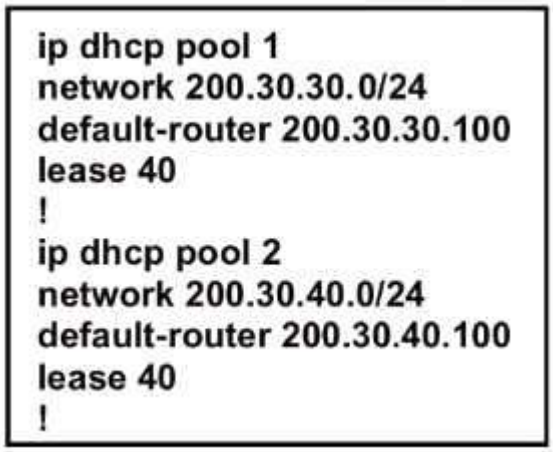
- **Vendor:** Cisco
- **Exam Code:** 300-410
- **Exam Name:** Implementing Cisco Enterprise Advanced Routing and Services (ENARSI)
- **New Updated Questions from Braindump2go (Updated in Jan./2021)**

**QUESTION 125**
Refer to the exhibit. The server for the finance department is not reachable consistently on the 200.30.40.0/24 network and after every second month it gets a new IP address.



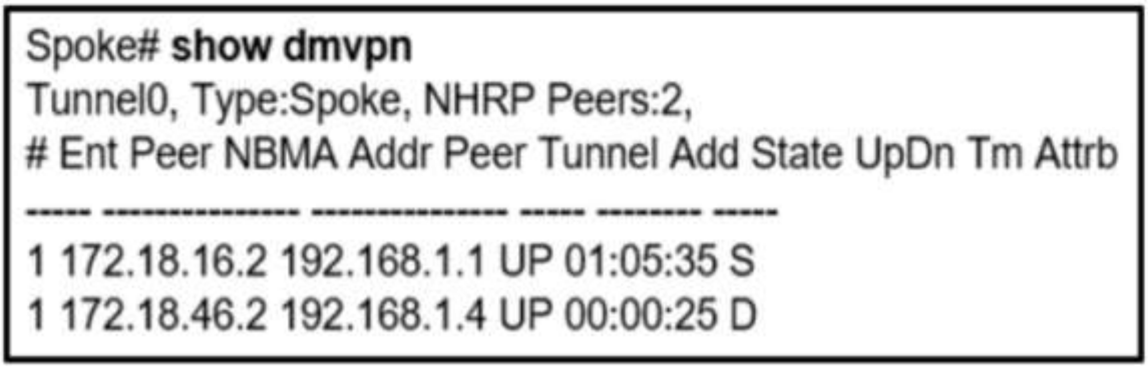
```
ip dhcp pool 1
network 200.30.30.0/24
default-router 200.30.30.100
lease 40
!
ip dhcp pool 2
network 200.30.40.0/24
default-router 200.30.40.100
lease 40
!
```

Which two actions must be taken to resolve this Issue? (Choose two.)

A. Configure the server to use DHCP on the network with default gateway 200 30.40.100.
B. Configure the server with a static IP address and default gateway.
C. Configure the router to exclude a server IP address.
D. Configure the server to use DHCP on the network with default gateway 200 30.30.100.
E. Configure the router to exclude a server IP address and default gateway.

**Answer:** BC

**QUESTION 126**
Refer to the exhibit. An engineer has configured DMVPN on a spoke router.



```
Spoke# show dmvpn
Tunnel0, Type:Spoke, NHRP Peers:2,
# Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
----- --------------- --------------- ----- -------- -----
1 172.18.16.2 192.168.1.1 UP 01:05:35 S
1 172.18.46.2 192.168.1.4 UP 00:00:25 D
```

What is the WAN IP address of another spoke router within the DMVPN network?

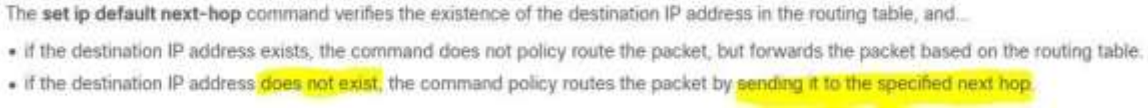
A. 172.18.46.2
B. 192.168.1.4
C. 172.18.16.2
D. 192.168.1.1

**Answer:** A

**QUESTION 127**
An engineer is configuring a network and needs packets to be forwarded to an interface for any destination address that is not in the routing table.
What should be configured to accomplish this task?

A. set ip next-hop
B. set ip default next-hop
C. set ip next-hop recursive
D. set ip next-hop verify-availability

**Answer:** B
**Explanation:**



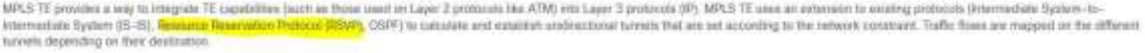
The **set ip default next-hop** command verifies the existence of the destination IP address in the routing table, and...

- if the destination IP address exists, the command does not policy route the packet, but forwards the packet based on the routing table.
- if the destination IP address does not exist, the command policy routes the packet by sending it to the specified next hop.

**QUESTION 128**
Which protocol does MPLS use to support traffic engineering?

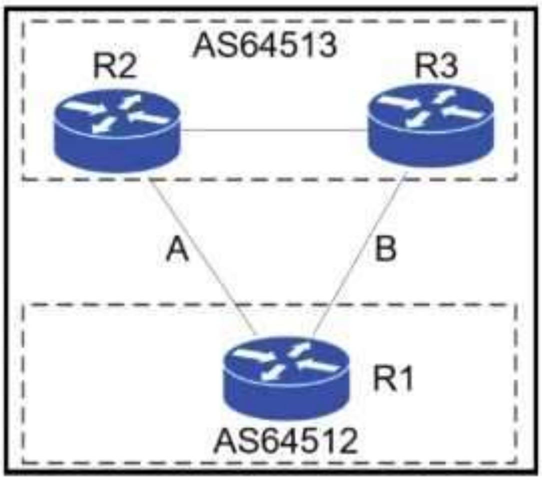
A. Tag Distribution Protocol
B. Resource Reservation Protocol
C. Border Gateway Protocol
D. Label Distribution Protocol

**Answer:** B
**Explanation:**



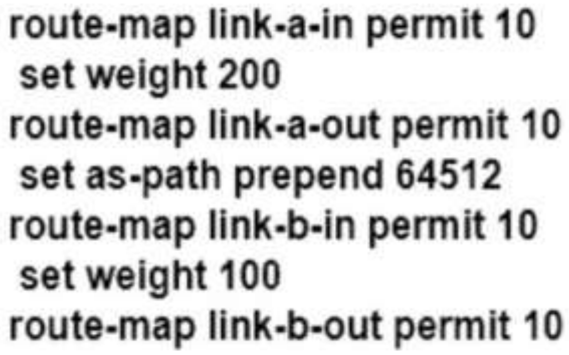
MPLS TE provides a way to integrate TE capabilities (such as those used on Layer 2 protocols like ATM) into Layer 3 protocols (IP). MPLS TE uses an extension to existing protocols (Intermediate System-to-Intermediate System (IS-IS), Resource Reservation Protocol (RSVP), OSPF) to calculate and establish unidirectional tunnels that are set according to the network constraint. Traffic flows are mapped on the different tunnels depending on their destination.

**QUESTION 129**
Refer to the exhibit. A network engineer for AS64512 must remove the inbound and outbound traffic from link A during maintenance without closing the BGP session so that there . ........... a backup link over link A toward the ASN.



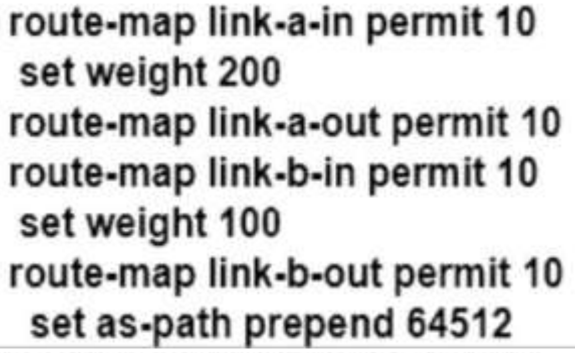
Which BGP configuration on R1 accomplishes this goal?

A.



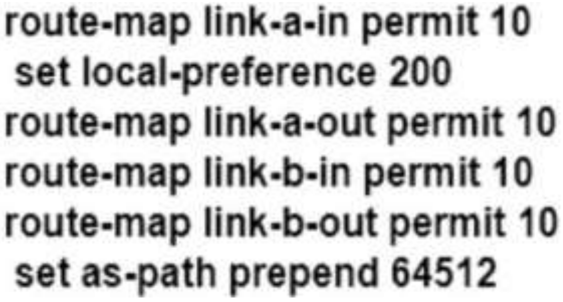
```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
```

B.



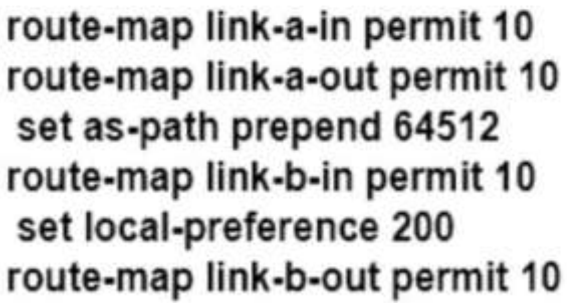
```
route-map link-a-in permit 10
 set weight 200
route-map link-a-out permit 10
route-map link-b-in permit 10
 set weight 100
route-map link-b-out permit 10
  set as-path prepend 64512
```

C.



```
route-map link-a-in permit 10
 set local-preference 200
route-map link-a-out permit 10
route-map link-b-in permit 10
route-map link-b-out permit 10
 set as-path prepend 64512
```

D.

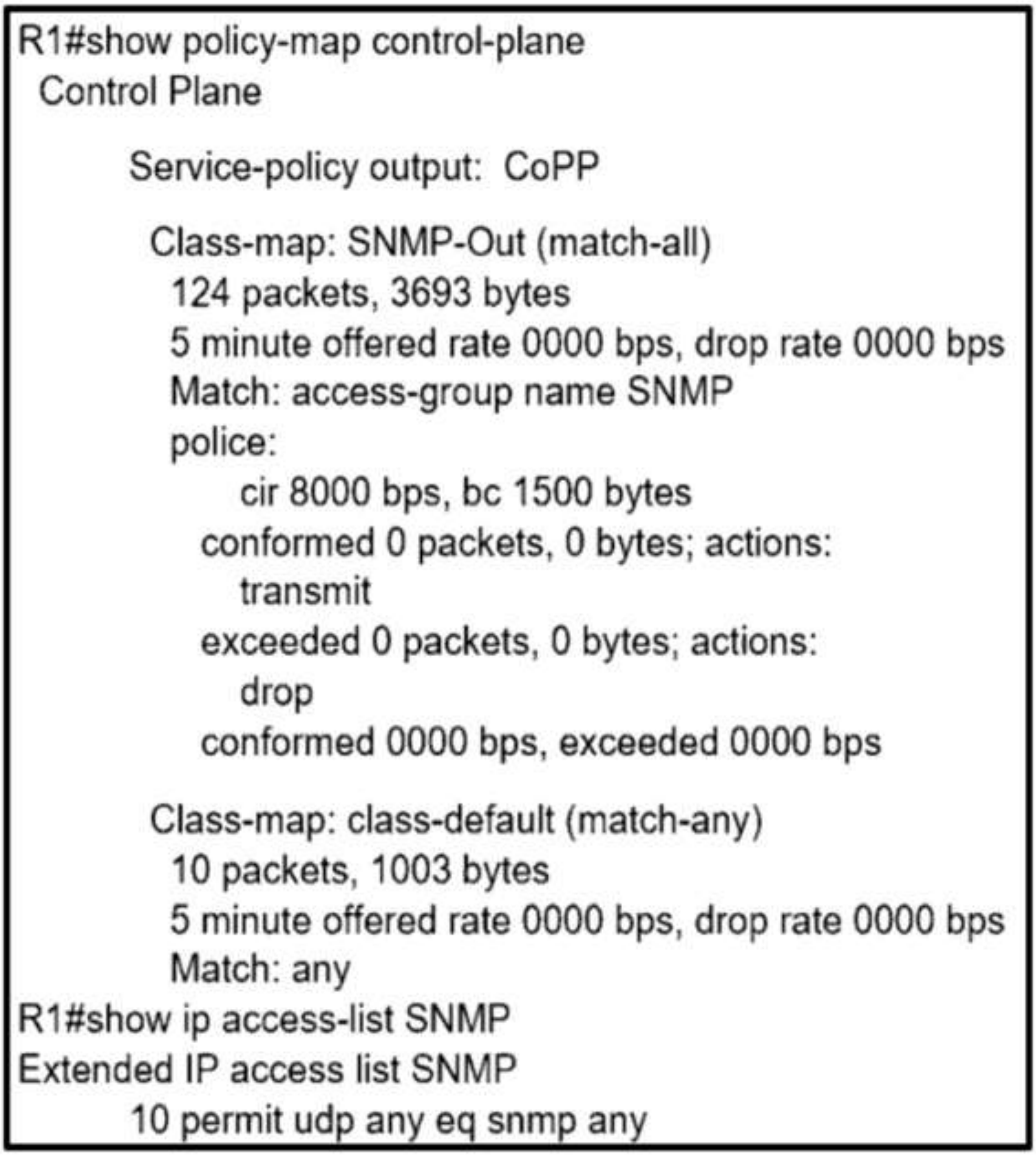


```
route-map link-a-in permit 10
route-map link-a-out permit 10
 set as-path prepend 64512
route-map link-b-in permit 10
 set local-preference 200
route-map link-b-out permit 10
```

**Answer:** D

**QUESTION 130**

Refer to the exhibit. R1 is being monitored using SNMP and monitoring devices are getting only partial information. What action should be taken to resolve this issue?

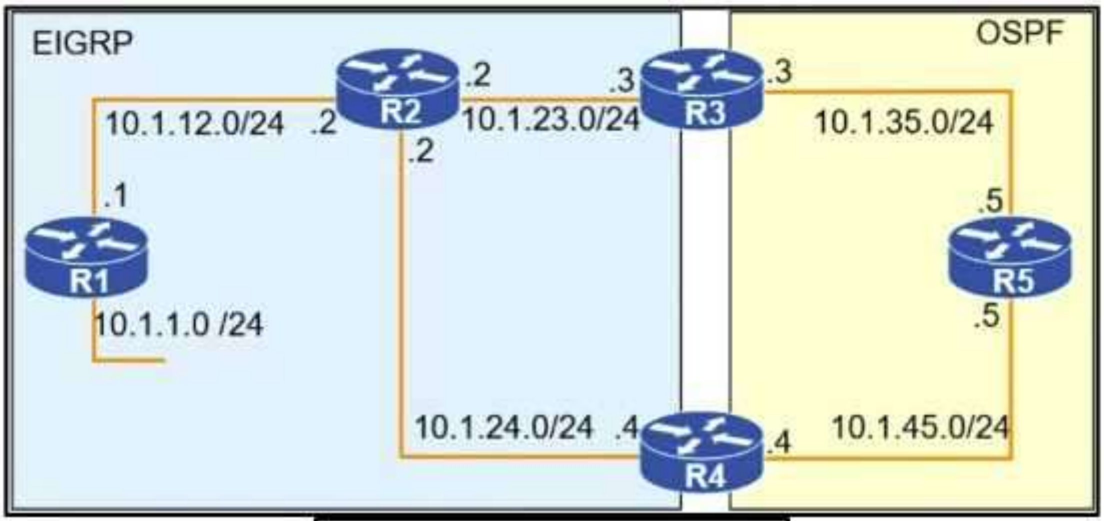


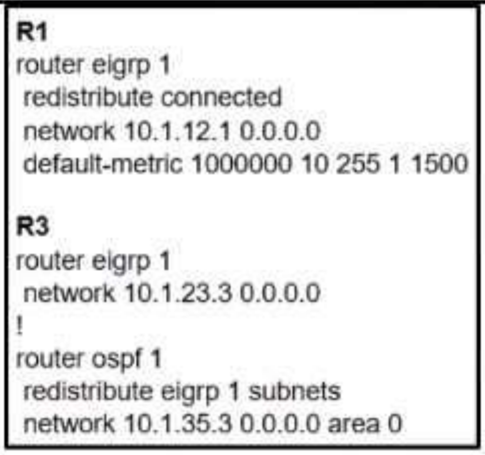
```
R1#show policy-map control-plane
 Control Plane

     Service-policy output:  CoPP

      Class-map: SNMP-Out (match-all)
       124 packets, 3693 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
       Match: access-group name SNMP
       police:
           cir 8000 bps, bc 1500 bytes
         conformed 0 packets, 0 bytes; actions:
           transmit
         exceeded 0 packets, 0 bytes; actions:
           drop
         conformed 0000 bps, exceeded 0000 bps

      Class-map: class-default (match-any)
       10 packets, 1003 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
       Match: any
R1#show ip access-list SNMP
Extended IP access list SNMP
     10 permit udp any eq snmp any
```

A. Modify the CoPP policy to increase the configured exceeded limit for SNMP.
B. Modify the access list to include snmptrap.
C. Modify the CoPP policy to increase the configured CIR limit for SNMP.
D. Modify the access list to add a second line to allow udp any any eq snmp.

**Answer:** B

**QUESTION 131**
Refer to the exhibit. 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 ........... 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?



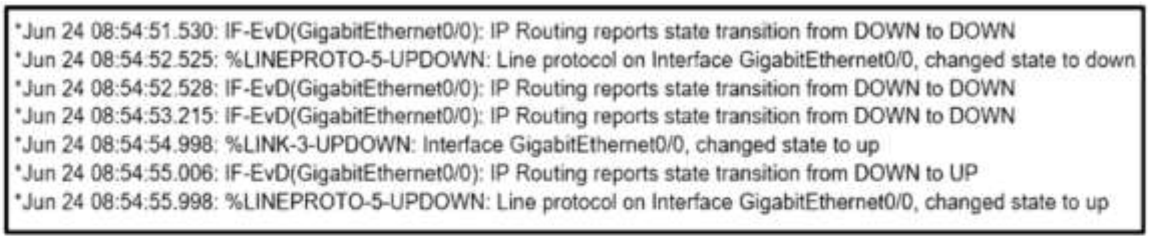


```
R1
router eigrp 1
 redistribute connected
 network 10.1.12.1 0.0.0.0
 default-metric 1000000 10 255 1 1500

R3
router eigrp 1
 network 10.1.23.3 0.0.0.0
!
router ospf 1
 redistribute eigrp 1 subnets
 network 10.1.35.3 0.0.0.0 area 0
```

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.

**Answer:** A

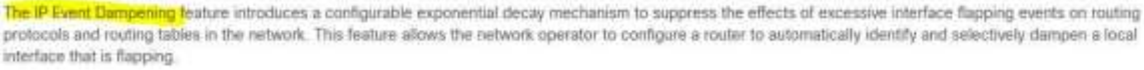
**QUESTION 132**
Refer to the exhibit. R1 is connected with R2 via GigabitEthernet0/0, and R2 cannot ping R1. What action will fix the issue?



```
*Jun 24 08:54:51.530: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:52.525: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to down
*Jun 24 08:54:52.528: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:53.215: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to DOWN
*Jun 24 08:54:54.998: %LINK-3-UPDOWN: Interface GigabitEthernet0/0, changed state to up
*Jun 24 08:54:55.006: IF-EvD(GigabitEthernet0/0): IP Routing reports state transition from DOWN to UP
*Jun 24 08:54:55.998: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
```

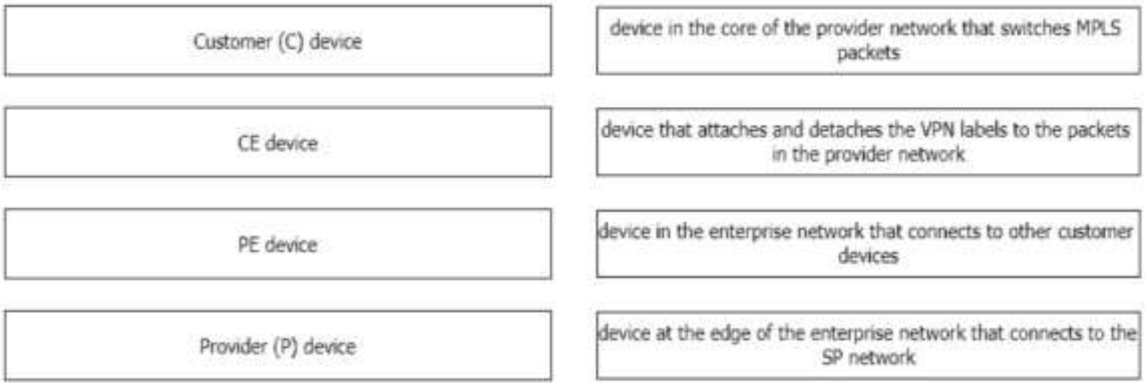
A. Fix route dampening configured on the router.
B. Replace the SFP module because it is not supported.
C. Fix IP Event Dampening configured on the interface.
D. Correct the IP SLA probe that failed.

**Answer:** C
**Explanation:**



The IP Event Dampening feature introduces a configurable exponential decay mechanism to suppress the effects of excessive interface flapping events on routing protocols and routing tables in the network. This feature allows the network operator to configure a router to automatically identify and selectively dampen a local interface that is flapping.

**QUESTION 133**
Drag and Drop Question
Drag and drop the MPLS VPN device types from me left onto the definitions on the right.



Customer (C) device

CE device

PE device

Provider (P) device

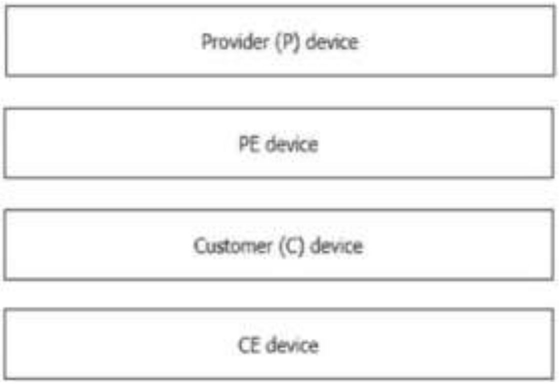
device in the core of the provider network that switches MPLS packets

device that attaches and detaches the VPN labels to the packets in the provider network

device in the enterprise network that connects to other customer devices

device at the edge of the enterprise network that connects to the SP network

**Answer:**



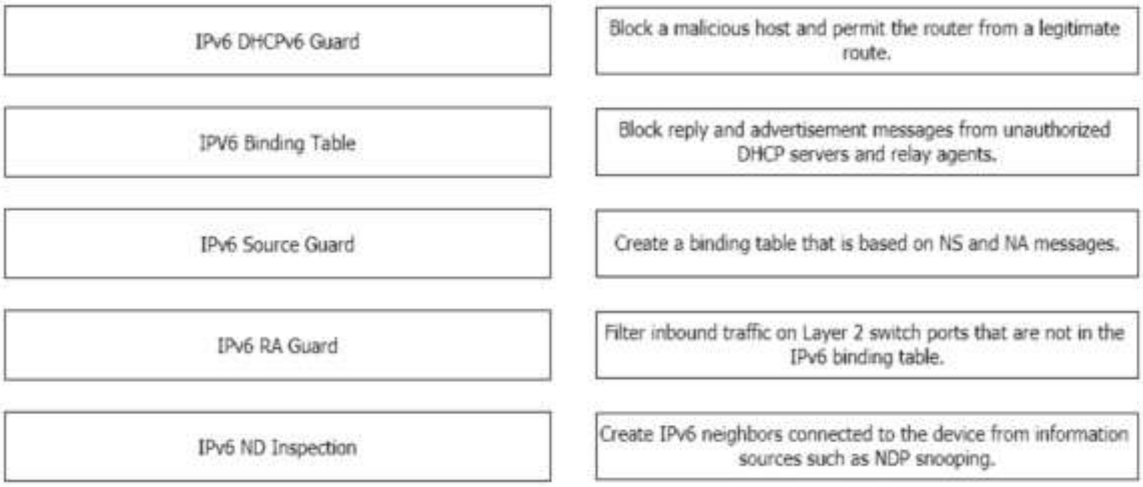
Provider (P) device

PE device

Customer (C) device

CE device

**QUESTION 134**
Drag and Drop Question
Drag and Drop the IPv6 First-Hop Security features from the left onto the definitions on the right.



IPv6 DHCPv6 Guard

IPV6 Binding Table

IPv6 Source Guard

IPv6 RA Guard

IPv6 ND Inspection

Block a malicious host and permit the router from a legitimate route.

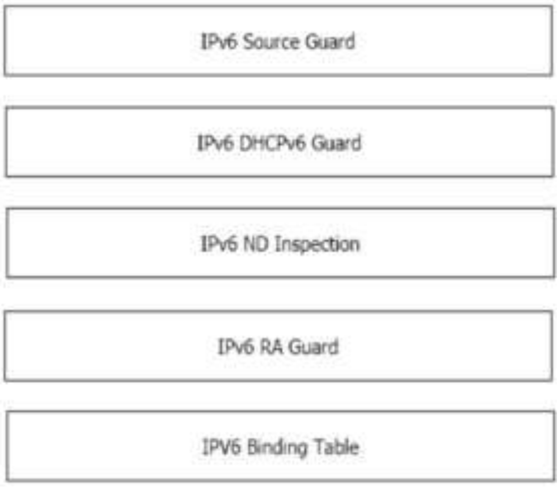
Block reply and advertisement messages from unauthorized DHCP servers and relay agents.

Create a binding table that is based on NS and NA messages.

Filter inbound traffic on Layer 2 switch ports that are not in the IPv6 binding table.

Create IPv6 neighbors connected to the device from information sources such as NDP snooping.

**Answer:**



IPv6 Source Guard

IPv6 DHCPv6 Guard

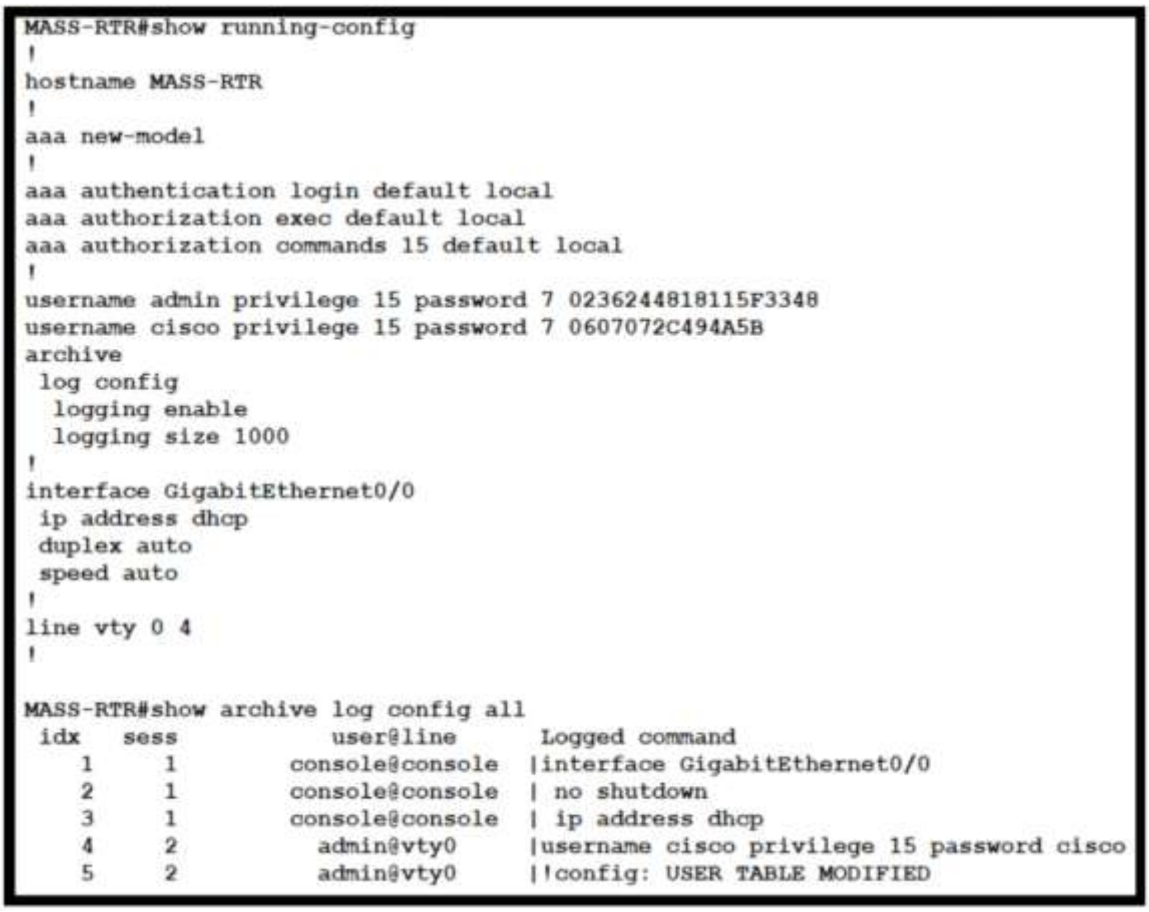
IPv6 ND Inspection

IPv6 RA Guard

IPV6 Binding Table

**QUESTION 135**

Refer to the exhibit. A client is concerned that passwords are visible when running this show archive **log config all.**



```
MASS-RTR#show running-config
!
hostname MASS-RTR
!
aaa new-model
!
aaa authentication login default local
aaa authorization exec default local
aaa authorization commands 15 default local
!
username admin privilege 15 password 7 0236244818115F3348
username cisco privilege 15 password 7 0607072C494A5B
archive
 log config
  logging enable
  logging size 1000
!
interface GigabitEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
line vty 0 4
!

MASS-RTR#show archive log config all
 idx   sess          user@line      Logged command
    1     1        console@console  |interface GigabitEthernet0/0
    2     1        console@console  | no shutdown
    3     1        console@console  | ip address dhcp
    4     2          admin@vty0     |username cisco privilege 15 password cisco
    5     2          admin@vty0     |!config: USER TABLE MODIFIED
```

Which router configuration is needed to resolve this issue?

A. MASS-RTR(config-archive-log-cfg)#hidekeys
B. MASS-RTR(config-archive-log-cfg)#password encryption aes
C. MASS-RTR(config)#service password-encryption
D. MASS-RTR(config)#aaa authentication arap

**Answer:** C