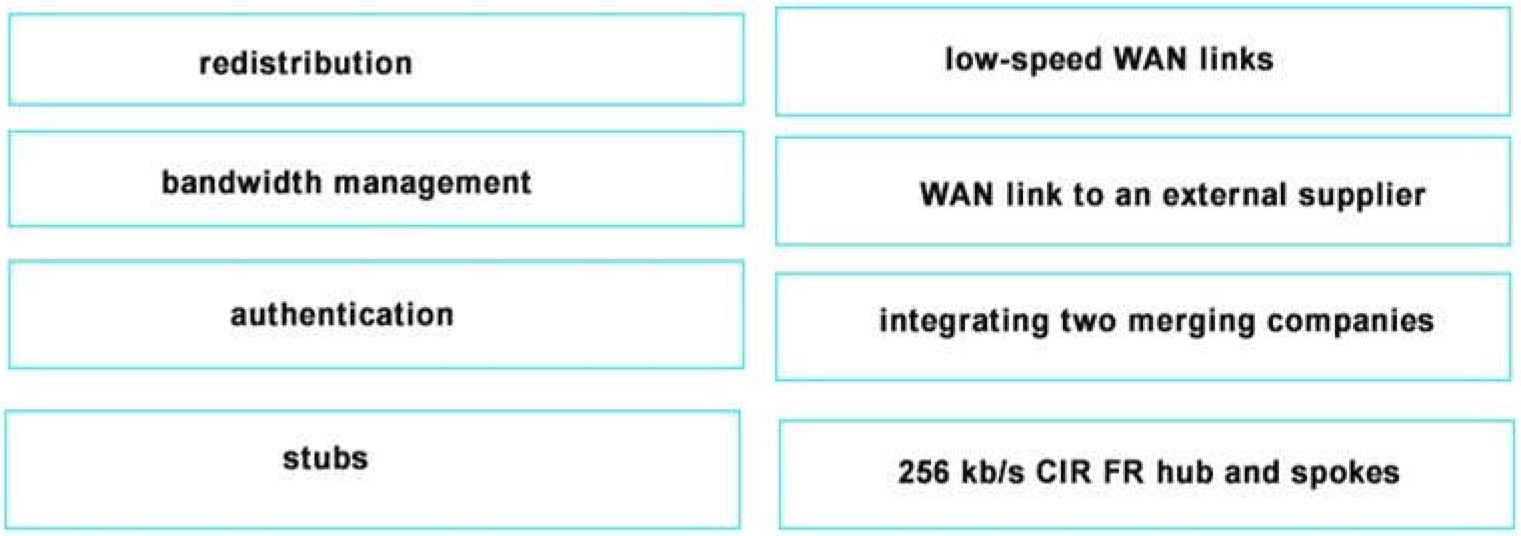
ASBRs

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 476
DRAG DROP
Click and drag the associated EIGRP functionality on the left corresponding topology characteristic on the right.

Select and Place:


redistribution

bandwidth management

authentication

stubs

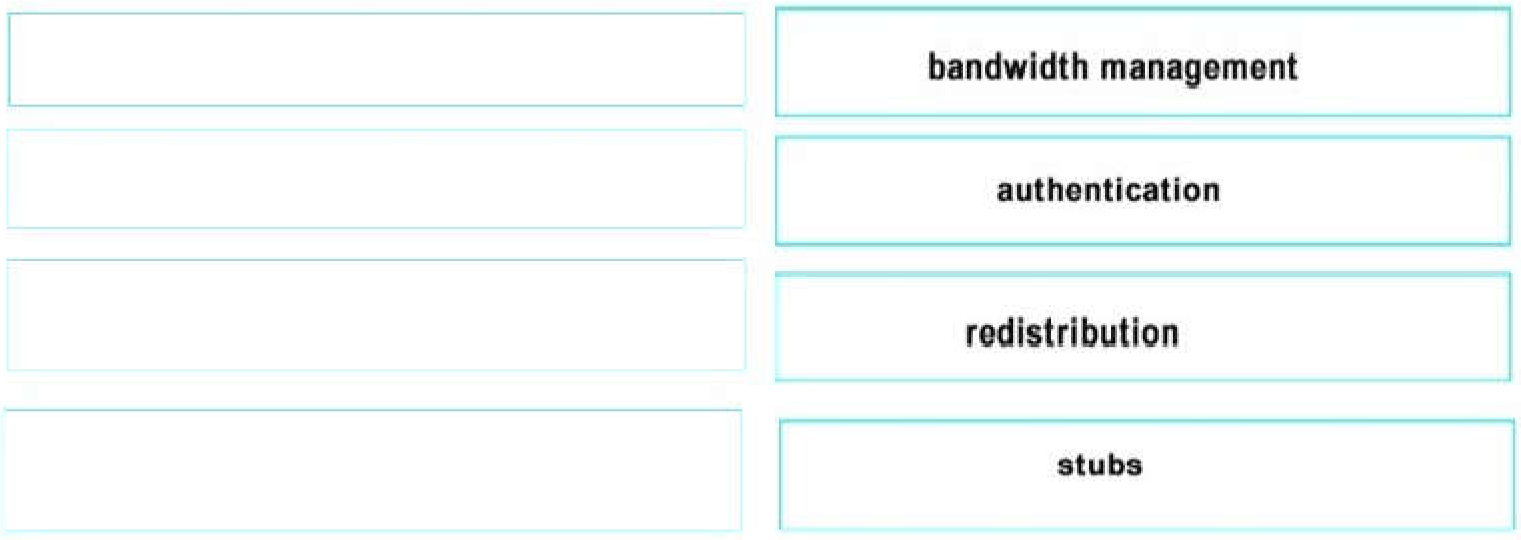
low-speed WAN links

WAN link to an external supplier

integrating two merging companies

256 kb/s CIR FR hub and spokes

Correct Answer:


bandwidth management

authentication

redistribution

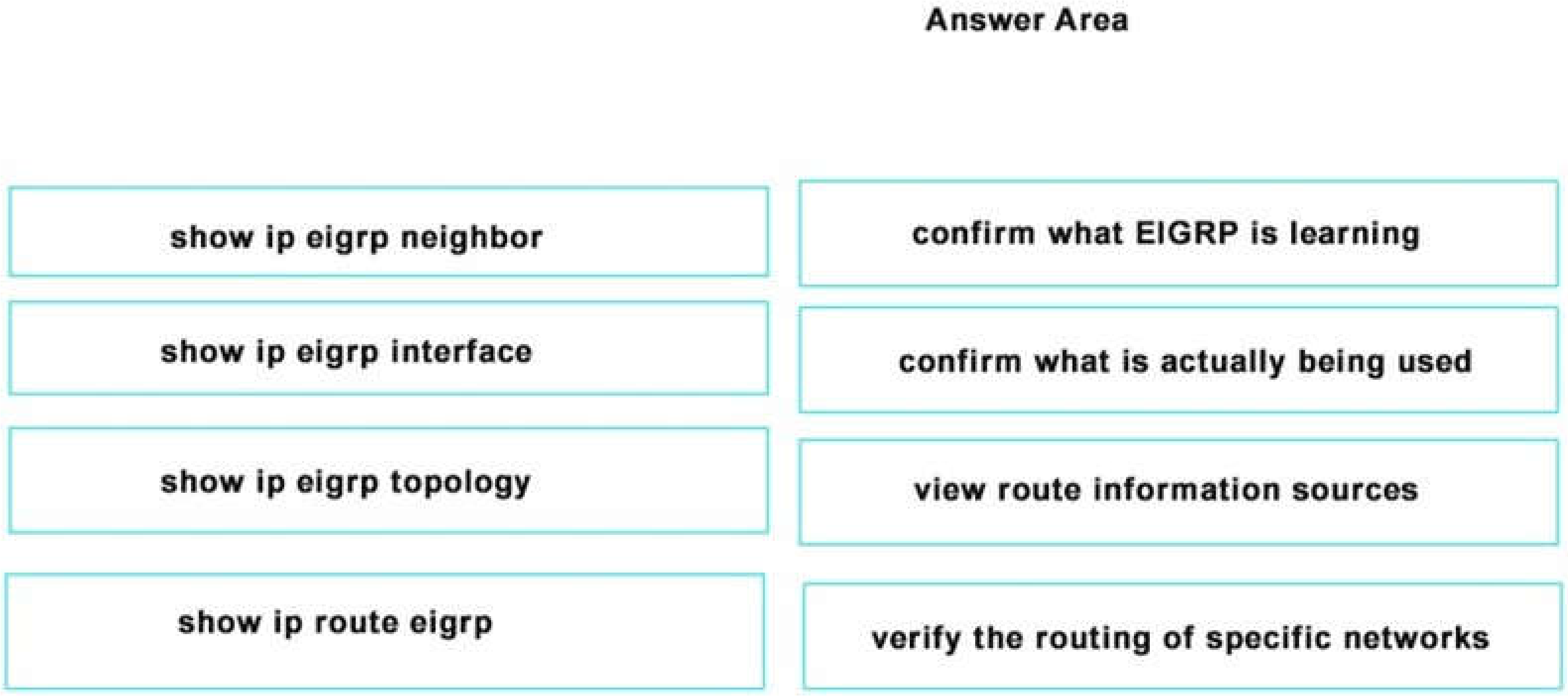
stubs

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 477
DRAG DROP
Click and drag the command on the left to the associated tack on the right.

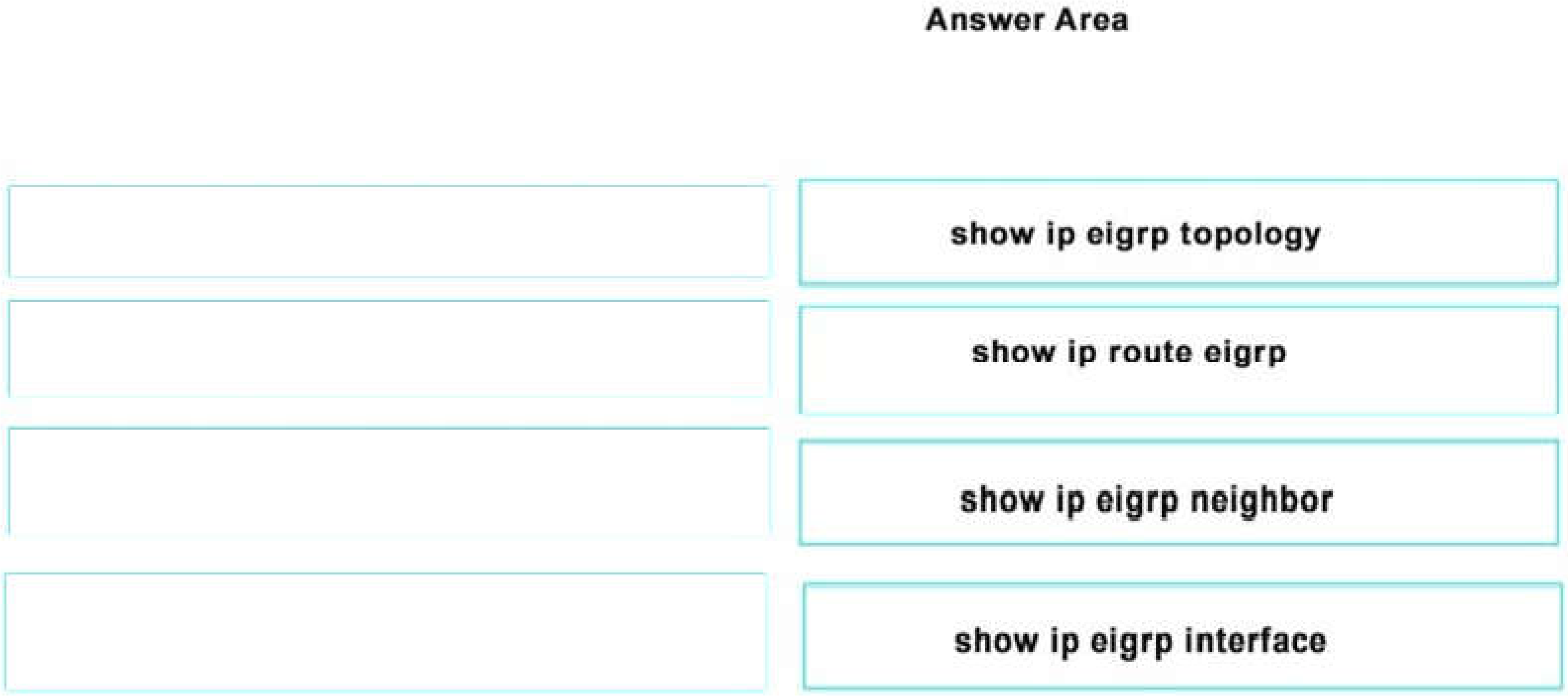
Select and Place:



Answer Area

show ip eigrp neighbor	confirm what EIGRP is learning
show ip eigrp interface	confirm what is actually being used
show ip eigrp topology	view route information sources
show ip route eigrp	verify the routing of specific networks

Correct Answer:



Answer Area

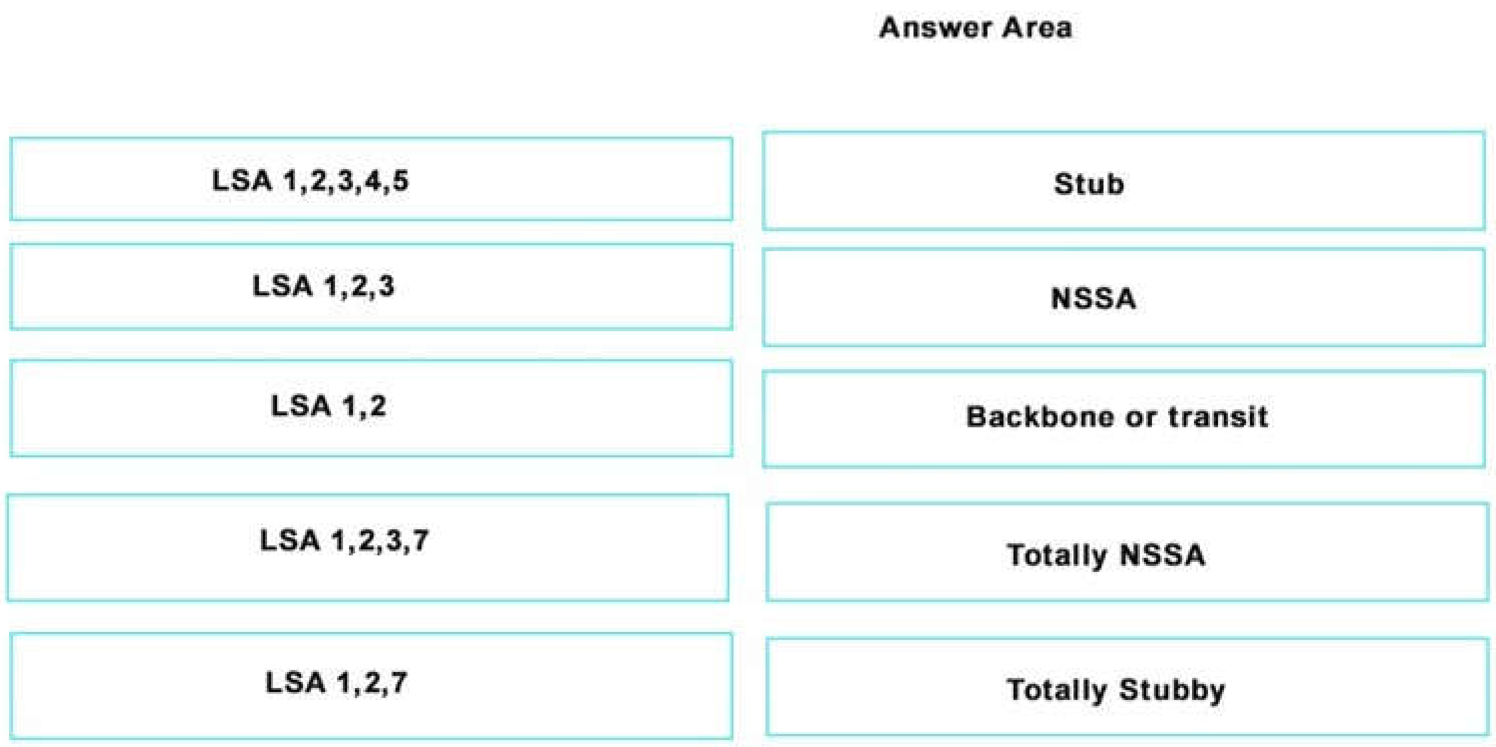
	show ip eigrp topology
	show ip route eigrp
	show ip eigrp neighbor
	show ip eigrp interface

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 478
DRAG DROP
Click and drag the associated set of OSPF LEAs on the left of the corresponding area type on the right where this set of LEAs may be seen.

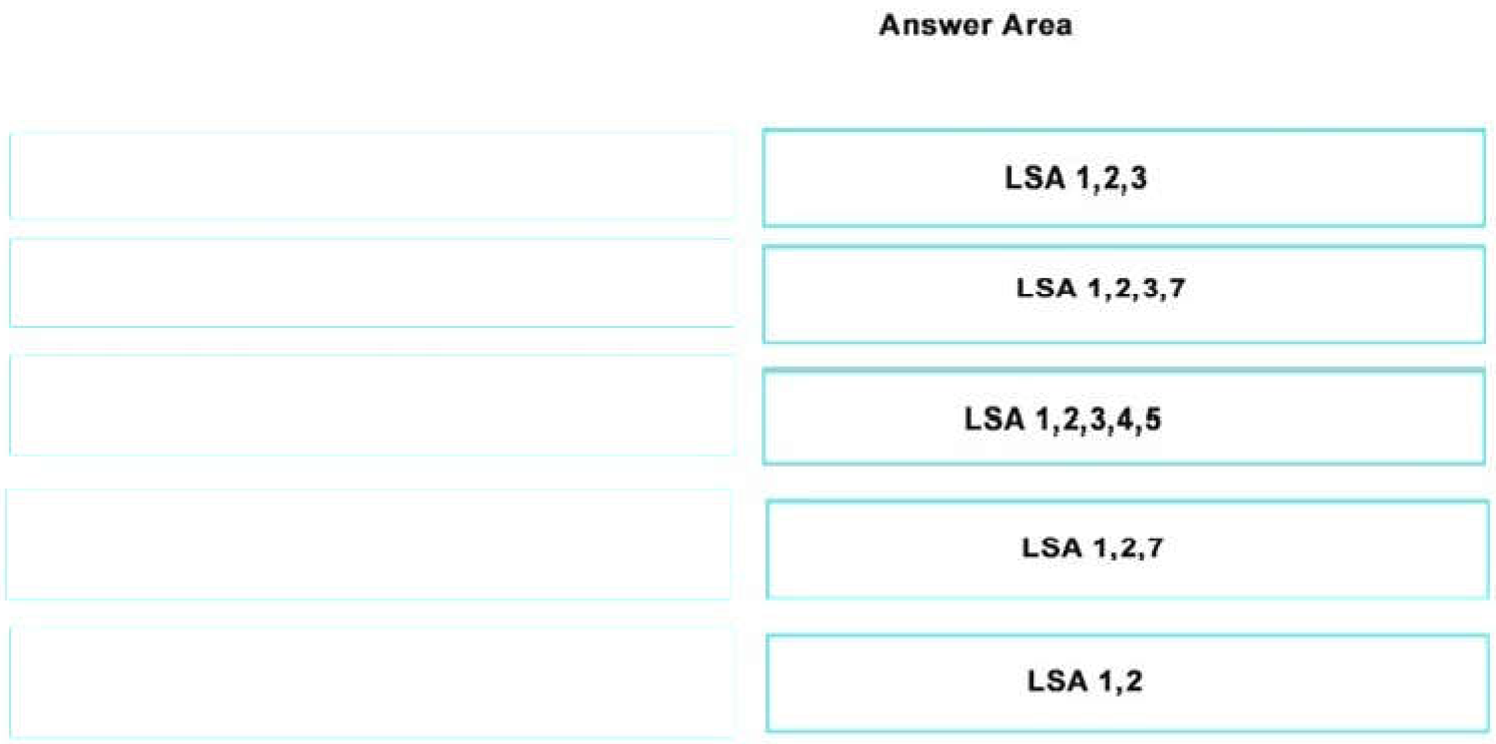
Select and Place:



Answer Area

LSA 1,2,3,4,5	Stub
LSA 1,2,3	NSSA
LSA 1,2	Backbone or transit
LSA 1,2,3,7	Totally NSSA
LSA 1,2,7	Totally Stubby

Correct Answer:



Answer Area

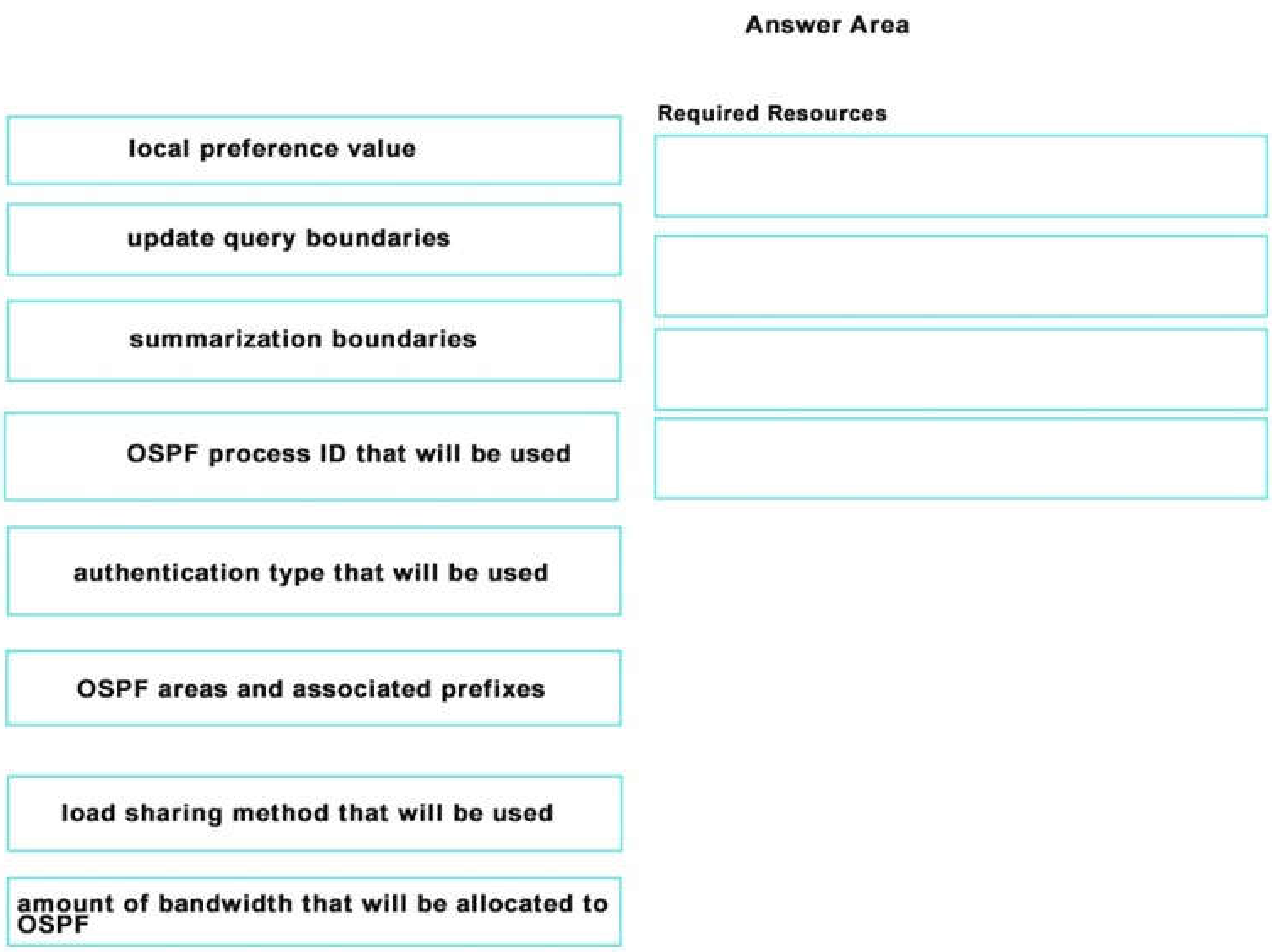
	LSA 1,2,3
	LSA 1,2,3,7
	LSA 1,2,3,4,5
	LSA 1,2,7
	LSA 1,2

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 479
DRAG DROP
Click the resources on the left that you need to create an implementation plan for an OSPF project and drag them to the target zone on the right.

Select and Place:



Answer Area

Required Resources

local preference value

update query boundaries

summarization boundaries

OSPF process ID that will be used

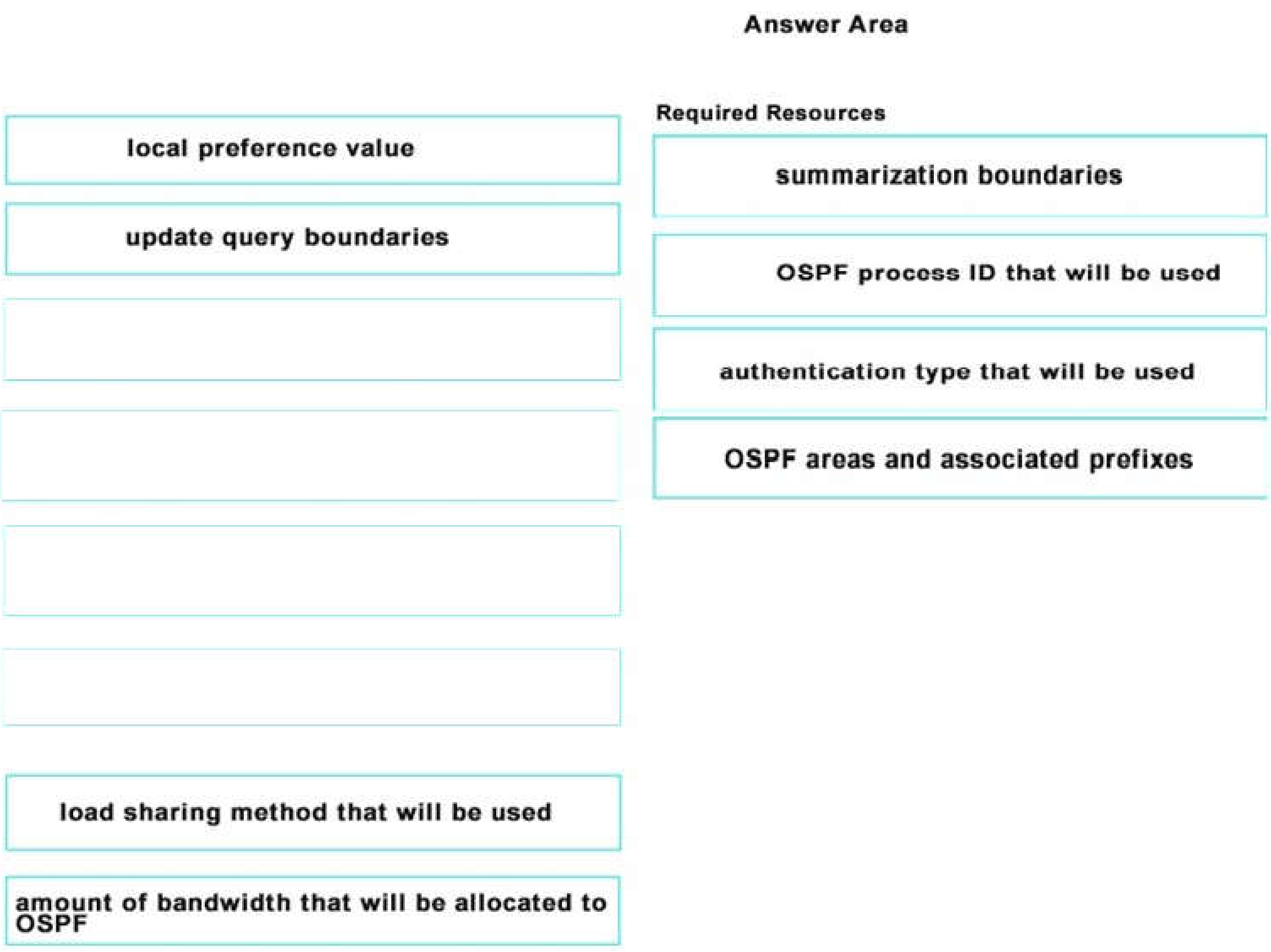
authentication type that will be used

OSPF areas and associated prefixes

load sharing method that will be used

amount of bandwidth that will be allocated to OSPF

Correct Answer:



Answer Area

Required Resources

local preference value

update query boundaries

load sharing method that will be used

amount of bandwidth that will be allocated to OSPF

summarization boundaries

OSPF process ID that will be used

authentication type that will be used

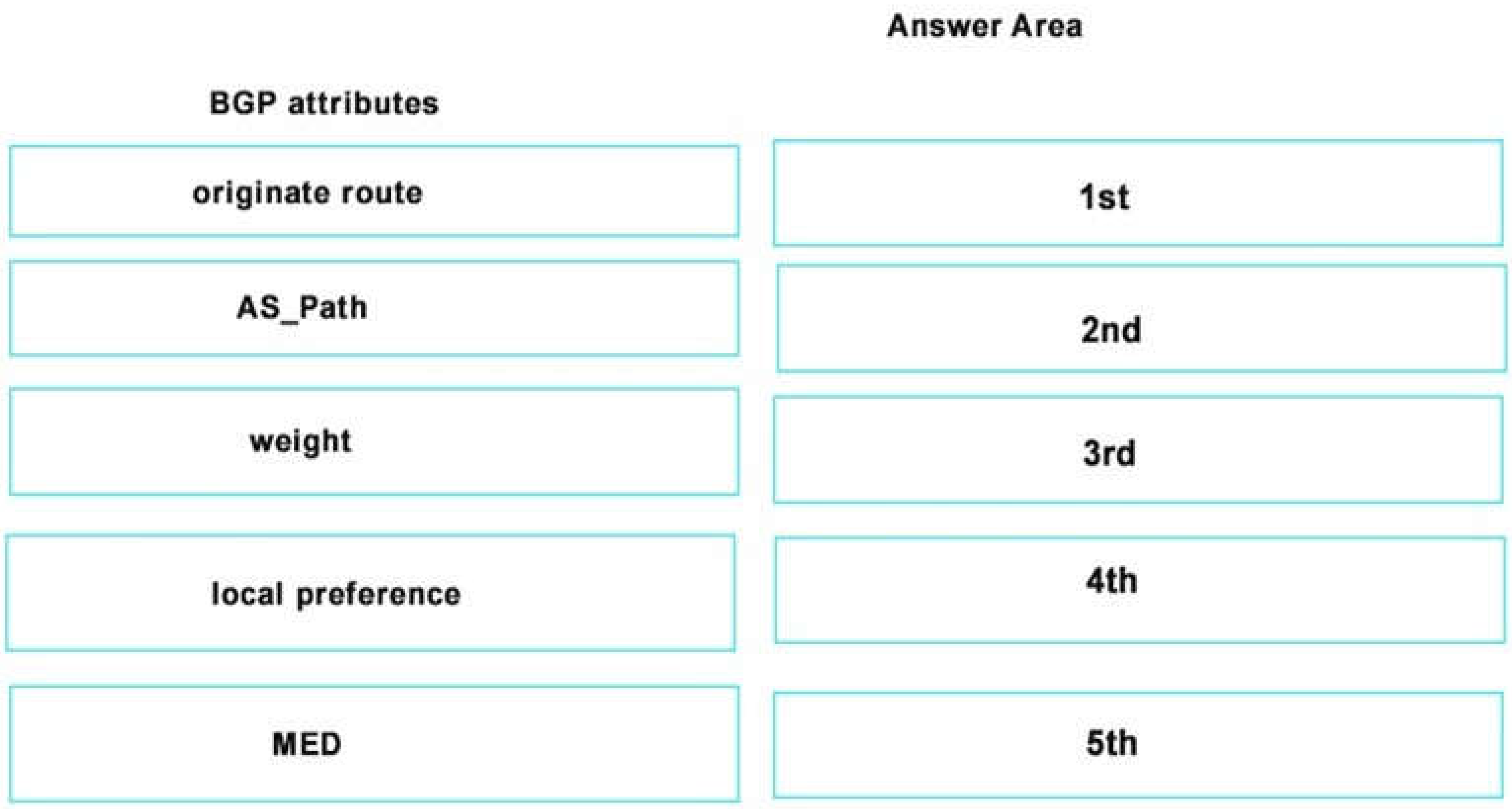
OSPF areas and associated prefixes

Section: Mix Questions
Explanation

Explanation/Reference:

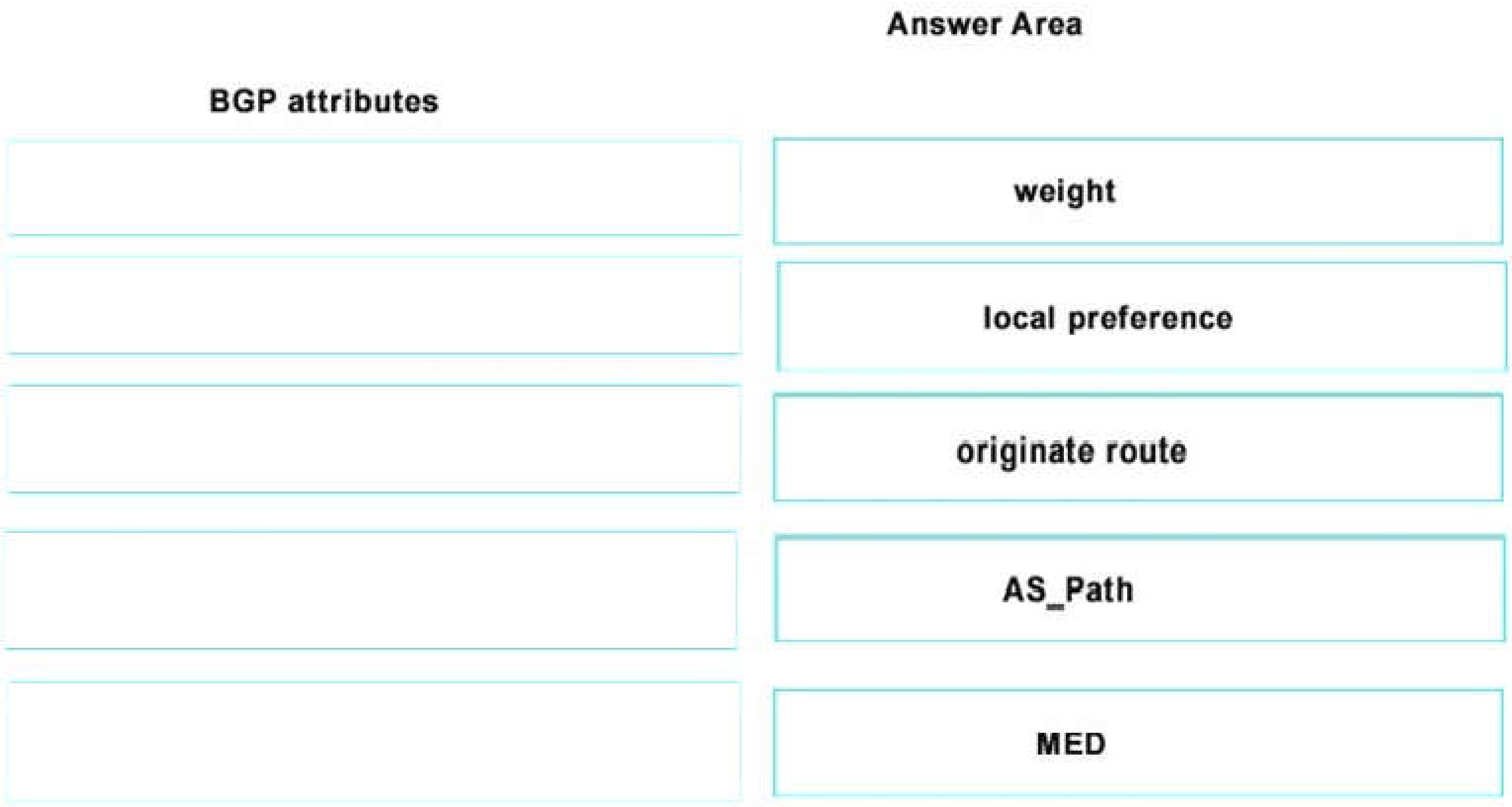
QUESTION 480
DRAG DROP
Place the BGP attributes in the correct order used for determining a route.

Select and Place:



BGP attributes	Answer Area
originate route	1st
AS_Path	2nd
weight	3rd
local preference	4th
MED	5th

Correct Answer:



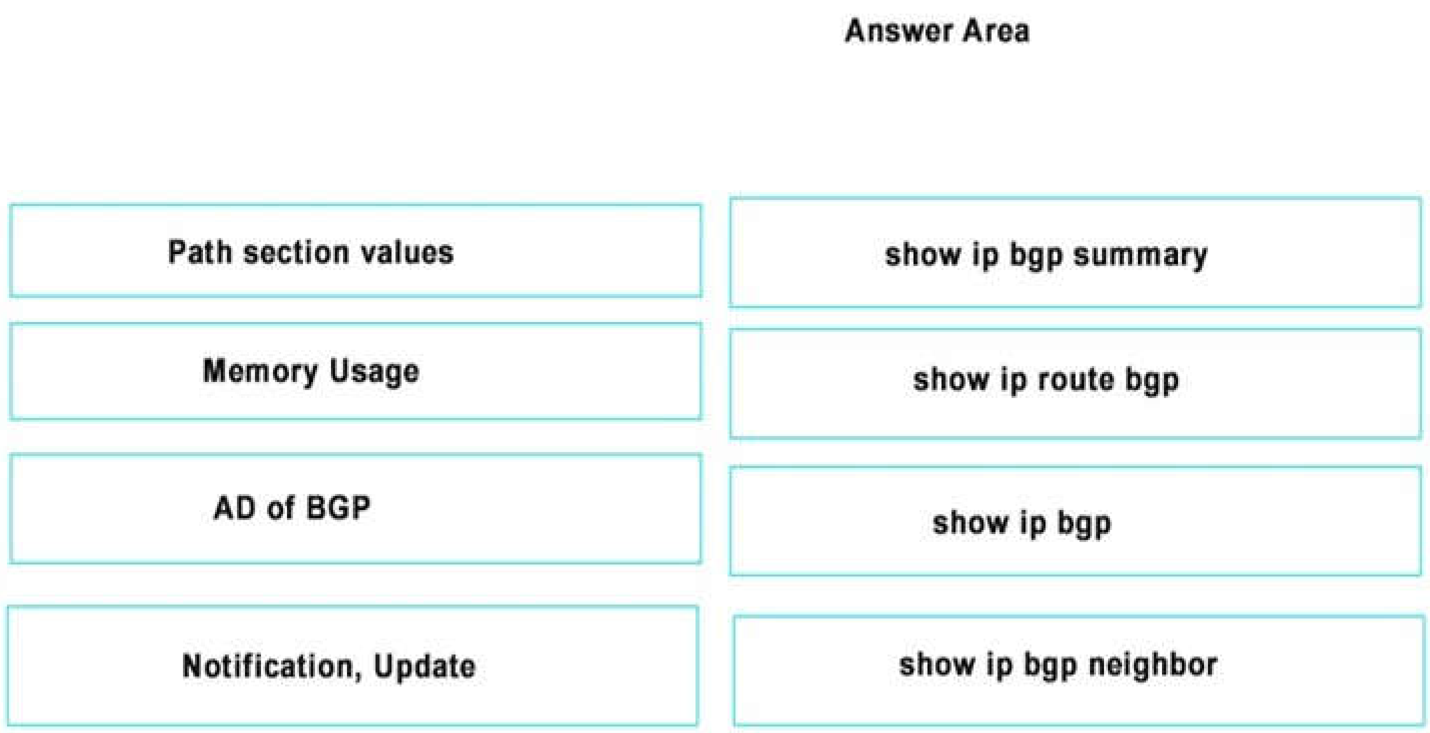
BGP attributes	Answer Area
	weight
	local preference
	originate route
	AS_Path
	MED

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 481
DRAG DROP
Place the BGP commands to the proper locations.

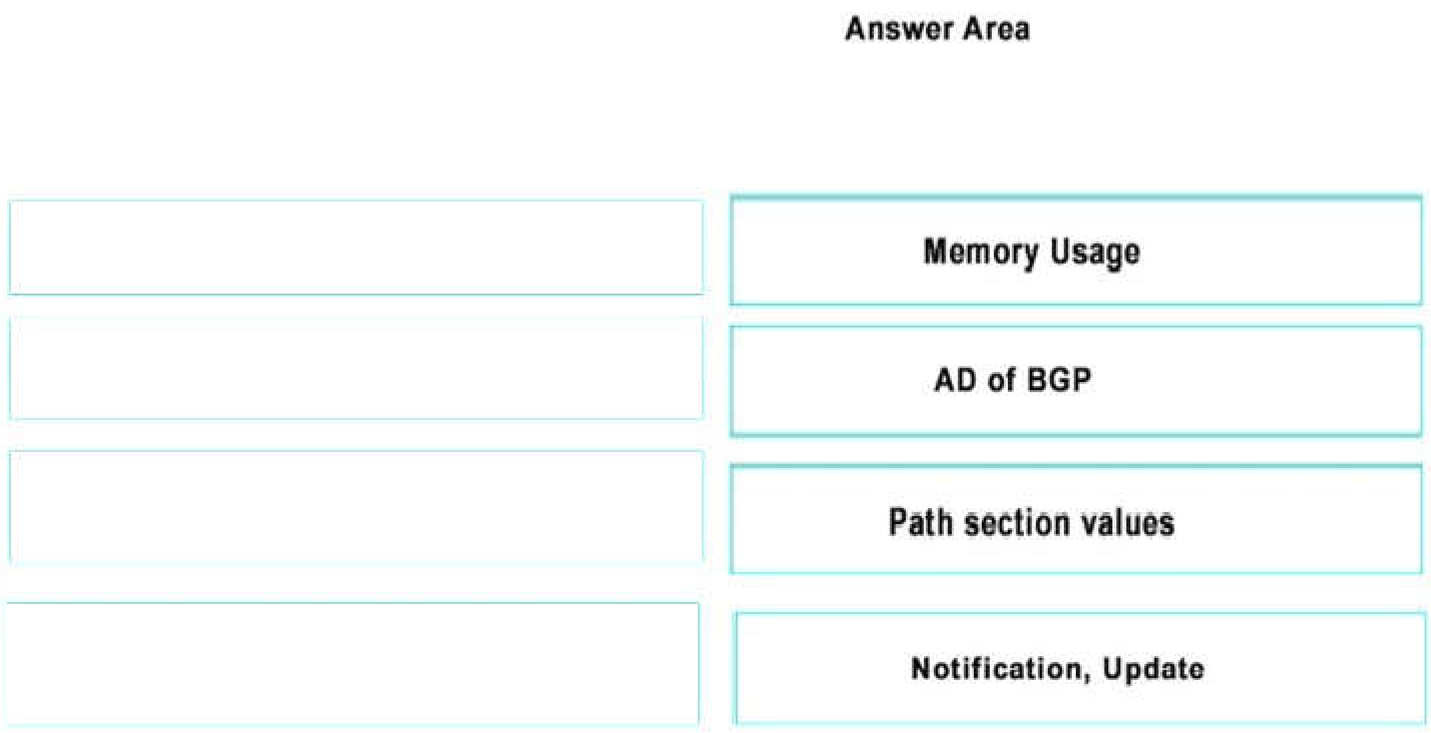
Select and Place:



Answer Area

Path section values	show ip bgp summary
Memory Usage	show ip route bgp
AD of BGP	show ip bgp
Notification, Update	show ip bgp neighbor

Correct Answer:



Answer Area

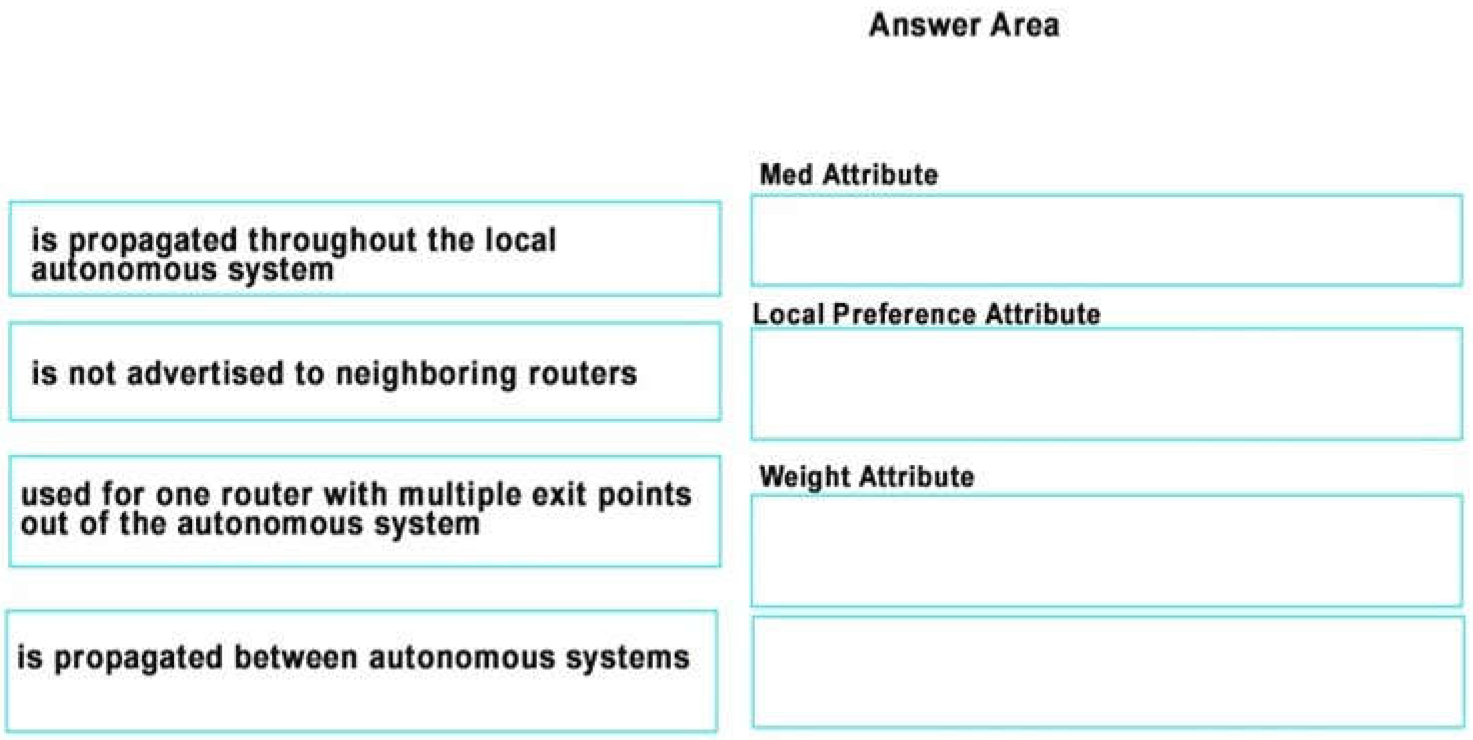
	Memory Usage
	AD of BGP
	Path section values
	Notification, Update

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 482
DRAG DROP
Click and drag the BGP attribute characterization on the left to the correct BGP attribute on the right.

Select and Place:



Answer Area

is propagated throughout the local autonomous system

is not advertised to neighboring routers

used for one router with multiple exit points out of the autonomous system

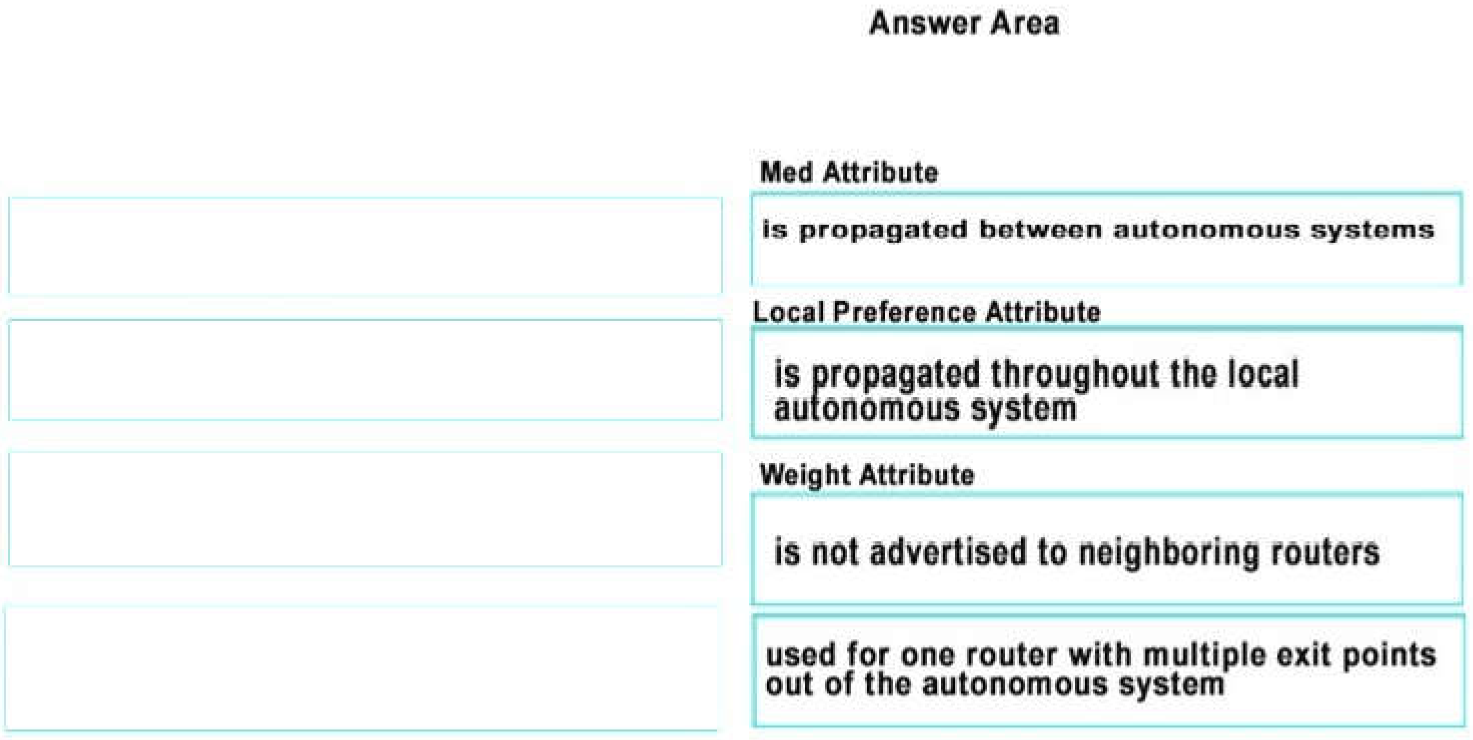
is propagated between autonomous systems

Med Attribute

Local Preference Attribute

Weight Attribute

Correct Answer:



Answer Area

Med Attribute

is propagated between autonomous systems

Local Preference Attribute

is propagated throughout the local autonomous system

Weight Attribute

is not advertised to neighboring routers

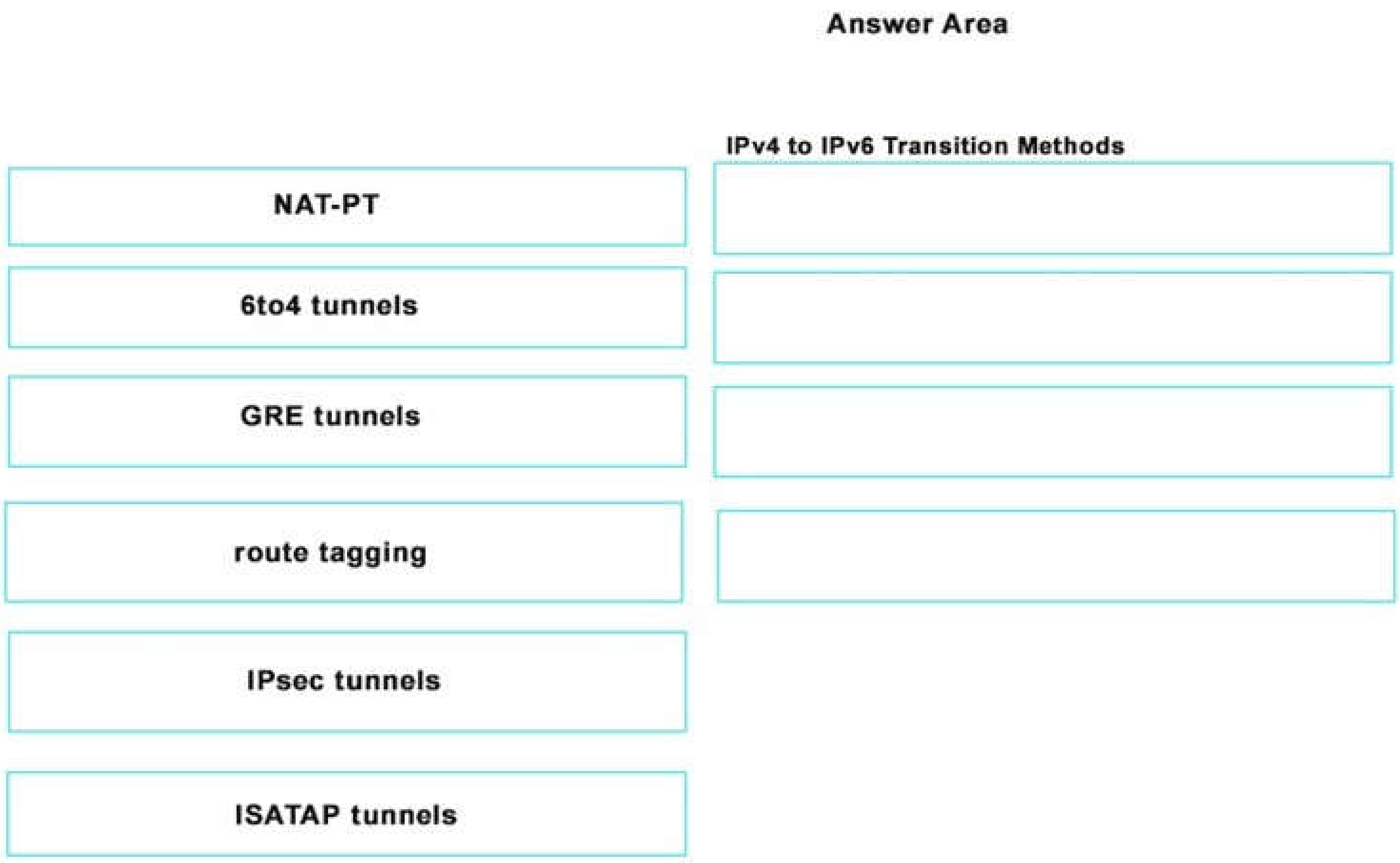
used for one router with multiple exit points out of the autonomous system

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 483
DRAG DROP
Click and drag the correct techniques for transitioning networks or devices from IPv4 to IPv6 from the left to the target zone on the right.

Select and Place:



Answer Area

IPv4 to IPv6 Transition Methods

NAT-PT

6to4 tunnels

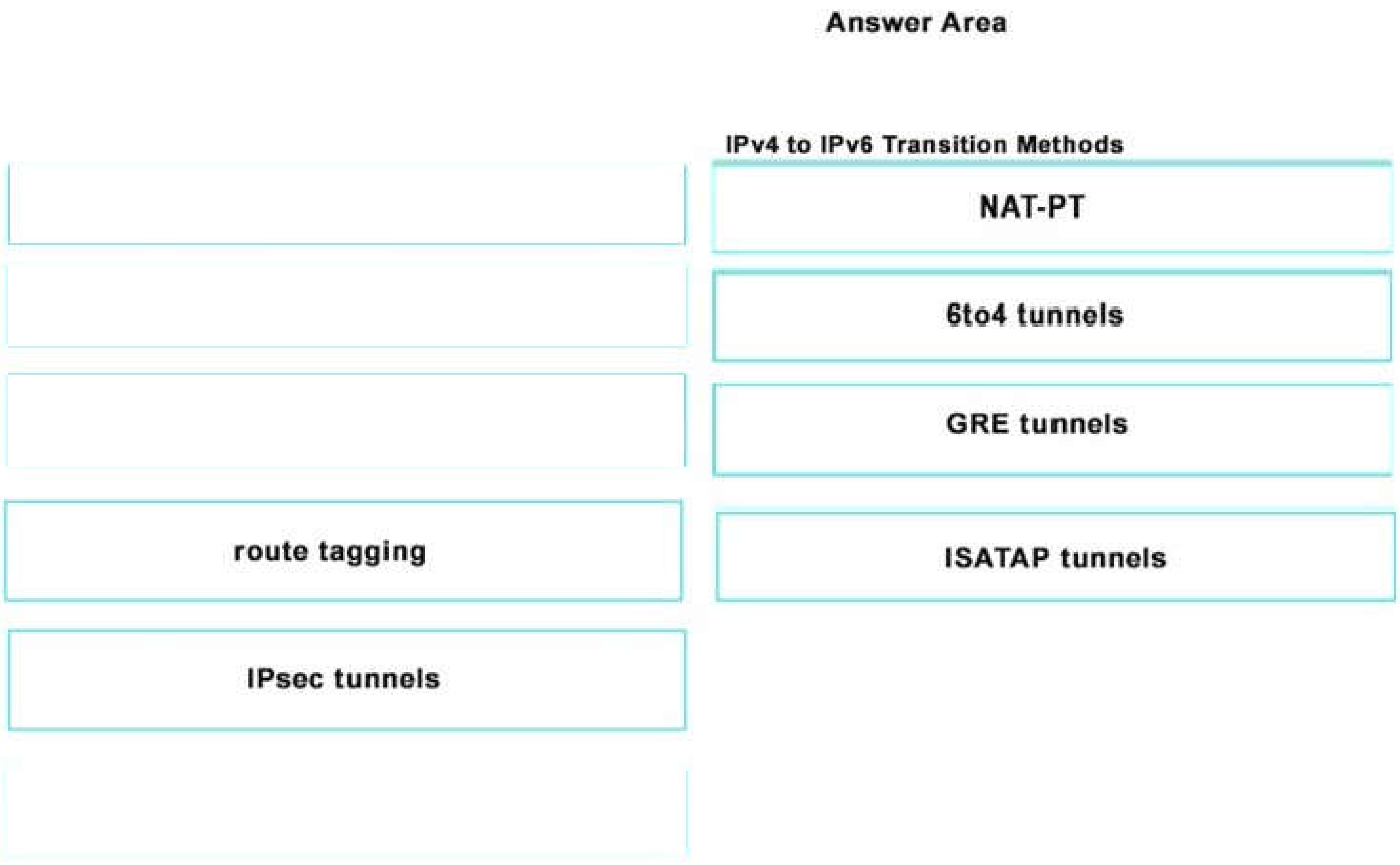
GRE tunnels

route tagging

IPsec tunnels

ISATAP tunnels

Correct Answer:



Answer Area

IPv4 to IPv6 Transition Methods

route tagging

IPsec tunnels

NAT-PT

6to4 tunnels

GRE tunnels

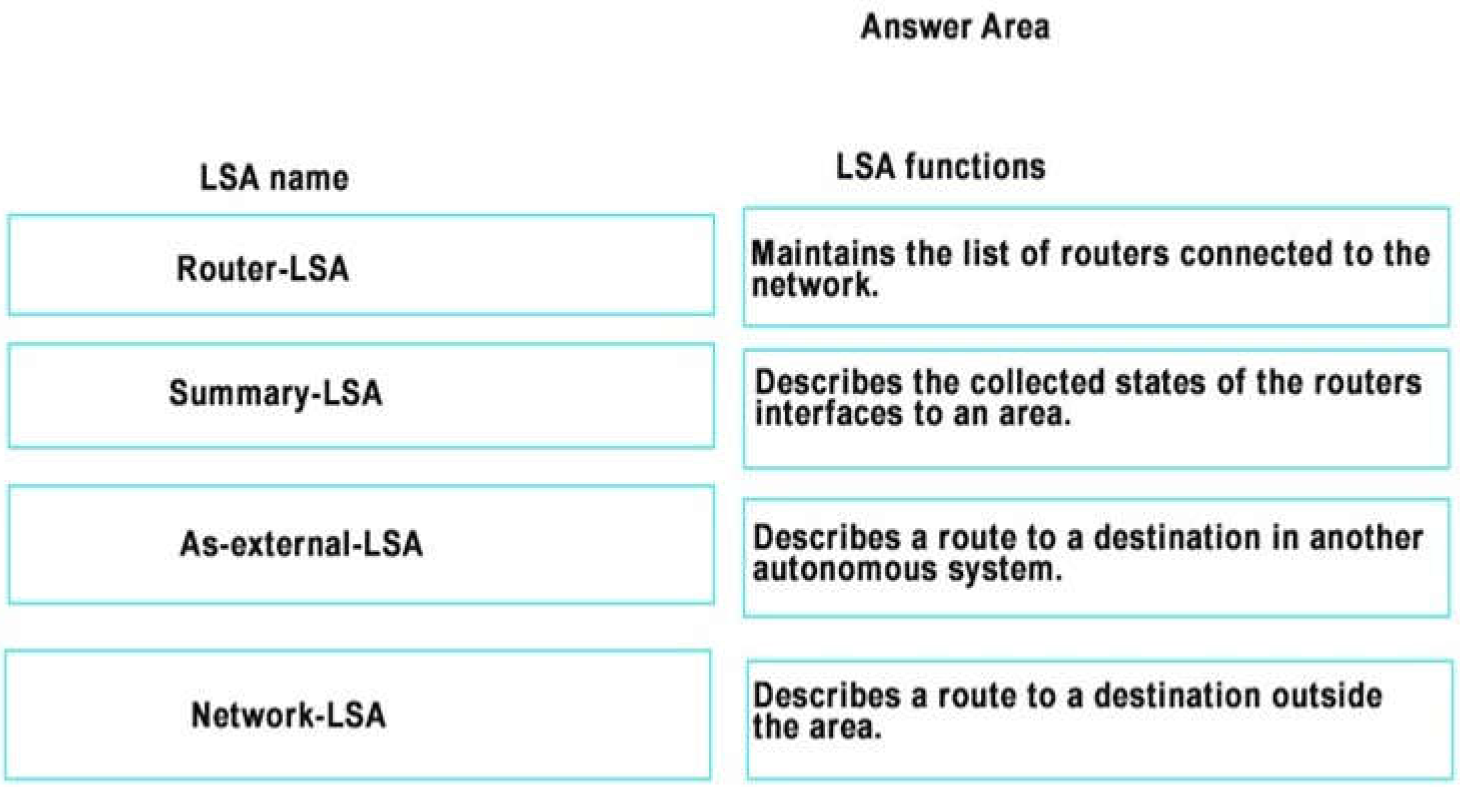
ISATAP tunnels

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 484
DRAG DROP

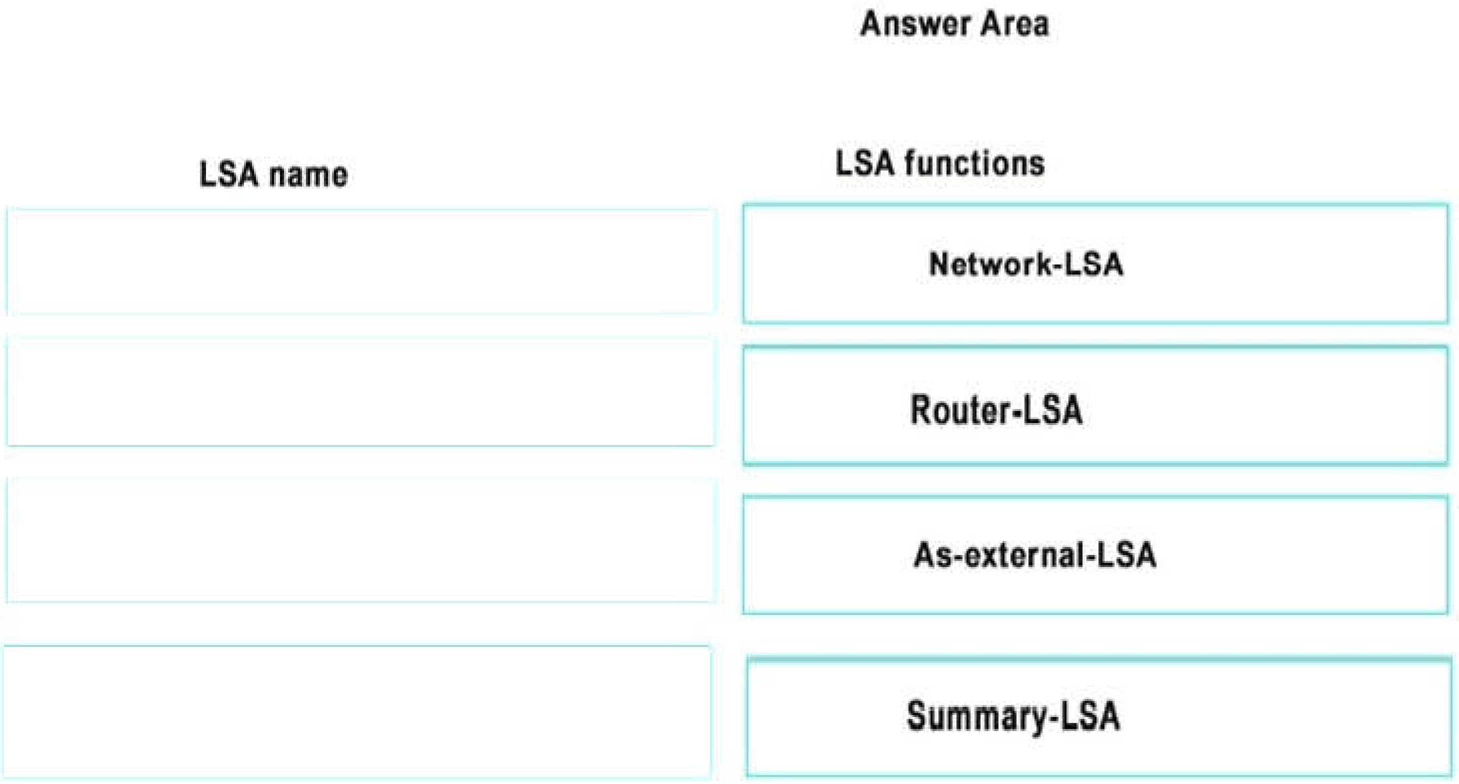
Select and Place:



Answer Area

LSA name	LSA functions
Router-LSA	Maintains the list of routers connected to the network.
Summary-LSA	Describes the collected states of the routers interfaces to an area.
As-external-LSA	Describes a route to a destination in another autonomous system.
Network-LSA	Describes a route to a destination outside the area.

Correct Answer:



Answer Area

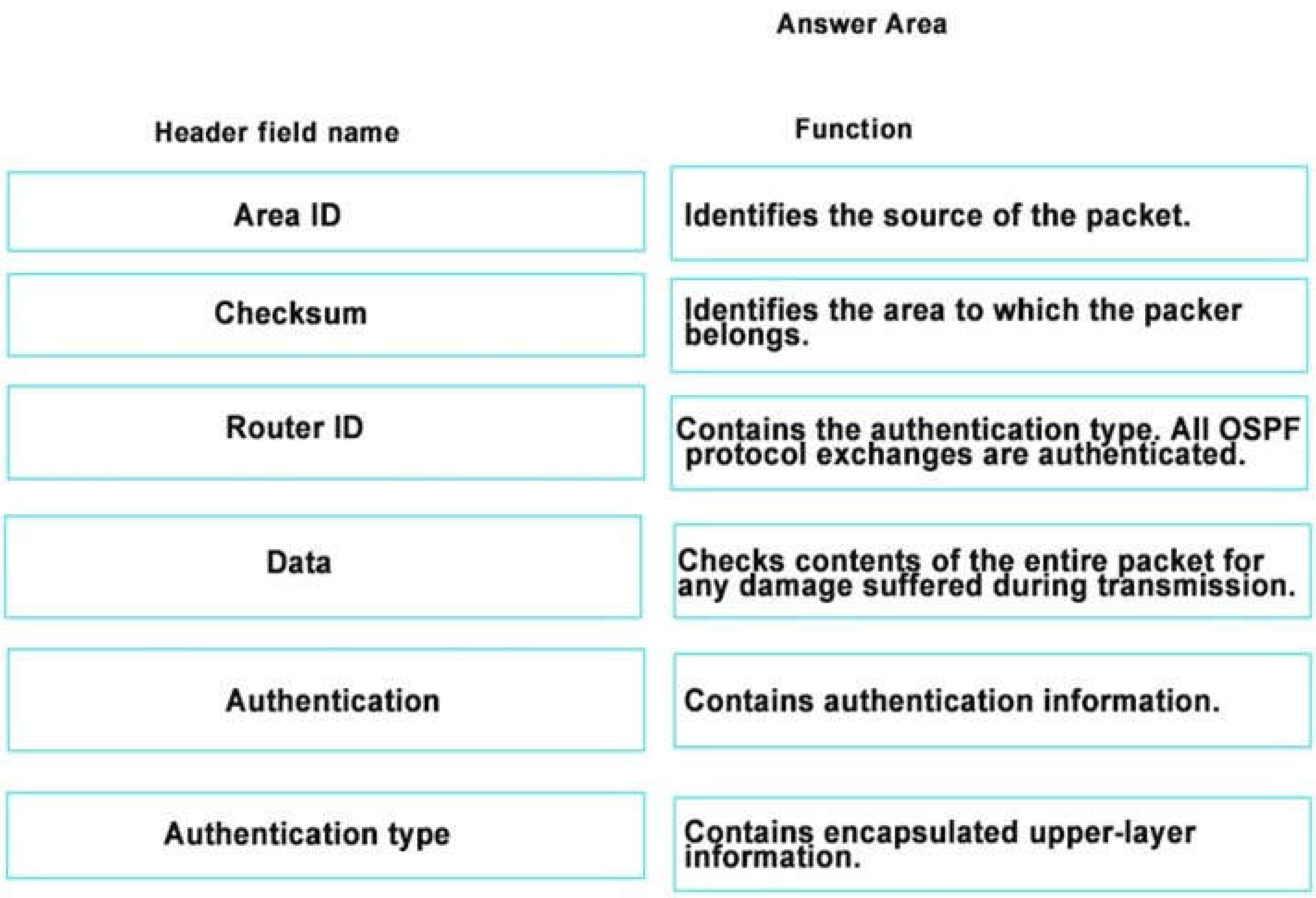
LSA name	LSA functions
	Network-LSA
	Router-LSA
	As-external-LSA
	Summary-LSA

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 485
DRAG DROP

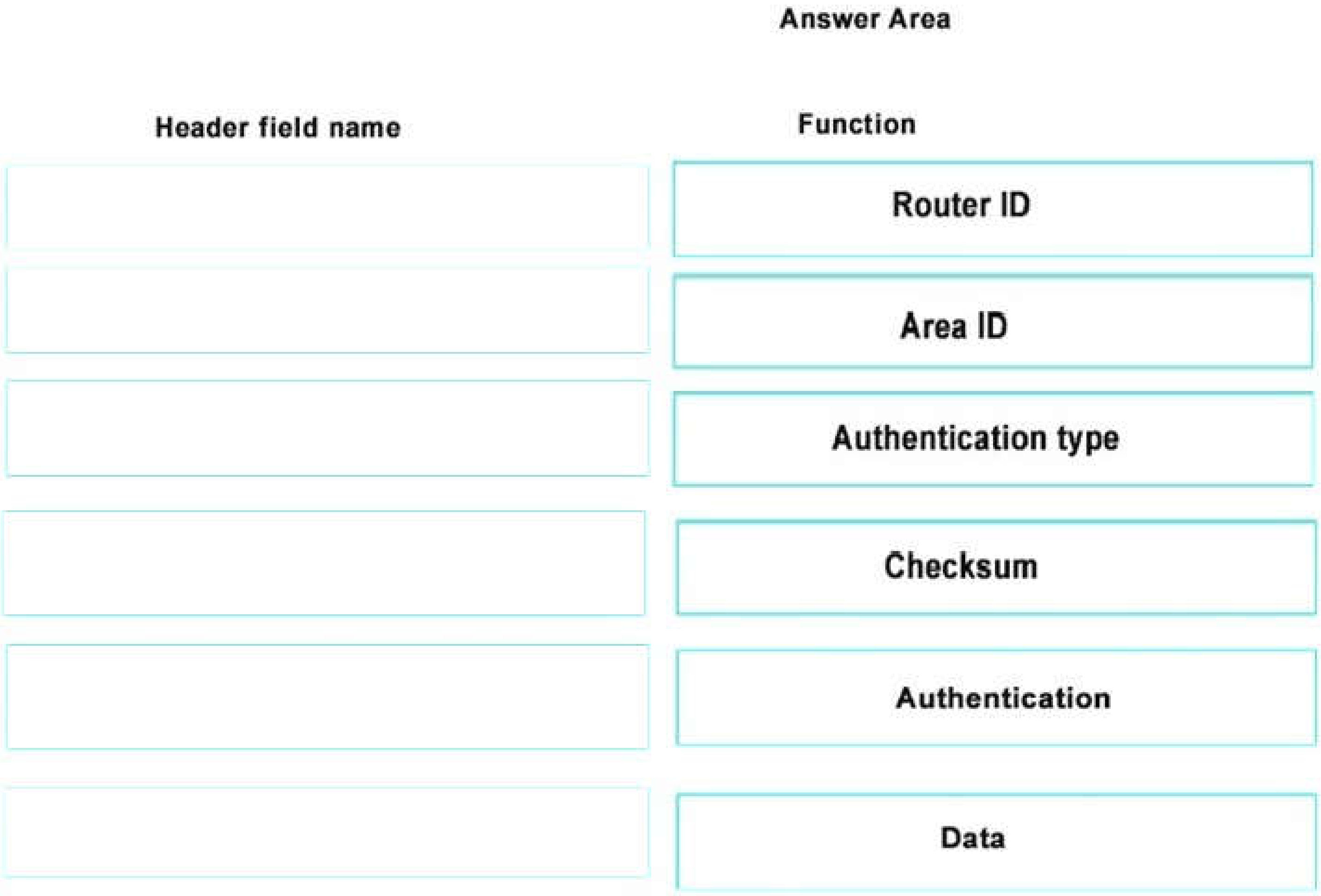
Select and Place:



Answer Area

Header field name	Function
Area ID	Identifies the source of the packet.
Checksum	Identifies the area to which the packer belongs.
Router ID	Contains the authentication type. All OSPF protocol exchanges are authenticated.
Data	Checks contents of the entire packet for any damage suffered during transmission.
Authentication	Contains authentication information.
Authentication type	Contains encapsulated upper-layer information.

Correct Answer:



Answer Area

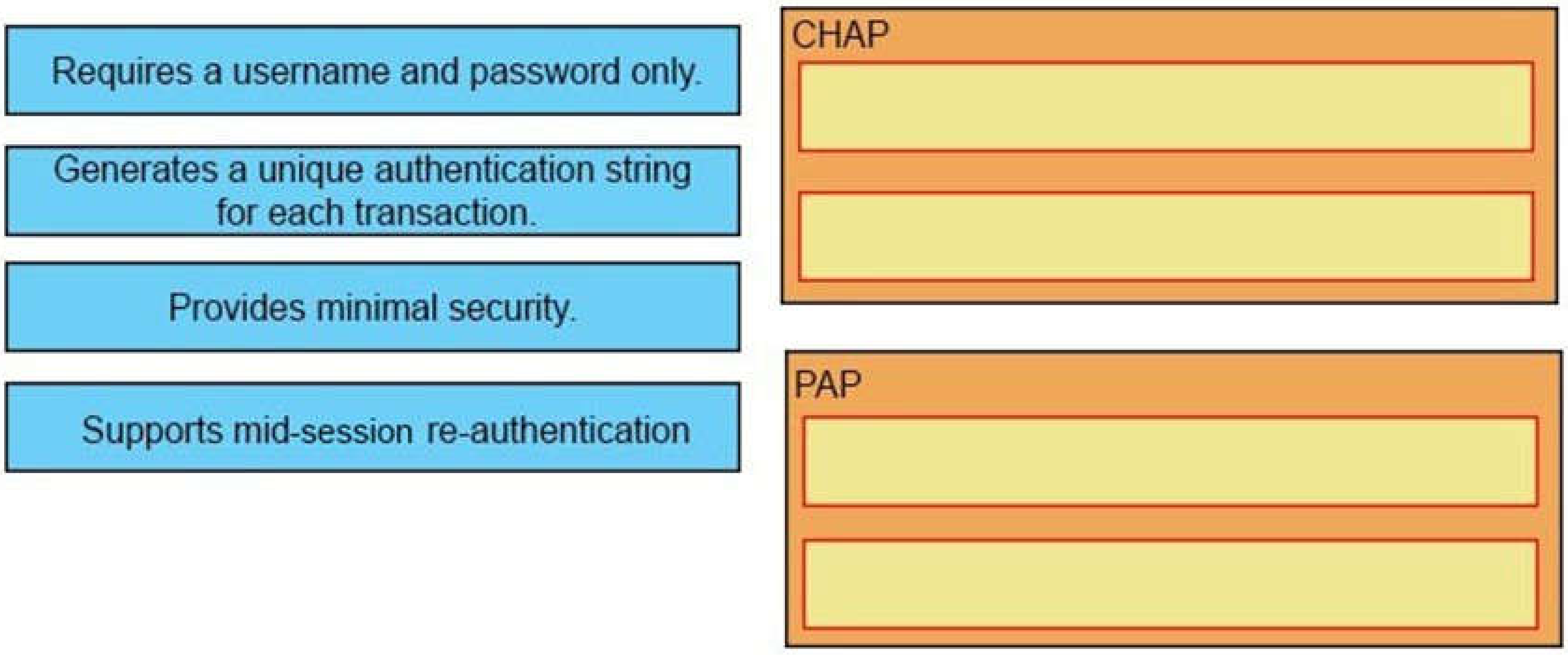
Header field name	Function
	Router ID
	Area ID
	Authentication type
	Checksum
	Authentication
	Data

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 486
DRAG DROP
Drag each statement about authentication mechanisms on the left to the matching authentication type on the right.

Select and Place:



Requires a username and password only.

Generates a unique authentication string for each transaction.

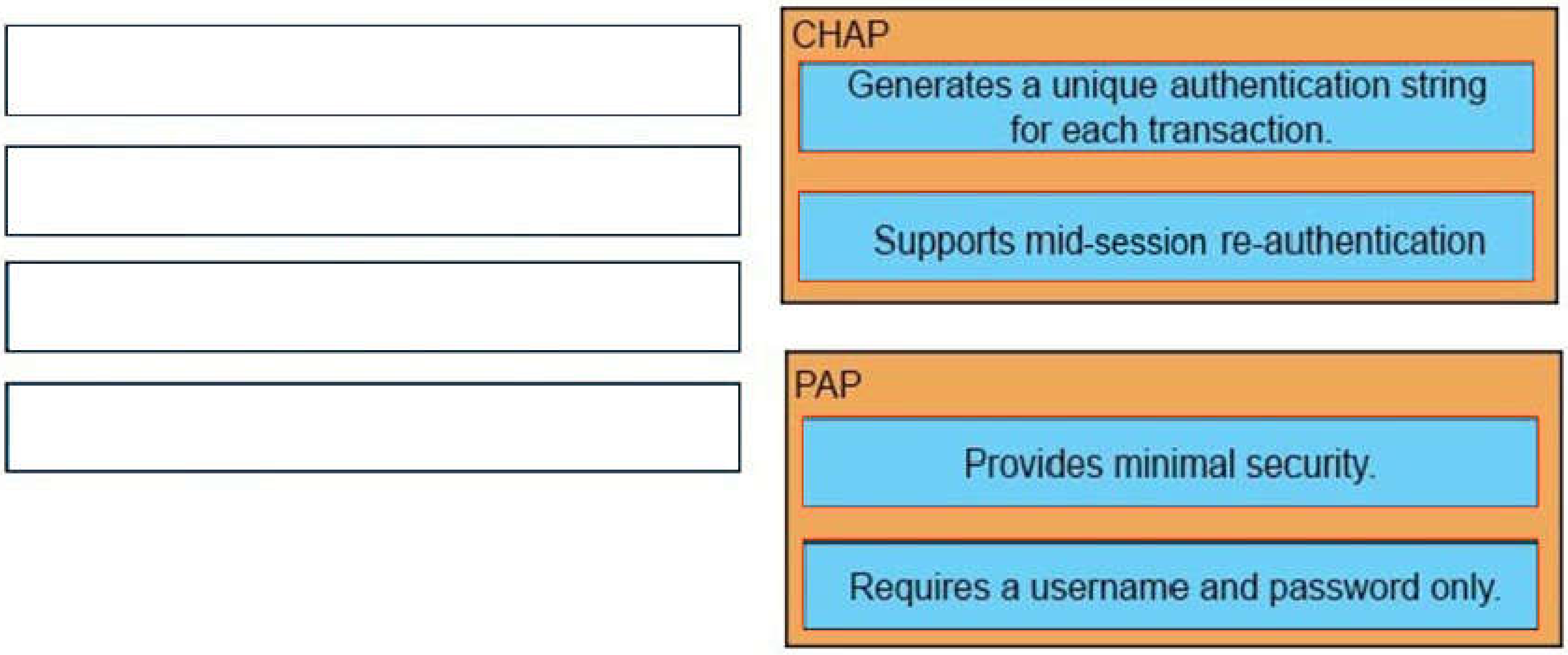
Provides minimal security.

Supports mid-session re-authentication

CHAP

PAP

Correct Answer:



CHAP

Generates a unique authentication string for each transaction.

Supports mid-session re-authentication

PAP

Provides minimal security.

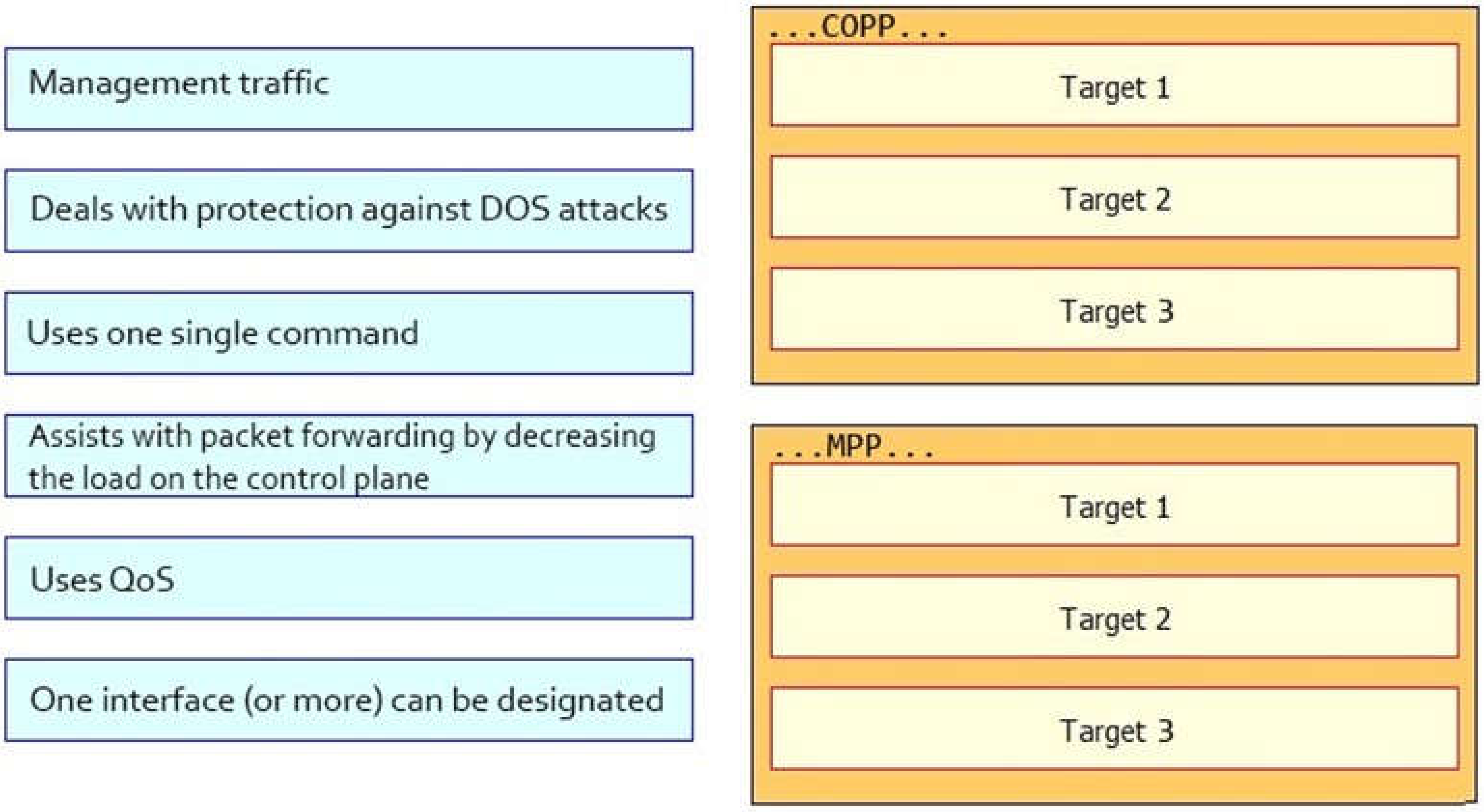
Requires a username and password only.

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 487
DRAG DROP

Select and Place:



Management traffic

Deals with protection against DOS attacks

Uses one single command

Assists with packet forwarding by decreasing the load on the control plane

Uses QoS

One interface (or more) can be designated

...COPP...

Target 1

Target 2

Target 3

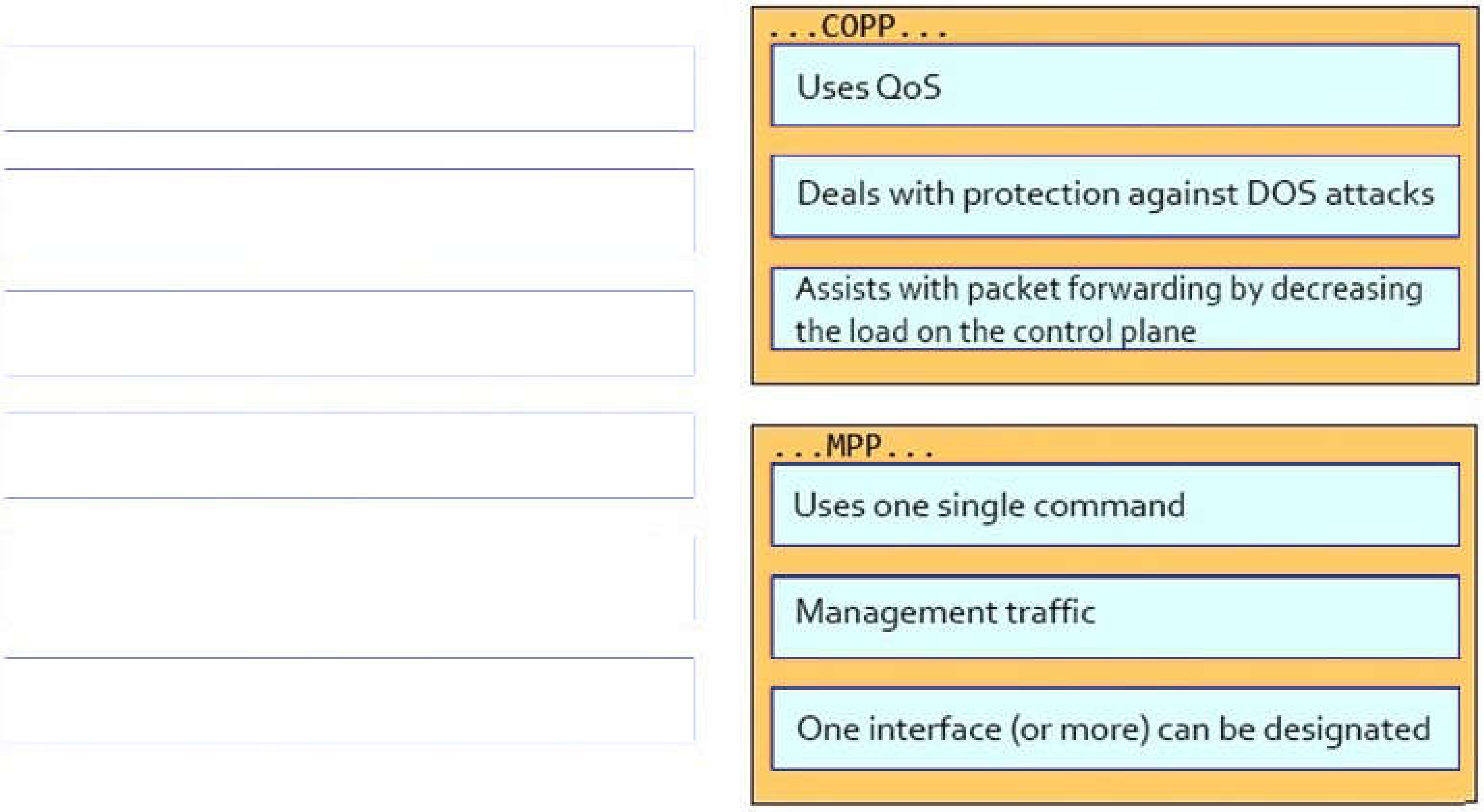
...MPP...

Target 1

Target 2

Target 3

Correct Answer:



...COPP...

Uses QoS

Deals with protection against DOS attacks

Assists with packet forwarding by decreasing the load on the control plane

...MPP...

Uses one single command

Management traffic

One interface (or more) can be designated

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
CoPP and MPP
https://www.cisco.com/c/en/us/about/security-center/copp-best-practices.html

Control Plane Policing (CoPP) – CoPP is the Cisco IOS-wide route processor protection mechanism. As illustrated in Figure 2, and similar to rACLs, CoPP is deployed once to the punt path of the router. However, unlike rACLs that only apply to receive destination IP packets, CoPP applies to all packets that punt to the route processor for handling. CoPP therefore covers not only receive destination IP packets, it also exceptions IP packets and non-IP packets. In addition, CoPP is implemented using the Modular QoS CLI (MQC) framework for policy construction. In this way, in addition to simply permit and deny functions, specific packets may be permitted but rate-limited. This behavior substantially improves the ability to define an effective CoPP policy. (Note: that “Control Plane Policing” is something of a misnomer because CoPP generally protects the punt path to the route processor and not solely the control plane.)

CoPP Policy Construction and Deployment Concepts

Before describing the details of CoPP policy construction and deployment, some of the important details related to MQC and its operation, especially within the context of CoPP are discussed.

In MQC, the class-map command is used to define a traffic class. A traffic class contains three major elements: a name, one or a series of match commands, and an instruction on how to evaluate these match commands. Match commands are used to specify various criteria for classifying packets. Packets are checked to see whether they match the criteria specified in the match commands. If a packet matches the specified criteria, that packet is considered a member of the class and is treated according to the QoS specifications set in the service policy. Packets that fail to meet any of the matching criteria are classified as members of the default class.

The instruction for evaluating match commands is specified as either match-any or match-all. When more than one match statement is included, match-any requires that a packet match at least one of the statements to be included in the class. If match-all is used, a packet must match all of the statements to be included in the class.

The policy-map command is used to associate a traffic class, defined by the class-map command, with one or more QoS policies. The result of this association is called a service policy. A service policy contains three elements: a name, a traffic class (specified with the class command), and the QoS policies. The purpose of the service policy is to associate a traffic class with one or more QoS policies. Classes included within policy maps are processed top-down. When a packet is found to match a class, no further processing is performed. That is, a packet can only belong to a single class, and it is the first one to which a match occurs. When a packet does not match any of the defined classes, it is automatically placed in the class class-default. The default class is always applied, whether it is explicitly configured or not.

The service-policy command is used to attach the service policy, as specified with the policy-map command, to an interface. In the case of CoPP, this is the control-plane interface. Because the elements of the service policy can be applied to packets entering, or in some versions of CoPP, leaving the interface, users are required to specify whether the service policy characteristics should be applied to incoming or outgoing packets.

It is important to note that MQC is a general framework used for enabling all QoS throughout Cisco IOS, and not exclusively for CoPP. Not all features available within the MQC framework are available or applicable to CoPP policies. For example, only certain classification (match) criteria are applicable to CoPP. In some instances, there are MQC platform and/or IOS-dependencies that may apply to CoPP. Consult the appropriate product references and configuration guides for any CoPP-specific dependencies.

Constructing the CoPP Policy
Deploying the CoPP Policy
Verifying the CoPP Policy
Tuning the CoPP Policy

https://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t11/htsecmpp.html#wp1049321

Management Plane

The management plane is the logical path of all traffic related to the management of a routing platform. One of three planes in a communication architecture that is structured in layers and planes, the management plane performs management functions for a network and coordinates functions among all the planes (management, control, data). The management plane also is used to manage a device through its connection to the network.

Examples of protocols processed in the management plane are Simple Network Management Protocol (SNMP), Telnet, HTTP, Secure HTTP (HTTPS), and SSH. These management protocols are used for monitoring and for CLI access. Restricting access to devices to internal sources (trusted networks) is critical.

Benefits of the Management Plane Protection Feature

Implementing the MPP feature provides the following benefits:

-Greater access control for managing a device than allowing management protocols on all interfaces

-Improved performance for data packets on nonmanagement interfaces
-Support for network scalability

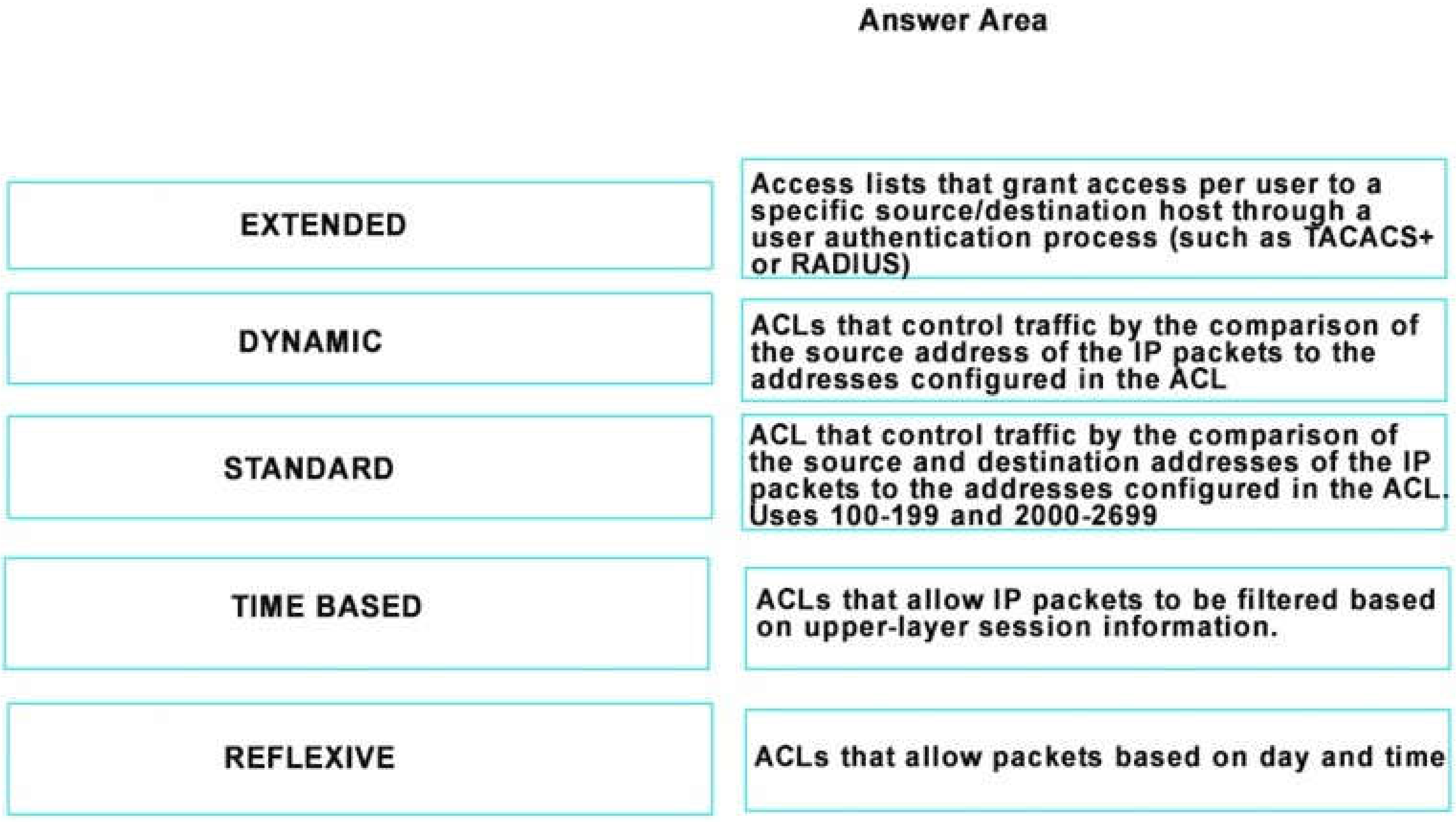
-Simplifies the task of using per-interface ACLs to restrict management access to the device

-Fewer ACLs needed to restrict access to the device

-Management packet floods on switching and routing interfaces are prevented from reaching the CPU

QUESTION 488
DRAG DROP

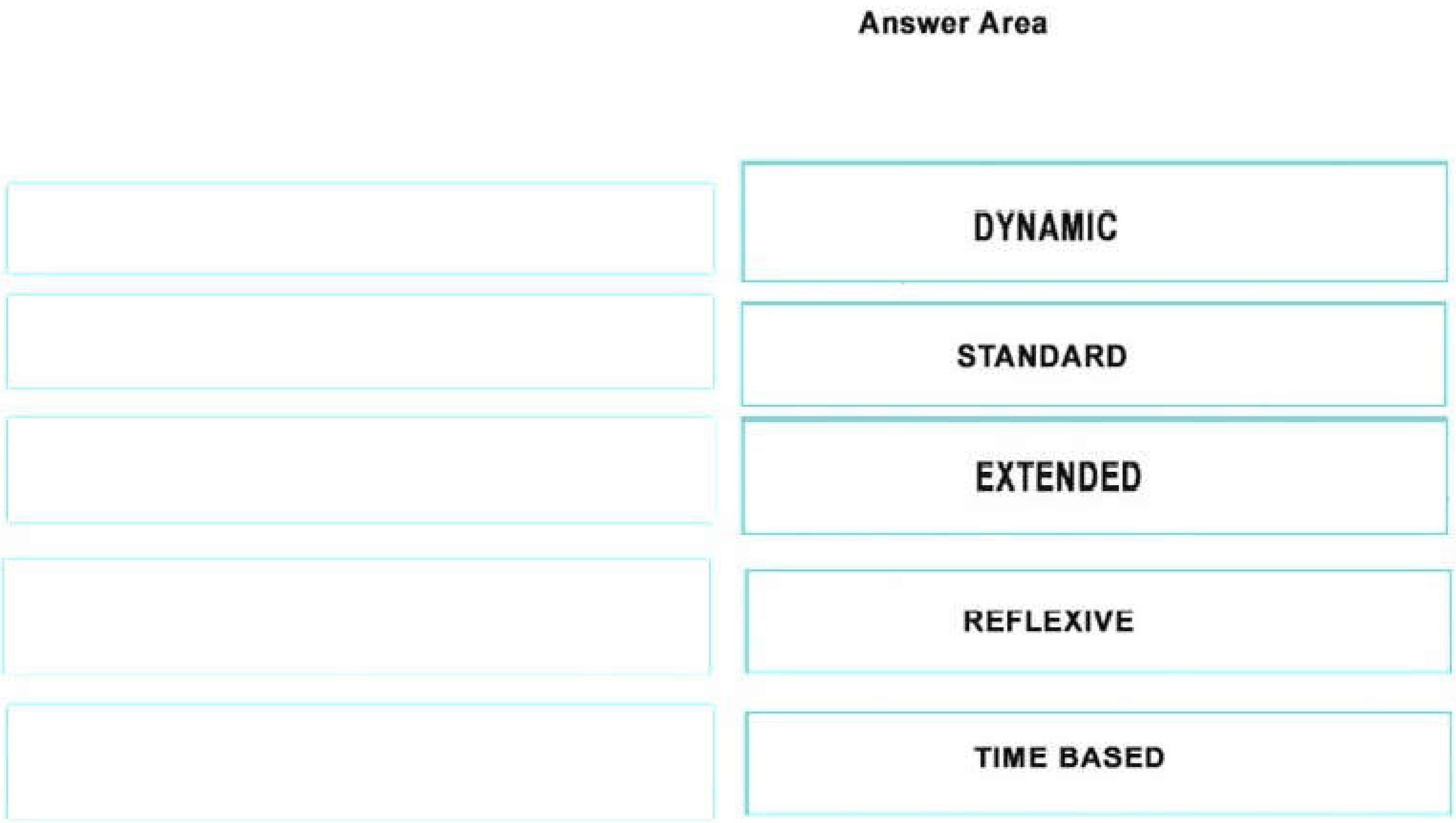
Select and Place:



Answer Area

EXTENDED	Access lists that grant access per user to a specific source/destination host through a user authentication process (such as TACACS+ or RADIUS)
DYNAMIC	ACLs that control traffic by the comparison of the source address of the IP packets to the addresses configured in the ACL
STANDARD	ACL that control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL. Uses 100-199 and 2000-2699
TIME BASED	ACLs that allow IP packets to be filtered based on upper-layer session information.
REFLEXIVE	ACLs that allow packets based on day and time

Correct Answer:



Answer Area

DYNAMIC

STANDARD

EXTENDED

REFLEXIVE

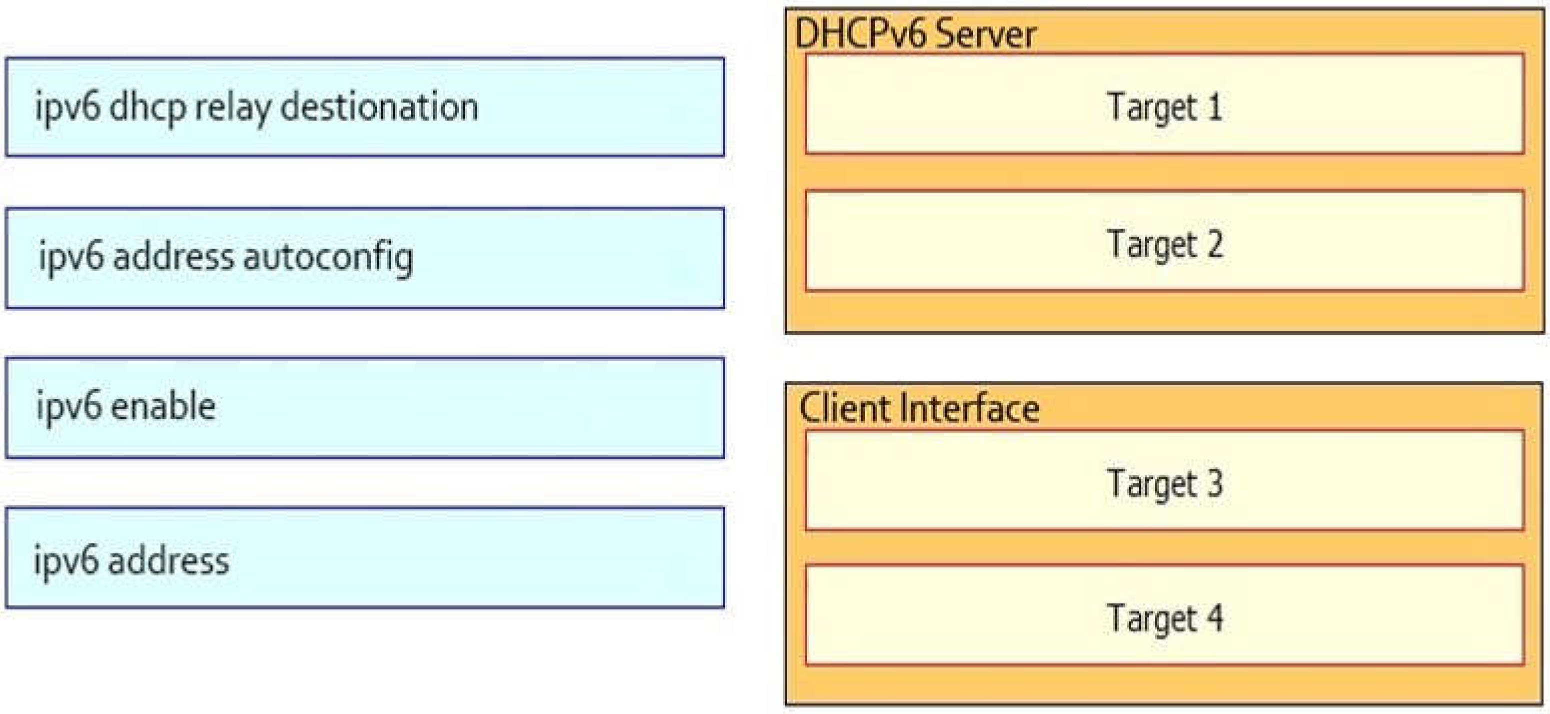
TIME BASED

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 489
DRAG DROP
How to configure IPv6 DHCP Relay?

Select and Place:



ipv6 dhcp relay destionation

ipv6 address autoconfig

ipv6 enable

ipv6 address

DHCPv6 Server

Target 1

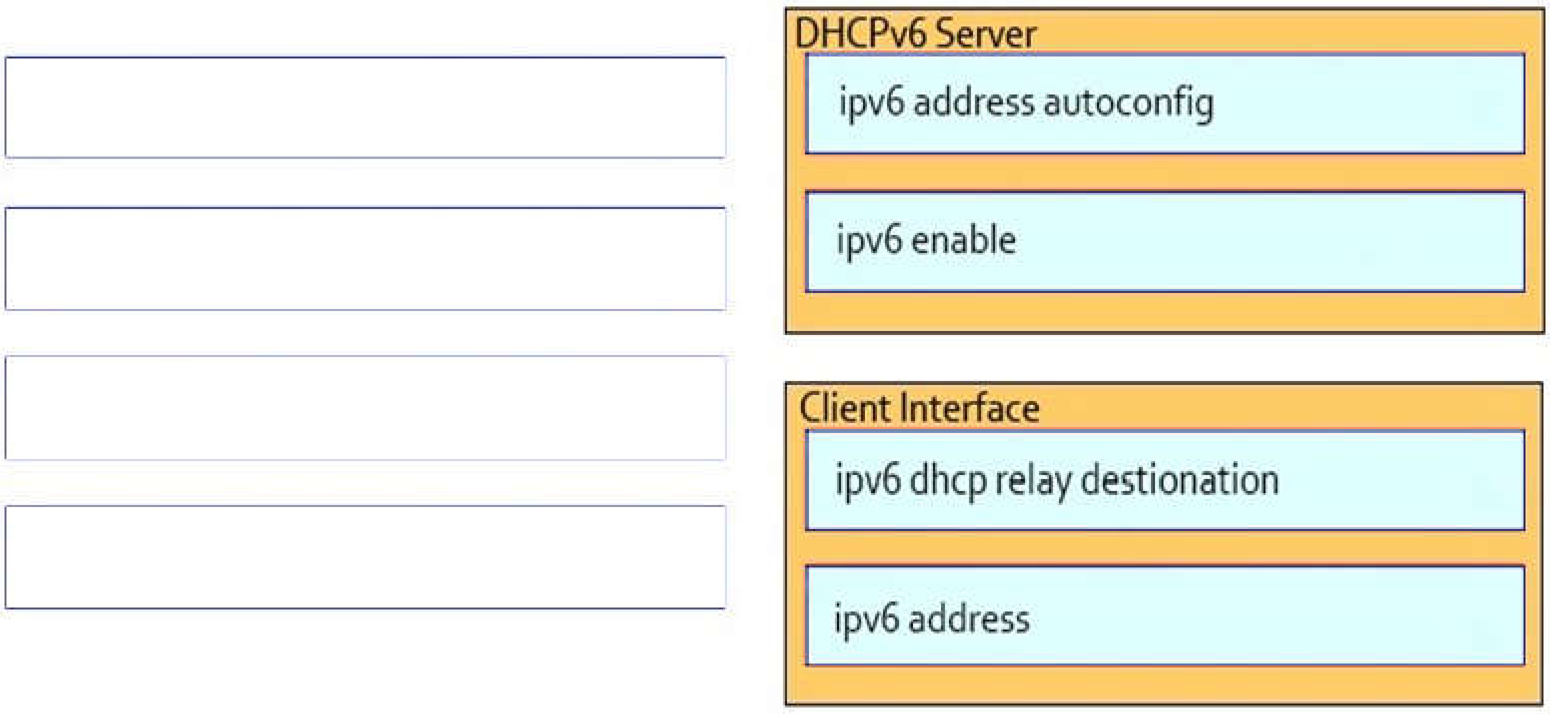
Target 2

Client Interface

Target 3

Target 4

Correct Answer:



DHCPv6 Server

ipv6 address autoconfig

ipv6 enable

Client Interface

ipv6 dhcp relay destionation

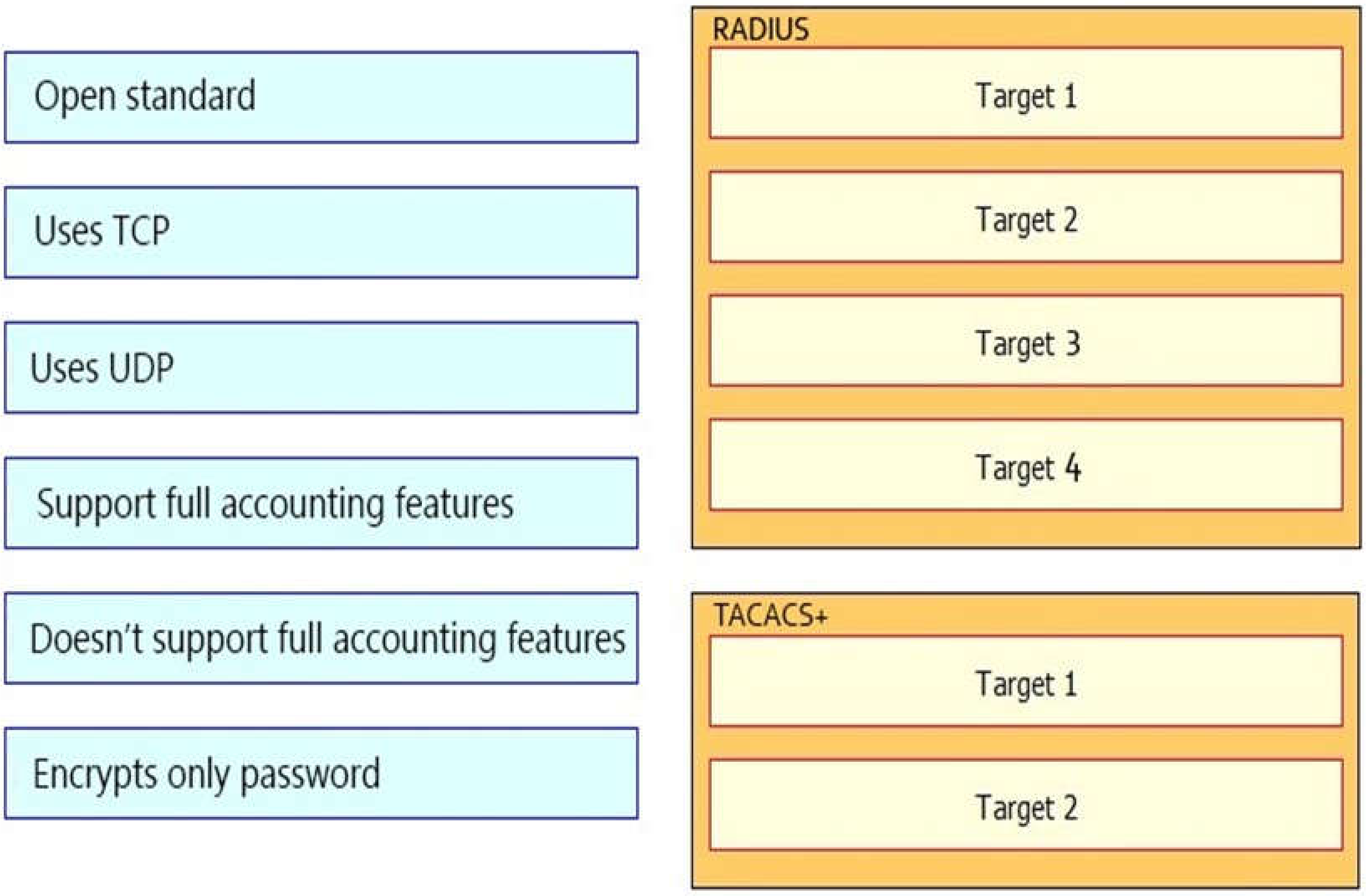
ipv6 address

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 490
498 DRAG DROP

Select and Place:



Open standard

Uses TCP

Uses UDP

Support full accounting features

Doesn't support full accounting features

Encrypts only password

RADIUS

Target 1

Target 2

Target 3

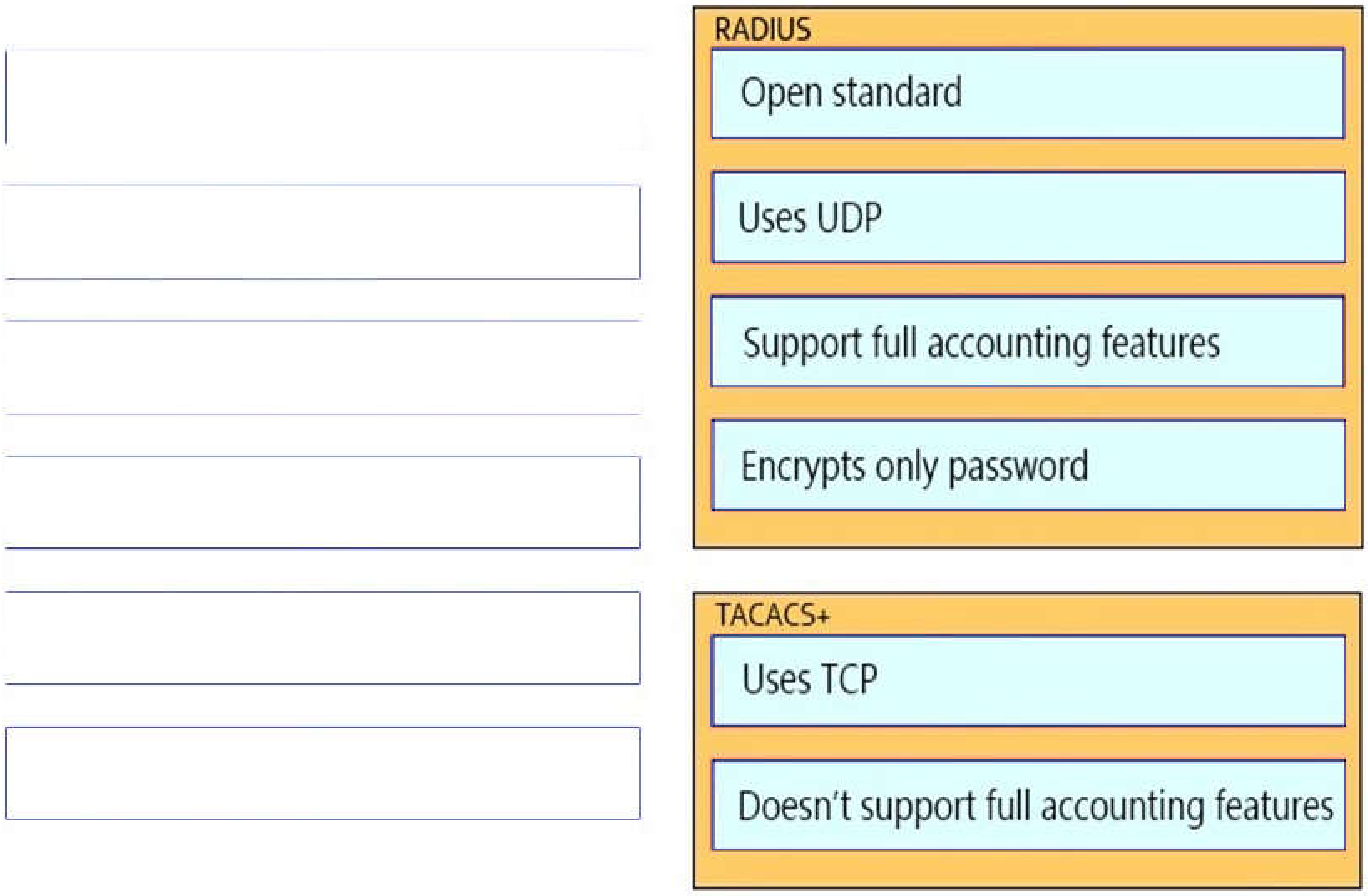
Target 4

TACACS+

Target 1

Target 2

Correct Answer:



RADIUS

Open standard

Uses UDP

Support full accounting features

Encrypts only password

TACACS+

Uses TCP

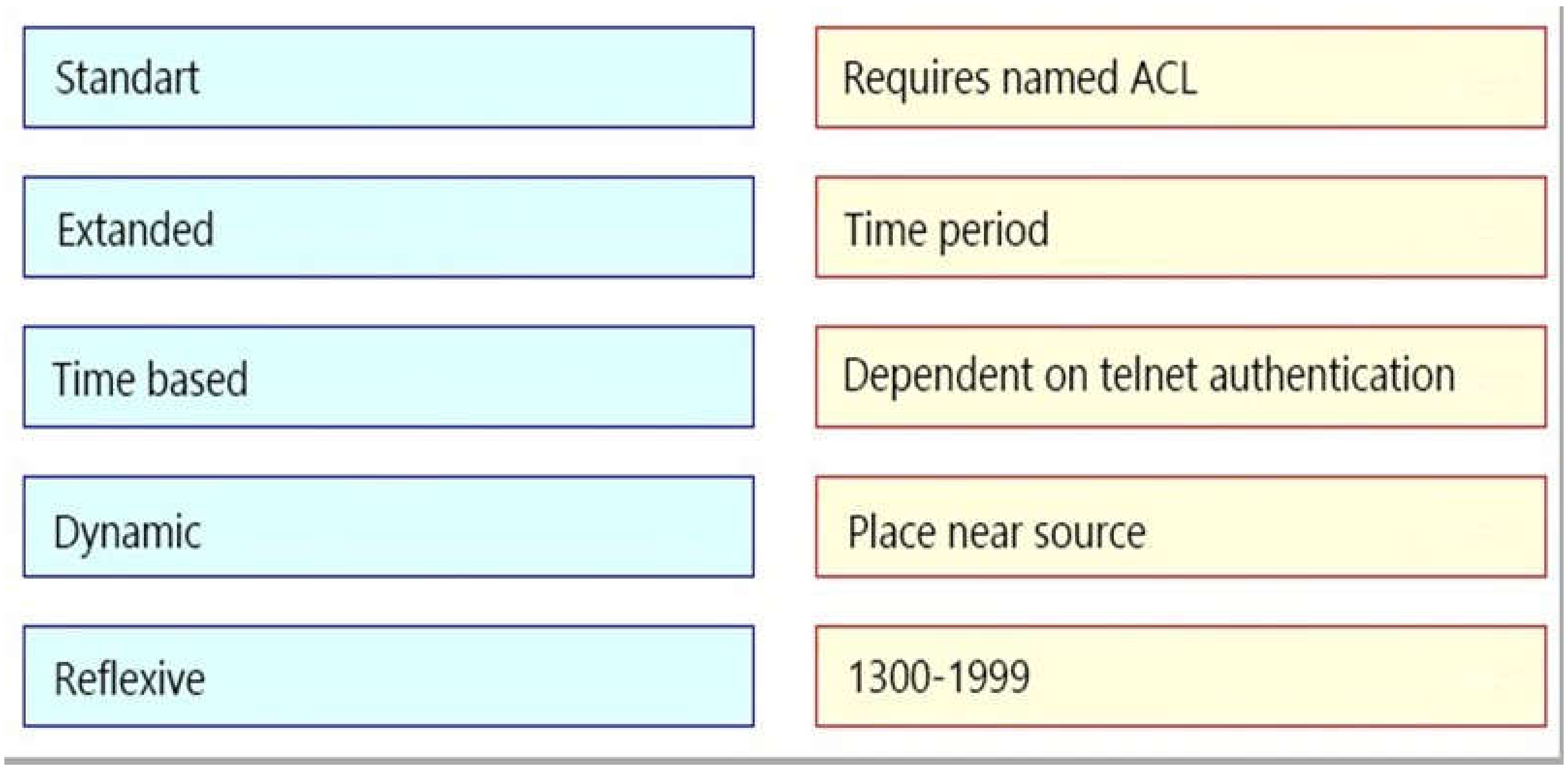
Doesn't support full accounting features

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 491
DRAG DROP

Select and Place:



Standart

Extanded

Time based

Dynamic

Reflexive

Requires named ACL

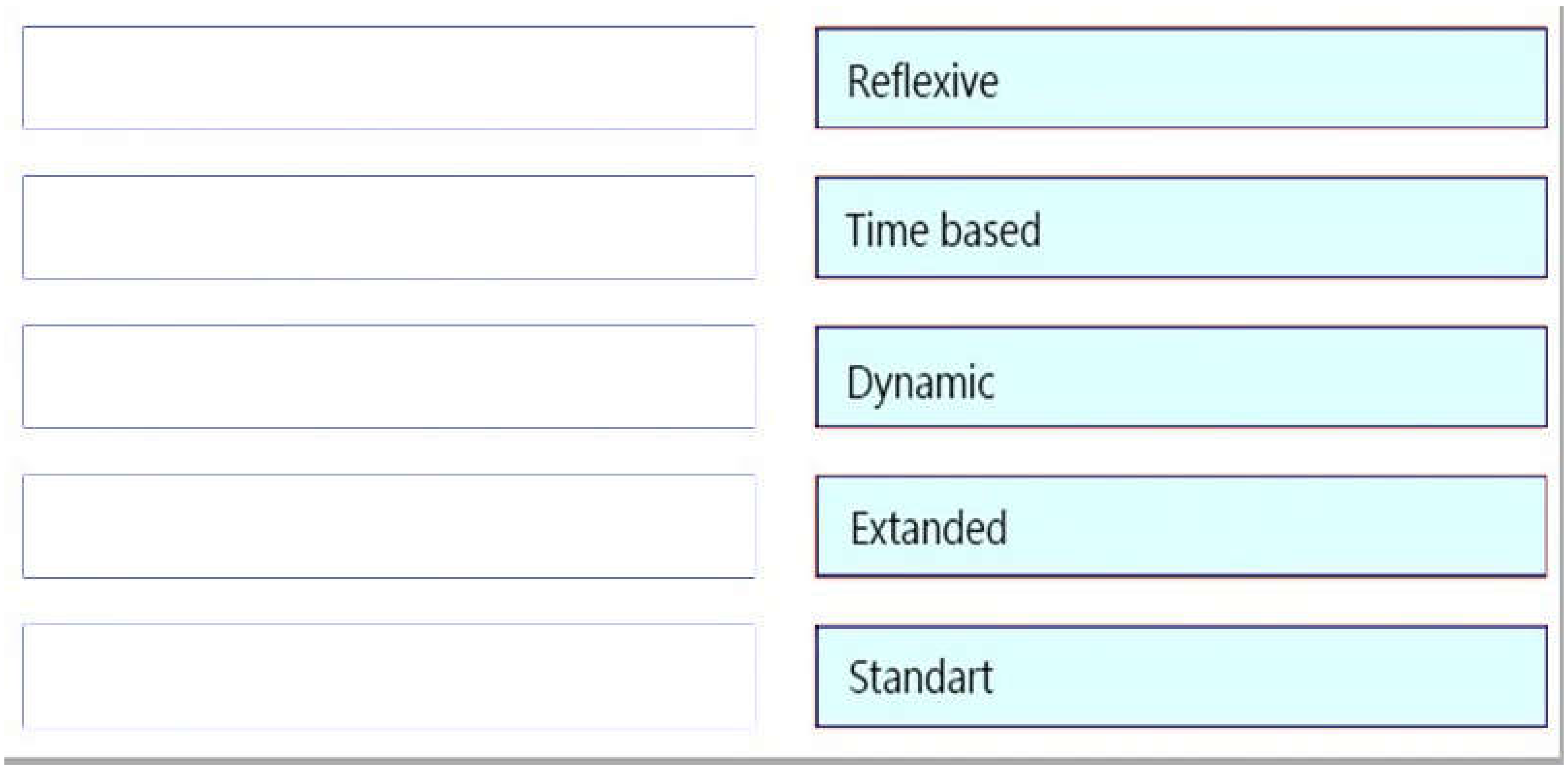
Time period

Dependent on telnet authentication

Place near source

1300-1999

Correct Answer:



Reflexive

Time based

Dynamic

Extanded

Standart

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

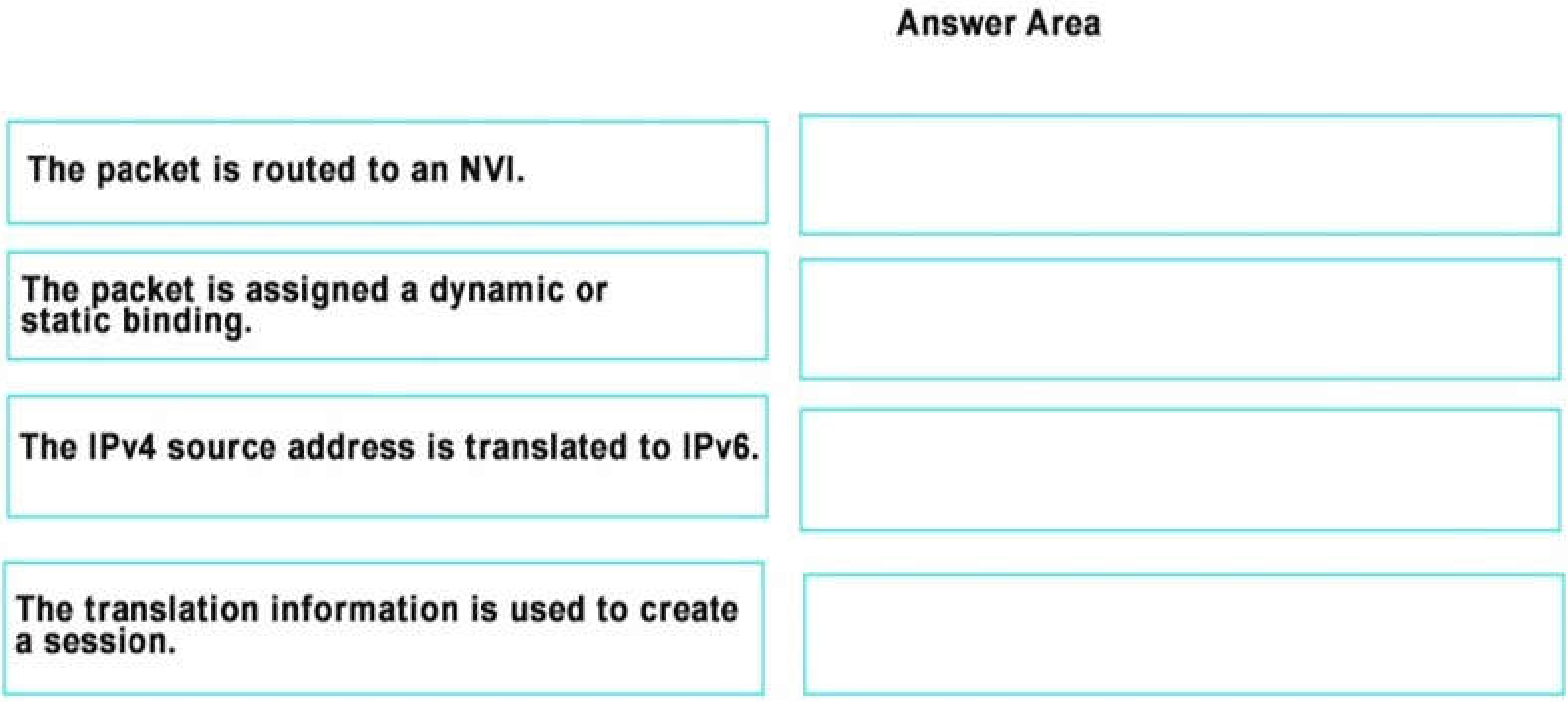
Reflexive ACLs allow IP packets to be filtered based on upper-layer session information. They are generally used to allow outbound traffic and to limit inbound traffic in response to sessions that originate inside the router. Reflexive ACLs can be defined only with extended named IP ACLs. They cannot be defined with numbered or standard named IP ACLs, or with other protocol ACLs. Reflexive ACLs can be used in conjunction with other standard and static extended ACLs. Outbound ACL will have the 'reflect' keyword. It is the ACL that matches the originating traffic. Inbound ACL will have the 'evaluate' keyword. It is the ACL that matches the returning traffic.

Lock and key, also known as dynamic ACLs, was introduced in Cisco IOS Software Release 11.1. This feature is dependent on Telnet, authentication (local or remote), and extended ACLs.
Lock and key configuration starts with the application of an extended ACL to block traffic through the router. Users that want to traverse the router are blocked by the extended ACL until they Telnet to the router and are authenticated. The Telnet connection then drops and a single-entry dynamic ACL is added to the extended ACL that exists. This permits traffic for a particular time period; idle and absolute timeouts are possible.

Reference:
https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html

QUESTION 492
DRAG DROP
Drag and drop the steps in the NAT process for IPv4-initiated packets from the left into the correct sequence on the right.

Select and Place:



Answer Area

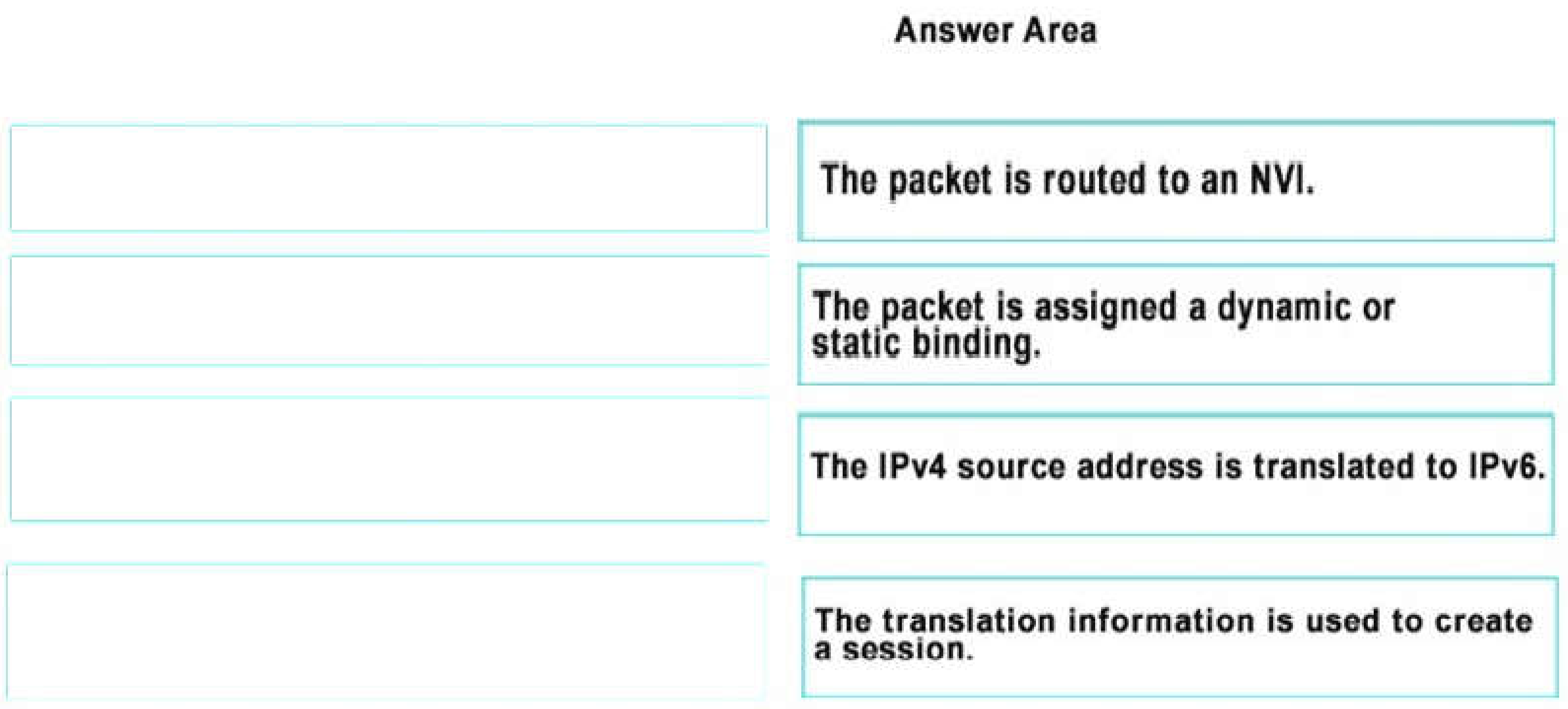
The packet is routed to an NVI.

The packet is assigned a dynamic or static binding.

The IPv4 source address is translated to IPv6.

The translation information is used to create a session.

Correct Answer:



Answer Area

The packet is routed to an NVI.

The packet is assigned a dynamic or static binding.

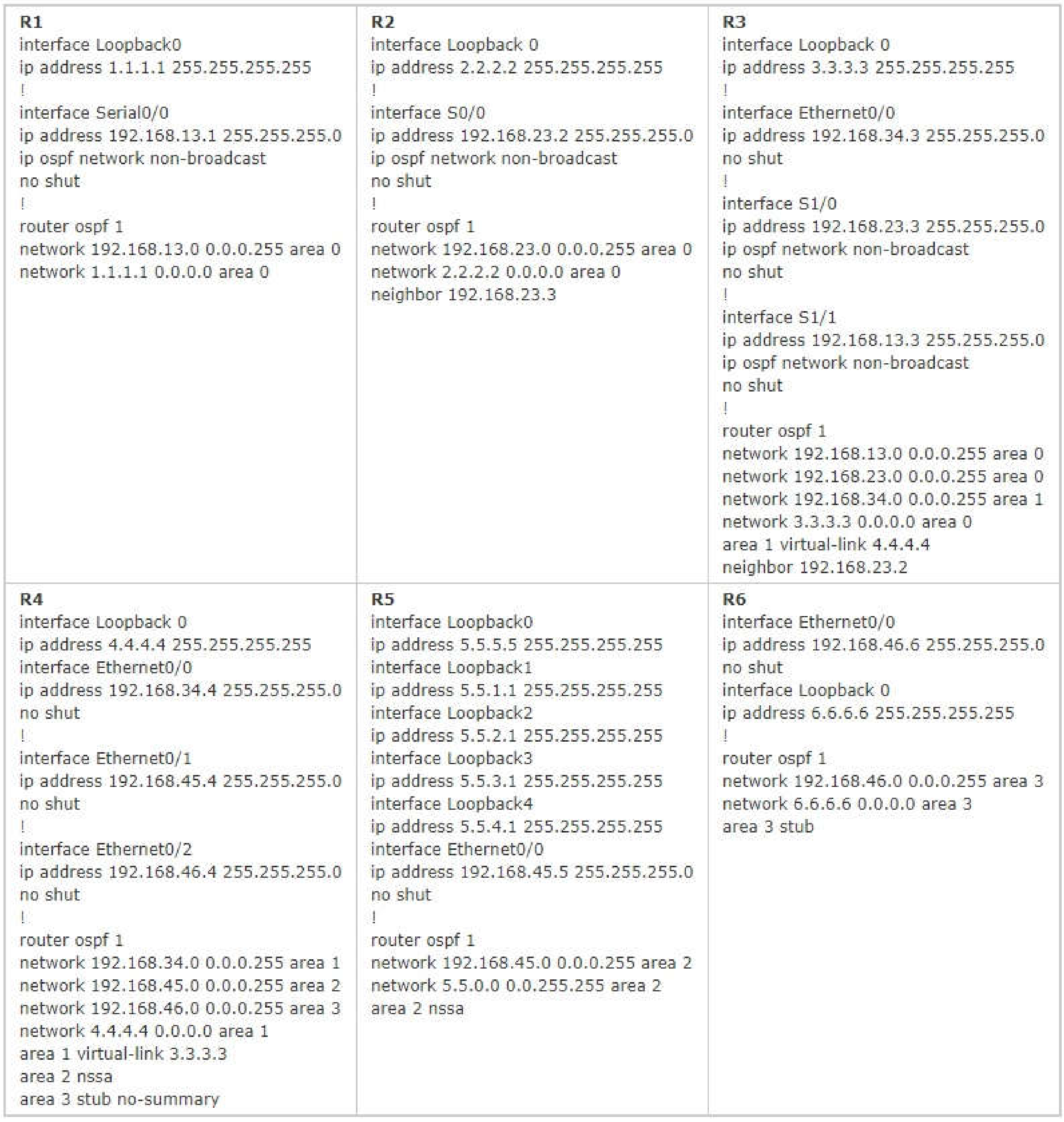
The IPv4 source address is translated to IPv6.

The translation information is used to create a session.

Section: Mix Questions
Explanation

Explanation/Reference:
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-2/nat-xe-2-book/iadnat-stateful-nat64.html

QUESTION 493
Case study.



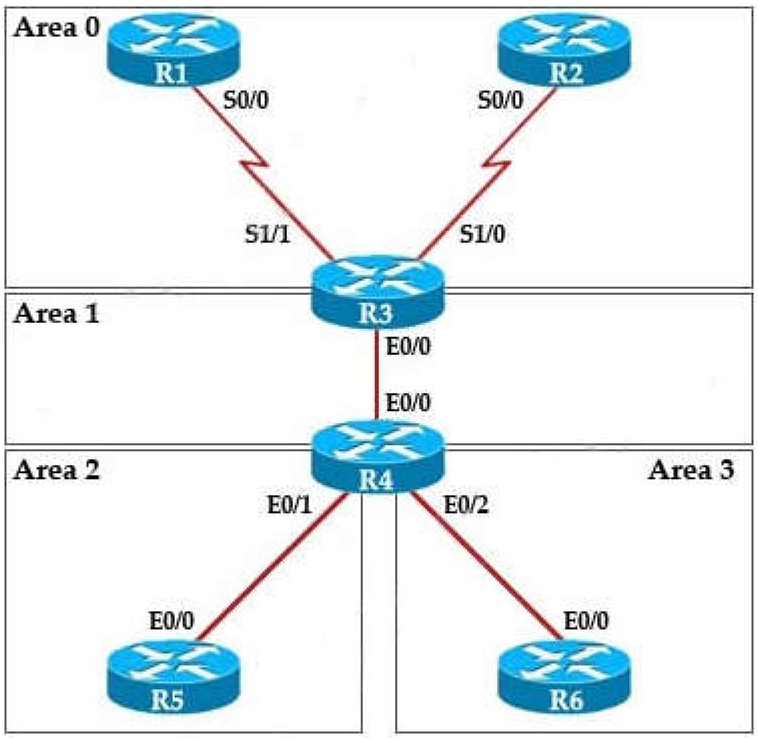
R1 interface Loopback0 ip address 1.1.1.1 255.255.255.255 ! interface Serial0/0 ip address 192.168.13.1 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.13.0 0.0.0.255 area 0 network 1.1.1.1 0.0.0.0 area 0	**R2** interface Loopback 0 ip address 2.2.2.2 255.255.255.255 ! interface S0/0 ip address 192.168.23.2 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.23.0 0.0.0.255 area 0 network 2.2.2.2 0.0.0.0 area 0 neighbor 192.168.23.3	**R3** interface Loopback 0 ip address 3.3.3.3 255.255.255.255 ! interface Ethernet0/0 ip address 192.168.34.3 255.255.255.0 no shut ! interface S1/0 ip address 192.168.23.3 255.255.255.0 ip ospf network non-broadcast no shut ! interface S1/1 ip address 192.168.13.3 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.13.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.34.0 0.0.0.255 area 1 network 3.3.3.3 0.0.0.0 area 0 area 1 virtual-link 4.4.4.4 neighbor 192.168.23.2
R4 interface Loopback 0 ip address 4.4.4.4 255.255.255.255 interface Ethernet0/0 ip address 192.168.34.4 255.255.255.0 no shut ! interface Ethernet0/1 ip address 192.168.45.4 255.255.255.0 no shut ! interface Ethernet0/2 ip address 192.168.46.4 255.255.255.0 no shut ! router ospf 1 network 192.168.34.0 0.0.0.255 area 1 network 192.168.45.0 0.0.0.255 area 2 network 192.168.46.0 0.0.0.255 area 3 network 4.4.4.4 0.0.0.0 area 1 area 1 virtual-link 3.3.3.3 area 2 nssa area 3 stub no-summary	**R5** interface Loopback0 ip address 5.5.5.5 255.255.255.255 interface Loopback1 ip address 5.5.1.1 255.255.255.255 interface Loopback2 ip address 5.5.2.1 255.255.255.255 interface Loopback3 ip address 5.5.3.1 255.255.255.255 interface Loopback4 ip address 5.5.4.1 255.255.255.255 interface Ethernet0/0 ip address 192.168.45.5 255.255.255.0 no shut ! router ospf 1 network 192.168.45.0 0.0.0.255 area 2 network 5.5.0.0 0.0.255.255 area 2 area 2 nssa	**R6** interface Ethernet0/0 ip address 192.168.46.6 255.255.255.0 no shut interface Loopback 0 ip address 6.6.6.6 255.255.255.255 ! router ospf 1 network 192.168.46.0 0.0.0.255 area 3 network 6.6.6.6 0.0.0.0 area 3 area 3 stub

Some notices from above configuration:
+The OSPF network type berween R2&R3 is non broadcast.

Q1: Show ip ospf database
Q2: Show ip ospf interface serial 1/0
Q3: Show ip ospf

Q4: Show ip route

You have been asked to evaluate an OSPF network and to answer questions a customer has about its operation. Note: You are not allowed to use the **show running-config** command.



Although in this sim we are not allowed to use “show running-config” command but we post the configuration here so that you can understand more about the topology.

R1

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
no shut
interface Serial0/0
ip address 192.168.13.1 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
```

R2

```
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
no shut
interface S0/0
ip address 192.168.23.2 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
neighbor 192.168.23.3
```

R3

```
interface Loopback 0
ip address 3.3.3.3 255.255.255.255
no shut
interface fa0/0
ip address 192.168.34.3 255.255.255.0
no shut
interface S0/1
ip address 192.168.23.3 255.255.255.0
ip ospf network non-broadcast
no shut
interface S0/0
ip address 192.168.13.3 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 1
network 3.3.3.3 0.0.0.0 area 0
area 1 virtual-link 4.4.4.4
neighbor 192.168.23.2
```

R4

```
interface Loopback 0
ip address 4.4.4.4 255.255.255.255
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
interface Fa0/1
ip address 192.168.45.4 255.255.255.0
no shut
interface Fa1/0
ip address 192.168.46.4 255.255.255.0
no shut
router ospf 1
```

```
network 192.168.34.0 0.0.0.255 area 1
network 192.168.45.0 0.0.0.255 area 2
network 192.168.46.0 0.0.0.255 area 3
network 4.4.4.4 0.0.0.0 area 1
area 1 virtual-link 3.3.3.3
area 2 nssa
area 3 stub no-summary
```

R5

```
interface Loopback0
ip address 5.5.5.5 255.255.255.255
interface Loopback1
ip address 5.5.1.1 255.255.255.255
interface Loopback2
ip address 5.5.2.1 255.255.255.255
interface Loopback3
ip address 5.5.3.1 255.255.255.255
interface Loopback4
ip address 5.5.4.1 255.255.255.255
no shut
interface Fa0/0
ip address 192.168.45.5 255.255.255.0
no shut
router ospf 1
network 192.168.45.0 0.0.0.255 area 2
network 5.5.0.0 0.0.255.255 area 2
area 2 nssa
```

R6

```
interface Fa0/0
ip address 192.168.46.6 255.255.255.0
no shut
interface Loopback 0
ip address 6.6.6.6 255.255.255.255
no shut
router ospf 1
network 192.168.46.0 0.0.0.255 area 3
network 6.6.6.6 0.0.0.0 area 3
area 3 stub
```

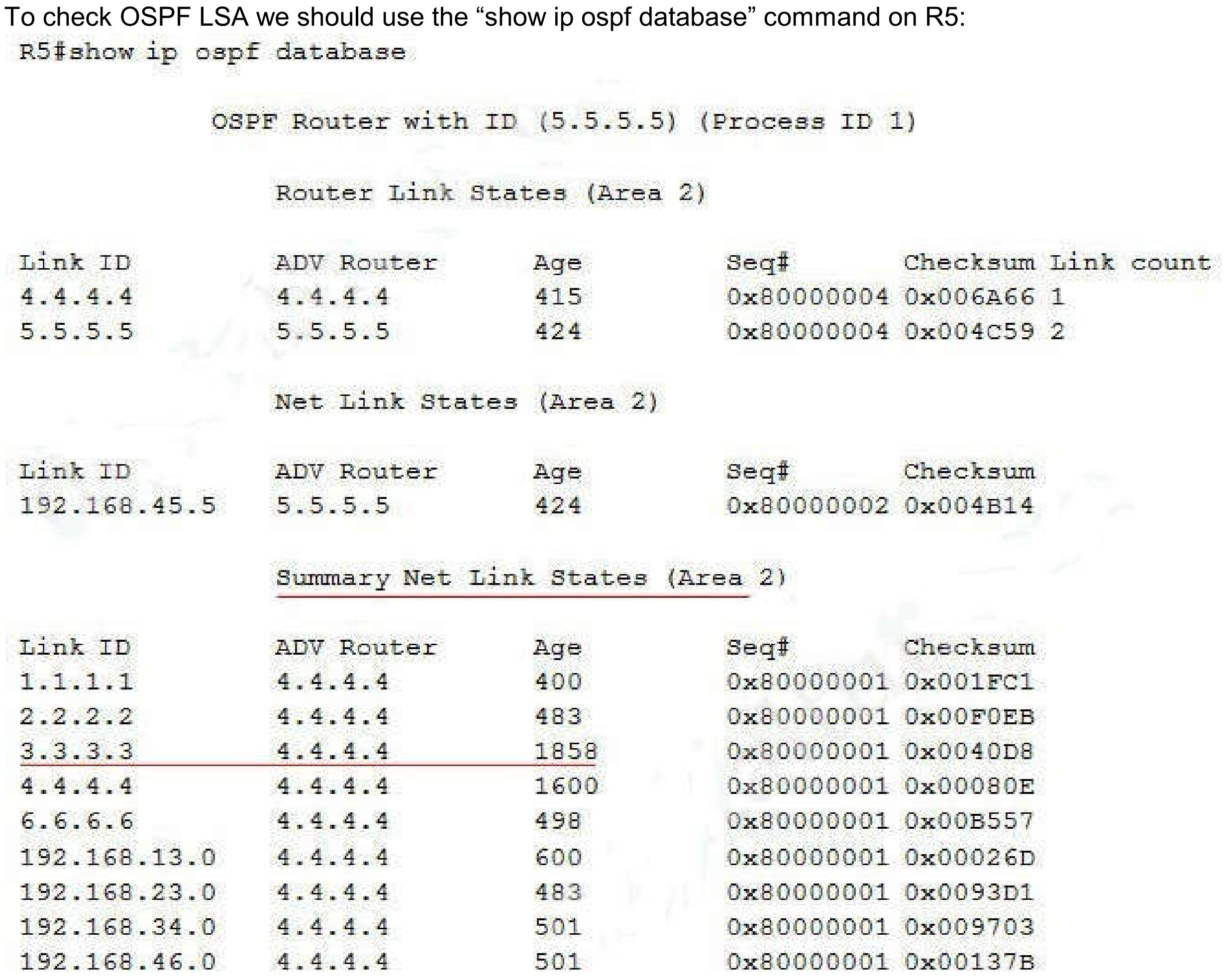
How old is the Type 4 LSA from Router 3 for area 1 on the router R5 based on the output you have examined?

A. 1858
B. 1601
C. 600
D. 1569

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation

To check OSPF LSA we should use the “show ip ospf database” command on R5:



```
R5#show ip ospf database

            OSPF Router with ID (5.5.5.5) (Process ID 1)

                Router Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum Link count
4.4.4.4         4.4.4.4         415         0x80000004 0x006A66 1
5.5.5.5         5.5.5.5         424         0x80000004 0x004C59 2

                Net Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
192.168.45.5    5.5.5.5         424         0x80000002 0x004B14

                Summary Net Link States (Area 2)

Link ID         ADV Router      Age         Seq#       Checksum
1.1.1.1         4.4.4.4         400         0x80000001 0x001FC1
2.2.2.2         4.4.4.4         483         0x80000001 0x00F0EB
3.3.3.3         4.4.4.4         1858        0x80000001 0x0040D8
4.4.4.4         4.4.4.4         1600        0x80000001 0x00080E
6.6.6.6         4.4.4.4         498         0x80000001 0x00B557
192.168.13.0    4.4.4.4         600         0x80000001 0x00026D
192.168.23.0    4.4.4.4         483         0x80000001 0x0093D1
192.168.34.0    4.4.4.4         501         0x80000001 0x009703
192.168.46.0    4.4.4.4         501         0x80000001 0x00137B
```

In this sim there is no LSA Type 4 because there is no ASBR so maybe this question wants to ask about LSA Type 3 (Summary Net Link States).

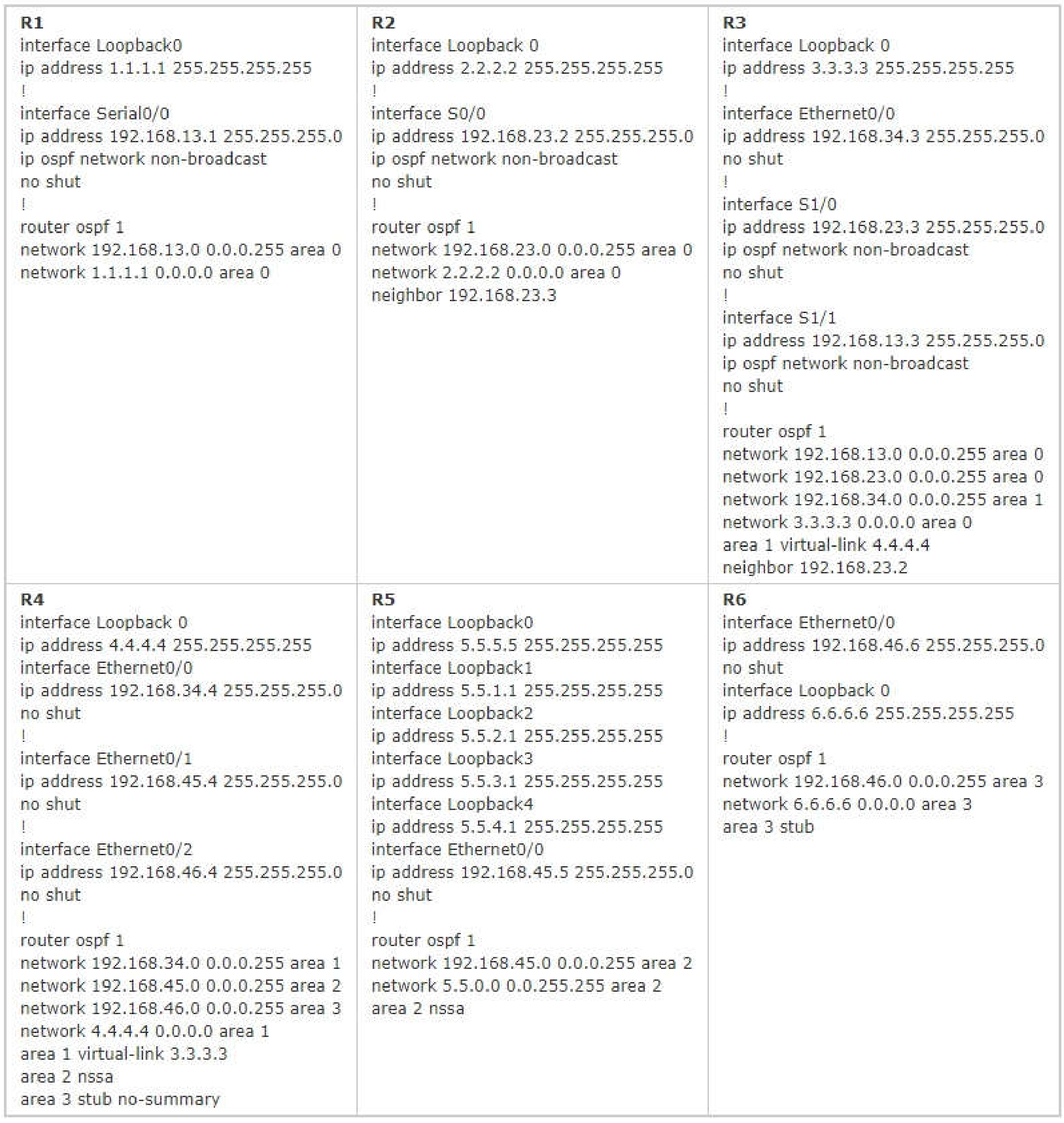
Note: LSA Type 4 is generated by ABR, not ASBR but without ASBR inside the network there are no LSA Type 4 generated. For more information about

OSPF LSA Types please read our OSPF LSA Types Lab tutorial.

R3 advertises LSA Type 1 to R4 then R4 converts it into Type 3 and sends to R5 (because R4 is the ABR) so we see the “Link ID” 3.3.3.3 of R3 is advertising by R4 (4.4.4.4). According to the “Age” column, this LSA was advertised 1858 seconds ago.

QUESTION 494

Case study.



```
R1
interface Loopback0
ip address 1.1.1.1 255.255.255.255
!
interface Serial0/0
ip address 192.168.13.1 255.255.255.0
ip ospf network non-broadcast
no shut
!
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
```

```
R2
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
!
interface S0/0
ip address 192.168.23.2 255.255.255.0
ip ospf network non-broadcast
no shut
!
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
neighbor 192.168.23.3
```

```
R3
interface Loopback 0
ip address 3.3.3.3 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.34.3 255.255.255.0
no shut
!
interface S1/0
ip address 192.168.23.3 255.255.255.0
ip ospf network non-broadcast
no shut
!
interface S1/1
ip address 192.168.13.3 255.255.255.0
ip ospf network non-broadcast
no shut
!
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 1
network 3.3.3.3 0.0.0.0 area 0
area 1 virtual-link 4.4.4.4
neighbor 192.168.23.2
```

```
R4
interface Loopback 0
ip address 4.4.4.4 255.255.255.255
interface Ethernet0/0
ip address 192.168.34.4 255.255.255.0
no shut
!
interface Ethernet0/1
ip address 192.168.45.4 255.255.255.0
no shut
!
interface Ethernet0/2
ip address 192.168.46.4 255.255.255.0
no shut
!
router ospf 1
network 192.168.34.0 0.0.0.255 area 1
network 192.168.45.0 0.0.0.255 area 2
network 192.168.46.0 0.0.0.255 area 3
network 4.4.4.4 0.0.0.0 area 1
area 1 virtual-link 3.3.3.3
area 2 nssa
area 3 stub no-summary
```

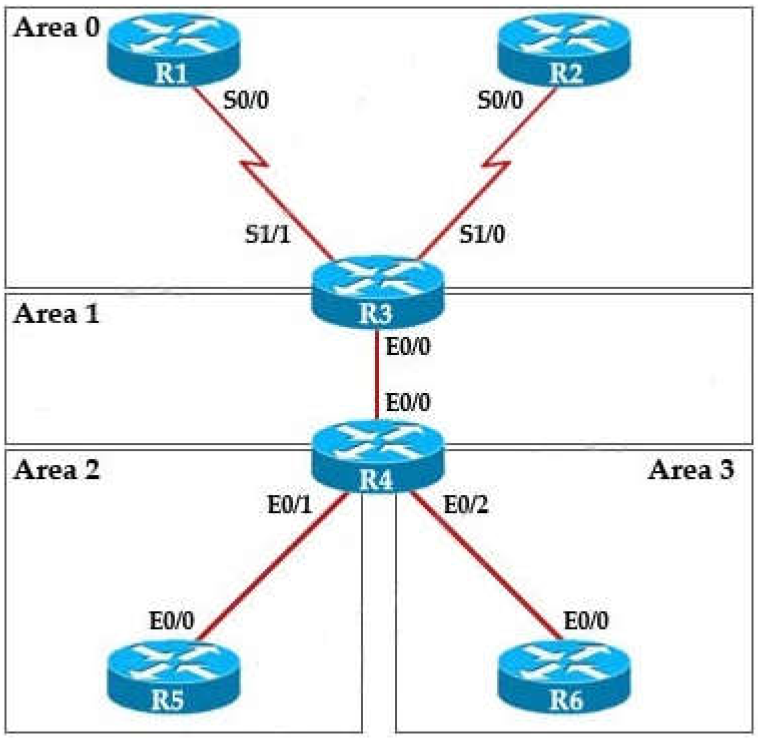
```
R5
interface Loopback0
ip address 5.5.5.5 255.255.255.255
interface Loopback1
ip address 5.5.1.1 255.255.255.255
interface Loopback2
ip address 5.5.2.1 255.255.255.255
interface Loopback3
ip address 5.5.3.1 255.255.255.255
interface Loopback4
ip address 5.5.4.1 255.255.255.255
interface Ethernet0/0
ip address 192.168.45.5 255.255.255.0
no shut
!
router ospf 1
network 192.168.45.0 0.0.0.255 area 2
network 5.5.0.0 0.0.255.255 area 2
area 2 nssa
```

```
R6
interface Ethernet0/0
ip address 192.168.46.6 255.255.255.0
no shut
interface Loopback 0
ip address 6.6.6.6 255.255.255.255
!
router ospf 1
network 192.168.46.0 0.0.0.255 area 3
network 6.6.6.6 0.0.0.0 area 3
area 3 stub
```

Some notices from above configuration:
+The OSPF network type between R2&R3 is non broadcast.

Q1: Show ip ospf database
Q2: Show ip ospf interface serial 1/0
Q3: Show ip ospf
Q4: Show ip route

You have been asked to evaluate an OSPF network and to answer questions a customer has about its operation. Note: You are not allowed to use the **show running-config** command.



Although in this sim we are not allowed to use “show running-config” command but we post the configuration here so that you can understand more about the topology.

R1

interface Loopback0

```
ip address 1.1.1.1 255.255.255.255
no shut
interface Serial0/0
ip address 192.168.13.1 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
```

R2

```
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
no shut
interface S0/0
ip address 192.168.23.2 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
neighbor 192.168.23.3
```

R3

```
interface Loopback 0
ip address 3.3.3.3 255.255.255.255
no shut
interface fa0/0
ip address 192.168.34.3 255.255.255.0
no shut
interface S0/1
ip address 192.168.23.3 255.255.255.0
ip ospf network non-broadcast
no shut
interface S0/0
ip address 192.168.13.3 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 1
network 3.3.3.3 0.0.0.0 area 0
area 1 virtual-link 4.4.4.4
neighbor 192.168.23.2
```

R4

```
interface Loopback 0
ip address 4.4.4.4 255.255.255.255
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
interface Fa0/1
ip address 192.168.45.4 255.255.255.0
no shut
interface Fa1/0
ip address 192.168.46.4 255.255.255.0
no shut
router ospf 1
network 192.168.34.0 0.0.0.255 area 1
network 192.168.45.0 0.0.0.255 area 2
network 192.168.46.0 0.0.0.255 area 3
network 4.4.4.4 0.0.0.0 area 1
area 1 virtual-link 3.3.3.3
area 2 nssa
area 3 stub no-summary
```

R5

```
interface Loopback0
ip address 5.5.5.5 255.255.255.255
interface Loopback1
ip address 5.5.1.1 255.255.255.255
interface Loopback2
ip address 5.5.2.1 255.255.255.255
interface Loopback3
ip address 5.5.3.1 255.255.255.255
interface Loopback4
ip address 5.5.4.1 255.255.255.255
no shut
interface Fa0/0
ip address 192.168.45.5 255.255.255.0
no shut
router ospf 1
network 192.168.45.0 0.0.0.255 area 2
network 5.5.0.0 0.0.255.255 area 2
area 2 nssa
```

R6

```
interface Fa0/0
ip address 192.168.46.6 255.255.255.0
no shut
interface Loopback 0
ip address 6.6.6.6 255.255.255.255
no shut
```

router ospf 1
network 192.168.46.0 0.0.0.255 area 3
network 6.6.6.6 0.0.0.0 area 3
area 3 stub

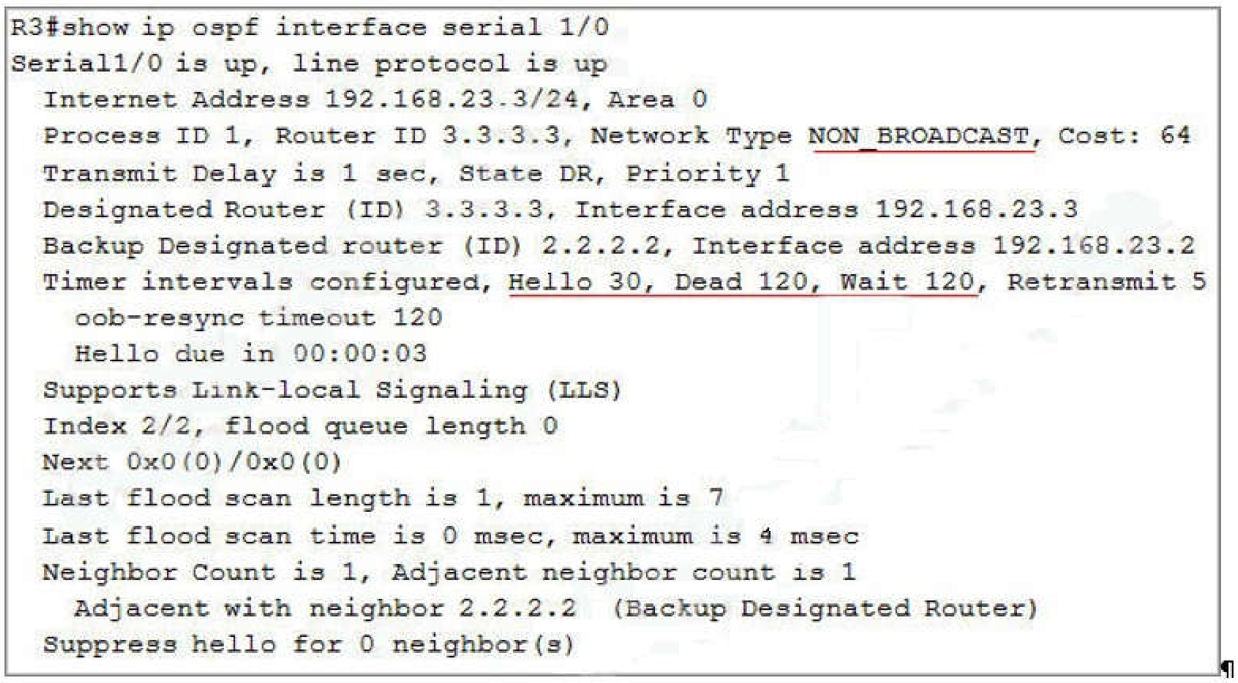
Which of the following statements is true about the serial links that terminate in R3?

A. The R1-R3 link needs the neighbor command for the adjacency to stay up
B. The R2-R3 link OSPF timer values are 30, 120, 120
C. The R1-R3 link OSPF timer values should be 10,40,40
D. R3 is responsible for flooding LSUs to all the routers on the network.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Check the Serial1/0 interface of R3 which is connected to R2 with the “show ip ospf interface serial 1/0” command:



```
R3#show ip ospf interface serial 1/0
Serial1/0 is up, line protocol is up
  Internet Address 192.168.23.3/24, Area 0
  Process ID 1, Router ID 3.3.3.3, Network Type NON_BROADCAST, Cost: 64
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 3.3.3.3, Interface address 192.168.23.3
  Backup Designated router (ID) 2.2.2.2, Interface address 192.168.23.2
  Timer intervals configured, Hello 30, Dead 120, Wait 120, Retransmit 5
    oob-resync timeout 120
    Hello due in 00:00:03
  Supports Link-local Signaling (LLS)
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 7
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 2.2.2.2  (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

There are two things we should notice from the output above:
+ The “network type” connection between R2-R3 is “NON_BROADCAST” (usually we have “BROADCAST”). OSPF neighbors are discovered using multicast Hello packets. In non broadcast environment, multicast (and broadcast) messages are not allowed so OSPF neighborship cannot be formed automatically. Therefore we have to establish OSPF neighborship manually by using “neighbor ” command under OSPF process (OSPF will send unicast Hello message to this address). For example on R2 we have to use these commands:

router ospf 1
neighbor 192.168.23.3

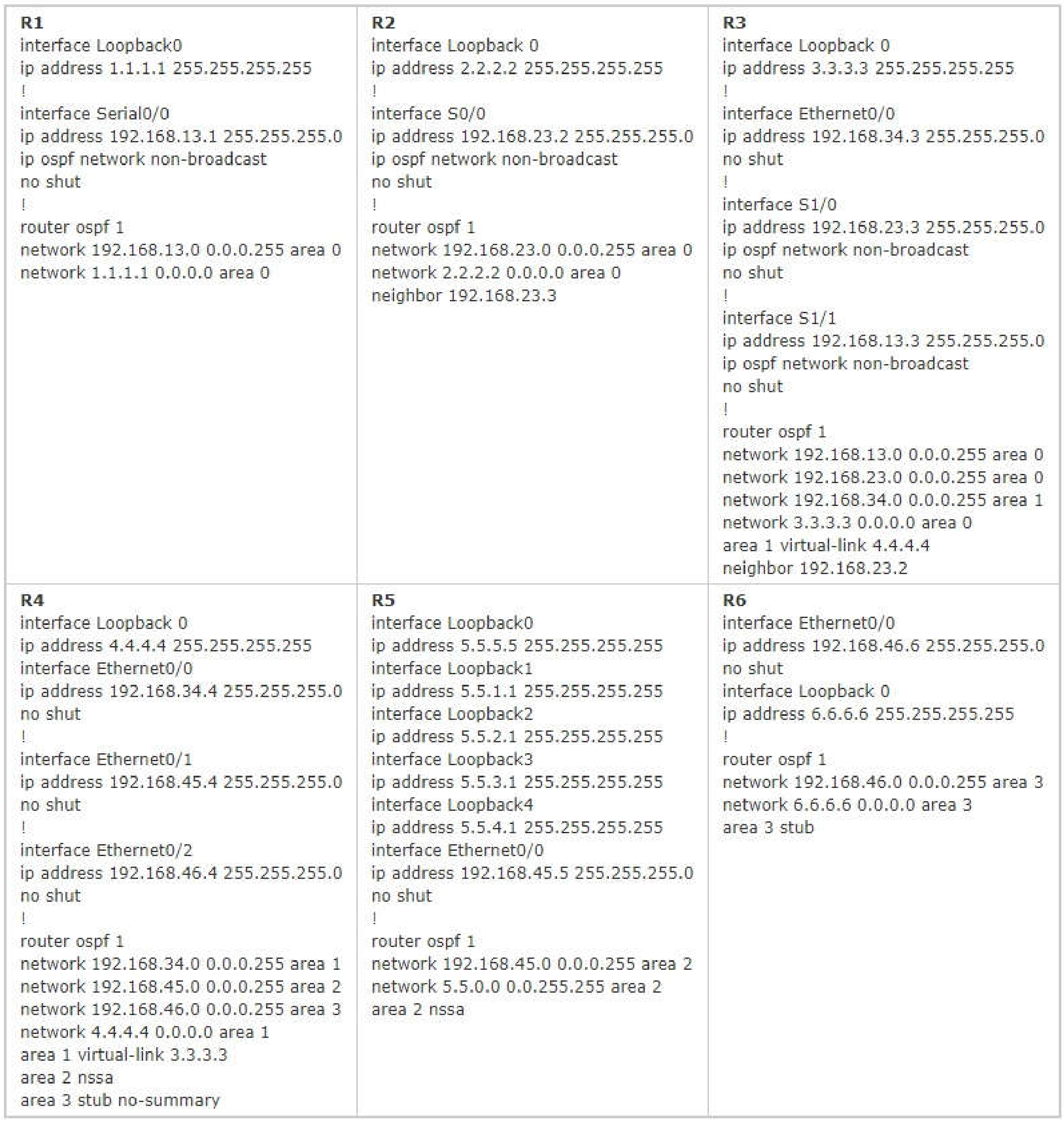
And on R3:

router ospf 1
neighbor 192.168.23.2

+ For non broadcast environment the default Hello timer is 30 seconds; Dead timer (time to wait before declaring a neighbor dead) is 120 seconds and Wait timer (causes the interface to exit out of the wait period and select a DR on a broadcast network. This timer is always equal to the dead timer interval) is 120 seconds. In the output we also see the default timers for non broadcast network.

QUESTION 495
FILL BLANK

Case study.

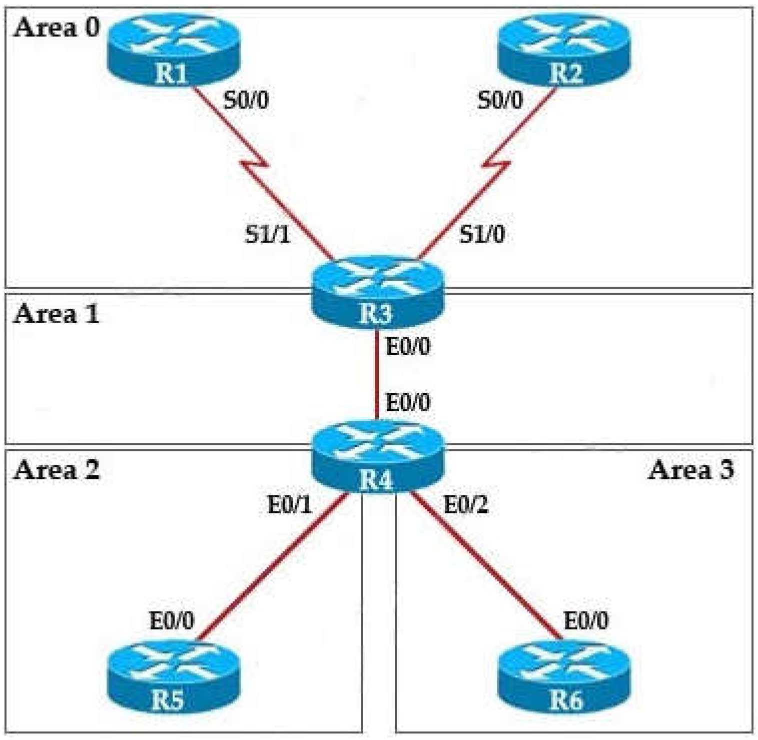


R1 interface Loopback0 ip address 1.1.1.1 255.255.255.255 ! interface Serial0/0 ip address 192.168.13.1 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.13.0 0.0.0.255 area 0 network 1.1.1.1 0.0.0.0 area 0	R2 interface Loopback 0 ip address 2.2.2.2 255.255.255.255 ! interface S0/0 ip address 192.168.23.2 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.23.0 0.0.0.255 area 0 network 2.2.2.2 0.0.0.0 area 0 neighbor 192.168.23.3	R3 interface Loopback 0 ip address 3.3.3.3 255.255.255.255 ! interface Ethernet0/0 ip address 192.168.34.3 255.255.255.0 no shut ! interface S1/0 ip address 192.168.23.3 255.255.255.0 ip ospf network non-broadcast no shut ! interface S1/1 ip address 192.168.13.3 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.13.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.34.0 0.0.0.255 area 1 network 3.3.3.3 0.0.0.0 area 0 area 1 virtual-link 4.4.4.4 neighbor 192.168.23.2
R4 interface Loopback 0 ip address 4.4.4.4 255.255.255.255 interface Ethernet0/0 ip address 192.168.34.4 255.255.255.0 no shut ! interface Ethernet0/1 ip address 192.168.45.4 255.255.255.0 no shut ! interface Ethernet0/2 ip address 192.168.46.4 255.255.255.0 no shut ! router ospf 1 network 192.168.34.0 0.0.0.255 area 1 network 192.168.45.0 0.0.0.255 area 2 network 192.168.46.0 0.0.0.255 area 3 network 4.4.4.4 0.0.0.0 area 1 area 1 virtual-link 3.3.3.3 area 2 nssa area 3 stub no-summary	R5 interface Loopback0 ip address 5.5.5.5 255.255.255.255 interface Loopback1 ip address 5.5.1.1 255.255.255.255 interface Loopback2 ip address 5.5.2.1 255.255.255.255 interface Loopback3 ip address 5.5.3.1 255.255.255.255 interface Loopback4 ip address 5.5.4.1 255.255.255.255 interface Ethernet0/0 ip address 192.168.45.5 255.255.255.0 no shut ! router ospf 1 network 192.168.45.0 0.0.0.255 area 2 network 5.5.0.0 0.0.255.255 area 2 area 2 nssa	R6 interface Ethernet0/0 ip address 192.168.46.6 255.255.255.0 no shut interface Loopback 0 ip address 6.6.6.6 255.255.255.255 ! router ospf 1 network 192.168.46.0 0.0.0.255 area 3 network 6.6.6.6 0.0.0.0 area 3 area 3 stub

Some notices from above configuration:
+The OSPF network type berween R2&R3 is non broadcast.

Q1: Show ip ospf database
Q2: Show ip ospf interface serial 1/0
Q3: Show ip ospf
Q4: Show ip route

You have been asked to evaluate an OSPF network and to answer questions a customer has about its operation. Note: You are not allowed to use the **show running-config** command.



Although in this sim we are not allowed to use "show running-config" command but we post the configuration here so that you can understand more about the topology.

```
R1
interface Loopback0
ip address 1.1.1.1 255.255.255.255
no shut
interface Serial0/0
ip address 192.168.13.1 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
```

R2

```
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
no shut
interface S0/0
ip address 192.168.23.2 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
neighbor 192.168.23.3
```

R3

```
interface Loopback 0
ip address 3.3.3.3 255.255.255.255
no shut
interface fa0/0
ip address 192.168.34.3 255.255.255.0
no shut
interface S0/1
ip address 192.168.23.3 255.255.255.0
ip ospf network non-broadcast
no shut
interface S0/0
ip address 192.168.13.3 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 1
network 3.3.3.3 0.0.0.0 area 0
area 1 virtual-link 4.4.4.4
neighbor 192.168.23.2
```

R4

```
interface Loopback 0
ip address 4.4.4.4 255.255.255.255
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
interface Fa0/1
ip address 192.168.45.4 255.255.255.0
no shut
interface Fa1/0
ip address 192.168.46.4 255.255.255.0
no shut
router ospf 1
network 192.168.34.0 0.0.0.255 area 1
network 192.168.45.0 0.0.0.255 area 2
network 192.168.46.0 0.0.0.255 area 3
network 4.4.4.4 0.0.0.0 area 1
area 1 virtual-link 3.3.3.3
area 2 nssa
area 3 stub no-summary
```

R5

```
interface Loopback0
ip address 5.5.5.5 255.255.255.255
interface Loopback1
ip address 5.5.1.1 255.255.255.255
interface Loopback2
ip address 5.5.2.1 255.255.255.255
interface Loopback3
ip address 5.5.3.1 255.255.255.255
interface Loopback4
ip address 5.5.4.1 255.255.255.255
no shut
interface Fa0/0
ip address 192.168.45.5 255.255.255.0
no shut
router ospf 1
network 192.168.45.0 0.0.0.255 area 2
network 5.5.0.0 0.0.255.255 area 2
area 2 nssa
```

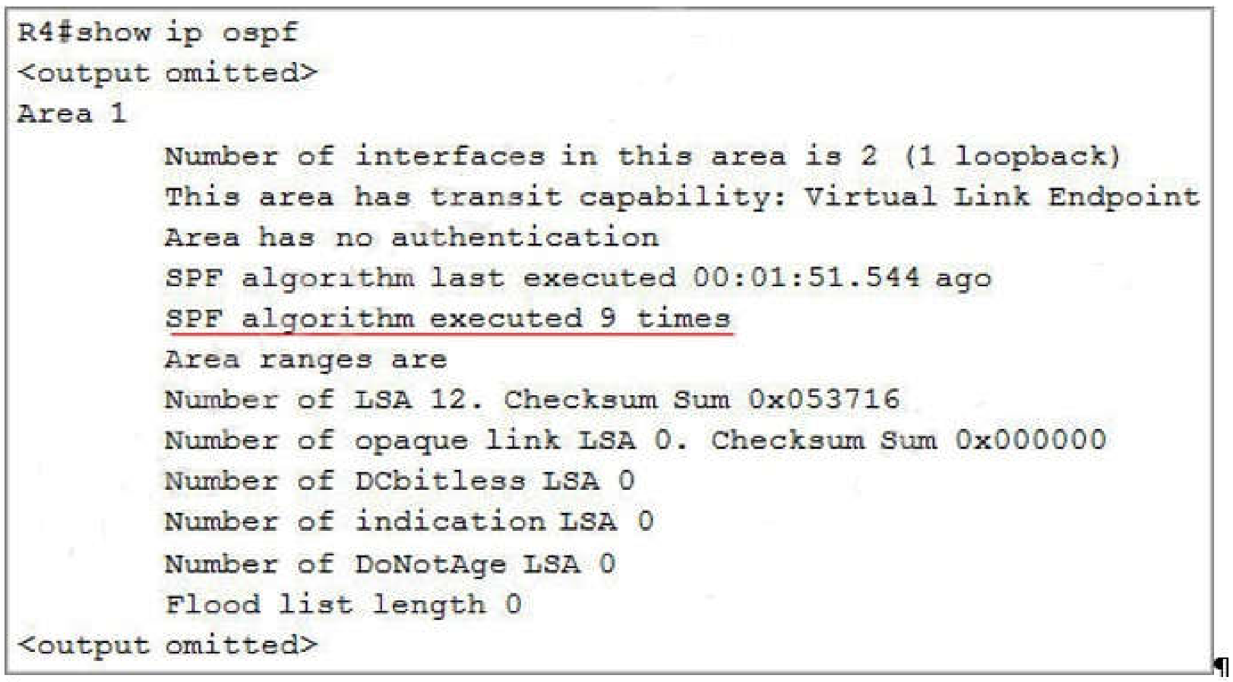
R6

```
interface Fa0/0
ip address 192.168.46.6 255.255.255.0
no shut
interface Loopback 0
ip address 6.6.6.6 255.255.255.255
no shut
router ospf 1
network 192.168.46.0 0.0.0.255 area 3
network 6.6.6.6 0.0.0.0 area 3
area 3 stub
```

How many times was SPF algorithm executed on R4 for Area 1?

Correct Answer: 9
Section: Mix Questions
Explanation

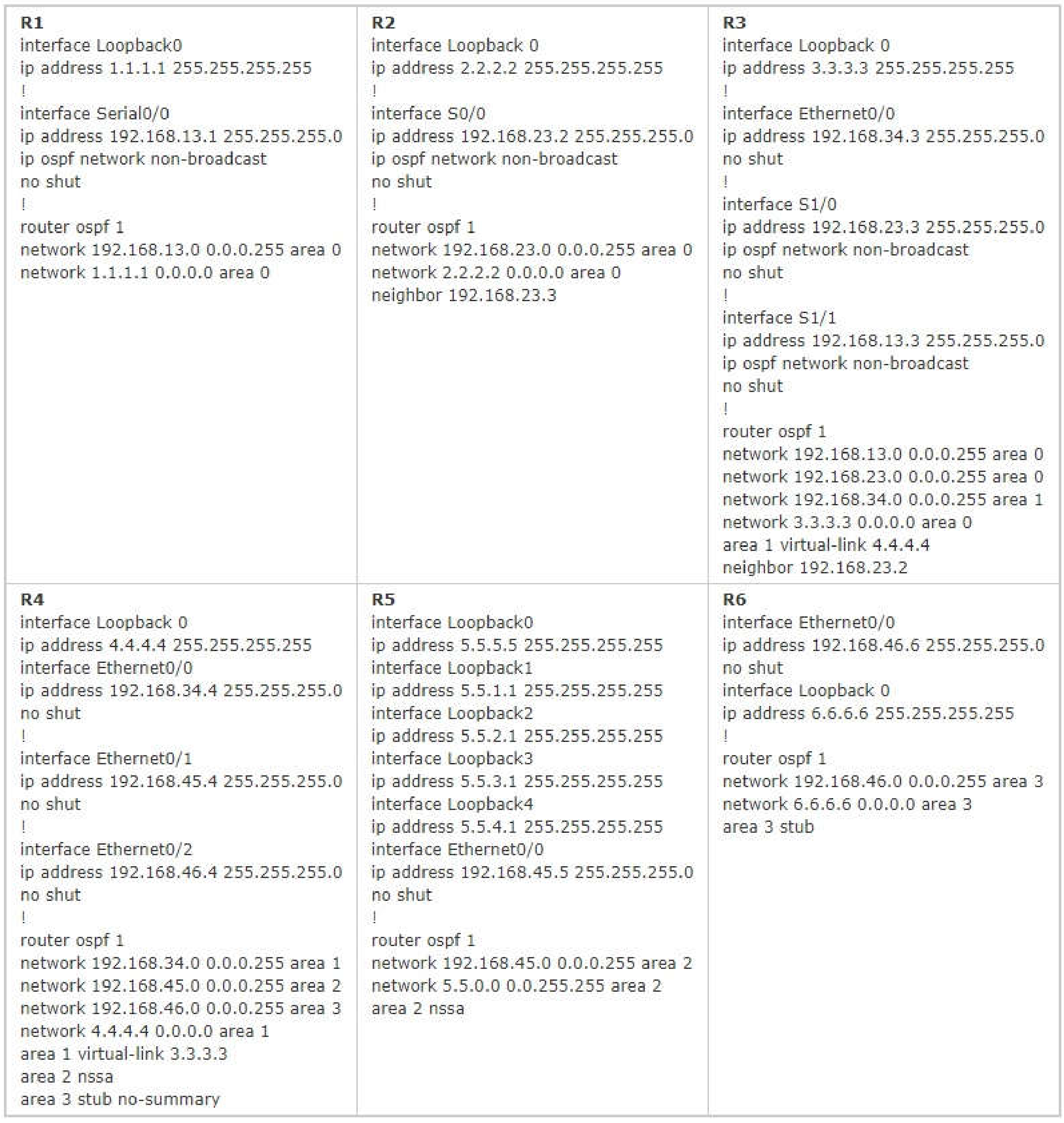
Explanation/Reference:
Explanation:
We can check the number of executed SPF algorithm via the “show ip ospf” command on R4:



```
R4#show ip ospf
<output omitted>
Area 1
        Number of interfaces in this area is 2 (1 loopback)
        This area has transit capability: Virtual Link Endpoint
        Area has no authentication
        SPF algorithm last executed 00:01:51.544 ago
        SPF algorithm executed 9 times
        Area ranges are
        Number of LSA 12. Checksum Sum 0x053716
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
<output omitted>
```

In the output above we can see SPF has been executed 9 times.

QUESTION 496
Case study.

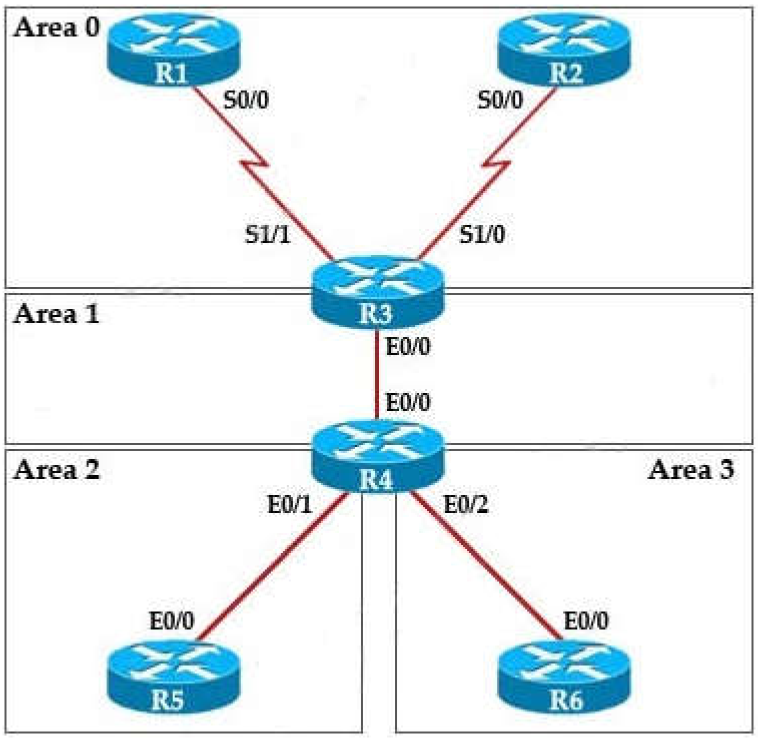


R1 interface Loopback0 ip address 1.1.1.1 255.255.255.255 ! interface Serial0/0 ip address 192.168.13.1 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.13.0 0.0.0.255 area 0 network 1.1.1.1 0.0.0.0 area 0	**R2** interface Loopback 0 ip address 2.2.2.2 255.255.255.255 ! interface S0/0 ip address 192.168.23.2 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.23.0 0.0.0.255 area 0 network 2.2.2.2 0.0.0.0 area 0 neighbor 192.168.23.3	**R3** interface Loopback 0 ip address 3.3.3.3 255.255.255.255 ! interface Ethernet0/0 ip address 192.168.34.3 255.255.255.0 no shut ! interface S1/0 ip address 192.168.23.3 255.255.255.0 ip ospf network non-broadcast no shut ! interface S1/1 ip address 192.168.13.3 255.255.255.0 ip ospf network non-broadcast no shut ! router ospf 1 network 192.168.13.0 0.0.0.255 area 0 network 192.168.23.0 0.0.0.255 area 0 network 192.168.34.0 0.0.0.255 area 1 network 3.3.3.3 0.0.0.0 area 0 area 1 virtual-link 4.4.4.4 neighbor 192.168.23.2
R4 interface Loopback 0 ip address 4.4.4.4 255.255.255.255 interface Ethernet0/0 ip address 192.168.34.4 255.255.255.0 no shut ! interface Ethernet0/1 ip address 192.168.45.4 255.255.255.0 no shut ! interface Ethernet0/2 ip address 192.168.46.4 255.255.255.0 no shut ! router ospf 1 network 192.168.34.0 0.0.0.255 area 1 network 192.168.45.0 0.0.0.255 area 2 network 192.168.46.0 0.0.0.255 area 3 network 4.4.4.4 0.0.0.0 area 1 area 1 virtual-link 3.3.3.3 area 2 nssa area 3 stub no-summary	**R5** interface Loopback0 ip address 5.5.5.5 255.255.255.255 interface Loopback1 ip address 5.5.1.1 255.255.255.255 interface Loopback2 ip address 5.5.2.1 255.255.255.255 interface Loopback3 ip address 5.5.3.1 255.255.255.255 interface Loopback4 ip address 5.5.4.1 255.255.255.255 interface Ethernet0/0 ip address 192.168.45.5 255.255.255.0 no shut ! router ospf 1 network 192.168.45.0 0.0.0.255 area 2 network 5.5.0.0 0.0.255.255 area 2 area 2 nssa	**R6** interface Ethernet0/0 ip address 192.168.46.6 255.255.255.0 no shut interface Loopback 0 ip address 6.6.6.6 255.255.255.255 ! router ospf 1 network 192.168.46.0 0.0.0.255 area 3 network 6.6.6.6 0.0.0.0 area 3 area 3 stub

Some notices from above configuration:
+The OSPF network type between R2&R3 is non broadcast.

Q1: Show ip ospf database
Q2: Show ip ospf interface serial 1/0
Q3: Show ip ospf
Q4: Show ip route

You have been asked to evaluate an OSPF network and to answer questions a customer has about its operation. Note: You are not allowed to use the **show running-config** command.



Although in this sim we are not allowed to use “show running-config” command but we post the configuration here so that you can understand more about the topology.

R1

```
interface Loopback0
ip address 1.1.1.1 255.255.255.255
no shut
interface Serial0/0
ip address 192.168.13.1 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 1.1.1.1 0.0.0.0 area 0
```

R2

```
interface Loopback 0
ip address 2.2.2.2 255.255.255.255
no shut
interface S0/0
ip address 192.168.23.2 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 2.2.2.2 0.0.0.0 area 0
neighbor 192.168.23.3
```

R3

```
interface Loopback 0
ip address 3.3.3.3 255.255.255.255
no shut
interface fa0/0
ip address 192.168.34.3 255.255.255.0
no shut
interface S0/1
ip address 192.168.23.3 255.255.255.0
ip ospf network non-broadcast
no shut
interface S0/0
ip address 192.168.13.3 255.255.255.0
ip ospf network non-broadcast
no shut
router ospf 1
network 192.168.13.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 1
network 3.3.3.3 0.0.0.0 area 0
area 1 virtual-link 4.4.4.4
neighbor 192.168.23.2
```

R4

```
interface Loopback 0
ip address 4.4.4.4 255.255.255.255
interface FastEthernet0/0
ip address 192.168.34.4 255.255.255.0
interface Fa0/1
ip address 192.168.45.4 255.255.255.0
no shut
interface Fa1/0
ip address 192.168.46.4 255.255.255.0
no shut
router ospf 1
network 192.168.34.0 0.0.0.255 area 1
network 192.168.45.0 0.0.0.255 area 2
network 192.168.46.0 0.0.0.255 area 3
network 4.4.4.4 0.0.0.0 area 1
area 1 virtual-link 3.3.3.3
```

area 2 nssa
area 3 stub no-summary

R5
interface Loopback0
ip address 5.5.5.5 255.255.255.255
interface Loopback1
ip address 5.5.1.1 255.255.255.255
interface Loopback2
ip address 5.5.2.1 255.255.255.255
interface Loopback3
ip address 5.5.3.1 255.255.255.255
interface Loopback4
ip address 5.5.4.1 255.255.255.255
no shut
interface Fa0/0
ip address 192.168.45.5 255.255.255.0
no shut
router ospf 1
network 192.168.45.0 0.0.0.255 area 2
network 5.5.0.0 0.0.255.255 area 2
area 2 nssa

R6
interface Fa0/0
ip address 192.168.46.6 255.255.255.0
no shut
interface Loopback 0
ip address 6.6.6.6 255.255.255.255
no shut
router ospf 1
network 192.168.46.0 0.0.0.255 area 3
network 6.6.6.6 0.0.0.0 area 3
area 3 stub

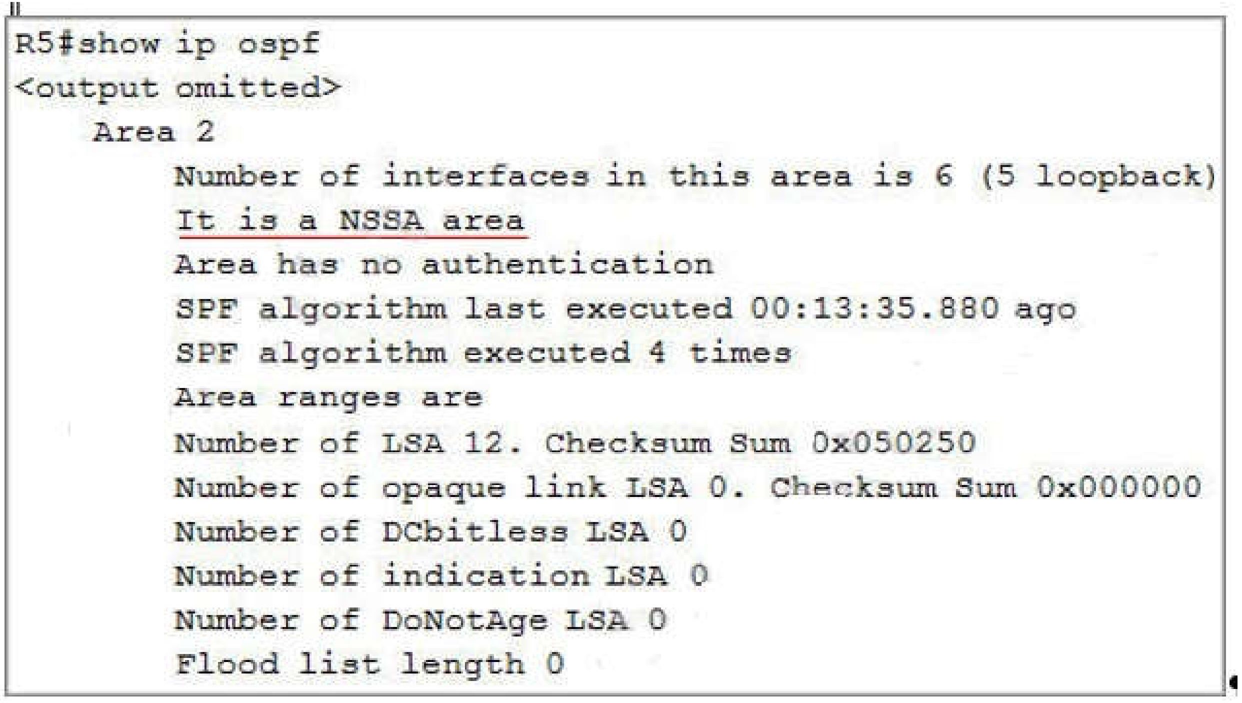
Areas of Router 5 and 6 are not normal areas, inspect their routing tables and determine which statement is true?

A. R5′s Loopback and R6′s Loopback are both present in R5′s Routing table
B. R5′s Loopback and R6′s Loopback are both present in R6′s Routing table
C. Only R5′s loopback is present in R5′s Routing table
D. Only R6′s loopback is present in R5′s Routing table
E. Only R5′s loopback is present in R6′s Routing table

Correct Answer: A
Section: Mix Questions
Explanation

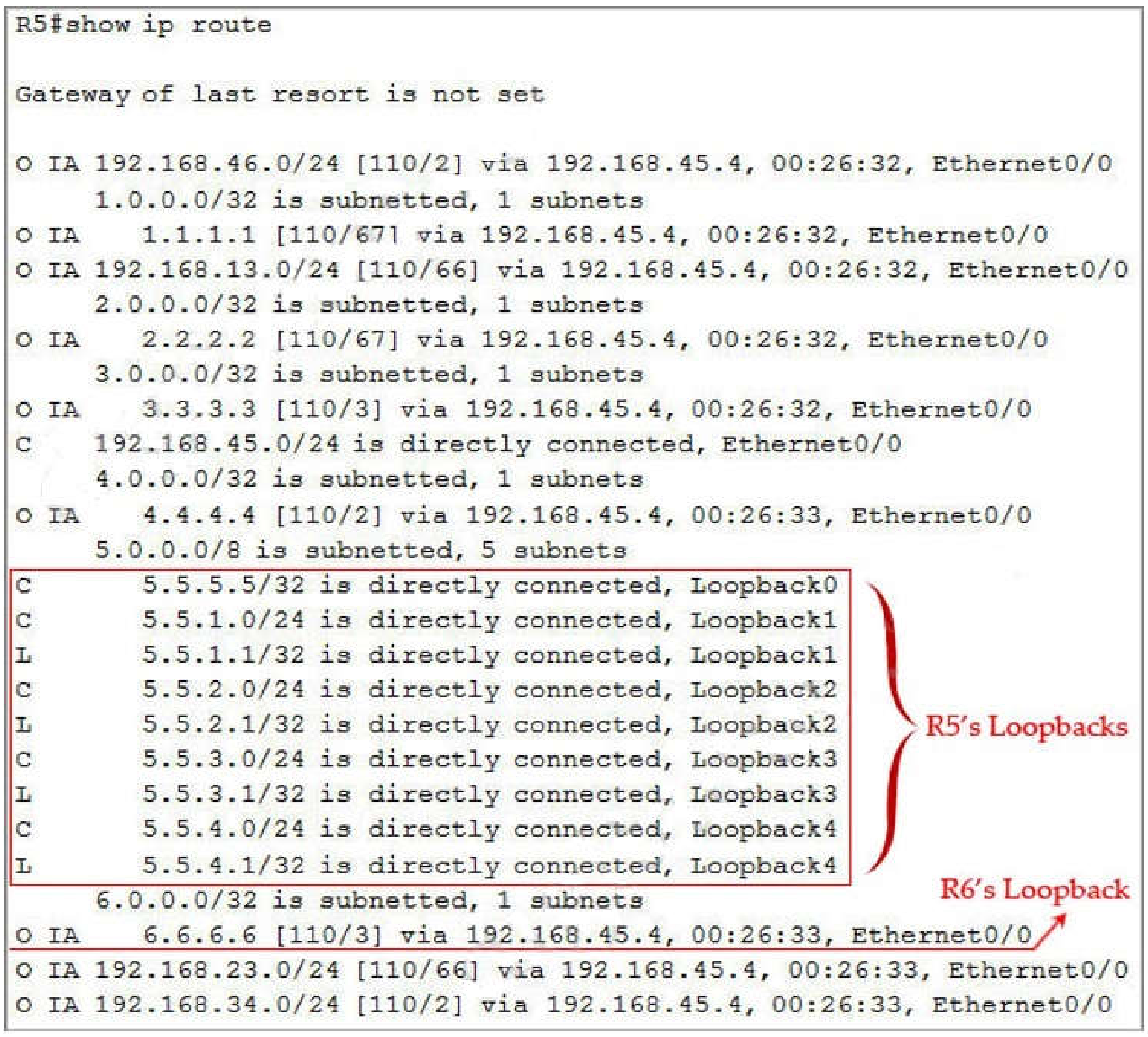
Explanation/Reference:
Explanation:

Area 2 (of R5) is a Not-so-Stubby area (NSSA). You can check it by the “show ip ospf” command on R4 or R5 (in Area 2 section). For example, below is the output of “show ip ospf” command on R5:



```
R5#show ip ospf
<output omitted>
    Area 2
        Number of interfaces in this area is 6 (5 loopback)
        It is a NSSA area
        Area has no authentication
        SPF algorithm last executed 00:13:35.880 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 12. Checksum Sum 0x050250
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

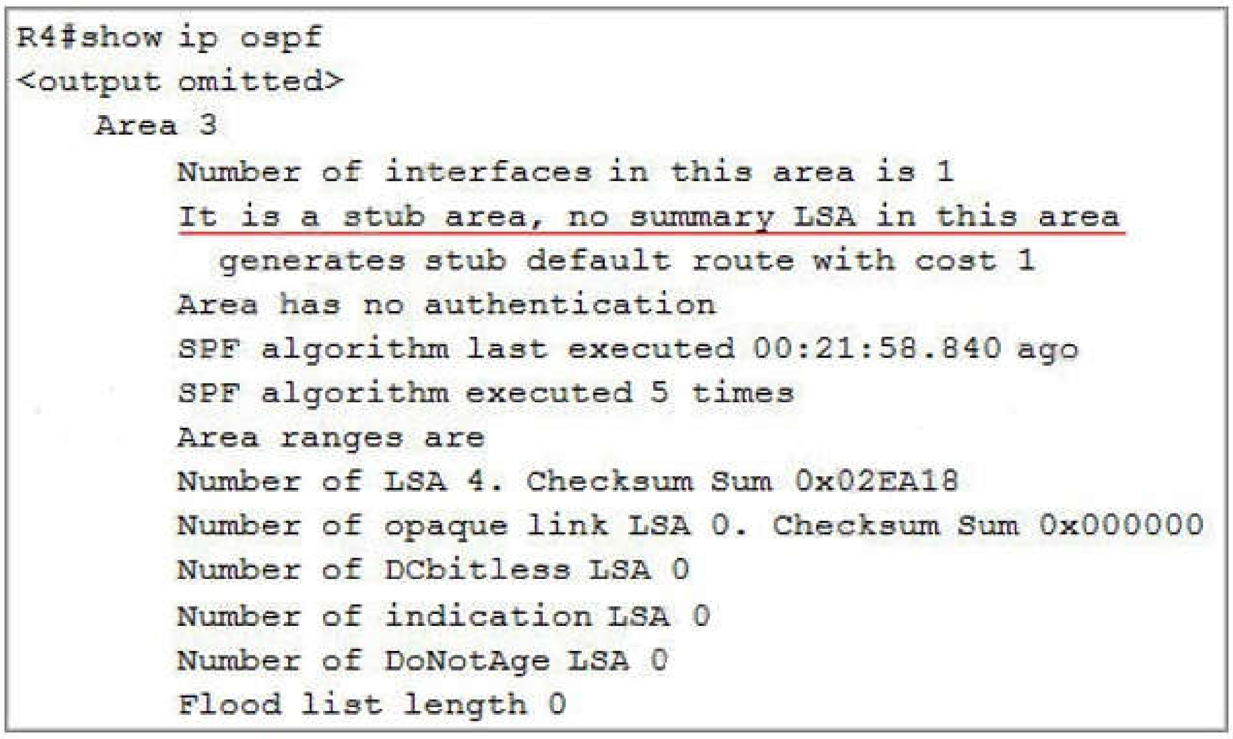
In general, NSSA is same as normal area except that it can generate LSA Type 7 (redistribute from another domain) so we can see both Loopback interfaces of R5 & R6 in the routing table of R5.



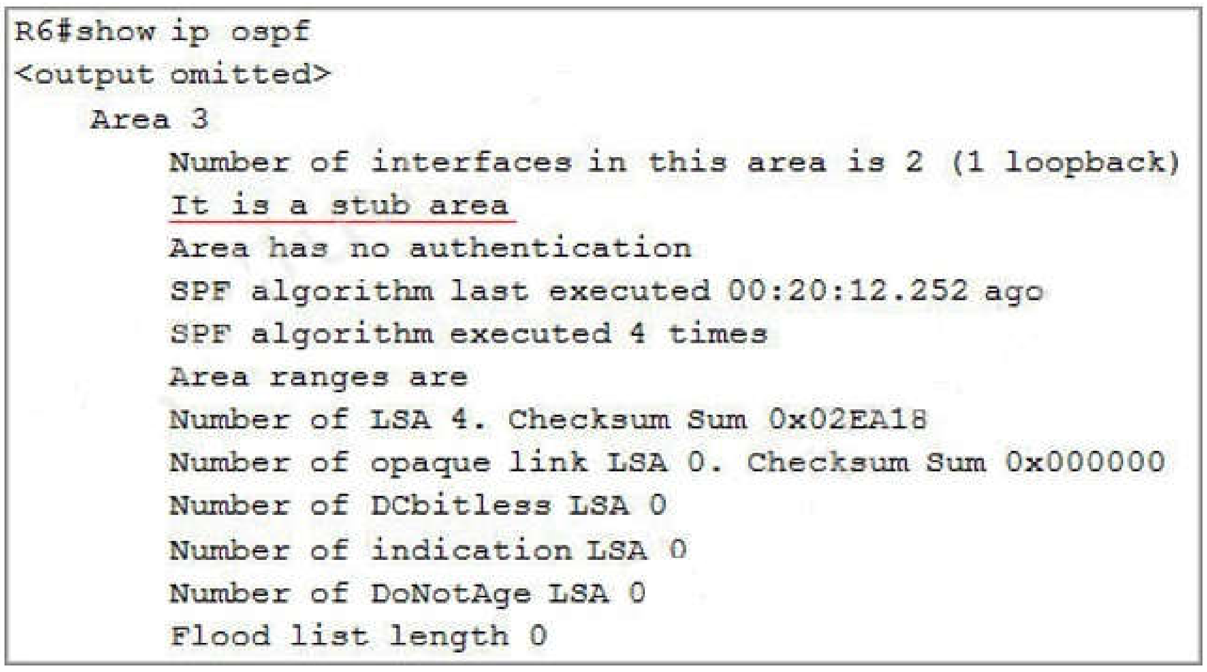
```
R5#show ip route

Gateway of last resort is not set

O IA 192.168.46.0/24 [110/2] via 192.168.45.4, 00:26:32, Ethernet0/0
     1.0.0.0/32 is subnetted, 1 subnets
O IA    1.1.1.1 [110/671 via 192.168.45.4, 00:26:32, Ethernet0/0
O IA 192.168.13.0/24 [110/66] via 192.168.45.4, 00:26:32, Ethernet0/0
     2.0.0.0/32 is subnetted, 1 subnets
O IA    2.2.2.2 [110/67] via 192.168.45.4, 00:26:32, Ethernet0/0
     3.0.0.0/32 is subnetted, 1 subnets
O IA    3.3.3.3 [110/3] via 192.168.45.4, 00:26:32, Ethernet0/0
C    192.168.45.0/24 is directly connected, Ethernet0/0
     4.0.0.0/32 is subnetted, 1 subnets
O IA    4.4.4.4 [110/2] via 192.168.45.4, 00:26:33, Ethernet0/0
     5.0.0.0/8 is subnetted, 5 subnets
C       5.5.5.5/32 is directly connected, Loopback0
C       5.5.1.0/24 is directly connected, Loopback1
L       5.5.1.1/32 is directly connected, Loopback1
C       5.5.2.0/24 is directly connected, Loopback2
L       5.5.2.1/32 is directly connected, Loopback2
C       5.5.3.0/24 is directly connected, Loopback3
L       5.5.3.1/32 is directly connected, Loopback3
C       5.5.4.0/24 is directly connected, Loopback4
L       5.5.4.1/32 is directly connected, Loopback4
     6.0.0.0/32 is subnetted, 1 subnets
O IA    6.6.6.6 [110/3] via 192.168.45.4, 00:26:33, Ethernet0/0
O IA 192.168.23.0/24 [110/66] via 192.168.45.4, 00:26:33, Ethernet0/0
O IA 192.168.34.0/24 [110/2] via 192.168.45.4, 00:26:33, Ethernet0/0
```

Note: NSSA does not receive a default route by default so you will not see a default route on R5.

Area 3 (of R6) is a Totally-Stubby area so R6 only has one default route to outside world. You can check with the "show ip ospf" command on R4 and R6 (area 3 section):



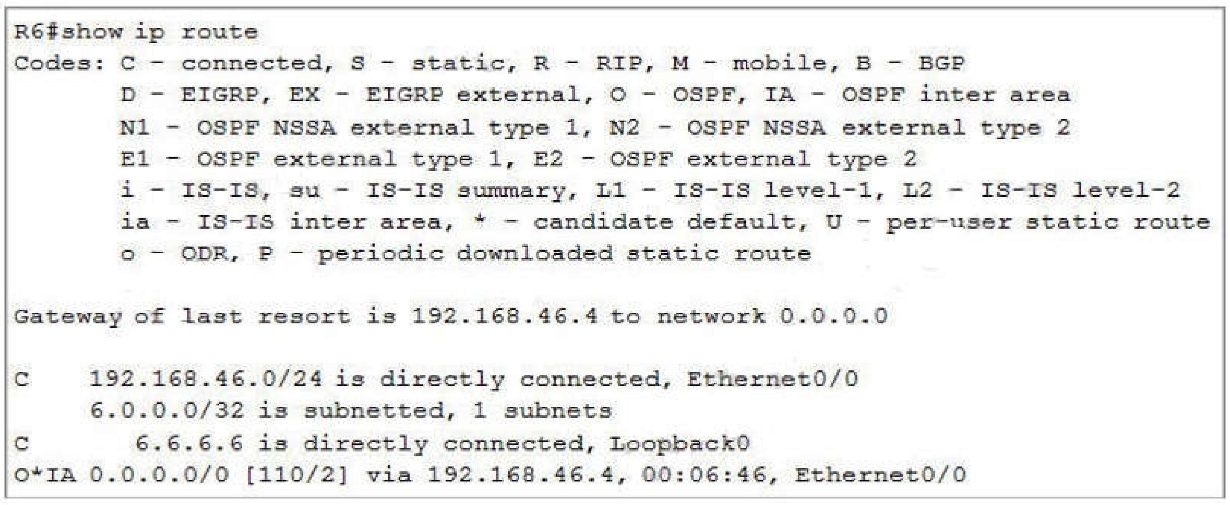
```
R4#show ip ospf
<output omitted>
    Area 3
        Number of interfaces in this area is 1
        It is a stub area, no summary LSA in this area
          generates stub default route with cost 1
        Area has no authentication
        SPF algorithm last executed 00:21:58.840 ago
        SPF algorithm executed 5 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x02EA18
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```



```
R6#show ip ospf
<output omitted>
    Area 3
        Number of interfaces in this area is 2 (1 loopback)
        It is a stub area
        Area has no authentication
        SPF algorithm last executed 00:20:12.252 ago
        SPF algorithm executed 4 times
        Area ranges are
        Number of LSA 4. Checksum Sum 0x02EA18
        Number of opaque link LSA 0. Checksum Sum 0x000000
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

Notice that on R4 you will get more detail (shows “stub area, no summary LSA”) than on R6 (only shows “stub area”).

R6 is in a totally-stubby area so we will not see any R5’s Loopback interfaces in R6 routing table:

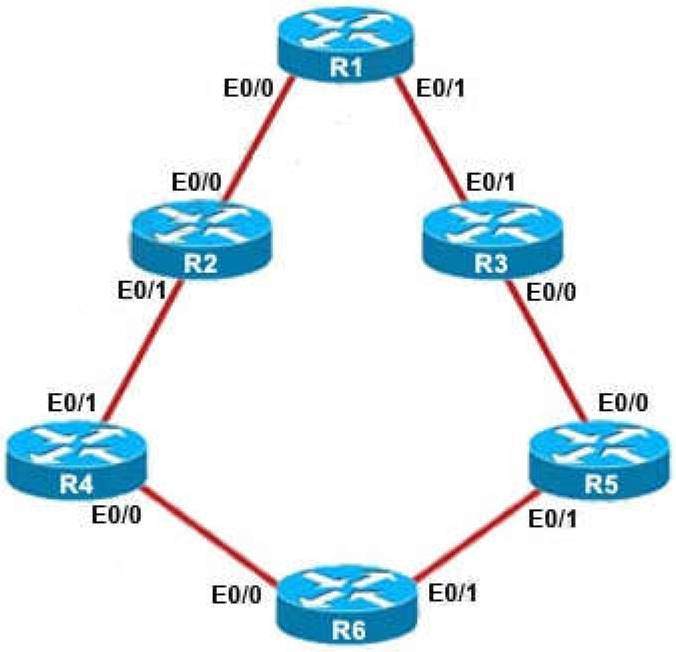


```
R6#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.46.4 to network 0.0.0.0

C    192.168.46.0/24 is directly connected, Ethernet0/0
     6.0.0.0/32 is subnetted, 1 subnets
C       6.6.6.6 is directly connected, Loopback0
O*IA 0.0.0.0/0 [110/2] via 192.168.46.4, 00:06:46, Ethernet0/0
```

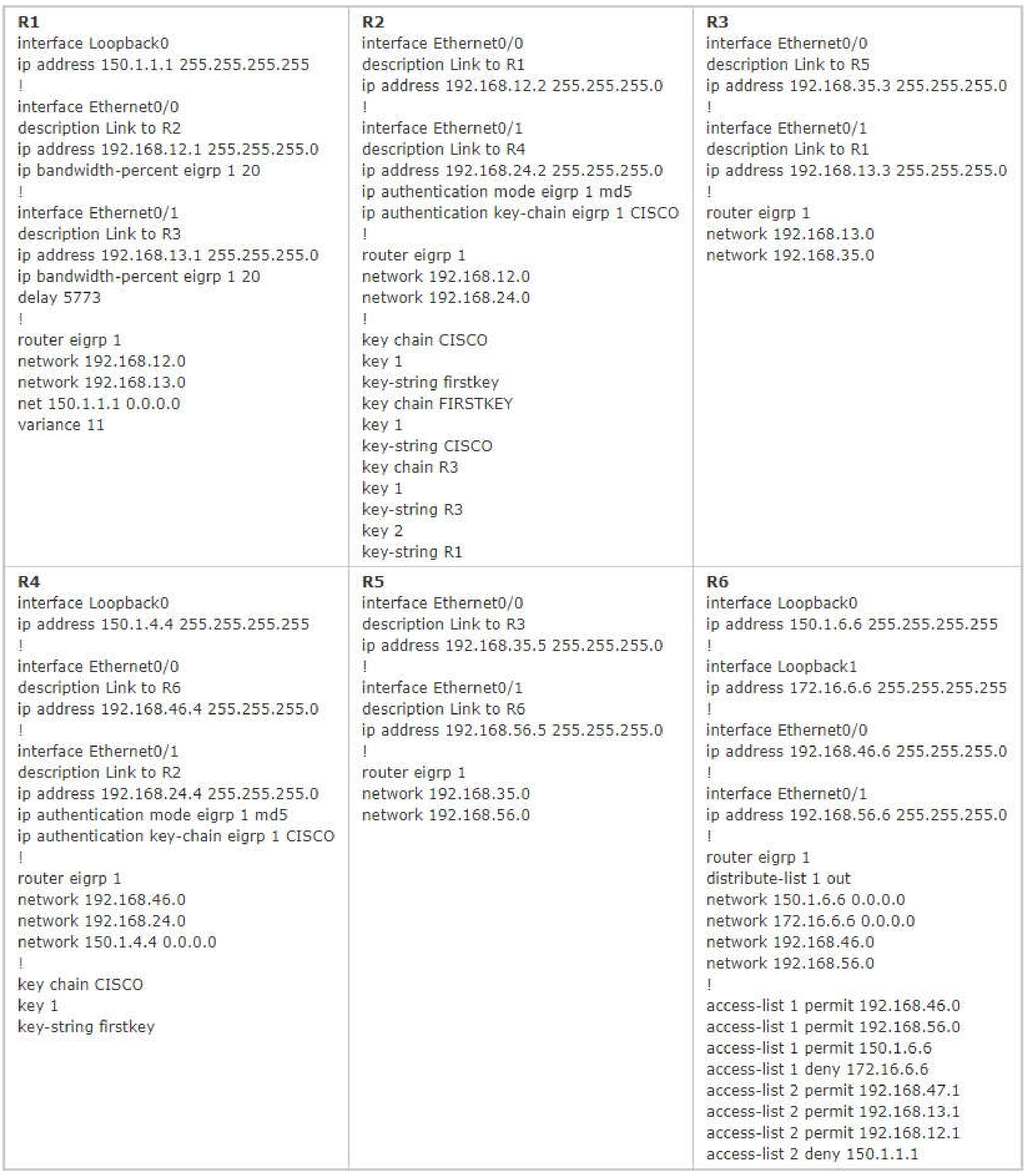
Note: You can see a default (summary) route to the outside (O*IA 0.0.0.0/0 …)

Even though this exercise looks complicated, it can be solve with simple commands:
Q1: show ip ospf database
Q2: show ip ospf database int s0/1
Q3: Show ip ospf
Q4: show ip ospf and show ip route

QUESTION 497



The configuration of R1 to R6 are posted below for your reference, useless lines are omitted:



```
R1
interface Loopback0
ip address 150.1.1.1 255.255.255.255
!
interface Ethernet0/0
description Link to R2
ip address 192.168.12.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
!
interface Ethernet0/1
description Link to R3
ip address 192.168.13.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
delay 5773
!
router eigrp 1
network 192.168.12.0
network 192.168.13.0
net 150.1.1.1 0.0.0.0
variance 11
```

```
R2
interface Ethernet0/0
description Link to R1
ip address 192.168.12.2 255.255.255.0
!
interface Ethernet0/1
description Link to R4
ip address 192.168.24.2 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.12.0
network 192.168.24.0
!
key chain CISCO
key 1
key-string firstkey
key chain FIRSTKEY
key 1
key-string CISCO
key chain R3
key 1
key-string R3
key 2
key-string R1
```

```
R3
interface Ethernet0/0
description Link to R5
ip address 192.168.35.3 255.255.255.0
!
interface Ethernet0/1
description Link to R1
ip address 192.168.13.3 255.255.255.0
!
router eigrp 1
network 192.168.13.0
network 192.168.35.0
```

```
R4
interface Loopback0
ip address 150.1.4.4 255.255.255.255
!
interface Ethernet0/0
description Link to R6
ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/1
description Link to R2
ip address 192.168.24.4 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.46.0
network 192.168.24.0
network 150.1.4.4 0.0.0.0
!
key chain CISCO
key 1
key-string firstkey
```

```
R5
interface Ethernet0/0
description Link to R3
ip address 192.168.35.5 255.255.255.0
!
interface Ethernet0/1
description Link to R6
ip address 192.168.56.5 255.255.255.0
!
router eigrp 1
network 192.168.35.0
network 192.168.56.0
```

```
R6
interface Loopback0
ip address 150.1.6.6 255.255.255.255
!
interface Loopback1
ip address 172.16.6.6 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.46.6 255.255.255.0
!
interface Ethernet0/1
ip address 192.168.56.6 255.255.255.0
!
router eigrp 1
distribute-list 1 out
network 150.1.6.6 0.0.0.0
network 172.16.6.6 0.0.0.0
network 192.168.46.0
network 192.168.56.0
!
access-list 1 permit 192.168.46.0
access-list 1 permit 192.168.56.0
access-list 1 permit 150.1.6.6
access-list 1 deny 172.16.6.6
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny 150.1.1.1
```

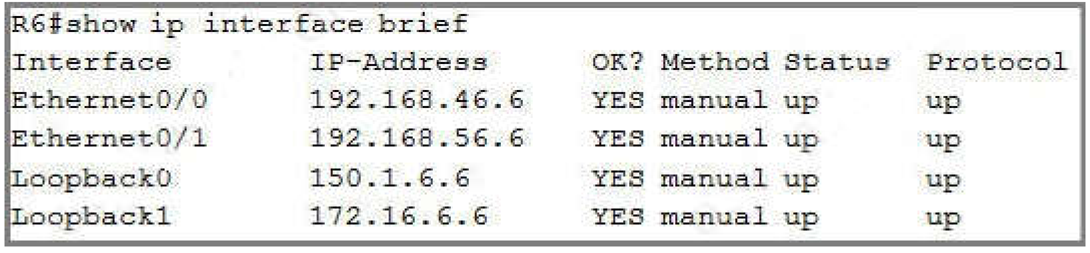
Traffic from R1 to R61 s Loopback address is load shared between R1-R2-R4-R6 and R1- R3-R5-R6 paths. What is the ratio of traffic over each path?

A. 1:1
B. 1:5
C. 6:8
D. 19:80

Correct Answer: D
Section: Mix Questions
Explanation

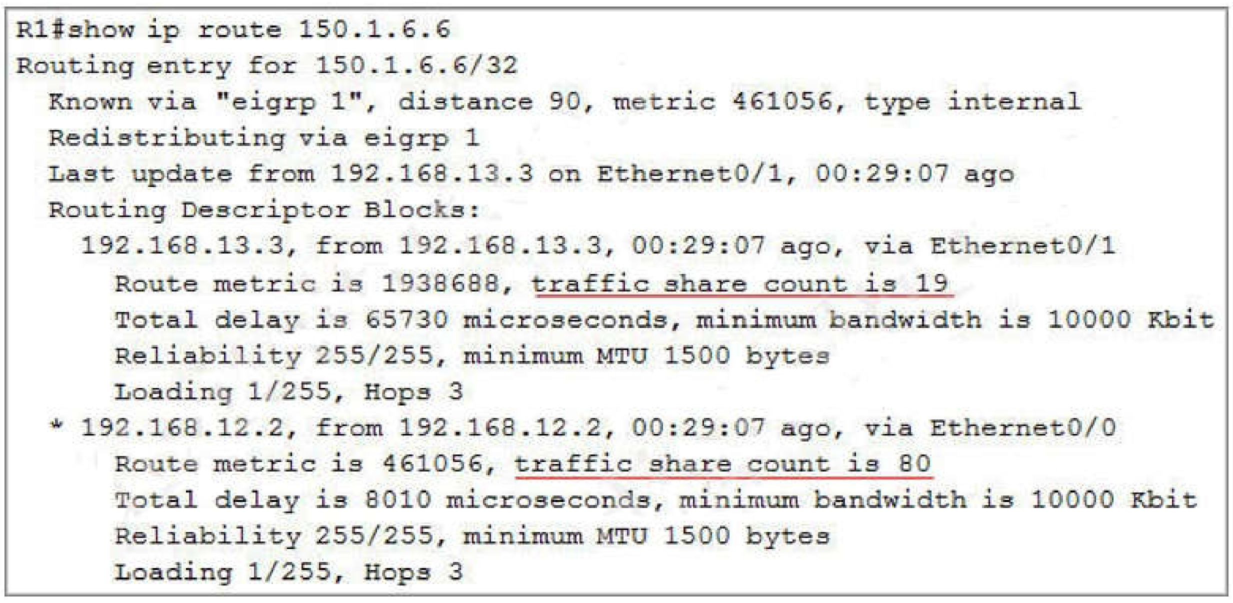
Explanation/Reference:
Explanation:

First we need to get the IP address of R6's loopback address by "show ip interface brief" command on R6:



```
R6#show ip interface brief
Interface        IP-Address      OK? Method Status    Protocol
Ethernet0/0      192.168.46.6    YES manual up        up
Ethernet0/1      192.168.56.6    YES manual up        up
Loopback0        150.1.6.6       YES manual up        up
Loopback1        172.16.6.6      YES manual up        up
```

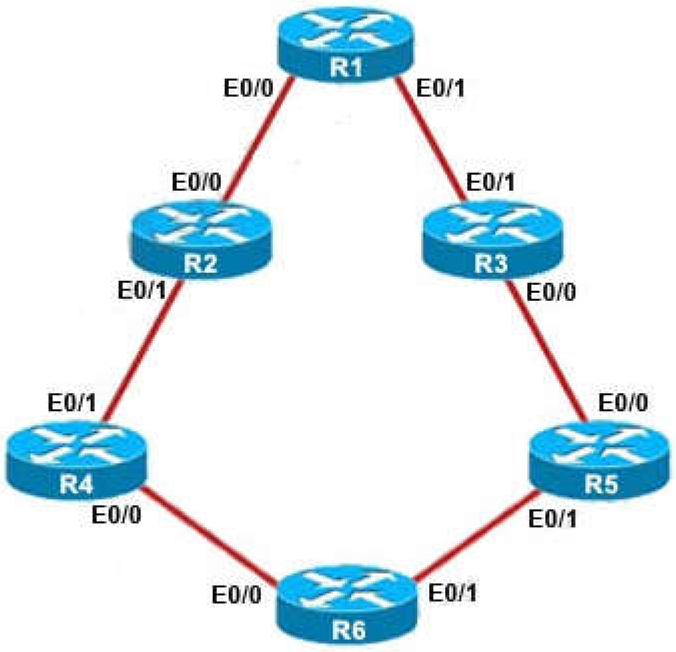
Now we learned the R6's loopback address is 150.1.6.6. To see the ratio of traffic that is load shared between paths, use the "show ip route 150.1.6.6" command on R1:



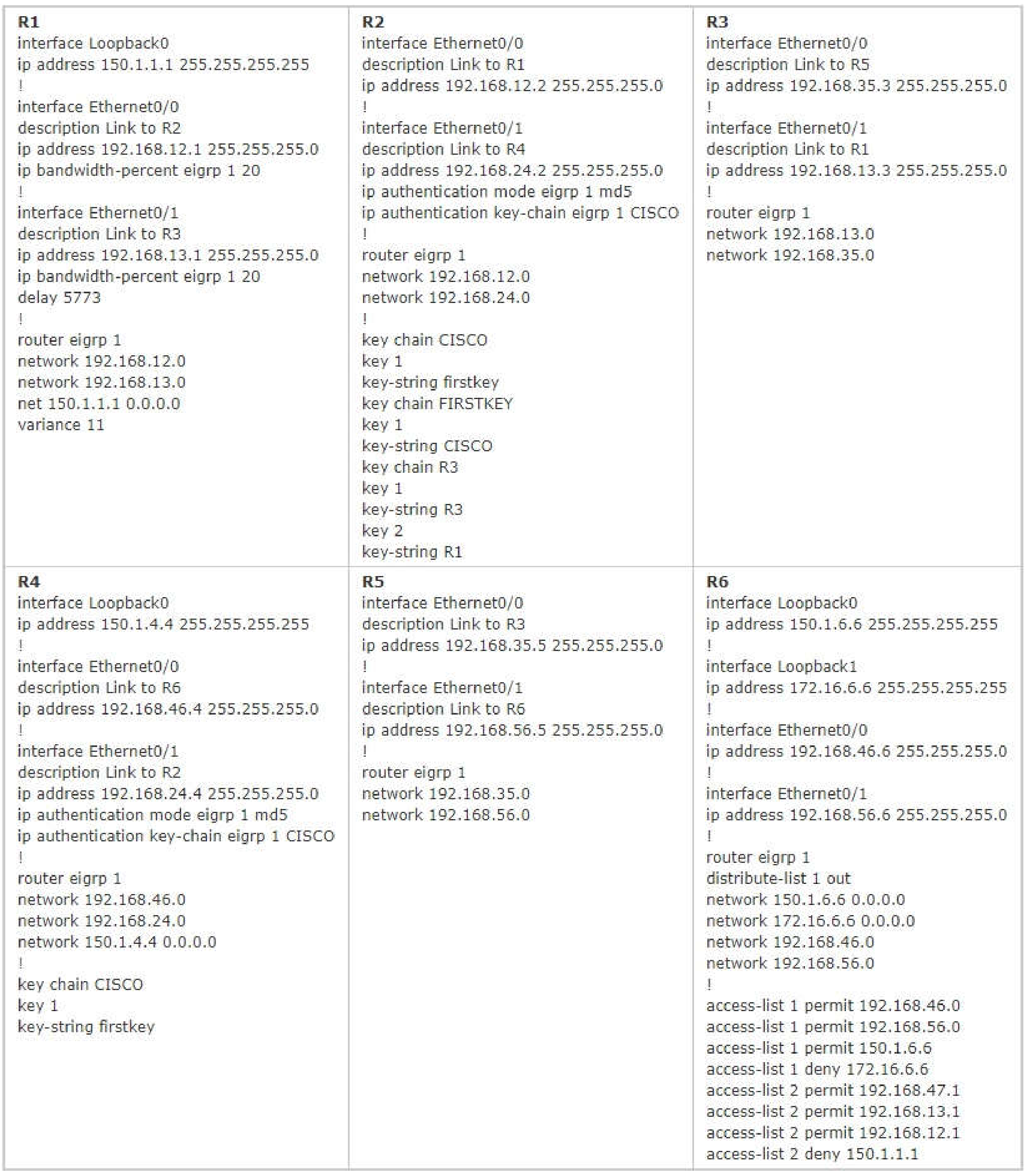
```
R1#show ip route 150.1.6.6
Routing entry for 150.1.6.6/32
  Known via "eigrp 1", distance 90, metric 461056, type internal
  Redistributing via eigrp 1
  Last update from 192.168.13.3 on Ethernet0/1, 00:29:07 ago
  Routing Descriptor Blocks:
    192.168.13.3, from 192.168.13.3, 00:29:07 ago, via Ethernet0/1
      Route metric is 1938688, traffic share count is 19
      Total delay is 65730 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 3
  * 192.168.12.2, from 192.168.12.2, 00:29:07 ago, via Ethernet0/0
      Route metric is 461056, traffic share count is 80
      Total delay is 8010 microseconds, minimum bandwidth is 10000 Kbit
      Reliability 255/255, minimum MTU 1500 bytes
      Loading 1/255, Hops 3
```

This means that after 19 packets are sent to 192.168.13.3, R1 will send 80 packets to 192.168.12.2 (ratio 19:80). This is unequal cost path Load balancing (configured with “variance” command).

QUESTION 498



The configuration of R1 to R6 are posted below for your reference, useless lines are omitted:



R1 interface Loopback0 ip address 150.1.1.1 255.255.255.255 ! interface Ethernet0/0 description Link to R2 ip address 192.168.12.1 255.255.255.0 ip bandwidth-percent eigrp 1 20 ! interface Ethernet0/1 description Link to R3 ip address 192.168.13.1 255.255.255.0 ip bandwidth-percent eigrp 1 20 delay 5773 ! router eigrp 1 network 192.168.12.0 network 192.168.13.0 net 150.1.1.1 0.0.0.0 variance 11	**R2** interface Ethernet0/0 description Link to R1 ip address 192.168.12.2 255.255.255.0 ! interface Ethernet0/1 description Link to R4 ip address 192.168.24.2 255.255.255.0 ip authentication mode eigrp 1 md5 ip authentication key-chain eigrp 1 CISCO ! router eigrp 1 network 192.168.12.0 network 192.168.24.0 ! key chain CISCO key 1 key-string firstkey key chain FIRSTKEY key 1 key-string CISCO key chain R3 key 1 key-string R3 key 2 key-string R1	**R3** interface Ethernet0/0 description Link to R5 ip address 192.168.35.3 255.255.255.0 ! interface Ethernet0/1 description Link to R1 ip address 192.168.13.3 255.255.255.0 ! router eigrp 1 network 192.168.13.0 network 192.168.35.0
R4 interface Loopback0 ip address 150.1.4.4 255.255.255.255 ! interface Ethernet0/0 description Link to R6 ip address 192.168.46.4 255.255.255.0 ! interface Ethernet0/1 description Link to R2 ip address 192.168.24.4 255.255.255.0 ip authentication mode eigrp 1 md5 ip authentication key-chain eigrp 1 CISCO ! router eigrp 1 network 192.168.46.0 network 192.168.24.0 network 150.1.4.4 0.0.0.0 ! key chain CISCO key 1 key-string firstkey	**R5** interface Ethernet0/0 description Link to R3 ip address 192.168.35.5 255.255.255.0 ! interface Ethernet0/1 description Link to R6 ip address 192.168.56.5 255.255.255.0 ! router eigrp 1 network 192.168.35.0 network 192.168.56.0	**R6** interface Loopback0 ip address 150.1.6.6 255.255.255.255 ! interface Loopback1 ip address 172.16.6.6 255.255.255.255 ! interface Ethernet0/0 ip address 192.168.46.6 255.255.255.0 ! interface Ethernet0/1 ip address 192.168.56.6 255.255.255.0 ! router eigrp 1 distribute-list 1 out network 150.1.6.6 0.0.0.0 network 172.16.6.6 0.0.0.0 network 192.168.46.0 network 192.168.56.0 ! access-list 1 permit 192.168.46.0 access-list 1 permit 192.168.56.0 access-list 1 permit 150.1.6.6 access-list 1 deny 172.16.6.6 access-list 2 permit 192.168.47.1 access-list 2 permit 192.168.13.1 access-list 2 permit 192.168.12.1 access-list 2 deny 150.1.1.1

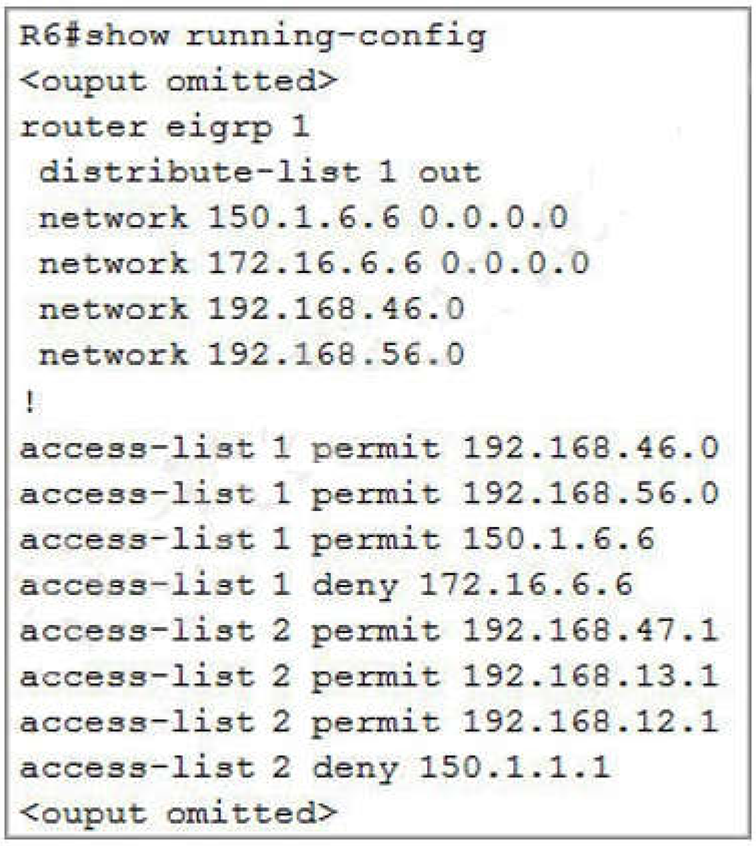
What type of route filtering is occurring on R6?

A. Distribute-list using an ACL
B. Distribute-list using a prefix-list
C. Distribute-list using a route-map
D. An ACL using a distance of 255

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

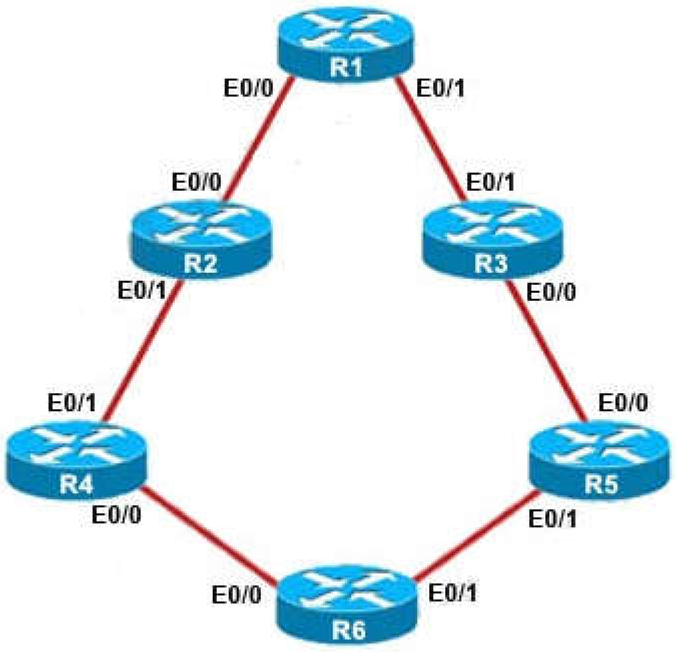
Use the “show running-config” on R6 we will see a distribute-list applying under EIGRP:



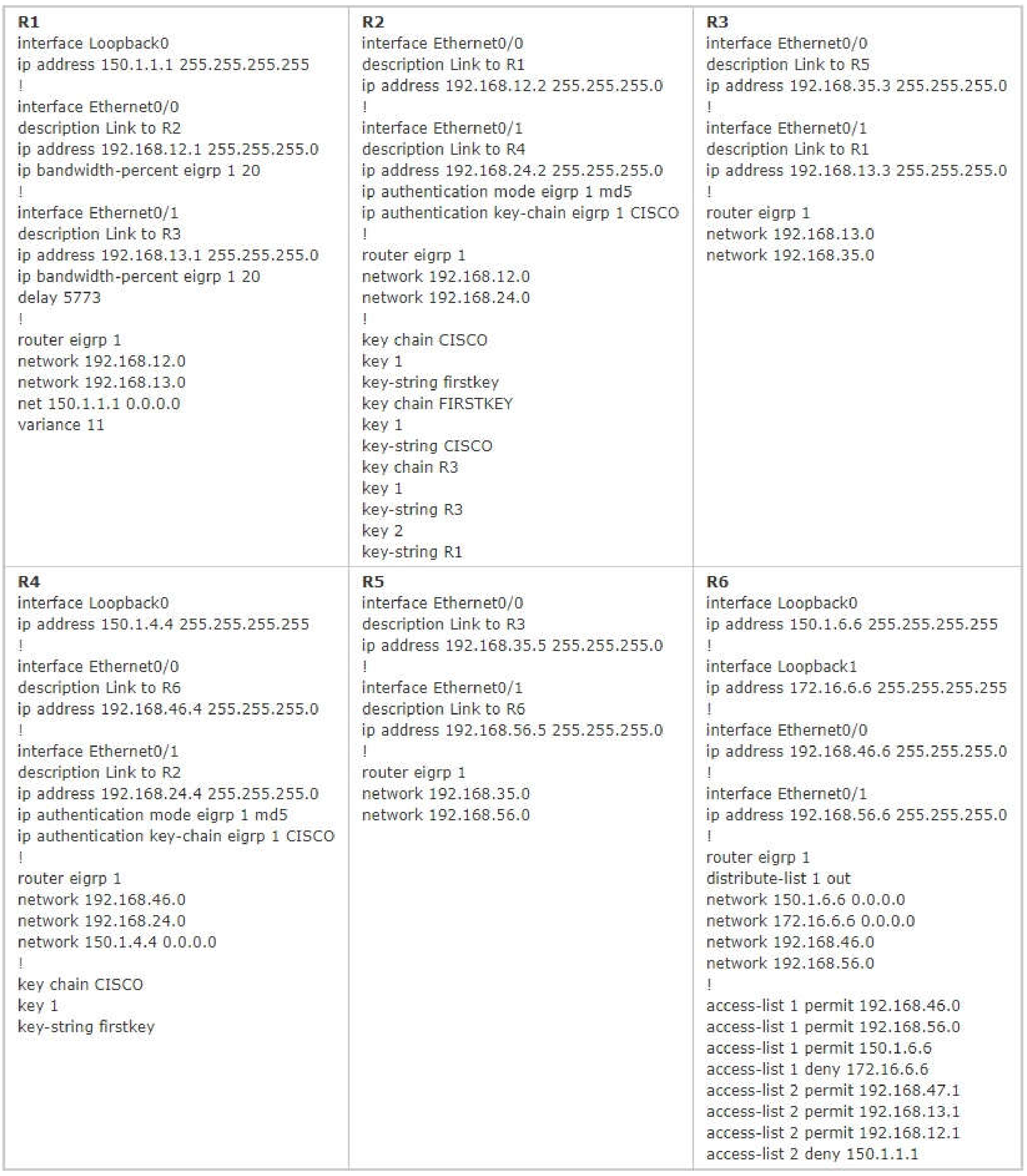
```
R6#show running-config
<ouput omitted>
router eigrp 1
 distribute-list 1 out
 network 150.1.6.6 0.0.0.0
 network 172.16.6.6 0.0.0.0
 network 192.168.46.0
 network 192.168.56.0
!
access-list 1 permit 192.168.46.0
access-list 1 permit 192.168.56.0
access-list 1 permit 150.1.6.6
access-list 1 deny 172.16.6.6
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny 150.1.1.1
<ouput omitted>
```

With this distribute-list, only networks 192.168.46.0; 192.168.56.0 and 150.1.6.6 are advertised out by R6.

QUESTION 499



The configuration of R1 to R6 are posted below for your reference, useless lines are omitted:



R1 interface Loopback0 ip address 150.1.1.1 255.255.255.255 ! interface Ethernet0/0 description Link to R2 ip address 192.168.12.1 255.255.255.0 ip bandwidth-percent eigrp 1 20 ! interface Ethernet0/1 description Link to R3 ip address 192.168.13.1 255.255.255.0 ip bandwidth-percent eigrp 1 20 delay 5773 ! router eigrp 1 network 192.168.12.0 network 192.168.13.0 net 150.1.1.1 0.0.0.0 variance 11	**R2** interface Ethernet0/0 description Link to R1 ip address 192.168.12.2 255.255.255.0 ! interface Ethernet0/1 description Link to R4 ip address 192.168.24.2 255.255.255.0 ip authentication mode eigrp 1 md5 ip authentication key-chain eigrp 1 CISCO ! router eigrp 1 network 192.168.12.0 network 192.168.24.0 ! key chain CISCO key 1 key-string firstkey key chain FIRSTKEY key 1 key-string CISCO key chain R3 key 1 key-string R3 key 2 key-string R1	**R3** interface Ethernet0/0 description Link to R5 ip address 192.168.35.3 255.255.255.0 ! interface Ethernet0/1 description Link to R1 ip address 192.168.13.3 255.255.255.0 ! router eigrp 1 network 192.168.13.0 network 192.168.35.0
R4 interface Loopback0 ip address 150.1.4.4 255.255.255.255 ! interface Ethernet0/0 description Link to R6 ip address 192.168.46.4 255.255.255.0 ! interface Ethernet0/1 description Link to R2 ip address 192.168.24.4 255.255.255.0 ip authentication mode eigrp 1 md5 ip authentication key-chain eigrp 1 CISCO ! router eigrp 1 network 192.168.46.0 network 192.168.24.0 network 150.1.4.4 0.0.0.0 ! key chain CISCO key 1 key-string firstkey	**R5** interface Ethernet0/0 description Link to R3 ip address 192.168.35.5 255.255.255.0 ! interface Ethernet0/1 description Link to R6 ip address 192.168.56.5 255.255.255.0 ! router eigrp 1 network 192.168.35.0 network 192.168.56.0	**R6** interface Loopback0 ip address 150.1.6.6 255.255.255.255 ! interface Loopback1 ip address 172.16.6.6 255.255.255.255 ! interface Ethernet0/0 ip address 192.168.46.6 255.255.255.0 ! interface Ethernet0/1 ip address 192.168.56.6 255.255.255.0 ! router eigrp 1 distribute-list 1 out network 150.1.6.6 0.0.0.0 network 172.16.6.6 0.0.0.0 network 192.168.46.0 network 192.168.56.0 ! access-list 1 permit 192.168.46.0 access-list 1 permit 192.168.56.0 access-list 1 permit 150.1.6.6 access-list 1 deny 172.16.6.6 access-list 2 permit 192.168.47.1 access-list 2 permit 192.168.13.1 access-list 2 permit 192.168.12.1 access-list 2 deny 150.1.1.1

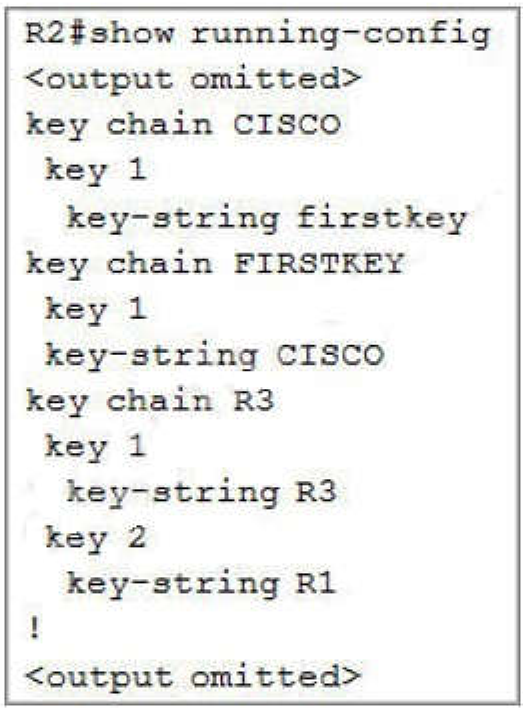
Which key chain is being used for authentication of EIGRP adjacency between R4 and R2?

A. CISCO
B. EIGRP
C. key
D. MD5

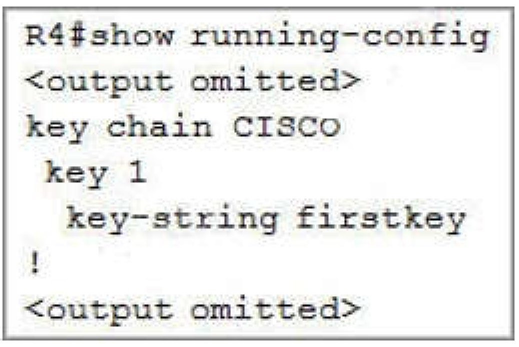
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Check on both R2 and R4:



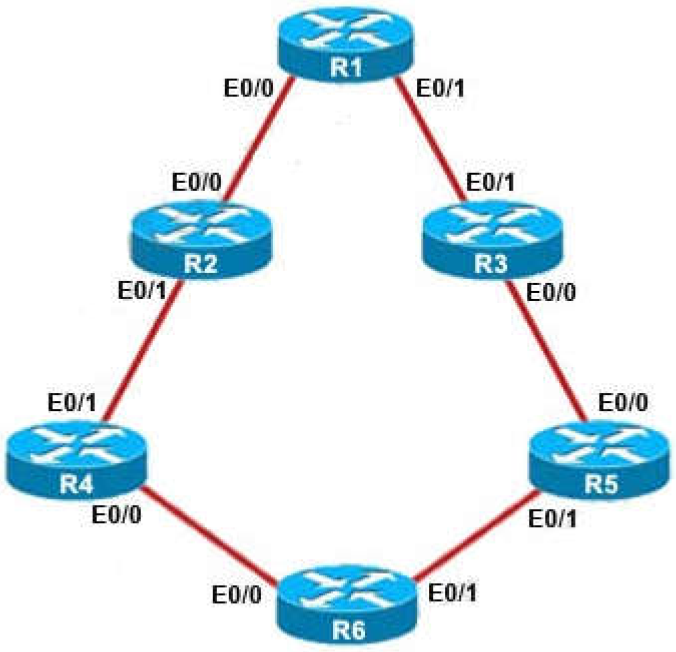
```
R2#show running-config
<output omitted>
key chain CISCO
 key 1
  key-string firstkey
key chain FIRSTKEY
 key 1
 key-string CISCO
key chain R3
 key 1
  key-string R3
 key 2
  key-string R1
!
<output omitted>
```



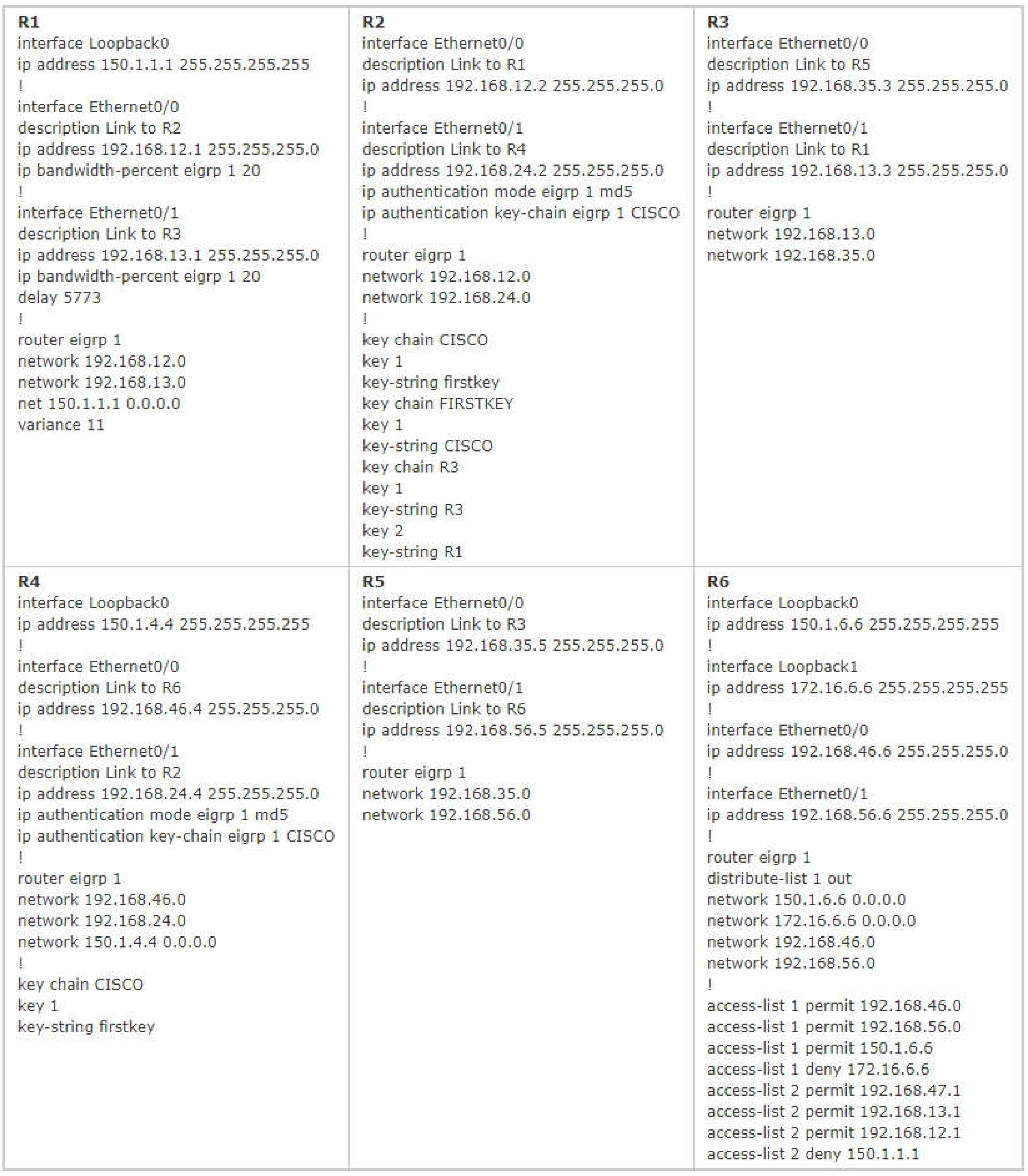
```
R4#show running-config
<output omitted>
key chain CISCO
 key 1
  key-string firstkey
!
<output omitted>
```

To successfully authenticate between two EIGRP neighbors, the key number and key-string must match. The key chain name is only for local use. In this case we have key number “1” and key-string “CISCO” and they match so EIGRP neighbor relationship is formed.

QUESTION 500



The configuration of R1 to R6 are posted below for your reference, useless lines are omitted:



```
R1
interface Loopback0
ip address 150.1.1.1 255.255.255.255
!
interface Ethernet0/0
description Link to R2
ip address 192.168.12.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
!
interface Ethernet0/1
description Link to R3
ip address 192.168.13.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
delay 5773
!
router eigrp 1
network 192.168.12.0
network 192.168.13.0
net 150.1.1.1 0.0.0.0
variance 11
```

```
R2
interface Ethernet0/0
description Link to R1
ip address 192.168.12.2 255.255.255.0
!
interface Ethernet0/1
description Link to R4
ip address 192.168.24.2 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.12.0
network 192.168.24.0
!
key chain CISCO
key 1
key-string firstkey
key chain FIRSTKEY
key 1
key-string CISCO
key chain R3
key 1
key-string R3
key 2
key-string R1
```

```
R3
interface Ethernet0/0
description Link to R5
ip address 192.168.35.3 255.255.255.0
!
interface Ethernet0/1
description Link to R1
ip address 192.168.13.3 255.255.255.0
!
router eigrp 1
network 192.168.13.0
network 192.168.35.0
```

```
R4
interface Loopback0
ip address 150.1.4.4 255.255.255.255
!
interface Ethernet0/0
description Link to R6
ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/1
description Link to R2
ip address 192.168.24.4 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.46.0
network 192.168.24.0
network 150.1.4.4 0.0.0.0
!
key chain CISCO
key 1
key-string firstkey
```

```
R5
interface Ethernet0/0
description Link to R3
ip address 192.168.35.5 255.255.255.0
!
interface Ethernet0/1
description Link to R6
ip address 192.168.56.5 255.255.255.0
!
router eigrp 1
network 192.168.35.0
network 192.168.56.0
```

```
R6
interface Loopback0
ip address 150.1.6.6 255.255.255.255
!
interface Loopback1
ip address 172.16.6.6 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.46.6 255.255.255.0
!
interface Ethernet0/1
ip address 192.168.56.6 255.255.255.0
!
router eigrp 1
distribute-list 1 out
network 150.1.6.6 0.0.0.0
network 172.16.6.6 0.0.0.0
network 192.168.46.0
network 192.168.56.0
!
access-list 1 permit 192.168.46.0
access-list 1 permit 192.168.56.0
access-list 1 permit 150.1.6.6
access-list 1 deny 172.16.6.6
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny 150.1.1.1
```

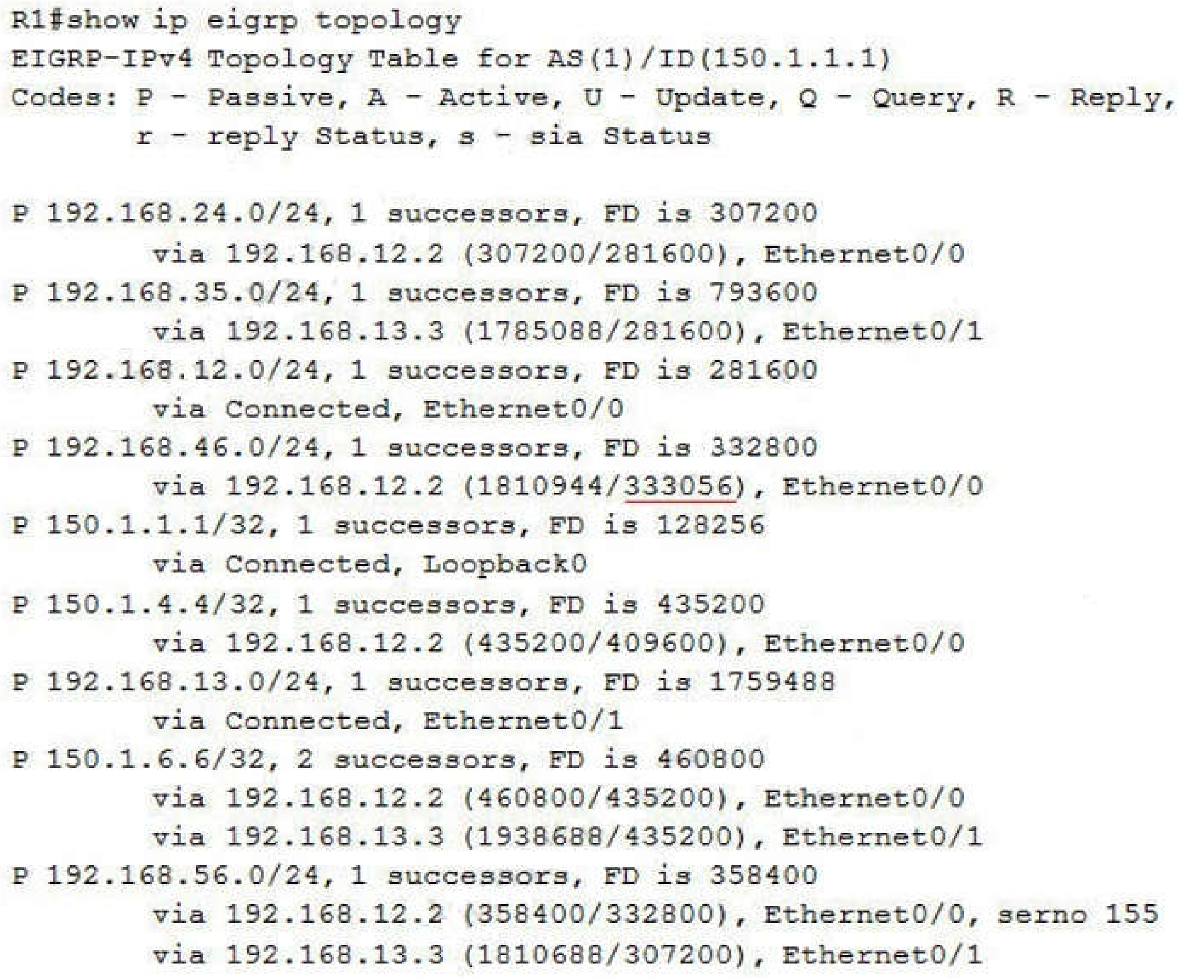
What is the advertised distance for the 192.168.46.0 network on R1?

A. 333056
B. 1938688
C. 1810944
D. 307456

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

To check the advertised distance for a prefix we cannot use the “show ip route” command because it only shows the metric (also known as Feasible Distance). Therefore we have to use the “show ip eigrp topology” command:

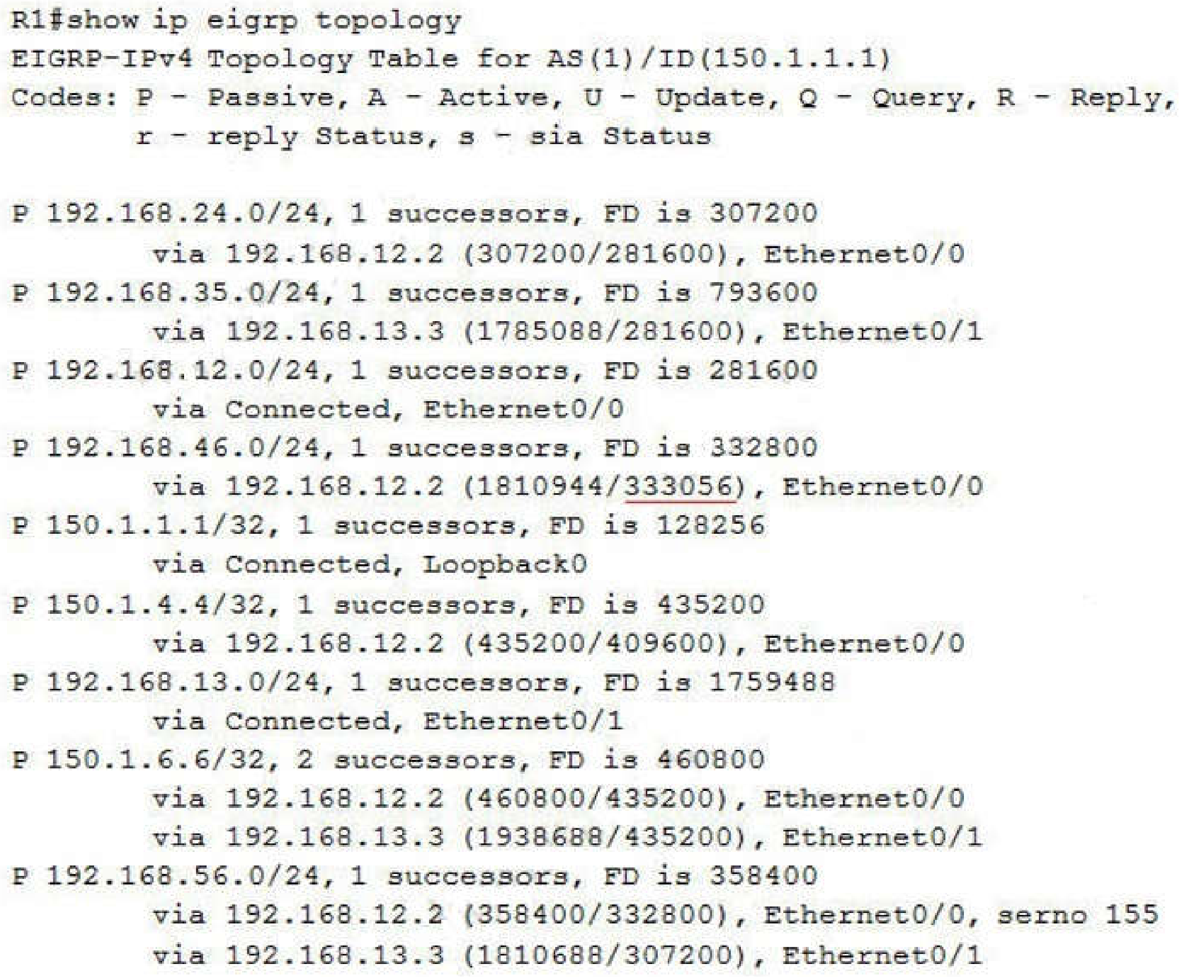


```
R1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(150.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.24.0/24, 1 successors, FD is 307200
        via 192.168.12.2 (307200/281600), Ethernet0/0
P 192.168.35.0/24, 1 successors, FD is 793600
        via 192.168.13.3 (1785088/281600), Ethernet0/1
P 192.168.12.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 192.168.46.0/24, 1 successors, FD is 332800
        via 192.168.12.2 (1810944/333056), Ethernet0/0
P 150.1.1.1/32, 1 successors, FD is 128256
        via Connected, Loopback0
P 150.1.4.4/32, 1 successors, FD is 435200
        via 192.168.12.2 (435200/409600), Ethernet0/0
P 192.168.13.0/24, 1 successors, FD is 1759488
        via Connected, Ethernet0/1
P 150.1.6.6/32, 2 successors, FD is 460800
        via 192.168.12.2 (460800/435200), Ethernet0/0
        via 192.168.13.3 (1938688/435200), Ethernet0/1
P 192.168.56.0/24, 1 successors, FD is 358400
        via 192.168.12.2 (358400/332800), Ethernet0/0, serno 155
        via 192.168.13.3 (1810688/307200), Ethernet0/1
```

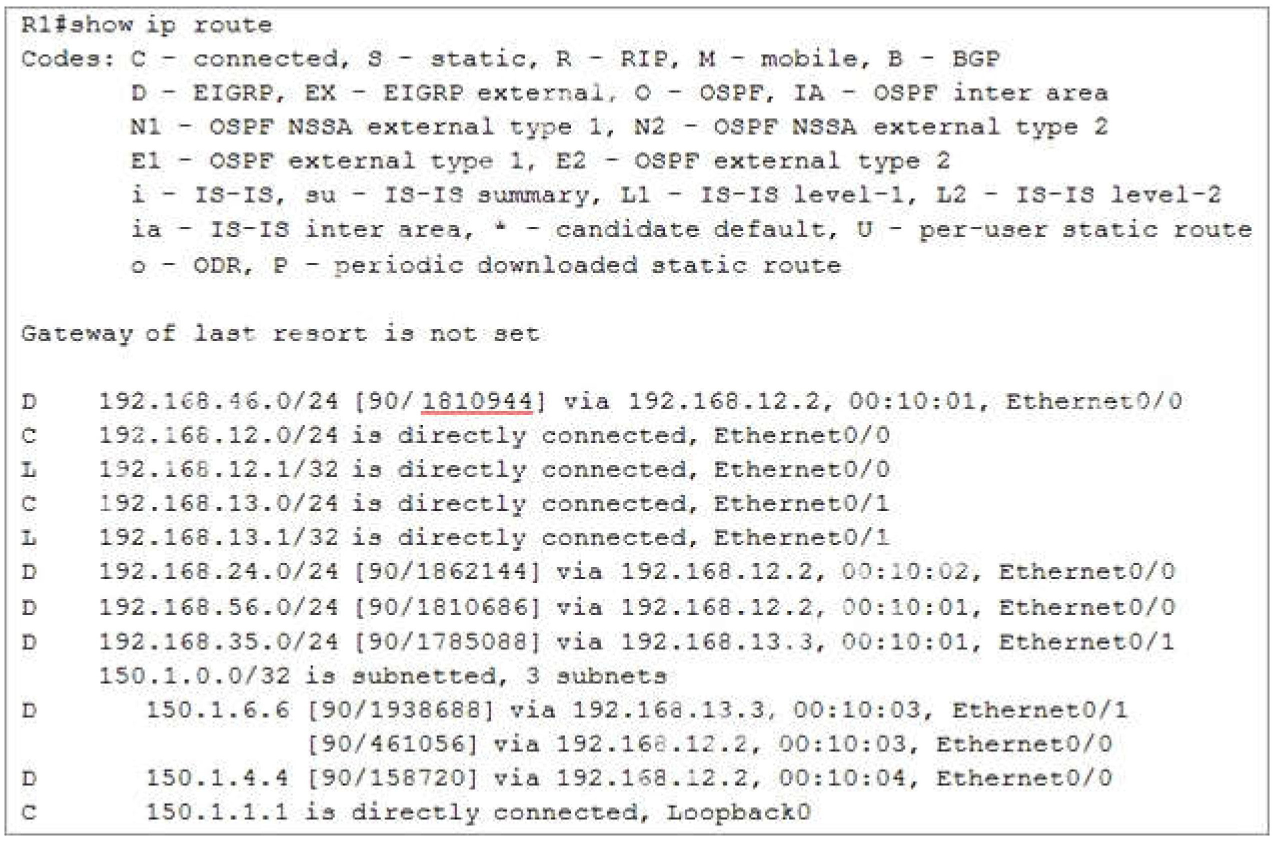
Update: Although the “show ip eigrp topology” does not work in the exam but the “show ip eigrp 1 topology” does work so please use this command instead and we will find out the advertised distance on R1.

There are two parameters in the brackets of 192.168.46.0/24 prefix: (1810944/333056). The first one “1810944” is the Feasible Distance (FD) and the second “333056” is the Advertised Distance (AD) of that route -> A is correct.

Just for your reference, this is the output of the “show ip route” command on R1:

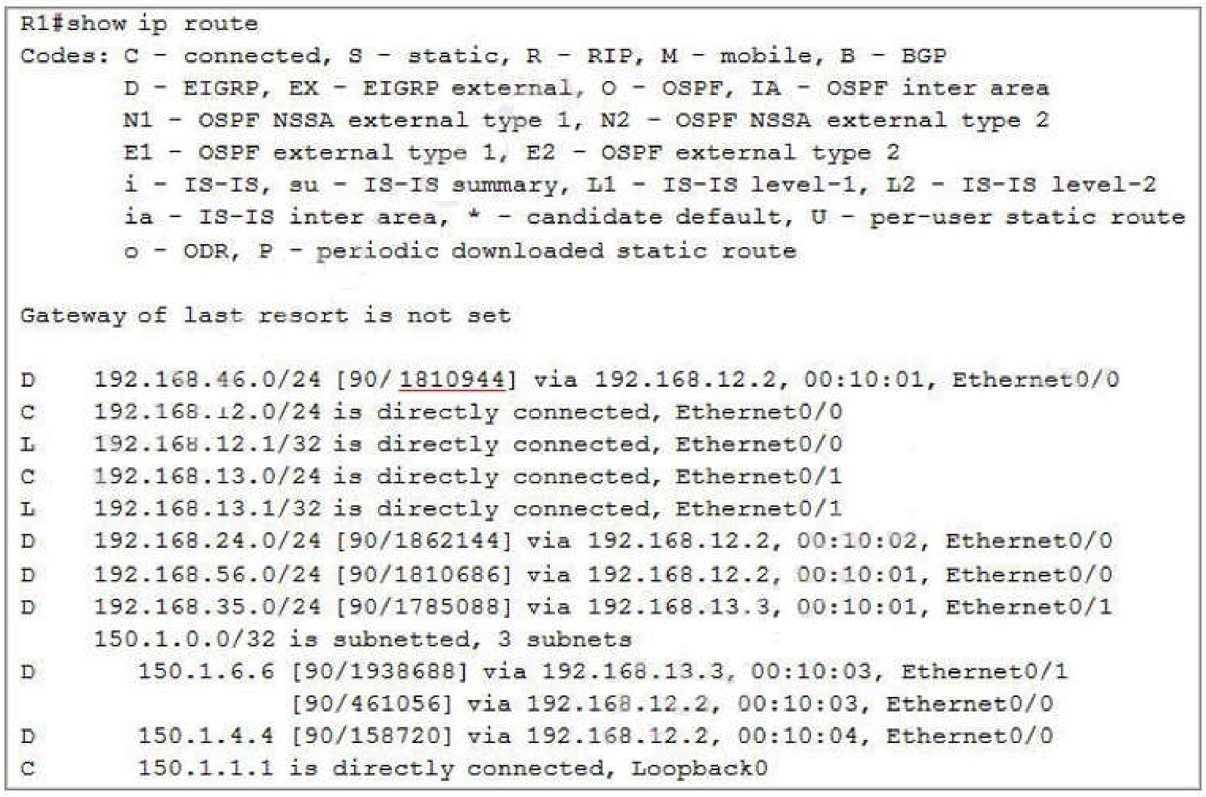


```
R1#show ip eigrp topology
EIGRP-IPv4 Topology Table for AS(1)/ID(150.1.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.24.0/24, 1 successors, FD is 307200
        via 192.168.12.2 (307200/281600), Ethernet0/0
P 192.168.35.0/24, 1 successors, FD is 793600
        via 192.168.13.3 (1785088/281600), Ethernet0/1
P 192.168.12.0/24, 1 successors, FD is 281600
        via Connected, Ethernet0/0
P 192.168.46.0/24, 1 successors, FD is 332800
        via 192.168.12.2 (1810944/333056), Ethernet0/0
P 150.1.1.1/32, 1 successors, FD is 128256
        via Connected, Loopback0
P 150.1.4.4/32, 1 successors, FD is 435200
        via 192.168.12.2 (435200/409600), Ethernet0/0
P 192.168.13.0/24, 1 successors, FD is 1759488
        via Connected, Ethernet0/1
P 150.1.6.6/32, 2 successors, FD is 460800
        via 192.168.12.2 (460800/435200), Ethernet0/0
        via 192.168.13.3 (1938688/435200), Ethernet0/1
P 192.168.56.0/24, 1 successors, FD is 358400
        via 192.168.12.2 (358400/332800), Ethernet0/0, serno 155
        via 192.168.13.3 (1810688/307200), Ethernet0/1
```



```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.46.0/24 [90/1810944] via 192.168.12.2, 00:10:01, Ethernet0/0
C    192.168.12.0/24 is directly connected, Ethernet0/0
L    192.168.12.1/32 is directly connected, Ethernet0/0
C    192.168.13.0/24 is directly connected, Ethernet0/1
L    192.168.13.1/32 is directly connected, Ethernet0/1
D    192.168.24.0/24 [90/1862144] via 192.168.12.2, 00:10:02, Ethernet0/0
D    192.168.56.0/24 [90/1810686] via 192.168.12.2, 00:10:01, Ethernet0/0
D    192.168.35.0/24 [90/1785088] via 192.168.13.3, 00:10:01, Ethernet0/1
     150.1.0.0/32 is subnetted, 3 subnets
D       150.1.6.6 [90/1938688] via 192.168.13.3, 00:10:03, Ethernet0/1
                  [90/461056] via 192.168.12.2, 00:10:03, Ethernet0/0
D       150.1.4.4 [90/158720] via 192.168.12.2, 00:10:04, Ethernet0/0
C       150.1.1.1 is directly connected, Loopback0
```

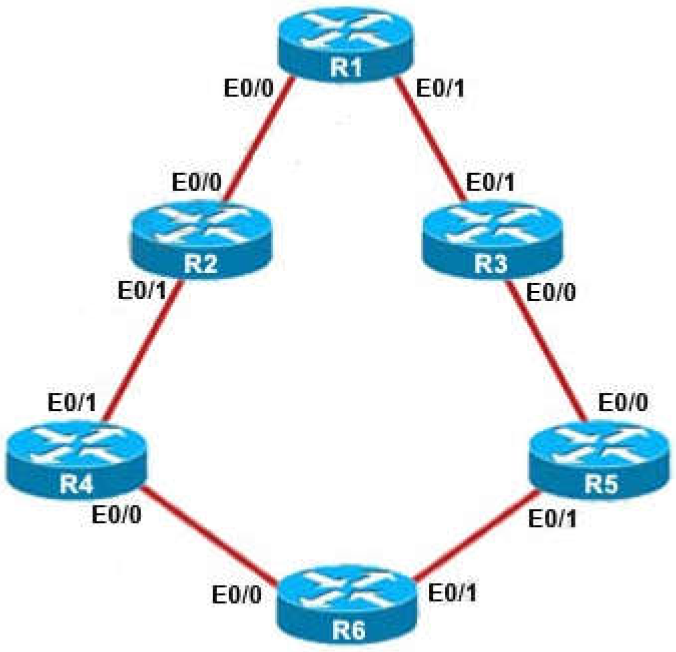
In the first line:



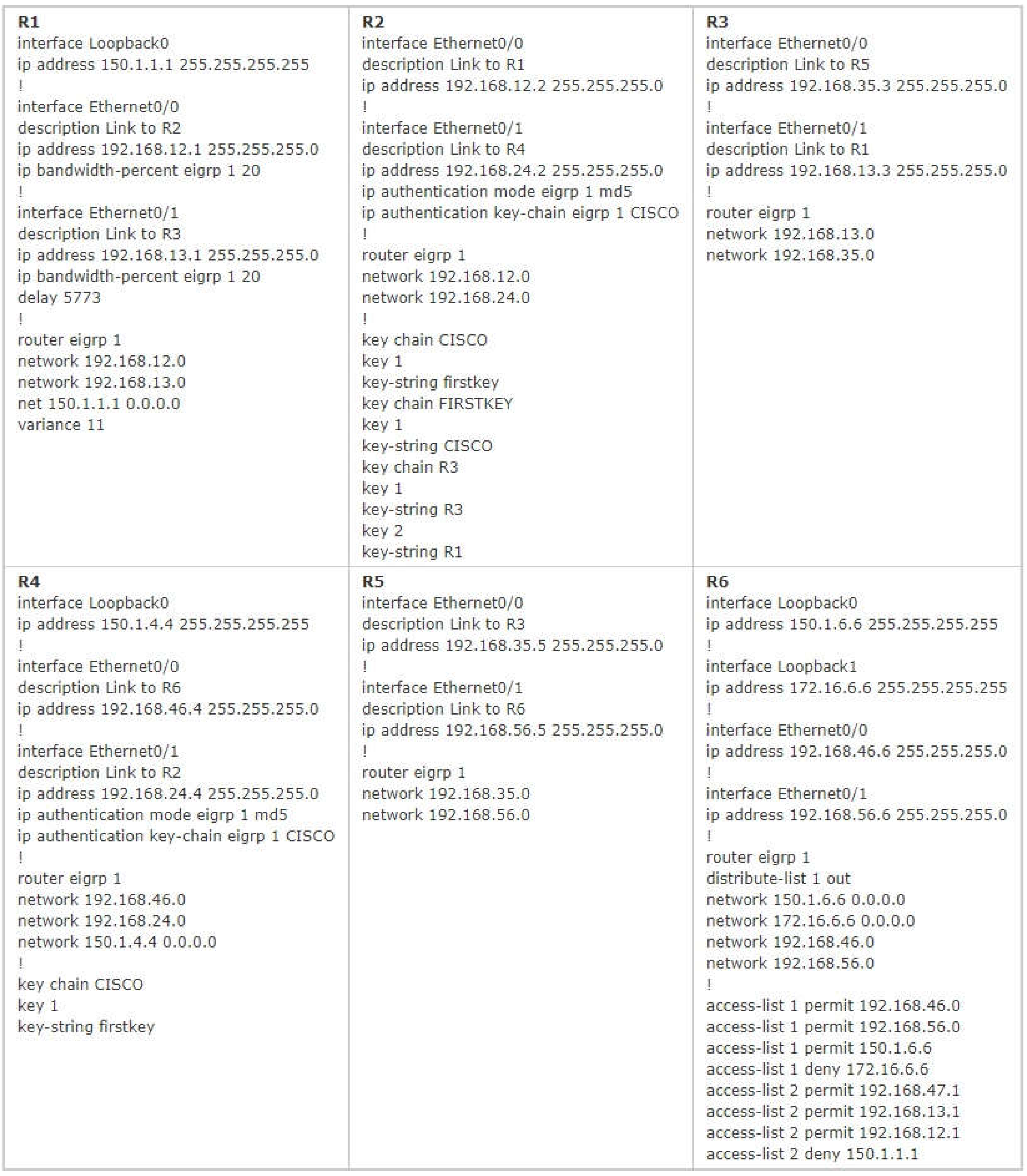
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D    192.168.46.0/24 [90/1810944] via 192.168.12.2, 00:10:01, Ethernet0/0
C    192.168.12.0/24 is directly connected, Ethernet0/0
L    192.168.12.1/32 is directly connected, Ethernet0/0
C    192.168.13.0/24 is directly connected, Ethernet0/1
L    192.168.13.1/32 is directly connected, Ethernet0/1
D    192.168.24.0/24 [90/1862144] via 192.168.12.2, 00:10:02, Ethernet0/0
D    192.168.56.0/24 [90/1810686] via 192.168.12.2, 00:10:01, Ethernet0/0
D    192.168.35.0/24 [90/1785088] via 192.168.13.3, 00:10:01, Ethernet0/1
     150.1.0.0/32 is subnetted, 3 subnets
D       150.1.6.6 [90/1938688] via 192.168.13.3, 00:10:03, Ethernet0/1
                  [90/461056] via 192.168.12.2, 00:10:03, Ethernet0/0
D       150.1.4.4 [90/158720] via 192.168.12.2, 00:10:04, Ethernet0/0
C       150.1.1.1 is directly connected, Loopback0
```

D 192.168.46.0/24 [90/ 1810944] via 192.168.12.2, 00:10:01, Ethernet0/0
The first parameter “90” is the EIGRP Administrative Distance. The second parameter “1810944” is the metric of the route 192.168.46.0/24. R1 will use this metric to advertise this route to other routers but the question asks about “the advertised distance for the 192.168.46.0 network on R1” so we cannot use this command to find out the answer.

QUESTION 501



The configuration of R1 to R6 are posted below for your reference, useless lines are omitted:



```
R1
interface Loopback0
ip address 150.1.1.1 255.255.255.255
!
interface Ethernet0/0
description Link to R2
ip address 192.168.12.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
!
interface Ethernet0/1
description Link to R3
ip address 192.168.13.1 255.255.255.0
ip bandwidth-percent eigrp 1 20
delay 5773
!
router eigrp 1
network 192.168.12.0
network 192.168.13.0
net 150.1.1.1 0.0.0.0
variance 11
```

```
R2
interface Ethernet0/0
description Link to R1
ip address 192.168.12.2 255.255.255.0
!
interface Ethernet0/1
description Link to R4
ip address 192.168.24.2 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.12.0
network 192.168.24.0
!
key chain CISCO
key 1
key-string firstkey
key chain FIRSTKEY
key 1
key-string CISCO
key chain R3
key 1
key-string R3
key 2
key-string R1
```

```
R3
interface Ethernet0/0
description Link to R5
ip address 192.168.35.3 255.255.255.0
!
interface Ethernet0/1
description Link to R1
ip address 192.168.13.3 255.255.255.0
!
router eigrp 1
network 192.168.13.0
network 192.168.35.0
```

```
R4
interface Loopback0
ip address 150.1.4.4 255.255.255.255
!
interface Ethernet0/0
description Link to R6
ip address 192.168.46.4 255.255.255.0
!
interface Ethernet0/1
description Link to R2
ip address 192.168.24.4 255.255.255.0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 CISCO
!
router eigrp 1
network 192.168.46.0
network 192.168.24.0
network 150.1.4.4 0.0.0.0
!
key chain CISCO
key 1
key-string firstkey
```

```
R5
interface Ethernet0/0
description Link to R3
ip address 192.168.35.5 255.255.255.0
!
interface Ethernet0/1
description Link to R6
ip address 192.168.56.5 255.255.255.0
!
router eigrp 1
network 192.168.35.0
network 192.168.56.0
```

```
R6
interface Loopback0
ip address 150.1.6.6 255.255.255.255
!
interface Loopback1
ip address 172.16.6.6 255.255.255.255
!
interface Ethernet0/0
ip address 192.168.46.6 255.255.255.0
!
interface Ethernet0/1
ip address 192.168.56.6 255.255.255.0
!
router eigrp 1
distribute-list 1 out
network 150.1.6.6 0.0.0.0
network 172.16.6.6 0.0.0.0
network 192.168.46.0
network 192.168.56.0
!
access-list 1 permit 192.168.46.0
access-list 1 permit 192.168.56.0
access-list 1 permit 150.1.6.6
access-list 1 deny 172.16.6.6
access-list 2 permit 192.168.47.1
access-list 2 permit 192.168.13.1
access-list 2 permit 192.168.12.1
access-list 2 deny 150.1.1.1
```

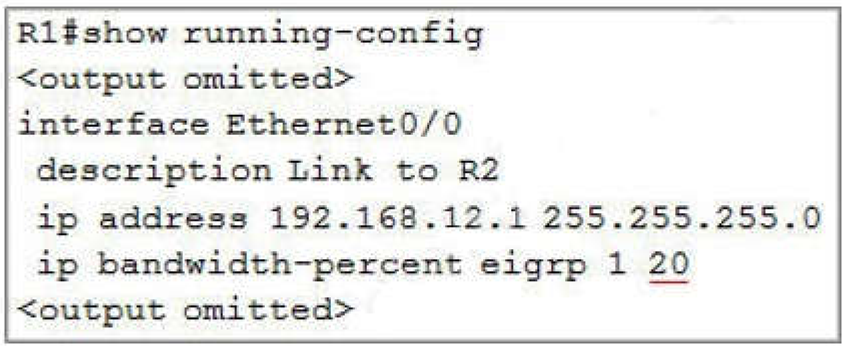
How much bandwidth is available for use by EIGRP on the R1 Ethernet 0/0 interface?

A. 1
B. 10
C. 20
D. 100

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

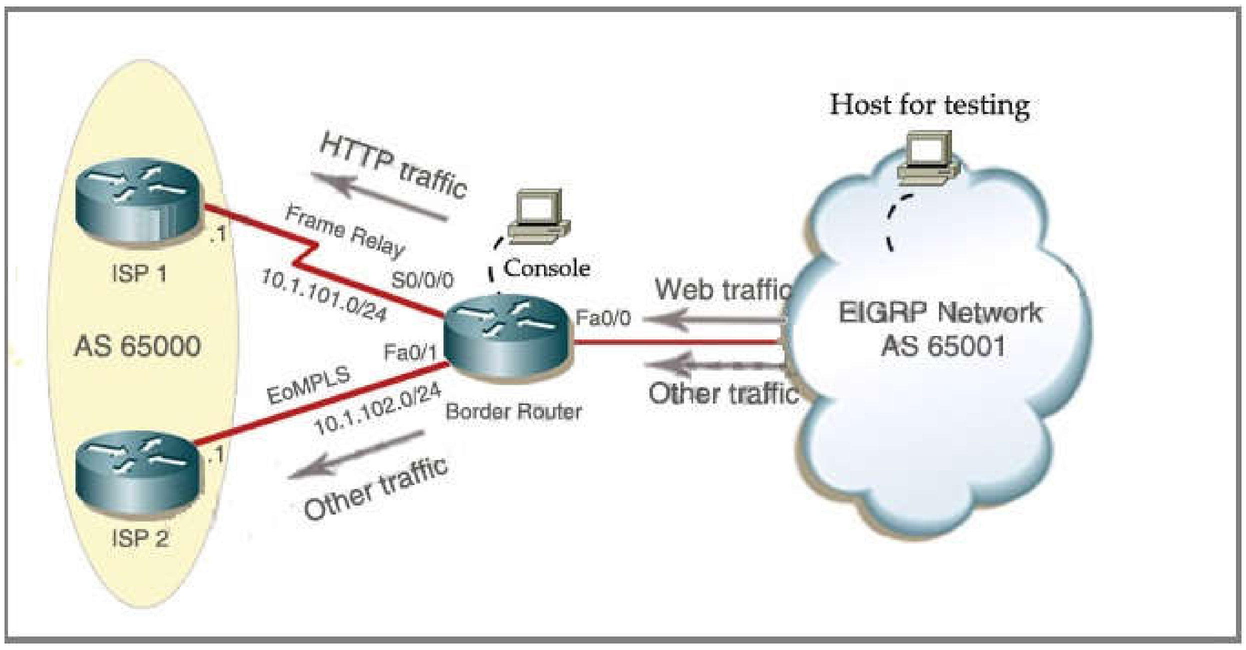
Check with the “show running-config” command on R1:



```
R1#show running-config
<output omitted>
interface Ethernet0/0
 description Link to R2
 ip address 192.168.12.1 255.255.255.0
 ip bandwidth-percent eigrp 1 20
<output omitted>
```

In the “ip bandwitdh-percent eigrp 1 20” command, “1” is the EIGRP AS number while “20” is the percent of interface’s bandwidth that EIGRP is allowed to use.

QUESTION 502
SIMULATION
Policy Based Routing Sim



Company A can has two links which can take it to the Internet. The company policy demands that you use web traffic to be forwarded only to Frame Relay link if available and other traffic can go through any links. No static or default routing is allowed.

1) Access list that catches the HTTP traffic:
BorderRouter(config)#access-list 101 permit tcp any any eq www
2) Route map that sets the next hop address to be ISP1 and permits the rest of the traffic:
BorderRouter(config)#route-map pbr permit 10
BorderRouter(config-route-map)#match ip address 101
BorderRouter(config-route-map)#set ip next-hop 10.1.101.1
BorderRouter(config-route-map)#exit
3) Apply the route-map on the interface to the server in the EIGRP Network:
BorderRouter(config-route-map)#exit
BorderRouter(config)#int fa0/0
BorderRouter(config-if)#ip policy route-map pbr
BorderRouter(config-if)#exit
BorderRouter(config)#exit

BorderRouter#show route-map

Correct Answer: See explanation below
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
All the HTTP traffic from the EIGRP Network should go through Frame Relay link if available and all the other traffic should go through either link. The only router you are able to administrate is the Border Router, from the EIGRP Network you may only send HTTP traffic. As the other people mentioned, actually it is not a BGP lab. You are not able to execute the command “router bgp 65001″
1) Access list that catches the HTTP traffic:
BorderRouter#access-list 101 permit tcp any any eq www

Note that the server was not directly connected to the Border Router. There were a lot of EIGRP routes on it. In the real exam you do not know the exact IP address of the server in the EIGRP network so we have to use the source as “any” to catch all the source addresses.

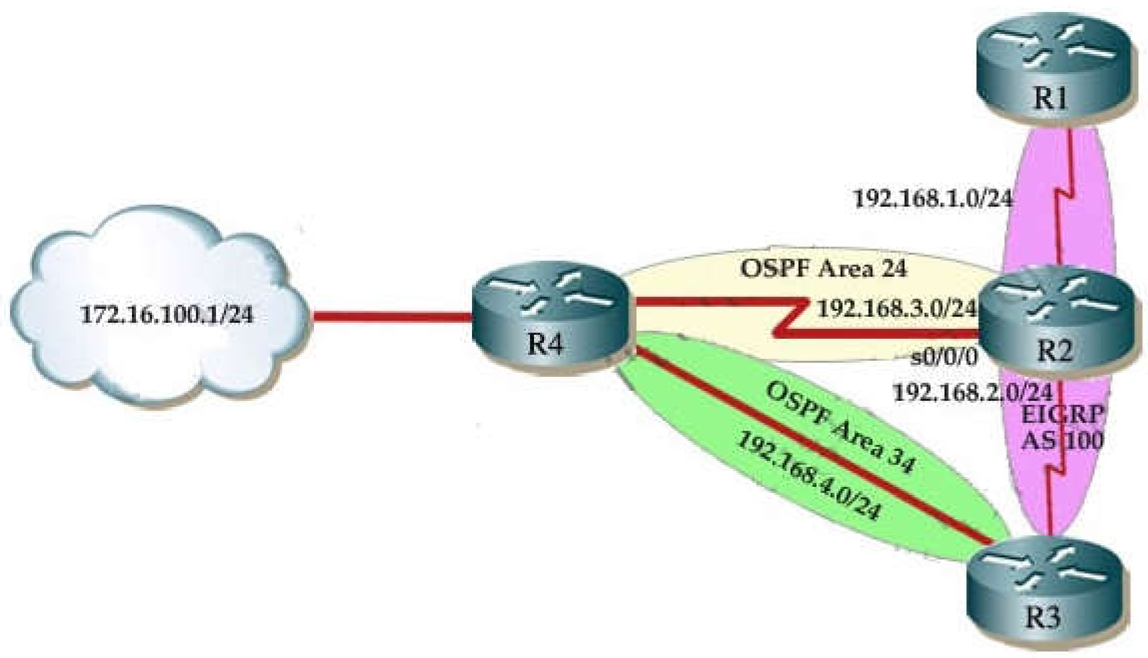
2) Route map that sets the next hop address to be ISP1 and permits the rest of the traffic:
BorderRouter(config)#route-map pbr permit 10
BorderRouter(config-route-map)#match ip address 101
BorderRouter(config-route-map)#set ip next-hop 10.1.101.1
BorderRouter(config-route-map)#exit

“If the packets do not meet any of the defined match criteria (that is, if the packets fall off the end of a route map), then those packets are routed through the normal destination-based routing process. If it is desired not to revert to normal forwarding and to drop the packets that do not match the specified criteria, then interface Null 0 should be specified as the last interface in the list by using the set clause.”
Reference: http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml)

3) Apply the route-map on the interface to the server in the EIGRP Network:
BorderRouter(config-route-map)#exit
BorderRouter(config)#int fa0/0
BorderRouter(config-if)#ip policy route-map pbr
BorderRouter(config-if)#exit
BorderRouter(config)#exit

4) There is a “Host for Testing”, click on this host to open a box in which there is a button named “Generate HTTP traffic”. Click on this button to generate some packets for HTTP traffic. Jump back to the BorderRouter and type the command “show route-map”.
BorderRouter#show route-map
In the output you will see the line “Policy routing matches: 9 packets…”. It means that the route-map we configured is working properly.

QUESTION 503
SIMULATION
EIGRP OSPF Redistribution Sim



You are a network engineer with ROUTE.com, a small IT company. They have recently merged two organizations and now need to merge their networks as shown in the topology exhibit. One network is using OSPF as its IGP and the other is using EIGRP as its IGP. R4 has been added to the existing OSPF network to provide the interconnect between the OSPF and EIGRP networks. Two links have been added that will provide redundancy.

The network requirements state that you must be able to ping and telnet from loopback 101 on R1 to the OPSF domain test address of 172.16.1.100. All traffic must use the shortest path that provides the greatest bandwidth. The redundant paths from the OSPF network to the EIGRP network must be available in case of a link failure. No static or default routing is allowed in either network.

A previous network engineer has started the merger implementation and has successfully assigned and verified all IP addressing and basic IGP routing. You have been tasked with completing the implementation and ensuring that the network requirements are met. You may not remove or change any of the configuration commands currently on any of the routers. You may add new commands or change default values.

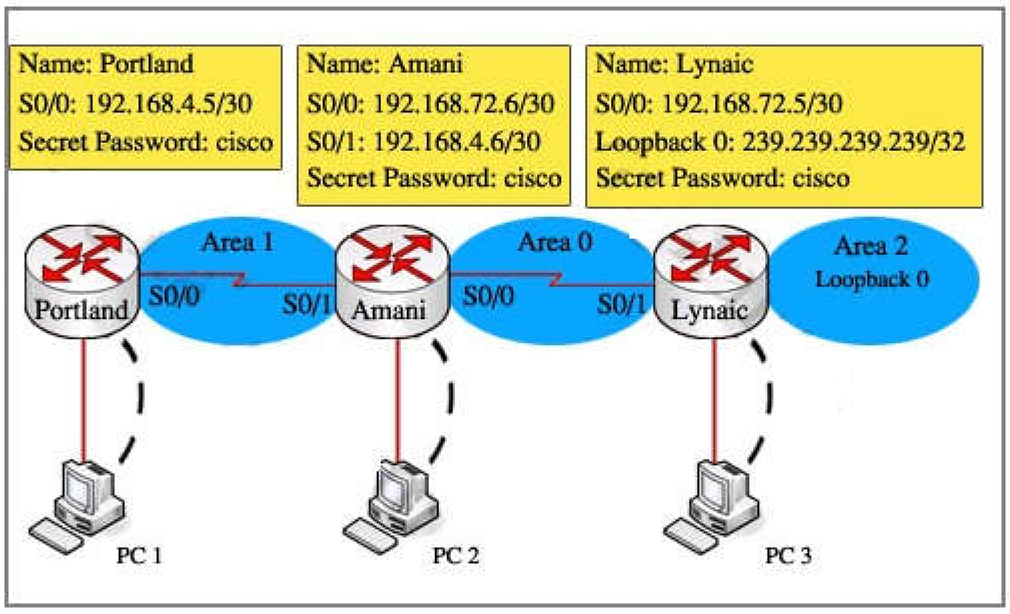
Correct Answer: See explanation below
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
R2#show interface s0/0/0
Bandwidth=1544 Kbit, Delay=20000 us, Reliability=255, Load=1, MTU=1500 bytes
R2#config terminal
R2(config)# router ospf 1
R2(config-router)# redistribute eigrp 100 metric-type 1 subnets
R2(config-router)#exit
R2(config-router)#router eigrp 100
R2(config-router)#redistribute ospf 1 metric 1544 2000 255 1 1500

R3#show interface fa0/0
Bandwidth=10000 Kbit, Delay=1000 us, Reliability=255, Load=1, MTU=1500 bytes
R3#config terminal
R3(config)#router ospf 1
R3(config-router)#redistribute eigrp 100 metric-type 1 subnets
R3(config)#exit
R3(config-router)#router eigrp 100
R3(config-router)#redistribute ospf 1 metric 10000 100 255 1 1500

If the link between R2 and R3 is FastEthernet link
R2(config-router)# distance eigrp 90 105

QUESTION 504
SIMULATION
OSPF Sim



OSPF is configured on routers Amani and Lynaic. Amani’s S0/0 interface and Lynaic‘s S0/1 interface are in Area 0. Lynaic‘s Loopback0 interface is in Area 2.

Your task is to configure the following:
Portland’s S0/0 interface in Area 1 Amani’s S0/1 interface in Area 1 Use the appropriate mask such that ONLY Portland’s S0/0 and Amnani’s S0/1 could be in Area 1. Area 1 should not receive any external or inter-area routes (except the default route).

Correct Answer: See explanation below
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
+ Configure Portland router as a stub:

```
Portland#configure terminal
Portland(config)#router ospf 1
```

Allow network 192.168.4.4/30 to join Area 1, notice that you have to convert subnet mask into wildcard mask:

```
Portland(config-router)#network 192.168.4.4 0.0.0.3 area 1
```

Configure Portland as a stub:

```
Portland(config-router)#area 1 stub
Portland#copy running-config startup-config
```

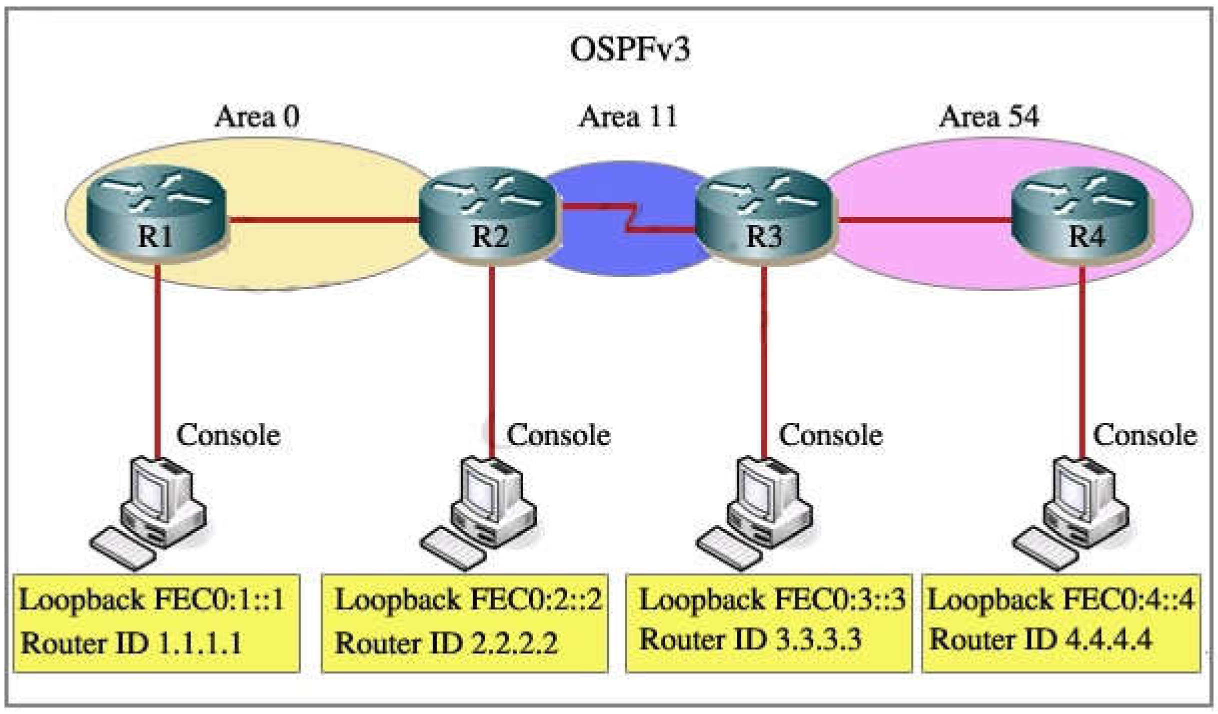
+ Configure Amani router as a “totally stub”:

```
Amani#configure terminal
Amani(config)#router ospf 1
Amani(config-router)#network 192.168.4.4 0.0.0.3 area 1
```

Make area 1 become a totally stubby area, notice that we can only use this command on ABR router:

```
Amani(config-router)#area 1 stub no-summary

Amani#copy running-config startup-config
```

QUESTION 505
SIMULATION
IPv6 OSPF Virtual Link



Acme is a small export company that has an existing enterprise network that is running IPv6 OSPFv3. Currently OSPF is configured on all routers. However, R4‘s loopback address (FEC0:4:4) cannot be seen in R1‘s IPv6 routing table. You are tasked with identifying the cause of this fault and implementing the needed corrective actions that uses OSPF features and does no change the current area assignments. You will know that you have corrected the fault when R4‘s loopback address (FEC0:4:4) can be seen in the routing table of R1.

Correct Answer: See explanation below
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

```
R2>enable
R2#configure terminal
R2(config)#ipv6 router ospf 1
R2(config-rtr)#area 11 virtual-link 3.3.3.3
```

(Notice that we have to use neighbor router-id 3.3.3.3, not R2’s router-id 2.2.2.2)
+ Configure virtual link on R3 (from the second output above, we learned that the OSPF process ID of R3 is 1 and we have to disable the wrong configuration of “area 54 virtual-link 4.4.4.4”):

```
R3>enable
R3#configure terminal
R3(config)#ipv6 router ospf 1
R3(config-rtr)#no area 54 virtual-link 4.4.4.4
R3(config-rtr)#area 11 virtual-link 2.2.2.2
```

We should check the configuration on R4:

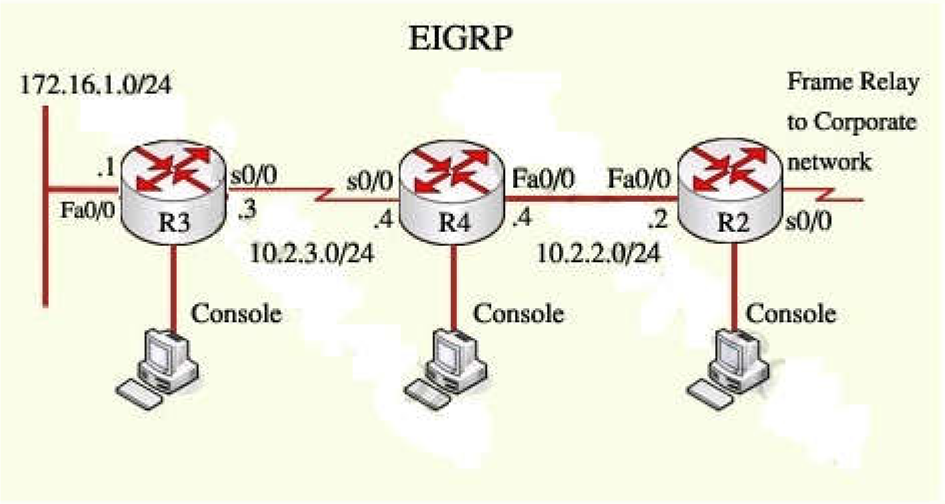
```
R4>enable
R4#show running-config
```

You will see a wrongly configured virtual-link command. To get full mark we have to disable this command:

```
R4#configure terminal
R4(config)#ipv6 router ospf 1
R4(config-rtr)#no area 54 virtual-link 3.3.3.3
```

QUESTION 506
SIMULATION

EIGRP Stub Sim



By increasing the first distant office, JS manufactures has extended their business. They configured the remote office router (R3) from which they can reach all Corporate subnets. In order to raise network stableness and lower the memory usage and broadband utilization to R3, JS manufactures makes use of route summarization together with the EIGRP Stub Routing feature. Another network engineer is responsible for the implementing of this solution. However, in the process of configuring EIGRP stub routing connectivity with the remote network devices off of R3 has been missing.
Presently JS has configured EIGRP on all routers in the network R2, R3, and R4. Your duty is to find and solve the connectivity failure problem with the remote office router R3. You should then configure route summarization only to the distant office router R3 to complete the task after the problem has been solved.
The success of pings from R4 to the R3 LAN interface proves that the fault has been corrected and the R3 IP routing table only contains two 10.0.0.0 subnets.

Correct Answer: See explanation below
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Notice that R3 is configured as a stub receive-only router. The **receive-only** keyword will restrict the router from sharing any of its routes with any other router in that EIGRP autonomous system. This keyword will also prevent any type of route from being sent.
Therefore, we will remove this command and replace it with the **eigrp stub** command:

```
R3#configure terminal
R3(config)#router eigrp 123
R3(config-router)#no eigrp stub receive-only
R3(config-router)#eigrp stub
R3(config-router)#end
```

Because we want the routing table of R3 only have 2 subnets so we have to summary sub-networks at the interface which is connected with R3, the s0/0 interface of R4.

```
R4>enable
R4#configure terminal
R4(config)#interface s0/0
R4(config-if)#ip summary-address eigrp 123 10.2.0.0 255.255.0.0
```

Now we jump back to R3 and use the **show ip route** command to verify the effect
But in your real exam, if you see the line “10.0.0.0/8 is a summary,….Null0” then you need to summary using the network 10.0.0.0/8 with the command “ip summary-address eigrp 123 10.0.0.0 255.0.0.0” . This configuration is less optimize than the first but it summaries into 2 subnets as the question requires (maybe you will not see this case, don’t worry!).

QUESTION 507
What command allows permit or deny IPv6 traffic?

A. ipv6 traffic-filter access-list-name { in | out }
B. ipv6 access-list [access-list-name]
C. access-list ipv6 [access-list-name]
D. ipv6 access-group [access-list-name] { in | out }

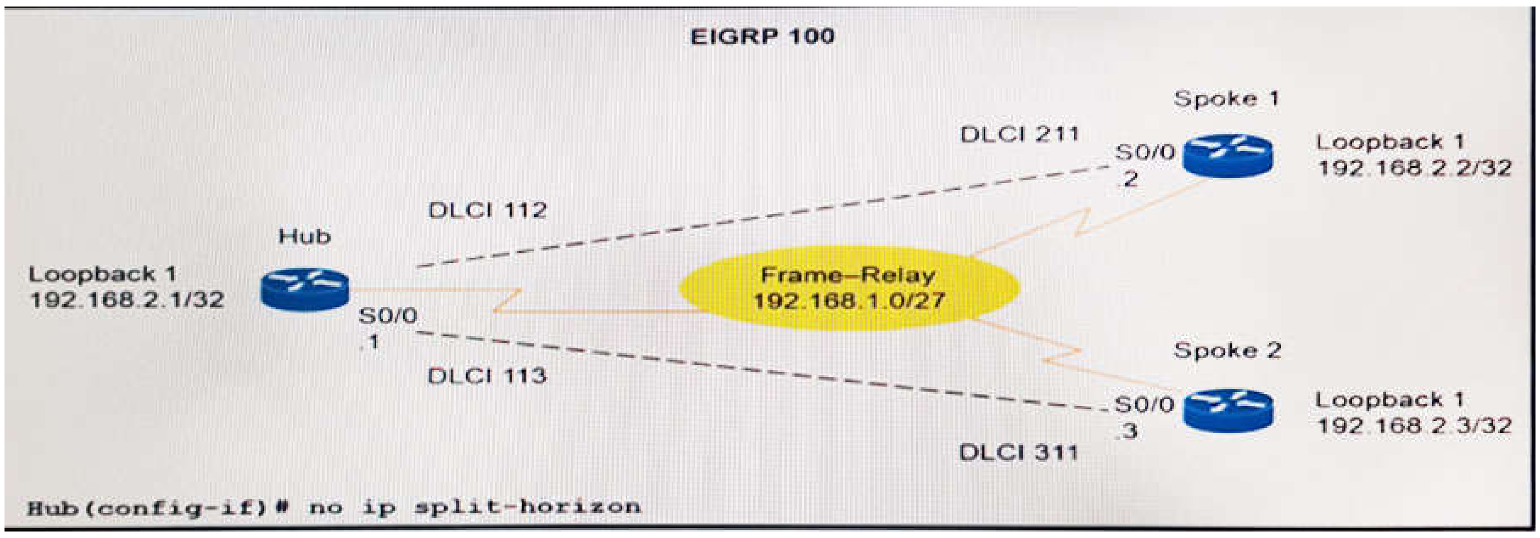
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The command “ipv6 traffic-filter access-list-name { in | out }” applies the access list to incoming or outgoing traffic on the interface.

Reference:
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/12-2_55_se/configuration/guide/scg3750/swv6acl.html

QUESTION 508



```
Hub(config-if)# no ip split-horizon
```

Refer to the exhibit. A network engineer is working on the network topology and executes the command no ip split-horizon on interface SO/0 of the hub router. What is the result of this command?

A. The spoke routers can see the routers are advertised by the hub router.
B. Each of the spoke routers can see the routers that are advertised from the other spoke routers.
C. A routing loop is created.
D. The hub router can see the routes that are advertised by the spoke routers.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 509
Which technology uses the many-to-one method of mapping IP addresses?

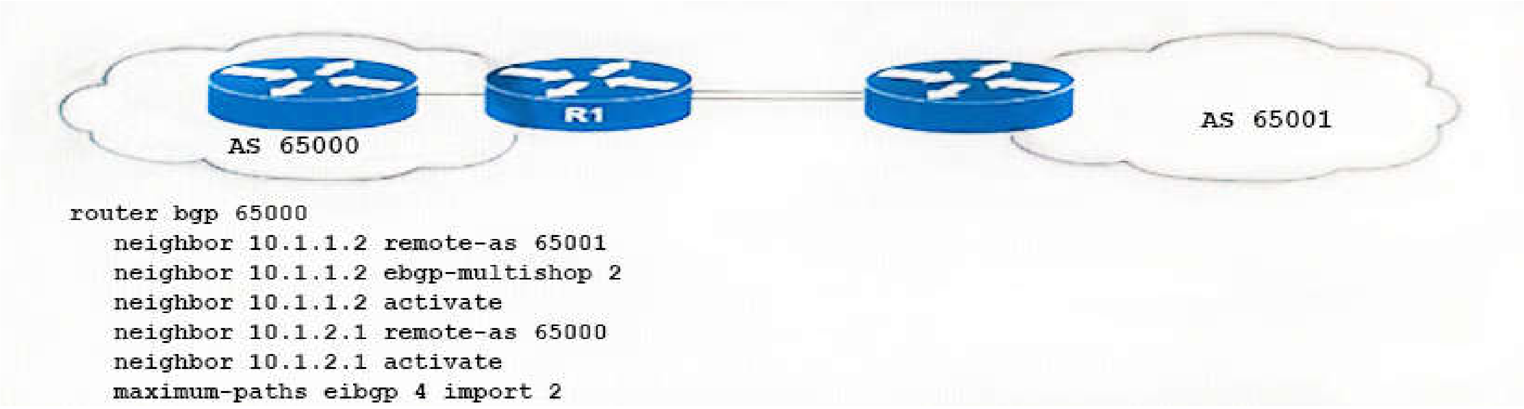
A. dynamic NAT
B. PAT
C. NAT-PT
D. static NAT

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Overloading--Maps multiple unregistered IP addresses to a single registered IP address (many to one) using different ports.
This method is also known as Port Address Translation (PAT).
By using overloading, thousands of users can be connected to the Internet by using only one real global IP address

QUESTION 510



```
router bgp 65000
   neighbor 10.1.1.2 remote-as 65001
   neighbor 10.1.1.2 ebgp-multishop 2
   neighbor 10.1.1.2 activate
   neighbor 10.1.2.1 remote-as 65000
   neighbor 10.1.2.1 activate
   maximum-paths eibgp 4 import 2
```

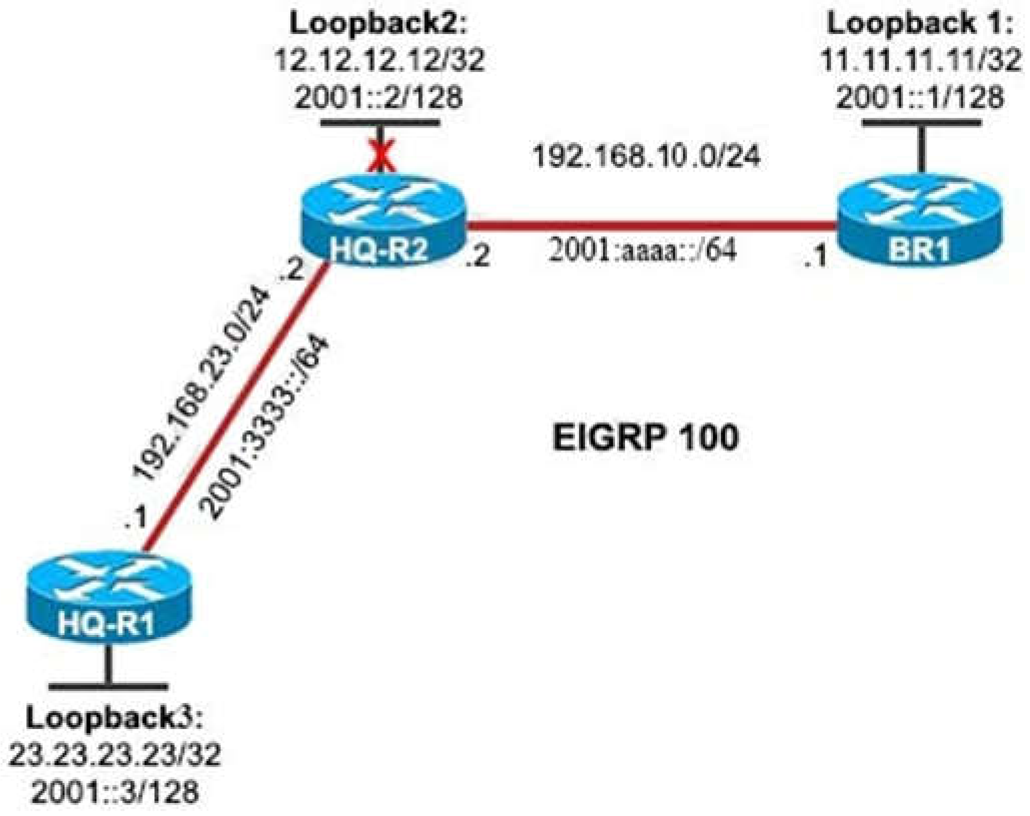
Refer to the exhibit. After you apply this configuration to router R1, it fails to establish an eBGP neighbor relationship with R2. Which action do you take to correct the problem?

A. Configure the **update-source** for 10.1.1.2.
B. replace the **maximum-paths** command at the end of the configuration with **maximum-paths ibgp 4 import 2.**
C. Change the **ebgp-multihop value to 1.**
D. Add the **no synchronization** statement at the end of the configuration.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 511



Refer to the exhibit. All interfaces on each router are participating in the EIGRP 100 process. Interface Loopback 2 on NQ-R2 is currently in shutdown mode. An engineer issues the **eigrp stub** command on router BR1. Which statement about the query messages sent from router HQ-R2 for a route to reach the 12.12.12.12/32 network is true?

A. Router HQ-R1 receives query messages from HQ-R2 for a route to 12.12.12.12/32 network.
B. Router HQ-R1 and BR1 receives query massages from HQ-R2 for a route 12.12.12.12/32 network.
C. Router HQ-R2 sends a query message to the feasible successor for a route to 12.12.12.12/32 network
D. BR1 receives query messages from HQ-R2 for route to 12.12.12.12/32 network

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 512
A network engineer executes the command **show ip eigrp vrf purple topology**. Which type of information is displayed as a result?

A. route successors for a specific routing table
B. routes for a global routing table
C. active neighbors for a global routing table
D. updates that were sent for a specific routing table

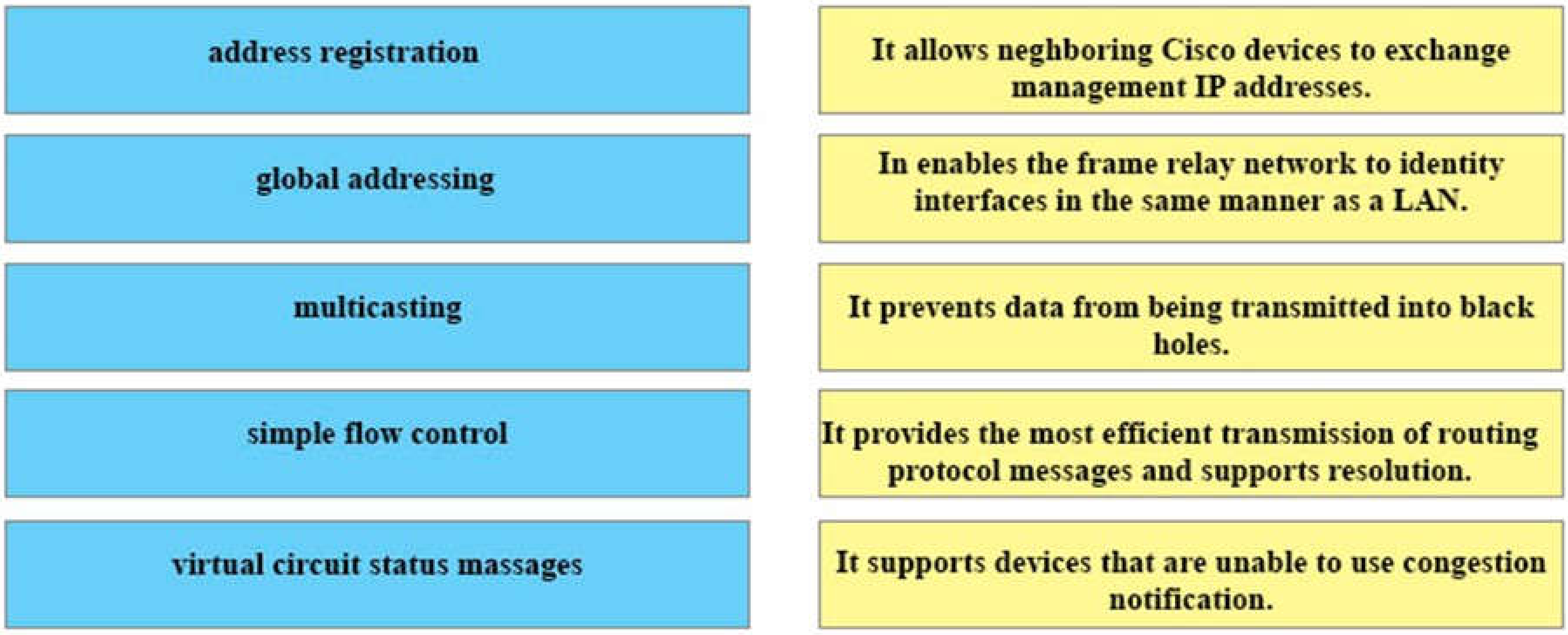
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 513
DRAG DROP

Drag and drop the Frame Relay LMI extensions from the left onto the correct descriptions on the right.

Select and Place:



address registration

global addressing

multicasting

simple flow control

virtual circuit status massages

It allows neghboring Cisco devices to exchange management IP addresses.

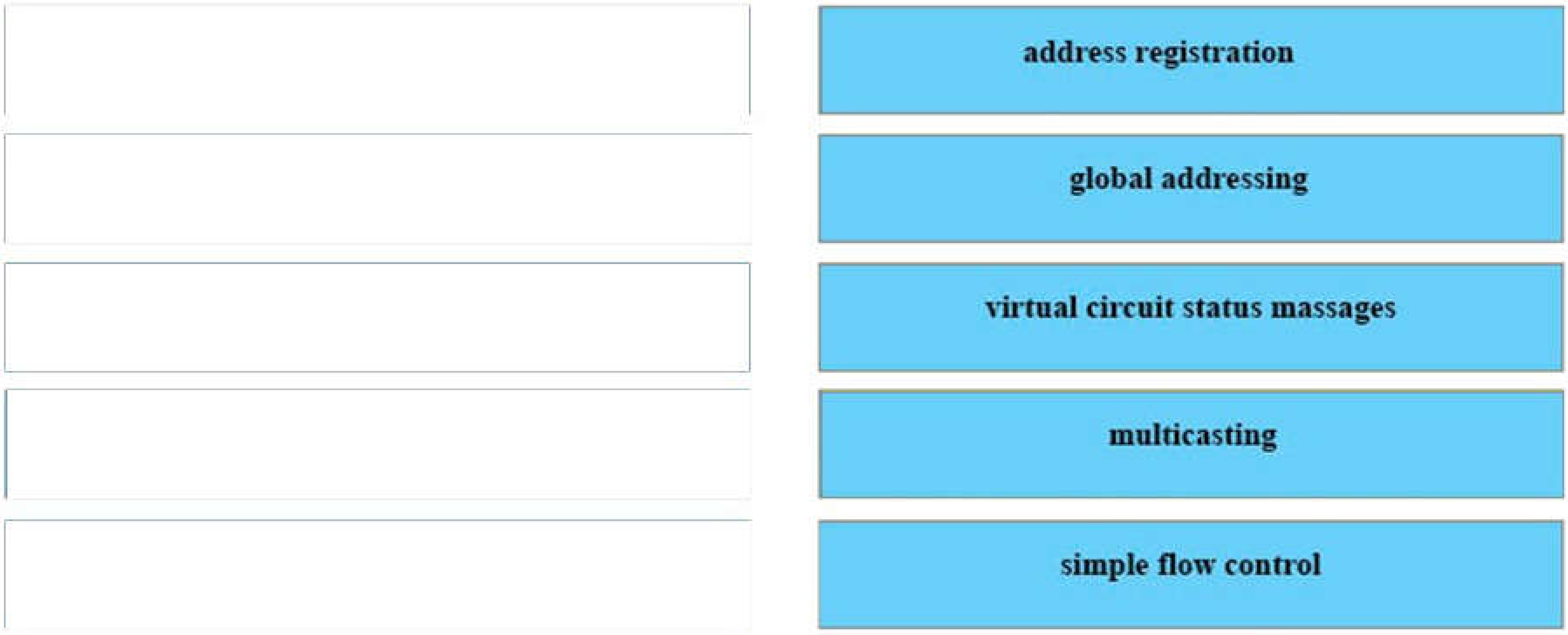
In enables the frame relay network to identity interfaces in the same manner as a LAN.

It prevents data from being transmitted into black holes.

It provides the most efficient transmission of routing protocol messages and supports resolution.

It supports devices that are unable to use congestion notification.

Correct Answer:



address registration

global addressing

virtual circuit status massages

multicasting

simple flow control

Section: Mix Questions
Explanation

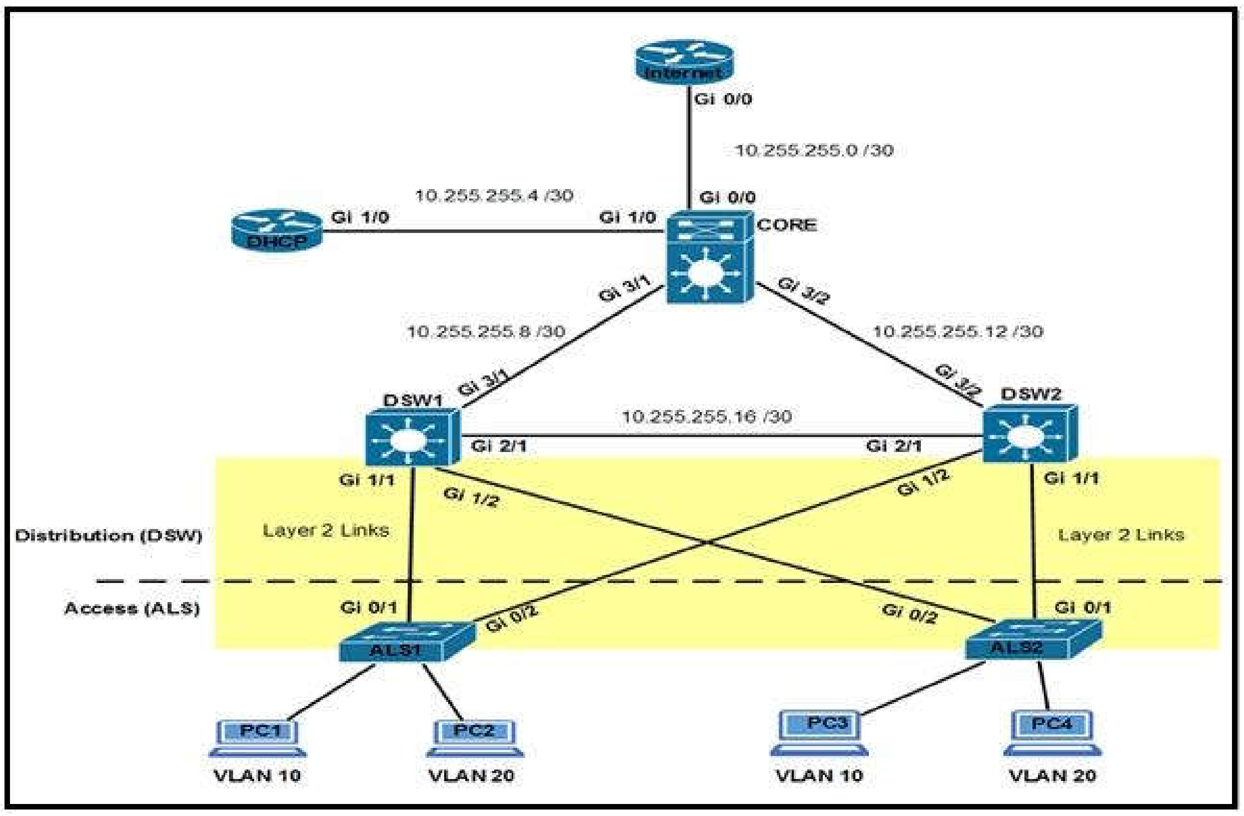
Explanation/Reference:
Explanation:

LMI Extensions
In addition to the basic Frame Relay protocol functions for transferring data, the consortium Frame Relay specification includes LMI extensions that make supporting large, complex internetworks easier. Some LMI extensions are referred to as "common" and are expected to be implemented by everyone who adopts the specification. Other LMI functions are referred to as "optional." A summary of the LMI extensions follows:

- **Virtual circuit status messages (common)**—Provide communication and synchronization between the network and the user device, periodically reporting the existence of new PVCs and the deletion of already existing PVCs, and generally provide information about PVC integrity. Virtual circuit status messages prevent the sending of data into black holes—that is, over PVCs that no longer exist.
- **Multicasting (optional)**—Allows a sender to transmit a single frame but have it delivered by the network to multiple recipients. Thus, multicasting supports the efficient conveyance of routing protocol messages and address resolution procedures that typically must be sent to many destinations simultaneously.
- **Global addressing (optional)**—Gives connection identifiers global rather than local significance, allowing them to be used to identify a specific interface to the Frame Relay network. Global addressing makes the Frame Relay network resemble a local-area network (LAN) in terms of addressing; Address Resolution Protocols, therefore, perform over Frame Relay exactly as they do over a LAN.
- **Simple flow control (optional)**—Provides for an XON/XOFF flow control mechanism that applies to the entire Frame Relay interface. It is intended for devices whose higher layers cannot use the congestion notification bits and that need some level of flow control.

Reference: https://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1918.html

QUESTION 514



Refer to the exhibit. Which option prevents routing updates for 10.255.255.0/30 from being sent to the DHCP router, while still allowing all other routing update messages?

A.
```
Core(config)#access-list 10 deny 10.255.255.0.0.0.0.3
Core(config)#access-list 10 permit any
Core(config-router)#distribute-list 10 out interface Gi1/0
```

B.
```
DHCP(config)#access -list 10 deny 10.255.255.0.0.0.0.3
DHCP(config)#access-list 10 permit any
DHCP(config-if)#distribute-list 10 in interface Gi1/0
```

C.
```
Core(config)#access -list 10 deny 10.255.255.0.0.0.0.3
Core(config)#access-list 10 permit any
Core(config-if)#distribute-list 10 out interface Gi1/0
```

D.
```
DHCP(config)#access -list 10 deny 10.255.255.0.0.0.0.3
DHCP(config)#access-list 10 permit any
DHCP(config-router)#distribute-list 10 out interface Gi1/0
```

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 515
A network engineer configured an IOS router to send syslog messages to a Window syslog server. Several events occurred on the IOS router, and the network engineer noticed that Windows syslog server had not received any messages from the IOS router. What is the reason for this?

A. Either a firewall between the two devices or an ACL on the router is blocking TCP port 514.
B. Either a firewall between the two devices or an ACL on the router is blocking UDP port 514.
C. Either a firewall between the two devices or an ACL on the router is blocking IP protocol number 514.
D. Either a firewall between the two devices or an ACL on the router is blocking UDP port 512.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 516
Which two configurations can a PPPoE client support? (Choose two.)

A. The client is connected to multiple hosts over DMVPN.
B. The client is connecting over an ATM PVC/
C. The client is installed on a native IPv6 network.
D. Eight clients are configured on a single CPE.
E. The client is installed on the same network device as the server.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Restrictions for PPP over Ethernet Client

The PPPoE client does not support the following:
• More than ten clients per customer premises equipment (CPE)
• Quality of service (QoS) transmission with queueing on the dialer interface
• Dial-on-demand
• Easy VPN
• Native IPv6
• PPPoE client over ATM permanent virtual circuit (PVC)
• Coexistence of the PPPoE client and server on the same device
• Multilink PPP (MLP) on dialer interfaces
• Nonstop forwarding (NSF) with stateful switchover (SSO)
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bbdsl/configuration/xe-3s/bba-xe-3s-book/bba-pppoe-client-xe.pdf

QUESTION 517
Which Cisco Express Forwarding table or tables hold forwarding information?

A. FIB and adjacency tables only
B. adjacency tables only
C. FIB, RIB, and adjacency tables
D. FIB table only

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Information conventionally stored in a route cache is stored in several data structures for Cisco Express Forwarding switching.
The data structures provide optimized lookup for efficient packet forwarding. The two main components of Cisco Express Forwarding operation are the forwarding information base (FIB) and the adjacency tables.

The FIB is conceptually similar to a routing table or information base. A router uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation. The FIB is updated when changes occur in the network and contains all routes known at the time. For more information, see the FIB Overview section.

Adjacency tables maintain Layer 2 next-hop addresses for all FIB entries. For more information, see the CEF Adjacency Tables Overview section.
This separation of the reachability information (in the Cisco Express Forwarding table) and the forwarding information (in the adjacency table), provides a number of benefits:
The adjacency table can be built separately from the Cisco Express Forwarding table, allowing both to be built without any packets being process-switched.
The MAC header rewrite used to forward a packet is not stored in cache entries, so changes in a MAC header rewrite string do not require validation of cache entries.
Reference:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/15-mt/isw-cef-15-mt-book/isw-cef-overview.html

QUESTION 518
A network engineer is configuring a DHCP server to support a specialized application. Which additional DHCP feature must be enabled to support the delivery of various additional parameters to DHCP clients?

A. vendor extensions
B. modules
C. options
D. scopes

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 519
Which two statements about Frame Relay LMI autosense are true on a Router? (Choose two.)

A. It operates when the line is up but the line protocol is down.
B. It requires the line protocol to be up.
C. It operates on Frame relay DTE interfaces.
D. It requires the LMI type to be explicitly configured.
E. It operates on frame Relay DCE interfaces.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

LMI autosense is automatically enabled in the following situations:

+ The router is powered up or the interface changes state to up
+ The line protocol is down but the line is up
+ The interface is a Frame Relay DTE
+ The LMI type is not explicitly configured on the interface

https://www.cisco.com/c/en/us/td/docs/ios/12_2/wan/configuration/guide/fwan_c/wcffrely.html

QUESTION 520
What does the number 16 in the following command represent?

```
router (config)#snmp-server user abcd public v2c access 16
```

A. the user ID that is allowed to use the community string public
B. the number of concurrent users who are allowed to query the SNMP community
C. the mask of the files that are allowed to use community string public.
D. the standard named access list 16, which contains the access rules that apply to user abcd

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 521
What is the function of the **snmp-server enable traps** and **snmp-server host 192.168.1.3 traps version 2c public** commands?

A. to allow private communications between the router and the host
B. to disable all SNMP informs that are on the system
C. to collect information about the system on a network management server
D. to allow only 192.168.1.3 to access the system using the community string public.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 522
Which two options for authenticating a user who is attempting to access a network device are true? (Choose two.)

A. PAP
B. 802.1x
C. CHAP
D. TACACS+
E. RADIUS

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 523
Which three statements about IPv6 EIGRP are true? (Choose three.)

A. EIGRP neighbor relationships can be formed only on the configured IPv6 address.
B. It supports EUI-64 addresses only.
C. EIGRP route advertisement is configured under the interface configuration.
D. EIGRP neighbor relationships are formed using the link-local address.
E. EIGRP route advertisement is configured under the **ipv6 router eigrp** configuration.
F. An IPv6 EIGRP router ID is required.

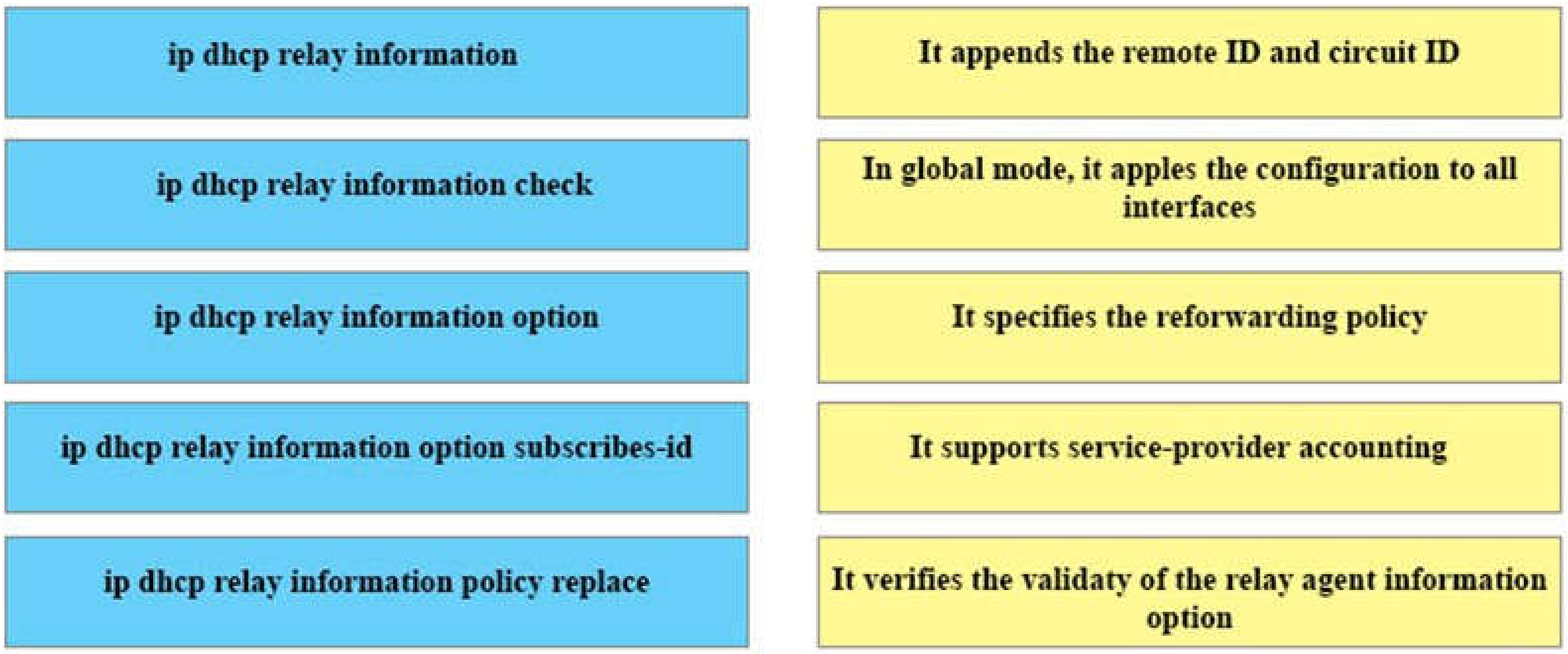
Correct Answer: CDF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 524
DRAG DROP

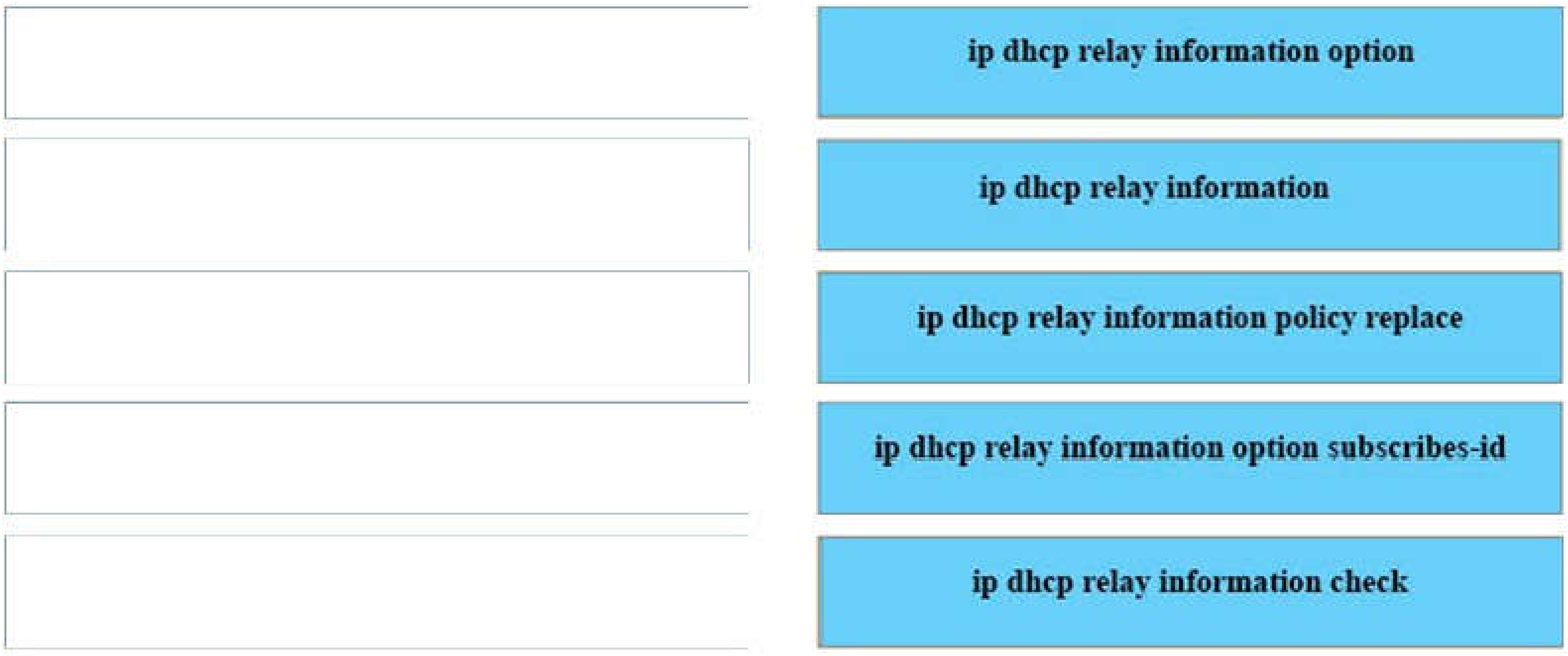
Drag and drop the Cisco IOS DHCP relay agent configuration commands from the left onto the correct effects on the right.

Select and Place:



ip dhcp relay information	It appends the remote ID and circuit ID
ip dhcp relay information check	In global mode, it apples the configuration to all interfaces
ip dhcp relay information option	It specifies the reforwarding policy
ip dhcp relay information option subscribes-id	It supports service-provider accounting
ip dhcp relay information policy replace	It verifies the validaty of the relay agent information option

Correct Answer:



	ip dhcp relay information option
	ip dhcp relay information
	ip dhcp relay information policy replace
	ip dhcp relay information option subscribes-id
	ip dhcp relay information check

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 525
The Neighbor Discovery Protocol in IPv6 replaces which protocol in IPv4?

A. ICMP
B. CDP
C. ARP
D. IGMP

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 526
Which two options are components of a dual stack? (Choose two.)

A. Layer 2 switch
B. IPv6 traffic
C. OSPF
D. Layer 3 switch
E. IPv4 traffic
F. EIGRP

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 527
If you convert a WAN connection with OSPF from T1 to a Frame relay circuit, which two actions must you take to enable the connection? (Choose two.)

A. Change the OSPF network type to multipoint nonbroadcast.
B. Change the OSPF network type to broadcast.
C. Manually configure the hello and dead timers.
D. Manually configure neighbors in the OSPF process.
E. Change the OSPF network type to nonbroadcast.

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Frame Relay is a non-broadcast multi-access (NBMA) environment so when migrating to a Frame Relay circuit we must change the OSPF network to non-broadcast. This type of network does not accept broadcast and muticast packets so we must manually configure neighbors for OSPF.

QUESTION 528
Which keyword of the **aaa authentication ppp** command applies to PAP only?

A. local
B. local-case
C. krb5
D. enable
E. Line

Correct Answer: C
Section: Mix Questions
Explanation

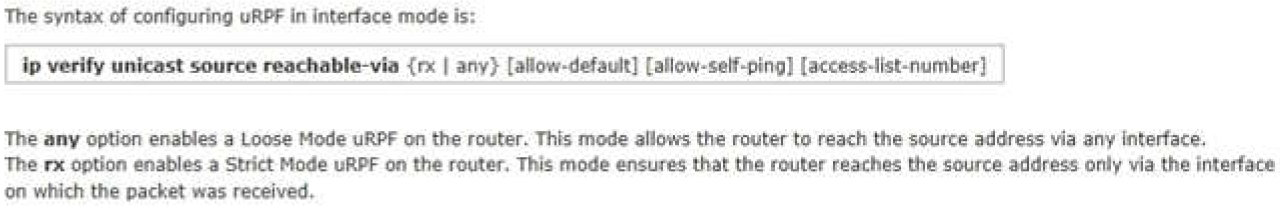
Explanation/Reference:

QUESTION 529
Which two statements about uRPF are true? (Choose two.)

A. It is enabled on a per-interface basis.
B. It is enabled globally.
C. Strict mode is most appropriate for networks with asymmetric routing.
D. Strict mode may drop legitimate traffic.
E. The keyword **any** can be used with both strict mode and loose mode.
F. Loose mode may drop traffic when asymmetric routing occurs on the network.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



The syntax of configuring uRPF in interface mode is:

```
ip verify unicast source reachable-via {rx | any} [allow-default] [allow-self-ping] [access-list-number]
```

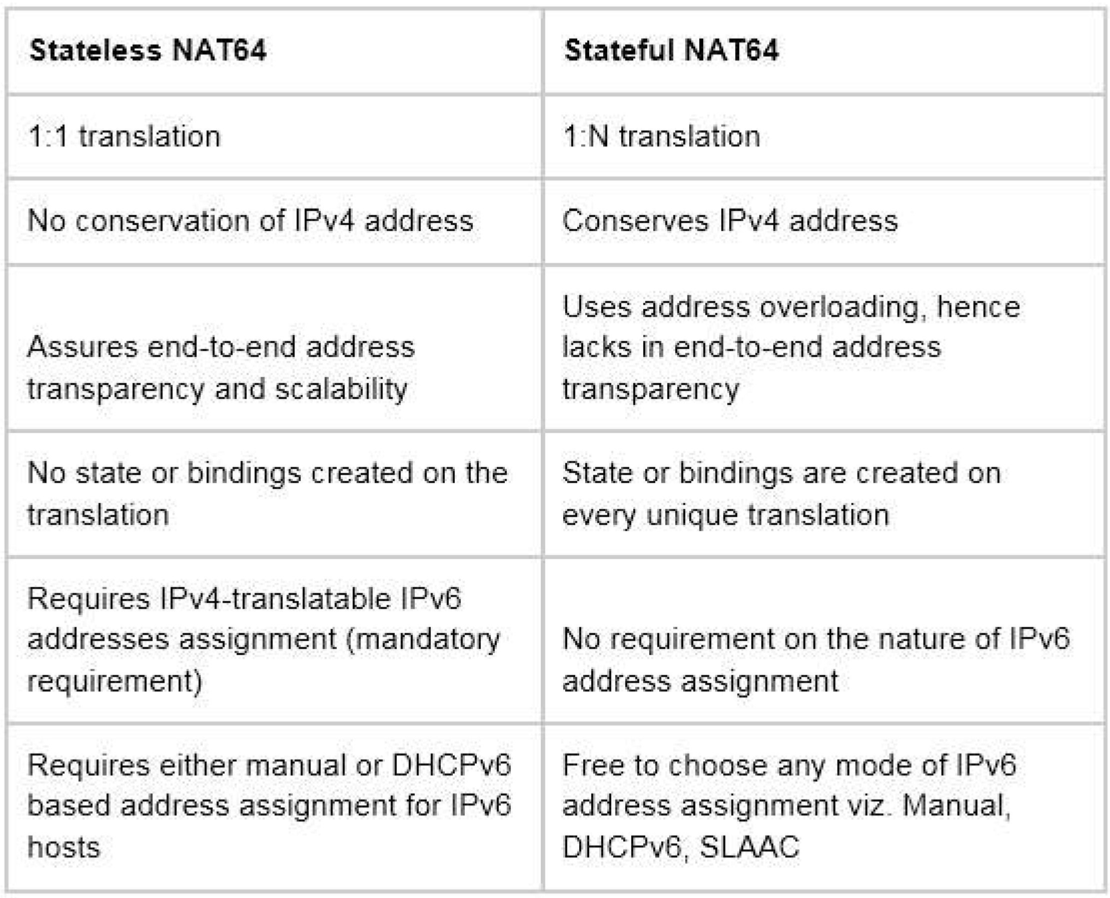
The **any** option enables a Loose Mode uRPF on the router. This mode allows the router to reach the source address via any interface.
The **rx** option enables a Strict Mode uRPF on the router. This mode ensures that the router reaches the source address only via the interface on which the packet was received.

QUESTION 530
Which three functionalities are specific to stateful NAT64? (Choose three.)

A. It requires IPv4-translatable IPv6 addresses.
B. It requires either manual or DHCPv6-based address assignment for IPv6 hosts.
C. It conserves IPv4 addresses.
D. It helps ensure end-to-end address transparency and scalability.
E. No constraint is put on the number of endpoints due to 1:N translation.
F. A state or bindings are created on every unique translation.

Correct Answer: CEF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Differences Between Stateless NAT64 and Stateful NAT64



Stateless NAT64	Stateful NAT64
1:1 translation	1:N translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment (mandatory requirement)	No requirement on the nature of IPv6 address assignment
Requires either manual or DHCPv6 based address assignment for IPv6 hosts	Free to choose any mode of IPv6 address assignment viz. Manual, DHCPv6, SLAAC

Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-676277.html

QUESTION 531
In SNMP v3, which security level provides encryption of the data?

A. noAuthNoPriv
B. authPriv
C. authMember
D. authNoPriv

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

+ noAuthNoPriv – Security level that does not provide authentication or encryption.
+ authNoPriv – Security level that provides authentication but does not provide encryption.
+ authPriv – Security level that provides both authentication and encryption.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.pdf

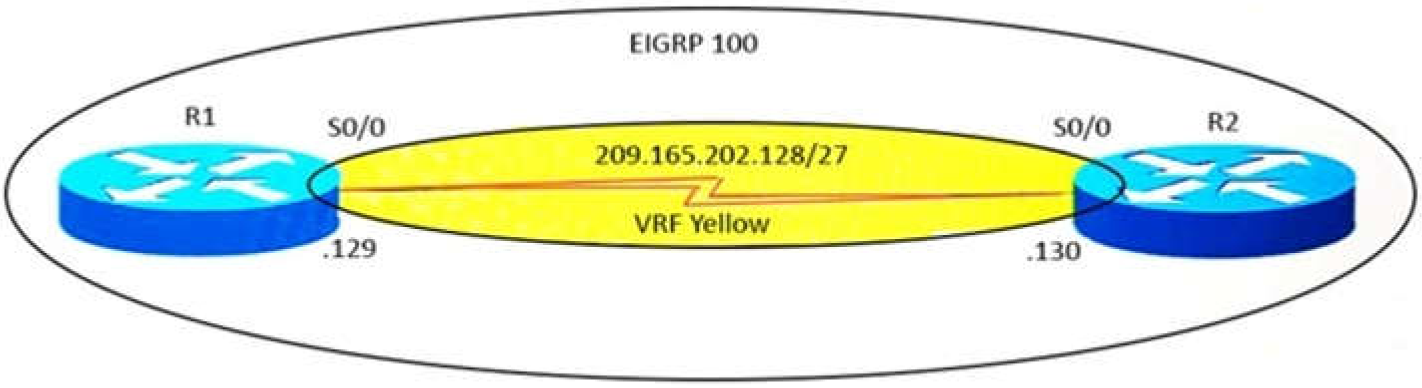
QUESTION 532
Which technology does Easy Virtual Network use?

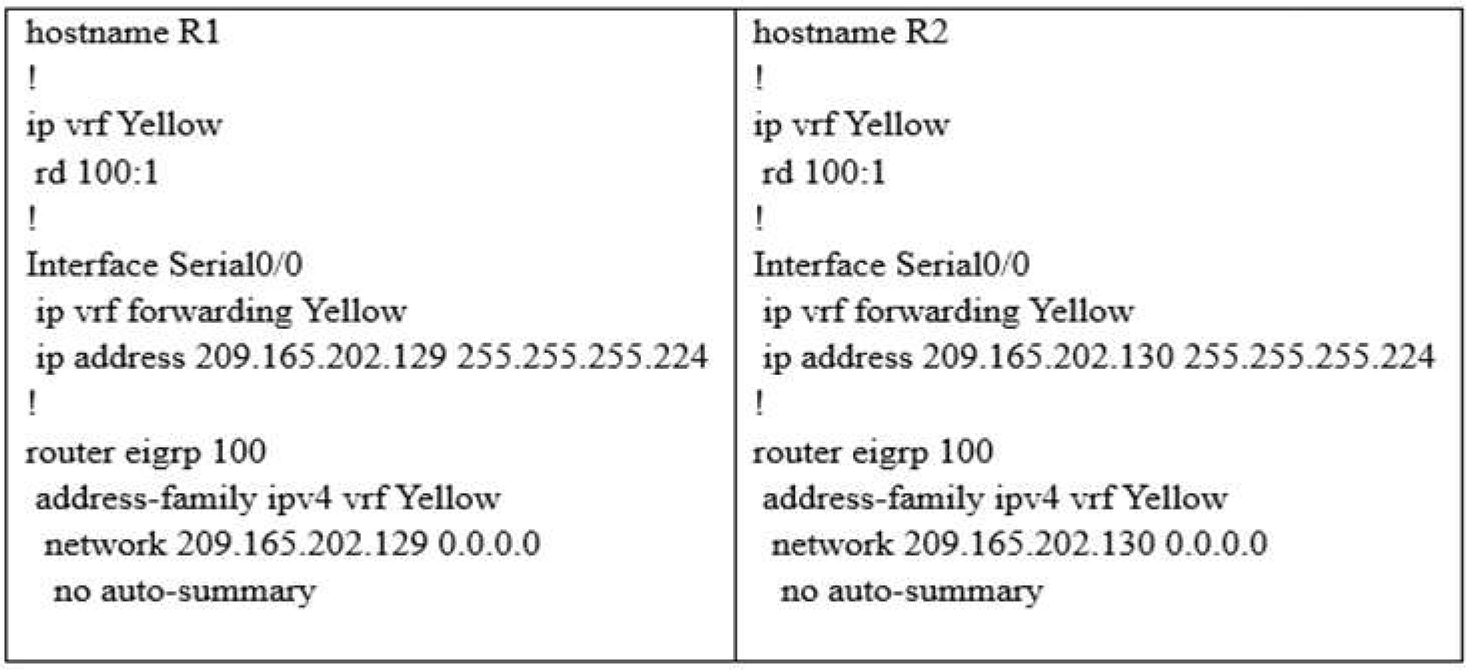
A. MP-BGP
B. MPLS
C. DMVPN
D. VRF-Lite

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 533





```
hostname R1
!
ip vrf Yellow
 rd 100:1
!
Interface Serial0/0
 ip vrf forwarding Yellow
 ip address 209.165.202.129 255.255.255.224
!
router eigrp 100
 address-family ipv4 vrf Yellow
  network 209.165.202.129 0.0.0.0
   no auto-summary
```

```
hostname R2
!
ip vrf Yellow
 rd 100:1
!
Interface Serial0/0
 ip vrf forwarding Yellow
 ip address 209.165.202.130 255.255.255.224
!
router eigrp 100
 address-family ipv4 vrf Yellow
  network 209.165.202.130 0.0.0.0
   no auto-summary
```

Refer to exhibit. A network engineer is unable to make VRF lite EIGRP adjacency work. There is nothing wrong with communication between R1 and R2. What command will eliminate the issue when executed on both routers?

A. (config-router-af)#network 209.165.202.128.0.0.0.31
B. (config)#ip multicast-routing
C. (config-router-af)#autonomous-system 100
D. (config-vrf)#route target both 100:1

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

To configure the autonomous-system number for EIGRP to run within a VPN routing and forwarding (VRF) instance, use the “autonomous-system” command in address-family configuration mode. In particular:

```
Router(config)# router eigrp 100
Router(config-router)# address-family ipv4 vrf Yellow
Router(config-router-af)# autonomous-system 100
```

QUESTION 534
Which value does a point-to-point GRE tunnel use to identity a peer?

A. VC ID
B. DLCI
C. IP address
D. configured multicast address
E. Mac address

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 535
Which type of NetFlow information is displayed when the **show ip flow export** command is executed?

A. export interface configurations
B. top talkers
C. sent status and statistics
D. local status and statistics

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 536
Which technology is required on an EVN trunk interface?

A. VRF-Lite
B. 802.1q
C. IS-IS
D. NAT

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
An EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.
Reference:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.pdf

QUESTION 537
A network engineer wants to baseline the network to determine suitability for real-time voice applications. Which IP SLA operation is best suited for this task?

A. ICMP -echo
B. UDP -connect
C. TCP -connect
D. ICMP -jitter
E. UDP -jitter
F. UDP -echo

Correct Answer: E
Section: Mix Questions
Explanation

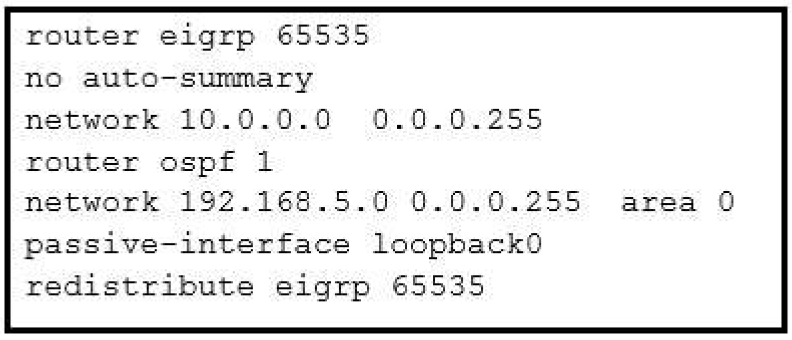
Explanation/Reference:
Explanation:
The IP SLAs VoIP UDP jitter operation accurately simulates VoIP traffic using common codecs and calculates consistent voice quality scores (MOS and ICPIF) between Cisco devices in the network.

Note:
+ UDP Jitter: generates UDP traffic and measures Round-trip Delay, One-way Delay, One-way Jitter, One-way Packet Loss, and overall Connectivity.
+ UDP-echo: measures Round-trip Delay for UDP traffic.

There is also a special “UDP Jitter for VoIP” which can simulate various codecs and spits out voice quality scores (MOS, and ICPIF)

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipsla/configuration/15-mt/sla-15-mt-book/sla_udp_jitter_voip.html

QUESTION 538
Refer to the exhibit.



```
router eigrp 65535
no auto-summary
network 10.0.0.0  0.0.0.255
router ospf 1
network 192.168.5.0 0.0.0.255  area 0
passive-interface loopback0
redistribute eigrp 65535
```

If this configuration is applied to a device that redistributes EIGRP routes into OSPF, which two statements about the behavior of the device are true? (Choose two.)

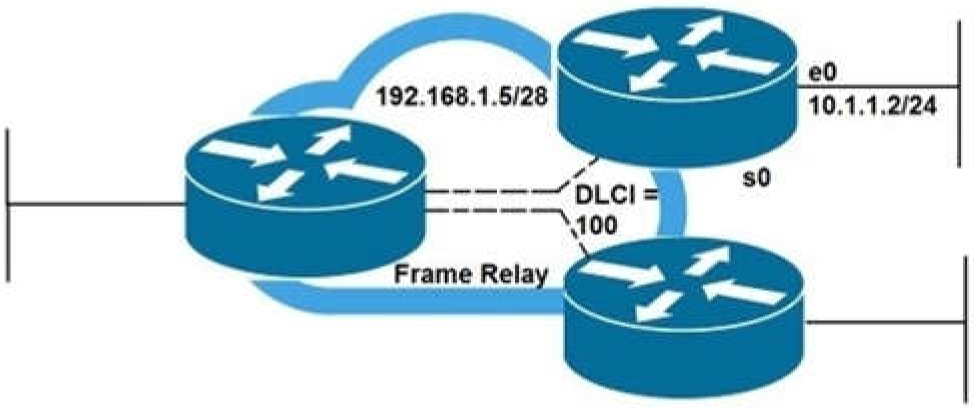
A. EIGRP routes appears in the routing table as N2 OSPF routes.
B. The device redistributes all EIGRP networks into OSPF.
C. The device redistributes only classful EIGRP networks into OSPF.
D. EIGRP routes appears in the routing table as E2 OSPF routes.
E. The device router ID is set to Loopback0 automatically.
F. EIGRP routes appears as type 3 LSAs in the OSPF database.

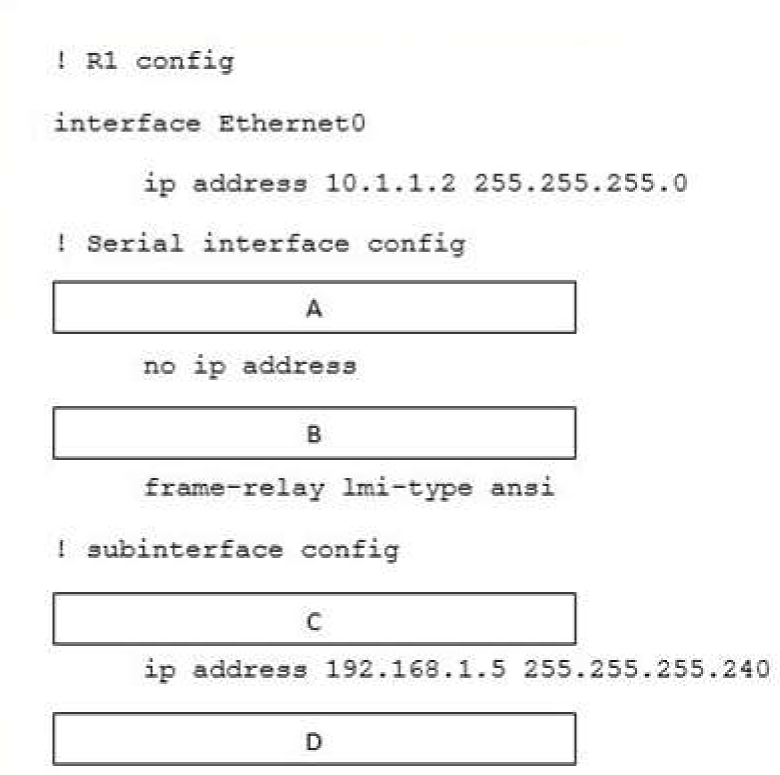
Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 539
DRAG DROP

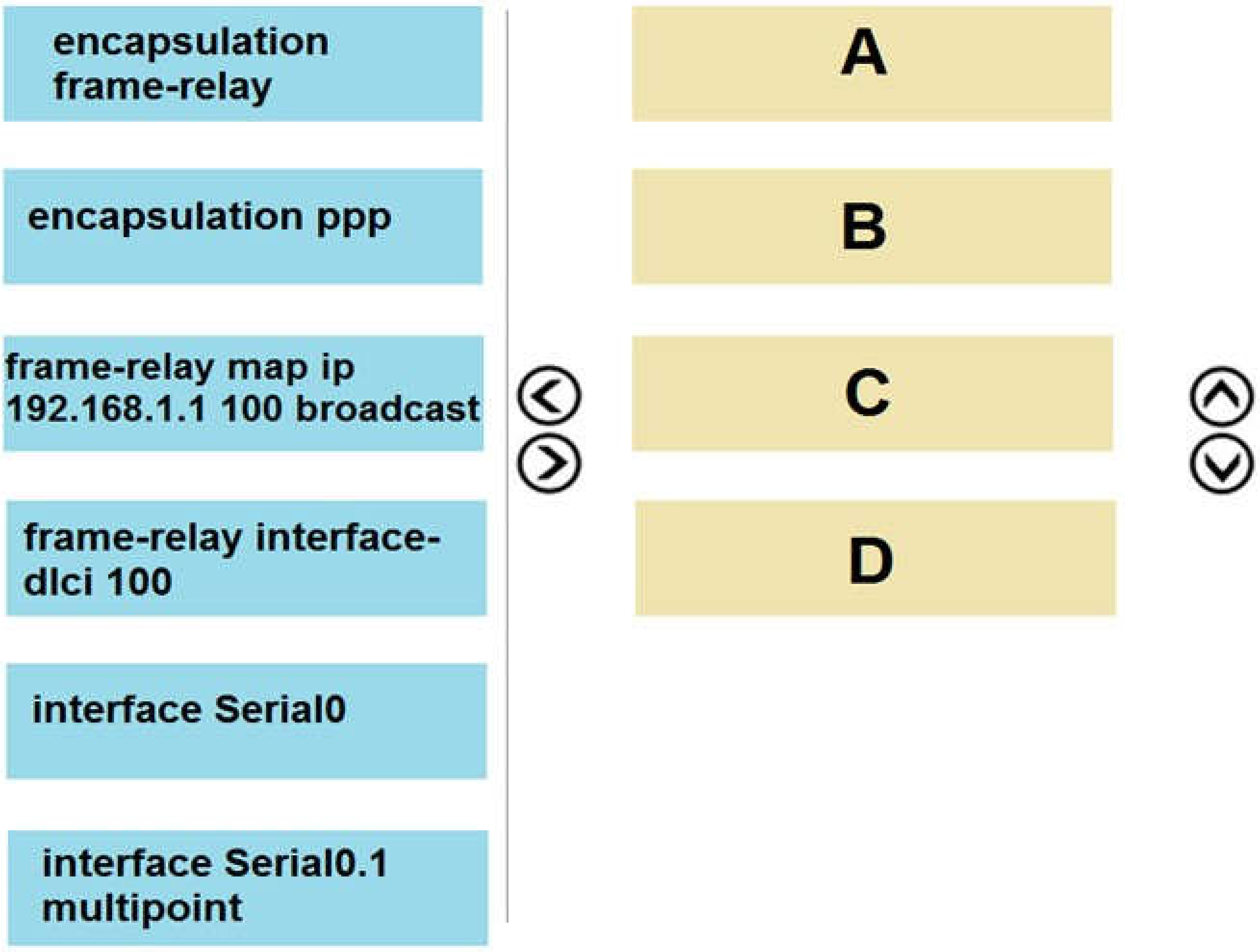
Refer to the exhibit. You are configuring the R1 Serial0 interface for a multipoint connection. Drag and drop the required configuration statements from the left onto the corresponding locations from the diagram on the right.





```
! R1 config
interface Ethernet0
      ip address 10.1.1.2 255.255.255.0
! Serial interface config
[                A                ]
      no ip address
[                B                ]
      frame-relay lmi-type ansi
! subinterface config
[                C                ]
      ip address 192.168.1.5 255.255.255.240
[                D                ]
```

Select and Place:



encapsulation frame-relay

encapsulation ppp

frame-relay map ip 192.168.1.1 100 broadcast

frame-relay interface-dlci 100

interface Serial0

interface Serial0.1 multipoint

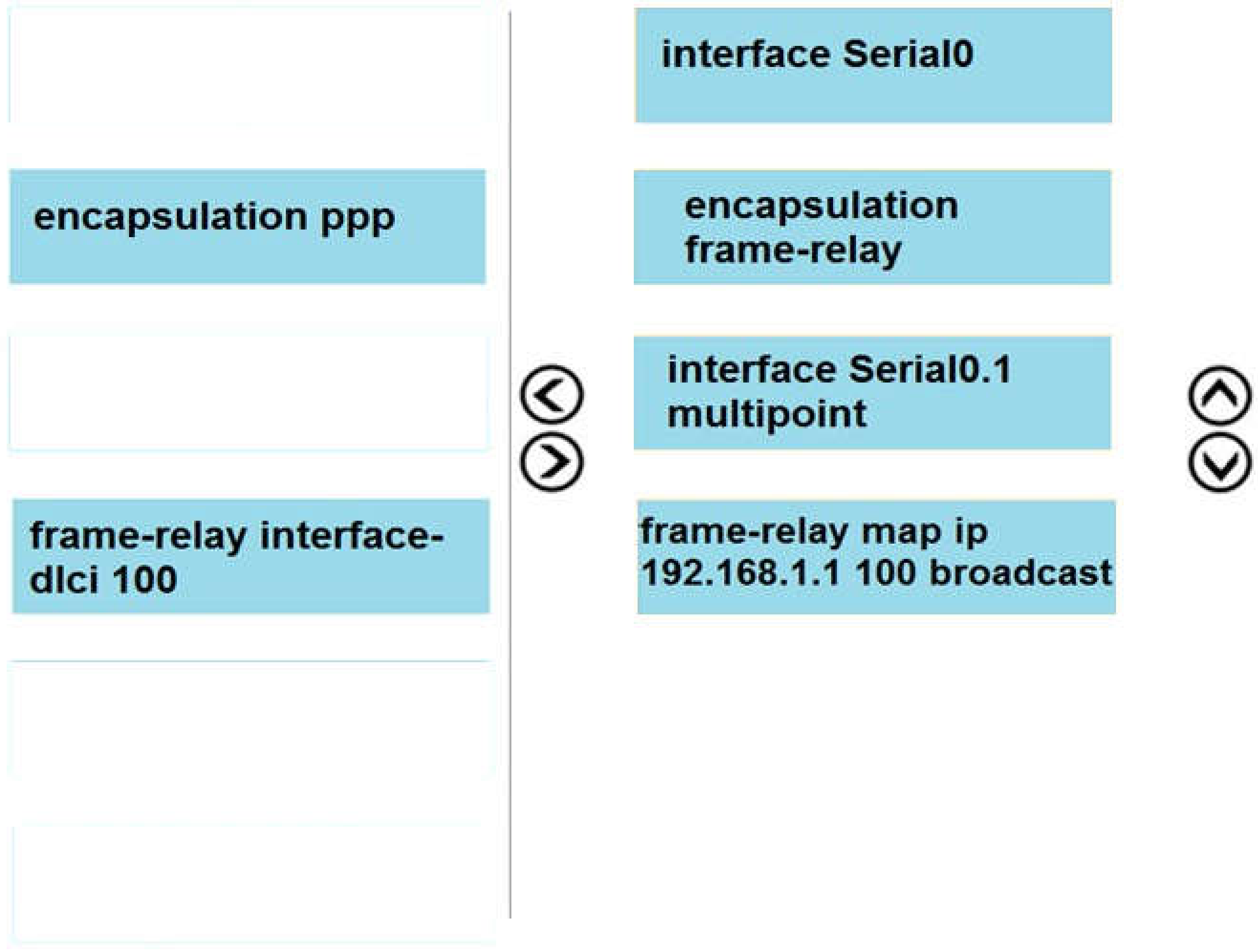
A

B

C

D

Correct Answer:



encapsulation ppp

frame-relay interface-dlci 100

interface Serial0

encapsulation frame-relay

interface Serial0.1 multipoint

frame-relay map ip 192.168.1.1 100 broadcast

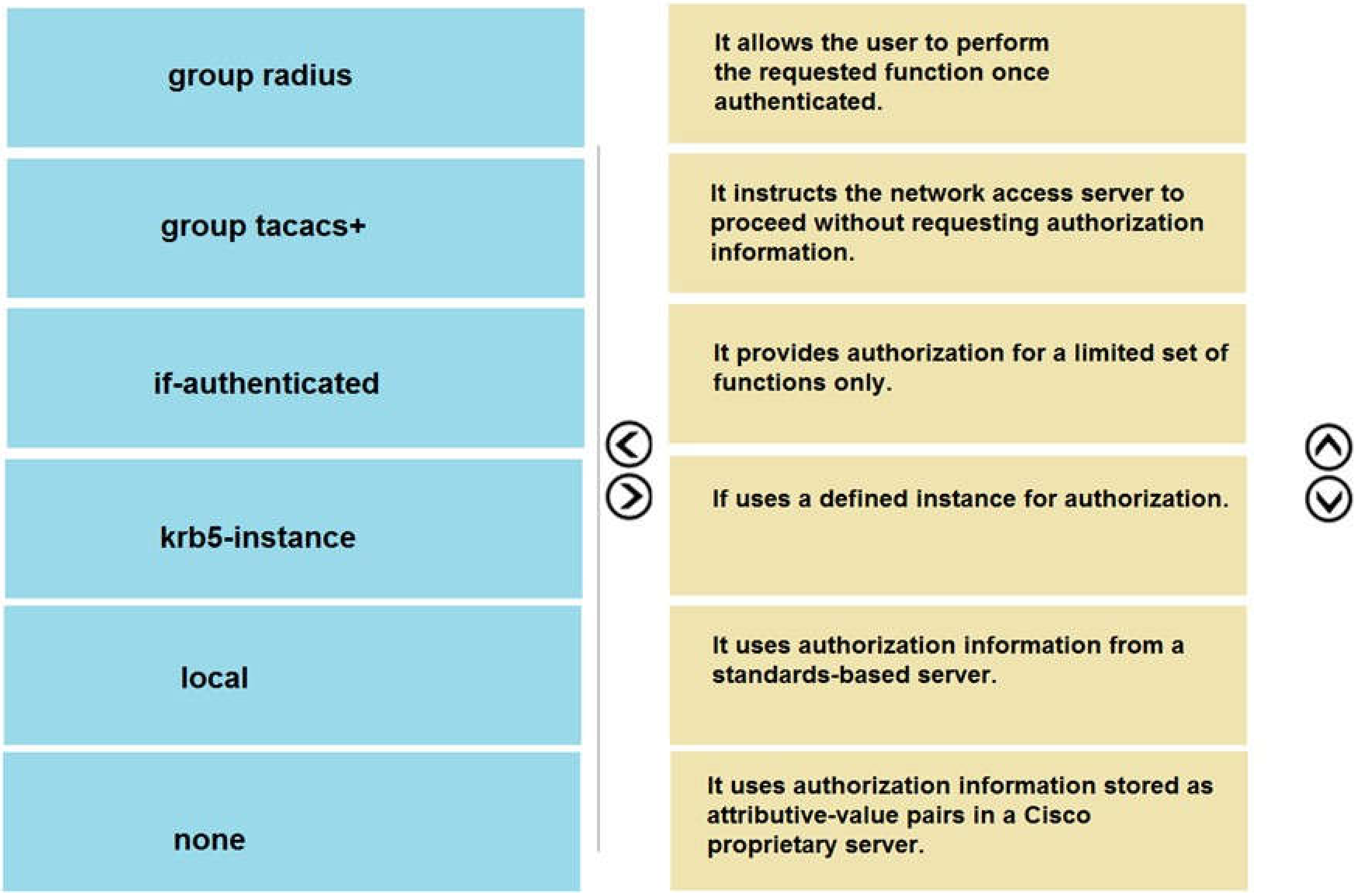
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
A - Interface serial 0
B - Encapsulation frame-relay
C – Interface serial 0.1 multipoint
D – frame-relay map ip 192.168.1.1 100 broadcast

QUESTION 540
DRAG DROP

Drag and drop the methods supported by the aaa authorization command from the left into the correct descriptions on the right.

Select and Place:



group radius

group tacacs+

if-authenticated

krb5-instance

local

none

It allows the user to perform the requested function once authenticated.

It instructs the network access server to proceed without requesting authorization information.

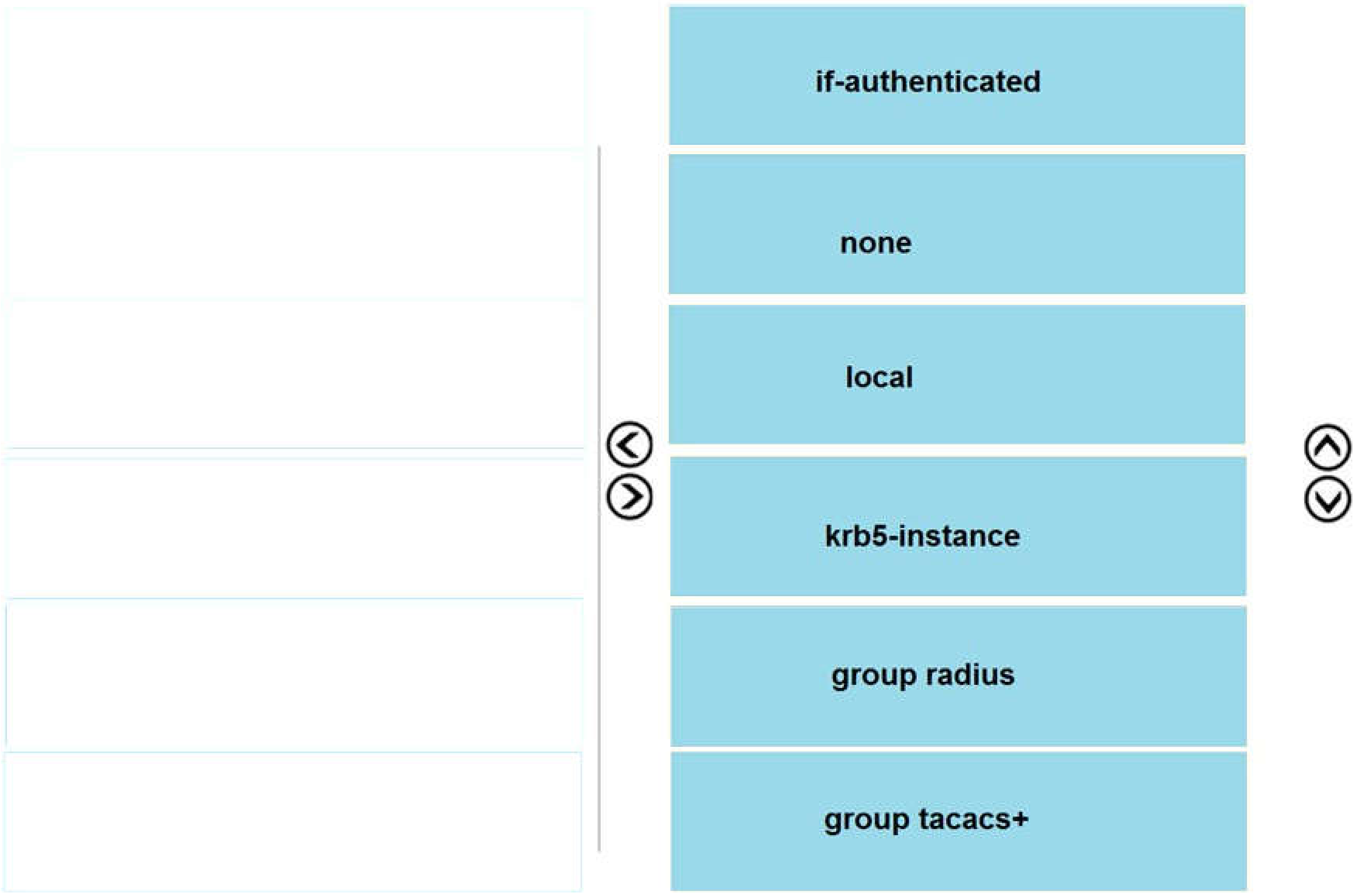
It provides authorization for a limited set of functions only.

If uses a defined instance for authorization.

It uses authorization information from a standards-based server.

It uses authorization information stored as attributive-value pairs in a Cisco proprietary server.

Correct Answer:



if-authenticated

none

local

krb5-instance

group radius

group tacacs+

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 541
Which statement describes what this command accomplishes when inside and outside interfaces are correctly identified for NAT?

ip nat inside static tcp 192.168.1.50 80 209.165.201.1 8080 extendable

A. It allows host 192.168.1.50 to access external websites using TCP port 8080.
B. It represents an incorrect NAT configuration because it uses standard TCP ports.
C. It allows external clients to connect to a web server hosted on 192.168.1.50.
D. It allows external clients coming from public IP 209.165.201.1 to connect to a web server at 192.168.1.50.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

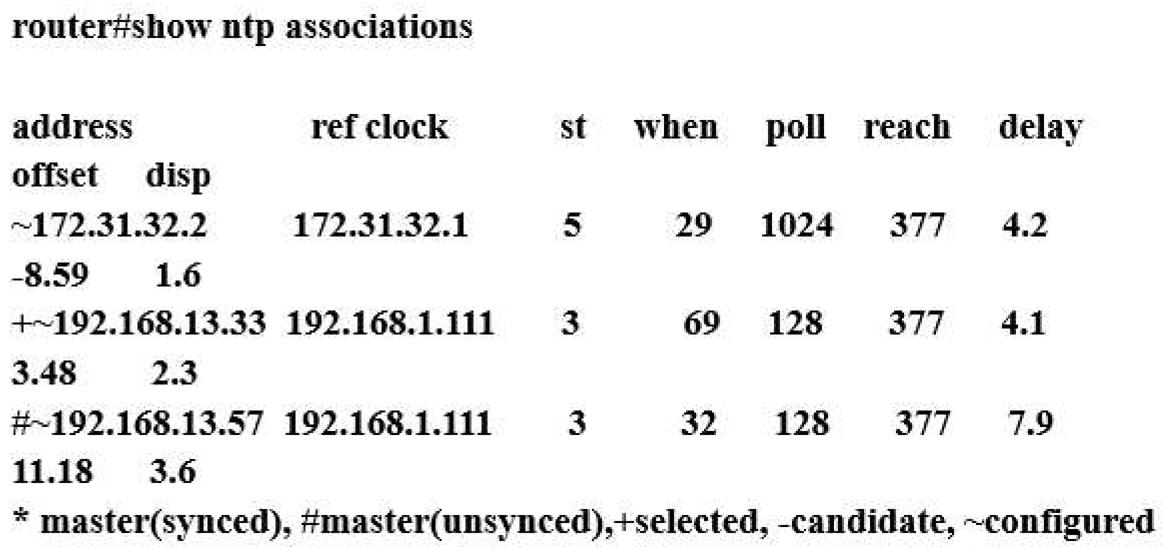
QUESTION 542
Which command denies the default route?

A. **ip prefix-list deny-route seq 5 deny 0.0.0.0/0**
B. **ip prefix-list deny-route seq 5 deny 0.0.0.0/16**
C. **ip prefix-list deny-route seq 5 deny 0.0.0.0/32**
D. **ip prefix-list deny-route seq 5 deny 0.0.0.0/8**

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 543
Refer to the exhibit. A network engineer has configured NTP on a Cisco router, but the time on the router us still incorrect. What is the reason for this problem?



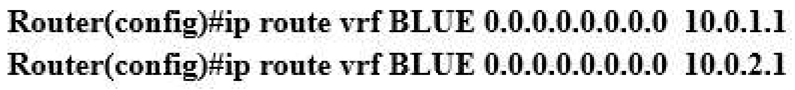
```
router#show ntp associations

address            ref clock       st   when   poll   reach   delay
offset    disp
~172.31.32.2       172.31.32.1     5      29   1024    377     4.2
-8.59      1.6
+~192.168.13.33  192.168.1.111     3      69    128    377     4.1
3.48       2.3
#~192.168.13.57  192.168.1.111     3      32    128    377     7.9
11.18      3.6
* master(synced), #master(unsynced),+selected, -candidate, ~configured
```

A. The router is not syncing with the peer, and the NTP request and response packets are not being exchanged.
B. The router is not syncing with the peer, even though the NTP request and response packets are being exchanged.
C. The router is syncing with the peer, and the NTP request and response packets are being exchanged.
D. The router is dropping all NTP packets.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
A pound sign (#) displayed next to a configured peer in the show ntp associations command output indicates that the router isn't syncing with the peer even though NTP request and response packets are being exchanged.
Reference: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html

QUESTION 544
Refer to the exhibit.



```
Router(config)#ip route vrf BLUE 0.0.0.0.0.0.0.0  10.0.1.1
Router(config)#ip route vrf BLUE 0.0.0.0.0.0.0.0  10.0.2.1
```

After configuring the rotes, the network engineer executes the show ip route command. What is the expected result?

A. Gateway of last resort is 10.0.2.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 2 subbnetsC 10.0.2.0 is directly connected, FastEthernet0/0C 10.0.1.0 is directly connected, FastEthernet0/1S" 0.0.0.0/0[1/0] via 10.0.2.1 [1/0] via 10.0.1.1Router #
B. Gateway of last resort is 10.0.1.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 1 subnet C 10.0.1.0 is directly connected, FastEthernet0/1 S" 0.0.0.0/0 [1/0] via 10.0.1.1 Router #
C. Gateway of last resort is not set Router #
D. Gateway of last resort is 10.0.2.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 1 subnet C 10.0.2.0 is directly connected, FastEthernet0/0 S"0.0.0.0/0 [1/0] via 10.0.2.1 Router #

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The show ip route command shows the global routing table routes, not the VRF routes.

QUESTION 545
Based on the configuration command below, which statement is true?

router(config)#**service timestamps log datetime msec**

A. All syslog messages that are generated will indicate the date and time when the event occurred.
B. All high-priority syslog messages that are generated will indicate the data and time when the event occurred.
C. All IOS services will indicate the data and time when the service was last used.
D. All IOS services will indicate the data and time when the service was started.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:

https://www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html#wp1055126

QUESTION 546
Which two options can you use to configure an EIGRP stub router? (Choose two.)

A. **not-so-stubby**
B. **receive-only**
C. **totally-stubby**

D. **external**

E. **summary-only**

F. **summary**

Correct Answer: BF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
eigrp stub [[receive-only] || [connected] [static] [summary] [redistributed]] The following options are available:

- Receive-only: router only accepts, but does not explicitly advertise, any routes. This option may not be used in combination with any other options.
- Connected: router advertises directly-connected networks
- Static: router advertises any configured static routes
- Summary: router advertises any configured summarized routes
- Redistributed: router advertises any routes learned from another protocol, such as OSPF The eigrp stub configuration need only be entered on the spoke routers. The hub routers determine that they are talking to a stub router by examining the TLV in the HELLO packet.

Reference: https://www.cisco.com/en/US/technologies/tk648/tk365/technologies_white_paper0900aecd8023df6f.html

QUESTION 547
Which Cisco Express Forwarding component(s) contain forwarding information?

A. FIB, adjacency table

B. adjacency table

C. FIB, RIB, Adjanceny table

D. FIB

E. RIB

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 548
Which command is needed to get the ip address assigned from the PPPOE server?

A. Interface dialer

B. pppoe enable

C. ip address negotiated

D. ip address auto negotiated

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 549
Which security level is supported throughout all SNMP versions?

A. authPriv

B. authNoPriv

C. noAuthNoPriv

D. noAuthoPriv

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 550
An administrator needs to setup an NTP client to provide updates to local without synchronizing to server. What is the command?

A. Serve

B. Serve-only

C. peer

D. query

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Serve:
--Permits router to reply NTP request;
--Reject NTP updates;
--NTP queries are Accepted.

Serve-Only:
--Permits router to respond to NTP request ONLY;
--Reject to synchronize local time;
--Not access control queries

QUESTION 551
Which three protocols are supported with EVN? (Choose three.)

A. IS-IS
B. EIGRP
C. RIP
D. OSPFv2
E. BFD
F. BGP

Correct Answer: BDF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Restrictions for EVN

An EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.
There are additional platform and line-card restrictions for an EVN trunk. Check Cisco Feature Navigator, www.cisco.com/go/cfn for supported platforms and line cards.

A single IP infrastructure can be virtualized to provide up to 32 virtual networks end-to-end.
If an EVN trunk is configured on an interface, you cannot configure VRF-Lite on the same interface.

OSPFv3 is not supported; OSPFv2 is supported.

The following are not supported by EVN:
--IS-IS
--RIP
--Route replication is not supported with BGP
--Certain SNMP set operations

The following are not supported on an EVN trunk:
--Access control lists (ACLs)
--BGP interface commands are not inherited
--IPv6, except on vnet global
--Network address translation (NAT)
--NetFlow
--Web Cache Communication Protocol (WCCP)

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.html

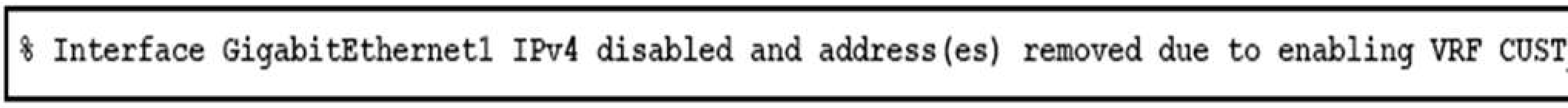
QUESTION 552
Which two statements about PAP and CHAP authentication are true? (Choose two)

A. PAP uses a challenge string from the server to the client.
B. PAP can query a TACACS+ server to verify access credentials.
C. CHAP requires the client to supply a username and optional password.
D. PAP requires the client to supply a username and optional password.
E. CHAP uses a challenge string from the server to the client.

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 553
Refer to the exhibit.



```
% Interface GigabitEthernet1 IPv4 disabled and address(es) removed due to enabling VRF CUST
```

An engineer is enabling VPN service for a customer and notices this output when placing the customer-facing interface into a VRF. Which action corrects the issue?

A. Reset interface Gigabit Ethernet 1.
B. Disabling the VRF CUST_A
C. Reconfigure the IP address on Gigabit Ethernet 1.
D. Enabling IPv6 on the interface.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 554
Which two reductions are the correct reductions if the IPv6 address 2001:0d02:0000:0000:0014:0000:0000:0095? (Choose two)

A. 2001:0d02:::0014:::0095
B. 2001:d02::14::95
C. 2001:d02:0:0:14::95
D. 2001:d02::14:0:0:95

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

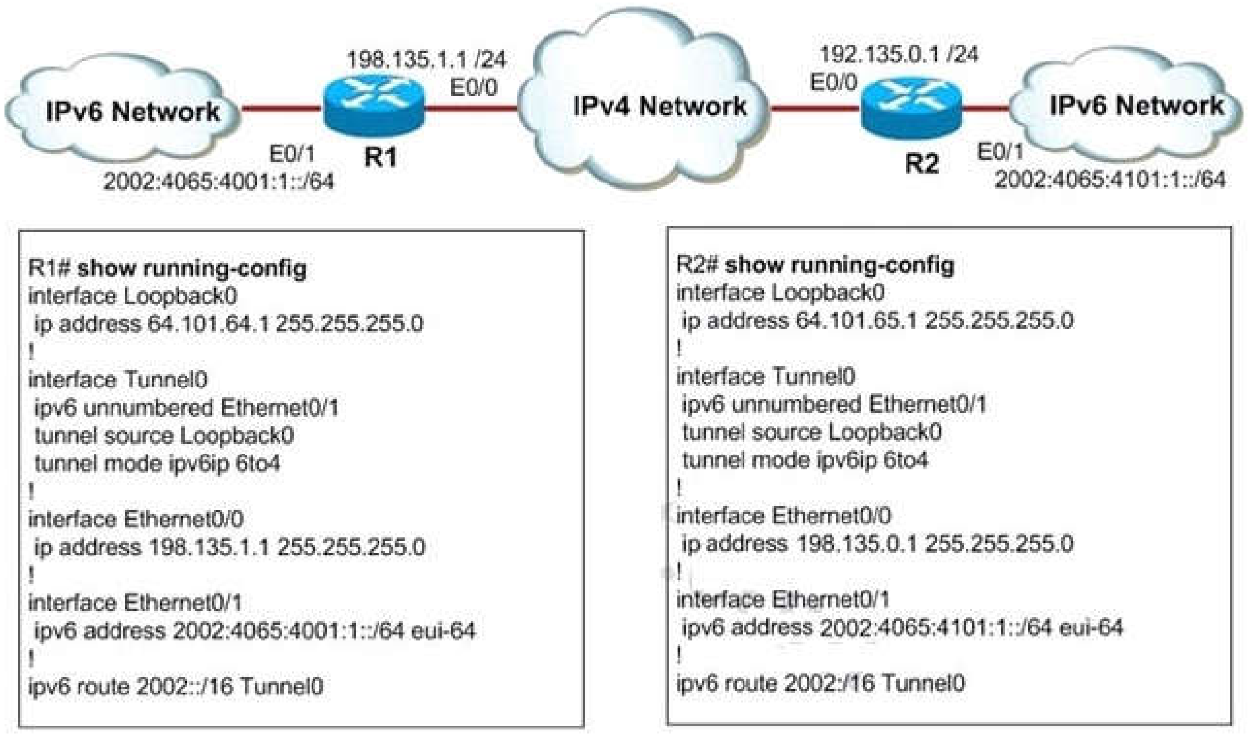
We can't use triple colons (:::) in IPv6 presentation. Also we can't use double colons (::) twice. You can use it only once in any address because if two double colons are placed in the same address, there will be no way to identify the size of each block of 0s.

Remember the following techniques to shorten an IPv6 address:
- Omit leading 0s in the address field, so :0000 can be compressed to just and :0d02 can be compressed to :d02 (but :1d00 can not be compressed to :1d)
- Use double colons (::), but just once, to represent a contiguous block of 0s,

So
2001:0d02:0000:0000:0014:0000:0000:0095 can be compressed to

2001:d02:0:0:14::95
OR
2001:d02::14:0:0:95

QUESTION 555
Refer to the exhibit.



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

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

The 6to4 overlay tunnel configuration has been applied on each router to join isolated IPv6 networks over a IPv4 network.
Which statements regarding the 6to4 overlay tunnel is true?

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

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

6to4 tunnels use IPv6 addresses that concatenate 2002::/16 with the 32-bit IPv4 address of the edge router, creating a 48-bit prefix.

The tunnel interface on R1 has an IPv6 prefix of 2002:4065:4001:1::/64, where 4065:4001 is the hexadecimal equivalent of 64.101.64.1, the IPv4 address of its interface in the IPv4 network.
The tunnel interface on R2 has an IPv6 prefix of 2002:4065:4101:1::/64, where 4065:4101 is the hexadecimal equivalent of 64.101.65.1, the IPv4 address of its interface in the IPv4 network.

When R1 receives a packet with IPv6 destination address of 2002:4065:4101:1:: (from the left IPv6 network, for example) R1 will:

* Take the IPv6 destination address of that packet (2002:4065:4101:1::) and convert it into an IPv4 address. In this case, the IPv4 address is 40.65.41.01 in hexa, which is 64.101.65.1 in decimal format.
* R1 encapsulates the IPv6 packet in an IPv4 packet with a destination address of 64.101.65.1; the packet is routed normally through the IPv4 network to R2
* R2 receives the IPv4 packet, decapsulates and routes it normally to its final IPv6 destination.

QUESTION 556
What happens when an IPv6 enabled router running 6to4 must send a packet to a remote destination and the next hop is the address of 2002::/16?

A. The IPv6 packet has its header removed and replaced with an IPv4 header
B. The IPv6 packet is encapsulated in an IPv4 packet using an IPv4 protocol type of 41
C. The IPv6 packet is dropped because that destination is unable to route IPv6 packets
D. The packet is tagged with an IPv6 header and the IPv6 prefix is included

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

6to4 and Teredo are dynamic tunneling techniques used by desktop operating systems to help their users gain access to the IPv6 Internet. These techniques tunnel the IPv6 packets within IPv4 packets.

The 6to4 method places the IPv6 packets within IPv4 protocol 41 packets.
The Teredo method places the IPv6 packets within IPv4 packets with a UDP 3544 header.

QUESTION 557
What are three IPv6 transition mechanisms? (Choose three)

A. 6to4 tunneling
B. VPN tunneling
C. GRE tunneling
D. ISATAP tunneling
E. PPP tunneling
F. Teredo tunneling

Correct Answer: ADF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Below is a summary of IPv6 transition technologies:

6 to 4 tunneling: This mechanism allows IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup. The main advantage of this technology is that it requires no end-node reconfiguration and minimal router configuration but it is not intended as a permanent solution.

ISATAP tunneling (Intra-Site Automatic Tunnel Addressing Protocol): is a mechanism for transmitting IPv6 packets over IPv4 network. The word "automatic" means that once an ISATAP server/router has been set up, only the clients must be configured to connect to it.

Teredo tunneling: This mechanism tunnels IPv6 datagrams within IPv4 UDP datagrams, allowing private IPv4 address and IPv4 NAT traversal to be used.

In fact, GRE tunneling is also a IPv6 transition mechanism but is not mentioned in BSCI so we shouldn't choose it (there are 4 types of IPv6 transition mechanisms mentioned in BSCI; they are manual, 6-to-4, Teredo and ISATAP).

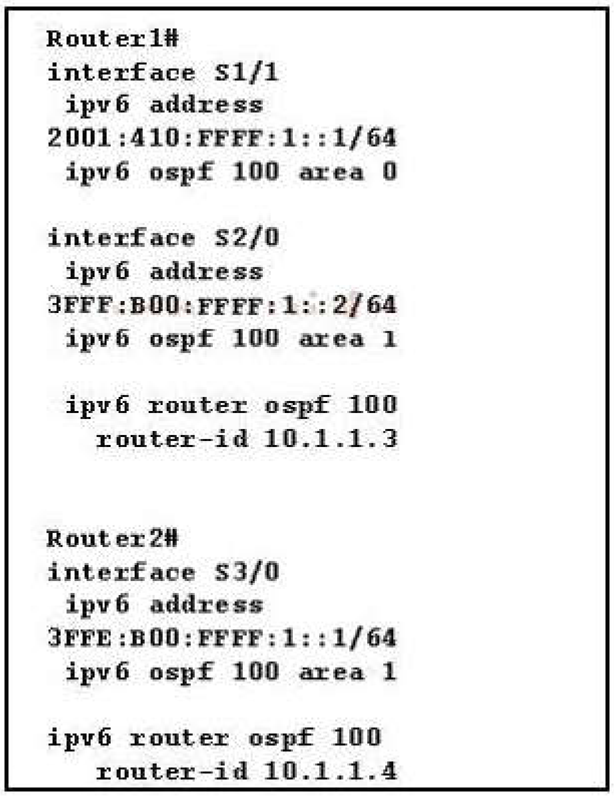
QUESTION 558
What are two rules for compacting IPv6 addresses? (Choose two.)

A. Every 16-bit segment that consists of all zeroes can be represented with a single colon.
B. The trailing zeroes in any 16-bit segment do not have to be written.
C. The leading zeroes in any 16-bit segment do not have to be written.
D. Any single, continuous string of one or more 16-bit segments that consists of all zeroes can be represented with a double colon.
E. The maximum number of times a double colon can replace a 16-bit segment that consists of all zeroes is two.
F. Two zeroes in the middle of any 16-bit segment do not have to be written.

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 559
Refer to the exhibit.



```
Router1#
interface S1/1
 ipv6 address
2001:410:FFFF:1::1/64
 ipv6 ospf 100 area 0

interface S2/0
 ipv6 address
3FFF:B00:FFFF:1::2/64
 ipv6 ospf 100 area 1

 ipv6 router ospf 100
   router-id 10.1.1.3


Router2#
interface S3/0
 ipv6 address
3FFE:B00:FFFF:1::1/64
 ipv6 ospf 100 area 1

ipv6 router ospf 100
   router-id 10.1.1.4
```

A. Interface authentication must be configured.
B. The routing processes must be configured with an area ID.
C. IP unicast routing must be enabled.
D. IPv4 addresses must be applied to the interfaces.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 560
Which functionality is required within an IP router that is situated at the boundary of an IPv4 network and an IPv6 network to allow communication between IPv6-only and IPv4-only nodes?

A. Autoconfiguration
B. Automatic 6to4 Tunnel
C. Automatic 6to4 Relay
D. Network Address Translator-Protocol Translator (NAT-PT)
E. Intrasite Automatic Tunnel Address Protocol (ISATAP)

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

NAT-PT provides IPv4/IPv6 protocol translation. It resides within an IP router, situated at the boundary of an IPv4 network and an IPv6 network. By installing NAT-PT between an IPv4 and IPv6 network, all IPv4 users are given access to the IPv6 network without modification in the local IPv4-hosts (and vice versa). Equally, all hosts on the IPv6 network are given access to the IPv4 hosts without modification to the local IPv6-hosts. This is accomplished with a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries.

QUESTION 561
During the IPv6 auto configuration, what does the device append to the 64-bit prefix that it receives from the router to create its IPv6 address?

A. a pseudorandom generated number
B. its locally configured IPv4 address
C. the DHCP-supplied device ID
D. its MAC address

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The automatic configuration is a great feature of IPv6. Imagine you have to manually configure an IPv6 address with 128-bit long, what a pain!

With this feature, it is no longer necessary to configure each host manually. But notice that host only autonomously configures its own Link- local address (the IP address used on a LAN). The Link-local address can be created automatically using a link-local prefix of FE80::/10 and a 64-bit interface identifier (based on 48-bit MAC address).

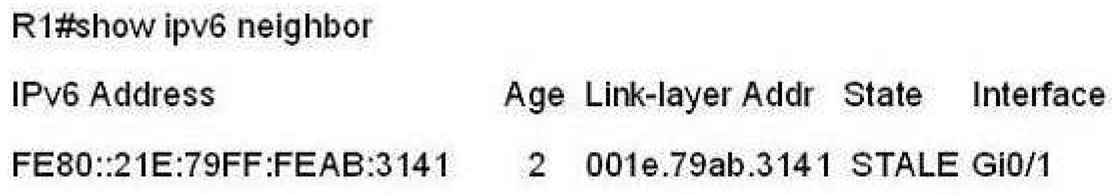
For example, if your MAC address is 00:12:34:56:78:9a, your 64-bit interface identifier is 0012:34FF:FE56:789a (16-bit FFFE is inserted in the middle). And notice that the notation has been changed because IPv6 addresses require 16-bit pieces to be separated by ":".

Then, according to the RFC 3513 we need to invert the Universal/Local bit ("U/L" bit) in the 7th position of the first octet (start counting from 0). The "u" bit is set to 1 to indicate Universal, and it is set to zero (0) to indicate local scope. In this case we set this bit to 1 because the MAC address is universally unique. Thus the result is: 0212:34FF:FE56:789a.

Finally, add the link-local prefix FE80 to create the full IPv6 address: FE80:0:0:0:0212:34FF:FE56:789a (or FE80::212:34FF:FE56:789a in short form)

Note: The reason for inverting the "U/L" bit is to allow ignoring it for short values in the manual configuration case. For example, you can manually assign the short address fc80::1 instead of the long fc80:0:0:0:0200::1

QUESTION 562
Refer to the exhibit.



```
R1#show ipv6 neighbor

IPv6 Address                  Age  Link-layer Addr  State   Interface

FE80::21E:79FF:FEAB:3141       2   001e.79ab.3141   STALE Gi0/1
```

Which statement about this neighbor of R1 is true?

A. OSPFv3 adjacency has been lost, which causes the neighbor to be considered Stale.
B. Aggregate global addresses are always used between IPv6 neighbors.
C. OSPFv3 adjacency will not work between link-local addresses.
D. R1 used ICMP to learn about this neighbor.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
ICMP is a ping echo. IPv6 uses ICMP to learn about its neighbor.

QUESTION 563
Which IPv6 address correctly compresses the IPv6 unicast address 2001:0:0:0:0DB8:0:0:417A?

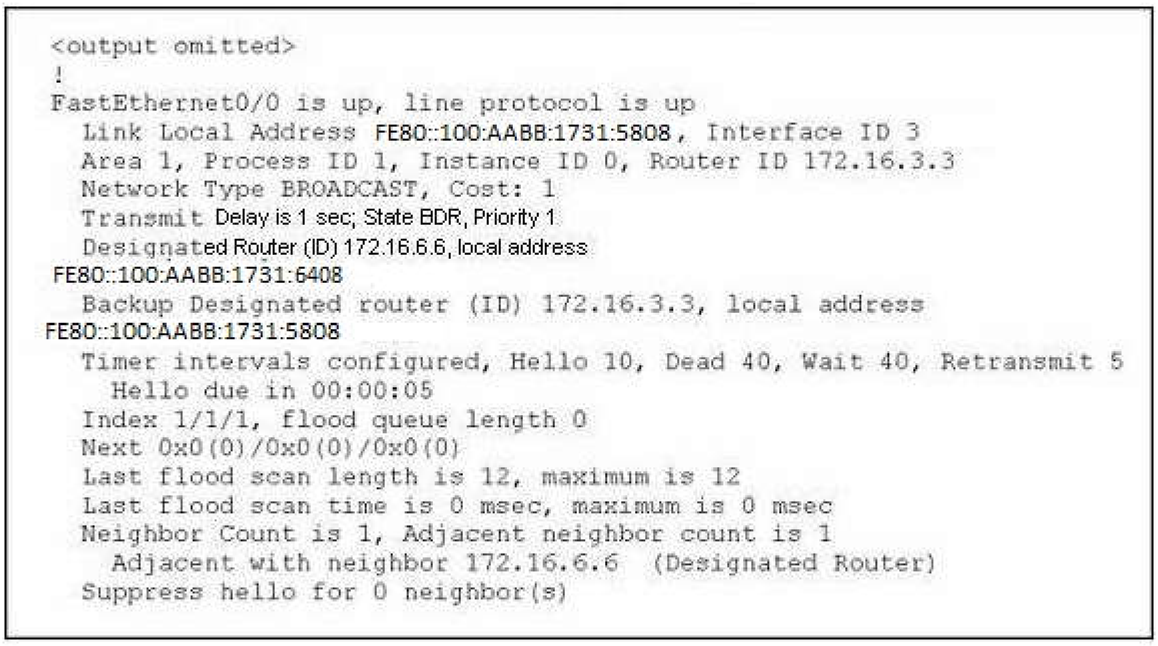
A. 2001:0DB8:417A
B. 2001::0DB8::417A
C. 2001:::0DB8::417A
D. 2001:0DB8:0:0:417A
E. 2001::DB8:0:0:417A
F. 2001:::0DB8:0:0:417A

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The point of this question is the about the different form of Ipv6 address.
The IPv6 address is 128 bits long, written as eight 16-bit pieces, separated by colons.
Each piece is represented by four hexadecimal digits. You can compact multiple contiguous fields of zero even further. This is the exception to the rule that at least one digit must be present in every field. You can replace multiple fields of zeros with double colons (::).
Note that :: can replace only one set of contiguous zero fields.
Multiple ::s would make the address ambiguous.

QUESTION 564
Refer to the exhibit. What two statements are true? (Choose two)



```
<output omitted>
!
FastEthernet0/0 is up, line protocol is up
  Link Local Address FE80::100:AABB:1731:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec; State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address
FE80::100:AABB:1731:6408
  Backup Designated router (ID) 172.16.3.3, local address
FE80::100:AABB:1731:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

A. Interface FastEthernet 0/0 was configured with the ipv6 ospf 1 area 1 command.
B. OSPF version 2 has been enabled to support IPv6.
C. The IP address of the backup designated router (BDR) is FE80::100:AABB:1731:5808.
D. The output was generated by the show ip interface command.
E. The router was configured with the commands: router ospf 1 network 172.16.6.0 0.0.0.255 area 1
F. This is the designated router (DR) on the FastEtheroet 0/0 link.

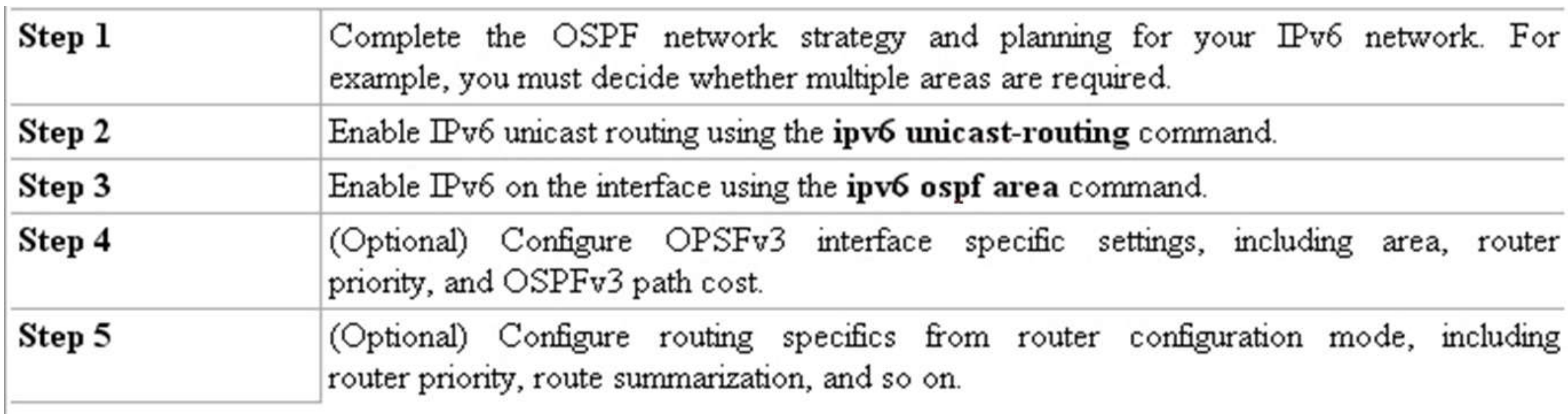
Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

OSPFv3 supports IPv6.
The configuration of OSPFv3 is not a subcommand mode of the router ospf command as it is in OSPFv2 confguration.

For example, instead of using the network area command to identify networks that are part of the OSPFv3 network, the interfaces are directly configured to specify that IPv6 networks are part of the OSPFv3 network.

The following describes the steps to configure OSPF for IPv6:



Step 1	Complete the OSPF network strategy and planning for your IPv6 network. For example, you must decide whether multiple areas are required.
Step 2	Enable IPv6 unicast routing using the **ipv6 unicast-routing** command.
Step 3	Enable IPv6 on the interface using the **ipv6 ospf area** command.
Step 4	(Optional) Configure OPSFv3 interface specific settings, including area, router priority, and OSPFv3 path cost.
Step 5	(Optional) Configure routing specifics from router configuration mode, including router priority, route summarization, and so on.

There are several commonly used OSPFv3 show commands, including the show ipv6 ospf [process-id] [area-id] interface [interface] command.

QUESTION 565
Which two statements about the **enable secret** and **enable password** commands are true? (Choose two.)

A. If both commands are missing from the global configuration, vty lines use the console password.
B. The **enable secret** and **enable password** command overrides enable password.
C. The **enable secret** command overrides **enable password**.
D. The **enable secret** command is backwards-compatible with more versions of IOS.
E. The **enable password** command has a stronger encryption algorithm than **enable secret**.

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

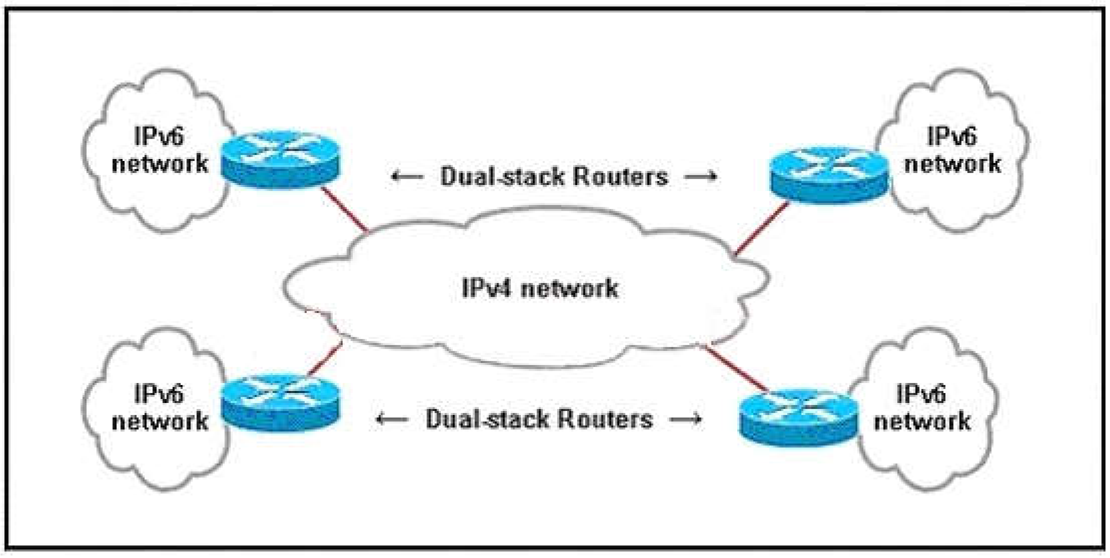
QUESTION 566
Which statement is true about the command ipv6 ospf 1 area 0?

A. It must be issued in router global configuration mode to enable the OSPF process for IPv6.
B. It must be issued in interface configuration mode to enable the OSPF process for IPv6.
C. It must be issued before the network command to enable the OSPF process for IPv6.
D. It must be issued after the network command to enable the OSPF process for IPv6.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 567
Refer to the exhibit. Which interoperability technique implemented on the dual-stack routers would allow connectivity between IPv6 sites across automatic created tunnels using the 2002::/16 prefix?



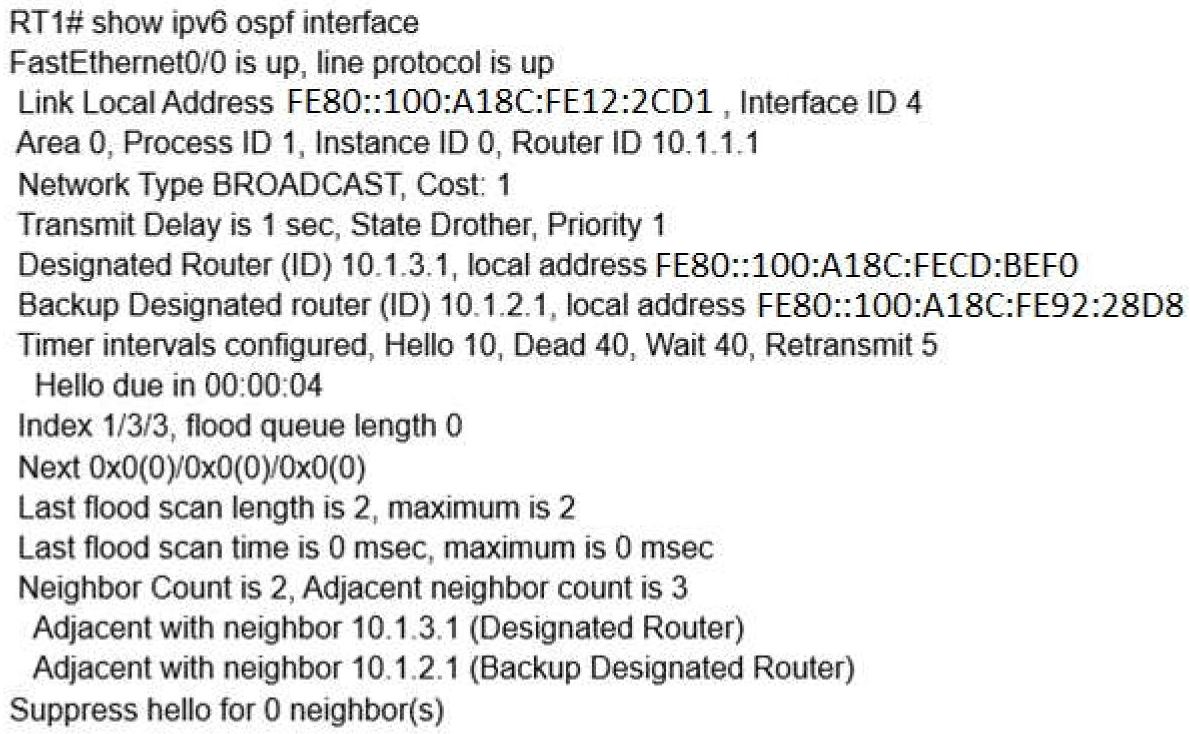
A. Dual Stack

B. NAT-PT
C. 6to4 tunnel
D. GRE tunnel
E. ISATAP tunnel

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 568
Refer to the exhibit. Based on the output from the show command on RT1 which statement is true?



```
RT1# show ipv6 ospf interface
FastEthernet0/0 is up, line protocol is up
 Link Local Address FE80::100:A18C:FE12:2CD1 , Interface ID 4
 Area 0, Process ID 1, Instance ID 0, Router ID 10.1.1.1
 Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State Drother, Priority 1
 Designated Router (ID) 10.1.3.1, local address FE80::100:A18C:FECD:BEF0
 Backup Designated router (ID) 10.1.2.1, local address FE80::100:A18C:FE92:28D8
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:04
 Index 1/3/3, flood queue length 0
 Next 0x0(0)/0x0(0)/0x0(0)
 Last flood scan length is 2, maximum is 2
 Last flood scan time is 0 msec, maximum is 0 msec
 Neighbor Count is 2, Adjacent neighbor count is 3
   Adjacent with neighbor 10.1.3.1 (Designated Router)
   Adjacent with neighbor 10.1.2.1 (Backup Designated Router)
Suppress hello for 0 neighbor(s)
```

A. OSPFv3 uses global IPv6 addresses to establish neighbor adjacencies.
B. RT1 has a subnet mask of 64 bits.
C. RT1 has FastEthernet0/0 set as a DR for network type broadcast.
D. OSPFv3 uses Link-local addresses to establish neighbor adjacencies.
E. RT1 does not have a global IPv6 address set on FastEthernet0/0.
F. OSPFv3 uses IPv4 addresses to establish neighbor adjacencies

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

OSPFv3 is an updated version of OSPF designed to accommodate IPv6 natively. OSPFv3 uses the multicast address FF02::5 and FF02::6, but like EIGRP it uses its link-local address as the source address in advertisements.

QUESTION 569
Your Company trainee asks you, in the context of IPv6 and OSPF, what best describes a type 9 LSA?

A. Link LSA
B. Interarea prefix LSA for ABRs
C. Router LSA
D. Switch LSA
E. Intra-area prefix LSA
F. None of the above

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 570
Company plans on migrating their network from IPv4 to IPv6 in the near future. Which three techniques can be used to transition from IPv4 to IPv6? (Select three.)

A. Dual stack
B. NAT
C. Flow label
D. Mobile IP
E. 6to4 tunneling
F. Anycast
G. MBGP

Correct Answer: ABE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 571
Which command must be globally enabled on a Cisco router to support IPv6?

A. ip routing ipv6
B. ipv6 unicast-routing
C. ipv6 routing
D. ip classless
E. ipv6 cef

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 572
What number is a valid representation for the 200F:0000:AB00:0000:0000:0000:0000/56 IPv6 prefix?

A. 200F:0:0:AB/56
B. 200F:0:AB00::/56
C. 200F::AB00/56
D. 200F:AB/56

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The 0s are truncated.

QUESTION 573
Company has migrated to IPv6 in their network.
Which three IPv6 notations represent the same address? (Select three.)

A. 2031::130F::9C0:876A:130B
B. 2031:0000:130F:0000:0000:09C0:876A:130B
C. 2031:0:130F:::9C0:876A:130B
D. 2031::130F:0::9C0:876A:130B
E. 2031:0:130F:0:0:09C0:876A:130B
F. 2031:0:130F::9C0:876A:130B

Correct Answer: BEF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

With IP version 6, octets containing all zero's can be simply represented as :, while consecutive zero fields can be represented as ::.

ANSWER choices E and F are simply the shorthand version of the fully written IPv6 address shown in choice.

QUESTION 574
Which statement is true about 6to4 tunneling?

A. IPv4 traffic is encapsulated with an IPv6 header
B. the edge router can use locally configured IPv6 address
C. host and routers inside a 6to4 site will need a special code
D. an edge router must use IPv6 address of 2002::/16 in its prefix

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

6to4 tunnel is a technique which relies on reserved address space 2002::/16 (you must remember this range).
These tunnels determine the appropriate destination address by combining the IPv6 prefix with the globally unique destination 6to4 border router's IPv4 address, beginning with the 2002::/16 prefix, in this format:

2002:border-router-IPv4-address::/48

Because the border-router-IPv4-address is added, we will have a /48 prefix (we all know an IPv4 address consists of 32 bits).
An example of a 6to4 address with the border-router-IPv4-address of 192.168.1.2 is 2002:C0A8:01:02::/48.

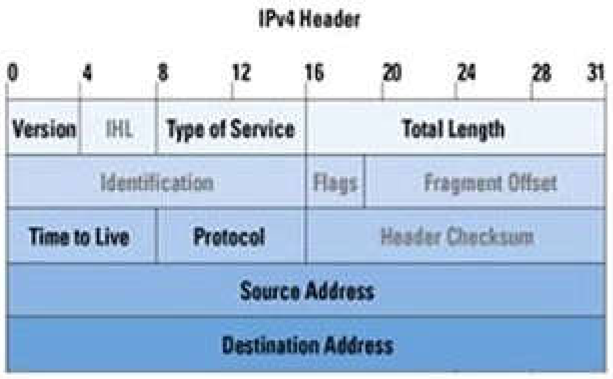
QUESTION 575
In a comparison of an IPv4 header with an IPv6 header, which three statements are true? (Choose three)

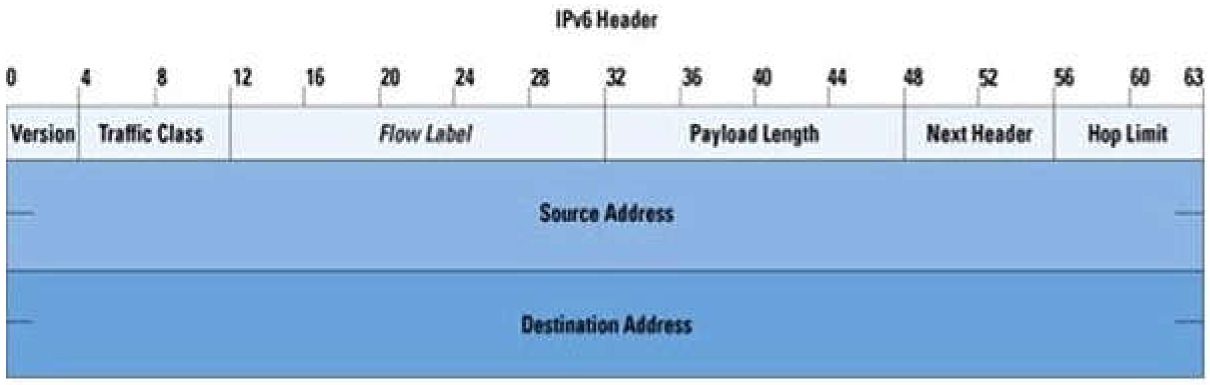
A. An IPv4 header includes a checksum. However, an IPv6 header does not include one.
B. A router has to recompute the checksum of an IPv6 packet when decrementing the TTL.
C. An IPv6 header is half the size of an IPv4 header.
D. An IPv6 header has twice as many octets as an IPv4 header.
E. An IPv6 header is simpler and more efficient than an IPv4 header.
F. The 128-bit IPv6 address makes the IPv6 header more complicated than an IPv4 header.

Correct Answer: ADE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The image below shows the differences between an IPv4 header and an IPv6 header:





Reference:

https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-13/ipv6-internals.html

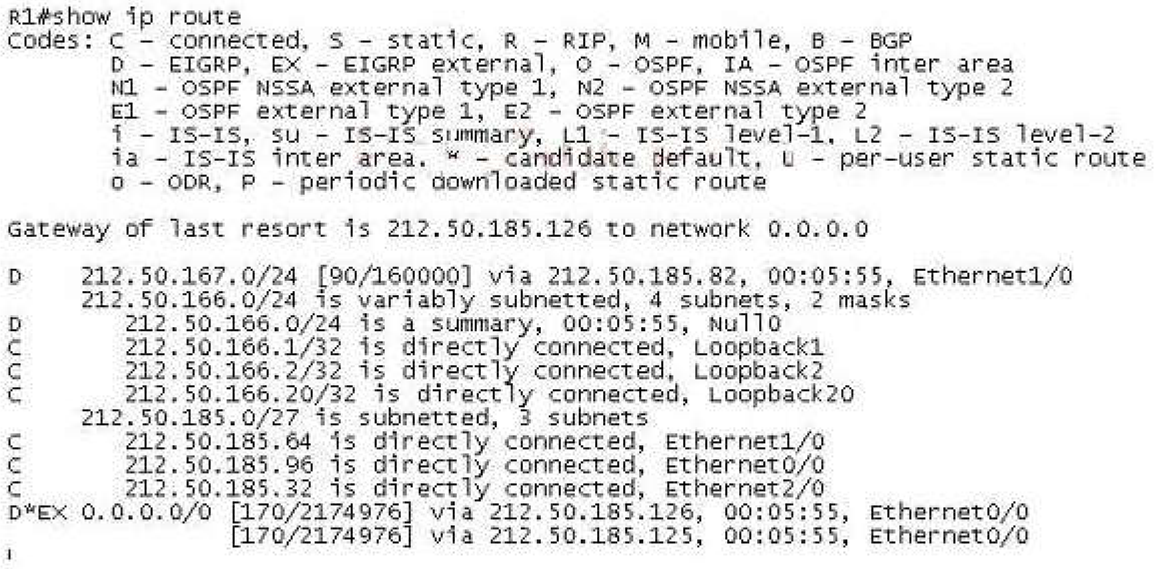
QUESTION 576
Which statement about conditional debugging is true?

A. You can limit the output to a specific interface.
B. It is limited to Ethernet, serial, and multilink interfaces.
C. It can support only one condition at a time.
D. It generates debug messages only for packets entering the router.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 577
Refer to the exhibit.



```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 212.50.185.126 to network 0.0.0.0

D    212.50.167.0/24 [90/160000] via 212.50.185.82, 00:05:55, Ethernet1/0
     212.50.166.0/24 is variably subnetted, 4 subnets, 2 masks
D       212.50.166.0/24 is a summary, 00:05:55, Null0
C       212.50.166.1/32 is directly connected, Loopback1
C       212.50.166.2/32 is directly connected, Loopback2
C       212.50.166.20/32 is directly connected, Loopback20
     212.50.185.0/27 is subnetted, 3 subnets
C       212.50.185.64 is directly connected, Ethernet1/0
C       212.50.185.96 is directly connected, Ethernet0/0
C       212.50.185.32 is directly connected, Ethernet2/0
D*EX 0.0.0.0/0 [170/2174976] via 212.50.185.126, 00:05:55, Ethernet0/0
               [170/2174976] via 212.50.185.125, 00:05:55, Ethernet0/0
!
```

How would you confirm on R1 that load balancing is actually occurring on default-network (0.0.0.0)?

A. Use ping and the show ip route command to confirm the timers for each default network resets to 0
B. Load balancing does not occur over default networks; the second route will only be used for failover.
C. Use an extended ping along with repeated show ip route commands to confirm the gateway of last resort address toggles back and forth.
D. Use the traceroute command to an address that is not explicitly in the routing table.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The simplest method to test load balancing is to use the "traceroute" command. If load balancing is working correctly, we will see different paths to reach the destination each time we use that command.

Unknown address will be routed via the default-network 0.0.0.0 so we must use an address that is not explicitly in the routing table.

QUESTION 578
An IPv6 overlay tunnel is required to communicate with isolated IPv6 networks across an IPv4 infrastructure. There are currently five IPv6 overlay tunnel types. Which three IPv6 overlay tunnel statements are true? (Choose three)

A. Overlay tunnels can only be configured between border routers capable of supporting IPv4 and IPv6.
B. Overlay tunnels can be configured between border routers or between a border router and a host capable of supporting IPv4 and IPv6.
C. Cisco IOS supports manual, generic, routing encapsulation (GRE), IPv6-compatible, 4to6, and multiprotocol Label Switching (MPLS) Overlay tunneling mechanism.
D. Cisco IOS supports manual, generic routing encapsulation (GRE), IPv4-compatible, 6to4, and IntraSite Automatic Tunnel Addressing Protocol (ISATAP) overlay tunneling mechanisms.
E. A manual overlay tunnel supports point-to-multipoint tunnels capable of carrying IPv6 and Connectionless Network Service (CLNS) packets.
F. Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure.

Correct Answer: BDF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

B: Overlay tunnels can be configured between border routers or between a border router and a host capable of supporting IPv4 and IPv6.
D. Cisco IOS supports manual, generic routing encapsulation (GRE), IPv4-compatible, 6to4, and IntraSite Automatic Tunnel Addressing Protocol (ISATAP) overlay tunneling mechanisms.
F: Overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure.

QUESTION 579
What would you configure on SNMPv3 to allow authentication?

A. Authpriv
B. authnopriv
C. noauthnopriv
D. authmember

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The SNMPv3 Agent supports the following set of security levels:

+ NoAuthnoPriv: Communication without authentication and privacy.
+ AuthNoPriv: Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).
+ AuthPriv: Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA ; and for Privacy, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used. For Privacy Support, you have to install some third-party privacy packages

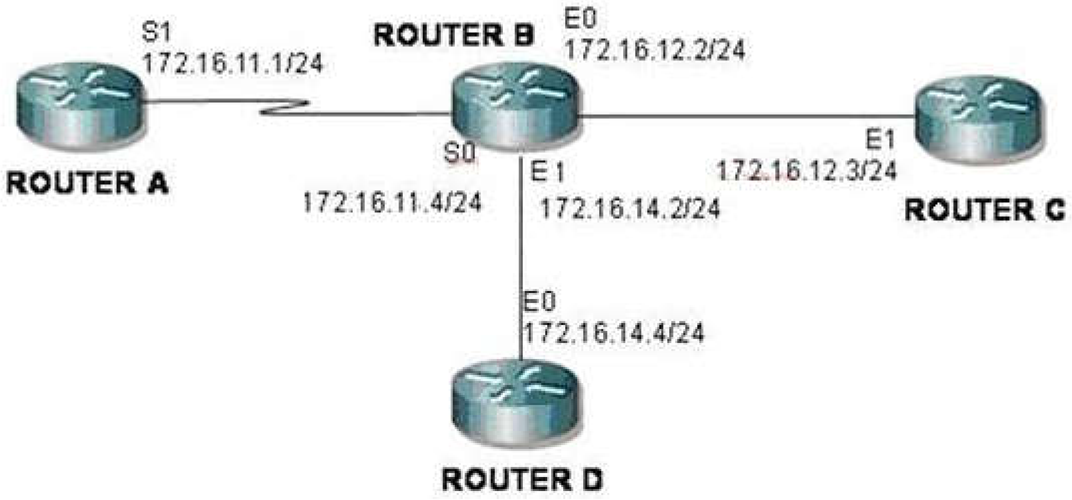
QUESTION 580
Which of the following NSAP addresses is a private, locally administered address?

A. 39.0f01.0002.0000.0c00.1111.00
B. 48.0f01.0002.0000.0c00.1111.00
C. 49.0004.30ac.0000.3090.c7df.00
D. 52.0f01.0002.0000.0c00.1111.00

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 581
A policy needs to be implemented on Router B so that any traffic sourced from 172.16.10.0/24 will be forwarded to Router C.



Which configuration on Router B will achieve the desired effect?

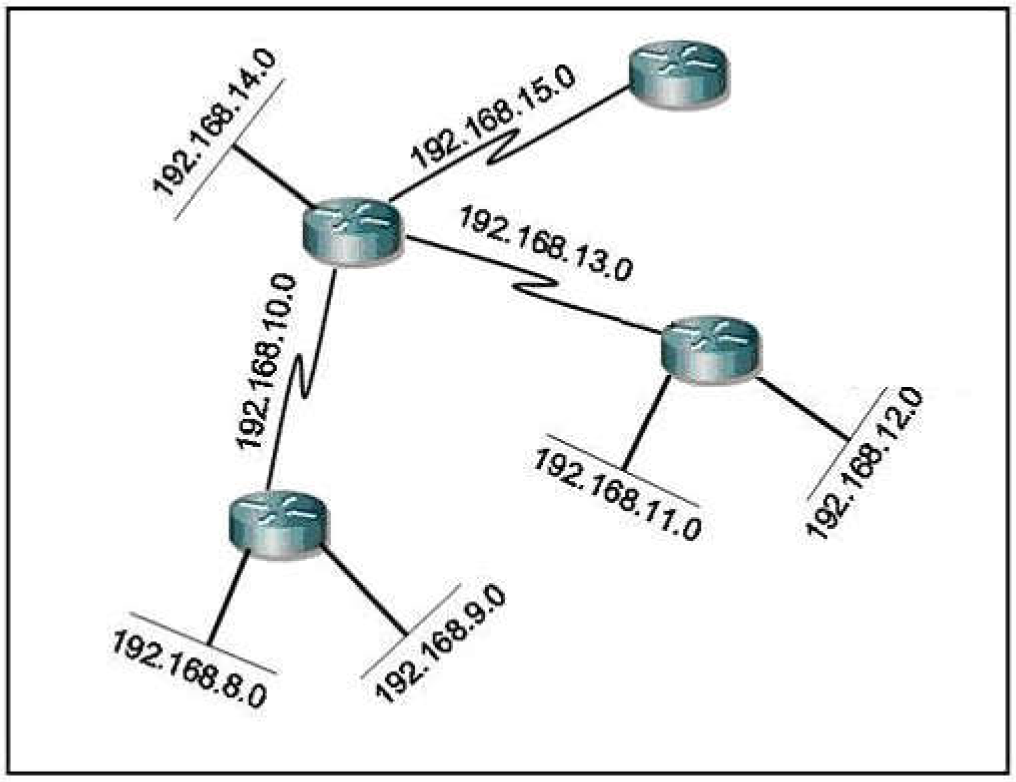
A. access-list 1 permit 172.16.10.0 0.0.0.255
interface S0
ip policy route-map policy
route-map policy permit 10
match ip address 1
set ip next-hop 172.16.12.3
B. access-list 1 permit 172.16.10.0 0.0.0.255
interface E0
ip policy route-map policy
route-map policy permit 10
match ip address 1
set ip next-hop 172.16.12.2
C. access-list 1 permit 172.16.10.0 0.0.0.255
!interface E0
ip policy route-map policy
route-map policy permit 10
match ip address 1
set ip next-hop 172.16.14.4
D. access-list 1 deny 172.16.10.0 0.0.0.255
interface S0
ip policy route-map policy
route-map policy permit 10
match ip address 1
set ip next-hop 172.16.12.2

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The "next-hop" IP address should be the E1 interface of router C (172.16.12.3).

QUESTION 582



Which address would successfully summarize only the networks seen?

A. 192.168.0.0/24
B. 192.168.8.0/20
C. 192.168.8.0/21
D. 192.168.12.0/20
E. 192.168.16.0/21
F. These networks cannot be summarized.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Let's suppose it is a /20 then we would have addresses from 192.168.0.1 to 192.168.15.255
Now let's suppose it is a /21 then we would have addresses from 192.168.8.1 to 192.168.15.255

So both summaries encompass the networks we want to summarize but the second one is the most restrictive one as it only encompasses the networks we were asked to summarize and not others so it is the correct summary.

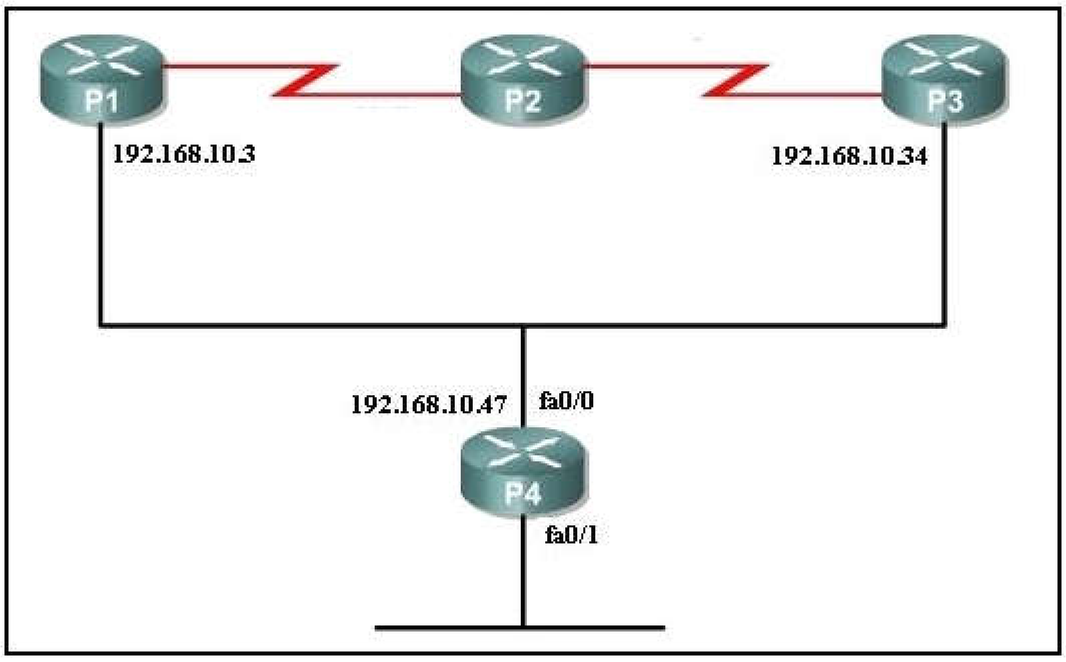
In fact just count the number if subnets which is 8 and find the exponent of 2 which is 8, that gives you 3 and to find out the summary mask just do /24 - 3 = /21.

If you make it an binary you'll find out the answer too:
the interesting octet is 3rd one so let's convert in binary.

8	00001 000
9	00001 001
10	00001 010
11	00001 011
12	00001 100
13	00001 101
14	00001 110
15	00001 111

I've bolded the bits in common there are 5 so 16+5=21 which is mask and address is 192.168.8.0

QUESTION 583



What is the correct configuration to enable router P4 to exchange RIP routing updates with router P1 but not with router P3?

```
A.  P4(Config)# interface fa0/0
    P4(Config-if)# neighbor 192.168.10.3
    P4(config-if)# passive-interface fa0/0
B.  P4(config)# router rip
    P4(config-router)# neighbor 192.168.10.3
    P4(Config-router)# passive-interface fa0/0
C.  P4(config)# interface fa0/0
    P4(config-if)# neighbor 192.168.10.3
    P4(config-if)# passive interface 192.168.10.34
D.  P4(config)# router rip
    P4(config-router)# neighbor 192.168.10.34 no broadcast
    P4(config-router)# passive-interface fa0/0
```

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

When you configure router P1 to be the neighbor of P4 with a passive interface, the RIP routing updates will be exchanged with the neighbor ONLY.

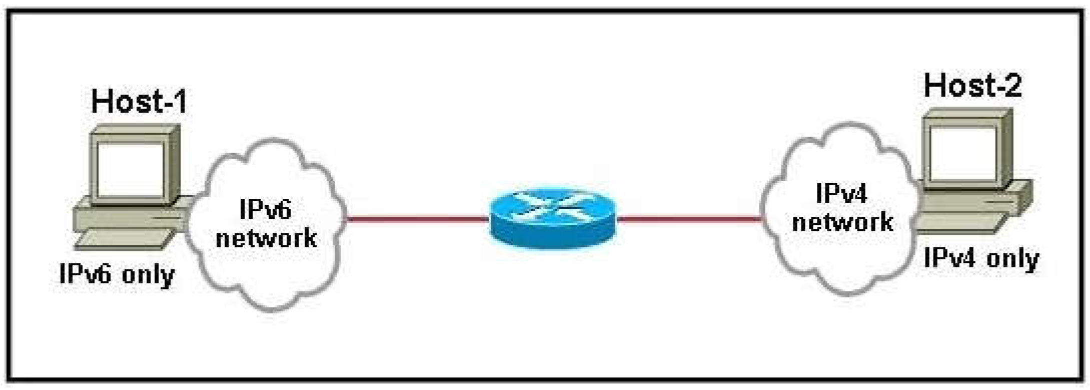
QUESTION 584
Which two statements about 6to4 tunneling are accurate? (Choose two)

A. Prepending a reserved IPv6 code to the hexadecimal representation of 192.168.0.1 facilitates 6to4 tunneling.
B. Each 6to4 site receives a /48 prefix in a 6to4 tunnel.
C. 2002::/48 is the address range specifically assigned to 6to4.
D. Prepending 0x2002 with the IPv4 address creates an IPv6 address that is used in 6to4 tunneling.
E. 6to4 is a manual tunnel method.

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 585



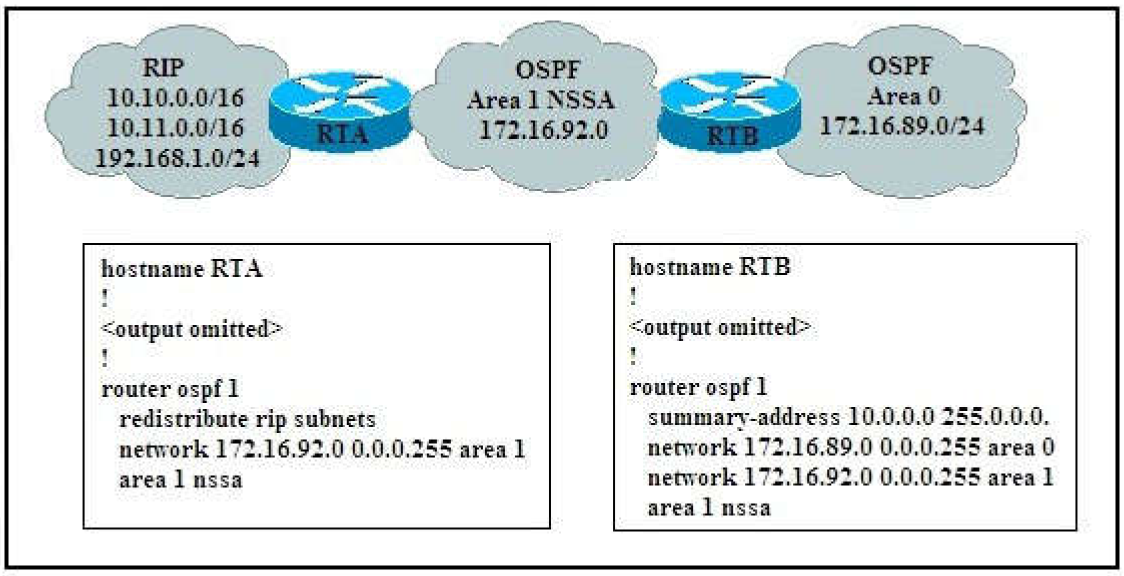
Which interoperability technique implemented on the router would allow Host-1 to communicate with Host-2?

A. Dual Stack
B. NAT-PT
C. 6to4 tunnel
D. GRE tunnel
E. ISATAP tunnel

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 586
Refer to the exhibit.



```
hostname RTA
!
<output omitted>
!
router ospf 1
  redistribute rip subnets
  network 172.16.92.0 0.0.0.255 area 1
  area 1 nssa
```

```
hostname RTB
!
<output omitted>
!
router ospf 1
  summary-address 10.0.0.0 255.0.0.0.
  network 172.16.89.0 0.0.0.255 area 0
  network 172.16.92.0 0.0.0.255 area 1
  area 1 nssa
```

Which statement is true?

A. RTA will redistribute the RIP routers into the NSSA as type 7 LSAs.
   RTB will translate the type 7 LSAs into type LSAs and flood them throughout the OSPF backbone.
B. RTA will redistribute the RIP routers into the NSSA as type 7 LSAs.
   RTB will flood the type 7 LSAs throughout the backbone.
C. RTA will redistribute the RIP routers into the NSSA as type 5 LSAs.
   RTB will flood the type 5 LSAs throughout the backbone.
D. RTA will redistribute the RIP routers into the NSSA as type 5 LSAs.
   RTB will translate the type of 5 LSAs unto type 7 LSAs and flood them throughout the OSPF backbone.
E. RTA will not redistribute the RIP routers into the NSSA.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 587
To configure 6to4 tunneling on a dual-stack edge router. Which three of the following are valid components in 6to4 Tunneling configuration? (Choose Three)

A. IPv4 Tunnel IP address
B. Tunnel mode (6to4)
C. Tunnel Keepalives
D. IPv4 Tunnel Destination
E. IPv4 Tunnel Source
F. 6to4 IPv6 address (within 2002::/16)

Correct Answer: BEF
Section: Mix Questions
Explanation

Explanation/Reference:

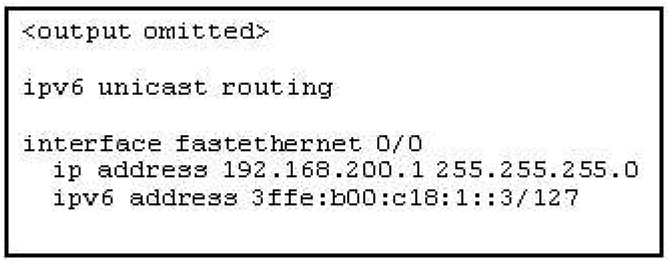
QUESTION 588
Which three statements about configuring OSPF in a IPv6 network are true? (Choose three)

A. OSPF version 2 will support IPv6.
B. OSPF version 3 will support IPv6.
C. Multiple instances of OSPF for IPv6 can be run on a link.
D. Networks must be explicitly configured using the network command in router OSPF configuration mode.
E. IPv4 addresses cannot be used as the router ID in OSPF for IPv6.
F. The interface command ipv6 ospf <process-id> area <area-id> is all that is required to enable OSPF for IPv6 on an interface.

Correct Answer: BCF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 589
Refer to the exhibit.



```
<output omitted>

ipv6 unicast routing

interface fastethernet 0/0
  ip address 192.168.200.1 255.255.255.0
  ipv6 address 3ffe:b00:c18:1::3/127
```

Which two statements are true about the router configuration? (Choose two)

A. This configuration allows applications on the same segment to communicate via IPv4 or IPv6.
B. This configuration is referred to as a dual-stack 6to4 tunnel.
C. This configuration is referred to as a dual stack.
D. This configuration will attempt to route packets using IPv4 first, and if that fails, then IPv6.

Correct Answer: AC
Section: Mix Questions
Explanation

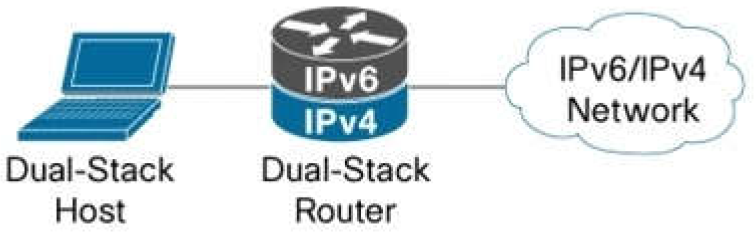
Explanation/Reference:
Explanation:

This router demonstrates an example of an IPv6 Dual Stack configuration.

Dual stack (Figure 1 below) runs both IPv4 and IPv6 protocol stacks on a router in parallel, making it similar to the multiprotocol network environments of the past, which often ran Internetwork Packet Exchange (IPX), AppleTalk, IP, and other protocols concurrently.

The technique of deploying IPv6 using dual-stack backbones allows IPv4 and IPv6 applications to coexist in a dual IP layer routing backbone.
The IPv4 communication uses the IPv4 protocol stack, and the IPv6 communication uses the IPv6 stack.
As a transition strategy, dual stack is ideal for campus networks with a mixture of IPv4 and IPv6 applications.

Figure 1: Dual-Stack Example



QUESTION 590
When implementing a 6to4 tunnel, which IPv6 address is the correct translation of the IPv4 address 192.168.99.1?

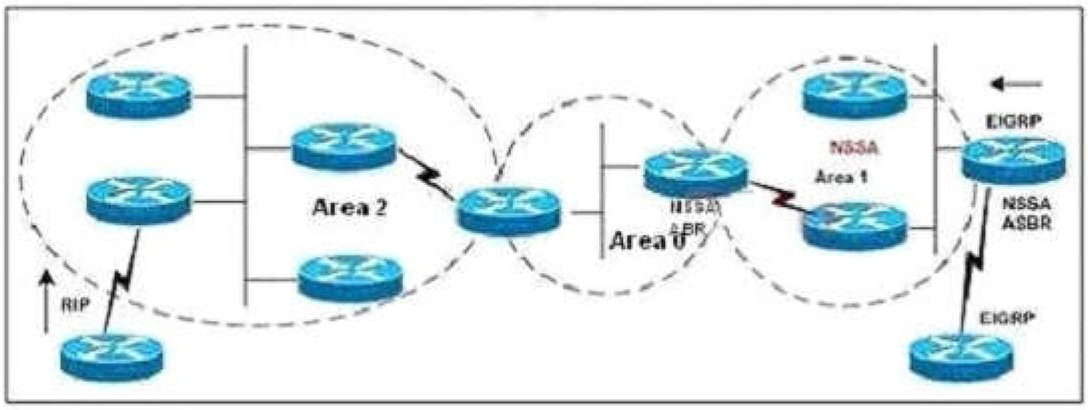
A. c0a8:6301:2002::/48
B. 2002:c0a8:6301::/48
C. 2002:c0a8:6301::/8
D. 2002::/16

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

16 bits for the most significant 6to4 reserved bits (2002::/16) + 32 bits source ipv4 address (traslated in HEX format) = 48 bits.

QUESTION 591
Refer to the exhibit. Will redistributed RIP routes from OSPF Area 2 be allowed in Area 1?



A. Because Area 1 is an NSSA, redistributed RIP routes will not be allowed.
B. Redistributed RIP routes will be allowed in Area 1 because they will be changed into type 5 LSAs in Area 0 and passed on into Area 1.
C. Because NSSA will discard type 7 LSAs, redistributed RIP routes will not be allowed in Area 1.
D. Redistributed RIP routes will be allowed in Area 1 because they will be changed into type 7 LSAs in Area 0 and passed on into Area 1.
E. RIP routes will be allowed in Area 1 only if they are first redistributed into EIGRP.

Correct Answer: A
Section: Mix Questions
Explanation

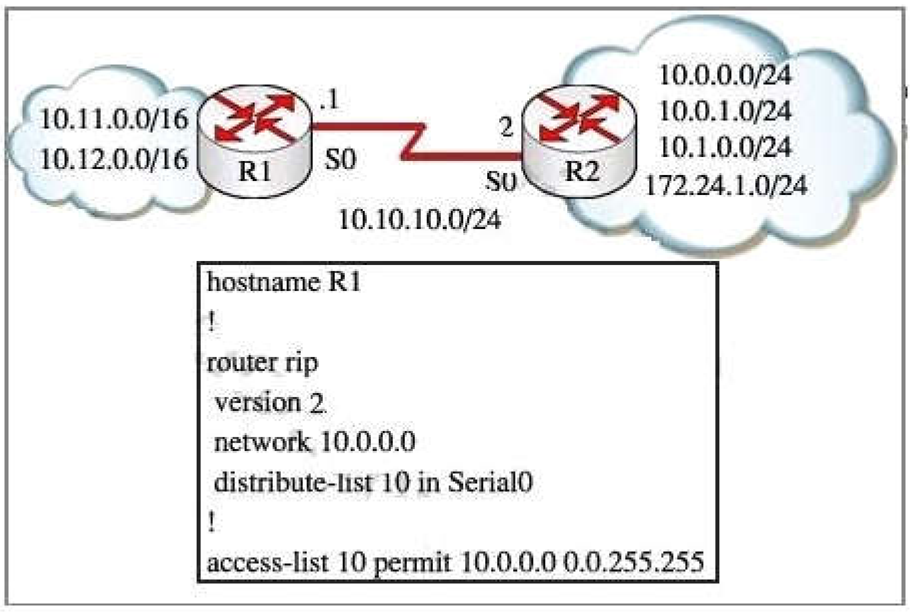
Explanation/Reference:
Explanation:

Area 1 is a NSSA so we can inject EIGRP routes into this area with Type 7 LSAs. Notice that Type 7 LSAs can only be existed in a NSSA. The NSSA ABR of area 1 must converted it into LSA Type 5 before flooding to the whole OSPF domain.

When redistribute RIP into area 2, LSA Type 5 will be created an sent through area 0. But a NSSA is an extension of a stub area. The stub area characteristics still exist, which includes no type 5 LSAs allowed.

Note: A stub area only allows LSA Type 1, 2 and 3.

QUESTION 592
Study this exhibit below carefully.



```
hostname R1
!
router rip
 version 2
 network 10.0.0.0
 distribute-list 10 in Serial0
!
access-list 10 permit 10.0.0.0 0.0.255.255
```

What is the effect of the distribute-list command in the R1 configuration?

A. R1 will permit only the 10.0.0.0/24 route in the R2 RIP updates
B. R1 will not filter any routes because there is no exact prefix match
C. R1 will filter the 10.1.0.0/24 and the 172.24.1.0/24 routes from the R2 RIP updates
D. R1 will filter only the 172.24.1.0/24 route from the R2 RIP updates

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The command “distribute-list 10 in Serial0” will create an incoming distribute list for interface serial 0 and refers to access list 10.
So it will permit routing updates from 10.0.x.x network while other entries (in this case the 10.1.0.0/24 and 172.24.1.0/24 networks) will be filtered out from the routing update received on interface S0.

QUESTION 593
Which three route filtering statements are true? (Choose three)

A. After the router rip and passive-interface s0/0 commands have been issued, the s0/0 interface will not send any RIP updates, but will receive routing updates on that interface.
B. After the router eigrp 10 and passive-interface s0/0 commands have been issued, the s0/0 interface will not send any EIGRP updates, but will receive routing updates on that interface
C. After the router ospf 10 and passive-interface s0/0 commands have been issued , the s0/0 interface will not send any OSPF updates, but will receive routing updates on that interface
D. When you use the passive-interface command with RIPv2, multicasts are sent out the specified interface
E. When you use the passive-interface command with EIGRP, hello messages are not sent out the specified interface
F. When you use the passive-interface command with OSPF, hello messages are not sent out the specified interface

Correct Answer: AEF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

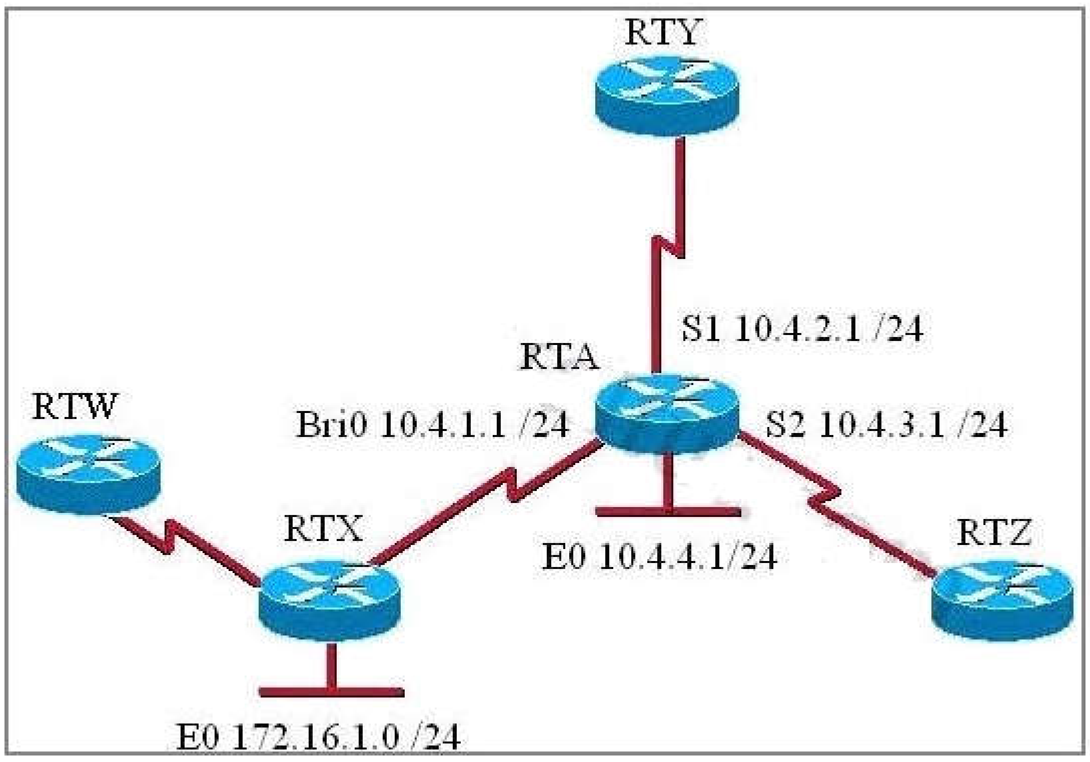
Passive-interface command is used in all routing protocols to disable sending updates out from a specific interface. However the command behavior varies from one protocol to another”

-- In RIP, this command will not allow sending multicast updates via a specific interface but will allow listening to incoming updates from other RIP speaking neighbors. This means that the router will still be able to receive updates on that passive interface and use them in its routing table.

-- In EIGRP and OSPF the passive-interface command stops sending outgoing hello packets, hence the router can not form any neighbor relationship via the passive interface. This behavior stops both outgoing and incoming routing updates.

QUESTION 594
Router RTA is configured as follows:

```
RTA (config)# router rip
RTA(config-router)# network 10.0.0.0
RTA(config-router)# distribute-list 44 in interface BRIO
RTA(config-router)# exit
RTA(config)# access-list 44 deny 172.16.1.0 0.0.0.255
RTA(config)# access-list 44 permit any
```



What are the effects of this RIP configuration on router RTA? (Choose two)

A. no routing updates will be sent from router RTA on interface BRIO to router RTX
B. router RTA will not advertise the 10.0.0.0 network to router RTX
C. the route to network 172.16.1.0 will not be entered into the routing table on router RTA
D. user traffic from the 172.16.1.0 network is denied by access-list 44
E. the routing table on router RTA will be updated with the route to router RTW

Correct Answer: CE
Section: Mix Questions
Explanation

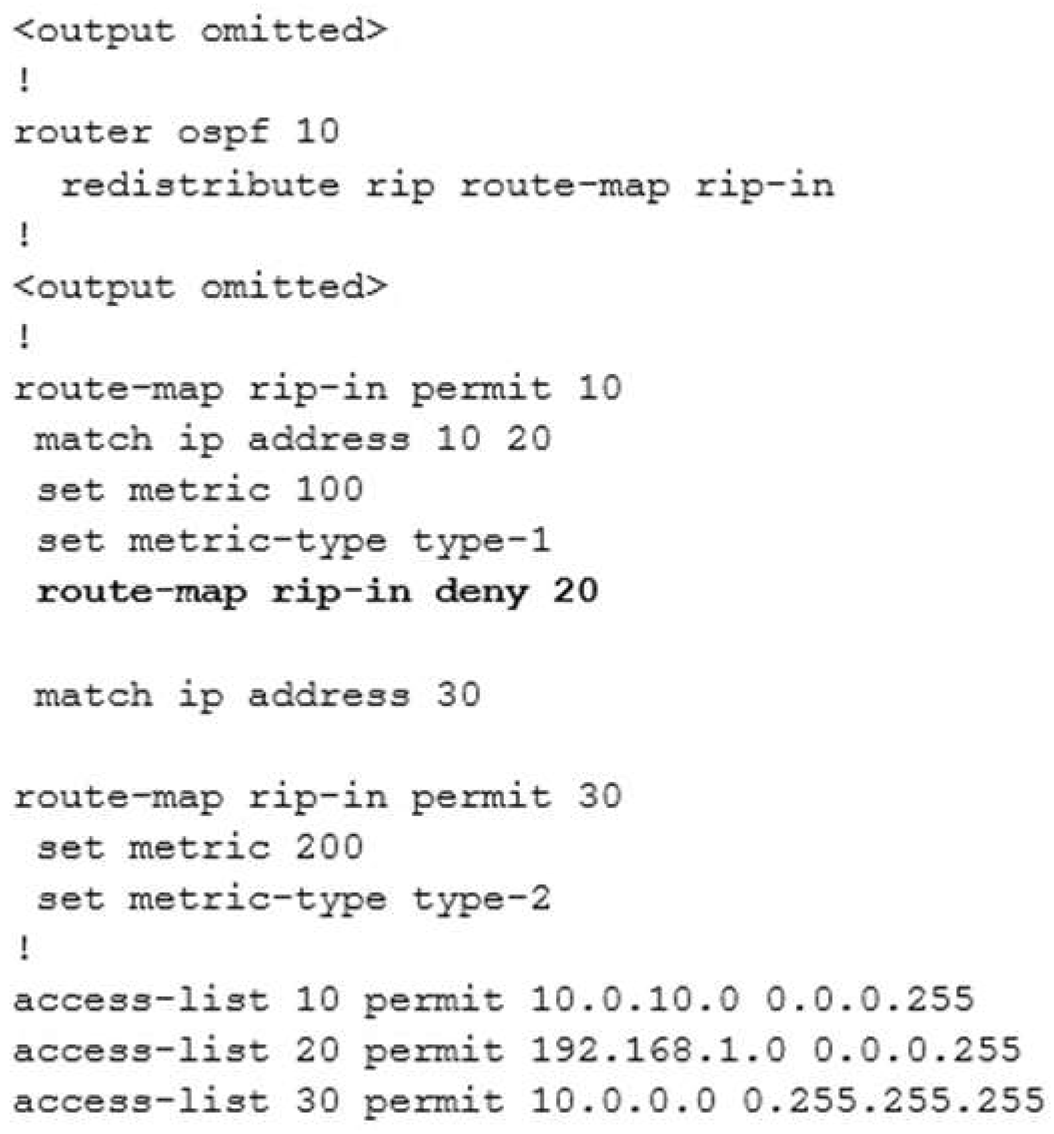
Explanation/Reference:
Explanation:

Distribute list are used to filter routing updates and they are based on access lists. In this case, an access list of 44 was created to deny the route from network 172.16.1.0/24 so this route will not be entered into the routing table of RTA.
But the route from RTW can be entered because it is not filtered by the access list.

A and B are not correct because the distribute list is applied to the inbound direction of interface BRIO so outgoing routing updated will not be filtered.

D is not correct because distribute list just filters routing updates so user traffic from network 172.16.1.0 will not be denied.

QUESTION 595
Refer to the exhibit.



```
<output omitted>
!
router ospf 10
  redistribute rip route-map rip-in
!
<output omitted>
!
route-map rip-in permit 10
 match ip address 10 20
 set metric 100
 set metric-type type-1
 route-map rip-in deny 20

 match ip address 30

route-map rip-in permit 30
 set metric 200
 set metric-type type-2
!
access-list 10 permit 10.0.10.0 0.0.0.255
access-list 20 permit 192.168.1.0 0.0.0.255
access-list 30 permit 10.0.0.0 0.255.255.255
```

Which two statements are correct regarding the routes to be redistributed into OSPF? (Choose two)

A. The network 192.168.1.0 will be allowed and assigned a metric of 100.
B. The network 192.168.1.0 will be allowed and assigned a metric of 200.
C. All networks except 10.0.0.0/8 will be allowed and assigned a metric of 200.
D. The network 172.16.0.0/16 will be allowed and assigned a metric of 200.
E. The network 10.0.10.0/24 will be allowed and assigned a metric of 200.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 596
Into which two types of areas would an area border router (ABR) inject a default route? (Choose two)

A. stub
B. the autonomous system of an exterior gateway protocol (EGP)
C. NSSA
D. totally stubby
E. the autonomous system of a different interior gateway protocol (IGP)
F. area 0

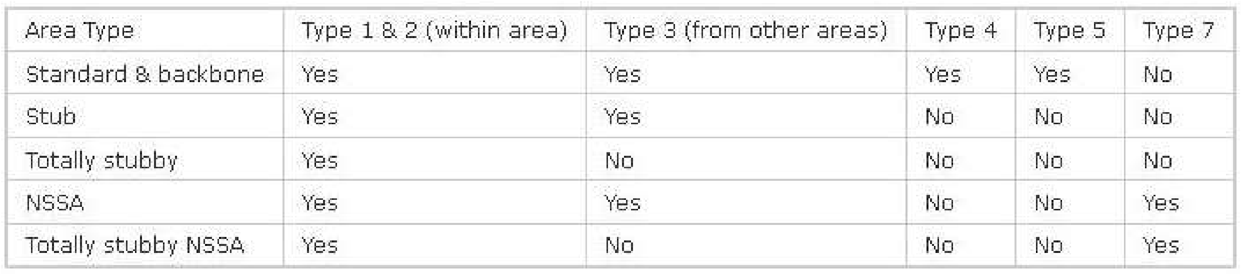
Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Both stub area & totally stubby area allow an ABR to inject a default route. The main difference between these 2 types of areas is:

+ Stub area replaces LSA Type 5 (External LSA – created by an ASBR to advertise network from another autonomous system) with a default route
+ Totally stubby area replaces both LSA Type 5 and LSA Type 3 (Summary LSA – created by an ABR to advertise network from other areas, but still within the AS, sometimes called interarea routes) with a default route.

Below summarizes the LSA Types allowed and not allowed in area types:



Area Type	Type 1 & 2 (within area)	Type 3 (from other areas)	Type 4	Type 5	Type 7
Standard & backbone	Yes	Yes	Yes	Yes	No
Stub	Yes	Yes	No	No	No
Totally stubby	Yes	No	No	No	No
NSSA	Yes	Yes	No	No	Yes
Totally stubby NSSA	Yes	No	No	No	Yes

QUESTION 597
What two situations could require the use of multiple routing protocols? (Choose two)

A. when using UNIX host-based routers
B. when smaller broadcast domains are desired
C. because having multiple routing protocols confuses hackers
D. when migrating from an older Interior Gateway Protocol (IGP) to a new IGP
E. when all equipment is manufactured by Cisco
F. when there are multiple paths to destination networks

Correct Answer: AD
Section: Mix Questions
Explanation

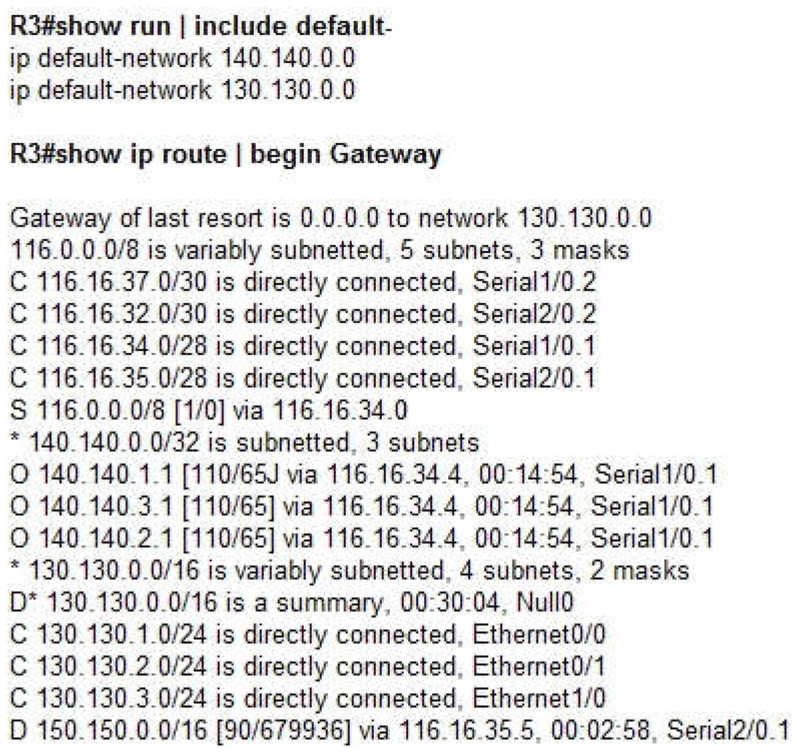
Explanation/Reference:
Explanation:

Simple routing protocols work well for simple networks, but networks grow and become more complex.

While running a single routing protocol throughout your entire IP internetwork is desirable, multiprotocol routing is common for a number of reasons, including company mergers, multiple departments managed by multiple network administrators, multivendor environments, or simply because the original routing protocol is no longer the best choice.

Often, the multiple protocols are redistributed into each other during a migration period from one protocol to the other.

QUESTION 598
Refer to the exhibit. Why is the 140.140.0.0 network not used as the gateway of last resort even though it is configured first?



```
R3#show run | include default-
ip default-network 140.140.0.0
ip default-network 130.130.0.0

R3#show ip route | begin Gateway

Gateway of last resort is 0.0.0.0 to network 130.130.0.0
116.0.0.0/8 is variably subnetted, 5 subnets, 3 masks
C 116.16.37.0/30 is directly connected, Serial1/0.2
C 116.16.32.0/30 is directly connected, Serial2/0.2
C 116.16.34.0/28 is directly connected, Serial1/0.1
C 116.16.35.0/28 is directly connected, Serial2/0.1
S 116.0.0.0/8 [1/0] via 116.16.34.0
* 140.140.0.0/32 is subnetted, 3 subnets
O 140.140.1.1 [110/65J via 116.16.34.4, 00:14:54, Serial1/0.1
O 140.140.3.1 [110/65] via 116.16.34.4, 00:14:54, Serial1/0.1
O 140.140.2.1 [110/65] via 116.16.34.4, 00:14:54, Serial1/0.1
* 130.130.0.0/16 is variably subnetted, 4 subnets, 2 masks
D* 130.130.0.0/16 is a summary, 00:30:04, Null0
C 130.130.1.0/24 is directly connected, Ethernet0/0
C 130.130.2.0/24 is directly connected, Ethernet0/1
C 130.130.3.0/24 is directly connected, Ethernet1/0
D 150.150.0.0/16 [90/679936] via 116.16.35.5, 00:02:58, Serial2/0.1
```

A. The last default-network statement will always be preferred.
B. A route to the 140.140.0.0 network does not exist in the routing table.
C. Default-network selection will always prefer the statement with the lowest IP address.
D. A router will load balance across multiple default-networks; repeatedly issuing the show ip route command would show the gateway of last resort changing between the two networks.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In the routing table of R3, we can only see the route 130.130.0.0/16 is learned via EIGRP (marked with D) and is being chosen as the “Gateway of last resort”.

The route to 140.140.0.0 is not present in the routing table so the command “ip default-network 140.140.0.0” has no effect.

Remember that a route must appear in the routing table (via static route or learned via a routing protocol before it can be set as “Gateway of last resort” by the “ip default-network” command.

QUESTION 599
How is network layer addressing accomplished in the OSI protocol suite?

A. Internet Protocol address
B. Media Access Control address
C. Packet Layer Protocol address
D. Network Service Access Point address
E. Authority and Format Identifier address

Correct Answer: D
Section: Mix Questions
Explanation

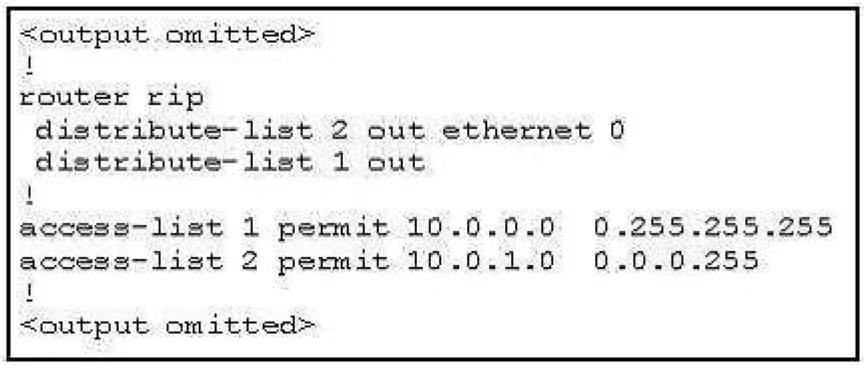
Explanation/Reference:
Explanation:

OSI network-layer addressing is implemented by using two types of hierarchical addresses: network service access-point addresses and network-entity titles.

A network service-access point (NSAP) is a conceptual point on the boundary between the network and the transport layers.
The NSAP is the location at which OSI network services are provided to the transport layer.
Each transport-layer entity is assigned a single NSAP, which is individually addressed in an OSI internetwork using NSAP addresses.

Network Service Address Point (NSAP) address is the equivalent of an IP address for an OSI network; A NSAP address is a hexadecimal address with a length of up to 40 hexadecimal digits.
NSAP addresses are used in ATM and IS-IS.

QUESTION 600
Refer to the exhibit.



```
<output omitted>
!
router rip
 distribute-list 2 out ethernet 0
 distribute-list 1 out
!
access-list 1 permit 10.0.0.0  0.255.255.255
access-list 2 permit 10.0.1.0  0.0.0.255
!
<output omitted>
```

On the basis of the partial configuration, which two statements are correct? (Choose two)

A. Only routes matching 10.0.1.0/24 will be advertised out Ethernet 0.
B. Only routes 10.0.1.0/24 will be sent out all interfaces.
C. Only routes 10.0.1.0/24 will be allowed in the routing table.
D. Only routes matching 10.0.0.0/8 will be advertised out Ethernet 0.
E. Only routes matching 10.0.0.0/8 will be advertised out interfaces other than Ethernet 0.
F. All routes will be advertised out interfaces other than Ethernet 0.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In this case, the following algorithm is used when multiple distribute-lists are used:

1. First check which interface is being sent out. If it is Ethernet 0, distribute-list 2 is applied first. If the network is denied then no further checking is done for this network. But if distribute-list 2 permits that network then distribute-list 1 is also checked. If both distribute-lists allow that network then it will be sent out.

2. If the interface is not Ethernet 0 then only distribute-list 1 is applied.

Now let's take some examples.
+ If the advertised network is 10.0.1.0/24, it will be sent out all interfaces, including Ethernet 0.
+ If the advertised network is 10.0.2.0/24, it will be sent out all interfaces, excepting Ethernet 0.
+ If the advertised network is 11.0.0.0/8, it will be dropped.

Note: It is possible to define one interface-specific distribute-list per interface and one protocol-specific distribute-list for each process/autonomous-system.

QUESTION 601
Which routing protocol will continue to receive and process routing updates from neighbors after the passive interface router configuration command is entered?

A. EIGRP
B. RIP
C. OSPF
D. IS-IS

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 602
Which three statements are true when configuring redistribution for OSPF? (Choose three)

A. The default metric is 10.
B. The default metric is 20.
C. The default metric type is 2.
D. The default metric type is 1.
E. Subnets do not redistribute by default.
F. Subnets redistribute by default.

Correct Answer: BCE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 603
What is the benefit of deploying IPv6 in a campus network using dual stack mode?

A. Dual Stack Mode takes advantage of IPv6 over IPv4 tunnel within a network.
B. IPv4 and IPv6 run alongside one another and have no dependency on each other to function
C. IPv4 and IPv6 share network resources.
D. IPv6 can depend on existing IPv4 routing, QoS, security, and multicast policies.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Deploying IPv6 in the campus using the dual-stack model offers several advantages over the hybrid and service block models.

The primary advantage of a dual stack model is that it does not require tunneling within the campus network.

The dual stack model runs the two protocols as ships in the night, meaning that IPv4 and IPv6 run alongside one another and have no dependency on each other to function except that they share network resources. Both have independent routing.

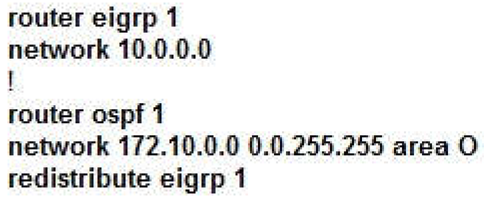
QUESTION 604
To configure 6to4 on a dual-stack edge router. Which three of the following are valid in 6to4 Tunneling configuration? (Choose three)

A. IPv4 Tunnel IP address
B. Tunnel mode (6to4)
C. Tunnel Keepalives
D. IPv4 Tunnel Destination
E. IPv4 Tunnel Source.
F. 6to4 IPv6 address (within 2002::/16)

Correct Answer: BEF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 605
A network administrator is troubleshooting a redistribution of OSPF routes into EIGRP.



```
router eigrp 1
network 10.0.0.0
!
router ospf 1
network 172.10.0.0 0.0.255.255 area O
redistribute eigrp 1
```

Given the exhibited commands, which statement is true?

A. Redistributed routes will have an external type of 1 and a metric of 1.
B. Redistributed routes will have an external type of 2 and a metric of 20.
C. Redistributed routes will maintain their original OSPF routing metric.
D. Redistributed routes will have a default metric of 0 and will be treated as reachable and advertised.
E. Redistributed routes will have a default metric of 0 but will be treated as unreachable and not advertised.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

By default, all routes redistributed into OSPF will be tagged as external type 2 (E2) with a metric of 20, except for BGP routes (with a metric of 1).

Note:

The cost of a type 2 route is always the external cost, irrespective of the interior cost to reach that route.
A type 1 cost is the addition of the external cost and the internal cost used to reach that route.

QUESTION 606
Which three steps are most helpful in verifying proper route redistribution? (Choose three)

A. On the routers not performing the route redistribution, use the show ip route command to see if the redistributed routes show up.
B. On the ASBR router performing the route redistribution, use the show ip protocol command to verify the redistribution configurations.
C. On the ASBR router performing the route redistribution, use the show ip route command to verify that the proper routes from each routing protocol are there.
D. On the routers not performing the route redistribution, use the show ip protocols command to verify the routing information sources.
E. On the routers not performing the route redistribution, use the debug ip routing command to verify the routing updates from the ASBR.

Correct Answer: ABC
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In order to verify proper route redistribution, use the "show ip route" command on all routers within the network, as well as the ABSR, to verify that the routes are properly being advertised to all routers.

In addition, issuing the "show ip protocol" can be used on the router performing the redistribution to verify that routes are being redistributed into each other.

QUESTION 607
A router is configured for redistribution to advertise EIGRP routes into OSPF on a boundary router.
Given the configuration:

router ospf 1
redistribute eigrp 1 metric 25 subnets

What is the **function of the 25 parameter** in the redistribute command?

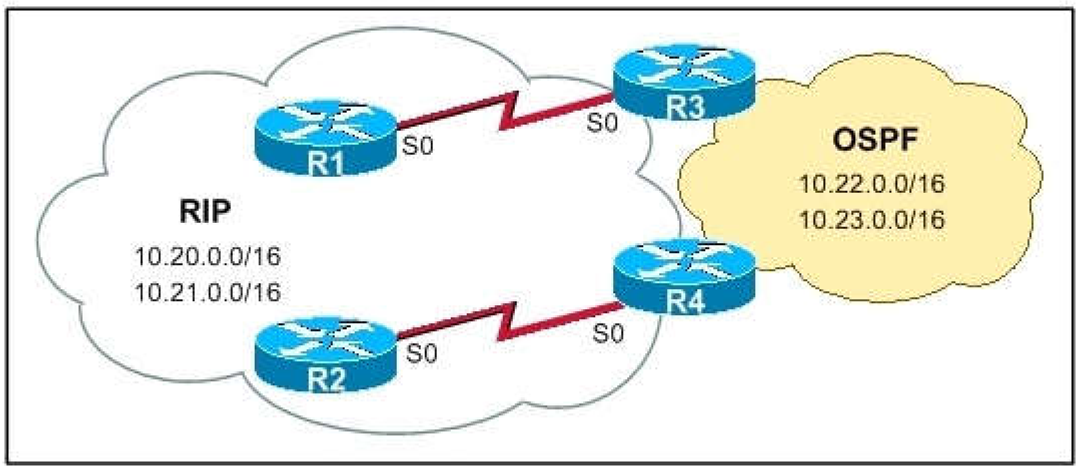
A. It specifies the seed cost to be applied to the redistributed routes.
B. It specifies the administrative distance on the redistributed routes.
C. It specifies the metric limit of 25 subnets in each OSPF route advertisement.
D. It specifies a new process-id to inject the EIGRP routes into OSPF.

Correct Answer: A
Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 608
Refer to the exhibit.



R1 and R2 belong to the RIP routing domain that includes the networks 10.20.0.0/16 and 10.21.0.0/16.
R3 and R4 are performing two-way route redistribution between OSPF and RIP.
A network administrator has discovered that R2 is receiving OSPF routes for the networks 10.20.0.0/16 and 10.21.0.0/16 and a routing loop has occurred.
Which action will correct this problem?

A. Apply an inbound ACL to the R2 serial interface.
B. Change the RIP administrative distance on R3 to 110.
C. Configure distribute-lists on R3 and R4.
D. Set the OSPF default metric to 20.
E. Change the OSPF administrative distance on R3 to 110.

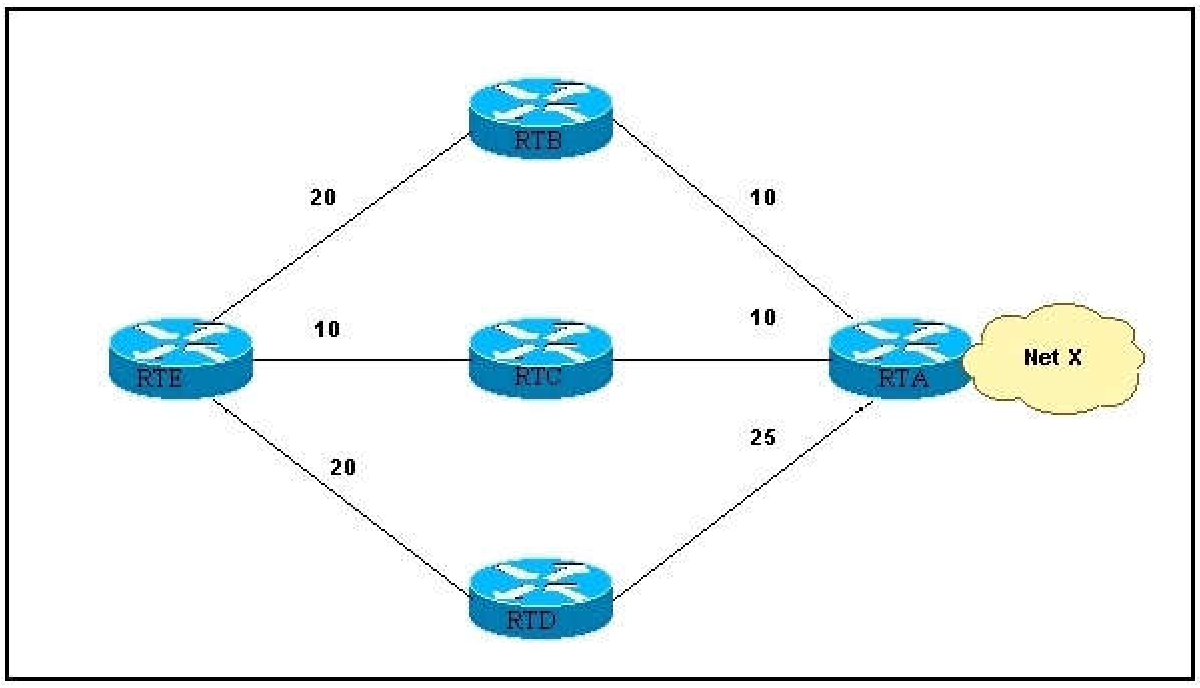
Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Distribute List is Like an access-list, use to deny or permit the routing update to pass through a router/interface.
Distribute List allow you apply an access list to a routing updates.
It can be applied on in or out bond of an interface under a routing process. e.g in fig.

R1 want to send a routing update to it neighbor, this update will go through from interface S0/0, router will check, is there some Distribute List apply to this interface. If there is a Distribute List which would contain the allow route to pass through this interface.

QUESTION 609
Observe the exhibit.



If the command variance 3 were added to RTE, which path or paths would be chosen to route traffic to network X?

A. E-B-A
B. E-B-A and E-C-A
C. E-C-A and E-D-A
D. E-B-A, E-C-A and E-D-A

Correct Answer: B
Section: Mix Questions
Explanation

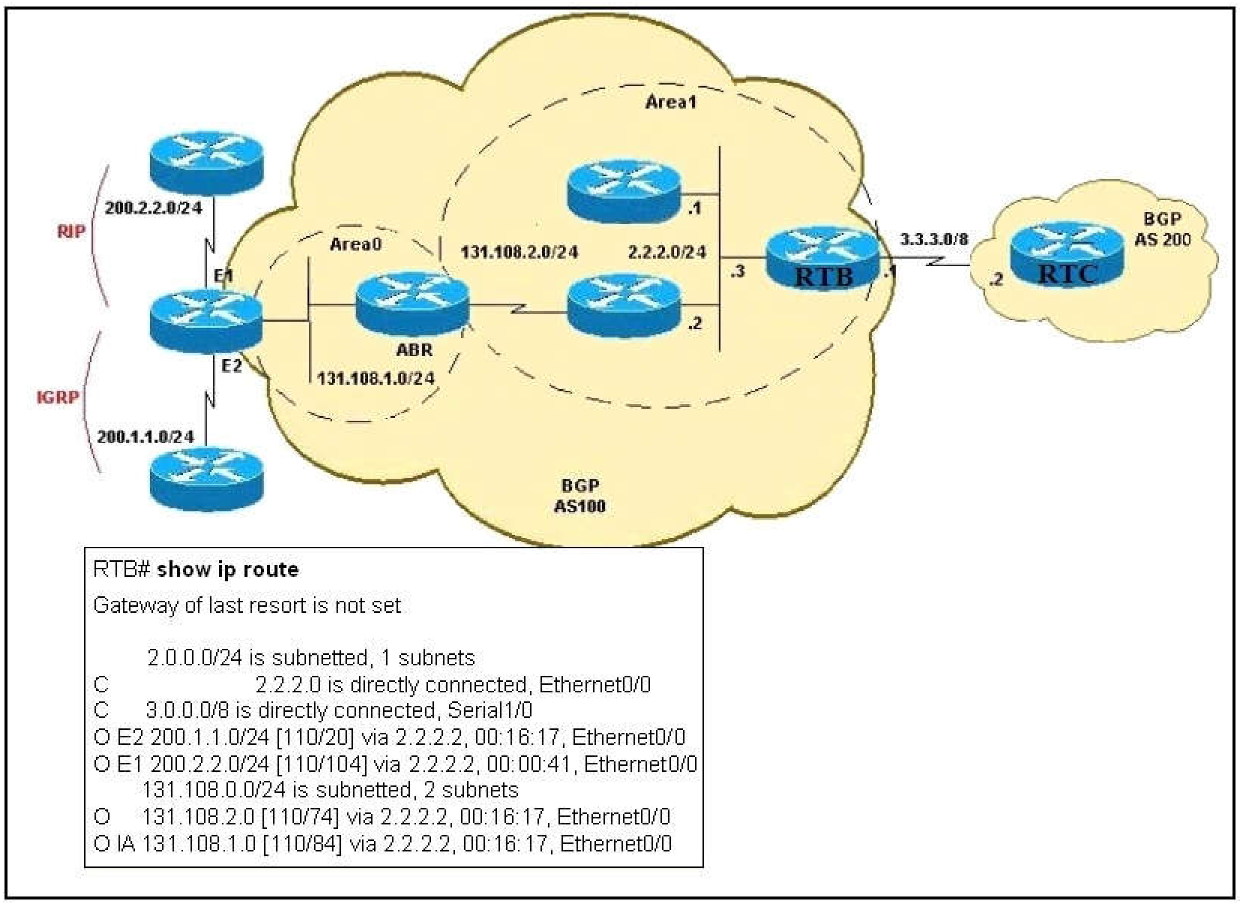
Explanation/Reference:
Explanation:

Advertised distance of RTD is greater than FD of RTE-RTC-RTA, so the route through D will not be used.

Please notice that routes must first satisfy the feasible condition to be considered for “variance” command:
The feasible condition states:
“To qualify as a feasible successor, a router must have an AD less than the FD of the current successor route”.

In this case, the current successor route is E -> C -> A and the FD of this successor route is 20. But the AD of route E-D-A is 25 which is bigger than the FD of the successor route -> It will not be put into the routing table even if the “variance 3” command is used.

QUESTION 610
Which command should be added to RTB under router bgp 100 to allow only the external OSPF routes to be redistributed to RTC?



```
RTB# show ip route
Gateway of last resort is not set

      2.0.0.0/24 is subnetted, 1 subnets
C                 2.2.2.0 is directly connected, Ethernet0/0
C     3.0.0.0/8 is directly connected, Serial1/0
O E2 200.1.1.0/24 [110/20] via 2.2.2.2, 00:16:17, Ethernet0/0
O E1 200.2.2.0/24 [110/104] via 2.2.2.2, 00:00:41, Ethernet0/0
     131.108.0.0/24 is subnetted, 2 subnets
O    131.108.2.0 [110/74] via 2.2.2.2, 00:16:17, Ethernet0/0
O IA 131.108.1.0 [110/84] via 2.2.2.2, 00:16:17, Ethernet0/0
```

A. redistribute ospf 1
B. redistribute ospf 1 match external 1
C. redistribute ospf 1 match external 2
D. redistribute ospf 1 match external 1 external 2

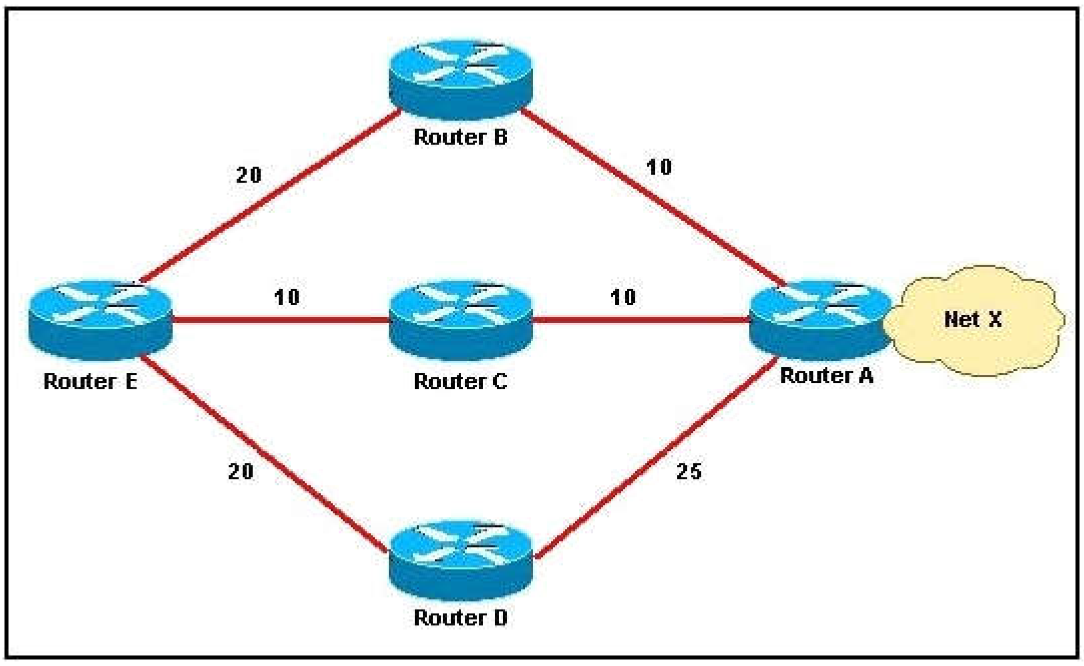
Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Use the external keyword along with the redistribute command under router bgp to redistribute OSPF external routes into BGP.

With the external keyword, you have three choices:
1. redistribute both external type-1 and type-2 (Default)
2. redistribute type-1
3. redistribute type-2 Enter the commands in the configuration mode as described here:
 RTB(config-router)# router bgp 100
 RTB(config-router)# redistribute ospf 1 match external.

QUESTION 611
Router E is configured with the EIGRP variance 2 command.



What path will Router E take to reach Router A?

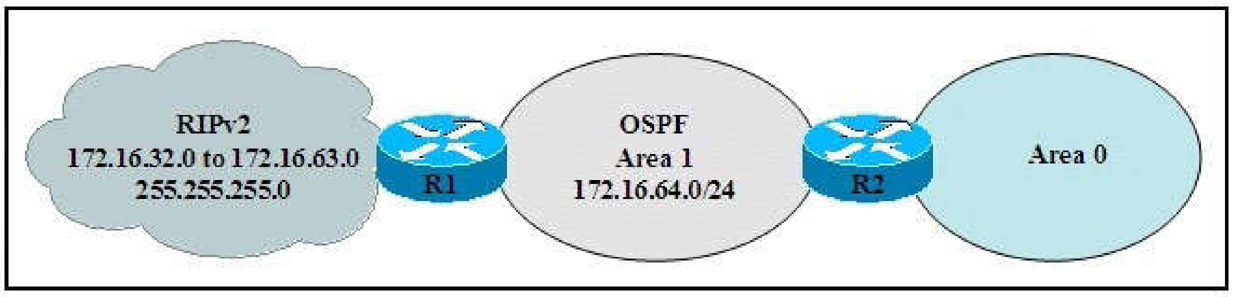
A. only E-D-A
B. only E-B-A
C. only E-C-A
D. both E-B-A and E-C-A
E. both E-B-A and E-D-A
F. all available paths.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

By using the "variance 2" command we can share traffic to other feasible successor routes.
But by default, EIGRP only shares traffic to 4 paths. So we need to use the "maximum-paths 6" to make sure all of these routes are used.

QUESTION 612
A network administrator recently redistributed RIP routes into an OSPF domain.
However, the administrator wants to configure the network so that instead of 32 external type-5 LSAs flooding into the OSPF network, there is only one.



What must the administrator do to accomplish this?

A. Configure summarization on R1 with area 1 range 172.16.32.0 255.255.224.0
B. Configure summarization on R1 with summary-address 172.16.32.0 255.255.224.0
C. Configure area 1 as a stub area with area 1 stub
D. Configure area 1 as a NSSA area with area 1 stub nssa

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In many cases, the router doesn't even need specific routes to each and every subnet (for example, 172.16.1.0/24).
It would be just as happy if it knew how to get to the major network (for example, 172.16.0.0/16) and let another router take it from there.
In our telephone network example, the local telephone switch should only need to know to route a phone call to the switch for the called area code.
Similarly, a router's ability to take a group of subnetworks and summarize them as one network (in other words, one advertisement) is called route summarization.
Besides reducing the number of routing entries that a router must keep track of, route summarization can also help protect an external router from making multiple changes to its routing table due to instability within a particular subnet.

For example, let's say that we were working on a router that connected to 172.16.2.0/24. As we were working on the router, we rebooted it several times. If we were not summarizing our routes, an external router would see each time 172.16.2.0/24 went away and came back. Each time, it would have to modify its own routing table. However, if our external router were receiving only a summary route (i.e., 172.16.0.0/16), then it wouldn't have to be concerned with our work on one particular subnet. This is especially a problem for EIGRP, which can create stuck in active (SIA) routes that can lead to a network melt-down.

Summarization Example We have the following networks that we want to advertise as a single summary route:
* 172.16.100.0/24 * 172.16.101.0/24 * 172.16.102.0/24 * 172.16.103.0/24 * 172.16.104.0/24 * 172.16.105.0/24 * 172.16.106.0/24

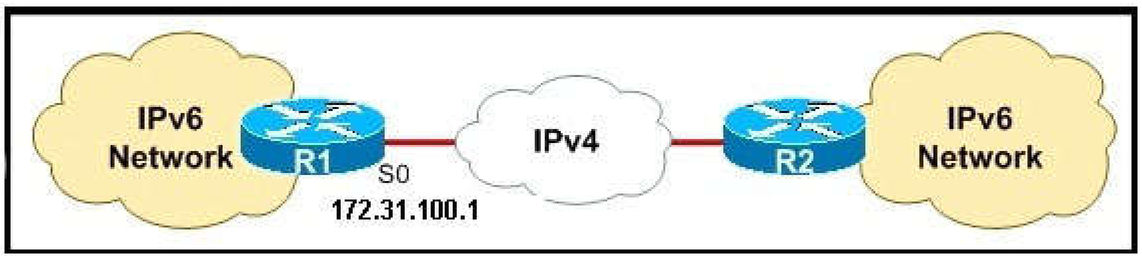
QUESTION 613
Under which circumstance can TCP starvation occur?

A. when HTTP and HTTPS traffic are transmitted on the same link
B. when TCP and UDP traffic are mixed in the same class of service
C. when DNS TFTP traffic are transmitted on the same link
D. when UDP traffic is processed in a policy-map before TCP traffic
E. when TCP traffic is blocked by an ACL

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 614
Refer to the exhibit.



If R1 is configured for 6to4 tunneling, what will the prefix of its IPv6 network be?

A. 1723:1100:1::/48
B. FFFF:AC1F:6401::/16
C. AC1F:6401::/32
D. 2002:AC1F:6401::/48
E. 3FFE:AC1F:6401::/32

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 615
Which protocols support DMVPN?

A. EIGRP
B. RIP2
C. OSPF
D. BGP
E. ISIS

Correct Answer: ACD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Some documents say RIPv2 also supports DMVPN but, EIGPR, OSPF and BGP are the better choices, so we should choose them.

Several routing protocols can be used in a DMVPN design, including:

Enhanced Interior Gateway Protocol (EIGRP)
Open Shortest Path First (OSPF)
Routing Information Protocol version 2 (RIPv2)
Border Gateway Protocol (BGP)
On-Demand Routing (ODR)

https://www.cisco.com/c/dam/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/dmvpn_design_guide.pdf#wp37674

https://www.networkcomputing.com/networking/cisco-dmvpn-choosing-right-routing-protocol/1432661326

QUESTION 616
An EUI-64 bit address is formed by adding a reserved 16-bit value, in which position of the Mac address?

A. between the vendor OID and the NIC-specific part of the MAC address.
B. after the NIC-specific part of the MAC address.
C. before the vendor OID part of the MAC address.
D. anywhere in the Mac address, because the value that is added is reserved.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 617
An EUI-64 bit address is formed by inserting which 16-bit value into the MAC address of a device?

A. 3FFE
B. FFFE
C. FF02
D. 2001

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 618
By default, which type of IPv6 address is used to build the EUI-64 bit format?

A. unique-local address
B. IPv4-compatible IPv6 address
C. link-local address
D. aggregatable-local address

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:

https://howdoesinternetwork.com/2013/slaac-ipv6-stateless-address-autoconfiguration

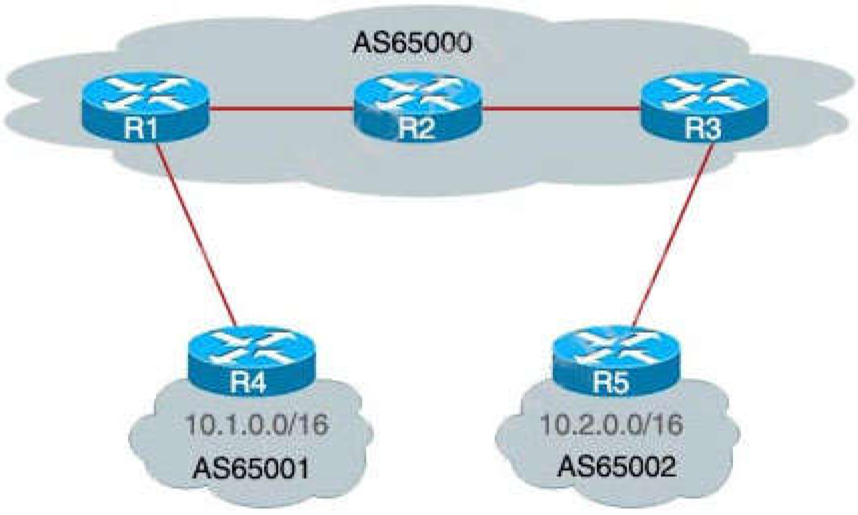
QUESTION 619
What is the minimum privilege level to enter all commands in usermode?

A. Level 1
B. Level 0
C. Level 14
D. Level 15

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 620



Refer to exhibit. If the IGP in AS65000 is RIPv2, which networks are displayed when you enter show ip route on router R2?

A. VLSM subnets in 10.0.0.0/16 and the major network 10.2.0.0/16 only
B. VLSM subnets in 10.0.0.0/16 and the major network 10.2.0.0/16 only
C. VLSM subnets in 10.0.0.0/16 only
D. major networks 10.1.0.0/16 and 10.2.0.0/16 only
E. VLSM subnets in 10.0.0.0/16 and the major networks 10.1.0.0/16 10.2.0.0/16

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 621
Which of the following situations results in a routing loop?

A. when you have a single point of redistribution
B. when you use NAT translation on the edge of your network
C. when you implement contiguous IP routing blocks
D. when you implement noncontiguous IP routing blocks
E. when you have multiple points of redistribution

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 622
Which two options are limitations of stateful NAT64? (Choose Two)

A. It is unable to route VRF traffic.

B. It is unable to route multicast traffic.
C. It supports FTP traffic only with an ALG.
D. It supports DNS64 only.
E. Layer 4 supports TCP only

Correct Answer: AB
Section: Mix Questions
Explanation

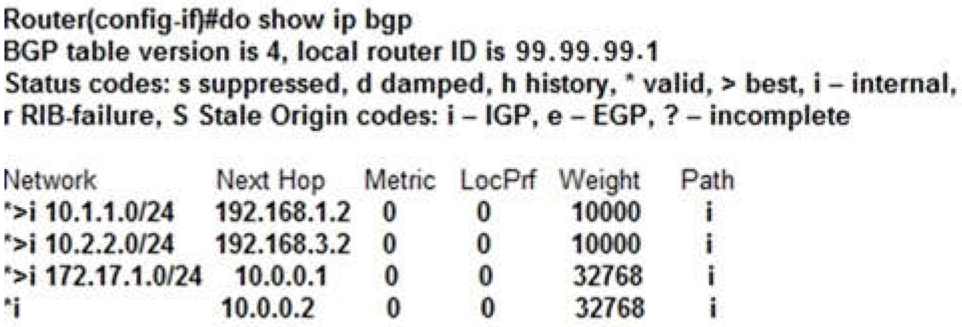
Explanation/Reference:
Explanation:

Restrictions for Configuring Stateful Network Address Translation 64

- Applications without a corresponding application-level gateway(ALG) may not work properly with the Stateful NAT64 translator.
- IP Multicast is not supported.
- The translation of IPv4 options,IPv6 routing headers,hop-by-hop extension headers,destination option headers,and source routing headers is not supported.
- Virtual routing and forwarding(VRF)-aware NAT64 is not supported.
- When traffic flows from IPv6 to IPv4,the destination IP address that you have configured mustmatch a stateful prefix to prevent hairpinning loops.However,the source IPaddress (source address of the IPv6 host) must not match the stateful prefix.If the source IP address matches the stateful prefix,packets are dropped. Hair pinning allows two endpoints inside Network Address Translation(NAT) to communicate with each other,even when the endpoints use only each other's external IPaddresses and ports for communication.
- Only TCP and UDP Layer4 protocols are supported for header translation.
- Route maps are not supported.
- Application-level gateways (ALGs) FTP and ICMP are not supported.
- In the absence of apre-existing state in NAT64,stateful translation only supports IPv6-initiated sessions.
- If a static mapping host-binding entry exists for an IPv6 host,the IPv4 nodes can initiate communication. In dynamic mapping,IPv4 nodes can initiate communication only if a host-binding entry is created for the IPv6 host through a previously established connection to the same or a different IPv4 host. Dynamic mapping rules that use Port-Address Translation(PAT),host-binding entries cannot be created because IPv4-initiated communication not possible through PAT.
- Both NAT44 (static,dynamic and PAT)configuration and stateful NAT64 configuration are not supported on the same interface.

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/nat-xe-3s-book/iadnat-stateful-nat64.pdf

QUESTION 623
Which next hop is going to be used for 172.17.1.0/24 ?



```
Router(config-if)#do show ip bgp
BGP table version is 4, local router ID is 99.99.99.1
Status codes: s suppressed, d damped, h history, * valid, > best, i – internal,
r RIB-failure, S Stale Origin codes: i – IGP, e – EGP, ? – incomplete

Network          Next Hop     Metric  LocPrf  Weight   Path
*>i 10.1.1.0/24  192.168.1.2   0       0      10000     i
*>i 10.2.2.0/24  192.168.3.2   0       0      10000     i
*>i 172.17.1.0/24  10.0.0.1    0       0      32768     i
*i                 10.0.0.2    0       0      32768     i
```

A. 10.0.0.1
B. 192.168.1.2
C. 10.0.0.2
D. 192.168.3.2

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
The > indicates the best route to the destination 172.17.1.0/24
Reference: https://www.cisco.com/c/en/us/td/docs/ios/iproute_bgp/command/reference/irg_book/irg_bgp5.html#wp1156281

QUESTION 624
What are two limitations when in use of NPTv6 for IPV6 vs IPV6 Address translation?

A. stateful address translation
B. a limit of 32 1-to-1 translations
C. lack of overloading functionality
D. identify all interfaces NAT inside or outside
E. 1-to-1 prefix rewrite
F. mismatched prefix allocations

Correct Answer: CF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

So what is NPTv6? NPTv6 is simply rewriting IPv6 prefixes. If your current IPv6 prefix is 2001:db8:cafe::/48 then using NPTv6 it would allow you to change it to 2001:db8:fea7::/48 – that is it.

It is a one for one prefix rewrite – you can’t overload it, have mismatching prefix allocations sizes, re-write ports or anything else. Importantly, it doesn’t touch anything other than the prefix. Your network/host portion remains intact with no changes.

http://www.howfunky.com/2012/02/ipv6-to-ipv6-network-prefix-translation.html

QUESTION 625
Which two statements about NHRP in a DMVPN environment are true? (Choose two)

A. It can authenticate VPN endpoints.
B. It can identify PIM-SM RPs over a tunnel.
C. It routes traffic through the tunnel.
D. It provides address resolution to route traffic
E. It requires each endpoint to have a unique network ID.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 626
Which set of actions does a network engineer perform to set the IPv6 address of a DHCP relay server at the VLAN interface level?

A. Enter the VLAN interface configuration mode and define the IPv6 address of a DHCP relay server
B. Enter the global configuration mode and enable the IPv6 DHCP relay
C. Enter the global configuration mode, enable IPv6 DHCP relay from interface configuration mode and define the IPv6 address of a DHCP relay server
D. Enter the VLAN interface configuration mode, enable IPv6 DHCP relay, and define the IPv6 address of a DHCP relay server

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

You can accept DHCP requests from clients on the associated context or VLAN interface and enable the DHCP relay agent by using the ipv6 dhcp relay enable command (for IPv6) or the ip dhcp relay enable command (for IPv4).
The DHCP relay starts forwarding packets to the DHCP server address specified in the ipv6 dhcp relay server command or the ip dhcp relay server command for the associated context or VLAN interface.

An example of how to set the IPv6 address of a DHCP relay server at the VLAN interface level:

```
host1/Admin(config)# interface vlan 50
host1/Admin(config-if)# ipv6 dhcp relay enable
host1/Admin(config-if)# ipv6 dhcp relay server 2001:DB8:1::1/64
```

Reference: https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/command/reference/ACE_cr/if.html

QUESTION 627
Which two types of authentication does EIGRP offer? (Choose two)

A. TKIP
B. MD5
C. WPA
D. Plain text

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The router uses two types of authentication:
• Simple password authentication (also called plain text authentication)—Supported by Integrated System-Integrated System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol Version 2 (RIPv2)

• MD5 authentication—Supported by OSPF, RIPv2, BGP, and EIGRP

If the service password-encryption command is not used when implementing EIGRP authentication, the key-string will be stored as plain text in the router configuration. If you configure the service password-encryption command, the key-string will be stored and displayed in an encrypted form; when it is displayed, there will be an encryption-type of 7 specified before the encrypted key-string.

EIGRP originally only supported MD5 authentication but since IOS 15.1(2)S and 15.2(1)T we can also use SHA-256 authentication. Nowadays, this form of authentication is far more secure than MD5.

They ask for 2 options. The one that we know MD5 and the must lose to the reality is plain text. However I didn´t find and official article that mentioned plain Text.
The router uses two types of authentication:

• Simple password authentication (also called plain text authentication)—Supported by Integrated System-Integrated System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol Version 2 (RIPv2)
• MD5 authentication—Supported by OSPF, RIPv2, BGP, and EIGRP

Plaint text is NOT supported in EIGRP.
In EIGRP supported only MD5 and SHA but this is the more acceptable choice

QUESTION 628
Refer to the following:

Logging Console 7

Which option is one of the effects entering this command on a Cisco IOS router, with no additional logging configuration?

A. Debug messages can be seen on the console by enabling "terminal monitor."
B. Debug messages are logged only on active console connections.
C. A user that is connected via SSH sees level 7 messages
D. The router can experience high CPU utilization

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Console logging: By default, the router sends all log messages to its console port. Hence only the users that are physically connected to the router console port can view these messages.

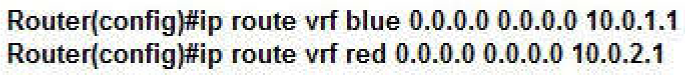
The router does not check if a user is logged into the console port or a device is attached to it; if console logging is enabled, messages are always sent to the console port that can cause CPU load.

To stop the console logging, use the “no logging console” global configuration command. You might want to limit the amount of messages sent to the console with the “logging console level” configuration command (for example, logging console Informational).

Reference:

http://blog.router-switch.com/2013/12/configure-logging-in-cisco-ios/

QUESTION 629
Refer to the exhibit.



```
Router(config)#ip route vrf blue 0.0.0.0 0.0.0.0 10.0.1.1
Router(config)#ip route vrf red 0.0.0.0 0.0.0.0 10.0.2.1
```

After configuring the routes, the network engineer executes the show ip route command. What is the expected results?

A. Gateway of last resort is 10.0.2.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 2 subnets
C 10.0.2.0 is directly connected, FastEthernet0/0 10.0.1.0 is directly connected, FastEthernet0/1
S*0.0.0.0/0 [1/0] via 10.0.2.1(1/0] via 10.0.1.1
B. Gateway of last resort is 10 0.2 1 to network 0.0.0.0 10 0.0 0/24 is subnetted, 1 subnet
C 10.0.2.0 is directly connected, FastEthernet0/0
S* 0.0.0 0/0 [1/0] via 10.0.2.1
C. Gateway of last report is not set
D. Gateway of test resort is 10.0.1.1 to network 0.0.0.0 10.0.0.0/24 is subnetted 1 subnet
C 10.0.1.0 is directly connected FastEthernet0/1
S*0.0.0.0/0 [1/0] via 10.0.1.1

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

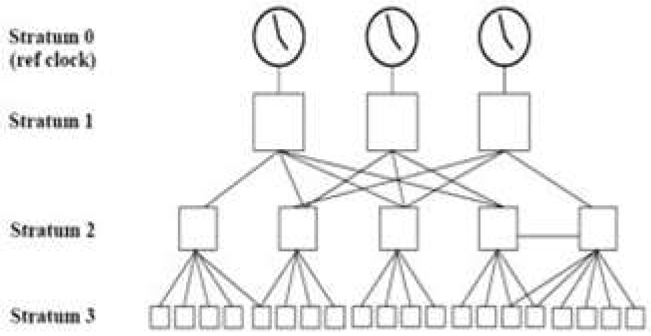
QUESTION 630
Which two statements about NTP stratum are true? (Choose two)

A. Stratum 15 indicates a device that is not synchronized
B. Stratum 1 devices receive their time from a peer that is connected directly to an authoritative time source.
C. The highest stratum level a synchronized device can have is 16.
D. Stratum 2 devices receive their time from a peer that is connected directly to an authoritative time source
E. Stratum 0 devices are connected directly to an authoritative time source
F. Stratum 1 devices are connected directly to an authoritative time source

Correct Answer: DF
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The stratum levels define the distance from the reference clock. A reference clock is a stratum 0 device that is assumed to be accurate and has little or no delay associated with it. Stratum 0 servers cannot be used on the network but they are directly connected to computers which then operate as stratum-1 servers. A stratum 1 time server acts as a primary network time standard.



A stratum 2 server is connected to the stratum 1 server; then a stratum 3 server is connected to the stratum 2 server and so on. A stratum 2 server gets its time via NTP packet requests from a stratum 1 server. A stratum 3 server gets its time via NTP packet requests from a stratum-2 server... A stratum server may also peer with other stratum servers at the same level to provide more stable and robust time for all devices in the peer group (for example a stratum 2 server can peer with other stratum 2 servers).

NTP uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. **A stratum 1 time server typically has an authoritative time source** (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

Reference:

https://www.cisco.com/c/en/us/td/docs/routers/asr920/configuration/guide/bsm/16-6-1/b-bsm-xe-16-6-1-asr920/bsm-time-calendar-set.html

QUESTION 631
Which two statements about OSPF E1 routes are true? (Choose two)

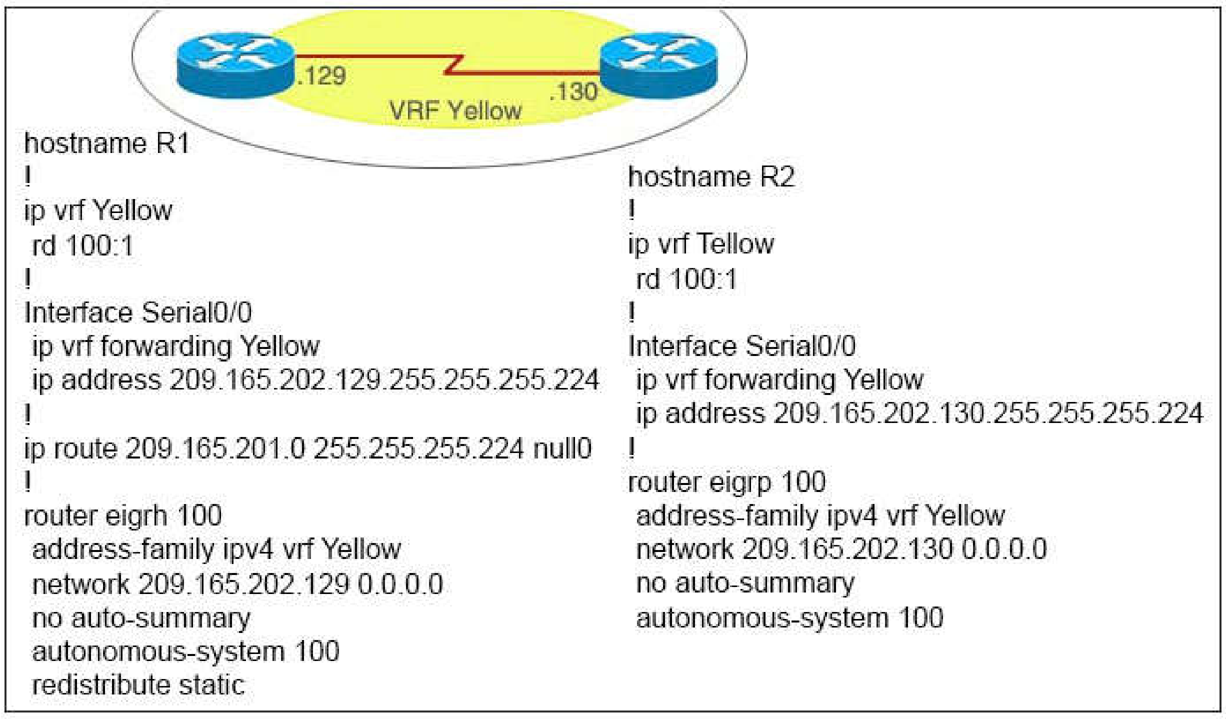
A. They are preferred over interarea routes
B. They use the OSPF cost from redistribution and the OSPF cost to the ASBR.
C. They are preferred over E2 routes
D. They use only the OSPF cost to the ASBR
E. They use only the OSPF cost from redistribution

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:
Reference:

http://blog.ine.com/2011/04/04/understanding-ospf-external-route-path-selection/

QUESTION 632



```
hostname R1
!
ip vrf Yellow
 rd 100:1
!
Interface Serial0/0
 ip vrf forwarding Yellow
 ip address 209.165.202.129.255.255.255.224
!
ip route 209.165.201.0 255.255.255.224 null0
!
router eigrh 100
 address-family ipv4 vrf Yellow
 network 209.165.202.129 0.0.0.0
 no auto-summary
 autonomous-system 100
 redistribute static
```

```
hostname R2
!
ip vrf Tellow
 rd 100:1
!
Interface Serial0/0
 ip vrf forwarding Yellow
 ip address 209.165.202.130.255.255.255.224
!
router eigrp 100
 address-family ipv4 vrf Yellow
 network 209.165.202.130 0.0.0.0
 no auto-summary
 autonomous-system 100
```

A senior network engineer tries to propagate a summary route 209.165.201.0/27 to R2 by redistributing static route on R1, but setup is not working. What is the issue with the configuration in the exhibit?

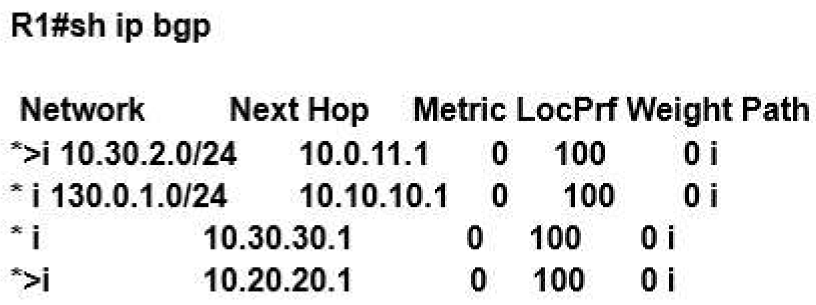
A. The summary route is in the global routing table.
B. The wildcard bit in network command is incorrect.
C. The redistribute command is in the wrong address-family.
D. The route target is missing.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Two connected interfaces S0/0 are in VRF Yellow so we have to put the static route into this VRF too.
So it should be “ip route vrf Yellow 209.165.202.129 255.255.255.224 null0”.

QUESTION 633
Refer to the exhibit.



```
R1#sh ip bgp

 Network        Next Hop     Metric LocPrf Weight Path
*>i 10.30.2.0/24      10.0.11.1      0    100       0 i
* i 130.0.1.0/24      10.10.10.1    0     100       0 i
* i                 10.30.30.1         0    100    0 i
*>i                 10.20.20.1         0    100    0 i
```

Based on the output, which option is the next hop to get to the 130.0.1.0/24 network?

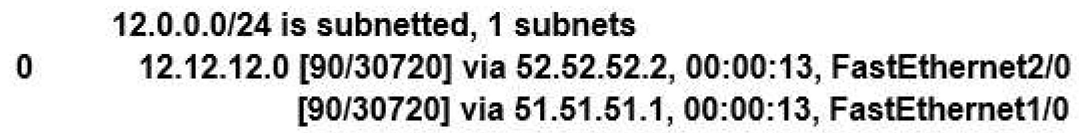
A. 10.30.30.1
B. 10.0.11.1
C. 10.20.20.1
D. 10.10.10.1

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

This is the BGP routing table. Only the best entry of each prefix (marked with “>”) is placed into the routing table. In the output above, the next hop 130.0.1.0/24 network can be reached via three next hops (which are 10.10.10.1; 10.30.30.1 and 10.20.20.1) but only 10.20.20.1 is the best path and is placed into the routing table.

QUESTION 634
Refer to the exhibit.



```
          12.0.0.0/24 is subnetted, 1 subnets
 0          12.12.12.0 [90/30720] via 52.52.52.2, 00:00:13, FastEthernet2/0
                       [90/30720] via 51.51.51.1, 00:00:13, FastEthernet1/0
```

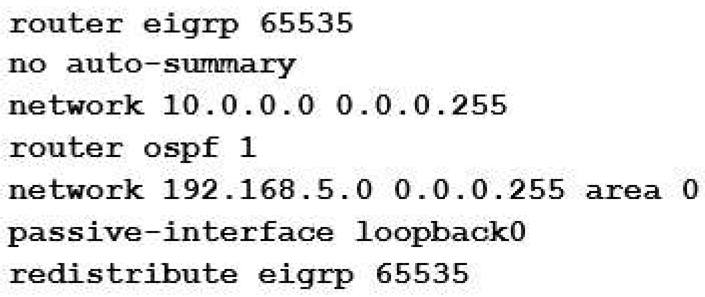
The excerpt was taken from the routing table of router SATX.
Which option ensures that routes from 51.51.51.1 are preferred over routes from 52.52.52.2?

A. SATX(config-router)distance 90 51.51.51.1 0.0.0.0
B. SATX(config-router)distance 89.52.52.52.2 0.0.0.0
C. SATX(config-router)distance 90.52.52.52.2 0.0.0.0
D. SATX(config-router)administrative distance 91 51.51.51 0.0.0.0
E. SATX(config-router)distance 89 51.51.51.1 0.0.0.0
F. SATX(config-router)administrative distance 91 52.52.52.2 0.0.0.0

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 635
Refer to the exhibit.



```
router eigrp 65535
no auto-summary
network 10.0.0.0 0.0.0.255
router ospf 1
network 192.168.5.0 0.0.0.255 area 0
passive-interface loopback0
redistribute eigrp 65535
```

If this configuration is applied to a device that redistributes EIGRP routes into OSPF. which two statements about the behavior of the device are true? (Choose Two)

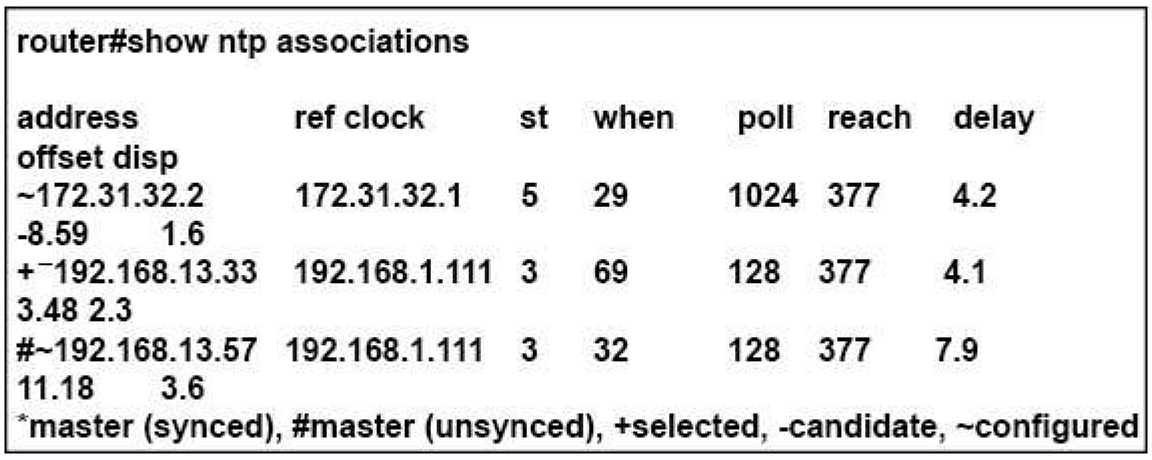
A. EIGRP routes appears in the routing table as E2 OSPF routes
B. The device router ID is set to Loopback0 automatically
C. The device redistributes all EIGRP networks into OSPF
D. EIGRP routes appears in the routing table as N2 OSPF routes
E. The device redistributes only classful EIGRP networks into OSPF.

F. EIGRP routes appears as type 3 LSAs in the OSPF database.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 636
Refer to the exhibit.



```
router#show ntp associations

address           ref clock      st   when     poll  reach   delay
offset disp
~172.31.32.2      172.31.32.1    5    29       1024  377      4.2
-8.59      1.6
+¯192.168.13.33   192.168.1.111  3    69       128   377     4.1
3.48 2.3
#~192.168.13.57  192.168.1.111   3    32       128   377     7.9
11.18      3.6
*master (synced), #master (unsynced), +selected, -candidate, ~configured
```

A network engineer has configured NTP on a Cisco router, but the time on the router is still incorrect. What is the reason for this problem?

A. The router is not syncing with the peer, even though the NTP request and response packets are being exchanged.
B. The router is not syncing with peer, and the NTP request and response packets are not being exchanged.
C. The router is syncing with the peer, and the NTP request and response packets are being exchanged.
D. The router is dropping all NTP packets.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In the output you can see a * next to the ip address that is the primary NTP server.

Also the 377 that means everything was received and processed.
Negotiation done.

https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html

377 = 1 1 1 1 1 1 1 1 Time 0: Last eight responses from server were received
376 = 1 1 1 1 1 1 1 0 Time 1: Last NTP response was NOT received (lost in network)

Values below this 376 is that Last NTP response was received

QUESTION 637
Which action can you take to mitigate unicast flooding in a network?

A. Configure VLANs to span multiple access-layer switches.
B. Implement a nonlooped network topology.
C. Set the ARP timer value to less than the CAM timer value.
D. Set the CAM timer value to less than the ARP timer value.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 638
Which two technologies can encapsulate an IPv6 payload in an IPv4 packet for transmission across a network? (Choose Two)

A. L2TPv3
B. trunking
C. AToM
D. ISATAP
E. NAT-PT

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The Network Address Translator – Protocol Translator (NAT-PT) defines a set of network-layer translation mechanisms designed to allow nodes that only support IPv4 to communicate with nodes that only support IPv6, during the transition to the use of IPv6 in the Internet.

NAT-PT provides IPv4/IPv6 protocol translation. It resides within an IP router, situated at the boundary of an IPv4 network and an IPv6 network. By installing NAT-PT between an IPv4 and IPv6 network, all IPv4 users are given access to the IPv6 network without modification in the local IPv4-hosts (and vice versa). Equally, all hosts on the IPv6 network are given access to the IPv4 hosts without modification to the local IPv6-hosts. This is accomplished with a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries

Reference:
http://www.ietf.org/rfc/rfc4966.txt
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps8802/ps6969/ps1835/prod_white_paper09186a008011ff51_ps6640_Products_White_Paper.html

ISATAP tunneling (Intra-Site Automatic Tunnel Addressing Protocol): is a mechanism for transmitting IPv6 packets over IPv4 network. The word “automatic” means that once an ISATAP server/router has been set up, only the clients must be configured to connect to it.

QUESTION 639
Which command do you enter to filter only routing updates that are sent through interface GigabitEthernet0/0?

A. R1(config-if)# passive-interface GigabitEthernet0/0.
B. R1(config-router)# no passive-interface GigabitEthernet0/0
C. R1(config-router)# passive-interface GigabitEthernet0/0
D. R1(config-router)# passive-interface default
E. R1(config-if)# passive-interface default
F. R1(config-router)# distribute-list 1 out GigabitEthernet0/0

Correct Answer: F
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 640
Which value does a point-to-point GRE tunnel use to identify a peer?

A. MAC address
B. configured multicast address.
C. DLCI
D. IP address
E. VC ID

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 641
Where must a network engineer configure the **ip helper-address** command on a router?

A. on the global configuration mode
B. on the DHCP configuration
C. on the interface that will receive the broadcasts
D. on the interface that is closest to the destination DHCP server

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 642
Which keyword of the aaa authentication ppp command supports PAP only?

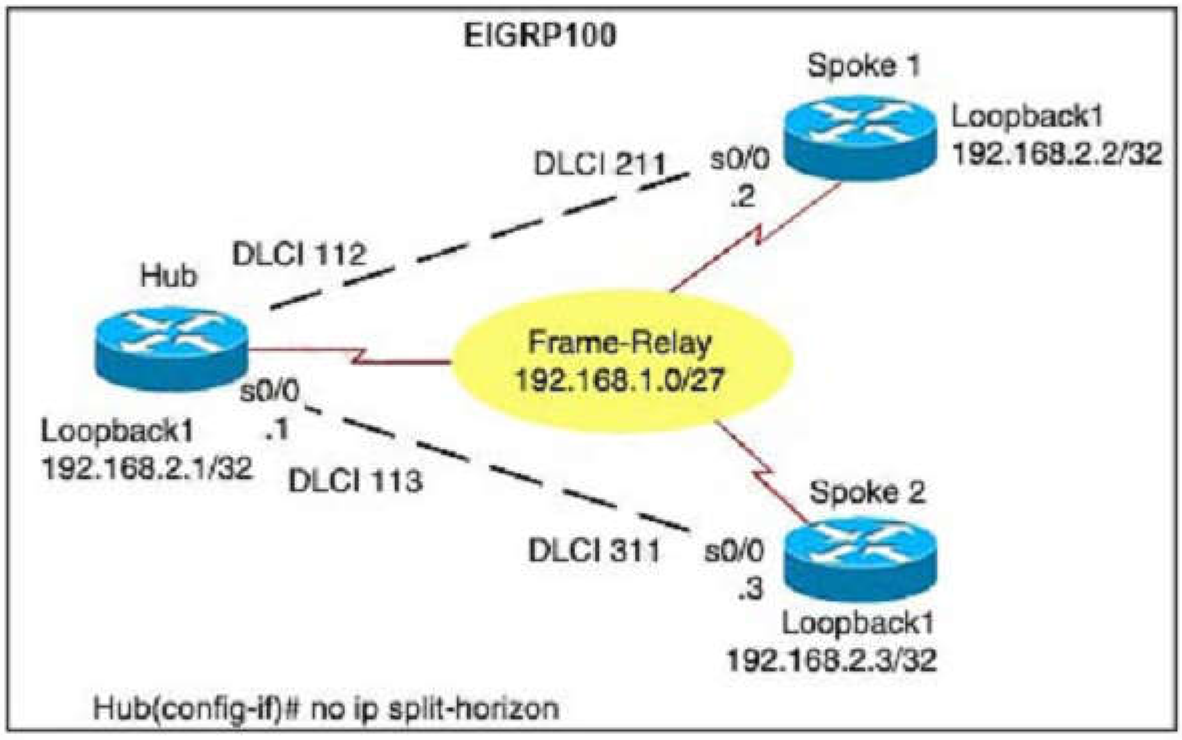
A. line
B. krb5
C. local
D. local-case
E. enable

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Kerberos 5 is only supported for PAP only.

QUESTION 643



A network engineer is working on the network topology and executes the command no ip split-horizon on interface S0/0 of the Hub router.
What is the result of this command?

A. routing loop is created.
B. Each of the spoke routers can see the routes that are advertised from the other spoke routers.
C. The Spoke routers can see the routes that are advertised by the hub router
D. The hub router can see the routes that are advertised by the spoke routers.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 644
Which two routers can do OSPF route summarization? (Choose two)

A. ABR
B. ASBR
C. Summary router
D. Internal router
E. Backbone router

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 645
Which two commands do you need to implement on a router to support PPPoE client? (Choose two)

A. peer default ip address pool
B. MTU
C. bba-group pppoe
D. pppoe enable group
E. pppoe-client dialer-pool-number

Correct Answer: BE
Section: Mix Questions
Explanation

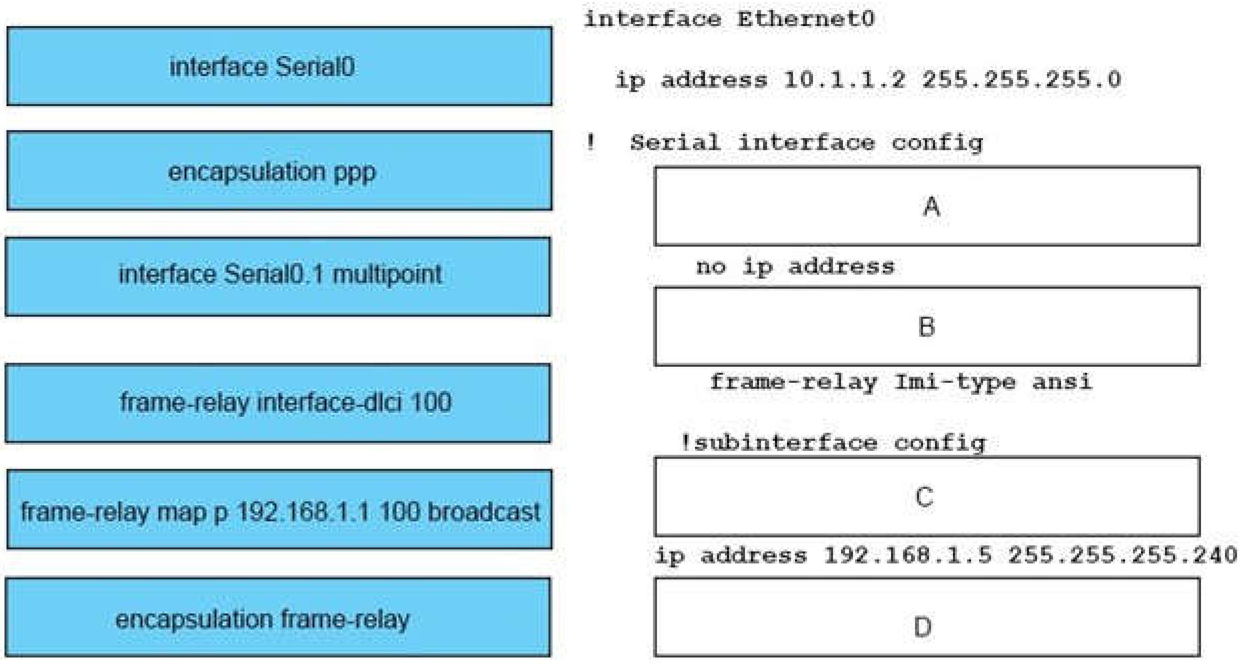
Explanation/Reference:

QUESTION 646
DRAG DROP

Refer to the exhibit.

You are configuring the R1 Serial0 interface for a Multipoint connection.
Drag and Drop the required configuration statements from the left onto the corresponding locations from the diagram on the right.

Select and Place:



interface Serial0

encapsulation ppp

interface Serial0.1 multipoint

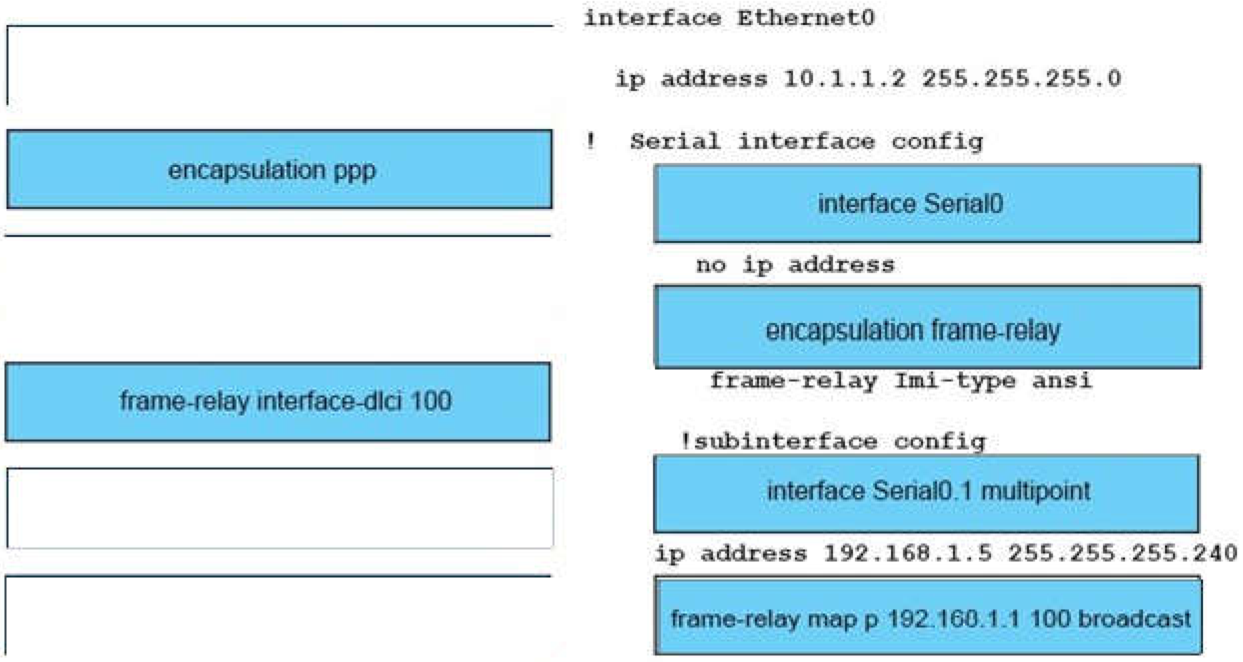
frame-relay interface-dlci 100

frame-relay map p 192.168.1.1 100 broadcast

encapsulation frame-relay

```
interface Ethernet0
  ip address 10.1.1.2 255.255.255.0
!  Serial interface config
    A
    no ip address
    B
     frame-relay Imi-type ansi
   !subinterface config
    C
ip address 192.168.1.5 255.255.255.240
    D
```

Correct Answer:



encapsulation ppp

frame-relay interface-dlci 100

```
interface Ethernet0
  ip address 10.1.1.2 255.255.255.0
!  Serial interface config
    interface Serial0
    no ip address
    encapsulation frame-relay
     frame-relay Imi-type ansi
   !subinterface config
    interface Serial0.1 multipoint
ip address 192.168.1.5 255.255.255.240
    frame-relay map p 192.160.1.1 100 broadcast
```

Section: Mix Questions
Explanation

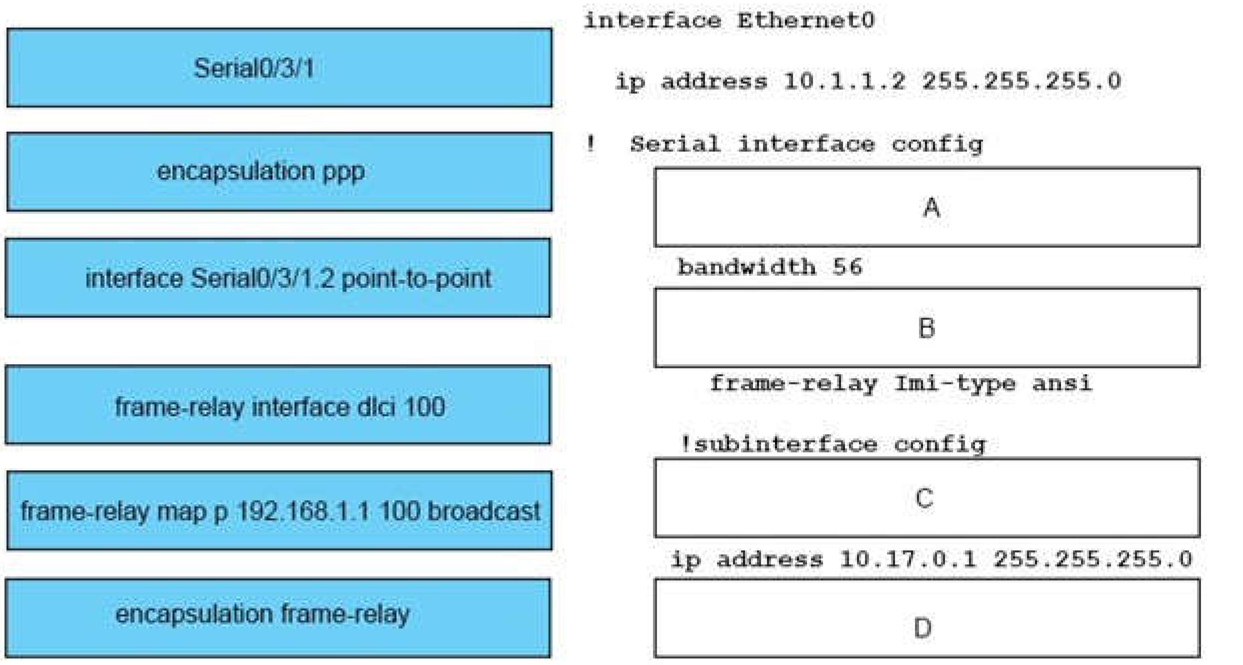
Explanation/Reference:

QUESTION 647
DRAG DROP

Refer to the exhibit.

You are configuring the R1 Serial0 interface for a Point-to-point connection.
Drag and Drop the required configuration statements from the left onto the corresponding locations from the diagram on the right.

Select and Place:



Serial0/3/1

encapsulation ppp

interface Serial0/3/1.2 point-to-point

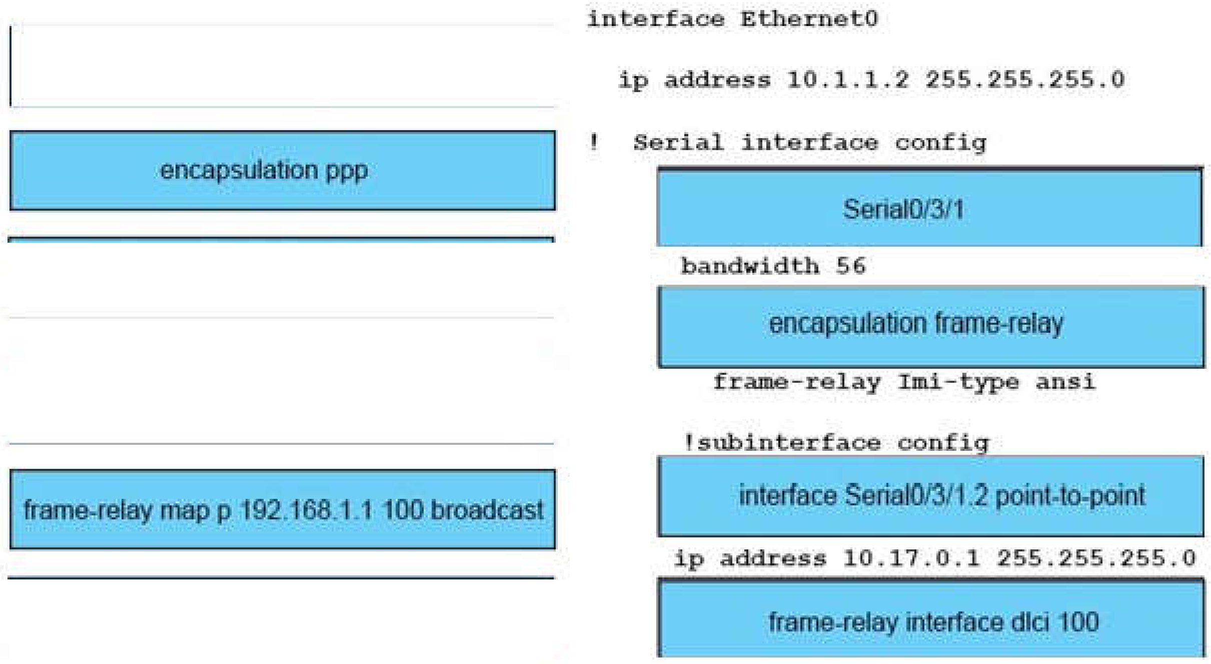
frame-relay interface dlci 100

frame-relay map p 192.168.1.1 100 broadcast

encapsulation frame-relay

```
interface Ethernet0
  ip address 10.1.1.2 255.255.255.0
!  Serial interface config
    A
   bandwidth 56
    B
     frame-relay Imi-type ansi
   !subinterface config
    C
 ip address 10.17.0.1 255.255.255.0
    D
```

Correct Answer:



```
interface Ethernet0
 ip address 10.1.1.2 255.255.255.0
! Serial interface config
  Serial0/3/1
  bandwidth 56
  encapsulation frame-relay
   frame-relay Imi-type ansi
  !subinterface config
  interface Serial0/3/1.2 point-to-point
  ip address 10.17.0.1 255.255.255.0
  frame-relay interface dlci 100
```

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Example:

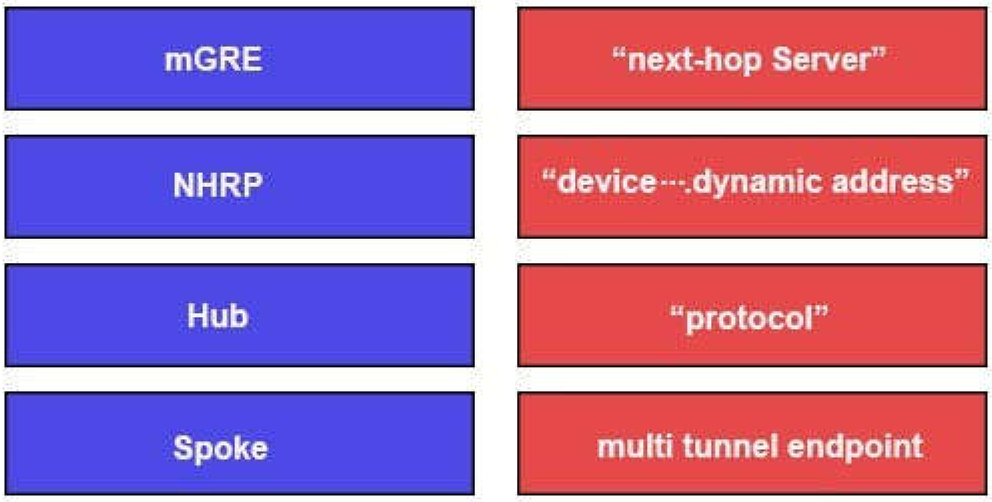
http://www.ciscopress.com/articles/article.asp?p=100603&seqNum=3

```
Atlanta(config)#interface serial0
Atlanta(config-if)#encapsulation frame-relay
Atlanta(config-if)#interface serial 0.1 point-to-point
Atlanta(config-subif)#ip address 140.1.1.1 255.255.255.0
Atlanta(config-subif)#frame-relay interface-dlci 52
Atlanta(config-fr-dlci)#interface serial 0.2 point-to-point
Atlanta(config-subif)#ip address 140.1.2.1 255.255.255.0
Atlanta(config-subif)#frame-relay interface-dlci 53
Atlanta(config-fr-dlci)#interface serial 0.3 point-to-point
Atlanta(config-subif)#ip address 140.1.3.1 255.255.255.0
Atlanta(config-subif)#frame-relay interface-dlci 54
```

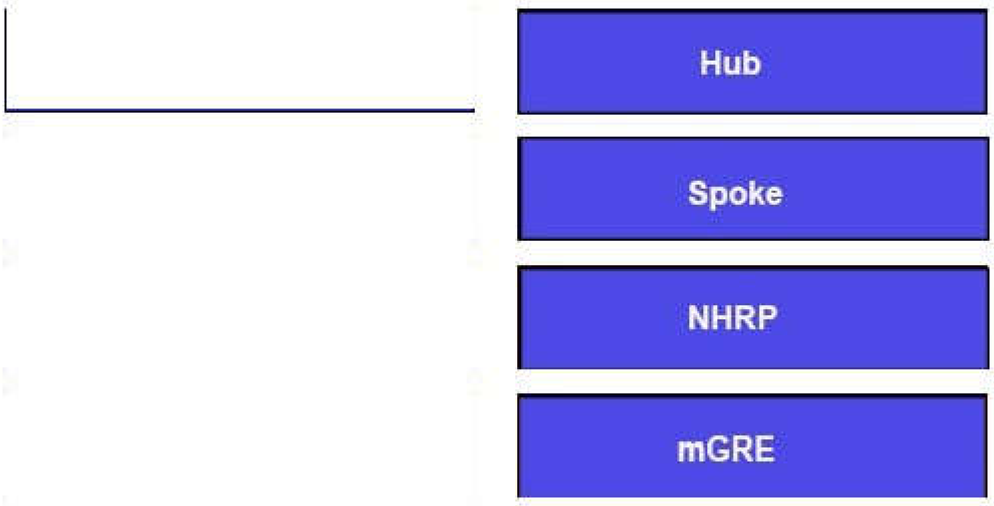
QUESTION 648
DRAG DROP

Drag and drop each DMVPN in the left to the correct statement in the right.

Select and Place:



Correct Answer:



Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 649
What from the following can cause an issue for uRPF?

A. Asymetric routing
B. CEF not enabled
C. uRPF not applied to the traffic source
D. if it is used as ingress filtering

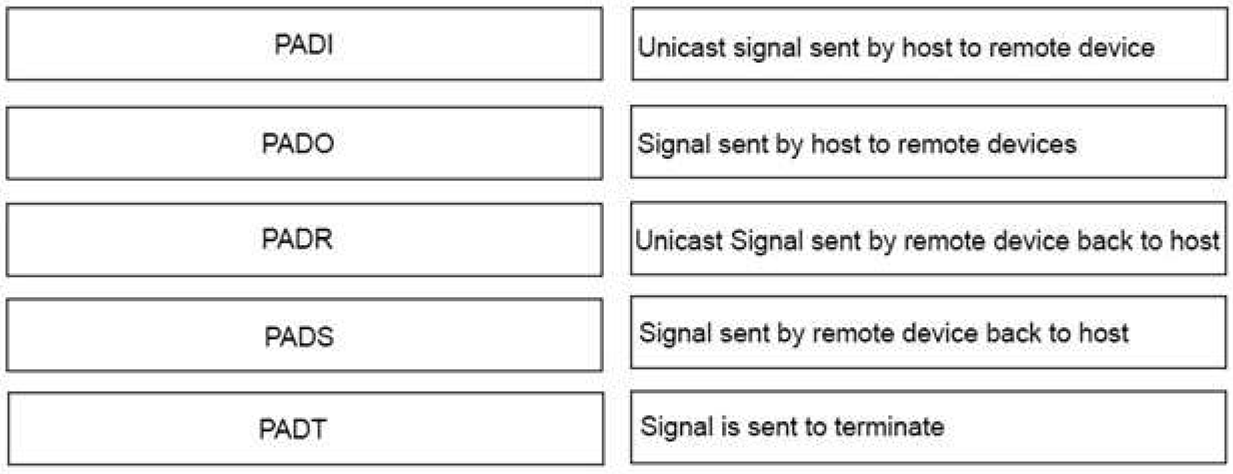
Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 650
DRAG DROP

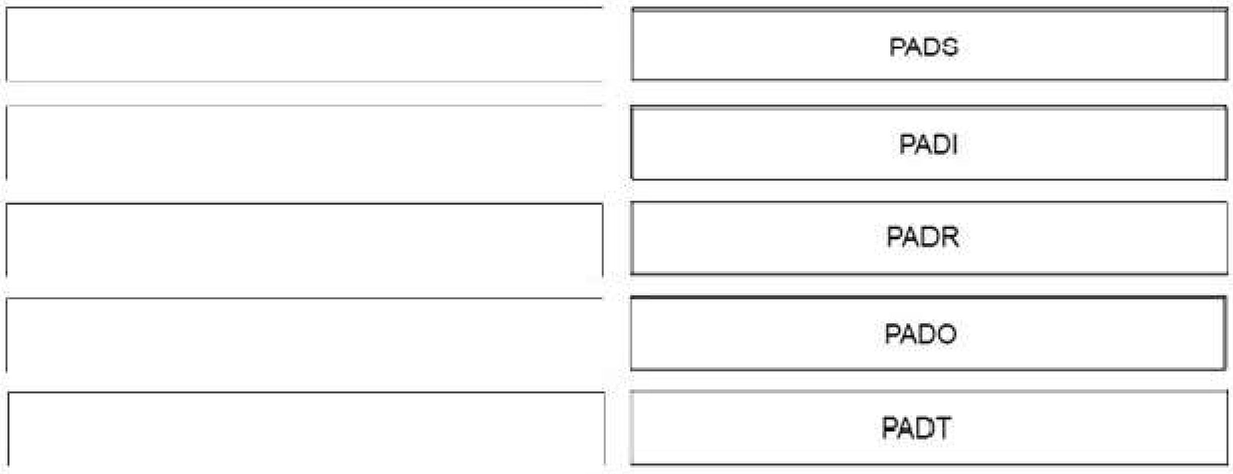
DRAG the PPPoE operations on the left with the definitions on the right.

Select and Place:



PADI	Unicast signal sent by host to remote device
PADO	Signal sent by host to remote devices
PADR	Unicast Signal sent by remote device back to host
PADS	Signal sent by remote device back to host
PADT	Signal is sent to terminate

Correct Answer:



	PADS
	PADI
	PADR
	PADO
	PADT

Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

+ PPPoE Active Discovery Initiation (PADI): The client initiates a session by broadcasting a PADI packet to the LAN to request a service.

+ PPPoE Active Discovery Offer (PADO): Any access concentrator that can provide the service requested by the client in the PADI packet replies with a PADO packet that contains its own name, the unicast address of the client, and the service requested. An access concentrator can also use the PADO packet to offer other services to the client.

+ PPPoE Active Discovery Request (PADR): From the PADOs it receives, the client selects one access concentrator based on its name or the services offered and sends it a PADR packet to indicate the service or services needed.

+ PPPoE Active Discovery Session-Confirmation (PADS): When the selected access concentrator receives the PADR packet, it accepts or rejects the PPPoE session:
– To accept the session, the access concentrator sends the client a PADS packet with a unique session ID for a PPPoE session and a service name that identifies the service under which it accepts the session.
– To reject the session, the access concentrator sends the client a PADS packet with a service name error and resets the session ID to zero.

+ After a session is established, the client or the access concentrator can send a PPPoE Active Discovery Termination (PADT) packet anytime to terminate the session. The PADT packet contains the destination address of the peer and the session ID of the session to be terminated. After this packet is sent, the session is closed to PPPoE traffic.

QUESTION 651
What is supported RADIUS server? (Choose two)

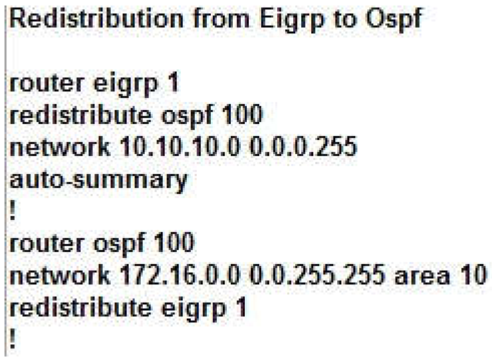
A. telnet
B. authentication

C. accounting
D. authorization
E. SSH

Correct Answer: BD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 652



```
Redistribution from Eigrp to Ospf

router eigrp 1
redistribute ospf 100
network 10.10.10.0 0.0.0.255
auto-summary
!
router ospf 100
network 172.16.0.0 0.0.255.255 area 10
redistribute eigrp 1
!
```

Based on the configuration information shown above, which of the following are true? (Choose two)

A. will redistribute only clasfull routes
B. routes will be redistributed as E2
C. routes will be redistributed as N2
D. will redistribute all eigrp routes

Correct Answer: AB
Section: Mix Questions
Explanation

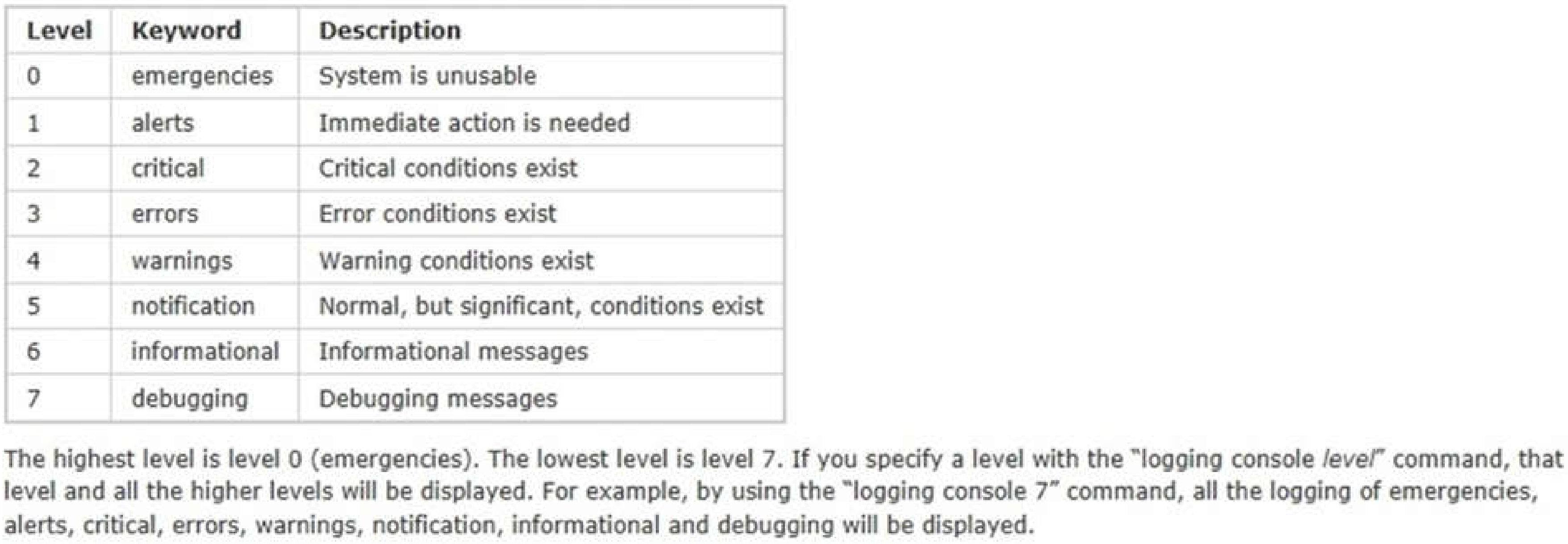
Explanation/Reference:

QUESTION 653
What is show on logging console 7?

A. Debugging and all above level
B. Information and all above level
C. Error and all above level
D. Emergencies and all above level

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:



Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

The highest level is level 0 (emergencies). The lowest level is level 7. If you specify a level with the "logging console *level*" command, that level and all the higher levels will be displayed. For example, by using the "logging console 7" command, all the logging of emergencies, alerts, critical, errors, warnings, notification, informational and debugging will be displayed.

QUESTION 654
Choose the best IP SLA deployment cycle that reduce deployment time. (Choose four.)

A. baseline (network performance)
B. understand (network performance baseline)
C. Understand Quality results
D. quantify (results)
E. fine tune and optimize
F. Update Understanding

Correct Answer: ABDE
Section: Mix Questions

Explanation

Explanation/Reference:
Explanation:

baseline (network performance), understand (network performance baseline), fine tune and optimize, quantify (results)

Reference:

https://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper0900aecd8017f8c9.html

QUESTION 655
Which two protocols are used to deploy a single Hub-DMVPN supporting Spoke-to Spoke tunnels? (Choose two)

A. MPLS
B. RSVP
C. NHRP
D. BFB
E. Multipoint GRE

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 656
What would you configure on SNMPv3 to allow authentication and encryption?

A. authpriv
B. authnopriv
C. noauthnopriv
D. authmember

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

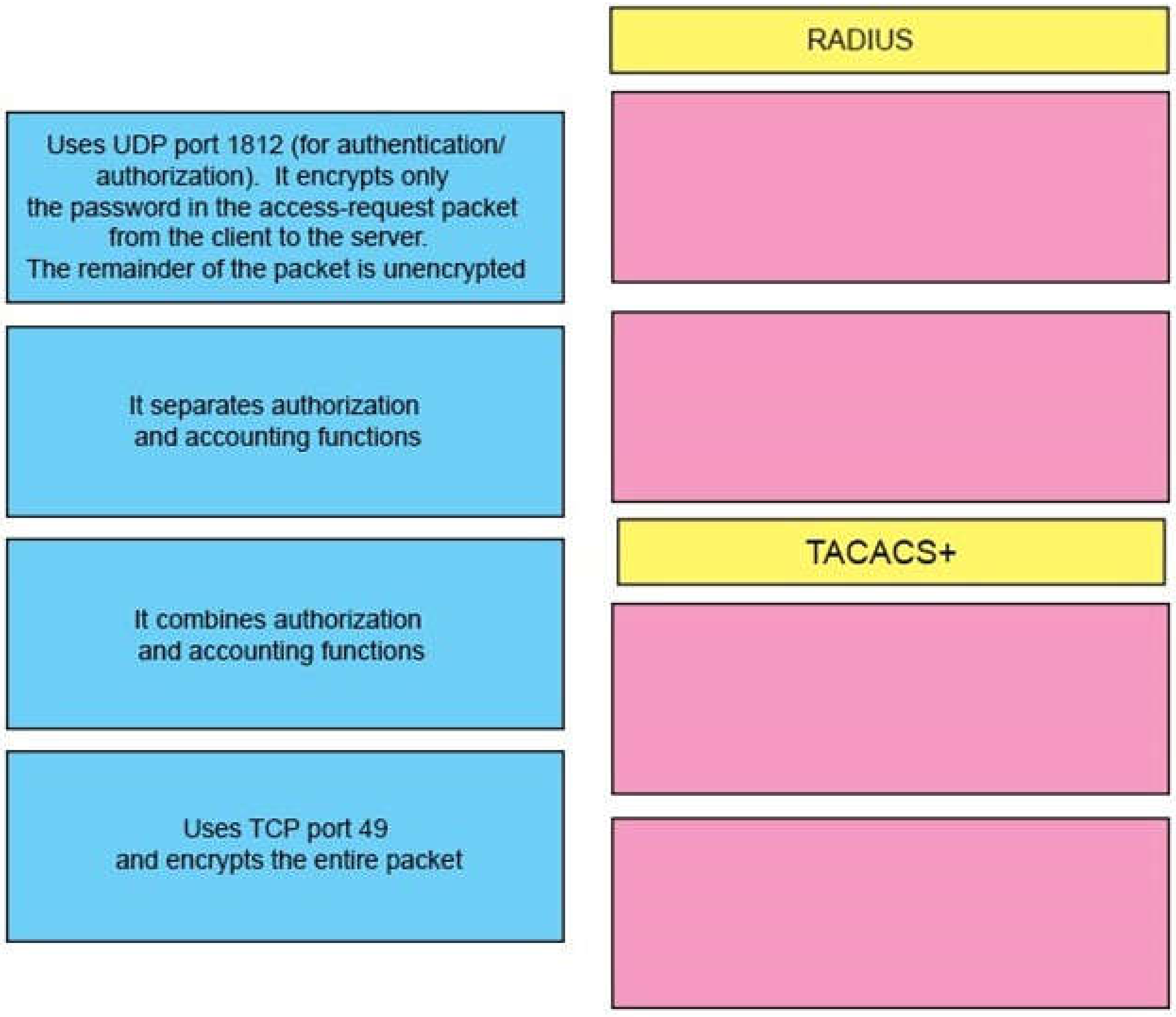
The SNMPv3 Agent supports the following set of security levels:

+ NoAuthnoPriv: Communication without authentication and privacy.
+ AuthNoPriv: Communication with authentication and without privacy. The protocols used for Authentication are MD5 and SHA (Secure Hash Algorithm).
+ AuthPriv: Communication with authentication and privacy. The protocols used for Authentication are MD5 and SHA ; and for Privacy, DES (Data Encryption Standard) and AES (Advanced Encryption Standard) protocols can be used. For Privacy Support, you have to install some third-party privacy packages

QUESTION 657
DRAG DROP

Drag the items on the left to the proper locations on the right.

Select and Place:



RADIUS

Uses UDP port 1812 (for authentication/ authorization). It encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted

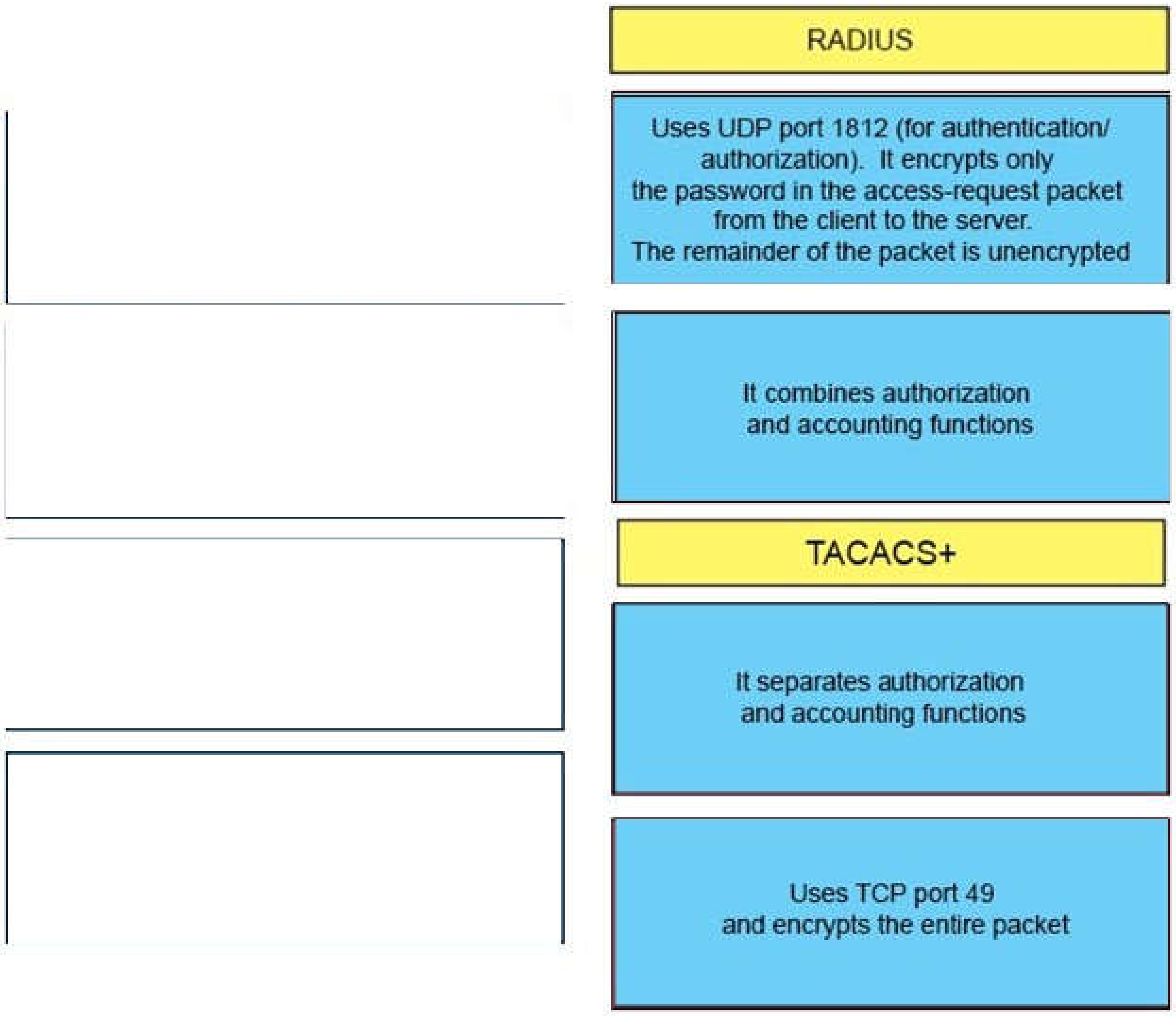
It separates authorization and accounting functions

It combines authorization and accounting functions

TACACS+

Uses TCP port 49 and encrypts the entire packet

Correct Answer:



RADIUS

Uses UDP port 1812 (for authentication/ authorization). It encrypts only the password in the access-request packet from the client to the server. The remainder of the packet is unencrypted

It combines authorization and accounting functions

TACACS+

It separates authorization and accounting functions

Uses TCP port 49 and encrypts the entire packet

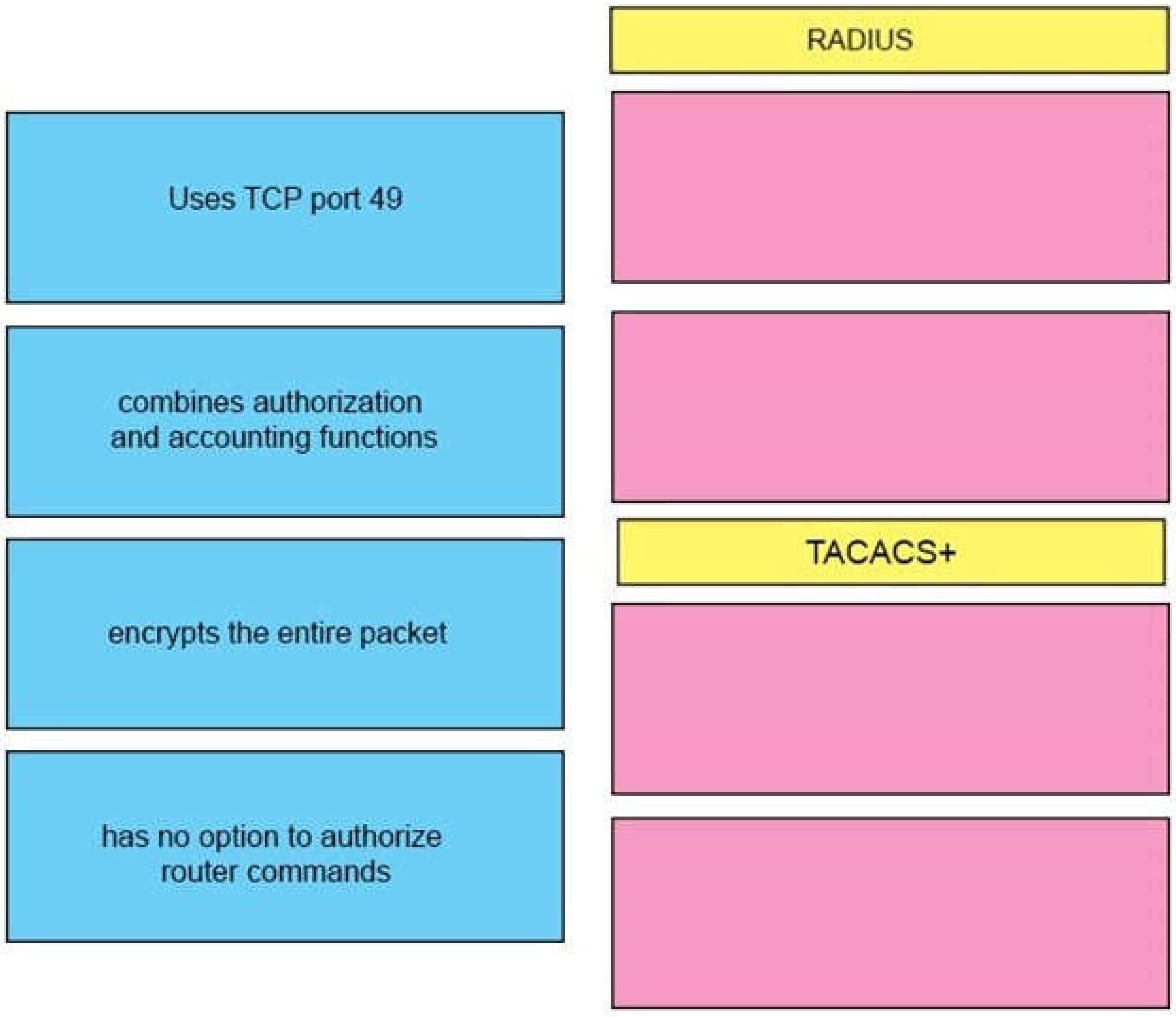
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 658
DRAG DROP

Drag the items on the left to the proper locations on the right.

Select and Place:



Uses TCP port 49

combines authorization and accounting functions

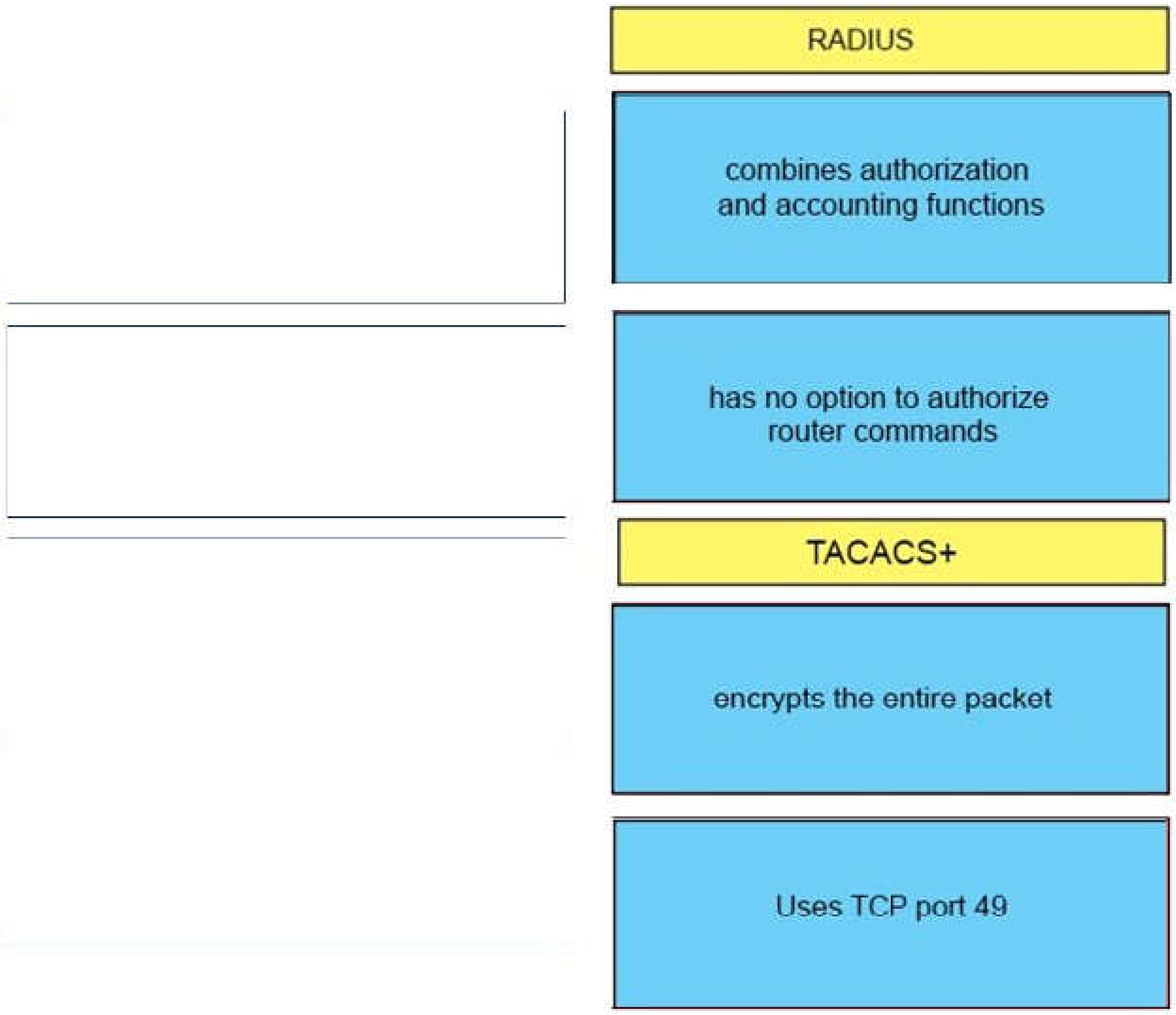
encrypts the entire packet

has no option to authorize router commands

RADIUS

TACACS+

Correct Answer:



RADIUS

combines authorization and accounting functions

has no option to authorize router commands

TACACS+

encrypts the entire packet

Uses TCP port 49

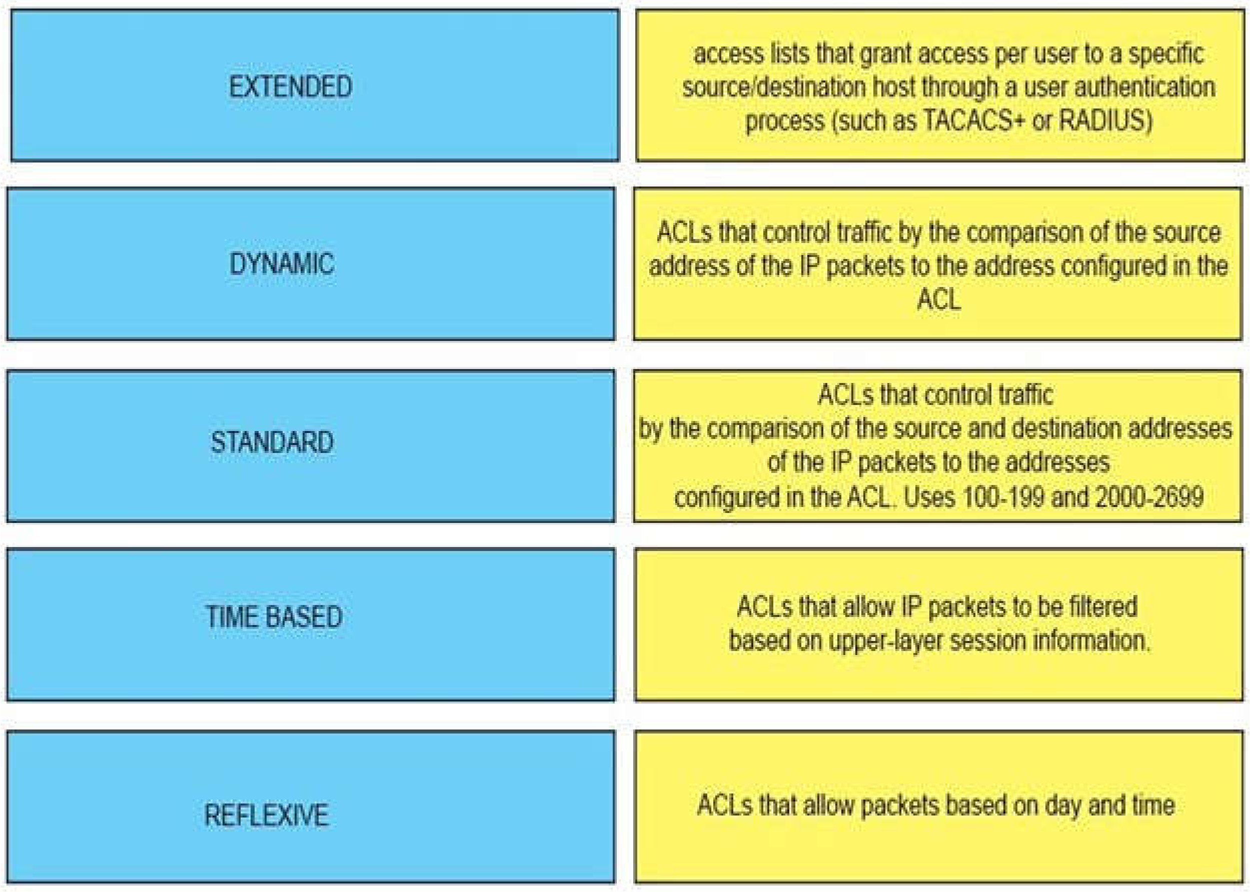
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 659
DRAG DROP

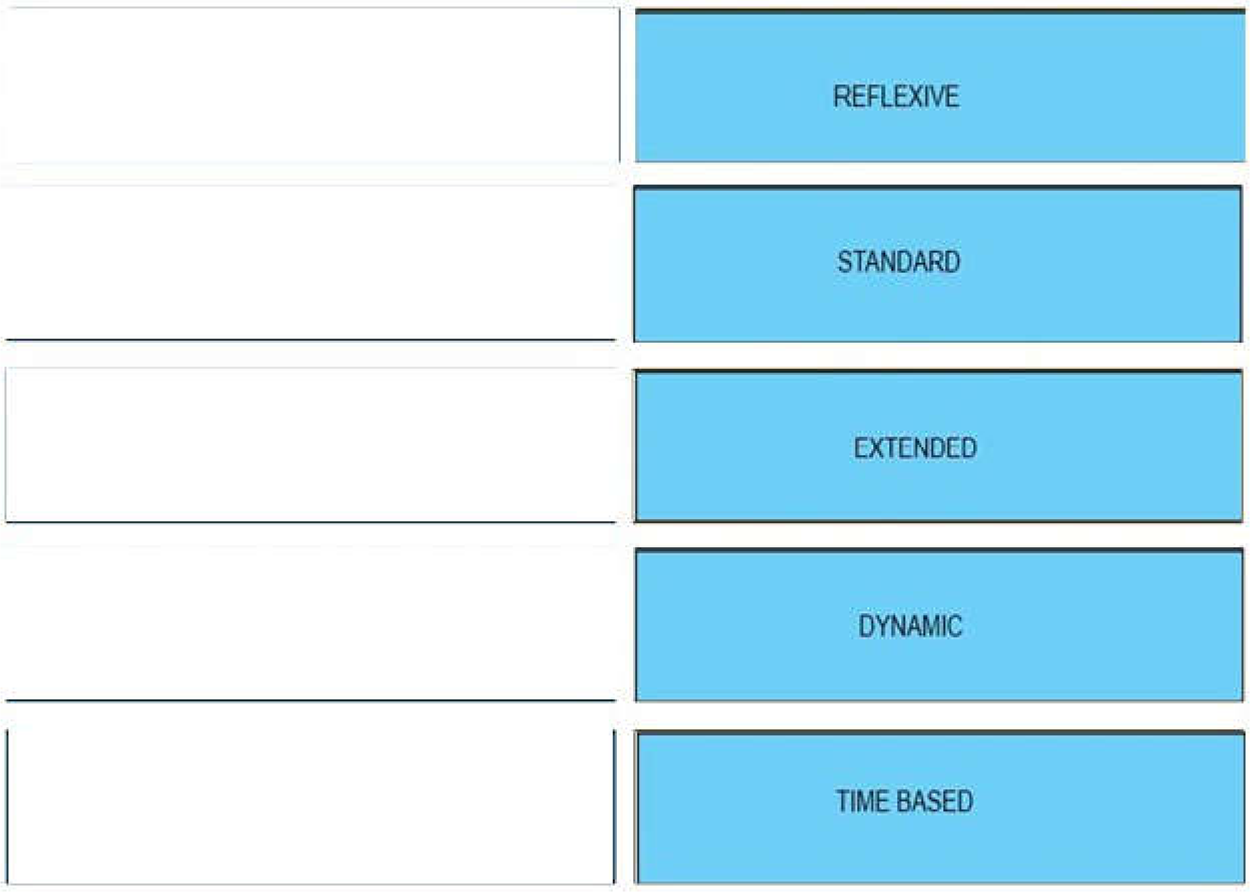
Drag and drop the ACL types onto their description

Select and Place:



EXTENDED	access lists that grant access per user to a specific source/destination host through a user authentication process (such as TACACS+ or RADIUS)
DYNAMIC	ACLs that control traffic by the comparison of the source address of the IP packets to the address configured in the ACL
STANDARD	ACLs that control traffic by the comparison of the source and destination addresses of the IP packets to the addresses configured in the ACL. Uses 100-199 and 2000-2699
TIME BASED	ACLs that allow IP packets to be filtered based on upper-layer session information.
REFLEXIVE	ACLs that allow packets based on day and time

Correct Answer:



	REFLEXIVE
	STANDARD
	EXTENDED
	DYNAMIC
	TIME BASED

Section: Mix Questions
Explanation

Explanation/Reference:
Reference:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#timebasedtimerange

QUESTION 660
If you run the command auto-cost reference-bandwidth 10000 on one of the router in the network, what will happen?

A. It will make 10 Gbps on all of them
B. it will make 1 Gbps on all of them
C. it will make 10 Gbps on this router only
D. it will remain the same on all links of the router

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

This command affects all the OSPF costs on the local router as all links are recalculated with formula:
cost = reference-bandwidth (in Mbps) / interface bandwidth
Therefore, in this case the command “auto-cost reference-bandwidth 10000” allows the local router to calculate the link up to 10Gbps.

QUESTION 661

What does the command show ip vrf purple TOPOLOGY shows?

A. shows the feasible successors for a specific route table
B. shows routing table for vrf purple
C. show topology table
D. show protocols to be used

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

From EIGRP Stub Score 95X

QUESTION 662
What’s the gateway in the global configuration? (Choose three.)

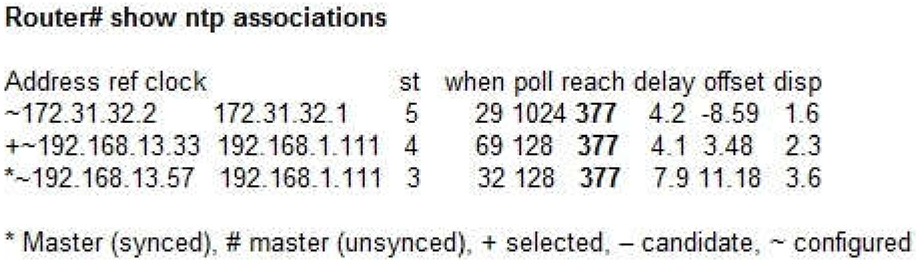
Router(config)#ip route vrf blue 0.0.0.0 0.0.0.0 192.168.1.1
Router(config)#ip route vrf red 0.0.0.0 0.0.0.0 192.168.1.2

A. If you type “show ip route” you will see “Gateway of last resort it not set”.
B. If you type "show ip route vrf blue” you will see “192.168.1.1 as gateway of last resort”.
C. If you type "show ip route vrf red” you will see “192.168.1.1 as gateway of last resort”.
D. If you type "show ip route vrf blue” you will see “192.168.1.2 as gateway of last resort”.
E. Global routing table does not overlap with VRF routing tables.

Correct Answer: ABE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 663



```
Router# show ntp associations

Address ref clock              st   when poll reach delay offset disp
~172.31.32.2      172.31.32.1    5     29 1024 377    4.2  -8.59   1.6
+~192.168.13.33  192.168.1.111  4     69 128   377    4.1  3.48    2.3
*~192.168.13.57   192.168.1.111  3     32 128   377    7.9 11.18   3.6

* Master (synced), # master (unsynced), + selected, – candidate, ~ configured
```

Which of the following is true?

A. Master is syncing and exchanging NTP packets successfully
B. Master is not syncing but exchanging NTP packets successfully
C. Master is not syncing and not exchanging NTP packets
D. All NTP packets are droped

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

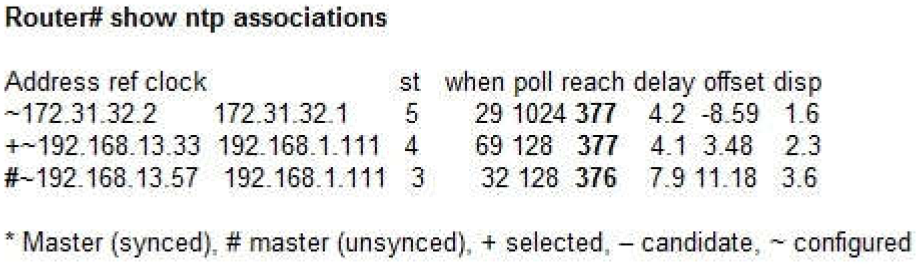
In the output you can see a * next to the ip address that is the primary NTP server.

Also the 377 that means everything was received and processed. Negotiation done.
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc

377 = 1 1 1 1 1 1 1 1 Time 0: Last eight responses from server were received
376 = 1 1 1 1 1 1 1 0 Time 1: Last NTP response was NOT received (lost in network)

Values below this 376 is that Last NTP response was received

QUESTION 664



```
Router# show ntp associations

Address ref clock              st   when poll reach delay offset disp
~172.31.32.2      172.31.32.1    5     29 1024 377    4.2  -8.59   1.6
+~192.168.13.33  192.168.1.111  4     69 128   377    4.1  3.48    2.3
#~192.168.13.57   192.168.1.111  3     32 128   376    7.9 11.18   3.6

* Master (synced), # master (unsynced), + selected, – candidate, ~ configured
```

Which of the following is true?

A. Master is syncing and exchanging NTP packets successfully
B. Master is not syncing but exchanging NTP packets successfully
C. Master is not syncing and not exchanging NTP packets
D. All NTP packets are dropped

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In the output you can see a * next to the ip address that is the primary NTP server.

Also the 377 that means everything was received and processed. Negotiation done.
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc

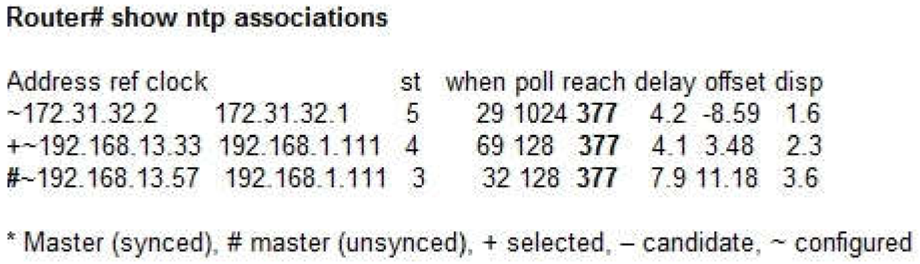
377 = 1 1 1 1 1 1 1 1 Time 0: Last eight responses from server were received
376 = 1 1 1 1 1 1 1 0 Time 1: Last NTP response was NOT received (lost in network)

Values below this 376 is that Last NTP response was received

A pound sign (#) displayed next to a configured peer in the show ntp associations command output indicates that the router isn't syncing with the peer but NTP request and response packets are NOT exchanged.

Reference: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html

QUESTION 665



```
Router# show ntp associations

Address ref clock                  st   when poll reach delay offset disp
~172.31.32.2      172.31.32.1      5      29 1024 377    4.2  -8.59   1.6
+~192.168.13.33  192.168.1.111    4      69 128   377    4.1  3.48    2.3
#~192.168.13.57  192.168.1.111    3       32 128  377    7.9 11.18    3.6

* Master (synced), # master (unsynced), + selected, – candidate, ~ configured
```

Which of the following is true?

A. Master is syncing and exchanging NTP packets successfully
B. Master is not syncing but exchanging NTP packets successfully
C. Master is not syncing and not exchanging NTP packets
D. All NTP packets are dropped

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

In the output you can see a * next to the ip address that is the primary NTP server.

Also the 377 that means everything was received and processed. Negotiation done.
https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc

377 = 1 1 1 1 1 1 1 1 Time 0: Last eight responses from server were received
376 = 1 1 1 1 1 1 1 0 Time 1: Last NTP response was NOT received (lost in network)

Values below this 376 is that Last NTP response was received

A pound sign (#) displayed next to a configured peer in the show ntp associations command output indicates that the router isn't syncing with the peer even though NTP request and response packets are being exchanged.

Reference: https://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/15171-ntpassoc.html

QUESTION 666
Which of these can be used for IPv4 to IPv6 communication?

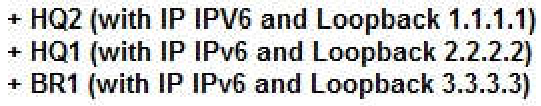
A. NAT-PT
B. ISATAP
C. L2 to L3 VPN
D. IPSec

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

NAT-PT provides IPv4/IPv6 protocol translation.
It resides within an IP router, situated at the boundary of an IPv4 network and an IPv6 network. By installing NAT-PT between an IPv4 and IPv6 network, all IPv4 users are given access to the IPv6 network without modification in the local IPv4-hosts (and vice versa).
Equally, all hosts on the IPv6 network are given access to the IPv4 hosts without modification to the local IPv6-hosts.
This is accomplished with a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries.

QUESTION 667
A diagram with 3 routers: HQ2 – HQ1 – BR1.



+ HQ2 (with IP IPV6 and Loopback 1.1.1.1)
+ HQ1 (with IP IPv6 and Loopback 2.2.2.2)
+ BR1 (with IP IPv6 and Loopback 3.3.3.3)

When you are running with EIGRP 100 on both routers, what command will you implement so that you will see the loopback IP of BR1 to be advertised at HQ2A diagram with 3 routers: HQ2 – HQ1 – BR1.

A. HQ2(config)# ipv6 router eigrp 100
   HQ2(config-rtr)# no eigrp stub
B. BR1(config)#ipv6 router eigrp 100
   BR1(config-rtr)# no eigrp stub receive-only
C. HQ2(config)# ipv6 router eigrp 100
   HQ2(config-rtr)# no eigrp stub only
D. BR1(config)# ipv6 router eigrp 100
   BR1(config-rtr)# no eigrp stub only

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

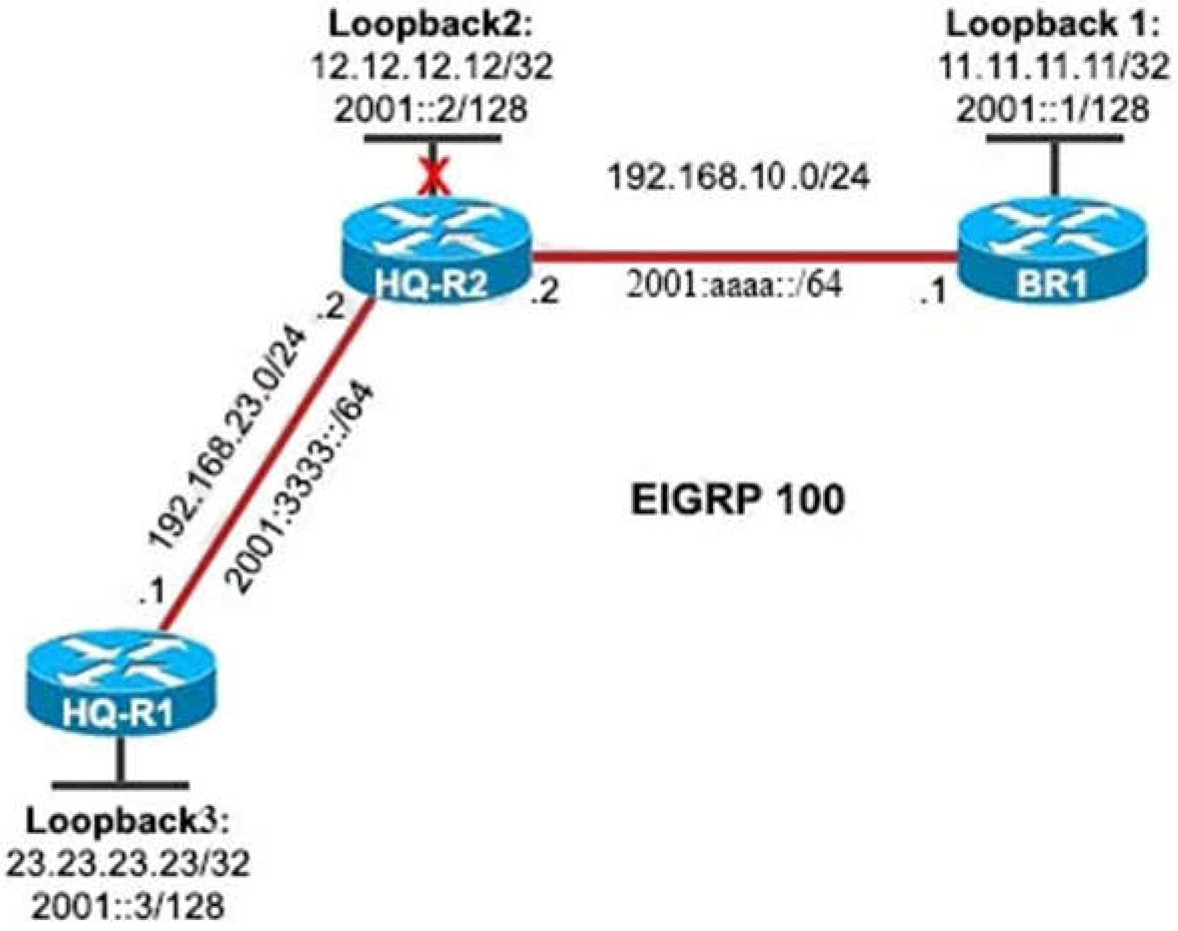
B because BR1 is the router that has to advertise the loopback to his neighbors but if it is only receiving routes (no stub receive-only) It cannot advertise his loopback.

"eigrp stub recieve-only" will restrict the router from sharing any of its routes, meaning: connected, summary, redistributed or static routes to any other router in the EIGRP AS. Learned eigrp routes will never be shared as that would defeat the whole purpose of STUB.

There are other stub options that can be configured. The list looks like this:
– receive-only
– connected
– static
– summary
– redistribute

If you configure the receive-only option, you can't include any of the other options on the above list. If you just configure the router as a stub and don't specify any option, the default behavior is to share connected and summary routes. Some other caveats also arise when using these options. For instance, if you configure the static option, you still must allow EIGRP to share the static routes by issuing the redistribute static command in the config-router context, or the router won't share the routes. The same goes for the connected option. If a network statement does not include the connected routes you want to share, then you must issue the redistribute connected command. One last aspect which may seem counterintuitive is that if you use the redistribute option, you are permitting the router to share redistributed routes, but you still must actually redistribute the routes for them to be shared. If you choose the summary option, don't forget to either manually create summary routes or enable auto-summary.

QUESTION 668



All interfaces on each router are participating in the EIGRP 100 process.
An engineer issues the eigrp stub command on router BR1.
What will the show ip route be on HQ-R1 look like?

A. HQ-R1 will install only route 12.12.12.12/32 network in its routing table
B. HQ-R1 will install routes 12.12.12.12/32 network and 192.168.10.0/24 in its routing table
C. HQ-R1 will install only route 192.168.10.0/24 network in its routing table
D. All routes will be installed in its routing table on HQ-R1

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Stub advertise summary and connected so you are going to see R1 (loopback)connected, R2(loopback) eigrp, R3 (loopback) eigrp , (network rage between HQ-R1 and HQ-R2) connected, (network rage between HQ-R2 and BR1) eigrp.

BR1 is a STUB and there are just two CONNECTED networks, so it will ADVERTISE them to other routers.

QUESTION 669
How to set up IP SLA to monitor jitter between the certain limits?

A. Timeout (not timer)
B. Frequency
C. Threshold
D. Queue-limit

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 670
How can you mitigate fragmentation issues between endpoints separated by a GRE tunnel?

A. PMTU
B. TCP MSS
C. windowing
D. ICMP DF bit

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

The IP protocol was designed for use on a wide variety of transmission links. Although the maximum length of an IP datagram is 65535, most transmission links enforce a smaller maximum packet length limit, called an MTU. The value of the MTU depends on the type of the transmission link. The design of IP accommodates MTU differences since it allows routers to fragment IP datagrams as necessary. The receiving station is responsible for the reassembly of the fragments back into the original full size IP datagram.

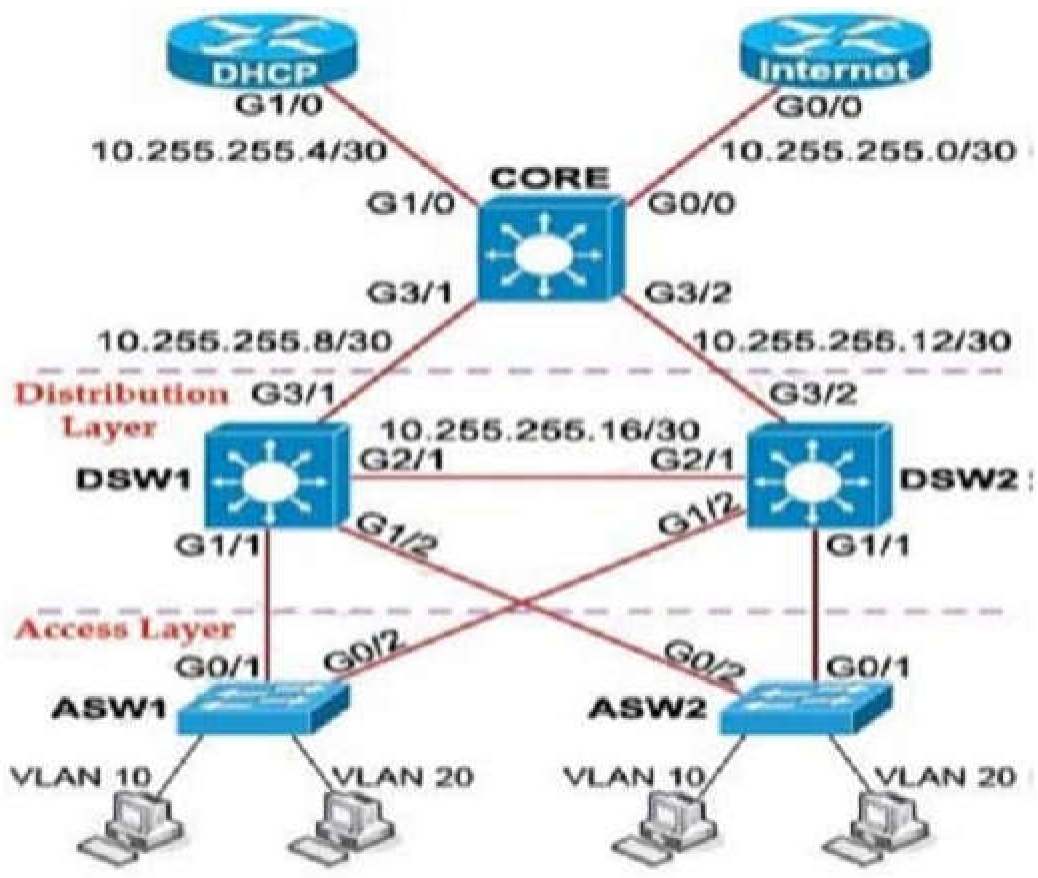
Fragmentation and Path Maximum Transmission Unit Discovery (PMTUD) is a standardized technique to determine the maximum transmission unit (MTU) size on the network path between two hosts, usually with the goal of avoiding IP fragmentation. PMTUD was originally intended for routers in IPv4. However, all modern operating systems use it on endpoints.

The TCP Maximum Segment Size (TCP MSS) defines the maximum amount of data that a host is willing to accept in a single TCP/IP datagram. This TCP/IP datagram might be fragmented at the IP layer. The MSS value is sent as a TCP header option only in TCP SYN segments. Each side of a TCP connection reports its MSS value to the other side. Contrary to popular belief, the MSS value is not negotiated between hosts. The sending host is required to limit the size of data in a single TCP segment to a value less than or equal to the MSS reported by the receiving host.
TCP MSS takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints. PMTUD was developed in order to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet’s source to its destination.

http://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html
(there is some examples of how TCP MSS avoids IP Fragmentation in this link but it is too long so if you want to read please visit this link)

Note: IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later.

QUESTION 671
Refer to the exhibit. Which option prevents routing updates from being sent to the DHCP router, while still allowing routing update messages to flow to the Internet router and the distribution switches?



A. CORE(config)# access-list … deny
   CORE(config)# access-list … permit
   CORE(config-router)# distribute-list .. out
B. CORE(config)# access-list … deny
   CORE(config)# access-list … permit
   CORE(config-if)# distribute-list .. out
C. DHCP(config)# access-list … deny
   DHCP(config)# access-list … permit
   CORE(config-router)# distribute-list .. out
D. CORE(config)# access-list … deny
   CORE(config)# access-list … permit
   DHCP(config-if)# distribute-list .. out

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 672
What is the function of the snmp-server enable traps and snmp-server host 192.168.1.3 trap version 1c public commands?

A. to allow only 192.168.1.3 to access the system using the community-string public
B. to allow private communications between the router and the host.
C. to collect information about the system on a network management server
D. to disable all SNMP informs that are on the system

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 673
Windows Server Syslog blocked by ACL and….?

A. port UDP 514
B. port UDP 541
C. port UDP 520
D. port UDP 521

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 674
OSPF routers that communicate with other network routers like EIGRP are called?

A. ASBR
B. ABR
C. Backbone
D. Internal

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 675
Which feature can filter information at the interface level?

A. Conditional Debugging
B. Local Logging
C. Prefix-List
D. Syslog

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

If you enter the debug condition interface command, the debugging output will be turned off for all interfaces except the specified interface.
To reenable debugging output for all interfaces, use the no debug interface command.

The debug condition commands limit these debugging messages to those related to a particular interface.

QUESTION 676
Which statement about NTP authentication is true?

A. The ntp trusted-key command authenticate the identify of a system.
B. The ntp authentication-key command enables NTP authentication.
C. It suppose DES, 3DES, and MD5 authentication.
D. Only one authentication key can be defined at a time.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

config)# ntp authentication-key 42 md5 aNiceKey
Defines the authentication keys. The device does not synchronize to a time source unless the source has one of these authentication keys and the key number is specified by the ntp trusted-key number command.
The range for authentication keys is from 1 to 65535. Cisco NX-OS Release 5.2(3) and later 5.x releases support up to 15 alphanumeric characters for the MD5 string. Earlier releases support up to 8 alphanumeric characters.

(config)# ntp trusted-key 42
Specifies one or more keys that a time source must provide in its NTP packets in order for the device to synchronize to it. The range for trusted keys is from 1 to 65535.
This command provides protection against accidentally synchronizing the device to a time source that is not trusted.

B is not Correct because to enable NTP Authentication is required this command ntp authenticate.
So A is Correct.

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/system_management/configuration/guide/sm_nx_os_cg/sm_3ntp.html#93976

QUESTION 677
Which feature is supported with the PPPoE client?

A. DMVPN
B. QoS on the dialer interface
C. MLPPP on the interface
D. Dial-on-demand

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

QUESTION 678
Which condition prevents the establishment of a DMVPN tunnel between two spokes?

A. The two spokes are behind different PAT devices.
B. The two spokes have different tunnel keepalive settings.
C. IPsec is enabled on the spoke devices.
D. HSRP is enabled on the spoke devices.

Correct Answer: D
Section: Mix Questions

Explanation

Explanation/Reference:

QUESTION 679
Which two statements are benefits of BGP peer groups? (Choose two.)

A. Each neighbor in a peer group can have different inbound BGP policies.
B. A configuration change can be applied simultaneously to all peers in the peer group.
C. They use soft updates to minimize bandwidth consumption.
D. They can optimize backdoor routes.
E. They support groups of paths.
F. They can be updated via multicast.

Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 680
Which two statements about AAA with the local database are true? (Choose two.)

A. It supports a limited number of usernames and passwords.
B. The local database can server only as a backup authentication method.
C. By default, it is queried before a TACACS+ or RADIUS server.
D. Accounting is not supported locally.
E. Authorization is available only for one-time use logins.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 681
Which three causes of unicast flooding are true? (Choose three.)

A. asymmetric routing
B. forwarding table overflow
C. excess space in the forwarding table
D. consistent STP topology
E. symmetric routing
F. changes in the STP topology

Correct Answer: ABF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 682
A company is deploying a multicast application that must be accessible between sites, but must not be accessible outside of the organization. Based on the scoping requirements, the multicast group address for the application will be allocated out of which range?

A. FF02::/16
B. FF08::/16
C. FFOE::/16
D. FF00::/16

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 683
What is the default authentication in RIPv2 when authentication is enabled?

A. SHA1 authentication
B. MD5 authentication
C. plaintext authentication
D. enable password authentication

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:

Cisco implementation of RIPv2 supports two modes of authentication: plain text authentication and Message Digest 5 (MD5) authentication. Plain text authentication mode is the default setting in every RIPv2 packet, when authentication is enabled. Plain text authentication should not be used when security is an issue, because the unencrypted authentication password is sent in every RIPv2 packet.
Reference: https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13719-50.html

QUESTION 684
After configuring RIPng on two routers that are connected via a WAN link, a network engineer notices that the two routers cannot exchange routing updates.

What is the reason for this?

A. Either a firewall between the two routers or an ACL on the router is blocking TCP 521.
B. Either a firewall between the two routers or an ACL on the router is blocking UDP 520.
C. Either a firewall between the two routers or an ACL on the router is blocking UDP 521.
D. Either a firewall between the two routers or an ACL on the router is blocking TCP 520.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
RIPng is a UDP-based protocol. Each router that uses RIPng has a routing process that sends and receives datagrams on UDP port number 521, the RIPng port.
Reference: https://tools.ietf.org/html/rfc2080

QUESTION 685
Which LSA type on OSPFv3 is used for link-local updates?

A. Link LSA type 8
B. Link LSA type 5
C. Link LSA type 6
D. Link LSA type 4

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
LSAs that are responsible to carry IPv6 Routes:

- LSA Type 8: Link LSA
- Link Local scope: LSA is only flooded on the local link and is further used for the LINK-LSA

Reference: https://www.cisco.com/c/en/us/support/docs/ip/ip-version-6-ipv6/212828-link-lsa-lsa-type-8-and-intra-area-pr.html

QUESTION 686
Which feature is an invalid redistribute command option for redistributing routes from EIGRP into OSPF?

A. access list
B. metric
C. route map
D. tag

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 687
What is the role of a route distinguisher in a VRF-Lite setup implementation?

A. It manages the import and export of routes between two or more VRF instances.
B. It enables multicast distribution for VRF-Lite setups to enhance EGP routing protocol capabilities.
C. It extends the IP address to identify which VRF instance it belongs to.
D. It enables multicast distribution for VRF-Lite setups to enhance IGP routing protocol capabilities.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 688
A customer asks its service provider for VPN support IPv4 and IPv6 address families.

Which command enables a VRF that supports these requirements?

A. Router (config-vrf)#**rd 004:006**
B. Router (config-vrf)#**route-target 004:006**
C. Router (config)#**vrf definition CUSTOMER**
D. Router(config)#**ip vrf CUSTOMER**

Correct Answer: C

Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/software/15_4_1_cg/vrf_cgr1000.html

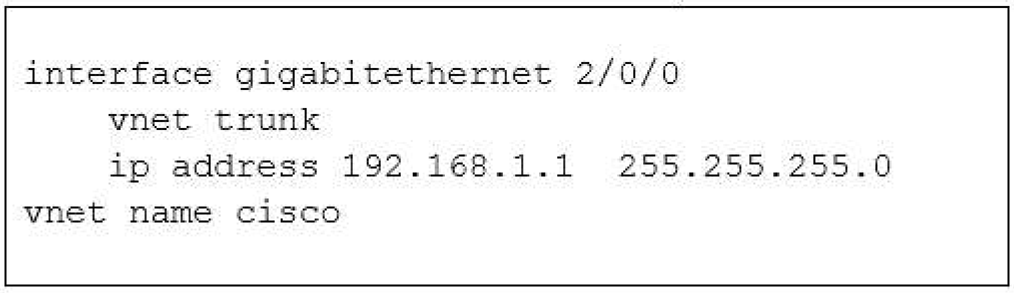
QUESTION 689
Which two tasks must you perform to configure a BGP peer group? (Choose two.)

A. Activate each neighbor.
B. Activate the default route.
C. Configure the soft-update value.
D. Assign neighbor to the peer-group.
E. Set the advertisement interval.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 690
Refer to the exhibit. Which effect of this configuration is true?



```
interface gigabitethernet 2/0/0
    vnet trunk
    ip address 192.168.1.1  255.255.255.0
vnet name cisco
```

A. It removes VTP from the interface.
B. It designates the interface as a GRE tunnel endpoint.
C. It designates the interface as an EVN trunk.
D. It configures 802.1q trunking on the interface.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 691
What is the administrative distance of an EIGRP summary route?

A. 1
B. 90
C. 5
D. 170

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 692
Which two features were added in MSCHAP version 2? (Choose two.)

A. backwards-compatibility with MSCHAP version 1
B. using the MD5 hash for stronger security
C. mutual authentication between peers
D. ability to change an expired password
E. using three-way handshakes for authentication

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
MSCHAP V2 authentication is an updated version of MSCHAP that is similar to but incompatible with MSCHAP Version 1 (V1). MSCHAP V2 introduces mutual authentication between peers and a Change Password feature.
Reference: https://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_aaa/configuration/15-2mt/sec-mschap-ver2.html

QUESTION 693
A network engineer wants to monitor hop-by-hop response time on the network. Which IP SLA operation accomplishes this task?

A. ICMP path jitter

B. ICMP-echo
C. ICMP path echo
D. UDP-echo

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

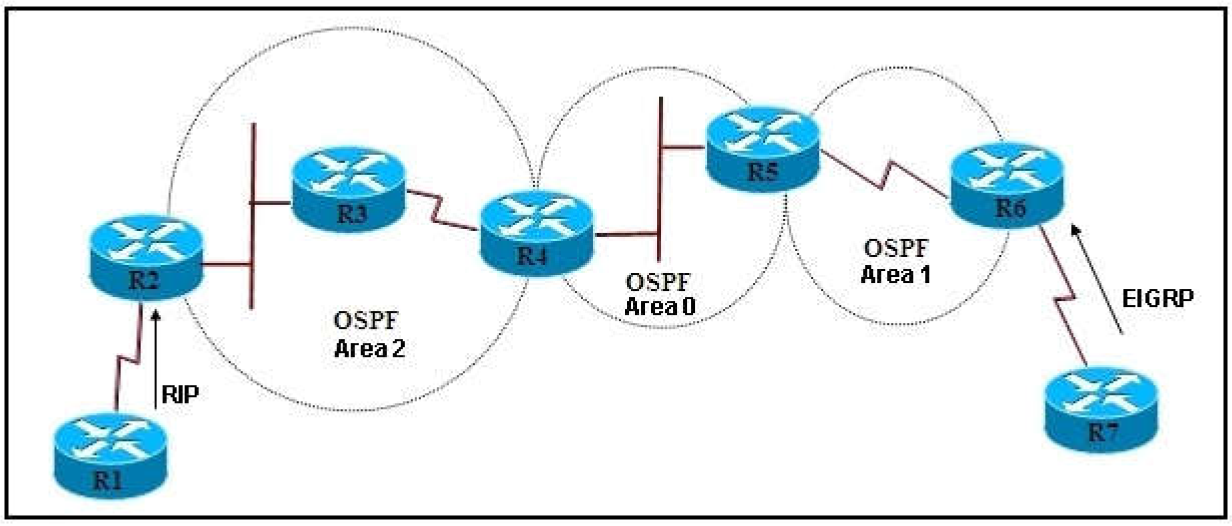
QUESTION 694
Which location within the network is preferred when using a dedicated router for Cisco IP SLA operations?

A. user edge
B. distribution edge
C. access edge
D. provider edge

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/en/US/technologies/tk648/tk362/tk920technologies_white_paper09186a00802d5efe.html

QUESTION 695
Refer to the exhibit.



Routers R2, R3, R4, and R5 have OSPF enabled.

What should be configured on the routers in area 1 to ensure that all default summary routes and redistributed EIGRP routes will be forwarded from R6 to area 1, and only a default route for all other OSPF routes will be forwarded from R5 to area 1.

A. R5(config-router)# area 1 stub
R6(config-router)# area 1 stub
B. R5(config-router)# area 1 stub no-summary
R6(config-router)# area 1 stub
C. R5(config-router)# area 1 nssa
R6(config-router)# area 1 nssa
D. R5(config-router)# area 1 nssa no-summary
R6(config-router)# area 1 nssa

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 696
If device R1 has 1-Gigabit and 10-Gigabit Ethernet interfaces, which command do you enter so that it takes full advantage of OSPF costs?

A. R1(config-router)#**auto-cost reference-bandwidth 10000**
B. R1(config-route-map)#**set metric 10000000000**
C. R1(config-if)#**ip ospf cost 10000000000**
D. R1(config-route-map)#**set metric 10000**
E. R1(config-router)#**auto-cost reference-bandwidth 10000000000**
F. R1(config-if)#**ip ospf cost 10000**

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 697

Which task must you perform to enable a point-to-point Frame Relay connection?

A. Enable inverse ARP
B. Disable inverse ARP
C. Configure the encapsulation type
D. Configure static address mapping

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 698
When a new PC is connected to the network, which step must it take first to receive a DHCP address?

A. It sends a DHCPREQUEST message to 255.255.255.255.
B. It sends a DCHPDISCOVER message to 255.255.255.255.
C. It sends a DHCPHELLO message to the DHCP server IP address.
D. It sends a DHCPREQUEST message to the DHCP server IP address

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 699
A network engineer is enabling RIPng on a new customer link. Under which configuration mode is RIPng enabled?

A. global
B. interface
C. IPv6
D. router

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 700
Which two causes of latency are true? (Choose two.)

A. split horizon
B. propagation delay
C. serialization delay
D. high bandwidth on a link
E. under-utilization of a link

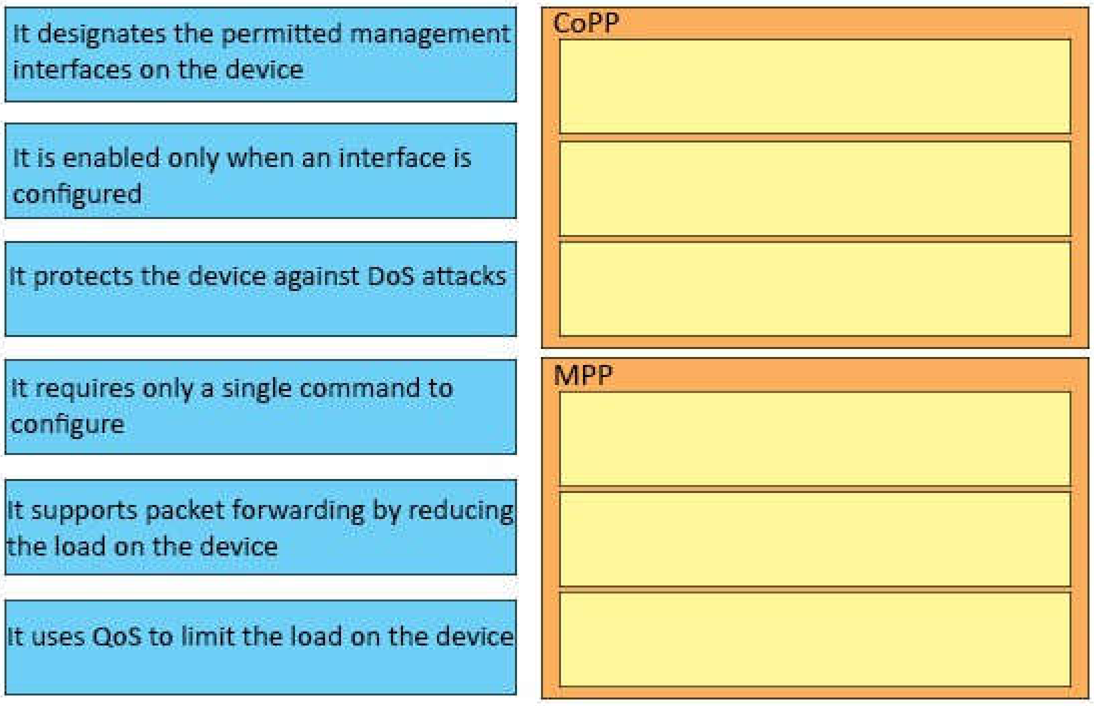
Correct Answer: BC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 701
DRAG DROP

Drag and drop the statements about device security from the left onto the correct features on the right.

Select and Place:



It designates the permitted management interfaces on the device

It is enabled only when an interface is configured

It protects the device against DoS attacks

It requires only a single command to configure

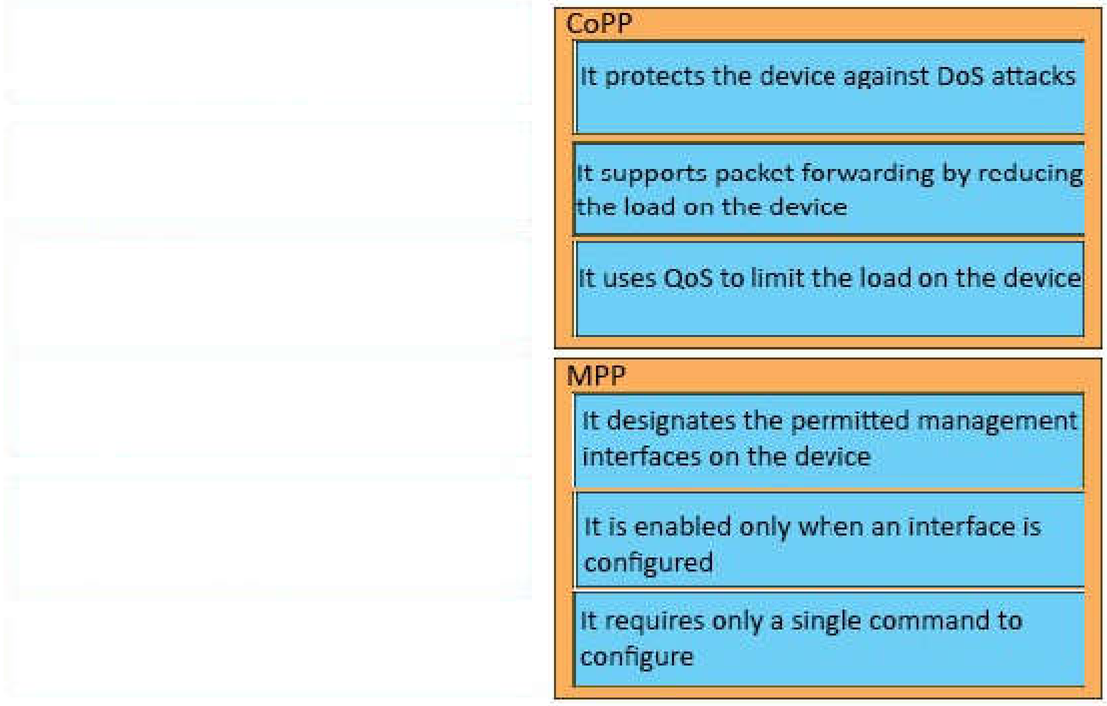
It supports packet forwarding by reducing the load on the device

It uses QoS to limit the load on the device

CoPP

MPP

Correct Answer:



CoPP

It protects the device against DoS attacks

It supports packet forwarding by reducing the load on the device

It uses QoS to limit the load on the device

MPP

It designates the permitted management interfaces on the device

It is enabled only when an interface is configured

It requires only a single command to configure

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 702
Which IP SLA operation can be used to simulate voice traffic on a network?

A. TCP-connect
B. ICMP-echo
C. ICMP-jitter
D. UDP-jitter

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 703
How can you minimize unicast flooding in a network?

A. Set the router’s ARP timeout value to less than the timeout value for Layer 2 forwarding table entries.
B. Set the router’s ARP timeout value to be the same as timeout value for Layer 2 forwarding table entries.
C. Configure HSRP on two routers, with one subnet preferred on the first router and a different subnet preferred on the second router.
D. Set the router’s ARP timeout value to greater than the timeout value for Layer 2 forwarding table entries.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 704

Which statement is true about an edge interface in relation to the Cisco Easy Virtual Network?

A. An edge interface connects to end devices such as hosts and servers that are VRF-aware.
B. An edge interface is used to differentiate VRF instances
C. An edge interface is configured using the vnet trunk command under the switches virtual interface
D. An edge interface connects a user device to the EVN while defining the EVN boundaries.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
An edge interface connects a user device to the EVN and in effect defines the boundary of the EVN. Edge interfaces connect end devices such as hosts and servers that are not VRF-aware. Traffic carried over the edge interface is untagged. The edge interface classifies which EVN the received traffic belongs to. Each edge interface is configured to belong to only one EVN.

Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.html

QUESTION 705
Which two statements about OSPFv3 are true? (Choose two.)

A. It uses loopback IPv6 addresses to form neighbor relationships.
B. The router ID is configured as an IPv4 address.
C. It uses LSA type 6 for intra-area prefixes.
D. The router ID is configured as an IPv6 address.
E. It is backwards-compatible with OSPFv2 through the use of a sham link.
F. It uses link-local addresses to form neighbor relationships.

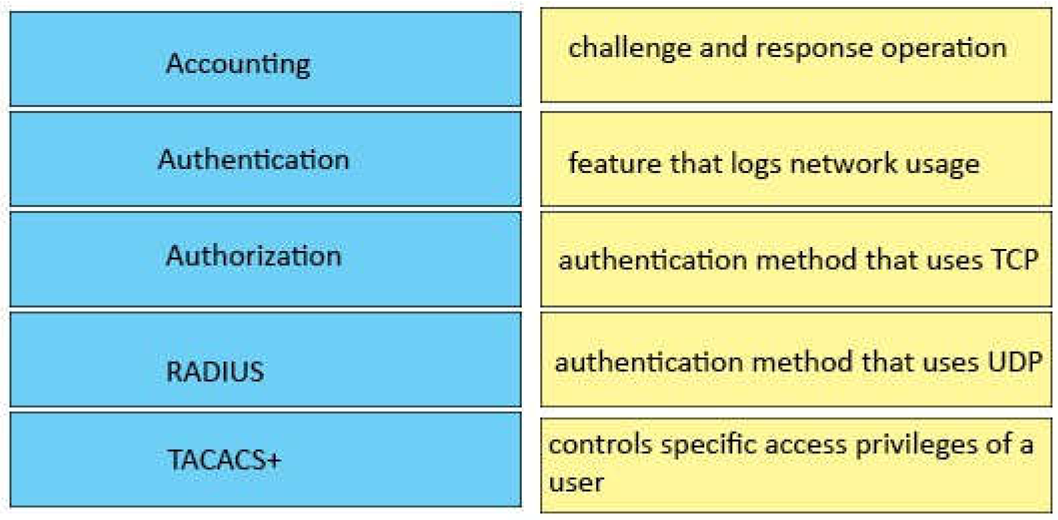
Correct Answer: BF
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/5_x/nx-os/unicast/configuration/guide/l3_cli_nxos/l3_ospfv3.pdf

QUESTION 706
DRAG DROP

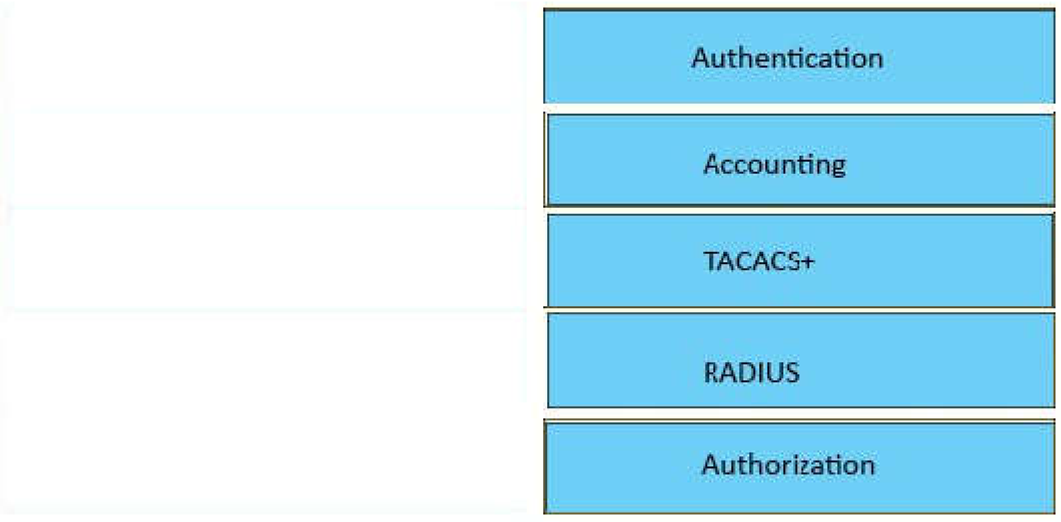
Drag and drop the AAA security features from the left onto the correct descriptions on the right.

Select and Place:



Accounting	challenge and response operation
Authentication	feature that logs network usage
Authorization	authentication method that uses TCP
RADIUS	authentication method that uses UDP
TACACS+	controls specific access privileges of a user

Correct Answer:



	Authentication
	Accounting
	TACACS+
	RADIUS
	Authorization

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 707
Which three methods can a network engineer use to fix a metric-based routing loop in the network? (Choose three.)

A. Implement offset lists at network boundaries
B. Filter routes manually using prefix lists
C. Filter routes based on tags
D. Filter routes manually using distribute lists
E. Utilize route database filters
F. Implement proper network summarization on key routing points

Correct Answer: ACF
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 708
Which two features are provided by EIGRP for IPv6? (Choose two.)

A. scaling
B. backbone areas
C. partial updates
D. Area Border Router
E. SPF algorithm

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-eigrp.html

QUESTION 709
Which two statements about DMVPN are true? (Choose two.)

A. Multicast traffic is not supported.
B. It requires full-mesh connectivity on the network.
C. IPsec encryption is not supported with statically addressed spokes.
D. It uses NHRP to create a mapping database of spoke addresses.
E. It supports dynamic addresses for spokes in a hub-and-spoke VPN topology.

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 710
Which two actions are common methods for migrating a network from one protocol to another? (Choose two.)

A. changing the relative administrative distances of the two routing protocols
B. changing the network IP addresses and bringing up the new Ip addresses using the new routing protocol.
C. removing the current routing protocol to the new routing protocol
D. redistributing routes from the current routing protocol to the new routing protocol
E. disabling IP routing globally and implementing the new routing protocol

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 711
A network engineer is enabling conditional debugging and executes two commands: **debug condition interface serial 0/0** and **debug condition interface serial 0/1**.

Which debugging output is displayed as a result?

A. Interfaces cannot be used as a debug condition.
B. Output is displayed for both specified interfaces.
C. Output is displayed for interface serial 0/1 only.
D. Output is displayed for interface serial 0/0 only.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/debug/command/reference/122debug/dbfcndtr.html#wp1017131

QUESTION 712
Which feature or technology is supported with stateful NAT64?

A. FTP and ICMP on an application layer gateway
B. IP multicast
C. VFR
D. NAT44 and NAT64 on the same interface

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/nat-xe-3s-book/iadnat-stateful-nat64.pdf

QUESTION 713
A network engineer is configuring two dedicated Internet connections within the Internet module. One connection is the primary connection to all wired business communications, while the other is the primary connection for all customer wireless traffic. If one of the links goes down, the affected traffic needs to be redirected to the redundant link.

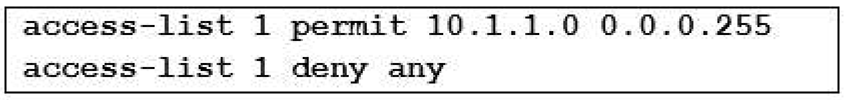
Which current technology should be deployed to monitor the scenario?

A. PBR
B. IP QoS
C. MMC
D. IP SLA
E. IP SAA

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 714
Refer to the exhibit.



```
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 deny any
```

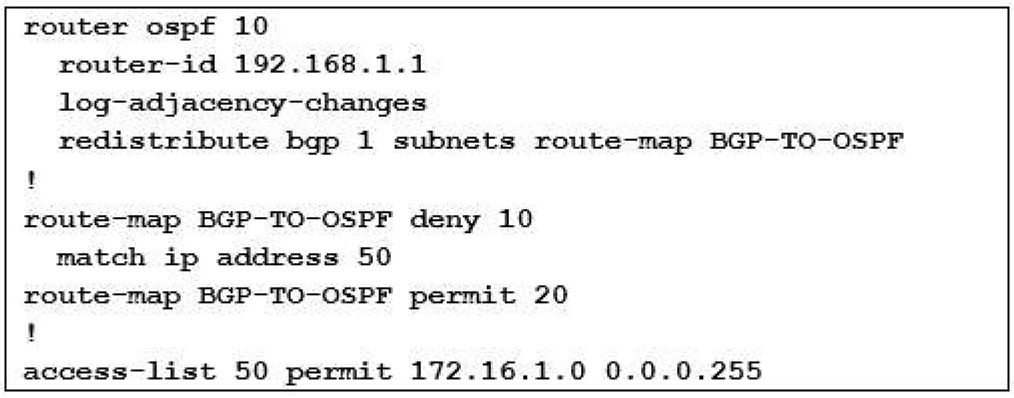
Which command is used to control the type of routes that are processed in incoming route updates?

A. ip vrf forwarding
B. distribute-list 1 out
C. passive-interface
D. distribute-list 1 in

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 715
Refer to the exhibit.



```
router ospf 10
  router-id 192.168.1.1
  log-adjacency-changes
  redistribute bgp 1 subnets route-map BGP-TO-OSPF
!
route-map BGP-TO-OSPF deny 10
  match ip address 50
route-map BGP-TO-OSPF permit 20
!
access-list 50 permit 172.16.1.0 0.0.0.255
```

Which statement about redistribution from BGP into OSPF process 10 is true?

A. Network 172.16.1.0/24 is not redistributed into OSPF.
B. Network 172.16.1.0/24 is redistributed with administrative distance of 1.
C. Network 10.10.10.0/24 is not redistributed into OSPF.
D. Network 10.10.10.0/24 is redistributed with administrative distance of 20.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

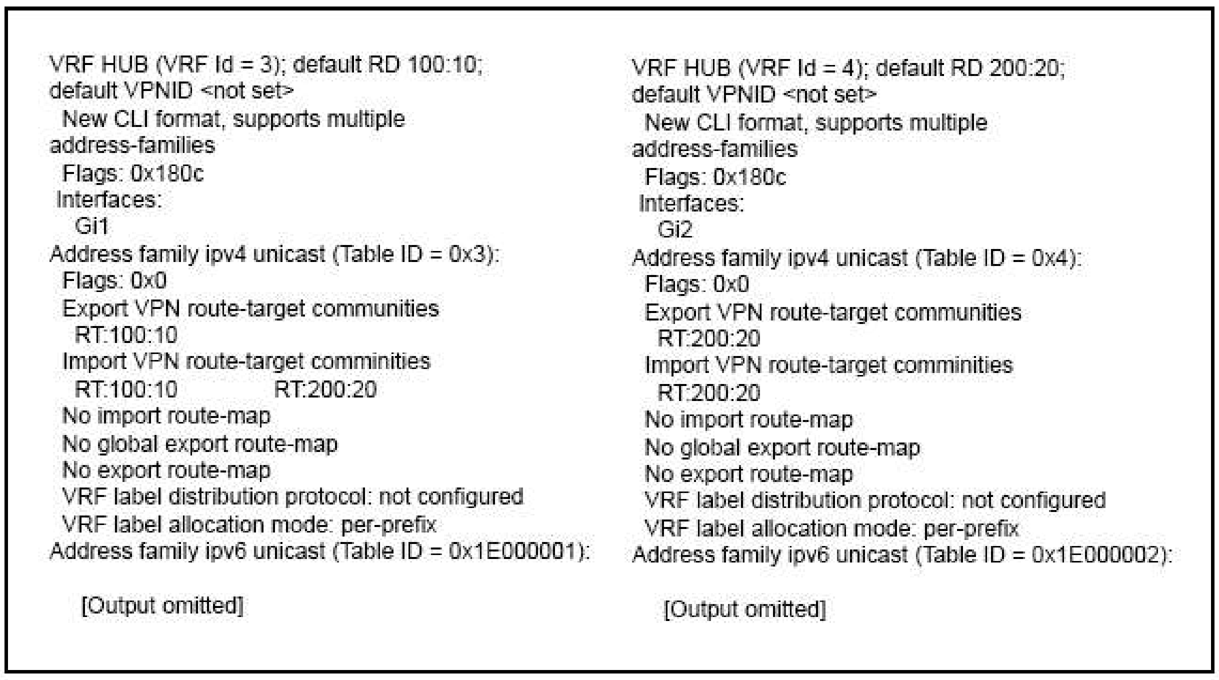
QUESTION 716
Which two statements are differences between AAA with TACACS+ and AAA with RADIUS? (Choose two.)

A. Unlike TACACS+, RADIUS sends packets with only the password encrypted.
B. Only TACACs+ uses TCP.
C. Only RADIUS uses TCP.
D. Unlike TACACS+, RADIUS supports accounting and authorization only.
E. Only TACACS+ combines authentication and authorization.

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html#comp_udp_tcp

QUESTION 717
Refer to the exhibit.



```
VRF HUB (VRF Id = 3); default RD 100:10;
default VPNID <not set>
  New CLI format, supports multiple
address-families
  Flags: 0x180c
 Interfaces:
    Gi1
Address family ipv4 unicast (Table ID = 0x3):
  Flags: 0x0
  Export VPN route-target communities
    RT:100:10
  Import VPN route-target comminities
    RT:100:10             RT:200:20
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 unicast (Table ID = 0x1E000001):

     [Output omitted]
```

```
VRF HUB (VRF Id = 4); default RD 200:20;
default VPNID <not set>
  New CLI format, supports multiple
address-families
  Flags: 0x180c
 Interfaces:
    Gi2
Address family ipv4 unicast (Table ID = 0x4):
  Flags: 0x0
  Export VPN route-target communities
    RT:200:20
  Import VPN route-target comminities
    RT:200:20
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 unicast (Table ID = 0x1E000002):

     [Output omitted]
```

A network engineer is modifying configurations for a customer that currently uses VPN connectivity between their sites. The customer had added a new spoke site but it does not have reachability to servers located at the hub.

Based on the output, which statement describes the cause?

A. The HUB VRF is not exporting Route-Target 200:20
B. The default VPNID is not on VRF HUB or VRF SPOKE
C. The SPOKE VRF is not importing Route-Target 100:10
D. The interfaces of VRF HUB and VRF SPOKE do not match.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 718
Which command can be entered on router R5 to configure 80 percent of the bandwidth of a link for EIGRP Autonomous System 55?

A. R5(config-if#)#ip bandwidth percent eigrp bandwidth 55 80
B. R5(config-pmap-c)#priority percent 80
C. R5(config-if)#ipv6 bandwidth-percent eigrp 55 80
D. R5(config-if)#ipv6 bandwidth-percent eigrp 80 55
E. R5(config-if)#ip bandwidth-percent eigrp 80 55

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 719
Which statement about the metric calculation in EIGRP is true?

A. The mean value of bandwidth between the source and destination is used.
B. The minimum bandwidth between the source and destination is used.
C. The minimum delay along the path is used.
D. The maximum delay along the path is used.

Correct Answer: C

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 720
Which statement best describes the following two OSPF commands, which are used to summarize routes?

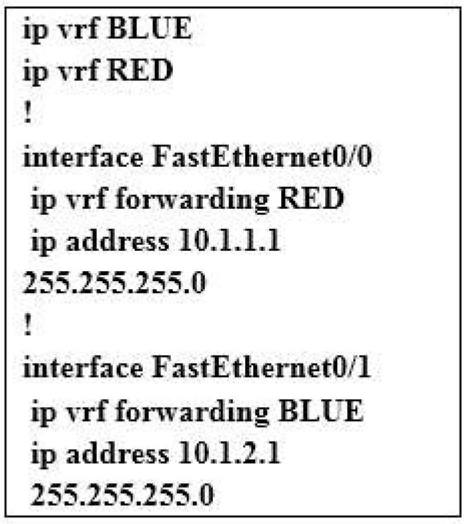
area 0 range 192.168.110.0 255.255.0.0
summary-address 192.168.110.0 255.255.0.0

A. The area range command specifies the area where the subnet resides are summarizes it to other areas. The summary-address command summarized external routes.
B. The area range command summarized subnets for a specific area. The summary-address command summarizes a subnet for all areas.
C. The area range command defines the area where the network resides. The summary-address command enables autosummarization.
D. the area range command defines the area where the network resides. The summary-address command summarizes a subnet for all areas.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 721
Refer to the exhibit.



```
ip vrf BLUE
ip vrf RED
!
interface FastEthernet0/0
 ip vrf forwarding RED
 ip address 10.1.1.1
255.255.255.0
!
interface FastEthernet0/1
 ip vrf forwarding BLUE
 ip address 10.1.2.1
 255.255.255.0
```

Network users on the 10.1.2.0/24 subnet have a default gateway of 10.1.2.254.

Which command will configure this gateway?

A. router(config)#**ip route 0.0.0.0 0.0.0.0 fastethernet0/1**
B. router(config)#**ip route vrf BLUE 0.0.0.0 0.0.0.0 10.1.2.254**
C. router(config)#**ip route vrf RED 0.0.0.0 0.0.0.0 10.1.2.254**
D. router(config)#**ip route 0.0.0.0 0.0.0.0 10.1.2.254**

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 722
Which two statements about PPPoE packet types are true? (Choose two.)

A. PADR is a broadcast packet sent from the client to request a new server.
B. PADO is a broadcast reply packet sent to the client.
C. PADO is a unicast reply sent to the client.
D. PADI is an initialization packet sent as a broadcast message.
E. PADR is a unicast confirmation packet sent to the client.

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 723
What is VRF-Lite?

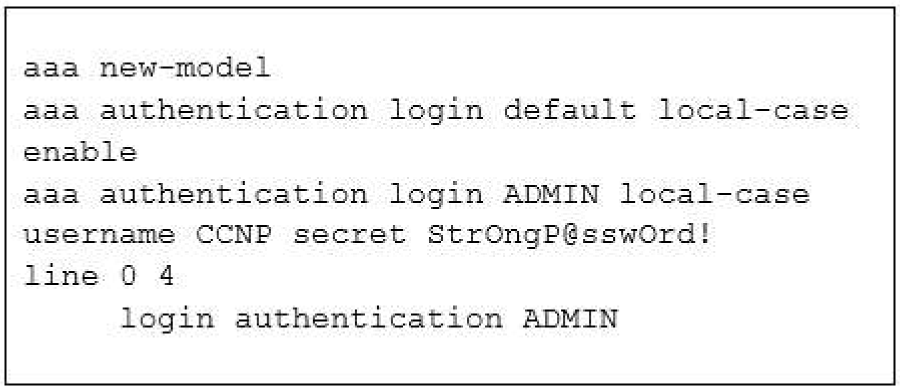
A. VRF without MPLS
B. VRF without VPN
C. VRF without Cisco Express Forwarding switching
D. VRF without independent routing tables

Correct Answer: A

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 724
Refer to the exhibit.



```
aaa new-model
aaa authentication login default local-case
enable
aaa authentication login ADMIN local-case
username CCNP secret StrOngP@sswOrd!
line 0 4
     login authentication ADMIN
```

How can you change this configuration so that when user CCNP logs in, the **show run** command is executed and the session is terminated?

A. Assign privilege level 15 to the CCNP username
B. Assign privilege level 14 to the CCNP username
C. Add the **access-class** keyword to the **aaa authentication** command.
D. Add the **autocommand** keyword to the **username** command.
E. Add the **autocommand** keyword to the **aaa authentication** command.
F. Add the **access-class** keyword to the username command.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/cmdrefs/username.htm

QUESTION 725
Which two statements about redistributing EIGRP into OSPF are true? (Choose two.)

A. The redistributed EIGRP routes appear as OSPF external type 2 routes in the routing table.
B. The redistributed EIGRP routes are placed into an OSPF area whose area ID matches the EIGRP autonomous system number.
C. The redistributed EIGRP routes appear as type 5 LSAs in the OSPF database.
D. The administrative distance of the redistributed routes is 170.
E. The redistributed EIGRP routes appear as OSPF external type 1.
F. The redistributed EIGRP routes as type 3 LSAs in the OSPF database.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 726
A network administrator is attempting to configure IP SLA to allow one time stamp to be logged when a packet arrives on the interface and one time stamp to be logged when a packet leaves the interface.

Which IP SLA accuracy tool enables this functionality?

A. Trigger
B. Responder
C. Trap
D. Logging
E. RTT

Correct Answer: E
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 727
A network engineer executes the **show ip flow interface** command. Which type of information is displayed on the interface?

A. NetFlow configuration
B. IP Cisco Express Forwarding statistics
C. route cache information
D. error statistics

Correct Answer: A
Section: Mix Questions

Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/command/nf-cr-book.pdf

QUESTION 728
Which IOS commands can you use to limit the CPU impact of log generation and transmission on an IOS router?

A. You can use the ip access-list logging limit command in conjunction with the **logging rate-interval** command.
B. You can use the ip access-list syslog-logging interval command in conjunction with the **logging rate-limit** command.
C. You can use the ip access-list logged interval command in conjunction with the **logged rate-limit** command.
D. You can use the ip access-list logging interval command in conjunction with the **logging rate-limit** command.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/about/security-center/access-control-list-logging.html

QUESTION 729
Which issue is important to address when integrating two networks with different routing protocols?

A. preventing asymmetric routing
B. preventing UDP starvation
C. mitigating UDP latency
D. controlling unicast flooding
E. handling IPv4 fragmentation

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 730
A network engineer wants to implement an SNMP notification process for host machines using the strongest security available. Which command accomplishes this task?

A. router(config)#snmp-server host 172.16.200.225 traps v1
B. router(config)#snmp-server host 172.16.200.225 traps v2c auth
C. router(config)#snmp-server host 172.16.200.225 traps v3
D. router(config)#snmp-server host 172.16.200.225 traps v2c

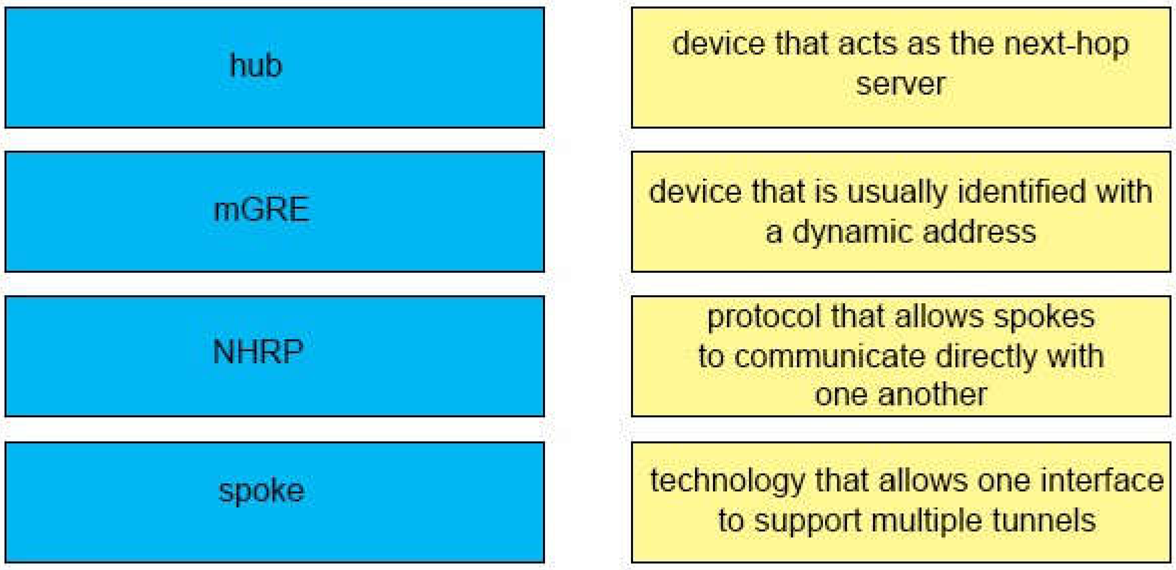
Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 731
DRAG DROP

Drag and drop the DMVPN components from the left onto the correct descriptions on the right.

Select and Place:



hub	device that acts as the next-hop server
mGRE	device that is usually identified with a dynamic address
NHRP	protocol that allows spokes to communicate directly with one another
spoke	technology that allows one interface to support multiple tunnels

Correct Answer:

hub

spoke

NHRP

mGRE

Section: Mix Questions
Explanation

Explanation/Reference:

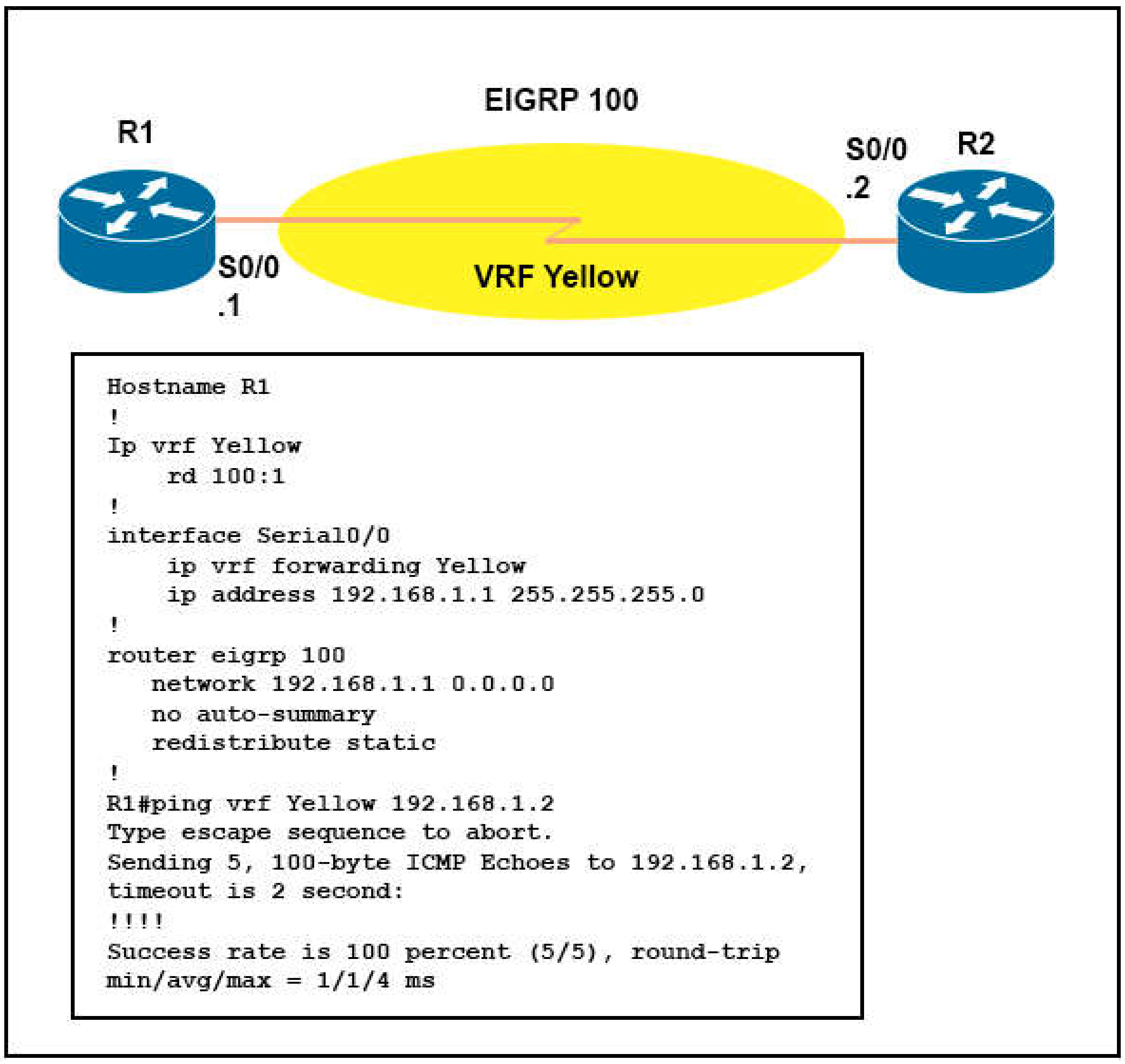
QUESTION 732
What does SNMP v2c use for authentication?

A. SSL certificate
B. community string
C. username and password
D. Hash algorithm

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv2c.pdf

QUESTION 733
Refer to the exhibit.



```
Hostname R1
!
Ip vrf Yellow
    rd 100:1
!
interface Serial0/0
    ip vrf forwarding Yellow
    ip address 192.168.1.1 255.255.255.0
!
router eigrp 100
   network 192.168.1.1 0.0.0.0
   no auto-summary
   redistribute static
!
R1#ping vrf Yellow 192.168.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 192.168.1.2,
timeout is 2 second:
!!!!
Success rate is 100 percent (5/5), round-trip
min/avg/max = 1/1/4 ms
```

R1 is configured with VRF-Lite and can ping R2. R2 is fully configured, but it has no active EIGRP neighbors in vrf Yellow. If the configuration of r2 is complete, then which issue prevents the EIGRP 100 neighbor relationship in vrf Yellow from forming?

A. The interface IP address are not in the same subnet.
B. The no auto-summary command is preventing the EIGRP neighbor relationship from forming.
C. EIGRP 100 network 192.168.1.0/24 is configured in the global routing table on R1.

D. There is a Layer 1 issue that prevents the EIGRP neighbor relationship from forming.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 734
If you want to migrate an IS-IS network to another routing protocol with a lower AD, which two protocols do you consider? (Choose two.)

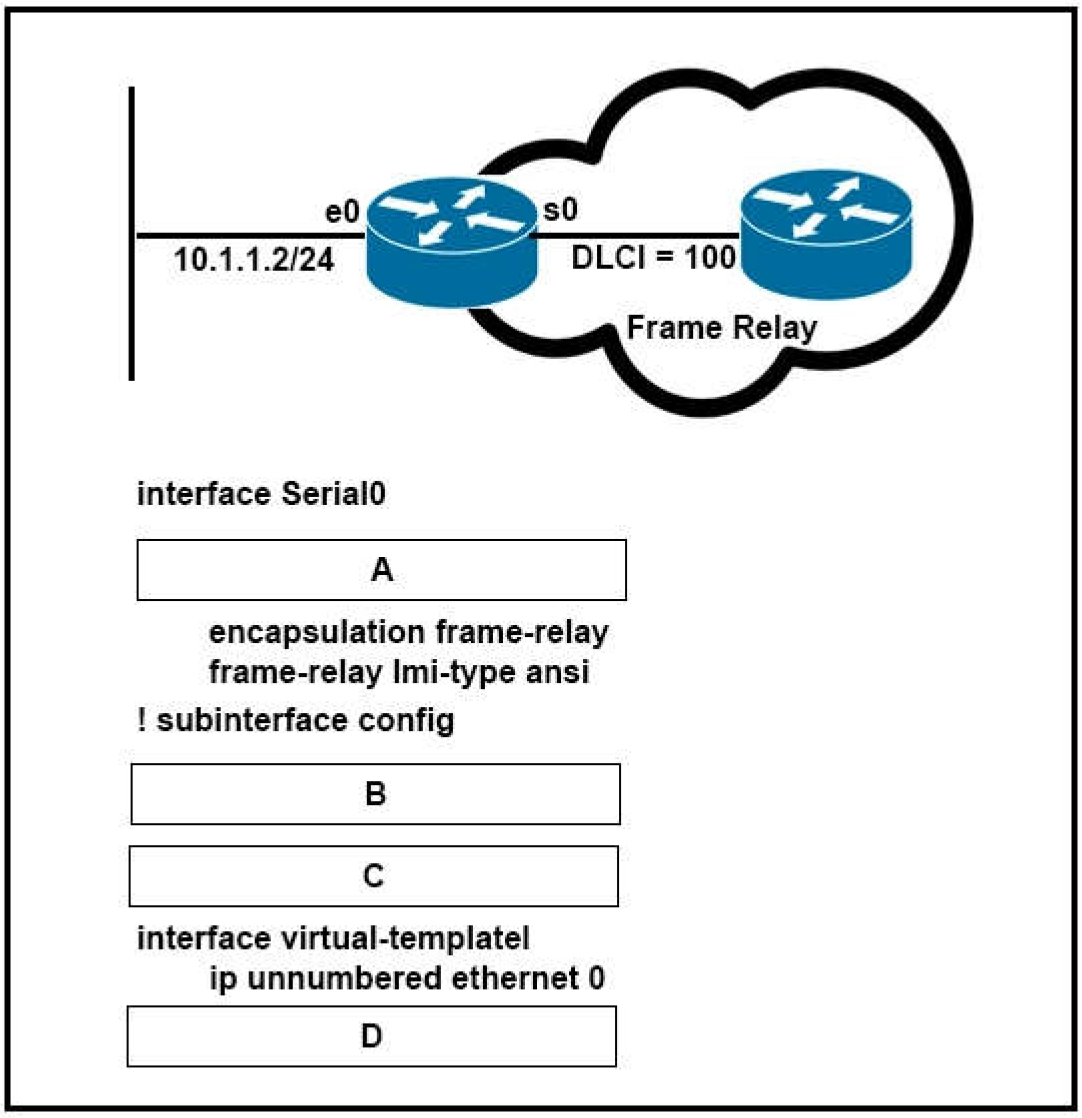
A. RIP
B. UDP
C. TCP/IP
D. EIGRP
E. OSPF
F. internal BGP

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Administrative_distance

QUESTION 735
DRAG DROP

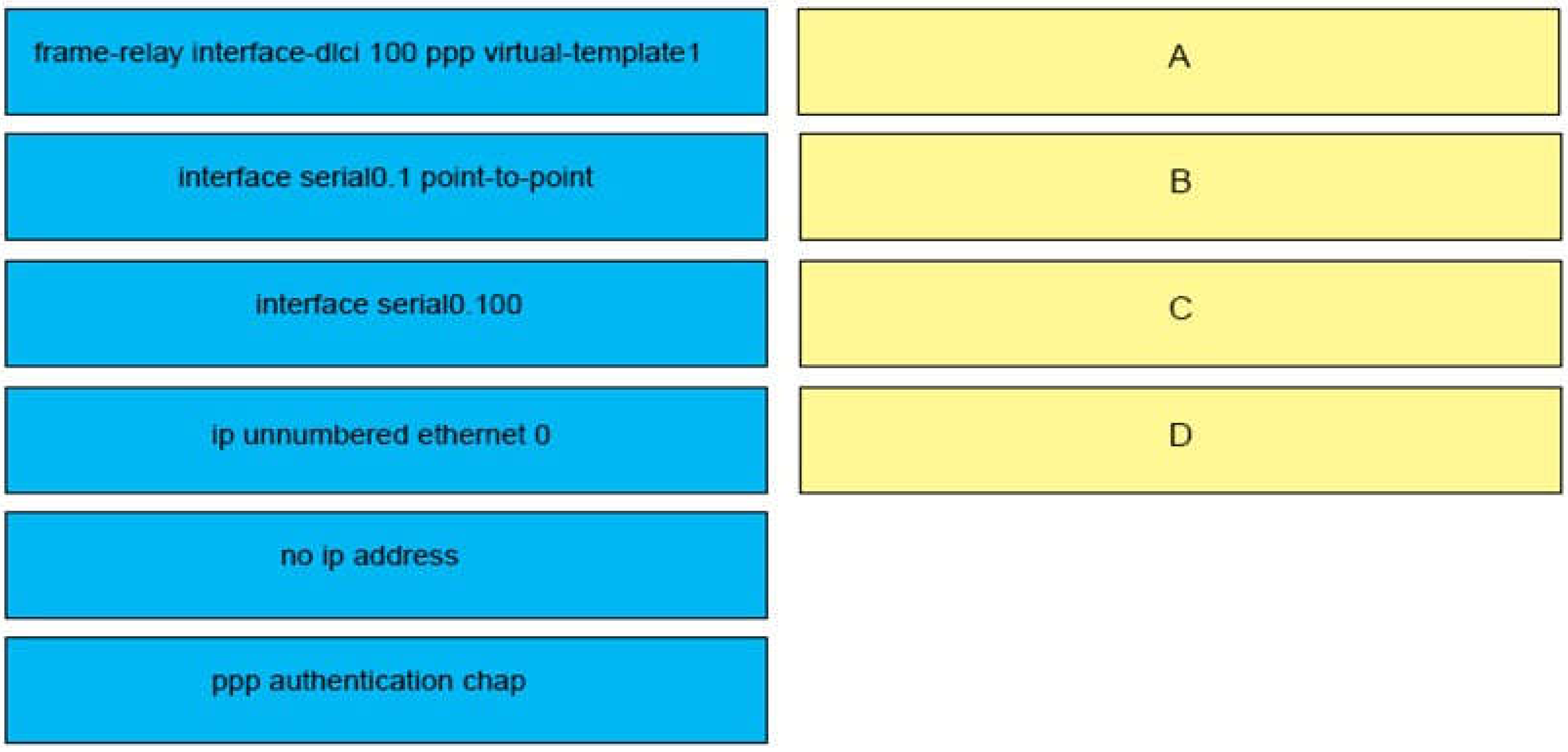
Refer to the exhibit.



```
interface Serial0
[ A ]
        encapsulation frame-relay
        frame-relay lmi-type ansi
! subinterface config
[ B ]
[ C ]
interface virtual-templatel
        ip unnumbered ethernet 0
[ D ]
```

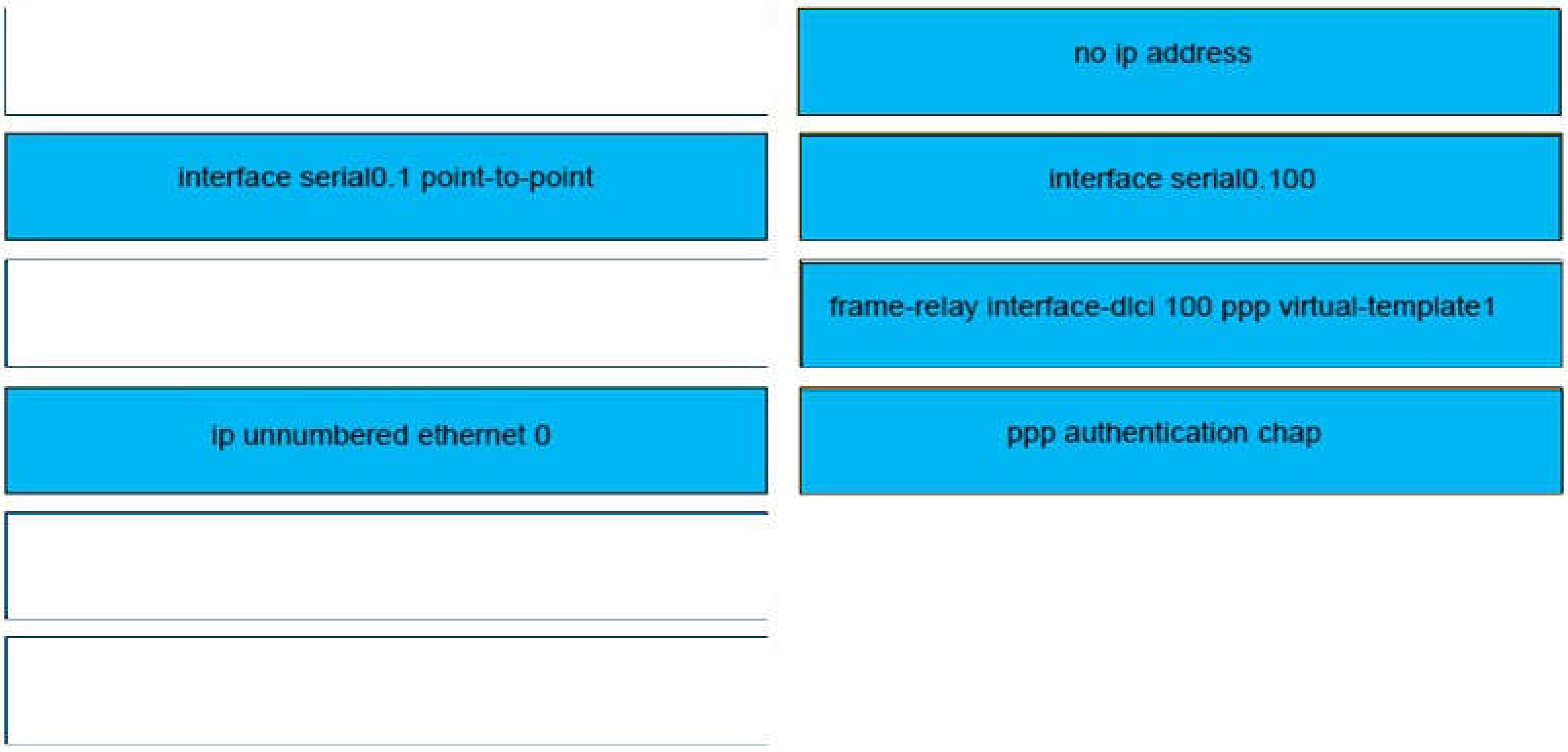
You are configuring the R1 Serial0 interface for a point-to-point connection. drag and drop the required configuration statements from the left onto the correct locations from the diagram on the right. Not all commands are used.

Select and Place:



frame-relay interface-dlci 100 ppp virtual-template1	A
interface serial0.1 point-to-point	B
interface serial0.100	C
ip unnumbered ethernet 0	D
no ip address	
ppp authentication chap	

Correct Answer:



	no ip address
interface serial0.1 point-to-point	interface serial0.100
	frame-relay interface-dlci 100 ppp virtual-template1
ip unnumbered ethernet 0	ppp authentication chap

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 736
Which action is the most efficient way to handle route feedback when converting a RIPv2 network to OSPF?

A. Implementing IP prefix lists
B. Implementing distribute lists
C. Implementing route maps with access lists.
D. Implement route tags.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 737
Which two effects of asymmetric routing are true? (Choose two.)

A. unicast flooding
B. uRPF failure
C. errdisabling of ports
D. port security violations
E. excessive STP convergence

Correct Answer: AB
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 738
Which functions are included in the two-message rapid exchange that a DHCPv6 client can receive from a server?

A. advertise and request
B. solicit and reply
C. solicit and request
D. advertise and reply

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html

QUESTION 739
Which two statements are examples of the differences between IPv4 and IPv6 EIGRP? (Choose two.)

A. Network command is not used in IPv6.
B. DUAL is used for route calculations.
C. IPv6 keyword is used in many EIGRP commands.
D. DUAL is not used for route calculations.
E. Network command is used in IPv6.

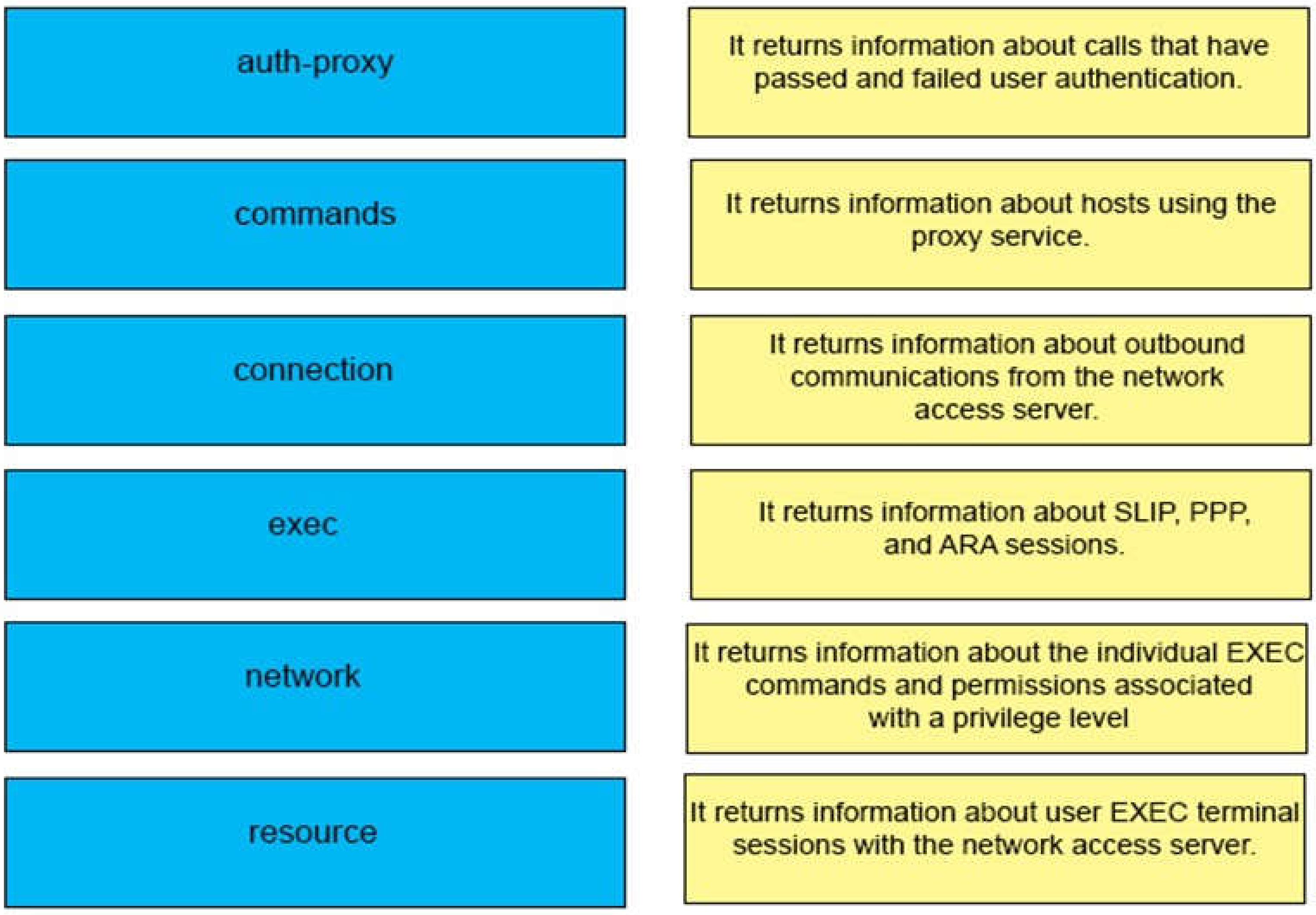
Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: http://www.ciscopress.com/articles/article.asp?p=2137516&seqNum=4

QUESTION 740
DRAG DROP

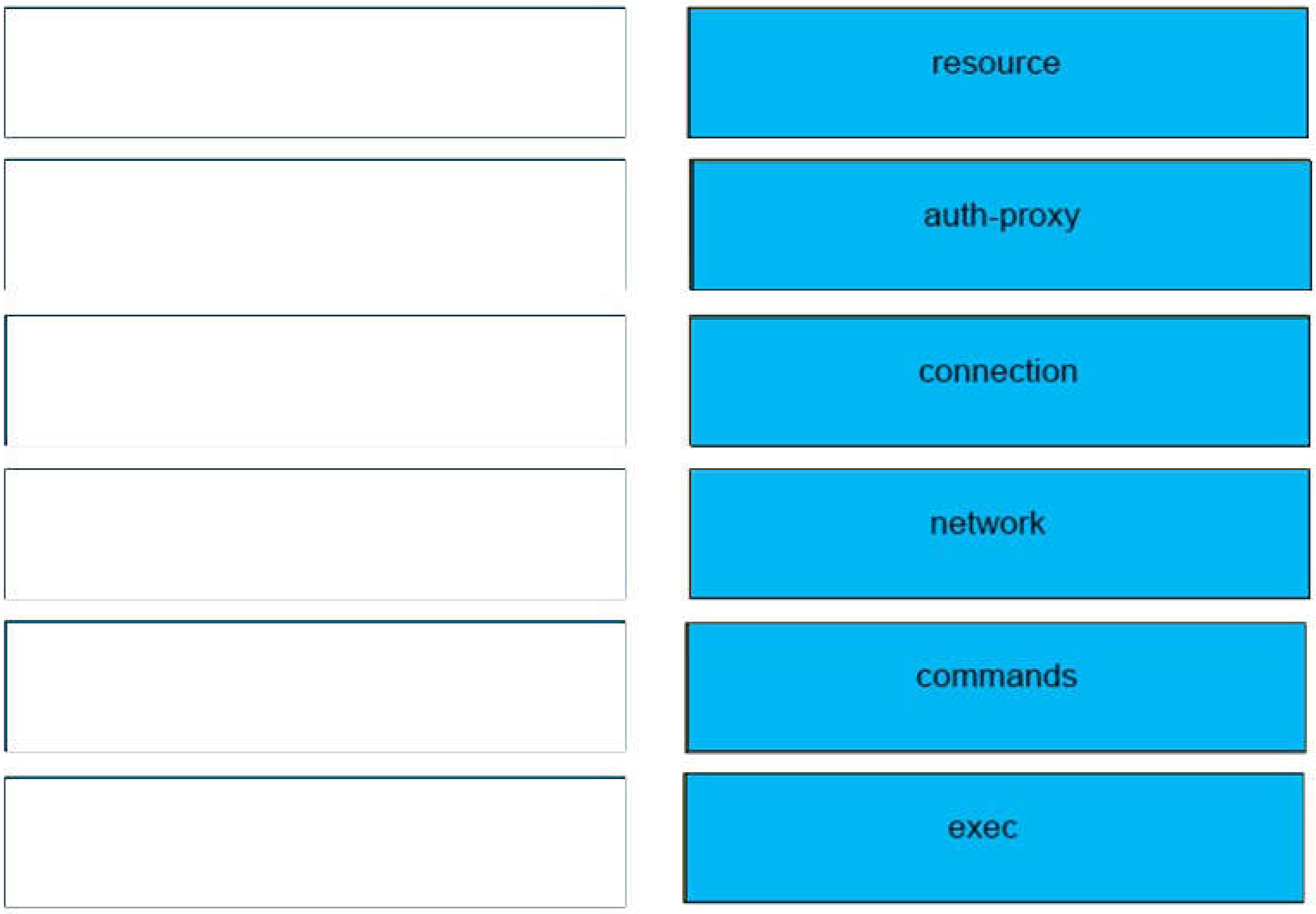
Drag and drop the methods supported by the **aaa accounting** command from the left onto the correct descriptions on the right.

Select and Place:



auth-proxy	It returns information about calls that have passed and failed user authentication.
commands	It returns information about hosts using the proxy service.
connection	It returns information about outbound communications from the network access server.
exec	It returns information about SLIP, PPP, and ARA sessions.
network	It returns information about the individual EXEC commands and permissions associated with a privilege level
resource	It returns information about user EXEC terminal sessions with the network access server.

Correct Answer:



Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/security/command/reference/fsecur_r/srfacct.html

QUESTION 741
Which statement about the split-horizon rule for distance vector routing protocols is true?

A. A router advertises a route to an unreachable network with an infinite metric.
B. A router does not advertise routes to any neighboring router.
C. A router advertises routes back out the interface on which it learned them with an infinite metric.
D. A router does not advertise routes back out the interface on which it learned them.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 742
A customer requests policy-based routing. Packets arriving from source 209.165.200.225 should be sent to the next hop at 209.165.200.227, with the precedence bit set to priority. Packets arriving from source 209.165.200.226 should be sent to the next hop at 209.165.200.228, with the precedence bit set to critical.

Which configuration completes these requirements?

A.
```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
route-map Texas permit 10
match ip address 1
set ip precedence critical
set ip next –hop 209.165.200.227
!
route-map Texas permit 20
match ip address 2
set ip precedence priority
set ip next-hop  209.165.200.228
!
interface ethernet 1
ip policy route-map Texas
```

B.
```
access-list 1 permit 209.165.200.225
access-list 2 permit 209.165.200.226
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next –hop 209.165.200.227
!
route-map Texas permit 20
match ip address 2
```

set ip precedence critical
set ip next-hop 209.165.200.228
!
interface ethernet 1
ip policy route-map Texas

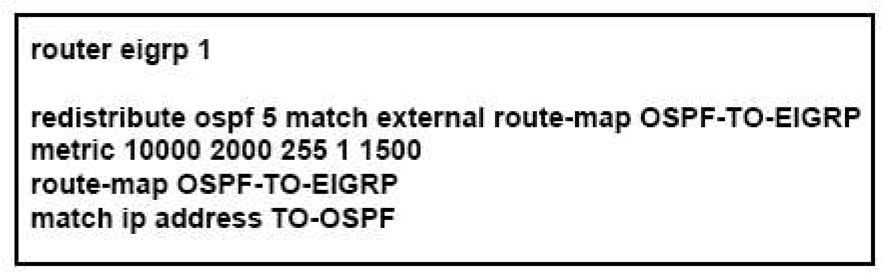
C. **access-list 1 permit 209.165.200.228**
access-list 2 permit 209.165.200.227
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next –hop 209.165.200.226
!
route-map Texas permit 20
match ip address 2
set ip precedence critical
set ip next-hop 209.165.200.225
!
interface ethernet 1
ip policy route-map Texas

D. **access-list 1 permit 209.165.200.227**
access-list 2 permit 209.165.200.228
!
route-map Texas permit 10
match ip address 1
set ip precedence priority
set ip next –hop 209.165.200.225
!

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 743
Refer to the exhibit.



```
router eigrp 1

redistribute ospf 5 match external route-map OSPF-TO-EIGRP
metric 10000 2000 255 1 1500
route-map OSPF-TO-EIGRP
match ip address TO-OSPF
```

Which routes from OSPF process 5 are redistributed into EIGRP?

A. E1 and E2 subnets matching access list TO-OSPF
B. E1 and E2 subnets matching prefix list TO-OSPF
C. only E2 subnets matching access list TO-OSPF
D. only E1 subnets matching prefix list TO-OSPF

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

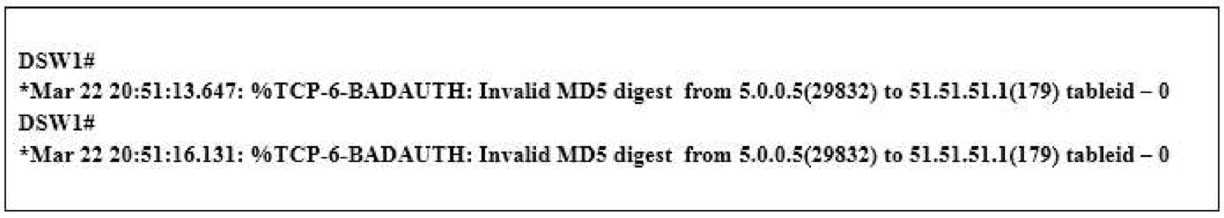
QUESTION 744
Which SNMP security level is available across all versions of the protocol?

A. authPriv
B. NoAuthPriv
C. AuthNoPriv
D. NoAuthNoPriv

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 745
Refer to the exhibit.



```
DSW1#
*Mar 22 20:51:13.647: %TCP-6-BADAUTH: Invalid MD5 digest  from 5.0.0.5(29832) to 51.51.51.1(179) tableid – 0
DSW1#
*Mar 22 20:51:16.131: %TCP-6-BADAUTH: Invalid MD5 digest  from 5.0.0.5(29832) to 51.51.51.1(179) tableid – 0
```

All neighbor routers are in the BGP peer group named PEER-1. All passwords are configured as cisco. These messages are logged to the console of router DSW1, which is peering with router Core.

Which two configurations allow a peering session to form between DSW1 and the Core? (Choose two.)

A. DSW1(config-router)#neighbor 5.0.0.5 peer-group PEER-1
   DSW1(config-router)#neighbor PEER-1 password cisco
B. Core(config-router)#neighbor 5.0.0.5 peer-group PEER-1
   Core(config-router)#neighbor PEER-1 password cisco
C. Core(config-router)#neighbor 51.51.51.1 peer-group PEER-1
   Core(config-router)#neighbor PEER-1 password cisco
D. DSW1(config-router)#neighbor 51.51.51.1 peer-group PEER-1
   DSW1(config-router)#neighbor PEER-2 password cisco
E. Core(config-router)#neighbor 5.0.0.5 peer-group PEER-2
   Core(config-router)#neighbor PEER-1 password cisco

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 746
Which address is an IPv6 multicast address?

A. 2002:0:0:0:0:0:0:2
B. 0002:0:0:0:0:0:0:2
C. FF02:0:0:0:0:0:0:2
D. FE02:0:0:0:0:0:0:2

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 747
Which two statements about VRF-Lite configurations are true? (Choose two.)

A. They support IS-IS.
B. Each customer has its own dedicated TCAM resources.
C. Different customers can have overlapping IP addresses on different VPNs.
D. They support the exchange of MPLS labels.
E. They support a maximum of 512,000 routes.
F. Each customer has its own private routing table.

Correct Answer: CF
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/25ew/configuration/guide/conf/vrf.pdf

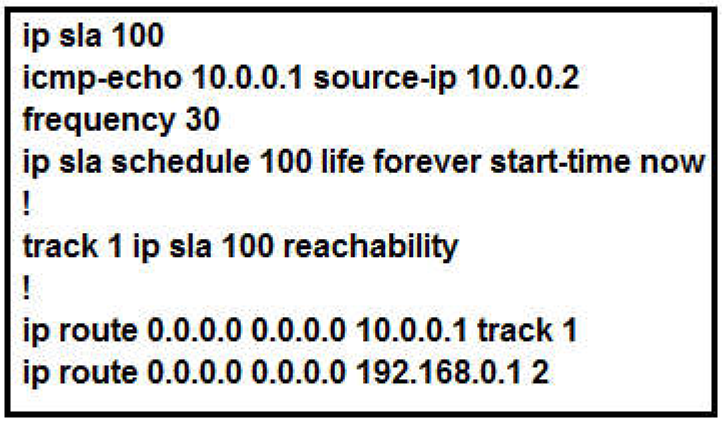
QUESTION 748
What is the default maximum segment size for TCP traffic?

A. 536
B. 1492
C. 1500
D. 1508
E. 3340
F. 4096

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://en.wikipedia.org/wiki/Maximum_segment_size

QUESTION 749



```
ip sla 100
icmp-echo 10.0.0.1 source-ip 10.0.0.2
frequency 30
ip sla schedule 100 life forever start-time now
!
track 1 ip sla 100 reachability
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1 track 1
ip route 0.0.0.0 0.0.0.0 192.168.0.1 2
```

Refer to the exhibit. Which statement describes the effect of this configuration on a Cisco router?

A. The default route through 10.0.0.1 is never used.
B. The default route through 192.168.0.1 is used only when 10.0.0.1 is unreachable.
C. The default route through 192.168.0.1 is never used.
D. The default route through 10.0.0.1 is used only when 192.168.0.1 is unreachable.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 750
A network engineer has configured an IOS router to synchronize its clock with a Windows server. After several minutes, the network engineer notices that the local time on the router does not match the time on the Windows server. What is the reason for this?

A. Either a firewall between the two devices or on ACL on the router is blocking UDP port 123.
B. Either a firewall between the two devices or an ACL on the router is blocking TCP port 958.
C. Either a firewall between the two devices or an ACL on the router is blocking UDP port 958.
D. Either a firewall between the two devices or an ACL on the router is blocking TCP port 123.

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 751
Which types of LSAs are present in the stub area?

A. LSA type 1, 2, 3, 4, and 5
B. LSA type 3 and 5
C. LSA type 1 and 2
D. LSA type 1, 2 and 3

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 752
Which command creates a manual summary on an interface when using EIGRP?

A. **summary-address eigrp 100 172.32.0.0 255.255.254.0**
B. **ip summary-address eigrp 100 172.32.0.0 255.255.254.0**
C. **area 100 range 172.32.0.0 255.255.254.0**
D. **ip summary-address 100.172.32.0.0 255.255.254.0**

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 753
DRAG DROP

Drag and drop the statements about NAT64 from the left onto the correct NAT64 types on the right.

Select and Place:

Correct Answer:

Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/xe-3s/nat-xe-3s-book/iadnat-stateful-nat64.pdf

QUESTION 754
Which two steps must you perform to allow access to a device when the connection to a remote TACACS+ authentication server fails? (Choose two.)

A. Configure accounting to reference the log of previously authenticated connections.
B. Include the **local** keyword in the AAA configuration.
C. Configure the device to accept Telnet and SSH connections.
D. Remove the **aaa new model** command from the global configuration.
E. Configure a local username and password on the device.

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 755
Which statement about the IP SLA feature is true?

A. It keeps track of the number of packets and bytes that are observed in each flow by storing information in a cache flow.
B. It classifies various traffic types by examining information within Layers 3 through 7.
C. It measures how the network treats traffic for specific applications by generating traffic that bears similar characteristics to application traffic.
D. It ensures that there are appropriate levels of service for network applications.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 756
Which feature mitigates fragmentation issues caused by endpoint hosts?

A. TCP Flow Control
B. ICMP DF bit
C. PMTUD
D. TCP MSS

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 757
Which two statements about the OSPF down bit are true? (Choose two.)

A. It is set when MP-BGP routes are redistributed into OSPF.
B. It is set only for LSA types 1, 2, and 4.
C. It is set only for LSA types 3, 5, and 7.
D. It is set when OSPF routes are redistributed into BGP.
E. It is set only when an OSPF virtual link is created.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 758
Which two LSA types were introduced to support OSPF for IPv6? (Choose two.)

A. type 9
B. type 5
C. type 10
D. type 8
E. type 7

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 759
Which statement about dynamic NAT is true?

A. It maps inside addresses to different port numbers.

B. It creates a one-to-one mapping of inside addresses to a global address.
C. It maps inside addresses to a pool of global addresses.
D. It uses the **overload** command to map addresses.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

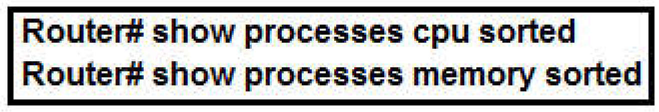
QUESTION 760
Which two types of traffic can benefit from LLQ? (Choose two.)

A. email
B. video
C. file transfer
D. telnet
E. voice

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 761



```
Router# show processes cpu sorted
Router# show processes memory sorted
```

Refer to the exhibit. Based on Cisco best practice, which statement about the output is true?

A. The output should be analyzed by a network engineer before executing other show commands on an IOS router in production.
B. The output should be analyzed by a network engineer before executing any debug commands on an IOS router in production.
C. The output should be analyzed by a network engineer before allocating additional memory and CPU usage to processes on an IOS router in production.
D. The output should be analyzed by a network engineer before executing any configuration commands on an IOS router in production.

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 762
Users were moved from the local DHCP server to the remote corporate DHCP server. After the move, none of the users were able to use the network.
Which two issues will prevent this setup from working properly? (Choose two.)

A. The route to the new DHCP server is missing.
B. The broadcast domain is too large for proper DHCP propagation.
C. 802.1X is blocking DHCP traffic.
D. Auto-QoS is blocking DHCP traffic.
E. The DHCP server IP address configuration is missing locally.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 763
Which command do you enter on router R6 so that BGP supports multiple protocols?

A. R6(config-router)#**no bgp default ipv4-unicast**
B. R6(config-router-af)# **bgp additional-paths install**
C. R6(config-router)#**bgp default ipv4-multicast**
D. R6(config-router-af)#**no bgp default ipv4-multicast**
E. R6(config-router)#**no address-family ipv4 unicast**

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 764
PPPoE requires certain signals and information to establish, accept, control and terminate the session.
The basic signalling is shown below.

A. (PPPoE Active Discovery Request), PADI (PPPoE Active Discovery Initiation)
B. (PPPoR Active Discovery Request), PARP (PPPoE Active Discovery Initiation)

C. (PPPoE Active Discovery Reaching), PADI (PPPoE Active Discovery Initiating)
D. (PPP Active Discovery Request), PADI (PPP Active Discovery Initiation)

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 765
Choose correct statement about Dynamic NAT. (Choose two.)

A. inside local
B. outside local
C. this list will be translated to this subnet (which is pool)
D. outside global

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 766
Which two conditions can cause BGP neighbor establishment to fail? (Choose two.)

A. There is an access list blocking all TCP traffic between the two BGP neighbors
B. The IBGP neighbor is not directly connected.
C. BGP synchronization is enabled in a transit autonomous system with fully-meshed IBGP neighbors.
D. The BGP update interval is different between the two BGP neighbors
E. The BGP neighbor is referencing an incorrect autonomous system number in its neighbor statement.

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 767
Which feature can be used to reduce the number of ICMP unreachable message egressing a router?

A. uRPF
B. ICMP rate-limiting
C. ip unreachables command
D. Asymmetric routing

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 768
What happens when a router receives a route with an administrative distance of 255?

A. The router installs the route as the most preferred path in the routing table.
B. The router installs the route as the least preferred path in the routing table
C. The router becomes the feasible successor for the route
D. The router is unable to install the route into the routing table

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 769
A network access server using TACACS+ for AAA operations receives an error message from the TACACS server.

Which action does the network access server take next?

A. It attempts to authenticate the user against RADIUS
B. It restarts and attempts to reconnect to the TACACS+ server
C. It rejects the user access request the
D. It checks the method list for an additional AAA option

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 770
Which purpose of the AAA accounting feature is true when you use TACACS+ authentication?

A. It prompts users to change their passwords when they expire
B. It saves a timestamped record of user activity
C. It controls the activities that the user is permitted to perform
D. It verifies the user identity

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 771
Which command configure a default authentication list that uses a local database and a case-insensitive username?

A. aaa authentication exec CONSOLE group local-case if authenticated
B. aaa authentication login CONSOLE group local
C. aaa authentication login default group local
D. aaa authentication exec default group local-case

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 772
Which LAN feature enables a default gateway to inform its end devices when a better path to a destination is available?

A. HSRP
B. ICMP unreachable messages
C. ICMP redirects
D. Proxy ARP

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 773
Which routing protocol searches for a better route through other autonomous systems to achieve convergence?

A. Link-state
B. Hybrid
C. Path vector
D. Distance vector

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 774
For RIPv2, how long a static route remains if the point to point interface is down?

A. 30s
B. 60s
C. 180s
D. 240s

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 775
How big is the smallest packet that will always be fragmented on a standard Ethernet network with default configuration?

A. 1500 bytes
B. 1800 bytes
C. 2048 bytes
D. 2100 bytes

Correct Answer: B

Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 776
Which task must you perform to implement EIGRP for IPv6 on a device?

A. Use the ipv6 cef command to enable Cisco Express Forwarding on the device.
B. Configure a loopback interface on the device.
C. Manually configure the router ID
D. Statically configure a neighbor statement

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 777
Which criterion does the BGP maximum paths feature use for load balancing?

A. MED
B. local preference
C. weight
D. router ID

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 778
What happens when unicast flood protection is triggered on a VLAN?

A. The VLAN is shut down
B. Traffic on the VLAN is load-balanced across multiple links
C. The VLAN is removed from the VLAN database
D. Traffic on the VLAN is passed to another VLAN with lower load

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 779
Which option is the best for protecting CPU utilization on a device?

A. fragmentation
B. COPP
C. ICMP redirects
D. ICMP unreachable messages

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 780
Which two statements about EVN are true? (Choose two.)

A. It supports IPv6 traffic.
B. It can support up to 16 VNs.
C. It uses redistribution to share routes between VNs.
D. It supports SSM only.
E. A configuration can be based on an existing VRF configuration

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 781
What are two important differences between OSPFv2 and OSPFv3? (Choose two.)

A. Only OSPFv3 provides support for IPv6.

B. Only OSPFv3 automatically chooses a router ID for the local device.
C. Only OSPFv3 automatically enable interfaces when you create them in device configuration mode.
D. Only OSPFv3 supports multiple OSPF instances on a single link.
E. Only OSPFv3 automatically detects OSPF neighbors on an NBMA interface.

Correct Answer: AD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 782
Which adverse event can occur as a consequence of asymmetric routing on the network?

A. vulnerability to a man-in the - middle atack
B. inadvertent HSRP active router preemption
C. errdisabled port
D. unicast flooding

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

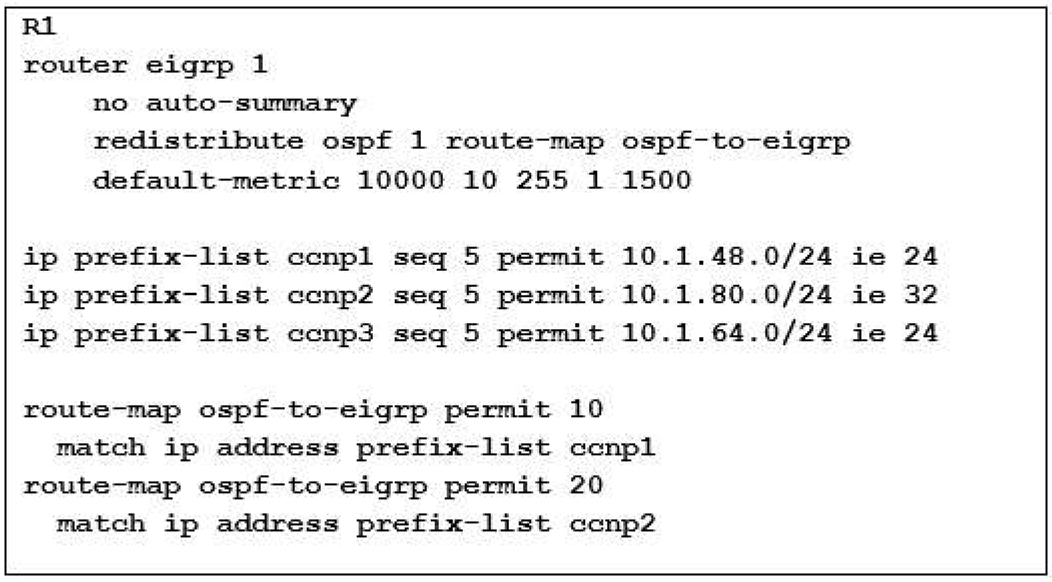
QUESTION 783
Which feature can automatically assign IP addresses in a PPPoE environment?

A. DHCP
B. BOOTP
C. PPP
D. APIPA

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 784
How does R1 handle the route to network 10.1.80.0.0/24?



```
R1
router eigrp 1
    no auto-summary
    redistribute ospf 1 route-map ospf-to-eigrp
    default-metric 10000 10 255 1 1500

ip prefix-list ccnp1 seq 5 permit 10.1.48.0/24 ie 24
ip prefix-list ccnp2 seq 5 permit 10.1.80.0/24 ie 32
ip prefix-list ccnp3 seq 5 permit 10.1.64.0/24 ie 24

route-map ospf-to-eigrp permit 10
  match ip address prefix-list ccnp1
route-map ospf-to-eigrp permit 20
  match ip address prefix-list ccnp2
```

A. R1 redistributes network 10.1.80.0/24 into EIGRP without changing the mask
B. R1 changes the mask to /32 and then redistributes network 10.1.80.0/24 into EIGRP as a classful network
C. R1 changes the mask to /32 and then redistributes network 10.1.80.0/24 into EIGRP as a classless network
D. R1 fails to redistribute network 10.1.80.0/24 into EIGRP

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 785
Which STP feature can reduce TCNs on ports that are connected to end devices?

A. BPDU guard
B. Root guard
C. PortFast
D. BackboneFast

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 786
Which command must you configure globally to support RIPng?

A. ip routing
B. ip cef
C. ipv6 enable
D. ipv6 unicast-routing

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 787
Which protocol does VRF-Lite support?

A. IS-IS
B. ODR
C. EIGRP
D. IGRP

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 788
Which two statements about NAT in a DMVPN environment are true? (Choose two.)

A. A hub router can be behind a dynamic NAT on a device.
B. Spoke routers can reside only on the public side of a NAT device.
C. Two spokes can establish session among themselves using PAT behind different NAT devices.
D. A spoke router can be represented by a static NAT on a device.
E. A hub router can user static NAT for its public UP address.

Correct Answer: DE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 789
Which adverse circumstance can the TTL feature prevent?

A. routing loops
B. DoS attacks
C. link saturation
D. CAM table overload

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

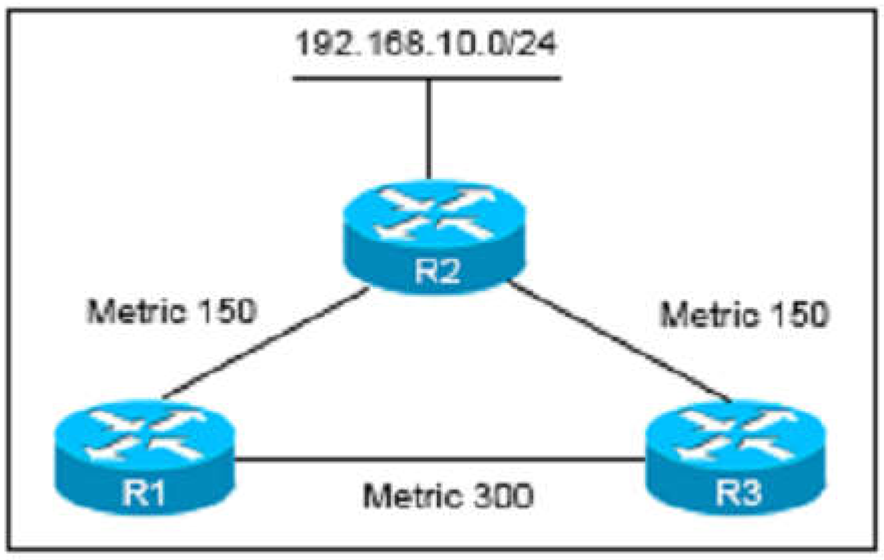
QUESTION 790
Which two EIGRP metrics have nonzero K values by default? (Choose two.)

A. reliability
B. delay
C. cost
D. load
E. bandwidth

Correct Answer: BE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 791
Refer to the exhibit. You want router r1 to perform unequal-cost routing to the 172.168.10.0/24 network.



What is the smallest EIGRP variance value that you can configure on R1 to achieve this result?

A. 1
B. 2
C. 3
D. 4

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 792
Which IP SLA operation can be used to simulate voice traffic on a network?

A. TCP connect
B. UDP-jitter
C. ICMP-echo
D. ICMP-jitter

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 793
Device R1 has 1 Gigabit and 10 Gigabit Ethernet interfaces. Which command do you enter so that takes full advantage of OSPF costs?

A. R1(config router)#auto-cost reference-bandwidth 10000
B. R1(config route-map)#set metric 10000000000
C. R1(config if)#ip ospf cost 10000
D. R1(config router)#auto*cost reference-bandwidth 10000000000
E. R1(config if)# ip ospf cost 100000000
F. R1(config route-map)#set metric 10000

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 794
In which network environment is AAA with RADIUS most appropriate?

A. when Apple Talk Remote Access is in user
B. when NetBIOS Frame Control Protocol is in use
C. when users require access to only one device at a time
D. when you need to separate all AAA services

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 795
Which SNMP model and level can provide DES encryption?

A. SNMPV2 noAuthNoPriv

B. SNMPV3 authNoPriv
C. SNMPV3 authPriv
D. SNMPV3 noAuthNoPriv

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 796
Which value determines the amount of traffic that a network path can hold in transit?

A. route cache setting
B. maximum windows size
C. bandwidth delay product
D. MSS

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 797
Which protocol can you use to remotely install an IOS on a Cisco switch?

A. SFTP
B. NetFlow
C. FTP
D. SNMP

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 798
A user is attempting to authentication on the device connected to a TACACS+ server but the server require more information from the user to complete authentication.

Which response does the TACACS+ daemon return?

A. ACCEPT
B. ERROR
C. REJECT
D. CONTINUE

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 799
Which security feature can protect DMVPN tunnels?

A. IPsec
B. TACACS+
C. RTBH
D. RADIUS

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

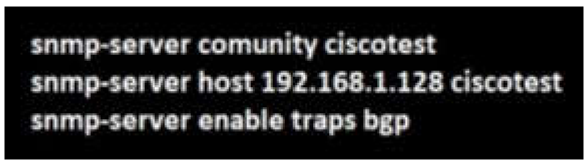
QUESTION 800
What happens when two EIGRP peers have mismatched K values?

A. The two devices are unable to correctly perform equal-cost routing
B. The two devices fail to perform EIGRP graceful shutdown when one device goes down
C. The two devices fail to from an adjacency
D. The two devices are unable to correctly perform unequal-cast load balancing

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 801
Refer to exhibit. Which effect of this configuration is true?



```
snmp-server comunity ciscotest
snmp-server host 192.168.1.128 ciscotest
snmp-server enable traps bgp
```

A. The device sends SNMP traps related to BGP operations to host 192.168.1.128
B. It configures an ACL to protect SNMP manager from receiving BGP traps.
C. It configures the device to use string ciscotest for read and write access to any SNMP manager on the network
D. It configures the device to communicate with other devices in the ciscotest community using SNMPv3

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 802
When an EIGRP router discovers a new neighbor, which packet type does the router send to help the neighbor build its topology table?

A. Replies
B. Requests
C. Updates
D. Queries

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 803
Which Technology supports overlapping IP address on a single interface?

A. policy-based routing
B. VRF-Lite
C. On-Demand Routing
D. QoS

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 804
Which two statements about ICMP unreachable messages are true? (Choose two.)

A. They are sent when a route to the destination is missing from the routing table
B. They can be enable and disable on a device only on a global level
C. They are sent when a destination address responds to an ARP request
D. They include the entire packet so that the source can identify the process that generated the message
E. They include a portion of the original data so that the source can identify the process that generated the message

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 805
Which password takes precedence if you configure multiple passwords for Telnet connections to a Cisco IOS device?

A. Console line password
B. Enable secret password
C. Enable password
D. Aux line password

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 806

Which two statements about GRE tunnel keys are true? (Choose two.)

A. The key ID must be the same on each device.
B. They prevent the injection of unwanted frames.
C. They prevent the injection of unwanted packets.
D. They must be stored to a keychain.
E. They provide the highe level of security that is available.

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 807
A router receives a routing advertisement for 10.1.1.0/24 from an EIGRP peer and from an OSPF peer. Which route does the router install in the routing table, and for which reason?

A. The OSPF route, because the administrative distance is lower.
B. The EIGRP route, because the metric is lower.
C. The OSPF route, because the metric is lower.
D. The EIGRP route, because the administrative distance is lower.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 808
Which criterion does BGP evaluate first when determining the best path?

A. MED value
B. neighbor address
C. local preference value
D. weight

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 809
When does a Cisco router send an ICMP redirect?

A. when the packet's source and destination VRFs are different
B. when the packet is source-routed
C. when the packet's destination has load-balanced entries in the route table
D. when the packet's ingress and egress interface are the same

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

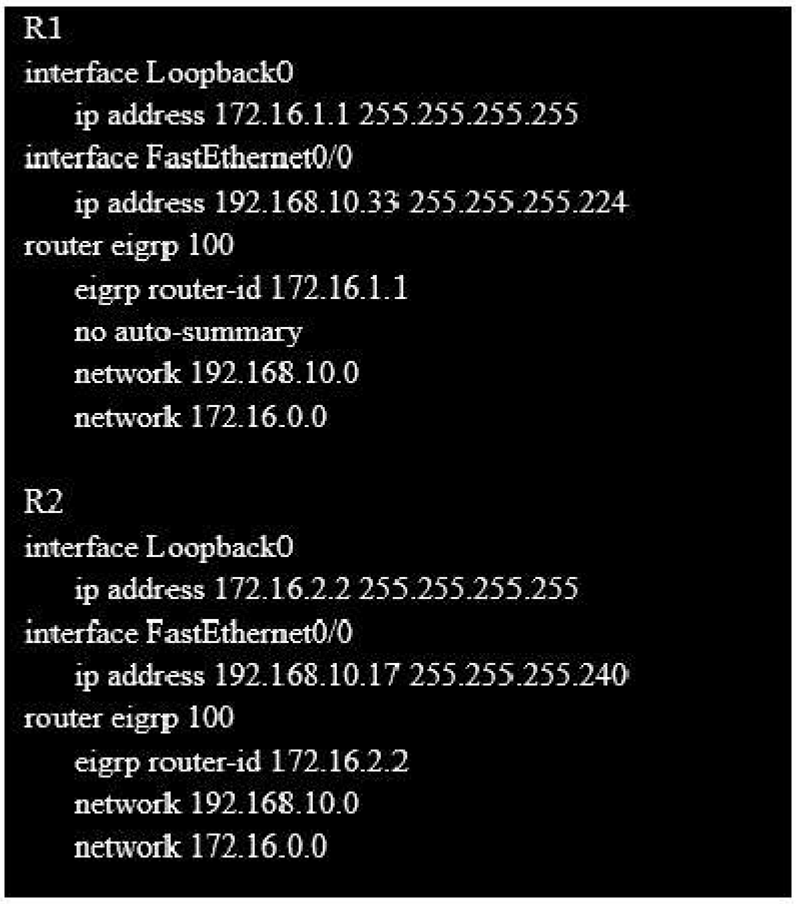
QUESTION 810
You are configuring a static route. Which action must you take to avoid the possibility of recursive row?

A. Use the ip route command to specify the next-hop IP address only
B. Specify the next hop a directly connected interface
C. Use the ip route command to specify both the next-hop IP address and the connected interface
D. User the ip route command to specify the connected interface only

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 811
Refer to the exhibit. R1 and R2 are unable to establish an EIGRP adjacency.



```
R1
interface Loopback0
     ip address 172.16.1.1 255.255.255.255
interface FastEthernet0/0
     ip address 192.168.10.33 255.255.255.224
router eigrp 100
     eigrp router-id 172.16.1.1
     no auto-summary
     network 192.168.10.0
     network 172.16.0.0

R2
interface Loopback0
     ip address 172.16.2.2 255.255.255.255
interface FastEthernet0/0
     ip address 192.168.10.17 255.255.255.240
router eigrp 100
     eigrp router-id 172.16.2.2
     network 192.168.10.0
     network 172.16.0.0
```

Which action corrects the problem?

A. Change the eigrp route-id on one of the routers so that values on the two routers are different.
B. Add the no auto-summary command to the R2 configuration so that it matches the R1 configuration
C. Change the autonomous system number on one of the routers so that each router has different values
D. Change the IP address and subnet mask on R2 so that is on the same subnet as R1.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 812
Which routing protocol routers traffic through the best path and second best path at the same time?

A. EIGRP
B. BGP
C. OSPF
D. RIP

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 813
A router with default RIPv2 settings loses connectivity to it's next-hop neighbor.
How long downs the router wait before removing the route to the next hop from its route table?

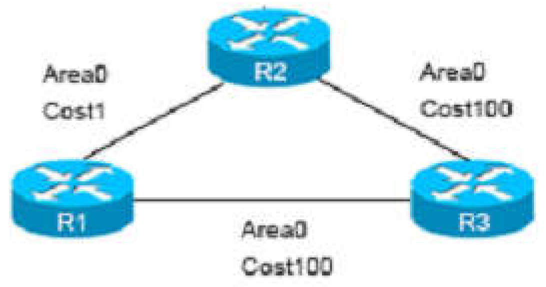
A. 30 seconds
B. 60 seconds
C. 180 seconds
D. 240 seconds

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 814
Refer to the exhibit. You notice that traffic from R1 to the 192.168.10.0/24 network prefers the path through R3 instead of the least-cost path through R2.

What is the most likely reason for this router selection?



A. OSPF prefers external routers over interarea router.
B. OSPF prefers interarea routers over intra-area routers.
C. OSPF prefers external routers over intra-area routers.
D. OSPF prefers intra-area routers over interarea routers.

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 815
You want to configure a device to select an OSPF-learned route as the preferred path over an EBGP-learned route.

Which action must you take?

A. Increase the OSPF cost
B. Decrease the OSPF cost
C. Increase the OSPF administrative distance
D. Decrease the OSPF administrative distance

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 816
What is the maximum number of hops on a router that RIPng advertises as reachable?

A. 15
B. 30
C. 99
D. 255

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 817
OSPF chooses routes in which order, regardless of route's administrative distance and metric?

A. Intra-Area (O) - Inter-Area (O IA) - External Type 1 (E1) - External Type 2 (E2) - NSSA Type 1 (N1) - NSSA Type 2 (N2)
B. Intra-Area (O) - Inter-Area (O IA) - NSSA Type 1 (N1) - NSSA Type 2 (N2) - External Type 1 (E1) - External Type 2 (E2)
C. Intra-Area (O) - Inter-Area (O IA) - NSSA Type 1 (N1) - External Type 1 (E1) - NSSA Type 2 (N2) - External Type 2 (E2)
D. Intra-Area (O) - NSSA Type 1 (N1) - External Type 1 (E1) - Inter-Area (O IA) - NSSA Type 2 (N2) - External Type 2 (E2)
E. Intra-Area (O) - Inter-Area (O IA) - NSSA Type 1 (N1) - External Type 1 (E1) - NSSA Type 2 (N2) - External Type 2 (E2)
F. NSSA Type 1 (N1) - NSSA Type 2 (N2) - Intra-Area (O) - Inter-Area (O IA) - External Type 1 (E1) - External Type 2 (E2)

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:
Explanation:
Regardless of a route’s metric or administrative distance, OSPF will choose routes in the following order:

Intra-Area (O)
Inter-Area (O IA)
External Type 1 (E1)
External Type 2 (E2)
NSSA Type 1 (N1)
NSSA Type 2 (N2)

QUESTION 818
Which calculation is used to determine the default EIGRP metric?

A. Bandwidth+Delay
B. Bandwidth*Delay
C. Bandwidth-Delay

D. Bandwidth/Delay

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 819
Which two packet types can an EIGRP router send when a route goes into the Active state? (Choose two.)

A. query
B. update
C. request
D. hello
E. reply

Correct Answer: AE
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 820
Which condition must be met before two EVN devices can connect?

A. One VLAN interface must be configured between devices.
B. An EtherChannel configured with at least 2 interfaces connected between the devices.
C. A trunk interface must be configured between devices
D. A fiber connection must be established between the devices.

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 821
Which algorithm is used by EIGRP to determine the best path through a network?

A. DUAL
B. Dijkstra
C. SPF
D. A* Search

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

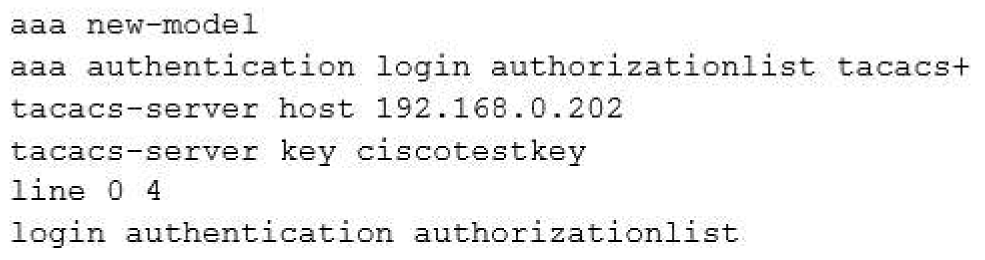
QUESTION 822
What happens when a router receives a packet with a TTL of 0?

A. The router attempts to forward the packet along an alternate path in the route table
B. The router sends an ICMP Time Exceeded Message to the host that sent the packet
C. The router sends an ICMP Destination Unreachable Message to the host that sent the packet
D. The router flags the packet and forwards it to the next hop

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 823
Refer to the exhibit. Which effect of this configuration is true?



```
aaa new-model
aaa authentication login authorizationlist tacacs+
tacacs-server host 192.168.0.202
tacacs-server key ciscotestkey
line 0 4
login authentication authorizationlist
```

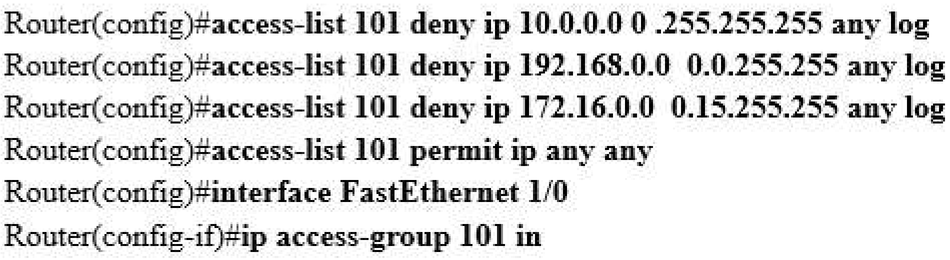
A. The device will authenticate all users connecting to vty lines 0 4 against TACACS+
B. When users attempt to connect to vty lines 0 4, the device will authenticate them against TACACS+ if local authentication fails
C. The device will allow users at 192.168.0.202 to connect to vty lines 0 4 using the password **ciscotestkey**

D. The device will allow only users at 192.168.0.202 to connect to vty line 0 4

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 824
What does the following access list, which is applied on the external interface FastEthernet 1/0 of the perimeter router, accomplish?



```
Router(config)#access-list 101 deny ip 10.0.0.0 0 .255.255.255 any log
Router(config)#access-list 101 deny ip 192.168.0.0  0.0.255.255 any log
Router(config)#access-list 101 deny ip 172.16.0.0  0.15.255.255 any log
Router(config)#access-list 101 permit ip any any
Router(config)#interface FastEthernet 1/0
Router(config-if)#ip access-group 101 in
```

A. it prevents private internal addresses to be accessed directly from outside
B. it prevents the internal network from being used in spoofed denial of service attacks and logs any exit to the Internet
C. It filters incoming traffic from private address ranges 10.0.0.0-10.0.0.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 and logs any intrusion attempts
D. It filters incoming traffic from private addresses in order to prevent spoofing and logs any intrusion attempts

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

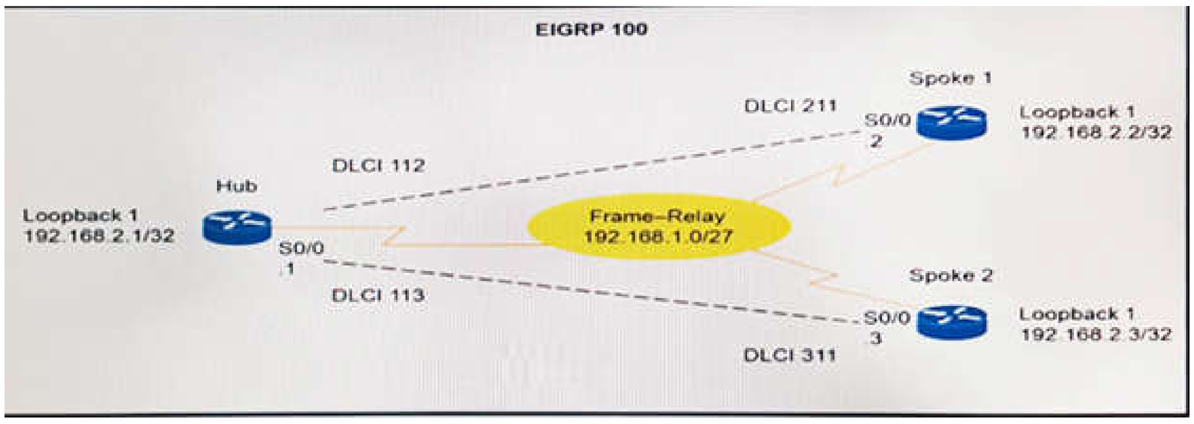
QUESTION 825
Which OSPF network type uses a DR?

A. point-to-point nonbroadcast
B. point-to-multicast
C. nonbroadcast multiaccess
D. point-to-point

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 826



Refer to the exhibit. A network engineer is implementing a Frame Relay design using EIGRP as the routing protocol EIGRP 100 is up and the hub is receiving advertisements for both loopback interfaces from Spoke 1 and Spoke2. Spoke 1 and Spoke 2 can see Loopback 1 advertisements from the hub, but neither spoke sees loopback advertisements from the other spoke. Why are the routing updates not prorogating properly?

A. The network mask that is used on the loopback interfaces of the spoke routers is invalid
B. Split horizon on the hub interface is preventing advertisements
C. There is a physical Layer 1 issue between one of the spokes and the hub
D. Split horizon on one of the spoke interfaces is preventing advertisements

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 827
Which two tasks must you perform when you install SSH on a Cisco IOS device? (Choose two.)

A. Enable TACACS+
B. Delete the VTY lines
C. Generate an SSH key

D. Configure a device hostname
E. Disable Telnet

Correct Answer: CD
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 828
Which protocol allows hosts to rearrange out-of-order packets at Layer 3?

A. Use UDP, which sequences packets and can place them in the correct order
B. Use TCP, which works with the STP root bridge to transmit packets in the correct order
C. Use TCP, which sequences packets and can place them in the correct order
D. Use UDP, which can retransmit missing packets

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 829
To enable policy-based routing, which function specifies the match criteria and resulting action of all the match clauses that are met?

A. class map
B. route map
C. service policy
D. ACL

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfpbr.pdf

QUESTION 830
A router in an EVN environment is choosing a route. Which value is given the highest selection priority?

A. VNET tag of the route
B. lexical value of the source VRF name
C. replication status of the route
D. IGP administrative distance of the route
E. default administrative distance of the route

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/layer-3-vpns-l3vpn/whitepaper_c11-638769.html

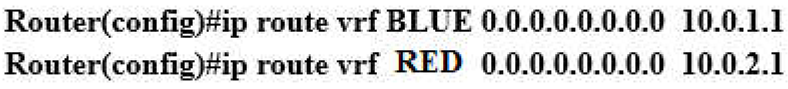
QUESTION 831
What is the range for private AS numbers?

A. 64512 to 65535
B. 1 to 64511
C. 1024 to 65535
D. 1 to 1024

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 832
Refer to the exhibit.



```
Router(config)#ip route vrf BLUE 0.0.0.0.0.0.0.0  10.0.1.1
Router(config)#ip route vrf  RED  0.0.0.0.0.0.0.0  10.0.2.1
```

After configuring the rotes, the network engineer executes the show ip route command. What is the expected result?

A. Gateway of last resort is 10.0.2.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 2 subnetsC 10.0.2.0 is directly connected, FastEthernet0/0C 10.0.1.0 is directly connected, FastEthernet0/1S” 0.0.0.0/0[1/0] via 10.0.2.1 [1/0] via 10.0.1.1Router #
B. Gateway of last resort is 10.0.1.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 1 subnet C 10.0.1.0 is directly connected, FastEthernet0/1 S” 0.0.0.0/0 [1/0] via 10.0.1.1 Router #
C. Gateway of last resort is not set Router #
D. Gateway of last resort is 10.0.2.1 to network 0.0.0.0 10.0.0.0/24 is subnetted, 1 subnet C 10.0.2.0 is directly connected, FastEthernet0/0 S”0.0.0.0/0 [1/0]

via 10.0.2.1 Router #

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

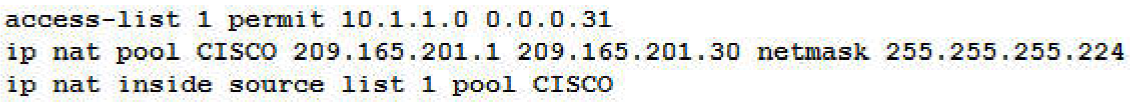
QUESTION 833
Which protocol proposes IETF as the viable successor to NAT-PT?

A. NAT64
B. 64NAT
C. NAT-PT64
D. 64NAT-PT

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 834
Refer to the exhibit. Which two effects of this configuration are true? (Choose two.)



```
access-list 1 permit 10.1.1.0 0.0.0.31
ip nat pool CISCO 209.165.201.1 209.165.201.30 netmask 255.255.255.224
ip nat inside source list 1 pool CISCO
```

A. The 10.1.1.0/27 subnet is assigned as the inside local addresses
B. The 209.165.201.0/27 subnet is assigned as the outside local address range
C. Inside source addresses are translated to the 209.165.201.0/27 subnet
D. It establishes a one-to-one NAT translation
E. The 10.1.1.0/27 subnet is assigned as the inside global address range

Correct Answer: AC
Section: Mix Questions
Explanation

Explanation/Reference:

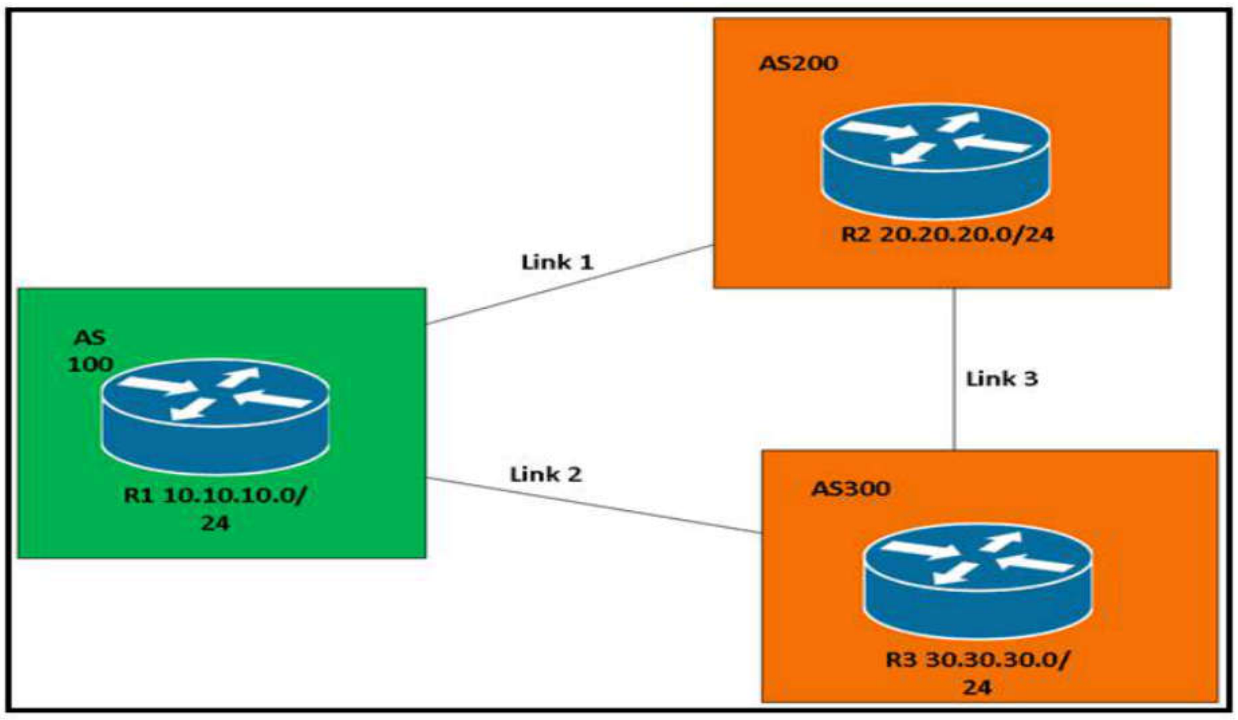
QUESTION 835
Which feature eliminates the need for Cisco Express Forwarding to maintain a route cache?

A. MAC address table
B. RIB
C. adjacency table
D. FIB

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/XE3-8-0E/15-24E/configuration/guide/xe-380-configuration/cef.pdf

QUESTION 836
Refer to the exhibit. Which BGP attribute can be used to influence traffic from AS200 and AS300 to enter AS100 via link 1?



A. AS-path

B. weight
C. local preference
D. MED

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 837
Which IP SLA deployment cycle reduces the deployment time for network applications?

A. Collect, Measure, Optimize
B. Scan, Adjust, Modify
C. Baseline, Understand, Quantify, Optimize
D. Monitor, Collect, Tune

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/en/US/technologies/tk648/tk362/tk920/technologies_white_paper0900aecd8017531d.pdf

QUESTION 838
Which two OSPF area types filter type 4 and type 5 LSAs? (Choose two.)

A. Level 2
B. not-so-stubby
C. totally stubby
D. level 1
E. stub
F. Level1 – Level2

Correct Answer: CE
Section: Mix Questions
Explanation

Explanation/Reference:

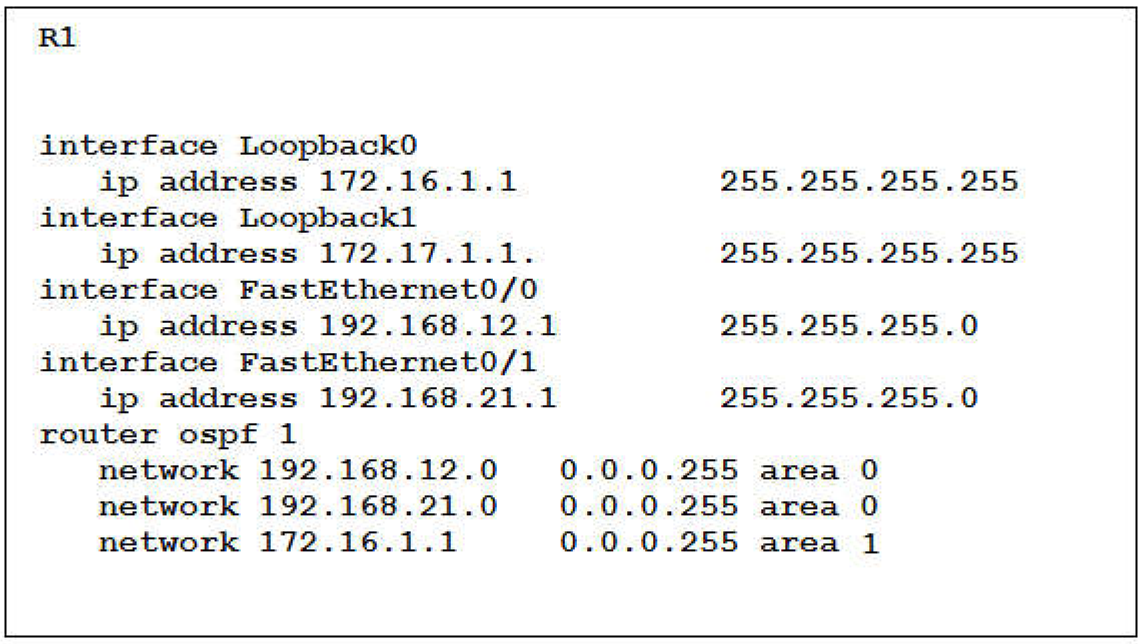
QUESTION 839
Which value identifies traffic, intended for different paths in an EVN environment?

A. VLAN ID
B. route target
C. route tag
D. VNET tag

Correct Answer: D
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 840
Refer to the exhibit. Which IP address does OSPF choose as the R1 router ID?



```
R1


interface Loopback0
   ip address 172.16.1.1          255.255.255.255
interface Loopback1
   ip address 172.17.1.1.         255.255.255.255
interface FastEthernet0/0
   ip address 192.168.12.1        255.255.255.0
interface FastEthernet0/1
   ip address 192.168.21.1        255.255.255.0
router ospf 1
   network 192.168.12.0    0.0.0.255 area 0
   network 192.168.21.0    0.0.0.255 area 0
   network 172.16.1.1      0.0.0.255 area 1
```

A. 172.16.1.1
B. 172.17.1.1
C. 192.168.12.1

D. 192.168.21.1

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

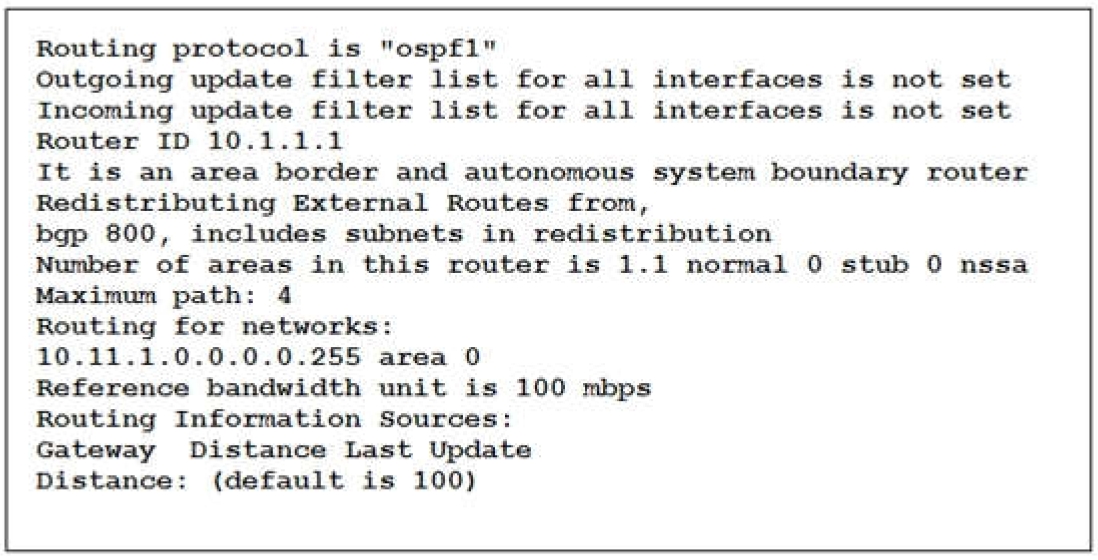
QUESTION 841
Which type of Cisco Express Forwarding adjacency is created when the next hop is directly connected, but its MAC header rewrite information is missing?

A. discard
B. glean
C. punt
D. null

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipswitch_cef/configuration/15-mt/isw-cef-15-mt-book/isw-cef-overview.html

QUESTION 842
Refer to the exhibit. Based on the output from the show ip protocols vrf RED command, what is happening with the routing processes?



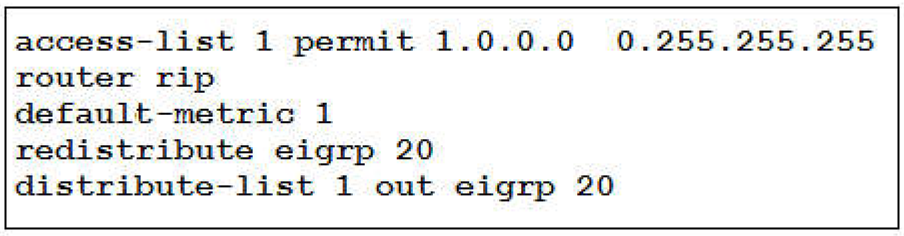
```
Routing protocol is "ospf1"
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Router ID 10.1.1.1
It is an area border and autonomous system boundary router
Redistributing External Routes from,
bgp 800, includes subnets in redistribution
Number of areas in this router is 1.1 normal 0 stub 0 nssa
Maximum path: 4
Routing for networks:
10.11.1.0.0.0.0.255 area 0
Reference bandwidth unit is 100 mbps
Routing Information Sources:
Gateway  Distance Last Update
Distance: (default is 100)
```

A. BGP 800 is redistributing into OSPF 1
B. Static routers are redistributing into BGP 800
C. OSPF 1 is redistributing into BGP 800
D. Static routes are redistributed into OSPF 1

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 843
Refer to the exhibit. Which routes will be injected into the routing protocol?



```
access-list 1 permit 1.0.0.0  0.255.255.255
router rip
default-metric 1
redistribute eigrp 20
distribute-list 1 out eigrp 20
```

A. the RIP routes into EIGRP 20 that match access-list 1
B. the EIGRP 20 routes into RIP that match access-list 1
C. all RIP routes into EIGRP 20
D. any routing update with a metric of 1

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 844
Which command is the correct way to summarize routes that were injected into OSPF area 100 from RIP?

A. **redistribute rip metric 20 subnets**

B. **summary-address 172.32.64.0 255.255.224.0**
C. **area 100 range 172.32.64.0 255.255.224.0**
D. **ip summary-address 172.32.64.0 255.255.224.0**

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 845
Which condition must be met before you can configure SSH on a device running Cisco IOS?

A. The device must have a modern connection
B. The IOS must be a crypto image
C. The device must have an auxiliary port
D. Telnet must be disabled on the device

Correct Answer: B
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 846
Which command instructs a PPPoE client to obtain its IP address from the PPPOE server?

A. ip address DHCP
B. ip address dynamic
C. ip address negotiated
D. ip address auto negotiated

Correct Answer: C
Section: Mix Questions
Explanation

Explanation/Reference:

QUESTION 847
The OSPF database of a router shows LSA types 1, 2, 7, and 3 default router only. Which type of area is this router connected to?

A. NSSA totally stub
B. stub area
C. totally stubby area
D. NSSA

Correct Answer: A
Section: Mix Questions
Explanation

Explanation/Reference: