BraindumpStudy

BraindumpStudy
Leader of IT Certifications Study

http://www.braindumpstudy.com

BraindumpStudy Exam Dumps, High Pass Rate!

Exam : **300-410**

Title : Implementing Cisco Enterprise Advanced Routing and Services

Vendor : Cisco

Version : DEMO

NO.1 Which statement about IPv6 RA Guard is true?
A. It does not offer protection in environments where IPv6 traffic is tunneled
B. It cannot be configured on a switch port interface in the ingress direction.
C. Packets that are dropped by IPv6 RA Guard cannot be spanned.
D. It is not supported in hardware when TCAM is programmed.
Answer: A
Explanation:
Restrictions for IPv6 RA Guard
+ The IPv6 RA Guard feature does not offer protection in environments where IPv6 traffic is tunneled.
+ This feature is supported only in hardware when the ternary content addressable memory (TCAM) is programmed.
+ This feature can be configured on a switch port interface in the ingress direction.
+ This feature supports host mode and router mode.
+ This feature is supported only in the ingress direction; it is not supported in the egress direction.
+ This feature is not supported on EtherChannel and EtherChannel port members.
+ This feature is not supported on trunk ports with merge mode.
+ This feature is supported on auxiliary VLANs and private VLANs (PVLANs). In the case of PVLANs, primary VLAN features are inherited and merged with port features.
+ Packets dropped by the IPv6 RA Guard feature can be spanned.
+ If the platform ipv6 acl icmp optimize neighbor-discovery command is configured, the IPv6 RA Guard feature cannot be configured and an error message will be displayed. This command adds default global Internet Control Message Protocol (ICMP) entries that will override the RA guard ICMP entries.
Reference: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/xe-3s/ip6f-
xe-3s-book/ip6-ra-guard.html

NO.2 A new site has been added to an OPSF network using area 2. Area 2 is connected only to area 1 of this OSPF network. Area 1 is used to connect area 1 to the backbone area 0. Should you expect full connectivity to the networks located in area 2 from area 0 in this scenario?
A. Yes, by default there will be full connectivity.
B. No, you will need to redistribute the area 2 routes into area 0.
C. No, a virtual link is needed to logically connect area 2 info area 0.
D. Yes, but area 2 will need to be configured as a stub area.
Answer: C

NO.3 Which two features are required for MPLS forwarding on which types of routers? (Choose two.)
A. MPLS on PE and core routers
B. LDP on PE and core routers
C. MPLS on CE and core routers
D. LDP on PE and CE routers
E. CEF on PE and CE routers

Answer: AB

NO.4 Refer to the exhibit. SW101 could not transfer its startup configuration to a TFTP server. No ACL
is configured on the switch, and it can successfully ping the host. Which action resolves the issue?

```
SW101#cop nvram:startup-config tftp:
Address or name of remote host []? 10.1.0.1
Destination filename [sw101-confg]?
%Error opening tftp://10.1.0.1/sw101-confg (Permission denied)
SW101#

SW101#ping 10.1.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/7/15 ms
SW101#
```

A. Open UDP port 69 on the TFTP server.
B. Open UDP port 179 on the TFTP server.
C. Configure a FW in the middle to allow bidirectional communication for TFTP.
D. Start the TFTP server on the host.
Answer: D

NO.5 What is the purpose of an OSPF sham-link?
A. to allow inter-area routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network
B. to allow intra-area routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network
C. to correct OSPF backdoor routing when OSPF is used as the PE-CE connection protocol in an MPLS VPN network
D. to correct OSPF backdoor routing when OSPF is used as the PE-PE connection protocol in an MPLS VPN network
Answer: C
Explanation:
In an MPLS VPN network, OSPF is often used as the routing protocol between the Provider Edge (PE) and Customer Edge (CE) routers. A problem arises when there is an OSPF backdoor link between two CE routers in the same OSPF area. This link may be preferred over the MPLS VPN path, as OSPF inherently prefers intra-area routes over inter-area routes.
A sham-link is configured to create a logical intra-area link between the PE routers, ensuring that traffic uses the MPLS VPN backbone instead of the backdoor link. This allows the MPLS VPN backbone to maintain OSPF intra-area routing and avoids the suboptimal routing caused by OSPF's preference for intra-area routes.

NO.6 Which protocol is used in a DMVPN network to map logical IP address to physical IP addresses?

A. BGP

B. LLDP

C. EIGRP

D. NHRP

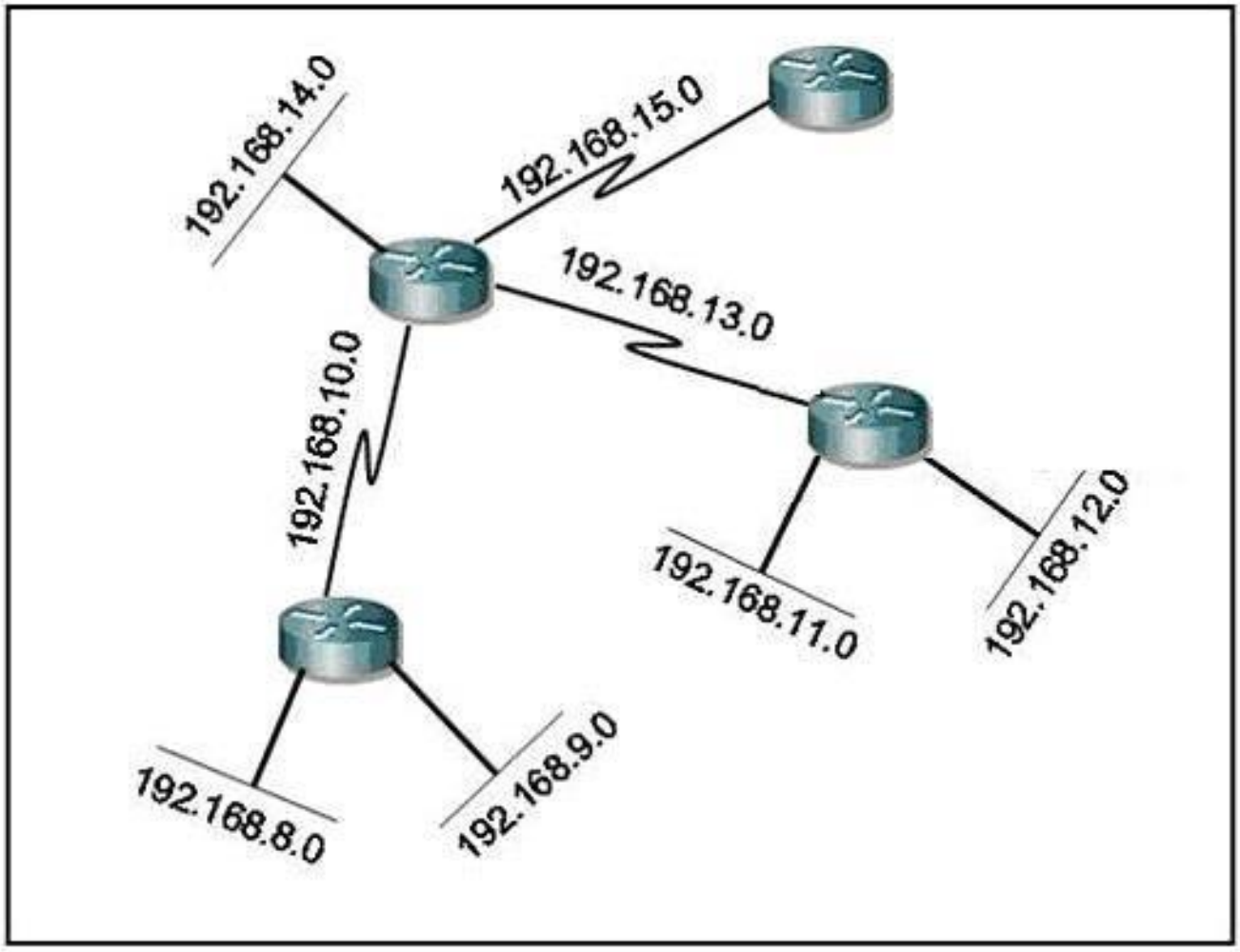
Answer: D

Explanation:

Next Hop Resolution Protocol (NHRP), defined in RFC 2332, is a Layer 2 address resolution protocol and cache, like Address Resolution Protocol (ARP). NHRP is used by a branch router connected to a non-broadcast, multi-access (NBMA) sub-network to determine the IP address of the "NBMA next hop"; in this case, the headend router or the destination IP address of another branch router.

NHRP is used to map tunnel IP addresses to "physical" or "real" IP addresses, used by endpoint routers. It resolves private addresses (those behind mGRE and optionally IPSEC) to a public address. NHRP is layer 2 resolution protocol and cache, much like Address Resolution Protocol (ARP) or Reverse ARP (Frame Relay).

NO.7 Given the network diagram, which address would successfully summarize only the networks seen?

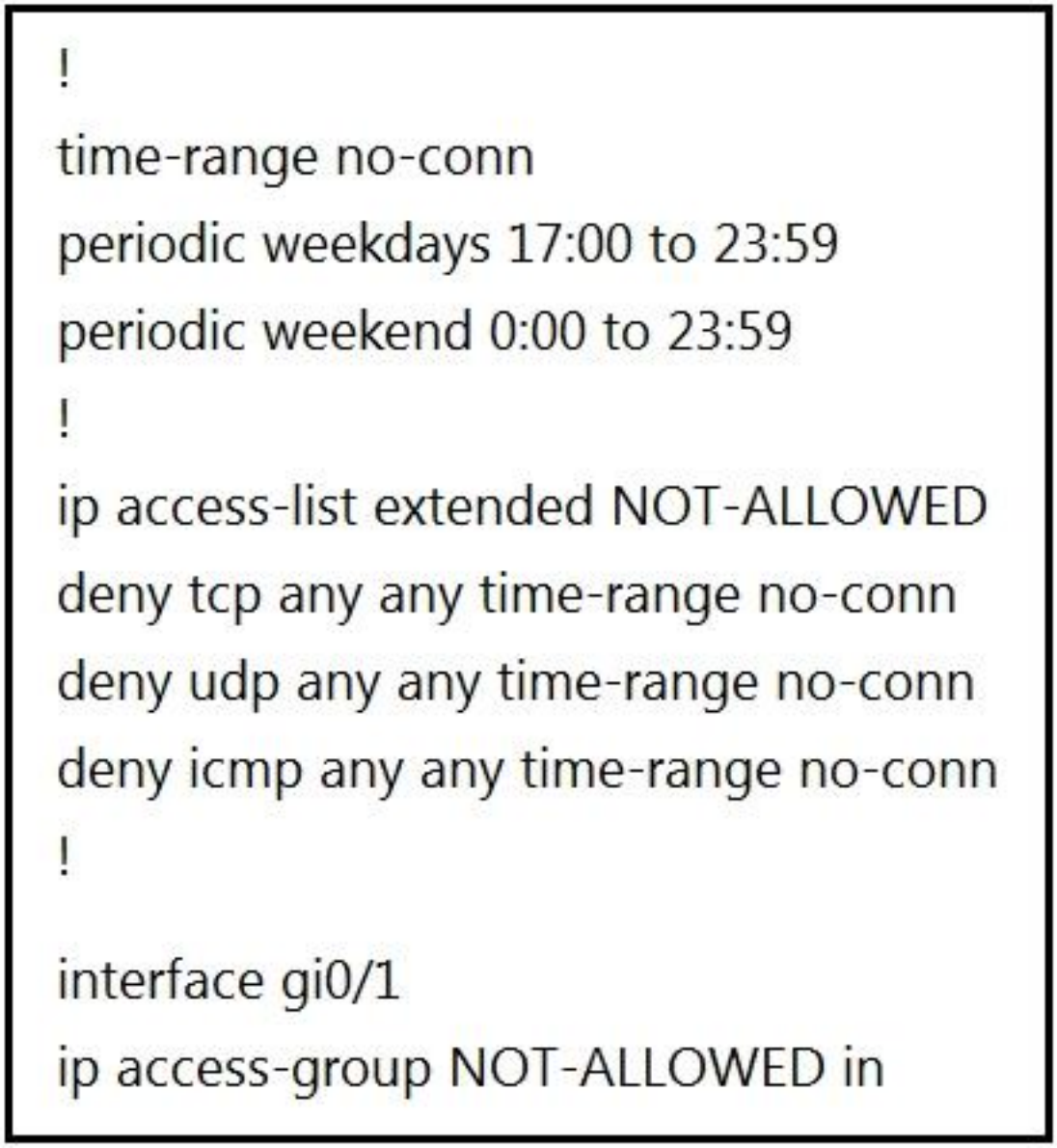


A. 192.168.0.0/24

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.
Answer: C

NO.8 Refer to the exhibit. A network administrator wants to block all traffic toward the Internet after
business hours and on weekends. When the administrator applies an access list on interface Gi0/1, all traffic is blocked and there is no access to the Internet at any time.
Which action resolves the issue?



A. Add the permit ip any any time-range no-conn statement after the deny udp any any time-range no-conn command in the access list.
B. Add the permit ip any any statement after the deny icmp any any time-range no-conn command in the access list.
C. Add the permit allowed time-range no-conn statement after the deny icmp any any time-range no

-
conn command in the access list.
D. Add the permit ip any any time-range no-conn statement after the deny icmp any any time-range no-conn command in the access list.
Answer: B

NO.9 Refer to the exhibit. An engineer has configured policy-based routing and applied the configuration to the correct interface. How is the configuration applied to the traffic that matches the access list?

```
Route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access lists): FILTER_ACL
  Set clauses:
    ip next-hop verify-availability 209.165.202.129 1 track 100 [down]
    ip next-hop verify-availability 209.165.202.131 2 track 200 [up]
  Policy routing matches: 0 packets, 0 bytes
route-map PBR, deny, sequence 20
  Match clauses:
  Set clauses:
    ip next-hop 209.165.201.30
  Policy routing matches: 275364861 packets, 12200235037 bytes
```

A. It is sent to 209.165.202.131.
B. It is sent to 209.165.202.129.
C. It is dropped.
D. It is forwarded using the routing table lookup.
Answer: A
Explanation:
The first next hop IP is down, so the second one will be used.

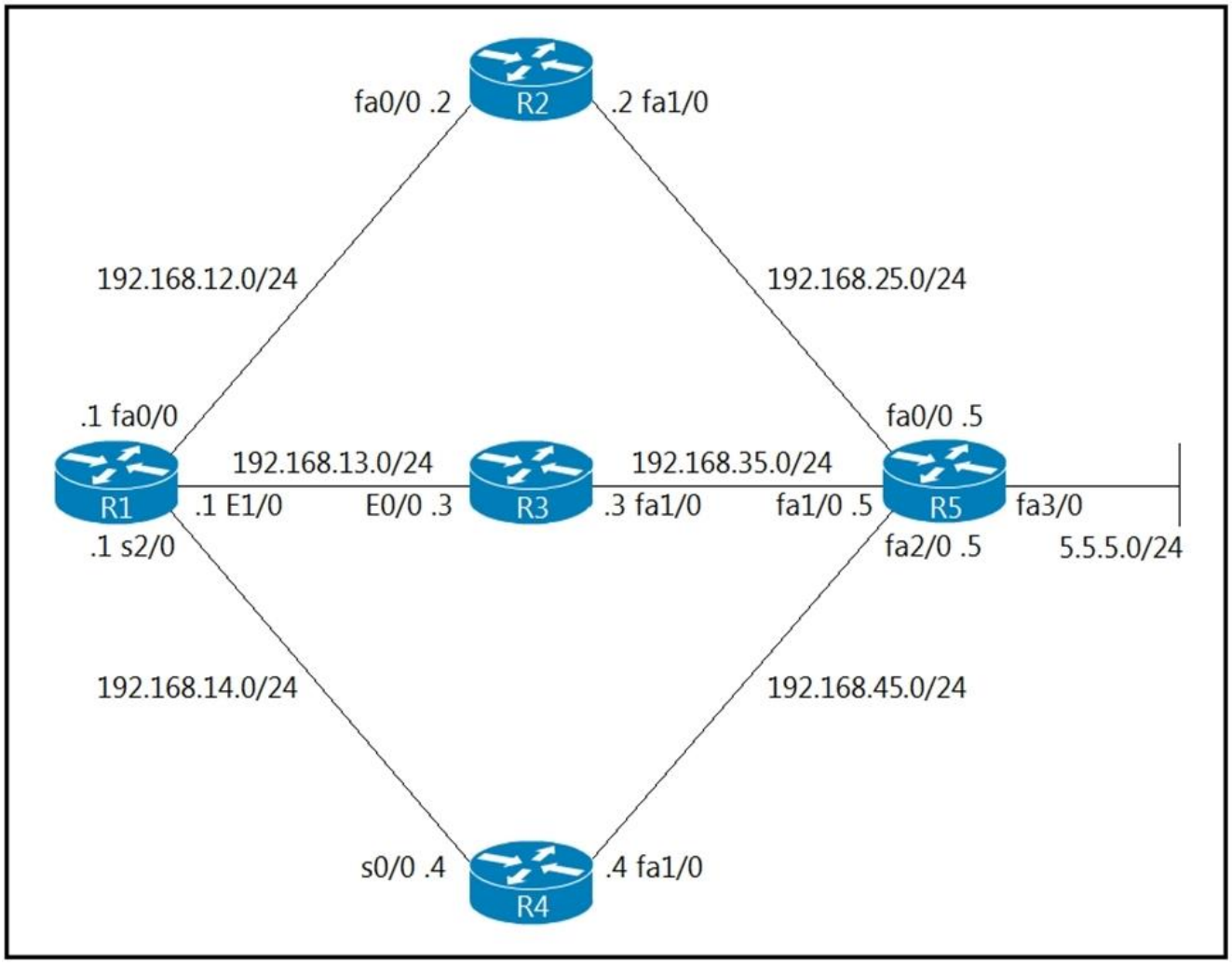
NO.10 Refer to the exhibit. Which action limits the access to R2 from 192.168.12.1?

```
R2#show policy-map control-plane
 Control Plane
  Service-policy input: CoPP
    Class-map: SSH (match-all)
      29 packets, 2215 bytes
      5 minute offered rate 0000 bps
      Match: access-group 100

    Class-map: ANY (match-all)
      46 packets, 3878 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: access-group 199
      drop

    Class-map: class-default (match-any)
      41 packets, 5687 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any

R2#show access-list 100
Extended IP access list 100
    10 deny tcp any any eq 22 (14 matches)
    20 permit tcp host 192.168.12.1 any eq 22 (29 matches)
R2#show access-list 199
Extended IP access list 199
    10 permit ip any any (51 matches)
```

A. Swap sequence 10 with sequence 20 in access-list 100.
B. Modify sequence 20 to permit tcp host 192.168.12.1 eq 22 any to access-list 100
C. Swap sequence 20 with sequence 10 in access-list 100
D. Modify sequence 10 to deny tcp any eq 22 any to access-list 100.
Answer: C

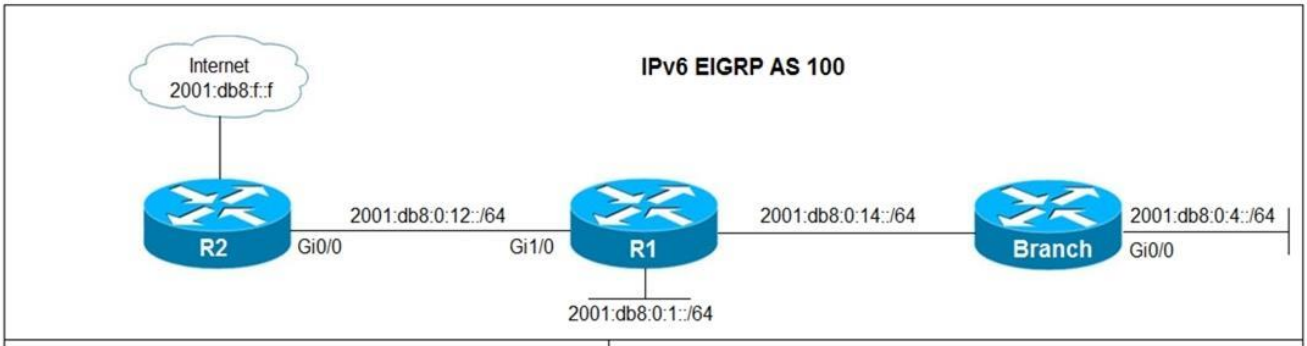
NO.11 Which attribute eliminates LFAs that belong to protected paths in situations where links in a network are connected through a common fiber?
A. Interface-dispoint
B. Shared risk link group-disjoint
C. Linecard-disjoint
D. Lowest-repair-path-metric
Answer: B
Explanation:
Shared Risk Link Group (SRLG)-disjoint-Eliminates LFAs that belong to any of the protected path SRLGs. SRLGs refer to situations where links in a network share a common fiber (or a common physical attribute). If one link fails, other links in the group may also fail. Therefore, links in a group share risks.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xe-3s/asr1000/ire-xe-3s-asr1000/ire-ipfrr.html

NO.12 Refer to the exhibits. An engineer investigates a routing issue on R1 and finds that traffic destined
to 5.5.5.0/24 does not take all of the paths.
Which action resolves the issue?



A. Increase the variance value in EIGRP.
B. Decrease the variance value in EIGRP.
C. Remove the adjacency of R3 from EIGRP.
D. Stop advertising 192.168.13.0/24 in EIGRP.
Answer: A
Explanation:
EIGRP variante enables unequal cost path balance routing and add those prefixes to the EIGRP routing table.

NO.13 Refer to the exhibit. Users in the branch network of 2001:db8:0:4::/64 report that they cannot
access the Internet. Which command is issued in IPv6 router EIGRP 100 configuration mode to solve this issue?




```
R1# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(10.1.12.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 28416
       via FE80::C828:DFF:FEF4:1C (28416/2816), FastEthernet3/0
P 2001:DB8:0:1::/64, 1 successors, FD is 2816
       via Connected, GigabitEthernet0/0
P ::/0, 1 successors, FD is 2816
       via FE80::C821:17FF:FE04:8 (2816/256), GigabitEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
       via Connected, FastEthernet3/0
P 2001:DB8:0:12::/64, 1 successors, FD is 2816
       via Connected, GigabitEthernet1/0
```

```
Branch# show ipv6 eigrp topology
EIGRP-IPv6 Topology Table for AS(100)/ID(4.4.4.4)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status
P 2001:DB8:0:4::/64, 1 successors, FD is 2816
       via Connected, GigabitEthernet0/0
P 2001:DB8:0:1::/64, 1 successors, FD is 28416
       via FE80::C820:17FF:FE04:54 (28416/2816), FastEthernet1/0
P 2001:DB8:0:14::/64, 1 successors, FD is 28160
       via Connected, FastEthernet1/0
P 2001:DB8:0:12::/64, 1 successors, FD is 28416
       via FE80::C820:17FF:FE04:54 (28416/2816), FastEthernet1/0
```

A. Issue the eigrp stub command on R1.

B. Issue the no eigrp stub command on R1.

C. Issue the eigrp stub command on R2.

D. Issue the no eigrp stub command on R2.

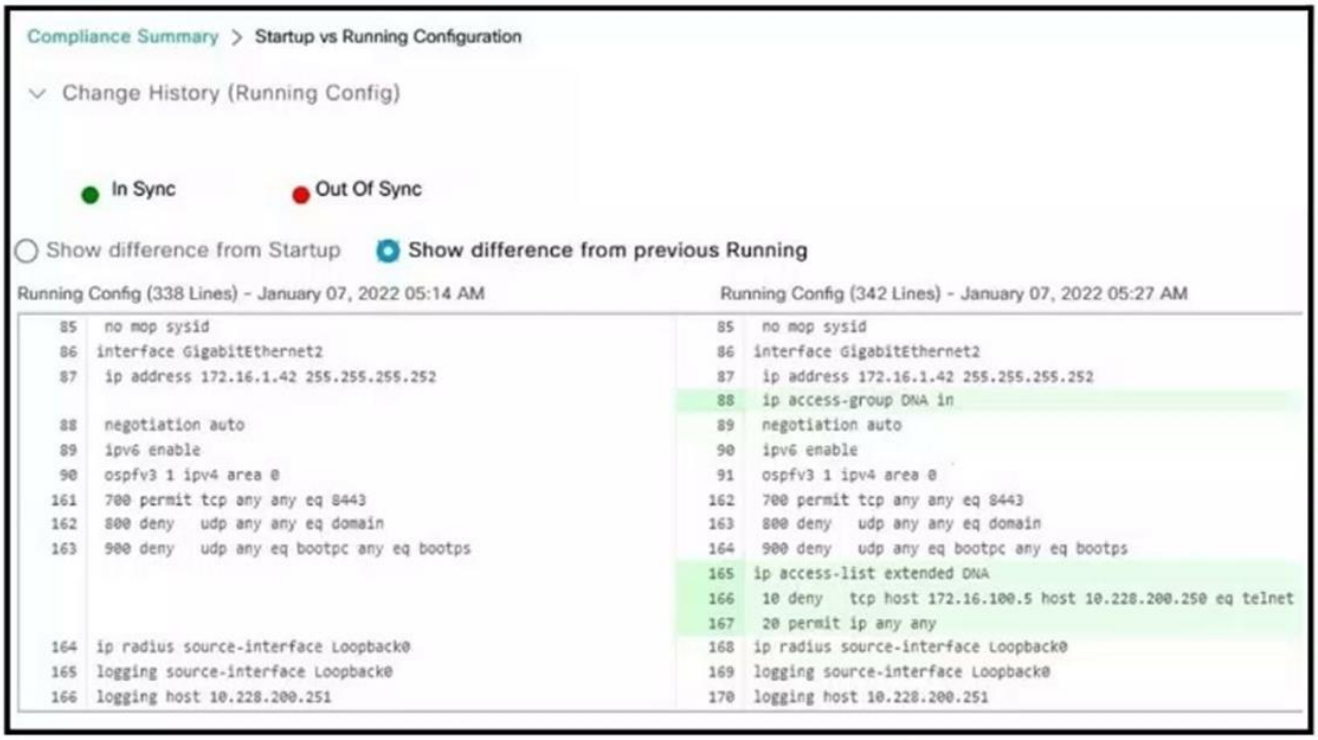
Answer: B

Explanation:

In the output of R1, we see R1 has a default route to the Internet via G1/0, which is correct but R2 does not have this route. One reasonable answer of this issue is R1 has been configured as a stub router so it only advertised connected and summary routes. In Branch router output, we also see routes that are directly connected to R1 only.

Note: In this topology, only Branch router should be configured as stub, not R1 router.

NO.14 Refer to the exhibit. After an engineer updates the configuration on the device, they noticed unexpected behavior. Which command resolves the issue by completely replacing the startup configuration?



A. configure replace nvram:startup-config

B. copy system:running.config nvram:startup-config

C. configure replace nvram:private-config

D. copy running-config startup-config

Answer: A

Explanation:

configure replace nvram:startup-config replaces the current running configuration with the saved startup configuration, removing unintended changes and restoring the device to the exact startup-config state. This is the correct command when a full replacement is required rather than merging configuration lines.

NO.15 Refer to the exhibit. Routers R1 and R2 exchange routes to each other's loopback through OSPF. Telnet traffic must be blocked from R2 Lo0 to R1 Lo2. Which configuration resolves the issue?

```
R1

Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
ipv6 traffic-filter DENY_TELNET_Lo2 in
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

A.

R1

```
Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
ipv6 access-class DENY_TELNET_Lo2 in
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

B.

R1

```
interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 access-class DENY_TELNET_Lo2 in
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

C.

R1

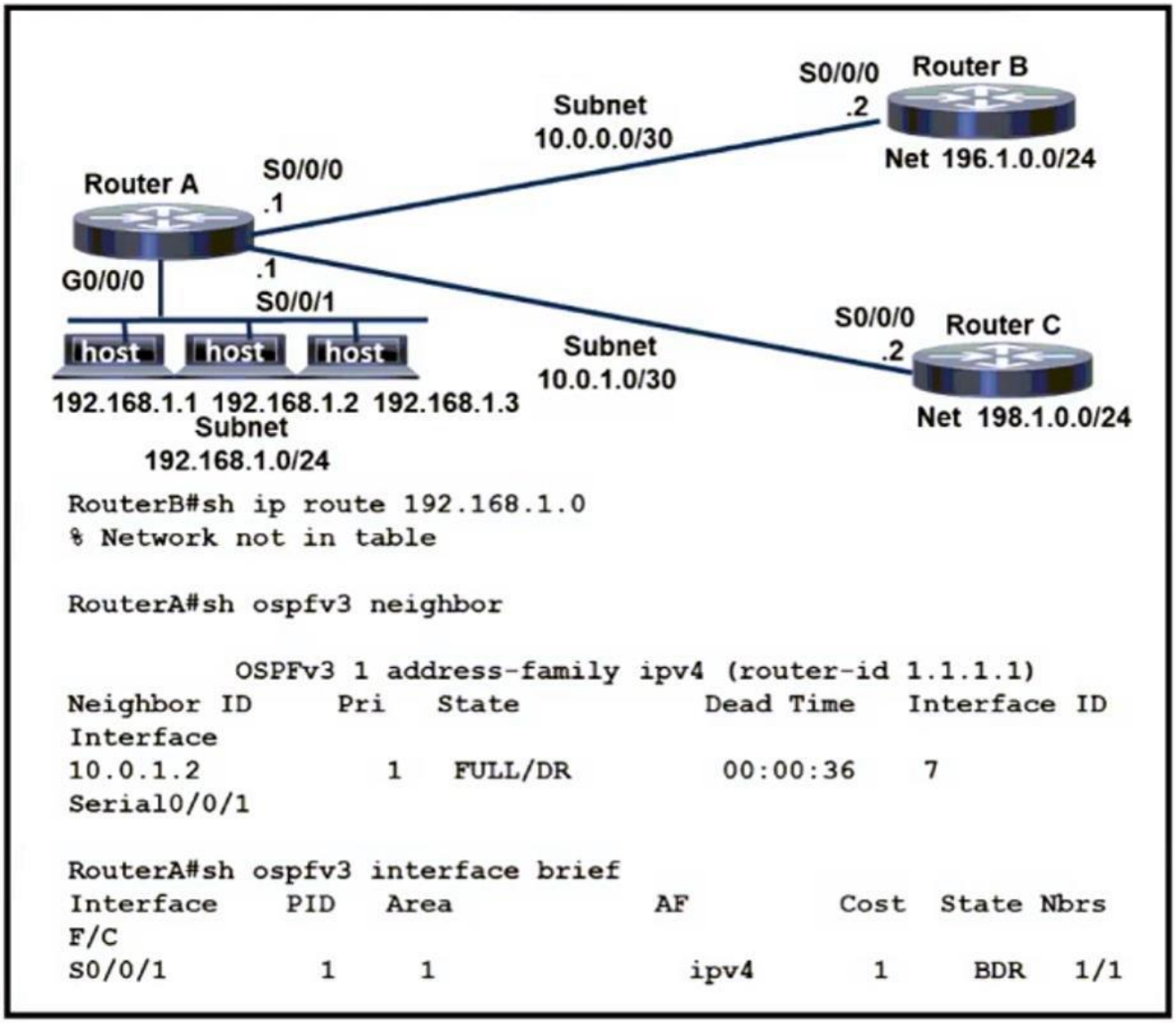
```
Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 ipv6 traffic-filter DENY_TELNET_Lo2 in
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

D.

```
R1
Interface loopback1
 no ip address
 ipv6 address 100A:0:100C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 !
interface Loopback2
 no ip address
 ipv6 address 200A:0:200C::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
!
interface GigabitEthernet0/0
 no ip address
 ipv6 address AB01:2011:8:100::/64 eui-64
 ipv6 enable
 ipv6 ospf network point-to-point
 ipv6 ospf 1 area 0
 !
ipv6 access-list DENY_TELNET_Lo2
 sequence 20 deny tcp host 100B:1:310B::1 host 200A:0:210C::1 eq telnet
 permit ipv6 any any
```

Answer: C

NO.16 Refer to the exhibit. An engineer must advertise LAN network 192.168.1.0 of router A to router B
through OSPF. The engineer notices that router B was configured, but the LAN network of router A is not in the routing table of router B. Which configuration on router A resolves the problem?


S0/0/0
Router B
.2
Subnet
10.0.0.0/30
Net 196.1.0.0/24
Router A
S0/0/0
.1
.1
G0/0/0
S0/0/1
host
host
host
192.168.1.1 192.168.1.2 192.168.1.3
Subnet
192.168.1.0/24
S0/0/0
Router C
.2
Subnet
10.0.1.0/30
Net 198.1.0.0/24
RouterB#sh ip route 192.168.1.0
% Network not in table
RouterA#sh ospfv3 neighbor
OSPFv3 1 address-family ipv4 (router-id 1.1.1.1)
Neighbor ID Pri State Dead Time Interface ID
Interface
10.0.1.2 1 FULL/DR 00:00:36 7
Serial0/0/1
RouterA#sh ospfv3 interface brief
Interface PID Area AF Cost State Nbrs
F/C
S0/0/1 1 1 ipv4 1 BDR 1/1

A.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

B.

```
interface GigabitEthernet0/0/0
 ip address 192.168.1.254 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

interface Serial0/0/0
 ip address 10.0.0.1 255.255.255.0
 negotiation auto
 ipv6 enable
 ospfv3 1 ipv4 area 1

router ospfv3 1
 address-family ipv4 unicast
 router-id 1.1.1.1
 exit-address-family
```

C.

```
interface Serial0/0/0
   ip address 10.0.0.1 255.255.255.0
   negotiation auto
   ipv6 enable
   ospfv3 1 ipv4 area 1

router ospfv3 1
   address-family ipv4 unicast
   area 1 range 192.168.1.0 255.255.255.0
   router-id 1.1.1.1
   exit-address-family
```

D.

```
interface GigabitEthernet0/0/0
   ip address 192.168.1.254 255.255.255.0
   negotiation auto
   ipv6 enable
   ospfv3 1 ipv4 area 1

interface Serial0/0/0
   ip address 10.0.0.1 255.255.255.0
   negotiation auto
   ipv6 enable

router ospfv3 1
   address-family ipv4 unicast
   router-id 1.1.1.1
   exit-address-family
```

Answer: B

NO.17 What is an advantage of using BFD?

A. It detects local link failure at layer 1 and updates routing table.

B. It detects local link failure at layer 2 and updates routing protocols.

C. It has sub-second failure detection for layer 1 and layer 3 problems.

D. It has sub-second failure detection for layer 1 and layer 2 problems.

Answer: D

Explanation:

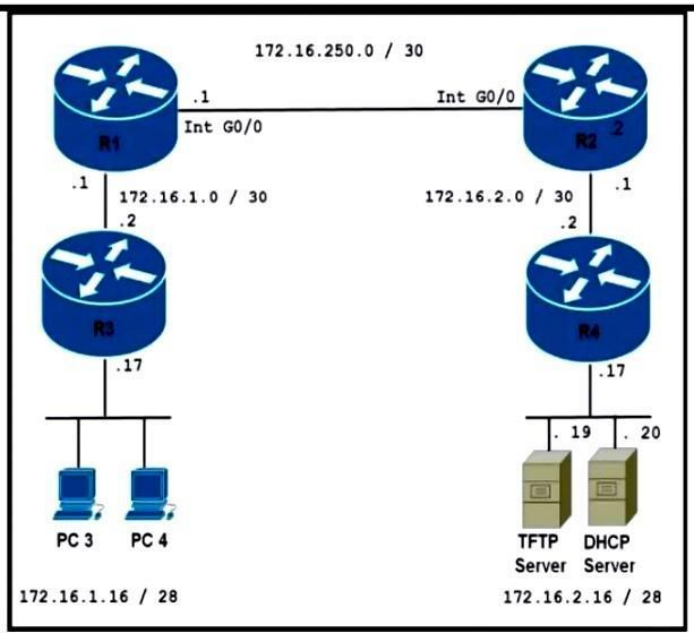
BFD provides rapid, sub-second failure detection independent of the underlying protocol and works across Layer 3, allowing routing protocols to quickly react to both Layer 1 and Layer 3 failures.

NO.18 Which access list entry checks for an ACK within a packet 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
Answer: C

NO.19 Refer to the exhibit. The engineer is trying to transfer the new IOS file to the router R3 but is getting an error. Which configuration achieves the file transfer?

```
R3#sh ip int brie
Interface                  IP-Address      OK? Method Status
Protocol
GigabitEthernet0/0         unassigned      YES NVRAM  administratively
down down
GigabitEthernet0/1         172.16.250.2    YES manual up
up
GigabitEthernet0/2         172.16.250.14   YES manual up
up
GigabitEthernet0/3         172.16.1.17     YES manual up
up
R3#

R3#sh run | begin router eigrp
router eigrp 100
 network 172.16.1.0 0.0.0.3
 network 172.16.1.16 0.0.0.15
!
no ip http server
no ip http secure-server
ip tftp source-interface GigabitEthernet0/3
!
line con 0
line aux 0
line vty 0 4
 login
 transport input none
!
```

```
R4#sh run
!
hostname R4
!
ip cef
!
interface GigabitEthernet0/0
 ip address 172.16.2.2 255.255.255.252
 ip access-group 120 in
!
interface GigabitEthernet0/1
 ip address 172.16.2.17 255.255.255.240
!
router eigrp 100
 network 172.16.2.0 0.0.0.3
 network 172.16.2.16 0.0.0.15
 !
access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq tftp
access-list 120 deny   udp any any eq tftp
access-list 120 permit tcp any any
```

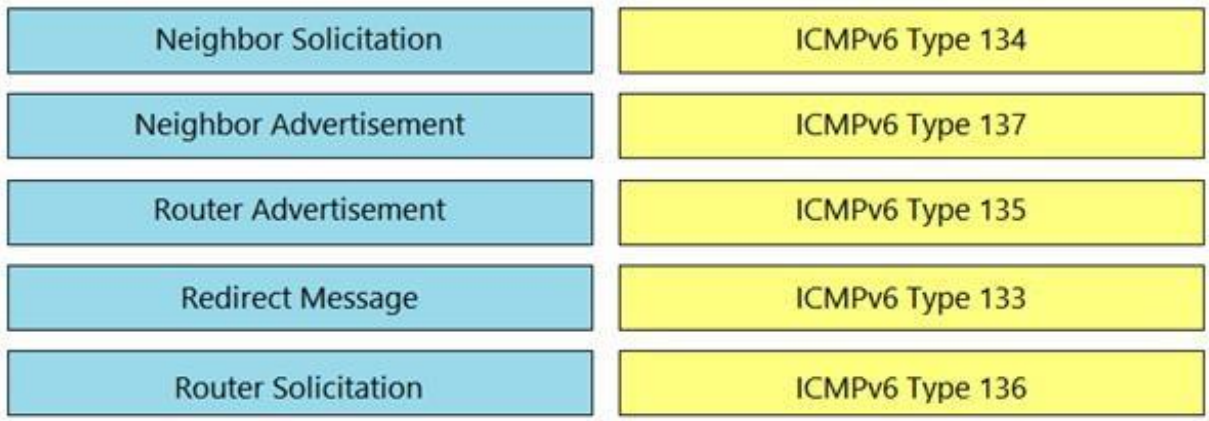


A. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R4(config)#no access-list 120 deny udp any any eq tftp

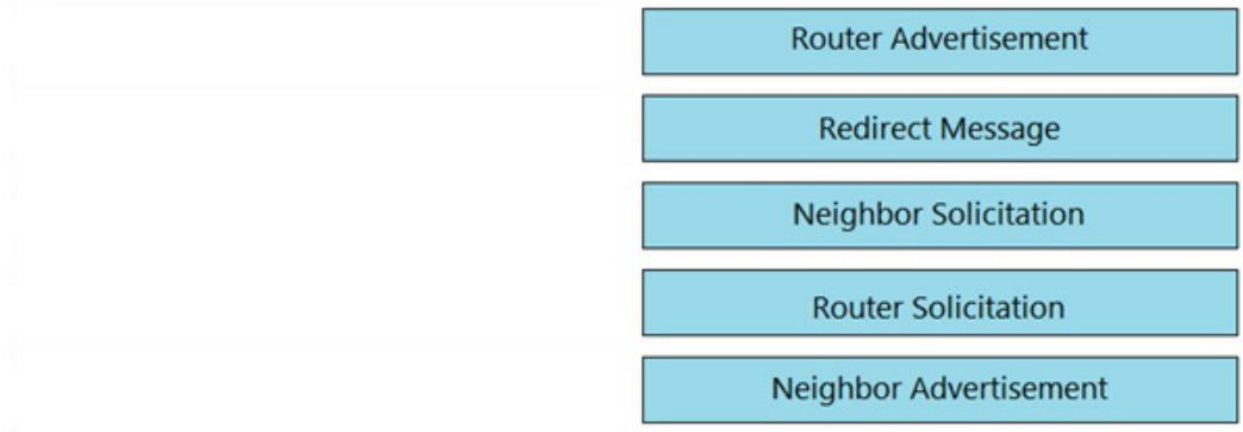
R4(config)#access-list 120 permit tcp any any
B. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit udp host 172.16.1.17 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit tcp any any
C. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R3(config)#no ip tftp source-interface GigabitEthernet0/3
D. R4(config)#no access-list 120 permit udp host 172.16.1.2 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit tcp host 172.16.1.17 host 172.16.2.19 eq 69
R4(config)#access-list 120 permit tcp any any
Answer: B
Explanation:
The issue arises because the current access list on R4 only permits TFTP traffic between 172.16.1.2 and 172.16.2.19 on UDP port 69. However, R3 is using its GigabitEthernet0/3 interface with IP 172.16.1.17 as the source for TFTP transfers.
To resolve this, update the ACL on R4 to permit TFTP traffic from 172.16.1.17 (R3's source IP) to 172.16.2.19 (TFTP server) on UDP port 69. Additionally, ensure that other TCP traffic is permitted for the transfer process by maintaining access-list 120 permit tcp any any. This allows the file transfer from R3 to the TFTP server on R4.

NO.20 Which statement about MPLS LDP router ID is true?
A. The force keyword changes the router ID to the specific address causing any impact.
B. The loopback with the highest IP address is selected as the router ID.
C. If not configured, the operational physical interface is chosen as the router ID even if a loopback is configured.
D. If MPLS LDP router ID must match the IGP router ID.
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4m/mp-ldp-12-4m-book.pdf

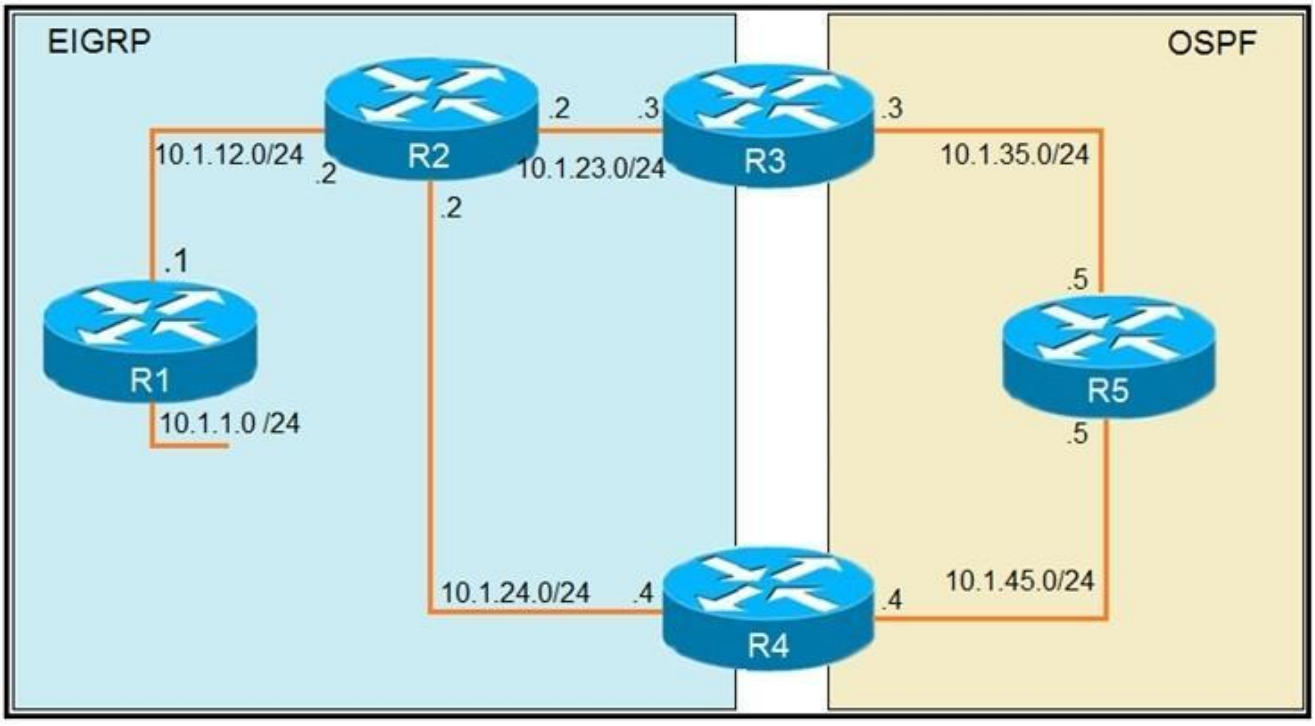
NO.21 Drag and Drop Question
Drag and drop the ICMPv6 neighbor discovery messages from the left onto the correct packet types on the right.

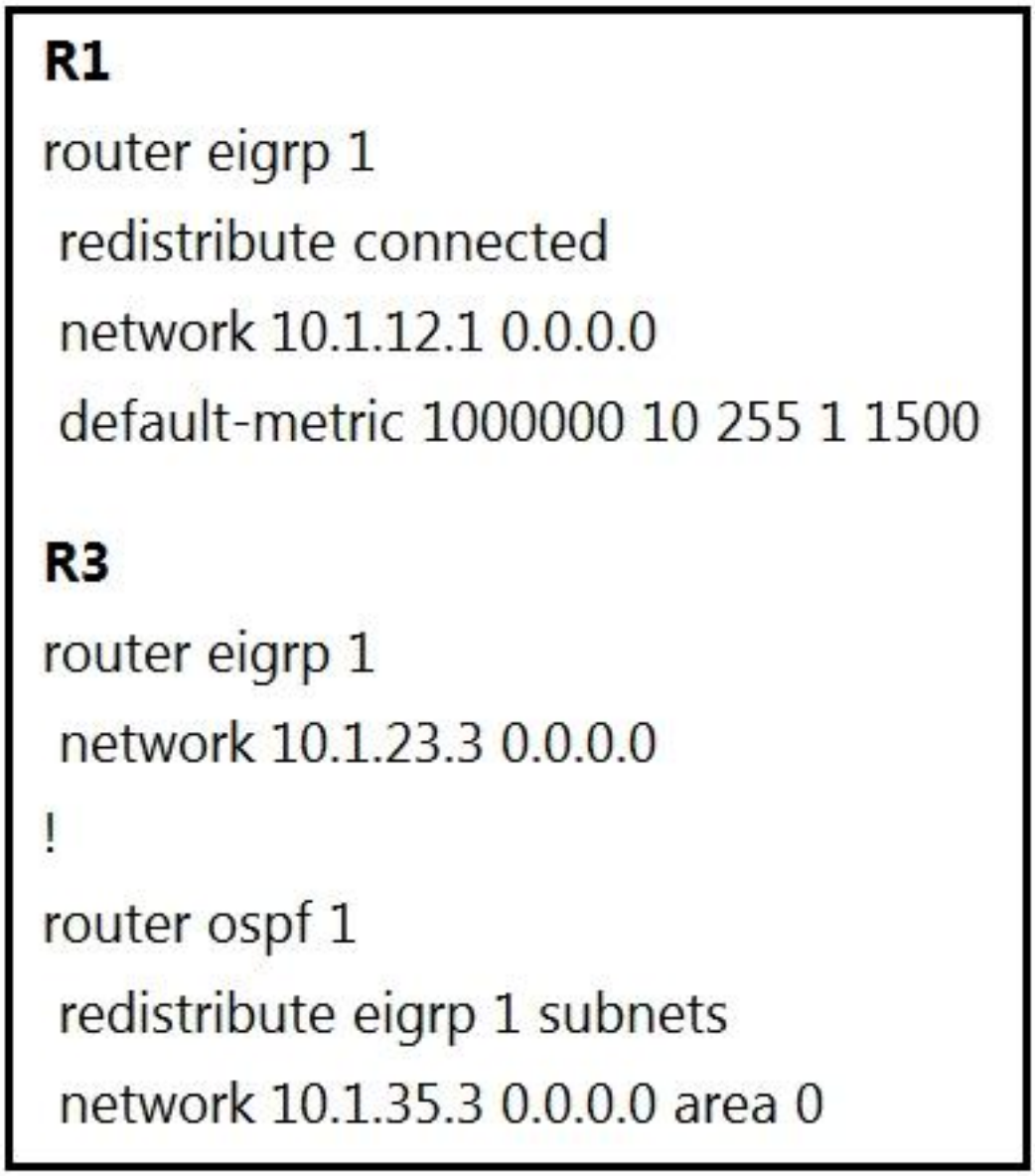


Answer:



NO.22 Refer to the exhibits. To provide reachability to network 10.1.1.0/24 from R5, the network administrator redistributes EIGRP into OSPF on R3 but notices that R4 is now taking a suboptimal path through R5 to reach 10.1.1.0/24 network.
Which action fixes the issue while keeping the reachability from R5 to 10.1.1.0/24 network?





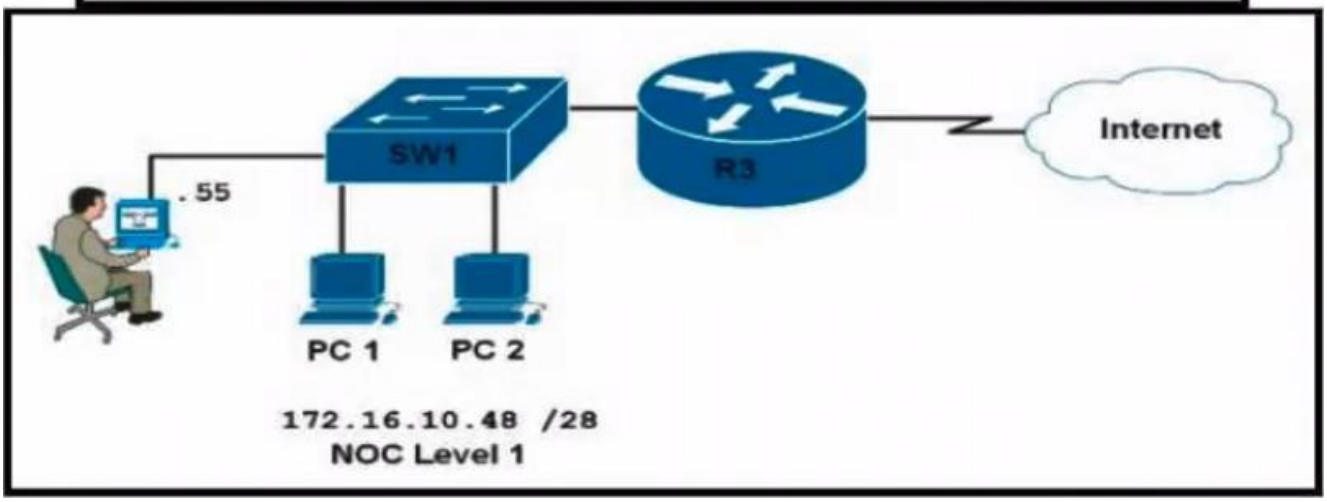
A. Change the administrative distance of the external EIGRP to 90.
B. Apply the outbound distribution list on R5 toward R4 in OSPF.
C. Change the administrative distance of OSPF to 200 on R5.
D. Redistribute OSPF into EIGRP on R4
Answer: A
Explanation:
The subnet 10.1.1.1/24 is redistributed into EIGRP domain so it will have the Administrative Distance (AD) of 170. Therefore R4 also learns about this subnet advertised from R2 with the same AD of 170.
In the other hand, subnet 10.1.1.0/24 is also redistributed into OSPF on R3 so R5 & R4 will learn about this subnet with AD of 110, which is better than the above AD of 170 so R4 will choose path R4 -> R5 -> R3 -> R2 -> R1.
In order to solve this problem, we can configure an outbound distribute list on R5 to prevent (filter out) this subnet from advertising to R4. Then R4 only has one way to reach R1, which is R4 -> R2 - > R1. But this method will remove the backup route so it is not the best solution.
Another solution is to reduce the AD of the external EIGRP to a value smaller than 110. This

method reserves the backup route in case of the main route fails -> This is the best solution. To do this, we can use the following command on R4:
router eigrp 1
distance eigrp 90 91 //Changes the AD to 90 for internal EIGRP routes and changes the AD to 91 for EIGRP external routes
We tested this lab in GNS3 and you can read this lab here. This is the result when we type the "distance eigrp ..." command above on R4:
R4#show ip route
Gateway of last resort is not set
10.0.0.0/24 is subnetted, 6 subnets
D 10.1.12.0 [90/30720] via 10.1.24.2, 00:00:05, FastEthernet0/0 D EX 10.1.1.0 [91/33280] via 10.1.24.2, 00:00:05, FastEthernet0/0 C 10.1.24.0 is directly connected, FastEthernet0/0
D 10.1.23.0 [90/30720] via 10.1.24.2, 00:00:05, FastEthernet0/0 C 10.1.45.0 is directly connected, FastEthernet1/0
O 10.1.35.0 [110/2] via 10.1.45.5, 00:00:11, FastEthernet1/0
Note: We can change the AD of EIGRP routes via the "distance eigrp ..." command but the effect of this command is local only.

NO.23 Which transport layer protocol is used to form LDP sessions?
A. UDP
B. SCTP
C. TCP
D. RDP
Answer: C
Explanation:
LDP uses TCP as a reliable transport for sessions. When multiple LDP sessions are required between two LSRs, there is one TCP session for each LDP session.
Reference: https://tools.ietf.org/html/rfc5036

NO.24 Refer to the exhibit. Which configuration allows the operation level 1 team of 10 engineers to log
in at least three at a time to router R3 using network credentials over HTTP?

```
R3#sh run | begin ip http server
ip http server
ip http access-class 20
ip http authentication local
no ip http secure-server
ip http max-connections 2
!
access-list 20 permit 172.16.10.48 0.0.0.15
!
end
```



A. R3(config)#ip http authentication enable
R3(config)#no access-list 20 permit 172.16.10.48 0.0.0.15
R3(config)#access-list 20 permit 172.16.10.48 0.0.0.7
B. R3(config)#ip http max-connections 3
R3(config)#ip http accounting commands 3 default
C. R3(config)#ip http authentication aaa
R3(config)#ip http max-connections 3
D. R3(config)#ip http authentication aaa
R3(config)#no access-list 20 permit 172.16.10.48 0.0.0.15
R3(config)#access-list 20 permit 172.16.10.48 0.0.0.7
Answer: C

NO.25 Which two components are needed for a service provider to utilize the L3VPN MPLS application?
(Choose two.)
A. The P routers must be configured for MP-iBGP toward the PE routers
B. The P routers must be configured with RSVP.
C. The PE routers must be configured for MP-iBGP with other PE routers
D. The PE routers must be configured for MP-eBGP to connect to CEs
E. The P and PE routers must be configured with LDP or RSVP

Answer: CE
Explanation:
MPLS Network Protocols
+ IGP: OSPF, EIGRP, IS-IS on core facing and core links + RSVP and/or LDP on core and/or core facing links
+ MP-iBGP on PE devices (for MPLS services), MP-BGP: Multiprotocol Border Gateway Protocol, used for MPLS L3 VPN
Reference: https://www.uio.no/studier/emner/matnat/ifi/IN3230/h19/kursmateriell/mpls-lecture.pdf

NO.26 A network engineer needs to verify IP SLA operations on an interface that shows on indication of
excessive traffic. Which command should the engineer use to complete this action?
A. show frequency
B. show track
C. show reachability
D. show threshold
Answer: B

NO.27 Drag and Drop Question
Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.

IPv6 Binding Table	Block reply and advertisement messages from unauthorized DHCP servers and relay agents
IPv6 DHCPv6 Guard	Create a binding table that is based on NS and NA messages
IPv6 Source Guard	Filter inbound traffic on Layer 2 switch port that are not in the IPv6 binding table
IPv6 ND Inspection	Block a malicious host and permit the router from a legitimate route
IPv6 RA Guard	Create IPv6 neighbors connected to the device from information sources such as NDP snooping

Answer:

Explanation:
The DHCPv6 Guard feature blocks DHCP reply and advertisement messages that originate from unauthorized DHCP servers and relay agents that forward DHCP packets from servers to clients. Client messages or messages sent by relay agents from clients to servers are not blocked.
IPv6 ND Inspection creates a binding table that is based on NS (Neighbor Solicitation) and NA (Neighbor Advertisement) messages. The switch then uses this table to check any future NS/NA messages. When the IPv6-LLA combination does not match, it drops the message. This only applies to NS/NA messages, it doesn't drop any actual data packets that have a spoofed IPv6 or MAC address.
IPv6 Source Guard filters inbound traffic on L2 switch ports that are not in the IPv6 binding table. The binding table stores the following information:
+ IPv6 address
+ MAC address
+ VLAN
+ Interface ID
Source Guard only looks at information found in the binding table, and it doesn't fill the binding table.
The IPv6 RA Guard feature provides support for allowing the network administrator to block or reject unwanted or rogue RA guard messages that arrive at the network device platform. RAs are used by devices to announce themselves on the link. The IPv6 RA Guard feature analyzes these RAs and filters out RAs that are sent by unauthorized devices.

NO.28 The network administrator configured CoPP so that all HTTP and HTTPS traffic from the administrator device located at 172.16.1.99 toward the router CPU is limited to 500 kbps. Any traffic that exceeds this limit must be dropped.
access-list 100 permit ip host 172.16.1.99 any
!
class-map CM-ADMIN
match access-group 100
!
policy-map PM-COPP
class CM-ADMIN
police 500000 conform-action transmit

!
interface E0/0
service-policy input PM-COPP
CoPP failed to capture the desired traffic and the CPU load is getting higher.
Which two configurations resolve the issue? (Choose two.)
A. interface E0/0
no service-policy input PM-COPP
!
control-plane
service-policy input PM-COPP
B. policy-map PM-COPP
class CM-ADMIN
no police 500000 conform-action transmit
police 500 conform-action transmit
!
control-plane
service-policy input PM-COPP
C. no access-list 100
access-list 100 permit tcp host 172.16.1.99 any eq 80
D. no access-list 100
access-list 100 permit tcp host 172.16.1.99 any eq 80
access-list 100 permit tcp host 172.16.1.99 any eq 443
E. policy-map PM-COPP
class CM-ADMIN
no police 500000 conform-action transmit
police 500 conform-action transmit
Answer: A

NO.29 With Internal BGP, there is a requirement for all peers to be logically fully meshed, where all IBGP routers must peer with all other IBGP routers. For scaling purposes, there are two mechanisms that were developed to bypass this requirement. What are they? (Choose two.)
A. Confederations
B. IBGP to EBGP route redistribution
C. BGP peer filtering
D. Route reflectors.
Answer: AD

NO.30 Refer to the exhibit. An engineer must troubleshoot an issue with the aaa authentication that affected the user's login to router R1. Which command allows the configured user to authenticate?

A. aaa authentication login default group radius local

B. aaa authentication login default group radius tacacs+

C. aaa authentication login default group tacacs+

D. aaa authentication login default group radius

Answer: C

Explanation:

The debug log shows an "Invalid AUTHEN packet (check keys)" error, which indicates a mismatch between the shared key configured on the router and the TACACS+ server. Once the shared key is corrected on both the TACACS+ server and the router, the appropriate AAA authentication method must be applied.

The correct command is aaa authentication login default group tacacs+, which specifies that the router should use TACACS+ for authentication. If TACACS+ is the intended authentication method and the shared key is properly configured, this command ensures that the user can successfully log in to the router using TACACS+.

NO.31 What are two MPLS label characteristics? (Choose two.)

A. The label edge router swaps labels on the received packets.

B. Labels are imposed in packets after the Layer 3 header.

C. LDP uses TCP for reliable delivery of information.

D. An MPLS label is a short identifier that identifies a forwarding equivalence class.

E. A maximum of two labels can be imposed on an MPLS packet.

Answer: CD

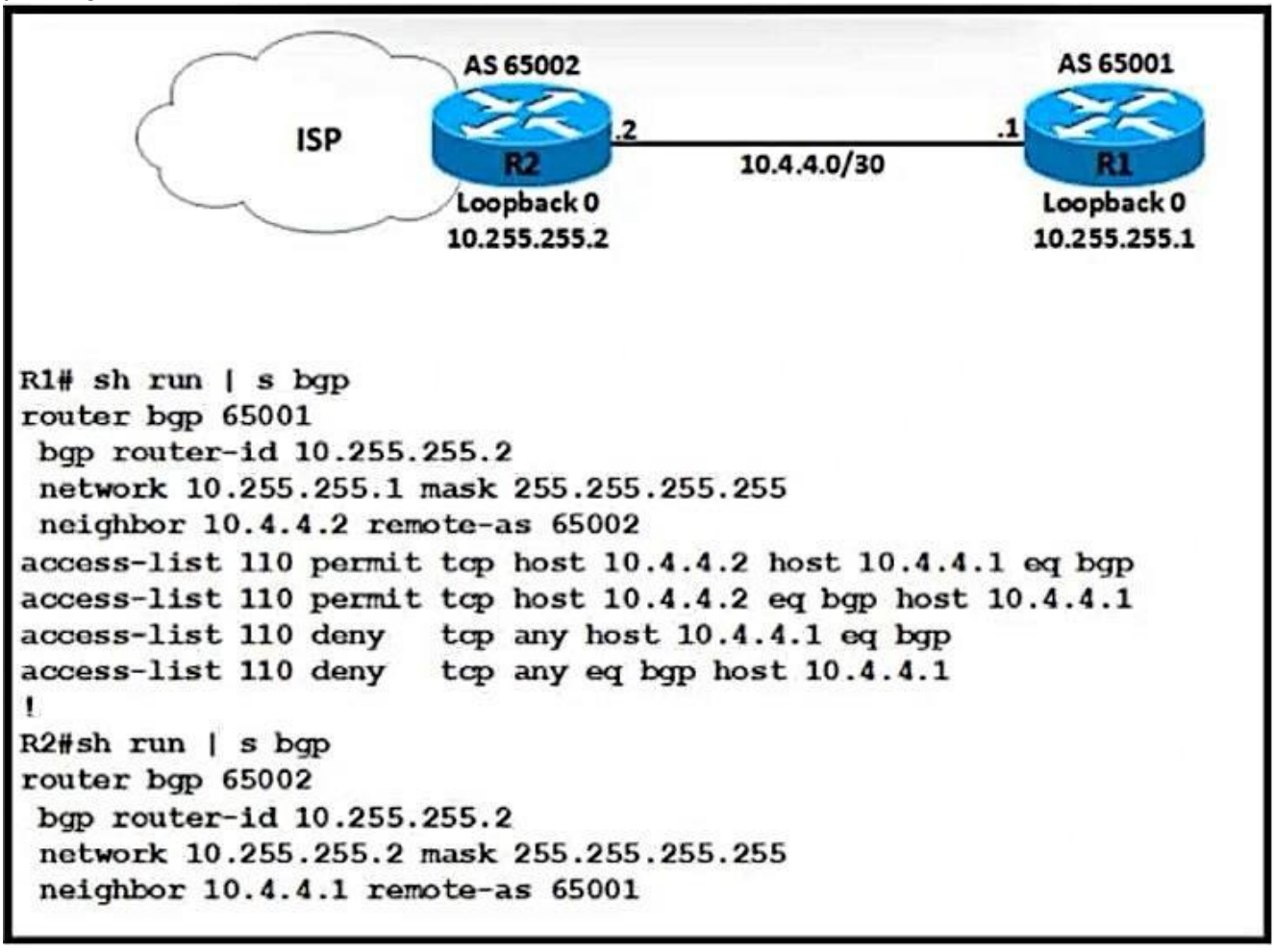
Explanation:

A label edge router (LER, also known as edge LSR) is a router that operates at the edge of an MPLS network and acts as the entry and exit points for the network. LERs push an MPLS label

onto an incoming packet and pop it off an outgoing packet.
MPLS labels are added between the Layer 2 and the Layer 3 header in the packets (-> Therefore MPLS labels are added before Layer 3 header).
There are no limit on the number of labels in a stack.
A label is a short, four-byte, fixed-length, locally-significant identifier which is used in order to identify a Forwarding Equivalence Class (FEC). The label which is put on a particular packet represents the FEC to which that packet is assigned.
LDP uses TCP as a reliable transport for sessions. Each TCP connection has only one LDP session.
Reference: https://www.cisco.com/c/en/us/support/docs/multiprotocol-label-switching-mpls/mpls/4649-mpls-faq-4649.html

NO.32 What is the downstream unsolicited distribution method in MPLS?
A. It advertises labels to peers only when the peer requests.
B. It sends a unicast hello message to a specific LSR.
C. It sends a unicast hello message to a specific LER.
D. It advertises labels to peers without peer request.
Answer: D

NO.33 Refer to the exhibit. A network engineer notices that R1 and R2 cannot establish an eBGP peering.



The following messages appear in the log:

```
*Dec 21 12:08:59.991: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x6A8B3998:1) NSF delete stale NSF not active
*Dec 21 12:08:59.995: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x44361063:8) NSF no stale paths state is NSF not active
*Dec 21 12:08:59.995: BGP: br topo global 10.4.4.2 IPv4 Unicast:base (0x6A8B3998:1) Resetting ALL counters.
*Dec 21 12:09:09.819: BG-3-NOTIFICATION: sent to neighbor 10.4.4.2 passive 2/3 (BGP identifier wrong) 4 bytes OAFFFF02
*Dec 21 12:09:09.823: BGP-4-MSGDUMP: unsupported or mal-formatted message received from 10.4.4.2:
*Dec 21 12:09:12.443: 8BGP SESSION-5-ADJCHANGE: neighbor 10.4.4.2 IPv4 Unicast topology base removed from session BGP Notification received
*Dec 21 12:09:00.191: BGP: br global 10.4.4.2 Open active delayed 12288ms (35000ms max, 60% jitter)
```

Which configuration must the engineer apply to R1 to restore the eBGP peering?

A.

```
router bgp 65001
  bgp router-id 10.255.255.1
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit udp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit udp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny udp any host 10.4.4.1 eq 179
access-list 110 deny udp any eq 179 host 10.4.4.1
```

B.

```
router bgp 65001
  bgp router-id 10.255.255.2
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit tcp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit tcp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny tcp any host 10.4.4.1 eq 179
access-list 110 deny tcp any eq 179 host 10.4.4.1
```

C.

```
router bgp 65001
  bgp router-id 10.255.255.2
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit udp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit udp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny udp any host 10.4.4.1 eq 179
access-list 110 deny udp any eq 179 host 10.4.4.1
```

D.

```
router bgp 65001
  bgp router-id 10.255.255.1
  neighbor 10.4.4.2 remote-as 65002
access-list 110 permit tcp host 10.4.4.2 host 10.4.4.1 eq 179
access-list 110 permit tcp host 10.4.4.2 eq 179 host 10.4.4.1
access-list 110 deny   tcp any host 10.4.4.1 eq 179
access-list 110 deny   tcp any eq 179 host 10.4.4.1
```

Answer: D

NO.34 An administrator wants to implement security on his company's router. Please select three options that you will use on your router to secure it. (Choose three.)

A. Control Access to the router

B. Restrict all traffic through the router

C. Restrict SNMP

D. Enable all unused services
E. Encrypt all passwords
F. Disable logging
Answer: ACE

NO.35 Refer to the exhibit. The static route is not present in the routing table of an adjacent OSPF neighbor router. Which action resolves the issue?

```
ip prefix-list DMZ-STATIC seq 5 permit 10.1.1.0/24
!
route-map DMZ permit 10
     match ip addresss prefix-list DMZ-STATIC
!
router ospf 1
network 0.0.0.0 0.0.0.0 area 0
redistribute static route-map DMZ
!
ip route 10.1.1.0 255.255.255.0 10.20.20.1
```

A. Configure the next hop of 10.20.20.1 in the prefix list DMZ-STATIC
B. Configure the next-hop interface at the end of the static router for it to get redistributed
C. Configure a permit 20 statement to the route map to redistribute the static route
D. Configure the subnets keyword in the redistribution command
Answer: D
Explanation:
When you include the subnets keyword, the OSPF redistributes the routes, which are subnetted. The process uses 20 as the default metric. This happens when no metric is specified by the use of the metric-type keyword.